ACTIVE DIRECTORY PRO

Active Directory Auditing

This quick reference guide shows you which policy settings to enable to log important changes in your Active Directory.

Advanced Auditing Policy Settings

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration

Category	Policy Settings Name	Policy Setting
Account Logon	Audit Credential Validation	Failure
Account Logon	Audit Kerberos Authentication Service	Success and Failure
Account Logon	Audit Kerberos Service Ticket Operations	Failure
Account Management	Audit Computer Account Management	Success
Account Management	Audit Other Account Management Events	Success
Account Management	Audit Security Group Management	Success
Account Management	Audit User Account Management	Success and Failure
Detailed Tracking	Audit PNP Activity	Success
Detailed Tracking	Audit Process Creation	Success
DS Access	Audit Directory Service Access	Failure
DS Access	Audit Directory Service Changes	Success
Logon/Logoff	Audit Account Lockout	Failure
Logon/Logoff	Audit Group Membership	Success
Logon/Logoff	Audit Logon	Success and Failure
Logon/Logoff	Audit Other Logon/Logoff Events	Success and Failure
Logon/Logoff	Audit Special Logon	Success
Object Access	Audit Detailed File Share	Failure
Object Access	Audit File Share	Success and Failure
Object Access	Audit Other Object Access Events	Success and Failure
Object Access	Audit Removable Storage	Success and Failure
Policy Change	Audit Audit Policy Change	Success
Policy Change	Audit Authentication Policy Change	Success
Policy Change	Audit MPSSVC Rule-Level Policy Change	Success and Failure
Policy Change	Audit Other Policy Change Events	Failure
Privilege Use	Audit Sensitive Privilege Use	Success and Failure
System	Audit Other System Events	Success and Failure
System	Audit Security State Change	Success
System	Audit Security System Extension	Success
System	Audit System Integrity	Success and Failure

Event Log Settings

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Event Log

Policy Path	Policy Settings Name	Policy Setting
Event Log	Maximum application log size	4194240 kB
Event Log	Maximum Security log size	4194240 kB
Event Log	Maximum system log size	4194240 kB
Event Log	Retention method for security log	Overwrite as needed