CORVASEC

Windows Event ID Quick Reference

A practical investigation reference for high-value Windows Security, System, and Application events used in troubleshooting and security monitoring.

DOCUMENT CENTER

Compiled September 2026

IMPORTANT: Event meaning depends on audit policy, Windows version, event fields, and surrounding activity. An event ID by itself is not proof of malicious behavior. Correlate account, host, source, process, timing, and related telemetry.

Use this guide as a practical reference. Verify commands, targets, permissions, paths, versions, and organizational policy before making changes. Examples with placeholders must be adapted to the environment.

Contents

#	Section	Entries
1	High-value Windows event IDs	77
2	Useful PowerShell queries	8

Total reference entries: 85

1. High-value Windows event IDs

Event ID	Log	Meaning	Investigation note
1100	Security	Event logging service shut down	Review unexpected shutdowns of event logging.
1102	Security	Security audit log cleared	High-value event; validate who cleared the log and why.
4608	Security	Windows starting up	Useful boot correlation marker.
4616	Security	System time changed	Review unexpected clock changes.
4624	Security	Successful logon	Correlate account, logon type, source address, workstation, and process.
4625	Security	Failed logon	Review account, failure reason, source address, and repeated attempts.
4634	Security	Logoff	Session ended; high volume in many environments.
4647	Security	User initiated logoff	Interactive logoff initiated by the user.
4648	Security	Logon with explicit credentials	May indicate runas, mapped resources, services, or lateral movement context.
4672	Security	Special privileges assigned to new logon	Administrator-equivalent privileges assigned to a session.
4688	Security	New process created	Core process-creation telemetry when Audit Process Creation is enabled.
4689	Security	Process exited	Useful when process termination auditing is enabled.
4697	Security	Service installed	Review new service creation, binary path, and account.
4698	Security	Scheduled task created	Review task action, trigger, author, and creation context.
4699	Security	Scheduled task deleted	Review unexpected task removal.
4700	Security	Scheduled task enabled	Review task activation.
4701	Security	Scheduled task disabled	Review unexpected task disablement.
4702	Security	Scheduled task updated	Inspect modified task action/triggers.
4719	Security	System audit policy changed	Review audit-policy changes.
4720	Security	User account created	Validate new accounts and creator.
4722	Security	User account enabled	Review re-enabled accounts.
4723	Security	Password change attempted	Account attempted to change its password.
4724	Security	Password reset attempted	Review administrative resets.
4725	Security	User account disabled	Review planned vs unexpected disablement.
4726	Security	User account deleted	Validate account removal.
4728	Security	Member added to global security group	Review privileged group additions.
4729	Security	Member removed from global security group	Review privileged group changes.
4732	Security	Member added to local security group	Common privileged-group monitoring event.
4733	Security	Member removed from local security group	Review changes to sensitive local groups.
4738	Security	User account changed	Review modified account attributes.
4740	Security	User account locked out	Correlate caller computer and failed logons.
4741	Security	Computer account created	Review unexpected computer-account creation.
4742	Security	Computer account changed	Review sensitive machine-account modifications.
4767	Security	User account unlocked	Review who unlocked an account.
4768	Security	Kerberos TGT requested	Core Kerberos authentication event on domain controllers.
4769	Security	Kerberos service ticket requested	Useful for service access and Kerberos investigation.
4771	Security	Kerberos pre-authentication failed	Review failure code, account, and client address.
4776	Security	Credential validation attempted	NTLM credential validation event on authoritative system.
4778	Security	Session reconnected	Remote Desktop/session reconnect context.
4779	Security	Session disconnected	Remote Desktop/session disconnect context.

Event ID	Log	Meaning	Investigation note
4798	Security	User local group membership enumerated	May be benign administration or discovery.
4799	Security	Security-enabled local group membership enumerated	Review unusual enumeration on sensitive hosts.
4800	Security	Workstation locked	User/session lock event.
4801	Security	Workstation unlocked	User/session unlock event.
4825	Security	Remote Desktop connection denied	Review RDP authorization failures.
4902	Security	Per-user audit policy table created	Audit policy context.
4946	Security	Firewall rule added	Review new firewall rule.
4947	Security	Firewall rule modified	Review firewall rule modification.
4948	Security	Firewall rule deleted	Review unexpected firewall rule removal.
4956	Security	Windows Firewall active profile changed	Review network profile/firewall state changes.
5024	Security	Windows Firewall service started	Firewall operational event.
5033	Security	Windows Firewall driver started	Firewall driver operational event.
5059	Security	Key migration operation	Cryptographic key operation context.
5136	Security	Directory service object modified	Important Active Directory change auditing event.
5137	Security	Directory service object created	Active Directory object creation.
5140	Security	Network share accessed	Share-level access event.
5145	Security	Detailed network share access check	Useful for file/share access investigations.
5156	Security	Windows Filtering Platform allowed connection	High-volume network connection telemetry when enabled.
5157	Security	Windows Filtering Platform blocked connection	Blocked connection event.
5379	Security	Credential Manager credentials read	Review unexpected credential enumeration.
6416	Security	New external device recognized	Device installation/connection telemetry.
41	System	Kernel-Power unexpected restart	Often associated with power loss, crash, or forced reset.
6005	System	Event Log service started	Common boot marker.
6006	System	Event Log service stopped	Common clean shutdown marker.
6008	System	Previous shutdown unexpected	Indicates an unclean shutdown.
7000	System	Service failed to start	Review service name and error.
7001	System	Service dependency failed	Review dependency chain.
7009	System	Service connection timeout	Service did not connect within expected time.
7011	System	Service transaction timeout	A service operation timed out.
7031	System	Service terminated unexpectedly	Review crash pattern and recovery actions.
7034	System	Service terminated unexpectedly	Service Control Manager termination event.
7040	System	Service start type changed	Review unexpected changes.
7045	System	Service installed	Service Control Manager service-install event; review binary path.
1000	Application	Application Error	Common application crash event.
1001	Application	Windows Error Reporting	Crash/hang report metadata.
1002	Application	Application Hang	Application stopped responding.
10016	System	DistributedCOM permission/event	Common DCOM event; interpret in application context rather than treating every occurrence as malicious.

2. Useful PowerShell queries

Command	Purpose / Notes
`Get-WinEvent -FilterHashtable @{LogName="Security";Id=4625}`	Find failed logons.
`Get-WinEvent -FilterHashtable @{LogName="Security";Id=4688}`	Find process creation events.
`Get-WinEvent -FilterHashtable @{LogName="Security";Id=4740}`	Find account lockouts.
`Get-WinEvent -FilterHashtable @{LogName="Security";Id=4768,4769,4771}`	Review Kerberos authentication events.
`Get-WinEvent -FilterHashtable @{LogName="System";Id=41,6008}`	Review unexpected shutdown/restart events.
`Get-WinEvent -FilterHashtable @{LogName="System";Id=7045}`	Find service installations.
`Get-WinEvent -FilterHashtable @{LogName="Application";Id=1000,1001,1002}`	Review crashes and hangs.
`Get-WinEvent -LogName Security -MaxEvents 100 | Select TimeCreated,Id,ProviderName,Message`	Create a concise recent-security view.

Authoritative references

Use vendor and standards documentation for exact syntax, current behavior, version-specific details, licensing, and policy requirements.

Microsoft Sentinel Windows Security Event ID Reference

https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference

Microsoft Event 4624 documentation

https://learn.microsoft.com/windows/security/threat-protection/auditing/event-4624