EventTracker
Secure. Comply. Succeed.

Advanced Audit Policy Configuration

Quick Reference Guide

EventTracker v7.x

Publication Date: May 6, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Advanced Audit Policy Configuration

System Audit Policy	Category/Sub Category	Success	Failure
System	Ipsec Driver	Disable	Disable
	Other System Events	Disable	Disable
	Security State Change	Enable	Enable
	Security System Extension	Enable	Enable
	System Integrity	Enable	Enable
Logon/logoff	Account lockout	Enable	Enable
	IPsec Main Mode	Disable	Disable
	IPsec Extended Mode	Disable	Disable
	IPsec Quick Mode	Disable	Disable
	Logoff	Enable	Enable
	Logon	Enable	Enable
	Network Policy Server	Enable	Enable
	Other Logon/Logoff Events	Enable	Enable
	Special Logon	Enable	Enable
Object Access	Application Generated	Enable	Enable
	Certification Services	Enable	Enable
	Detailed File Share	Disable	Disable
	File Share	Enable	Enable
	File System	Enable	Enable
	Filtering Platform Connection	Disable	Disable
	Filtering Platform Packet Drop	Disable	Disable
	Handle Manipulation	Disable	Disable
	Kernel Object	Enable	Enable
	Other Object Access Events	Disable	Disable
	Registry	Enable	Enable
	SAM	Disable	Disable
Privilege Use	Non Sensitive Privilege Use	Enable	Enable
	Sensitive Privilege Use	Enable	Enable
	Other Privilege Use Events	Enable	Enable
Detailed Tracking	DPAPI Activity	Disable	Disable
	Process Creation	Enable	Enable
	Process Termination	Enable	Enable
	RPC Events	Enable	Enable
Policy Change	Audit Policy Change	Enable	Enable
	Authentication Policy Change	Enable	Enable
	Authorization Policy Change	Enable	Enable
	Filtering Platform Policy Change	Disable	Disable
	MPSSVC Rule-Level Policy Change	Disable	Disable
	Other Policy Change Events	Disable	Enable
Account Management	User Account Management	Enable	Enable
	Computer Account Management	Enable	Enable

	Security Group Management	Enable	Enable
	Distribution Group Management	Enable	Enable
	Application Group Management	Enable	Enable
	Other Account Management Events	Enable	Enable
DS Access	Detailed Directory Service Replication	Disable	Disable
	Directory Service Access	Enable	Enable
	Directory Service Changes	Enable	Enable
	Directory Service Replication	Disable	Disable
Account Logon	Kerberos Service Ticket Operations	Enable	Enable
	Other Account Logon Events	Enable	Enable
	Kerberos Authentication Service	Enable	Enable
	Credential Validation	Enable	Enable
Global Object Access Auditing	File System (GOAA)	Optional	Optional
	Registry (GOAA)	Optional	Optional