Quick Reference Guide

netwrix
#1 for change auditing

Active Directory Auditing

How to enable logging of important Active Directory events in security event log

Audit Policy Settings

- Run **GPMC.msc** *(url2open.com/gpmc)* > open "**Default Domain Controllers Policy**" > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy:
  - *Audit account management* > Define > Success
  - *Audit directory service access* > Define > Success
  - *Audit account logon events* > Define > Success and Failure
  - *Audit logon events* > Define > Success and Failure

Object-level Active Directory Auditing

- Open **ADSI Edit** *(url2open.com/adsi)* > Connect to Default naming context > Right-click DomainDNS object with the name of your domain > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and Descendant objects" > Permissions > Select all check boxes except the following: Full Control, List Contents, Read all properties, Read permissions > Click "OK"

Security Event Log Settings

- Run **GPMC.msc** > open "**Default Domain Controllers Policy**" > Computer Configuration > Policies > Windows Settings > Security Settings > Event Log > Define
  - *Maximum security log size* to 1gb
  - *Retention method for security log* to *Overwrite events as needed*
- Open *Event viewer* and search Security log for event id's listed in the Event ID Reference box

For Detailed Active Directory Auditing, Try Netwrix Auditor — netwrix.com/go/trial-ad

- **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.
- **Configuration assessment**: State-in-time™ reports show configuration settings at any point in time, such as group membership or password policy settings as they were configured a year ago.
- **Predefined reports, alerts 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)

- 517/1102 – Security log cleared
- 528, 540/4624 – Login succeeded
- 534, 529, 530, 531, 532, 533, 534, 535, 536, 537, 539, 675/4625, 4771 – Failed login
- 535, 675/4625, 4771 (Failure code 0x17) – Password expired
- 624/4720 – User account created
- 626/4722 – User account enabled
- 628/4724 – Password reset attempt
- 629/4725 – User account disabled
- 630/4726 – User account deleted
- 631, 635, 648, 653, 658, 663/4727, 4731, 4754 , 4759, 4744, 4749 – Group created
- 632, 636, 650, 655, 660, 665/4728, 4732, 4756 , 4761, 4746, 4751 – Member added to a group
- 633, 637, 651, 656, 661, 666/4729, 4733, 4757, 4762, 4747, 4752 – Member removed from a group
- 634, 638, 652, 662, 667, 657/4730, 4734, 4758, 4748, 4753, 4763 – Group deleted
- 644/4740 – User account locked out
- 647/4743 – Computer deleted
- 668/4764 – Group type changed
- 671/4767 – User account unlocked

Corporate Headquarters:
20 Pacifica, Suite 625, Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social