New Search

```
sourcetype=_json datasource=sysmon event.code=13
| table timestamp host.name process.name registry.key registry.value
```

Last 24 hours

✓ **21 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:26:13.000 AM) No Event Sampling

Events (21)

Format Timeline

1 hour per column

SELECTED FIELDS

a	host	1
a	source	1
a	sourcetype	1

INTERESTING FIELDS

a	datasource	1
a	event.action	1
#	event.code	1
a	host.name	11
a	index	1
#	linecount	1
a	process.name	1
#	process.pid	21
a	punct	2
a	registry.key	11
a	registry.path	11
a	registry.value	3
a	splunk_server	1
a	timestamp	21

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765689973.257)

Time Event

12/14/25 5:03:09.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3452
   process.pid: 3764
   registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName
   registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName
   registry.value: FriendlyName
   timestamp: 12/14/2025 05:03:09.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25 5:01:22.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3456
   process.pid: 3878
   registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName
   registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName
   registry.value: FriendlyName
   timestamp: 12/14/2025 05:01:22.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
5:01:10.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3458
   process.name: spoolsv.exe
   process.pid: 3613
   registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName
   registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName
   registry.value: FriendlyName
   timestamp: 12/14/2025 05:01:10.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
5:00:06.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3451
   process.name: spoolsv.exe
   process.pid: 3623
   registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName
   registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName
   registry.value: FriendlyName
   timestamp: 12/14/2025 05:00:06.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time Event

12/14/25
4:53:49.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry
Event)
   event.code: 13
   host.name: win-3457
   process.name: spoolsv.exe
   process.pid: 3841
   registry.key: SOFTWARE\Microsoft\Windows NT\Curr
entVersion\Print\Printers\Fax (redirected 5)\DsDriv
er\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows N
T\CurrentVersion\Print\Printers\Fax (redirected 5)
\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:53:49.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:49:36.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry
Event)
   event.code: 13
   host.name: win-3460
   process.name: spoolsv.exe
   process.pid: 3746
   registry.key: SOFTWARE\Microsoft\Windows NT\Curr
entVersion\Print\Printers\Fax (redirected 4)\DsDriv
er\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows N
T\CurrentVersion\Print\Printers\Fax (redirected 4)
\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:49:36.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:46:54.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3452
   process.pid: 3727
   registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion
   registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion
   registry.value: DriverVersion
   timestamp: 12/14/2025 04:46:54.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:44:18.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3449
   process.name: spoolsv.exe
   process.pid: 3844
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:44:18.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:43:27.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3455
   process.name: spoolsv.exe
   process.pid: 3913
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:43:27.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:42:23.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3450
   process.name: spoolsv.exe
   process.pid: 3846
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:42:23.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:41:15.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry
Event)
   event.code: 13
   host.name: win-3454
   process.name: spoolsv.exe
   process.pid: 3953
   registry.key: SOFTWARE\Microsoft\Windows NT\Curr
entVersion\Print\Printers\Microsoft Print to PDF (r
edirected 5)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows N
T\CurrentVersion\Print\Printers\Microsoft Print to
PDF (redirected 5)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:41:15.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:40:30.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry
Event)
   event.code: 13
   host.name: win-3449
   process.name: spoolsv.exe
   process.pid: 3645
   registry.key: SOFTWARE\Microsoft\Windows NT\Curr
entVersion\Print\Printers\Microsoft Print to PDF (r
edirected 4)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows N
T\CurrentVersion\Print\Printers\Microsoft Print to
PDF (redirected 4)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:40:30.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:34:02.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3450
   process.pid: 3939
   registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion
   registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion
   registry.value: DriverVersion
   timestamp: 12/14/2025 04:34:02.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:33:42.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3456
   process.pid: 3915
   registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName
   registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName
   registry.value: FriendlyName
   timestamp: 12/14/2025 04:33:42.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time Event

12/14/25
4:32:12.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3449
   process.name: spoolsv.exe
   process.pid: 3743
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:32:12.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:28:15.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3457
   process.name: spoolsv.exe
   process.pid: 3855
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:28:15.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:25:36.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3461
   process.name: spoolsv.exe
   process.pid: 3598
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:25:36.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:25:30.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3455
   process.name: spoolsv.exe
   process.pid: 3703
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 4)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 4)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:25:30.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time Event

12/14/25
4:25:22.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3456
   process.name: spoolsv.exe
   process.pid: 3650
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:25:22.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:24:52.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3456
   process.pid: 3957
   registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion
   registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion
   registry.value: DriverVersion
   timestamp: 12/14/2025 04:24:52.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time Event

12/14/25
4:24:12.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Registry value set (rule: Registry Event)
   event.code: 13
   host.name: win-3449
   process.name: spoolsv.exe
   process.pid: 3978
   registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion
   registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion
   registry.value: driverVersion
   timestamp: 12/14/2025 04:24:12.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json