

Get-AllEventLogsTimeFrame

Make changes to the variables \$startTime and \$endTime for exact dates/times, otherwise utilize the commented out sections.

```
#example: get all logs in the last minute
if($computerName -eq "" -OR $null -eq $computerName)
{
    $computerName = $env:COMPUTERNAME
}
#gather the log names
$logNames = @()
$allLogNames = get-winevent -computerName $computerName -ListLog *
foreach($logName in $allLogNames)
{
    if($logName.recordcount -gt 0) #filter empty logs
    {
        $logNames += $logName
    }
}
#get the time range
$startTime = '3/3/2025 05:17:15'#(Get-date).AddMinutes(-1)
$endTime = '3/3/2025 05:18:00'#Get-date
#get the actual logs
$logEvents = Get-WinEvent -computerName $computerName -FilterHashtable @{
    LogName=$logNames.logName; StartTime=$startTime; EndTime=$endTime}
#this makes Out-GridView show the full log properties
($logEvents | ConvertTo-Json | ConvertFrom-Json).syncroot | Export-Csv -Path .\events.csv -
NoTypeInfoation
```

Revision #2

Created 2025-03-03 19:15:18 UTC by Ryan

Updated 2025-03-12 17:18:08 UTC by Ryan