

How to pull specific event ID's from Event Viewer to a .csv file using PowerShell

Step#	Task
1	From either a computer on the same network as the machine with the logs or directly on the machine with the logs launch Powershell as an administrator
2	Run the command: <code>\$StartDate = (Get-Date).adddays(-##)</code> Replace the ## with how many days you want to go back from today.
3	Then run: <code>Get-WinEvent -ComputerName 'MachineName' -FilterHashtable @{LogName='Security';id='eventid,eventid,etc';dataName=';StartTime=\$StartDate'} Export-Csv C:\temp\'NameOfFile'.csv</code> Replace the following values: 'MachineName' = The computer you want to pull logs from, or delete the entire string '-ComputerName 'MachineName' if you are running it on the computer in which you have the logs

'eventid' = These are the event IDs you
looking for for example 4624,4634

'Username' = With the user login with
domain part

'NameOfFile' = The title your want for
file.

Author: Justin Wilson

Online URL: <https://kb.naturalnetworks.com/article.php?id=623>