Event ID Reference Guide

For Help Desk Technicians

Quick Diagnostic Reference for Windows Event Viewer Logs

Prepared by: Desktechpro

Contact:
Email: support@desktechpro.com
Website: desktechpro.com

Helping IT teams troubleshoot faster and smarter.

Event ID Reference Guide for Help Desk Technicians

Use this guide to quickly reference critical Windows Event IDs across common logs. These are especially useful when triaging user issues, security incidents, and system crashes.

System Log Event IDs

Path: *Event Viewer > Windows Logs > System*

- **Event ID 41** – Kernel-Power: System rebooted without clean shutdown (common in BSODs).
- **Event ID 6005** – Event log service start (used as a startup time marker).
- **Event ID 6006** – Event log service stop (used as a shutdown time marker).
- **Event IDs 7000–7099** – Driver failures and service start issues.

Application Log Event IDs

Path: *Windows Logs > Application*

- **Event ID 1000** – Application Error: Faulting application and module details.
- **Event ID 1026** – .NET Runtime error.
- **Event ID 1001** – Windows Error Reporting (often follows a crash or hang).

Security Log Event IDs

Path: *Windows Logs* > *Security*

- **Event ID 4624** – Successful user logon.
- **Event ID 4625** – Failed user logon attempt.
- **Event ID 4634** – Logoff event.
- **Event ID 4648** – Logon using explicit credentials (e.g., runas).
- **Event ID 4672** – Special privileges assigned at logon (admin logon).

Setup Log Event IDs

Path: *Windows Logs* > *Setup*

- **Event ID 20** – Windows Update installation failure.
- **Event ID 200** – Setup diagnostics and feature installation tracking.

Applications and Services Log Event IDs

Path: *Applications and Services Logs* > *Microsoft* > *Windows* > *[Component]*

- **Event ID 3006** – Windows Defender detected malware or PUP.
- **Event ID 8193** – VSS (Volume Shadow Copy) writer error – backup failure.
- **Event ID 1129** – Group Policy processing failure (often network or AD related).

Quick Tips for Using Event Viewer Effectively

- Filter logs by Event ID, level (Error, Warning, etc.), and time range.
- Save custom views for repeated issues like failed logins or BSODs.
- Cross-reference log timestamps with user reports to validate issues.
- Not all warnings are critical—focus on **Errors** and **Critical** levels first.