GitHub Gist | Search... | All gists Back to GitHub | Sign in | Sign up

Instantly share code, notes, and snippets.

nasbench / howto.txt

☆ Star 0   Fork 0

Forked from andrewkroh/howto.txt
Created last year

<> **Code**   ◦─ **Revisions** 2

Embed ▾ | `<script src="https://` | 📋 | 📥 | Download ZIP

Microsoft-Windows-Windows Defender Event Log Message Resources

<> **gistfile1.txt**   Raw

```
 1    800, AntiVirus
 2    801, AntiSpyware
 3    802, Antimalware
 4    803, Full
 5    804, Delta
 6    805, Full Scan
 7    806, Quick Scan
 8    807, Custom Scan
 9    808, Remove
10    809, Quarantine
11    810, Clean
12    811, Allow
13    812, Unknown
14    813, Suspended
15    814, Allowed
16    815, User
17    816, Scheduled
18    817, Signature Update Folder
19    818, Real-Time Protection
20    819, Downloads and attachments
21    820, System
22    821, Heuristics
23    822, Concrete
24    823, Generic
25    824, Current
26    825, Backup
```

```
27    826, Default
28    827, Windows Defender Antivirus
29    828, Microsoft Forefront Endpoint Protection
30    829, Microsoft Standalone System Sweeper
31    830, Crash
32    831, Hang
33    832, Not Applicable
34    833, IE Downloads and Outlook Express Attachments
35    834, On Access
36    835, Behavior Monitoring
37    836, The filter driver has successfully restarted.
38    837, The filter driver was unloaded unexpectedly.
39    838, The filter driver skipped scanning items and is in pass through mode. This may be due to low resou
40    839, The filter driver has restarted scanning items and is out of pass through mode.
41    840, Real-time protection has stopped functioning for an unknown reason. Restart the service in order t
42    841, Real-time protection has recovered from an unknown failure. It is recommended that you run a quick
43    842, The filter driver requires an up-to-date engine in order to function. You must install the latest
44    843, Suspicious
45    844, Unknown
46    845, Local machine
47    846, Network share
48    847, Internet
49    848, Executing
50    849, Internal Definition Update Server
51    850, File Share
52    851, Microsoft Malware Protection Center
53    852, Search
54    853, Download
55    854, Install
56    855, Low
57    856, Medium
58    857, High
59    858, Antimalware protection has stopped functioning for an unknown reason. In some instances, restartin
60    859, Microsoft Update Server
61    860, Microsoft Antimalware
62    861, Microsoft Antimalware
63    862, FastPath
64    863, Signature update
65    864, Signature disable notification
66    865, VDM version
67    866, Timestamp
68    867, No limit
69    868, Manual
70    869, Automatic
71    870, Duration
```

```
 72    871, None
 73    872, Grace period
 74    873, Windows Activation Technologies genuine validation failed
 75    874, Information Protection Control
 76    875, Unknown
 77    876, Detected
 78    877, Cleaned
 79    878, Quarantined
 80    879, Removed
 81    880, Allowed
 82    881, Clean Failed
 83    882, Quarantine Failed
 84    883, Remove Failed
 85    884, Allow Failed
 86    885, Unknown
 87    886, Network Inspection System
 88    887, Not Applicable
 89    888, Outgoing traffic
 90    889, Incoming traffic
 91    890, Block
 92    891, Internet Explorer Extension Validation
 93    892, The system is missing updates that are required for running Network Inspection System.  Install th
 94    893, Early Launch Antimalware
 95    894, TCG Log Inspection
 96    895, Remote Server
 97    896, The Network Inspection System did not successfully start due to an error.
 98    897, AMSI
 99    898, AMSI UAC provider
100    899, Windows Defender Advanced Threat Protection
101    900, Shared Signature Root
102    901, Enabled
103    902, Disabled
```

‹› **howto.txt**   Raw

```
1    wevtutil.exe gp "Microsoft-Windows-Windows Defender" | Out-File -Encoding UTF8 microsoft-windows-window
2
3    # Then see https://gist.github.com/andrewkroh/665dca0682bd0e4daf194ab291694012 for how to convert the D
```

‹› **microsoft-windows-windows-defender.txt**   Raw

```
1    name: Microsoft-Windows-Windows Defender
2    guid: 11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78
3    helpLink: https://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Corporation&ProdName=Microsoft%
4    resourceFileName: C:\Program Files\Windows Defender\MpEvMsg.dll
5    parameterFileName: C:\Program Files\Windows Defender\MpEvMsg.dll
```

```
 6    messageFileName: C:\Program Files\Windows Defender\MpEvMsg.dll
 7    message: 2415919105
 8    channels:
 9      channel:
10        name: Microsoft-Windows-Windows Defender/Operational
11        id: 16
12        flags: 0
13        message:
14      channel:
15        name: Microsoft-Windows-Windows Defender/WHC
16        id: 17
17        flags: 0
18        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:
```

Terms   Privacy   Security   Status   Docs   Contact   Manage cookies   Do not share my personal information

© 2024 GitHub, Inc.