

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

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

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

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:

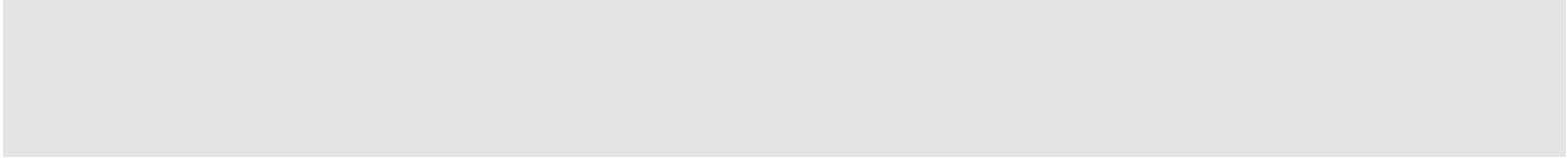
```
PAExec \\test-server -w "C:\path with space" "C:\program files\app.exe"
```

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:

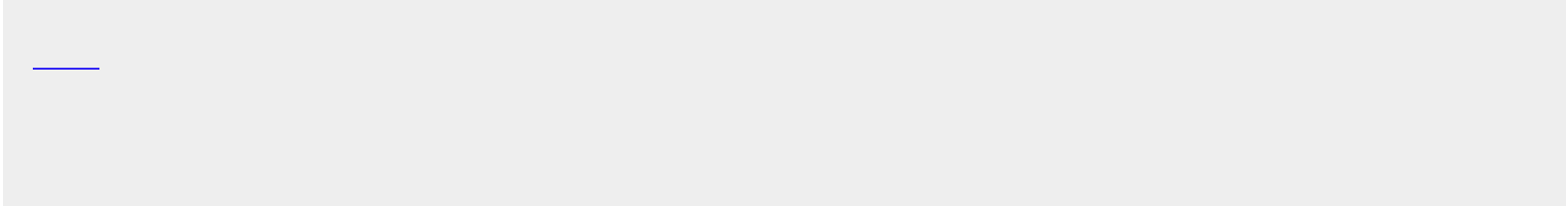
- 1 = internal error
- 2 = command line error
- 3 = failed to launch app (locally)
- 4 = failed to copy PAExec to remote (connection to ADMIN\$ might have failed)
- 5 = connection to server taking too long (timeout)
- 6 = PAExec service could not be installed/started on remote server
- 7 = could not 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



\_\_\_\_\_

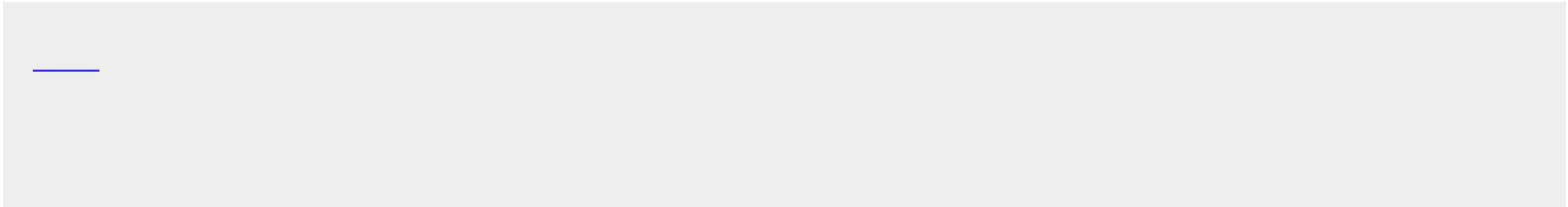
\_\_\_\_\_

\_\_\_\_\_



\_\_\_\_\_

\_\_\_\_\_



\_\_\_\_\_

\_\_\_\_\_





