PsLogList v2.8

06/28/2016 • 2 minutes to read • Contributors

In this article

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

The Resource Kit comes with a utility, elogdump, that lets you dump the contents of an Event Log on the local or a remote computer. *PsLogList* is a clone of elogdump except that *PsLogList* lets you login to remote systems in situations your current set of security credentials would not permit access to the Event Log, and *PsLogList* retrieves message strings from the computer on which the event log you view resides.

Installation

Just copy *PsLogList* onto your executable path, and type "psloglist".

Using PsLogList

The default behavior of *PsLogList* is to show the contents of the System Event Log on the local computer, with visually-friendly formatting of Event Log records. Command line options let you view logs on different computers, use a different account to view a log, or to have the output formatted in a string-search friendly way.

usage: psloglist [-] [\\computer[,computer[,...] | @file [-u username [-p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e ID[,ID[,...]]] [-o event source[,event source][,..]]] [-q event source[,event source][,..]]] [-l event log file] <eventlog>

Parameter	Description
@file	Execute the command on each of the computers listed in the file.
-a	Dump records timestamped after specified date.

Parameter	Description
-b	Dump records timestamped before specified date.
-c	Clear the event log after displaying.
-d	Only display records from previous n days.
-c	Clear the event log after displaying.
-e	Exclude events with the specified ID or IDs (up to 10).
-f	Filter event types with filter string (e.g. "-f w" to filter warnings).
-h	Only display records from previous n hours.
-i	Show only events with the specified ID or IDs (up to 10).
-l	Dump records from the specified event log file.
-m	Only display records from previous n minutes.
-n	Only display the number of most recent entries specified.
-o	Show only records from the specified event source (e.g. \"-o cdrom\").
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
-q	Omit records from the specified event source or sources (e.g. \"-q cdrom\").
-r	SDump log from least recent to most recent.
-s	This switch has *PsLogList* print Event Log records one-per-line, with comma delimited fields. This format is convenient for text searches, e.g. psloglist
-t	The default delimeter is a comma, but can be overriden with the specified character.
-u	Specifies optional user name for login to remote computer.
-w	Wait for new events, dumping them as they generate (local system only).
-x	Dump extended data
eventlog	eventlog

How it Works

Like Win NT/2K's built-in Event Viewer and the Resource Kit's elogdump, *PsLogList* uses the Event Log API, which is documented in Windows Platform SDK. *PsLogList* loads message source modules on the system where the event log being viewed resides so that it correctly displays event log messages.

Download PsTools (2.7 MB)

PsTools
PsLogList 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.