Windows 7/2008 x64 Audit Policy Registry Structure (HKLM¥SECURITY¥Policy¥PolAdtEv)

Byte	Hex	Category/Subcategory		Default (Windows 7)	Default (2008 x64)	Description
0	0	N/A		00 01	00 01	Unknown
2	2			00 00	00 00	
4	4			09 00	09 00	
6	6			Unknown	Unknown	
8	8			78 00	78 00	
10	A			00 00	00 00	
12	C	System	Security State Change	01 00	01 00	00 00 : No Auditing 01 00 : Success 02 00 : Failure 03 00 : Success and Failure
14	E		Security System Extension	00 00	00 00	
16	10		System Integrity	03 00	03 00	
18	12		IPsec Driver	00 00	00 00	
20	14		Other System Events	03 00	03 00	
22	16	Logon/Logoff	Logon	01 00	03 00	
24	18		Logoff	01 00	01 00	
26	1A		Account Lockout	01 00	01 00	
28	1C		IPsec Main Mode	00 00	00 00	
30	1E		Special Logon	01 00	01 00	
32	20		IPsec Quick Mode	00 00	00 00	
34	22		IPsec Extended Mode	00 00	00 00	
36	24		Other Logon/Logoff Events	00 00	00 00	
38	26		Network Policy Server	03 00	03 00	
40	28	Object Access	File System	00 00	00 00	
42	2A		Registry	00 00	00 00	
44	2C		Kernel Object	00 00	00 00	
46	2E		SAM	00 00	00 00	
48	30		Other Object Access Events	00 00	00 00	
50	32		Certification Services	00 00	00 00	
52	34		Application Generated	00 00	00 00	
54	36		Handle Manipulation	00 00	00 00	
56	38		File Share	00 00	00 00	
58	3A		Filtering Platform Packet Drop	00 00	00 00	
60	3C		Filtering Platform Connection	00 00	00 00	
62	3E		Detailed File Share	00 00	00 00	
64	40	Privilege Use	Sensitive Privilege Use	00 00	00 00	
66	42		Non Sensitive Privilege Use	00 00	00 00	
68	44		Other Privilege Use Events	00 00	00 00	
70	46	Detailed Tracking	Process Creation	00 00	00 00	
72	48		Process Termination	00 00	00 00	
74	4A		DPAPI Activity	00 00	00 00	
76	4C		RPC Events	00 00	00 00	
78	4E	Policy Change	Audit Policy Change	01 00	01 00	
80	50		Authentication Policy Change	01 00	01 00	
82	52		Authorization Policy Change	00 00	00 00	
84	54		MPSSVC Rule-Level Policy Change	00 00	00 00	
86	56		Filtering Platform Policy Change	00 00	00 00	
88	58		Other Policy Change Events	00 00	00 00	
90	5A	Account Management	User Account Management	01 00	01 00	
92	5C		Computer Account Management	00 00	01 00	
94	5E		Security Group Management	01 00	01 00	
96	60		Distribution Group Management	00 00	00 00	
98	62		Application Group Management	00 00	00 00	
100	64		Other Account Management Events	00 00	00 00	
102	66	DS Access	Directory Service Access	00 00	01 00	
104	68		Directory Service Changes	00 00	00 00	
106	6A		Directory Service Replication	00 00	00 00	
108	6C		Detailed Directory Service Replication	00 00	00 00	
110	6E	Account Logon	Credential Validation	00 00	01 00	
112	70		Kerberos Service Ticket Operations	00 00	01 00	
114	72		Other Account Logon Events	00 00	00 00	
116	74		Kerberos Authentication Service	00 00	01 00	
118	76	N/A		Unknown	Unknown	Unknown
120	78			05 00	05 00	
122	7A			09 00	09 00	
124	7C			0C 00	0C 00	
126	7E			03 00	03 00	
128	80			04 00	04 00	
130	82			06 00	06 00	
132	84			06 00	06 00	
134	86			04 00	04 00	
136	88			04 00	04 00	

rev. 2 (2010/08/08)

Windows 2008 x86/Vista Audit Policy Registry Structure (HKLM¥SECURITY¥Policy¥PolAdtEv)

Byte	Hex	Category/Subcategory		Default (2008 x86)	Default (Vista)	Description
0	0	N/A		00 01	00 01	Unknown
2	2			00 00	00 00	
4	4			09 00	09 00	
6	6			Unknown	Unknown	
8	8			76 00	76 00	
10	A			00 00	00 00	
12	C	System	Security State Change	01 00	01 00	00 00 : No Auditing 01 00 : Success 02 00 : Failure 03 00 : Success and Failure
14	E		Security System Extension	00 00	00 00	
16	10		System Integrity	03 00	03 00	
18	12		IPsec Driver	00 00	00 00	
20	14		Other System Events	03 00	03 00	
22	16	Logon/Logoff	Logon	03 00	01 00	
24	18		Logoff	01 00	01 00	
26	1A		Account Lockout	01 00	01 00	
28	1C		IPsec Main Mode	00 00	00 00	
30	1E		Special Logon	01 00	01 00	
32	20		IPsec Quick Mode	00 00	00 00	
34	22		IPsec Extended Mode	00 00	00 00	
36	24		Other Logon/Logoff Events	00 00	00 00	
38	26		Network Policy Server	03 00	00 00	
40	28	Object Access	File System	00 00	00 00	
42	2A		Registry	00 00	00 00	
44	2C		Kernel Object	00 00	00 00	
46	2E		SAM	00 00	00 00	
48	30		Other Object Access Events	00 00	00 00	
50	32		Certification Services	00 00	00 00	
52	34		Application Generated	00 00	00 00	
54	36		Handle Manipulation	00 00	00 00	
56	38		File Share	00 00	00 00	
58	3A		Filtering Platform Packet Drop	00 00	00 00	
60	3C		Filtering Platform Connection	00 00	00 00	
62	3E	Privilege Use	Sensitive Privilege Use	00 00	00 00	
64	40		Non Sensitive Privilege Use	00 00	00 00	
66	42		Other Privilege Use Events	00 00	00 00	
68	44	Detailed Tracking	Process Creation	00 00	00 00	
70	46		Process Termination	00 00	00 00	
72	48		DPAPI Activity	00 00	00 00	
74	4A		RPC Events	00 00	00 00	
76	4C	Policy Change	Audit Policy Change	01 00	01 00	
78	4E		Authentication Policy Change	01 00	01 00	
80	50		Authorization Policy Change	00 00	00 00	
82	52		MPSSVC Rule-Level Policy Change	00 00	00 00	
84	54		Filtering Platform Policy Change	00 00	00 00	
86	56		Other Policy Change Events	00 00	00 00	
88	58	Account Management	User Account Management	01 00	01 00	
90	5A		Computer Account Management	01 00	00 00	
92	5C		Security Group Management	01 00	01 00	
94	5E		Distribution Group Management	00 00	00 00	
96	60		Application Group Management	00 00	00 00	
98	62		Other Account Management Events	00 00	00 00	
100	64	DS Access	Directory Service Access	01 00	00 00	
102	66		Directory Service Changes	00 00	00 00	
104	68		Directory Service Replication	00 00	00 00	
106	6A		Detailed Directory Service Replication	00 00	00 00	
108	6C	Account Logon	Credential Validation	01 00	00 00	
110	6E		Kerberos Service Ticket Operations	01 00	00 00	
112	70		Other Account Logon Events	00 00	00 00	
114	72		Kerberos Authentication Service	01 00	00 00	
116	74	N/A		Unknown	Unknown	Unknown
118	76			05 00	05 00	
120	78			09 00	09 00	
122	7A			0B 00	0B 00	
124	7C			03 00	03 00	
126	7E			04 00	04 00	
128	80			06 00	06 00	
130	82			06 00	06 00	
132	84			04 00	04 00	
134	86			04 00	04 00	

rev. 2 (2010/08/08)