



Windows Server Auditing

How to enable logging of important Windows Server events in Windows event logs

Local Policy Audit Settings

- Run **gpedit.msc** > Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy:
 - *Audit account management* > Define > Success
 - *Audit object access* > Define > Success

Registry-level Auditing Settings

- Run **regedit.exe** > HKEY_LOCAL_MACHINE > Right-click "SOFTWARE" > Permissions > Advanced > Auditing (Tab) > Click "Add" > Principal "Everyone" > Type "Success" > Applies to "This key and subkeys" > Advanced Permissions > Check "Set Value", "Create Subkey", "Delete", "Write DAC", "Write Owner" > Click "OK"
- Repeat steps above for the "HKEY_LOCAL_MACHINE\SYSTEM" and "HKEY_USERS\DEFAULT" nodes

Event Log Settings

- Run **eventvwr.msc** > Windows Logs > Right-click "Application" log > Properties:
 - Make sure the "Enable logging" check box is selected
 - Set retention method to "Overwrite events as needed" or "Archive the log when full"
- Repeat this operation for the "Security" and "System" event logs
- Open *Event viewer* and search the corresponding log for the id's listed in the Event ID Reference box

For Detailed Windows Server Auditing, Try Netwrix Auditor - netwrix.com/go/trial-ws

- Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- AuditArchive™:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.
- Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

Event ID Reference (2003/2008 - 12)

Security Log

- 636/4732 – Local group member added
- 637/4733 – Local group member removed
- 635/4731 – Local group created
- 638/4734 – Local group deleted
- 624/4720 – User account created
- 630/4726 – User account deleted
- 639/4735 – Local group changed
- 642/4738 – User account changed
- 627/4723 – Change password attempt
- 628/4724 – User account password set
- 685/4781 – User name changed
- 567/4657,4663 – Object access attempt
- 560/4656 – Object open
- 562/4658 – Handle closed
- 602/4698, 4699, 4700, 4701, 4702 – Scheduled task created, deleted, enabled, disabled, updated

Application Log

Event Source: MsiInstaller

- 11707 – Software was installed
- 11724 – Software was uninstalled

System Log

Event Source: Service Control Manager

- 7036 – Service state changed
- 7040 – Service start type changed

netwrix
#1 for change auditing

Try Windows Server
Auditing For Free:

netwrix.com/go/trial-ws