Previše EventID 5156 za moj ukus

written by js | 2023-11-21

```
C:\> auditpol /set /subcategory:”Filtering Platform Packet Drop” /success:disable /failure:disable
C:\> auditpol /set /subcategory:”Filtering Platform Connection” /success:disable /failure:disable
C:\> gpupdate /force
```

Iako.. ovaj “failure” možda nije loše ostaviti na “enable” da vidiš neuspjele pokušaje?

Vidi i `auditpol /get /category:*`

Takodjer https://learn.microsoft.com/en-us/windows/win32/fwp/auditing-and-logging?redirectedfrom=jednostavnoSomwareOrg

Kepćur

Želiš li pohvatati nešto paketa:

```
netsh wfp capture start
netsh wfp capture stop
```

To će kreirati fajl:

```
wfpdiag.cab
```

---

eventid5156 eventlog5156 5156 xeventid5156 xeventlog5156 x5156 id5156 xid5156