PsExec v2.2

06/29/2016 • 4 minutes to read • Contributors

In this article

By Mark Russinovich

Published: June 29, 2016

 **Download PsTools (2.7 MB)**

Introduction

Utilities like Telnet and remote control programs like Symantec's PC Anywhere let you execute programs on remote systems, but they can be a pain to set up and require that you install client software on the remote systems that you wish to access. PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.

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.

Installation

Just copy PsExec onto your executable path. Typing "psexec" displays its usage syntax.

Using PsExec

See the July 2004 issue of *Windows IT Pro Magazine* for Mark's article 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 executable [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]

Parameter	Description
-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"

Parameter	Description
-c	Copy the specified executable 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).

Parameter	Description
-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 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"

 Download PsTools **(2.7 MB)**

PSTools

PsExec is part of a growing kit of Sysinternals command-line tools that aid in the adminstration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.