Audit Policy Registry Format (http://www.kazamiya.net/en/poladtev) HKLM¥SECURITY¥Policy¥PolAdtEv

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

rev. 4 (2017/01/29)

Offset Dec	Offset Hex	(00 00: No Auditi	Category/Subcategory(Description) ng, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)	Default (Vista)	Default (2008 x86
		(00 001 110 714414			
0	0		Unknown	00 01	00 01
2		2	Unknown	00 00	00 00
4	4	Header	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	А		Unknown	00 00	00 00
12	С		Security State Change	01 00	01 00
14	E		Security System Extension	00 00	00 00
16	10	System	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	01 00	03 00
24	18		Logoff	01 00	01 00
	1				
26	1A		Account Lockout	01 00	01 00
28	1C		IPsec Main Mode	00 00	00 00
30	1E	Logon/Logoff	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		File System	00 00	00 00
	1				
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	Object Access	Certification Services	00 00	00 00
52	34		Application Generated	00 00	00 00
54	36		Handle Manipulation	00 00	00 00
	1		· ·		
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		Sensitive Privilege Use	00 00	00 00
64	40	Privilege Use	Non Sensitive Privilege Use	00 00	00 00
66	42		Other Privilege Use Events	00 00	00 00
68	44		Process Creation	00 00	00 00
70	46		Process Termination	00 00	00 00
		Detailed Tracking			
72	48		DPAPI Activity	00 00	00 00
74	4A		RPC Events	00 00	00 00
76	4C		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	Policy Change	MPSSVC Rule-Level Policy Change	00 00	00 00
84	54		Filtering Platform Policy Change	00 00	00 00
	1				
86	56		Other Policy Change Events	00 00	00 00
88	58		User Account Management	01 00	01 00
90	5A		Computer Account Management	00 00	01 00
92	5C	Account Management	Security Group Management	01 00	01 00
94	5E	ccoant riundyement	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		Directory Service Access	00 00	01 00
100	66			00 00	00 00
	1	DS Access	Directory Service Changes		
104	68		Directory Service Replication	00 00	00 00
106	6A		Detailed Directory Service Replication	00 00	00 00
108	6C		Credential Validation	00 00	01 00
110	6E	Account Logan	Kerberos Service Ticket Operations	00 00	01 00
112	70	Account Logon	Other Account Logon Events	00 00	00 00
114	72		Kerberos Authentication Service	00 00	01 00
116	74		Unknown	00 00	00 00
	1				
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	Footer	Subcategory number of Privilege Use	03 00	03 00
126	7E	rooter	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
	1				
132	84		Subcategory number of DS Access	04 00	04 00
134	86		Subcategory number of Account Logon	04 00	04 00

rev. 4 (2017/01/29)

	Offset	(00.00	Category/Subcategory(Description)	Default	Default
Dec	Hex	(00 00: No Auditi	ng, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)	(7)	(2008 x64
0	0		Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4	Header	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	Α		Unknown	00 00	00 00
12	C		Security State Change	01 00	01 00
14	E		Security System Extension	00 00	00 00
16	10	System	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	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	Logon/Logoff	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		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	Object Access	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		Sensitive Privilege Use	00 00	00 00
		Privilege Use	-		
66	42	Privilege Use	Non Sensitive Privilege Use	00 00	00 00
68	44		Other Privilege Use Events	00 00	00 00
70	46		Process Creation	00 00	00 00
72	48	Detailed Tracking	Process Termination	00 00	00 00
74	4A		DPAPI Activity	00 00	00 00
76	4C		RPC Events	00 00	00 00
78	4E		Audit Policy Change	01 00	01 00
80	50		Authentication Policy Change	01 00	01 00
82	52	Policy Change	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				00 00
	١, ٠١		User Account Management	01 00	01 00
92	5C		User Account Management Computer Account Management	01 00 00 00	
92 94		Account Management			01 00
	5C	Account Management	Computer Account Management	00 00	01 00 01 00
94	5C 5E	Account Management	Computer Account Management Security Group Management	00 00 01 00	01 00 01 00 01 00
94 96	5C 5E 60	Account Management	Computer Account Management Security Group Management Distribution Group Management	00 00 01 00 00 00	01 00 01 00 01 00 00 00
94 96 98	5C 5E 60 62	Account Management	Computer Account Management Security Group Management Distribution Group Management Application Group Management	00 00 01 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00
94 96 98 100	5C 5E 60 62 64		Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events	00 00 01 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00
94 96 98 100	5C 5E 60 62 64 66	Account Management DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access	00 00 01 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00
94 96 98 100 102 104	5C 5E 60 62 64 66 68		Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes	00 00 01 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00
94 96 98 100 102 104 106	5C 5E 60 62 64 66 68 6A		Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication	00 00 01 00 00 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00
94 96 98 100 102 104 106 108	5C 5E 60 62 64 66 68 6A 6C	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Replication Detailed Directory Service Replication	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
94 96 98 100 102 104 106 108	5C 5E 60 62 64 66 68 6A 6C		Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00
94 96 98 100 102 104 106 108 110 112	5C 5E 60 62 64 66 68 6A 6C 6E 70	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 01 00 01 00 01 00
94 96 98 100 102 104 106 108 110 112 114	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 01 00 01 00 01 00
94 96 98 100 102 104 106 108 110 112 114 116	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 01 00 01 00 01 00 01 00
94 96 98 100 102 104 106 108 110 112 114 116 118 120	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74 76 78	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System	00 00 01 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 01 00 01 00 01 00 01 00 01 00 01 00
94 96 98 100 102 104 106 108 110 112 114 116 118 120 122	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74 76 78	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System Subcategory number of Logon/Logoff	00 00 01 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 01 00 01 00 01 00 01 00 00 00 01 00 00 00 01 00 01 00 00 00
94 96 98 100 102 104 106 108 110 112 114 116 118 120 122 124	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74 76 78 7A	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System Subcategory number of Logon/Logoff Subcategory number of Object Access	00 00 01 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00
94 96 98 100 102 104 106 108 110 112 114 116 118 120 122 124 126	5C 5E 60 62 64 66 68 6A 6C 70 72 74 76 78 7A 7C 7E	DS Access	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System Subcategory number of Logon/Logoff Subcategory number of Object Access Subcategory number of Privilege Use	00 00 01 00 00 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 01 00 01 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
94 96 98 100 102 104 106 108 110 112 114 116 118 120 122 124 126 128	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74 76 78 7A 7C 7E 80	DS Access Account Logon	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System Subcategory number of Logon/Logoff Subcategory number of Privilege Use Subcategory number of Privilege Use Subcategory number of Detailed Tracking	00 00 01 00	01 00 01 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 01 00 01 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
94 96 98 100 102 104 106 108 110 112 114 116 118 120 122 124 126 128 130	5C 5E 60 62 64 66 68 6A 6C 72 74 76 78 7A 7C 7E 80 82	DS Access Account Logon	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System Subcategory number of Doject Access Subcategory number of Privilege Use Subcategory number of Detailed Tracking Subcategory number of Policy Change	00 00 01 00	01 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
94 96 98 100 102 104 106 108 110 112 114 116 118 120 122 124 126 128	5C 5E 60 62 64 66 68 6A 6C 6E 70 72 74 76 78 7A 7C 7E 80	DS Access Account Logon	Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Credential Validation Kerberos Service Ticket Operations Other Account Logon Events Kerberos Authentication Service Unknown Subcategory number of System Subcategory number of Logon/Logoff Subcategory number of Privilege Use Subcategory number of Privilege Use Subcategory number of Detailed Tracking	00 00 01 00	01 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0

Windows	s 8.1/20	12 x64 (HKLM¥SECURITY	'¥Policy¥PolAdtEv)	ī	T
Offset Dec	Offset Hex	(00 00: No Auditi	Category/Subcategory(Description) ng, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)	Default (8.1)	Default (2012)
0	0		Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4			09 00	09 00
		Header	Number of categories		
6	6		Unknown	00 00	00 00
8	8		Offset to subcategory number of System category	7E 00	7E 00
10	Α		Unknown	00 00	00 00
12	С		Security State Change	01 00	01 00
14	Е		Security System Extension	00 00	00 00
16	10	System	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	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	Logon/Logoff	Special Logon	01 00	01 00
32	20	5	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		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
	38	Object Access		00 00	00 00
56			Handle Manipulation		
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		Sensitive Privilege Use	00 00	00 00
72	48	Privilege Use	-	00 00	00 00
		riiviiege Ose	Non Sensitive Privilege Use		
74	4A		Other Privilege Use Events	00 00	00 00
76	4C		Process Creation	00 00	00 00
78	4E	Detailed Tracking	Process Termination	00 00	00 00
80	50	Detailed Tracking	DPAPI Activity	00 00	00 00
82	52		RPC Events	00 00	00 00
84	54		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
		Policy Change			
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		User Account Management	01 00	01 00
98	62		Computer Account Management	00 00	01 00
100	64	A	Security Group Management	01 00	01 00
102	66	Account Management	Distribution Group Management	00 00	00 00
104	68		Application Group Management	00 00	00 00
			''		00 00
106	6A		Other Account Management Events	00 00	
108	6C		Directory Service Access	00 00	01 00
110	6E	DS Access	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		Credential Validation	00 00	01 00
118	76		Kerberos Service Ticket Operations	00 00	01 00
120	78	Account Logon	Other Account Logon Events	00 00	00 00
			-		
122	7A		Kerberos Authentication Service	00 00	01 00
124	7C		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
	82		Subcategory number of Object Access	0E 00	0E 00
130			Subcategory number of Privilege Use	03 00	03 00
	24	Footer	Subcategory number of Privilege ose Subcategory number of Detailed Tracking	04 00	03 00
132	84 86				UT UU
132 134	86				06.65
132 134 136	86 88		Subcategory number of Policy Change	06 00	06 00
132 134	86				06 00 06 00
132 134 136	86 88		Subcategory number of Policy Change	06 00	

Windows	s 10/Sen	ver TP (HKLM¥SECURITY	¥Policy¥PolAdtEv)		
Offset	Offset		Category/Subcategory(Description)	Default	Default
Dec	Hex	(00 00: No Auditi	ng, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)	(10 TP)	(Server TP)
0	0		Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4		Number of categories	09 00	09 00
6	6	Header	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		Security State Change	01 00	01 00
14	Е		Security System Extension	00 00	00 00
16	10	System	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	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	Logon/Logoff	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
40	2A		Group Membership	00 00	00 00
44	2C		File System	00 00	00 00
46	2C 2E		Registry	00 00	00 00
48	2E 30			00 00	00 00
			Kernel Object		
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	Object Access	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		Sensitive Privilege Use	00 00	00 00
74	4A	Privilege Use	Non Sensitive Privilege Use	00 00	00 00
76	4C		Other Privilege Use Events	00 00	00 00
78	4E		Process Creation	00 00	00 00
80	50		Process Termination	00 00	00 00
82	52	Detailed Tracking	DPAPI Activity	00 00	00 00
84	54		RPC Events	00 00	00 00
86	56		PNP Activity	00 00	00 00
88	58		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	Policy Change	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		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
104	6A	Account Management	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
110	70			00 00	01 00
112	70 72		Directory Service Access	00 00	01 00
		DS Access	Directory Service Changes	00 00	00 00
116	74 76		Directory Service Replication		
118	76 78		Detailed Directory Service Replication	00 00	00 00
120			Credential Validation	00 00	01 00
122	7A	Account Logon	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
	80		Unknown	7F 8E	14 4F
128			Subcategory number of System	05 00	05 00
130	82				100.00
			Subcategory number of Logon/Logoff	0В 00	0В 00
130	82		Subcategory number of Logon/Logoff Subcategory number of Object Access	OB 00 OE 00	0E 00
130 132	82 84	Footer			
130 132 134	82 84 86	Footer	Subcategory number of Object Access	0E 00	0E 00
130 132 134 136	82 84 86 88	Footer	Subcategory number of Object Access Subcategory number of Privilege Use	0E 00 03 00	0E 00 03 00
130 132 134 136 138	82 84 86 88 8A	Footer	Subcategory number of Object Access Subcategory number of Privilege Use Subcategory number of Detailed Tracking	0E 00 03 00 05 00	0E 00 03 00 05 00
130 132 134 136 138 140	82 84 86 88 8A 8C	Footer	Subcategory number of Object Access Subcategory number of Privilege Use Subcategory number of Detailed Tracking Subcategory number of Policy Change	0E 00 03 00 05 00 06 00	0E 00 03 00 05 00 06 00

rev. 4 (2017/01/29)

Offset Dec	Offset Hex	(00 00: No Auditi	Category/Subcategory(Description) ng, 01 00: Success, 02 00: Failure, 03 00: Success and Failure)	Default (10(1607))	Default (2016)
0	0		Unknown	00 01	00 01
2	2		Unknown	00 00	00 00
4	4	Header	Number of categories	09 00	09 00
6	6	rieddei	Unknown	00 00	00 00
8	8		Offset to subcategory number of System category	84 00	84 00
10	Α		Unknown	00 00	00 00
12	C		Security State Change	01 00	01 00
14	Е		Security System Extension	00 00	00 00
16	10	System	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	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	Logon/Logoff	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		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	Object Access	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		Sensitive Privilege Use	00 00	00 00
74	4A	Privilege Use	Non Sensitive Privilege Use	00 00	00 00
76	4C		Other Privilege Use Events	00 00	00 00
78	4E		Process Creation	00 00	00 00
80	50		Process Termination	00 00	00 00
82	52	Detailed Tracking	DPAPI Activity	00 00	00 00
84	54	Detailed Tracking	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		Audit Policy Change	01 00	01 00
92	5C		Authentication Policy Change	01 00	01 00
94	5E	Delias Char	Authorization Policy Change	00 00	00 00
96	60	Policy Change	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		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	Account Management	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		Directory Service Access	00 00	01 00
116	74		Directory Service Changes	00 00	00 00
118	76	DS Access	Directory Service Replication	00 00	00 00
120	78		Detailed Directory Service Replication	00 00	00 00
122	76 7A		Credential Validation	00 00	01 00
124	7C		Kerberos Service Ticket Operations	00 00	01 00
124	7C 7E	Account Logon	Other Account Logon Events	00 00	00 00
128	80		Kerberos Authentication Service	00 00	01 00
130	82		Unknown	OC 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	Footer	Subcategory number of Privilege Use	03 00	03 00
140	8C	. 55557	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
			Subcategory number of Account Logon	04 00	04 00