



Kabylake Platforms RVP/CRB BIOS Release Notes

Kabylake – SPT LP / SPT H

August 2017 (WW32, 2017)

CRB BIOS v103

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

45-nm products are manufactured on a lead-free process. Lead-free per EU RoHS directive July, 2006. Some E.U. RoHS exemptions may apply to other components used in the product package. Residual amounts of halogens are below November, 2007 proposed IPC/JEDEC J-STD-709 standards.

Intel, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2008, Intel Corporation. All rights reserved.



Contents

1	SPI Images	19
1.1	SPI Images for Kabylake (KBL + SPT LP / SPT H) platforms.....	19
2	Supported Hot Keys	20
2.1	ACPI Hot-keys	20
3	BIOS – KBL CRB v103	21
3.1	Resolved Client BIOS HSD sightings.....	22
3.2	BP Client Common Core Sync-up Changes	22
4	BIOS – KBL CRB v102	23
4.1	Resolved Client BIOS HSD sightings.....	24
4.2	BP Client Common Core Sync-up Changes	24
5	BIOS – KBL CRB v101	26
5.1	Resolved Client BIOS HSD sightings.....	27
5.2	BP Client Common Core Sync-up Changes	27
5.3	Known Issues / Limitations	27
6	BIOS – KBL CRB v100	28
6.1	Resolved Client BIOS HSD sightings.....	29
6.2	BP Client Common Core Sync-up Changes	29
6.3	Known Issues / Limitations	29
7	BIOS – KBL CRB v099	30
7.1	Resolved Client BIOS HSD sightings.....	31
7.2	BP Client Common Core Sync-up Changes	31
7.3	Known Issues / Limitations	31
8	BIOS – KBL CRB v098	32
8.1	Resolved Client BIOS HSD sightings.....	33
8.2	BP Client Common Core Sync-up Changes	33
8.3	Known Issues / Limitations	33
9	BIOS – KBL CRB v097	35
9.1	Resolved Client BIOS HSD sightings.....	36
9.2	BP Client Common Core Sync-up Changes	37
9.3	Known Issues / Limitations	37
10	BIOS – KBL CRB v096	38
10.1	Resolved Client BIOS HSD sightings.....	39
10.2	BP Client Common Core Sync-up Changes	39
10.3	Known Issues / Limitations	39
11	BIOS – KBL CRB v095	40
11.1	Resolved Client BIOS HSD sightings.....	41
11.2	BP Client Common Core Sync-up Changes	41
11.3	Known Issues / Limitations	41
12	BIOS – KBL CRB v094.1	42



	12.1	Resolved Client BIOS HSD sightings.....	43
	12.2	BP Client Common Core Sync-up Changes	44
	12.3	Known Issues / Limitations	44
13		BIOS – KBL CRB v093	45
	13.1	Resolved Client BIOS HSD sightings.....	46
	13.2	BP Client Common Core Sync-up Changes	46
	13.3	Known Issues / Limitations	46
14		BIOS – KBL CRB v092	47
	14.1	Resolved Client BIOS HSD sightings.....	48
	14.2	BP Client Common Core Sync-up Changes	49
	14.3	Known Issues / Limitations	49
15		BIOS – KBL CRB v091	50
	15.1	Resolved Client BIOS HSD sightings.....	51
	15.2	BP Client Common Core Sync-up Changes	51
	15.3	Known Issues / Limitations	51
16		BIOS – KBL CRB v090	52
	16.1	Resolved Client BIOS HSD sightings.....	53
	16.2	BP Client Common Core Sync-up Changes	53
	16.3	Known Issues / Limitations	53
17		BIOS – KBL CRB v089	54
	17.1	Resolved Client BIOS HSD sightings.....	55
	17.2	BP Client Common Core Sync-up Changes	55
	17.3	Known Issues / Limitations	55
18		BIOS – KBL CRB v088	56
	18.1	Resolved Client BIOS HSD sightings.....	57
	18.2	BP Client Common Core Sync-up Changes	57
	18.3	Known Issues / Limitations	58
19		BIOS – KBL CRB v087	59
	19.1	Resolved Client BIOS HSD sightings.....	60
	19.2	BP Client Common Core Sync-up Changes	61
	19.3	Known Issues / Limitations	61
20		BIOS – KBL CRB v086	62
	20.1	Resolved Client BIOS HSD sightings.....	63
	20.2	BP Client Common Core Sync-up Changes	64
	20.3	Known Issues / Limitations	64
21		BIOS – KBL CRB v085	65
	21.1	Resolved Client BIOS HSD sightings.....	66
	21.2	BP Client Common Core Sync-up Changes	67
	21.3	Known Issues / Limitations	67
22		BIOS – KBL CRB v084	68
	22.1	Resolved Client BIOS HSD sightings.....	69
	22.2	BP Client Common Core Sync-up Changes	70
	22.3	Known Issues / Limitations	70



23	BIOS – KBL CRB v083	71
	23.1 Resolved Client BIOS HSD sightings.....	72
	23.2 BP Client Common Core Sync-up Changes	73
	23.3 Known Issues / Limitations	73
24	BIOS – KBL CRB v082	74
	24.1 Resolved Client BIOS HSD sightings.....	75
	24.2 BP Client Common Core Sync-up Changes	75
	24.3 Known Issues / Limitations	75
25	BIOS – KBL CRB v081	77
	25.1 Resolved Client BIOS HSD sightings.....	78
	25.2 BP Client Common Core Sync-up Changes	78
	25.3 Known Issues / Limitations	78
26	BIOS – KBL CRB v080	80
	26.1 Resolved Client BIOS HSD sightings.....	81
	26.2 BP Client Common Core Sync-up Changes	82
	26.3 Known Issues / Limitations	82
27	BIOS – KBL CRB v079	83
	27.1 Resolved Client BIOS HSD sightings.....	84
	27.2 BP Client Common Core Sync-up Changes	84
	27.3 Known Issues / Limitations	84
28	BIOS – KBL CRB v078	85
	28.1 Resolved Client BIOS HSD sightings.....	86
	28.2 BP Client Common Core Sync-up Changes	87
	28.3 Known Issues / Limitations	87
29	BIOS – KBL CRB v077	88
	29.1 Resolved Client BIOS HSD sightings.....	89
	29.2 BP Client Common Core Sync-up Changes	90
	29.3 Known Issues / Limitations	90
30	BIOS – KBL CRB v076	91
	30.1 Resolved Client BIOS HSD sightings.....	92
	30.2 BP Client Common Core Sync-up Changes	93
	30.3 Known Issues / Limitations	93
31	BIOS – KBL CRB v075	94
	31.1 Resolved Client BIOS HSD sightings.....	95
	31.2 BP Client Common Core Sync-up Changes	96
	31.3 Known Issues / Limitations	96
32	BIOS – KBL CRB v074	97
	32.1 Resolved Client BIOS HSD sightings.....	98
	32.2 BP Client Common Core Sync-up Changes	98
	32.3 Known Issues / Limitations	98
33	BIOS – KBL CRB v073.1.....	99
	33.1 Resolved Client BIOS HSD sightings.....	100
	33.2 BP Client Common Core Sync-up Changes	100



	33.3	Known Issues / Limitations	101
34		BIOS – KBL CRB v072	102
	34.1	Resolved Client BIOS HSD sightings.....	103
	34.2	BP Client Common Core Sync-up Changes	103
	34.3	Known Issues / Limitations	103
35		BIOS – KBL CRB v071	104
	35.1	Resolved Client BIOS HSD sightings.....	105
	35.2	BP Client Common Core Sync-up Changes	105
	35.3	Known Issues / Limitations	105
36		BIOS – KBL CRB v070	106
	36.1	Resolved Client BIOS HSD sightings.....	107
	36.2	BP Client Common Core Sync-up Changes	107
	36.3	Known Issues / Limitations	107
37		BIOS – KBL CRB v069.2.....	108
	37.1	Resolved Client BIOS HSD sightings.....	109
	37.2	BP Client Common Core Sync-up Changes	109
	37.3	Known Issues / Limitations	109
38		BIOS – KBL CRB v069.1.....	110
	38.1	Resolved Client BIOS HSD sightings.....	111
	38.2	BP Client Common Core Sync-up Changes	111
	38.3	Known Issues / Limitations	111
39		BIOS – KBL CRB v069	112
	39.1	Resolved Client BIOS HSD sightings.....	113
	39.2	BP Client Common Core Sync-up Changes	114
	39.3	Known Issues / Limitations	114
40		BIOS – KBL CRB v068	115
	40.1	Resolved Client BIOS HSD sightings.....	116
	40.2	BP Client Common Core Sync-up Changes	116
	40.3	Known Issues / Limitations	116
41		BIOS – KBL CRB v067	118
	41.1	Resolved Client BIOS HSD sightings.....	119
	41.2	BP Client Common Core Sync-up Changes	119
	41.3	Known Issues / Limitations	119
42		BIOS – KBL CRB v066	120
	42.1	Resolved Client BIOS HSD sightings.....	121
	42.2	BP Client Common Core Sync-up Changes	122
	42.3	Known Issues / Limitations	122
43		BIOS – KBL CRB v065	123
	43.1	Resolved Client BIOS HSD sightings.....	124
	43.2	BP Client Common Core Sync-up Changes	125
	43.3	Known Issues / Limitations	125
44		BIOS – KBL CRB v064	126
	44.1	Resolved Client BIOS HSD sightings.....	127



	44.2	BP Client Common Core Sync-up Changes	127
	44.3	Known Issues / Limitations	128
45		BIOS – KBL CRB v063	129
	45.1	Resolved Client BIOS HSD sightings.....	130
	45.2	BP Client Common Core Sync-up Changes	131
	45.3	Known Issues / Limitations	131
46		BIOS – KBL CRB v062	132
	46.1	Resolved Client BIOS HSD sightings.....	133
	46.2	BP Client Common Core Sync-up Changes	134
	46.3	Known Issues / Limitations	134
47		BIOS – KBL CRB v061	135
	47.1	Resolved Client BIOS HSD sightings.....	136
	47.2	BP Client Common Core Sync-up Changes	136
	47.3	Known Issues / Limitations	136
48		BIOS – KBL CRB v060	137
	48.1	Resolved Client BIOS HSD sightings.....	138
	48.2	BP Client Common Core Sync-up Changes	138
	48.3	Known Issues / Limitations	138
49		BIOS – KBL CRB v059	139
	49.1	Resolved Client BIOS HSD sightings.....	140
	49.2	BP Client Common Core Sync-up Changes	141
	49.3	Known Issues / Limitations	141
50		BIOS – KBL CRB v058	142
	50.1	Resolved Client BIOS HSD sightings.....	143
	50.2	BP Client Common Core Sync-up Changes	143
	50.3	Known Issues / Limitations	144
51		BIOS – KBL CRB v057	145
	51.1	Resolved Client BIOS HSD sightings.....	146
	51.2	BP Client Common Core Sync-up Changes	147
	51.3	Known Issues / Limitations	147
52		BIOS – KBL CRB v056	148
	52.1	Resolved Client BIOS HSD sightings.....	149
	52.2	BP Client Common Core Sync-up Changes	149
	52.3	Known Issues / Limitations	149
53		BIOS – KBL CRB v055	150
	53.1	Resolved Client BIOS HSD sightings.....	151
	53.2	BP Client Common Core Sync-up Changes	152
	53.3	Known Issues / Limitations	152
54		BIOS – KBL CRB v054	153
	54.1	Resolved Client BIOS HSD sightings.....	154
	54.2	BP Client Common Core Sync-up Changes	155
	54.3	Known Issues / Limitations	155
55		BIOS – KBL CRB v053	156



	55.1	Resolved Client BIOS HSD sightings.....	157
	55.2	BP Client Common Core Sync-up Changes	157
	55.3	Known Issues / Limitations	157
56		BIOS – KBL CRB v052.1	159
	56.1	Resolved Client BIOS HSD sightings.....	160
	56.2	BP Client Common Core Sync-up Changes	161
	56.3	Known Issues / Limitations	161
57		BIOS – KBL CRB v051	162
	57.1	Resolved Client BIOS HSD sightings.....	163
	57.2	BP Client Common Core Sync-up Changes	164
	57.3	Known Issues / Limitations	164
58		BIOS – KBL CRB v050.1	165
	58.1	Resolved Client BIOS HSD sightings.....	166
	58.2	BP Client Common Core Sync-up Changes	166
	58.3	Known Issues / Limitations	166
59		BIOS – KBL CRB v050	167
	59.1	Resolved Client BIOS HSD sightings.....	168
	59.2	BP Client Common Core Sync-up Changes	168
	59.3	Known Issues / Limitations	168
60		BIOS – KBL CRB v049.1	169
	60.1	Resolved Client BIOS HSD sightings.....	170
	60.2	BP Client Common Core Sync-up Changes	170
	60.3	Known Issues / Limitations	170
61		BIOS – KBL CRB v049	171
	61.1	Resolved Client BIOS HSD sightings.....	172
	61.2	BP Client Common Core Sync-up Changes	172
	61.3	Known Issues / Limitations	173
62		BIOS – KBL CRB v048	174
	62.1	Resolved Client BIOS HSD sightings.....	175
	62.2	BP Client Common Core Sync-up Changes	175
	62.3	Known Issues / Limitations	176
63		BIOS – KBL CRB v047.1	177
	63.1	Resolved Client BIOS HSD sightings.....	178
	63.2	BP Client Common Core Sync-up Changes	178
	63.3	Known Issues / Limitations	178
64		BIOS – KBL CRB v047	179
	64.1	Resolved Client BIOS HSD sightings.....	180
	64.2	BP Client Common Core Sync-up Changes	181
	64.3	Known Issues / Limitations	181
65		BIOS – KBL CRB v046	182
	65.1	Resolved Client BIOS HSD sightings.....	183
	65.2	BP Client Common Core Sync-up Changes	184
	65.3	Known Issues / Limitations	184



66	BIOS – KBL CRB v045.1	185
	66.1 Resolved Client BIOS HSD sightings	186
	66.2 BP Client Common Core Sync-up Changes	186
	66.3 Known Issues / Limitations	186
67	BIOS – KBL CRB v045	187
	67.1 Resolved Client BIOS HSD sightings	188
	67.2 BP Client Common Core Sync-up Changes	189
	67.3 Known Issues / Limitations	189
68	BIOS – KBL CRB v044	190
	68.1 Resolved Client BIOS HSD sightings	191
	68.2 BP Client Common Core Sync-up Changes	192
	68.3 Known Issues / Limitations	192
69	BIOS – KBL CRB v043.3	193
	69.1 Resolved Client BIOS HSD sightings	194
	69.2 BP Client Common Core Sync-up Changes	194
	69.3 Known Issues / Limitations	194
70	BIOS – KBL CRB v043.2	195
	70.1 Resolved Client BIOS HSD sightings	196
	70.2 BP Client Common Core Sync-up Changes	196
	70.3 Known Issues / Limitations	196
71	BIOS – KBL CRB v043	197
	71.1 Resolved Client BIOS HSD sightings	198
	71.2 BP Client Common Core Sync-up Changes	199
	71.3 Known Issues / Limitations	199
72	BIOS – KBL CRB v042	200
	72.1 Resolved Client BIOS HSD sightings	201
	72.2 BP Client Common Core Sync-up Changes	202
	72.3 Known Issues / Limitations	202
73	BIOS – KBL CRB v041	203
	73.1 Resolved Client BIOS HSD sightings	204
	73.2 BP Client Common Core Sync-up Changes	205
	73.3 Known Issues / Limitations	205
74	BIOS – KBL CRB v040	206
	74.1 Resolved Client BIOS HSD sightings	207
	74.2 BP Client Common Core Sync-up Changes	210
	74.3 Known Issues / Limitations	210
75	BIOS – KBL CRB v039.1	211
	75.1 Resolved Client BIOS HSD sightings	212
	75.2 BP Client Common Core Sync-up Changes	212
	75.3 Known Issues / Limitations	212
76	BIOS – KBL CRB v039	213
	76.1 Resolved Client BIOS HSD sightings	214
	76.2 BP Client Common Core Sync-up Changes	214



	76.3	Known Issues / Limitations	214
77		BIOS – KBL CRB v038	215
	77.1	Resolved Client BIOS HSD sightings.....	216
	77.2	BP Client Common Core Sync-up Changes	218
	77.3	Known Issues / Limitations	218
78		BIOS – KBL CRB v037	219
	78.1	Resolved Client BIOS HSD sightings.....	220
	78.2	BP Client Common Core Sync-up Changes	221
	78.3	Known Issues / Limitations	221
79		BIOS – KBL CRB v036	222
	79.1	Resolved Client BIOS HSD sightings.....	223
	79.2	BP Client Common Core Sync-up Changes	224
	79.3	Known Issues / Limitations	224
80		BIOS – KBL CRB v035	225
	80.1	Resolved Client BIOS HSD sightings.....	226
	80.2	BP Client Common Core Sync-up Changes	227
	80.3	Known Issues / Limitations	227
81		BIOS – KBL CRB v034	228
	81.1	Resolved Client BIOS HSD sightings.....	229
	81.2	BP Client Common Core Sync-up Changes	230
	81.3	Known Issues / Limitations	230
82		BIOS – KBL CRB v033.1	231
	82.1	Resolved Client BIOS HSD sightings.....	232
	82.2	BP Client Common Core Sync-up Changes	232
	82.3	Known Issues / Limitations	232
83		BIOS – KBL CRB v033	233
	83.1	Resolved Client BIOS HSD sightings.....	234
	83.2	BP Client Common Core Sync-up Changes	234
	83.3	Known Issues / Limitations	234
84		BIOS – KBL CRB v032	235
	84.1	Resolved Client BIOS HSD sightings.....	236
	84.2	BP Client Common Core Sync-up Changes	237
	84.3	Known Issues / Limitations	237
85		BIOS – KBL CRB v031	238
	85.1	Resolved Client BIOS HSD sightings.....	239
	85.2	BP Client Common Core Sync-up Changes	240
	85.3	Known Issues / Limitations	240
86		BIOS – KBL CRB v030	241
	86.1	Resolved Client BIOS HSD sightings.....	242
	86.2	BP Client Common Core Sync-up Changes	243
	86.3	Known Issues / Limitations	243
87		BIOS – KBL CRB v029	244
	87.1	Resolved Client BIOS HSD sightings.....	245



	87.2	BP Client Common Core Sync-up Changes	245
	87.3	Known Issues / Limitations	245
88		BIOS – KBL CRB v028.1	246
	88.1	Resolved Client BIOS HSD sightings	247
	88.2	BP Client Common Core Sync-up Changes	247
	88.3	Known Issues / Limitations	247
89		BIOS – KBL CRB v028	248
	89.1	Resolved Client BIOS HSD sightings	249
	89.2	BP Client Common Core Sync-up Changes	250
	89.3	Known Issues / Limitations	250
90		BIOS – KBL CRB v027	251
	90.1	Resolved Client BIOS HSD sightings	252
	90.2	BP Client Common Core Sync-up Changes	253
	90.3	Known Issues / Limitations	253
91		BIOS – KBL CRB v026	254
	91.1	Resolved Client BIOS HSD sightings	255
	91.2	BP Client Common Core Sync-up Changes	256
	91.3	Known Issues / Limitations	256
92		BIOS – KBL CRB v025.1	258
	92.1	Resolved Client BIOS HSD sightings	259
	92.2	BP Client Common Core Sync-up Changes	259
	92.3	Known Issues / Limitations	259
93		BIOS – KBL CRB v025	260
	93.1	Resolved Client BIOS HSD sightings	261
	93.2	BP Client Common Core Sync-up Changes	263
	93.3	Known Issues / Limitations	263
94		BIOS – KBL CRB v024	264
	94.1	Resolved Client BIOS HSD sightings	265
	94.2	BP Client Common Core Sync-up Changes	267
	94.3	Known Issues / Limitations	267
95		BIOS – KBL CRB v023.1	268
	95.1	Resolved Client BIOS HSD sightings	269
	95.2	BP Client Common Core Sync-up Changes	269
	95.3	Known Issues / Limitations	269
96		BIOS – KBL CRB v023	270
	96.1	Resolved Client BIOS HSD sightings	271
	96.2	BP Client Common Core Sync-up Changes	272
	96.3	Known Issues / Limitations	272
97		BIOS – KBL CRB v022	273
	97.1	Resolved Client BIOS HSD sightings	274
	97.2	BP Client Common Core Sync-up Changes	275
	97.3	Known Issues / Limitations	275
98		BIOS – KBL CRB v021	276



	98.1	Resolved Client BIOS HSD sightings.....	277
	98.2	BP Client Common Core Sync-up Changes	277
	98.3	Known Issues / Limitations	277
99		BIOS – KBL CRB v020	278
	99.1	Resolved Client BIOS HSD sightings.....	279
	99.2	BP Client Common Core Sync-up Changes	280
	99.3	Known Issues / Limitations	280
100		BIOS – KBL CRB v019.1.....	281
	100.1	Resolved Client BIOS HSD sightings.....	282
	100.2	BP Client Common Core Sync-up Changes	282
	100.3	Known Issues / Limitations	282
101		BIOS – KBL CRB v019	283
	101.1	Resolved Client BIOS HSD sightings.....	284
	101.2	BP Client Common Core Sync-up Changes	285
	101.3	Known Issues / Limitations	285
102		BIOS – KBL CRB v018	286
	102.1	Resolved Client BIOS HSD sightings.....	287
	102.2	BP Client Common Core Sync-up Changes	289
	102.3	Known Issues / Limitations	289
103		BIOS – KBL CRB v017	290
	103.1	Resolved Client BIOS HSD sightings.....	291
	103.2	BP Client Common Core Sync-up Changes	292
	103.3	Known Issues / Limitations	292
104		BIOS – KBL CRB v016	293
	104.1	Resolved Client BIOS HSD sightings.....	294
	104.2	BP Client Common Core Sync-up Changes	296
	104.3	Known Issues / Limitations	296
105		BIOS – KBL CRB v015.2.....	297
	105.1	Resolved Client BIOS HSD sightings.....	298
	105.2	BP Client Common Core Sync-up Changes	298
	105.3	Known Issues / Limitations	298
106		BIOS – KBL CRB v015.1.....	299
	106.1	Resolved Client BIOS HSD sightings.....	300
	106.2	BP Client Common Core Sync-up Changes	300
	106.3	Known Issues / Limitations	300
107		BIOS – KBL CRB v015	301
	107.1	Resolved Client BIOS HSD sightings.....	302
	107.2	BP Client Common Core Sync-up Changes	304
	107.3	Known Issues / Limitations	304
108		BIOS – KBL CRB v014	305
	108.1	Resolved Client BIOS HSD sightings.....	306
	108.2	BP Client Common Core Sync-up Changes	307
	108.3	Known Issues / Limitations	307



109	BIOS – KBL CRB v013.1	308
	109.1 Resolved Client BIOS HSD sightings	309
	109.2 BP Client Common Core Sync-up Changes	309
	109.3 Known Issues / Limitations	309
110	BIOS – KBL CRB v013	310
	110.1 Resolved Client BIOS HSD sightings	311
	110.2 BP Client Common Core Sync-up Changes	312
	110.3 Known Issues / Limitations	312
111	BIOS – KBL CRB v012	313
	111.1 Resolved Client BIOS HSD sightings	314
	111.2 BP Client Common Core Sync-up Changes	317
	111.3 Known Issues / Limitations	317
112	BIOS – KBL CRB v011	318
	112.1 Resolved Client BIOS HSD sightings	319
	112.2 BP Client Common Core Sync-up Changes	321
	112.3 Known Issues / Limitations	321
113	BIOS – KBL CRB v010	323
	113.1 Resolved Client BIOS HSD sightings	324
	113.2 BP Client Common Core Sync-up Changes	327
	113.3 Known Issues / Limitations	327
114	BIOS – KBL CRB v009	328
	114.1 Resolved Client BIOS HSD sightings	329
	114.2 BP Client Common Core Sync-up Changes	330
	114.3 Known Issues / Limitations	330
115	BIOS – KBL CRB v008	331
	115.1 Resolved Client BIOS HSD sightings	332
	115.2 BP Client Common Core Sync-up Changes	334
	115.3 Known Issues / Limitations	334
116	BIOS – KBL CRB v007	335
	116.1 Resolved Client BIOS HSD sightings	336
	116.2 BP Client Common Core Sync-up Changes	337
	116.3 Known Issues / Limitations	337
117	BIOS – KBL CRB v006	338
	117.1 Resolved Client BIOS HSD sightings	339
	117.2 BP Client Common Core Sync-up Changes	340
	117.3 Known Issues / Limitations	340
118	BIOS – KBL CRB v005	341
	118.1 Resolved Client BIOS HSD sightings	342
	118.2 BP Client Common Core Sync-up Changes	343
	118.3 Known Issues / Limitations	343
119	BIOS – KBL CRB v004	344
	119.1 Resolved Client BIOS HSD sightings	345
	119.2 BP Client Common Core Sync-up Changes	346



	119.3	Known Issues / Limitations	346
120		BIOS – KBL CRB v003	347
	120.1	Resolved Client BIOS HSD sightings.....	348
	120.2	BP Client Common Core Sync-up Changes	351
	120.3	Known Issues / Limitations	351
121		BIOS – KBL CRB v002	352
	121.1	Resolved Client BIOS HSD sightings.....	353
	121.2	BP Client Common Core Sync-up Changes	354
	121.3	Known Issues / Limitations	354
122		BIOS – KBL CRB v001	355
	122.1	Resolved Client BIOS HSD sightings.....	356
	122.2	BP Client Common Core Sync-up Changes	356
	122.3	Known Issues / Limitations	356



Revision History

Revision Number	Description	Revision Date
0.103	Kabylake CRB BIOS V103	11 Aug 2017
0.102	Kabylake CRB BIOS V102	4 Aug 2017
0.101	Kabylake CRB BIOS V101	28 July 2017
0.100	Kabylake CRB BIOS V100	21 July 2017
0.99	Kabylake CRB BIOS V099	15 July 2017
0.98	Kabylake CRB BIOS V098	7 July 2017
0.97	Kabylake CRB BIOS V097	2 July 2017
0.96	Kabylake CRB BIOS V096	22 June 2017
0.95	Kabylake CRB BIOS V095	15 June 2017
0.94.2	Kabylake CRB BIOS V094.2	22 June 2017
0.94.15	Kabylake CRB BIOS V094.15	14 June 2017
0.94.1	Kabylake CRB BIOS V094.1	13 June 2017
0.93	Kabylake CRB BIOS V093	2 June 2017
0.92	Kabylake CRB BIOS V092	26 May 2017
0.91	Kabylake CRB BIOS V091	19 April 2017
0.90	Kabylake CRB BIOS V090	12 May 2017
0.89	Kabylake CRB BIOS V089	5 May 2017
0.88	Kabylake CRB BIOS V088	28 April 2017
0.87	Kabylake CRB BIOS V087	23 April 2017
0.86	Kabylake CRB BIOS V086	14 April 2017
0.85	Kabylake CRB BIOS V085	09 April 2017
0.84	Kabylake CRB BIOS V084	31 March 2017
0.83	Kabylake CRB BIOS V083	24 March 2017
0.82	Kabylake CRB BIOS V082	17 March 2017
0.81	Kabylake CRB BIOS V081	9 March 2017
0.80	Kabylake CRB BIOS V080	3 March 2017
0.79	Kabylake CRB BIOS V079	23 Feb 2017
0.78	Kabylake CRB BIOS V078	20 Feb 2017
0.77	Kabylake CRB BIOS V077	10 Feb 2017



0.76	Kabylake CRB BIOS V076	1 Feb 2017
0.75	Kabylake CRB BIOS V075	20 Jan 2017
0.74	Kabylake CRB BIOS V074	13 Jan 2017
0.73.1	Kabylake CRB BIOS V073.1	11 Jan 2017
0.72	Kabylake CRB BIOS V072	29 Dec 2016
0.71	Kabylake CRB BIOS V071	23 Dec 2016
0.70	Kabylake CRB BIOS V070	16 Dec 2016
0.69.2	Kabylake CRB BIOS V069.2	14 Dec 2016
0.69.1	Kabylake CRB BIOS V069.1	14 Dec 2016
0.69	Kabylake CRB BIOS V069	10 Dec 2016
0.68	Kabylake CRB BIOS V068	5 Dec 2016
0.67	Kabylake CRB BIOS V067	25 Nov 2016
0.66	Kabylake CRB BIOS V066	18 Nov 2016
0.65	Kabylake CRB BIOS V065	11 Nov 2016
0.64	Kabylake CRB BIOS V064	4 Nov 2016
0.63	Kabylake CRB BIOS V063	28 Oct 2016
0.62	Kabylake CRB BIOS V062	25 Oct 2016
0.61	Kabylake CRB BIOS V061	17 Oct 2016
0.60	Kabylake CRB BIOS V060	10 Oct 2016
0.59	Kabylake CRB BIOS V059	3 Oct 2016
0.58	Kabylake CRB BIOS V058	27 Sept 2016
0.57	Kabylake CRB BIOS V057	19 Sept 2016
0.56	Kabylake CRB BIOS V056	9 Sept 2016
0.55	Kabylake CRB BIOS V055	5 Sept 2016
0.54	Kabylake CRB BIOS V054	29 Aug 2016
0.53	Kabylake CRB BIOS V053	22 Aug 2016
0.52.1	Kabylake CRB BIOS V052.1	16 Aug 2016
0.51	Kabylake CRB BIOS V051	8 Aug 2016
0.50.1	Kabylake CRB BIOS V050.1	1 Aug 2016
0.50	Kabylake CRB BIOS V050	29 July 2016
0.49.1	Kabylake CRB BIOS V049.1	25 July 2016
0.49	Kabylake CRB BIOS V049	25 July 2016
0.48	Kabylake CRB BIOS V048	18 July 2016
0.47.1	Kabylake CRB BIOS V047.1	11 July 2016
0.47	Kabylake CRB BIOS V047	11 July 2016
0.46	Kabylake CRB BIOS V046	1 July 2016



0.45.1	Kabylake CRB BIOS V045.1	29 June 2016
0.45	Kabylake CRB BIOS V045	27 June 2016
0.44	Kabylake CRB BIOS V044	20 June 2016
0.43.3	Kabylake CRB BIOS V043.3	20 June 2016
0.43.2	Kabylake CRB BIOS V043.2	16 June 2016
0.43	Kabylake CRB BIOS V043	13 June 2016
0.42	Kabylake CRB BIOS V042	6 June 2016
0.41	Kabylake CRB BIOS V041	30 May 2016
0.40	Kabylake CRB BIOS V040	23 May 2016
0.39.1	Kabylake CRB BIOS V039.1	9 May 2016
0.39	Kabylake CRB BIOS V039	6 May 2016
0.38	Kabylake CRB BIOS V038	2 May 2016
0.37	Kabylake CRB BIOS V037	25 April 2016
0.36	Kabylake CRB BIOS V036	15 April 2016
0.35	Kabylake CRB BIOS V035	8 April 2016
0.34	Kabylake CRB BIOS V034	1 April 2016
0.33.1	Kabylake CRB BIOS V033.1	31 Mar 2016
0.33	Kabylake CRB BIOS V033	28 Mar 2016
0.32	Kabylake CRB BIOS V032	22 Mar 2016
0.31	Kabylake CRB BIOS V031	14 Mar 2016
0.30	Kabylake CRB BIOS V030	8 Mar 2016
0.29	Kabylake CRB BIOS V029	28 Feb 2016
0.28.1	Kabylake CRB BIOS V028.1	25 Feb 2016
0.28	Kabylake CRB BIOS V028	23 Feb 2016
0.27	Kabylake CRB BIOS V027	15 Feb 2016
0.26	Kabylake CRB BIOS V026	8 Feb 2016
0.25.1	Kabylake CRB BIOS V025.1	2 Feb 2016
0.25	Kabylake CRB BIOS V025	1 Feb 2016
0.24	Kabylake CRB BIOS V024	25 Jan 2016
0.23.1	Kabylake CRB BIOS V023.1	22 Jan 2016
0.23	Kabylake CRB BIOS V023	18 Jan 2016
0.22	Kabylake CRB BIOS V022	11 Jan 2016
0.21	Kabylake CRB BIOS V021	04 Jan 2016
0.20	Kabylake CRB BIOS V020	29 Dec 2015
0.19.1	Kabylake CRB BIOS V019.1	23 Dec 2015
0.19	Kabylake CRB BIOS V019	22 Dec 2015



0.18	Kabylake CRB BIOS V018	14 Dec 2015
0.17	Kabylake CRB BIOS V017	7 Dec 2015
0.16	Kabylake CRB BIOS V016	1 Dec 2015
0.15.2	Kabylake CRB BIOS V015.2	30 Nov 2015
0.15.1	Kabylake CRB BIOS V015.1	28 Nov 2015
0.15	Kabylake CRB BIOS V015	23 Nov 2015
0.14	Kabylake CRB BIOS V014	15 Nov 2015
0.13.1	Kabylake CRB BIOS V013.1	10 Nov 2015
0.13	Kabylake CRB BIOS V013	08 Nov 2015
0.12	Kabylake CRB BIOS V012	04 Nov 2015
0.11	Kabylake CRB BIOS V011	28 Oct 2015
0.10	Kabylake CRB BIOS V010	15 Oct 2015
0.09	Kabylake CRB BIOS V009	05 Oct 2015
0.08	Kabylake CRB BIOS V008	29 Sept 2015
0.07	Kabylake CRB BIOS V007	22 Sept 2015
0.06	Kabylake CRB BIOS V006	15 Sept 2015
0.05	Kabylake CRB BIOS V005	08 Sept 2015
0.04	Kabylake CRB BIOS V004	02 Sept 2015
0.03	Kabylake CRB BIOS V003	27 August 2015
0.02	Kabylake CRB BIOS V002	19 August 2015
0.01	Kabylake CRB BIOS V001	13 August 2015



1 *SPI Images*

1.1 **SPI Images for Kabylake (KBL + SPT LP / SPT H) platforms**

Flash Part Size	Platform Segment	Platforms Supported	Flash Image		
			SPI 00	SPI 01	Full SPI Image



2 Supported Hot Keys

CTRL+ALT+SHIFT+<KEY> causes a Hot-Key Event to the SBIOS. The specific <KEY> to complete the sequence is defined in the following table.

2.1 ACPI Hot-keys

F1	IGFX Display Switch using Toggle List 1.
F2	IGFX Display Switch using Toggle List 2.
F3	IGFX Display Switch using Toggle List 3.
F4	IGFX Display Switch using Toggle List 4.
F5	Virtual Power Switch Event (Toggle between Virtual AC and Virtual Battery Mode)
F8	IGFX Panel Fitting Hot-Key
F9	IGFX LCD Brightness Level – Decrease 10% if percentage > = 10%
F10	IGFX LCD Brightness Level – Increase 10% if percentage < = 90%
1/!	10% Virtual Battery
2/@	20% Virtual Battery
3/#	30% Virtual Battery
4/\$	40% Virtual Battery
5/%	50% Virtual Battery
6/^	60% Virtual Battery
7/&	70% Virtual Battery
8/*	80% Virtual Battery
9/(90% Virtual Battery
0/)	100% Virtual Battery
-/_	Virtual Battery % = Virtual Battery – 2%
= /+	Virtual Battery % = Virtual Battery + 2%

Notes:

1. The Virtual Battery hot-key values are a single key with dual purposes.
2. IGFX hot-keys are only supported when IGFX is present and is the primary display device. If that is not the case, the hot-keys will be disabled.
3. The virtual battery hot-keys are only valid when a virtual battery is present. If any real battery is present at all, these hot-keys are disabled. Additionally, the user will only be allowed to decrease battery percentages when in virtual battery mode and will only allow the user to increase battery percentages when in virtual AC Mode. Also, please note that some operating systems only display battery percentage differences that are $\geq \pm 4\%$.
4. All of the above hot-keys work in ONLY ACPI aware operating systems.



3 BIOS – KBL CRB v103

BIOS version	0.103	
BP common core revision	1.3.4.2	
RoyalPark core version	1.3.4.2	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1069	
1.5MB ME Firmware SKU	11.7.0.3307 (Consumer)	
5MB ME Firmware SKU	11.7.0.3307	
RST RAID OROM	15.9 (revision 3138)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x6E CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.7.0
	MRC Version	2.7.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 522695 (2016_Kabylake)	

3.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1805437438	Uploading new RST binaries, version 15.9.0.3138
1604427362	[KBL-Y]Hot Plug/Unplug of SD Card after 2 Minutes idle is not Enumerating/Ejecting if O2-Micro card reader
220512580	[KBL][Security] [UEFI work around] Debug Verbosity change
1304712545	[OC] - MRC is not detecting memory topology changes correctly
1604406500	FSP should not lock SPI FLASH_CONFIGURATION_LOCKDOWN (FLOCKDN) register
220573014	KBL CustomDefaults v4 settings are causing regressions in S3 and HLK testing, and should be removed
220512582	Resolve VS2017 linker error due to use of intrinsic function.
1405568250	[CFL/KBP][MRC][OC] - Expose all memory timings for Memory Custom profile

3.2 BP Client Common Core Sync-up Changes

NoneKnown Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



4 BIOS – KBL CRB v102

BIOS version	0.102	
BP common core revision	1.3.4.2	
RoyalPark core version	1.3.4.2	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1069	
1.5MB ME Firmware SKU	11.7.0.3307 (Consumer)	
5MB ME Firmware SKU	11.7.0.3307	
RST RAID OROM	15.9 (revision 3104)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x6E CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.7.0
	MRC Version	2.7.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 520493 (2016_Kabylake)	

4.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604253862	Enable SLP_S0 with LPA and display ON on KBL R
220561963	Remove/hide PCH-IO Configuration / PMC Read Disable BIOS SETUP option
220295629	Implement long term solution for Xml CLI on KBL & CFL BIOS - Part 2
1504556474	[KBL] Need to fix KBL Platform Klocwork Weekly_100_00_142 Issue
220512590	Preserve descriptors across call to PciGetBusRange
NO HSD	Integrate CFL U0 patch 0x6E
220513131	Enable Energy reporting by default: PCH-IO Configuration/PMC Read Disable = Disable
1604420612	CFL S + KBP-H - SUT hangs at Intel logo screen with PCA7 after enabling Overclocking
220513799	[KBL] Finalize code that sets Bit 11 in SPIBAR+0x04
1604420478	SKL/KBL/CFL - Integrate latest CFL GOP 1069
1604398952	Regarding FSP-M UPD values, some may need clarification, some may get modified
1406351739	WWAN ACPI_DSW race caused unexpected D3/L3 resulted in modem crash & CATERR
1604346959	KBL BKC_WSTV:[PETS][Compliance_AMT.xml]:BAE Platform Event Trap support with alternate Boot device is getting fail in PETS AMT_015 in PETS Compliance_AMT Package
1604347602	[KBL RVP-7 EC]:Sporadically Base EC-FW version,Base EC Protocol versions shown as "Not present" in BIOS under platform information menu during multiple G3 cycles
1504526414	Duplicate PcdPeim.efi which occupied more temp ram
1604410933	KBL-Y-IFWI: PCIe Slot1 (X4) is not working in KBL Y (ULX- Type C) boards

4.2 BP Client Common Core Sync-up Changes

NoneKnown Issues / Limitations

Sighting #	Description	how_to_reproduce
------------	-------------	------------------



	None	
--	------	--



5 BIOS – KBL CRB v101

BIOS version	0.101	
BP common core revision	1.3.4.2	
RoyalPark core version	1.3.4.2	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1068	
1.5MB ME Firmware SKU	11.7.0.3307 (Consumer)	
5MB ME Firmware SKU	11.7.0.3307	
RST RAID OROM	15.9 (revision 3104)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x6A CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.7.0
	MRC Version	2.7.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 517535 (2016_Kabylake)	

5.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604414439	[KBL-R TBT NE] : HW Scan is required every time to get TBT devices to enumerate during hot plug or tear down to happen during unplug when PCIe RP is in D3
220445641	Add new CFL-S device IDs to check for CFL-S.
1209086964	[KBL][OC]: Add voltage control for Vccio, VccSA, VccSFR_OC and VccST.
1604410553	KBL BIOS : TBT3 SSD/Display hot plug is not working with BIOS V099 on RS3 16232
220488120	[CFL-S/KBP] Please change PL2 value to 122W to improve performance

5.2 BP Client Common Core Sync-up Changes

None

5.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



6 BIOS – KBL CRB v100

BIOS version	0.100	
BP common core revision	1.3.4.2	
RoyalPark core version	1.3.4.2	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1068	
1.5MB ME Firmware SKU	11.7.0.3307 (Consumer)	
5MB ME Firmware SKU	11.7.0.3307	
RST RAID OROM	15.9 (revision 3104)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x6A CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.6.0
	MRC Version	2.6.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 515948 (2016_Kabylake)	

6.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504537629	[KBL-Y] The initial setting of WWAN PEWAKE on KBL-Y RVP3 isn't aligned to KBL-R RVP
1209086964	[KBL][OC]: Add voltage control for Vccio, VccSA, VccSFR_OC and VccST.
	Back out changelist [220445641]Add new CFL-S device IDs to check for CFL-S.
220494977	KBL-G-BIOS: Regression-Ethernet is not working with the latest BIOS 97.02
220447387	HSTI test failure: PCH Security Configuration when PMC read is unlocked.
220203659	System Hangs at Post Code 0055 on S3 Resume
1604405857	UA01 is always initialized as PchSerialIoLegacyUart
220426893	Add BIOS ACPI PEP constraint for CSME D0/F1
1504533829	KBL-FSP: SMBIOS Memory Info Data HOB Structure name and parameters are not generic accross platforms

6.2 BP Client Common Core Sync-up Changes

None

6.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



7 BIOS – KBL CRB v099

BIOS version	0.099	
BP common core revision	1.3.4.2	
RoyalPark core version	1.3.4.2	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1068	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.9 (revision 3104)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x6A CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.6.0
	MRC Version	2.6.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 512078 (2016_Kabylake)	

7.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504526713	PL4 override error with KBL SiC v.2.5.0
22080080	[KBL-R MR][BIOS] Default Virtual Sensor Calibration Tables define Targets that are not POR for the platform
1305045758	TBT BIOS: RTD3/CS/MS support
1305045709	TBT BIOS: Native PCIe enumeration
1504532632	Kabylake MRC Klocwork issue in Weekly_98_00_139
NO HSD	Move to 15.9.0.3104 RST Pre OS version for RS3 release.
220445641	Add new CFL-S device IDs to check for CFL-S.
1504532643	Kabylake platform Klocwork issue in Weekly_98_00_139
220416460	Request for reference code fix: TBAR + 40h : TT - Thermal Throttling register

7.2 BP Client Common Core Sync-up Changes

None

7.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



8 BIOS – KBL CRB v098

BIOS version	0.098	
BP common core revision	1.3.4.2	
RoyalPark core version	1.3.4.2	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1068	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.8 (revision 3109)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x6A CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.5.1
	MRC Version	2.5.1.3



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 512078 (2016_Kabylake)	

8.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504531441	[KBL-Y] M.2 7360 support on KBL-Y
1504527437	[kaby_lake.other]BP1342 core sync to KBL codebase
1604400832	[CFL-S6+2-EV/CRB] In SGX functionality EPID & PSE Provision part is failing.
NO HSD	Integrate CFL U0 patch 0x6A
20398882	[KBL][MRC] Late Command Training corner case failure seen with certain memory cfg's
NO HSD	[CFL/KBP][MRC] Add CPU Stepping for CFL-S 4+2
220403747	[Capsule]Windows driver signing failed with Capsule .inf file.
1504395857	[KBL][MRC] Debug BIOS not boot up, 3200 evaluation
1604350361	[FSP]: Update in Integration guide required - HPET Usage, TempRam Buffer Usage and about different FSP segment version support.
1805279438	Uploading new RST binaries, version 15.8.3109
1604382418	CFL-S BIOS: Platform Settings Option is missing in BIOS
220380739	[KBL][BIOS] No Runtime D3 (RTD3) support for PCH SDCard controller (no ACPI _S0W method)
220336627	[KBL] BIOS specifies incorrect frequency for SLP_S0 residency counter in ACPI LPIT table
1504527716	Empty value shown on BCT Tool for Fsp.bsf in FSP 2.4.0

8.2 BP Client Common Core Sync-up Changes

None

8.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
------------	-------------	------------------



	None	
--	------	--



9 BIOS – KBL CRB v097

BIOS version	0.097	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1068	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.8 (revision 3057)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x5E CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.5.0
	MRC Version	2.5.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 510878 (2016_Kabylake)	

9.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604398433	[KBL EBAT] " Display Not Getting on HDMI port "
220175741	[WSVT_KBL_SV][KBL-R-WWAN] Flashing the M.2 7360 WWAN Modem with the Telephony tool a time out error is displayed. WWAN notify function added back
220403588	KBL-G-BIOS-OC:Request to Modify the Cock Frequency Help text in Intel ICC Page
1504526713	PL4 override error with KBL SiC v.2.5.0
1604397513	Enable RTD3 by default for KBL-R
1504527552	[KBL-R] PERST should be de-asserted after WWAN BBRST de-assertion
1604361768	[KBL-G][HLK]:-USB Exposed Port System Test Failed due to Improper Port Mapping
1604395819	UCSI W/A implementation -To retry read/write from UCSI to EC through ACPI to avoid timeout before EC goes out of burst mode
1604363649	SMBIOS Type-9 System slot information is not listing in EFI shell and OS
1604211138	KBL BIOS: [OC] Memory Voltage value is not reflecting in BET Tool after changing that corresponding value in BIOS.
220343204	KBLG BIOS:SMBIOS shows only two entries on types 17 instead of four
1604395884	Add CFL-S 4+2 support in KBL code with GT DID change
220291145	[KabyLake_RVP7] System fails Legacy Boot to Win7x86 and DOS using Skylake [GT3] CPU on Kabylake BIOS
220295629	XMLCII script doesn't work on KBL. Implement long term solution for Xml CLI on KBL & CFL BIOS
22044880	[KBLG PO]: Disabling Thunderbolt Support automatically disable PEG.
1406248060	CFL BIOS OC: Realtime Memory XTU control ID support
220290214	Enable DPTF Power Share Policy by default in BIOS
1405838025	Add CPUID values for CFL 8 +2 P0.
1209619097	[CFL/KBP][MRC][OC] Increase Max Memory Ratio



1406186943	New RCR: Bios work around for "System hang up when running burnIn test and plug in/out the usb docking"
1604393361	[KBL-R] Set WWAN disabled by default for performance build
1406270484	SV Build unable to find BIOS Guard module
220263159	CFL-S failing Preset 10 in SigTest
1504510700	Clear NVRAM after capsule update.

9.2 BP Client Common Core Sync-up Changes

None

9.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



10 BIOS – KBL CRB v096

BIOS version	0.096	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1066	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.8 (revision 3057)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x5E CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.5.0
	MRC Version	2.5.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 508149 (2016_Kabylake)	

10.1 Resolved Client BIOS HSD sightings

HSD#	Title
1406204510	SPD not powergating causing PCH to not enter Gen2PLL shut down in Hybrid Gfx mode in IDLE Display On Scenario AND [KBLG PO][Power]:Storage device is not in L1.2 when connected to either the M.2 slot or PCH Pcie X4
1406181738	Remove production BIOS Guard binaries module support from SV BIOS Build
1305113404	Update to support dynamic BIOS Guard Module binary loading.
NO HSD	Remove WWAN notify code from ASL
1604384816	Optimized MTRR usage by rounding flash region from 7MB to 8MB.
1706668816	Fix Branding in SG code
1209704990	[WOS]:[KBL-SDS]:BIOS changes for the specific HW components
1604370154	KBL- EC:EC version is showing incorrect in both BIOS and OS
1604379632	CMS Exit latency(575ms) is not meeting the PV target (525ms)on KBL-H With RS2 OS build 15063.
1604346667	[CFLS62+KBL_PCH][HLK][RS2][IFWI]:-USB Exposed Port System Test Failed with Error "Failing Exposed Connector" and "Failed to verify consistent USB 3.0 Port Mapping.

10.2 BP Client Common Core Sync-up Changes

None

10.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



11 BIOS – KBL CRB v095

BIOS version	0.095	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1066	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.8 (revision 3057)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x5E CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.4.0
	MRC Version	2.4.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 505980 (2016_Kabylake)	

11.1 Resolved Client BIOS HSD sightings

HSD#	Title
220291859	[CFL/KBP][MRC] DMFC should not be modified for CFL-S CPU
1304919325	TBT BIOS: AR: Removed: PCIE Switch Flow Control and Add: Device Downstream Port Software L1 workarounds
220123776	Expose BIOS SETUP option to enable/disable CPU 3-strike counter in release BIOS used in CCG BKC
1604350361	[FSP]: Update in Integration guide required - HPET Usage, TempRam Buffer Usage and about different FSP segment version support (Sync CL:505002 from CNL to KBL)
1504516817	KBL: Add CleanMemory UPD in FSP to support memory clean security feature
NO HSD	[CFL] Add new CPUID to list
1305162509	[CFL][OC] Ring downbin is disabled by default
1304689105	[KBL][MRC] Fix error in calculation for ShiftPI in special case in Pi Reserves changes.
NO HSD	WWAN PV blocker issue fix
220175741	[WSVT_KBL_SV][KBL-R-WWAN] Flashing the M.2 7360 WWAN Modem with the Telephony tool a time out error is displayed
1304689105	Updates to KBL MRC from Latest Feedback
1805148910	BIOS to avoid FCERR when setting FLOCKDN and WRSDIS in SPI

11.2 BP Client Common Core Sync-up Changes

None

11.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



12 BIOS – KBL CRB v094.1

BIOS version	0.094.1	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1066	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.8 (revision 3057)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x66 KBL S/H B0: 0x5E CFL-S 6+2: 0x5E CFL-S 4+2: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.4.0
	MRC Version	2.4.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.2.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 501623 (KBL_GO_PO)	

12.1 Resolved Client BIOS HSD sightings

HSD#	Title
220175741	[WSVT_KBL_SV][KBL-R-WWAN] Flashing the M.2 7360 WWAN Modem with the Telephony tool a time out error is displayed
1604375746	[KBL-R][WW22.3][RS2][WWAN] No Internet access is observed during online video playback over WWAN
1604375923	[KBL-R][WW22.3][RS2][WWAN] Caterr observed with different working scenarios when WWAN connected to the network
1304689105	[KBL][MRC]Updates to KBL MRC from Latest Feedback
NO HSD	[Ingredient] Integrate KBL Y0 patch 0x66
NO HSD	[Ingredient] Integrate CFL B0 patch 0x5E
NO HSD	[Ingredient] Integrate CFL U0 patch 0x5E
NO HSD	[TXT][KBL] Release BIOSAC and SINIT version 1.2.0
220173639	CFL BIOS needs to sync to the latest CFL VR POR overrides.
220173639	Add CFL-S 4+2 support for VR overrides.
1504405873	[KBL] V73 KBL system's F7 boot list pop new item "Boot Device List", but it only into BIOS setup not "Boot Manager Menu"
1604371493	KBL BIOS : Unknown device yellow bangs observed in device manager after enabled DPTF in BIOS V089.3
220173639	CFL BIOS needs to sync to the latest CFL VR POR overrides
1405829799	[cannon_lake]CNL CFL-S/CFL-H with 12/16 Threads encounter exception during boot with Release BIOS - Default set TsegSize as 8MB
NO HSD	KBL- EC:EC version is showing incorrect in both BIOS and OS.
22066828	dGPU VR cannot be disabled for RTD3 flows due to non-enabled BIOS/EC flow causing 6-7W power consumption even when the device is in D3 Cold.
22088242	PEG1 slot cannot enter into compliance mode because reference clock disappears just after booting



12.2 BP Client Common Core Sync-up Changes

None

12.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



13 BIOS – KBL CRB v093

BIOS version	0.093	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1066	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.8 (revision 3057)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x64 KBL S/H B0: 0x5E CFL-S 6+2: 0x5C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.4.0
	MRC Version	2.4.0.0
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.1.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 501623 (2016_Kabylake)
----------	--------------------------

13.1 Resolved Client BIOS HSD sightings

HSDES#	Title
220202694	Set Bit 11 in SPIBAR+0x04
1805140525	Uploading RST binaries, version 15.8.0.3057
1504505721	IpClean -i feature is disabled if restricted process is disabled by -k command and no macro being defined the same time.
220166216	[KBL G] Pkg-C10 not achievable in Hybrid Graphics mode
220230916	External KBLG DEBUG and RELEASE BIOS fails to boot on RVP17

13.2 BP Client Common Core Sync-up Changes

None

13.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



14 BIOS – KBL CRB v092

BIOS version	0.092	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1066	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.7 (revision 3054)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x64 KBL S/H B0: 0x5E CFL-S 6+2: 0x5C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.3.0
	MRC Version	2.3.0.0
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.1.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 500504 (2016_Kabylake)
----------	--------------------------

14.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604360543	[KBL-R] Clean up the WWAN workaround which was previously created for CATERROR issue
1805126055	Uploading new RST PreOS binaries, version 15.7.0.3054_PV
1604359690	[KBL SX_WSTV]:System hang with PC:00CS while running CS cycle
220207371	[KBL]CPU MP driver not updating the PcdCpuApLoopMode based on Setup/UPD & must depend on MonitorMWaitEnable UPD/Setup
1504502151	Fix FSR tool bug not able to patch utf-16 with BOM codec files correctly
220206651	DEBUG BIOS ASSERTS on RVP17 on V89.15
220178646	Set WRSDIS bit in SPI flash controller as security recommendation
NO HSD	[CFL][OC] Interrupt storm at idle
1504499010	[cannon_lake]Removed duplicate memory hob in FSP.
22088242	PEG1 slot cannot enter into compliance mode because reference clock disappears just after booting
220172108	Add ACPI code to external build for G project
NO HSD	WWAN delay must be avoided in performance build.
1504493460	Latest MinTree #2675 build hang with POST CODE 4E25.
1405826962	[KBL-R] M.2 7360 PCIe PEWAKE# assert still triggered a SCI system wake in S0/D0
1804992429	[CFL][OC] PLL Trim voltage offset feature is not working well
220183448	Add support for FAB-B power sequencing on RVP17
220171424	Update default PSVT on KBL-G to only include POR participants (and exclude row with CPU as target)
220183996	DEBUG BIOS ASSERTS on RVP17
NO HSD	[Ingredient] Integrate KBL Y0 patch 0x64
1805116834	Adding RST SMM Module for handling SSCP during S3 resume. Fixed NVMe init.



14.2 BP Client Common Core Sync-up Changes

None

14.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



15 BIOS – KBL CRB v091

BIOS version	0.091		
BP common core revision	1.3.4.1		
RoyalPark core version	1.3.4.1		
Video Option ROM (VBIOS)	1051		
GOP Driver	9.0.1066		
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.7 (revision 3019)		
MEBx	11.0.0.0010		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x5E KBL S/H B0: 0x5E CFL-S 6+2: 0x5C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	2.3.0	
	MRC Version	2.3.0.0	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.1.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 498212 (2016_Kabylake)
----------	--------------------------

15.1 Resolved Client BIOS HSD sightings

HSDES#	Title
220185355	Update IpClean to support md file
220153046	BIOS is not programming default TDC limits according to spec
22062499	BIOS iccmax values for core/GT/SA do not match EDS
1604334659	Bios Conf Tool Verification Failed for TPM devices
1504492692	clean up IgdHdcpEnable and HdcpAlgorithm options
1604351777	[KBL security] BIOS Boot time out variable should be initialized to reasonable value.
1805114849	[NVMe][KBL-R][BSOD][CAT ERR] bsod DRIVER_POWER_STATE_FAILURE with NVMe PS or SB disk
1209974283	KBL-R-U: XmlCli IFWI not booting for FVME IFWI
1405895325	[1x1]:[KBL-RVP3]:[Power]:[P3]:power button action not working in v83 Bios with the CS Bios setting
1604356575	PchScsSdCardSidebandEventsSupport option cleanup to enable Pnp validation with TBT enabled by default
220106359	Intel Reference Code. Bug Report. Wrong PpmCtdpOverrideTable will be chosen for SKL
1805112873	[KBL] USB2 devices may misbehave after resume from S3
1405899805	Sometimes system will hang at code "04" after resume from S3

15.2 BP Client Common Core Sync-up Changes

None

15.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



16 BIOS – KBL CRB v090

BIOS version	0.090		
BP common core revision	1.3.4.1		
RoyalPark core version	1.3.4.1		
Video Option ROM (VBIOS)	1051		
GOP Driver	9.0.1066		
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.7 (revision 3019)		
MEBx	11.0.0.0010		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x62 Y0 : 0x5E KBL S/H B0: 0x5E CFL-S 6+2: 0x5C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	2.1.0	
	MRC Version	2.1.0.5	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.1.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 495522 (2016_Kabylake)
----------	--------------------------

16.1 Resolved Client BIOS HSD sightings

HSDES#	Title
NO HSD	CFLS6+2 - CRBBIOS -CFL DT and SERVER SKU missing from the CFL source
NO HSD	CFLS6+2 - SVBIOS -CFL Coretype information missing
1209711179	Password string is not cleared after use.
1209714499	TxtSmm does not check SMM communication buffer.
22067249	[KBLG PO] S3 cycling fails at a random cycle (seen on two platforms)
1604332791	[KBLR] WWAN device is not enumerating in OS after changing the BIOS Options
1805110089	Uploading RST binaries, version 15.7.0.3019.
1209753830	[CCB - new] [RS2 HLK requirement] Reserve 128KB of non-volatile NVRAM memory for UEFI variables for FSP Wrapper and EDK builds.
1504459969	IpClean -K command may disable -i command as well
NO HSD	Integrate KBL H0 patch 0x62
1209704115	Made PcdPhysicalPresent FALSE by default.
1405880005	Use CpuDxe driver from UefiCpuPkg, instead of CpuInitDxe driver from CPU RC, for building BIOS in MinTree. Remove usage of MSR_CORE_THREAD_COUNT for MinTee.
1604328700	KBL-R BIOS: power limit 4 value is not overriding on KBL-R Board.

16.2 BP Client Common Core Sync-up Changes

None

16.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



17 BIOS – KBL CRB v089

BIOS version	0.089		
BP common core revision	1.3.4.1		
RoyalPark core version	1.3.4.1		
Video Option ROM (VBIOS)	1051		
GOP Driver	9.0.1066		
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.8 (revision 3010)		
MEBx	11.0.0.0010		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x5E Y0 : 0x5E KBL S/H B0: 0x5E CFL-S 6+2: 0x5C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	2.1.0	
	MRC Version	2.1.0.5	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.1.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 493684 (2016_Kabylake)
----------	--------------------------

17.1 Resolved Client BIOS HSD sightings

HSDES#	Title
NO HSD	Back out changelist 440267 (FPS as Wake source is not POR), [1604177808][KBL_BKC_WSTV] :FPS failed to wake the system from S3 through biometric scan (FPS1021A)
1604348293	[FSP] FspProducerId should not be used as INTEL_C for external customers built FSP image
22071885	DPTF is disabled by default in the PO BIOS, we need to re-enable this as soon as possible
1805105249	Uploading RST 15.8.0.3010 PreOS binaries.
220131365	[TXT][KBL] Release BIOSAC and SINIT version 1.1.0
1504476302	Change PCH Thermal Device to disable or Enable in ACPI mode would hang
1209714766	[2017 KBL HaT] [KBL-R HaT] UEFI Variable deletion - System doesn't recover after deleting CpuSetup variable from UEFI Shell
1209705059	[2017 KBL HaT] Recommendation for TrEEPlatform
1209995449	[KBL][MRC] Workaround for display underrun in KBL 23e when pressing WIN key - two 4K panels and EDRAM SW always-on mode
1405596962	[kaby_lake.rvp11]The KBL SV Bios cant boot to 0x00F6 because of the CL 460003
1209694031	[2017 KBL HaT] CHIPSEC able to corrupt some variables.
1208226650	XmlCli Support code - Part 4 - Modified latest

17.2 BP Client Common Core Sync-up Changes

None

17.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



18 BIOS – KBL CRB v088

BIOS version	0.088		
BP common core revision	1.3.4.1		
RoyalPark core version	1.3.4.1		
Video Option ROM (VBIOS)	1051		
GOP Driver	9.0.1066		
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.5 (revision 2875)		
MEBx	11.0.0.0010		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x5E Y0 : 0x5E KBL S/H B0: 0x5E CFL-S 6+2: 0x5C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	2.1.0	
	MRC Version	2.1.0.5	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 491677 (2016_Kabylake)
----------	--------------------------

18.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1504477308	Fix FSR tool bug which cannot load UTF-16 file successfully
1305022408	Increase release TSEG Size to 8 MB from 4 MB in PlatformPkg.dsc.
1305041622	[CFL][OC] BCLK Aware Adaptive voltage feature is not being enabled
1305041786	[CFL][OC] DDR runtime OC feature is not being enabled
220115935	Fix in PlatformSetup.uni file to replace unknown UTF-16 characters
1304898452	TBT BIOS: LTR: Missing LTR values configurations
1604343236	PPI based debug lib for FSP
1604328700	KBL-R BIOS: power limit 4 value is not overriding on KBL-R Board.
1504459750	Support KBL RVP3 board in MinTree
1504459989	[CNL] Klocwork issues for Platform code base on CNL Release_81_00_215 - VTIO
1209921714	Add DPTF support for RVP17
1209903794	Clean up unnecessary code for booting Windows for MinTree - Security features
1604307019	[KBL-KC] update PCIe src clk for Rtd3
22097344	Fix BIOS configuration changes from PO in RVP17
22083294	Merge CNL to KBL Overclocking support for 6-8 core FSP portion. Non-FSP already moved.
1209537430	Part2: Make 'Thunderbolt port enabled' default in KBL-R BIOS.
1604305906	[KBL-R]Measuring 150mW High PCH power with Audio Driver ADSP-09.21.00.2168 during video playback scenerio.
22080837	Fix HSTI failures observed with recent OverClocking changes
1405759683	Push upstreamed patch to intel internal FSP code.

18.2 BP Client Common Core Sync-up Changes

None



18.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



19 BIOS – KBL CRB v087

BIOS version	0.087	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1066	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA H0 : 0x5E Y0 : 0x5E KBL S/H B0: 0x5E CFL-S 6+2: 0x5C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.1.0
	MRC Version	2.1.0.5
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 489520 (2016_Kabylake)
----------	--------------------------

19.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604342485	Integrate SKL/KBL GOP V1066 which has CFL-S 6+2 sku support
NO HSD	Merge 6 and 8 core support from KBL_GO stream for Overclocking.
1405435690	CFL BIOS: [OC] Realtime Memory Timings enable/disable
1405435920	CFL BIOS: [OC] Voltage PLL trim for all CPU domains
1405335600	CFL/CNL/ICL OC - New PLL Trim option for Ring, GT, SA, Mc
1209928769	KBX-BIOS:BIOS does not have VCC ST Voltage knob for Overclock Testing
1209537430	Make 'Thunderbolt port enabled' default in KBL-R BIOS.
22064840	If GDT is in flash, copy to memory.
1604331739	Type c to be enabled by default in Bios
22041337	Intel Reference Code. GpioLib can't properly update GPIO_DIRECTION setting when pad is configured for output or has RX&TX buffers disabled
1604300685	[KBL-R TBT TypeC]: Observed CATERROR and BSOD while connecting TBT3 HP dock with two 4K DP display
NO HSD	Merge Cannon Lake CL462583, 462717 6 and 8 core support changes into KBL_GO stream except FSP UPDs and Policies.[FIX CpuRegs.h]
NO HSD	W/A Clear all machine checks from bank 6 until end of banks.
1405583522	CNL-U/Y: AC/DC default loadline overrides, 1405718651 - CFL/CNL IccMax and TDC Power Limit overrides
NO HSD	Add microcode for CFL U0 0x5C. Remove G0 and A0 microcode.
1405561447	[KBL KC] TBT2/3 device doesn't auto re-enumerate after S3/S4 Resume sporadically
1604264730	Force Power doesn't work for PCIe Root 5 (FP is always Low and no PCIe Bridge enumeration)
1604323400	[KBL-KC]:Yellow bang observed on PCI-to-PC
NO HSD	Merging KBL_GO_PO to 2016_Kabylake. MiniBIOS Support for CFL-S CPU.
1209711179	Password string is not cleared after use.
1604281266	KBL-R BIOS: System hangs at PC00A7 when CSM Control option set as "Always ON" in BIOS with Storage device (SSD/HDD/NGFF) connected.



1604322247	[KBL-R]RCR to Enable "GPP_A23 with 20K pull down"
1209648520	SMBIOS Type 16 No of Memory device showing wrong for KBL S UDIMM Platform.
1504439819	[coffee_lake] Add new XTU controls defined in XTU 6.2 spec
1504459755	Cleanup redundant BoardId in structure: HSIO_PTSS_TABLES, also generic code PeiBoardConfigLib should not have RVP3 check.
1209688581	[2017 KBL HaT] [KBL-R HAT] MeSetup variable
1504463082	[KBL-G] Add support in TPV GFX ACPI methods for overclocking enable bits

19.2 BP Client Common Core Sync-up Changes

None

19.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



20 BIOS – KBL CRB v086

BIOS version	0.086	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1064	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xBA R0/D0: 0xBA G0 : 0x26 H0 : 0x5E Y0 : 0x5E KBL S/H A0: 0x34 KBL S/H B0: 0x5E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.1.0
	MRC Version	2.1.0.5



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 487339 (2016_Kabylake)	

20.1 Resolved Client BIOS HSD sightings

HSD#	Title
1209952774	[KBL][SDS] SDS lost a primary boot device(PCIe NVMe) after KBL BIOS v78
NO HSD	Fixed S3 resume fail start from - Merge 8 core support from 2017_Cofeelake_S&H_TestSku - Based on CL#485965 missed pep.asl
1405827036	Additional cleanup for MinTree
1209995449	[KBL][MRC] Workaround for display underrun in KBL 23e when pressing WIN key - two 4K panels and EDRAM SW always-on mode
1504458612	[KBL][MRC] Fix SA Klocwork issues
22040060	Integrate SKL patch 0xBA for D0/R0
NO HSD	Merge 8 core support from 2017_Cofeelake_S&H_TestSku - Based on CL#485965 missed pep.asl
1405809739	[KBL-R] BIOS: Port configuration for Camera
1504458939	KBLFSP: Typos and Duplicated PCD Entries
22034934	Integrate 3 KBL patches, for B0/H0/Y0 0x5E
1209858110	Improve error resiliency after BIOS SETUP option for PCH-IO-> SSC (spread spectrum %) value needs upgrade to support 100MHz Overclock modes 3 and 5
1304698458	[KBL] [OC] - Overclocking WS - DDR OC capability with KBL MRC is lower than SKL MRC
1209901008	[KBL][MRC] Additional Changes for CL#481151 Remove Read Dependency from Early Write Centering Training Steps
1209952019	[KBL] SEN5 sensor has unexpected Power Control capability when it should not
1405741439	Additional Changes for CL#482326 for KBL-R LPDDR3 MiniBIOS enabling
1804919715	Add Z350 PCH support
1604320926	KBL BIOS: SUT is not entering into CS using power button with CMOS settings done in BIOS on HALO boards
NO HSD	Platform Klocwork issues in Weekly_85_00_95



20.2 BP Client Common Core Sync-up Changes

None

20.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



21 BIOS – KBL CRB v085

BIOS version	0.085	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1064	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xB8 R0/D0: 0xB8 G0 : 0x26 H0 : 0x58 Y0 : 0x5C KBL S/H A0: 0x34 KBL S/H B0: 0x58	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.1.0
	MRC Version	2.1.0.2



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 485560 (2016_Kabylake)	

21.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504450934	[cannon_lake]Ensure RoyalPark override tags have correct naming - RoyalParkOverride
1604331813	[KBL-R] Optane enabling on KBL-R U42 SKU with proper Bios settings
1209692931	[2017 KBL HaT] why we still include SmmThunk driver
1604331160	[title] Processor Stepping shown as Unknown for KBL-R QS Samples
1604332210	Support CFL-S 6+2 Sku by adding DID
1604310995	[KBL KC_FAB-2] interrupt storm (_GPE._L6F() seen in S0 Idle condition on KBL KC Board
1405766712	[KBL] ISP does not have _DEP listed in PEP.asl
1504390825	[cannon_lake]Potentially system hang caused by accessing SMM code in DXE phase - PlatformVarCheckLib issue
1604321052	KBL-R BIOS: SX functionality is not working with NVIDIA Graphics card connected
1208226650	XmlCli Support code - Part 3
1209920670	[KBL][SDS][Capsule][Crashdump]Realign Capsule memory allocation not to conflict with Crashdump support.
1209988527	Update to PEP SATA settings has not been done on MSFT specific DxeCustomDefaults driver
1804736025	Provide BCFS (BIOS control feature support) to disable and enable System Acceleration with Optane Memory
1209977430	Integrate SKL patch 0xB8 for D0/R0
1504384343	Clean up unnecessary code for booting Windows for MinTree - ME
1405568365	Please remove all IDE related code
1604320505	[KBL-Security]: The JHI Initialization failing.



21.2 BP Client Common Core Sync-up Changes

None

21.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



22 BIOS – KBL CRB v084

BIOS version	0.084	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1064	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xB6 R0/D0: 0xB6 G0 : 0x26 H0 : 0x58 Y0 : 0x5C KBL S/H A0: 0x34 KBL S/H B0: 0x58	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.1.0
	MRC Version	2.1.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 482788 (2016_Kabylake)	

22.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604300189	CpuMpPei driver uses - Non-Reserved Memory for S3 case FSP & Doesn't update it's memory usage to wrapper code for FSP.
1209931665	Storage participant PTP is set for SATA (8) instead of NVME (29)
1209907122	Update help text to match values programmed
1209142413	Glitch noise issue in the system having HD-A and USB type-C with power delivery
1804724729	[KBL-R] Docking Station ACPI devices show up after resume from S3 or S4
NO HSD	[KBL] [MRC] Add support for KBL-R LPDDR3 in miniBios
1209901454	KBX-BIOS:Core Max OC,Ring Min and Ring Max Ratio option allowing us to set ratio Value below 8
1209866616	[KBL-R][MRC] Enable LPDDR3 ODT Training for 2133+ Frequency
1604319286	[KBL] Specific GPIO's which are not common across boards should be seperated
NO HSD	Update RC version to 2.1.0
1209920930	Add GPIO changes for FPS interrupt work around on RVP17.
1209926839	Integrate KBL patch for Y0 0x5C
1209926840	Integrate SKL patch 0xB6 for D0/R0
1209921579	Add support for optimized settings on KBL.
1209908102	[KBL] Cosmetic change: ConfigureEsp() routine has the debug message even before variable declaration
1504408965	KBL system hang up at 0000 or 00CS when sleep into Connected standby, issue only reproduce with debug build.
1209901008	[KBL][MRC] Remove Read Dependency from Early Write Centering Training Steps
1209920162	[KBL-H][MRC] System will hang up by doing S4 long run with single 16G DDR4 DIMM populated - LLC_COMMAND_TIMEOUT
1604323786	[KBL/SKL - Integrate latest GOP 1064]



1604312681	HDA-Link is used by Chrome for HDMI Audio so it should be enabled even in case of I2S enabled
1209828627	Need EvLoader UPD param for MMA for SKL and KBL.
1209908074	[KBL/CNL] The setup help string STR_MMIO_ABOVE_4G_HELP is wrong.
1604281266	KBL-R BIOS: System hangs at PC00A7 when CSM Control option set as "Always ON" in BIOS with Storage device (SSD/HDD/NGFF) connected.

22.2 BP Client Common Core Sync-up Changes

None

22.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



23 BIOS – KBL CRB v083

BIOS version	0.083	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1051	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB4 G0 : 0x26 H0 : 0x58 Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x58	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	2.0.0
	MRC Version	2.0.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 480401 (2016_Kabylake)	

23.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO HSD	Fix a system hang observed in specific debug setting. PcdDebugPropertyMask=0x27 PcdFixedDebugPrintErrorLevel=0x80000000
1504432367	[KBL/KBL-R] Incorrect TBARB define in HSTI caused read HSTI SPI lock status failure
1209689959	[2017 KBL HaT] About BIOS GUARD
1604317067	LPM & CMP policies are not visible in BIOS v81.P00 IFWI
1209714736	[KBL-R] UEFI Variable deletion - System doesn't recover after deleting Setup variable from UEFI Shell
1504420193	[KBL]V78_Performance_S3 resume time is not match the criterion with KBLs.
1604304869	Removing the BoardID override and add new boardID support for BoardIdKabylakeKcDdr3, BoardIdKabylakeRlpDdr3, BoardIdKabylakeRDdr4.
1804711205	Implement Debug Print level lib for FSP
1604268163	KBL BIOS[OC] :BET tool shows blank for ACPI + SMI window while corresponding values changed from BET & reboot.
1604319554	KBL/SKL - Integrate latest VBIOS 1051
1209739370	[KBL] Missing check before the attribute of PCI host controller was being set
1604307019	KBL-kc update PCIe src clk for Rtd3.
NO HSD	Removing unused TbtLoadedDefaultValue variable
1604314724	[KBL-R][HLK][RS2][IFWI]:-USB Type-C ACPI Validation Test Failed and throwing error "AreEqual(g_numberOfTypeCPorts, expectedNumberOfTypeCPorts)"
NO HSD	Removing unused ACPI Global NVS variables related to WWAN enabling in KBL R.
1504384338	Clean up unnecessary code for booting Windows for MinTree - PCH
1405619853	Client BIOS launches 3rd party video OROM prior to gEfiEndOfDxeEventGroupGuid event
1604318430	[title] KBL-BIOS: Config TDP Power Limit 1 "Time Window "Should have Drop Down to Select Values in Bios on KBL-R Board.



1504415639	[title] [KBL] Fix implementation to support 32MB+ cache sizes, and add new socket types from SMBIOS 3.1.1.
1504414426	IpClean may remove spaces or quotes unexpectedly
1504434431	[KBL] Disabled SATA controller may cause S3 long run failure.
1209885760	[title] Integrate SKL patch 0xB4 for D0/R0
1209714499	TxtSmm does not check SMM communication buffer.
1209714757	[KBL-R HAT] UEFI Variable deletion - System doesn't recover after deleting SaSetup variable from UEFI Shell
1604315111	[KBL-R]Getting an error message "Security Violation" when we run the tool with security boot enabled.
1604318230	[KBL EBAT]System Hangs at PC:0092 with External Debug Build & FSP_EXT_VS_Debug 82_178
1604267971	Sporadically Modem (7360) Enumeration is disappearing from Device manager on Multiple Scenario's
1604304869	Back out changelist that enable TBT settings by default.

23.2 BP Client Common Core Sync-up Changes

None

23.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



24 BIOS – KBL CRB v082

BIOS version	0.082	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB2 G0 : 0x26 H0 : 0x58 Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x58	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.9.0
	MRC Version	1.9.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 477983 (2016_Kabylake)	

24.1 Resolved Client BIOS HSD sightings

HSDS#	Title
1209646318	Hang at 0096 PC After enabling BIOS Console redirection feature
1604276073	CS wake through power button, sporadically Display get blink and enter into CS again
NO HSD	Add support for ALPS touchpad
1405612506	KBL Booting legacy with smi periodic disable to Grub the keyboard doesnt work
1604274113	CNL BIOS:SATA drive attached to PCIe SATA card is not detected in Bios BBS menu
1504351398	Scrub undocumented register access - MSR
1804735745	[KBL] USB port disable function failed after deep S3 resume
NO HSD	Update scripts for supporting KBL-G external release
1209853477	Integrate 2 KBL patches, for B0/H0 0x58
1209758656	Bios page prompts for password after flashing v77 capsule with the load set default bios setting
1604240470	BIOS PEP constraints incorrect when PEP constraints are set to storage controller.
1604294039	LPDDR3 spd to be used for KBL-R Sku 2
1209821052	The capsule update fails after BIOS v68.50 when EnableCustomDefaults is set on KBL-SDS.
1604284524	[KBL-R-PO] System taking more time to boot into OS with LPC enabled EC

24.2 BP Client Common Core Sync-up Changes

None

24.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
------------	-------------	------------------



	None	
--	------	--



25 BIOS – KBL CRB v081

BIOS version	0.081	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB2 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.9.0
	MRC Version	1.9.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 475701 (2016_Kabylake)	

25.1 Resolved Client BIOS HSD sightings

HSDS#	Title
1604284524	[KBL-R-PO] System taking more time to boot into OS with LPC enabled EC
1504414257	KBL Klocwork issues in Weekly_77_00_90 - CPU
1604267971	[KBL-R-PO] WWAN specific Device wake related changes/recommendations.
1209690540	Production BIOS does not set PcdCpuSmmProfileEnable, mXdSupported becomes FALSE.
1304901394	[OC] Enabling BCLK change permanent in Intel ICC BIOS menu does not survive reset
1504426089	[KBL][external]UCSI WHQL test failed in USB Type-C in RS2 for external release
1209820044	Cleanup SecCpulib for server defines as they are not used
1604302297	FSP should not override pad configuration for Serial Io devices
NO HSD	Update Vcc in default to safe value.
1604258267	KBL : USB is not responding when trying to wake from S3 with Debug mode enabled
1504384348	Clean up unnecessary code for booting Windows for MinTree - SA
1604309016	iTouch not working during POST on customer platform
1504408318	[kaby_lake.rvp3]Update SiPkg Doxygen to remove Skylake statement.
1504425747	64bit address is masked out improperly in ..\Hsti\Dxe\SecureMemoryMapConfiguration.c
1804734141	[KBL] Incorrect RST mode string with SPT C236 PCH

25.2 BP Client Common Core Sync-up Changes

None

25.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
------------	-------------	------------------



	None	
--	------	--



26 BIOS – KBL CRB v080

BIOS version	0.080	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2875)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB2 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.9.0
	MRC Version	1.9.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 473616 (2016_Kabylake)	

26.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604309574	BIOS needs to program TBT force power GPIO to E0 instead of using IO expander pin.
1504367416	TurnAround Timing Adjustment after JEDEC Write Leveling
1209689966	[2017 KBL HaT] BIOS Guard Update file has integer overflow
NO HSD	Correct NvsArea and Setup structure revision to meet RC guideline
1604281518	KBL-R BIOS : Espi initialization is not happening in EFI shell.
1504422104	KBLFSP: MTTR values not programmed before FspTempRamExit
1604252199	[KBL-RVP 8 S CRB][Security][Optane] [WW45.4] [GOLD RS1 14393]While performing Secure erase over LAN with Optane enabled getting error called "failed to erase the device"
1208226650	Enable XML CLI to run with CCG Automation - Part 2
1504413714	[kaby_lake.other]Use Feature or IP base flag to exclude unnecessary code for MinTree
1804733426	Uploading RST PreOS, version 15.5.0.2875.
NO HSD	merge uni from KBL to update core max oc ratio string.
1604306828	KBX-BIOS:VCC IO Voltage knob showing Wrong string in BIOS.
1604306440	[KBL-R][KBL-Refresh] With Bios 78 PL1 and ICCMAX values for core,GT and SA are not set properly. This impacts performance KPI's
1604265917	[HLK][RS2]:-Secure Boot Logo Test Fails with error"The signature below does not match any signatures in the database"
1209742441	[KBL/CNL] iTouch not working even though BIOS code is returning passing status
1604304869	Load BKC (Best Known Configuration) for TBT with TBT support enable by default for KBL-R (BoardIdKabylakeRlpDdr3, BoardIdKabylakeRDdr4) Board.
1209705499	In FSP, code cache size is incorrectly determined.
1604303551	[SA_DT] Debug_Error message reduction



1604267971	[KBL-R-PO] Sporadically Modem (7360) Enumeration is disappearing from Device manager on Multiple Scenario's
NO_HSD	Responsiveness failiure due to delay added in bios coder for modem enumeration
1209739360	[KBL/CNL]DispatchHandle issue in PchSmmCoreRegister
1405535506	PwrBtnOverridePeriod does not work
1504403944	[KBLR][KBL PERF]V75 KBLR's cold boot out of criteria.

26.2 BP Client Common Core Sync-up Changes

None

26.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



27 BIOS – KBL CRB v079

BIOS version	0.079	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2858)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB2 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.8.0
	MRC Version	1.8.0.2



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 469887 (2016_Kabylake)	

27.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604225634	Run Edit command at EFI shell, the edit window show black screen.
NO_HSD	KBL-R-BIOS: Remove CMP and LPM from setup option for DPTF.
1209644968	BIOS rcr to set Host EXI Enable Lock (HOST_EXI_EN_LOCK)
1304798230	[BSF][KBL-X][OC]System fails to boot at Memory frequency 3200MHz
1209715552	[KBL-X] Remove support for x16 and x32 DIMMs
1405287151	SKX DMI max payload size should be 128B
1604294280	KBL SECURITY : SUT hangs observed after changing Lock Enable (LE) Bit to 0 and Write Protect Disable (WPD) bit to 1
1405639714	ClientCommonPkg has incorrect use of UnicodeStrToAsciiStrS()
1604301806	Include MemInfoHob in FspmUpd.h
1504394003	Printing Hexdump of FSP UPD parameter values inside FSP-M and FSP-S
1604300779	KBL:IFWI:Disabled option listed twice for "TCC offset clamp Enable option & TCC offset Time window" option in BIOS menu

27.2 BP Client Common Core Sync-up Changes

None

27.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



28 BIOS – KBL CRB v078

BIOS version	0.078	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2858)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB2 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.8.0
	MRC Version	1.8.0.2



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 467897 (2016_Kabylake)	

28.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504416113	[KBL] RVP17 name not showing up in BIOS menu
1209692983	[2017 KBL HaT] GetRsePassword() does not clear password in memory after use.
1209692940	[2017 KBL HaT] Password is not cleared after use
1504413382	KBL BIOS: Setup item cannot save after resume from S3 and start system.
1804722512	[KBL] RVP11 - NVM disc is not enumerated on m.2 port after pressing reset button
1209387078	CPU temperature cannot be read due to PECI communication fail
1504414284	KBL Klocwork issues in Weekly_77_00_90 - SA
1209435465	KBX-BIOS:BIOS not exposing PCH RID Value and CRID Enable and disable BIOS Options
1504414257	KBL Klocwork issues in Weekly_77_00_90 - CPU
1604294052	CSME doesn't powergate on Poppy board
1504415230	MinTree broken by several checkins
1405600947	BT UART Wake Signal should not configured by BIOS as a Wake Source
1604267971	[KBL-R-PO] Sporadically Modem (7360) Enumeration is disappearing from Device manager on Multiple Scenario's
1504414262	KBL Klocwork issues in Weekly_77_00_90 - ME
1209680691	[KBL] Duplicate RVP11 board init for new RVP
NO HSD	Clean up PPV setup options no impact on CCG flow
1504414271	KBL Klocwork issues in Weekly_77_00_90 - PCH
NO HSD	Update CPU RC and Setup relative base on coding standard and KBL RC 1.8.0 API Change Review feedback.
1604294213	Remove *Rebased*.fd from the <Platform>FspBinPkg, as it is getting released causing confusion
1804666534	[KBL] Missing PEP Constraints for SATA ports cause intermittent issues with SATA LPM flows affecting platform SLP_S0 state



1604291852	KBL-SECURITY : TCG2 configuration is not accessible in BIOS under TPM2 in TPM configuration
1304820855	Bios Bug with duplicated UQI
1209648954	Integrate SKL patch 0xB2 for D0/R0

28.2 BP Client Common Core Sync-up Changes

None

28.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



29 BIOS – KBL CRB v077

BIOS version	0.077	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2858)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB0 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.8.0
	MRC Version	1.8.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 465471 (2016_Kabylake)	

29.1 Resolved Client BIOS HSD sightings

HSD#	Title
1209644968	BIOS rcr to set Host EXI Enable Lock (HOST_EXI_EN_LOCK)
1209101467	[SCS] Provide eMMC_DSM Function 9 as part of SDBUS driver requirement
1504384327	[KBL] Clean up unnecessary code for booting Windows for MinTree - Platform
1504411133	IpClean to support SH file format
1209205735	DEBUG_ERROR Messages Reduction by replacing ERROR level with WARN or INFO based on its severity.
1209177293	[vProME11.6]Post Screen Hang after Enter User Consent Code into VNC Viewer Opened at S4S5, AMT_044,045 Fail (60%)
1209558309	Enhanced SMM setup questions are no longer tied to PCDs
1604291689	FSP overrides GDT causing S3 resume failure
1405532038	KBL-R BIOS: Power Management default overrides for KBL-R skus
1209649441	RS2 HLK Requirement for Security: NoPPIClear must be set to TRUE or PPRequiredForClear must be set to FALSE
1504399041	Fixed a pointer bug in TXT save/restore of SMI enables.
1604294039	Added support for Micron MT52L512M32D2PF 78b DDP LPDDR3 SPD for KBL-R Sku 2.
1209249341	SKX-BIOS:Unable to see LAN PHY Version in System information Page
1209423606	HSTI error "Non lockable MMIO ranges overlap other critical regions" with PEG0 enabled with any PCI device on PEG0.
1804723091	Upload RST PreOS, version 15.5.0.2858
1604286378	KBL BIOS: SUT is halting at Postcode 0063 (~2 min) While resuming from S3 with performance BIOS on KBL-R Board.
1604279123	KBL-R-BIOS: BSOD is observed while preloading through onboard EFI network on KBL_R board
1504408318	[kaby_lake.rvp3]Update SiPkg Doxygen to remove Skylake statement.



1209636512	Update the latest DBXupdate.bin from UEFI Revocation list file
1405584744	[kaby_lake]Request to change PEP constraints in BIOS for audio
1405523949	Non-POR LPC DID should not be visible to customers
1209420923	Clean up CPU reference code that is not required for MinTree BIOS

29.2 BP Client Common Core Sync-up Changes

None

29.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



30 BIOS – KBL CRB v076

BIOS version	0.076	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.5 (revision 2841)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB0 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 462509 (2016_Kabylake)	

30.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604235502	[KBL-Halo][Optane][SB-ES1] Stonybeach disk not enumerated on Halo RVP11(M.2 SSD port-J6v1) with CM238/CM236 PCH
1405532038	[KBL-R] Power Management default overrides for KBL-R skus
1804719836	Uploading RST PreOS, version 15.5.0.2841
1304828511	BIOS doesn't wait for CSME FW to complete its loading after enabling ME via HECI
1504384171	Investigate the effort for removing CPU_SETUP, ME_SETUP, SA_SETUP and PCH_SETUP from MinTree.
NO_HSD	Update FspBuildSteps.md for the BP1341 integration versions
1504403065	[kaby_lake.rvp3] Merge and remove duplicate files - KabylakePlatSamplePkg/Library/PeiFspPolicyInitLib.
1504336032	More folders cleanup for MinTree.
NO_HSD	KBL KW failure : Null pointer 'EngStringHash' may be dereferenced in CL#458388
1504403560	Correct value in C-state Un-demotion related variable
1405532038	[KBL-X][OC] WDT disable is not working when BCLK is overclocked
1209388893	C7 % is low when HMDI/DP monitor is being used.
1604284095	iDisplay programing should be skipped in FSP when HDA-Link Audio Codec is not used
1304811484	[kaby_lake_refresh]Add support for KBL U Refresh
1209572288	[p2-high][open] [HP_CMINT_DT] KBL-S/KBP System hang on HP logo POST screen (70B9)
1504367416	DDR4 Rank Interleave I/O buffer switching mismatch between KBL-S memory controller and SK hynix 2400 ECC UDIMM 2Rx8 on Greenlow-R. Request for MRC W/A
1504388472	[kaby_lake.other]BP1341 integration.
NO_HSD	ME State not updating until it is accessed from setup page.
1209144110	Performance impact of SVENTX Catalog messages for release BIOS
1504384327	[KBL] Clean up unnecessary code for booting Windows for MinTree - Platform - part5



1209358682	PECI May Not be Functional After Package C10 Resume
------------	---

30.2 BP Client Common Core Sync-up Changes

None

30.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



31 BIOS – KBL CRB v075

BIOS version	0.075	
BP common core revision	1.3.4.1	
RoyalPark core version	1.3.4.1	
Video Option ROM (VBIOS)	1050	
GOP Driver	9.0.1063	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB0 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 459065 (2016_Kabylake)	

31.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804717008	S3 resume hangs at PC dd5A or 0C09 [Description] Reverted KabylakeSiliconPkg\Override\UefiCpuPkg\CpuMpPei changes to versions before BP1341 sync.
1504388472	BP1341 integration.
NO HSD	BP1341 Modify Doxygen from KabylakePlatSamplePkg to ClientCommonPkg Update externals.txt under KabylakeSiliconPkg
NO HSD	Security Sync up BP 1314 for Kabylake
1209566581	Merge UefiCpuPkg BP 1.3.4.1 into overrides.
NO HSD	Move override to ClientCommonPkg: BpCommonPkg/Csm/VariableSmiInt15Dxe, BpCommonPkg/Universal/VariableSmi.
1209060887	Bios Password protection issue in KabylakePlatSamplePkg\Setup\SecuritySetup.c
NO HSD	Enable XML CLI to run with CCG Automation.
1209570375	AMT_024 Remote Graceful shutdown doesn't work
1504398488	BSOD observed while booting to OS on KBL KC boards
1604267971	[KBL-R-PO] Sporadically Modem (7360) Enumeration is disappearing from Device manager on Multiple Scenario's
1504396370	KBL-S RVP will hang 00 with PCH H270 chip when "PCIE port swap" is disabled.
1504388047	KBLFSP: GenCfgOpt is not enforcing type requirement and is causing unexpected BSF entries in the generated bsf file
1504322261	USBC: Split USB sub system - Changes based on Code review feedback.
1405577916	PciePllSc is not properly initialized inside RC after 1.4.0 1405576015 KBL DMI_TRAINING_TIMEOUT MCA
1209091706	KBL ACPI folder re-structure to align Cove Creek requirement] Bug fix for miss the initialization of GlobalNVS



1504384327	Clean up unnecessary code for booting Windows for MinTree - Platform - part4
1604282023	KBL/SKL - Integrate latest GOP 1063 and VBIOS 1050

31.2 BP Client Common Core Sync-up Changes

None

31.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



32 BIOS – KBL CRB v074

BIOS version	0.074	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1062	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB0 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 457148 (2016_Kabylake)	

32.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804713804	Platform hangs at PC 0A7F
1604280652	PostMemSaReset function can be improved for responsiveness
1504393586	I2C accessing problem with PCI above 4G decode
1504216703	Prevent the duplicate notify events in FSP wrapper mode
1604277893	S3 resume fail after running SGX BIOS info tool and allow the system to sleep before restart
1504382212	FSP should initial Graphics if CB (bootloader) do pass VBT pointer during S3 resume
1604279970	KBL Bios: PEP Pre-Voteo device not registered and Fx Unregistered Device _SB.PCI0.ISP0 found and Hardware residency is showing 0% from sleepstudy data in CS
1504384327	Clean up unnecessary code for booting Windows for MinTree - Platform - part3
1504394130	FSP Wrapper boot hang up due to lack of temp ram.
1504384327	Clean up unnecessary code for booting Windows for MinTree - Platform - part2
1209420923	Clean up CPU reference code that is not required for MinTree BIOS

32.2 BP Client Common Core Sync-up Changes

None

32.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



33 BIOS – KBL CRB v073.1

BIOS version	0.073.1	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1062	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB0 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 456528 (KBL_GO_PO)	

33.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604279970	KBL Bios: PEP Pre-Voteo device not registered and Fx Unregistered Device _SB.PCI0.ISP0 found and Hardware residency is showing 0% from sleepstudy data in CS
1504394130	FSP Wrapper boot hang up due to lack of temp ram.
1604279511	TBT BIOS:Implementing Different SMI for each controller in case of Multiple controllers
1304302557	TBT BIOS: Native MSFT OS support / OS Downgrade/upgrade support: OS Up/Down, TBT BIOS: Native MSFT OS support / OS Downgrade/upgrade support : Native enumeration
1504322261	USBC: Split USB sub system - Part I
1504388079	KBLFSP: Fail to open bsf file by BCT due to invalid string found in BSE OPTION field
1209258702	Image Signal Processor blocking HW DRIPS and allowing 100% SW DRIPS
1504384327	[KBL] Clean up unnecessary code for booting Windows for MinTree - Platform - part1
1604243153	[kaby_lake_refresh]PO for KBL-R ERB RVP
1604268926	[KBL_KC] TR1 TBT controller influencing TR2 TBT connection because of incorrect PCIe Clock Req mapping with Dual TR controllers
1405540633	DoxygenPostCode.h updates needed to sync new postcodes
1604234037	On Samsung SSD PM951 SLP_S0 values getting <30% during 12 hour CS idle. Issue not seen with pleasant star
1604277621	[FSP] Create Separate TscTimerLib for PEI & SEC, as SEC can't use HOB
NO_HSD	KBL RVP3 and RVP7 system 's s3 resume time is too long.
1304635603	Need to remove BoardTypeRvpPpv from BoardConfig->BoardType list

33.2 BP Client Common Core Sync-up Changes

None



33.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



34 BIOS – KBL CRB v072

BIOS version	0.072	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1062	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xB0 G0 : 0x26 H0 : 0x4E Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 453522 (2016_Kabylake)	

34.1 Resolved Client BIOS HSD sightings

HSD#	Title
1209536241	On KBL-R RVP, LPC is not used. CLKRUN_B needs to be set high via internal pull up of 20 K to GPIO GPP_a_8.
1604258448	Remove PEGS Method from PegOnOff.asl to detect PEG port presence and and do it using IsPchLinkDmi () function in .c and load PEG SSDT based on that
1604258443	Update SG related policies used in SaMiscPeiPreMemConfig.h config block in FSP
1504326211	ACPI memory debug output to NPK (ADBG->NPK)
1604271394	KBL-DT-OC -RVP: Board ID is shown as 'TBD' in BIOS setup on KBL OC RVP board
1209538710	Integrate KBL patch, for H0 0x4E
1604261609	[kaby_lake_refresh][KBL-Refresh U DDR4 SIP]On-board MIC and DMIC is not working
1604243153	[kaby_lake_refresh]PO for KBL-R ERB RVP
1604259123	[Request to set bit[8] of GTTMMADR offset 0x4090 for SKL Cpu
1209535070	Integrate SKL patch 0xB0 for D0

34.2 BP Client Common Core Sync-up Changes

None

34.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



35 BIOS – KBL CRB v071

BIOS version	0.071	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1062	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x4A Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 452285 (2016_Kabylake)	

35.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604268201	[KBL-S-CRB][Optane] [SB-B0][BIOS -Regression] Thunderbolt Controller is not Enumerating in Device manager with latest alpha Optane
1604258408	[Type-C KBL-R] USB UCSI connector manager driver is not enumerating in device manager.
1209517630	Move SecCore to override folder so cherry picking will be not needed.
1804685465	MeBiosExtensionSetup variable is improperly initialized in platform code.
1604270032	Update KBL-R DID 0x5914 CNL SKU
1405529885	PowerButtonCallback() in SmmPlatform.c looks to be having coding error
1209458539	[KBL] [CNL] Microcode load in SEC phase won't work if patches are not 2K aligned
1209262306	[basin_falls.ev][BSF] Correct discrepancy for restricted tagged lined for DID definitions in PchRegsLpc.h & PchInfoStrLib.c
1405435485	[cAVS] BIOS W/A for DPIB status write
1604250879	PchHdAudioInit() function of PchInit of FspSiliconInit Phase takes more time in FSP2.0 than in FSP1.1

35.2 BP Client Common Core Sync-up Changes

None

35.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



36 BIOS – KBL CRB v070

BIOS version	0.070	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1062	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x4A Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 450282 (2016_Kabylake)	

36.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO_HSD	RC 1.4.1 cause POST time increase 1 more seconds(max: ~3) and shows "(A7)" message after close ME
1208162827	KBL BIOS Advertises overlapping memory resources for TPM 2.0
1504383150	[kaby_lake.rvp3]Potential failure when checking PCD in batch file.
1504379905	[Mintree]Remove RTD3 and THER related code in AcpiPlatform.c in MinTree
1209483714	Update CPUID for KBL-R in MRC and MiniBIOS
1604253600	KBL BIOS: Mismatch is observed in desired config TDP support in OS with J1 silicon
1209387221	BSF BIOS to implement TPM 2.0 TCG PPI 1.3 for RS2 HLK passing (MSFT says no waivers)
1504378369	[KBL] [CNL] Potential risk when scanning for microcode in PeiCpuPolicyLib
1804669771	Add support for QMS185 and C422A SKUs
NO_HSD	System Hang Issue seen KBLR.
1209057910	Update some batch files in UtilitiesInternalOnly folder for supporting BasinFalls one tree.
1405516353	BCLK Heci message should remove ASSERT
1604261997	Create separate FV Segment for FSP-S

36.2 BP Client Common Core Sync-up Changes

None

36.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



37 BIOS – KBL CRB v069.2

BIOS version	0.069.2	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1062	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x4A Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 449465 (KBL_G0_PO)	

37.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604266916	KBL/SKL - Integrate latest GOP 1062

37.2 BP Client Common Core Sync-up Changes

None

37.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



38 BIOS – KBL CRB v069.1

BIOS version	0.069.1	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1061	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x4A Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 449428 (KBL_G0_PO)	

38.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604265980	System Hang Issue seen on KBLR
1604261997	Fix FSP boot failure
1604261997	Create separate FV Segment for FSP-S

38.2 BP Client Common Core Sync-up Changes

None

38.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



39 BIOS – KBL CRB v069

BIOS version	0.069	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1061	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x4A Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.6.0
	MRC Version	1.6.0.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 448247 (2016_Kabylake)	

39.1 Resolved Client BIOS HSD sightings

HSDES#	Title
NO_HSD	Move DetectBootMode call before first PeiServicesGetBootMode.
1604234170	KBL_Sx:C6DRAM setup option is enabled in SUT even though BIOS option disabled causing LLC_Cache CATERR
1804675750	[kaby_lake.rvp7][PCH BIOS CI] Debug BIOS asserts in PeiPlatformHooklib.c at PC 000d
1604263492	[KBL] IPC : McdecsMisc.Bits.Spare_RW=0x13 code line to be added to the official BIOS release
1504355241	[kaby_lake.rvp11][KBL PERF]V62.2 RVP11 S3 resume time out of criteria
1604264300	GPIO changes needed for KBL-R and KBL KC as per the requirement changes requested by Board Team
NO_HSD	[KBL]V42_Performance_S3 resume time is not match the criterion with RVP8.
1604253600	KBL BIOS: Mismatch is observed in desired config TDP support in OS with J1 silicon
1405368703	iTouch: KBL MEInfo unable to communicate with iTouch using BIOS 52.4 (works with BIOS 50.2)
NO_HSD	Changing debug level with INFO for error debug messages which are actually not an error.
1604262286	KBL BIOS: Mismatch is observed with PDT unlock message in debug BIOS
1304650909	OS state not restored after 1st resume from S4
1504366252	[kaby_lake]Unit show black screen more than 30S before login HP Logo screen when restart after S3
1604230502	Premem Code cache programming is incorrect in FSP wrapper build
1405423129	iTouch not working during POST on customer platform
1604257096	FSP: change the command to determine GCC version
1604261997	Create separate FV Segment for FSP-S
1209282496	[BETA] KBX-BIOS:With PTT Enabled BIOS-Current TPM Device showing Unknown in TCG 2 Configuration Page



1504373641	[kaby_lake.rvp3]Cleanup all boardId definitions in PlatformBoardId.h in MinTree
------------	---

39.2 BP Client Common Core Sync-up Changes

None

39.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



40 BIOS – KBL CRB v068

BIOS version	0.068	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1049	
GOP Driver	9.0.1061	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x4A Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.5.0
	MRC Version	1.5.0.0



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 446576 (2016_Kabylake)	

40.1 Resolved Client BIOS HSD sightings

HSDS#	Title
1604252405	Add multiple TBT controller support
1604243153	PO for KBL-R ERB RVP
1405435928	[MRC][KBL] Need to ensure that DDRIO is reset after any MRC step where we move RxDQ/Rcven to ensure DDRPHY is not corrupted
1405411887	Default value for PepSata should be set to "no Constraint" for MS CoEng
1208480283	S3 resume from Windows 10 from Intel 750 PCIE NVME card throws BSOD
1209280431	UpStream Changes from HEDT to KBL KBX-BIOS:EFI variables read operation failed-while reading from HII Database using BIOS Configuration Tool.
1504373641	[kaby_lake.rvp3]Cleanup all boardId definitions in PlatformBoardId.h in MinTree
1209358466	Integrate KBL patch for H0 0x4A
1209289934	Update CPU information for KBL-R.
1504373757	[KBL DEBUG]V67 SDS system's S4 sleep failed and hang up at 0004 with debug build, issue only reproduced with SDS and can't reproduce with KBL-S.
1405443712	[KBL-BM141][FSP]SSID for Intel GFX device could not be configured in KBL FSP
1604245007	KBL IFWI : Audio recording functionality is not working after S3
1604257968	KBL/SKL - Integrate latest VBIOS 1049 and latest GOP 1061

40.2 BP Client Common Core Sync-up Changes

None

40.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	





41 BIOS – KBL CRB v067

BIOS version	0.067	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1060	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x48 Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.4.1
	MRC Version	1.4.1.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 444326 (2016_Kabylake)	

41.1 Resolved Client BIOS HSD sightings

HSDS#	Title
NO_HSD	MEBx settings not retained with ME Unconfig on RTC Clear option as Disabled in BIOS
1504351442	Scrub undocumented register access - MMIO code in CPU (cont.)
1209057910	Align BSF BIOS code to Client BIOS One Tree Proposal
1604245007	Back out CL 430804 to WA the Audio issue with Audio Driver.
1504372319	BOM ID 0 to support Micron 2133 Parts for KBL -KC
1209267075	Fadt is incorrectly initialized.
1405415372	SpiEiss and BiosLock are not set with BIOS Guard during capsule update flow.
1604243153	KBL-R PO for KBL-R ERB RVP
1604255411	KBL/SKL - Integrate latest GOP 1060
1504357760	Clean up unused Library and Include files from PlatSamplePkg

41.2 BP Client Common Core Sync-up Changes

None

41.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



42 BIOS – KBL CRB v066

BIOS version	0.066	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1059	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xAE R0/D0: 0xAE G0 : 0x26 H0 : 0x48 Y0 : 0x48 KBL S/H A0: 0x34 KBL S/H B0: 0x48	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.4.1
	MRC Version	1.4.1.1



	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698
P4 Label	@ 443161 (2016_Kabylake)	

42.1 Resolved Client BIOS HSD sightings

HSDES#	Title
NO_HSD	Revert PiSmmCpuDxeSmm and CpuMpPei to BP1.3.3.
1405472926	Integrate 3 KBL patches, for B0/H0/Y0 0x48
1504357015	[kaby_lake.rvp3]Remove PlatSamplePkgOverrideSecurityPkg from MinTree
1804668046	[PCH BIOS CI] FSP VS BIOS hangs at PC 9b47
NO_HSD	Remove AdvancedFeatures tags for UniTool execution.
1304660544	BIOS JHI Service Fails When Trying to Connect to CSE JHI.
1209264546	Add ReadMe file for Min-Tree source code
1405411887	Bios default CS settings need S0 Enabled S3 disabled for MS
1405282986	RVP8 - NVIDIA NVS 810 Card cannot assign enough free resources on a Dual Graphics config
1504357760	[kaby_lake.rvp3]Clean up unused Library and Include files from PlatSamplePkg
1209057910	Align BSF BIOS code to Client BIOS One Tree Proposal
1209267522	Integrate 2 SKL patches, for R0/D0 0xAE
1804344626	Add BCCD entry and _DEP method for RST RAID volumes.
1604252405	Add multiple TBT controller support
1504357764	[kaby_lake.rvp3]Move MultiPlatSupportLib from PlatSamplePkgOverrideClientCommonPkg to PlatSamplePkgOverrideMdeModulePkg
1209154505	CPU BIST information does not look to be passed from SEC properly "Does not find any stored CPU BIST information from PPI!"
1504357012	Remove PlatSamplePkgOverrideUefiCpuPkg and use open source in MinTree
1209188616	With FSP, Processor trace memory values are not maintained after S3 resume
1504366948	Fix KW issues of KBL CPU RC
1804665608	BIOS Root Port Destination ID data misses values for KBL-PCH-H



1404582479	[kaby_lake.rvp1]Remove duplicate and unused DataHob and FVs
1604177808	[KBL_BKC_WSTV]: FPS failed to wake the system from S3 through biometric scan (FPS1021A)
1604250814	KBL/SKL - Integrate latest GOP 1059
1209140008	The Latest KBL BIOS hangs at PC0x36 on PPV RVP10 after a fuse override
1604246891	Port KBL-KC platform changes to KBL source

42.2 BP Client Common Core Sync-up Changes

None

42.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



43 BIOS – KBL CRB v065

BIOS version	0.065	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1058	
1.5MB ME Firmware SKU	11.6.0.1142 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA6 R0/D0: 0xAC G0 : 0x26 H0 : 0x44 KBL S/H A0: 0x34 KBL S/H B0: 0x42	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.4.1
	MRC Version	1.4.1.1
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 440188 (2016_Kabylake)
----------	--------------------------

43.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604246891	Port KBL-KC platform changes to KBL source
1504336032	More folders cleanup for MinTree.
1209246142	KBL OC RVP BIOS does not have Turbo Setup options
NO HSD	Update BIOS version to 065
1504357760	Clean up unused Library and Include files from PlatSamplePkg
1504366723	ARRAY_SIZE marco may be redefined with future EDK open source.
NO HSD	Update doxygen and review feedback for ME RC 1.4.1
1504357760	Clean up unused Library and Include files from PlatSamplePkg partI
NO HSD	Update doxygen for CPU RC 1.4.1
1504336032	More folders cleanup for MinTree.
NO HSD	Update doxygen for SA RC 1.4.1
NO HSD	Update doxygen for PCH RC 1.4.1
1405311706	DPTF: Add BIOS setup options for new Active Policy 2.0
1504357797	Support BSD header in CopyRightParser script
1604235607	File explorer is not showing "Connected to USB 3.0" when we hot plug USB3.0 Device to USB3.0 port (issue observed only with two USB 3.0 ports Out of four USB 3.0 ports) and Safe remove icon is not displaying in task bar
1504351444 1504351436 1504351429 1504351408	Scrub undocumented register access - IO, MMIO, ACPI, Configuration Space code in SA
1504357797	Support BSD header in CopyRightParser script
NO HSD	Align BSF BIOS code to Client BIOS One Tree Proposal
1604238705	CpuRatio is being set to 0x0 without regard to override
1804344626	Add BCCD entry and _DEP method for RST RAID volumes, Back out changelist 437092.



1504245070	Privacy LED and Shared voltage rails enablement for IPU
1504245118	
1209018840	Memory is represented incorrectly under BIOS
1504268806	Request a policy for disabling USB disabled in PEI phase
1304656872	KBL: At the first time of entering correct "Master Password", an error of "mismatch error" is received.
1804665919	Integrate CRB CSME FW 11.6.10.1180 into BIOS
1504336032	More folders cleanup for MinTree.
1604248034	KBL/SKL - Integrate latest GOP 1058

43.2 BP Client Common Core Sync-up Changes

None

43.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



44 BIOS – KBL CRB v064

BIOS version	0.064		
BP common core revision	1.3.4.0		
RoyalPark core version	1.3.4.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1057		
1.5MB ME Firmware SKU	11.6.0.1141 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2740)		
MEBx	11.0.0.0010		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA6 R0/D0: 0xAC G0 : 0x26 H0 : 0x44 KBL S/H A0: 0x34 KBL S/H B0: 0x42		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.4.1	
	MRC Version	1.4.1.0	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 437723 (2016_Kabylake)
----------	--------------------------

44.1 Resolved Client BIOS HSD sightings

HSD#	Title
1209083062	KBL BIOS :Processor trace memory values are not maintained after S3 resume
1209188272	Integrate 2 SKL patches, for R0/D0 0xAC
NO HSD	Update BIOS version to 064
1604247148	Sync IntelFsp2Pkg & IntelFsp2WrapperPkg and update the Platform Code for proper FSP Performance measurement: Part3
1504347742	Clean up unused Library and Modules from SiliconPkg : Phase5 Other parts
1604247148	Sync IntelFsp2Pkg & IntelFsp2WrapperPkg and update the Platform Code for proper FSP Performance measurement Part 2/2
1504355806	MinTree process wrongly removed *.sh file from open source package.
1504347742	Clean up unused Library and Modules from SiliconPkg : Phase4 SA parts
1504336032	More folders cleanup for MinTree.
1604219444	KBL BIOS :Processor trace memory values set in BIOS are not reflecting in OS
1604247148	Sync IntelFsp2Pkg & IntelFsp2WrapperPkg and update the Platform Code for proper FSP Performance measurement
NO HSD	Back out changelist 418065. [hsdes] 1804344626 [title] Add BCCD entry and _DEP method for RST RAID volumes
1504346183	Changing SATA.EGCR.TSCAS programming: now TSCAS bit is cleared always, not only when remapping PCIe storage with no MSI-X support.
1504347742	Clean up unused Library and Modules from SiliconPkg : Phase3 PCH parts
1209175675	In ResetShutdown() routine, power button status clear is not done properly.
1209173531	Enable eDP Panel for Cove Creek
1504174771	external version of RC 0.71, PCH should add SmbusLib instance

44.2 BP Client Common Core Sync-up Changes

None



44.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



45 BIOS – KBL CRB v063

BIOS version	0.063	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1057	
1.5MB ME Firmware SKU	11.6.0.1128 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0010	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA6 R0/D0: 0xA8 G0 : 0x26 H0 : 0x44 KBL S/H A0: 0x34 KBL S/H B0: 0x42	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.4.0
	MRC Version	1.4.0.0
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 435917 (2016_Kabylake)
----------	--------------------------

45.1 Resolved Client BIOS HSD sightings

HSDES#	Title
9301106	Add support for 'OOK+' and 'Aggressive DCC' to KBL to enable MSFT KBL42 @18W SKU
NO_HSD	Update ucode to 0x44 for 806E9 (H0)
1504347742	Clean up unused Library and Modules from SiliconPkg
1604243153	KBL-R PO for KBL-R ERB RVP
1208707076	[KBL-SDS] Offline Crashdump: No Windows dump header found in the rawdump
1209080986	The Platform Overclocking drivers SMI interface does not perform SMRAM range checking
1604242709	[KBL-S-CRB] [RVP8] [OS-WIN7] [Power Management] [IFWI-52P12] Frequently DUT hang at Post code 0096/ 00AE while performing Warm reset/ S5/ S4 cycles (4/10 cycles) in 52.P12 IFWI with Win7 OS. Revert VBIOS to 1046
1604243968	KBL IFWI: Unable to preload WIN 7 OS on KBL UDIM boards with WW43_5_01 IFWI
1504349027	Added SATA.EGCR programming for Optane memory to S3 boot script.
1604242421	KW issues in KBL
NO_HSD	Will get error message '(A7)ME FW downgrade - Request MeSpiLock Failed. ' after doing clear CMOS on MEFW 1109
1208882263	[WW43-44WS][CMF] [DELL_BR_KBL]Check DG/CG Compatible will displayed HSTI validation failed.
1209091706	KBL ACPI folder re-structure to align Cove Creek requirement
1405396098	[KBL] IntelUefiRaidDiskInfo does not dispatch RSTe driver.
1209087479	[KBL] BIOS does not dispatch legacy RST OPRM with AlternateId enabled.
1604189079	Implementing a new BOM ID to support soldered down 2133 speed LPDDR3 on RVP16 boards
1504335505	[CNL] Merge Dynamic PCIEXBAR solution from KBL to CNL
1604242974	KBL BIOS: HII DB export through BIOSConf failing with Daily Bios Build 61_463 & 62_464
1304662507	[KBL]Adding MEBx version 11.0.0.0010
1504246986	Require follow bspec sequence to initialize the CD Clock by BIOS



1604242665	[KBL FSP] Remove FSP DATA Table reference as it is not in EAS, and read FSP Base address from Info Header instead of DATA Table
1209019817	KBLX-BIOS: Intel Speed Step getting disabled after enabling OC BIOS option.
1405320001	KBLX-BIOS: Turbo Boost Power time window default value is not showing correctly in XTU Tool
1604243579	KBL/SKL - Integrate latest GOP 1057
1504344063	[KBL] Create a MemMapDump library class and instance for debugging memory map inconsistent issue cross S4.
1504343796	[MinTree] Use Pei VBT table in OpRegion and eliminate Dxe GOP/VBT.
1604200152	[KBL BKC_WSTV]: CLTM DDR Temperature is always showing zero in TAT Tool and couldn't do CLTM Measurement

45.2 BP Client Common Core Sync-up Changes

None

45.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



46 BIOS – KBL CRB v062

BIOS version	0.062		
BP common core revision	1.3.4.0		
RoyalPark core version	1.3.4.0		
Video Option ROM (VBIOS)	1048		
GOP Driver	9.0.1056		
1.5MB ME Firmware SKU	11.6.0.1128 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2740)		
MEBx	11.0.0.0009		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA6 R0/D0: 0xA8 G0 : 0x26 H0 : 0x42 KBL S/H A0: 0x34 KBL S/H B0: 0x42		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.3.1	
	MRC Version	1.3.1.0	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 433355 (2016_Kabylake)
----------	--------------------------

46.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1209083975	KBL [OC]: KBL OC RVP board needs post code output on release BIOS
1209084035	KBL [OC]: KBL OC RVP board needs serial debug output enabled
1208971942	KBLX-BIOS:HDD device not sensing after enabling spin device option in BIOS
1209091706	KBL ACPI folder re-structure to align Cove Creek requirement
1804661390	[GPIO 2-tier GPE handling (_L6F) may miss an event]
1405391719	GNL-R RSTe OpROM is not dispatch on Client BIOS [BETA v052.8] not able to create Raid Arrays.
1604240046	[KBL-Y][HLK]:-USB Exposed Port System Test Fails with Error ***Failing Exposed Connector***
NO_HSD	Machine hung in EFI while running warm restarts
1405401215	CpuRatioOverride needs to be disabled by default.
1504305144	KBL: SMBIOS : SMBIOS (Type 17) always show 4 memory device
1504342483	[kaby_lake]Intel Self-test tool reported failure on SKL i5-6500 CPU
1504343401	Create Flash folder for SPI related Platform drivers and Platform FspWrapper cleanup
1604219444	KBL BIOS :Processor trace memory values set in BIOS are not reflecting in OS
1604241405	KBL/SKL - Integrate latest VBIOS 1048
NO_HSD	[KBL PERF]V57 1.5M cold boot time all increase about 400~600 ms with RVP 3,7,8 and 11 boards.
1504336297	Fix Klocwork issue #8501
1209090592	DqTimeCentering1D does not print out ECC training results
1207523015	Memory Address Decoder UEFI Driver accessible from the UEFI shell
1504338910	Incorporate SiliconPkg cleanup change from SSG to MinTree.
1804337038	Fix EC access before EC region is available
1304650909	OS state not restored after 1st resume from S4
1304649862	KBL BIOS: PPI: GetPhysicalPresenceConfirmationStatus() is affecting GetPhysicalPresenceRequest().



46.2 BP Client Common Core Sync-up Changes

None

46.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



47 BIOS – KBL CRB v061

BIOS version	0.061	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1047	
GOP Driver	9.0.1056	
1.5MB ME Firmware SKU	11.6.0.1128 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0009	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA6 R0/D0: 0xA8 G0 : 0x26 H0 : 0x42 KBL S/H A0: 0x34 KBL S/H B0: 0x42	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.3.0
	MRC Version	1.3.0.0
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 431109 (2016_Kabylake)
----------	--------------------------

47.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1405269524	KBL:HW:p1:[LAB_BLOCKER]Issues during the system idle on transformer machines
1404716333	Config Block linkage and document updates
1209101467	[SCS] Provide eMMC _DSM Function 9 as part of SDBus driver requirement
1504331134	Request T12 timing to meet >500ms as VESA spec
1504338909	Remove gPlatformInfoProtocolGuid protocol dependency from MinTree so we can eliminate PlatformInitDxe driver.
1209112259	Integrate 2 KBL patches, for B0/H0 0x42
1405311613	[KBL] Add BIOS setup options for new PID Policy
1208554306	Enable Ph2/3 on PEG immediately after clearing DEFER_OC
1504342182	[kaby_lake]Invalid UUID error in _OSC
1504338910	Incorporate SiliconPkg cleanup change from SSG to MinTree.
1604217500	Bug check "CRITICAL PROCESS DIED" observed after S3 exit in Pleasant Star ES1 & ES2 samples with only Opal2.0 BIOS Password enabled
1209081137	Link CmdTristateDis from BIOS Setup to Memory Configuration block
NO_HSD	disable watchdog timer using new test menu setup option
1604219445	[KBL S/H SG]: eGPU FAN is continuously rotating with B0/B1 Processor without any workload.
1504330198	KBL S USB Type C : USB Type C ACPI HLK failure on Discrete & TBT Type C Ports configs on KBL S Platforms

47.2 BP Client Common Core Sync-up Changes

None

47.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



48 BIOS – KBL CRB v060

BIOS version	0.060	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1047	
GOP Driver	9.0.1056	
1.5MB ME Firmware SKU	11.6.0.1128 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0009	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA6 R0/D0: 0xA8 G0 : 0x26 H0 : 0x3E KBL S/H A0: 0x34 KBL S/H B0: 0x3E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.2.0
	MRC Version	1.2.0.3
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 428810 (2016_Kabylake)
----------	--------------------------

48.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504334842	[KBL] Latest MinTree build caused BSOD when booting WIN10.
1804659285	Touch Input Filter KlocWork Issue
1208820911	Global_remove_if_unreferenced usage should be cleared
1604229060	KBL: VTIO: Implement XHCI Descriptor and ACPI device SDEV entries
1604229065	KBL: VTIO: Add Heci and SPI controller entries in SDEV table
1604229071	KBL: VTIO: Add setup option to include/exclude SDEV entries
1604235973	KBL/SKL - Integrate latest GOP 1056 and VBIOS 1047
1304585330	[OC]Release Bios hangs at postcode 0xDD23 when BCLK is set to 300MHz
1404734569	Need to update USB3 PDO flow for BIOS

48.2 BP Client Common Core Sync-up Changes

None

48.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



49 BIOS – KBL CRB v059

BIOS version	0.059	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1055	
1.5MB ME Firmware SKU	11.6.0.1128 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0009	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA6 R0/D0: 0xA8 G0 : 0x26 H0 : 0x3E KBL S/H A0: 0x34 KBL S/H B0: 0x3E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.2.0
	MRC Version	1.2.0.2
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 426673 (2016_Kabylake)
----------	--------------------------

49.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604072230	[Beta Req]KBL FSP BIOS: BCLK values are not reflecting correctly in BIOS, after changing the value and restarting.[trriage]
1405316507	PCH DMI ASPM option in BIOS should have L0s and L1
1504335486	Support Release FSP Binary to boot with Debug build Wrapper
1404582479	Remove duplicat and unused DataHob & FVs
1804657060	PCH Voltage Margining in SLP_S0 option value incorrect
1208820911	Global_remove_if_unreferenced usage should be cleared
1304652740	PSF address-based peer-to-peer decoding should be disabled by default
1604232887	Updating SETUP_DATA_REVISION
1208998357	Package C-State demotion & Un-demotion option disabled by default
1504305144	KBL: SMBIOS : SMBIOS (Type 17) always show 4 memory device
1405360466	KBP PCIe Cm/Cp values are lost after S3 exit
1604228387	[KBL FSP]: Enable Natural Alignment check for FSP UPD's
1604228445	[KBL FSP]: Keep all FSP UPD in naturally aligned byte order
1405269347	CLKREQ routing wrong for M.2 SSD - version 2
1304617714	[kaby_lake.other]Wake on WiGig Disable
NO_HSD	BIos ROM 51 with ME 1104 - Long Boot time with RVP11
1504334842	[KBL] Latest MinTree build caused BSOD when booting WIN10
1604232887	Expose the Setup option from InternalOnly tag : SA_SETUP.CmdTriStateDis
1405323227	[Variable lock should happen within the driver]
1604228375	[FSP]: Update GenCfgOpt to generate UnusedUpdSpace as UINT8 array fields
1504329973	KBL:GPIO table initial need early than read GPIO pin status]
1208820911	[KBL]Remove unused Global_remove_if_unreferenced variables in CPU code.
1304662812	Fix Klocwork issue #59613 from CNL Stream



1304662528	[KBL]Integrate CRB CSME FW 11.6.0.1128 into BIOS
1604231754	[KBL FSP]: Reduce the FSP T reserved space
1504327148	MinTree Cleanup by removing dependency on BpCommonPkg, ClientCommonPkg and KabylakeFspPkg.
1304662507	[KBL]Adding MEBx version 11.0.0.0009
1504268811	[KBL FSP] Request to add memory info for resource calculate - Addressing review comments
1504335231	Fix ASSERT or potential hang when retrieving Bist structure by calling SecPlatformInformation ()
1504334833	Move PCD MinTreeEnable to SiPkg.

49.2 BP Client Common Core Sync-up Changes

None

49.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



50 BIOS – KBL CRB v058

BIOS version	0.058		
BP common core revision	1.3.4.0		
RoyalPark core version	1.3.4.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1055		
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2740)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA6 R0/D0: 0xA8 G0 : 0x26 H0 : 0x3E KBL S/H A0: 0x34 KBL S/H B0: 0x3E		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.2.0	
	MRC Version	1.2.0.1	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 424432 (2016_Kabylake)
----------	--------------------------

50.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1405343913	Expose gPlatformModuleTokenSpaceGuid.PcdSmmThunkEnable to external code (remove InternalOnly mark)
1504306586	Enable and Disable the iMMA control flag settings (EvLoader and EvLoaderdelay setting) over BIOS Setup menu option for KBL/SKL platform iMMA memory Training
1405256724	Add ability to change SSC settings
1504327148	MinTree Cleanup by removing dependency on BpCommonPkg, ClientCommonPkg and KabylakeFspPkg.
1405352908	PCH Energy Reporting Enable/Disable is opposite
1604221183	Voltage Margining is enabled by default when SLP_S0# is asserted
1208901626	Workaround with 0xA2[2], 0x50[2] and 0x80E0[16]
1405320122	[BSF] [1SWS] PCH PCIe root port MPC bit incorrect with VTd
1304640554	KBL: Remote Secure Erase: BiosLastStatus doesn't report the match error.
1504299769	V48_external and External VS_Build no display with Display Port on KBL-S board_KBPI
1604198225	SUT entering to S4 while doing hotplug of Type-C charger
1405337392	Revert Chipsetinit for SPT-LP and SPT-H to version 52
1504330198	KBL S USB Type C : USB Type C ACPI HLK failure on Discrete & TBT Type C Ports configs on KBL S Platforms
1209016016	Integrate 2 KBL patches, for B0/H0 0x3E
1304606577	[OC] Platform recovery is not working in high BCLK
1304611326	[OC] Command stretch with N:1 is not working
1604229115	[KBL/SKL - Integrate latest GOP 1055]
1504268811	[KBL FSP] Request to add memory info for resource calculate

50.2 BP Client Common Core Sync-up Changes

None



50.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



51 BIOS – KBL CRB v057

BIOS version	0.057	
BP common core revision	1.3.4.0	
RoyalPark core version	1.3.4.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1054	
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2740)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA4 R0/D0: 0xA8 G0 : 0x26 H0 : 0x3C KBL S/H A0: 0x34 KBL S/H B0: 0x3C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.1.0
	MRC Version	1.1.0.5
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3698



P4 Label	@ 422572 (2016_Kabylake)
----------	--------------------------

51.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1504328294	[CNL] CPU RC Klockwork issues - Sync to KBL
1504281192	[KBL FSP]Request FSP debug binary and interface for modifying serial port configuration
1604228445	[KBL FSP]: Keep all FSP UPD in naturally aligned byte order
NO_HSD	Sync CpuMpPci Override with BP 1.3.4 UefiCpuPkg
1209010145	Integrate SKL patch for D0 0xA8
1405053128	[KBL][MRC]PMO: Memory Voltage option inside the Overclocking menu to adjust VDD down from 1.2V to 1.10V
1209009097	KBL V56 hits assert when booting on SKL ULX silicon
1404716333	Config Block linkage and document updates.
1304560618	Fixes to CL#409617 BIOS is not behaving as expected when mixing XMP and non-XMP DDR4 modules.
1504322676	[KBLS][I2C] I2C controller always D0 after connect to Touch Panel
1405237484	[ME RCR] Touch filter code for customization requests
1604219722	Uploading RST PreOS 15.2.0.2740 to solve Ctrl+I delay issue in legacy mode.
1304510823	TBT BIOS: TR Support
1504311483	[KBL] Port KabylakePlatSamplePkg\Override\ClientCommonPkg\Universal\SmiVariable to new BpCommonPkg\Universal\VariableSmi from BP1340.
1208897515	Can not Disable BIOS Guard without Manually Operations - BIOS KBLSE2R1.R00X050.P01.16080111715
1405320712	S3_MEMORY_VARIABLE_NAME variable is used instead of ACPI_GLOBAL_VARIABLE variable which causes security issue.
1209002310	KBL FSP BIOS Fails to Compile a Performance Build
1405337392	[kaby_lake.other][SPT-LP/H, KPB-H] Update to Chipsetinit files to make use of calculated byte enables
NO_HSD	HeciPdtUnlockMsg() contains incorrect usage of sizeof()
1604225564	KBL-Security: After enabling TXT system is not booting beyond Alias CHECK (ACHECK postcode: A670 & A700) and not at all entering into OS



1804340886	BIOS should use LPC as default HPET and IOxAPIC requester/completer ID
1405332763	Memory property value (buffered/unbuffered) in SMBIOS is incorrect in 2016 mWS platform
1504302841	Fixes to KBL: SMBIOS : MaximumCapacity (Type 16) will be wrong for Memory Down platform
1604225843	C6Dram disabling in BIOS by default
1504326763	[Tarpon][AMT]Disk information doesn't show ODD devices info in WebUI.
NO_HSD	BIOS Fail To Enter SV Module With DBG Bios

51.2 BP Client Common Core Sync-up Changes

None

51.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



52 BIOS – KBL CRB v056

BIOS version	0.056		
BP common core revision	1.3.4.0		
RoyalPark core version	1.3.4.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1054		
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA4 R0/D0: 0xA6 G0 : 0x26 H0 : 0x3C KBL S/H A0: 0x34 KBL S/H B0: 0x3C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.1.0	
	MRC Version	1.1.0.3	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 419837 (2016_Kabylake)
----------	--------------------------

52.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1405320712	[kaby_lake.rvp3]S3_MEMORY_VARIABLE_NAME variable is used instead of ACPI_GLOBAL_VARIABLE variable which causes security issue.
1404716333	[KBL] Config Block linkage and document updates
1208974830	[OC] Disabling thermal monitor also disables BIDIR_PROCHO
NO_HSD	Back out changelist 405833. [1208511776] Error for Audio device in Modern Standby Sleep Study report when HD Audio device is disabled
1604225843	C6Dram disabling in BIOS by default
1504328694	[KBL PERF]V52.2 and V52.3 RVP3's s3 resume time too long when "PTT enable".
1404582479	Remove duplicate and unused DataHob & FVs
NO_HSD	Assign Board Id for KBL Hawk Mountain IDV
1604224919	[kaby_lake.rvp3]KBL USB Type C : USB Type C ACPI HLK failure on Discrete TBT Type C Ports on KBL Platforms
1504281170	[KBL FSP] Request to add hook for checking memory initial fail
1604225172	Integrate 2 KBL patches, for H0/B0 0x3C
1604225086	KBL/SKL - Integrate latest GOP 1054
1405234460	Public Key provisioning in the platform DB via BIOS Setup
NO_HSD	Fix BSOD dump data not crated for RAID/SRT device:

52.2 BP Client Common Core Sync-up Changes

None

52.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



53 BIOS – KBL CRB v055

BIOS version	0.055		
BP common core revision	1.3.4.0		
RoyalPark core version	1.3.4.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1053		
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA4 R0/D0: 0xA6 G0 : 0x26 H0 : 0x3A KBL S/H A0: 0x34 KBL S/H B0: 0x3A		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.1.0	
	MRC Version	1.1.0.0	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3698	



P4 Label	@ 418008 (2016_Kabylake)
----------	--------------------------

53.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1804345663	Assert with Debug BIOS on RVP7
NO_HSD	Disable Reset by setup option for KBL
1404529814	SKL needs to support DXE GOP debug print
1304633041	[kaby_lake.other]KBL MRC: KW scan error fix in MrcWriteLeveling.c
1208976798	Integrate SKL patch for R0 0xA6
1208932040	Fix security issue related to EBDA pointer access inside USB RT module
1604209725	USB 3.1 Device not Enumerating as Booting Device in BIOS Menu With TBT Card.
1604160580	[Type-C KBL-Y RVP3] : File explorer is not refreshing as expected while plug/unplug the USB devices through USB ports.
1404834048	please release GenNVS tool
1504326471	Fix Klocwork issues
1504324581	capsule update scatter gather corruption
1604223415	RpFunctionSwap does not work on KBL PCH RC
1604223298	KBL Security : Integrate new ACM binaries with fix for HSD:1304566156
NO_HSD	BP 1340 sync up
1604218477	KBL Security: Unable to change secure boot profile into Windows Preproduction & Android in BIOS setup
1604220431	UCB Type C HLK failure on AR TBT or Discrete Type C Ports on KBL Platforms
NO HSD	Update RC version to 1.1.0
1405269347	CLKREQ routing wrong for M.2 SSD
1604220536	[DPTF] _OSC Error logs shows up in event viewer on S4/S5 resume
1208910415	Exact same Modules listed twice in FDF under SiPkgBinary usage when compared to src code version
1404716333	[KBL] Config Block linkage and document updates
1405069356	DisplayDimmPopulationErrMsg should have been a board feature not part of SaPlatformInit



1804343577	Legacy IO low latency mode is required for some robotic applications
1604171280	Port Micro SFF RVP changes to KBL bios source code.
1504324257	some of warning messages will be shown after update FRC 1.0.4
1604220177	Changed LSPCON setting does not reflected in the VBT after IFWI flashing
1304581726	When CSM Control set to Always On platform hangs during boot after FWupdate failure with Corporate image
1504323149	[KBL] Remove obsolete SPT LP stepping specific checks in USB _UPC and _PLD methods

53.2 BP Client Common Core Sync-up Changes

None

53.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



54 BIOS – KBL CRB v054

BIOS version	0.054	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1053	
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA4 R0/D0: 0xA4 G0 : 0x26 H0 : 0x3A KBL S/H A0: 0x34 KBL S/H B0: 0x3A	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.5
	MRC Version	1.0.5.3
	BIOS Guard(PFAT)	2.0.3683
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 415108 (2016_Kabylake)
----------	--------------------------

54.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1804299193	[KBL] SOL redirection doesn't display HDD password Popu-up
1405294562	[SVBIOS] Assert when booting in V52 module String.c
1804344071	PI_Swing should be programmed per chipset type, not per board
1504315836	[PEGAX8][Sailfish MFF] After adding NSID code change, AMT_013 will fail when we use M.2 NVMe SSD to be Add-in PCIe card during test.
1405263812	[KBP] Wrong USB OC mapping by BIOS
1405307532	[KBL] Integrate SV BIOS Guard Module based on BIOS Guard Module 2.0.3683
1604169328	SA PCIe init code risk which may burn power with unused port
1804343798	[cAVS] HDAS _DSM Fun3 does not return correct status
NO_HSD	Assign Board ID for KBL Hawk Mountain
1208485250	PchVerbTable structure definition doesn't allow auto compute of array size
1208946713	Integrate 2 KBL patches, for H0/B0 0x3A
1405199463	Fix for issue "Changing cache attribute during DXE where interrupt can happen at the same time would hang the system". -- rework
1504281133	Request to have BCT interface for modify Pcds
1604217979	KBL FSP BIOS : SUT is hangs at Post code "0096" when CSM control is set to ON
1804340191	Add a PTSS HSIO table for KBL A0 chipset, RVP8 board
1604214586	Address Coreboot.org comments on KBL FSP 1.3.0 header files
1604220050	KBL/SKL - Integrate latest GOP 1053
1604216881	[Kabylake] RC1.3.0 CMOS access library implementation bug
1504302841	KBL: SMBIOS : MaximumCapacity (Type 16) will be wrong for Memory Down platform
1304603040	KBL: HWPS maximum performance should be set to 0xFF when enabling the overclocking menu
1405287213	Fix for PCR[1] variation through boots
1405267931	[SATA] BIOS does not set SATA's SATAGC.AIE bit when Alternate ID is enabled for SATA Controller



1804280102	Fixed RTD3 for SATA devices and RAID volumes:
1604190350	[KBL-S] [HLK]: -USB Exposed Port System Test fails on RVP8 DT with multiple USB ports mapping.
1405076210	uSFF Interposer support using existing KBL RVP11 platforms

54.2 BP Client Common Core Sync-up Changes

None

54.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



55 BIOS – KBL CRB v053

BIOS version	0.053		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1052		
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA4 R0/D0: 0xA4 G0 : 0x26 H0 : 0x38 KBL S/H A0: 0x34 KBL S/H B0: 0x38		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.5	
	MRC Version	1.0.5.3	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@ 413151 (2016_Kabylake)
----------	--------------------------

55.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1304603881	OC: When setting Maximum GT frequency in BIOS menu to 300MHz the ratio in the MMIO is being set to 350MHz
1804342403	Wrong GPIO ACPI Device ID on KBL PCH-H
1604219207	Integrate 2 KBL patches, for H0/B0 0x38
1405255194	CPU temperature does not update (is not accurate) while in CS
1604218612	Integrate 2 SKL patches, for R0/D0 0xA4
1804342741	RSE: BIOS does not report Drive Authentication Failure in one RSE scenario
1504304319	USB3 Termination Test failing with "No Valid SuperSpeed USB Device found after reboot"
1804341867	BIOS must not access ICC registers after EOP
1604213450	Microsoft PS/2 Mouse Yellow bang observed on KBL-S DT CRB
1405264760	[SVBIOS] Assert when booting in PeiSaOcInitLib.c
1504298653	KBL:BISOGuardHobInit reference to wrong setup
1304496859	Script to remove extra files in FSP codebase
1208859356	[KBL] [CNL] Need _TSP added to wireless participant and
1405274837	BIOS Setup under DPTF section shows "participant" string twice for Wireless participant
1504311727	[KBL DT]V50 NR_Perf_S3 resume fail but NR build can not reproduce.
1504314128	[HP]The Sideband port 0xB0 for KBPs PCIE20-23 cant be accessed after POST
1604139463	KBL FSP fails GCC build. - Documentation Update

55.2 BP Client Common Core Sync-up Changes

None

55.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
------------	-------------	------------------



	None	
--	------	--



56 BIOS – KBL CRB v052.1

BIOS version	0.052.1		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1052		
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA2 R0/D0: 0xA2 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x36		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.5	
	MRC Version	1.0.5.3	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@ 411352 (KBI DOT Stream KBL_G0_PO)
----------	-------------------------------------

56.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604210233	Deep Sx functionality not working on KBL boards. Back out Offending changelist 400687
1604181637	[kaby_lake.rvp6]KBL: Cat err (MCA error) seen when SA GV memory frequency set to 1200 MHz
1504299844	[KBL] Change PEI_MIN_MEMORY_SIZE size back to 48MB during PEI phase
1804339653	add DetectTimeout setup option to each rootport
1208906550	Uploading new RST PreOS binaries, version 15.2
1804340712	PEI Post-mem BoardConfigInit() function called in Pre-mem phase
1604216874	Integrate 2 KBL patches, for B0 0x36
1208882263	ME HFSTS resgisters change based on power source and causes inconsistent TPM measurements.
1208882590	Add SBI lock test into HSTIp
1804299193	[KBL] SOL redirection doesn't display HDD password Popu-up
NO_HSD	One Click Optane Enable
1304603288	[kaby_lake.other]KBL MRC: Sweep range should be per channel in JWL Cleanup step
1405267682	[NVMr] BIOS resets Cycle Router's EGCR.TSCAS bit despite remapped PCIe SSD is not configured to use legacy interrupts.
1804341418	[kaby_lake.rvp7]Debug BIOS hangs at PC 0036
1405234460	Public Key provisioning in the platform DB via BIOS Setup
1304560618	Fixes to CL#407717 BIOS is not behaving as expected when mixing XMP and non-XMP DDR4 modules.
1405274794	[Pull in latest IntelFsp2Pkg and IntelFsp2WrapperPkg from open source https://github.com/tianocore/edk2.git]
1804340737	[KBL] SlpS0 doesn't work on ULX boards
1604215688	[kaby_lake.other]KabyLake OC board porting
1405274691	[kaby_lake.other]KBP: Update the HSIO version number in the platform menu to reflect ModPHY table used for KBP-H
1208770623	Clean-up LCD Control BIOS Setup options per customer request



1304538731	[kaby_lake.other]KBL MRC: Avoid false pass in JWL Cleanup step
------------	--

56.2 BP Client Common Core Sync-up Changes

None

56.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



57 BIOS – KBL CRB v051

BIOS version	0.051		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1046		
GOP Driver	9.0.1052		
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA2 R0/D0: 0xA2 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.4	
	MRC Version	1.0.4.4	
	BIOS Guard(PFAT)	2.0.3683	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@ 407839 (2016_Kabylake)
----------	--------------------------

57.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1604193343	[KBL BIOS] Error handling is not proper for AllocatePool function calls under KabylakePlatSamplePkg [debug] part2
1304560618	KBL][OC] - BIOS is not behaving as expected when mixing XMP and non-XMP DDR4 modules
1208770623	Clean-up LCD Control BIOS Setup options
1804339738	[PCH BIOS CI] All platforms hang at PC 0055 after resume from S3
1504307868	[kaby_lake.rvp8_I][KBL DT]V50_KBPI gets S4 resume fail with Debug Build but V49.1 can not reproduce.
1208852021	KBL:BIOS:P3: MSFT Coengineering request to disable secondary screen in BIOS
1405268624	[KBL] Integrate BIOS Guard Module 2.0.3683
1208708951	[KBL] When PcdBootGuardEnable is FALSE, post build script fails without proper error handling
1405262966	Add the missing SmBusLib dependency in PeiSaiPolicyLib.inf
1405268153	Incorrect register XHCI DBC DBCCTL offset setting
1208872213	[SVCPU] Create a separated PiSmmCpuDxeSmm for KabylakeSvRestrictedPkg
1504306596	PRMRR Base is 0x0 even if EnableC6Dram is set to 1
1504306345	No Room for BootloaderTolumSize
NO_HSD	Voltage Optimization setup default does not work properly[debug]
1604212942	Integrate 2 SKL patches, for R0/D0 0xA2
1208820911	Global_remove_if_unreferenced usage should be cleared (platform part)
NO_HSD	Update hash key CoreVerify_RP1330_RP01_CSP020_KBLTEST.db.
1405255240	Default sample period (_TSP) for all thermister (GENx) participants should be 5
1504289987	[kaby_lake.other][Error QUI log while building BIOS]
1504307849	[KBL DT]V50 FSP GCC build boot fail with KBPI board, this issue can't reproduce with RVP3 KBL.
1504298157	[kaby_lake.rvp3]KBL: Build failed on Windows 7 32 bits



1604212427	[KBL BIOS : Intel Logo is not observed on POST Screen]
1208511776	Error for Audio device in Modern Standby Sleep Study report when HD Audio device is disabled
1304588852	[kaby_lake.other][KBL MRC: Skip CKE Power Down enabling during SAGV switch]
1604151910	KBL BIOS: DP display is not observed in BIOS and EDK shell with Dual display connected to SUT with FSP GCC wrapper image
1404501683	[FSP] Enable BootGuard support in FSP wrapper build
1304551464	[OC] Memory Ratio Sporadically Displaying Incorrect Values
1208512300	iTouch code is asserting due to ME is not ready after hard reset
1504305571	Cannot detect PCIe end device after update to RC101.
1405167930	To add detection time out for each of PCI root port
1504305099	Dell D8 Sailfish-MT7[Wistron] AMT MT_AMT_ODD information not shown on WebUI and AMT commander
1208838133	Push from sunrise_point: KBP-H. PCIe3 not performing link equalization
1208820889	FreePool usage in PEI clean up for Cpu, Core, SystemAgent, Csme and Security.

57.2 BP Client Common Core Sync-up Changes

None

57.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



58 BIOS – KBL CRB v050.1

BIOS version	0.050.1	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1052	
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.4
	MRC Version	1.0.4.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 405958 (KBI DOT Stream KBL_G0_PO)
----------	-------------------------------------

58.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504307849	[KBL DT]V50 FSP GCC build boot fail with KBPI board, this issue can't reproduce with RVP3 KBL.
1604212427	KBL BIOS : Intel Logo is not observed on POST Screen

58.2 BP Client Common Core Sync-up Changes

None

58.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



59 BIOS – KBL CRB v050

BIOS version	0.050	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1046	
GOP Driver	9.0.1052	
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.4
	MRC Version	1.0.4.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 405200 (2016_Kabylake)
----------	--------------------------

59.1 Resolved Client BIOS HSD sightings

HSD#	Title
1304407212	[OC] System does not seem to be factoring BCLK into fast boot flow
1404256869	Use IntelFrameworkPkg and IntelFrameworkModulePkg only when CSM is enabled otherwise we should build without them, starting from BP 1.4
1404403499	[SKL-SDS] Capsule update of BKC13 BIOS/ME results in TPM Yellow Bang and Sporadic BSODs
1404834325	Limit CMOS usage and move to a CMOS library part2
1405204838	Kabylake silicon init reclassification to Intel Confidential
1604209715	KBL/SKL - Integrate latest GOP 1052 and VBIOS 1046
1208849274	PchXhciLegacySmiEnGet() & PchXhciLegacySmiEnSet() points to PCI Base & not MMIO Base
NO_HSD	Voltage Optimization setup default does not work properly[debug]
1604202327	Wrong error check after AllocatePool function in HiiConfigAccess.c
1604206176	Sync latest IntelFsp2Pkg & IntelFsp2WrapperPkg from GIT hub
1504280849	[KBL FSP] Need CSM support for FSP Wrapper Build
1604162289	[kaby_lake.rvp7]KBL_Sx: System hang on postcode 009b with CATERROR during Reboot cycle - Removal of XHCI duplicate resets as per the UEFI core team request. More details on HSD., Changes in Comments
1208852347	Inserting any X8 or X4 PCIe card in to the PEG slot will cause the debug BIOS to ASSERT and fail to boot
1208839200	Remove stale data from CPU's Doxygen overview pages

59.2 BP Client Common Core Sync-up Changes

None

59.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



60 BIOS – KBL CRB v049.1

BIOS version	0.049.1	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1045	
GOP Driver	9.0.1051	
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.4
	MRC Version	1.0.4.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 403249 (KBI DOT Stream KBL_G0_PO)
----------	-------------------------------------

60.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604162289	[kaby_lake.rvp7]KBL_Sx: System hang on postcode 009b with CATERROR during Reboot cycle - Removal of XHCI duplicate resets as per the UEFI core team request

60.2 BP Client Common Core Sync-up Changes

None

60.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



61 BIOS – KBL CRB v049

BIOS version	0.049	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1045	
GOP Driver	9.0.1051	
1.5MB ME Firmware SKU	11.6.0.1099 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.4
	MRC Version	1.0.4.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 402652 (2016_Kabylake)
----------	--------------------------

61.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1208849317	[SKL_PVT_SDS] SUT hangs in S4 on CI Build 5835 - https://fm-codecollab.intel.com/ui#review:id=152908
1304491029	[KBL] WiGig Regulatory Updates
1404834325	Limit CMOS usage and move to a CMOS library
1405204838	Kabylake silicon init reclassification to Intel Confidential
1208820889	FreePool usage in PEI clean up
1404874522	Need to encapsulate Btg Eventlog creation into a Lib for ease of integration
1208815140	[KBL] Fill SinitAcmSize value when Sinit is loaded into TxtHeap
1208838133	Push from sunrise_point: KBP-H. PCIe3 not performing link equalization
1405216219	BIOS bat scripts do not produce valid spi images
1404585568	Request to print out both default policy values and updated policy values
1208838375	Lock CPU soft straps on S3 Resume path
1804198388	XHCI XHCC settings are lost after S5
1604206176	Sync latest IntelFsp2Pkg & IntelFsp2WrapperPkg from GIT hub
1405195075	Should use PCD instead of Build flags in our BIOS code base
1504298793	CNL/KBL FSP: PCH_DEVICE_INTERRUPT_CONFIG structure missing from UPD header
1804217195	Enable Pmic SlpS0 VM support by default
1604158615	[kaby_lake.rvp1]SA_DT: For silicon NVS, it should consume config block
1504285041	KBL-Y: DPTF , Temperature show "0" under Critical Policy
1208789415	BIOS 43 : 0 Temp in TCPU on KBL- KBL boards
1604185728	Samsung & Pleasant-star ES1 PCIe NVMe disk lost during warm reboot cycle

61.2 BP Client Common Core Sync-up Changes

None



61.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



62 BIOS – KBL CRB v048

BIOS version	0.048		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1045		
GOP Driver	9.0.1051		
1.5MB ME Firmware SKU	11.5.5.1000 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.3	
	MRC Version	1.0.3.0	
	BIOS Guard(PFAT)	2.0.3561	
	ACM (TXT)	Version 1.0.0	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@ 400326 (2016_Kabylake)
----------	--------------------------

62.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206679608	KBL: Enable testing for UserPhysicalPresent related features
1208830313	Integrate 3 KBL patches, for A0/B0/H0 0x34
1405164019	[KabyLake][MSFT HLK]Connected Standby Hardware Security Test fail - "SPI Flash Configuration SPI Region Access Rights Invalid"
1208442059	Capsule Update Infrastrucure for Update firmware to set CS as the default power state instead of S3
1208552934	Fix FSP UPD description
1208552934	Control Intel ME Global Reset on Critical Failure Addendum
1208541948	Re-inialize spinlock if AP times outs on StartupAllAps.
1604202421	KBL FSP: DmiVcm UPD Default value is mentioned as 1 but set to 0
1804332300	KPT-H B250: Intel RST and System Acceleration with Intel Optane Technology Mode NOT available to select for SATA Mode
1504289987	Error QUI log while building BIOS
1504262382	[kaby_lake.rvp7][KBL]dynamics update solution to detect KBL and SKL for DMAR OEM Table ID
1208771125	[KBL] Need to change WiFi and WiGig participants into 1 participant (Wireless participant)
1504292303	[Kaby Lake] BIOS should assign B0:D27 PCIe to ITSS_PIR6
1504295537	[KBL][SST][BIOS RCR] Add 3rd Party Post-Processing module in BIOS -bitmask/GUID
1504295018	KBL: mPchResetProtocol protocol installation incorrect
1504277370	CoveCreek: Align with min tree structure in Setup folder
1405142094	incorrect usage of assert_efi_error

62.2 BP Client Common Core Sync-up Changes

None



62.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



63 BIOS – KBL CRB v047.1

BIOS version	0.047.1	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1045	
GOP Driver	9.0.1051	
1.5MB ME Firmware SKU	11.5.5.1000 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x34 KBL S/H A0: 0x34 KBL S/H B0: 0x34	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.3
	MRC Version	1.0.3.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 398479 (KBI DOT Stream KBL_G0_PO)
----------	-------------------------------------

63.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO_HSD	Update to Patch #34 for all KBL Steppings

63.2 BP Client Common Core Sync-up Changes

None

63.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



64 BIOS – KBL CRB v047

BIOS version	0.047	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1045	
GOP Driver	9.0.1051	
1.5MB ME Firmware SKU	11.5.5.1000 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x30 KBL S/H A0: 0x2C KBL S/H B0: 0x2C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.3
	MRC Version	1.0.3.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 1.0.0
	ACM (Boot Guard)	2.0.3554



P4 Label	@397974 (2016_Kabylake)
----------	-------------------------

64.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1208702997	Remove macro RELEASE_MODE_DEBUG() and macro RELEASE_MODE_DIAGNOSTICS() usage
1208708498	SKL/KBL/CNL - Prevent PCI lanes Tx/Rx till reference clock is available
1208757509	[kaby_lake.rvp11]PEG GFX have no display on KBL PPV system for B0 Unit
1207743958	Provide Crash Dump using Capsule
1208442059	Dxe Driver - Update firmware to set CS as the default power state instead of S3
NO_HSD	Integrate TXT BIOS ACM revision 1.0.0
1804330233	[KBL]Integrate CRB CSME FW 11.5.5.1000 into BIOS
1405157542	[Create BIOS setup option for disabling PMC patch when requiring access to modphy iolanes related to common lane2]
1304529166	[SVBIOS] Change default value to knob SmbusSpdWriteDisable to 0x0
1304509300	[SVBIOS] Enable SGX by default in SVBIOS
1208751917	[HEDT-BSFBIOS] : After setting BIOS Password and resetting the system. The BIOS does not accept the new password when attempting to enter the BIOS screens
NO_HSD	Disabling SINIT ACM by default
1205667562	SINIT module integrated in BIOS
1604180977	change GPIO initialization and RTD3 ASL for WWAN.
1804257266	[KBL][HddLockPassword] After disk lock and escape 'Unlock' pop-up platform hangs on black screen with prompt
1604190337	[KBL BIOS][KBL_S_CRB] : Sx functionality broken with Type-C enabled system[debug]
1604186199	[kaby_lake.rvp8]KBL BIOS: SUT hangs at the postcode 0036 with warm reboot cycling through GPV Tool.
1208763621	Serial Agent(Serial port) can't work for KBL BIOS release build
NO_HSD	Bios Bug "CpuPrivateData should be pointer with valid value". It is currently 0x00.
1405165000	Workaround for eSPI PCH bug that prevent SLP_S0
1208731743	[[KBL-ULT H5 PO] [WW27.02] System unable to Boot and stuck at PC 0002 in PPV Screening



1207164182	[Yellow bang for IGD device in Device Manager with Aperture Size set to 4096MB]
------------	---

64.2 BP Client Common Core Sync-up Changes

None

64.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



65 BIOS – KBL CRB v046

BIOS version	0.046		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1045		
GOP Driver	9.0.1051		
1.5MB ME Firmware SKU	11.6.0.1062 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0xA0 R0/D0: 0xA0 G0 : 0x26 H0 : 0x30 KBL S/H A0: 0x2C KBL S/H B0: 0x2C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.2	
	MRC Version	1.0.2.4	
	BIOS Guard(PFAT)	2.0.3561	
	ACM (TXT)	Version 0.7.2	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@396401 (2016_Kabylake)
----------	-------------------------

65.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1208709388	BIOS chain of trust is broken as FVMain is not authenticated by PEI Core eventhough FVMain is
1208278796	Identify, remove Royal Park functionality which is redundant with regard to Bailey Park : PlatformCmosAccessLib
1504276409	[KBL]V44 KBL debug boot very long time with 0036 which debug message always running "Allocate...."[trriage]
1804327133	KBL PCH RC cleanup from unused InternalOnly and Restricted code
1405151628	iTouch Driver binding support attaches to all PciIo instances causing problem for other driver in the system
1304235556	xHCI SKL: The mass USB device drop off during the reboot
1405170161	File explorer is not refreshing as expected while plug/unplug the USB2 devices through Type
1604162732	KBL-U: In EDK Shell & BIOS-Caps lock/Numslock/Scroll lock LED's not blinking while pressing Lock key's in USB Keyboard
NO_HSD	KBL Security: Unable to set keys in Custom mode option under Secure Boot in BIOS
1208735654	Integrate 2 SKL patches, for R0/D0 0xA0
1304543983	[kaby_lake.other][KBL MRC] DDR4 PDA fixes in WriteVoltageCentering2D
1304543889	[kaby_lake.other][KBL MRC] Updates to Retrain limits
1604195199	[KBL/SKL - Integrate latest GOP 1051 and VBIOS 1045]
1604152921	Cannot enable serial logs when FSP-T is skipped and FSP-M is used
1504279007	Fix KabylakePlatSamplePkg Klocwork issues of G0_PO_X043_3
1208278796	Identify, remove Royal Park functionality which is redundant with regard to Bailey Park : PlatformCmosAccessLib
1208727925	Integrate KBL patch for H0 0x30
1304530698	[kaby_lake.other][KBL MRC] Add Early Write Drive Strength / Equalization step for U/Y LPDDR3 2133 support
1304540383	[kaby_lake.other][KBL MRC] MrcGetCpuTime() is used with UINT32, can cause wrong timeout calculation



1804326054	USB device should not get reported in the Hardware Asset Tables
1604189857	WOL not working with PCIe Native mode disabled in BIOS Setup
1504276007	[kaby_lake.rvp3]Fix multiple definition of "mCpuGlobalNvsAreaPtr" in KabylakeSiliconPkgCpuPowerManagementSmm module
1604187500	Fix bug in CL374190 for NR builds
1404836819	BIOS support to expose I2C ACPI device to OS and manage I2C/GPIO resource
1207743319	Executing 'Continue' from BIOS screen fails on first attempt when triggered from Windows
1504252530	[kaby_lake.rvp8]KBL:Cache for SPI area is set to UC of Certain memory size
1304538731	[kaby_lake.other][KBL MRC] Avoid false pass in JWL Cleanup step
1304371812	KBL OC: Frequencies in OC Memory menu do not show real XMP values
1405125558	SWEQ not selecting the proper Cm/Cp coefficients in KBP
1405055843	PC 0x0b00 hang issue on KBL-LP ULX

65.2 BP Client Common Core Sync-up Changes

None

65.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



66 BIOS – KBL CRB v045.1

BIOS version	0.045.1		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1043		
GOP Driver	9.0.1049		
1.5MB ME Firmware SKU	11.6.0.1062 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0x9E R0/D0: 0x9E G0 : 0x26 H0 : 0x30 KBL S/H A0: 0x2C KBL S/H B0: 0x2C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.2	
	MRC Version	1.0.2.0	
	BIOS Guard(PFAT)	2.0.3561	
	ACM (TXT)	Version 0.7.2	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@ 395722 (KBI DOT Stream KBL_G0_PO)
----------	-------------------------------------

66.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604186199	PC 0x36 Hang - Skip CheckProcessorFeature if feature is disabled
1604190337	[kaby_lake.rvp8][KBL BIOS][KBL_S_CRB] : Sx functionality broken with Type-C enabled system[debug]
1208727925	Integrate KBL patch for H0 0x30
1208727962	Integrate 2 SKL patches, for R0/D0 0x9E
NO_HSD	Incorporate RC 1.0.2 Feedback.

66.2 BP Client Common Core Sync-up Changes

None

66.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



67 BIOS – KBL CRB v045

BIOS version	0.045	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1049	
1.5MB ME Firmware SKU	11.6.0.1062 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x9C R0/D0: 0x9C G0 : 0x26 H0 : 0x2C KBL S/H A0: 0x2C KBL S/H B0: 0x2C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.1
	MRC Version	1.0.1.1
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554



P4 Label	@ 393899 (2016_Kabylake)
----------	--------------------------

67.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1405118544	Source level debug via UDK debugger not working once under BDS phase
1405023712	[kaby_lake.other]KBL-PCH: ModPHY BIOS Request for BasinFalls platforms (AC coupled DMI links) and PCIe/DMI L1 BIOS w/a for E1
1208197584	[BP1410] Review files in ClientCommonPkg and clean unnecessary file/definitions
1208537431	PCIe link stuck in L0 for disabled controller/port
1304529666	BIOS Fail To Enter PKG C, and many Fail to Dispatch while running through xMon
1208510068	[cAVS] Provide platform hook into PCHHDA.asl to enable DspModule
1205651442	[SKL] Bios to send Shutdown(clear) before any reset to prevent TPM lockout from too many disorderly reset
1604187636	High VCCSA power observed with KBL-Y boards.
1604186541	KBL-BIOS-OC: Value of MSR 194[20] is incorrect when enable OverClocking Lock option in BIOS[debug]
1304506667	[KBL][OC]: Core PLL VccTrim offset requires an extra warm reset
1405124608	CreateDynamicSmBiosTable() is implemented wrong and itself is out of spec
1504276178	KBLFP: BCT fail to open bsf file from RomImage - Submitting with updated hash for RpCoreMeasure
1208391545	Update RoyalPark_BP14xx_Dev to use PACKAGE_PATH Build: Kabylake stream.
1604174181	KBL BIOS: Not able to read PL3 values from [MSR 615(23:17)] as per PL3 bios option help text .[debug]
1304419984	[SV BIOS] System doesn't boot with Txt enabled and fuse SMX_DIS = 0x0
1208539957	Remove restricted tag, causing BasinFalls boot issues.
1208555421	Integrate 2 SKL patches, for R0/D0 0x9C
1208491851	[kaby_lake.other] [SKLSDS-KBLBIOS] : KBL 39.99 Capsule does not update ISH
1504276326	KBLFSP: BuildFsp.cmd not working as expected when run it under project root
NO_HSD	Warm Reset on KBL Bioses not working properly
1405065812	Need SysBIOS to set 0x9044[30] = 1 as Frame Buffer Caching is not enabled



1405090229	File extension from GPIODefine.asl to .h
1804294217	[KBL] Platform automatically wake up from S5 (WebUI)

67.2 BP Client Common Core Sync-up Changes

None

67.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



68 BIOS – KBL CRB v044

BIOS version	0.044		
BP common core revision	1.3.3.0		
RoyalPark core version	1.3.3.0		
Video Option ROM (VBIOS)	1043		
GOP Driver	9.0.1049		
1.5MB ME Firmware SKU	11.6.0.1062 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.2 (revision 2649)		
MEBx	11.0.0.0008		
PXE OROM	1.3.21		
Microcode Update –	M0: 0x94 R0/D0: 0x96 G0 : 0x26 H0 : 0x2C KBL S/H A0: 0x2C KBL S/H B0: 0x2C		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	1.0.1	
	MRC Version	1.0.1.1	
	BIOS Guard(PFAT)	2.0.3561	
	ACM (TXT)	Version 0.7.2	
	ACM (Boot Guard)	2.0.3554	



P4 Label	@ 392175 (2016_Kabylake)
----------	--------------------------

68.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804323542	Upload RST PreOS binaries, version 15.2.0.2649.
NO_HSD	Back out change list 376869 to fix 0036 hang issue, Merge UefiCpuPkg PiSmmCpuDxeSmm updates into override. Remove ClientCpuSmmDefLib.h and move into needed definitions into appropriate h file.
NO_HSD	Update KBL ucode to 2C
1604186207	BSF UPD Signature doesn't match with the FSP Binary
1404785465	KBL: Move EPOC, cpu Straps and BCLK resets to pre-mem phase
1604182026	KBL Security: MOR related code cleanup in HSTI log on KBL
NO_HSD	Request policy for specific VR commands for KBL UEFI codebase - (PS4 exit and VR decay BIOS mailbox commands)
1207698876	ResetEnd feature need implement.
1804320448	Useless and confusing code for L1 substates support
1405105641	incorrect library class name being used - PeiDxeI2CMasterCommonLib
1404823897	SPT: BIOS to patch the attached the PMC patch and set plllockok in PMC for ULX/ULT Platforms
1208450829	Integrate 1 KBL patches, for B0 0x26
1304511669	Preset10 coefficients update for PEG
NO_HSD	Back out changelist 386910, which case that Virtual battery percentage shown 0% with cross mark while swithcing from AC to DC
1208446127	Support NX protections for Device Guard
1404585478	Config policy in PEI and DXE should share the same one
1604160580	[Type-C KBL-Y RVP3] : File explorer is not refreshing as expected while plug/unplug the USB device
1504270767	TCO_STS bit does not cleared as expected in PchSmmClearSmi()
NO_HSD	Back out changelist 387853, Merge CL#375514 from CNL stream - [1504207348] Replace DxeSiFviInitLib with DxeSmbiosFirmwareVersionInfoLib
1208391545	Update RoyalPark_BP14xx_Dev to use PACKAGE_PATH Build: Kabylake stream.



1405104050	[SVCPU] SVBIOS 40_77 does not boot to SV module - Stuck at 0xCCD2
1405104020	[SVCPU] SVBIOS 40_77 does not boot to SV module - Stuck at 0xA0DA
1208355757	Build fails when setting gSiPkgTokenSpaceGuid.PcdSourceDebugEnable to TRUE
1604173666	[KBL U/Y PnP] SLP_S0 is active in Idle Display ON with Voltage Margining disabled

68.2 BP Client Common Core Sync-up Changes

None

68.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



69 BIOS – KBL CRB v043.3

BIOS version	0.043.3	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1049	
1.5MB ME Firmware SKU	11.5.0.1055 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.2 (revision 2649)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x94 R0/D0: 0x96 G0 : 0x26 H0 : 0x2A KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.1
	MRC Version	1.0.1.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 392173 (on dot build stream KBL_G0_PO)	



69.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604186199	Back out changelist 376869, 380554 [1208249321] Merge UefiCpuPkg PiSmmCpuDxeSmm updates into override. Causing 0x36 Hang during S4/S5 Cycling
1804323542	Upload RST PreOS binaries, version 15.2.0.2649.

69.2 BP Client Common Core Sync-up Changes

None

69.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



70 BIOS – KBL CRB v043.2

BIOS version	0.043.2	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1049	
1.5MB ME Firmware SKU	11.5.0.1055 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x94 R0/D0: 0x96 G0 : 0x26 H0 : 0x2A KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	1.0.1
	MRC Version	1.0.1.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 390944 (on dot build stream KBL_G0_PO)	



70.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO_HSD	Update RC version to 1.0.1
1604183664	Back out changelist 386910 for following HSD "Virtual battery percentage shown 0% with cross mark while swithcing from AC to DC"
1604184073	Back out changelist 387853 for following issue "KBL BIOS:SUT Is Not Booting to EDK Shell as First Bootable"

70.2 BP Client Common Core Sync-up Changes

None

70.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



71 BIOS – KBL CRB v043

BIOS version	0.043	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1049	
1.5MB ME Firmware SKU	11.5.0.1055 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x94 R0/D0: 0x96 G0 : 0x26 H0 : 0x2A KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.9.0
	MRC Version	0.9.0.4
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 389602 (2016_Kabylake)	



71.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804316503	[kaby_lake.rvp3]Cannot perform any Sx with KBL Daily build number 3341404932705] [Type-C KBL-S RVP8] EC needs to indicate to TI PD for sending source cap for 5v3A in Sx state
1405086366	Unable to install any Windows OS on GT3 Systems when CSM=ON [debug]
1604164741	[kaby_lake.other]KBL FSP: FSP should not reset the platform but instead it should return from the API with proper "FSP_STATUS_RESET_REQUIRED" return code---
1404785465	KBL: Move EPOC, cpu Straps and BCLK resets to pre-mem phase
1405076215	AMT code is not properly tagged
1405091332	Copying the wrong size of SMBIOS Static tables to Dynamic table
1404834325	Limit CMOS usage and move to a CMOS library
1604123026	KBL FSP BIOS: Total memory is not reflecting correctly in EFI shell on RVP8 Boards with FSP GCC BIOS[debug]
NO_HSD	Integrate SKL patches, for R0 0x96. Integrate KBL patch, for H0/J0 0x2A
1604143808	KBL RVP8: BET Tool showing Error for All OC parameters.[debug]
1208183454	[kaby_lake.other]Provide WSMT ACPI table [REV III]
1504207348	Merge CL#375514 from CNL stream Replace DxeSiFviInitLib with DxeSmbiosFirmwareVersionInfoLib
1208430499	Using wrong variable when attempting to check return value in SetupBrowserDxe/Expression.c
1504265129	Replace InternalIsAddressInSmram with SmmIsBufferOutsideSmmValid in ClientCommonPkg
1207834587	[KBL]Fix last check-in from "Load microcode update from CpuMpPei driver."
1205613076	[KB Lake] TME participant not POR for KBL.
1208374024	Implement FSP UPD new type: union
1504253059	CoveCreek: Add Features tags for Advance feature
1208436659	[BP KBL CNL] Using wrong variable when checking return value of function in DxeHstiLib/HstiDxe.c
1604130551	KBL FSP BIOS: Package C3 and above states are not achieving with FSP GCC Wrapper BIOS in KBL Halo Boards.[debug]
1504249610	CoveCreek: Refactoring EC folder to libraries and match min tree structure



1208437012	Clean up the usage of BNUM in dsdtnvs region
1404582470	Library_Class should not have been labelled as DXE_DRIVER and DXE_RUNTIME_DRIVER --- phase2
1604165018	BSOD observed with Multiprocessor_Configuration_Not_Support during Warm Reset

71.2 BP Client Common Core Sync-up Changes

None

71.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



72 BIOS – KBL CRB v042

BIOS version	0.042	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1049	
1.5MB ME Firmware SKU	11.5.0.1055 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x94 R0/D0: 0x94 G0 : 0x26 H0 : 0x26 KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.9.0
	MRC Version	0.9.0.4
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 386637 (2016_Kabylake)	



72.1 Resolved Client BIOS HSD sightings

HSD#	Title
1404937814	[SVCPU] Latest SVBIOS 35_67 does not boot to SV module - Stuck at 0x00D0
1604175205	[kaby_lake.rvp7]KBL BIOS: After Disabling Intel Speed Shift Technology in bios SUT is not booting to OS (BSOD is observed)
1504252175	[cannon_lake][CNL]V33_FSP_RVP5 get Assert and post code:ddA8.[debug]--
1208236414	[Bailey Park Kabylake Cannonlake] Incorrect order of operations due to missing parentheses in SvSummaryBiosGuardDetails.c
1405077822	[[SPT-H] Add support for LPC DID uSFF SKU A155 QMU185]
1405015009	Apple requests to suppress AMT related code using AMT_FLAG as they do not use AMT
NO_HSD	Fix for "Apple Feedback: GpioSetAttributes returns failure and asserts when trying to set PadConfiguration."
1604175773	KBL BIOS : Changes in Active Processor Core values are not reflecting in BIOS and OS
1604175960	[KBL/SKL - Integrate latest GOP 1049]
1208179473	Incorrect return definition of SerialPortRead in SerialPortLib
1304487953	[SV BIOS] System doesn't boot with BiosGuard and BiosGuardModuleSelection
1504253059	CoveCreek: Add Features tags for Advance features - Phase 1
1804303180	[PCH BIOS] Cannot perform reset after re-enable ME State.
1405068973	KBL: ACPI: remove restricted comment from external release
1207541024	KBL EC Support for Power Boss
1604173612	FSP Bit map feature in UPD BSF
1404991495	When shutting down via PM1_CNT register. System asserted in GbeWolWorkaround
1208183454	[kaby_lake.other]Provide WSMT ACPI table [REV II]
1304495782	[kaby_lake.other][Need to add a banner showing SYSTEM REBOOT in the debug log]
1404582470	Library_Class should not have been labelled as DXE_DRIVER and DXE_RUNTIME_DRIVER
1504257084	[kaby_lake.other][KBL] Since we only use 32bit width for MCHBAR base address, we should change our whole source code to use UINT32 for MCHBAR
1604147569	[kaby_lake.rvp8]KBL FSP BIOS: SUT hangs at Post code "9E82" on RVP 8 Board after changing Processor trace memory allocation as 64 Kb in BIOS [debug]
1604134417	KBL_Sx: System hang with postcode 0092/0096 during Warm Reboot/S4 cycle [BLOCKING PV]



1304311681	DO NOT SYNC to CNL - Need to remove UniBIOS from Kabylake
1208450829	Integrate 2 SKL patches, for R0/D0 0x94
1208391545	Update RoyalPark_BP14xx_Dev to use PACKAGE_PATH Build: Kabylake stream.
1604162112	KBL GT2 down GT1 - SPC Unit registers in Gfx need to be locked after checking the GT config with right programming sequence

72.2 BP Client Common Core Sync-up Changes

None

72.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



73 BIOS – KBL CRB v041

BIOS version	0.041	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1048	
1.5MB ME Firmware SKU	11.5.0.1055 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x92 R0/D0: 0x92 G0 : 0x26 H0 : 0x26 KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.9.0
	MRC Version	0.9.0.4
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 384589 (2016_Kabylake)	



73.1 Resolved Client BIOS HSD sightings

HSD#	Title
1208355757	Build fails when setting gSiPkgTokenSpaceGuid.PcdSourceDebugEnable to TRUE
1304481702	[kaby_lake.other]Adding WiGig F1 PEP constraint for Kbl
1208183454	[kaby_lake.other]Provide WSMT ACPI table [REV I]
1504249217	[kaby_lake]Request to add ACPI variable for DTS event and make _L62 a general function call
1208429978	Disable SMBIOS build flag in Basic Build
1504243308	Fix CPU RC Klocwork issues
NO_HSD	For RC 1.0.0 review feedback: GetVariable is deprecated for security reasons. CL 377402 should not use GetVariable to replace GetVariable2
1304475301	Remote Boot to Bios isn't redirected via SOL terminal.
1504174813	external version of RC 0.71, PCH should add ResetSystemLib instance
1604169161	KBL FSP: Remove PcdImageRevision and use PcdSiliconVersionxxxx to report FSP Image version
NO_HSD	Reversion of previous submitted changes "@379132 - Apple request Adding #ifdef AMT_SUPPORT around AMT related code as they do not use AMT"
1207808895	Added w/a for 32KB MMIO Ston Beach remapping. Added SATA.EGCR programming to mask BAR0 address bit[14].
1504184491	[Linux KBL] MCFG MMIO config space at 0xe0000000 is not reserved in the memory map table ---phase2
1604164629	Sync IntelFsp2pkg and IntelFsp2Wrapper pkg from EDK2 open source to KBL - Synced the review comments from the EDK2 OpenSource
1604166322	[TXT]KBL_Security: TBOOT is failing with KBL BIOS v38.2 and v38.25 while performing GETSEC SENTER [debug]
1504106065	[kaby_lake.other]Align BP build environment and tools define for GCC and Clang Step 2 : Refactoring CNL PackageToolInternalOnly\tools_def.template
1504243308	Fix CPU RC Klocwork issues
1604170964	SATA devslp for SATA port2 (M.2 SSD)is not asserting in ULT boards
1208382866	Peg1Enable set to disabled sometimes results in Timeout disabling link
NO_HSD	KBL: Vboost enable/disable in bios menu doesn't work
1604155463	KBL Include UEFI variable control of Flashtools Security: Not able to flash IFWI using FPT tool



1405014952	Apple request "Modify CalculateTimeout" function as it does not handle UINT64 timeout value properly
------------	--

73.2 BP Client Common Core Sync-up Changes

None

73.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



74 BIOS – KBL CRB v040

BIOS version	0.040	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1043	
GOP Driver	9.0.1048	
1.5MB ME Firmware SKU	11.5.0.1055 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x92 R0/D0: 0x92 G0 : 0x26 H0 : 0x26 KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.9.0
	MRC Version	0.9.0.4
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 381879 (2016_Kabylake)	



74.1 Resolved Client BIOS HSD sightings

HSD#	Title
1208370382	Kabylake PTT driver installs TPM2 ACPI for all TPM2 modules
1206933821	Security RC null library needs to be reviewed/cleaned up/ and validated
1304291551	KBL: HWPS maximum performance should be set to 0xFF when enabling the overclocking menu
1208398783	Integrate 2 SKL patches, for R0/D0 0x92
1304407143	KBL: Can't save BIOS setting (F4) with message "Submit Fail for Form: ACPI Settings." - new sighting [debug]
1405014995	Apple Feedback #24 Make CONFIG_BLOCK_HEADER static to avoid inline memcpy codegen that fails to link (CLANG)
1405014930	Apple request change "Finished argument to TRUE on entry, this does not follow PI definition of the function"
1208278139	Push from sunrise_point: [PCIe] LTR override gets re-enforced after device hot-unplugged
1404977037	dead code in PCH NVS needs to be deleted
NO_HSD	Assign BID for uSFF RVP
1604155086	Enable MicroChip eSPI Support on KBL (REV II)
1504184491	[Linux KBL] MCFG MMIO config space at 0xe0000000 is not reserved in the memory map table
1405014546	Apple request change to fix RVP3 boots to assertion
1405015009	Apple request Adding #ifdef AMT_SUPPORT around AMT related code as they do not use AMT
1604164599	[kaby_lake.rvp8]KBL BIOS[OC]: SUT hangs at PC dd80 after changing tRTP value from default value.[debug]
1207728911	MSFT RS1 Co-Engineering/SKL SDS BIOS Defaults Change
1504201276	Determine MMIO resource issue on Hybrid Graphics with KBL Reference Code. [NON BLOCKING PV]
1208375786	Push from sunrise_point: [KBP-H][PCIe] BIOS disable L1.substate pcipm onlyif I select the disable option in BIOS Menu
1304478991	[kaby_lake.other][KBL MRC: Adjust Vtt panic comp threshold for more power savings]
1405005533	[KBL_RVP7] [WW19.4] [WIN10 TH2 10586] WWAN M.2 7160 power is not off during S3



1504181278	[Linux KBL] two error detected when evaluating '_SB_.UBTC.CR01._PLD' and '_SB_.PCI0.LPCB.H_EC' method when doing ACPI DSDT Method Semantic tests
1604166214	ZPODD GPIOs H_16 and H_17 to be configured in KBL-S DT as GPIOs
1208249321	Merge UefiCpuPkg PiSmmCpuDxeSmm updates into override.
NO_HSD	Remove override of fce tool
1604165941	[KBL_Type-C] : Request for Bios WA to support SLP_S0 LED on TYPE C board
1804294833	[KBL][SKL][uPEP] SATA PEP Settings - "Storage controller" constraint not enabled even if chosen in BIOS menu
1604057575	[KBL] USB power management for S sku only
NO_HSD	Enable CoreMeasure for KBL
1504181703	Remove PchResetPpi usage as it is not compliant with PI 1.4 spec
1604164629	Sync IntelFsp2pkg and IntelFsp2Wrapper pkg from EDK2 open source to KBL
1504246641	[cannon_lake]Add GCC version detect in BuildFv.sh
1208271866	[SKLSDS-KBLBIOS] KBL Bios incorrectly sets the Slow Slew Rate for SA for the SKL SDS board.
1208247063	[KBL PV] BIOS - unable to set Vir1 or Vir2 Active Thermal Trip Point <40
1208236669	[KBL PV] Camera - IVCAM has no trip points defined
1604165083	[KBL/SKL - Integrate latest VBIOS 1043]
1504229765	Kabylake FSP binary can not use BCT tool [Updated]
1604134417	KBL_Sx: System hang on postcode 0092 during S4 cycle [BLOCKING PV]
1604162986	Sync IntelFspPkg & IntelFspWrapperPkg of KBL to the RP - OpenSource GIT, by removing overrides - Fix and rename of FspToolpy to sync with openSource git
1207733839	Fix Doxygen warning messages for CPU RC
1304424795	SKL BIOS: BIOS may leave TPM uninitialized on wake from S3. Impact: PlatformAuth will be default and PCRs can be compromised.
1208227851	KBL: Cleanup the EC offsets in the EC opregion of BIOS code
1504217444	Fix building error for enabling the "deprecated function Interface remove" flag
1207143262	Push from mpg_customer_enabling: [Skylake-H] M.2 SATA SSD, non NVME, then we found PCIE CTLE of PCIE#8 is set to 6 (It should be set 8)
1208225777	KBL-PCH: ModPHY BIOS Release Files v154RC4
1604123893	KBL BKC_WSTV : BOOT from usb 3.1 is not working with TBT CARD.



1208253784	Correct TPL for timer events in MpServices Protocol.
1304451243	SSC disable PEG BIOS option cause issues with BIOS boot, also fixed RVP8 hang issue after CL#377335.
NO_HSD	Removed CPU RC and PolicyLib extra space from External code when restricted code removed - RC 0.9.0 Draft1 feedback.
1504240162	[kaby_lake][KBL] The OEM Table ID still show SKL for Kabylake processor [debug]
1405001321	Add support for BoardID 0xE CNL X0 RVP in KBL BIOS.
1804294756	[KBL]Integrate CRB CSME FW 11.5.0.1055 into BIOS
1804185055	[SKL][BIOS] m.2 SSD is not powered off during S3/S4/S5
1604156544	KBL X0 DOE platform porting && 1604126145: KBL RVP5 Crystal DOE BIOS request
1207541024	KBL EC Support for Power Boss
1604144709	CPU DT: Move the Default initialization from SiliconPkg to PlatformPkg & Isolate the Setup updates to separate library along with Null instance
1207908977	KBL: Fix ACPI CPU remarks
1604155463	KBL Security: Not able to flash IFWI using FPT tool
1604152931	kaby_lake.other - FSP uses MTRRs to determine CAR size instead of UPD paramI
1504240251	Fix klocwork issues of Platform Code.
1804268730	[kaby_lake.other]KBL BIOS: Changing Console Output Mode does NOT work[debug]
1604144731	SA DT: Move the Default initialization from SiliconPkg to PlatformPkg & Isolate the Setup updates to separate library along with Null instance
1504230500	Pchsmb.asl asl code lost.
1404256869	Remove IntelFrameworkPkg and IntelFrameworkModulePkg from Royal Park effective BP 1.4
1208255846	Integrate 2 SKL patches, for R0/D0 0x8E and 0x90
1208253979	[kaby_lake.rvp3][KBL PV] Adjust BIOS charge rate table to align with initial EC charge rate
1208236567	[skylake.rvp7][KBL PV] UI - Camera participants named the same in table drop downs
1404970320	ProgramSataTestMode routine optimization
1208249321	Merge UefiCpuPkg PiSmmCpuDxeSmm updates into override. Remove ClientCpuSmmDefLib.h and move into needed definitions into appropriate h file.
1404875981	Feedback to RP impl for Pyrite Drive: ComId for Block SID authentication command



1404876007	Feedback to RP impl for Pyrite Drive: GlobalLockingRangeKey is not supported by Pyrite
1804286344	Yellow Bang at device 85D9

74.2 BP Client Common Core Sync-up Changes

None

74.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



75 BIOS – KBL CRB v039.1

BIOS version	0.039.1	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1041	
GOP Driver	9.0.1048	
1.5MB ME Firmware SKU	11.5.0.1038 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x8C R0/D0: 0x8C G0 : 0x26 H0 : 0x26 KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.8.1
	MRC Version	0.8.1.6
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 377389 (on dot build stream KBL_G0_PO)	



75.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804286344	Yellow Bang at device 85D9

75.2 BP Client Common Core Sync-up Changes

None

75.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



76 BIOS – KBL CRB v039

BIOS version	0.039	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1041	
GOP Driver	9.0.1048	
1.5MB ME Firmware SKU	11.5.0.1038 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x8C R0/D0: 0x8C G0 : 0x26 H0 : 0x26 KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.8.1
	MRC Version	0.8.1.6
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 376611 (2016_Kabylake)	



76.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207762684	Use Cpuid.h & Msr .h files from UefiCpgPkg, remove duplicated defines from CpuRegs.h
1604158285	[kaby_lake.rvp3]FSP BIOS:SUT hangs at 0096 post code sporadically after multiple warm reset & multiple G3 with FSP GCC debug build
1504200243	LGE][KBL][Gram][The MMIO PL1 Tau value is not correct when DPTF enable]
1205613076	[KB Lake] TMEM participant not POR for KBL.
1208240885	[KBL][MRC] BSSA API call for BiosSetMarginParamOffset for TxVref incorrectly uses ChangeMargin
1404980904	[SPT-LP] SMBus - HTIM Register must be configured with optimal value
NO_HSD	merge from KBP-H PO: new mPhy settings, add setup options for rootports 21-24
1604156851	KBL_Security: System is hanging while running VT info tool with V38 BIOS
1604114021	KBL-BKC : Wake from S3/S4 is not working through TBT dock.
1604158902	[KBL FSP] Support FSP 2.0 Draft 9 changes
1604155579	[Kabylake.other] Need to change the FSP UPD signature to align with FSP2.0 spec
1504229765	Kabylake FSP binary can not use BCT tool
1206682624	Push from mpg_customer_enabling:[triage] Skylake U + Win 7 32bit: Platform does not enter 0 Watt / D3 cold
1604144709	CPU DT: Move the Default initialization from SiliconPkg to PlatformPkg & Isolate the Setup updates to separate library along with Null instance
NO_HSD	merge from KBP-H PO: new mPhy settings, recipe v4
1804267543	KBL BIOS does not allow RTD3 on PCI CR1/2/3[debug]
1604155086	Enable MicroChip eSPI Support on KBL

76.2 BP Client Common Core Sync-up Changes

None

76.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



77 BIOS – KBL CRB v038

BIOS version	0.038	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1041	
GOP Driver	9.0.1048	
1.5MB ME Firmware SKU	11.5.0.1038 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0008	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x8C R0/D0: 0x8C G0 : 0x26 H0 : 0x26 KBL S/H A0: 0x26	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.8.1
	MRC Version	0.8.1.5
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 374089 (2016_Kabylake)	



77.1 Resolved Client BIOS HSD sightings

HSDS#	Title
NO_HSD	[KBL FSP]Cache related machine checks should be cleared after NEM.
1207531285	Move create and initialization of BIOSGUARD_HOB from PeiCpuPolicyUpdate.c to Platform Init file
1207406011	[SKLSDS-KBLBIOS]: BIOS allows user to enter 20 characters into the password field but only accepts 9 characters[triage] [BLOCKING PV]
1404979865	FlashWearOutProtection is set to Disabled
1804280302	Enable Catalog Debug Feature
1304295822	Back out changelist portion of 347939 for [hsdes] <1304295822 since already fixed in core update and causes this behavior
NO_HSD	Update of SmiVariable:
1804280896	DCN: Change RSE BIOS workaround for Intel Stoney Beach (NGSA) NVMe SSD Crypto Erase issue.
1804280604	Wrong 'Local Fw Update Heci' message content
1604144709	CPU DT: Move the Default initialization from SiliconPkg to PlatformPkg & Isolate the Setup updates to separate library along with Null instance
1804280208	BIOS to set HDA EM1.LFLCS to 0 by default
1504232882	[kaby_lake.other]Duplicate _UID number issue an error in OS event log
1804280218	HDA: Update iDisplay Audio codec Device ID for KBL
1604105911	[Beta Req][Kaby Lake] [TH2] [ULX-ULT] During warm reboot cycling system hang observed in bios with 0E02 postcode[debug]
1504207203	Fix the build error after enable /wall in VS2015
1207525778	@ Some Type-A ports are in unusable state due to overcurrent being detected
1604144735	PCH DT: Move the Default initialization from SiliconPkg to PlatformPkg & Isolate the Setup updates to separate library along with Null instance
NO_HSD	Removing Bios WA to limit the memory frequency for KBL RVP3 to 1600MHz
1804276228	[PCH BIOS CI] Assert on Debug BIOS (in PeiSiFvi.c)
1404716594	Keyboard input does not work during BIOS HDD Password Pop-up causing system to become a brick and unable to boot or recover.
1404939570	Add support for ACM startup on Locality 3 [BtG]
1208123075	HSTI to capture the SMM_FEATURE_CONTROL SMM Code access enables.



1304422421	SKL BIOS: White-Box: BIOS PTT
1208021289	PTTHCI library should be removed from SKL/KBL RC]
1207762684	Use Cpuid.h and Msr .h files from UefiCpgPkg, and remove duplicated defines from CpuRegs.h
1404949834	SV BIOS doesn't install SGX (partial success of debug patch load)
1208142618	1: KBL FSP: expose Psys configuration policies to UPD
1804280302	Change the way BIOS identifies devices before sending data to AMT.
NO_HSD	KBL: Cleanup: CPU get number of threads: remove API GetEnabledCount() usage from platform and use MpService->GetNumberOfProcessors.
1504229699	Have a teamcity to build Fsp wrapper from FspBinPkg without FspPkg
NO_HSD	[Linux KBL] Detected error 'Mutux not acquired' when evaluating '_SB_.PCI0.LPCB.NVT6.UARA.* when doing ACPI DSDT Method Semantic tests failed with firmware test suite with v33 BIOS
1504086604	[skylake][Skylake] Incorrect RemapLimit register mask definition.
1208212249	Integrate 2 SKL patches, for R0/D0 0x8C
1604151805	KBL BIOS: Remove SLP_S0 with display ON feature from KBL BIOS
1604150285	"Start Boot Option Menu Control" Setup Option is always Grayed Out
1604152834	[KBL/SKL - Integrate latest GOP 9.0.1048 and VBIOS 1041]
1404716312	Request to create a PolicySetupUpdate Lib
1304431424	[skylake][SKL MRC: Add support for DDR4 DDP parts with shared clock and ZQ pins]
1304438393	[kaby_lake.other][KBL MRC: CalcOptPowerByte calculates Tx slew rate incorrectly]
1304429473	[kaby_lake.rvp9][KBL MRC: Add Command Margin training steps: Slew Rate and Drive Strength / Equalization]
1604118031	KBL-DT: Battery icon is always shown in OS on KBL-DT Board
1208180312	During capsule update MSFT variables are not restored
1208205661	Integrate 2 KBL patches, for G0/A0 0x26
1804276467	[KBL]Adding MEBx version 11.0.0.0008
1304313839	Platform hang in BIOS in s4/s5 when USB Device Tree is plugged to the rootport
1208082432	LPC/eSPI PCI offset 82h & PCR[DMI] + 2774h[15:0] registers value are different.
1504227037	Enable SIO NCT6776f serial debug in early phase.



1504226935	wrong bios id show up in platform information menu
1304433592	[kaby_lake.other][Implement RefPi=7 for QCLK 1600]
1404801189	[kaby_lake.rvp3]BIOS fails to see Solid State Drive intermittently
1604133654	LPIT table ResidencyCounterFrequency update

77.2 BP Client Common Core Sync-up Changes

None

77.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



78 BIOS – KBL CRB v037

BIOS version	0.037	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1040	
GOP Driver	9.0.1047	
1.5MB ME Firmware SKU	11.5.0.1038 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x8A R0/D0: 0x8A G0 : 0x22 H0 : 0x26 KBL S/H A0: 0x22	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.8.1
	MRC Version	0.8.1.1
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 371301 (2016_Kabylake)	



78.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO_HSD	Changes to Update DMI training flow as per latest Documentation
1804272997	[KBL] Shorten strings for RST remapping menu in BIOS setup
1304433592	[kaby_lake.other][Implement RefPi=7 for QCLK 1600]
1604127908	huge delay has been observed while sending two consecutive TBT mailbox commands
1604149204	KBL Security: Force Secure Erase is not getting auto disabled after manual restart [debug]
1604147456	[KBL J0 PO] : KBL RVP5 board not booting with debug image
1804251895	KBL Adapt SLP_S0 with display ON solution for platforms with non-premium PMICs/discrete VRs
1208112143	RVP8 boot without Gfx console once will boot system always without gfx[triage]
1304429473	[kaby_lake.rvp9][KBL MRC: Add Command Margin training steps: Slew Rate and Drive Strength / Equalization]
NO_HSD	Update for more readable debug message in GetConfigBlock function
1604149505	Enable CLK Request Support for KBL S Board
1504216785	Clean up the duplicate FIT definitions in PlatSamplePkg
1604147680	[KBL FSP BIOS: AMD/NVIDIA SG Card fan and LED is always on even after installing SG DRIVER[debug]]
1207871205	Leverage SecCore from UefiCpuPkg.
1604133654	CPU PeP Constraint applied based on Number of threads instead of number of cores
1504169354	[KBL]V27 and V28 KBL system's BIOS setting "CSM control" default was "Always Off" which different with F3 default was "Detect Legacy VGA".
1207123081	[SKL PPV][triage] SKL-BIOS-RVP11: Display message [Power surge on the USB port] after resumed from S4
1504185956	[Linux KBL] wmi: GUID 86CCFD48-205E-4A77-9C48-2021CBEDE341 has multiple associated methods WMTF defined
NO_HSD	Fix Embedded build failure introduce by CL#368092
1804267414	[KBL] Cannot set HDD Password [debug]
1208174007	Integrate KBL patch for H0 0x26
1604132245	[KBL][ULX][WSDS][PnP]: Observing 15 mins delay while booting into OS with V31.1 IFWI.[debug]



1604133868	KBL-Perf[RVP-3]: Sysmark test score are not meeting PV target on ULX with Win10 TH2 OS
1804269000	Change defaults for Flash lock policies
1604143872	During POST if system BIOS pass NULL of UPD region pointer to FspMemoryInit & FspSiliconInit then System will hang
1604143845	Using FSP Release binary with Debug Fsp Wrapper causes Hang in KBL
1504216690	[KBL PCH] Prevent the duplicate notify events in FSP wrapper mode
NO_HSD	Reflection of ZephyrID in Platformconfig xml
1207978058	[KBL FSP]Incorrect FSP Resource Owner Hob data on S3 resume.
1207653920	[Responsiveness] Resume time increase from 171ms to 180ms after CL336918(KBL25.1)

78.2 BP Client Common Core Sync-up Changes

None

78.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



79 BIOS – KBL CRB v036

BIOS version	0.036	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1040	
GOP Driver	9.0.1047	
1.5MB ME Firmware SKU	11.5.0.1038 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x8A R0/D0: 0x8A G0 : 0x22 H0 : 0x22 KBL S/H A0: 0x22	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.8.0
	MRC Version	0.8.0.4
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 368438 (2016_Kabylake)	



79.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804270621	Uploading latest RST PreOS version: 15.1.0.2562
1504216026	client RC should move EndOfDxe dependency to PciEnumerationDone for FSP security consideration - fixing FSP_GCC build#4383 failure.
1604142999	KBL FSP: S3 resume hangs at postcode b87f on RVP 8 boards with FSP GCC wrapper image
1604116217	[KBL FSP] Enable MTRR Programming from FSP wrapper
1208155604	Enable virtual touch keyboard if booting in tablet mode on SDS
NO_HSD	[SKLSDS-KBLBIOS] Update #2 to 350498: Add mechanism to have secure boot enabled build from TeamCity to be picked up for MSFT builds. Enable SDS stream overrides to be merged to KBL
1804269303	Change the Nvme Identify Command to unblock Secure Erase flow for remapped drives and RAID volumes
1804269345	non-native support for hotplug on KBL-H PCIe ports is missing
1504207204	Fix some Silicon modules/Libraries are not included on Silicon dsc files
1604084798	Handle both enable/disable case of CSM properly in KabylakeSiliconPkg
1207762684	Use CpuId.h and Msr .h files from UefiCpgPkg, and remove duplicated defines from CpuRegs.h
1208105403	KBL: ACPI: fix compiler warnings and remarks, Part 1
1504216026	client RC should move EndOfDxe dependency to PciEnumerationDone for FSP security consideration.
1504220495	Make Kbylake source code 100% align with BP1330 RC2
NO_HSD	UART DEV ID CSPEC MISMATCH
1604136266	Serial port not detected in devicemanager in win10
1804229434	[OPAL] Not possible to skip password prompt by hitting Esc during platform boot
1404880157	System hangs during Capsule update
1404256869	Remove IntelFrameworkPkg and IntelFrameworkModulePkg from Royal Park effective BP 1.4
1304417543	KBL: Debug Bios asserts when changing and saving Bios ICC menu [debug]
1804267623	[PCH BIOS CI] USB keyboard does not work under BIOS Setup and EFI Shell
1304420028	[KBL MRC: Swap the order of TAT/RTL steps and 2D steps]



1207873737	Kabylake code base fails to build with VS2012
1604138645	Request to add Type C AIC enable and disable option in BIOS setup menu
1208096765	cAVS: Addition of new Audio FW IPs (for audio DSP pre-processing and post-processing) for Intel Smart Sound Technology ISVs
1604105711	Create SMBIOS Type 9 Table as per SMBIOS 3.0.0 Specification (M2 support)
1208015621	Utilize PackageDocumentTools to generate ClientCommonPkg documentation with generic solution
1208120478	Integrate 2 SKL patches, for R0/D0 0x8A
1304163615	KeyboardLock boot option is not working, during SOL session.
1504198634	[KBL][Adding UINT8 Revision field in all setup variable.]
1604127817	[KBL-H] [HLK]: -USB Exposed Port System Test fails on RVP11 halo with multiple USB ports mapping.
1504176237	[Linux KBL] 45 out of 1591 ACPI DSDT Method Semantic tests failed with firmware test suite
1207907806	[BIOS] PCI ROM Priority under PCI Subsystem Settings in BIOS Setup doesn't work as expected with CSM always On
NO_HSD	[KBL-H] CM236 is not recognised as premium SKU on KBL bios V34
1604139575	Uploading new version of RST PreOS binaries with support for KBL-S RPID.

79.2 BP Client Common Core Sync-up Changes

None

79.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



80 BIOS – KBL CRB v035

BIOS version	0.035	
BP common core revision	1.3.3.0	
RoyalPark core version	1.3.3.0	
Video Option ROM (VBIOS)	1040	
GOP Driver	9.0.1047	
1.5MB ME Firmware SKU	11.5.0.1038 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x88 R0/D0: 0x88 G0 : 0x22 H0 : 0x22 KBL S/H A0: 0x22	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.8.0
	MRC Version	0.8.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.2
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 365591 (2016_Kabylake)	



80.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804262578	EOP not detected after entering Setup.
NO_HSD	KBL Security: PCR 7 Configuration showing as "Binding not possible" when Secure boot is enabled[debug]
1208027516	[KBL]Checkpoint 0x36 hang during reboot test in SmmProfile.c CheckProcessorFeature.
1404220114	cAVS DMIC pull down enable
1504214563	BP 1330 sync up
1804265460	Assert on Debug BIOS
1207871205	Leverage SecCore from UefiCpuPkg.
1207978058	[KBL FSP]Incorrect FSP Resource Owner Hob data on S3 resume.
1404906232	Optimum BIOS setting for cAVS SRAM retention energy break even
1604137799	[KBL][VTIO]SDEV table should not be exposed if Vtd is disabled in BIOS setup
1207529223	BIOS settings not visible through EPCS Tool (automation)
1604137711	[KBL/SKL - Integrate latest GOP 9.0.1047 and VBIOS 1040]
1404869605	KBL SGX random OWNER_EPOCH option locks system[debug]
1804263487	[KBL-PCH-H] Add Kabylake PCH-H LPC DIDs
1604122753	[skylake.rvp11][SKL_RS1][BKC-14279] :- Package C10 achieved < 98% on Halo, pointing to eMMC and SDC unregistered in PEP in Sleep Study.
1604124582	@ S3 Resume fails with CatError on SKL RVP3 Boards.[Debug]
1604133654	CPU PeP Constraint fix: related to HSD 1604133654
1404670330	Consolidate the number of calling APIs in SGX lib
1207762684	Use CpuId.h and Msr .h files from UefiCpgPkg, and remove duplicated defines from CpuRegs.h
1207538018	2nd Patch load is happening in blocking mode.
1208002800	Integrate BIOS ACM Rev 0.7.2
1304389325	Need to remove HSW redundant from KBL BIOS
1804261712	[KBL RVP] Can not disable UART in BIOS, option unavailable
1804263396	[KBL]Integrate CRB CSME FW 11.5.0.1038 into BIOS



1604125913	[KBL BIOS[debug]: Unable to open AMD SG Card Graphics properties with AMD SG card connected.]
1304380866	TBT BIOS:Part 1 of KBL BIOS should be aligned with latest TBT BIOS guide
1207820658	PTT ACPI structure is not aligned between ASL and C code in External BIOS
1207406011	[SKLSDS-KBLBIOS]: BIOS allows user to enter 20 characters into the password field but only accepts 9 characters[triage]
1404872666	KBL BIOS: Merge CL#2799494 to disable HWP under Win8 to KBL source

80.2 BP Client Common Core Sync-up Changes

None

80.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



81 BIOS – KBL CRB v034

BIOS version	0.034	
BP common core revision	1.3.2.0	
RoyalPark core version	1.3.2.0	
Video Option ROM (VBIOS)	1039	
GOP Driver	9.0.1046	
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x88 R0/D0: 0x88 G0 : 0x22 H0 : 0x22 KBL S/H A0: 0x22	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.7.3
	MRC Version	0.7.3.2
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.0
	ACM (Boot Guard)	2.0.3554
P4 Label	@ 363264 (2016_Kabylake)	



81.1 Resolved Client BIOS HSD sightings

HSD#	Title
1208027451	Integrate 3 KBL patches, for G0/H0/A0 0x22
1804227838	KBL Allow SLP_S0 with display ON
1504206407	[kaby_lake.other]EDRAM support on KBL J0 stepping
1504201047	Sync IOTG embedded platform Saddlebrook code changes from Skylake to kabylake
1604062360	No password: VTIO: CSME to VTL1 Symmetric Key Distribution - BIOS to read the key from CSME and expose it as UEFI variable
1207707638	Remove _DSM from SGX EPC device
1207164619	[skylake.rvp7]MRC MEMORY_CONFIG_NO_CRC.CleanMemory is not honored on warm reset - Part 2
1404897610	[KBL-PCH-LP] Add New Kabylake PCH-LP LPC DIDs
1207578345	[Responsiveness]IFWI 11.5.0.1016, the HeciGetFwCapsSkuMsg() cant be removed for Perf build.
1207834356	Incorporate new platform code for Coyote Mtn to Kabylake stream
1404889115	[KBL] Machine hangs at post code 0004 in SecCarInit on resme S3 because 'invd' instruction causes machine check in midlevel cache unit
1604062379	No password: VTIO support from ME BIOS.
1804232838	Memory Init Status always set to 0 = SUCCESS for DID message
1504188709	After restoring s3 boot script, BIOS should not use 64-bit MMIO address at EndOfPei phase.
1207852392	DCN for BIOS RSE Ref and Platform code changes/clean-up
1804237977	RSE doesn't work using RAID Mode
1207889683	DCN request to add limit enforcement on inputting invalid drive password during Remote Secure Erase (RSE) flow.
1604075319	KBL-Bios: Platform power and AC-brick power values are shown as '0' in TAT tool on KBL-RVP3 and KBL-DT boards.
1207517451	[KBL-SDS] Remove "PCH-IO Config->PCH-IO DeepSx Power Policies" configuration option in BIOS
1604129521	KBL BIOS: SLP-S0 is not asserting in KBL Halo Boards.
1304399677	[kaby_lake.rvp3][KBL MRC: Add support for CNL X0 RVP5 with board ID = 0xE]



1504175343	[external version of RC 0.71 SA RC DxeLegacyRegionLib should be NULL class and remove LegacyRegionInstall() API]
1504198634	[KBL][Adding UINT8 Revision field in all setup variable.]
1208003064	RVP8 failed to detect Legacy external Graphics card when "Firmware Configuration" is set to "Production".
1604134383	Integrate Boot Guard ACM 2.0.3554 QS
1404670330	Consolidate the number of calling APIs in SGX lib
1207666558	[SKL-SDS-KBL Bios] Align SDS IVCAM with the new platform design part2
1604133849	KBL Security: Unable to set the PRMRR size through EFI variable request[debug]
1207911791	[SKL-COENG] [SKLSDS-KBLBIOS]: Cleanup PcdResetSarSensorEnable to be only when WWAN is enabled on SDS
1504182943	[kaby_lake.rvp3]Generate SA GlobalNvs asl code and header file from GenNvs tool.
1207774101	KBL: Update ACPI LPIT to use SLP_S0# residency counter with BIOS switch option to use Package C10 residency counter
1304395557	[kaby_lake.other][KBL MRC: Full grid DIMM ODT in 1DPC should be enabled for margin training, not for power training]
1304383315	[FlexCon] Test Menu knobs are not being generated correctly
1404785322	[KBL]Part 2: Remove unused files from Ia32FamilyCpuPkg Override. Cleanup SmmFeaturesLib removing commented code. Use PiSmmCommunication from UefiCpuPkg.
1304291551	KBL: HWPS maximum performance should be set to 0xFF when enabling the overclocking menu
1604129619	KBL_Security: FSP BIOS Guard(BGUP) images are not available in Artifactory

81.2 BP Client Common Core Sync-up Changes

None

81.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



82 BIOS – KBL CRB v033.1

BIOS version	0.033.1	
BP common core revision	1.3.2.0	
RoyalPark core version	1.3.2.0	
Video Option ROM (VBIOS)	1039	
GOP Driver	9.0.1046	
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x88 R0/D0: 0x88 G0 : 0x1E H0 : 0x1E KBL S/H A0: 0x1E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.7.3
	MRC Version	0.7.3.0
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.0
	ACM (Boot Guard)	3460
P4 Label	@ 362290 (on dot build stream KBL_G0_PO)	



82.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604129521	KBL BIOS: SLP-S0 is not asserting in KBL Halo Boards.

82.2 BP Client Common Core Sync-up Changes

None

82.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



83 BIOS – KBL CRB v033

BIOS version	0.033	
BP common core revision	1.3.2.0	
RoyalPark core version	1.3.2.0	
Video Option ROM (VBIOS)	1039	
GOP Driver	9.0.1046	
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x88 R0/D0: 0x88 G0 : 0x1E H0 : 0x1E KBL S/H A0: 0x1E	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.7.2
	MRC Version	0.7.2.5
	BIOS Guard(PFAT)	2.0.3561
	ACM (TXT)	Version 0.7.0
	ACM (Boot Guard)	3460
P4 Label	@ 360341 (2016_Kabylake)	



83.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207642553	Implement Use Case #1 for Fast Boot behavior change (Home Button)
1604123927	Sync IntelFspPkg and IntelFspWrapperPkg from _Dev stream - Part 2
1304315142	TBT BIOS: Wrong Sx Entry/Exit handling
1604027529	HiiExport variable to made more secure - Added Missing Restricted Label
1207899452	Remove obsolete SV policy SkipPmrr
1207836145	If UPD SkipMpInit is enabled, skip CpuMpPei starting APs.
1207940394	Integrate 3 KBL patches, for G0/H0/A0 0x1E
1207762684	Use Cpuid.h and Msr .h files from UefiCpgPkg, and remove duplicated defines from CpuRegs.h
1207634688	[KBL] Adding WiGig F1 PEP constraint
1604130650	KBL FSP BIOS : NO Display in BIOS setup with edp panel when CSM control is on[Debug]
1304391808	[skylake][SKL MRC: MrcSetupVtt uses hard-coded value for CMD Target]

83.2 BP Client Common Core Sync-up Changes

None

83.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



84 BIOS – KBL CRB v032

BIOS version	0.032	
BP common core revision	1.3.2.0	
RoyalPark core version	1.3.2.0	
Video Option ROM (VBIOS)	1039	
GOP Driver	9.0.1046	
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x88 R0/D0: 0x88 G0 : 0x1C H0 : 0x1C KBL S/H A0: 0x1C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.7.2
	MRC Version	0.7.2.0
	BIOS Guard(PFAT)	1.1.0 (2.0.3561)
	ACM (TXT)	Version 0.7.0
	ACM (Boot Guard)	3460
P4 Label	@ 358665 (2016_Kabylake)	



84.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504192520	FSP GCC CI#1629 build boot failed with PC 0000 and pop CATTER error. - Partial Fix
1804187640	RST RAID UEFI driver must be available when SATA controller is in AHCI mode to allow RST UEFI handling StonyBeach disks.
1304389950	[kaby_lake.rvp3][KBL MRC: StubMrc fixes / improvements]
1404229602	System shutdown observed ~1min after S3 exit when warm reset overclocking is enable
1207921808	Integrate 2 SKL patches, for R0/D0 0x88
1207762684	Use Cpuid.h & Msr .h files from UefiCpgPkg, remove duplicated defines from CpuRegs.h
1404745292	Sensor orientation information is required in BIOS for cameras (RGB & RealSense) in KBL
1304380843	[FlexCon] SharedMailbox base is being posted before PC.xml is ready
1504192530	[KBL]FSP VS EXT build got boot failed with PC 007F
1207687127	ACPI interrupt storm (interrupts at 2ms interval) due to GPE 0x6F causing ~24% CPU utilization causing regression in Power and Performance during screen-on
1207911220	Update MeFwUpdate API Library to 11.5 Beta
1404803612	KBL OC: BIOS support for BCLK Aware V/F curve
1504174283	Warning 3104 - Reserved method should not return a value
1207900674	Fix TXT can return supported even when SMX or VMX is not supported
1207907540	KBL: DPTF: Enable interrupts by default for KBL
1207902281	KBL DPTF Add set up options for Display Depth Upper and Lower Limits
1604129538	[kaby_lake.other][KBL/SKL - Integrate latest GOP 9.0.1046 and VBIOS 1039]
1304328660	TBT BIOS: BIOS assigns overlapped resources to TBT root port, and SMBus Controller, YB on LAN controller
1804257119	Warning message during boot platform to EFI shell with ME State disabled
1604098314	Security SPCUnit - Random IA writes to a Power on FSM control register causes an Invalid Arc
1504163015	[Prevent to use Uefi as file/protocol/ppi name in SA RC]
1304137932	TBT BIOS: AR PCIE Switch Flow Control issue workaround
1604121558	Unable to connect with External display using WIGIG Communication on KBL ULX board (RVP13)



1604128415	[Lot of ASL warning messages on KBL Project- Fix SA ASL Warnings]
1207837181	[KBL FSP]Restore S3 resume MTRRs before giving control to OS.
1207673708	Deprecate the usage of S3 reset mechanism for capsule update
1207901445	KBL: DPTF: add DCFG object, remove SuperDebug object.
1207864828	[kaby_lake.rvp3]Un-restrict the DPTF threshold conversion from 0 -> 0xFFFFFFFF
1304356962	TBT BIOS: Boot from TBT: unable to use external device/platform hang
1604123927	Sync IntelFspPkg and IntelFspWrapperPkg from _Dev stream
1304309194	External GPU support over Thunderbolt connection
1404785322	[KBL]Part 1: Remove unused files from Ia32FamilyCpuPkg Override.
1207834426	[skylake][MRC] MRC shall ensure DDR4 Self Refresh is set to ASR Mode
1804256437	Set KBL PDM interface clock default rate to 2.4Mhz with dc offset compensation enabled
1404832388	[UsbRmrrUpdateCallback and RegisterUsbSaCallbacks should be moved to internal only]
1504175057	Change PlatformPcdInit to a Pei library and call it from PlatformInit post mem phase
1207853541	[PPV]Since BIOS29, it failed to launch apps inside Startup.nsh
1207647011	[SKLSDS-KBLBIOS] : When BIOS Guard is on, Capsule update is not successful
1804238940	Cleanup of PCH PCIe support in BIOS
1304315142	TBT BIOS: Wrong Sx Entry/Exit handling
1604117846	[kaby_lake.rvp3]Remove the "Include" path from #include <Include/Private...
1206744707	[KBL FSP] Video output on FSP stopped working after V82_160[debug]
1604062359	[POC] No password: VTIO: Disable Controller sideband access
1504184806	asl compile WarningId 3115 - Not all control paths return a value in (PSRC)

84.2 BP Client Common Core Sync-up Changes

None

84.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



85 BIOS – KBL CRB v031

BIOS version	0.031	
BP common core revision	1.3.2.0	
RoyalPark core version	1.3.2.0	
Video Option ROM (VBIOS)	1037	
GOP Driver	9.0.1044	
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x86 R0/D0: 0x86 G0 : 0x1C H0 : 0x1C KBL S/H A0: 0x1C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.7.1
	MRC Version	0.7.1.2
	BIOS Guard(PFAT)	1.1.0 (2.0.3561)
	ACM (TXT)	Version 0.7.0
	ACM (Boot Guard)	3460
P4 Label	@ 354708 (2016_Kabylake)	



85.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504185245	[kaby_lake.other][KBL]V31 KBL RVP11 system can't boot into Legacy HDD or USB , system will reset or hang up at 00AE.
1504185031	[kaby_lake.rvp7][KBL][debug]V31_FSP and Debug Build get assert and post code dd00. Fixing SV build failure.
NO_HSD	Merging from CL#354624 in CNL (a correction for Simics)
1804215242	Enable PMIC VM at boot if audio is disabled
1207170544	Lot of ASL warning messages on KBL Project
1207151886	[KBL] [SGX] KBL SGX status report variable is needed for ISVs
1404841019	Update BIOS Guard BGUP signing tools to current QS version
1207733839	Fix Doxygen warning messages for CPU RC
NO_HSD	Add new ID Family support for PLATFORM NAME string iin PlatformConfig XML file
1604120176	KBL Exploratory : Voice Activity Detection option is hidden when unchecking the DSP based Speech option in BIOS[debug]
1604117582	external version of RC 0.7 gEfiGraphicsInfoHobGuid is not installed in Fsp Wrapper by default
1207661849	Add BIOS reporting of PCIe SSD in ME Management Media Table and also update the ME BWG Media Table documentation to include PCIe Interface Type.
1504173974	SPTLP eMMC to re-run HS400 DLL tuning flow whenever a different driver strength is selected
1504106920	[KBL][Remove BoardId from PlatformPkg - phase2]
1604122881	[KBL] KBL CPU Family Class to be added for PiSmmCpuDxeSmm module.
1604117846	Remove the "Include" path from #include <Include/Private...
1504165735	Several cleanups in RoyalPark -- Phase2
1804254442	[PCH BIOS CI] "Detect Legacy VGA" option works as "Always On" even without external GFX connected
1404704745	KBL-PO-SV: With PO BIOS 21 SVBios Cafe/Satellite/PPV content hangs
1804238940	Cleanup of PCH PCIe support in BIOS
1604103228	[FSP: FSP shouldn't take decision to initial Gfx when CB pass VBT pointer]
1504174540	external version of RC 0.71, silicon package SystemAgent should NOT include DataHub protocol



1604000661	[SKL-COENG][SKLSDS-KBLBIOS] PVT: BIOS allows user to disable internal graphics which freezes system and requires a CMOS clear to recover back
1504158088	[SiPolicy] builds a HOB to preserve the Policy data which are need for both Pei and Dxe
1504138083	BP 1320 sync up, remove unnecessary override of PCD.
1604097857	[KBL FSP] gWdtPpiGuid available for FSP , remove the instance under FSP_WRAPPER_FLAG
1804233881	Platform code doesn't check for PCIe rootport function swap on rootports above 8
1207459743	Update CPU RC policy documentation
1207852418	BIOS cannot detect some of old PEG Video cards when "Detect Legacy VGA" is selected as CSM control.
1804252538	Wrong detection of valid PCIe dev/func numbers on KBL
1304319043	TBT BIOS: Boot from TBT/USB On boot: TBT devices are not visible in BIOS.
1304371702	[kaby_lake.rvp5]KBL-PO-H0 RVP15 and rvp5 are booting to 1600 instead 2133 fused with QKUF
1504173969	SPTLP eMMC HS400 DLL tuning to use 40-ohm driver strength by default
1504178449	[KBL]Prevent to use any private file/protocol/ppi from SiliconPkg in PlatformSamplePkg
1504157262	Prevent to use Uefi as file/protocol/ppi name in PCH RC
1504164163	Create public library of PCH WDT PPI and install WdtPpi in FSP and FSP wrapper
1604119648	LP3 DDP memory support needed for RVP16
1604119231	KBL BIOS [debug] : Delay observed in reflecting the battery status in OS
1504087621	[KBL FSP] Switch to NASM in Fsp building
1207809003	[basin_falls.rvp]Basin Falls need support for DDR4 2666MHz
1207849927	Integrate 2 SKL patches, for R0/D0 0x86

85.2 BP Client Common Core Sync-up Changes

None

85.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



86 BIOS – KBL CRB v030

BIOS version	0.030	
BP common core revision	1.3.2.0	
RoyalPark core version	1.3.2.0	
Video Option ROM (VBIOS)	1037	
GOP Driver	9.0.1044	
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)	
5MB ME Firmware SKU	N.A	
RST RAID OROM	15.0 Pre-Alpha (revision 2371)	
MEBx	11.0.0.0007	
PXE OROM	1.3.21	
Microcode Update –	M0: 0x84 R0/D0: 0x84 G0 : 0x1C H0 : 0x1C KBL S/H A0: 0x1C	
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31	
Reference code version	Reference Code	Version
	RC Version	0.7.1
	MRC Version	0.7.1.0
	BIOS Guard(PFAT)	1.1.0 (2.0.3561)
	ACM (TXT)	Version 0.7.0
	ACM (Boot Guard)	3460
P4 Label	@ 351942 (2016_Kabylake)	



86.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504177086	[KBL]V30 Debug get assert and post code 0096 with RVP11.
1207814027	Update MeFwUpdate API Library to 11.5
1206853323	No Karkom ULT/ULX production image
1504177000	[KBL]V30_Debug gets assert and pose cost 0C09 with RVP8.
1504165735	Several cleans up in RoyalPark
1604082798	[Need BIOS OPTION to DISABLE IOMMU DEVICE ENUMERATION] - Fixing the issue by skipping DMAR so OS does not take control of IOMMU device.
1604117537	[kaby_lake.rvp3][KBL] Potential issue in CPU code which executed DEBUG MACRO on all APs in parallel.
1404698798	BIOS to add new logic for VR topology
1504175100	[CoveCreek] Grouping folders by features
1504168319	[ME] Add PostCodes to indicate 'exit' for previous 'entry' PostCodes.
1604120229	[VBT Settings needed for KBL S RVPs, which include Board ID 0x66, 0x67 and 0x69.]
1207703709	iTouch: KBL Virtual Keyboard is not functional on KBL RVP3 and RVP7 platforms.
1504158087	[kaby_lake.rvp3][PCH] builds a HOB to preserve the Policy data which are need for both Pei and Dxe.
1404784021	[cannon_lake.vp]Setting PcdIgdEnable to FALSE causes ACPI error with Windows boot failure.
1804221562	[PCH BIOS CI] Can't perform S5 after resume from S3
1604120429	KBL S EV CRB PO support
1206639116	[KBL]Load microcode update for BSP even if microcode not loaded by FIT.
NO_HSD	[SKLSDS-KBLBIOS] Add mechanism to have secure boot enabled build from TeamCity to be picked up for MSFT builds. Enable SDS stream overrides to be merged to KBL
1207814503	Integrate 3 KBL patches, for G0/H0/A0 0x1C
1207808994	[SKL SDS] IVCAM RTD3 doesn't work on SKL SDS with KBL BIOS.
1304357040	KBL: Can't save BIOS setting (F4) with message "Submit Fail for Form: ACPI Settings."
1207761865	Increase MICROCODE_FV size to make room for patches for future KBL steppings
NO_HSD	Fix [Beta Req] [KBL-U] [HLK]: WHLK:- TPM 2.0 UEFI Preboot Interface Test fails with "PCRExtendPerf Test "



1804247931	Some fixes for Exiting SV module to FlexCon code
1604116727	KBL-DT: Board ID is shown as 'TBD' in BIOS setup on KBL-S board.
1804237236	[PCH BIOS CI] Ctrl+P MEBx prompt is not seen during platform boot.
1804242664	Adding MEBx version 11.0.0.0007
1207170544	Lot of ASL warning messages on KBL Project
1604075664	[Type-C KBL-Y RVP3] Type-C DP works in only X4 mode using Type-C NXP Dock
NO_HSD	Request to put HW default values instead of zero for PSI cutoff in BIOS Setup
1207808893	Integrate 2 SKL patches, for R0/D0 0x84
1404751826	[SVCPU] Latest SVBIOS 26 does not boot to SV module - Stuck at 0x00D0
1604100621	Add support for SG/HG for KBL-Y
1804233936	BusNumberTranslator data produced by ACE.exe for desktop platform doesn't have rootports 21-24
1604114577	[kaby_lake.rvp3] Add support for new touch controller - WACOM 9015
1207496657	[SKLSDS-KBLBIOS] : Cannot disable COM0 option after enabling it, rollback #346847
1804238136	[KBL-PCH-LP] Add Kabylake PCH-LP LPC DIDs
1207695058	BIOS ACM Rev 0.7.0; Replaced ACM non-production-worthy (NPW) binary with production-worthy (PW) binary.
1804238940	Cleanup of PCH PCIe support in BIOS
1304362156	[kaby_lake.rvp3][KBL MRC: Need to program RefPi = 7 only on KBL CPUs]
1804236339	[PCH BIOS CI] Yellow Bang on PS2 mouse
1504164335	RC 0.7 build fail with VS2015 compiler

86.2 BP Client Common Core Sync-up Changes

None

86.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



87 BIOS – KBL CRB v029

BIOS version	0.029		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1044		
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x82 R0/D0: 0x82 G0 : 0x1A KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		0.7.0
	MRC Version		0.7.0.9
	BIOS Guard(PFAT)		1.1.0 (2.0.3561)
	ACM (TXT)		Version 0.7.0
	ACM (Boot Guard)		3460
P4 Label	@ 348225 (2016_Kabylake)		



87.1 Resolved Client BIOS HSD sightings

HSD#	Title
1304225534	KBL: [debug]After Disable PTT Ship state by FPT, Bios indicate PTT is enabled.
1503941557	SPTLP eMMC HS400 Strobe DLL tuning to use worst case pattern
1504167586	external version of RC 0.7 will hang if set PcdS3Enable FALSE
1504106920	[KBL][Remove BoardId from PlatformPkg - phase2]
1504168240	[KBL]V28_53_RVP15 system get assert with V28_53_RVP7_IFWI.]
1604003568	[SKL PPV] [Platform-CI-WW32.3] SKL_BKC: USB wake from S3 & S4 is not happening through keyboard/mouse connected to USB walk-up port 2 on RVP3
1304354036	Include Production signed Bios Guard binary 2.0.3561 in KBL Bios
1804236675	[KBL] Wrong I2S blob for ALC286S codec
1804232899	[kaby_lake.rvp7]Platform hangs at multiple post codes (0A64, 004F, 0E02) during warm reset cycles - fix FSP wrapper Build error
1604082673	[[SG/HG][KBL] BSOD/DGPU card not detected in OS after power events]
1207172263	BIOS does not have the right constraints thus preventing connected standby
1604065544	Clean remain BID & BBID
1207496657	[SKLSDS-KBLBIOS] : Cannot disable COM0 option after enabling it
1207659920	Implement Real battery dynamic detection for SKL SDS base system.
1804234097	Device side MPS programmed too early may get reset in SWEQ flow causing detection failure
1207706787	[ME11] MEI driver got yellow bang and not disappear in Device manager when press hot key to pull up HDA_SDO.

87.2 BP Client Common Core Sync-up Changes

None

87.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



88 BIOS – KBL CRB v028.1

BIOS version	0.028.1		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1044		
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x80 R0/D0: 0x82 G0 : 0x1A KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		0.7.0
	MRC Version		0.7.0.9
	BIOS Guard(PFAT)		1.1.0 (2.0.20150625)
	ACM (TXT)		Version 0.7.0
	ACM (Boot Guard)		3460
P4 Label	@ 346971 (2016_Kabylake_PO)		



88.1 Resolved Client BIOS HSD sightings

HSD#	Title
1804232899	[kaby_lake.rvp7]Platform hangs at multiple post codes (0A64, 004F, 0E02) during warm reset cycles - fix FSP wrapper Build error

88.2 BP Client Common Core Sync-up Changes

None

88.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



89 BIOS – KBL CRB v028

BIOS version	0.028		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1044		
1.5MB ME Firmware SKU	11.5.0.1030 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x80 R0/D0: 0x82 G0 : 0x1A KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		0.7.0
	MRC Version		0.7.0.9
	BIOS Guard(PFAT)		1.1.0 (2.0.20150625)
	ACM (TXT)		Version 0.7.0
	ACM (Boot Guard)		3460
P4 Label	@ 340578 (2016_Kabylake)		



89.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207529100	Dos Stress test hang on 0x92 when AP Manners set to MWAIT
NO_HSD	Back out changelist 337385 for 0E02 issue
1207733326	Integrate 2 SKL patches, for R0/D0 0x82
1207733265	Integrate KBL G0 patch 0x1A
1207723277	[kaby_lake.rvp3]PRMRR Memory Region is not being configured as WRITE_BACK
1207666558	[SKL-SDS-KBL Bios] Align SDS IVCAM with the new platform design
1304311684	[FlexCon] Need to add checksum on the BiosKnobs.xml
NO_HSD	Back out changelist 345059 because the chnaged cuases GCC wrapper boot fail!!
1304355239	[skylake.customer_platform][SKL MRC: W/A for MC may lose RCH completion credits while it enables clock gating]
1304311679	[FlexCon] Fix Knobs that are updated only at SvBootPcd path
1304319134	[OC] BIOS doesn't program Ring related options in Overclocking menu
1207679114	[kaby_lake.rvp3]KBL26's NR build, no screen output when boot into OS.
1207679114	[kaby_lake.rvp3]KBL26's NR build, no screen output when boot into OS.
1804234692	[KBL]Integrate CRB CSME FW 11.5.0.1030 into BIOS
1504106920	[[KBL][Remove BoardId from PlatformPkg - phase2]
1304317190	TBT BIOS: BIOS assigns wrong amount of resources to devices with SSID == 0x11112222
1207406209	The "Wake up System from S5" setting does not have a provision to enter the 'day' it should wake up as indicated by help text
1604111144	[[KBL] Support New Kabylake CPU Family ID Changes in SA code]
1207674788	[KBL FSP]Skip Mp Initialization is not completely skipping all feature initialization across threads
1604108471	[KBL [ULX] SX: BSOD 9F Observed with ACPI.sys during S3 cycling with 0x9f_3_power_down_acpi_analysis_inconclusive!unknown_function error]
1207538018	[kaby_lake.other]2nd Patch load is happening in blocking mode.
1604082798	[Need BIOS OPTION to DISABLE IOMMU DEVICE ENUMERATION]
1604096527	[Need BIOS WA for KBL HW HSD 4712215]



1604108654	[KBL] New Kabylake Family ID Changes for CPU
1604020511	[KBL BIOS:[debug] GT2 override values are not enumerated properly in OS, according to the changed Bios settings.]
1205658837	Remove IA32FamilyCpuPkg Override files as this PKG is not supported
1304291494	SKL-S/SPT system will not stay in S5 after pressing the power button
1804225881	[CSME RCR] Control Intel? ME Global Reset on Critical Failure.
1604084798	[kaby_lake.rvp3]Handle both enable/disable case of CSM properly in KabylakeSiliconPkg
1207695058	Integrate BIOS ACM Rev 0.7.0
1304293282	Need to align ConFlex SharedMailbox to SV Spec
1304316190	[skylake.rvp11][SKL MRC: Initial RecvEn PI setting is not optimal for DDR4 1867 in some cases]
1304339329	[skylake.rvp11][SKL SMBIOS type17 table serial number incorrect]
1604034285	KBL: Unable to remote wakeup from S3(Sleep)/S4(Hibernate) with BT Keyboard/Mouse on ULT/ULX
1504137164	CoveCreek: Refactory ACPI" directory, and separate it as features
1604060717	[kaby_lake.rvp3]KBL FSP BIOS :[debug]PAVP override unsolicited attack mode registers mismatch is observed in OS and BIOS.
1207680022	Integrate 2 SKL patches, for R0/D0 0x80
1207666434	DPTF KBL : Add support for IVCAM participant
1804230740	Add a setup option that allows skipping Option Roms on NVMe drives to unblock RSE validation.
1604102812	AMD/NVIDIA SG Card fan and LED is always on even when dGPU is not in use

89.2 BP Client Common Core Sync-up Changes

None

89.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



90 BIOS – KBL CRB v027

BIOS version	0.027		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.1018 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x7E R0/D0: 0x7E G0 : 0x14 KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.7.0	
	MRC Version	0.7.0.5	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 340578 (2016_Kabylake)		



90.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207674713	[SKL PEG/DMI] Incorrect values were observed in some of DMI/PEG registers)
1207578072	[KBL Beta] VIR2 tripping passive at idle
1207666434	DPTF KBL : Add support for IVCAM participant
1604003209	[KBL] FSP BIOS: Package C3 and above states are not reaching with FSP image
1404316919	DCI Enable not working in latest BIOS KIT
1604105309	KBL FSP - Cleanup dead references to FspUpdVpd.h files
1404519112	WDT recovery flow does not revert all OC settings to default
1604002685	SKL BIOS : [debug]BET tool showing error for "Host clock frequency & Turbo extended time window" parameters.
1604056321	KBL 3D Imaging Module Restructuring phase 1 - DS4 camera rotation and restructuring
1604101044	[Beta Req]KBL_Sx: RVP7 [Corporate] SUT hang at PC 0036 while running reboot & hybrid S5 cycle[debug]
1604103978	[kaby_lake.rvp7]KBL BIOS: SUT hangs at postcode 0096 during PXE preload with "CSM ON"
1207659610	[kaby_lake.rvp3]Kabylake core is mis-aligned. Revert 340497
1604083966	Remove Dual FSP support from FSP & Wrapper - Recommitting after Rollback with CL341713
1604104612	[KBL/SKL - Integrate latest GOP 9.0.1044]
1304329247	[kaby_lake.rvp8][KBL OC: Choosing XMP profile as memory profile will set the memory speed at highest even ratio and not at the highest odd ratio]
1604105711	Create SMBIOS Type 9 Table as per SMBIOS 3.0.0 Specification
1207665377	SKL SDS Dock state is not propagated to OS with KBL v26 BIOS
1207585214	[KBL-PCH-H] Add support for a new KBL-H SKUs
1207116020	Display brightness controls need to be re-worked
1404720329	Include Zumba Beach and UP Server Flavor support in PlatformPkg folder
1604072747	[[KBL] - VBT settings to support RVP board default display configuration]
1604062837	[Beta Req]KBL Y RVP3 [WW50 Gold config] System is not entering SLP_S0 on KBL Y [new RVP3 board]
1207659863	Integrate 2 SKL patches, for R0/D0 0x7E



1207515080	[SKLSDS-KBLBIOS] PCH LAN Controller is erroneously marked "enable" after loading defaults(F3)[trriage]
NO_HSD	Support new Board ID 0x1A for PPV5 paltform
1404386466	BIOS needs to set NPK CTC_RESYNC bit)
1207520508	[SKL] System not coming out from Hibernate state

90.2 BP Client Common Core Sync-up Changes

None

90.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



91 BIOS – KBL CRB v026

BIOS version	0.026		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.1018 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x7C G0 : 0x16 KBL S/H A0: 0x16		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.7.0	
	MRC Version	0.7.0.3	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 340578 (2016_Kabylake)		



91.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO_HSD	Missing PLD and UPC methods for RVP3 in scope XDCI
1304043789	[kaby_lake.other]CSME: Boot to legacy USB devices isn't redirected via SOL terminal
1604086794	[KBL][debug]V23 and V24 KBL RVP7 system got debug ASSERT after enable overclock.
1207644442	[KBL Beta] display, fans, and memory have incorrect ACPI type code
1404735394	MSR MSR_IA32_HWP_INTERRUPT (0x773) BSP value is different than APs value after disabling HT by fuse
1207595026	Suppress debug post codes in ACPI code unless ACPI debug is enabled
1304306170	[SVCPU] MSR MSR_PMG_CST_CONFIG_CONTROL(0xe2) BSP value is different than APs value after disabling HT by fuse
1604100118	Rename FSP Structure varname to match version 2.0 draft 5
1604008286	SKL Security[triage]: Loading of CSM is not blocked when Secure boot is enabled
1504143443	Fix Platform Klocwork issues
1504005677	Enabling Performance measurement for FSP Binary
1604100817	[KBL-U/Y] [HLK] : Watchdog timer test failing with error "Unable to find event log entry indicating that watchdog triggered a system reset"
1604065544	[Fix migration mistake: blue screen (ACPI_BIOS_ERROR) can't boot to Windows on both RVP3 and SDS in CL#339513]
1404743322	[KBL] [BIOS Guard] Integrate SV BIOS Guard Module based on BIOS Guard Module 2.0.3517
1207577115	[title] Integrate 2 KBL patches, for G0/A0 0x16
1404520597	Bclk - Ctrl of multiple BCLK settings types in ICC UI
1804228027	Add Sound Research GUID for IntelSST config
1206933824	SA RC null library needs to be reviewed/cleaned up/ and validated.
1604065544	Remove Board ID usage from ASL Code
NO_HSD	[KBL][Fix migration mistake on Ivcam Common Gpio data structure in CL#335429]
1604060717	KBL FSP BIOS :[debug]PAVP override unsolicited attack mode registers mismatch is observed in OS and BIOS
1207627301	KBL: Add PPCC to Storage Participant
1207612001	Need trip points defined in BOS for PerC (Camera) participant



1207633815	[SMBIOS] Replace hardcoded values for memory type with MdePkg enums
1207164619	MRC MEMORY_CONFIG_NO_CRC.CleanMemory is not honored on warm reset
1207512249	Cleanup needed in KabylakePlatSamplePkg\Platform\PlatformSetup\Dxe\PlatformSetup.c
1504138083	Clean and sync up KabylakePlatSamplePkg\Override with BP1320 changes
1604038864	[KBL FSP]Merge from Skylake to enable Coreboot to Skip MP Initialization.
1504106920	[KBL][Remove BoardId from PlatformPkg - phase 2]
1504135675	[CPU] List the API we produce from core package and search which spec it refers
1504135710	[SA] List the API we produce from core package and search which spec it refers
1604092389	BoardId is not init properly whe BootMode != BOOT_WITH_FULL_CONFIGURATION
1206639116	[KBL]Load microcode updates on APs if not loaded by FIT.
1207598254	[SKLSDS-KBLBIOS] : 3 Battery Icons displayed on SDS w/BIOS 24.99
1804226981	[KBL]Integrate CRB CSME FW 11.5.0.1018 into BIOS
1404732533	SD Card SDR104 auto-tune failure - WA to fix clock selection for Rx Sampling.
1206900784	[kaby_lake.other]Sync Rng library with the opensource version in MdePkg
1304182149	[OPAL BIOS MENU] Toshiba NVMe Pyrite drive not listed in Opal BIOS Menu
1804227189	[PCH BIOS CI] Very low performance after BIOS Power Management changes
1207620275	Integrate 2 SKL patches, for R0/D0 0x7C
1207618952	KBL: remove restricted tags on Virtual Sensor and Storage participants
1207565688	KBL-H: Need a BIOS DCN to Program Bit 22of 0xfe00031C to 1 for system t o avoid check on crystal clock
1304294285	[SVCPU]Make SV and FlexCon Request/Response buffers the same

91.2 BP Client Common Core Sync-up Changes

None

91.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	





92 BIOS – KBL CRB v025.1

BIOS version	0.025.1		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x7A G0 : 0x14 KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.7.0	
	MRC Version	0.7.0.2	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	



P4 Label	@ 338362 (on dot build stream KBL_G0_PO)
----------	--

92.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206900784	[kaby_lake.other]Sync Rng library with the opensource version in MdePkg - MRC part
1804227189	[PCH BIOS CI] Very low performance after BIOS Power Management changes
NO_HSD	Merging CL 338243 for RC3 changes
1206900784	[kaby_lake.other]Sync Rng library with the open source version in MdePkg

92.2 BP Client Common Core Sync-up Changes

None

92.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



93 BIOS – KBL CRB v025

BIOS version	0.025		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x7A G0 : 0x14 KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.7.0	
	MRC Version	0.7.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	



P4 Label	@ 337559 (2016_Kabylake)
----------	--------------------------

93.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1206371435	Add GCC Support to Kabylake BIOS
1604072158	[Beta Req]KBL FSP Security: [PTT][debug] PCR value showing as zero after S3 resume
1404582465	[1404582462] BIOS Guard Protocol Changes
1404582465	[KBL] [BIOS Guard] BIOSGuardServices.inf installs BIOS Guard protocol even if BIOS Guard is not enabled
1404582462	[KBL] [BIOS Guard] SmmSpiFlashCommonLib doesnt work if BIOS Guar
1504152887	CoveCreek: Clean up the code to use S3MemVariable
1404602097	BIOS Power Management overrides for KBL
1206835426	[KBL] : [debug]Core ratio limits do not get set to manually set values if 1-core ratio limit and 2-core ratio limit are set to 25 and 18 respectively
1804226687	Uploaded beta version of RST UEFI driver and legacy oprom.
1207611150	Integrate 2 SKL patches, for R0/D0 0x7A
1207484333	Create a setup option "HID Event Base Capabilities" for the user to be able to set the value returned by the HEBC ACPI method
1604072767	[FSP] Implement and Export SMBIOS_PROCESSOR_INFO and SMBIOS_CACHE_INFO HOB for FSP
NO HSD	fix S3 resume fail. Bios Guard info should be installed always
1504143443	Fix Platform Klocwork issues
1207586444	Remove xxxFsp.inf in CPU RC, that are identical to regular xxx.inf
1207378323	Use MtrrLib from UefiCpuPkg and stop producing PEI_CACHE_PPI
1504143303	Fix ME RC Klocwork issues.
1604088443	[kaby_lake.rvp3][KBL] Incorporate SA RC 0.7.0 draft1 review feedbacks.
1207509529	[kaby_lake.other]RVP3 specific files in the KabylakeSiliconPkgPchLibraryPeiPchPolicyLib
1207266356	[KBL] [BIOS Guard] Update Bios guard driver to find Flash address dynamically instead of hardcoded address
1604089114	GtConfig->PeiGraphicsPeimInit should not be cast to a VBT_TABLE_DATA as it is a 1 bit value only.



1206208528	Rollback "FirmwareConfiguration" default should set to "Production" value
1207443798	[SKLSDS-KBLBIOS] System reboots when sent to CS
1504143109	[ME] Remove redundant policies between PEI and DXE ConfigBlocks.
1604085703	[kaby_lake.rvp3]Remove duplicate code in SA PolicyInitLib
1207418659	Fix for RSE requirement change to execute Secure Erase on all connected drives (SATA & NVMe) in a multi-disk configuration which includes RST configurations such as RAID/NGSA.
1207418659	RSE requirement change to execute Secure Erase on all connected drives (SATA & NVMe) in a multi-disk configuration which includes RST configurations such as RAID/NGSA.
1804224289	[cAVS] Remove support for Sensory IP and Samsung postporcessing from IntelSST BIOS
1504106920	[KBL][Remove BoardId from PlatformPkg - phase 2]
1504153199	[kaby_lake.rvp3]Set PcdFrameworkCompatibilitySupport to False
1404705050	KBL-PO-SV: With PO BIOS 21 SVBIOS Cafe hangs when Applying knobs
1404703432	[kaby_lake.rvp8]KBL-PO-SV: With PO BIOS 21 SVBIOS asserts when fuse "iGD" is enabled.
1603998538	[SKL-COENG][SKLSDS-KBLBIOS] BIOS displays misleading number of cores in the "View/Configure Turbo Options" Menu
NO_HSD	Fix RVP16 SPD Addres Table Data that was incorrectly modified during check in for changelist 326777 "[1504106920][KBL][Remove BoardId from PlatformPkg - phase2 - final post mem phase"
1207577609	Skylake's maximum link width (MLW) of PCI Express Controller (B0:D1:F0) is always x16
1207578513	[SKLSDS-KBLBIOS] : KBL BIOS v24 hangs/freezes
1404695753	Update RSTe Pre OS(4.5.0.1012) drivers for Workstation and AMT Server
1804224667	[[KBL] Assert on debug bios with enabled Intel Test Menu [debug]]
1404716594	Keyboard input does not work during BIOS HDD Password Pop-up causing system to become a brick and unable to boot or recover.
1804215522	Fixed resetting HECI when ME want it.
1304303443	TBT BIOS: With default settings for Two Port HR BIOS failed to enumerate TBT tree
1404236477	NVMe Mode - Opal BIOS PWD (OBP) Management Support in the BIOS
1504140195	[skylake]When FVB header is corrupted, system hangs
1504143310	Fix PCH RC Klocwork issues - take 3



1504140807	[KBL]V22_FSP_GCC and VS_Debug Build get restart from S4 resuming but V21 can not reproduce.
1604065544	Remove Board ID usage from ASL Code
1604082942	[kaby_lake.other][KBL] Create CpuPolicyCommon.h instead of CpuPolicy.h
1504143290	Fix CPU RC Klocwork issues
1304236359	KBL:[debug] Max speed received from BIOS in SMBIOS_PROCESSOR_TABLE_TYPE is 0
1504130568	[KBL FSP GCC]V20 RVP3 and RVP7 system got ASSERT with GCC debug build, issue can't reproduce with V20 VS debug.
1207568231	DPTF:KBL: Disable Memory Participant in BIOS Set up option
1504155064	Add gSiPkgTokenSpaceGuid.PcdCsmEnable and CSM_FLAG back to external code
1504154467	[Push from mpg_customer_enabling: DevSlp PadRstCfg register initialization failure]

93.2 BP Client Common Core Sync-up Changes

None

93.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



94 BIOS – KBL CRB v024

BIOS version	0.024		
BP common core revision	1.3.2.0		
RoyalPark core version	1.3.2.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x78 G0 : 0x14 KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.7.0	
	MRC Version	0.7.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	



P4 Label	@ 334587 (2016_Kabylake)
----------	--------------------------

94.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1504153286	[KBL]V24 RVP11 system got assert with debug build, it hang up at PC "0b00".
1604072072	Unable to preload WIN7 32 bit OS with RTD3 enabled
NO_HSD	KBLY - RVP3 - Yellow Bang on UCSI Driver on Win 10 OS ver: 586/575
1404703927	XDCI _DSM return Integer 0 for unsupported UUID instead of returning a buffer containing 0
1207459743	Update CPU RC policy documentation
NO_HSD	Resolved boot failures with TXT when the FirmwareConfiguration Setup option was set to "Production".
1504132161	[SKL] Request policy to active the patch fix using BIOS Mailbox for Sighting# 5349347 VR issue: PS4 exit fails to assert alert after VCCSA ramp
1603998538	[SKL-COENG][SKLSDS-KBLBIOS] BIOS displays misleading number of cores in the "View/Configure Turbo Options" Menu
1404690283	Remove all references to PTTSwitch from code to minimize confusion for customers as it is no longer needed.
1504147379	[KBL]V23 KBL BIOS flash EC got fail message with FFT and EFIflash, issue cant reproduce with V22. (BIOS guard was disabled.)
1604055835	[KBL-U] [HLK]: WHCK:- TPM 2.0 UEFI Preboot Interface Test fails with "PCRExtendPerf Test "
1804223144	[KBL][SkyCam][CSI2] Move Rvp3 specific policy settings for CtleEnable to common RC code where it belongs.
1804223696	[[PCH BIOS CI] External PCIe card not enumerated after resume from S3]
1503992328	[KBL Security: SINIT launch failing when DVMT pre-allocated size set as 2048M]
1504138083	Update lost synchronization files
1504138083	Fix TC build error.
1504138083	BP 1320 sync up
1504143318	[kaby_lake.other]Fix SA RC Klocwork issues.
1504126337	Fix EFI runtime drivers are not 4KB alignment
1804223199	[PCH BIOS CI] Hang on PC 0055 during resume from S3



1504143318	[kaby_lake.other]Fix SA RC Klocwork issues.
1207552102	Integrate 2 SKL patches, for R0/D0 0x78
1206744088	[KBL]Remove CPU S3 resume boot script. Use the same CPU init for S3 resume as normal.
1404605083	Fix FSP build error since the new file was missing in the INF file
1404605083	modPHY update for KBL PCH -H A0 compile error for FSP build.
NO_HSD	[PPV][CPV]CPV's SVOS screen corrupt after KBL011
1404605083	Kabylake PCH-H ModPHY support
1604077822	PCH power increased by 40 mw across all power KPI's with ULT 3.2 GC[debug]. Backout CL#323385, 1404520597 - Bclk - Ctrl of multiple BCLK settings types in ICC UI
1504123624	[CoveCreek: Merge GopPolicyInit\Dxe to PolicyInit\Dxe module]
1804191612	[KBL-PCH-H] Add Kabylake PCH-H A0 stepping
1304288457	Move UniBIOS and SV to 8M build
1504137164	CoveCreek: Refactory ACPI directory, and separate it as features
1504135739	[kaby_lake.rvp3]Use VS2015 for RC build
1207505805	[SKLSDS-KBLBIOS][Touch screen not responsive after flashing BIOS 22]
NO_HSD	[PPV][CPV]CPV's SVOS not boot build 94_04, but 88_86 is still OK.
1207538944	[Power Boss] [MUST FIX - KBL Beta] Platform Power Source updates correctly in TPWR participant tab, but not in Power Boss Policy tab
1207528090	BIOS_DEVICE_IGFX_FREQUENCY is hard-coded in OverClockSmiHandler.c file
1206933824	SA RC null library needs to be reviewed/cleaned up/ and validated.
1804220774	[KBL][trriage] System can not enter to SLP_S0
1206933824	SA RC null library needs to be reviewed/cleaned up/ and validated.
1804221881	[PCH] PostCodes to be added for individual components - PCH-ME part
1804215548	Allow to boot with FPT flag set for ME SPS
1504143401	[KBL Debug]V22 KBL debug message disapper after change BIOS setting
NO_HSD	Fix EC.ASL 332738
1207475003	KBL DPTF : Add Power Boss Policy
1206933754	[kaby_lake.rvp3]CPU RC null library needs to be reviewed/cleaned up/ and validated



1207537359	Remove SKL patches C0 and M0, and integrate KBL patch: G0 0x0E
1604034285	KBL: Unable to remote wakeup from S3(Sleep)/S4(Hibernate) with BT Keyboard/Mouse on ULT/ULX
1504145371	KabylakeSiliconPkg: Point out all API's usage(Produces/Consumes) on all inf files
1604065544	Remove Board ID usage from ASL Code
1504143310	Fix PCH RC Klocwork issues - take2
1604063982	[kaby_lake.rvp7][win 10]KBL BKC :- PAVP session getting pass when disabled PAVP in bios.[debug]
1207431635	[SKLSDS-KBLBIOS]:Help text states user can reserve 1-4096 MB for root bridge but system does not allow more than 20 MB

94.2 BP Client Common Core Sync-up Changes

None

94.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



95 BIOS – KBL CRB v023.1

BIOS version	0.023.1		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x76 G0 : 0x14 KBL S/H A0: 0xE		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.10	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	



P4 Label	@ 333875 (on dot build stream KBL_G0_PO)
----------	--

95.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604077822	PCH power increased by 40 mw across all power KPI's with ULT 3.2 GC[debug]. Backout CL#323385, 1404520597 - Bclk - Ctrl of multiple BCLK settings types in ICC UI
1207537359	Remove SKL patches C0 and M0, and integrate KBL S/H A0 patch: 0x0E

95.2 BP Client Common Core Sync-up Changes

None

95.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



96 BIOS – KBL CRB v023

BIOS version	0.023		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x76 G0 : 0x14		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.10	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 331968 (2016_Kabylake)		



96.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207532574	[kaby_lake.rvp3]Include Production signed Bios Guard binary in KBL Bios
1404501684	[FSP] Enable BIOS guard support in FSP wrapper build
1504143310	Fix PCH RC Klocwork issues
1404497724	[KBL] [SGX] Remove CR4.SGXE Bit (BIT15) for SKL B0 steppings
1304226421	Intel Test Menu - PTT: Suppress TPM commands does not work and BIOS still sends TPM commands[debug]
1404602035	BIOS Power Management UI feedback
1404556977	ICC WDT enable disable option
1604073905	cAVS NHLT: Add BT NHLT blob to support BT HFP over I2S
1504086526	V13 RVP11 system always hang up at Ab04 from S4 resume, issue depend on KSC1.19 but 1.16 can't reproduce.
1804221562	[PCH BIOS CI] Can't perform S5 after resume from S3
1206208528	"FirmwareConfiguration" default should set to "Production" value
1504106920	[KBL][Remove BoardId from PlatformPkg - phase 2]
1207459743	[KBL]Update CPU RC policy documentation.
1404582487	Should Zero out TPM Cmd/Rsp Buffer for TPM2 CommandLibs
1207523851	Integrate KBL patch: G0 0x14
1207350279	[Error status update in ESRT during capsule update]
1207471041	Bios SSA Variable and Results GUIDs missing in EvLoader code
1304163871	Updated BIOS remapping flow to allow storage devices with sub-class code 0x80 remapping.
NO_HSD	[SVCPU] Need to add support for Exiting SV module to FlexCon
1205720920	[PeiDxeSmmGpioLib does not handle more than 32 pads in a group]
1804221147	[KBL]Integrate CRB CSME FW 11.5.0.1015 into BIOS
1804219622	[SkyCam][CSI2] Implementation of Test Menu option allowing PCE register manipulation. Changing PCE Register value to be displayed as hex number in BIOS menu
1804194100	Add "expose LTR force override" setting for AlpineRidge to Pcie device override table
1804219622	[SkyCam][CSI2] Implementation of Test Menu option allowing PCE register manipulation



1504135524	BIOS should program NRMO to 0x00F and MSL to 0 for the RST disable case to fix ABAR decoding confusing.
1504127856	KBL RVP DT PO support.
1303967082	[SKL eDRAM size in BIOS]
1604047988	WiGig Dock Not connecting issue
1504104435	Allow MEI messages while NFTP corruption for FWupdate\Capsule Update.
1207511235	Peg max link speed policy configuration being bypassed in furcation cases where other Gen3 endpoint is present
1207384368	Incorporate the changes for Grizzly Mountain IDV power on to the Kabylake stream
1404453991	[kaby_lake.other]KBL MRC: Break the current HOB_SAVE_MEMORY_DATA hob to 2 separate HOBs
1304287810	[KBL MRC: write power calculation fix]
1304287812	[KBL MRC: Add full grid sweep in DIMM ODT training for DDR4 1DPC]
1304283036	[KBL MRC: Fix CompOptimization corner case with COMP code down]
1404680243	Update SKL Audio PLL setting after bug fixes in latest stepping
1504106920	[KBL][Remove BoardId from PlatformPkg - phase 2]
1207175208	[Update the latest ACPI 6.0 compiler]
NO_HSD	FSP: S3 Performance data missing in Performance build
1207475003	KBL DPTF : Add Power Boss Policy
1207152993	[KBL]ApWakeUpBuffer start address is hard-coded at 0x58000 in AllocateWakeUpBuffer.
1804191213	Updated NVM Remapping flow in BIOS to support additional PCIe controller on KBP-H PCH.

96.2 BP Client Common Core Sync-up Changes

None

96.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



97 BIOS – KBL CRB v022

BIOS version	0.022		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1037		
GOP Driver	9.0.1043		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x76 G0 : 0x10		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.4	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 329110 (2016_Kabylake)		



97.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207498321	Integrate 2 SKL patches, for R0/D0 0x76
1504138083	BP 1320 sync up phase 1 : only sync up CpuMpCpu of uefiCpuPkg.
1404677770	cAVS: To introduce an enable/disable option in the SKL BIOS for Conexant Smart Amp per HP's request
1804196463	PCH RC PSF library changes
1804219371	[kaby_lake.rvp3][PCH BIOS CI] Can't perform S5 after resume from S3
1207426974	[skylake.sds][SKLSDS-KBLBIOS]:System hangs with PC dd80 if DVMT Pre-Allocated memory is set to any value > 512 MB. Display is lost if DVMT is set to 0 MB.
1504127856	KBL RVP DT PO support
1604074550	[KBL/SKL - Integrate latest GOP 9.0.1043 and VBIOS 1037]
1206917641	[SKL-SDS] BIOS default change for SKC Flashing and Audio
NO_HSD	Fixing NaturalAlignment found issues in CpuBiosGuardConfig.h and IgdDxeConfig.h.
1504026311	[KBL PCH] Update to Config Block for PCH policy - take 5, Use pointer policy for VerbTable structure and PCIE device ASPM override structure
1804197234	Disable TCO watchdog timer by default and add option to enable
NO_HSD	based on the SDS rebase to 104. CL 308315, Confirm the BIOS setup default for the following: If these defaults are not correct then change them accordingly.
1604001284	Selected Memory timing override values are not displayed correctly
1504026311	[KBL PCH] Update to Config Block for PCH policy - take 5, Use pointer policy for VerbTable structure and PCIE device ASPM override structure
1504026311	[KBL PCH] Update to Config Block for PCH policy - take 5, Use pointer policy for VerbTable structure and PCIE device ASPM override structure
1504135739	[kaby_lake.rvp3]Use VS2015 for RC build and enforce VS2013 for default build
NO_HSD	Update ME FW update lib and use HECI method. Update ME FW update library to 1180
1804214760	BIOS shall not program PCIe L1 PM Substates Common_Mode_Restore_Time in upstream ports
1504106920	[KBL][Remove BoardId from PlatformPkg - phase2 - final post mem phase
1504130509	ME RC generates a HOB for the premem ConfigBlock by itself, need to replace it by premem silicon HOB.
1504133804	Move Board Init from PlatformInitPreMem to PlatformInit.



1207471700	[title] Integrate KBL patch: G0 0x10
1404619956	SMBus requires setting for thigh and tlow fields on HTIM register in order to achieve operation frequency - LP segment
1404598578	Set BoardIdOrgValue also for Zumba Beach platforms - extension of CL 299839
1504005677	FPDT Wrapper Performance Measurement through Performance build

97.2 BP Client Common Core Sync-up Changes

None

97.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



98 BIOS – KBL CRB v021

BIOS version	0.021		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1034		
GOP Driver	9.0.1040		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x70 G0 : 0x0E		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.3	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 326319 (2016_Kabylake)		



98.1 Resolved Client BIOS HSD sightings

HSDS#	Title
1207128653	Port SKL SDS Dungeon stream to KBL 1207128653.1: [SKL-SDS] Define Idle Resilency Entry/Exit commands to the EC
1304141448	FlexCon support
1504005677	FPDT Wrapper Performance Measurement through Performance build
1604054624	[debug]System hangs at post code 0x92 when Aperture Size is set to 4096MB]
1504106920	[KBL][Remove BoardId from PlatformPkg - phase2- create rvp13 folder]
1304229202	[PCH] Failed to recognize NVME (M.2) on RVP5 with BKC BIOS ver 104.
1206844799	[SKL-SDS] Enabling PS3/PS4 causes instability in Sx Cycling
1504072282	Use PCH register definition in ASL code
1206957084	[SKL-SDS] BIOS setting to change VR slew rate (for Intersil issue)
1604061369	KBL BIOS: [debug]SUT is not booting to Legacy OS with FSP VS/ GCC Bios
3866154	[Client TXT HSD] SFT BIOS/CircusH/SI2/00.64 : System hang on HP Logo while running SEnter/SExit/10s Wait/Cold Boot on stress efi mode
1504131254	[skylake]Integrate 2 patches: SKL D0 patch 0x70 and SKL R0 patch 0x70.
1604056692	KBL RVP Y[triage] [Enabling] - Vertical USB Port J2A1 not functional

98.2 BP Client Common Core Sync-up Changes

None

98.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



99 BIOS – KBL CRB v020

BIOS version	0.020		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1034		
GOP Driver	9.0.1040		
1.5MB ME Firmware SKU	11.5.0.7013 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.0.0.0006		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x6C G0 : 0x0E		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.3	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 325385 (2016_Kabylake)		



99.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504130568	[KBL FSP GCC]V20 RVP3 and RVP7 system got ASSERT with GCC debug build, issue can't reproduce with V20 VS debug.
1604062479	[KBL] PCIbus driver allocating more resources when rootport is hotplug capable
1504062692	USBC support: BSSB changes
1604069294	[Skylake] [ME]: In S3 resume path ME is delaying due to EOP.
1207372240	[skylake&Kabylake]Change the default state of ApIdleManner and ApHandoffManner to MWAIT
1504106920	[KBL][Remove BoardId from PlatformPkg - phase 2]
1504062692	USBC support: BSSB changes
1206976235	Porting from SKL SDS dungeon. [SKL-SDS] vPro -- BIOS Test (Memory device type) fails when running BVT
1207445553	Integrate 2 SKL patches, for R0/D0 0x6E
1604039316	Sync PCDs between Platform and FSP
1207175208	Update Kabylake to use latest ACPI 6.0 compiler
1404592065	Push from sunrise_point: SPT-LP PePV: Vccprimcore voltage dropped to 0.9v after warm reset
1604031903	Error Seen "Submit Fail For Form Secure Boot Configuration Menu" or system hang seen while enabling and disabling Secure boot option in BIOS for more than 5 times
1504106920	[KBL][Remove BoardId from PlatformPkg - phase2- create board folders]
NO_HSD	SmiVariable library doesn't have CopyMem sub-function. As a result, EPCS tool fails on linux.
1504125479	[kaby_lake.rvp3]Fix Kabylake source code build error issue with VS2015
1207436484	Remove call of CollectProcessorFeature across all threads
1207164465	SMBUS ASL code is not compatible for Linux i801 driver
1504108497	Fix incorrect tagging of Restricted code as internal only code
1207442382	[basin_falls.fpga]Duplicate GUID used in driver: CpuInitDxe
1207431273	Save on CPU_TXT_PREMEM_CONFIG size by reducing some UINT64 elements to UINT32 and adjust the order for natural alignment.
1804216852	[KBL]Integrate CRB CSME FW 11.5.0.7013 into BIOS



1804216820	Adding MEBx version 11.0.0.0006
1604068353	Extended PostCodes to be added by SA DT in the RC
1304253194	[kaby_lake.rvp3]KBL MRC: LPDDR3 ECT fails on NO_RTT boards at 1867
1504106920	[KBL]Remove BoardId from PlatformPkg - phase2
1604068243	KBL Security: TPM configuration throws Error: "Question value mismatch" when dTPM is connected
1207094968	[SKL-SDS] Enable PS3/Ps4, RTD3, RTD3 Camera & eMMC be default
1304182772	[skylake.rvp3]CAT Error during PCI scan on MiniBios
1304192390	[SKL MRC]: Margin overflow in GetPdaMargins
1604040392	[ME] Review the ME RC for the case of PcdAmtEnable sets to FALSE.

99.2 BP Client Common Core Sync-up Changes

None

99.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



100 BIOS – KBL CRB v019.1

BIOS version	0.019.1		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1034		
GOP Driver	9.0.1040		
1.5MB ME Firmware SKU	11.5.0.7009v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x6C G0 : 0x0E		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 324597 (on dot build stream)		



100.1 Resolved Client BIOS HSD sightings

HSDS#	Title
1604068243	KBL Security: TPM configuration throws Error: "Question value mismatch" when dTPM is connected

100.2 BP Client Common Core Sync-up Changes

None

100.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



101 BIOS – KBL CRB v019

BIOS version	0.019		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1034		
GOP Driver	9.0.1040		
1.5MB ME Firmware SKU	11.5.0.7009v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x6C G0 : 0x0E		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.6.0	
	MRC Version	0.6.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.2	
	ACM (Boot Guard)	3460	
P4 Label	@ 324118 (2016_Kabylake)		



101.1 Resolved Client BIOS HSD sightings

HSD#	Title
NO HSD	Fix S4 TraceHub Out of resource issue.
1504128362	V19 RVP3 and 7 system EXT release and NR hang up 0090 , and EXT debug build got ASSERT (00d3).
NO HSD	Add retry mechanism to BIOS for failed EC detect/board id cmd
1804193583	[PCH] PostCodes to be added for individual components. Doxygen update.
1504122638	V18 RVP3 system always got assert with debug build, release build can't reproduce it.[d87f]
1504125634	Add Fsp Wrapper type indicator to Kabylake BIOS Binary
1304234293	SV BIOS - enable INIT less with Kfir interface
1604043487	[kaby_lake.rvp8]KBL BIOS :[debug]S3 exit hangs at postcode 0055 with R2 silicon on RVP 8 boards.
1207363212	[kaby_lake.other][Responsiveness] Resume time increase after KBL_Release0013.3_13 (176ms -> 548ms)
1207436683	Integrate 2 SKL patches, for R0/D0 0x6C
1404601922	BIOS update to IMON Offset VR command
1404543193	KBL OC: BIOS support for AVX ratio offset command
1604065872	[FSP] PostCodes to be added by CPU DT in the RC
1404520597	Bclk - Ctrl of multiple BCLK settings types in ICC UI
1804215887	[KBL] Platform hangs at PC 0x0C15 during boot after CL#322961
1207384368	Incorporate the changes for Grizzly Mountain IDV power on to the Kabylake stream
1207431487	Integrate BIOS ACM Rev 0.5.2
1207384368	Incorporate the changes for Grizzly Mountain IDV power on to the Kabylake stream
1207426931	SCLEAN SVN is programmed as 0 when booted in a non TXT capable silicon
1504125403	[kaby_lake.other]Clean up the unused policy item from SiPolicyStruct.h
1207148680	[PNP][SKL-SDS][CS] Disable WWAN RTD3 by default and Gray Out (don't let user edit)
1207351543	Splitting FspUpdVpd.h to FsptUpd.h/FspmUpd.h/FspsUpd.h
1304233389	KBL BIOS: Need to integrate version 0.0.13 of UEFI PXE for Jacksonville
1304233440	KBL BIOS: Need to integrate version 0.1.09 of Legacy PXE for Jacksonville



1804196572	Uploading new RstNvmeDriver.efi binary with Format command unblocked.
1504123826	[skylake][SKL and above] Do not set x2APIC OptOut by default in DMAR table.
1504124737	[KBL] Request to fix SA Config block DWORD size alignment issues captured by NaturalAlignment check.
1604060654	8254 Static Clock Gating Enable (8254CGE) not set in FSP
1207418980	Follow up BoardId of BasinFalls
1603996161	[skylake.rvp8]SKL BIOS :[debug]Memory voltage values are not reflecting correctly in BET tool for corresponding BIOS values
1404558731	KBL - Remove Safe Mode Settings
1804213668	[KBL] Debug BIOS v18 - unable to enter BIOS.
1404580798	KBL BIOS 12 unable to work with EPCS util tool
1207163253	[KBL BIOS on SKL-COENG]][SKLSDS-KBLBIOS]System boots to EFI after flashing new SPI image
1404591851	Push from sunrise_point: CLONE from skylake: [Zumba Beach]WOL through I210,shutdown by power button, after some seconds the system auto switch on For each PCIE RP clear PME SCI status and disable SCI, then PCIEXP_WAKE_STS from PMC.
1205663672	Update the INF files format in SkylakePlatSamplePkg to follow ECC rules
1206067810	[Customer requests to add an PS2 Keyboard/Mouse enable/disable setup option for RVP]
1206745023	Remove McuUpdateDataAddr from TXT_CONFIG and the TXT HOB.
1304231335	[SVCPU] Shared Mailbox changes
1804193583	[PCH] PostCodes to be added for individual components

101.2 BP Client Common Core Sync-up Changes

None

101.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



102 BIOS – KBL CRB v018

BIOS version	0.018		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1034		
GOP Driver	9.0.1040		
1.5MB ME Firmware SKU	11.5.0.7009v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x68 G0 : 0x0E		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.5.0	
	MRC Version	0.5.0.4	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.1	
	ACM (Boot Guard)	3460	



P4 Label	@ 320602 (2016_Kabylake)
----------	--------------------------

102.1 Resolved Client BIOS HSD sightings

HSD#	Title
1404520555	BCLK - Frequency report
1304223865	KBL BIOS: HLK TPM 2.0 - Supplemental tests fails due to BIOS incorrect PCR[0] value
1504068127	[WCT] Method for telling the power source and notification for its change event
1504106920	[KBL] Remove BoardId from PlatformPkg - phase2
1205667340	Implement correct setup design in ME Restricted Policy code.
1207123074	[SKL PPV] SKL-BIOS-RVP11: Windows Event Viewer - Wake Source shown [Unknown], while SUT resumed from S3 by USB Keyboard/USB Mouse
1207399314	Merging CL#319866 from Skylake for [1207399314][skylake]System throws BSOD ACPI_BIOS_ERROR while booting to windows when Aperture Size is set to 4096MB.
1207167924	Enable a BIOS WWAN/GNSS disable option that disables and power gates the WWAN/GNSS option and removes the SAR related boot delay
1404593507	Let UiApp.inf able to access gSetupVariableGuid
1207394811	[kaby_lake.rvp3]MC oldest VC1 forward progress during demote to solve DE under run bug
1404593190	Merging //ClientBIOS/2015_Skylake/SkylakeSiPkg/Pch/PchInit/Dxe/PchRstPcieStorage.c to //ClientBIOS/2016_Kabylake/KabylakeSiliconPkg/Pch/PchInit/Dxe/PchRstPcieStorage.c
NO_HSD	Fix the RVP7. RVP10 post hang in MRC after CL#319385 & CL#319403
1504103737	Warning 3107 - Reserved method must return a value (Integer required for _STA)
1205665381	Remove FSP_FLAG build switch and relative code from SiPkg
1604059168	[kaby_lake.rvp8]KBL BIOS: Max/Min Turbo Power Limit default values are not listing in BIOS
1207396652	Integrate KBL patch: G0 0x0E
1207396655	Integrate 2 SKL patches, for R0/D0 0x68



1504106920	[KBL] Remove BoardId from PlatformPkg - phase2
1207384368	Incorporate the changes for Grizzly Mountain IDV power on to the Kabylake stream
1804197299	[KBL]Integrate CRB CSME FW 11.5.0.7009v2 into BIOS
1504029797	[KBL-BIOS][trriage] : DP Functionality is not working with KBL V001 BIOS
1404316822	merge from SKL: [Apple]: Policy setting request to disable CPM on PCIe root port
1804196309	[KBL] [BIOS v17] S3 causes restart or BSOD during wake
1504073425	[kaby_lake.rvp3]Remove simics flag and relative code
1804187708	[KBL][FSP] [debug]ME FW 0.0.0.0 when FSP BIOS 12 is present
1205599904	[Platform SysDebug][CNL BIOS][debug] : SGX_Debug_Mode and Lock_Bit is not configured.
1604047938	Legacy 4sec Shutdown doesn't work with 10sec power button override disable
No HSD	Set DISB before the warm reset during the SCLEAN test.
1304002304	[skylake.skl_rvp3]KBL BIOS: Setting SAGV fixed to LOW does not change FCLK frequency
1304229860	[SVCPU]Change default for FlexConEnable policy after. [SVCPU] Allocate SV shared mailbox memory in MRC
1504109100	[KBL]V16_FSP_GCC build got S3 resume failed, post code stop at b87f to 987f.
1207346523	Push from sunrise_point: [GDC PCIe] - BSOD 0x124: WHEA_UNCORRECTABLE_ERROR while doing hot plug testing
1504091415	[KBL] Add notify phase 1 & 2 for S3 resume flow in wrapper bios.
1804196648	Change End of Post Message policy setup option and move it to debug menu
1404585345	Wrong use of Assert_EFI_Error in SA code
1207359574	[KBL Alpha] VSCT tables are identical for both VIR1 and VIR2
1304221179	EventManager: Bios doesn't send System Firmware Progress Events to FW.
1207224483	[skylake]Skylake FSP: need UPD to configure SPD Write Disable bit
1504110595	SKL PCH PCIe MPC.SRL bit can't be set in current code



102.2 BP Client Common Core Sync-up Changes

None

102.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



103 BIOS – KBL CRB v017

BIOS version	0.017		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1034		
GOP Driver	9.0.1040		
1.5MB ME Firmware SKU	11.5.0.7007 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x66 G0 : 0x0A		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.5.0	
	MRC Version	0.5.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.1	
	ACM (Boot Guard)	3460	



P4 Label	@ 317486 (2016_Kabylake)
----------	--------------------------

103.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604051603	SKL: FSP not to set the ACCTRL bit for XHCI Device
1604046964	KBL BKC: [debug]Package C10 is achieved, though C state is limited to C7 from BIOS
1207111933	Missing FastSlew Enable/Disable implementation for GT and SA and documentation
1604059140	KBL/SKL - Integrate latest GOP 9.0.1040 and VBIOS 1034]
1304225731	TBT BIOS: Add AR-C0 device ID
1304229888	[KBL][BIOS] Secure boot in BIOS is disable option on first boot to return it need to reset for default settings.
1504102175	[KBL]V15 FSP_VS_Debug build system got long time resume from S3, it spend about 5 mins
1404582483	Platform_PCIEXPRESS_LENGTH is not used]
1404590712	Integrate KBL patch: G0 0x0A
1207352128	[KBL]: BIOS/EC: Support DPTF Power Participant on KBL/CNL
1207329722	[KBL Alpha] Generic fan participant name in ART
1207355299	[KBL-BIOS] System does not POST with BIOS KBL-16
1604044063	[kaby_lake.rvp3]KBL BIOS: [debug]Active Processor Core is not Reflecting correctly in BIOS during first reboot
1207326348	[kaby_lake.other]CPU MP Services Init increased 94ms from SKL to KBL - Part 1
1504107862	[KBL]V15.2 RVP3 System hang up post code dd69 with external debug build, it can't reproduce with external release build.
1207356362	Integrate 2 SKL patches, for R0/D0 0x66
1404523390	SSIC extra D3 entry with D3HE set (https://hsdes.intel.com/home/default.html#article?id=1404523390)
1207250619	[Kabylake.zumba_beach]Feature Request: MRC failure upon RDIMM detection
NO_HSD	Reserved FIT support



1604053911	[kaby_lake.other]KBL_Security: Error message observed in Vt-d info tool on KBL
1504106920	[KBL] Remove BoardId from PlatformPkg - phase2
1404523390	SSIC extra D3 entry with D3HE set (https://hsdes.intel.com/home/default.html#article?id=1404523390)
1804189610	PCIe: expose LTR force override platform policy
1804194324	[KBL] PID 0xB0 cannot be used by SSIC in KBL-H
NO_HSD	Updating RST binaries (legacy option rom and uefi driver) to RST 15.0 Alpha version (build number 2391).
1804192953	[KBL] [debug]Duplicated option in SerialIO menu

103.2 BP Client Common Core Sync-up Changes

None

103.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



104 BIOS – KBL CRB v016

BIOS version	0.016		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1033		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7007 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x64 G0 : 0x8		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.5.0	
	MRC Version	0.5.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 0.5.1	
	ACM (Boot Guard)	3460	



P4 Label	@ 315234 (2016_Kabylake)
----------	--------------------------

104.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207345836	Integrate 2 SKL patches, for R0/D0 0x64
1206755323	Implement FSP 2.0 without v1.1 compatibility (no FSP-c)>
1804192646	SATA port implemented bit should not be set for disabled port
1504106065	Align BP build environment and tools define for GCC and Clang
1504072866	[kaby_lake.rvp3]Replace Str**S with Strn**S for Security - Phase 1 take 2.
1504040892	[skylake]CPUID update for SkyLake N0 stepping
1504102123	[kaby_lake.rvp7][KBL]V15_FSP_GCC_Debug and Release get assert(post code 9800 and 9C00) on RVP7.
1206881811	Fix Check in 314780 Need to update SV module after [1206881811]Leverage CpuMpPeimInit from UefiCpuPkg to Client silicon reference code Change in [1504090233][ME] Merge ME/AMT config block to SI and remove policy PPIs in PEI phase
1504104435	Allow MEI messages while NFTP corruption for FWupdate\Capsule Update.
1206913341	Add BIOS RSE (Remote Secure Erase) support for PCIe NVMe SSD
1404470650	Add additional step to the W/A for the mphy Power gating issue for pcie owned lanes
1304001142	[KBL-PCH-H] Add new 4 PCIe lanes and new root port DIDs
1604052942	[kaby_lake.other]KBL Security: SUT hangs at 0B7F Post Code after flashing Boot Guard profile
1604027129	[KBL BC-RQTBC-10656 - BIOS option to select runtime Max GT Frequency]
1206577060	Push from sunrise_point: [SPT PCIe] Unable device exit from RTD3 after 1st iteration.
1504102982	[FSP WRAPPER] Add UPD to support PCH Test and Restricted policies
1604027496	KBL RealSense 3D Camera Requirements
1604054902	[KBL - ULT] - IRMT not supported in the KBL U skew in bios
1504090233	[ME] Merge ME/AMT config block to SI and remove policy PPIs in PEI phase.



1604052405	[debug]OEM table ID is showing wrongly in ACPI tables
1504064420	[Please move out PlatformSpecificAcpiEnableHook control from mEcPresent status]
1604047101	KBL BIOS : No debug log captured after making any changes in Intel advance menu
1604052714	FFU.efi tool is failing to execute when secure boot is enabled.
1804188854	[KBL-PCH-H] Add support for PSF registers
1504064412	KBL FSP : Restructure EndOfPost Policyand flow to send EOP message in PEI or DXE alternately
1504090233	Remove AMT_SUPPORT workaround [ME] Merge ME/AMT config block to SI and remove policy PPIs in PEI phase.
1504102260	[KBL] Bug found in SA OverrideDev0Did() Restricted code
1404531810	Merge - To KBL Workaround for eSPI PCH bug that prevent SLP_S0
1206884970	[KBL] [SGX] Task 3 - Restructure ReloadMicrocode ()
1504090233	[ME] Merge ME/AMT config block to SI and remove policy PPIs in PEI phase.
1207307596	Integrate BIOS ACM Rev 0.5.1 and adjusted flash layout.
1404442326	SKL Fsp: FSP does not do TempRamInit (CAR setup) and let bootloader do that
1604034205	FSP 2.0 UPD structure changes
1804189867	ByteAcc must be used for Power Management Control & Status in GPEH
1804192977	[KBL]Integrate CRB CSME FW 11.5.0.7007 into BIOS
1504051833	cAVS NHLT: Set KBL PDM interface clock default rate to 2.4Mhz
1504102123	[kaby_lake.rvp7][KBL]V15_FSP_GCC_Debug and Release get assert(post code 9800 and 9C00) on RVP7.
1206340635	Rename PciClockRun policy to LpcClockRun, checkin part 2
1504064602	KBL FSP : Program HECI1-HECI3 BAR in RC
1804192883	[KBL][merge]BIOS Change needed for: USB KB may not wake up in S3
1504101043	[kaby_lake.other]Add setup item for Pmic SlpS0 VM support and default with disable



104.2 BP Client Common Core Sync-up Changes

None

104.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



105 BIOS – KBL CRB v015.2

BIOS version	0.015.2		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1033		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7006v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x60 G0 : 0x8		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.5.0	
	MRC Version	0.5.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@ 314758 (on dot build stream)
----------	--------------------------------

105.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504102123	[kaby_lake.rvp7][KBL]V15_FSP_GCC_Debug and Release get assert(post code 9800 and 9C00) on RVP7.
1504090233	[ME] Merge ME/AMT config block to SI and remove policy PPIs in PEI phase.
1604054162	MRC version mismatch observed with the release notes for BIOS V015.
1504064602	KBL FSP : Program HECI1-HECI3 BAR in RC.
1404442326	FSP2.0 – Make TempRamInit Optional.
1604034205	FSP 2.0 UPD structure changes.
NO_HSD	CPU Pre-Mem RC Policies classification for Production , Test & Restricted after FSP 2.0 changes
1404367613	Move TPM2 in scripts and other files to be available in Royal Park (FSP #3)
1206340635	Rename PciClockRun policy to LpcClockRun, checkin part 2
1504064412	(KBL FSP : Restructure EndOfPost Policyand flow to send EOP message in PEI or DXE alternately)
1206884970	[KBL] [SGX] Task 3 - Restructure ReloadMicrocode ()

105.2 BP Client Common Core Sync-up Changes

None

105.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



106 BIOS – KBL CRB v015.1

BIOS version	0.015.1		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1033		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7006v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x60 G0 : 0x8		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.5.0	
	MRC Version	0.5.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@ 314592 (on dot build stream)
----------	--------------------------------

106.1 Resolved Client BIOS HSD sightings

HSD#	Title
1604052942	KBL Security: SUT hangs at 0B7F Post Code after flashing Boot Guard profile

106.2 BP Client Common Core Sync-up Changes

None

106.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



107 BIOS – KBL CRB v015

BIOS version	0.015		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1033		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7006v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x60 G0 : 0x8		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.5.0	
	MRC Version	0.5.0.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@ 312731 (2016_Kabylake)
----------	--------------------------

107.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504101043	[kaby_lake.other]Add setup item for Pmic SlpS0 VM support and default with disable
1404501665	[FSP] Enable SGX support in FSP wrapper build
1206884970	[KBL] [SGX] Task 3 - Restructure ReloadMicrocode
1604039851	[KBL] [SGX] KBL Security: [debug]SGX MSR Value 503h is not programmed with debug interface enbaled
1404439076	[BIOS Guard] [KBL] Integrate BIOS Guard PO module
1604033098	[FSP] PostCodes to be added by PCH DT in the RC
1206912046	Create DxeSmbiosProcessorInfoLib to consume HOBs from SI code and produce SMBIOS tables 4 and 7
1206906072	Decouple SMBIOS processor table generation (types 4 and 7) from Silicon Initialization code
1207098889	Push from mpg_customer_enabling: SMBIOS L1 Cache Information
1404446891	XHCI D3HE disable flow support for SSIC ports
1206881811	Leverage CpuMpPeimInit from UefiCpuPkg to Client silicon reference code
1207207985	[KBL FSP]S3 resume hangs due to TBT
1804188710	[KBL-PCH-H] Add Kabylake PCH-H DID support
1504089418	SLP_S0# support with VM on premium PMIC vs Discrete VR systems
1604033023	[FSP] PostCodes to be added by SA DT in the RC
1504096339	[KBL] SA refactor & cleanup for 0.5.0 release
1604032996	[FSP] PostCodes to be added by CPU DT in the RC
1804188109	[KBL] BSOD durring Windos 7 CHK instalation
1504086001	[skylake][Wrong use of ARRAY_COUNT macro, pointer size is used instead of array size
1604051770	[KBL] Add Supported WiFi NICs for KBL



1207255410	[Responsiveness] "TCG2 implementation - take 1" make the responsiveness score bad
1404525177	[Kabylake]Micron TCR Sensitivity W/A
1207288345	[Responsiveness] "SA Config Blocks should be spl't into PreMem and PostMem phases." make 100ms delay for RVP11
1603968412	TBT code cleanup
1206745439	SKL Security:[debug] Error message observed while accessing TPM configuration in BIOS with dTPM 1.2 connected
1404562555	PPV7 hang 96 when CSM on
1404549861	[skylake.skl_rvp16_sip]BIOS XDCI _DSM need to avoid changing XDCI APBFC_U3PMU_CFG4 (SIP_USB3_XDCI_Controller_HAS section 8.4.5: Offset 10F818) bit 3. Resetting XDCI core may result in RVP16 CATERR
1604045496	[KBL] [SGX] SINIT SVN is not correct when TXT is not in the flash image
1207293040	To add an ACPI method that will report to the HID Event Filter driver the buttons supported on the platform
1207294601	Integrate KBL patch: G0 0x08
1207294593	Integrate 2 SKL patches, for R0/D0 0x60
1404376166	BtG now includes options to allow different error approach for TPM error flow
1304141448	[FlexCon support]sol
1804187794	[KBL][FSP] SX hangs with BIOS KBL 12
1504072866	[kaby_lake.rvp3]Replace Str**S with Strn**S for Security
1504083967	Merge SA Config Blocks into main Si Config Blocks to achieve single policy structure for all components
1205659552	Custom TDP Table Menu Change
1206362742	BIOS changes to emulate PM_TMR in uCode
1604022087	[SKL_PPV][SKL_HLK] WatchDog Timer Test fails with error " Unable to find event log entry indicating that watchdog triggered a system reset. Hardware did not report this to the HAL! "
1604033114	[FSP] PostCodes to be added by ME DT in the RC
1207124687	EnumPs2Keyboard function uses ConInAct without size validation
1207124670	DxeOverclockEntry doesn't properly handle EFI_BUFFER_TOO_SMALL



1207124623	ModifySetupAttr function doesn't NULL check memory allocations of an untrusted input
1207124645	FastBootUpdateBootOrder memory leaks and arithmetic overflow
1207124725	UEFI Var ConIn used without size validation in multiple instances
1504030139	[KBL CPU] Add Config Block support for CPU Policy
1604037606	[KBL-U] [HLK]: SUT got hang at S0 state during watchdog timer test
1604027529	HiiExport variable to made more secure

107.2 BP Client Common Core Sync-up Changes

None

107.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



108 BIOS – KBL CRB v014

BIOS version	0.014		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1033		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7006v2 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x58 G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.4.5	
	MRC Version	0.4.5.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@ 309588 (2016_Kabylake)
----------	--------------------------

108.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504030139	[KBL CPU] Add Config Block support for CPU Policy
NO HSD	Bios must add XTU interface enable/disable option
1804187794	[KBL][FSP] SX hangs with BIOS KBL 12
1604028830	Unable to access the TBT hard disk after resuming from S3/S4
1304188098	Add AR_LP device ID
1604036196	KBL Y LPDDR3 RVP porting
1207117646	Enable Quad Output and Dual Output on KBL IFWI for SPT-LP Cx and later and SPT-H Dx and later
1604027606	Support for Intel ICC
1604028329	[Adding support for the Cdynmax Clamping Feature for the GT4 Halo (4+4e) parts (Iccp Feature)]
1504030139	[KBL CPU] Add Config Block support for CPU Policy
1207232838	Integrate 2 patches: SKL R0 patch 0x5C and SKL D0 patch 0x5C to both RVP and SV builds.
1304133094	[kaby_lake.other]EFI TouchPanelDriver Driver Binding Protocol implemented not according to Platform Initialization Specification
1304163823	Intel Smart Sound Technology - codec selection setup option
NO HSD	Remove Clang workaround
1504086506	[kaby_lake.rvp7][KBL]V13_FSP hang up post code 007F on RVP7.
NO HSD	KBL Security:By Default PRMR size is displayed as 128 MB when SGX in Software Controlled
1504026311	[KBL PCH] Update to Config Block for PCH policy
1504086023	When we have two or more timers with different ticks, but same period, so the first one (with shortestest tick) is going ok, but the others goes quicker than they should be.
1207231279	Align 2016_Kabylake with BP_1.3.1.0



1706521417	[skylake.rvp15_sip]KBL MRC: Enable TCR for DDR4 Hynix 1512
1404512675	BIOS should remove Ring VR implementation for KBL
1207216224	Unable to retrieve disk information from Shell with external sata pci-e card.
1604045380	FSP postbuild script, fdf and dsc update to generate production bios
1604045474	Security - FSP UPD/VPD Policies in KBL
No HSD	Update PM_TMR Emulation changes to match latest SKL revision
1207212140	[skylake.rvp15_sip][KBL-PH1][RVP15] Postcode [ddab], the platform do not boot with the configuration of memory [MTA18ASF2G72HZ-2G3A1] [micron] in both channels.
NO HSD	Fix BIOS API functions to resolve Cafe issue
1604043828	KBL BIOS: SUT doesnt boot with FSP GSS/VS BIOS images

108.2 BP Client Common Core Sync-up Changes

None

108.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



109 BIOS – KBL CRB v013.1

BIOS version	0.013.1		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1031		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7004 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x58 G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.4.5	
	MRC Version	0.4.5.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@ 288178 (on dot build stream)
----------	--------------------------------

109.1 Resolved Client BIOS HSD sightings

HSD#	Title
	CL#307926 Back out changelist 303182 [hsdes] 1604027496 [title] RealSense 3D Camera requirements on KBL

109.2 BP Client Common Core Sync-up Changes

None

109.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



110 BIOS – KBL CRB v013

BIOS version	0.013		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1031		
GOP Driver	9.0.1039		
1.5MB ME Firmware SKU	11.5.0.7004 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x58 G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.4.5	
	MRC Version	0.4.5.0	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@ 305646 (2016_Kabylake)
----------	--------------------------

110.1 Resolved Client BIOS HSD sightings

HSD#	Title
1207216224	Unable to retrieve disk information from Shell with external sata pci-e card
1207212132	KBL V11 hangs/asserts on SKL SD
1207202510	Push from sunrise_point: PROMOTE from mpg_customer_enabling: [Start] XHCI Yellow bang issue
1404502190	SKL/M.2 SSIC - disable AP stall in polling mode
1207107226	[SKL-COENG] Add additional Bios fields to control EC LED behavior and EC Base Pwr Policy
1304168224	SPI Protocol doesn't allow to write/erase when FlashRegionAll option is used
1604027500	[KBL] Connectivity(CNV) BIOS Code Changes to KBL
1504083754	Override FCE tools in KBL stream to resolve long delay during build process (after folder re-name)
1206863050	System hangs when "AP threads Handoff Manner" is set to "MWAIT Loop"
1207208158	PcdUefiShellBuildSource = TRUE fail the build
1604038950	Implement GOP config driver changes for GOP version 1039
1304158709	[SVBIOS] PSMI support
1604027496	RealSense 3D Camera requirements on KBL
1604013073	Debug Info display the size of the ACPI C-state table, instead of the P-State table
1604035310	Rename SKL folders to KBL folders name in KBL stream



1304130920	RTD3 support for NVME Remapped Drives
------------	---------------------------------------

110.2 BP Client Common Core Sync-up Changes

None

110.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



111 BIOS – KBL CRB v012

BIOS version	0.012		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1031		
GOP Driver	9.0.1037		
1.5MB ME Firmware SKU	11.5.0.7004 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x58 G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code	Version	
	RC Version	0.4.0	
	MRC Version	0.4.0.1	
	BIOS Guard(PFAT)	1.1.0 (2.0.20150625)	
	ACM (TXT)	Version 1.3	
	ACM (Boot Guard)	3376	



P4 Label	@302633 (2016_Kabylake)
----------	-------------------------

111.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206746721	Remove POST code displays from _Qxx EC interrupt methods
1804186980	[KBL] Unexpected error popup during setting TPM configuration
1207173200	[kaby_lake.other]Implement new KBL CPU signatures
1207114044	Gray-out the TXT Setup Option when PcdTxtEnable is FALSE
1404455154	[SKL RVP3][WWAN]SKL BIOS: Modify _ON/_OFF method to follow M.2 power sequencing requirements
1404455172	[SKL RVP3][WWAN][7260][SSIC]SKL BIOS: Add support for WWAN
1504080534	[KBL FSP Wrapper] SA FSP UPD support for full feature validation purpose
1304160825	USB Precondition to remove in Kabylake BIOS
1804186658	[PCH BIOS CI]Assert while booting debug BIOS on RVP8
1604036045	wrapper bios hang during POST - part#1: Fix assert failure if PcdAmtEnable is FALSE
1206930592	Create Config Block Table, per phase, for config blocks related to silicon policies
1206930592	Create Config Block Table, per phase, for config blocks related to silicon policies
1604039301	[KBL][V11.2]RVP System all hang up at 000d and got CATERR error, issue only reproduced with NR and EXT build
1404217478	Update Embedded platform Saddlebrook in kblake
1207049117	Implement Crash Dump feature



1207145589	circuitLock Bit for MSR_PACKAGE_POWER_LIMIT (MSR 0x610) and MSR_DDR_RAPL_LIMIT (MSR 0x618) are different in code implementation and SKL EDS
1404516835	[KBL] [SGX] SINIT SVN is not correct when TXT is not in the flash image
1206962658	Integrate TXT BIOS ACM version 1.3
1207175705	Integrate 2 SKL patches, for R0/D0 0x58
1804186932	[KBL]Integrate CRB CSME FW 11.5.0.7004 into BIOS
1504026311	KBL PCH] Update to Config Block for PCH policy - take3
1604038671	@ KBL BIOS : DPTF Configuration page in BIOS is blank on KBL RVP7 Boards
1504026311	[KBL PCH] Update to Config Block for PCH policy - take3
1504067110	Remove PowerCycleReset and GlobalResetWithEc support from PCH RESET
1604031132	Add lost drivers back into the wrapper
1604027709	[Platform-CI-WW41.2]VPB Device (HW id ACPI\INT33D6) is enumerated in Device Manager for RVP 10 with Bios 101_00 FVME+11.0.0.1180
1206746990	[Kabylake] DVT: System fails to boot and can not recover it if user selects SHA512 and SM_256 for Active PCR Banks under TPM configurations
1304090117	ASF table: Reported table size is larger than actual table
1206738595	System Agent platform code has incorrect CPUID stepping information
1504080499	[KBL] SA Config Blocks should be spltd into PreMem and PostMem phases
1504071260	[FSP WRAPPER] Full function (production) enabling - PCH UPD support
1504032768	[KBL] Remove BoardId from PlatformPkg - phase1: gathering the BoardId check - Specific Board Function
1206600912	CPU - FSP UPD/VPD Policies in KBL



1504032768	[KBL] Remove BoardId from PlatformPkg - phase1: gathering the BoardId check - Final cleanup
1207143256	Push from sunrise_point: PROMOTE from mpg_customer_enabling: Failed to enter S3 or resume hang with black screen in DC mode
1504078226	[skylake]When Periodic timer and SWSMI timer interrupts are triggered at the same time, one of the interrupt will not be dispatched
1206779654	Enhancement in MRC log file to print additional data
1604034205	FSP 2.0 UPD strcture changes part II
1206641185	[PPV][RCR]Need gEfiSerialIoProtocolGuid installed when in shell
1504055707	PlatformInit module should be included in FSP wrapper build
1604037780	HD Audio not power gating in I2S mode. All power gating domains are active
1804186541	[kaby_lake.rvp7][KBL] [triage]No display on RVP7 with KBL MCP
1206907873	[kaby_lake.rvp7][KBL - U PO] - System does not go to SLP_S0 when CS Sleep Entry is attempted on KBL ULT RVP 7 boards
1504070829	Eliminate the warning message of "VfrCompile" during bios build
1504071464	[FSP WRAPPER] modify bios flash map to enlarge FvRecovery3 space
1604036025	[FSPWRAPPER]enlarge UPD size to put all RC policies
1304181697	ME RC cleanup part 4
1206884970	[SGX] [KBL] Task 2.2, 2.3, 2.4, 2.5 - Modify the calling sequence of SGX Initialization to make it more modular
1304188513	[PCH BIOS CI] Hang during resume from S3
1504032768	[KBL] Remove BoardId from PlatformPkg - phase1: gathering the BoardId check - VERB_TABLE



111.2 BP Client Common Core Sync-up Changes

None

111.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



112 BIOS – KBL CRB v011

BIOS version	0.011		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1031		
GOP Driver	9.0.1037		
1.5MB ME Firmware SKU	11.5.0.7003 (Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	15.0 Pre-Alpha (revision 2371)		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x50 G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150909_DEBUG_Rev_1.1.bin SKL_BIOSAC_20150909_PRODUCTION_Rev_1.1.bin	
	ACM (Boot Guard)	3376	



P4 Label	@298700 (2016_Kabylake)
----------	-------------------------

112.1 Resolved Client BIOS HSD sightings

HSD#	Title
1304188513	[PCH BIOS CI] Hang during resume from S3
1304089382	SKL FSP]SKL-BIOS: S3 exit hangs at Post code 0055 on RVP7 board with FSP GCC wrapper image
1504076279	[skylake]Integrate 2 patches: SKL R0 patch 0x56 and SKL D0 patch 0x56 to both RVP and SV builds
1206904311	[KBL]Move PchSmmControlLib and PeiSmmAccessLib from private library to public library
1604034205	FSP 2.0 UPD strcture changes part I
1804184571	[PCH BIOS CI] Assert while booting debug BIOS on RVP8
1304180152	[SVCPU]BIOS should add initial value of NPK_STH_APICBAR_BASE (0x80) to PC.xml
1504071464	[FSP WRAPPER] modify bios flash map to enlarge FvRecovery3 space
1504062544	[kaby_lake.rvp3]Refactoring private interface files to align with IntelFspPkg
1206885427	Implement PL1/PL2 override values for KBL SKUs
1504032768	[KBL]Remove BoardId from PlatformPkg - phase1: gathering the BoardId check
1404491790	[skylake.rvp16_sip]Request to modify existing XDCI _DSM function index 4 to disable PMU PME for supporting XDCI hibernation while connected (Soft Disconnect)
1404473771	[skylake.rvp16_sip]Request to add a new _DSM Func
1206965867	[KBY] In order to pass BVT need to make sure that LPDDR3 memory chips report as form factor "row of chips" for SMBIOS type17
1304156285	RTD3 XDCI ACPI code contains strange location of XDCI MMIO BAR



1504060917	[kaby_lake.rvp3]Move all interface files of Hsti to ClientSiliconPkg
1304170460	PCH RC GPIO library API changes for GPIO reset settings
1504062524	Update to follow the RoyalPark_BP131x_Internal stream
1404217478	Enable Embedded platform Saddlebrook in kblake
1206750288	[kaby_lake.other]L"Boot%04x" (lower case) is used everywhere in Intel Source(both in Platform RC Code & Royal Park code)
1504055707	PlatformInit module should be included in FSP wrapper build
1504070810	[ME] Convert MePolicy to config block
1206882518	SKL SDS: Rename HDA PME Enable Help Text
1404412781	[skylake]Occasional 2 second pause during AP startup on SKL
1206922738	Add Unit Test Framework to ClientCommonPkg, add Unit Tests for Kaby Lake Si Code to SkylakeSiPkg
1206472152	SKL SDS RTD3 needs clean up. It has a lot of unused code in ASL
1404455154	[WWAN]SKL BIOS: Modify _ON/_OFF method to follow M.2 power sequencing requirements
1304181704	[kaby_lake.rvp3]KBL MRC: MrcSet/ResetDISB functions are broken
1304179754	[UniBios][SvBios]Add DCI Support
1404469799	Add ConfigBlock for System Agent DXE Protocol
1304175742	[kaby_lake.other][UniBios][KBL] Change DEBUG_ERROR to DEBUG_INFO when not being in an error path
1304032621	BIOS changes to support NXP NPC300 Card for SKL
1206601457	Push from sunrise_point: PROMOTE from mpg_customer_enabling: [MSFT SKL Y/U Platforms]: Disabling HDA audio using BIOS policy settings not fully disabling the device
1304171259	[skylake.rvp3] SKL MRC: Change RefPi to 7 for better VccSA Vmin



1206912780	Push from mpg_customer_enabling: Win7 checked version boot failure
1604033837	KBL/SKL - Integrate latest GOP 9.0.1038 and VBIOS 1032
1504026311	[KBL PCH] Update to Config Block for PCH policy - take2, separate to premem and postmem policy
1206722801	Linux throws error for "Scope() inside If() conditon" in ASL files
1206884970	[SGX] [KBL] Modify the calling sequence of SGX Initialization to make it more modular
1504054439	[skylake.rvp8]RHEL 7.1 ACPI error with 3.7GHz CPU
1206738595	Remove Post Codes from _SB.PCI0.DOCK._STA and _DCK methods. Use ADBG instead
1206641185	[PPV][RCR]Need gEfiSerialIoProtocolGuid installed when in shell
1304163864	RST 15.0 OROM and UEFI driver
1304178370	[KBL]Integrate CRB CSME FW 11.5.0.7003 into BIOS
1404348258	SKL FSP: need to have clearly defined Post code (granularity) in FSP
1504066897	KBL FSP : split "FspWrapperInitApiV2()" into 2 part, premem & postmem portion
1604027033	Implement GOP config driver changes for SKL GOP release 1037
1604028181	SKL - Integrate latest GOP 9.0.1037 and VBIOS 1031

112.2 BP Client Common Core Sync-up Changes

Updated RP core 1.3.1.0

112.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
------------	-------------	------------------



	None	
--	------	--



113 BIOS – KBL CRB v010

BIOS version	0.010		
BP common core revision	1.3.1.0		
RoyalPark core version	1.3.1.0		
Video Option ROM (VBIOS)	1029		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.7001v2(Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x50 G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150909_DEBUG_Rev_1.1.bin SKL_BIOSAC_20150909_PRODUCTION_Rev_1.1.bin	
	ACM (Boot Guard)	3376	



P4 Label	@ 294272 (2016_Kabylake)
----------	---------------------------------

113.1 Resolved Client BIOS HSD sightings

HSD#	Title
1504061129	Convert SiPolicy to config block
1706518412	[greenlow][Customer reported issue]: MrcMcAddress Decode/Encode functions getting ASSERT when used in PEI Phase
1206927535	Push from mpg_customer_enabling: System get hang up problem if set SGX is disabled and set IGD pre-allocated memory to 64MB
1404265400	[kaby_lake.other]Cannot change debug level using setup menu on Skylake_2015
1504060983	[kaby_lake.rvp3]Clean up EDK style GUID defines under SkylakeSiPkg
1207050227	Memory overflow in SmbiosMiscDxe driver
1504062524	Merge BP 1.3.1.0 core code to KBL stream
1206746721	Remove POST code displays from _Qxx EC interrupt methods
1304137459	[UniBIOS] Need to remove PcdUniBiosBuild==FALSE when PcdSvBuild==TRUE
1706519641	Integrate 2 SKL patches, for R0/D0 0x50
1404348258	SKL FSP: need to have clearly defined Post code (granularity) in FSP
1404217478	Enable Embedded build flag for kblake, Added SIO Nuvoton6776f support
1206755323	Implement FSP 2.0 without v1.1 compatibility (no FSP-c) - Part 5
1404221248	[BIOS Guard] [KBL] BIOS Guard Flash Wear Out Feature and PCH FPRR feature clean up
1304168270	Almost all values in platform information Menu are N/A



1304163762	[UniBios]Change IoRead(0x61) calls to MicrosecondDelay calls in NativeSmmLib.c
1404386588	BIOS must add Race To Halt setup option
1206955210	[MRC] Bdat Memory Hob pointer is zeroed out when SAGV is enabled
1206956761	Bdat Header doesn't report full size of Bdat Structure
1304118383	PEG/DMI Recipe Rev12 Update
1304077979	PTC Gen3 BIOS Test : Common Clock Test2 failure
1404331141	SKL DT/HALO - Control AFE_PM_TMR_0_0_0_DMIBAR.cstate_l1_timer depending on DMI Gen speed
1304159887	Add support for PCH-H QMS180 Add DID 0xA151 for SFF
1206187208	BIOS must update SKL EDRAM ratio implementation
1206927526	Push from mpg_customer_enabling: Skylake H core voltage mode issue
1206880627	(Merge from SKL fix) Push from mpg_customer_enabling: The 65W I5-6500 CPU's frequency cannot meet spec if core multi processing set t
1206721048	Set PS3 and PS4 as 'Enabled' by default in BIOS
1304066187	[SV-Bios] BIOS done hook\event
1304163667	[skylake.customer_platform][SKL MRC: WRDSUDT step is causing memory failures]
1304159927	[skylake.rvp15_sip]SKL MRC: MRS FSM is not programming DDR4 DQ Vref during SAGV transitions
1206584926	Push from mpg_customer_enabling: CMIT_TDC: The Integrated Video have no video output under OS when add-on graphics card is installed
1206858098	[SKL]Insufficient NVRAM resources - changing OS startup mode is removing boot options from BIOS boot manager
1206750288	kaby_lake.other]L"Boot%04x" (lower case) is used everywhere in Intel Source(both in Platform RC Code & Royal Park code
1504032768	Remove BoardId from PlatformPkg - phase1: gathering the BoardId check - for AcipPlatform driver



1206963567	The ZumbaBeach's CSM setting should be ALWAYS_ON
1504061857	V09 FSP_VS _Debug gets assert but V08 can not reproduce
1206957636	[SKL-SDS] Enable a BIOS IVCAM disable option that hides and power gates IVCAM
1404453636	USB Host Controller BIOS Guide Update to Disable USB2 HW LPM (rev 19)
1206927529	Push from mpg_customer_enabling: PCIE NVME remap link speed downgrades to Gen1 on S3 resume
1604024560	Provide Chipset Init Info Hob for FSP on SKL
1504061842	[KBL][V09 FSP_VS _Release no display and post code 1414 but V08 can not reproduce.]
1304161416	Platform hangs at PC 000d with CATERR
1404370696	De-feature SPT-LP Voltage Margining from CL275158
1304123294	[kaby_lake.other]PlatfromPkg Need to support EFI_SMM_CPU_SAVE_STATE_PROTOCOL (gEfiSmmCpuSaveStateProtocolGuid)
1304155641	[Setup] Amt Configuration Menu to be moved to PCH-FW Menu
1304147807	[KBL BIOS] Wrong help description for Manageability State in Bios setup
1504061590	[kaby_lake.other]PCH RC PREMEM to POSTMEM restructure in KBL
1604017655	[FSP] Move PcieRpEnable,PcieRpClkReqSupport, PcieRpClkReqNumber to post mem
1206916532	[kaby_lake.rvp7]KBL - PO: SVBIOS is not loading MicrocodePatch correctly
1206950193	Integrate 2 SKL patches, for R0/D0 0x4C
1206574738	: [SPT-H] BIOS changes for DMI 70us L1 exit Latency
1304151756	Fix CATERR after second S3 with storage remap in some configurations
1304141080	PCIe security lock bit PCD.SRL is not set in some cases



1304137627	PCIe Gen3 hot-plug requires change in HWEQ initialization
1206828911	When NVMe remapping is enabled the X1 PCIe SD Card Reader is no longer visible in the system
1304154067	Device IOTR is causing BSOD during Windows 7 Debug CHK Installation

113.2 BP Client Common Core Sync-up Changes

Updated RP core 1.3.1.0

113.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



114 BIOS – KBL CRB v009

BIOS version	0.009		
BP common core revision	1.2.2.1		
RoyalPark core version	BP1.2.2.1_RP01		
Video Option ROM (VBIOS)	1029		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.7001v2(Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x4A G0 : 0x6		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150909_DEBUG_Rev_1.1.bin SKL_BIOSAC_20150909_PRODUCTION_Rev_1.1.bin	
	ACM (Boot Guard)	3376	



P4 Label	@289251 (2016_Kabylake)
----------	-------------------------

114.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206935819	Integrate KBL patch: G0 0x06
1205656678	[client_platf][KabyLake] Move Bios ACM module location outside reference code
1304160506	[PCH BIOS CI] Can't enter to EFI Shell
1404442230	[BIOS Guard] [KBL] Update BIOS Guard Update Package generation for KBL
1304158709	[SVBIOS] PSMI support
1304153709	Win8.1 installer hangs if remapping is enabled
1206679038	[kaby_lake.other]Vulnerable the shell internal Argc/Argv process
1304156584	[KBL FSP] Platform Information doesn't display FW version properly .
1206535343	Push from mpg_customer_enabling: PSF programming in case of SMBUS disable
1604002066	ConfigureSerialIoAtS3Resume call in FSP on skylake is problematic
1206340635	Rename PciClockRun policy to LpcClockRun
1504032768	[KBL] Remove BoardId from PlatformPkg - phase1: gathering the BoardId check - PEI PreMem Phase 2 & PostMem
1604025695	Macros to be used in the dsc file
1404379519	Update PCIe Credit Values based on SKU/PCIe controllers enabled
1404356566	Clean up for PlatformPowerLimit programming



1404144519	[skylake]SKL BIOS: Add TPM2 provisioning support
1404373272	SPT - Sx/PTT customer issue workaround - Disable PSTH clock trunk gating during POST
1404308237	When TPM2_Startup(State) fails, BIOS incorrectly handling the failure path
1206905402	Sync up Kabylake's core to Royal Park 1.2.2.1 release
1206917758	[MRC] Feedback from Apple - Cleanup Debug Message in EvLoaderPeim
1304156973	[PPV]GuidForward PEI/DXE/SMM should be controlled by setup option
1404351885	SKL-PCH LAN Controller setup option
1404439076 [Reverted]	[BIOS Guard] [KBL] Integrate BIOS Guard PO module

114.2 BP Client Common Core Sync-up Changes

None

114.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



115 BIOS – KBL CRB v008

BIOS version	0.008		
BP common core revision	1.2.2.1		
RoyalPark core version	BP1.2.2.1_RP01		
Video Option ROM (VBIOS)	1029		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.7001v2(Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x4A G0 : 0x4		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150909_DEBUG_Rev_1.1.bin SKL_BIOSAC_20150909_PRODUCTION_Rev_1.1.bin	
	ACM (Boot Guard)	3376	



P4 Label	@287634 (2016_Kabylake)
----------	-------------------------

115.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206906072	Decouple SMBIOS processor table generation (types 4 and 7) from Silicon Initialization code.
1206912312	Adding Link Time Optimization (LTO) to Kabylake
1206638931	SLP_S0 is not achieved after 20-30 CS Cycles
1206912105	KBL MiniBIOS not recognizing device ID
1304125452	[KBL FSP] Platform boot without any display with FSP BIOS
1604017657	SKL FSP: Move EnableLan and CIO2 Enable to post-mem
1304141448	FlexCon support
1206907822	[KBL - U PO] - Bios Settings For Enabling Connected Standby not applicable on KBL RVP
1206874104	Move IntelFspPkg overrides from <Si>FspPkg to ClientSiliconPkg - Part 2
1206755323	Implement FSP 2.0 without v1.1 compatibility (no FSP-c) - Part 3
1206704179	Push from mpg_customer_enabling: XMP profile issue of SODIMM on skylake-H
1206908593	Push from mpg_customer_enabling: [Acer Brownie][IEP] SD card is not removable device with Intel embedded SD Card reader
1604024379	Use Adapter Power State notification for display turn on notification
1604022612	Adding support for the Cdynmax Clamping Feature for the GT4 Halo (4+4e) parts (lccp Feature)
1206874104	Move IntelFspPkg overrides from <Si>FspPkg to ClientSiliconPkg



1206857070	Investigate duplicate UUID issue
1206834896	Update firmware defaults to enable serial debugging
1503950800	Request to add debug messages in SKL FSP supported BIOS builds.
1206673515	[SKL-SDS][DCL] Keyboard backlit LEDs flash regularly at specific intervals while system in CS
1404382617	skylake FSP: remove FSP 1.0 compatibility support
1404366359	USB Host Controller BIOS Guide Update (rev 18)
1503950800	Request to add debug messages in SKL FSP supported BIOS builds.
1206744599	Entering wrong password in BIOS causes SUT to freeze
1304145480	[Due to decision of dropping KBL-PCH-H in Kabylake any KBP/CNP support needs to be cleaned.
1604004818	Move HSIO , USB Phy settings into Post-mem
1504050165	Security gaps in relation to Intel AMT USB provision feature.
1206407014	Push from mpg_customer_enabling: Request to make thermal events / HWP SCI envets and each notify conditionally in _L62 - merge from SKL
1206776106	Deep Cstate latency control MSRs only restored on ULT systems - merge from SKL
1404412887	HWP must be renamed to Intel Speed Shift. - merge from SKL
1304120750	SKL Demotion/Promotion algorithm enabling by default - merge from SKL.
1206863332	Customer reports SMBIOS socket max speed error in SMBIOS data - merge from SKL
1206869536	Need to add GPIO config and platform ID checks for Grizzly Mountain IDV



115.2 BP Client Common Core Sync-up Changes

None

115.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



116 BIOS – KBL CRB v007

BIOS version	0.007		
BP common core revision	1.2.2.1		
RoyalPark core version	BP1.2.2.1_RP01		
Video Option ROM (VBIOS)	1029		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.7001v2(Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x4A G0 : 0x4		
Mphy Revision	PCH-H Bx:0x3E PCH-H Dx:0x31 PCH-LP Bx:0x3E PCH-LP Cx:0x31		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150909_DEBUG_Rev_1.1.bin SKL_BIOSAC_20150909_PRODUCTION_Rev_1.1.bin	
	ACM (Boot Guard)	3376	



P4 Label	@284414 (2016_Kabylake)
----------	-------------------------

116.1 Resolved Client BIOS HSD sightings

HSD#	Title
1304152526	User password is not being bypassed during Remote Secure Erase flows
1304152129	[KBL]Integrate CRB CSME FW 11.5.0.7001v2 into BIOS
1504029013	SKL-H platforms that do not use PCIe lanes from the processor ? set FCLK to 800 MHz.
1206772321	[Utilize PackageDocumentTool for SiPkgApi documentation] Part II
1206883059	[Integrate 2 SKL patches, for R0/D0 0x4A]
1504035818	Sync up Skylake core with BP 1.2.2.1 release
1404405200	[SGX] With SGX Fuse off, EPC_BIOS and EPC_OS variables are not getting deleted
1304148985	More detailed descriptions are required in GPIO library headers
1304066187	[SV-Bios] BIOS done hook\event
1504032768	[KBL] Remove BoardId from PlatformPkg - phase1: gathering the BoardId check
1404412781	Occasional 2 second pause during AP startup on SKL
1304137932	TBT BIOS: AR PCIE Switch Flow Control issue workaround
1206866805	[FSP] Need to add doxygen style of comments for UPD and VPD in FspUpdVpd.h - Part 2
1206866805	[FSP] Need to add doxygen style of comments for UPD and VPD in FspUpdVpd.h
1206787481	Push from mpg_customer_enabling: System hang after modify PCI B00:D1F:F00 Reg0xDC, bit0 from 0 to 1



1504015520	Having boot loader initialize console and keeping FSP in sync
1604017653	SKL FSP: Move SataMode and Enable Sata to post mem
1303985489	BIOS doesn't direct chosen Aggressive Slumber / Partial value to OS.
1206856571	Update Royal Park internal documentation and version number for BP1221_RP1
1206107307	BIOS: Remove _S0W methods from RTD3 SSDT code to allow devices to enter low power states with BIOS RTD3 disabled

116.2 BP Client Common Core Sync-up Changes

None

116.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



117 BIOS – KBL CRB v006

BIOS version	0.006		
BP common core revision	1.2.2.1		
RoyalPark core version	BP1.2.2.1_RP01		
Video Option ROM (VBIOS)	1029		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.7000(Consumer)		
5MB ME Firmware SKU	N.A		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x42 G0 : 0x4		
Mphy Revision	A5		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150909_DEBUG_Rev_1.1.bin SKL_BIOSAC_20150909_PRODUCTION_Rev_1.1.bin	
	ACM (Boot Guard)	3376	
P4 Label	@282027 (2016_Kabylake)		



117.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206772321	Utilize PackageDocumentTool for SiPkgApi documentation - Part I
1206855557	[skylake]Integrate TXT BIOS ACM version 1.1
1304136858	BIOSLastStatus isn't updated after performing Secure Erase flow
1404393294	Correct the POTSCXUSB3 offset in PCH RC code
1304133792	Support wake from SD card events while host controller in D3 [GPP D10]
1206848775	Integrate 2 SKL patches, for R0/D0 0x42
1206755323	Implement FSP 2.0 without v1.1 compatibility (no FSP-c)
1604018796	NHLT SSP blob for I2S mode on SKL for ALC286S codec
1504035818	Sync up Skylake core with BP 1.2.2.1 release
1603986928	[Platform-CI-WW28.1]: USB3.0 detects as USB2.0 after deep S3
1304123445	SSPE must not be set for USB3 ports disabled with PDO (USB Host Controller BIOS Guide Update rev 18)
1404386375	Skylake FSP: addressing feedback comments on fsp v1.3.0 and v1.5.0
1304139800	[KBL]Integrate CRB CSME FW 11.5.0.7000 into BIOS
1503982083	KBL G0 PO Microcode Integration
1504042773	Change Boot order][RVP11] Change Boot order fail. Back out CL277195 [1604001532][KBL][debug]All RVP system all got a fail message when saving boot order change
1206753243	Push from mpg_customer_enabling: POST time / S3 resume time of Q150/H110 spends additional 800ms than Q170



1304054236	RTD3 RVP board support incomplete/incorrect
1604004294	KBL Security: Error "ERR_BAD_SVN (0X9)" observed while flashing KBL BGUP
1206207397	SKI_SDS: When BIOS Guard is on, Capsule update is not successful
1404390388	[skylake]when MOR is set, next boot MRC does full training instead of just clearing memory adding boot delay

117.2 BP Client Common Core Sync-up Changes

None

117.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



118 BIOS – KBL CRB v005

BIOS version	0.005		
BP common core revision	1.2.2.0		
RoyalPark core version	BP1.2.2.0_RP03		
Video Option ROM (VBIOS)	1029		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.1000(Consumer)		
5MB ME Firmware SKU	11.5.0.1000(Corporate)		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x3C		
Mphy Revision	A5		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150713_DEBUG_Rev_1.00_RC2.bin SKL_BIOSAC_20150713_PRODUCTION_Rev_1.00_RC2.bin	
	ACM (Boot Guard)	3376	
P4 Label	@279164 (2016_Kabylake)		



118.1 Resolved Client BIOS HSD sightings

HSD#	Title
1404386375	SKL FSP: addressing feedback comments on fsp v1.3.0 and v1.5.0
1304121270	[skylake.rvp10][SVBIOS] Creating a PlatformConfig.xml is causing an "unknow opcode" exception in BIOS
1604017497	SKL/KBL - Integrate latest VBIOS 1029
1206772050	Push from mpg_customer_enabling: Clear/Set HSIO_TX_DWORD19 Bit[1] after change to ModPHY register in USB 3.0 Tuning
1304135628	ME RC Cleanup
1404386375	[Skylake FSP: addressing feedback comments on fsp v1.3.0 and v1.5.0] SA Part
1304137429	[SVBIOS] Need to fix CLI reset using PchResetPpi
1304137459	[UniBIOS] Need to remove PcdUniBiosBuild==FALSE when PcdSvBuild==TRUE
1303968310	[CPUSV] Need to remove all SV_HOOKS from HFR/VFR files
1404386375	Skylake FSP: addressing feedback comments on fsp v1.3.0 and v1.5.0
1604015164	[kaby_lake.other][KBL] Provide support of the KBL SA/GT DIDs
1604003442	SKL FSP: Build Failures when using BuildFv.sh
1604009313	[skylake]DISB bit setting resetting clearing out write 1 to clear bits
1206680255	[SKL] Add SMBIOS Type 4 Processor Family values for Core m3, m5, m7
1206743531	[SKL-SDS] Enable PS3 & PS4 By Default
1404310558	SPT PCIe: Controller does not power gate when Hot plug and RTD3 is enabled
1404385776	BIOS should not set PWRMBASE + 0x30C [6] (CSME LTR Ignore)



1604001532	[KBL][debug]All RVP system all got a fail message when saving boot order change
1304134714	Zephyr support. need to save XML when generating SPI image

118.2 BP Client Common Core Sync-up Changes

None

118.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



119 BIOS – KBL CRB v004

BIOS version	0.004		
BP common core revision	1.2.2.0		
RoyalPark core version	BP1.2.2.0_RP03		
Video Option ROM (VBIOS)	1028		
GOP Driver	9.0.1035		
1.5MB ME Firmware SKU	11.5.0.1000(Consumer)		
5MB ME Firmware SKU	11.5.0.1000(Corporate)		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x3C		
Mphy Revision	A5		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150713_DEBUG_Rev_1.00_RC2.bin SKL_BIOSAC_20150713_PRODUCTION_Rev_1.00_RC2.bin	
	ACM (Boot Guard)	3376	
P4 Label	@277034 (2016_Kabylake)		



119.1 Resolved Client BIOS HSD sightings

HSDES#	Title
1304125244	SKL cAVS: Add mono microphone support (NHLT)
1304130839	PMC register cleanup for Kabylake project
1303968310	[CPUSV] Need to remove all SV_HOOKS from HFR/VFR files
1604000181	Cleanup trailing whitespaces in the FSP and SI Pkg files
1404305017	[IntelFspPkg] Fixing PatchFv.py per customer feedback
1404174911	HecigetIccProfile needs to be updated to the SPT definition
1206623563	Push from mpg_customer_enabling: [SkyLake-H] Power Limit 1 timewindow
1404319339	[IOTG] i5-6500TE cannot go turbo in Linux and Windows using default BIOS setup
1304030133	[kaby_lake.other]WRDD - Add SAR BIOS Control & SAR Limits
1304117954	[skylake.rvp3]Deprecated bios option: LAN PHY Drives LAN_WAKE#
1604003899	SKL Y LPDDR3 RVP3 board to support 1866 and 1600 memory frequency. Same board will be used for KBL PO
1205580536	SKL Security: UEFI Secure Boot enablement fails, bios not allowing PK certificate enrollment
1206744422	Rename ClientSiPkg to ClientSiliconPkg
1404354951	W/a for the mphy Power gating issue for pcie owned lanes
1206645456	Add Doxygen documentation for any POST codes related to Platform Technologies
1206756660	Integrate 2 SKL patches, for R0/D0 0x3C
1206750264	Add support for DEC "UserExtensions" section



1604008428	SKL - Integrate latest GOP 9.0.1035
1404360041	SKL FSP: remove GPIO configuration from FSP and leave that completely to bootloader
1205616521	[SKL-SDS] BIOS Implementation needed to report NVME Drive Information
1504000049	[SKL BKC][SKL_Resp] Unable to meet Standby responsiveness metric because of ACPI compliant
1604005648	IntelGraphicsPeim driver should not be called during S3 Resume
RollBack: 1206107307	BIOS: Remove _S0W methods from RTD3 SSDT code to allow devices to enter low power states with BIOS RTD3 disabled
1404349957	[SkI]RTC customized space in Intel RC
1404346720	SKL FSP - Feedback on FSP 1.3.0
1206618408	Implement Initial draft of FSP 2.0

119.2 BP Client Common Core Sync-up Changes

None

119.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



120 BIOS – KBL CRB v003

BIOS version	0.003		
BP common core revision	1.2.2.0		
RoyalPark core version	BP1.2.2.0_RP03		
Video Option ROM (VBIOS)	1028		
GOP Driver	9.0.1034		
1.5MB ME Firmware SKU	11.5.0.1000(Consumer)		
5MB ME Firmware SKU	11.5.0.1000(Corporate)		
RST RAID OROM	14.9.0.2287		
MEBx	11.5.0.1000		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	M0: 0x2E R0/D0: 0x38		
Mphy Revision	A5		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150713_DEBUG_Rev_1.00_RC2.bin SKL_BIOSAC_20150713_PRODUCTION_Rev_1.00_RC2.bin	
	ACM (Boot Guard)	3376	
P4 Label	@273931 (2016_Kabylake)		



120.1 Resolved Client BIOS HSD sightings

HSD#	Title
1206618408	Implement Initial draft of FSP 2.0 - Part 6
1604001532	[skylake.rvp3][KBL][debug]All RVP system all got a fail message when saving boot order change.
1206623556	Push from mpg_customer_enabling: Request to move the Display Audio Verbtale installation point to other Audio VerbTables
1404222758	[USRT] SMM Vulnerability in SkylakePlatSamplePkg: Verify SPI MMIO is in SMRAM space
1304125244	SKL cAVS: Add mono microphone support (NHLT)
1206107307	BIOS: Remove _S0W methods from RTD3 SSDT code to allow devices to enter low power states with BIOS RTD3 disabled
1504034752	[skylake]Update AcpiExec to support name space analysis only.
1206659961	PCD/policy settings scrub for skylake ref code
1206376997	[SKL][MRC] Implement MMA in FSP to support SKL-based chromebook platforms
1206415313	Deprecate the usage of IntelFrameworkPkg and IntelFrameworkModulePkg and reduce the package dependencies
1304074422	Enhance TBT ASPM configuration from ASPM menu - add L1 only and L0s only
1604004899	SKL - Integrate latest GOP 9.0.1034 and VBIOS 1028
1304103457	[UniBIOS][KBL SvModule PEI support
1304125847	[kaby_lake.vp][SVBios/UniBios]Put SvLt in FV.FVVALIDATION_COMPACT
2503749	[SKL DCN] Remove dependency on IntelFramework(Module)Pkg interfaces: use gEfiSmmCpuProtocol to access CPU SMM state instead of direct memory access, and relocate definition of gEfiCapsuleGuid
1206736716	Integrate SKL patch: R0 0x3A



1304125312	[PCH BIOS CI] Can't enable BIOS Setup redirection
1206727659	Promote PiSmmCore.inf, PiSmmIpl.inf, and HiiDatabaseDxe.inf generic override from PLATFORM to ClientCommonPkg
1206721085	[SKL][MRC] Add VrefAdjust1 to MrcSsaPopulateHostData to support Fastboot MMA testing for LPDDR3
1404351515	USB ports are not properly enable/disable in setup followed by Power Button shutdown/reset
1504032159	[skylake][SKL CPU] Klocwork bitwise operation have different size issue
1206715992	[kaby_lake.other]Change MRC from TickTock Model for CPU Family to properly differentiate specific changes
1206718225	[ClientSi] Remove offset table in config block library
1206722868	[PPV] boot menu should remove shell entry if shell not installed
1303999952	TBT BIOS: AIC Support for AR
1404346720	Feedback on FSP 1.3.0
1206686867	[skylake]Some of the PCI device registers are not getting saved/restored during S3
1206721643	Integrate 3 SKL patches, for M0 0x2E and R0/D0 0x38
1205947584	[UniBIOS] Need to move PCHSV PEIMs and DXE drivers into Validation FV
1706498532	[greenlow]MrcMcAddress Decode/Encode functions used with ECC Error handling don't work
1206686493	[SKL][MRC] Fixes for Bios SSA
1304067901	During RSE flow - no way to enter SSD password locally
1206666622	SecureErase takes around 1.4sec during DXE Phase
1504026311	[kaby_lake.vp][KBL PCH] Update to Config Block for PCH policy
1404228637	FCE tool (Platform support) optimization to save large amounts of build time



1404222140	[USRT] SMM Vulnerability in SkylakePlatSamplePkg: SmramSaveInfoHandler
1404347068	SKL BIOS : SUT fails to boot with SATA FVME image on RVP 8 & 10 Boards
1206207397	[SKL-SDS]: When BIOS Guard is on, Capsule update is not successful
1404339595	[skylake.rvp3][SKL]V95.RVP3_Release : Fix potentially uninitialized variable usage and enforce it moving forward
1206716452	[PPV][Refactoring] change PcdPpvEnable to PcdPpvEnforcement
1206707430	[KBL][SVBIOS]Merge SvCommonExtLib with SvCommonLib and remove SvCommonExtLib
1206632875	[Catch up Royal Park stream, then merge to KBL]
1206627831	Push from mpg_customer_enabling: PCIe devices disappear on all systems that the HSIO configuration registers are tuned
1304108062	InstallEfiMemory is adding two empty blocks into ResourceDescriptorHob
1304091982	Delete dead code from PciExpressHelpersLib
1206660457	Push from sunrise_point: Unexpected completion error was seen on nVidia GeForce GTX670 Gfx card while running Gen 3 benchmark traffics in Win 8.1" from SKL
1404338874	USB Host Controller BIOS Guide Update
1304121102	[KBL]Integrate CRB CSME FW 11.5.0.1000 & 12.0.0.7006 into BIOS
1304115480	ME RC Cleanup part 2
1205664324	BIOS exposes EPD FW and STM32 FW
1604000068	Adding KBL U DDR3L RVP7 Platform Changes to KBL Stream



120.2 BP Client Common Core Sync-up Changes

None

120.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



121 BIOS – KBL CRB v002

BIOS version	0.002		
BP common core revision	1.2.2.0		
RoyalPark core version	BP1.2.2.0_RP03		
Video Option ROM (VBIOS)	1027		
GOP Driver	9.0.1033		
1.5MB ME Firmware SKU	11.5.0.1000(Consumer)		
5MB ME Firmware SKU	11.5.0.1000(Corporate)		
RST RAID OROM	14.9.0.2287		
MEBx	11.0.0.0005		
PXE OROM	1.3.21		
UEFI UNDI Driver	-		
Microcode Update –	34		
Mphy Revision	A5		
Reference code version	Reference Code		Version
	RC Version		TBD
	MRC Version		TBD
	BIOS Guard(PFAT)	1.1.0 (2.0. 20150625)	
	ACM (TXT)	SKL_BIOSAC_20150713_DEBUG_Rev_1.00_RC2.bin SKL_BIOSAC_20150713_PRODUCTION_Rev_1.00_RC2.bin	
	ACM (Boot Guard)	3376	
P4 Label	@270966 (2016_Kabylake)		



121.1 Resolved Client BIOS HSD sightings

HSDES#	Title
[1206415313]	Deprecate the usage of IntelFrameworkPkg and IntelFramework
[1206705708]	FSP: Add BSF option into FspUpdVpd.h and FspUpdVpdInternal.
[1206707430]	[KBL][SVBIOS]Merge SvCommonExtLib with SvCommonLib and remo
[1304119396]	ABASE and PWRMBASE needs to be added to PchNVS for ACPI usa
[1604000068]	Adding KBL U DDR3L RVP7 Platform Changes to KBL Stream
[1404246519]	Google requested to USB phy settings to UPD for platform co
[1206702245]	[KBL][SVBIOS]Replace PLATFORM_CONTEXT with CPUSV_PEI_CONTEX
[1206632875]	Catch up Royal Park stream, then merge to KBL
[1206679741]	[PPV] Marvell boot default to use UEFI mode
[1504021466]	[ClientSi] Remove padding in AddConfigBlock()
[1304100952]	For KBL PCH temporary change DRAM Init Done message flow an
[1206701951]	[KBL][SVBIOS]Move All dynamic allocations to CpuSvPeiContext
[1604000181]	Cleanup trailing whitespaces in the FSP and SI Pkg files
[1603998078]	[skylake] SKL - Integrate latest GOP 9.0.1033 and VBIOS 102
[1404339595]	[skylake.rvp3][SKL]V95.RVP3_Release : Fix potentially unin
[1304053213]	Hii Data Export in SmiVariableInstallInt15 should go under
[1205947584]	[UniBIOS] Need to move PCHSV PEIMs and DXE drivers into Val



[1206613963]	MOR Memory clean bit handling on Capsule Update
[1206684538]	Remove SmiVariable subfunction from Royal Park 1.3
[1404331317]	HSTI optimization platform driver is not present in SKL/KBL
[1206639580]	When FlashProtectionEnabled is enabled, the capsule update
[1206680255]	[SKL] Add SMBIOS Type 4 Processor Family values for Core m3
[1504027463]	Removal of BIOS workaournd and transition to UEFI Opal driv
[1504008327]	[FSP]Fix FSP wrapper doesn't boot and assert happened on RV
[1206584926]	[skylake]Push from mpg_customer_enabling: CMIT_TDC: The Int
[1603999758]	[kaby_lake.other][KBL]All RVP system's S3 resume fail with
[1603997096]	KBL S UDIMM RVP need "CPV" board ID assigned and supported
[1206684442]	[skylake]Fix for the Monitor/Mwait c-states hint calculatio
[1304090117]	ASF table: Reported table size is larger than actual table

121.2 BP Client Common Core Sync-up Changes

None

121.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	



122 BIOS – KBL CRB v001

BIOS version	0.001		
BP common core revision	1.2.2.0		
RoyalPark core version	BP1.2.2.0_RP03		
Video Option ROM (VBIOS) GOP Driver			
1.5MB ME Firmware SKU 5MB ME Firmware SKU			
RST RAID OROM			
MEBx			
PXE OROM			
UEFI UNDI Driver			
Microcode Update			
Mphy Revision			
Reference code version	Reference Code	Version	
	RC Version	TBD	
	MRC Version	TBD	
	BIOS Guard(PFAT)		
	ACM (TXT)		
	ACM (Boot Guard)		
P4 Label	@268684 (2016_KabyLake)		



122.1 Resolved Client BIOS HSD sightings

Sighting#	Title
N.A	Initial source base (Based on SKL BIOS v92)
Refer P4 submitted changelist	Sync from SKL & CNL folders upto @ 268684 (2016_KabyLake)

122.2 BP Client Common Core Sync-up Changes

None

122.3 Known Issues / Limitations

Sighting #	Description	how_to_reproduce
	None	