Audit Policy Registry Format (http://www.kazamiya.net/en/poladtev)

HKLM¥SECURITY¥Policy¥PolAdtEv

Offset Hex	Size	Category/Subcategory(Description) (* 00 00: No Auditing, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)		Value
0	2	Header	Unknown	00 01
2	2		Unknown	00 00
4	2		Number of categories	n
6	2		Unknown	
8	2		Offset to subcategory number of category 1	x
A	2		Unknown	00 00
C	2	Category 1	Subcategory 1	*
				*
C+2y	2		Subcategory y	*
	2	Category n	Subcategory 1	*
				*
	2		Subcategory z	*
x-2	2	Footer	Unknown	
x	2		Subcategory number of category 1	y
x+2n	2		Subcategory number of category n	z

rev. 4 (2017/01/29)

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

Offset Dec	Offset Hex	Category/Subcategory(Description) (00 00: No Auditing, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)		Default (Vista)	Default (2008 x86)
0	0	Header	Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4		Number of categories	09 00	09 00
6	6		Unknown	**00 00**	**1F 00**
8	8		Offset to subcategory number of System category	**76 00**	**76 00**
10	A		Unknown	00 00	00 00
12	C	System	Security State Change	01 00	01 00
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	**00 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	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	**00 00**	**01 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	**00 00**	**01 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	**00 00**	**01 00**
110	6E		Kerberos Service Ticket Operations	**00 00**	**01 00**
112	70		Other Account Logon Events	00 00	00 00
114	72		Kerberos Authentication Service	**00 00**	**01 00**
116	74	Footer	Unknown	00 00	00 00
118	**76**		Subcategory number of System	05 00	05 00
120	78		Subcategory number of Logon/Logoff	09 00	09 00
122	7A		Subcategory number of Object Access	0B 00	0B 00
124	7C		Subcategory number of Privilege Use	03 00	03 00
126	7E		Subcategory number of Detailed Tracking	04 00	04 00
128	80		Subcategory number of Policy Change	06 00	06 00
130	82		Subcategory number of Account Management	06 00	06 00
132	84		Subcategory number of DS Access	04 00	04 00
134	86		Subcategory number of Account Logon	04 00	04 00

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

Offset Dec	Offset Hex	Category/Subcategory(Description) (00 00: No Auditing, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)		Default (7)	Default (2008 x64)
0	0	Header	Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4		Number of categories	09 00	09 00
6	6		Unknown	00 00	00 00
8	8		Offset to subcategory number of System category	**78 00**	**78 00**
10	A		Unknown	00 00	00 00
12	C	System	Security State Change	01 00	01 00
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	Footer	Unknown	00 00	00 00
120	**78**		Subcategory number of System	05 00	05 00
122	7A		Subcategory number of Logon/Logoff	09 00	09 00
124	7C		Subcategory number of Object Access	**0C 00**	**0C 00**
126	7E		Subcategory number of Privilege Use	03 00	03 00
128	80		Subcategory number of Detailed Tracking	04 00	04 00
130	82		Subcategory number of Policy Change	06 00	06 00
132	84		Subcategory number of Account Management	06 00	06 00
134	86		Subcategory number of DS Access	04 00	04 00
136	88		Subcategory number of Account Logon	04 00	04 00

rev. 4 (2017/01/29)

Windows 8.1/2012 x64 (HKLM¥SECURITY¥Policy¥PolAdtEv)

Offset Dec	Offset Hex	Category/Subcategory(Description) (00 00: No Auditing, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)		Default (8.1)	Default (2012)
0	0	Header	Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4		Number of categories	09 00	09 00
6	6		Unknown	00 00	00 00
8	8		Offset to subcategory number of System category	**7E 00**	**7E 00**
10	A		Unknown	00 00	00 00
12	C	System	Security State Change	01 00	01 00
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		**User / Device Claims**	00 00	00 00
42	2A	Object Access	File System	00 00	00 00
44	2C		Registry	00 00	00 00
46	2E		Kernel Object	00 00	00 00
48	30		SAM	00 00	00 00
50	32		Other Object Access Events	00 00	00 00
52	34		Certification Services	00 00	00 00
54	36		Application Generated	00 00	00 00
56	38		Handle Manipulation	00 00	00 00
58	3A		File Share	00 00	00 00
60	3C		Filtering Platform Packet Drop	00 00	00 00
62	3E		Filtering Platform Connection	00 00	00 00
64	40		Detailed File Share	00 00	00 00
66	42		**Removable Storage**	00 00	00 00
68	44		**Central Access Policy Staging**	00 00	00 00
70	46	Privilege Use	Sensitive Privilege Use	00 00	00 00
72	48		Non Sensitive Privilege Use	00 00	00 00
74	4A		Other Privilege Use Events	00 00	00 00
76	4C	Detailed Tracking	Process Creation	00 00	00 00
78	4E		Process Termination	00 00	00 00
80	50		DPAPI Activity	00 00	00 00
82	52		RPC Events	00 00	00 00
84	54	Policy Change	Audit Policy Change	01 00	01 00
86	56		Authentication Policy Change	01 00	01 00
88	58		Authorization Policy Change	00 00	00 00
90	5A		MPSSVC Rule-Level Policy Change	00 00	00 00
92	5C		Filtering Platform Policy Change	00 00	00 00
94	5E		Other Policy Change Events	00 00	00 00
96	60	Account Management	User Account Management	01 00	01 00
98	62		Computer Account Management	**00 00**	**01 00**
100	64		Security Group Management	01 00	01 00
102	66		Distribution Group Management	00 00	00 00
104	68		Application Group Management	00 00	00 00
106	6A		Other Account Management Events	00 00	00 00
108	6C	DS Access	Directory Service Access	**00 00**	**01 00**
110	6E		Directory Service Changes	00 00	00 00
112	70		Directory Service Replication	00 00	00 00
114	72		Detailed Directory Service Replication	00 00	00 00
116	74	Account Logon	Credential Validation	**00 00**	**01 00**
118	76		Kerberos Service Ticket Operations	**00 00**	**01 00**
120	78		Other Account Logon Events	00 00	00 00
122	7A		Kerberos Authentication Service	**00 00**	**01 00**
124	7C	Footer	Unknown	**FE 7F**	**FD 7F**
126	**7E**		Subcategory number of System	05 00	05 00
128	80		Subcategory number of Logon/Logoff	**0A 00**	**0A 00**
130	82		Subcategory number of Object Access	**0E 00**	**0E 00**
132	84		Subcategory number of Privilege Use	03 00	03 00
134	86		Subcategory number of Detailed Tracking	04 00	04 00
136	88		Subcategory number of Policy Change	06 00	06 00
138	8A		Subcategory number of Account Management	06 00	06 00
140	8C		Subcategory number of DS Access	04 00	04 00
142	8E		Subcategory number of Account Logon	04 00	04 00

Windows 10/Server TP (HKLM¥SECURITY¥Policy¥PolAdtEv)

Offset Dec	Offset Hex	Category/Subcategory(Description) (00 00: No Auditing, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)		Default (10 TP)	Default (Server TP)
0	0	Header	Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4		Number of categories	09 00	09 00
6	6		Unknown	00 00	00 00
8	8		Offset to subcategory number of System category	**82 00**	**82 00**
10	A		Unknown	00 00	00 00
12	C	System	Security State Change	01 00	01 00
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		User / Device Claims	00 00	00 00
42	2A		**Group Membership**	00 00	00 00
44	2C	Object Access	File System	00 00	00 00
46	2E		Registry	00 00	00 00
48	30		Kernel Object	00 00	00 00
50	32		SAM	00 00	00 00
52	34		Other Object Access Events	00 00	00 00
54	36		Certification Services	00 00	00 00
56	38		Application Generated	00 00	00 00
58	3A		Handle Manipulation	00 00	00 00
60	3C		File Share	00 00	00 00
62	3E		Filtering Platform Packet Drop	00 00	00 00
64	40		Filtering Platform Connection	00 00	00 00
66	42		Detailed File Share	00 00	00 00
68	44		Removable Storage	00 00	00 00
70	46		Central Access Policy Staging	00 00	00 00
72	48	Privilege Use	Sensitive Privilege Use	00 00	00 00
74	4A		Non Sensitive Privilege Use	00 00	00 00
76	4C		Other Privilege Use Events	00 00	00 00
78	4E	Detailed Tracking	Process Creation	00 00	00 00
80	50		Process Termination	00 00	00 00
82	52		DPAPI Activity	00 00	00 00
84	54		RPC Events	00 00	00 00
86	56		**PNP Activity**	00 00	00 00
88	58	Policy Change	Audit Policy Change	01 00	01 00
90	5A		Authentication Policy Change	01 00	01 00
92	5C		Authorization Policy Change	00 00	00 00
94	5E		MPSSVC Rule-Level Policy Change	00 00	00 00
96	60		Filtering Platform Policy Change	00 00	00 00
98	62		Other Policy Change Events	00 00	00 00
100	64	Account Management	User Account Management	01 00	01 00
102	66		Computer Account Management	**00 00**	**01 00**
104	68		Security Group Management	01 00	01 00
106	6A		Distribution Group Management	00 00	00 00
108	6C		Application Group Management	00 00	00 00
110	6E		Other Account Management Events	00 00	00 00
112	70	DS Access	Directory Service Access	**00 00**	**01 00**
114	72		Directory Service Changes	00 00	00 00
116	74		Directory Service Replication	00 00	00 00
118	76		Detailed Directory Service Replication	00 00	00 00
120	78	Account Logon	Credential Validation	**00 00**	**01 00**
122	7A		Kerberos Service Ticket Operations	**00 00**	**01 00**
124	7C		Other Account Logon Events	00 00	00 00
126	7E		Kerberos Authentication Service	**00 00**	**01 00**
128	80	Footer	Unknown	**7F 8E**	**14 4F**
130	**82**		Subcategory number of System	05 00	05 00
132	84		Subcategory number of Logon/Logoff	**0B 00**	**0B 00**
134	86		Subcategory number of Object Access	0E 00	0E 00
136	88		Subcategory number of Privilege Use	03 00	03 00
138	8A		Subcategory number of Detailed Tracking	**05 00**	**05 00**
140	8C		Subcategory number of Policy Change	06 00	06 00
142	8E		Subcategory number of Account Management	06 00	06 00
144	90		Subcategory number of DS Access	04 00	04 00
146	92		Subcategory number of Account Logon	04 00	04 00

rev. 4 (2017/01/29)

Windows 10(1607)/2016 (HKLM¥SECURITY¥Policy¥PolAdtEv)

Offset Dec	Offset Hex	Category/Subcategory(Description) (00 00: No Auditing, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)		Default (10(1607))	Default (2016)
0	0	Header	Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4		Number of categories	09 00	09 00
6	6		Unknown	00 00	00 00
8	8		Offset to subcategory number of System category	**84 00**	**84 00**
10	A		Unknown	00 00	00 00
12	C	System	Security State Change	01 00	01 00
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		User / Device Claims	00 00	00 00
42	2A		Group Membership	00 00	00 00
44	2C	Object Access	File System	00 00	00 00
46	2E		Registry	00 00	00 00
48	30		Kernel Object	00 00	00 00
50	32		SAM	00 00	00 00
52	34		Other Object Access Events	00 00	00 00
54	36		Certification Services	00 00	00 00
56	38		Application Generated	00 00	00 00
58	3A		Handle Manipulation	00 00	00 00
60	3C		File Share	00 00	00 00
62	3E		Filtering Platform Packet Drop	00 00	00 00
64	40		Filtering Platform Connection	00 00	00 00
66	42		Detailed File Share	00 00	00 00
68	44		Removable Storage	00 00	00 00
70	46		Central Policy Staging	00 00	00 00
72	48	Privilege Use	Sensitive Privilege Use	00 00	00 00
74	4A		Non Sensitive Privilege Use	00 00	00 00
76	4C		Other Privilege Use Events	00 00	00 00
78	4E	Detailed Tracking	Process Creation	00 00	00 00
80	50		Process Termination	00 00	00 00
82	52		DPAPI Activity	00 00	00 00
84	54		RPC Events	00 00	00 00
86	56		Plug and Play Events	00 00	00 00
88	58		**Token Right Adjusted Events**	00 00	00 00
90	5A	Policy Change	Audit Policy Change	01 00	01 00
92	5C		Authentication Policy Change	01 00	01 00
94	5E		Authorization Policy Change	00 00	00 00
96	60		MPSSVC Rule-Level Policy Change	00 00	00 00
98	62		Filtering Platform Policy Change	00 00	00 00
100	64		Other Policy Change Events	00 00	00 00
102	66	Account Management	User Account Management	01 00	01 00
104	68		Computer Account Management	**00 00**	**01 00**
106	6A		Security Group Management	01 00	01 00
108	6C		Distribution Group Management	00 00	00 00
110	6E		Application Group Management	00 00	00 00
112	70		Other Account Management Events	00 00	00 00
114	72	DS Access	Directory Service Access	**00 00**	**01 00**
116	74		Directory Service Changes	00 00	00 00
118	76		Directory Service Replication	00 00	00 00
120	78		Detailed Directory Service Replication	00 00	00 00
122	7A	Account Logon	Credential Validation	**00 00**	**01 00**
124	7C		Kerberos Service Ticket Operations	**00 00**	**01 00**
126	7E		Other Account Logon Events	00 00	00 00
128	80		Kerberos Authentication Service	**00 00**	**01 00**
130	82	Footer	Unknown	**0C DB**	**33 CC**
132	**84**		Subcategory number of System	05 00	05 00
134	86		Subcategory number of Logon/Logoff	0B 00	0B 00
136	88		Subcategory number of Object Access	0E 00	0E 00
138	8A		Subcategory number of Privilege Use	03 00	03 00
140	8C		Subcategory number of Detailed Tracking	**06 00**	**06 00**
142	8E		Subcategory number of Policy Change	06 00	06 00
144	90		Subcategory number of Account Management	06 00	06 00
146	92		Subcategory number of DS Access	04 00	04 00
148	94		Subcategory number of Account Logon	04 00	04 00

rev. 4 (2017/01/29)