



Launch Remote Windows Apps

PAExec lets you launch Windows programs on remote Windows computers without needing to install software on the remote computer first. For example, you could launch CMD.EXE remotely and have the equivalent of a terminal session to the remote server. PAExec is useful for doing remote installs, checking remote configuration, etc.

PAExec - The Redistributable PsExec

Microsoft's [PsExec](#) tool (originally by SysInternal's Mark Russinovich) is a favorite of system administrators everywhere. It just has one tiny flaw: Microsoft will not allow PsExec to be redistributed.

We needed something that we could ship, and not finding a suitable replacement, decided to write our own.

Anyone can download and use PAExec. You can include it in your open source, freeware and even commercial applications. You may distribute it on your website, on CDs, mail to friends, etc. There is no cryptography built in so there aren't any export restrictions that we know of. See the [License](#) for all the legalese.

[Update: When we wrote PAExec, PsExec was not encrypting data sent across the network, so command lines, credentials, etc. would be sent in plain text. PAExec didn't either, but it did do a simple XOR scrambling of the data, so it was a tiny bit safer. As of version 2.1, PsExec now DOES encrypt data sent across the network.]

Is PAExec Malware?



PAExec is a utility program that system administrators in IT use to do their work. As mentioned above, it is very similar to Microsoft's free PsExec utility. Unfortunately, like most tools, it can be used for good or bad, and some malware authors include PAExec and/or PsExec in their malware. Because of this, both PAExec and PsExec sometimes get mislabeled as malware. If this happens to you, you can submit a report to your security software vendor and tell them they have a false report and point them to this page.

PAExec is used daily by IT personnel, and it is included in many legitimate products, including our software. Neither PAExec nor PsExec get around any operating system security procedures - they are simply using documented APIs to accomplish their job. There are other similar tools and source code available that do the same thing.

How to Remove PAExec

If you are here because you found PAExec on your computer, it is most likely part of a legitimate software package (ours, or from many other vendors). Some companies use this utility to update drivers for example.

PAExec is self-contained and doesn't use an installer. You can simply delete PAExec.exe. This might cause issues with whatever other product was using it. We don't have any idea who uses PAExec - it is free on the Internet so any company can download it and use it in their products, which is also how Microsoft's PsExec is distributed.

DOWNLOAD PAEXEC V1.29

SHA1:

0FC135B131D0BB47C9A0AAF02490701303B76D3B

Source code is available on GitHub at <https://github.com/poweradminllc/PAExec>

Examples

```
PAExec \\{server IP address} -s cmd.exe
```

Creates a telnet-like session on the remote server, running as Local System.

```
PAExec \\{server IP address} ipconfig
```

View network configuration on the remote server without needing to do an RDP session.

```
PAExec \\{server IP address} -u {username} -p {password} -i -c MyApp.exe
```

Copy MyApp.exe to the remote server and run it as {username} so that it shows up on the remote server.

Usage

PAExec uses the same command-line options as PsExec, plus a few additional options of its own. Run PAExec.exe /? to see a list of supported options, which are also shown below:

PAExec is a freely-redistributable re-implementation of SysInternal/Microsoft's popular PsExec program. PAExec aims to be a drop in replacement for PsExec, so the command-line usage is identical, with additional options also supported. This work was originally inspired by Talha Tariq's RemCom.

```
Usage: PAExec [\\computer[,computer2[,...]] | @file]
[-u user [-p psswd]][-p@ file [-p@d]]]
[-n s] [-l] [-s] [-e] [-x] [-i [session]] [-c [-f|-v] [-csrc path]]
[-lo path] [-rlo path] [-ods] [-w directory] [-d][-][-a n,n,...]
[-dfr] [-noname] [-to seconds] cmd [arguments]
```

Standard PAExec\PsExec command line options:

- 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). This option is not compatible with -to
 - e Does not load the specified account's profile.
 - f Copy the specified program even if the file already exists on the remote system. Requires -c
 - i Run the program so that it interacts with the desktop of the specified session on the specified 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 [EXPERIMENTAL] 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. Also see -p@ and -p@d below.
 - s Run the 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 than the one on the remote system. Requires -c
 - 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} Specify -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 PAExec to run the application on the remote computer or computers specified. If you omit the computer name PAExec runs the application on the local system, and if you specify a wildcard (*), PAExec runs the

command on all computers in the current domain.

@file PAExec will execute the command on each of the computers listed in the file.

program Name of application to execute.

arguments Arguments to pass (note that file paths must be absolute paths on the target system).

Additional options only available in PAExec:

-cnodel If a file is copied to the server with -c, it is normally deleted (unless -d is specified). -cnodel indicates the file should not be deleted.

-clist When using -c (copy), -clist allows you to specify a text file that contains a list of files to copy to the target. The text file should just list file names, and the files should be in the same folder as the text file.
Example: -c -clist "C:\test path\filelist.txt"

filelist.txt might contain:

myapp.exe
mydata.dat

Myapp.exe and mydata.dat would need to be in C:\test path in the example above.

IMPORTANT: The first file listed is assumed to be the one that will be executed.

-clist and -csrc cannot be used together.

-csrc When using -c (copy), -csrc allows you to specify an alternate path to copy the program from.
Example: -c -csrc "C:\test path\file.exe"

-dbg Output to DebugView (OutputDebugString)

-dfr Disable WOW64 File Redirection for the new process

-lo Log Output to file. Ex: -lo C:\Temp\PAExec.log
The file will be UTF-8 with a Byte Order Mark at the start.

-p@ Will read the first line of the given file and use that as the password. File should be saved as UTF-8 with or without Byte Order Mark.

-p@d Deletes the file specified by -p@ as soon as the password is

read.

-rlo Remote Log Output: Log from remote service to file (on remote server).

Ex: -rlo C:\Temp\PAExec.log

The file will be UTF-8 with a Byte Order Mark at the start.

-to Timeout in seconds. The launched process must exit within this number of seconds or it will be terminated. If it is terminated, the exit code will be -10

This option is not compatible with -d

Ex: -to 15

Terminate the launched process after 15 seconds if it doesn't shut down first

-noname In order to robustly handle multiple simultaneous connections to a server, the source server's name is added to the remote service name and remote PAExec executable file. If you do NOT want this behavior, use -noname

The application name, copy source, working directory and log file entries can be quoted if the path contains a space. For example:

```
PAExec \\test-server -w "C:\path with space" "C:\program files\app.exe"
```

Like PsExec, input is sent to the remote system when Enter is pressed, and Ctrl-C stops the remote process and stops PAExec.

PAExec will scramble the parameters to protect them from casual wire sniffers, but they are NOT encrypted. Note that data passed between PAExec and the remote program is NOT scrambled or encrypted. If encryption is needed, use PsExec v2.1 or newer.

PAExec will return the error code it receives from the application that was launched remotely. If PAExec itself has an error, the return code will be one of:

- 1 = internal error
- 2 = command line error
- 3 = failed to launch app (locally)
- 4 = failed to copy PAExec to remote (connection to ADMIN\$ might have failed)
- 5 = connection to server taking too long (timeout)
- 6 = PAExec service could not be installed/started on remote server
- 7 = could not communicate with remote PAExec service
- 8 = failed to copy app to remote server
- 9 = failed to launch app (remotely)
- 10 = app was terminated after timeout expired
- 11 = forcibly stopped with Ctrl-C / Ctrl-Break

Update Notes:

Version (and some downloads)	SHA1 Checksum
1.30 - Interactive mode works better when no credentials are given.	61e56575c7565833fe5bfe26c8c0795bfcbbbe3b0
1.29 - Tries to use given credentials before making remote connection, handles input redirects, hides destination window if -i not given	0FC135B131D0BB47C9A0AAF02490701303B76D3
1.28 - Won't create an interactive PAExec service, can run locally as non-administrator if credentials given.	5fd0c019e47d19ec1bcef2a0664bd4f7625dc15c
1.27 - Added exdiva logging to see why the local computer list can't be obtained	1fb0e4efaf0ee0dabc525ff37059a76486311642
1.26 - -s option works on non-English versions of Windows	31754ee85d21ce9188394a939c15a271c2562f93
1.25 - Allow -s and -h options. -h will be silently ignored when combined.	3238e8522bd0e9e1a1de8ba5e845bd44131d38b8
1.24 - Some fixes when launching apps locally	ea9c9799394ab8e6a1374832d5e3eec6830d5e56

[1.22](#) - More effort to delete the PAExec-{pid}-{source} service on the target computer, compiling with a new compiler f9ff4582f6c3d68c84aa2d1da913b51b440ae68e

[1.21](#) - Added -p@ and -p@d options 820dee796573b93f154cfa484c35354e41ef7a51

[1.19](#) - Silently ignore /accepteula 8f1646da42c1602de60a61eb6bf10ae10394593b

[1.18](#) - Reworked the -i flag. Added the -noname flag. 1daf79b3aa3172446b829b04d7478ac8cc0ea130

[1.17](#) - Uses a uniquely-named service and executable filename so multiple instances can run at once e742288f30a4c052add983a96ea005e8bfb0bbde

1.16 - Improved error logging

1.15 - Better clean up of service with multiple clients connecting

1.14 - Better support for interactive sessions

1.13 - Fix so -h fails gracefully on x64 XP and 2003

1.12 - Fix to -cnodel option. -u and -s can be specified together

1.11 - Fix to the -h implementation

1.10 - Added support for -h, and blank passwords

1.9 - Running with -d will show PID of started process

1.8 - Minor improvement to command-line parsing

1.7 - Multiple PAExec's can be running against the same target computer

1.6 - Added the -to option

1.5 - Fixed some command-line parsing problems

1.4 - Added the -clist option for copying lists of files

1.3 - Works on Windows 2000 now

Email: support@poweradmin.com

Phone: +1 (800) 401-2339

Fax: +1 (866) 266-8330

Power Admin LLC

22052 W 66th Street

Suite #292

Shawnee, KS 66226-3500

USA



Microsoft®
CERTIFIED

PRODUCTS

[Compare Products](#)

[Downloads](#)

[PA Server Monitor](#)

[PA Storage Monitor](#)

[PA File Sight](#)

SERVICES/UTILITIES

[PAExec](#)

[PA-Ping](#)

[SpeedFan HTTP Agent](#)

[SIP-Ping Utility](#)

SUPPORT

[Documentation Home](#)

[FAQ](#)

[Support Forum](#)

[Training Videos](#)

[Glossary](#)

[Branding/White Labeling](#)

PURCHASING

[Order Licenses](#)

[Purchase Orders](#)

[Perpetual Licenses](#)

[Subscriptions](#)

[Perpetual Licenses](#)

[Price List - PA Server Monitor](#)

[Price List - PA Storage Monitor](#)

[Price List - PA File Sight](#)

[Education Discounts](#)

[Find a Reseller](#)

[Become a Reseller](#)

CUSTOMERS

[Customer Testimonials](#)

[Client List](#)

[Case Studies](#)

POWER ADMIN

[About Us](#)

[Blog](#)

[Privacy Policy](#)

[DMCA](#)

[Press](#)

[Product Newsletter](#)