nasbench / howto.txt

Forked from andrewkroh/howto.txt

Created last year

Microsoft-Windows-Windows Defender Event Log Message Resources

gistfile1.txt Raw

```
800, AntiVirus
801, AntiSpyware
802, Antimalware
803, Full
804, Delta
805, Full Scan
806, Quick Scan
807, Custom Scan
808, Remove
809, Quarantine
810, Clean
811, Allow
812, Unknown
813, Suspended
814, Allowed
815, User
816, Scheduled
817, Signature Update Folder
818, Real-Time Protection
819, Downloads and attachments
820, System
821, Heuristics
822, Concrete
823, Generic
824, Current
825, Backup
826, Default
827, Windows Defender Antivirus
828, Microsoft Forefront Endpoint Protection
829, Microsoft Standalone System Sweeper
830, Crash
831, Hang
832, Not Applicable
833, IE Downloads and Outlook Express Attachments
834, On Access
835, Behavior Monitoring
836, The filter driver has successfully restarted.
837, The filter driver was unloaded unexpectedly.
838, The filter driver skipped scanning items and is in pass through mode. This may be due to low resource conditions.
839, The filter driver has restarted scanning items and is out of pass through mode.
840, Real-time protection has stopped functioning for an unknown reason. Restart the service in order to recover.
841, Real-time protection has recovered from an unknown failure. It is recommended that you run a quick scan.
842, The filter driver requires an up-to-date engine in order to function. You must install the latest definition updates in order
843, Suspicious
844, Unknown
845, Local machine
846, Network share
847, Internet
848, Executing
849, Internal Definition Update Server
850, File Share
851, Microsoft Malware Protection Center
852, Search
853, Download
854, Install
```

```
855, Low
856, Medium
857, High
858, Antimalware protection has stopped functioning for an unknown reason. In some instances, restarting the service may resolve th
859, Microsoft Update Server
860, Microsoft Antimalware
861, Microsoft Antimalware
862, FastPath
863, Signature update
864, Signature disable notification
865, VDM version
866, Timestamp
867, No limit
868, Manual
869, Automatic
870, Duration
871, None
872, Grace period
873, Windows Activation Technologies genuine validation failed
874, Information Protection Control
875, Unknown
876, Detected
877, Cleaned
878, Quarantined
879, Removed
880, Allowed
881, Clean Failed
882, Quarantine Failed
883, Remove Failed
884, Allow Failed
885, Unknown
886, Network Inspection System
887, Not Applicable
888, Outgoing traffic
889, Incoming traffic
890, Block
891, Internet Explorer Extension Validation
892, The system is missing updates that are required for running Network Inspection System.  Install the required updates and resta
893, Early Launch Antimalware
894, TCG Log Inspection
895, Remote Server
896, The Network Inspection System did not successfully start due to an error.
897, AMSI
898, AMSI UAC provider
899, Windows Defender Advanced Threat Protection
900, Shared Signature Root
901, Enabled
902, Disabled
```

howto.txt Raw

```
wevtutil.exe gp "Microsoft-Windows-Windows Defender" | Out-File -Encoding UTF8 microsoft-windows-windows-defender.txt

# Then see https://gist.github.com/andrewkroh/665dca0682bd0e4daf194ab291694012 for how to convert the DLL to a list of codes.
```

microsoft-windows-windows-defender.txt Raw

```
name: Microsoft-Windows-Windows Defender
guid: 11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78
helpLink: https://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Corporation&ProdName=Microsoft%c2%ae%20Windows%c2%ae%20Oper
resourceFileName: C:\Program Files\Windows Defender\MpEvMsg.dll
parameterFileName: C:\Program Files\Windows Defender\MpEvMsg.dll
messageFileName: C:\Program Files\Windows Defender\MpEvMsg.dll
message: 2415919105
channels:
  channel:
    name: Microsoft-Windows-Windows Defender/Operational
    id: 16
    flags: 0
    message:
  channel:
    name: Microsoft-Windows-Windows Defender/WHC
    id: 17
    flags: 0
    message:
```

```
19  levels:
20    level:
21      name: win:Error
22      value: 2
23      message: 1342177282
24    level:
25      name: win:Warning
26      value: 3
27      message: 1342177283
28    level:
29      name: win:Informational
30      value: 4
31      message: 1342177284
32  opcodes:
33  tasks:
34  keywords:
```