

Quantum[®]

Scalar i6000, i3 & i6/i6H

RESTful Web Services API

6-68185-02, Rev. J

Quantum Scalar i6000, i3 & i6/i6H RESTful Web Services API, 6-68185-02 Rev J, March 2021, Product of USA.

Quantum Corporation provides this publication “as is” without representation or warranty of any kind, either express or implied, regarding the accuracy of the information, including but not limited to the implied warranties of merchantability or fitness for a particular purpose.. Reliance and use of the information presented in this document is at the sole risk of the user, Quantum makes no commitment to update or keep current the information in this document. Quantum Corporation may revise this publication from time to time without notice.

COPYRIGHT STATEMENT

© 2015-2021 Quantum Corporation. All rights reserved.

Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law.

TRADEMARK STATEMENT

Quantum, the Quantum logo and Scalar, are registered trademarks of Quantum Corporation and its affiliates in the United States and/or other countries. Products mentioned herein are for identification purposes only and may be registered trademarks or trademarks of their respective companies. All other brand names or trademarks are the property of their respective owners.

Quantum specifications contain information and technology developed by Quantum Corporation, that are protected by patent and copyright laws in the US and worldwide. Quantum specifications are subject to change without notice.

Scalar i6000, i3 & i6/i6H RESTful Web Services Application Programming Interface

Table of Contents

Scalar i6000, i3 & i6/i6H RESTful Web Services	3
Application Programming Interface	3
1. Introduction	25
1.1 General.....	25
1.2 Addressable Resources	25
1.3 Representation-Oriented Resources	25
1.4 Uniformed, Constrained Request Interfaces.....	25
2. Request and Response Interface Description	27
2.1 General.....	27
2.2 URI Examples	27
2.3 Web Services Request Examples.....	27
2.4 Web Services Response Code Objects.....	28
2.4.1 Response Codes.....	29
2.5 Cookies	31
2.6 Cache Controls	31
3. Web Services Application Programming Interface	32
3.1 Resource Tables.....	32
3.1.1 Table Entry Explanations	32
3.1.1.1 URI.....	32
3.1.1.2 Method	32
3.1.1.3 User Role Access.....	32
3.1.1.4 Version	33
3.1.1.5 Request/Response Header.....	33
3.1.1.5.1 Accept	33
3.1.1.5.2 Content-Type/Media Type.....	33
3.1.1.5.3 Location.....	34
3.1.1.5.4 Content-Disposition.....	34
3.1.1.6 Parameters.....	34
3.1.1.7 Version	35
3.1.1.8 Response Code	35
3.1.1.9 Request Data	35

3.1.1.10	Response Data.....	35
4.	Library Resources	36
4.1	Overview.....	36
4.2	Login Considerations.....	36
4.3	Access Groups, host, drive and partition access.	37
4.4	Partition Resource Assignments	37
4.5	Partition Control Path Configuration.....	37
4.6	Drive Data Path Configuration	38
4.7	Extended Data LifeCycle Management.....	38
4.8	Partition Configuration and Operations	39
4.9	Drive Cleaning Policies	39
4.10	IPv6 Network Configuration.....	40
5.	Web Services API Request Summary	42
6.	Resource Objects.....	272
7.	WSResultCode Custom Codes.....	333
8.	Appendix A – Web Service Request Examples	342
8.1	Linux Curl Script Example	342
8.2	Windows PowerShell Script Example	347
9.	Appendix B – Change History	356
9.1	Overview of Changes for revision F	356
9.1.1	Overall documentation differences to previous document revision E:	356
9.1.2	Specific Changes:.....	356
9.2	Overview of Changes for revision G	357
9.2.1	Overall documentation differences to previous document revision F:	357
9.2.2	Specific Changes:.....	357
9.3	Overview of Changes for revision H.....	358
9.3.1	Overall documentation differences to previous document revision G:.....	358
9.3.2	Specific Changes:.....	358
9.4	Overview of Changes for revision J	359
9.4.1	Overall documentation differences to previous document revision H:	359

Table of Web Service Interfaces

Table 1:	GET aml/	42
Table 2:	GET aml/access/devices.....	42
Table 3:	GET aml/access/groups.....	42
Table 4:	GET aml/access/group/{name}	43

Table 5: POST aml/access/group/{name}.....	43
Table 6: DELETE aml/access/group/{name}	44
Table 7: POST aml/access/group/{name}/device	44
Table 8: PUT aml/access/group/{name}/device.....	45
Table 9: DELETE aml/access/group/{name}/device/{serialNumber}	45
Table 10: GET aml/access/group/{name}/devices.....	46
Table 11: POST aml/access/group/{name}/devices	46
Table 12: POST aml/access/group/{name}/hosts.....	46
Table 13: DELETE aml/access/group/{name}/host/{WWPN}	47
Table 14: GET aml/access/host/{WWPN}.....	47
Table 15: PUT aml/access/host/{WWPN}.....	48
Table 16: DELETE aml/access/host/{WWPN}.....	48
Table 17: GET aml/access/hosts	48
Table 18: POST aml/access/hosts.....	49
Table 19: GET aml/access/licenses.....	49
Table 20: PUT aml/access/licenses.....	49
Table 21: GET aml/access/license/{serialNumber}	50
Table 22: POST aml/access/license/{serialNumber}	51
Table 23: DELETE aml/access/license/{serialNumber}.....	51
Table 24: GET aml/device/settings/robot.....	51
Table 25: PUT aml/device/settings/robot.....	52
Table 26: GET aml/devices/blades	52
Table 27: GET aml/devices/blades/ethernet.....	53
Table 28: GET aml/devices/blade/ethernet/{serialNumber}.....	53
Table 29: GET aml/devices/blade/ethernet/{serialNumber}/operations/identify	53
Table 30: POST aml/devices/blade/ethernet/{serialNumber}/operations/identify.....	54
Table 31: DELETE aml/devices/blade/ethernet/{serialNumber}/operations/ identify	54
Table 32: GET aml/devices/blade/ethernet/{serialNumber}/operations/powerCycle.....	54
Table 33: POST aml/devices/blade/ethernet/{serialNumber}/operations/powerCycle	55
Table 34: GET aml/devices/blades/fibreChannel	55
Table 35: GET aml/devices/blades/fibreChannel/hosts.....	56
Table 36: GET aml/devices/blades/fibreChannel/hpf	56
Table 37: GET aml/devices/blade/fibreChannel/{serialNumber}	56
Table 38: GET aml/devices/blade/fibreChannel/{serialNumber}/hosts.....	57
Table 39: POST aml/devices/blade/fibreChannel/{serialNumber}/hosts	57

Table 40: GET aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}	58
Table 41: PUT aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}	58
Table 42: DELETE aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}	59
Table 43: GET aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}/mapping	59
Table 44: PUT aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}/mapping	60
Table 45: GET aml/devices/blade/fibreChannel/{serialNumber}/hpf	61
Table 46: PUT aml/devices/blade/fibreChannel/{serialNumber}/hpf	61
Table 47: PUT aml/devices/blade/fibreChannel/{serialNumber}/hpf/intervention	62
Table 48: GET aml/devices/blade/fibreChannel/{serialNumber}/operations/identify	62
Table 49: POST aml/devices/blade/fibreChannel/{serialNumber}/operations/identify	63
Table 50: DELETE aml/devices/blade/fibreChannel/{serialNumber}/operations/identify	63
Table 51: GET aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle	63
Table 52: POST aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle	64
Table 53: GET aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot	64
Table 54: POST aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot	64
Table 55: POST aml/devices/blade/fibreChannel/{serialNumber}/port/{id}/operations/reset	65
Table 56: GET aml/devices/blade/fibreChannel/{serialNumber}/ports	65
Table 57: PUT aml/devices/blade/fibreChannel/{serialNumber}/ports	66
Table 58: GET aml/devices/blade/fibreChannel/{serialNumber}/zoning	66
Table 59: PUT aml/devices/blade/fibreChannel/{serialNumber}/zoning	67
Table 60: GET aml/devices/blades/firmware	68
Table 61: POST aml/devices/blades/firmware	68
Table 62: GET aml/devices/blades/library	69
Table 63: GET aml/devices/blade/library/{serialNumber}	69
Table 64: GET aml/devices/blades/ltfs	69
Table 65: GET aml/devices/blade/ltfs/{sectionNumber}	70
Table 66: DELETE aml/devices/blade/ltfs/{sectionNumber}	70
Table 67: GET aml/devices/blades/windows	70
Table 68: GET aml/devices/blade/windows/{sectionNumber}	71
Table 69: DELETE aml/devices/blade/windows/{sectionNumber}	71
Table 70: GET aml/devices/ieStations	71
Table 71: GET aml/devices/ieStation/{number}	72
Table 72: GET aml/devices/ieStation/{number}/lock	72
Table 73: PUT aml/devices/ieStation/{number}/lock	72
Table 74: GET aml/devices/magazines	73

Table 75: PUT aml/devices/magazines	73
Table 76: GET aml/devices/magazines/ieSlots	74
Table 77: PUT aml/devices/magazines/ieSlots	74
Table 78: POST aml/devices/magazines/eject	75
Table 79: POST aml/devices/magazines/ieAssign	75
Table 80: POST aml/devices/magazine/eject	75
Table 81: PUT aml/devices/magazines/release	76
Table 82: GET aml/devices/robots	76
Table 83: GET aml/devices/robots/enable	77
Table 84: POST aml/devices/robots/enable	77
Table 85: GET aml/devices/robot/{name}	77
Table 86: GET aml/devices/robot/{name}/state	78
Table 87: PUT aml/devices/robot/{name}/state	78
Table 88: POST aml/devices/robot/{name}/park	78
Table 89: GET aml/devices/towers	79
Table 90: GET aml/devices/tower/{id}	79
Table 91: POST aml/devices/tower/{id}/identify	79
Table 92: GET aml/devices/tower/{id}/mode	80
Table 93: PUT aml/devices/tower/{id}/mode	80
Table 94: POST aml/devices/tower/{id}/reset	80
Table 95: GET aml/devices/tower/{id}/state	81
Table 96: PUT aml/devices/tower/{id}/state	81
Table 97: GET aml/devices/usb	82
Table 98: POST aml/devices/usb	82
Table 99: DELETE aml/devices/usb	82
Table 100: POST aml/devices/usb/backup	83
Table 101: POST aml/devices/usb/restore	83
Table 102: POST aml/devices/usb/erase	83
Table 103: POST aml/devices/usb/pause	84
Table 104: POST aml/devices/usb/resume	84
Table 105: POST aml/devices/usb/eject	84
Table 106: GET aml/drives	85
Table 107: DELETE aml/drives/firmware/image/{name}	85
Table 108: GET aml/drives/firmware/images	86
Table 109: POST aml/drives/firmware/images	86

Table 110: GET aml/drives/firmware/operations/update.....	86
Table 111: POST aml/drives/firmware/operations/update	87
Table 112: GET aml/drives/logs.....	87
Table 113: GET aml/drives/log/{name}	88
Table 114: DELETE aml/drives/log/{name}.....	88
Table 115: POST aml/drives/log/{name}/email	89
Table 116: GET aml/drives/ports	89
Table 117: POST aml/drives/powerCycle	89
Table 118: GET aml/drives/reports/activity	90
Table 119: GET aml/drives/reports/activity/details.....	90
Table 120: GET aml/drives/reports/cleaning.....	91
Table 121: POST aml/drives/reports/cleaning/email.....	92
Table 122: GET aml/drives/reports/utilization	92
Table 123: POST aml/drives/reports/utilization/email	93
Table 124: GET aml/drive/{serialNumber}	93
Table 125: GET aml/drive/{serialNumber}/dataPath.....	94
Table 126: PUT aml/drive/{serialNumber}/dataPath	94
Table 127: GET aml/drive/{serialNumber}/operations/clean.....	95
Table 128: POST aml/drive/{serialNumber}/operations/clean	95
Table 129: GET aml/drive/{serialNumber}/operations/clean/{id}	96
Table 130: DELETE aml/drive/{serialNumber}/operations/clean/{id}	96
Table 131: POST aml/drive/{identifier}/operations/configure	96
Table 132: POST aml/drive/{serialNumber}/operations/eject	97
Table 133: GET aml/drive/{serialNumber}/operations/identify	97
Table 134: POST aml/drive/{serialNumber}/operations/identify	98
Table 135: DELETE aml/drive/{serialNumber}/operations/identify	98
Table 136: POST aml/drive/{serialNumber}/operations/powerCycle	99
Table 137: POST aml/drive/{serialNumber}/operations/performanceTest.....	99
Table 138: GET aml/drive/{identifier}/operations/state	99
Table 139: PUT aml/drive/{identifier}/operations/state.....	100
Table 140: POST aml/drive/{serialNumber}/operations/test	100
Table 141: POST aml/drive/{serialNumber}/operations/wrapTest	101
Table 142: GET aml/drive/{serialNumber}/ports	101
Table 143: PUT aml/drive/{serialNumber}/ports	102
Table 144: GET aml/drive/{serialNumber}/log	103

Table 145: POST aml/drive/{serialNumber}/log/email	103
Table 146: GET aml/drive/{serialNumber}/mode	104
Table 147: PUT aml/drive/{serialNumber}/mode	104
Table 148: POST aml/drive/{serialNumber}/removeITNexus	105
Table 149: GET aml/enum	105
Table 150: GET aml/enum/{component}	106
Table 151: GET aml/enum/{component}/{element}	107
Table 152: GET aml/media	107
Table 153: GET aml/media/cleaning.....	109
Table 154: GET aml/media/edlm	109
Table 155: POST aml/media/edlm.....	110
Table 156: GET aml/media/edlm/results.....	110
Table 157: GET aml/media/edlm/result/{id}	111
Table 158: DELETE aml/media/edlm/result/{id}	111
Table 159: GET aml/media/edlm/sessions	112
Table 160: GET aml/media/edlm/session/{id}.....	112
Table 161: PUT aml/media/edlm/session/{id}/operations/pause	113
Table 162: PUT aml/media/edlm/session/{id}/operations/resume	113
Table 163: PUT aml/media/edlm/session/{id}/operations/stop	113
Table 164: GET aml/media/operations/moveMedium	114
Table 165: POST aml/media/operations/moveMedium	114
Table 166: GET aml/media/operations/moveMedium/maxAllowed	115
Table 167: PUT aml/media/operations/moveMedium/maxAllowed	115
Table 168: GET aml/media/reports/crossPartitionMoves	116
Table 169: POST aml/media/reports/crossPartitionMoves/email	117
Table 170: GET aml/media/reports/edlm	117
Table 171: POST aml/media/reports/edlm/email	118
Table 172: GET aml/media/reports/inventory	118
Table 173: POST aml/media/reports/inventory/email	119
Table 174: GET aml/media/reports/securityEvents	119
Table 175: POST aml/media/reports/securityEvents/email	120
Table 176: GET aml/media/reports/tapeAlerts	121
Table 177: POST aml/media/reports/tapeAlerts/email	122
Table 178: GET aml/media/reports/usage	122
Table 179: POST aml/media/reports/usage/email	123

Table 180: GET aml/medium/{barcode}.....	123
Table 181: GET aml/partitions	124
Table 182: POST aml/partitions	124
Table 183: GET aml/partitions/policy/activeVault	126
Table 184: POST aml/partitions/policy/activeVault	127
Table 185: GET aml/partitions/policy/autoImport.....	127
Table 186: GET aml/partitions/policy/autoExport.....	128
Table 187: GET aml/partitions/policy/driveCleaning	128
Table 188: GET aml/partitions/policy/edlm	129
Table 189: POST aml/partitions/policy/edlm	129
Table 190: GET aml/partitions/policy/ekm	130
Table 191: GET aml/partitions/policy/ekm/keySets	131
Table 192: POST aml/partitions/policy/ekm/keySets	131
Table 193: PUT aml/ partitions/policy/ekm/keySet/{name}	131
Table 194: GET aml/partitions/reports/utilization	132
Table 195: POST aml/partitions/reports/utilization/email	133
Table 196: GET aml/partition/{name}	133
Table 197: PUT aml/partition/{name}	134
Table 198: DELETE aml/partition/{name}	134
Table 199: GET aml/partition/{name}/ampExtensionsCount - deprecated	135
Table 200: PUT aml/partition/{name}/ampExtensionsCount - deprecated	135
Table 201: GET aml/partition/{name}/barcodeReporting - deprecated.....	136
Table 202: PUT aml/partition/{name}/barcodeReporting - deprecated	136
Table 203: GET aml/partition/{name}/controlPath	137
Table 204: PUT aml/partition/{name}/controlPath.....	137
Table 205: GET aml/partition/{name}/dataPath	141
Table 206: PUT aml/partition/{name}/dataPath	141
Table 207: GET aml/partition/{name}/driveSerialNumbers	141
Table 208: POST aml/partition/{name}/driveSerialNumbers.....	142
Table 209: DELETE aml/partition/{name}/driveSerialNumbers	142
Table 210: GET aml/partition/{name}/mode.....	143
Table 211: PUT aml/partition/{name}/mode	143
Table 212: GET aml/partition/{name}/name.....	144
Table 213: PUT aml/partition/{name}/name	144
Table 214: GET aml/partition/{name}/operations	144

Table 215: GET aml/partition/{name}/operations/autolImport	145
Table 216: POST aml/partition/{name}/operations/autolImport	145
Table 217: GET aml/partition/{name}/operations/autolImport/{id}	146
Table 218: DELETE aml/partition/{name}/operations/autolImport/{id}	146
Table 219: GET aml/partition/{name}/operations/inventory	146
Table 220: POST aml/partition/{name}/operations/inventory	147
Table 221: GET aml/partition/{name}/operations/inventory/{taskId}	147
Table 222: DELETE aml/partition/{name}/operations/inventory/{taskId}	148
Table 223: GET aml/partition/{name}/policy/activeVault	148
Table 224: PUT aml/partition/{name}/policy/activeVault	149
Table 225: DELETE aml/partition/{name}/policy/activeVault	149
Table 226: GET aml/partition/{name}/policy/autolImport	150
Table 227: PUT aml/partition/{name}/policy/autolImport	150
Table 228: GET aml/partition/{name}/policy/autoExport	151
Table 229: PUT aml/partition/{name}/policy/autoExport	151
Table 230: GET aml/partition/{name}/policy/driveCleaning	152
Table 231: POST aml/partition/{name}/policy/driveCleaning	153
Table 232: PUT aml/partition/{name}/policy/driveCleaning	153
Table 233: DELETE aml/partition/{name}/policy/driveCleaning	153
Table 234: GET aml/partition/{name}/policy/driveLeveling	154
Table 235: PUT aml/partition/{name}/policy/driveLeveling	154
Table 236: GET aml/partition/{name}/policy/edlm	155
Table 237: PUT aml/partition/{name}/policy/edlm	156
Table 238: DELETE aml/partition/{name}/policy/edlm	157
Table 239: GET aml/partition/{name}/policy/ekm	157
Table 240: PUT aml/partition/{name}/policy/ekm	158
Table 241: GET aml/partition/{name}/segments	159
Table 242: POST aml/partition/{name}/segments	159
Table 243: DELETE aml/partition/{name}/segments	161
Table 244: PUT aml/partition/{name}/segments	162
Table 245: GET aml/physicalLibrary	163
Table 246: PUT aml/physicalLibrary	163
Table 247: GET aml/physicalLibrary/elements	166
Table 248: GET aml/physicalLibrary/environment	167
Table 249: POST aml/physicalLibrary/environment/email	168

Table 250: GET aml/physicalLibrary/i3-i6/modules	168
Table 251: GET aml/physicalLibrary/mode	168
Table 252: PUT aml/physicalLibrary/mode	169
Table 253: GET aml/physicalLibrary/operations	169
Table 254: GET aml/physicalLibrary/operations/inventory	170
Table 255: POST aml/physicalLibrary/operations/inventory	170
Table 256: GET aml/physicalLibrary/operations/inventory/{id}	171
Table 257: DELETE aml/physicalLibrary/operations/inventory/{id}	171
Table 258: GET aml/physicalLibrary/operations/shutdown.....	172
Table 259: POST aml/physicalLibrary/operations/shutdown	172
Table 260: GET aml/physicalLibrary/operations/shutdown/{id}	173
Table 261: DELETE aml/physicalLibrary/operations/shutdown/{id}.....	173
Table 262: GET aml/physicalLibrary/operations/reboot.....	173
Table 263: POST aml/physicalLibrary/operations/reboot	174
Table 264: GET aml/physicalLibrary/operations/reboot/{id}	174
Table 265: DELETE aml/physicalLibrary/operations/reboot/{id}	174
Table 266: GET aml/physicalLibrary/operations/reset	175
Table 267: POST aml/physicalLibrary/operations/reset.....	175
Table 268: GET aml/physicalLibrary/operations/reset/{id}.....	175
Table 269: DELETE aml/physicalLibrary/operations/reset/{id}	176
Table 270: GET aml/physicalLibrary/operations/teach	176
Table 271: POST aml/physicalLibrary/operations/teach.....	176
Table 272: GET aml/physicalLibrary/operations/teach/{id}	177
Table 273: DELETE aml/physicalLibrary/operations/teach/{id}	177
Table 274: GET aml/physicalLibrary/quattro/modules - deprecated.....	178
Table 275: GET aml/physicalLibrary/subset/configuration.....	178
Table 276: GET aml/physicalLibrary/subset/remoteAccess	178
Table 277: GET aml/physicalLibrary/subset/resources	179
Table 278: GET aml/physicalLibrary/subset/settings	179
Table 280: GET aml/physicalLibrary/segments	179
Table 281: GET aml/physicalLibrary/segments/amp	180
Table 282: PUT aml/physicalLibrary/segments/amp	180
Table 283: GET aml/physicalLibrary/segments/cleaning	181
Table 284: POST aml/physicalLibrary/segments/cleaning	182
Table 285: DELETE aml/physicalLibrary/segments/cleaning	182

Table 286: POST aml/physicalLibrary/segments/operations/inventory	182
Table 287: GET aml/physicalLibrary/status	183
Table 288: GET aml/service/logs	183
Table 289: GET aml/service/log/{name}	183
Table 290: POST aml/service/log/{name}/email	184
Table 291: POST aml/service/resetFactoryDefault	184
Table 292: GET aml/service/vt/test	185
Table 293: POST aml/service/vt/test/abort	185
Table 294: GET aml/service/vt/test/operations	185
Table 295: POST aml/service/vt/test/operations	186
Table 296: GET aml/service/vt/test/operation/{taskId}	189
Table 297: GET aml/service/vt/test/sessions	190
Table 298: GET aml/service/vt/test/session	190
Table 299: GET aml/service/vt/test/session/{id}	190
Table 300: DELETE aml/service/vt/test/session/{id}	191
Table 301: GET aml/system/configuration/record	191
Table 302: POST aml/system/configuration/record/email	192
Table 303: GET aml/system/configurationChanges/report	192
Table 304: POST aml/system/configurationChanges/report/email	193
Table 307: GET aml/system/dateTime	193
Table 308: PUT aml/system/dateTime	193
Table 309: POST aml/system/dateTime/clientDateTime	194
Table 310: GET aml/system/dateTime/ntp	194
Table 311: PUT aml/system/dateTime/ntp	195
Table 312: GET aml/system/dateTime/timeZoneIds	195
Table 313: GET aml/system/ekm/communicationCertificates	196
Table 314: POST aml/system/ekm/communicationCertificates	196
Table 315: GET aml/system/ekm/logs - deprecated	197
Table 316: GET aml/system/ekm/reports/audit/mediaStatus	197
Table 317: POST aml/system/ekm/reports/audit/mediaStatus/email	198
Table 318: GET aml/system/ekm/reports/audit/partitionActivity	199
Table 319: POST aml/system/ekm/reports/audit/partitionActivity/email	199
Table 320: GET aml/system/ekm/servers	200
Table 321: POST aml/system/ekm/servers	200
Table 322: GET aml/system/ekm/servers/{type}	202

Table 323: PUT aml/system/ekm/servers/{type}	202
Table 324: DELETE aml/system/ekm/servers/{type}	203
Table 325: POST aml/system/ekm/servers/{type}/test	203
Table 326: GET aml/system/emmc	203
Table 327: GET aml/system/file	204
Table 328: GET aml/system/licenses	204
Table 329: POST aml/system/licenses	204
Table 330: GET aml/system/network	205
Table 331: GET aml/system/network/access/certificate	205
Table 332: POST aml/system/network/access/certificate	206
Table 333: GET aml/system/network/access/certificate/activate	206
Table 334: POST aml/system/network/access/certificate/activate	206
Table 335: POST aml/system/network/access/certificate/csr	207
Table 336: GET aml/system/network/access/certificate/isSigned	207
Table 337: GET aml/system/network/interfaces	208
Table 338: GET aml/system/network/interface/{name}	208
Table 339: PUT aml/system/network/interface/{name}	209
Table 340: GET aml/system/network/configurations	209
Table 341: GET aml/system/network/configuration/{name}	209
Table 342: PUT aml/system/network/configuration/{name}/{version}	210
Table 343: GET aml/system/network/dns	212
Table 344: PUT aml/system/network/dns	212
Table 345: GET aml/system/network/emailServer	213
Table 346: PUT aml/system/network/emailServer	213
Table 347: GET aml/system/network/internal	214
Table 348: PUT aml/system/network/internal	214
Table 349: GET aml/system/network/internal/connectivity	215
Table 350: POST aml/system/network/internal/connectivity/email	215
Table 351: GET aml/system/network/ipv6/mode	216
Table 352: PUT aml/system/network/ipv6/mode	216
Table 353: POST aml/system/network/emailServer/test	216
Table 354: GET aml/system/network/snmp/MIBs	217
Table 355: POST aml/system/network/snmp/MIBs/email	217
Table 356: GET aml/system/network/syslogs	218
Table 357: POST aml/system/network/syslogs	218

Table 358: GET aml/system/network/syslog/{id}	219
Table 359: PUT aml/system/network/syslog/{id}	219
Table 360: DELETE aml/system/network/syslog/{id}.....	219
Table 361: POST aml/system/network/syslog/{id}/test	220
Table 362: GET aml/system/notifications/contact.....	220
Table 363: PUT aml/system/notifications/contact.....	220
Table 364: GET aml/system/notifications/emailRecipients	221
Table 365: POST aml/system/notifications/emailRecipients	221
Table 366: GET aml/system/notifications/emailRecipient/{id}	221
Table 367: DELETE aml/system/notifications/emailRecipient/{id}.....	222
Table 368: GET aml/system/notifications/heartbeat	222
Table 369: PUT aml/system/notifications/heartbeat	222
Table 375: GET aml/system/notifications/mediaSecurity	223
Table 376: PUT aml/system/notifications/mediaSecurity.....	223
Table 377: GET aml/system/notifications/reports	224
Table 378: POST aml/system/notifications/reports.....	224
Table 379: GET aml/system/notifications/report/{id}.....	225
Table 380: PUT aml/system/notifications/report/{id}.....	225
Table 381: DELETE aml/system/notifications/report/{id}.....	225
Table 382: GET aml/system/notifications/snmpTraps	226
Table 383: POST aml/system/notifications/snmpTraps.....	226
Table 384: POST aml/system/notifications/snmpTraps/test	226
Table 385: GET aml/system/notifications/snmpTrap/{id}.....	227
Table 386: PUT aml/system/notifications/snmpTrap/{id}.....	227
Table 387: DELETE aml/system/notifications/snmpTrap/{id}	227
Table 388: GET aml/system/notifications/telemetry	228
Table 389: GET aml/system/notifications/telemetric/{receiver}	228
Table 390: PUT aml/system/notifications/telemetric/{receiver}	229
Table 391: GET aml/system/notifications/tickets	229
Table 392: POST aml/system/notifications/tickets.....	229
Table 393: GET aml/system/notifications/ticket/{id}.....	230
Table 394: PUT aml/system/notifications/ticket/{id}.....	230
Table 395: DELETE aml/system/notifications/ticket/{id}	230
Table 396: GET aml/system/notifications/tickets/filters	231
Table 397: PUT aml/system/notifications/tickets/filters.....	231

Table 398: POST aml/system/operations/reboot	232
Table 399: POST aml/system/operations/shutdown	232
Table 400: GET aml/system/policy/externalApplicationServers	232
Table 401: POST aml/system/policy/externalApplicationServers	233
Table 402: GET aml/system/policy/externalApplicationServer/{name}.....	233
Table 403: PUT aml/system/policy/externalApplicationServer/{name}.....	234
Table 404: DELETE aml/system/policy/externalApplicationServer/{name}.....	234
Table 405: POST aml/system/policy/externalApplicationServer/{name}/test	235
Table 406: GET aml/system/ras.....	235
Table 407: GET aml/system/ras/{group}.....	236
Table 408: GET aml/system/ras/reports/tickets	236
Table 409: POST aml/system/ras/reports/tickets/email	237
Table 410: GET aml/system/ras/tickets	238
Table 412: GET aml/system/ras/ticket/{id}	239
Table 413: PUT aml/system/ras/ticket/{id}	239
Table 414: POST aml/system/ras/ticket/{id}/email.....	239
Table 415: GET aml/system/ras/ticket/{id}/history	240
Table 416: GET aml/system/ras/ticket/{id}/reports.....	240
Table 417: GET aml/system/ras/ticket/{id}/resolution	241
Table 418: GET aml/system/reports	241
Table 419: GET aml/system/reports/templates.....	241
Table 420: POST aml/system/reports/templates	242
Table 421: GET aml/system/reports/template/{name}	242
Table 422: PUT aml/system/reports/template/{name}	243
Table 423: DELETE aml/system/reports/template/{name}	243
Table 424: GET aml/system/saveRestore	244
Table 425: POST aml/system/saveRestore	244
Table 426: GET aml/system/saveRestore/rescue	244
Table 427: POST aml/system/saveRestore/rescue	245
Table 428: PUT aml/system/saveRestore/rescue.....	245
Table 429: GET aml/system/saveRestore/revert	245
Table 430: PUT aml/system/saveRestore/revert	246
Table 431: GET aml/system/sensor/configurations	246
Table 432: PUT aml/system/sensor/configurations	247
Table 433: GET aml/system/sensors	247

Table 434: GET aml/system/snapshot.....	248
Table 435: POST aml/system/snapshot/email.....	248
Table 436: GET aml/system/software.....	249
Table 437: POST aml/system/software	249
Table 438: GET aml/system/software/operations/update.....	250
Table 439: POST aml/system/software/operations/update	251
Table 440: GET aml/system/software/externalApplications	252
Table 441: POST aml/system/software/externalApplications	252
Table 442: GET aml/system/software/externalApplication/{name}.....	252
Table 443: DELETE aml/system/software/externalApplication/{name}.....	253
Table 444: GET aml/system/software/availableFirmware	253
Table 445: POST aml/system/software/availableFirmware	253
Table 446: POST aml/system/software/restartLMC	254
Table 447: GET aml/users	254
Table 448: POST aml/users.....	255
Table 449: GET aml/users/ldap	255
Table 450: PUT aml/users/ldap	255
Table 451: POST aml/users/ldap.....	256
Table 452: GET aml/users/ldap/certificates	256
Table 453: POST aml/users/ldap/certificates	257
Table 454: GET aml/users/ldap/enabled	257
Table 455: POST aml/users/ldap/keytab	257
Table 456: POST aml/users/ldap/test.....	258
Table 457: POST aml/users/login	258
Table 458: POST aml/users/login	260
Table 459: DELETE aml/users/login.....	262
Table 460: POST aml/users/login/mfa	262
Table 461: GET aml/users/login/mfa/{type}/key	263
Table 462: GET aml/users/login/mode	263
Table 463: PUT aml/users/login/mode.....	263
Table 464: GET aml/users/luiAccess.....	264
Table 465: PUT aml/users/luiAccess	264
Table 466: GET aml/users/luiAccess/mode.....	265
Table 467: GET aml/users/mfa	265
Table 468: PUT aml/users/mfa	265

Table 469: GET aml/users/reports/login	266
Table 470: POST aml/users/reports/login/email	266
Table 471: GET aml/users/service/mode	267
Table 472: PUT aml/users/service/mode	267
Table 473: GET aml/users/sessions	268
Table 474: DELETE aml/users/session/{id}	268
Table 475: GET aml/user	268
Table 476: GET aml/user/{name}	269
Table 477: PUT aml/user/{name}	269
Table 478: DELETE aml/user/{name}	270
Table 479: GET aml/user/{name}/mfa	270
Table 480: PUT aml/user/admin/reset	271
Table 481: Scalar i6000 SCSI Custom Codes 10000 – 80000	333
Table 482: Scalar i3/i6/i6H Custom Codes	335

List of Resource Objects

Figure 1: accessDeviceList	272
Figure 2: accessDevice	272
Figure 3: accessGroupList	272
Figure 4: accessGroup	272
Figure 5: activeVaultPolicyList	272
Figure 6: activeVaultPolicy	272
Figure 7: autoExportPolicyList	273
Figure 8: autoExportPolicy	273
Figure 9: autoImportPolicyList	273
Figure 10: autoImportPolicy	273
Figure 11: availableFirmware	274
Figure 12: bladeList	274
Figure 13: blade	274
Figure 14: bladeFirmwareList	274
Figure 15: bladeFirmware	274
Figure 16: cleanDriveTask	274
Figure 17: cleaningMediaList	274
Figure 18: cleaningMedia	275
Figure 19: communicationCertificateList	275

Figure 20: communicationCertificate	275
Figure 21: componentList (ENUM)	275
Figure 22: configurationChangeList	275
Figure 23: configurationChange	275
Figure 24: certificateInformation	276
Figure 25: contactInformation	276
Figure 26: coordinate	276
Figure 27: crossPartitionMovesList	276
Figure 28: crossPartitionMoves	277
Figure 29: dateTime	277
Figure 30: detailedDriveActivityStatistics	277
Figure 31: DNS	277
Figure 32: driveList	277
Figure 33: drive	278
Figure 34: driveActivityStatistics	279
Figure 35: driveCleaningList	281
Figure 36: driveCleaning	281
Figure 37: driveCleaningPolicyList	282
Figure 38: driveCleaningPolicy	282
Figure 39: driveLevelingPolicy	282
Figure 40: driveLogList	282
Figure 41: driveLog	282
Figure 42: drivePortList	283
Figure 43: drivePorts	283
Figure 44: driveSerialNumberList	283
Figure 45: driveUtilizationList	283
Figure 46: driveUtilization	283
Figure 47: edlmMediaList	283
Figure 48: edlmMedia	284
Figure 49: edlmMediaResultList	284
Figure 50: edlmMediaResult	284
Figure 51: edlmMediaScanTestList	286
Figure 52: edlmMediaScanTest	286
Figure 53: edlmPolicyList	286
Figure 54: edlmPolicy	287

Figure 55: edlmSessionList	287
Figure 56: edlmSession	287
Figure 57: ekmMediaStatusList	287
Figure 58: ekmMediaStatus	288
Figure 59: ekmPartitionActivityList	288
Figure 60: ekmPartitionActivity	288
Figure 61: ekmServersList	288
Figure 62: ekmServers	288
Figure 63: ekmServerTestResultList	289
Figure 64: ekmServerTestResult	289
Figure 65: elementList (ENUM)	289
Figure 66: elementList	289
Figure 67: element	289
Figure 68: email	290
Figure 69: emailServer	290
Figure 70: emailRecipientList	290
Figure 71: emailRecipient	290
Figure 72: emmc	290
Figure 73: entryList (ENUM)	291
Figure 74: environmentList	291
Figure 75: environment	291
Figure 76: ethernetExpansionBladeList	291
Figure 77: ethernetExpansionBlade	291
Figure 78: ethernetExpansionBladePort	291
Figure 79: externalApplicationList	291
Figure 80: externalApplication	292
Figure 81: externalApplicationServersList	292
Figure 82: externalApplicationServers	292
Figure 83: externalApplicationServerTestResultList	292
Figure 84: externalApplicationServerTestResult	292
Figure 85: fcBladeList	293
Figure 86: fcBlade	293
Figure 87: fcBladeHostsList	293
Figure 88: fcBladeHosts	293
Figure 89: fcBladeZoning	293

Figure 90: fcHostPortFailoverList.....	294
Figure 91: fcHostPortFailover	294
Figure 92: fcLunMapping	295
Figure 93: fcBladePortList.....	295
Figure 94: fcBladePort	295
Figure 95: firmwareList	296
Figure 96: firmware	296
Figure 97: firmwareFileList.....	296
Figure 98: firmwareUpdateList.....	296
Figure 99: firmwareUpdate	296
Figure 100: firmwareFile	296
Figure 101: firmwareStatusList	297
Figure 102: firmwareStatus.....	297
Figure 103: heartbeatNotification.....	297
Figure 105: hostList.....	297
Figure 106: host	297
Figure 107: ieSlots	298
Figure 108: ieStationList	298
Figure 109: ieStation.....	298
Figure 110: internalNetwork.....	298
Figure 111: inventoryTask	298
Figure 112: keySetList	299
Figure 113: keySet	299
Figure 114: latestFirmwareVersion	299
Figure 115: ldap	299
Figure 116: ldapTest	300
Figure 117: libraryControlBladeList.....	300
Figure 118: libraryControlBlade	300
Figure 119: libraryDiagnosticTestList.....	300
Figure 120: libraryDiagnosticTest	300
Figure 121: libraryDiagnosticTestResult	300
Figure 122: libraryDiagnosticTestSessionList.....	301
Figure 123: libraryDiagnosticTestSession	301
Figure 124: libraryDiagnosticTestTask	301
Figure 125: libraryStatus	302

Figure 126: licenseList	303
Figure 127: license	303
Figure 128: loginActivityList	303
Figure 129: loginActivity	304
Figure 130: ItfsBladeList.....	304
Figure 131: ItfsBlade	304
Figure 132: LUIAccess	304
Figure 133: magazineList.....	305
Figure 134: magazine.....	305
Figure 135: mediaList.....	305
Figure 136: media	305
Figure 137: mediaSecurityEventList	306
Figure 138: mediaSecurityEvent	306
Figure 139: mediaSecurityPolicy.....	306
Figure 140: mediaUsageList	306
Figure 141: mediaUsage	306
Figure 142: mfaList.....	307
Figure 143: mfa	307
Figure 144: mfaAuthentication	307
Figure 145: mfaSharedData.....	307
Figure 146: moduleList.....	308
Figure 147: module	308
Figure 148: moveMediumList.....	308
Figure 149: moveMedium	308
Figure 150: network.....	309
Figure 151: networkAccess.....	309
Figure 152: netConfigurationList	310
Figure 153: netConfiguration.....	310
Figure 154: netInterfaceList	310
Figure 155: netInterface	310
Figure 156: networkDeviceConnectivityInfoList	311
Figure 157: networkDeviceConnectivityInfo.....	311
Figure 158: NTP	311
Figure 159: onlineHelp	311
Figure 160: partitionList.....	311

Figure 161: partition	311
Figure 162: partitionEncryptionPolicyList.....	313
Figure 163: partitionEncryptionPolicy	313
Figure 164: physicalLibrary	313
Figure 165: physicalLibraryConfiguration	316
Figure 166: physicalLibraryRemoteAccess	316
Figure 167: physicalLibraryResources.....	317
Figure 168: physicalLibrarySettings.....	317
Figure 169: ping	318
Figure 170: port.....	318
Figure 171: RASGroupStatusList.....	319
Figure 172: RASGroupStatus	319
Figure 173: RASReportList	319
Figure 174: RASReport.....	319
Figure 175: RASTicketReports	319
Figure 176: RASTicketList	320
Figure 177: RASTicket.....	320
Figure 178: RASTicketState	321
Figure 179: rasNotificationList	321
Figure 180: rasNotification	321
Figure 181: reportList.....	321
Figure 182: report.....	321
Figure 183: reportCriteria	322
Figure 184: reportNotificationList	322
Figure 185: reportNotification.....	323
Figure 186: reportTemplateList.....	323
Figure 187: reportTemplate	323
Figure 188: robotList	323
Figure 189: robot.....	323
Figure 190: robotSettings.....	324
Figure 191: section.....	324
Figure 192: segmentList	324
Figure 193: segment	324
Figure 194: sendUsageStatistics	324
Figure 195: sensorList	325

Figure 196: sensor	325
Figure 197: sensorConfigurationList	325
Figure 198: sensorConfiguration	325
Figure 199: serviceLogList	325
Figure 200: serviceLog	326
Figure 201: shutdownTask	326
Figure 202: sysLogServerList	326
Figure 203: sysLogServer	326
Figure 204: teachTask	326
Figure 205: telemetricNotificationList	326
Figure 206: telemetricNotification	327
Figure 207: trapNotificationList	327
Figure 208: trapNotification	327
Figure 209: taskList	327
Figure 210: task	327
Figure 211: ticketFilterList	328
Figure 212: ticketFilter	328
Figure 213: timeZoneIDs	329
Figure 214: towerList	329
Figure 215: tower	329
Figure 216: usb	330
Figure 217: userList	330
Figure 218: user	330
Figure 219: userMfaList	331
Figure 220: userMfa	331
Figure 221: userSessionList	331
Figure 222: userSession	331
Figure 223: vtReportList	331
Figure 224: windowsBlade	331
Figure 225: windowsBladeList	332
Figure 226: WSResultCode	332

1. Introduction

1.1 General

The Scalar i6000, i3 and i6/i6H Web Services application interface uses the REpresentational State Transfer (REST) architectural principles. REST is a software architecture style that builds distributed systems consisting of clients and server components. Clients initiate requests and servers process these requests and return responses, where the response can be a status or a representation of the resources being requested.

REST is protocol independent. The Scalar i6000, i3 and i6/i6H uses the Hypertext Transfer Protocol (HTTP) as the application protocol. For more information regarding REST, visit http://en.wikipedia.org/wiki/Representational_state_transfer.

The Scalar i6000, i3 and i6/i6H REST architecture principles are defined as follows:

1.2 Addressable Resources

Information and data is represented as resources which are addressed by a Uniform Resource Identifier (URI). The format of a URI is as follows:

protocol://host:port/resource?query=action&filter=10

The Scalar i6000 communication protocol is either http or https; the Scalar i3 and Scalar i6/i6H communication protocol supports only https. The host is the library domain name or library IP address, accepting web service requests on port 80 for http and 443 for https.

While the host and port represent the library network location, the resource defines the web service resource request which consists of text separated by “/” characters to further define unique resource requests.

Optional query parameters are identified by the “?” character which separates the resource from the query strings. Query parameters are name value pairs delimited by the “&” character to allow multiple query string definitions.

1.3 Representation-Oriented Resources

Each resource can be represented in different formats. Different platforms require different formats; browsers use Hypertext Markup Language (HTML), JavaScript uses JavaScript Object Notation (JSON) and JAVA may require Extensible Markup Language (XML).

The HTTP communication protocol defines the representation in the message body of the request or response. The message body can return data in any format and the Content-Type header of the HTTP request and response informs the client or server of the message body format.

The library typically uses text/plain, application/xml and application/json. Depending on the request, it also supports application/x-tar, application/octet-stream and multipart/form-data for transferring binary or text data.

1.4 Uniformed, Constrained Request Interfaces

A small set of well-defined methods/operations manipulate library resources. Create, Read, Update, and Delete (CRUD) operations are performed via http methods POST, GET, PUT, and DELETE:

- POST is used to create a new resource, either permanently, or temporarily, such as requesting a robot operation. The request message body contains the details for the new resource to be created.
- GET is used to retrieve resource information.
- PUT is used to update/modify a resource. The request message body contains the information needed to update the resource.
- DELETE is used to remove an existing resource.

2. Request and Response Interface Description

2.1 General

As described earlier, clients use HTTP or HTTPS as the application protocol to make requests to the Scalar i6000 or HTTPS as the application protocol to make requests to the Scalar i3 and Scalar i6/i6H Web Services (WS) server. A client request identifies the resource URI, and any query parameters, and the library responds with status and/or request data.

The Scalar i6000, i3 and i6/i6H define a base URI which, by itself, provides library identification information, and also serves as the starting resource URI for all additional Web Services URI requests. The base URI is defined as follows:

HTTP(S)://LIBRARY-NAME-or-IP/aml

HTTP and HTTPS define unsecure or secure communication requests, respectively. The base URI identifies the library network location where library resources can be accessed. URIs are defined with intuitive naming conventions using a directory style structure.

2.2 URI Examples

To illustrate the use of Scalar i6000/i3/i6/i6H URIs, consider the following URI to interact with logical library partition resources for a tape library with domain name *myLibrary*:

https://myLibrary/aml/partitions

The above URI references all configured partition resources. A particular partition resource is referenced with a specific partition name:

https://myLibrary/aml/partition/{name}

The "{name}" URI path template represents the name of the partition resource being requested.

To limit partition resource information, query strings are added to the URI. In the following example, you can retrieve a list of storage segments in frame 2 that belong to the partition with the given '{name}' LL1:

https://myLibrary/aml/partition/LL1/segments?type=storage&frame=2

2.3 Web Services Request Examples

The requesting client accesses and manipulates library resources with the HTTP methods POST, GET, PUT and DELETE. These methods are included in the HTTP request header.

To illustrate, a *GET http://mylibrary/aml/partitions* request results in the following HTTP header data:

GET http://mylibrary/aml/partitions HTTP/1.1

Host: user@company.com

User-Agent: Mozilla/5.0

Content-type: text/plain

Accept: application/xml, application/json

The library web server response message is similar and contains the HTTP version being used, a response code, a short message that explains the response code, a variable set of optional headers and an optional message body.

HTTP/1.1 200 OK
Content-Type: application/xml
Server: Jetty(7.9.2 v20120308)
Content-Length: 870

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:partitionList xmlns:ns2="http://automatedMediaLibrary/">
  <partition>
    <name>Test Partition</name>
    <type>1</type>
    <driveDomainType>6</driveDomainType>
    <storageSlotCount>300</storageSlotCount>
    <driveCount>2</driveCount>
    <ieSlotCount>12</ieSlotCount>
    <xieSlotCount>0</xieSlotCount>
    <ampExtensionsCount>0</ampExtensionsCount>
    <mediaCount>209</mediaCount>
    <barcodeReporting>4</barcodeReporting>
    <vendorId>1</vendorId>
    <productId>3</productId>
  </partition>
</ns2:partitionList>
```

The response body in the above example contains a list (“<ns2:partitionList>” root element) of partition resources represented as XML data. The partition resources are defined as data objects which represents the library’s logical library partition configuration. The example shows an XML response, but as explained earlier, the data format of the message body could have been JSON and in this case, due to the HTTP request header containing the statement **Accept: application/xml, application/json** the library will report the data as requested either in XML or JSON.

The response message identifies the response type in the response message body via the “Content Type” or “Media Type” statement as to what data format is reported. In this particular case the requested resource supports XML (default) as well as a JSON format, however per request and default response, the XML format is returned, identified via the statement **Content-Type: application/xml**.

The Scalar i6000/i3/i6/i6H support the following formats:

- text/plain,
- application/xml,
- application/json,
- application/octet-stream,
- multipart/form-data, and
- application/x-tar

2.4 Web Services Response Code Objects

Typically, requests that perform creation or deletion operations (POST, DELETE methods) will receive a response code object as defined below:

```
<ns2:WSResultCode xmlns:ns2="http://automatedMediaLibrary/">
  <code>200</code>
  <description>OK</description>
  <summary>Operation Completed Successfully</summary>
  <action>Logout</action>
  <customCode>0</customCode>
</ns2:WSResultCode>
```

The Scalar i6000/i3/i6/i6H support the above WSRetCode object which contains the HTTP result code in the HTTP response. In the above case, the code “200” is reporting a successful request, a brief description of this code, such as “OK”, a summary of the result, such as “*Operation Completed Successfully*”, the action that was requested, such as “*Logout*” and an optional custom code that can further describe the result in certain contexts.

While GET requests for resource objects may report a single object or a list of objects, some requests may return plain text that are not resource object representations but report single scalar values.

An example would be a request to retrieve the current date configured on the library:

GET HTTP://mylibrary/aml/system/dateTime/date

The following is returned in the response body:

“2012-08-23”

PUT requests, typically, return the modified resource.

2.4.1 Response Codes

The response header contains an HTTP status code that reports the status of the request. These status codes are part of the HTTP standard. The library supports the following status codes:

200 OK

The request has succeeded. The information returned with the response is dependent on the method used in the request, for example:

GET an entity corresponding to the requested resource is sent in the response.

PUT returns the modified entity as if a GET had requested it.

POST an entity describing or containing the result of the action.

201 Created

The request has been fulfilled and resulted in a new resource being created.

Example: A request has been initiated, a new object has been created and the URI to the new resource can be found in the response header Location value.

202 Accepted

The request has been accepted, this is an asynchronous operation.

Example: A request has been initiated, but has not completed yet. Status polling will allow status testing to determine progress and eventual result codes.

400 Bad Request

The request could not be understood by the server due to malformed syntax.

Example: the URI and method are correct, but a request parameter is incorrect, or the JSON or XML is invalid.

401 Unauthorized

The request requires a valid user login session.

Example: The user session expired; a login is required again.

403 Forbidden

The request requires a valid login and the user needs to have access to the requested resource.

Example: Try to create a resource that already exists, or the request is not allowed for the current user role.

404 Not Found

The server has not found anything matching the Request-URI.

Example: The URI and media type are correct, but an identified resource is not found or no longer valid. The following URI “aml/partition/{name}” uses a path template “name”, which should represent a valid configured partition name.

405 Method Not Allowed

The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.

Example: The URI is supported, but the method requested (GET, POST, PUT, or DELETE) is not supported.

412 Precondition Failed

The request is good, but some license or configuration setting is preventing the request from completing.

Example: Attempt to email a report when the email server is not configured or the required license is not installed.

415 Unsupported Media Type

The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.

Example: The Content-Type (Media Type) header is not correct in the request message. That is, the WS request is expecting application/xml or application/json.

500 Internal Server Error

The server encountered an unexpected condition which prevented it from fulfilling the request.

Example: The HTTP request was determined to be valid, but the requested operation failed.

501 Not Implemented

The server does not recognize the request method, lacks the ability to fulfill the request or does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.

Example: The HTTP request is valid, but functionality has not been configured or implemented.

503 Service Unavailable

The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. The implication is that this is a temporary condition which will be alleviated after some delay. If known, the length of the delay MAY be indicated in a Retry-After header. If no Retry-After is given, the client SHOULD handle the response as it would for a

500 response.

Example: The request is not allowed due to a service user being logged in to perform maintenance.

2.5 Cookies

A successful login to the WS interface responds with a session cookie in the response header data. This cookie will need to be used on each successive http/https request for request authentication purposes after the initial login.

2.6 Cache Controls

All responses have cache controls turned off. No caching mechanisms are provided through the WS interface.

3. Web Services Application Programming Interface

3.1 Resource Tables

All library resource URIs are defined within tables in the following sections. Each supported Web Services URI

- identifies to which product the command request applies;
- identifies any required license need;
- provides guidance as to how quickly a command can be expected to respond and what possible timeout may be considered in the event the command encounters retry and recovery operations. Note that the response time information assumes a single outstanding request involving one or more resources. Adjustments need to be made if the request is issued while the tape library is already performing or queuing a command request;
- provides a short description of the command request. The command request description precedes each table and may also describe some differences between supported library models. The following table entries provide detailed command request information as follows:
 - the URI to a particular resource.
 - the supported CRUD methods, GET, POST, PUT and DELETE.
 - request data objects (XML or JSON), used with most PUT and POST methods.
 - response data objects, resources, primarily represented in XML and JSON.
 - the Content-type (Media Types) supported for that resource.
 - any Location URIs for newly created objects.
 - any parameter query strings, and
 - the possible response codes.

3.1.1 Table Entry Explanations

3.1.1.1 URI

URI	aml/drives
------------	-------------------

The first row of a table is the URI. The URI is a unique identifier to a resource or a list of resources. The above *aml/drives* URI points to configured drive resources. When a client makes a request, it will use this partial URI to build the full URI that is needed to complete the request. For example, if a client wanted to GET a list of drives configured in a library with domain name is *TEST*, the request URI would be <http://TEST/aml/drives>

3.1.1.2 Method

Method	POST, GET, PUT or DELETE
---------------	---------------------------------

The Method row lists the available request method(s) for the URI. Each URI may support all or a subset of the defined CRUD methods.

3.1.1.3 User Role Access

User Role Access	Admin, Service and User
-------------------------	--------------------------------

The User Role Access list the user roles that have access to the given interface. The

supported user roles are 'Admin', 'Service' and 'User'.

3.1.1.4 Version

Version	700(i6000), 110(i3/i6/i6H)
----------------	-----------------------------------

The version of code when the interface was first supported. The table only shows the first 3 digits of the code release. In the above example the 700 represents the Scalar i6000 code release 700Q.GS22301 and the 110 represents the Scalar i3/i6/i6H code release 110G.GS185.

3.1.1.5 Request/Response Header

The Request Header and Response Header fields describe what data formats are expected or reported.

Request Header	Content-Type: text/plain, application/xml, application/json, multipart/form-data
Response Header	Content-Type: application/xml, application/json, application/octet-stream, application/x-tar

3.1.1.5.1 Accept

The Accept header is used in an HTTP request to inform the server what Content-Type it expects in the response body. The library web server must support the requested Content-Type, of course, and the 'Header Response' table row specifies the supported content types. Most the requests support the Content-types 'application/xml' and 'application/json' where the default is 'application/xml'.

3.1.1.5.2 Content-Type/Media Type

The Content-Type defines the content format contained in the body of the HTTP request or response. The Media Type for **Requests** only apply to POST and PUT Methods and the following types are supported:

- **text/plain** – The client has inserted some plain text in the body of the request. This text is user to indicate some change that needs to be made to a resource. An example of this would be to change a partitions mode online/offline. If the client wanted to take a partition offline, they would insert a "2" in the body of the request (see Table 210: GET aml/partition/{name}/mode.)
- **application/xml** – The content of the request body is Extensible Markup Language (XML) and this XML describes a resource as an object. This is used to update an existing resource or create a new resource.
- **application/json** – The content of the request is JavaScript Object Notation (JSON). The JSON describes the resource that needs to be update or created. When a Content-Type Request is defined as "application/xml, application/json" this means that the Web Service server is expecting XML since it is reported first, but it can also accept JSON. If the client sends the resource representation as JSON they need to tell the server to expect JSON. This is done by adding the 'Content-Type: application/json' header to the request. Most of the URI interfaces support both XML and JSON.
- **multipart/form-data** – This Content-Type is used to send file binary data to the Web Server. Form data is made of a key, value pair, where the key is an identifier and the value

is the file data. For example, this type is currently used to upload library and drive firmware to the library (see Table 427: GET aml/system/software).

The Content-Type for **Responses** apply to all request methods and the following types are supported:

- **text/plain** – The client HTTP response body will contain text. This is typically used to report a specific property of a resource. For example, to find the mode of a partition the response body will contain a “1” or “2” (Online/Offline) (see Table 210: GET aml/partition/{name}/mode).
- **application/xml** – The content of the response body is XML and this XML represents the resource(s) as an object or the WSResultCode.
- **application/json** – The content of the response is JavaScript Object Notation (JSON). The requested resource is represented as a JSON object. When a Content-Type Response is defined as “application/xml, application/json” this means that the Web Service response will be XML by default, since it is listed first. If the client wants the response to be represented as a JSON object, then the client must add ‘Accept: application/json’ to the header of the HTTP request.
- **application/octet-stream** – The response body contains byte data; this could be readable text data or binary data.
- **application/x-tar** – The response body contains a compressed tar file.

3.1.1.5.3 Location

This response header field is used to convey the URI of a newly created resource and is typically used in conjunction with a HTTP response status code of 201. For example, if a user creates a new partition the response header would contain a location reference like “Location: http://library/partition/LL1” where ‘LL1’ is the name of the new partition.

3.1.1.5.4 Content-Disposition

This response header field is used to notify the client, specifically a browser client, that the response will contain an attachment. This response header will trigger the browser to use its default mechanism to save any file attachments/downloads. This header is typically used when the client browser needs to save library data. This field is mainly listed when save query parameters are specified. The format of the header field is “Content-Disposition: attachment; filename=”the file name to apply for the save operation”. If the ‘save=name’ name/value pair is not specified, a default file name will be applied.

3.1.1.6 Parameters

Parameters	
------------	--

Parameters are primarily used to filter the response from a GET request. The client sends supported query parameters as part of the URI request.

For example, to filter the aml/drives URI to return available unassigned drives only (drives currently not owned by a partition), issue a *GET* <http://TEST/aml/drive?status=available>

Multiple query parameters can be used if the URI interface supports them. In the case of the aml/media URI interface, to filter media for a particular partition, such as LL1, and only report

media that are in drives, issue a GET <http://TEST/aml/media?partition=LL1&location=drive>

3.1.1.7 Version

Version	700(i6000)
---------	------------

The Version identifies when the interface was first introduced. In the above example, the version '700' is the short form of the official Scalar i6000 release '700Q.GS22301'.

3.1.1.8 Response Code

Response Code	Supported HTTP Status codes
---------------	-----------------------------

The Response Code identifies all supported command status codes for the request.

Note: Response codes 400, 401, 405, 415 or 500 are not listed separately here since any interface request can encounter such HTTP status code. For the Scalar i3/i6/i6H, as of firmware version 250, any request may receive response code 412 (custom code 705) if a password change is required for the user before a command request will be accepted.

3.1.1.9 Request Data

Request Data	
--------------	--

The Request Data reports the resource object or singleton data expected by the library web server in the body of the HTTP request.

3.1.1.10 Response Data

Response Data	
---------------	--

The Response Data details the data returned in the body of the HTTP response.

4. Library Resources

4.1 Overview

Typically, library command requests require a valid user login. Operations are supported based on login user role, such that any user can perform read operations, with few exceptions for user ID retrieval. Admin and service users will be able to perform all read, as well as create, update and delete operations.

To allow library discovery and frequent status monitoring, a read of the “aml” resource (see Table 1: GET aml/) allows library detection without valid login sessions (no authentication needed).

Operational functionality, pre-requisite conditions, dependencies and license requirements are documented in product documentation and not always identified for each listed method as such information could be too repetitive.

A summary of various background information is listed in the sections below.

4.2 Login Considerations

The library management interface requires login sessions to allow library management functionality for configuring, monitoring and operating the tape library. User roles exist for service users (service), administrator users (admin), and user users (user) to define and limit login user capabilities.

While multiple admin and user sessions may be active at any time, a service user session will require a single service user session and therefore log out any other admin or user users to obtain sole access to all library resources and most library configuration, monitoring and operational functionality. Remote service user login access is disabled by default, and service login access needs to be enabled by an administrator user before service login access will be granted.

Login access can be configured for Multi-Factor Authentication (MFA), which requires a login session to not only provide user name and password credentials, but also a Time-based One-Time Password (TOTP), authentication passcode, to allow a successful login session. If MFA is enabled for library access, all admin and user users will be required to provide an authentication passcode. Service user access will not require a passcode as remote service user access can be disabled to secure access to the library.

Two methods exist to establish a login session. Refer to Table 448: POST aml/users/login for logging in using http form data (see also examples in Appendix A – Web Service Request Examples), or Table 449: POST aml/users/login for logging in with an XML or JSON object.

Login requests with MFA enabled will identify the need to provide an authentication passcode by returning a custom header in the response message to the login request to indicate MFA authentication is required. The login request must then be followed by the validation of the MFA authentication passcode to complete the login process. See Table 451: POST aml/users/login/mfa. If the authentication passcode is not provided, any request will be rejected with http error code 412 (Precondition Failed).

Login requests that require a default password change will establish a login session and report a custom header response message indicating “Warning: Default Password Supplied”. This

custom header warning message requires that the user's login password must be changed by the logged in user before requests will be accepted. The established user session will experience http error code 412, Precondition Failed, until the logged in user updates the password. Note that if the provided password cannot be accepted (i.e. system default password used), custom code 706 will be reported in the error response message to indicate that the system default password may not be applied.. Also note that if MFA has not been enabled, the user password needs to be provided right after the login request (see Table 468: PUT aml/user/{name}), but if MFA has been enabled, the MFA passcode needs to be authenticated before the user password change is provided. See Table 451: POST aml/users/login/mfa.

4.3 Access Groups, host, drive and partition access.

The following interfaces under "**aml/access**" (*supported by the Scalar i6000 only*) provide the ability to control which hosts can access which drives and partitions configured in the library. By default, all drives and partitions can be accessed by all hosts connected to the SAN. However, Quantum-branded libraries support a *Path Failover/Native Storage Networking* (SNW) license which once applied and associated with a drive (HP drive only), prevents device access and requires access configurations to define which hosts may access the drive or partition that is hosted by a control path drive.

To grant host access to a device (drive or partition), an access group resource must first be created (see Table 3: GET aml/access/groups). Once groups are defined, hosts must be added to an access group so that access can then be assigned to devices (see Table 17: GET aml/access/hosts, and Table 12: POST aml/access/group/{name}/hosts).

Drive devices and partitions (hosted by a control path drive) are added to the access groups to define the host access to the drive or partition (see Table 2: GET aml/access/devices and Table 7: POST aml/access/group/{name}/device).

NOTE: A host can only belong to a single access group.

4.4 Partition Resource Assignments

The following interface provides the capability to add and delete Drives, Storage, Import/Export (IE) and Extended IE (XIE) slots to and from a partition. Each of these resources are presented as a segment where Storage, IE and XIE segments contain either 6 slot magazine segments (Scalar i6000) or single slot segments (Scalar i3/i6/i6H). Drive segments contain a single drive element. To determine the location and type of a segment, use the "coordinate" element of the segment object. If a segment is removed/deleted from a partition, it is reassigned back to the physical library's pool of unassigned segments and hereby available for assignment to any other partition. To find all segments in the physical library, use the URI Table 279: GET aml/physicalLibrary/segments. This URI provides query parameters to filter for segment types, segment states, etc..

4.5 Partition Control Path Configuration

Standard partitions require a control path to support host connection for SCSI Medium Changer (SMC) control commands. The Scalar i6000, Scalar i6/i6H and Scalar i3 tape libraries do not automatically assign a control path when a partition is created. While the Scalar i3 and Scalar i6/i6H support control paths via drives that provide the physical interface,

The Scalar i6000 supports partition control paths via FC I/O blade connections or an Ethernet Expansion Blade connected LTO5 and higher tape drive.

A feature license is not required when configuring a single control path to a partition; however, redundant control path failover configurations require a Path Failover / Storage Networking (SNW) license in the Scalar i6000, and depending on configuration setting an Advanced Path Failover or Multipath Failover license in the Scalar i3 and Scalar i6/i6H tape library.

Basic Control Path Failover (BCPF) is supported only by the Scalar i6000 with HP LTO5 and/or LTO6 FC drives. This configuration enables an alternate control path via a second drive when the preferred control path via the primary control path drive fails.

Advanced Control Path Failover (ACPF) is supported with IBM and HP LTO drives requiring IBM LTO5 or HP LTO6 and higher FC drive generations. This configuration enables alternate control paths via configured redundant control path drives when the preferred control path connection fails. ACPF requires either an IBM drive or HP drive supported SCSI device driver on the attached host(s) to select the respective alternate path. A partition can support ACPF with either HP drives or IBM drives, but not a mixed solution as the ACPF with HP drives configures a primary and secondary/redundant control path connections, while ACPF with IBM drives configures all IBM control path drives as primary drives.

Multi-Path Failover (MPF) enables all configured primary control path drives to accept control commands. This configuration requires host application support for proper partition access.

4.6 Drive Data Path Configuration

Drives with two FC ports support configurations of different redundancy/failover settings. While the Scalar i6000 requires a *Path Failover / Storage Networking (SNW)* license to configure supported Basic Data Path Failover, Advanced Data Path Failover or Multi-Path Failover configurations, the Scalar i3 and Scalar i6/i6H support two licenses for specific configuration options, either a *Path Failover* license for Multi-Path Failover configurations or an *Advanced Path Failover* license for an Advanced Path Failover configuration.

Basic Data Path Failover (BDPF) is supported only by the Scalar i6000 with dual ported HP LTO5 and LTO6 FC drives only. This configuration enables an alternate data path when a preferred data path fails.

Advanced Data Path Failover (ADPF) is supported with IBM and HP LTO drives requiring dual ported IBM LTO5 or HP LTO6 and higher FC drive generations. This configuration enables an alternate data path when the preferred connection fails, but requires either an IBM drive or HP drive supported SCSI device driver on the attached host(s) to select the respective alternate path.

Multi-Path Failover (MPF) enables both drive ports and allows I/O via any connection link. This configuration requires host application support for proper drive access.

Note: The Scalar i3 with single-ported half-high drives does not support data path failover configurations.

4.7 Extended Data LifeCycle Management

The Extended Data Lifecycle Management (EDLM) requires an EDLM license. This feature is supported by the Scalar i6000 and Scalar i6. One license covers the entire library.

One library-managed partition is required for the media scans. This library-managed partition

is accessible only by a library administrator. It is not presented to any other application. The library-managed partition is assigned its own dedicated resources and EDLM scans may be performed for tapes configured for the EDLM partition or from other partitions configured for EDLM policies. Cartridges are moved into EDLM-scanning drives residing in the EDLM library managed partition and once scanned, tapes are returned to their original locations.

Automatic media scanning policies may be configured by partition. Each partition can have its own unique set of media scanning and action policies. Optionally, StorNext Storage Manager connections may be configured to trigger media scans and automatically copy data from suspect or failed tapes.

4.8 Partition Configuration and Operations

The following URIs provide the ability to change a partition's configuration and perform certain operations. To create a new partition, you must use the following interface: Table 182: POST `aml/partitions`. This interface does not allow the user to select specific storage or I/E slots or drives; the user can only specify the number of slots or drives they want assigned to the new partition. The interface does not provide for policies such as drive cleaning or automatic drive firmware leveling. If a user wants to create a partition with specific drive, IE and storage slot resources and configure partition policies, they will need to issue multiple Web Service interface requests.

For example, to create a standard partition with name "SalesPartition":

- Use the interface: Table 182: POST `aml/partitions` and specify only the required elements in the XML request.
- After this request has completed successfully, use the interface: Table 242: POST `aml/partition/{name}/segments`, interface to add specific slots, I/E and drives to the partition, see the interface for more details.
- To set up a drive cleaning policy for the partition use the following interface: Table 231: POST `aml/partition/{name}/policy/driveCleaning`; this interface also provides the capability to update and delete a drive cleaning policy from a partition.
- The partition drive leveling policy is provided using the interface: Table 234: GET `aml/partition/{name}/policy/driveLeveling`; this interface can also be used to remove selective firmware files from partition drive leveling (see interface for more information). To modify the partition name, barcode reporting, vendor ID and product ID in one request you could use the following interface: Table 197: PUT `aml/partition/{name}`.

4.9 Drive Cleaning Policies

Drive cleaning policies are configured on a per-partition basis. While IBM drives request drive cleaning operations per internal algorithms, HP LTO drives allow for selective configuration options to request cleaning after a configured tape motion hour interval. Library-managed EDLM partitions also allows for a number of mount count configuration to trigger drive cleaning operations once the selected mount count interval is reached.

Drive cleaning configurations support manual, library-initiated automatic cleaning, and application managed cleaning configurations. If hosts are performing cleaning (application managed), the library partition should not get configured for library-initiated, automatic cleaning too.

Note: The Scalar i6000 modified support for drive cleaning policies as of release i12.1 (710) to no longer require the use of the POST or DELETE method to configure or remove a drive cleaning policy for a partition. An element “enable” has been added to the driveCleaningPolicy object that determines if a policy is configured or not for a particular partition(driveCleaningPolicy.enable). The configuration of driveCleaningPolicy.driveCleaning.motionTime applies only to HP LTO5 drives or greater) and driveCleaningPolicy.driveCleaning.mountCount applies only to EDLM partitions.

4.10 IPv6 Network Configuration

The IPv6 configuration information and setup is handled differently than IPv4, since an interface (eth0 or eth2) can be configured to have multiple IPv6 addresses. With IPv4 an interface can only have one IP address.

To make a configurations request, see Table 337: GET aml/system/network/configurations, a netConfigurationList is returned containing netConfiguration objects:

```
<netConfiguration>
  <name>eth0 or eth2</name>
  <version>1</version> 1(IPv4) or 2(IPv6)
  <hostName>dvt4</hostName> The hostname assigned to this interface
  <type>1</type> -1(Unknown), 0(None), 1(Static), 2(DHCP), 3(DHCP6) and 4(Static and DHCP6)
  <netMask>255.255.248.0</netMask>
  <netGateway>10.20.168.1</netGateway>
  <ipAddress>10.20.171.14</ipAddress>
</netConfiguration>
```

For IPv4 netConfiguration objects, version element = 1, the type element can only be 1(Static) or 2(DHCP) and the netMask, netGateway and ipAddress elements will always contain a valid IPv4 address.

With IPv6 netConfiguration objects, version element =2, there will be only one object that will have a type element of 0(None), 1(Static), 3(DHCP6) or 4(Static and DHCP6) and all the rest of the objects will have a type element of -1(Unknown). The reason for -1 (Unknown) type is it cannot determine how this address was created: Manually, DHCP6, Stateless Address Autoconfiguration.

The netConfiguration object that contains a type element that is NOT -1 is used to determine if a static IPv6 address was configured (Manual Configuration) for this interface, whether DHCP6 was configured, whether both static and DHCP6 was configured or whether none, Static nor DHCP6 was configured. If the type is 1 or 4, the object will contain an IP address, which will be the static IP address.

The following object reports that both a static address and DHCP6 is configure on interface eth0, the type element is 4, and the ipAddress reported is the static IP.

```
<netConfiguration>
  <name>eth0</name>
  <version>2</version>
  <hostName>dvt4</hostName>
  <type>4</type>
  <netMask>64</netMask>
  <netGateway>2001::</netGateway>
  <ipAddress>2001::abcd/64</ipAddress>
</netConfiguration>
```


When you configure IPv6 (Static, DHCP, Both or None) for a particular interface (eth0 or eth2) use the netConfiguration object (see Table 339: PUT aml/system/network/configuration/{name}/{version}). Each time you request an update of the interface, you must specify all the values you want for the new configuration.

Note: When configuring a static IPv6 address on interface eth2, you do not need to supply a netGateway element. The gateway is not required.

5. Web Services API Request Summary

Table 1: GET aml/

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: *Minimum* <= 1 second; *Maximum* = 15 seconds

Description: Retrieve the library ping resource. The ping can be requested without logging in to the Web Services server (no authentication is needed). The ping can be used to discover the libraries on your network.

URI	aml/
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 168: ping

Table 2: GET aml/access/devices

Product Support: Scalar i6000

Response Time: *Minimum* <= 1 second; *Maximum* = 180 seconds

Description: Retrieve a list of configured Access Device resources that could be added to an Access Group.

An access device is a drive or partition.

For a drive access device, the drive must be HP LTO 5 or greater, belong to a partition, have an SNW license applied, must be in P2P/Fabric mode and be connected to an Ethernet Expansion Blade.

For a partition access device, the partition must have a control path drive and the drive must have the above prerequisites.

URI	aml/access/devices
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 1: accessDeviceList

Table 3: GET aml/access/groups

Product Support: Scalar i6000

Response Time: *Minimum* <= 1 second; *Maximum* = 180 seconds

Description: Retrieve a list of Access Group resources.

URI	<i>aml/access/groups</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 3: accessGroupList

Table 4: GET *aml/access/group/{name}*

Product Support: Scalar i6000

Response Time: *Minimum* <= 1 second; *Maximum* = 60 seconds

Description: Retrieve the Access Group resources identified by the URI path template “name”.

URI	<i>aml/access/group/{name}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 5: POST *aml/access/group/{name}*

Product Support: Scalar i6000

Response Time: *Minimum* <= 1 second; *Maximum* = 180 seconds

Description: Create a new Access Group with the name identified by URI path template “name”. To create a new access group with name “AG3”, use the following:
aml/access/group/AG3.

URI	<i>aml/access/group/{name}</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 6: DELETE aml/access/group/{name}

Product Support: Scalar i6000

Response Time: *Minimum* <= 1 second; *Maximum* = 60 seconds

Description: Delete the Access Group identified by the URI path template “name”.

URI	aml/access/group/{name}
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 7: POST aml/access/group/{name}/device

Product Support: Scalar i6000

Response Time: *Minimum* <= 1 second; *Maximum* = 120 seconds

Description: Add a new access device to the access group identified by the URI path template “name”. The <access> element must be set to true, otherwise access will not be granted on that port.

A partition accessDevice (type=2) is a drive that is configured as a control path drive (see Table 203: GET aml/partition/{name}/controlPath).

The following example would allow access on port 1 for the drive with serial number F001396025 to all hosts that belong to the identified access group.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:accessDevice xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>F001396025</serialNumber>
  <type>1</type>
  <port>
    <id>1</id>
    <access>true</access>
  </port>
</ns2:accessDevice>
```

URI	aml/access/group/{name}/device
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 2: accessDevice
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 8: PUT aml/access/group/{name}/device

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Update the access device that belongs to the access group identified by the URI path template “name”.

The example below modifies access so the first port on the device will no longer be seen and the second port will be seen by all hosts in the access group.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:accessDevice xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>F001396025</serialNumber>
  <type>1</type>
  <port>
    <id>1</id>
    <access>>false</access>
  </port>
  <port>
    <id>2</id>
    <access>>true</access>
  </port>
</ns2:accessDevice>
```

URI	aml/access/group/{name}/device
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 2: accessDevice
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 9: DELETE aml/access/group/{name}/device/{serialNumber}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Remove the access device with serial number identified by the URI path template “serialNumber” from the access group identified by the URI path template “name”. This access device (drive or partition) will no longer be seen by hosts belonging to this access group.

URI	aml/access/group/{name}/device/{serialNumber}
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 10: GET aml/access/group/{name}/devices

Product Support: Scalar i6000

Response Time: Minimum <= 5 seconds; Maximum = 120 seconds

Description: Retrieve the access devices configured for the access group identified by the URI path template “name”.

<i>URI</i>	<i>aml/access/group/{name}/devices</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 1: accessDeviceList

Table 11: POST aml/access/group/{name}/devices

Product Support: Scalar i6000

Response Time: Minimum <= 5 seconds; Maximum = 180 seconds

Description: Add the access device list to the access group identified by the URI path template “name”. None of the access devices may already belong to the access group.

Note: Access is on a port basis so the access element of each port must be set to true to grant access to each port on the device. Not all devices have multiple ports.

<i>URI</i>	<i>aml/access/group/{name}/devices</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 1: accessDeviceList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 12: POST aml/access/group/{name}/hosts

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Add a host to the Access Group resource identified by the URI path template “name”.

The only element required in the host object is WWPN. All other elements will be ignored.

URI	<i>aml/access/group/{name}/hosts</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 105: host
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 13: DELETE *aml/access/group/{name}/host/{WWPN}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete a host WWPN identified by the URI path template “WWPN” from the Access Group resource identified by the URI path template “name”.

To delete host with WWPN “1234ABCD:1234ABCD” from Access Group “AG2”, use the following URI: *aml/access/group/AG2/host/1234abcd:1234abcd*

URI	<i>aml/access/group/{name}/host/{WWPN}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 4: accessGroup

Table 14: GET *aml/access/host/{WWPN}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 10 seconds

Description: Retrieve the host resource identified by the URI path template “WWPN”. Use colon-separated template format *aml/access/host/1234ABCD:1234ABCD*

URI	<i>aml/access/host/{WWPN}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 105: host

Table 15: PUT aml/access/host/{WWPN}

Product Support: Scalar i6000

Response Time: Minimum <= 5 seconds; Maximum = 30 seconds

Description: Update the host resource identified by the URI path template “WWPN”. This would be primarily used to change the host name and host type. The WWPN element is required to find the host that needs to be updated.

URI	aml/access/host/{WWPN}
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 105: host
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 105: host

Table 16: DELETE aml/access/host/{WWPN}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 15 seconds

Description: Delete the host identified by the URI path template “WWPN”. This will remove the host from the libraries host cached data. An online host (mode = 1) cannot be deleted.

URI	aml/access/host/{WWPN}
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 17: GET aml/access/hosts

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 10 seconds

Description: Retrieve a list of host resources that were seen on the SAN from configured tape drives that are connected to the SAN.

URI	aml/access/hosts
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 104: hostList

Table 18: POST aml/access/hosts

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Create a new host resource.

Note: This functionality is used primarily for testing purposes.

<i>URI</i>	<i>aml/access/hosts</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 105: host
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: aml/access/host/{wwpn}
Response Data	See Figure 105: host

Table 19: GET aml/access/licenses

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve a list of drives that have a Storage Networking/Failover (SNW) license or are eligible to have an SNW license applied. An eligible drive must be owned by a partition.

Note: Most features that use an SNW license, require the drive to:

1. be attached to an Ethernet Expansion Blade (EEB) or be a dual-ported IBM drive, and
2. be an HP or IBM LTO5 drive type generation or greater.

A drive that has an SNW license applied to it will have the drive.settings.license element with a value of 11.

<i>URI</i>	<i>aml/access/licenses</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 32: driveList

Table 20: PUT aml/access/licenses

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Modify the SNW licenses for the drives in the requested driveList. The only drive elements required are the physicalSerialNumber or logicalSerialNumber and the settings.license.

To apply a license set the license element value to 11. To remove a license, set the license element to an empty string.

The example below applies a license to drive with serial number F001396043 and removes a license from the drive with serial number F00139603D.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F001396043</logicalSerialNumber>
    <settings>
      <license>11</license>
    </settings>
  </drive>
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <license></license>
    </settings>
  </drive>
</ns2:driveList>
```

When you apply an SNW license to a drive, that drive will no longer be seen on the SAN. The drive must then be configured in an Access Group before hosts can access the drive.

URI	aml/access/licenses
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 32: driveList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 32: driveList

Table 21: GET aml/access/license/{serialNumber}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 15 seconds

Description: Retrieve the drive identified by the URI path template “serialNumber”. This interface would be used to determine if the drive has an SNW license. Unlike the interface, Table 19: GET aml/access/licenses, the drive returned may not be eligible for an SNW license.

URI	aml/access/license/{serialNumber}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	None (dataStore support deprecated)

Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 33: drive

Table 22: POST [aml/access/license/{serialNumber}](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 10 seconds

Description: Apply an SNW license to the drive identified by the URI path template “serialNumber”.

<i>URI</i>	<i>aml/access/license/{serialNumber}</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	201, 403, 404
Response Header	Content-Type:application/xml or application/json Location: aml/access/license/{serialNumber}
Response Data	See Figure 225: WSResultCode

Table 23: DELETE [aml/access/license/{serialNumber}](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 15 seconds

Description: Remove an SNW license from the drive identified by the URI path template “serialNumber”.

You cannot remove an SNW license from a drive if it is currently configured for Data Path Failover or Control Path Failover.

<i>URI</i>	<i>aml/access/license/{serialNumber}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 24: GET [aml/device/settings/robot](#)

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 120 seconds

Description: Retrieve the configurable robot settings.

URI	aml/device/settings/robot
Method	GET
User Role Access	Admin, Service, User
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 189: robotSettings

Table 25: PUT aml/device/settings/robot

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the robot settings. The configurable settings include the following:

- parkingDelay – Set the number of seconds the robot waits before parking. Valid values are 5 – 900, inclusive.
- serviceTrayRelease – Enable or disable physical button functionality to request the robot prepare for replacement into the Service Tray.

URI	aml/device/settings/robot
Method	PUT
User Role Access	Admin, Service
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 189: robotSettings
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 189: robotSettings

Table 26: GET aml/devices/blades

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Retrieve a list of blade resources.

URI	aml/devices/blades
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000), 140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 12: bladeList

Table 27: GET aml/devices/blades/ethernet**Product Support:** Scalar i6000**Response Time:** Minimum <= 10 seconds; Maximum = 120 seconds**Description:** Retrieve a list of ethernetExpansionBlade (Ethernet Expansion Blade (EEB)) resources. EEBs provide the option for Ethernet connectivity to LTO-5 and higher drives (for MCB-to-drive communication purposes only). The EEB provides a control path to the drive for commands as well as facilitates taking drive logs and downloading drive firmware.

<i>URI</i>	<i>aml/devices/blades/ethernet</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 76: ethernetExpansionBladeList

Table 28: GET aml/devices/blade/ethernet/{serialNumber}**Product Support:** Scalar i6000**Response Time:** Minimum <= 10 seconds; Maximum = 60 seconds**Description:** Retrieve an ethernetExpansionBlade resource identified by the URI path template “serialNumber”.

<i>URI</i>	<i>aml/devices/blade/ethernet/{serialNumber}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 77: ethernetExpansionBlade

Table 29: GET aml/devices/blade/ethernet/{serialNumber}/operations/identify**Product Support:** Scalar i6000**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Retrieve the EEB identify task identified by the URI path template “serialNumber”.

<i>URI</i>	<i>aml/devices/blade/ethernet/{serialNumber}/identify</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A

Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 30: POST [aml/devices/blade/ethernet/{serialNumber}/operations/identify](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Start the EEB identify task identified by the URI path template “serialNumber”. This starts the status LED on the EEB to flash rapidly.

URI	<i>aml/devices/blade/ethernet/{serialNumber}/identify</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 31: DELETE [aml/devices/blade/ethernet/{serialNumber}/operations/ identify](#)

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Stop the EEB identify task identified by the URI path template “serialNumber”. This stops the status LED on the EEB from flashing rapidly.

URI	<i>aml/devices/blade/ethernet/{serialNumber}/identify</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 32: GET [aml/devices/blade/ethernet/{serialNumber}/operations/powerCycle](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the last request EEB power cycle task identified by the URI path template “serialNumber”.

URI	<i>aml/devices/blade/ethernet/{serialNumber}/powerCycle</i>
Method	GET
User Role Access	Admin, Service, User

Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 33: POST aml/devices/blade/ethernet/{serialNumber}/operations/powerCycle

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Power cycle the EEB identified by the URI path template “serialNumber”. This is an asynchronous request, use the interface, Table 32: GET aml/devices/blade/ethernet/{serialNumber}/operations/powerCycle, to determine when the power cycle has finished.

URI	aml/devices/blade/ethernet/{serialNumber}/powerCycle
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 34: GET aml/devices/blades/fibreChannel

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 120 seconds

Description: Retrieve a list of fcBlade (FC IO Blades) resources. There is one Fibre Channel (FC) I/O blade type supported: 7404 that auto-negotiates up to 4 Gbps. The 7404 FC I/O blade has an embedded controller that provides connectivity and features that enhance the performance and reliability of tape operations. It also provides two host communication ports and four connection ports to drives.

URI	aml/devices/blades/fibreChannel
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 85: fcBladeList

Table 35: GET aml/devices/blades/fibreChannel/hosts

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Retrieve the FC IO Blade host resources list. This list reports the blade and hosts seen by that blade. Multiple blades may see the same host. In essence, this interface reports the blades and the host seen by those blades.

<i>URI</i>	<i>aml/devices/blades/fibreChannel/hosts</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 87: fcBladeHostsList

Table 36: GET aml/devices/blades/fibreChannel/hpf

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 120 seconds

Description: Retrieve the FC IO Blade host port failover resource list. This list reports the host port failover configuration for each blade installed in the library. Host port failover only applies to the host (target) ports on the IO blade, 1 and 2.

<i>URI</i>	<i>aml/devices/blades/fibreChannel/hpf</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 90: fcHostPortFailoverList

Table 37: GET aml/devices/blade/fibreChannel/{serialNumber}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the FC IO Blade identified by the URI path template “serialNumber”.

<i>URI</i>	<i>aml/devices/blade/fibreChannel/{serialNumber}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 86: fcBlade

Table 38: GET aml/devices/blade/fibreChannel/{serialNumber}/hosts

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Retrieve the FC IO Blade Hosts identified by the URI path template “serialNumber”.

URI	aml/devices/blade/fibreChannel/{serialNumber}/hosts
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 88: fcBladeHosts

Table 39: POST aml/devices/blade/fibreChannel/{serialNumber}/hosts

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create an FC IO Blade host resource. This interface is provided to define hosts, if they are currently not yet connected. For example, the following “TEST_HOST” will be detected by the blade with serial number “AMQ002639-0009”.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladeHosts xmlns:ns2="http://automatedMediaLibrary/">
  <host>
    <name>TEST_HOST</name>
    <type>3</type>
    <mode>1</mode>
    <WWPN>1234ABCD:1234ABCD</WWPN>
    <port>0</port>
  </host>
  <blade>
    <coordinate>
      <frame>2</frame>
      <rack>1</rack>
      <section>1</section>
      <column>7</column>
      <row>1</row>
      <type>0</type>
    </coordinate>
    <name>FC IO Blade</name>
    <type>1</type>
    <firmwareVersion>5.12.01.50</firmwareVersion>
    <serialNumber> AMQ002639-0009</serialNumber>
  </blade>
</ns2:fcBladeHosts>
```

The blade with serial number “AMQ002639-0009” must exist. The host.WWPN must not already be configured on this blade. The WWPN is the unique identifier for a host configured on the blade. The elements highlighted are the only ones that are required. All other elements

will be ignored. The fcBladeHosts object must only contain one host and blade object. If more than one host object is included, the request will fail.

Note: The WWPN ‘1234ABCD:1234ABCD’ and ‘1234abcd:1234abcd’ are considered the same. The WWPN is case-insensitive.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/hosts</i>
Method	POST
User Role Access	Admin, Service
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 88: fcBladeHost
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: aml/devices/blades/fibreChannel/host/{wwpn}
Response Data	See Figure 225: WSResultCode

Table 40: GET aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve the FC IO Blade Host for the host identified by the URI path template “wwpn” and the blade identified by the URI template “serialNumber”. This interface is the same as Table 38: GET aml/devices/blade/fibreChannel/{serialNumber}/hosts, except this interface will only include the host object with the requested wwpn in the fcBladeHosts object. A host is uniquely identified by the blade to which it is connected, since any operation on that host, changing its name, deleting it, LUN Mapping, etc. must be done in the context of the blade to which it is connected since the same physical host may be connected to multiple blades.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 88: fcBladeHosts

Table 41: PUT aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Update the FC IO Blade Host for the identified by the URI path template “wwpn” and the blade identified by the URI path template “serialNumber”. The following example modifies a host with WWPN “1234ABCD:1234ABCD” that is seen by the blade with serial number “AMQ002639-0009”.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```

<ns2:fcBladeHosts xmlns:ns2="http://automatedMediaLibrary/">
  <host>
    <name>TEST</name>
    <type>3</type>
    <WWPN>1234ABCD:1234ABCD</WWPN>
    <port>0</port>
  </host>
</blade>
<serialNumber>AMQ002639-0009</serialNumber>
</blade>
</ns2:fcBladeHosts>

```

The blade with serial number “AMQ002639-0009” and host with WWPN “1234ABCD:1234ABCD” must exist. The elements highlighted are the only ones that can be modified.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}</i>
Method	PUT
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 88: fcBladeHosts
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 88: fcBladeHosts

Table 42: DELETE *aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Delete the FC IO Blade Host resource for the host identified by the URI path template “wwpn” and the blade identified by the URI path template “serialNumber”.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}</i>
Method	DELETE
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 43: GET *aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}/mapping*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 120 seconds

Description: Retrieve the FC IO Blade Host Mapping resource for the host identified by the URI path template “wwpn” and the blade identified by the URI path template “serialNumber”. Host LUN mapping enables you to create a virtual private remapping of available LUNs for a specific Fibre Channel-attached host. LUN mapping is required to give hosts access to partitions and drives. You can also make devices appear to the host as if they were at lower

LUNs in order to optimize system performance.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}/mapping</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 92: fcLunMapping

Table 44: PUT *aml/devices/blade/fibreChannel/{serialNumber}/host/{wwpn}/mapping*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 120 seconds

Description: Update the FC IO Blade Host Mapping resource for the host identified by the URI path template “wwpn” and the blade identified by the URI path template “serialNumber”. This feature provides the ability to give a selected host access to partitions and drives. By default, the host(s) connected to the blade will not have access to the devices (drives and partitions) presented by that blade.

The following example configures the blade with serial number ‘AMQ002753-0039’ to allow access to partition ‘PartitionSales’ using LUN number 4 and drive ‘1013000426’ using LUN number 10 to host with WWPN ‘2100001b:328586ab’.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcLunMapping xmlns:ns2="http://automatedMediaLibrary/">
  <fcBladeHost>
    <hostWwpn>2100001b:328586ab</hostWwpn>
    <bladeSerialNumber> AMQ002753-0039</bladeSerialNumber>
    <mapping>
      <deviceName>PartitionSales</deviceName>
      <deviceSerialNumber>273190049_LL4</deviceSerialNumber>
      <deviceType>2</deviceType>
      <internalLun>4</internalLun>
      <externalLun>4</externalLun>
    </mapping>
    <mapping>
      <deviceName>IBM ULTRIUM-TD7-Fibre</deviceName>
      <deviceSerialNumber>1013000426</deviceSerialNumber>
      <deviceType>1</deviceType>
      <internalLun>10</internalLun>
      <externalLun>-1</externalLun>
    </mapping>
  </ns2:fcLunMapping>
```

In the above example, the required fields are highlighted. The mapping.internalLun element cannot be modified. The mapping.externalLun element number cannot be already used by another mapping device. The valid values for this element are -1 to 255. To remove access for a mapped device, set the externalLun to ‘-1’. When set to -1, the host will no longer see this device.

Note: If a partition is deleted, see Table 198: DELETE *aml/partition/{name}*, the partition

mapping device and the drive mapping devices associated with that partition will no longer be reported for the fcHostBlade.

There is also a Command and Control LUN device, type (3), which is mapped by default to externalLun 0 and is always reported as internalLun 0. This device should rarely, if ever, be modified. It is used by the host to scan available LUNs.

URI	<i>aml/devices/blades/fibreChannel/{serialNumber}/host/{wwpn}/mapping</i>
Method	PUT
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 92: fcLunMapping
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 92: fcLunMapping

Table 45: GET *aml/devices/blade/fibreChannel/{serialNumber}/hpf*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 120 seconds

Description: Retrieve the FC IO Blade host port failover resource for the blade identified by the URI path template “serialNumber”. Host port failover only applies to the host (target) ports on the IO blade, 1 and 2.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/hpf</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 91: fcHostPortFailover

Table 46: PUT *aml/devices/blade/fibreChannel/{serialNumber}/hpf*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 120 seconds

Description: Update the FC IO Blade host port failover (hpf) resource for the blade identified by the URI path template “serialNumber”. Enabling hpf allows the “standby” port on an IO blade the ability to assume the identity and LUN mapping configuration of the primary “active” target port if the primary port fails. The target ports (1 and 2) must be configured in point to point (Fabric) topology and public target mode. To enable hpf, channel zoning must be configured correctly, both target ports must be zoned to the same initiator ports.

The following example enables hpf on the blade with serial number AMP015770-0075. The primary port will be set to port 2 and port 1 will take on the responsibility of the standby port. The link down status will be reported after 5 seconds of the physical link being down.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcHostPortFailover xmlns:ns2="http://automatedMediaLibrary/">
  <bladeSerialNumber>AMP015770-0075</bladeSerialNumber>
  <configuration>
    <enabled>true</enabled>
    <linkDownDelayTime>5</linkDownDelayTime>
    <primaryPort>2</primaryPort>
  </configuration>
</ns2:fcHostPortFailover>
```

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/hpf</i>
Method	PUT
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 91: fcHostPortFailover
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 91: fcHostPortFailover

Table 47: PUT aml/devices/blade/fibreChannel/{serialNumber}/hpf/intervention

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 120 seconds

Description: Enable the FC IO Blade host port failover port(s) for the blade identified by the URI path template “serialNumber”. Intervention is required when a target port fails due to link problems or some other event. This interface should only be used when hpf is enabled and any of the fcHostPortFailover.port.intervention elements is set to ‘true’.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/hpf/intervention</i>
Method	PUT
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 91: fcHostPortFailover

Table 48: GET aml/devices/blade/fibreChannel/{serialNumber}/operations/identify

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the FC IO Blade identify task identified by the URI path template “serialNumber”.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/operations/identify</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A

Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 49: POST [aml/devices/blade/fibreChannel/{serialNumber}/operations/identify](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Start the FC IO Blade identify task identified by the URI path template “serialNumber”. This starts the status LED on the IO Blade to flash rapidly.

URI	aml/devices/blade/fibreChannel/{serialNumber}/operations/identify
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json Location: aml/devices/blade/fibreChannel/{serialNumber}/operations/identify
Response Data	See Figure 209: task

Table 50: DELETE [aml/devices/blade/fibreChannel/{serialNumber}/operations/identify](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Stop the FC IO Blade identify task identified by the URI path template “serialNumber”. This stops the status LED on the IO Blade from flashing rapidly.

URI	aml/devices/blade/fibreChannel/{serialNumber}operations//identify
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 51: GET [aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the FC IO Blade power cycle task identified by the URI path template “serialNumber”.

URI	aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle
Method	GET

User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 52: POST [aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle](#)

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Start the FC IO Blade power cycle task identified by the URI path template “serialNumber”. This operation will power-cycle the IO Blade.

URI	aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json Location: aml/devices/blade/fibreChannel/{serialNumber}/operations/powerCycle
Response Data	See Figure 209: task

Table 53: GET [aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the FC IO Blade reboot task identified by the URI path template “serialNumber”.

URI	aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 54: POST [aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot](#)

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Start the FC IO Blade reboot task identified by the URI path template “serialNumber”. This operation will reboot the IO Blade.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json Location: aml/devices/blade/fibreChannel/{serialNumber}/operations/reboot
Response Data	See Figure 209: task

Table 55: POST *aml/devices/blade/fibreChannel/{serialNumber}/port/{id}/operations/reset*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Reset the fibre channel blade’s port identified by the URI path’s blade ‘serial number’ and port ‘id’.

URI	<i>aml/devices/blade/fibreChanned/{serial_number}/port/{id}/reset</i>
Method	POST
User Role Access	Admin, Service
Version	779(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 56: GET *aml/devices/blade/fibreChannel/{serialNumber}/ports*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Retrieve the FC IO Blade ports resource for the blade identified by the URI path template “serialNumber”.

URI	<i>aml/devices/blade/library/{serialNumber}/ports</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 93: fcBladePortList

Table 57: PUT aml/devices/blade/fibreChannel/{serialNumber}/ports

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Update the FC IO Blade ports resource for the blade identified by the URI path template “serialNumber”. The following example configures ports 1 and 2:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladePortList xmlns:ns2="http://automatedMediaLibrary/">
  <bladeSerialNumber>AMQ002639-0009</bladeSerialNumber>
  <fcBladePort>
    <number>1</number>
    <softLoop>true</softLoop>
    <loopId>0</loopId>
    <mode>17</mode>
    <topology>1</topology>
    <autoSpeed>true</autoSpeed>
    <speed>0</speed>
    <frameSize>2048</frameSize>
  </fcBladePort>
  <fcBladePort>
    <number>2</number>
    <softLoop>true</softLoop>
    <loopId>0</loopId>
    <mode>17</mode>
    <topology>1</topology>
    <autoSpeed>true</autoSpeed>
    <speed>0</speed>
    <frameSize>2048</frameSize>
  </fcBladePort>
</ns2:fcBladePortList>
```

URI	aml/devices/blade/fibreChannel/{serialNumber}/ports
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 93: fcBladePortList
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 93: fcBladePortList

Table 58: GET aml/devices/blade/fibreChannel/{serialNumber}/zoning

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Retrieve the FC IO Blade channel zoning configuration resource for the blade identified by the URI path template “serialNumber”. Channel zoning enables you to control access between specific host (target) ports (1 and 2) and initiator ports (these are always connected to tape drives, 3,4,5 and 6) on an IO blade in the library.

URI	aml/devices/blade/library/{serialNumber}/zoning
Method	GET

User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 89: fcBladeZoning

Table 59: PUT aml/devices/blade/fibreChannel/{serialNumber}/zoning

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Update the FC IO Blade channel zoning configuration resource for the blade identified by the URI path template “serialNumber”. The following example allows access to hosts connect to ports 1 and 2 access to drives connected to ports 5 and 6 on the blade with serial number ‘AMQ002639-0009’:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladeZoning xmlns:ns2="http://automatedMediaLibrary/">
  <bladeSerialNumber>AMQ002639-0009</bladeSerialNumber>
  <targetPort>
    <portNumber>1</portNumber>
    <initiatorPort>
      <portNumber>3</portNumber>
      <accessEnabled>>false</accessEnabled>
    </initiatorPort>
    <initiatorPort>
      <portNumber>4</portNumber>
      <accessEnabled>>false</accessEnabled>
    </initiatorPort>
    <initiatorPort>
      <portNumber>5</portNumber>
      <accessEnabled>>true</accessEnabled>
    </initiatorPort>
    <initiatorPort>
      <portNumber>6</portNumber>
      <accessEnabled>>true</accessEnabled>
    </initiatorPort>
  </targetPort>
  <targetPort>
    <portNumber>2</portNumber>
    <initiatorPort>
      <portNumber>3</portNumber>
      <accessEnabled>>false</accessEnabled>
    </initiatorPort>
    <initiatorPort>
      <portNumber>4</portNumber>
      <accessEnabled>>false</accessEnabled>
    </initiatorPort>
    <initiatorPort>
      <portNumber>5</portNumber>
      <accessEnabled>>true</accessEnabled>
    </initiatorPort>
    <initiatorPort>
      <portNumber>6</portNumber>
    </initiatorPort>
  </targetPort>
</ns2:fcBladeZoning>
```

```

    <accessEnabled>true</accessEnabled>
  </initiatorPort>
</targetPort>
</ns2:fcBladeZoning>

```

You will not be allowed to re-configure channel zoning on a blade that has host port failover (hpf) configured.

URI	<i>aml/devices/blade/fibreChannel/{serialNumber}/zoning</i>
Method	PUT
User Role Access	Admin, Service
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 89: fcBladeZoning
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 89: fcBladeZoning

Table 60: GET *aml/devices/blades/firmware*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the blade firmware resource list.

URI	<i>aml/devices/blades/firmware</i>
Method	GET
User Role Access	Admin, Service, User
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 14: bladeFirmwareList

Table 61: POST *aml/devices/blades/firmware*

Product Support: Scalar i3, Scalar i6/i6H

License Requirement: Service

Response Time: Minimum <= 30 seconds; Maximum = 180 seconds

Description: Upload the blade firmware bundle to the library. The multipart form data key is 'file' and the value is the file to be uploaded.

URI	<i>aml/devices/blades/firmware</i>
Method	POST
User Role Access	Admin, Service
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: multipart/formdata
Request Data	File to be updated
Response Codes	200

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 62: GET aml/devices/blades/library

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the library main controller blade (MCB) list resource.

URI	aml/devices/blades/library
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 116: libraryControlBladeList

Table 63: GET aml/devices/blade/library/{serialNumber}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the library controller blade resource identified by the URI path template “serialNumber”.

URI	aml/devices/blade/library/{serialNumber}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 117: libraryControlBlade

Table 64: GET aml/devices/blades/lufs

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the LTFS blade resource list.

URI	aml/devices/blades/lufs
Method	GET
User Role Access	Admin, Service, User
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 129: ItfsBladeList

Table 65: GET aml/devices/blade/itfs/{sectionNumber}

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Get the LTFS blade resource identified by the URI path template “sectionNumber”.

<i>URI</i>	<i>aml/devices/blade/itfs/{sectionNumber}</i>
Method	GET
User Role Access	Admin, Service, User
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 130: ItfsBlade

Table 66: DELETE aml/devices/blade/itfs/{sectionNumber}

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Delete the LTFS blade resource identified by the URI path template “sectionNumber”.

<i>URI</i>	<i>aml/devices/blade/itfs/{sectionNumber}</i>
Method	DELETE
User Role Access	Admin, Service
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 67: GET aml/devices/blades/windows

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the Windows blade resource list.

<i>URI</i>	<i>aml/devices/blades/windows</i>
Method	GET
User Role Access	Admin, Service, User
Version	140(i3/i6/i6H)
Parameters	N/A

Request Header	N/A
Request Data	N/A
Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 224: windowsBladeList

Table 68: GET aml/devices/blade/windows/{sectionNumber}

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Get the Windows blade resource identified by the URI path template “sectionNumber”.

<i>URI</i>	<i>aml/devices/blade/windows/{sectionNumber}</i>
Method	GET
User Role Access	Admin, Service, User
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 223: windowsBlade

Table 69: DELETE aml/devices/blade/windows/{sectionNumber}

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Delete the Windows blade resource identified by the URI I path template “sectionNumber”.

<i>URI</i>	<i>aml/devices/blade/windows/{sectionNumber}</i>
Method	DELETE
User Role Access	Admin, Service
Version	140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200,
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 70: GET aml/devices/ieStations

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of ieStation resources. I/E stations enable you to import and export cartridges without interrupting normal library operation. There are two types of I/E stations on Scalar i6000 libraries: 24-slot I/E stations and 72-slot I/E stations.

URI	<i>aml/devices/ieStations</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 107: ieStationList

Table 71: GET *aml/devices/ieStation/{number}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the ieStation resource identified by the URI path template “number”.

URI	<i>aml/devices/ieStation/{number}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 108: ieStation

Table 72: GET *aml/devices/ieStation/{number}/lock*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the ieStation resource lock status identified by the URI path template “number”. The valid status are 1 (locked) or 2 (Unlocked).

URI	<i>aml/devices/ieStation/{number}/lock</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	1 or 2

Table 73: PUT *aml/devices/ieStation/{number}/lock*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the ieStation resource lock status identified by the URI path template

“number”. The valid lock values are 1 (locked) or 2 (Unlocked).

URI	<i>aml/devices/ieStation/{number}/lock</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 (lock) or 2 (unlock)
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 74: GET *aml/devices/magazines*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of magazine resources. A magazine is the removable tray containing tape cartridge slots. Magazine columns on the right may be configured for Storage and/or Import/Export (IE) slots.

Note: The reported coordinate section number indicates the vertical section location and the column number indicates whether it is a right, left or center magazine. A left magazine’s column is the left most column and is always 1. A right magazine’s column is the right most column and is product dependent. In a Scalar i3 and i6, a right magazine column is 10, and in a Scalar i6H, it is 12. An optional center Drive Bay Storage magazine column is also product dependent and is either reporting column 11 or 13 for a i6 or Scalar i6H, respectively. The coordinate row number is always one.

URI	<i>aml/devices/magazines</i>
Method	GET
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 132: magazineList

Table 75: PUT *aml/devices/magazines*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the magazine release button functionality for one or more magazines. For each magazine object in the request data, the required elements are *coordinate* and *enabledRelease*.

To enable or disable the magazine release button functionality for all magazines in the library, see also Table 81: PUT *aml/devices/magazines/release*.

Note: See Table 74: GET *aml/devices/magazines* for an explanation of how a magazine

coordinate is specified.

URI	aml/devices/magazines
Method	PUT
User Role Access	Admin, Service
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 132: magazineList
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 132: magazineList

Table 76: GET aml/devices/magazines/ieSlots

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the ieSlots resource. An ieSlots object is used to configure or report how many Import/Export (IE) slots are configured in a Scalar I3 or Scalar i6/i6H library. The IE slots are configured in increments of 5. It is also used to configure and report the IE assignment mode. This mode determines how media placed in the IE slots are assigned to partitions.

URI	aml/devices/magazines/ieSlots
Method	GET
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 106: ieSlots

Table 77: PUT aml/devices/magazines/ieSlots

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the IE slots count and/or the assignment mode. Either the slotCount element or assignmentMode element (or both) may be specified. The slotCount element must be in increments of 5, with a minimum value of 0 (no IE slots configured) and a maximum of 240. The library will decide where to physically assign the IE slots. If only the assignment mode is being set, the slot count element should be set to -1.

Note: If IE slots are configured in a Scalar i6/i6H Service Module, all 10/12 magazine slots must be configured as IE. (Added in Scalar i6/i6H version 220.)

URI	aml/devices/magazines/ieSlots
Method	PUT
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A

Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 106: ieSlots
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 106: ieSlots

Table 78: POST aml/devices/magazines/eject

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 360 seconds

Description: Eject the magazines from the library. This allows the removal of the magazines from the library. The coordinate element of the magazine object is used to determine which magazine to eject. Only the coordinate element of the magazine object is required.

Note: See Table 74: GET aml/devices/magazines for an explanation of how a magazine coordinate is specified.

<i>URI</i>	<i>aml/devices/magazines/eject</i>
Method	POST
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 132: magazineList
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 79: POST aml/devices/magazines/ieAssign

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Assign the media in configured IE slots to a partition. Only the unassigned media will get assigned.

<i>URI</i>	<i>aml/devices/magazine/ieAssign</i>
Method	POST
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	The partition name
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 80: POST aml/devices/magazine/eject

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 60 seconds

Description: Eject a magazine from the library. This allows the removal of the magazine from

the library. The coordinate element of the magazine object is used to determine which magazine to eject. Only the coordinate object is required.

Note: See Table 74: GET aml/devices/magazines for an explanation of how a magazine coordinate is specified.

URI	aml/devices/magazine/eject
Method	POST
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 133: magazine
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 81: PUT aml/devices/magazines/release

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the release status for all magazines. The valid release values are 1 (enabled) or 2 (disabled).

To enable or disable the magazine release button functionality for selective magazines, see Table 75: PUT aml/devices/magazines.

URI	aml/devices/magazines/release
Method	PUT
User Role Access	Admin, Service
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1(enable) or 2(disable)
Response Codes	200, 403
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 82: GET aml/devices/robots

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of robot object resources.

URI	aml/devices/robots
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 187: robotList

Table 83: GET aml/devices/robots/enable

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current ready state, 'true' or 'false', of the robotics. If true, the library aisle power is enabled and the robotics are operational. If false, the library aisle power is disabled; i.e. the Control Module door had been opened.

<i>URI</i>	<i>aml/devices/robots/enable</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: text/plain or application/json
Response Data	'true' or 'false'

Table 84: POST aml/devices/robots/enable

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the robotics to enable. This simulates the pushing of the 'Enable Robotics' button on the Control Module of the i6000. This enables library aisle power, so robotics become operational. All module doors must be closed and the library aisle must be clear from any obstruction.

<i>URI</i>	<i>aml/devices/robots/enable</i>
Method	POST
User Role Access	Admin, Service
Version	735(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 85: GET aml/devices/robot/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the robot resource identified by the URI path template.

<i>URI</i>	<i>aml/devices/robot/{name}</i>
Method	GET
User Role Access	Admin, Service, User

Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 188: robot

Table 86: GET aml/devices/robot/{name}/state

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the state of a robot identified by the URI path template “name”.

<i>URI</i>	<i>aml/devices/robot/{name}/state</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1 (Varied On) or 2 (Varied Off)

Table 87: PUT aml/devices/robot/{name}/state

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Update the state of a robot identified by the URI path template “name”.

<i>URI</i>	<i>aml/devices/robot/{name}/state</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 (Varied On) or 2 (Varied Off)
Response Codes	200, 403, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1 (Varied On) or 2 (Varied Off)

Table 88: POST aml/devices/robot/{name}/park

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 30 seconds; Maximum = 120 seconds

Description: Park and vary off the robot identified by the URI path template “name”.

The request data value indicates the park location. A value of 1 will position the robot for removal and replacement. The robot will be varied off and will no longer be operational. A value of 2 will position the robot at the bottom of the library. The robot will remain operational

and subsequent motion requests will be accepted.

URI	<i>aml/devices/robot/{name}/park</i>
Method	POST
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 (position for removal) or 2(position at bottom floor)
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 89: GET aml/devices/towers

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve the list of tower resources. Towers are high-density expansion modules (HDEM). These modules have larger storage capacities making them ideal for libraries where space is an issue.

URI	<i>aml/devices/towers</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 213: towerList

Table 90: GET aml/devices/tower/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the tower resource identified by the URI path template “id”.

URI	<i>aml/devices/tower/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 214: tower

Table 91: POST aml/devices/tower/{id}/identify

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Identify the tower resource identified by the URI path template “id”. The Tower Enable status LED on the rear tower door will flash rapidly for about one minute.

<i>URI</i>	<i>aml/devices/tower/{id}/identify</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 92: GET aml/devices/tower/{id}/mode

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the mode of the tower resource identified by the URI path template “id”.

<i>URI</i>	<i>aml/devices/tower/{id}/mode</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1 (Online) or 2 (Offline)

Table 93: PUT aml/devices/tower/{id}/mode

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the mode of the tower resource identified by the URI path template “id”.

<i>URI</i>	<i>aml/devices/tower/{id}/mode</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 (Online) or 2 (Offline)
Response Codes	200, 403, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1 (Online) or 2 (Offline)

Table 94: POST aml/devices/tower/{id}/reset

Product Support: Scalar i6000

Response Time: Minimum <= 60 seconds; Maximum = 180 seconds

Description: Reset the tower's controller board identified by the URI path template "id".

Note: The tower must be varied off before you can reset its controller board.

URI	<i>aml/devices/tower/{id}/reset</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 95: GET *aml/devices/tower/{id}/state*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the state of the tower identified by the URI path template "id".

URI	<i>aml/devices/tower/{id}/state</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1(Varied On) or 2(Varied Off)

Table 96: PUT *aml/devices/tower/{id}/state*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the state of the tower identified by the URI path template "id".

URI	<i>aml/devices/tower/{id}/state</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 (Vary On) or 2 (Vary Off)
Response Codes	200, 403, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1(Varied On) or 2(Varied Off)

Table 97: GET aml/devices/usb

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the USB resource installed on the library.

<i>URI</i>	<i>aml/devices/usb</i>
Method	GET
User Role Access	Admin, Service, User
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 215: usb

Table 98: POST aml/devices/usb

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 180 seconds

Description: Enable the USB resource installed on the library. This will initialize the USB device if it has not already been initialized. If it is determined that the device is from another library, you will not be able to enable it. You will need to erase the device first before you could enable it for this library.

<i>URI</i>	<i>aml/devices/usb</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 215: usb

Table 99: DELETE aml/devices/usb

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Disable the USB resource installed on the library. This will prevent any backups from occurring.

<i>URI</i>	<i>aml/devices/usb</i>
Method	DELETE
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 100: POST aml/devices/usb/backup

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Start a backup to the USB resource installed on the library. The USB must be in an active state.

<i>URI</i>	<i>aml/devices/usb/format</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 101: POST aml/devices/usb/restore

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 180 seconds

Description: Restore the most recent backup image contained on the USB drive installed on the library. The library will automatically be rebooted when the restore completes. The USB device must be mounted before you can perform a restore.

<i>URI</i>	<i>aml/devices/usb/restore</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 102: POST aml/devices/usb/erase

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Erase the contents of the USB drive installed on the library, all backed up data will be lost. The USB must be disabled before you can erase it.

<i>URI</i>	<i>aml/devices/usb/erase</i>
Method	POST
User Role Access	Admin, Service

Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 103: POST aml/devices/usb/pause

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Pause the USB drive installed on the library. This will prevent any backups from occurring. The USB must be enabled before you can request a pause operation.

<i>URI</i>	<i>aml/devices/usb/pause</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 104: POST aml/devices/usb/resume

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Resume the backup state of the USB drive installed on the library. This will revert the paused state and allow backups to resume. The USB must be in a paused state before you can request a resume.

<i>URI</i>	<i>aml/devices/usb/resume</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 105: POST aml/devices/usb/eject

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Eject the USB drive installed on the library. This prepares the drive to be

physically removed from the library. If the drive is active for backups it cannot be ejected.

URI	<i>aml/devices/usb/eject</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 106: GET aml/drives

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve all tape drive resource instances. To filter the number of drives you want to receive use the query parameters described below.

URI	<i>aml/drives</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameter names are “partition” and “status” (dataStore parameter is deprecated). The valid value for the named parameters are as follows:</p> <ul style="list-style-type: none"> • partition = “partition name” • status = “available” or “used” <p>To retrieve all the drive in the library use “aml/drives”. To retrieve all drives not belonging to a partition use “aml/drives?status=available” To retrieve all drives belonging to a partition named Sales use “aml/drives?partition=Sales”</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 32: driveList

Table 107: DELETE aml/drives/firmware/image/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the specified drive firmware file identified by the 'name' path parameter.

URI	<i>aml/drives/firmware/image/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A

Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 108: GET aml/drives/firmware/images

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of currently installed firmware images.

<i>URI</i>	<i>aml/ drives/firmware/images</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameter names are vendor and type, with the following values <ul style="list-style-type: none"> • vendor=IBM or HP • type=LTO2, LTO3, LTO4, LTO5, LTO6, LTO7, LTO8 and LTO9
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 97: firmwareFileList

Table 109: POST aml/drives/firmware/images

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Upload a drive firmware image using multi-part form data where the key is 'file' and the value is the firmware image file to be uploaded.

Note: The firmware file name must have one of the following extensions, .drv or .fmr or .fmrz or .img or .ro or .e or .frm, and the entire name case insensitive.

<i>URI</i>	<i>aml/ drives/firmware/images</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: multipart/form-data
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 110: GET aml/drives/firmware/operations/update

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve progress information of any current drive firmware update operations.

This returns a firmwareStatusList object. The updateState element is set to 2 while the drive firmware upgrade is in progress, otherwise it will be set to 0.

Note: Any firmwareStatus object reporting status=Success and percentComplete=0% identifies that the drive is not available for a firmware update yet, such as a drive being varied off. (Support for percentComplete was added in Scalar i6000 version 775.)

URI	aml/drives/firmware/operations/update
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 101: firmwareStatusList

Table 111: POST aml/drives/firmware/operations/update

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 30 seconds; Maximum = 300 seconds

Description: Upgrade the selected drives with the specified firmware image files. To determine the progress status of the update, i6000 only, use Table 110: GET aml/drives/firmware/operations/update.

Note: The Scalar i6000 supports an asynchronous request. Scalar i3 and i6/i6H tape libraries support synchronous requests and block until the update has finished.

URI	aml/drives/firmware/operations/update
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 98: firmwareUpdateList
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 112: GET aml/drives/logs

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of drive log resources that were generated by the library because of certain tape alerts generated by a drive.

URI	<i>aml/drives/logs</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 40: driveLogList

Table 113: GET *aml/drives/log/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the drive log resource instance identified by the URI path template “name”.

URI	<i>aml/drives/log/{name}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameter names with respective values are as follows: <ul style="list-style-type: none"> save=the default name where the browser is to save the file content. If no name is specified a default name will be supplied by the Web Server. <p>The purpose of the save parameter is to tell the Web Browser that this is an attachment. If the client is not a Web Browser, then the ‘Accept: application/octet-stream’ can be used to retrieve the file data.</p>
Request Header	Accept: application/octet-stream (download the file content) Accept: application/xml or application/json (retrieve the driveLog resource object)
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/octet-stream, application/xml or application/json On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	The file content, or driveLog object, see Figure 41: driveLog

Table 114: DELETE *aml/drives/log/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the drive log resource instance identified by the URI path template “name”.

URI	<i>aml/drives/log/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)

Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 115: POST *aml/drives/log/{name}/email*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the drive log resource instance identified by the URI path template “name”.

URI	<i>aml/drives/log/{name}/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 404, 412
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 116: GET *aml/drives/ports*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve all drive port resource instances.

URI	<i>aml/drives/ports</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameter name is “configuration” with the following valid values: <ul style="list-style-type: none"> • configuration = “actual” or “requested” Note: The i6000 supports only the “requested: value”
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 42: drivePortList

Table 117: POST *aml/drives/powerCycle*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 180 seconds; Maximum = 360 seconds

Description: Power Cycle one or more drives. The drive serial numbers can be the physical or logical serial number.

URI	<i>aml/drives/powerCycle</i>
Method	POST
User Role Access	Admin, Service
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 44: driveSerialNumberList
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 118: GET *aml/drives/reports/activity*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the library drive(s) activity for the last 24 hours. A list of 24 driveActivityStatistics objects will be returned. Each object will represent an hour of activity in the last 24 hours and will report the read and writes in MB for all drives in the library, including the total mount counts and the hour of the day. The first entry in the list will represent the activity 23 hours ago, while the last entry in the list will represent activity for the current hour of the day.

URI	<i>aml/drives/reports/activity</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	The following query parameters are supported, partition and drive with the following values: <ul style="list-style-type: none"> • partition= the name of a specific partition • driveSerialNumber= The physical serial number of the drive <p>If no query parameters are used the request will return data for all drives in the library. If the partition parameter is specified, the data for the drives belonging to that partition will be reported. When the drive query parameter is specified then the data for that drive is reported.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 34: driveActivityStatistics

Table 119: GET *aml/drives/reports/activity/details*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the library drive(s) activity for the last 24 hours. A list of 24 driveActivityStatistics objects will be returned for each drive installed in the library, see Figure 34: driveActivityStatistics for details. The detailedDriveActivityStatistics.drive object reports the logical and physical serial number of the drive and the partition who owns the drive.

URI	<i>aml/drives/reports/activity/details</i>
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 30: detailedDriveActivityStatistics

Table 120: GET *aml/drives/reports/cleaning*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of drive cleaning records. The drive cleaning records provide information as to when a drive was last cleaned, what cleaning media was used, how many times the media was used to clean a drive and whether the cleaning media has expired.

URI	<i>aml/drives/reports/cleaning</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000), 110(i3/i6/i6H)
Parameters	<p>The following query parameters are supported, start, length, period, date, barcode, save with the following values:</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • barcode=The media barcode • save="name" where name is a file name to use to save the file. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified. <p>If no query parameters are used the request will return all drive cleaning data.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json, text/plain, application/octet-stream On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 35: driveCleaningList

Table 121: POST aml/drives/reports/cleaning/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of drive cleaning records. The information will be in an email attachment and the file format will be CSV.

URI	<i>aml/drives/reports/cleaning/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	760(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 122: GET aml/drives/reports/utilization

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of drive utilization records. The drive utilization record provides information as to when tape drives were mounted and un-mounted, capturing how much data the drives read and wrote during such mount sessions. The information provides details to allow further analysis as to which drives may be under- or over-utilized for tape cartridge load operations while also providing read/write performance data to assess tape cartridge residency needs.

Note: If the Media Type text/plain is selected (Accept http header) the data will be returned in CSV format.

URI	<i>aml/drives/reports/utilization</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	The following query parameters are supported, start, length, period, date, partition, driveSerialNumber, barcode, save with the following values: <ul style="list-style-type: none">• start=0-n• length=1-n, anything else means all records.• period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30.• date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored.

	<ul style="list-style-type: none"> • partition= the name of a specific partition • driveSerialNumber=The physical serial number of the drive • barcode=The media barcode • save="name" where name is a file name to use to save the file. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified. <p>If no query parameters are used the request will return all the drive utilization data. If the partition parameter is specified, the data for the drives belonging to that partition will be reported.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 403(i3/i6/i6H)
Response Header	Content-Type:application/xml or application/json, text/plain, application/octet-stream On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 45: driveUtilizationList

Table 123: POST aml/drives/reports/utilization/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirement: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of drive utilization records. The information will be in an email attachment and the file format will be CSV.

The reportCriteria object supports the same query parameters as Table 68: GET aml/drives/reports/utilization.

<i>URI</i>	<i>aml/drives/reports/utilization/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 124: GET aml/drive/{serialNumber}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the drive resource instance identified by the URI path template "serialNumber". The serialNumber can be the drives logical or physical serial number.

URI	<i>aml/drive/{serialNumber}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	None (dataStore support deprecated)
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 33: drive

Table 125: GET *aml/drive/{serialNumber}/dataPath*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the data path drive or capable data path drive identified by the URI path template “serialNumber”. The serialNumber can be the drive’s logical or physical serial number.

URI	<i>aml/drive/{serialNumber}/dataPath</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 33: drive

Table 126: PUT *aml/drive/{serialNumber}/dataPath*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: SNW/PathFailover (i6000), Multi-Path and/or Advanced Path Failover (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update a drive’s data path port access configuration for the drive identified by the URI path template “serialNumber”. The serialNumber can be the drive’s logical or physical serial number. The drive element field that needs to be updated is the *settings.dataPath* field. The valid values are: 1 (None, no failover = Standard single port drive access), 2 (Standard, i6000-only = Basic port failover with NPIV switch connected HP drives), 3 (Advanced), and 4 (MultiPath, i6/i6H only as I6000 defaults to multi-path if an SNW license is applied to a drive).

URI	<i>aml/drive/{serialNumber}/dataPath</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 33: drive

Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 33: drive

Table 127: GET aml/drive/{serialNumber}/operations/clean

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of clean drive tasks that were requested on the drive identified by the URI path template “{serialNumber}”. The serialNumber must be the drive’s logical serial number.

URI	aml/ drive/{serialNumber}/operations/clean
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 128: POST aml/drive/{serialNumber}/operations/clean

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time (Scalar i6000): Minimum <= 1 seconds ; Maximum = 30 seconds

Response Time (Scalar i3/i6/i6H): Minimum <= 60 seconds ; Maximum = 240 seconds

Description: Start a drive cleaning on the drive using the cleanDriveTask object. The serialNumber must be the drive’s logical serial number.

Before you can issue a drive cleaning operation, the drive mode must be changed to offline.

To determine what cleaning media to use to clean the drive you can first use the URI Table 247: GET aml/physicalLibrary/elements, to find the configured cleaning slot elements.

You can also use the URI Table 152: GET aml/media to find the cleaning media configured in the library.

Note: This request is an asynchronous request on a Scalar i6000 library. The new task object URI that was created will be included in the ‘Location’ header of the response, see Table 129: GET aml/drive/{serialNumber}/operations/clean/{id}. To determine if a drive cleaning task has completed, check the state element of the task object, when complete the state should be 5 (Completed) (see Figure 209: task).

On the Scalar i3/i6/i6H, this request will block until the cleaning operation has completed.

URI	aml/drive/{serialNumber}/operations/clean
Method	POST
User Role Access	i6000 - Admin, Service i3/i6/i6H - Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A

Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 16: cleanDriveTask
Response Codes	202(i6000) 200(I3/i6/i6H), 403, 404
Response Header	Content-Type:application/xml or application/json Location: aml/drive/{serialNumber}/operations/clean/{taskId}
Response Data	See Figure 225: WSResultCode

Table 129: GET aml/drive/{serialNumber}/operations/clean/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object with the id identified by the URI path template “id” and the componentId identified by the URI path template “serialNumber”. The serialNumber must be the drive’s logical serial number.

<i>URI</i>	<i>aml/drive/{serialNumber}/operations/clean/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 130: DELETE aml/drive/{serialNumber}/operations/clean/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Delete the cleaning task resource that was started/requested on the drive identified by the URI path template “serialNumber” with its task id identified by the URI path template “id”.

The task must be completed (See Figure 209: task) before it can be deleted.

<i>URI</i>	<i>aml/drive/{serialNumber}/operations/clean/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 131: POST aml/drive/{identifier}/operations/configure

Product Support: Scalar i6000

Response Time: Minimum <= 60 seconds; Maximum = 180 seconds

Description: Request a physical drive configuration validation for the drive location per the URI *identifier* template. The identifier must be specified in the location format specified as “frame,rack,section,column,row”, such as (aml/drive/2,1,4,1,1/operations/configure).

Note: This command provides a means to request a physical drive presence check for a configured drive location in case the library detected a drive sled communication loss due to a true drive sled connection issue or an actual physical removal of a drive sled.

URI	aml/drive/{identifier}/operations/configure
Method	POST
User Role Access	i6000 - Admin, Service
Version	777(i6000)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 33: drive

Table 132: POST aml/drive/{serialNumber}/operations/eject

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Eject media from the drive identified by the URI path template “serialNumber”. The serialNumber can be either the drive’s physical or logical serial number.

Note: In the event a tape cartridge is stuck in a tape drive, a forced eject command sequence may be attempted once, which simulates a manual, physical 10-second eject button press and hold. To force an eject operation, first vary-off a drive, then vary-on the drive, followed by an eject request again once the drive initialized. See Table 139: PUT aml/drive/{identifier}/operations/state.

URI	aml/drive/{serialNumber}/operations/eject
Method	POST
User Role Access	i6000 - Admin, Service i3/i6/i6H - Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 133: GET aml/drive/{serialNumber}/operations/identify

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the drive identify task on the drive identified by the URI path template “serialNumber”. The serialNumber must be the drive’s logical serial number.

URI	<i>aml/drive/{serialNumber}/operations/identify</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 134: POST *aml/drive/{serialNumber}/operations/identify*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Initiate a drive identify on the drive identified by the URI path template “serialNumber”. The serialNumber must be the drive’s logical serial number. Only one identify task can be initiated at a time.

Note: If an identify task is currently active on an i6000, it must be stopped (DELETE) before another task is started.

URI	<i>aml/drive/{serialNumber}/operations/identify</i>
Method	POST
User Role Access	i6000 - Admin, Service i3/i6/i6H - Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200(i3/i6/i6H), 202(i6000), 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 135: DELETE *aml/drive/{serialNumber}/operations/identify*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Stop a drive identify task for the drive identified by the URI path template “serialNumber”, which must be the drive’s logical serial number.

URI	<i>aml/drive/{serialNumber}/operations/identify</i>
Method	DELETE
User Role Access	i6000 - Admin, Service i3/i6/i6H – Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 136: POST aml/drive/{serialNumber}/operations/powerCycle**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 30 seconds; Maximum = 120 seconds**Description:** Power cycle the drive identified by the URI path template “serialNumber”. The serialNumber can be the drive’s logical or physical serial number.**Note:** Support for this command is deprecated and should be accomplished via operations to vary off a drive, followed by a command to vary-on a drive. See Table 139: PUT aml/drive/{identifier}/operations/state.

URI	aml/drive/{serialNumber}/operations/powerCycle
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 137: POST aml/drive/{serialNumber}/operations/performanceTest**Product Support:** Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 60 seconds; Maximum = 600 seconds**Description:** Run a performance test on the drive identified by the URI path template “serialNumber”, which can be the drive’s logical or physical serial number.

This command requires a scratch tape in a coordinate for a shared IE slot when the library is configured for *Remote UI/Host Assignment*. If no IE slots are configured, a scratch tape is required in a default location, which is the first bottom magazine slot in the right magazine of section 0 (Scalar i3/i6: 1,1, 0,10,1; Scalar i6H: 1,1,0,12,1).

URI	aml/drive/{serialNumber}/operations/performanceTest
Method	POST
User Role Access	Admin, Service, User (Partition Access Required)
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 135: media
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 138: GET aml/drive/{identifier}/operations/state**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Retrieve the current state (Varied On, Varied Off or Pending) of the drive identified by the URI path template “identifier”. The identifier can be the physical or logical

serial number of the drive or the drive coordinate in the following format:

“frame,rack,section,column,row” (aml/drive/2,1,4,1,1/operations/state).

The coordinate should be used when varying on a drive, because the drive serial numbers are not reported when the drive is in the Pending state.

URI	aml/drive/{identifier}/operations/state
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1(Varied On), 2(Varied Off) or 3(Pending/Initializing)

Table 139: PUT aml/drive/{identifier}/operations/state

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the drive state, 1 (Vary On) or 2 (Vary Off). This option should be used when replacing a drive.

The identifier can be the physical or logical serial number of the drive or the drive coordinate in the following format “frame,rack,section,column,row” such as (aml/drive/2,1,4,1,1/operations/state).

The coordinate should be used when varying on a drive, because the drive serial numbers are not reported when the drive is in the Pending state.

URI	aml/drive/{identifier}/operations/state
Method	PUT
User Role Access	i6000 - Admin, Service i3/i6/i6H – Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 or 2
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 140: POST aml/drive/{serialNumber}/operations/test

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Run a drive self-test on the drive identified by the URI path template “serialNumber”. The serialNumber can be the drive’s logical or physical serial number.

URI	aml/drive/{serialNumber}/operations/test
Method	POST

User Role Access	i6000 - Admin, Service i3/i6/i6H - Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 141: POST `aml/drive/{serialNumber}/operations/wrapTest`

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Perform a drive wrap test on the drive identified by the URI path template “serialNumber”. The serialNumber can be the drive’s logical or physical serial number.

Note: This test requires that a wrap test tool be applied to the tape drive interface port(s).

URI	<code>aml/drive/{serialNumber}/operations/wrapTest</code>
Method	POST
User Role Access	Admin, Service, User (Partition Access Required)
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 142: GET `aml/drive/{serialNumber}/ports`

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the drive port resources identified by the URI path template “serialNumber”. The serialNumber can be the drive’s logical or physical serial number.

This request will report both actual and requested port settings.

URI	<code>aml/drive/{serialNumber}/ports</code>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameter names are “configuration”. Valid values for configuration are “actual” and “requested”
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 43: drivePorts

Table 143: PUT aml/drive/{serialNumber}/ports

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Modify the port settings for the drive identified by the URI path template “serialNumber”. The drive serialNumber can be the drive’s logical or physical serial number.

The port settings are applied to the drive and affect all drive ports. If the drive’s port *id*, *type*, *address* or *status* elements of the port object are included in the request they will be ignored as these elements cannot be modified.

Note: When modifying port settings that have ‘actual’ and ‘requested’ elements, the ‘requested’ element must be used. The ‘*actual*’ settings refer to the actual, drive-negotiated and drive-reported individual port settings that cannot be modified. Actual settings may be different than the requested settings, especially if requested settings asked for automatic negotiation. Also, requested settings are requested for a drive, not a specific port, regardless of the drive having 1 or 2 interface ports and are modified via port id 1 of the port object. The Scalar i6000 only supports the following port.topology.requested types: 1(Loop Preferred “LN”), 2(P2P/Fabric “N”), 3(Loop “L”).

The example below changes the requested drive port topology to loop (3) with loop id 10 and a speed of 2Gb (2):

The required fields are:

```
<ns2:drivePorts xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>logical serial number</serialNumber>
  <!-- OR -->
  <physicalSerialNumber>physical serial number</physicalSerialNumber>
  <ports>
    <port>
      <id>1</id>
      <topology>
        <requested>3</requested>
      </topology>
      <loopId>10</loopId>
      <speed>
        <requested>2</requested>
      </speed>
    </port>
  </ports>
</ns2:drivePorts>
```

URI	aml/drive/{serialNumber}/ports
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 43: drivePorts
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 43: drivePorts

Table 144: GET aml/drive/{serialNumber}/log**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 120 seconds; Maximum = 360 seconds**Description:** Retrieve the drive log identified by the URI path template “serialNumber”. The “serialNumber” can be either the physical or logical serial number of the drive. For example, to retrieve a drive log from a drive with serial number DR1002, use the following URI:
aml/drive/DR1002/log**Note:** The drives in a Scalar i6000 must be connected to an I/O Blade or Ethernet Expansion Blade for this feature to work.

URI	aml/drive/{serialNumber}/log
Method	GET
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameter and their respective values are as follows: values <ul style="list-style-type: none"> save="name" where name is a file name to use to save the file. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/octet-stream, application/xml, application/json Cookie name= FileDownloadingProgressCookie
Response Data	Byte Stream if request completes successfully, otherwise See Figure 225: WSResultCode

Table 145: POST aml/drive/{serialNumber}/log/email**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 seconds; Maximum = 30 seconds**Description:** Email the drive log report for the drive identified by the URI path template “serialNumber”. The “serialNumber” can be either the physical or logical serial number of the drive.

The information will be in an email attachment.

Note: The drives in a Scalar i6000 must be connected to an IO Blade or Ethernet Expansion Blade for this feature to work.

URI	aml/drive/{serialNumber}/log/email
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml, application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 404, 412

Response Header	Content-Type: application/xml, application/json
Response Data	See Figure 225: WSResultCode

Table 146: GET aml/drive/{serialNumber}/mode

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current mode (Online/Offline) of the drive identified by the URI path template “serialNumber”. The “serialNumber” can be either the physical or logical serial number of the drive.

<i>URI</i>	<i>aml/drive/{serialNumber}/mode</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: test/plain, application/json
Response Data	1(Online) or 2(Offline)

Table 147: PUT aml/drive/{serialNumber}/mode

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the drive mode of the drive identified by the URI path template “serialNumber”. The “serialNumber” can be either the physical or logical serial number of the drive.

The mode can be, 1 (Online) or 2 (Offline). This option should be used to block SCSI hosts from moving media to a drive (mode offline). When offline, a Read Element Status will report an exception with ASC/ASCQ 0x83/0x05 and Move Medium requests are rejected with an ASC/ASCQ 0x83/0x05.

A situation where the drive should be taken offline is when updating drive firmware, or cleaning a drive.

<i>URI</i>	<i>aml/drive/{serialNumber}/mode</i>
Method	PUT
User Role Access	i6000 - Admin, Service i3/i6/i6H – Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: text/plain, application/json
Request Data	1 or 2
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml, application/json
Response Data	See Figure 225: WSResultCode

Table 148: POST aml/drive/{serialNumber}/removeITNexus

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Remove the IT Nexus from the drive identified by the URI path template “serialNumber”. The “serialNumber” can be either the physical or logical serial number of the drive.

The drive will clear all SCSI-host defined Initiator-Target (IT) reservations and media removal settings. This functionality only applies to HP LTO5 and greater drives.

URI	aml/drive/{serialNumber}/removeITNexus
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 149: GET aml/enum

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve all the enum resource instances. The enum resources describe the name value pairs for certain XML object elements. For example, the RASGroup object has a property group and a value of 1. To determine the value of 1, the componentList component name “RASGroup” contains keys for all possible values for an element name “group”, and the value of 1 is “Connectivity”. See the XML response data below:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<componentList xmlns:ns2="http://automatedMediaLibrary/">
  <component name="RASGroup">
    <element name="group">
      <entry key="0" value="All"/>
      <entry key="1" value="Connectivity"/>
      <entry key="2" value="Control"/>
      <entry key="3" value="Media"/>
      <entry key="4" value="Drives"/>
      <entry key="5" value="Power"/>
      <entry key="6" value="Robotics"/>
      <entry key="7" value="Library"/>
    </element>
  </component>
  <component name="RASGroupStatus">
    <element name="group">
      <entry key="1" value="Connectivity"/>
      <entry key="2" value="Control"/>
      <entry key="3" value="Media"/>
      <entry key="4" value="Drives"/>
      <entry key="5" value="Power"/>
      <entry key="6" value="Robotics"/>
      <entry key="7" value="Library"/>
    </element>
    <element name="status">
```

```

    <entry key="1" value="Good"/>
    <entry key="2" value="Failed"/>
    <entry key="3" value="Degraded"/>
    <entry key="4" value="Warning"/>
    <entry key="5" value="Informational"/>
    <entry key="6" value="Unknown"/>
    <entry key="7" value="Invalid"/>
    <entry key="8" value="Attention"/>
  </element>
</component>
</component>
.....
</componentList>

```

URI	aml/enum
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 21: componentList

Table 150: GET aml/enum/{component}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the enum resource instance identified by the URI path template “component”. This is similar to the aml/enum resource, except this URI should returns only the elements for the specific path component template parameter. The example output below shows the response for the component “RASGroup”. The URI “aml/enum/RASGroup” returns the response data below:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<elementList xmlns:ns2="http://automatedMediaLibrary/">
  <component name="RASGroup">
    <element name="group">
      <entry key="0" value="All"/>
      <entry key="1" value="Connectivity"/>
      <entry key="2" value="Control"/>
      <entry key="3" value="Media"/>
      <entry key="4" value="Drives"/>
      <entry key="5" value="Power"/>
      <entry key="6" value="Robotics"/>
      <entry key="7" value="Library"/>
    </element>
  </component>
</elementList>

```

URI	aml/enum/{component}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A

Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 21: componentList (ENUM)

Table 151: GET aml/enum/{component}/{element}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the enum component and element resource instance identified by the URI path templates “component” and “element”. The URI “aml/enum/partition/interfaceType” will return the response data below:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entryList xmlns:ns2="http://automatedMediaLibrary/">
  <component name="partition">
    <element name="interfaceType">
      <entry key="1" value="SCSI"/>
      <entry key="10" value="Mixed"/>
      <entry key="2" value="Fibre"/>
      <entry key="3" value="SAS"/>
    </element>
  </component>
</entryList>
```

URI	aml/enum/{component}/{element}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 73: entryList (ENUM)

Table 152: GET aml/media

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 180 seconds

Description: Retrieve the media resource instances.

URI	aml/media
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameters are partition, location, start, length, frame, rack, type, status, and save, and have the following values:</p> <ul style="list-style-type: none"> • partition=name of partition • location="storage", "drive", "ie" or "xie" <p>Range parameters</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • frame=0 – maximum number of frames

	<ul style="list-style-type: none"> • rack = 1 or 2 • type= 3(LTO2), 4(LTO3), 5(LTO4), 6(LTO5), 7(LTO6), 8(LTO7), 9(LTO8), 10(LTO9), 20(Cleaning) • status="used" or "available" to identify assigned or unassigned media. • save="name" where name is a file name to use to save the media information. The file format will be CSV. (i6000 Only) • sharedIE=true or false. (i3/i6/i6H Only) • includePreviousOwner=true. This will prompt the server to include the previousOwner information of the media object. This is only supported for Scalar i6000 version 738 or higher. • fields=A comma separate list of media object elements you want to get values for. The elements that are supported are barcode, coordinate, currentOwner, encryption and mediaType. This query parameter is provided to improve performance on libraries with large numbers of media. This is only supported for the Scalar i6000. • ltfExport=true or false (i3/i6/i6H only, added in version 160). If true, it returns media in an LTFS partition that may be exported via the library. It must be used in conjunction with the ?partition parameter, and may not be used with any other parameters. If false, do nothing. <p>The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified.</p> <p>The sharedIE query parameter is an indication if shared IE media (unassigned media in an IE slot while the library is in auto assignment mode) should specifically be included or excluded from the media list. If true, shared IE media will be included. If false, shared IE media are excluded. For example, /media?status=available, by default, includes shared IE media. Adding sharedIE=false (/media?used=available&sharedIE=false) will exclude the shared IE media from the list.</p> <p>To retrieve all media in one call, use "aml/media?start=0&length=-1" which is the default if no range is specified. To retrieve all media belonging to partition named TEST use "aml/media?partition=TEST". To retrieve all media in IE stations, use "aml/media?location=ie". To retrieve the first 50 media belonging to partition TEST use "aml/media?partition=TEST&start=0&length=50".</p> <p>Note: When using the range parameters, media are sorted by barcodes.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 134: mediaList

Table 153: GET aml/media/cleaning

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 60 seconds

Description: Retrieve a list of cleaning media resources. These are specific media used for drive cleaning.

Note: The cleaningMedia.state element is not supported for the Scalar i6000.

URI	aml/media/cleaning
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 17: cleaningMediaList

Table 154: GET aml/media/edlm

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 120 seconds

Description: Retrieve a list of EDLM media resources. These resources describe all the media in the library, except for media that are in IE slots or drives, and whether they have been tested by the EDLM feature. The list can be used to determine which media may need to have tests started. If a media has never been scanned, the value of the testType, testPriority, testState and testResult elements of the edlmMedia object can be ignored.

URI	aml/media/edlm
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	<p>The following query parameters are supported, partition, barcode, start, length, period, state, type and date with the following values:</p> <ul style="list-style-type: none">• partition=name (request only media belonging to this partition)• barcode=the media barcode to filter on (not supported for i3/i6/i6H)• start=0-n (range parameter)• length=1-n, anything else means all records.• period=1-n, the last number of days to include in the data reported. If you want to report for the last 3 months, you would specify 90.• date=At what date (the lastTested field of the edlmMedia object is used) you want to start your query. The data returned will include all records that are equal or older than the date specified and applied against the lastTested field of the edlmMedia object. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is "yyyy-MM-dd

	HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. <ul style="list-style-type: none"> state=the current/last test state: 1(pending), 2(In progress), 3(Complete), 4(Stopped), 5(Paused) or 6(Resume (scalar i6000 only)) type=the test type of the current/last test type: 1(Quick Scan), 2(Normal Scan) or 3(Full Scan).
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 47: edlmMediaList

Table 155: POST aml/media/edlm

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Start a new EDLM test session using the edlmMediaObject list. The required fields of the edlmMedia object are edlmMedia.barcode and edlmMedia.testType. Scalar i6/i6H libraries require also that the coordinate be specified. The edlmMedia.testPriority field may be specified.

This call is asynchronous, and the location header in the response will report the new session id URI that can be used to determine the test state.

URI	aml/media/edlm
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 47: edlmMediaList
Response Codes	200(i6000), 201(i3/i6/i6H), 403, 404
Response Header	Content-Type: application/xml or application/json Location: aml/media/edlm/session/#
Response Data	See Figure 225: WSResultCode

Table 156: GET aml/media/edlm/results

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of EDLM media result resources. These resources report the results of media that have been tested by the EDLM feature. Media may have more than one result, depending on how many times it has been tested.

URI	aml/media/edlm/results
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	Query parameters and their respective values are as follows: <ul style="list-style-type: none"> partition=name (request only results for media belonging to this partition)

	<ul style="list-style-type: none"> • barcode=the media barcode to filter on (not supported for i3/i6/i6H) • start=0-n (range parameter) • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the data reported. For example, for the last 3 months, specify 90. • date=At what date (the testDate (this is the date the media was last scanned) of the edlmMediaResult object field is used) you want to start your query. The data returned will include all records that are equal or older than the date specified and applied against the testDate field of the edlmMediaResult object. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • state=the current/last test state: 1(pending), 2(In progress), 3(Complete), 4(Stopped), 5(Paused), 6(Resume (Scalar i6000 only)) • type=the test type of the current/last test type: 1(Quick Scan), 2(Normal Scan) or 3(Full Scan). • sessionId=the session id that kicked off the test
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 49: edlmMediaResultList

Table 157: GET aml/media/edlm/result/{id}

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the EDLM media result resource instance identified by the URI path template “id”.

<i>URI</i>	<i>aml/media/edlm/result/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 50: edlmMediaResult

Table 158: DELETE aml/media/edlm/result/{id}

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the EDLM media result resource instance identified by the URI path

template “id”.

URI	<i>aml/media/edlm/result/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 50: edlmMediaResult

Table 159: GET aml/media/edlm/sessions

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of EDLM session resources. These session resources report the status of a collection of media that have either been tested, are currently being tested or are scheduled to be tested. When a user initiates an EDLM test, a new session is created and it aggregates the results of the media being tested, see Table 155: POST aml/media/edlm,

URI	<i>aml/media/edlm/sessions</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	The following query parameters are supported, active with the following values: <ul style="list-style-type: none"> active = true. When this parameter is requested, only sessions that are in a state of Pending (2), Paused (4) or In Progress (8) will be reported. This query parameter was added in version 760(i6000).
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 55: edlmSessionList

Table 160: GET aml/media/edlm/session/{id}

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the EDLM session resource instance identified by the URI path template “id”.

URI	<i>aml/media/edlm/session/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 56: edlmSession

Table 161: PUT aml/media/edlm/session/{id}/operations/pause

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Pause the EDLM media tests that were started by the session resource instance identified by the URI path template “id”. The tests that will be paused must have a current test state of Pending.

<i>URI</i>	<i>aml/media/edlm/session/{id}/operations/pause</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 162: PUT aml/media/edlm/session/{id}/operations/resume

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Resume paused EDLM media tests that were started by the session resource instance identified by the URI path template “id”.

<i>URI</i>	<i>aml/media/edlm/session/{id}/operations/resume</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 163: PUT aml/media/edlm/session/{id}/operations/stop

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Stop the EDLM media tests that were started by the session resource instance identified by the URI path template “id”. Tests with a current test state of paused, pending or in progress will be stopped.

<i>URI</i>	<i>aml/media/edlm/session/{id}/operations/stop</i>
Method	PUT

User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 164: GET aml/media/operations/moveMedium

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of moveMedium resources that are currently in progress. The moveMedium objects returned will include the source and destination coordinates, all other elements of the moveMedium object should be ignored. The list of move medium will only include those moves that were requested through the Web Services interface, Table 165: POST aml/media/operations/moveMedium.

<i>URI</i>	<i>aml/media/operations/moveMedium</i>
Method	GET
User Role Access	Admin, Service, User
Version	751(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 147: moveMediumList

Table 165: POST aml/media/operations/moveMedium

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 600 seconds

Description: Move a media from its source coordinate to the destination coordinate. The destination coordinate must be empty and can be any element type storage, drive, I/E or extended I/E. A moveClass bitmap element provides additional command qualification for the moveMedium request.

The mode element should be set to 2 if the partition involved in the move operation is to be taken offline before the move and put back online after the move. It is not necessary to take the partition offline and then back online since a SCSI host will be notified that there was an inventory change when a media is moved to/from a partition via a Web Services request..

When moving media from a drive (unload) use the mediaHomeCoordinate element of the drive object (see Figure 33: drive), to determine the slot coordinate where the media came from (this will be the destinationCoordinate).

Note: On a Scalar i3/i6/i6H, the following restrictions apply to moving and importing media from an IE slot:

- Media assigned to the System partition may only be moved to a cleaning slot or

another IE slot.

- Unassigned media, while the library is in RUI assignment mode, may be moved to a cleaning slot, another IE slot or to an assigned slot (with user partition access). The media may not be moved to an unassigned slot.
- Unassigned media, while the library is in LUI assignment mode, may only be moved to another IE slot.
- Media assigned to a standard partition may only be moved to another slot within the same partition.
- Media assigned to an Active Vault or EDLM partition may be moved to slots assigned to any partition.

URI	<i>aml/media/operations/moveMedium</i>
Method	POST
User Role Access	Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 148: moveMedium
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json Coordinate: i.e. 1,2,2,4,2,2 (Frame, Rack, Section, Column, Row, Type)
Response Data	See Figure 225: WSResultCode

Table 166: GET *aml/media/operations/moveMedium/maxAllowed*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the maximum number of allowed concurrent Web Service moveMedium requests.

URI	<i>aml/media/operations/moveMedium/maxAllowed</i>
Method	GET
User Role Access	Admin, Service, User
Version	751(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: text/plain or application/json
Response Data	A number representing the maximum number of allowed concurrent moves.

Table 167: PUT *aml/media/operations/moveMedium/maxAllowed*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 130 seconds

Description: Update the maximum number of concurrent move medium requests allowed, using Web Services.

URI	<i>aml/media/operations/moveMedium/maxAllowed</i>
Method	POST
User Role Access	Admin, Service
Version	751(i6000)
Parameters	N/A
Request Header	Content-Type: text/plain or application/json
Request Data	-1 (Unbounded, no maximum limit, this is the default) 0-n (0 means move medium is disabled and 1-n is the maximum concurrent moves allowed)
Response Codes	200, 503
Response Header	Content-Type: application/xml or application/json
Response Data	Figure 225: WSResultCode

Table 168: GET *aml/media/reports/crossPartitionMoves*

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the cross-partition moves report. This report contains a list of media that have been moved from one partition to another partition.

URI	<i>aml/media/reports/crossPartitionMoves</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>The following query parameters are supported, start, length, period, date, save with the following values:</p> <p>Range parameters</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last 3 months, you would specify 90. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • partition=the source or destination partition name to filter on. • barcode=the barcode of the media that was moved • type=the source or destination partition type involved in the move, 1(Standard), 2(EDLM), 3(AMP) or 4(Active Vault). • save="name" where name is a file name to use to save the file in CSV format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified. <p>If no query parameters are used the request will return all the cross-partition move data.</p>
Request Header	N/A

Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 27: crossPartitionMovesList

Table 169: POST aml/media/reports/crossPartitionMoves/email

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of cross partition media move records.

The information will be in an email attachment and the file format will be CSV.

URI	aml/media/reports/crossPartitionMoves/email
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 170: GET aml/media/reports/edlm

Product Support: Scalar i6000, Scalar i6/i6H

License Requirements: Extended Data LifeCycle Management (EDLM)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the EDLM Scan Test report resource. This report contains a list of media that have been scanned by the EDLM drive(s) installed in the library.

URI	aml/media/reports/edlm
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000), 110(i6/i6H)
Parameters	The following query parameters are supported, start, length, period, date, barcode, driveSerialNumber, partition, type, result and save with the following values: Range parameters <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last 3 months, you would specify 90. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days)

	<p>specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored.</p> <ul style="list-style-type: none"> • barcode=the specific media barcode you want to query on. • driveSerialNumber=the EDLM drive serial number (physical) that was used to scan the media. • partition=the name of the partition who last owned the media. • type=the test scan type to filter on, the valid values are 1(Quick), 2(Normal) and 3(Full). • result=the test result to filter on, the valid values are 1(Good), 2(Untested), 3(Suspect) and 4(Failed) • save=“name” where name is a file name to use to save the file in CSV format. <p>The save=“name” query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default “name” is provided if none is specified.</p> <p>If no query parameters are used the request will return all the media that have been tested/scanned.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 51: edlmMediaScanTestList

Table 171: POST aml/media/reports/edlm/email

Product Support: Scalar i6000, Scalar i6/i6H

License Requirements: Extended Data LifeCycle Management (EDLM)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the EDLM Scan Test report.

The information will be in an email attachment in CSV file format.

The reportCriteria object supports the same query parameters as Table 170: GET aml/media/reports/edlm, to filter on result, use the reportCriteria.state element.

<i>URI</i>	<i>aml/media/reports/edlm/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	760(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 172: GET aml/media/reports/inventory

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the media inventory resource instances.

URI	<i>aml/media/reports/inventory</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	<p>Query parameters are partition, location, start, length, frame, rack and have the following values:</p> <ul style="list-style-type: none"> • partition=name of partition • location="storage", "drive" or "ie" <p>Range parameters</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • frame=0 – maximum number of frames • rack = 1 or 2 • save="name" where name is a file name to use to save the file in CSV format. <p>The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified.</p> <p>Note: When using the range parameters, the media are sorted by their barcodes.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json, text/plain
Response Data	See Figure 134: mediaList

Table 173: POST *aml/media/reports/inventory/email*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of media records.

The information will be in an email attachment and the file format will be CSV.

URI	<i>aml/media/reports/inventory/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 174: GET *aml/media/reports/securityEvents*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Retrieve the list of media security records.

The media security records provide information as to which tape cartridge was removed either expectedly (properly exported) or removed unexpectedly (removed during open door condition or while library was powered off) to assist administrators with tape cartridge inventory verifications.

URI	<i>aml/media/reports/securityEvents</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>The following query parameters are supported, start, length, period, date, barcode, save with the following values:</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • barcode=The media barcode • save="name" where name is a file name to use to save the file in CSV format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified. <p>If no query parameters are used the request will return all the media security event data.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 136: mediaSecurityEventList

Table 175: POST *aml/media/reports/securityEvents/email***Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Email the list of media security records.

The information will be in an email attachment and the file format will be CSV.

The reportCriteria object supports the same query parameters as Table 174: GET

aml/media/reports/securityEvents.

URI	aml/media/reports/securityEvents/email
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 176: GET aml/media/reports/tapeAlerts

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of tape alert records.

URI	aml/media/reports/tapeAlerts
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>The following query parameters are supported, start, length, period, date, driveSerialNumber, barcode, save, alerts with the following values:</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last week, you would specify 7. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • driveSerialNumber= The physical serial number of the drive • barcode=The media barcode • alerts=a comma separated list of tape alerts. Valid tape alerts are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 30, 31, 32, 33, 34, 36, 37, 38, 39, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60. (Added in 770(i6000)) • save="name" where name is a file name to use to save the file in CSV format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser. A default "name" is provided if none is specified. <p>If no query parameters are used the request will return all the tape</p>

	alert data.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Error! Reference source not found.

Table 177: POST aml/media/reports/tapeAlerts/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of drive tape alert records.

The tape alert records provide information as to which drive reported which Tape Alert while being loaded with which tape cartridge. The report information provides details to allow further analysis as to which media or which drive may be a cause for media or drive failures.

The information will be in an email attachment and the file format will be CSV.

The reportCriteria object supports the same query parameters as Table 176: GET aml/media/reports/tapeAlerts. Use the reportCriteria.partition element for filtering the alerts query parameter.

<i>URI</i>	<i>aml/media/reports/tapeAlerts/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 178: GET aml/media/reports/usage

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of media usage records.

The media usage records provide media information capturing tape cartridge identification and media capacity and usage information as well as unrecovered and recovered read/write error count statistics.

<i>URI</i>	<i>aml/media/reports/usage</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)

Parameters	<p>The following query parameters are supported, start, length, period, date, barcode, save with the following values:</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • barcode=The media barcode • save=”name” where name is a file name to use to save the file in CSV format. The save=”name” query parameter should be used by a client browser to allow the data to be saved by the browser. A default “name” is provided if none is specified. <p>If no query parameters are used the request will return all the media usage data.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 139: mediaUsageList

Table 179: POST aml/media/reports/usage/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of media usage records in a CSV file format attachment.

URI	<i>aml/media/reports/usage/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 180: GET aml/medium/{barcode}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the media identified by the URI path template “barcode”. To retrieve the media object with barcode “100000L6”, use “aml/medium/100000L6”.

A list is returned where duplicate barcodes exist since multiple media may have the same barcode.

<i>URI</i>	<i>aml/medium/{barcode}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 134: mediaList

Table 181: GET aml/partitions

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve all partition resource instances configure on the library.

<i>URI</i>	<i>aml/partitions</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameters and their respective values are as follows:</p> <ul style="list-style-type: none"> fields=A comma separate list of partition object elements you want to retrieve values for. The partition elements id, name, type, mode and serialNumber will always be included and if the user specifies ‘fields=’, these are the elements that will have real values. The elements that are supported are driveDomainType , storageSlotCount, emptyStorageSlotCount, driveCount, emptyDriveCount, ieSlotCount, emptySlotCount, xieSlotCount, emptyXieSlotCount, ampExtensionsCount, mediaCount, barcodeReporting, vendorId, productId, controlPathProvider, policySettings. <p>Note: This query parameter is only supported on the i6000.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 159: partitionList

Table 182: POST aml/partitions

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Create a new partition resource. When using the partition XML object to create a

partition, the following valid values apply:

- type: 1 (Standard), 2 (EDLM), 3 (AMP), 4 (Active Vault)

Note: The Scalar i6/i6H support only types 1 (Standard), 2 (EDLM), and 4 (Active Vault). The Scalar i3 supports only types 1 (Standard) and 4 (Active Vault).

- driveDomainType: 0 (Unknown), 3 (LTO2), 4 (LTO3), 5 (LTO4), 6 (LTO5), 7 (LTO6), 8 (LTO7), 9 (LTO8), 10 (LTO9)
- barcodeReporting:
 - 1 (Prefix): media identifier expected and reported as prefix to the barcode
 - 2 (Suffix): media identifier expected and reported as suffix to the barcode
 - 3 (Disable): media identifier not expected, barcode reported without any media identifier
 - 4 (Pass Through): barcode reported as scanned by scanner
 - 5 (Standard Six): Scalar i3/i6/i6H): six character barcode label expected, any media identifier not reported
 - 6 (Plus Six Scalar i3/i6/i6H): six character barcode label plus media identifier expected and reported

- mediaTypeChecking: 1 Not Required, 2 Disabled, 3 Required

Note: The mediaTypeChecking definitions are supported by the Scalar i6000 only. (added in version 785)

- vendorId: 0 (ADIC), 1 (Quantum), – default 1
- productId: 0 (N/A), 1 (Scalar 24), 2 (Scalar 100), 3 (Scalar 1000), 4 (Scalar 10k), 5 (Scalar i500), 6 (Scalar i2000), 7 (Scalar i6000), 8 (Scalar i40-i80), 9 (Scalar i3-i6)

Note: The vendorId and productId definitions allow for product emulation, such that the SCSI inquiry string for a standard partition identifies the vendor and product per emulated specification to allow host applications to recognize the tape library in the event the actual product model is not supported by the application.

The productId values 5, 6 and 7 can only be used if the vendorId 1 (Quantum) is selected. For vendorId 0 (ADIC) the productId values 1,2,3,4,5 and 6 can be used. The Scalar i6000 supports productId values 1,2,3,4,5,6,7 and the Scalar i3/i6/i6H support productId values 5,7,8,9.

The example below creates a partition named “Test” with 2 LTO-5 drives and 300 slots. The vendor id will be “Quantum”, the product id will be “Scalar i6000” and the barcodeReporting method policy will be “Pass Through”.

The required fields for creating a partition are: “name” and “type”.

Note: When creating or modifying a Library Managed partition (EDLM, AMP or Active Vault), the productId and vendorId fields are ignored. Also, a vendorId of 0 (ADIC) will only allow the following productIds: 1 (Scalar 24), 2 (Scalar 100), 3 (Scalar 1000), 4 (Scalar 10k), 5 (Scalar i500), 6 (Scalar i2000), and a vendorId of 1 (Quantum) will only allow the following productIds: 5 (Scalar i500), 6 (Scalar i2000), 7 (Scalar i6000).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:partition xmlns:ns2="http://automatedMediaLibrary/">
  <name>Test</name>
  <type>1</type>
  <driveDomainType>6</driveDomainType>
  <storageSlotCount>300</storageSlotCount>
  <driveCount>2</driveCount>
  <ieSlotCount>12</ieSlotCount>
  <xieSlotCount>0</xieSlotCount>
  <ampExtensionsCount>0</ampExtensionsCount>
  <barcodeReporting>4</barcodeReporting>
  <vendorId>1</vendorId>
  <productId>7</productId>
</ns2:partition>
```

Note: The Scalar i3 and Scalar i6/i6H do not support the following partition elements:

- ieSlotCount
- xieSlotCount
- ampExtensionCount

A partition name can only contain the following characters: A-Z a-z 0-9 _ and spaces

The maximum number of characters allowed is 64.

Note: The partition name ‘System’ (case-insensitive) cannot be used when with Scalar i3 and Scalar i6/i6H libraries as the “System” partition is a library reserved partition.

URI	aml/partitions
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 160: partition
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 160: partition

Table 183: GET aml/partitions/policy/activeVault

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Get a list of activeVaultPolicy resources configured on the library. Active Vault policies are configured on standard partitions. The policies intercept host commands that export tape cartridges to library managed Active Vault partitions.

URI	aml/partitions/policy/activeVault
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 5: activeVaultPolicyList

Table 184: POST aml/partitions/policy/activeVault

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Active Vault

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new active vault policy for partition named LL2. You can either choose an externalDefinedExport policy, or a vaultDefinedExport policy, but not both.

URI	aml/partitions/policy/activeVault
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	<p>See Figure 6: activeVaultPolicy</p> <p>The following example would move any media barcode that contains the characters '00LTO5' to the active vault 'AV Partition' when the media is exported (moved to the IE station) from the partition 'LL2'.</p> <pre><?xml version="1.0" encoding="UTF-8" standalone="yes"?> <ns2:activeVaultPolicy xmlns:ns2="http://automatedMediaLibrary/"> <partitionName>LL2</partitionName> <vaultDefinedExport> <activeVaultName>AV Partition</activeVaultName> <mediaFilter>*00LTO5</mediaFilter> </vaultDefinedExport> </ns2:activeVaultPolicy></pre> <p>Note: If the above mediaFilter element is used, it must be a comma delimited set of alphanumeric tokens, with an optional prefix or suffix wildcard (*).</p> <p>The other option is to choose the external application server(s) configured on the library, see Table 392: GET aml/system/policy/externalApplicationServers. You would use the externalApplicationServers.name field.</p>
Response Codes	201, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 185: GET aml/partitions/policy/autoImport

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of Auto Import Policy resources. The Auto Import feature allows

the import of media from an AMP partition to a Standard partition based on an Auto Import Policy configured for a standard partition. The policy defines a range of media barcodes to use to determine which media get imported into which partition.

URI	<i>aml/partitions/policy/autoImport</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 9: autoImportPolicyList

Table 186: GET *aml/partitions/policy/autoExport*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of Auto Export Policy resources. The Auto Export feature reroutes the export of media (media moves by a host to IE stations) from a Standard partition to an AMP partition. This feature can only be configured if there is an AMP partition configured.

URI	<i>aml/partitions/policy/autoExport</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 7: autoExportPolicyList

Table 187: GET *aml/partitions/policy/driveCleaning*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of drive cleaning policy resources configured on the library.

URI	<i>aml/partitions/policy/driveCleaning</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 37: driveCleaningPolicyList

Table 188: GET aml/partitions/policy/edlm

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of edlmPolicy resources configured on the library.

URI	aml/partitions/policy/edlm
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 53: edlmPolicyList

Table 189: POST aml/partitions/policy/edlm

Product Support: Scalar i6000, Scalar i6/i6H

License Requirements: Extended Data LifeCycle management (EDLM)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new edlm policy. The example below creates a policy for partition LL1:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:edlmPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL1</partitionName>
  <tapeAlert>
    <scanType>1</scanType>
    <count>3</count>
  </tapeAlert>
  <timeInterval>
    <quickScan>0</quickScan>
    <normalScan>365</normalScan>
    <fullScan>1095</fullScan>
  </timeInterval>
  <onImport>1</onImport>
  <scanPriority>2</scanPriority>
  <concurrentScans>0</concurrentScans>
  <continueOnError>true</continueOnError>
  <disableRasTicketGeneration>true</disableRasTicketGeneration>
  <externalPolicies>
    <externalApplicationServersName>The name of the external applications server's configuration
  </externalApplicationServersName>
    <mediaCopyPolicy>3</mediaCopyPolicy>
    <suspectCountScanType>1</suspectCountScanType>
  </externalPolicies>
</ns2:edlmPolicy>
```

Note:

1. An EDLM partition must be configured before a policy can be configured.
2. The only required field is 'partitionName' and the following default values will be applied:

```
<ns2:edlmPolicy xmlns:ns2="http://automatedMediaLibrary/">
```

```
<partitionName>P1</partitionName>
</ns2:edlmPolicy>
```

Below are the default values, if the request does not include them:

```
edlmPolicy.onImport: 0 (None)
edlmPolicy.scanPriority: 0 (Immediate)
edlmPolicy.concurrentScans: 0
edlmPolicy.continueOnError: false
edlmPolicy.disableRasTicketGeneration: false
edlmPolicy.tapeAlert.scanType: 0
edlmPolicy.tapeAlert.count: 0
edlmPolicy.timeInterval.quickScan: 0
edlmPolicy.timeInterval.normalScan: 0
edlmPolicy.timeInterval.fullScan: 0
edlmPolicy.externalPolicies.externalApplicationServersName: null
edlmPolicy.externalPolicies.mediaCopyPolicy: 0 (media copy disabled)
edlmPolicy.externalPolicies.suspectCountScanType: 0 (None)
```

<i>URI</i>	<i>aml/partitions/policy/edlm</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 54: edlmPolicy
Response Codes	201, 403, 404, 412
Response Header	Content-Type:application/xml or application/json Location: aml/partition/{name}/policy/edlm
Response Data	See Figure 225: WSResultCode

Table 190: GET *aml/partitions/policy/ekm*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of partition encryption policy resources. Encryption key management systems generate, protect, store, and manage encryption keys. These keys are used by their respective tape drives to encrypt information being written to tape, and decrypt information being read from tape media. Encryption on the i6000 tape library is enabled by partition only.

If a configured partition does not support EKM, it will not be included in this list.

<i>URI</i>	<i>aml/partitions/policy/ekm</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Header	Content-Type:application/xml or application/json
Response Codes	200
Response Data	See Figure 161: partitionEncryptionPolicyList

Table 191: GET aml/partitions/policy/ekm/keySets

Product Support: Scalar i3, Scalar i6/i6H

License Requirements: EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of keySet group resources. The keySets are the sets of encryption keys used by the KMIP encryption server(s).

URI	<i>aml/partitions/policy/ekm/keySets</i>
Method	GET
User Role Access	Admin, Service, User
Version	160(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Header	Content-Type:application/xml or application/json
Response Codes	200
Response Data	See Figure 111: keySetList

Table 192: POST aml/partitions/policy/ekm/keySets

Product Support: Scalar i3, Scalar i6/i6H

License Requirements: EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Initiate the generation of a new keySet group resource. A request will be sent to the KMIP server to start the generation of a new set of encryption keys. The name and keyCount elements of the keySet object must be provided in the request. The keySet keys will not be available until all the keys have been generated.

URI	<i>aml/partitions/policy/ekm/keySets</i>
Method	POST
User Role Access	Admin, Service
Version	160(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 112: keySet
Response Header	Content-Type:application/xml or application/json
Response Codes	200, 403
Response Data	See Figure 111: keySetList

Table 193: PUT aml/partitions/policy/ekm/keySet/{name}

Product Support: Scalar i3, Scalar i6/i6H

License Requirements: EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the keySet group resource identified by the URI path template “name”. The name and keyCount elements of the keySet object must be provided in the request. The keyCount will indicate the additional number of keys to generate for this group.

URI	<i>aml/partitions/policy/ekm/keySet/{name}</i>
Method	PUT
User Role Access	Admin, Service
Version	160(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 112: keySet
Response Header	Content-Type:application/xml or application/json
Response Codes	200, 403
Response Data	See Figure 112: keySet

Table 194: GET aml/partitions/reports/utilization

Product Support: Scalar i6000

License Requirements: Partition Utilization

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the partition utilization file resource. The output below is a sample of what the report looks like.

The Partition Utilization Report provides information for library partition usage determination, capturing high watermark counts for drive, slot and media usage. The report information provides all necessary details to evaluate library and partition usage for proper sizing and/or usage determination, see below:

SN: 273190049

Date: Tue Jun 03 10:21:27 MDT 2014

```

----- June : 2014 -----
HIGH WATER MARKS:
DWM:2, SWM:12, MWM:2, PN:LL5
DWM:0, SWM:24, MWM:3, PN:AMP Part
DWM:1, SWM:24, MWM:3, PN:MEDIA Partition
DWM:3, SWM:12, MWM:6, PN:LL1
DWM:1, SWM:12, MWM:1, PN:edlm
DWM:0, SWM:108, MWM:17, PN:AV
DWM:1, SWM:18, MWM:0, PN:LL3
DWM:1, SWM:120, MWM:41, PN:LL2
DWM:1, SWM:120, MWM:2, PN:EDLM
DWM:0, SWM:12, MWM:1, PN:AMP
DWM:0, SWM:12, MWM:1, PN:amp partition
DWM:0, SWM:0, MWM:0, PN:JUnit Empty Partition
DWM:0, SWM:120, MWM:2, PN:AMPPY
DWM:2, SWM:660, MWM:126, PN:JUnit Standard LL One
DWM:0, SWM:330, MWM:55, PN:JUnit Active Vault Partition
DWM:2, SWM:660, MWM:126, PN:JUnit Standard Partition
DWM:1, SWM:24, MWM:2, PN:Sales Partition One
DWM:0, SWM:330, MWM:55, PN:JUnit AMP Partition
DWM:0, SWM:24, MWM:3, PN:AV Part
DWM:0, SWM:12, MWM:1, PN:amp
DWM:1, SWM:102, MWM:2, PN:LL4 IBM

PARTITION ACTIVITY:
Mon Jun 02 10:52:15 MDT 2014,LL1,0,0,0>Delete
Thu May 15 16:06:44 MDT 2014,Sales Partition One,1,24,2,Rename Sales Partition Sales Partition One
Fri May 09 16:24:29 MDT 2014,Sales Partition One,1,24,2,Create first

```

<i>URI</i>	<i>aml/partitions/reports/utilization</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none"> save="name" where name is a file name to use to save the file in text format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/octet-stream On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Partition utilization data

Table 195: POST *aml/partitions/reports/utilization/email*

Product Support: Scalar i6000

License Requirements: Partition Utilization

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the Partition Utilization activity report. The information will be in an email attachment and the file format will be text.

<i>URI</i>	<i>aml/partitions/reports/utilization/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 196: GET *aml/partition/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the partition identified by the URI path template "name". To retrieve the partition name "Test Partition", the following URI would be requested: "aml/partition/Test Partition".

<i>URI</i>	<i>aml/partition/{name}</i>
Method	GET
User Role Access	Admin, Service, User

Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 160: partition

Table 197: PUT aml/partition/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Modify the partition identified by the URI path template “name”.

The following URI “aml/partition/LL2” and XML request data will modify the partitions, name, barcodeReporting, vendorId and productId. The serialNumber field must be specified as this is used to identify the partition you want to modify.

Note: Depending on library model and partition type, not all fields are modifiable.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:partition xmlns:ns2="http://automatedMediaLibrary/">
  <name>Partition2</name>
  <serialNumber>273190048_LL3</serialNumber>
  <barcodeReporting>1</barcodeReporting>
  <vendorId>1</vendorId>
  <productId>7</productId>
</ns2:partition>
```

To change other partition attributes, refer to the following:

- Table 199: GET aml/partition/{name}/ampExtensionsCount
- Table 201: GET aml/partition/{name}/barcodeReporting
- Table 210: GET aml/partition/{name}/mode
- Table 212: GET aml/partition/{name}/name
- Table 241: GET aml/partition/{name}/segments
- Table 279: GET aml/physicalLibrary/segments

URI	aml/partition/{name}
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 160: partition
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 160: partition

Table 198: DELETE aml/partition/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 90 seconds

Description: Delete the partition identified by the URI path template “name”.

<i>URI</i>	<i>aml/partition/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 199: GET aml/partition/{name}/ampExtensionsCount - deprecated

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current amp extensions count for the partition identified by the URI path template “name”.

A single string value will be returned that represents the current configured extension count. The count represents the number of segments/magazines.

Note: This interface has been deprecated as of firmware version 785. It is recommended to use *GET aml/partition/{name}* to retrieve this value.

<i>URI</i>	<i>aml/partition/{name}/ampExtensionsCount</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	The number of AMP extensions

Table 200: PUT aml/partition/{name}/ampExtensionsCount - deprecated

Product Support: Scalar i6000

Response Time: Minimum <= 5 seconds; Maximum = 30 seconds

Description: Change the partition’s amp extensions count (segments). The number that is requested will be added or subtracted from the current extension count. If you want to add 5 segments to the current count, request 5. If you want to remove 4 segments, request -4.

This option only applies to standard partitions.

Note: This interface has been deprecated as of firmware version 785. It is recommended to use *PUT aml/partition/{name}* to update this value.

<i>URI</i>	<i>aml/partition/{name}/ampExtensionsCount</i>
Method	PUT
User Role Access	Admin, Service

Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	The number of extensions to add or subtract from the current count.
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 201: GET aml/partition/{name}/barcodeReporting - deprecated

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current barcodeReporting methodology (Prefix, Suffix, Disabled or Pass Through) of the partition identified by the URI path template “name”.

A single string value will be returned and the possible values are:

- 1 (Prefix, Media ID First), expect and report barcode label’s media id first
- 2 (Suffix, Media ID Last,) expect and report barcode label’s media id last
- 3 (Disabled, Standard), report barcode identifier without media identifier
- 4 (Pass Through), report barcode label information as scanned on label
- 5 (Standard 6), expect and report 6 character barcode without media identifier
- 6 (Plus 6), expect 6 character barcode label with additional media identifier

Note: Barcode reporting methodologies 5 and 6 are only supported by the Scalar i3/i6/i6H.

Note: This interface has been deprecated in firmware versions 785(i6000) and 260(i3/i6/i6H). It is recommended to use *GET aml/partition/{name}* to retrieve this value.

URI	aml/partition/{name}/barcodeReporting
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1,2,3,4,5 or 6 (5 and 6 only on i3/i6/i6H)

Table 202: PUT aml/partition/{name}/barcodeReporting - deprecated

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the partitions barcode reporting methodology for a standard, SCSI-host-connected partition identified by the URI path template “name”.

The partition’s mode must change before a connected host will see these changes. To change the partitions mode, see: Table 210: GET aml/partition/{name}/mode.

Note: This interface has been deprecated in firmware versions 785(i6000) and 260(i3/i6/i6H). It is recommended to use *PUT aml/partition/{name}* to update this value.

URI	<i>aml/partition/{name}/barcodeReporting</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1,2,3,4,5 or 6 (5 and 6 only on i3/i6/i6H)
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 203: GET *aml/partition/{name}/controlPath*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of control path capable drives for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/controlPath</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	None (dataStore support deprecated)
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	See Figure 32: driveList

Table 204: PUT *aml/partition/{name}/controlPath*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 120 seconds

Description: Update the control path (CP) settings on the requested drives that host a partition’s control path. See the XML REQUEST DATA examples below for more details:

Example 1: Configure a Standard CP drive, no failover. The controlPath type must be 2 and primary must be set to true.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>true</primary>
        <type>2</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>
```

Example 2: To remove a CP drive, the controlPath type must be set to 1. This is also used to

disable Control Path in the case where there are ControlPath Failover (CPF) drives configured. You only need to specify the CP drive to be disabled.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>true</primary>
        <type>1</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>
```

Example 3: Configure Basic CP/CPF pair. The controlPath type must be set to 3 and one of the drives must have primary set to true.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F001396043</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>true</primary>
        <type>3</type>
      </controlPath>
    </settings>
  </drive>
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>false</primary>
        <type>3</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>
```

Example 4: Set the CP/CPF pair to advanced mode. The controlPath type must be set to 4.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F001396043</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>true</primary>
        <type>4</type>
      </controlPath>
    </settings>
  </drive>
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>false</primary>
        <type>4</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>
```

```

    </controlPath>
  </settings>
</drive>
</ns2:driveList>

```

Example 5: Remove a CPF drive from a CP/CPF pair. The CPF drive controlPath type must be set to 1 and the CP drive controlPath type must be set to 2.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F001396043</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>true</primary>
        <type>2</type>
      </controlPath>
    </settings>
  </drive>
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>false</primary>
        <type>1</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>

```

Example 6: Add a basic CPF drive to an existing CP drive. Both drives must have their controlPath type set to 3.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <logicalSerialNumber>F001396043</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>true</primary>
        <type>3</type>
      </controlPath>
    </settings>
  </drive>
  <drive>
    <logicalSerialNumber>F00139603D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>false</primary>
        <type>3</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>

```

Example 7: Add an advanced CPF drive to an existing ACPF cluster.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">

```

```

<drive>
  <logicalSerialNumber>F001396025</logicalSerialNumber>
  <settings>
    <controlPath>
      <primary>>false</primary>
      <type>4</type>
    </controlPath>
  </settings>
</drive>
</ns2:driveList>

```

Example 8: Configure three multi control path drives. This would be the same for Advanced IBM control path, except the type field would be set to 6 instead of 5.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive>
    <!-- <physicalSerialNumber>GB120401FD</physicalSerialNumber> -->
    <logicalSerialNumber>F00139709D</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>>true</primary>
        <type>5</type>
      </controlPath>
    </settings>
  </drive>
  <drive>
    <!-- <physicalSerialNumber>10WT017350</physicalSerialNumber> -->
    <logicalSerialNumber>F001397091</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>>true</primary>
        <type>5</type>
      </controlPath>
    </settings>
  </drive>
  <drive>
    <!-- <physicalSerialNumber>10WT017242</physicalSerialNumber> -->
    <logicalSerialNumber>F001397097</logicalSerialNumber>
    <settings>
      <controlPath>
        <primary>>true</primary>
        <type>5</type>
      </controlPath>
    </settings>
  </drive>
</ns2:driveList>

```

To remove one or all the multi-control paths, supply the drive list to be removed and set the *type* field to 1. When configuring multi-path or an advanced control path configuration with IBM drives, the *primary* field must be set to true.

URI	<i>aml/partition/{name}/controlPath</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	The query parameters are takePartitionOffline. The valid values for the query parameters are as follows

	<ul style="list-style-type: none"> takePartitionOffline = true or false (this parameter allows you to take the partition offline before the operation is performed. The partition will be taken online when the operation has completed. If the partition was already offline before the operation was performed, it will be left in that state.)
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 32: driveList
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 32: driveList

Table 205: GET aml/partition/{name}/dataPath

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of drive resources that are data path failover capable who belong to the partition identified by the URI path template “name”. A drive is data path failover capable if it is internally Ethernet connected, drive generation LTO5 or greater and properly licensed for redundancy/failover configuration.

URI	aml/partition/{name}/dataPath
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	None (dataStore support deprecated)
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 32: driveList

Table 206: PUT aml/partition/{name}/dataPath

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 120 seconds

Description: Update the drive resources data path failover settings that belong to the partition identified by the URI path template “name”.

URI	aml/partition/{name}/dataPath
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 32: driveList
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 32: driveList

Table 207: GET aml/partition/{name}/driveSerialNumbers

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of drive serial numbers for the drives that are configured in the partition identified by the URI path template “name”.

URI	aml/partition/{name}/driveSerialNumbers
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 44: driveSerialNumberList

Table 208: POST aml/partition/{name}/driveSerialNumbers

Product Support: Scalar i6000

Response Time: Minimum <= 5 seconds; Maximum = 180 seconds

Description: Add the drives with the serial numbers specified in the driveSerialNumberList to the partition identified by the URI path template “name”.

The example below adds the drives with logical serial number, F001396031 and F001396007 to the partition identified by the URI path template “name”.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveSerialNumberList xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>F001396031</serialNumber>
  <serialNumber>F001396007</serialNumber>
</ns2:driveSerialNumberList>
```

URI	aml/partition/{name}/driveSerialNumbers
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 44: driveSerialNumberList
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 44: driveSerialNumberList

Table 209: DELETE aml/partition/{name}/driveSerialNumbers

Product Support: Scalar i6000

Response Time: Minimum <= 5 seconds; Maximum = 180 seconds

Description: Remove the drives with the serial numbers specified in the driveSerialNumberList from the partition identified by the URI path template “name”.

The example below removes the drive with logical serial number, F001396007 from the partition identified by the URI path template “name”.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<ns2:driveSerialNumberList xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>F001396007</serialNumber>
</ns2:driveSerialNumberList>
```

<i>URI</i>	<i>aml/partition/{name}/driveSerialNumbers</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 44: driveSerialNumberList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 44: driveSerialNumberList

Table 210: GET aml/partition/{name}/mode

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current mode (Online/Offline) of the partition identified by the URI path template “name”.

A single string value will be returned and the possible values are: 1 (online) or 2 (offline)

<i>URI</i>	<i>aml/partition/{name}/mode</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 211: PUT aml/partition/{name}/mode

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the partition mode, 1 (Online) or 2 (Offline) of the partition identified by the URI path template “name”. This option only applies to standard partitions or Scalar i3/6/i6H LTFS partitions.

<i>URI</i>	<i>aml/partition/{name}/mode</i>
Method	PUT
User Role Access	i6000 - Admin, Service i3/i6/i6H – Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 or 2
Response Codes	200, 403, 404

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 212: GET aml/partition/{name}/name

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current name of the partition identified by the URI path template 'name'. The return name should be the same as the 'name' template.

<i>URI</i>	<i>aml/partition/{name}/name</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:text/plain or application/json
Response Data	The name of the partition

Table 213: PUT aml/partition/{name}/name

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 5 seconds; Maximum = 60 seconds

Description: Change the name of the partition identified by the URI path template "name". A partition name can only contain the characters A-Z a-z 0-9 _ and spaces. The maximum number of characters allowed is 64.

<i>URI</i>	<i>aml/partition/{name}/mode</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	The new name of the partition
Response Codes	200, 403, 404
Response Header	Content-Type:text/plain or application/json
Response Data	See Figure 225: WSResultCode

Table 214: GET aml/partition/{name}/operations

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of task resources that were started/requested by the partition identified by the URI path template "name".

<i>URI</i>	<i>aml/partition/{name}/operations</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)

Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 215: GET *aml/partition/{name}/operations/autolImport*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of Auto Import media tasks that were requested on the AMP partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/operations/autolImport</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 216: POST *aml/partition/{name}/operations/autolImport*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Start an Auto Import on the partition identified by the URI path template “name”.

If the partition is an AMP partition, then all standard partitions that have an Auto Import policy configured will be candidates for moving media from the AMP to those partitions. If the partition is a standard partition, then only that partition will be considered when deciding if media should be moved from the AMP partition.

Note: This is an asynchronous request. The new task object URI that was created will be included in the ‘Location’ header of the response, see Figure 209: task.

To determine if an auto import task has completed, check the state element of the task object, when complete the state should be 5 (Completed), see Figure 209: task.

URI	<i>aml/partition/{name}/operations/autolImport</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 217: GET aml/partition/{name}/operations/autoImport/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object with the id identified by the URI path template “id” and the componentId (partition name) identified by the URI path template “name”.

URI	aml/partition/{name}/operations/autoImport/{id}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 218: DELETE aml/partition/{name}/operations/autoImport/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the task object with the id identified by the URI path template “id” and the componentId identified by the URI path template “name”.

Note: This does not stop the specific auto import request. It is a way to clean up operation tasks from the library’s database.

URI	aml/partition/{name}/operations/autoImport/{id}
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 219: GET aml/partition/{name}/operations/inventory

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of inventory tasks resources that were started/requested by the partition identified by the URI path template “name”.

URI	aml/partition/{name}/operations/inventory
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A

Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 220: POST aml/partition/{name}/operations/inventory

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: (Scalar i6000) Minimum <= 1 second; Maximum = 30 seconds

Response Time: (Scalar i3/i6/i6H) Minimum <= 30 seconds ; Maximum = 1500 seconds

Description: Request the library to do an inventory for the partition identified by the URI path template “name”. If the partition is not taken offline the inventory will fail.

The startElement must be a valid element address, if the elementCount is greater than the number of elements, the inventory will ignore the extra elements. To inventory the whole partition, set the startElement to 0 and the elementCount to 65000.

The example below requests to do an inventory of the first 10 slots in the partition.

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:inventoryTask xmlns:ns2="http://automatedMediaLibrary/">
  <offline>true</offline>
  <startElement>4096</startElement>
  <elementCount>10</elementCount>
</ns2:inventoryTask>
```

Note: The Scalar i6000 supports an inventory as an asynchronous request. The new task resource URI that was created will be included in the ‘Location’ header of the response. See Table 220: POST aml/partition/{name}/operations/inventory.

In the Scalar i3/i6/i6H, the request is synchronous and blocks until the inventory completes.

URI	aml/partition/{name}/operations/inventory
Method	POST
User Role Access	i6000 - Admin, Service i3/i6/i6H – Admin, Service, User (Partition Access Required)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 110: inventoryTask (i6000 only)
Response Codes	202(i6000) 200(i3/i6/i6H), 403, 404
Response Header	Content-Type:application/xml or application/json Location: aml/partition/{name}/operations/inventory
Response Data	See Figure 225: WSResultCode

Table 221: GET aml/partition/{name}/operations/inventory/{taskId}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the inventory tasks resources that were started/requested by the partition identified by the URI path template “name” and task id identified by the URI path template “taskId”.

To determine if an inventory task has completed, the state element of the task object, when complete, should be 5 (Completed). See Figure 209: task for more details.

URI	<i>aml/partition/{name}/operations/inventory/{taskId}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 222: DELETE *aml/partition/{name}/operations/inventory/{taskId}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the inventory task resources that were started/requested by the partition identified by the URI path template “name” and identified the task id by the URI path template “taskId”.

The task must be completed (See Figure 209: task) before it can be deleted.

URI	<i>aml/partition/{name}/operations/inventory/{taskId}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 223: GET *aml/partition/{name}/policy/activeVault*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the active vault policy resources for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/policy/activeVault</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See

Figure 6: activeVaultPolicy

Table 224: PUT aml/partition/{name}/policy/activeVault**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**License Requirements:** Active Vault**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Modify the active vault policy resources for the partition identified by the URI path template “name”.

To create a new active vault policy, see Table 184: POST aml/partitions/policy/activeVault.

The example below modifies the active vault policy for partition LL2. Instead of using StorNext to decide what to do on an export, move the media directly to the AV Partition vault.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:activeVaultPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL2</partitionName>
  <vaultDefinedExport>
    <activeVaultName>AV Partition</activeVaultName>
  </vaultDefinedExport>
</ns2:activeVaultPolicy>
```

URI	<i>aml/partition/{name}/policy/activeVault</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 6: activeVaultPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 6: activeVaultPolicy

Table 225: DELETE aml/partition/{name}/policy/activeVault**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Delete the active vault policy resources for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/policy/activeVault</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 226: GET aml/partition/{name}/policy/autolImport

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve Auto Import Policy resource for the partition identified by the URI path template “name”.

The Auto Import feature allows the import of media from an AMP partition to a Standard partition based on an Auto Import Policy configured for each standard partition. The policy defines a range of media barcodes to use to determine which media gets imported into which partition.

<i>URI</i>	<i>aml/partition/{name}/policy/autolImport</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 10: autolImportPolicy

Table 227: PUT aml/partition/{name}/policy/autolImport

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the Auto Import Policy resource for the partition identified by the URI path template “name”.

The required **autolImportPolicy** object fields are **partitionName**, which should be a valid partition name and match the URI path name.

If the **mediaBarcodeFilter** is not specified or is an empty string, then Auto Import will be turned off for this partition.

The **mediaBarcodeFilter** is constrained to the following regex "`([a-zA-Z0-9]{5,15}-[a-zA-Z0-9]{5,15};?\s*)*`". Examples of valid ranges are as follows:

000100-000200
00500-00550; 00000700-00000900
100400900-100500000

Examples of invalid ranges:

000200-000100
000100-000400; 000200-000300

The **importType** field is a mask that determines what import type to perform (Added in 770(i6000)). The following values are supported:

- 0 (Disable Auto Import)
- 1 (Auto Import is activated manually (requires user action))

- 2 (Automatically activate Auto import from AMP I/E station slots when media is placed in those slots)
- 4 (Automatically activate Auto import on a predefined interval basis)

For example, to configure Auto Import automatically from AMP I/E and Auto Import on an interval basis, the value would be 6. To request all, import types the value requested should be 7.

The **interval** object field provides the capability to automatically run an Auto Import on the partition at a specific time interval (Added in 770(i6000)). The support intervals are,

interval.frequency 1 (Daily), 2 (Weekly) and 3 (Monthly).

interval.dayOfWeek 0-6 where 0 is Sunday and 6 is Saturday

interval.hourOfDay 0-23

interval.includele If true import from AMP storage and AMP IE slots, otherwise only import from AMP storage slots.

URI	aml/partition/{name}/policy/autoImport
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 10: autoImportPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 10: autoImportPolicy

Table 228: GET aml/partition/{name}/policy/autoExport

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the Auto Export policy resource for the partition identified by the URI path template “name”.

The Auto Export feature reroutes media that have been moved from a standard partition storage slot to an IE station by a host application to an AMP partition.

URI	aml/partition/{name}/policy/autoExport
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 8: autoExportPolicy

Table 229: PUT aml/partition/{name}/policy/autoExport

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the Auto Export Policy resource for the partition identified by the URI path template “name”.

To configure an Auto Export policy for partition LL1 and have the media rerouted to the AMP partition Amp1 you would use the following:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:autoExportPolicy
  xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL2</partitionName>
  <destinationAmpPartitionName>amp</destinationAmpPartitionName>
</ns2:autoExportPolicy>
```

To un-configure Auto Export for partition LL2, do the following:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:autoExportPolicy
  xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL2</partitionName>
</ns2:autoExportPolicy>
```

An Auto Export policy can only be configured for a Standard partition. You cannot configure an Auto Export policy if no AMP partitions exist. If a partition has an Active Vault policy configured, an Auto Export policy cannot be configured.

URI	<i>aml/partition/{name}/policy/autoExport</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 8: autoExportPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 8: autoExportPolicy

Table 230: GET *aml/partition/{name}/policy/driveCleaning*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the drive cleaning policy resource for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/policy/driveCleaning</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110()
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 38: driveCleaningPolicy

Table 231: POST `aml/partition/{name}/policy/driveCleaning`

Product Support: Scalar i6000

Response Time: Minimum ≤ 1 second; Maximum = 30 seconds

Description: DEPRECATED. Create a new drive cleaning policy for the partition identified by the URI path template “name”. The mountCount element should only be used for EDLM partitions.

Note: It is recommended to use the PUT method instead of this deprecated POST method.

URI	<code>aml/partition/{name}/policy/driveCleaning</code>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 38: driveCleaningPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 38: driveCleaningPolicy

Table 232: PUT `aml/partition/{name}/policy/driveCleaning`

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum ≤ 1 second; Maximum = 30 seconds

Description: Update the drive cleaning policy resource for the partition identified by the URI path template “name”.

Note: As of Scalar i6000 firmware release i12.1 (710), the enabled element has been added to the driveCleaningPolicy object. This must be used to determine if a cleaning policy be applied to the partition.

URI	<code>aml/partition/{name}/policy/driveCleaning</code>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 38: driveCleaningPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 38: driveCleaningPolicy

Table 233: DELETE `aml/partition/{name}/policy/driveCleaning`

Product Support: Scalar i6000

Response Time: Minimum ≤ 1 second; Maximum = 30 seconds

Description: DEPRECATED. Delete the drive cleaning policy resources for the partition identified by the URI path template “name”.

Note: As of Scalar i6000 firmware release i12.1 (710), it is recommended to use the PUT method instead of this deprecated DELETE method.

URI	<i>aml/partition/{name}/policy/driveCleaning</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 234: GET *aml/partition/{name}/policy/driveLeveling*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the drive leveling policy resource for the partition identified by the URI path template “name”. The drive leveling policy uses specified drive firmware images(s) to be used on the different drive generations configured in the partition. To see what firmware images are currently available/installed on the library, see the following interface: Table 108: GET *aml/drives/firmware/images*.

The type element provides three options, 0 (No drive leveling), 1 (Auto leveling) and 2 (Selective leveling).

URI	<i>aml/partition/{name}/policy/driveLeveling</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 39: driveLevelingPolicy

Table 235: PUT *aml/partition/{name}/policy/driveLeveling*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the drive leveling policy resource for the partition identified by the URI path template “name”. See examples below for details:

Example 1: Add another firmware file to be used for leveling drives in a partition. The firmware file(s) selected must be compatible with the drive(s) configured in the library. In this example we are adding firmware file “LTO6_D7Y0.fcp_fh.fmrz”. For every PUT request you must specify all the firmware files you want to apply to the partition. In this example you need to include “LTO6FH_FC_J3KZ.E” even though it is already configured.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveLevelingPolicy
  xmlns:ns2="http://automatedMediaLibrary/">
  <partition>LL1</partition>
```

```

<type>2</type>
<firmwareFile>
  <name>LTO6FH_FC_J3KZ.E</name>
  <version>J3KZ</version>
  <vendor>HP</vendor>
  <type>LTO6</type>
</firmwareFile>
<firmwareFile>
  <name>LTO6_D7Y0.fcp_fh.fmrz</name>
  <version>D7Y0</version>
  <vendor>IBM</vendor>
  <type>LTO6</type>
</firmwareFile>
</ns2:driveLevelingPolicy>

```

Example 2: Remove firmware file “LTO6FH_FC_J3KZ.E” from the current configuration. The firmware file to be deleted is not included in the request.

Basically, this firmware file object is not included in the request. Again, when you want to configure selective drive leveling you must always include all the leveling firmware files in the request.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveLevelingPolicy
  xmlns:ns2="http://automatedMediaLibrary/">
  <partition>LL1</partition>
  <type>2</type>
  <firmwareFile>
    <name>LTO6_D7Y0.fcp_fh.fmrz</name>
    <version>D7Y0</version>
    <vendor>IBM</vendor>
    <type>LTO6</type>
  </firmwareFile>
</ns2:driveLevelingPolicy>

```

Note: The Scalar i6000 version 770 added support for driveLevelingPolicy.type 1 (Auto Leveling).

URI	<i>aml/partition/{name}/policy/driveLeveling</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 39: driveLevelingPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 39: driveLevelingPolicy

Table 236: GET *aml/partition/{name}/policy/edlm*

Product Support: Scalar i6000, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the edlm policy resources for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/policy/edlm</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 54: edlmPolicy

Table 237: PUT *aml/partition/{name}/policy/edlm*

Product Support: Scalar i6000, Scalar i6/i6H

License Requirements: Extended Data LifeCycle Management (EDLM)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Modify the edlm policy resources for the partition identified by the URI path template “name”.

The example below modifies the policy such that RAS ticket generation and notification is disabled on bad or suspect media and scan policy is scheduled every 30 days for normal scans and 60 days for full scans.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:edlmPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL1</partitionName>
  <disableRasTicketGeneration>true</disableRasTicketGeneration>
  <timeInterval>
    <quickScan>0</quickScan>
    <normalScan>30</normalScan>
    <fullScan>60</fullScan>
  </timeInterval>
</ns2:edlmPolicy>
```

Note: 1. edlmPolicy.partitionName: must be a currently configured policy. 2. The only required field is 'partitionName' and if the field is not specified, the following default values will be applied:

```
<ns2:edlmPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>P1</partitionName>
</ns2:edlmPolicy>
```

Here are the default values, if the request do not include them:

edlmPolicy.onImport: 0 (None)
edlmPolicy.scanPriority: 0 (Immediate)
edlmPolicy.concurrentScans: 0
edlmPolicy.continueOnError: false
edlmPolicy.disableRasTicketGeneration: false
edlmPolicy.tapeAlert.scanType: 0
edlmPolicy.tapeAlert.count: 0
edlmPolicy.timeInterval.quickScan: 0
edlmPolicy.timeInterval.normalScan: 0
edlmPolicy.timeInterval.fullScan: 0
edlmPolicy.externalPolicies: null

edlmPolicy.externalPolicies.externalApplicationServersName: If null, this setting is disabled
 edlmPolicy.externalPolicies.mediaCopyPolicy: 0 (media copy disabled)
 edlmPolicy.externalPolicies.suspectCountScanType: 0 (None)

URI	<i>aml/partition/{name}/policy/edlm</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 54: edlmPolicy
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 54: edlmPolicy

Table 238: DELETE *aml/partition/{name}/policy/edlm*

Product Support: Scalar i6000, Scalar i6/i6H

License Requirements: Extended Data LifeCycle Management (EDLM)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the edlm policy resources for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/policy/edlm</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 239: GET *aml/partition/{name}/policy/ekm*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the encryption key management (EKM) policy for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/policy/ekm</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 162: partitionEncryptionPolicy

Table 240: PUT aml/partition/{name}/policy/ekm

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Note: If SKM is configured as the EKM solution, and encryption keys did not get created during SKM server configuration due to connection issues, enabling a partition for LME for the first time will block this operation until all required keys are created and mirrored. In such case, the operation may take as long as 3600 seconds for a Scalar i6000, and 1800 seconds for a Scalar i3/i6/i6H.

Description: Update the encryption key management (EKM) policy for the partition identified by the URI path template “name”.

URI	aml/partition/{name}/policy/ekm
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	<p>See Figure 162: partitionEncryptionPolicy The Request data will be a little different depending on the ekmServerType requested, see the following examples for details:</p> <pre><ns2:partitionEncryptionPolicy xmlns:ns2="http://automatedMediaLibrary/"> <partitionName>LL2</partitionName> <ekmServerType>4</ekmServerType> <libraryManaged>true</libraryManaged> <fipsEnabled>>false</fipsEnabled> <keyReuse>>false</keyReuse> <keyType>2</keyType> </ns2:partitionEncryptionPolicy></pre> <p>The element fipsEnabled does not apply to partitions with ekmServerType 8 (QEKM) and 32 (TKLM).</p> <p>The ekmServerType 8 and 32 (QEKM/TKLM) only applies to partitions containing only IBM drives.</p> <p>Note: The partition must be taken offline before you can change the EKM policy. All drives in the partition must be unloaded before this request can be processed. The ekmServerType selected must be configured before you can set a policy to libraryManaged. If the server is currently configured by another partition to Key Per Library (keyType) then you must select the same keyType. If Key Per Partition is configure by another partition for this server type, then only Key Per Partition or Key Per Media can be selected. If Key Per Media is configure by another partition for this server type, then only Key Per Media or Key Per Partition can be selected.</p>
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 162: partitionEncryptionPolicy

Table 241: GET aml/partition/{name}/segments**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Retrieve the segments resources for the partition identified by the URI path template “name”.

URI	<i>aml/partition/{name}/segments</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameters names are type, state, start, length, frame and rack with the following valid values:</p> <ul style="list-style-type: none"> • type="storage", "ie", "drive" or "xie" • state="full" or "empty" • start=0-n • length=1-n, anything else means all records. • frame=0 – maximum number of frames • rack = 1 or 2 <p>As an example, to retrieve all segments in one call, use “aml/partition/{name}/segments?start=0&length=-1” which is the default if no range is specified. To retrieve all drive segments, use “aml/partition/{name}/segments?type=drive”</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 242: POST aml/partition/{name}/segments**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 5 seconds; Maximum = 60 seconds**Description:** Add the list of segments to the partition identified by the URI path template “name”. The added segments must not be currently owned by this partition or another partition, they must be available. To discover which segments are available, use the following URI: Table 279: GET aml/physicalLibrary/segments.**Example 1:** To add a drive to a partition, send the request shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segmentList xmlns:ns2="http://automatedMediaLibrary/">
  <segment>
    <coordinate>
      <frame>1</frame>
      <rack>1</rack>
      <section>2</section>
      <column>1</column>
      <row>1</row>
      <type>4</type>
    </coordinate>
  </segment>
</ns2:segmentList>
```

Example 2: Add 2 storage segments and on IE segment.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segmentList xmlns:ns2="http://automatedMediaLibrary/">
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>7</section>
      <column>3</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
  </segment>
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>8</section>
      <column>3</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
  </segment>
  <segment>
    <coordinate>
      <frame>1</frame>
      <rack>2</rack>
      <section>2</section>
      <column>3</column>
      <row>1</row>
      <type>3</type>
    </coordinate>
  </segment>
</ns2:segmentList>
```

Example 3: The above 2 requests combined into one single request.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segmentList xmlns:ns2="http://automatedMediaLibrary/">
  <segment>
    <coordinate>
      <frame>1</frame>
      <rack>1</rack>
      <section>2</section>
      <column>1</column>
      <row>1</row>
      <type>4</type>
    </coordinate>
  </segment>
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>7</section>
      <column>3</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
  </segment>
</ns2:segmentList>
```



```

<segment>
  <coordinate>
    <frame>0</frame>
    <rack>1</rack>
    <section>8</section>
    <column>3</column>
    <row>1</row>
    <type>2</type>
  </coordinate>
</segment>
<segment>
  <coordinate>
    <frame>1</frame>
    <rack>2</rack>
    <section>2</section>
    <column>3</column>
    <row>1</row>
    <type>3</type>
  </coordinate>
</segment>
</ns2:segmentList>

```

The following URI can be used to find what segments are currently available (not part of an existing partition): Table 279: GET aml/physicalLibrary/segments.

URI	aml/partition/{name}/segments
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 191: segmentList
Response Codes	201, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 243: DELETE aml/partition/{name}/segments

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 5 seconds; Maximum = 60 seconds

Description: Delete the list of segments from the partition identified by the URI path template “name”.

URI	aml/partition/{name}/segments
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 191: segmentList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 244: PUT aml/partition/{name}/segments

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 5 seconds; Maximum = 60 seconds

Description: Reconfigure the partition identified by the URI path template “name” with the new segmentList request data. The segmentList can contain storage, drive, ie and extended ie segments. The segmentList can contain segments that currently belong or are available (non-allocated) to the partition. Segments assigned to other partitions cannot be specified.

The example below reconfigures a partition with one drive and 3 storage segments (18 slots).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segmentList xmlns:ns2="http://automatedMediaLibrary/">
  <segment>
    <coordinate>
      <frame>1</frame>
      <rack>1</rack>
      <section>9</section>
      <column>1</column>
      <row>1</row>
      <type>4</type>
    </coordinate>
    <size>1</size>
    <configuredType>0</configuredType>
  </segment>
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>1</section>
      <column>4</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
    <size>6</size>
    <configuredType>0</configuredType>
  </segment>
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>2</section>
      <column>4</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
    <size>6</size>
    <configuredType>0</configuredType>
  </segment>
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>3</section>
      <column>4</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
    <size>6</size>
    <configuredType>0</configuredType>
  </segment>
</ns2:segmentList>
```

```

    </coordinate>
    <size>6</size>
    <configuredType>0</configuredType>
  </segment>
</ns2:segmentList>

```

URI	<i>aml/partition/{name}/segments</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 191: segmentList
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 245: GET aml/physicalLibrary

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the physical library resource instances.

Note: The autoClean element is deprecated in the Scalar i6000 as of firmware release i12.1 (710). Refer to Table 230: GET aml/partition/{name}/policy/driveCleaning to change partition cleaning policies.

The autoConfiguration and autoCalibration features are no longer supported as of firmware release 750 (i6000). The sendUsageStatistics element is also deprecated and no longer supported as of versions 775(i6000) and 210(i3/i6/i6H). Refer to Table 380: GET aml/system/notifications/telemetrics instead.

URI	<i>aml/physicalLibrary</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 163: physicalLibrary

Table 246: PUT aml/physicalLibrary

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 25 seconds; Maximum = 60 seconds

Description: Update the physical library settings features. The settings that can be modified are listed in the physicalLibrary.phySettings object, and include the following features:

- driveSerialNumberSpoofing – enable or disable the ability for the library to present drives with logical serial numbers, rather than physical serial numbers, to a host.

Note: The library needs to be power cycled (See Table 259: POST `aml/physicalLibrary/operations/shutdown`) before the changes take effect. This only applies to Scalar i6000 libraries.

- `driveCleaningCount` – Number of cleaning operations the library may request within any 24 hour time period due to specific error codes detected from a tape drive. Valid values are 0-3.

Note: Support added in firmware versions 779 (i6000), and 260 (i3/i6/i6H).

- `autoInventory` – enable/disable a library inventory every time the library is rebooted or a Scalar i6000 main access door closes.
- `autoCalibration` – Not used. Deprecated in Scalar i6000 as of firmware release i12 (680).
- `autoConfiguration` – Not used. This feature is deprecated in i6000 i12 (680).
- `autoCleaning` – Not used. Deprecated in Scalar i6000 as of firmware release i12 (680).

Drive cleaning is now configured on a partition basis, see Table 230: GET `aml/partition/{name}/policy/driveCleaning`.

- `autoDriveUnload` – enable/disable functionality for the library to perform drive unload and eject operation if the host application does not perform drive unload requests to a drive prior to requesting the tape library to move media from a drive to a new location.
- `autoFirmwareUpgrade` – Enable or disable functionality for the library to automatically install previously uploaded library firmware upon library restart. Library restart includes any library reboot, whether intentional reboot, power-cycle or power loss.

Note: This feature is only supported in Scalar i3 and Scalar i6.

- `Ipv6` – Support for IPv6 configurations is enabled by default and not changeable.

Note: Enabling and disabling functionality has been deprecated as of Scalar i6000 firmware release i12.3 (750).

- `extendedIe` – Enable or disable the Extended IE feature

Note: Supported in Scalar i6000 only. The ability to enable/disable Extended IE has been deprecated as of version 760 of Scalar i6000 firmware release. Extended IE will always be enabled.

- `sendUsageStatistics` – Configures the notification interval in which the library sends library usage and performance data to Quantum via email or a cloud interface.

Note: This feature has been deprecated in versions 775(i6000) and 210(i3/i6/i6H) and is no longer supported; configure using telemetrics notifications Table 382: PUT `aml/system/notifications/telemetric/{receiver}`

- `healthCheck` – Defines the interval in which the library performs automatic health checks on the robot(s), tower(s) and robotic power rails. The intervals are defined in days (0-180), 0 indicating the health check is turned off.

Note: This feature is only supported by the Scalar i6000.

- `aisleLights` – Defines the time period the aisle lights will be turned on. Valid values are 30 or 60 minutes, or 0 for always turned off.

Note: This feature is only supported by the Scalar i6000.

- `webCamera` – Set the IP of the host that is running the application that is managing the camera mounted in the library.

Note: This feature is only supported by the Scalar i6000.

- `icmpService` – Enable or disable the capability for device on the network to ping the library.
- `sshService` – Enable or disable the capability to establish a secure shell (ssh) connection to the library.

- cliService – Enable or disable support for the legacy command line interface (CLI).
Note: This feature is only supported by the Scalar i6000.
- xmlInterfaceService – Enable or disable the Quantum Vision access interface.
Note: This feature is only supported by the Scalar i6000.
- serviceLogin – Enable or disable the ability of a Service user to login to the library.
Note: i6000 - The serviceLogin.enabled element is the only element supported. To enable the service user, the following would be used:

```
<ns2:physicalLibrary xmlns:ns2="http://automatedMediaLibrary/">
  <phySettings>
    <serviceLogin>
      <enabled>true</enabled>
    </serviceLogin>
  </phySettings>
</ns2:physicalLibrary>
```

i3/i6/i6H - The service user may be enabled or disabled for remote access (Library UI) or local access (via the service port). If enabledRemoteAccess or enabledLocalAccess are true, remoteAccessTimeout and localAccessTimeout are required (respectively). To enable a service user to have access from the service port for 6 hours, and disable remote access, the following XML would be used. serviceLogin.enabled is returned on a GET, but ignored on a PUT.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:physicalLibrary xmlns:ns2="http://automatedMediaLibrary/">
  <phySettings>
    <serviceLogin>
      <enabledRemoteAccess>false</enabledRemoteAccess>
      <remoteAccessTimeout>0</remoteAccessTimeout>
      <enableLocalAccess>true</enableLocalAccess>
      <localAccessTimeout>6</localAccessTimeout>
    </serviceLogin>
  </phySettings>
</ns2:physicalLibrary>
```

- sessionTimeout: – Set the session timeout: a user will be automatically logged out (session will be terminated). The valid values are, 1 through 1440 minutes. The timeout: is based on the length of inactivity of a user login session.
- snmp – Configure the library SNMP settings.
- smis – Configure the library SMIS settings.
- autoWebRequests - Enable or disable library unsolicited web request; disabled by default. If enabled, the library will automatically query the web to determine if new firmware is available.
Note: Supported by Scalar i3/i6/i6H (added in version 230.)
- logicalSystemAddressing – enable or disable library logical system addressing support. When enabled, any SCSI-host-reported partition Serial Number (SN) and World Wide Name (WWN) information will be reported with a uniquely defined logical SN and WWN, that will be maintained and reported even if the library Control Module (CM) is replaced and a new physical SN and WWN is applied and assigned to the system.
Note: Supported by Scalar i3/i6/i6H (added in version 230.)

One or more settings can be applied with a single request by including multiple features in the request data. For example, to update the extended I/E and sessionTimeout: settings, the following XML is used:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:physicalLibrary xmlns:ns2="http://automatedMediaLibrary/">
  <phySettings>
    <extendeddle>
      <enabled>true</enabled>
    </extendeddle>
    <sessionTimeout>
      <minutes>15</minutes>
    </sessionTimeout>
  </phySettings>
</ns2:physicalLibrary>

```

A feature settings update may fail for some reason. If the feature was included with other feature updates in a single request, it will return a HTTP failure status, but that does not necessarily mean that all the features were not updated successfully. It is recommended that you do a GET request after a failure has occurred to retrieve the current setting of the individual features.

URI	<i>aml/physicalLibrary</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 163: physicalLibrary
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 163: physicalLibrary

Table 247: GET aml/physicalLibrary/elements

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the elementList resource instances.

URI	<i>aml/physicalLibrary/elements</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameters names are partition, state, type, start, length, frame, rack with the following valid values:</p> <ul style="list-style-type: none"> • partition=name of partition • state="full" or "empty". The slot contains a media (full) or the slot is empty (empty) • type="storage", "ie", "drive" "xie" or "cleaning" • start=0-n • length=1-n, anything else means all records. • frame=0 – maximum number of frames (specify which frame you want) • rack = 1 or 2 • coordinate = Frame,Rack,Section,Column,Row,Type. A comma separated coordinate. This query parameter should not be used with any other query parameter. See Figure 26:

	<p>coordinate</p> <p>To retrieve all elements in one call use “aml/physicalLibrary/elements?start=0&length=-1” which is the default if no range is specified.</p> <p>To retrieve all elements belonging to partition named TEST use “aml/physicalLibrary/elements?partition=TEST”.</p> <p>To retrieve all ie elements that contain media use “aml/physicalLibrary/elements?type=ie&state=full”.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 66: elementList

Table 248: GET aml/physicalLibrary/environment

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of environment records. The environment record provides information about temperature and humidity within the library over a period of time.

If the Media Type text/plain is selected (Accept http header) the data will be returned in CSV format.

URI	aml/physicalLibrary/environment
Method	GET
User Role Access	Admin, Service, User
Version	160(i3/i6/i6H), 770(i6000)
Parameters	<p>The following query parameters are supported, start, length, period, date, save with the following values:</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • save=”name” where name is a file name to use to save the file in CSV format. The save=”name” query parameter should be used by a client browser to allow the data to be saved by the browser. A default “name” is provided if none is specified. <p>If no query parameters are used the request will return all the environment data.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200

Response Header	Content-Type:application/xml or application/json, text/plain, application/octet-stream On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 74: environmentList

Table 249: POST *aml/physicalLibrary/environment/email*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email library temperature and humidity environmental data.

The information will be in an email attachment and the file format will be CSV.

The reportCriteria object supports the same query parameters as Table 248:

<i>URI</i>	<i>aml/physicalLibrary/environment/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	160(i3/i6/i6H), 770(i6000)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 250: GET *aml/physicalLibrary/i3-i6/modules*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of module resources. The module.section.status element is applicable to a Service Module, conveying operational status of the Service Tray. A status of 0 is returned for all other section types.

Note: Added in Scalar i3/i6/i6H version 220. This request replaces GET */aml/physicalLibrary/quattro/modules*.

<i>URI</i>	<i>aml/physicalLibrary/i3-i6/modules</i>
Method	GET
User Role Access	Admin, Service, User
Version	220 (i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 145: moduleList

Table 251: GET *aml/physicalLibrary/mode*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current physical library mode, 1 (online) or 2(offline).

URI	<i>aml/physicalLibrary/mode</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 252: PUT *aml/physicalLibrary/mode*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the physical library mode to 1 (online) or 2 (offline) which will affect all logical library access.

URI	<i>aml/physicalLibrary/mode</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 or 2
Response Codes	200, 403
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 253: GET *aml/physicalLibrary/operations*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of task resources that were started/requested.

URI	<i>aml/physicalLibrary/operations</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	Query parameters names are type with the following valid values: <ul style="list-style-type: none"> • type = 0 (All), • 1 (inventory), • 2 (library shutdown), • 3 (library reboot), • 4 (identify drive), • 5 (drive clean), • 6 (power cycle FC IO blade), • 7 (reset FC IO blade), • 8 (identify FC IO blade),

	<ul style="list-style-type: none"> • 9 (Identify Ethernet Expansion Blade), • 10 (Auto Import Media), • 11 (Generate Command History Logs)
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 254: GET aml/physicalLibrary/operations/inventory

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of inventory tasks that we requested on the physical library.

URI	aml/physicalLibrary/operations/inventory
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 255: POST aml/physicalLibrary/operations/inventory

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: (Scalar i6000) Minimum <= 1 second; Maximum = 30 seconds

Response Time: (Scalar i3/i6/i6H) Minimum <= 30 seconds ; Maximum = 1500 seconds

Description: This command requests that the library perform an inventory of the physical library. This inventory request does not account for any partition configuration and performs an inventory of the complete system (Scalar i6000 and Scalar i3/i6/i6H), or for a specific element type of specified element address and number of elements (Scalar i6000 only). For inventory operations within partition boundaries, see Table 220: POST aml/partition/{name}/operations/inventory.

Scalar i6000:

The Scalar i6000 requires the use of the inventoryTask object to specify the starting element address and the number of elements of same element type to inventory. Specifying 0 for the starting element address and a 0 for the element count will inventory all elements in the complete physical library. To determine any other valid starting element address, see Table 279: GET aml/physicalLibrary/segments.

The Scalar i6000 requires the physical library to be offline and if not taken offline from the local user interface or remotely already, the command needs to have the inventoryTask object specify that the operation be performed in offline mode. Unless the physical library is taken offline for this command, the command request will be rejected.

Note: *The Scalar i6000 supports an inventory as an asynchronous request. The new task resource URI that was created will be included in the 'Location' header of the response, see*

Table 256: GET aml/physicalLibrary/operations/inventory/{id}. To determine if an inventory task has completed, check the state element of the task object; when complete the state should be 5 (Completed), see Figure 209: task.

Depending on library size and library configuration, inventory completion times vary. An inventory request that uses a single robot to perform the scanning of all requested elements, may take 5 seconds per storage or drive column. A standard frame inventory may take about 1 minute per frame, and a high density module may take about 2 minutes per frame.

Scalar i3/i6/i6H:

The Scalar i3/i6/i6H support this command without parameters and always inventories the complete physical library. To inventory specific elements and ranges, see Table 285: POST aml/physicalLibrary/segments/operations/inventory.

Note: *The Scalar i3/i6/i6H perform the operation synchronously, blocking the request until the inventory completes. Depending on library size, an inventory may take up to 1.5 minutes for a Scalar i3 module, and 3 minutes per Scalar i6/i6H module.*

URI	aml/physicalLibrary/operations/inventory
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 110: inventoryTask (i6000 only)
Response Codes	202(i6000) 200(i3/i6/i6H), 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 256: GET aml/physicalLibrary/operations/inventory/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object with the id identified by the URI path template “id”.

To retrieve a task object with id of 86, use URI: ‘aml/physicalLibrary/operations/inventory/86’.

URI	aml/physicalLibrary/operations/inventory/{id}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 257: DELETE aml/physicalLibrary/operations/inventory/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the task object with the id identified by the URI path template “id”.

Note: This does not stop the specific inventory request. It will cleanup operation tasks from the library’s database.

URI	<i>aml/physicalLibrary/operations/inventory/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 258: GET *aml/physicalLibrary/operations/shutdown*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of shutdown tasks that were requested on the physical library.

URI	<i>aml/physicalLibrary/operations/shutdown</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 259: POST *aml/physicalLibrary/operations/shutdown*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Shut down the library using the shutdownTask object. This object must specify a reboot element with a value of false, otherwise the library will reboot. To complete the shutdown process, you must physically push the library power button.

URI	<i>aml/physicalLibrary/operations/shutdown</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 200: shutdownTask
Response Codes	202, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 260: GET *aml/physicalLibrary/operations/shutdown/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object of type 2 (Shutdown) with the id identified by the URI path template "id".

<i>URI</i>	<i>aml/physicalLibrary/operations/shutdown/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 261: DELETE *aml/physicalLibrary/operations/shutdown/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the task object (type 2 - Shutdown) with identified by the URI path template "id".

Note: This request does not stop the shutdown operation in progress.

<i>URI</i>	<i>aml/physicalLibrary/operations/shutdown/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 262: GET *aml/physicalLibrary/operations/reboot*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of reboot tasks that were previously requested.

<i>URI</i>	<i>aml/physicalLibrary/operations/reboot</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 263: POST *aml/physicalLibrary/operations/reboot*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Reboot the library using the shutdownTask object. This object must specify a reboot element with a value of true, otherwise the library will shut down.

URI	<i>aml/physicalLibrary/operations/reboot</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 200: shutdownTask
Response Codes	202, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 264: GET *aml/physicalLibrary/operations/reboot/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object of type 3 (Reboot) with the id identified by the URI path template "id".

URI	<i>aml/physicalLibrary/operations/reboot/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 265: DELETE *aml/physicalLibrary/operations/reboot/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the task object of type 3 (Reboot) with the id identified by the URI path template "id".

Note: This request does not stop the reboot operation in progress.

URI	<i>aml/physicalLibrary/operations/reboot/{id}</i>
Method	DELETE

User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 266: GET aml/physicalLibrary/operations/reset

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of reset tasks that were previously requested.

<i>URI</i>	<i>aml/physicalLibrary/operations/reset</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 260(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 267: POST aml/physicalLibrary/operations/reset

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Reset the library.

<i>URI</i>	<i>aml/physicalLibrary/operations/reset</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	202, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 268: GET aml/physicalLibrary/operations/reset/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object of type 53 (Reset Library) with the id identified by the URI path template “id”.

URI	<i>aml/physicalLibrary/operations/reset/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 269: DELETE *aml/physicalLibrary/operations/reset/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the task object of type 53 (Reset Library) with the id identified by the URI path template “id”.

Note: This request does not stop the reset operation in progress.

URI	<i>aml/physicalLibrary/operations/reset{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 270: GET *aml/physicalLibrary/operations/teach*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of teach tasks that were previously requested or are currently in progress.

URI	<i>aml/physicalLibrary/operations/teach</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 271: POST *aml/physicalLibrary/operations/teach*

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Request to run a teach configure or teach calibrate on the library using the teachTask object. To run a teach on the complete library you can specify the library startFrame and endFrame or startFrame of -1 and endFrame of -1 or not specify a range.

URI	<i>aml/physicalLibrary/operations/teach</i>
Method	POST
User Role Access	Admin, Service
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 203: teachTask
Response Codes	202, 403
Response Header	Content-Type:application/xml or application/json Location: aml/physicalLibrary/operations/teach/{id}
Response Data	See Figure 225: WSResultCode

Table 272: GET *aml/physicalLibrary/operations/teach/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task object of type 51 (Teach) with the id identified by the URI path template "id".

URI	<i>aml/physicalLibrary/operations/teach/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 273: DELETE *aml/physicalLibrary/operations/teach/{id}*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the task object of type 51 (Teach) with the id identified by the URI path template "id".

Note: This request does not stop the teach operation in progress.

URI	<i>aml/physicalLibrary/operations/teach/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 274: GET aml/physicalLibrary/quattro/modules - deprecated

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of module resources.

Note: This interface is supported but has been deprecated in Scalar i3/i6/i6H version 220. Use Table 250: GET aml/physicalLibrary/i3-i6/modules instead.

URI	aml/physicalLibrary/quattro/modules
Method	GET
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 145: moduleList

Table 275: GET aml/physicalLibrary/subset/configuration

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve a subset of the physicalLibrary resource, which groups all configuration options of the library.

URI	aml/physicalLibrary/subset/configuration
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 164: physicalLibraryConfiguration

Table 276: GET aml/physicalLibrary/subset/remoteAccess

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a subset of the physicalLibrary resource, which groups all remote network service access options of the library.

URI	aml/physicalLibrary/subset/remoteAccess
Method	GET
User Role Access	Admin, Service, User

Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 165: physicalLibraryRemoteAccess

Table 277: GET aml/physicalLibrary/subset/resources

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a subset of the physicalLibrary resource, which groups library storage and device resources.

<i>URI</i>	<i>aml/physicalLibrary/subset/resources</i>
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 166: physicalLibraryResources

Table 278: GET aml/physicalLibrary/subset/settings

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a subset of the physicalLibrary resource, which groups similar physical library settings.

<i>URI</i>	<i>aml/physicalLibrary/subset/settings</i>
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 167: physicalLibrarySettings

Table 279: GET aml/physicalLibrary/segments

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of segment resources.

<i>URI</i>	<i>aml/physicalLibrary/segments</i>
------------	-------------------------------------

Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameters names are partition, status, type, start, length, frame, rack with the following valid values:</p> <ul style="list-style-type: none"> • partition=name of partition • status="available" or "used" (owned by a partition or not) • type="storage", "ie", "drive", "xie" or "cleaning" • start=0-n • length=1-n, anything else means all records. • frame=0 – maximum number of frames • rack = 1 or 2 <p>To retrieve all segments in one call use "aml/physicalLibrary/segments?start=0&length=-1" which is the default if no range is specified.</p> <p>To retrieve all segments belonging to partition named LL1 use "aml/physicalLibrary/segments?partition=LL1".</p> <p>To retrieve all ie segments use "aml/physicalLibrary/segments?type=ie".</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 280: GET aml/physicalLibrary/segments/amp

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the storage segment resources belonging to Automated Media Pool (AMP) partitions.

URI	<i>aml/physicalLibrary/segments/amp</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 281: PUT aml/physicalLibrary/segments/amp

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the owner of the segments in the segmentList. This interface is used to reassign *storage* segments from a Standard partition to an Automated Media Pool (AMP) partition and vice versa.

When reassigning storage segments from an AMP to a Standard partition, the Standard

partition should have enough available AMP extensions configured to satisfy the request (reassign segments <= AMP extensions). The segment list in the request must belong to a single partition and must be reassigned to a single partition.

In the example below there is a segment that belongs to an AMP partition called AMP and we want to reassign it to a partition called LL1. The segmentList will contain a single segment that currently belongs to the AMP partition with its owner element changed to LL1, the partition to which the segment will be reassigned.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segmentList xmlns:ns2="http://automatedMediaLibrary/">
  <segment>
    <coordinate>
      <frame>0</frame>
      <rack>1</rack>
      <section>4</section>
      <column>3</column>
      <row>1</row>
      <type>2</type>
    </coordinate>
    <size>6</size>
    <owner>LL1</owner>
    <configuredType>0</configuredType>
  </segment>
</ns2:segmentList>
```

To retrieve a list of AMP storage segments, use the GET request above. To retrieve a list of Standard storage segments, use Table 241: GET aml/partition/{name}/segments with the appropriate query parameters.

URI	<i>aml/physicalLibrary/segments/amp</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 191: segmentList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 282: GET aml/physicalLibrary/segments/cleaning

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of cleaning segment resources configured for storage of cleaning tapes used for automatic, library-initiated cleaning.

URI	<i>aml/physicalLibrary/segments/cleaning</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 191: segmentList

Table 283: POST [aml/physicalLibrary/segments/cleaning](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Create a new cleaning tape segment resource. If the segment contains media, such media requires proper cleaning tape barcode label identification. If the segment is empty, cleaning tapes may be imported to the segment with or without proper cleaning media identification, see Table 165: POST [aml/media/operations/moveMedium](#).

URI	<i>aml/physicalLibrary/segments/cleaning</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 192: segment
Response Codes	201, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 284: DELETE [aml/physicalLibrary/segments/cleaning](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Remove a cleaning segment resource and return it to the pool of unassigned/unconfigured segments.

URI	<i>aml/physicalLibrary/segments/cleaning</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 192: segment. Identifies the cleaning segment to delete.
Response Codes	201, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 285: POST [aml/physicalLibrary/segments/operations/inventory](#)

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 30 seconds; Maximum = 1500 seconds

Description: Request the library to do an inventory on the list of segments/magazines/drives provided by the segmentList. The only element of the segment object that needs to be provided is the coordinate.

URI	<i>aml/physicalLibrary/segments/operations/inventory</i>
Method	POST
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 191: segmentList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 286: GET *aml/physicalLibrary/status*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the library status information resource. This resource reports general state/status information about the library.

Note: This URI does not affect the user's session timeout; all other URIs are considered a user activity and reset the session timeout.

URI	<i>aml/physicalLibrary/status</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 124: libraryStatus

Table 287: GET *aml/service/logs*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of service logs.

URI	<i>aml/service/logs</i>
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 198: serviceLogList

Table 288: GET *aml/service/log/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the service log identified by the URI path template “name”. The available log names are provided by the interface Table 287: GET aml/service/logs.

URI	aml/service/log/{name}
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	Query parameters and their respective values are as follows: <ul style="list-style-type: none">• save=the default name you want the browser to save the contents of the file too. If no name is specified, a default name will be supplied by the Web Server. The purpose of the save parameter is to tell the Web Browser that this is an attachment.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/octet-stream, application/xml or application/json Content-Disposition: attachment; filename="the name of the file" (This will only happen if the save query parameter is requested) On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	The log file content.

Table 289: POST aml/service/log/{name}/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the service log identified by the URI path template “name”.

URI	aml/service/log/{name}/email
Method	POST
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 290: POST aml/service/resetFactoryDefault

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Reset the library’s configuration to factory defaults.

URI	<i>aml/service/resetFactoryDefault</i>
Method	POST
User Role Access	Admin, Service
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	202, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 291: GET *aml/service/vt/test*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of supported tests.

URI	<i>aml/service/vt/test</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 118: libraryDiagnosticTestList

Table 292: POST *aml/service/vt/test/abort*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Stop the currently running diagnostic test and end the initiated diagnostic test session.

URI	<i>aml/service/vt/test/abort</i>
Method	POST
User Role Access	Admin, Service
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 293: GET *aml/service/vt/test/operations*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of requested Diagnostic, Verification Test (VT), tasks. The supported tasks are as follows:

- 12 (Start Test Diagnostic Session (i6000 only))
- 13 (Finish Test Diagnostic Session (i6000 only))
- 14 (Robot Accessor Test (i6000 only))
- 15 (Robot Picker Test (i6000 only))
- 16 (Robot Assembly Test (i6000 and i3/i6/i6H))
- 17 (IE Station Assembly Test (i6000 only))
- 18 (Tower Assembly Test (i6000 only))
- 19 (Tower Scanner Test (i6000 only))
- 20 (Robot Scanner Test (i6000 only))
- 21 (Library Get/Put Test (i6000 only))
- 22 (Drive Assembly Test (i6000 and i3/i6/i6H))
- 23 (Magazine Test (i3/i6/i6H only))
- 24 (Installation Verification Test (IVT) (i6000 and i3/i6/i6H))
- 27 (Library Alignment Test (i6000 only))
- 28 (Barcode Label Test (i6000 only))
- 29 (Module Assembly Test (i3/i6/i6H only))
- 51 (Teach Configure/Calibrate (i6000)) (Added in version 760(i6000))

URI	<i>aml/service/vt/test/operations</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000), 110(i3/i6/i6H)
Parameters	Query parameter names are type with the following valid values: <ul style="list-style-type: none">• type=# or lastRun If type = # then a taskList will be returned with the tasks of the specified task type number. To retrieve a list of Robot tasks that were run use the following <code>aml/service/vt/test/operations?type=16</code> If no Robot tests were run, you will get an empty list. If type=lastRun, you will get a list of the last run task types, no more than one for each task type and if a specific task type was never run, it will not be included.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 208: taskList

Table 294: POST *aml/service/vt/test/operations*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Start a Verification Test (VT) diagnostic test task.

Scalar i6000: To initiate a diagnostic test on the i6000, a request with task type 12 (Start Test

Diagnostic Session) must be issued first, except in the case of 24 (IVT). The start request prepares the library for diagnostic tests to run. Without a task type 12 running, no other diagnostic test task is permitted, except for task type 24. To complete the test session, for all task types except 24, the test type 13 (Finish Test Diagnostic Session) should be issued.

Scalar i3/i6/i6H: Start and Finish Test Diagnostic Sessions are not required. If issued, they are ignored. Media Locations may be the coordinate for a scratch tape in a shared IE slot when the library is configured for *Remote UI/Host Assignment*. If no IE slots are configured, the Scalar i3 and Scalar i6 will default to use the tape in location 1,1,0,10,1; the Scalar i6H will use location 1,1,0,12,1. Multiple media locations are not supported.

VT task types use the libraryTestParameters object which includes multiple options. A list of valid options, by test type, are listed below.

12 (Start Test Diagnostic Session (i6000 only)) No libraryTestParameters required

13 (Finish Test Diagnostic Session (i6000 only)) No libraryTestParameters required

14 (Robot Accessor Test (i6000 only))

- libraryTestParameters.robot

Note: You must specify 0(Left) or 1(Right) robot but not 2(Both).

15 (Robot Picker Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.mediaLocations (Scratch tape, must be an IE Station slot containing media, this parameter is optional.)
- libraryTestParameters.slotLocation (This can be a Storage, Drive or IE slot.)

16 (Robot Assembly Test (i6000 and i3/i6/i6H))

- libraryTestParameters.robot
- libraryTestParameters.startModule
- libraryTestParameters.endModule
- libraryTestParameters.startRack
- libraryTestParameters.endRack
- libraryTestParameters.mediaLocations (Scratch tape, must be an IE Station slot containing media)

17 (IE Station Assembly Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.startModule (Starting IE Station Number)
- libraryTestParameters.endModule (Ending IE Station Number)
- libraryTestParameters.mediaLocations (Scratch Tape, must be an IE Station slot containing media.)

18 (Tower Assembly Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.startModule
- libraryTestParameters.endModule

Note: The start and end modules/frames must contain towers. Use the interface Table 89: GET aml/devices/towers to retrieve a list of configured towers.

19 (Tower Scanner Test (i6000 only))

- libraryTestParameters.robot (DEPRECATED)
- libraryTestParameters.startModule
- libraryTestParameters.endModule

Note: The start and end modules/frames must contain towers with scanners installed.

Note: The libraryTestParameters.robot is no longer a required parameter and should be ignored.

20 (Robot Scanner Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.startModule
- libraryTestParameters.endModule
- libraryTestParameters.startRack
- libraryTestParameters.endRack

21 (Library Get/Put Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.startModule
- libraryTestParameters.endModule
- libraryTestParameters.startRack
- libraryTestParameters.endRack
- libraryTestParameters.mediaLocations (Scratch tapes, must be an IE Station slot containing media.)

22 (Drive Assembly Test (i6000 and i3/i6/i6H))

- libraryTestParameters.robot (i6000 Only)
- libraryTestParameters.mediaLocations (Scratch tape, must be an IE Station slot containing media. (i6000 Only))
- libraryTestParameters.startLocation
- libraryTestParameters.endLocation

23 (Magazine Test (i3/i6/i6H only))

- libraryTestParameters.startLocation
- libraryTestParameters.endLocation

24 (IVT Test (i6000 and i3/i6/i6H))

- libraryTestParameters.mediaLocations (Scratch tape(s), must be one or more IE Station slots containing media. It is recommended to use 2 scratch tapes in a library with dual robots (i6000 only))
- libraryTestParameters.partialIvt, this is optional and should include the following elements: libraryTestParameters.startModule, libraryTestParameters.endModule,

libraryTestParameters.startRack and libraryTestParameters.endRack. If set to true, it will perform a partial IVT on the modules and racks specified (i6000 only)

- libraryTestParameters.startLocation (i3/i6/i6H only)
- libraryTestParameters.endLocation i3/i6/i6H only)

27 (Library Alignment Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.startModule
- libraryTestParameters.endModule
- libraryTestParameters.startRack
- libraryTestParameters.endRack

28 (Barcode Label Test (i6000 only))

- libraryTestParameters.robot
- libraryTestParameters.slotLocation (This can be a Storage, Drive or IE slot).

29 (Module Assembly Test (i3/i6/i6H only))

- libraryTestParameters.mediaLocations

51 (Teach Configure/Calibrate (i6000)) (Added in version 760(i6000))

URI	<i>aml/service/vt/test/operations</i>
Method	POST
User Role Access	Admin, Service
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 123: libraryDiagnosticTestTask
Response Codes	202, 403
Response Header	Content-Type:application/xml or application/json Location: aml/service/vt/operation/taskId (i6000 only)
Response Data	See Figure 225: WSResultCode

Table 295: GET aml/service/vt/test/operation/{taskId}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the task identified by the URI template 'taskId'.

URI	<i>aml/service/vt/test/operation/{taskId}</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 209: task

Table 296: GET aml/service/vt/test/sessions

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of library diagnostic test session resources

<i>URI</i>	<i>aml/service/vt/test/sessions</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 121: libraryDiagnosticTestSessionList

Table 297: GET aml/service/vt/test/session

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the last or currently running library diagnostic test session. This can be used to get results for the current or last run VT session.

<i>URI</i>	<i>aml/service/vt/test/session</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 122: libraryDiagnosticTestSession

Table 298: GET aml/service/vt/test/session/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the session resource identified by the URI path template “id”.

<i>URI</i>	<i>aml/service/vt/test/session/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	735(i6000), 110(i3/i6/i6H)
Parameters	N/A

Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 122: libraryDiagnosticTestSession

Table 299: DELETE [aml/service/vt/test/session/{id}](#)

Product Support: Scalar i6000

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the session resource identified by the URI path template “id”. This will delete the session record from the library’s database.

<i>URI</i>	<i>aml/service/vt/test/session/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	735(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 300: GET [aml/system/configuration/record](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a library configuration record.

<i>URI</i>	<i>aml/system/configuration/record</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none"> save="name" where name is a file name to use to save the file in text format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: text/plain or application/octet-stream On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Byte Stream or text

Table 301: POST [aml/system/configuration/record/email](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email a library configuration record to recipients specified in the provided email object.

URI	<i>aml/system/configuration/record/email</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 302: GET [aml/system/configurationChanges/report](#)

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of configuration changes.

URI	<i>aml/system/configurationChanges/report</i>
Method	GET
User Role Access	Admin, Service, User
Version	240(i3/i6/i6H)
Parameters	<p>The following query parameters are supported, start, length, period, date, save with the following values:</p> <ul style="list-style-type: none">• start=0-n• length=1-n, anything else means all records.• period=1-n, the last number of days to include in the report. If you want to report for the last week, you would specify 7.• date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored.• save=”name” where name is a file name to use to save the file in CSV format. The save=”name” query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default “name” is provided if none is specified. <p>If no query parameters are used, the request will return all configuration change data.</p>
Request Header	N/A

Request Data	N/A
Response Codes	200
Response Header	Content-Type: text/plain or application/octet-stream On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 22: configurationChangeList or octet-stream or text

Table 303: POST [aml/system/configurationChanges/report/email](#)

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of library configuration change records.

The information will be in an email attachment and the file format will be CSV.

<i>URI</i>	<i>aml/system/configurationChanges/report/email</i>
Method	POST
User Role Access	Admin
Version	240(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 304: GET [aml/system/dateTime](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the date and time resource. This reports the time on the library with time zone included.

<i>URI</i>	<i>aml/system/dateTime</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 29: dateTime

Table 305: PUT [aml/system/dateTime](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the current date time resource on the library. The example XML object below shows the request body data used to update the time. To discover the available time zones, see Table 309: GET [aml/system/dateTime/timeZoneIDs](#).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:dateTime xmlns:ns2="http://automatedMediaLibrary/">
  <date>2013-05-22</date>
  <time>13:56:15</time>
  <timezone>American/Denver</timezone>
</ns2:dateTime>
```

URI	<i>aml/system/dateTime</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 29: dateTime
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 29: dateTime

Table 306: POST *aml/system/dateTime/clientDateTime*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Notify the server of your (requesting client) date and time. This interface can be used so as to help Quantum service in debugging issues.

URI	<i>aml/system/dateTime/clientDateTime</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000), 200(i3/i6/i6H)
Parameters	Required query parameter is DT, with the following valid values: <ul style="list-style-type: none"> DT="date/time" - Human readable date string that should include year, month, day, hour, minute and second, as in 2018-09-28 09:15:10
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	Figure 225: WSResultCode

Table 307: GET *aml/system/dateTime/ntp*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Retrieve the Network Time Protocol (NTP) resource which is used to synchronize the library's internal clock with one or more NTP servers.

URI	<i>aml/system/dateTime/ntp</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 157: NTP

Table 308: PUT aml/system/dateTime/ntp

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Update the NTP resource. To disable NTP send an empty NTP object, with no server defined.

URI	aml/system/dateTime/ntp
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 157: NTP
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 157: NTP

Table 309: GET aml/system/dateTime/timeZoneIDs

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve the available list of time zone IDs. When setting the time zone use the string value reported between the values reported in parentheses. For example, from the response data below: "<ID>(GMT+13:00) MIT (WSDT)</ID>" use "MIT".

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:timeZoneIDs xmlns:ns2="http://automatedMediaLibrary/">
  <ID>(GMT-12:00) Etc/GMT+12 (GMT-12:00)</ID>
  <ID>(GMT-11:00) Etc/GMT+11 (GMT-11:00)</ID>
  <ID>(GMT+13:00) MIT (WSDT)</ID>
  <ID>(GMT+13:00) Pacific/Apia (WSDT)</ID>
  <ID>(GMT-11:00) Pacific/Midway (SDT)</ID>
  <ID>(GMT-11:00) Pacific/Niue (NUST)</ID>
  <ID>(GMT-11:00) Pacific/Pago_Pago (SDT)</ID>
  <ID>(GMT-11:00) Pacific/Samoa (SDT)</ID>
  <ID>(GMT-11:00) US/Samoa (SDT)</ID>
  <ID>(GMT-10:00) America/Adak (HADT)</ID>
  .....
</ns2:timeZoneIDs>
```

URI	aml/system/dateTime/timeZoneIDs
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 212: timeZoneIDs

Table 310: GET aml/system/ekm/communicationCertificates

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of communicationCertificate resources installed on the library.

URI	aml/system/ekm/communicationCertificates
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 19: communicationCertificateList

Table 311: POST aml/system/ekm/communicationCertificates

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Install the communication certificates to be used between the library and the EKM servers. The following form data key value pairs are required:

For all server types, the key “type” is required:

type=qekm, tklm, skm, or kmip.

Note: Q-EKM and IBM TKLM/SKLM EKM solutions with the IBM Proprietary Protocol (IPP) interface are only supported by the Scalar i6000 with IBM drives. The IBM SKLM EKM solution may also be configured for KMIP communication.

QEKM or TKLM

root=The root certificate file

SKM

quantum=The Quantum certificate bundle file

Or the following

root= The root certificate file

admin=The admin certificate file

adminpassword=The admin password

client=The client certificate file

clientpassword=The client password

KMIP

root= The root certificate file

client=The client certificate file

clientpassword=The client password

Note: For type KMIP, the 'IBM SKLM' key server solution is supported as of firmware release 770(i6000).

URI	aml/system/ekm/communicationCertificates
Method	POST

User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: multipart/form-data
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 312: GET aml/system/ekm/logs - deprecated

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Retrieve the SKM server logs.

Note: This interface has been deprecated. The logs should be retrieved from the SKM server log capture functionality.

URI	<i>aml/system/ekm/logs</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	Query parameter names are type and save with the following valid values: <ul style="list-style-type: none"> • save=the default name you want the browser to save the contents of the file. If no name is specified, a default name will be supplied by the Web Server. The purpose of the save parameter is to tell the Web Browser that this is an attachment. If the client is not a Web Browser then the 'Accept: application/octet-stream' can be used to retrieve the file data. • type=0(Primary), 1(secondary) and 2(Import Warning) If no type is specified, then 0 is the default.
Request Header	Accept: application/octet-stream (download the file content)
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/octet-stream, application/xml or application/json Content-Disposition: attachment; filename="the name of the file" (This will only happen if the save query parameter is requested) Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	The file content, it is in tgz format.

Table 313: GET aml/system/ekm/reports/audit/mediaStatus

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of EKM media statistics resources.

URI	<i>aml/system/ekm/reports/audit/mediaStatus</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameter is start, length, period, date, partition and save, with the following valid values: <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • partition=The partition name. • save=”name” where name is a file name to use to save the file in CSV format. The save=”name” query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default “name” is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/xml or application/json On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 57: ekmMediaStatusList

Table 314: POST *aml/system/ekm/reports/audit/mediaStatus/email*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of media encryption status records. The information will be in an email attachment and the file format will be CSV.

The reportCriteria object supports the same query parameters as Table 313: GET *aml/system/ekm/reports/audit/mediaStatus*.

URI	<i>aml/system/ekm/reports/audit/mediaStatus/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 315: GET [aml/system/ekm/reports/audit/partitionActivity](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve the list of EKM partition activity resources.

The EKM (Encryption Key Management) Report provides partition encryption method summaries, providing historic information as to when a library partition was enabled or disabled for library managed encryption.

URI	<i>aml/system/ekm/reports/audit/partitionActivity</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none">• start=0-n• length=1-n, anything else means all records.• period=1-n, the last number of days to include in the report. If you want to report for the last month, you would specify 30.• partition=The partition name• save="name" where name is a file name to use to save the file in CSV format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/xml or application/json On success Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 59: ekmPartitionActivityList

Table 316: POST [aml/system/ekm/reports/audit/partitionActivity/email](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Email the list of partition encryption activity records.

The information will be in an email attachment and the file format will be CSV.

The reportCriteria object supports the same query parameters as Table 315: GET [aml/system/ekm/reports/audit/partitionActivity](#).

URI	<i>aml/system/ekm/reports/audit/partitionActivity/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json

Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 317: GET aml/system/ekm/servers

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of EKM server resources. These resources report all configured EKM server configured on the library. These servers are used to manage the encryption keys that are used to encrypt/decrypt the data read and written to media in the library.

Note: The list of servers will be returned in the order that was used to configure the servers.

URI	aml/system/ekm/servers
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 61: ekmServersList

Table 318: POST aml/system/ekm/servers

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Configure new EKM server resources.

Note: The order servers are received in the data object is the order in which the servers will be added. The Request data will be a little different depending on the EKM server types requested, see the following examples for details:

QEKM and TKLM

```
<ns2:ekmServers xmlns:ns2="http://automatedMediaLibrary/">
  <ekmServerType>8</ekmServerType>
  <server>
    <hostName>192.168.10.80</hostName>
    <port>3801</port>
  </server>
  <ssl>>false</ssl>
</ns2:ekmServers>
```

The ekmServerType must be 8 for QEKM and 32 for TKLM. You must provide at least one server and a maximum of two servers. If Transport Layer Security (TLS) is required between the library and the server, set ssl to true.

SKM

```
<ns2:ekmServers xmlns:ns2="http://automatedMediaLibrary/">
```



```

<ekmServerType>16</ekmServerType>
<server>
  <hostName>192.168.20.100</hostName>
</server>
<server>
  <hostName>192.168.20.101</hostName>
</server>
</ns2:ekmServers>

```

The ekmServerType must be set to 16. You are required to configure two servers. No port number is required since it is hard coded to 6000.

KMIP

```

<ns2:ekmServers xmlns:ns2="http://automatedMediaLibrary/">
  <ekmServerType>4</ekmServerType>
  <server>
    <hostName>10.20.169.146</hostName>
    <port>5696</port>
  </server>
  <server>
    <hostName>10.20.169.147</hostName>
    <port>5696</port>
  </server>
</ns2:ekmServers>

```

The ekmServerType must be set to 4. You must have at least one server but no more than 10 servers configured.

IBM SKLM

```

<ns2:ekmServers xmlns:ns2="http://automatedMediaLibrary/">
  <ekmServerType>2048</ekmServerType>
  <server>
    <hostName>10.20.169.146</hostName>
    <port>5696</port>
  </server>
  <server>
    <hostName>10.20.169.147</hostName>
    <port>5696</port>
  </server>
</ns2:ekmServers>

```

The ekmServerType must be set to 2048. You must have at least one server but no more than 10 servers configured. Added in 770(i6000).

You cannot configure a server type if it is already configured as each server type configuration request must be unique.

The ekmServers.ekmPathDiagnosticsInterval element determines if the path diagnostics test will be run and at what interval. The options are 0-60 minutes, where 0 means do not run these tests.

URI	<i>aml/system/ekm/servers</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 62: ekmServers

Response Codes	201, 403, 404, 412
Response Header	Content-Type:application/xml or application/json Location: aml/system/ekm/servers
Response Data	See Figure 225: WSResultCode

Table 319: GET aml/system/ekm/servers/{type}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the EKM servers with the type identified by the URI path template “type”. The type must be the server type to retrieve, see Figure 62: ekmServers, specifically the ekmServerType field.

URI	aml/system/ekm/servers/{type}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 62: ekmServers

Table 320: PUT aml/system/ekm/servers/{type}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Update the EKM servers with the type identified by the URI path template “type”. The type must be the server type you want to update (see Figure 62: ekmServers, the ekmServerType field).

All servers must be supplied in the request data, as this interface reconfigures the EKM servers for a given server type.

Note: The order in which servers are received in the data object determines the order these servers will be added. Servers are contacted and utilized in the order they are configured.

URI	aml/system/ekm/servers/{type}
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 62: ekmServers
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 62: ekmServers

Table 321: DELETE aml/system/ekm/servers/{type}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the EKM servers with the type identified by the URI path template “type”. The type must be the server type you want to delete, see Figure 62: ekmServers, the ekmServerType field.

Note: You cannot delete a server type if it is currently being used by a partition.

If you delete the servers then any media that was written using keys from the servers, can no longer be read.

URI	aml/system/ekm/servers/{type}
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 322: POST aml/system/ekm/servers/{type}/test

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: EKM (i6000), EKM and/or SKM (i3/i6/i6H)

Response Time: Minimum <= 30 seconds; Maximum = 180 seconds

Description: Test the EKM servers with the type identified by the URI path template “type”.

URI	aml/system/ekm/servers/{type}/test
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 63: ekmServerTestResultList

Table 323: GET aml/system/emmc

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current eMMC wear level status.

URI	aml/system/emmc
Method	GET
User Role Access	Admin, Service, User

Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 72: emmc

Table 324: GET aml/system/file

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a file from the library. Access is granted only to the '/var/log' and '/tmp' directories.

<i>URI</i>	<i>aml/system/file</i>
Method	GET
User Role Access	Admin, Service
Version	735(i6000), 110(i3/i6/i6H)
Parameters	Query parameters are name and type with the following valid values: <ul style="list-style-type: none"> name=The name of the file you want to retrieve. You must specify the full path of the file you want to retrieve type="binary" or "text" Note: You must specify the 'name' and 'type' query parameters.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: text/plain or application/octet-stream
Response Data	The requested file

Table 325: GET aml/system/licenses

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve all license resources. The request response will report all license features supported by the library, including features that have been installed and those that have not been installed.

<i>URI</i>	<i>aml/system/licenses</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 125: licenseList

Table 326: POST aml/system/licenses

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Add and enable a new licensable feature to the library. The object reported in the request data below should have a valid license key in the “feature” element of the “license” object.

URI	<i>aml/system/licenses</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 126: license
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 125: licenseList

Table 327: GET aml/system/network

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 60 seconds

Description: Retrieve the network resource information.

URI	<i>aml/system/network</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 149: network

Table 328: GET aml/system/network/access/certificate

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the Web Server communication certificate installed on the library.

URI	<i>aml/system/network/access/certificate</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 20: communicationCertificate

Table 329: POST aml/system/network/access/certificate

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Upload the signed certificate that was generated using Table 332: POST aml/system/network/access/certificate/csr.

The multipart form data key is 'file' and the value is the file to be uploaded.

After uploading the signed certificate, you will need to activate it (the library web server will start using it). See Table 331: POST aml/system/network/access/certificate/activate.

URI	aml/system/network/access/certificate
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type multipart/formdata
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 330: GET aml/system/network/access/certificate/activate

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Determine if an uploaded, signed certificate on the library has been activated.

URI	aml/system/network/access/certificate/activate
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:test/plain or application/json
Response Data	"true" or "false"

Table 331: POST aml/system/network/access/certificate/activate

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Activate the signed certificate uploaded to the library using Table 329: POST aml/system/network/access/certificate. The Web Server will start to use this certificate to authenticate communications with the Web Browser client. The Web Browser will need to be refreshed after the request completes successfully.

URI	aml/system/network/access/certificate/activate
Method	POST
User Role Access	Admin, Service

Version	700(i6000), Updated in 760(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 332: POST [aml/system/network/access/certificate/csr](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Generate a Certificate Signing Request (CSR) to be signed by a Certificate Authority. Once signed the CA Certificate can then be uploaded to the library.

The communicationCertificate fields that are required for generating the CSR are *keySize*, *digestAlgorithm* and *subject* (certificateInformation object). The required certificateInformation fields are *commonName*.

The maximum allowed characters for countryCode is 2. All other fields have a maximum length of 128 characters.

URI	aml/system/network/access/certificate/csr
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none"> save="name" where name is a file name to use to save the file in CSV format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default name of library.csr is provided if none is specified.
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 20: communicationCertificate
Response Codes	200, 403
Response Header	Content-Type:application/octet-stream On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Byte Stream

Table 333: GET [aml/system/network/access/certificate/isSigned](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Determine if the management communication certificate installed on the library was signed by a certificate authority.

URI	aml/system/network/access/certificate/isSigned
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A

Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	"true" or "false"

Table 334: GET aml/system/network/interfaces

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Retrieve the main controller network interface resources, eth0 and eth2.

URI	aml/system/network/interfaces
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 153: netInterfaceList

Table 335: GET aml/system/network/interface/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Request the network interface identified by the URI path template "name".

Example response for a request to the interface with name "eth0":

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netInterface xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <macAddress>00:30:8C:06:78:B5</macAddress>
  <location>N/A</location>
  <duplexMode>Full</duplexMode>
  <autoNegotiate>>false</autoNegotiate>
  <speed>1</speed>
  <linkStatus>1</linkStatus>
</ns2:netInterface>
```

URI	aml/system/network/interface/{name}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 154: netInterface

Table 336: PUT aml/system/network/interface/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 60 seconds

Description: Update the network interface identified by the URI path template “name”.

The client request data below indicates that the interface speed should be changed to 1 (10Mb/s).

To revert to auto negotiation set autoNegotiate element to true and remove the speed element. To set a specific speed (1,2 or 3) the autoNegotiate element must be set to false.

Note: The i6000 only supports setting the *speed* or *autoNegotiate* elements.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netInterface xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <autoNegotiate>>false</autoNegotiate>
  <speed>1</speed>
</ns2:netInterface>
```

URI	aml/system/network/interface/{name}
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 154: netInterface
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 154: netInterface

Table 337: GET aml/system/network/configurations

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 60 seconds

Description: Retrieve the network configurations for all the configured interfaces, eth0 and eth2, on the library.

URI	aml/system/network/configurations
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 151: netConfigurationList

Table 338: GET aml/system/network/configuration/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 60 seconds

Description: Retrieve the network parameters for the interface identified by the URI path template “name”.

An example XML response for interface with name “eth0” is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netConfigurationList xmlns:ns2="http://automatedMediaLibrary/">
  <netConfiguration>
    <name>eth0</name>
    <location>N/A</location>
    <version>1</version>
    <hostName>dvt8-jb</hostName>
    <domainName>dvt8-jb</domainName>
    <type>1</type>
    <netMask>64</netMask>
    <netGateway>10.20.168.1</netGateway>
    <ipAddress>10.20.171.17</ipAddress>
  </netConfiguration>
  <netConfiguration>
    <name>eth0</name>
    <location>N/A</location>
    <version>2</version>
    <hostName>dvt8-jb</hostName>
    <domainName>dvt8-jb</domainName>
    <type>3</type>
    <netGateway>0:0:0:0:0:0:0:0</netGateway>
    <ipAddress>2001:db8:fff:1:230:8cff:fe06:78b5/64</ipAddress>
    <ipAddress>fe80::230:8cff:fe06:78b5/64</ipAddress>
  </netConfiguration>
</ns2:netConfigurationList>
```

URI	<i>aml/system/network/configuration/{name}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 151: netConfigurationList

Table 339: PUT *aml/system/network/configuration/{name}/{version}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 30 seconds; Maximum = 120 seconds

Description: Update the network parameters identified by the URI path templates “name” and “version”.

The “version” template values are as follows: 1 (IPv4) and 2 (IPv6).

See the IPv4 examples below for more information:

Example 1: Update the hostname to “TestLibrary” using the IPv4 parameters version. The name, version (1-IPv4) and hostName elements must be specified.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <version>1</version>
  <hostName>TestLibrary</hostName>
</ns2:netConfiguration>
```

Example 2: Set DHCP for IPv4 on eth0. After sending this request, your session will no longer be valid and you will be disconnected from the library.

```
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <version>1</version>
  <type>2</type>
</ns2:netConfiguration>
```

Example 3: Set a new Static IPv4 address on eth0. After sending this request, your session will no longer be valid and you will be disconnected from the library.

```
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <version>1</version>
  <hostName>dvt8-jb</hostName>
  <type>1</type>
  <ipAddress>10.20.171.17</ipAddress>
</ns2:netConfiguration>
```

See the IPv6 examples below for more information:

Example 4: Set a new Static IPv6 address on interface eth0 where DHCP6 is disabled. If the current IPv6 or DHCP6 address was used to connect to the library, you will be disconnected from the library.

Note: When configuring a static IPv6 address on interface eth2, you do not need to supply a netGateway element. The gateway is not required.

```
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <version>2</version>
  <type>1</type>
  <netMask>64</netMask>
  <netGateway>fd80::</netGateway>
  <ipAddress>fd80::ffaa:abcd</ipAddress>
</ns2:netConfiguration>
```

Example 5: Set DHCP6 on eth2, with no static address, type element = 3.

```
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth2</name>
  <version>2</version>
  <type>3</type>
</ns2:netConfiguration>
```

Example 6: Configure both Static address and DHCP6 for interface eth0. Note the type element is 4 (Static and DHCP).

```
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <version>2</version>
  <type>4</type>
  <netMask>64</netMask>
  <netGateway>20FF::</netGateway>
```

```
<ipAddress>20FF::ffaa:abcd</ipAddress>
</ns2:netConfiguration>
```

Example 7: Configure new host name for interface eth2 using IPv6. When you configure a new hostname, you must supply the current configuration, static and or DHCP6 setting. Otherwise they will get removed.

```
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth2</name>
  <version>2</version>
  <hostName>TestLibrary-eth2</hostName>
  <type>4</type>
  <netMask>64</netMask>
  <netGateway>20FF:::</netGateway>
  <ipAddress>20FF::ffaa:abcd</ipAddress>
</ns2:netConfiguration>
```

URI	<i>aml/system/network/configuration/{name}/{version}</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 152: netConfiguration
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 152: netConfiguration

Table 340: GET *aml/system/network/dns*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve the Domain Name Servers (DNS) resource. This resource contains the IP address of the Domain Name Server configured on the library. These servers are used to resolve domain names to IP addresses.

URI	<i>aml/system/network/dns</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 31: DNS

Table 341: PUT *aml/system/network/dns*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Update the current DNS IP address configuration. To disable DNS just pass down an empty DNS object.

URI	<i>aml/system/network/dns</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 31: DNS
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 31: DNS

Table 342: GET *aml/system/network/emailServer*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the email server configuration resource.

URI	<i>aml/system/network/emailServer</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 69: emailServer

Table 343: PUT *aml/system/network/emailServer*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the current email server configuration.

TLS support was added to Scalar i3/i6/i6H in version 210. The server port is optional and may be configured to use values 1-65535. Once set, the server port may be reset to use the default port by using a null, empty or 0 value. TLS is optional and is disabled by default.

Example 1: Change the IP address of the email server. The required elements are server and senderEmailAddress. If authorization is turned on, the authorize element is set to true the accountName and accountPassword are required. Otherwise authorization will be turned off as in the following example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:emailServer xmlns:ns2="http://automatedMediaLibrary/">
  <server>10.20.169.9</server>
  <senderEmailAddress>john.doe@company.com</senderEmailAddress>
</ns2:emailServer>
```

Example 2: Disabling the server prevents the library from sending email notifications and other email features. When the email server is disabled the email server information that was persisted on the library will be deleted.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<ns2:emailServer xmlns:ns2="http://automatedMediaLibrary/">
</ns2:emailServer>
```

URI	<i>aml/system/network/emailServer</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 69: emailServer
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 69: emailServer

Table 344: GET aml/system/network/internal

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve the internal network resource. This resource provides information on the currently configured network address of the library's internal network. It also provides the network address options that are available if a conflict exists between the internal and external network to which the library is connected.

URI	<i>aml/system/network/internal</i>
Method	GET
User Role Access	Admin, Service, User
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 109: internalNetwork

Table 345: PUT aml/system/network/internal

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Update the internal network resource. This should only be used if there is a conflict between the library's internal network and the network to which the library is connected. The current element of the internalNetwork object is used to change the internal network. You must use one of the network address options provided by the GET method on this interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:internalNetwork xmlns:ns2="http://automatedMediaLibrary/">
  <current>10.247.240.0</current>
</ns2:internalNetwork>
```

Note: Before the changes can take effect, the library will need to be power cycled.

URI	<i>aml/system/network/internal</i>
Method	PUT

User Role Access	Admin, Service
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 109: internalNetwork
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 109: internalNetwork

Table 346: GET aml/system/network/internal/connectivity

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Retrieve the list of internal network device connectivity resources. These resources report information about network connected devices internal to the library.

URI	<i>aml/system/network/internal/connectivity</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	<p>Query parameters and their respective values are as follows:</p> <ul style="list-style-type: none"> save=the default name you want the browser to save the contents of the file too. If no name is specified a default name will be supplied by the Web Server. The file format will be CSV. The data separator has changed from “!” (exclamation point character) to a comma “,” in version 770(i6000). <p>The purpose of the save parameter is to tell the Web Browser that this is an attachment. If the client is not a Web Browser, then the ‘Accept: application/octet-stream’ can be used to retrieve the data.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 155: networkDeviceConnectivityInfoList

Table 347: POST aml/system/network/internal/connectivity/email

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Email the list of internal network device connectivity resources.

URI	<i>aml/system/network/internal/connectivity/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 348: GET aml/system/network/ipv6/mode

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the IPv6 current mode (enabled/disabled).

A single string value will be returned and the possible values are:

- 1 (enabled), or
- 2 (disabled)

Note: This interface has been deprecated, IPv6 is always enabled.

URI	aml/system/network/ipv6/mode
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	Will always return "1", enabled.

Table 349: PUT aml/system/network/ipv6/mode

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change IPv6 mode, 1 (enable) or 2 (disable).

Note: This interface has been deprecated, you can no longer disable IPv6.

URI	aml/system/network/ipv6/mode
Method	PUT
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1 or 2
Response Codes	410
Response Header	Content-Type:text/plain or application/json
Response Data	See Figure 225: WSResultCode

Table 350: POST aml/system/network/emailServer/test

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Verify validity of email server configuration. The required elements are shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:emailServer xmlns:ns2="http://automatedMediaLibrary/">
  <server>10.20.169.9</server>
```



```

<senderEmailAddress>admin@quantum.com</senderEmailAddress>
<testEmailAddress>john.doe@company.com</testEmailAddress>
</ns2:emailServer>

```

URI	<i>aml/system/network/emailServer/test</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 69: emailServer
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 351: GET *aml/system/network/snmp/MIBs*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the library's SNMP MIB file.

URI	<i>aml/system/network/snmp/MIBs</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none"> save="name" where name is a file name to use to save the file. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/octet-stream On success and when save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Octet stream (ZIP format)

Table 352: POST *aml/system/network/snmp/MIBs/email*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the library's SNMP MIB file(s).

URI	<i>aml/system/network/snmp/MIBs/email</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml, application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412

Response Header	Content-Type: application/xml, application/json
Response Data	See Figure 225: WSResultCode

Table 353: GET aml/system/network/syslogs

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of remote syslog server resources. Currently only one server is supported, so the list will only contain one server.

URI	aml/system/network/syslogs
Method	GET
User Role Access	Admin, Service, User
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 201: sysLogServerList

Table 354: POST aml/system/network/syslogs

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Configure a remote syslog server resource. Currently the interface will only allow the user to configure a single remote server. The following example will configure the library to send configuration change and event messages to a syslog server running on a server with IP address '192.168.1.100' on port 514 using TCP as the transport protocol.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sysLogServerList xmlns:ns2="http://automatedMediaLibrary/">
  <sysLogServer>
    <enabled>true</enabled>
    <name>192.168.1.100</name>
    <port>514</port>
    <transport>1</transport>
  </sysLogServer>
</ns2:sysLogServerList>
```

URI	aml/system/network/syslogs
Method	GET
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 201: sysLogServerList
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: aml/system/network/syslog/{id}
Response Data	See Figure 201: sysLogServerList

Table 355: GET aml/system/network/syslog/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the remote syslog server resource identified by the URI path template “id”.

URI	<i>aml/system/network/syslog/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 202: sysLogServer

Table 356: PUT aml/system/network/syslog/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Update the remote syslog server resource identified by the URI path template “id”. All sysLogServer elements can be updated except for the id element.

URI	<i>aml/system/network/syslog/{id}</i>
Method	PUT
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 202: sysLogServer
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 202: sysLogServer

Table 357: DELETE aml/system/network/syslog/{id}

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Delete the remote syslog server resource identified by the URI path template “id”.

URI	<i>aml/system/network/syslog/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 358: POST aml/system/network/syslog/{id}/test

Product Support: Scalar i6000

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Test the remote syslog server resource identified by the URI path template “id”. This will send a test message to the syslog server.

Note: The test feature is only supported for servers that are configured for TCP connections.

URI	aml/system/network/syslog/{id}/test
Method	POST
User Role Access	Admin, Service
Version	770(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 359: GET aml/system/notifications/contact

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the library contact information resource.

URI	aml/system/notifications/contact
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 25: contactInformation

Table 360: PUT aml/system/notifications/contact

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the contact information resource. If any element of the contactInformation object is not included the resulting value will be an empty string.

URI	aml/system/notifications/contact
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 25: contactInformation

Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 25: contactInformation

Table 361: GET aml/system/notifications/emailRecipients

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of emailRecipients resources. This is a list of e-mail addresses that are stored on the library.

URI	aml/system/notifications/emailRecipients
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 70: emailRecipientList

Table 362: POST aml/system/notifications/emailRecipients

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new emailRecipient resource. The required element is address.

URI	aml/system/notifications/emailRecipients
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json Location: aml/system/notifications/emailRecipients/email address
Request Data	See Figure 71: emailRecipient
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 363: GET aml/system/notifications/emailRecipient/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the emailRecipient resource identified by the URI path template “id”. The id can be either the object id or address.

URI	aml/system/notifications/emailRecipient/{id}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)

Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 71: emailRecipient

Table 364: DELETE [aml/system/notifications/emailRecipient/{id}](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the emailRecipient resource identified by the URI path template “id”. The id can be either the object id or address.

URI	<i>aml/system/notifications/emailRecipient/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 365: GET [aml/system/notifications/heartbeat](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the heartbeatNotification resource. If the heartbeat notification has not been configured, a null object is returned.

URI	<i>aml/system/notifications/heartbeat</i>
Method	GET
User Role Access	Admin, Service, User
Version	785 (i6k)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 103: heartbeatNotification Error! Reference source not found.

Table 366: PUT [aml/system/notifications/heartbeat](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the heartbeat notification by providing a list of email recipients, and an interval. Once configured, to update the notifications list, the entire list of recipients must be

included in the request data. To disable the notifications, set the interval to 0.

Note: The following data is contained in the notification email.

Library Heartbeat
 Library Name: Sales
 Library IPv4 Address: 10.10.0.100
 Library Serial Number: 2U31000001
 Heartbeat Interval: 60 minutes
 RAS Status:
 Connectivity : Good
 Control : Failed
 Media : Good
 Drives : Failed
 Power : Good
 Robotics : Good
 Library State: Online/Ready
 Date: Fri Nov 07 20:36:08 GMT 2014

URI	<i>aml/system/notifications/heartbeat</i>
Method	PUT
User Role Access	Admin, Service
Version	785 (i6k)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 103: heartbeatNotification
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 103: heartbeatNotification

Table 367: GET *aml/system/notifications/mediaSecurity*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the media security policy resource.

URI	<i>aml/system/notifications/mediaSecurity</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 138: mediaSecurityPolicy

Table 368: PUT *aml/system/notifications/mediaSecurity*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the media security policy resource. You can configure the library to automatically notify you via a RAS ticket when media is moved in or out of the library, either intentionally or unintentionally. First, you must choose under which circumstances you wish to be notified, and then you must enable automatic inventory on the library.

URI	<i>aml/system/notifications/mediaSecurity</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 138: mediaSecurityPolicy
Response Header	Content-Type: application/xml or application/json
Response Codes	200, 403, 404
Response Data	See Figure 138: mediaSecurityPolicy

Table 369: GET *aml/system/notifications/reports*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of reportNotification resources. These report notifications are scheduled to be e-mailed to recipients on a periodic basis.

URI	<i>aml/system/notifications/reports</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 183: reportNotificationList

Table 370: POST *aml/system/notifications/reports*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new report notification resource. The required reportNotification object elements are:

- emailAddress – The e-mail address of the recipient you want this report to be sent to.
- reportTemplateName – A valid reportTemplate name. The available templates can be found at the following URI: Table 410: GET *aml/system/reports/templates*.
- interval – See Figure 184: reportNotification.

If not specified, the enable element will default to false.

URI	<i>aml/system/notifications/reports</i>
Method	POST

User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json Location: aml/system/notifications/report/{id}
Request Data	See Figure 184: reportNotification
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 371: GET aml/system/notifications/report/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the reportNotification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/report/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 184: reportNotification

Table 372: PUT aml/system/notifications/report/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Advanced Reporting

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Modify the reportNotification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/report/{id}</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 184: reportNotification
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 184: reportNotification

Table 373: DELETE aml/system/notifications/report/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the reportNotification identified by the URI path template “id”.

URI	<i>aml/system/notifications/report/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 374: GET *aml/system/notifications/snmpTraps*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of snmp trap notification resources.

URI	<i>aml/system/notifications/snmpTraps</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 206: trapNotificationList

Table 375: POST *aml/system/notifications/snmpTraps*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new trapNotification resource. The required fields are host and port.

URI	<i>aml/system/notifications/snmpTraps</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 207: trapNotification
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: <i>aml/system/notifications/snmpTrap/{id}</i>
Response Data	See Figure 225: WSResultCode

Table 376: POST *aml/system/notifications/snmpTraps/test*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 30 seconds

Description: Send a trap notification to a specific IP/host. All elements of the trapNotification object are required except for the id element.

URI	<i>aml/system/notifications/snmpTraps/test</i>
Method	POST
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 207: trapNotification
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 377: GET *aml/system/notifications/snmpTrap/{id}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the snmp trap notification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/snmpTrap/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 207: trapNotification

Table 378: PUT *aml/system/notifications/snmpTrap/{id}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the snmp trap notification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/snmpTrap/{id}</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 207: trapNotification
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 207: trapNotification

Table 379: DELETE *aml/system/notifications/snmpTrap/{id}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the snmp trap notification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/snmpTrap/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 380: GET aml/system/notifications/telemetrics

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 60 seconds; Maximum = 600 seconds

Description: Retrieve a list of telemetric notification resources. Telemetric notifications include library usage metrics and performance data, which may be configured to be sent to either the predefined system telemetric E-Mail address or to the Auto Support cloud. To enable or disable such notifications, or to change the interval at which they are sent, see Table 382: PUT aml/system/notifications/telemetric/{receiver}.

URI	<i>aml/system/notifications/telemetrics</i>
Method	GET
User Role Access	Admin, Service, User
Version	775(i6000), 210(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 204: telemetricNotificationList

Table 381: GET aml/system/notifications/telemetric/{receiver}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of telemetric notification resources. Telemetric notifications include library usage metrics and performance data, which may be configured to be sent to either the predefined system telemetric E-Mail address or a cloud interface. To enable or disable such notifications, or to change the interval at which they are sent, see Table 382: PUT aml/system/notifications/telemetric/{receiver}.

URI	<i>aml/system/notifications/telemetric/{receiver}</i>
Method	GET
User Role Access	Admin, Service, User
Version	775(i6000), 210(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A

Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 205: telemetricNotification

Table 382: PUT aml/system/notifications/telemetric/{receiver}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Modify the telemetric resource whose receiver type is included in the URI. Telemetric notifications may be configured to be sent to Quantum via the cloud interface receiver (1) or the predefined system telemetric E-Mail address (2).

URI	aml/system/notifications/telemetric/{receiver}
Method	PUT
User Role Access	Admin, Service
Version	775(i6000), 210(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 205: telemetricNotification
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 205: telemetricNotification

Table 383: GET aml/system/notifications/tickets

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of RAS notification resources. These RAS notifications are e-mailed to recipients when a RAS ticket is opened. Tickets may be filtered by severity.

URI	aml/ system/notifications/tickets
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 178: rasNotificationList

Table 384: POST aml/system/notifications/tickets

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new RAS notification resource. The required rasNotification object elements are:

- *emailAddress* – e-mail address to receive the notification.
- *enabled* – set to true, otherwise the notification will not be sent.
- *severity1 ... severity5* – Severities set to true will receive email notifications.

URI	<i>aml/system/notifications/tickets</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 179: rasNotification
Response Codes	201, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 385: GET *aml/system/notifications/ticket/{id}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the RAS notification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/ticket/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 179: rasNotification

Table 386: PUT *aml/system/notifications/ticket/{id}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Modify the RAS notification resource identified by the URI path template “id”.

URI	<i>aml/system/notifications/ticket/{id}</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 179: rasNotification
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 179: rasNotification

Table 387: DELETE *aml/system/notifications/ticket/{id}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the RAS notification identified by the URI path template “id”.

URI	<i>aml/system/notifications/ticket/{id}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 388: GET *aml/system/notifications/tickets/filters*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of ticket filter resources.

URI	<i>aml/system/notifications/tickets/filters</i>
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	Optional query parameter is group, with the following valid values: <ul style="list-style-type: none"> group = 1(Connectivity), 2(Control), 3(Media), 4(Drives), 5(Power) and 6(Robotics)
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 210: ticketFilterList

Table 389: PUT *aml/system/notifications/tickets/filters*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the ticket filter resources. The library provides RAS ticket notifications whenever a problem occurs. The library also provides e-mail notifications which can be configured using the following interface, Table 384: POST *aml/system/notifications/tickets*. This interface allows the suppression of these notifications and ticket generation. The interface requires a list of ticketFilter objects. The only required elements of the ticketFilter object are id and suppressOption. The suppressOption are as follows:

- 0) None, no suppression of ticket.
- 1) Tech Support E-mail - No e-mail notification will be sent to Technical support for the ticket.
- 2) E-mail - No e-mail will be sent to anyone for the ticket.
- 3) Ticket - The RAS ticket will not be generated and no e-mail will be sent.

URI	<i>aml/system/notifications/tickets/filters</i>
Method	PUT
User Role Access	Admin, Service
Version	760(i6000)
Parameters	N/A

Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 210: ticketFilterList
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 210: ticketFilterList

Table 390: POST [aml/system/operations/reboot](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Reboot the library.

<i>URI</i>	<i>aml/system/operations/reboot</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 391: POST [aml/system/operations/shutdown](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 10 seconds; Maximum = 120 seconds

Description: Shutdown the library. After the library has shut down, you will need to physically power off the library by using the power button on the library's Control Module.

<i>URI</i>	<i>aml/system/operations/shutdown</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 392: GET [aml/system/policy/externalApplicationServers](#)

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of externalApplicationServers resources. These servers can be used when configuring Extended Data Life Management (EDLM) and Active Vault policies. If StorNext Storage Manager is managing your partition, you can configure a policy to use StorNext with Active Vault and/or EDLM. This feature requires an external application interface to be configured for application access.

URI	<i>aml/system/policy/externalApplicationServers</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 81: externalApplicationServersList

Table 393: POST *aml/system/policy/externalApplicationServers*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Configure new external application (StorNext) servers. The following externalApplicationServers elements are required:

- name: the name value must be unique.
- server: at least one server element is required, and both name and port elements of the server are required. The externalApplicationName is required if you are not using the StorNext Web Services interface. It must point to a configured externalApplication plugin, which the library will use to communicate with the external servers.

If you are using the StorNext Web Services interface, you must provide a 'username' and 'password'. The username and password can be found on the StorNext server. For configured externalApplications, see Table 431: GET *aml/system/software/externalApplications*.

URI	<i>aml/system/policy/externalApplicationServers</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 82: externalApplicationServers
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: <i>aml/system/externalApplicationServers/{name}</i>
Response Data	See Figure 225: WSResultCode

Table 394: GET *aml/system/policy/externalApplicationServer/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the externalApplicationServers resource identified by the URI path template "name".

URI	<i>aml/system/policy/externalApplicationServer/{name}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A

Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 82: externalApplicationServers

Table 395: PUT aml/system/policy/externalApplicationServer/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Modify the externalApplicationServers identified by the URI path template “name”.

The example below will change the name of the externalApplicationServers from EDLMservers to StorNext and reconfigure the policy to use server 10.20.169.88 only using the following URI: “aml/system/policy/externalApplicationServer/EDLMservers”

```
<ns2:externalApplicationServers xmlns:ns2="http://automatedMediaLibrary/">
  <name>StorNext</name>
  <server>
    <name>10.20.169.88</name>
    <port>61776</port>
  </server>
</ns2:externalApplicationServers>
```

If you just want to change the name, then just specify the name

```
<ns2:externalApplicationServers xmlns:ns2="http://automatedMediaLibrary/">
  <name>StorNext5.0</name>
</ns2:externalApplicationServers>
```

If you just want to change the external application name plugin

```
<ns2:externalApplicationServers xmlns:ns2="http://automatedMediaLibrary/">
  externalApplicationName>snapi-2.0.1</externalApplicationName>
</ns2:externalApplicationServers>
```

You can specify any combination of the above.

URI	aml/system/policy/externalApplicationServer/{name}
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 82: externalApplicationServers
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 82: externalApplicationServers

Table 396: DELETE aml/system/policy/externalApplicationServer/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the externalApplicationServers resource identified by the URI path template “name”.

URI	<i>aml/system/policy/externalApplicationServer/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i6/i6H), 230(i3)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 397: POST *aml/system/policy/externalApplicationServer/{name}/test*

Product Support: Scalar i6000, Scalar i6/i6H , Scalar i3

Response Time: Minimum <= 10 seconds; Maximum = 180 seconds

Description: Test the external applications servers configured on the library with the configuration name identified by the URI path template “name”. Tests will include a ping test to determine if each server is reachable over the network and a configuration path test to determine if the server is available for Web Service requests from the library.

URI	<i>aml/system/policy/externalApplicationServer/{name}/test</i>
Method	POST
User Role Access	Admin, Service
Version	770(i6000), 210(i6/i6H), 230(i3)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 83: externalApplicationServerTestResultList

Table 398: GET *aml/system/ras*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the supported Reliability, Accessibility and Serviceability (RAS) group status resource list.

URI	<i>aml/system/ras</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 170: RASGroupStatusList

Table 399: GET aml/system/ras/{group}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the RAS group status resource identified by the URI path template “group”.

Note: The Scalar i6000 supports overall Library RAS status reporting by requesting status for group 0.

URI	aml/system/ras/{group}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 171: RASGroupStatus

Table 400: GET aml/system/ras/reports/tickets

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the tickets report resource.

Note: If you are creating a report template for this report, the following elements should be used to map the query parameters, group, status and state:

- reportCriteria.state = state
- reportCriteria.type = group
- reportCriteria.id = status

URI	aml/system/ras/reports/tickets
Method	GET
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	Query parameters are period, date, group, status, state, save <ul style="list-style-type: none">• period=1-n, the last number of days to include in the report. If you want to report for the last week, you would specify 7.• date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored.• group values<ul style="list-style-type: none">255 (All),2 (Connectivity),4 (Control),

	<p>8 (Media), 16 (Drive), 32 (Power), 64 (Robotics) 128 (Library) I3/i6/i6H Only</p> <ul style="list-style-type: none"> • status values 255 (All) 4 (Failed), 8 (Degraded), 16 (Warning) • state values 255 (All), 4 (Opened), 16 (Closed), 32 (Verified) 64 (Suspended) (I3/i6/i6H Only) • save="name" where name is a file name to use to save the ticket information and resolution. The file format will be CSV. The data separator has changed from "!" (exclamation point character) to a comma "," in version 770(i6000). <p>The group, status and state query parameters work like a bit mask, for example if you want to report only tickets belonging to Control and Media you would specify 12 (4+8).</p> <p>The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json, text/plain On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 175: RASTicketList or text

Table 401: POST [aml/system/ras/reports/tickets/email](#)

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the tickets report resource.

Note: If using the reportCriteria element of the email object, the following elements should be used to map the filter parameters, group, status and state:

- reportCriteria.state = state
- reportCriteria.type = group
- reportCriteria.id = status

URI	<i>aml/system/ras/reports/tickets/email</i>
Method	POST
User Role Access	Admin, Service, User
Version	760(i6000)
Parameters	N/A

Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	Figure 225: WSResultCode

Table 402: GET aml/system/ras/tickets

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 180 seconds

Description: Retrieve the ticket summary resource instances using query parameter filters.

To retrieve all drive and control ticket summaries that are currently opened you would specify the following:

“aml/system/ras/tickets?group=20&state=4”

Status queries support bit mask queries for group, status and state values. For example, as shown above, group 20 represents group 4(control) + group 16(drive).

URI	aml/system/ras/tickets
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>Query parameters are group, status, state, serviceUser</p> <ul style="list-style-type: none"> • group values <ul style="list-style-type: none"> 255 (All), 2 (Connectivity), 4 (Control), 8 (Media), 16 (Drive), 32 (Power), 64 (Robotics) 128 (Library) I3/i6/i6H Only • status values <ul style="list-style-type: none"> 255 (All) 4 (Failed), 8 (Degraded), 16 (Warning) • state values <ul style="list-style-type: none"> 255 (All), 4 (Opened), 16 (Closed), 32 (Verified) 64 (Suspended) (I3/i6/i6H Only) • serviceUser values (i6000 only, added in version 751) <ul style="list-style-type: none"> true (report tickets that were opened or updated when the service user was logged in) false (report tickets that were opened or updated when the service user was not logged in) <p>These Query parameters work like a bit mask, for instance if you want find tickets belonging to Control and Media you would specify 12 (4+8).</p>
Request Header	N/A
Request Data	N/A

Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 175: RASTicketList

Table 403: GET aml/system/ras/ticket/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the ticket resource instance identified by the URI path template “id”.

URI	<i>aml/system/ras/ticket/{id}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none"> save="name" where name is a file name to use to save the file in zip format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/xml, application/json or application/octet-stream On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 176: RASTicket

Table 404: PUT aml/system/ras/ticket/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Change the state of the ticket resource instance identified by the URI path template “id”. The state will be changed to Closed. Only tickets that are in an ‘Open’ state can be closed.

URI	<i>aml/system/ras/ticket/{id}</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml or application/json
Response Data	See Figure 176: RASTicket

Table 405: POST aml/system/ras/ticket/{id}/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the ticket information to the recipients contained in the email object.

The email will have an attachment containing the resolution and the body will contain ticket information.

URI	<i>aml/system/ras/ticket/{id}/email</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 404, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 406: GET *aml/system/ras/ticket/{id}/history*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the ticket resource history list of related tickets for the ticket identified by the URI path template "id".

URI	<i>aml/system/ras/ticket/{id}/history</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 175: RASTicketList

Table 407: GET *aml/system/ras/ticket/{id}/reports*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the ticket resource reports list for the ticket identified by the URI path template "id".

URI	<i>aml/system/ras/ticket/{id}/reports</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 174: RASTicketReports

Table 408: GET aml/system/ras/ticket/{id}/resolution

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the RAS ticket resolution information. You can request a byte stream or an html page.

<i>URI</i>	<i>aml/system/ras/ticket/{id}/resolution</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none">• save="name" where name is a file name to use to save the file in HTML format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type: application/octet-stream or text/html On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Byte Stream or text/html

Table 409: GET aml/system/reports

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of supported reports.

<i>URI</i>	<i>aml/system/reports</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 180: reportList

Table 410: GET aml/system/reports/templates

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of report template resource instances. A report template is used to save report filtering data that can be used to create a report using these saved filters.

URI	aml/system/reports/templates
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 185: reportTemplateList

Table 411: POST aml/system/reports/templates

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Create a new reportTemplate resource. When you specify a reportCriteria for the new reportTemplate, the supported reportCriteria options will depend on the report type. You will need to look at the following URIs to see what reportCriteria options are available for each report.

- Table 176: GET aml/media/reports/tapeAlerts
- Table 122: GET aml/drives/reports/utilization
- Table 174: GET aml/media/reports/securityEvents
- Table 168: GET aml/media/reports/crossPartitionMoves
- Table 170: GET aml/media/reports/edlm
- Table 313: GET aml/system/ekm/reports/audit/mediaStatus
- Table 315: GET aml/system/ekm/reports/audit/partitionActivity
- Table 460: GET aml/users/reports/login
- Table 194: GET aml/partitions/reports/utilization
- Table 400: GET aml/system/ras/reports/tickets
- Table 302: GET aml/system/configurationChanges/report

The reportTemplate name can only contain the following characters A-Z a-z 0-9 _ and spaces. The maximum number of characters allowed is 64.

URI	aml/system/reports/templates
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 186: reportTemplate
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: aml/system/reports/templates/{id}
Response Data	See Figure 185: reportTemplateList

Table 412: GET aml/system/reports/template/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the report template resource instance identified by the URI path

template “name”.

URI	<i>aml/system/reports/template/{name}</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 186: reportTemplate

Table 413: PUT *aml/system/reports/template/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update a reportTemplate resource instance with the name identified by the URI path template “name”.

If you are modifying the reportTemplate name you need to specify the current reportTemplate id.

URI	<i>aml/system/reports/template/{name}</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 186: reportTemplate
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 186: reportTemplate

Table 414: DELETE *aml/system/reports/template/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the reportTemplate resource instance identified by the URI path template “name”.

URI	<i>aml/system/reports/template/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 415: GET aml/system/saveRestore

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 60 seconds; Maximum = 180 seconds

Description: Create a restore (library configuration) image. This image will be the payload in the response body. This image can be used to restore the library's configuration information.

URI	aml/system/saveRestore
Method	GET
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Optional query parameters and their respective values are as follows: <ul style="list-style-type: none">save="name" where name is a file name to use to save the file in gzip-ed tar file '.tar.gz' format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type: application/x-tar On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Byte Stream (Compressed tar format)

Table 416: POST aml/system/saveRestore

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 180 seconds; Maximum = 600 seconds

Description: Restore a saved configuration. Upload the configuration file using multipart form data, where the key is 'file' and the value is the file to be uploaded. After the restore is completed the library will reboot.

URI	aml/system/saveRestore
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: multipart/form-data
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml, application/json
Response Data	See Figure 225: WSResultCode

Table 417: GET aml/system/saveRestore/rescue

Product Support: Scalar i6000

Response Time: Minimum <= 120 second; Maximum = 300 seconds

Description: Determine if a rescue image has been created on the library.

URI	<i>aml/system/saveRestore/rescue</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	true or false

Table 418: POST *aml/system/saveRestore/rescue*

Product Support: Scalar i6000

Response Time: Minimum <= 120 seconds; Maximum = 300 seconds

Description: Create a rescue image on the library's file system. This image contains the library's current configuration information.

URI	<i>aml/system/saveRestore/rescue</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type: application/xml, application/json
Response Data	See Figure 225: WSResultCode

Table 419: PUT *aml/system/saveRestore/rescue*

Product Support: Scalar i6000

Response Time: Minimum <= 180 second; Maximum = 300 seconds

Description: Restore a library's configuration using the rescue image. The rescue image allows you to roll back the library's configuration settings to a previous state.

Note: After the operation has completed the library will automatically reboot.

URI	<i>aml/system/saveRestore/rescue</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/xml, application/json
Response Data	See Figure 225: WSResultCode

Table 420: GET *aml/system/saveRestore/revert*

Product Support: Scalar i6000

Response Time: Minimum <= 120 second; Maximum = 300 seconds

Description: Determine if a revert image has been created on the library. The revert image is automatically created and stored locally as the first step of any restore or rescue operation. The purpose of the Revert process is to revert to the last configuration that was used before a restore image was applied. If an incorrect restore image was applied, the Revert feature allows the MCB to revert to its prior configuration.

URI	<i>aml/system/saveRestore/revert</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	true or false

Table 421: PUT aml/system/saveRestore/revert

Product Support: Scalar i6000

Response Time: Minimum <= 120 seconds; Maximum = 300 seconds

Description: Restore a library's configuration using the Revert image.

Note: After the operation has completed the library will automatically reboot.

URI	<i>aml/system/saveRestore/revert</i>
Method	PUT
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 422: GET aml/system/sensor/configurations

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the sensor configuration resources. For each configurable sensor type, a sensorConfiguration object is returned.

Minimum and maximum limits are the defined range for the sensor type. The minimum and maximum values are configurable upper and lower thresholds which are applied when generating event tickets or SNMP traps. Temperature values are in degrees Celsius, humidity values represent a percentage.

URI	<i>aml/system/sensor/configurations</i>
Method	GET

User Role Access	Admin, Service, User
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 196: sensorConfigurationList

Table 423: PUT aml/system/sensor/configurations

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the sensor configuration values. The request data should include a sensorConfiguration object for each sensor type to be updated. Required fields in the object are type, minValue and maxValue.

Note: The range and defaults for each sensor type, defined by minLimit, maxLimit, minDefault and maxDefault, are determined by the library and may not be modified. If specified in the request data, these values are ignored. Temperature values are in degrees Celsius, humidity values represent a percentage.

<i>URI</i>	<i>aml/system/sensor/configurations</i>
Method	PUT
User Role Access	Admin, Service
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 196: sensorConfigurationList
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 196: sensorConfigurationList

Table 424: GET aml/system/sensors

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the sensor resource instances for the library. The sensor list will include cooling, power, temperature, voltage and humidity sensors for Scalar i6000 and power, temperature and humidity sensors for the Scalar i3/i6/i6H.

A configurationType element, added in version 220 (i3/i6/i6H), identifies sensors with user configurable ranges which are applied to event reporting. See Table 422: GET aml/system/sensor/configurations.

Note: The query parameter type="voltage" has been deprecated in Scalar i6000 version 743. The query will return an empty list.

<i>URI</i>	<i>aml/system/sensors</i>
Method	GET
User Role Access	Admin, Service, User

Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameter names are “type” with the following valid values <ul style="list-style-type: none"> type = “cooling” (i6000 only), “temperature”, “voltage” (i6000 only, deprecated), “power” or “humidity”
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 194: sensorList

Table 425: GET aml/system/snapshot

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 120 seconds; Maximum = 2000 seconds

Description: Capture a snapshot of the type specified by the specified query parameter. The snapshot will be returned in the body of the response.

URI	<i>aml/system/snapshot</i>
Method	GET
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameters are type and save where the valid values are as follows: <ul style="list-style-type: none"> type=basic, extended, reduced (i3/i6/i6H only). If no type is requested an extended snapshot will be captured for i6000 and a basic will be captured for i3/i6/i6H. save="name" where name is a file name to use to save the file in zipped TGZ format. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified.
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type: application/gzip, application/xml or application/json On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	Compress tar file (byte stream).

Table 426: POST aml/system/snapshot/email

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 120 seconds; Maximum = 2000 seconds

Description: Email a snapshot file log collection.

The information will be in an email attachment and the file format will be TGZ.

URI	<i>aml/system/snapshot/email</i>
Method	POST

User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	Query parameters are type where the valid values are as follows: <ul style="list-style-type: none"> type=basic, extended or reduced (i3/i6/i6H only). If no type is requested, an extended snapshot will be captured for i6000 and a basic will be captured for i3/i6/i6H.
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 427: GET aml/system/software

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the current library firmware components/distributions and versions saved on the library. The list will contain the currently installed version, component = Current, the previous distribution that was installed, component = Rollback and a distribution that has been uploaded to the library, component = Uploaded. For i6000 libraries, this uploaded component can be installed at any time if the version of this component is greater than the currently installed version.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareList xmlns:ns2="http://automatedMediaLibrary/">
  <lastInstallDate>2014-06-02 09:57:50 -0600</lastInstallDate>
  <firmware>
    <component>Current</component>
    <version>665H.TS07401</version>
  </firmware>
  <firmware>
    <component>Rollback</component>
    <version>665H.TS06701</version>
  </firmware>
  <firmware>
    <component>Uploaded</component>
    <version></version>
  </firmware>
</ns2:firmwareList>
```

URI	aml/system/software
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 95: firmwareList

Table 428: POST aml/system/software

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 60 seconds; Maximum = 1200 seconds

Description: Upload the software component/distribution file using multipart form data, where the key is 'file' and the value is the file to be uploaded. This will upload the distribution software to the library. This does not install this new distribution. To install it see Table 429: GET aml/system/software/operations/update.

Note: For i6000 libraries, the description element of the WSResultCode object will contain a colon “:” separated name value pair list as follows:

- STATUS="OK" or "WARNING"
- MESSAGE="Informational Status Message"

Example:

<description>STATUS=OK:MESSAGE=Signed by Production Certificate</description>

<i>URI</i>	<i>aml/system/software</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type: multipart/form-data
Request Data	Software distribution file
Response Codes	200, 400, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 429: GET aml/system/software/operations/update

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the progress of the current software update operation. This reports the current installation status. Initially the status element may be empty, but as the installation progresses, it will report a % complete. When the software update has completed, the status components will all report 100% or Failed if there was a problem.

The updateState element will report the overall state of the software update, see Figure 101: firmwareStatusList for details. For example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareStatusList xmlns:ns2="http://automatedMediaLibrary/">
  <updateState>2</updateState>
  <firmwareStatus>
    <component>FDM</component>
    <status>Awaiting RCU -- Overall 4%</status>
    <percentComplete>4%</percentComplete>
  </firmwareStatus>
  <firmwareStatus>
    <component>AMC</component>
    <status>Success</status>
    <percentComplete>100%</percentComplete>
  </firmwareStatus>
  <firmwareStatus>
    <component>MCB</component>
```

```

    <status>Success: 100%</status>
    <percentComplete>100%</percentComplete>
  </firmwareStatus>
  <firmwareStatus>
    <component>RCU</component>
    <status>In Progress: 5%</status>
    <percentComplete>5%</percentComplete>
  </firmwareStatus>
  <firmwareStatus>
    <component>CMB</component>
    <status>In Progress: 50%</status>
    <percentComplete>50%</percentComplete>
  </firmwareStatus>
  <firmwareStatus>
    <component>EEB</component>
    <status>Success: 100%</status>
    <percentComplete>100%</percentComplete>
  </firmwareStatus>
</ns2:firmwareStatusList>

```

Note: After the software update has completed successfully the library will automatically be rebooted, so the connection to the library will be lost and any requests to the library at this time will receive a 503 status code (Service Unavailable).

URI	<i>aml/system/software/operations/update</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000),
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 101: firmwareStatusList

Table 430: POST *aml/system/software/operations/update*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 120 seconds; Maximum = 600 seconds

Description: Start the software installation for the specified firmware object. In the example below, the library installs the previously installed software distribution (Rollback).

Note: After the install/update has completed the library will automatically reboot.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmware xmlns:ns2="http://automatedMediaLibrary/">
  <component>Rollback</component>
  <version>665H.TS07401</version>
</ns2:firmware>

```

URI	<i>aml/system/software/operations/update</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json

Request Data	See Figure 96: firmware
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 431: GET aml/system/software/externalApplications

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of externalApplication plugin resources, such as the StorNext software plugin installed on the library.

URI	aml/system/software/externalApplications
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 79: externalApplicationList

Table 432: POST aml/system/software/externalApplications

Product Support: Scalar i6000

Response Time: Minimum <= 10 seconds; Maximum = 60 seconds

Description: Upload an external application file using form data, where the key is 'file' and the value is the filename.

URI	aml/system/software/externalApplications
Method	POST
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	Content-Type: multipart/form-data
Request Data	The external application file
Response Codes	201, 403
Response Header	Content-Type:application/xml or application/json Location: aml/system/software/externalApplication/{name}
Response Data	See Figure 225: WSResultCode

Table 433: GET aml/system/software/externalApplication/{name}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the externalApplication resource identified by the URI path template "name".

URI	aml/system/software/externalApplication/{name}
Method	GET

User Role Access	Admin, Service, User
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 80: externalApplication

Table 434: DELETE aml/system/software/externalApplication/{name}

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the external application file identified by the URI path template “name”.

<i>URI</i>	<i>aml/system/software/externalApplication/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 435: GET aml/system/software/availableFirmware

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 60 seconds

Description: Retrieve the available firmware resource. This object reports the latest available library firmware version.

<i>URI</i>	<i>aml/system/software/availableFirmware</i>
Method	GET
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 11: availableFirmware

Table 436: POST aml/system/software/availableFirmware

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 15 seconds; Maximum = 60 seconds

Description: Initiate a download of the latest library firmware from the Web. This operation will load a library firmware bundle to the library but will not install it.

URI	<i>aml/system/software/availableFirmware</i>
Method	POST
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 437: POST *aml/system/software/restartLMC*

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Restart the Library Management Console (LMC), which supports the Local User Interface (LUI) as well as the RESTful Web Services interface. This interface is provided so that in the rare case the LMC exhibits problems and needs to be restarted, it can be restarted and does not require a library reboot or reset. The Web Service client will need to reconnect to the library after the LMC restarts.

URI	<i>aml/system/software/restartLMC</i>
Method	POST
User Role Access	Admin, Service
Version	760(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 438: GET *aml/users*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the user resource instances. Service and User roles retrieve only information for their username. Admin roles retrieve an entire list of users.

URI	<i>aml/users</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 216: userList

Table 439: POST aml/users**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Create a new user resource instance. Name, password and role are required elements. Valid user roles are 0 (ADMIN) or 1 (USER).

The name element allows the following characters: Upper and lower case a to Z, the numbers 0 to 9, a space, and an underscore (A-Za-z0-9 _). The maximum number of characters is 64. Names are case insensitive, and the account name will be created as lower-case. For example, joe, Joe or JOE will create the user 'joe'.

The password element allows all printable characters, !"#%&'()*+,-./:;<=>?@[\\]^_`{|}aAbBcCdDeEfFgGhHijJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ 0123456789, except back tick(`) and tilde(~). The minimum number of password characters is 8, and the maximum number of characters is 64.

Note: The following names are reserved and cannot be used to create a new user: service, admin, cvtl(i6000),security(i6000) and ilinkacc.

<i>URI</i>	<i>aml/users</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 217: user
Response Codes	200(i6000) 201(i3/i6/i6H), 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 217: user

Table 440: GET aml/users/ldap**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H**Response Time:** Minimum <= 1 second; Maximum = 30 seconds**Description:** Retrieve the LDAP configuration resource.

<i>URI</i>	<i>aml/users/ldap</i>
Method	GET
User Role Access	Admin, Service, User (If Service or User, the only information returned is whether LDAP is enabled/disabled)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	Figure 114: ldap

Table 441: PUT aml/users/ldap**Product Support:** Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Configure the LDAP resource. Initially all elements of the ldap object must be completed except for the alternateServer which may be null. When disabling LDAP, only the enable element is required. After the LDAP configuration has been saved, the library will persist this data. When the user disables LDAP, the configuration persists but it is not used. If you change the state from disabled to enabled, you will still need to pass down all the required elements even though the library has this data persisted. The exception to this is the ldap.searchUserPassword element, which does not need to be included; if it is empty or null the persisted value will be used.

URI	aml/users/ldap
Method	PUT
User Role Access	Admin, Service (i6000) and Admin (i3/i6/i6H)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	Figure 114: ldap
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	Figure 114: ldap

Table 442: POST aml/users/ldap - deprecated

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Upload LDAP certificate(s) to the library. These certificates are generally distributed public keys from the LDAP server. When uploading the file(s), the key is 'file' and the value is the 'file name'.

Note: This interface has been deprecated. Use Table 444: POST aml/users/ldap/certificates.

URI	aml/users/ldap
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:multipart/form-data
Request Data	LDAP Certificate file
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 443: GET aml/users/ldap/certificates

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve a list of LDAP certificates that were uploaded to the library. These certificates are generally distributed public keys from the LDAP server.

URI	aml/users/ldap/certificates
Method	GET

User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 19: communicationCertificateList

Table 444: POST aml/users/ldap/certificates

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Upload LDAP certificate(s) to the library. These certificates are generally distributed public keys from the LDAP server. When uploading the file(s), the key is 'file' and the value is the 'file name'.

<i>URI</i>	<i>aml/users/ldap/certificates</i>
Method	POST
User Role Access	Admin, Service
Version	720(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:multipart/form-data
Request Data	LDAP Certificate file
Response Codes	200, 403
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 445: GET aml/users/ldap/enabled

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Interface to determine if the LDAP resource is enabled. This interface does not require a user session or authentication (login not needed).

<i>URI</i>	<i>aml/users/ldap/enabled</i>
Method	GET
User Role Access	No authentication required
Version	760(i6000), 140(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:test/plain or application/json
Response Data	true or false

Table 446: POST aml/users/ldap/keytab

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Upload the LDAP keytab file to the library.

The multipart form data key is 'file' and the value is the file to be uploaded.

URI	<i>aml/users/ldap/keytab</i>
Method	POST
User Role Access	Admin, Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type multipart/formdata
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 447: POST *aml/users/ldap/test*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 3 seconds; Maximum = 180 seconds

Description: Test the LDAP user and configuration settings provided in the request. When testing LDAP configuration, you are not required to provide a user or password in the `ldapTest` object. If you want to verify the LDAP username and password you are required to provide the user and password and the configuration settings, `ldapTest.Ldap`.

URI	<i>aml/users/ldap/test</i>
Method	POST
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 115: <code>ldapTest</code>
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 448: POST *aml/users/login*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Login to the library. A successful login returns a session cookie that must be used with successive requests. If a service user is currently logged in a 503 status code is returned and the login request will be denied. There are three user roles supported; Service, Administrator (Admin) and User. If a Service user logs in, all other users will have their sessions terminated.

As of firmware release 779 (i6000) and 250(i3/i6/i6H):

- If remote service login access is disabled, the service user login will only succeed if an admin enables remote service user access, or a library generated authentication code is provided to the service user for successful login for Multi-Factor Authentication (MFA). The custom header response message of "Service: Authentication Code Required" indicates an MFA authentication is required to create a service login session

if access is disabled. See Table 451: POST aml/users/login/mfa.

- A default admin password change is required for new installations. If the custom header response message indicates “Warning: Default Password Supplied”, the admin’s login password must be changed. Once the login session has been created, any subsequent requests will return a 412 Precondition Failed error until the password has been updated.

As of firmware releases 785(i6000), 260(i3/i6/i6H), a default custom response header, “Warning: Default Admin Password Used”, is returned if the default admin user has logged in with the library default password. The header is informational only and does not affect the user session.

If Multi-Factor Authentication (MFA) has been enabled, a custom header is returned in the request message to indicate MFA authentication is required. The login request must be followed by the validation of the MFA authentication code to complete the login process. See Table 451: POST aml/users/login/mfa. If MFA has not been enabled, update the user password after the login request (see Table 468: PUT aml/user/{name}). MFA support was added in firmware versions 785(i6000) and 250(i3/i6/i6H).

As of firmware versions 250(i3/i6/i6H), not only must the default admin password be changed at initial installation/configuration, but also any subsequent default passwords created by an administrator for admin and user accounts, at first user account login. The custom response header, “Warning: Default Password Supplied”, will be returned. Once the login session has been created, any subsequent requests will be return a 412 Precondition Failed error until the password has been updated.

Note: Scalar i6000:

The Scalar i6000 supports 5 concurrent administrator user logins and 25 regular user logins or a single service user login. If the number of user logins exceed the limit, the customCode element of the WSResultCode will be set to 1 and an HTTP status of 503 will be returned.

Note: Scalar i3/i6/i6H:

The Scalar i3/i6/i6H support 25 concurrent administrator and regular user logins, but only a single service user login.

As of firmware release 250, not only must the default admin password must be changed at initial installation/configuration, but also any subsequent default passwords created by an administrator for admin and user accounts, at first user account login.

URI	aml/users/login
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 140(i3/i6/i6H)
Parameters	<p>The form parameters are name, password, ldap and forceLogin. The valid values for each parameter are as follows:</p> <ul style="list-style-type: none"> • name = valid user name • password = the user password • ldap = “true” or “false”, true, if you want to use LDAP to authenticate • forceLogin = “true” or “false” (Not supported on I3/i6/i6H) <p>The forceLogin parameter only applies to an admin user. This can be</p>

	<p>used when the number of admin logins has exceeded the maximum allowed. If used and the number of admin logins has exceeded the limit, then one of the current admin logins will be terminated. This parameter is not supported on I3/i6/i6H.</p> <p>On the i6000, If the number of user logins has exceeded the limit, the customCode element of the WSResultCode will be set to 1.</p> <p>Note: This interface does NOT support query parameters, only form parameters.</p>
Request Header	Content-Type: application/x-www-form-urlencoded
Request Data	HTTP form data
Response Codes	200, 404, 503
Response Header	<p>Content-Type:application/xml or application/json</p> <p>Warning: Default Password Supplied. Versions 785(i6000), 260(i3/i6/i6H) This header is returned on the first login for a new user or if an Admin has reset the user's password. This is not supported on the i6000.</p> <p>MFA: Validation Required (i3/i6/i6H version 250), 785 (i6000) This header is returned if MFA is enabled.</p> <p>Service: Authentication Code Required Versions 779(i6000), 260(i3/i6/i6H) This header is returned for a service user, if remote service user login access has been disabled.</p>
Response Data	See Figure 225: WSResultCode

Table 449: POST aml/users/login

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Login to the library using the user XML or JSON object. A successful login returns a session cookie that needs to be used for successive requests. If a service user is currently logged in, a 503 status code is returned and the login request will be denied. There are three user types/roles supported, Service, Administrator and Regular/User. If a Service user logs in, all other users will have their sessions terminated.

As of firmware release 779 (i6000) and 250(i3/i6/i6H):

- If remote service login access is disabled, the service user login will only succeed if an admin enables remote service user access, or a library generated authentication code is provided to the service user for successful login for Multi-Factor Authentication (MFA). The custom header response message of “Service: Authentication Code Required” indicates an MFA authentication is required to create a service login session if access is disabled. See Table 451: POST aml/users/login/mfa.
- A default admin password change is required for new installations. If the custom header response message indicates “Warning: Default Password Supplied”, the admin’s login password must be changed. Once the login session has been created, any subsequent requests will return a 412 Precondition Failed error until the password has been updated.

As of firmware releases 785(i6000), 260(i3/i6/i6H), a default custom response header, “Warning: Default Admin Password Used”, is returned if the default admin user has logged in with the library default password. The header is informational only and does not affect the user session.

If Multi-Factor Authentication (MFA) has been enabled, a custom header is returned in the request message to indicate MFA authentication is required. The login request must be followed by the validation of the MFA authentication code to complete the login process. See Table 451: POST aml/users/login/mfa. If MFA has not been enabled, update the user password after the login request (see Table 468: PUT aml/user/{name}). MFA support was added in firmware versions 785(i6000) and 250(i3/i6/i6H).

As of firmware versions 250(i3/i6/i6H), not only must the default admin password be changed at initial installation/configuration, but also any subsequent default passwords created by an administrator for admin and user accounts, at first user account login. The custom response header, “Warning: Default Password Supplied”, will be returned. Once the login session has been created, any subsequent requests will be return a 412 Precondition Failed error until the password has been updated.

Note: Scalar i6000:

The Scalar i6000 supports 5 concurrent administrator user logins and 25 regular user logins or a single service user login. If the number of user logins exceed the limit, the customCode element of the WSResultCode will be set to 1 and an HTTP status of 503 will be returned.

Note: Scalar i3/i6/i6H:

The Scalar i3/i6/i6H support 25 concurrent administrator and regular user logins, but only a single service user login.

URI	aml/users/login
Method	POST
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	<p>The query parameters forceLogin. The valid values for each parameter are as follows:</p> <ul style="list-style-type: none"> forceLogin = “true” or “false” (Not supported on I3/i6/i6H) <p>The forceLogin parameter only applies to an admin user. This can be used when the number of admin logins has exceeded the maximum allowed. If used and the number of admin logins has exceeded the limit, then one of the current admin logins will be terminated This parameter is not supported on I3/i6/i6H.</p> <p>On the i6000, If the number of user logins has exceeded the limit, the customCode element of the WSResultCode will be set to 1.</p>
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 217: user
Response Codes	200, 404, 503
Response Header	<p>Content-Type:application/xml or application/json</p> <p>Warning: Default Password Supplied. Versions 785(i6000), 260(i3/i6/i6H) This header is returned on the first login for a new user or if an Admin has reset the user’s password. This is not supported on the i6000.</p>

	<p>MFA: Validation Required (i3/i6/i6H version 250), 785 (i6000) This header is returned if MFA is enabled.</p> <p>Service: Authentication Code Required Versions 779(i6000), 260(i3/i6/i6H) This header is returned for a service user, if remote service user login access has been disabled.</p>
Response Data	See Figure 217: user

Table 450: DELETE aml/users/login

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Logout and end the library Web Services session.

URI	aml/users/login
Method	DELETE
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 451: POST aml/users/login/mfa

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Validate an authentication code for a Multi-Factor Authentication (MFA) type for the current user. With MFA enabled on the library, this is the second step in a login. It is required after a /users/login request to establish a user session.

Note: The MFA Time-based One-Time Password (TOTP) is supported for all users. This request is also required by the Admin user before MFA is enabled on the library for all user access.

MFA does not apply to service user logins; however, if remote service login access has been disabled and service login access cannot be enabled by an admin (admin lost password), the library generates, and locally displays, a pass code, which when provided to the remote service user will allow for service user login authentication as the second step of a service login request.

URI	aml/users/login/mfa
Method	POST
User Role Access	Admin, User
Version	231(i3/i6/i6H) 779(i6000 service only), 785(i6000 all users)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 143: mfaAuthentication
Response Codes	200, 403

Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 452: GET aml/users/login/mfa/{type}/key

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the data required for the current user to set up authentication using the MFA type indicated by the {type} in the URI path. This is applicable for those MFA types that require data to be shared with the user; for TOTP, this is the 32 character shared secret.

Once a user has validated an authentication code for this MFA type, the data may no longer be retrieved and a 403 Forbidden error will be returned.

For MFA types where this is not applicable, a 404 Not Found will be returned.

<i>URI</i>	<i>aml/users/login/mfa/{type}/key</i>
Method	GET
User Role Access	Admin, User
Version	231(i3/i6/i6H), 785(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type: application/json or application/xml
Response Data	See Figure 144: mfaSharedData

Table 453: GET aml/users/login/mode

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the login mode. A string value is returned:

- 1: Local user accounts are enabled.
- 2: Local user accounts are disabled. Only LDAP users may login to the library.

Note: Applicable to U/M Builds only.

<i>URI</i>	<i>aml/users/login/mode</i>
Method	GET
User Role Access	Admin, Service, User
Version	220M(i3/i6/i6H) Note: Supported only in M-build version 220M and higher
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json

Table 454: PUT aml/users/login/mode

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the login mode with the following values:

- 1: Enable local user accounts. This is the default library setting.
- 2: Disable all local user accounts, including the service user account. Logins are restricted to LDAP users.

Note: M-Build version only: Local user accounts may only be disabled by an Admin LDAP user.

<i>URI</i>	<i>aml/users/login/mode</i>
Method	PUT
User Role Access	Admin
Version	220M(i3/i6/i6H) Note: Supported only in M-build version 220M and higher
Parameters	N/A
Request Header	Content-Type:text/plain or application/json
Request Data	1(local accounts enabled), 2(local accounts disabled, LDAP users only)
Response Codes	200, 403
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 455: GET aml/users/luiAccess

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the local UI access resource.

<i>URI</i>	<i>aml/users/luiAccess</i>
Method	GET
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 131: LUIAccess

Table 456: PUT aml/users/luiAccess

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the local UI access resource.

<i>URI</i>	<i>aml/users/luiAccess</i>
Method	PUT
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 131: LUIAccess
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 131: LUIAccess

Table 457: GET aml/users/uiAccess/mode

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the I3/i6/i6H local access mode. This interface does not require authentication (a user does not have to be logged in).

URI	aml/users/uiAccess/mode
Method	GET
User Role Access	Admin, Service, User
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	1(Open), 2(Login Required) or 3(PIN required)

Table 458: GET aml/users/mfa

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the Multi-Factor Authentication (MFA) library configuration. A list of mfa objects is returned, indicating which MFA types are enabled for logins. The authenticationCode element is returned as null, but is required when enabling or disable MFA. See Table 459: PUT aml/users/mfa.

Note: Currently, only Time-based One-Time Password (TOTP), (type 1), is supported.

URI	aml/users/mfa
Method	GET
User Role Access	Admin, Service, User
Version	231(i3/i6/i6H), 785(i6000)
Parameters	N/A
Request Header	Accept: application/xml or application/json
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 141: mfaList

Table 459: PUT aml/users/mfa

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Enable or disable a Multi-Factor Authentication (MFA) for a specific MFA type. An authentication code is required to enable or disable MFA.

Note: In version 231, only Time-based One-Time Password (TOTP), (type 1), is supported.

URI	aml/users/mfa
Method	PUT
User Role Access	Admin

Version	231(i3/i6/i6H), 785(i6000)
Parameters	N/A
Request Header	Content-Type: application/xml or application/json
Request Data	See Figure 142: mfa
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 142: mfa

Table 460: GET aml/users/reports/login

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the list of user login activity records.

URI	aml/users/reports/login
Method	GET
User Role Access	Admin, Service (i6000 only), User (i6000 only)
Version	700(i6000), 230(i3/i6/i6H)
Parameters	<p>The following query parameters are supported, start, length, period, date, save with the following values:</p> <ul style="list-style-type: none"> • start=0-n • length=1-n, anything else means all records. • period=1-n, the last number of days to include in the report. If you want to report for the last week, you would specify 7. • date=At what date you want to start your query. The data returned will include all records that are equal or older than the date specified. When used with the period parameter, the data returned will include all records that are equal or older than the date specified up to the period (number of days) specified. The date format expected is “yyyy-MM-dd HH:mm:ss” or “yyyy-MM-dd HH:mm:ss Z”, the Z (time zone) will be ignored. • save="name" where name is a file name to use to save the file. The save="name" query parameter should be used by a client browser to allow the data to be saved by the browser to a file. A default "name" is provided if none is specified. <p>If no query parameters are used, the request will return all login activity data.</p>
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type: application/xml, application/json, text/plain, application/octet-stream On success and save= parameter is used Cookie: name= FileDownloadingProgressCookie, value=Done
Response Data	See Figure 127: loginActivityList or octet-stream or text

Table 461: POST aml/users/reports/login/email

Product Support: Scalar i6000

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Email the list of user login activity records.

The information will be in an email attachment and the file format will be CSV. The data separator has changed from “!” (exclamation point character) to a comma “,” in version 770(i6000).

URI	<i>aml/users/reports/login/email</i>
Method	POST
User Role Access	Admin, Service (i6000 only), User (i6000 only)
Version	700(i6000), 230(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 68: email
Response Codes	200, 403, 412
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 462: GET *aml/users/service/mode*

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the service mode. Service mode is reported as enabled when a service user is logged in or if the library has been placed in service mode by an administrator.

URI	<i>aml/users/service/mode</i>
Method	GET
User Role Access	Admin, Service, User
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:text/plain or application/json
Response Data	1(Enabled), 2(Disabled)

Table 463: PUT *aml/users/service/mode*

Product Support: Scalar i3, Scalar i6/i6H

License Requirements: Service

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update the service mode.

When service mode is enabled, all other users are logged off the system. Service type operations may be performed without reporting such events to Quantum. Service mode is automatically disabled when the user session ends.

URI	<i>aml/users/service/mode</i>
Method	PUT
User Role Access	Admin
Version	220(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:text/plain or application/json

Request Data	1(Enabled), 2(Disabled)
Response Codes	200, 403
Response Header	Content-Type:text/plain or application/json
Response Data	1 or 2

Table 464: GET aml/users/sessions

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the user sessions (current logged in user's) resources. For a Service (i3/i6/i6H only) or User role, only the current user's session is returned.

<i>URI</i>	<i>aml/users/sessions</i>
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 220: userSessionList

Table 465: DELETE aml/users/session/{id}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Log off the user with the id identified by the URI path template "id". The user ids are reported in the userSession objects URI aml/users/sessions. Only users with Admin privileges (role 0) can log off other users.

<i>URI</i>	<i>aml/users/session/{id}</i>
Method	DELETE
User Role Access	Admin, Service (i6000) and Admin (i3/i6/i6H)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 466: GET aml/user

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the user resource instance based on the cookie header parameter for the current user.

<i>URI</i>	<i>aml/user</i>
Method	GET

User Role Access	Admin, Service, User (If User return on the User information)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 217: user

Table 467: GET aml/user/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the user resource instance identified by the URI path template “name”.

URI	aml/user/{name}
Method	GET
User Role Access	Admin, Service, User
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 217: user

Table 468: PUT aml/user/{name}

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Update a user resource instance identified by the URI path template “name”. Passwords, roles and partition accesses may be modified for regular Admin or User role users.

An Admin user may modify Admin or User accounts. When modifying a User account, the role must be specified. If not specified, the account will default to a role of 0, and the user will be assigned an Admin role. If the partition access list is not included in the request data, any previously configured entitlements for the user will be deleted.

The password element allows all printable characters, !"#%&'()*+,-./:;<=>?@[\\]^_`{|}aAb BcCdDeEfGhHijJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ 0123456789, except back tick(`) and tilde(~). The minimum number of characters is 8, and the maximum number is 64. A null (or omitted) password element in the user object indicates that the password it to remain unchanged.

A User role user may only modify its own password. If specified, the role element of the user object should be set to -1 to indicate it is to be ignored.

Scalar i3/i6/i6H: As of version 220(i3/i6/i6H), the default ‘admin’ username may be changed. Only the default admin user has permission to change the name. The name may include the characters: “A-Za-z0-9_”, with a maximum of 64 characters. The default admin user account is identified by the protected element in the user object.

URI	<i>aml/user/{name}</i>
Method	PUT
User Role Access	Admin, Service, User (User restricted to password change)
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	Content-Type:application/xml or application/json
Request Data	See Figure 217: user
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 217: user (Scalar i3/i6/i6H) See Figure 225: WSResultCode (Scalar i6000)

Table 469: DELETE *aml/user/{name}*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Delete the user resource instance identified by the URI path template “name”.

URI	<i>aml/user/{name}</i>
Method	DELETE
User Role Access	Admin, Service
Version	700(i6000), 110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

Table 470: GET *aml/user/{name}/mfa*

Product Support: Scalar i6000, Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Retrieve the user MFA resources, for the user indicated by {name} in the URI path. A list of userMfa objects is returned, indicating which MFA types the user has configured and authenticated.

Note: Currently, only Time-based One-Time Password (TOTP), (type 1), is supported.

URI	<i>aml/user/{name}/mfa</i>
Method	GET
User Role Access	Admin, User
Version	231(i3/i6/i6H), 785(i6000)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 218: userMfaList

Table 471: PUT aml/user/admin/reset

Product Support: Scalar i3, Scalar i6/i6H

Response Time: Minimum <= 1 second; Maximum = 30 seconds

Description: Reset the default admin account. The password reverts to “password”. If the default admin username has been changed, the ‘admin’ username is restored in addition to resetting the password.

<i>URI</i>	<i>aml/user/admin/reset</i>
Method	PUT
User Role Access	Service
Version	110(i3/i6/i6H)
Parameters	N/A
Request Header	N/A
Request Data	N/A
Response Codes	200, 403, 404
Response Header	Content-Type:application/xml or application/json
Response Data	See Figure 225: WSResultCode

6. Resource Objects

The following figures list the supported resource objects (XML representation) available by the Web Services interfaces.

Figure 1: accessDeviceList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:accessDeviceList xmlns:ns2="http://automatedMediaLibrary/">
  <accessDevice/> <!-- List of accessDevice objects, see Figure 2: accessDevice -->
</ns2:accessDeviceList>
```

Figure 2: accessDevice

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:accessDevice xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>F001396025</serialNumber> <!-- drive or partition serial number -->
  <type>1</type> <!-- 1 (drive) 2 (Partition) -->
  <port>
    <id>1</id>
    <access>true</access>
  </port>
  <port>
    <id>2</id>
    <access>false</access>
  </port>
</ns2:accessDevice>
```

Figure 3: accessGroupList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:accessGroupList xmlns:ns2="http://automatedMediaLibrary/">
  <accessGroup/> <!-- List of accessGroup objects, see Figure 4: accessGroup -->
</ns2:accessGroupList>
```

Figure 4: accessGroup

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:accessGroup xmlns:ns2="http://automatedMediaLibrary/">
  <name>AG2</name>
  <hostList/> <!-- See Figure 104: hostList -->
  <accessDeviceList/> <!-- See Figure 1: accessDeviceList -->
</accessGroup>
```

Figure 5: activeVaultPolicyList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:activeVaultPolicyList xmlns:ns2="http://automatedMediaLibrary/">
  <activeVaultPolicy/> <!-- A list of activeVaultPolicy objects -->
</ns2:activeVaultPolicyList>
```

Figure 6: activeVaultPolicy

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:activeVaultPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL1</partitionName>
  <!-- The partition will have either a vaultDefinedExport policy or an externalDefinedExport policy -->
```



```

<vaultDefinedExport> <!-- Redirect exports to specific Active Vault -->
  <activeVaultName>AV Partition</activeVaultName>
  <mediaFilter>*00LTO5</mediaFilter>
</vaultDefinedExport>
<externalDefinedExport> <!-- Redirect exports to external application (StorNext) defined Active Vault -->
  <externalApplicationServersName>The external application server configuration
    name</externalApplicationServersName> <!-- See Figure 82: externalApplicationServers -->
</externalDefinedExport>
</activeVaultPolicy>
</ns2:activeVaultPolicyList>

```

Figure 7: autoExportPolicyList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:autoExportPolicyList xmlns:ns2="http://automatedMediaLibrary/">
  <autoExportPolicy/> <!-- A list of autoExportPolicy objects -->
</ns2:autoExportPolicyList>

```

Figure 8: autoExportPolicy

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:autoExportPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>LL2</partitionName> <!-- The partition you want to apply the policy too -->
  <destinationAmpPartitionName>AMP</destinationAmpPartitionName> <!-- The AMP partition to which to
    move media -->
</ns2:autoExportPolicy>

```

Figure 9: autoImportPolicyList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:autoImportPolicyList xmlns:ns2="http://automatedMediaLibrary/">
  <autoImportPolicy/> <!-- A list of autoImportPolicy objects -->
</ns2:autoImportPolicyList>

```

Figure 10: autoImportPolicy

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:autoImportPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>The name of the partition to apply the policy too</partitionName>
  <mediaBarcodeFilter>0000500-0000700</mediaBarcodeFilter> <!-- The media barcode filter range, the
    following regex applies "[a-zA-Z0-9]{5,15}-[a-zA-Z0-9]{5,15};?\s*" -->
  <importType>0</importType>
    <!-- The type of auto import you want to perform, since multiply types can be configure, this value
    is a mask
    0 (Auto Import is activated manually (requires user action))
    1 (Include media in AMP I/E station slots when Auto Import is activated)
    2 (Automatically activate Auto import from AMP I/E station slots when media is placed in those
    slots)
    4 (Automatically activate Auto import on a predefined interval basis)
    -->
  <interval> <!-- Schedule auto imports on a given interval -->
    <frequency>2</frequency> <!-- 1 (Daily) 2 (Weekly) 3 (Monthly) -->
    <dayOfWeek>0</dayOfWeek> <!-- Day of week when report should be sent, 0 = Sunday, 6 = Saturday -->
    <hourOfDay>14</hourOfDay> <!-- The hour of the day the report should be sent, 0 - 23 -->
    <includele>>false</includele> <!-- If true import from AMP storage and AMP IE slots, if false only import
    from AMP storage -->
  </interval>
</ns2:autoImportPolicy>

```

Figure 11: availableFirmware

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:availableFirmware xmlns:ns2="http://automatedMediaLibrary/">
  <firmwareVersion>The latest library firmware version</firmwareVersion>
  <isUpdated>true</isUpdated> <!--Indicates latest available and released library firmware -->
</ns2:availableFirmware>
```

Figure 12: bladeList

```
<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8"?>
<ns2:bladeList xmlns:ns2="http://automatedMediaLibrary/">
  <blade/> <!-- A list of blade objects. -->
</ns2:bladeList>
```

Figure 13: blade

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:blade xmlns:ns2="http://automatedMediaLibrary/">
  <coordinate/> <!-- See Figure 26: coordinate -->
  <name>name</name>
  <type>1</type> <!-- 1(FC IO Blade), 2(EEB), 3(MCB), 4(LTFS Blade), 5(Windows Blade) -->
  <firmwareVersion>firmwareVersion</firmwareVersion>
  <serialNumber>serialNumber</serialNumber>
</ns2:blade>
```

Figure 14: bladeFirmwareList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:bladeFirmwareList xmlns:ns2="http://automatedMediaLibrary/">
  <bladeFirmware/> <!-- A list of bladeFirmware objects. -->
</ns2:bladeFirmwareList>
```

Figure 15: bladeFirmware

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:bladeFirmware xmlns:ns2="http://automatedMediaLibrary/">
  <type>4</type> <!-- 4(LTFS Blade) 5(Windows Blade) -->
  <version>firmwareVersion</version>
</ns2:bladeFirmware>
```

Figure 16: cleanDriveTask

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:cleanDriveTask xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>The drives physical or logical serial number</serialNumber>
  <coordinate>The coordinate of the media to use for cleaning</coordinate> <!-- see Figure 26: coordinate -->
</ns2:cleanDriveTask>
```

Figure 17: cleaningMediaList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:cleaningMediaList xmlns:ns2="http://automatedMediaLibrary/">
  <cleaningMedia/> <!-- A list of cleaningMedia objects -->
</ns2:cleaningMediaList>
```

Figure 18: cleaningMedia

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:cleaningMedia xmlns:ns2="http://automatedMediaLibrary/">
  <media/> <!--see Figure 135: media -->
  <useCount>The number of times the media was used to clean a drive</useCount>
  <state>1</state> <!-- 0(Unknown), 1(Valid), 2(Invalid), 3(Expired) -->
</ns2:cleaningMedia>
```

Figure 19: communicationCertificateList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:communicationCertificateList xmlns:ns2="http://automatedMediaLibrary/">
  <communicationCertificate/> <!-- A list of communicationCertificate objects -->
</ns2:communicationCertificateList>
```

Figure 20: communicationCertificate

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:communicationCertificate xmlns:ns2="http://automatedMediaLibrary/">
  <keySize>2048</keySize> <!-- 1024, 2048 or 4096 -->
  <digestAlgorithm>0</digestAlgorithm> <!-- 0(Unknown), 1(MD5), 2(SHA1), 3(SHA224), 4(SHA256),
  5(SHA384), 6(SHA512), 7(MDC2), 8(RIPEMD160) -->
  <issuer/> <!-- certificateInformation object -->
  <subject/> <!-- certificateInformation object -->
  <type>Root</type> <!-- types are Root, Admin, Client, Identity or Unknown -->
  <validNotBefore>Apr 19 13:51:18 2011 GMT</validNotBefore>
  <validNotAfter>Apr 17 13:51:18 2021 GMT</validNotAfter>
  <serialNumber>12345678</serialNumber> <!-- This field is currently not being used -->
  <subjectAlternativeNames>*.company.com< subjectAlternativeNames> <!-- One or more SAN entries.
  Added in 770(i6000), 160(i3/i6/i6H) -->
</ns2:communicationCertificate>
```

Figure 21: componentList (ENUM)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<componentList xmlns:ns2="http://automatedMediaLibrary/">
  <component name="component name"> <!-- A list of one or more components -->
    <element name="component element name">
      <entry key="1" value="Connectivity"/> <!-- A list of entry elements, which are key, value pairs -->
    </element>
  </component>
</componentList>
```

Figure 22: configurationChangeList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:configurationChangeList xmlns:ns2="http://automatedMediaLibrary/">
  <configurationChange/> A list of configurationChange objects
</ns2:configurationChangeList>
```

Figure 23: configurationChange

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:configurationChange xmlns:ns2="http://automatedMediaLibrary/">
  <dateTime>admin</dateTime>
  <type>text</type><!-- The type of configuration change that was made -->
  <description>Login</description> <!--The updated value(s) or object -->
</ns2:configurationChange>
```

Figure 24: certificateInformation

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:certificateInformation xmlns:ns2="http://automatedMediaLibrary/">
  <countryCode>US</countryCode>
  <state>Colorado</state>
  <locality>Denver</locality>
  <organization>DVT</organization>
  <organizationalUnit>DVT</organizationalUnit>
  <commonName>Your Company Name</commonName>
  <emailAddress>E-mail address</emailAddress>
</ns2:certificateInformation >
```

Figure 25: contactInformation

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:contactInformation xmlns:ns2="http://automatedMediaLibrary/">
  <!-- each element can have a maximum of 256 characters -->
  <name>The contacts full name or first name if the lastName element is used</name>
  <lastName>The surname or last name of the contact</lastName> <!-- This field was added so the above
      element "name" could be used as a first name of the contact and this element could be
      used as a last name of the contact. If this element is empty or null, the library assumes
      the name element contains the full name of the contact -->
  <company>Company name</company>
  <phone>Contact phone number</phone>
  <email>Contact e-mail address</email>
  <description>A description of the library.</description>
  <address1>Unit 15</address1>
  <address2>1600 Pen Avenue</address2>
  <city>Sydney</city>
  <stateOrProvince>New South Wales</stateOrProvince>
  <zipCode>The city zip code</zipCode>
  <country>Australia</country>
</ns2:contactInformation>
```

Figure 26: coordinate

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:coordinate xmlns:ns2="http://automatedMediaLibrary/">
  <frame>1</frame> <!-- I3/i6/i6H – Always 1, I6000 – 0 through number of frames/modules -->
  <rack>1</rack> <!-- I3/i6/i6H.- Always 1, i6000, 1 back side, 2 door side -->
  <section>2</section> <!-- I3/i6/i6H - vertical location within the library module stack, with control module
      referencing section 0, and any 3U increments above or below CM section 0 being
      identified by positive, or negative integer respectively.
      i6000 – A row of magazines (1 -10) or drives (1-2) in a rack -->
  <column>1</column> <!-- I3/i6/i6H - magazine/bay column location, value is dependent on product type and
      library configuration. i3/i6: 1-5 left magazine, 6-10 right magazine. 11 center
      column for drives and optional drive bay storage magazines. i6H: 1-6 left
      magazine, 7-12 right magazine. 13 center column for drives and optional drive
      bay storage magazines.
      I6000 – A column of magazines (1-10) or drives (1-12) in a rack. -->
  <row>1</row> <!-- I3/i6/i6H - magazine slot, or drive location within column, bay, counting bottom up
      I6000 – Magazine slots or drive location -->
  <type>2</type> <!-- 0(N/A), 1(Robot), 2(Storage), 3(IE), 4(Drive), 5(XIE), 6(Cleaning) -->
</ns2:coordinate>
```

Figure 27: crossPartitionMovesList

```
<?xml version="1.0" encoding="UTF-8"?>
```

```

<ns2:crossPartitionMovesList xmlns:ns2="http://automatedMediaLibrary/">
  <crossPartitionMoves/> <!-- A list of crossPartitionMoves objects -->
</ns2:crossPartitionMovesList>

```

Figure 28: crossPartitionMoves

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:crossPartitionMoves xmlns:ns2="http://automatedMediaLibrary/">
  <barcode>barcode</barcode>
  <sourcePartition>sourcePartition</sourcePartition>
  <sourcePartitionType>Standard</sourcePartitionType> <!-- "Unknown", "Standard", "EDLM", "AMP", "Active Vault" -->

  <sourceElementAddress>250</sourceElementAddress>
  <destinationPartition>destinationPartition</destinationPartition>
  <destinationPartitionType>destinationPartition</destinationPartitionType> <!-- "Unknown", "Standard", "EDLM", "AMP", "Active Vault" -->

  <destinationElementAddress>4096</destinationElementAddress>
  <dateTime>2001-12-31 12:00:00</dateTime>
</ns2:crossPartitionMoves>

```

Figure 29: dateTime

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:dateTime xmlns:ns2="http://automatedMediaLibrary/">
  <date>2012-08-14</date>
  <time>21:34:02</time>
  <datetime>2012-08-14 21:34:02 -0600</datetime>
  <timezone>America/Denver</timezone>
  <itime>1345001642141</itime> <!-- time in seconds since EPOCH -->
</ns2:dateTime>

```

Figure 30: detailedDriveActivityStatistics

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:detailedDriveActivityStatistics xmlns:ns2="http://automatedMediaLibrary/">
  <drive> <!-- One of these for each drive installed in the library -->
    <physicalSerialNumber>1210007896</physicalSerialNumber>
    <logicalSerialNumber>F001397049</logicalSerialNumber>
    <partition>LL1</partition> <!-- NULL if the drive does not belong to a partition -->
    <driveActivityStatisticsList>
      <driveActivityStatistics/> <!-- 24 of these, see Figure 34: driveActivityStatistics -->
    </driveActivityStatisticsList>
  </drive>
</ns2:detailedDriveActivityStatistics>

```

Figure 31: DNS

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:DNS xmlns:ns2="http://automatedMediaLibrary/">
  <ipAddress>10.20.88.2</ipAddress>
  <ipAddress>192.168.23.5</ipAddress>
</ns2:DNS>

```

Figure 32: driveList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveList xmlns:ns2="http://automatedMediaLibrary/">
  <drive/> <!-- A list of drive objects, see Figure 33: drive -->

```

</ns2:driveList>

Figure 33: drive

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:drive xmlns:ns2="http://automatedMediaLibrary/">
  <physicalSerialNumber>physicalSerialNumber</physicalSerialNumber>
  <logicalSerialNumber>logicalSerialNumber</logicalSerialNumber>
  <address>address</address>      <!-- WWPN -->
  <coordinate /> See Figure 26: coordinate
  <elementAddress>256</elementAddress> <!-- Logical element address -->
  <firmwareVersion>firmwareVersion</firmwareVersion>
  <type>
    <domainType>3</domainType> <!-- 0(Unknown), 3(LTO2), 4(LTO3), 5(LTO4), 6(LTO5), 7(LTO6), 8(LTO7),
      9(LTO8), 10(LTO9), 554(Mixed Types) -->
    <vendor>UNKNOWN, IBM or HP</vendor>
    <productId>Ultrium 6-SCSI</productId>
    <sledType>1</sledType> <!-- 0(Unknown), 1(Standard), 2(EDLM) -->
    <interface>1</interface> <!-- 0(Unknown), 1(SCSI), 2(Fibre), 3(SAS) -->
    <formFactor>UNKNOWN, FH or HH</formFactor>
  </type>
  <mode>0</mode> <!-- 1(Online), 2(Offline) -->
  <state>1</state> <!-- 1(Varied On), 2(Varied Off), 3(Pending Status Change) -->
  <status>0</status> <!-- 0(Unknown), 1(Good/Operational),2(Failed), 3(Degraded), 4(Not Installed),
      5(Initializing),6(Not Ready) 7(Firmware Updating) i6000 only, added in 765(i6000) -->
  <owner>Owning partition or NULL</owner>
  <settings>
    <controlPath>
      <primary>true</primary>
      <type>1</type> <!-- 1(None), 2(Standard/CP), 3(Basic/CPF), 4(Advanced/ACPF), 5(Multi Control Path),
        6(Advanced Control Path IBM) -->
      <subType>1</subType> <!-- 1(None), 2(Active), 3(Standby) -->
    </controlPath>
    <dataPath>1</dataPath> <!-- 1(Standard), No data path failover configured.
      2(Basic), Basic failover configured, (uses NPIV). Only for HP LTO drives
      3(Advanced), This failover requires a host device driver (IBM or HP)
        depending on the configured drive vendor.
      4(MultiPath) i6/i6H and i6000. i6000 enables both ports for multi-path by default
    </dataPath>
    <encryption>
      <method>0</method> <!-- 0(None), 1(AME) Application-managed
        2(LME), Application-managed, 4(SME) System-managed -->
      <fips>true</fips>
    </encryption>
    <ipAddress>10.10.3.50</ipAddress>
    <bladeCoordinate/> <!-- See Figure 26: coordinate -->
    <bladeAttachedType>0</bladeAttachedType> <!-- 0(None), 1(FC IO Blade), 2(EEB),
      4(NAS/LTFS Blade) (i3/i6/i6H only)
      5(Windows Blade) (i3/i6/i6H only) -->
    <license>7</license> <!-- 7(EKM), 11(SNW – i6000 Path Failover/native Storage Networking)
      15(Path Failover - i3/i6/i6H), 16(Advance Path Failover - i3/i6/i6H), 17(SKM –
        i3/i6/i6H) -->
  </settings>
  <barcode>media barcode if drive is loaded</barcode>
  <mediaHomeCoordinate>The slot's SCSI source/home coordinate </ mediaHomeCoordinate> <!-- If no
    media is loaded in the drive this field will be null -->
  <sledSerialNumber>sledSerialNumber</sledSerialNumber>
  <sledBootFirmwareVersion>sledBootFirmwareVersion</sledBootFirmwareVersion>
  </drive>
</ns2:driveList>
```

```

<sledAppFirmwareVersion>sledAppFirmwareVersion</sledAppFirmwareVersion>
<portCount>0</portCount>
<fipsCapable>>false</fipsCapable> <!-- Can drive provide FIPS functionality (Added in version 760(i6000)) -->
<driveNumber>1</driveNumber><!-- Consecutive, top-down drive index within library (version 230(i3/i6/i6H)) -->
</ns2:drive>

```

Figure 34: driveActivityStatistics

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveActivityStatisticsList xmlns:ns2="http://automatedMediaLibrary/">
  <driveActivityStatistics>
    <hourOfDay>16</hourOfDay> <!-- 23 hours ago -->
    <mbRead>0</mbRead>
    <mbWritten>5677</mbWritten>
    <mountCount>2</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>17</hourOfDay> <!-- 22 hours ago -->
    <mbRead>0</mbRead>
    <mbWritten>22000</mbWritten>
    <mountCount>4</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>18</hourOfDay> <!-- 21 hours ago -->
    <mbRead>44567</mbRead>
    <mbWritten>0</mbWritten>
    <mountCount>4</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>19</hourOfDay>
    <mbRead>0</mbRead>
    <mbWritten>0</mbWritten>
    <mountCount>0</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>20</hourOfDay>
    <mbRead>0</mbRead>
    <mbWritten>0</mbWritten>
    <mountCount>0</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>21</hourOfDay>
    <mbRead>0</mbRead>
    <mbWritten>562209</mbWritten>
    <mountCount>5</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>22</hourOfDay>
    <mbRead>0</mbRead>
    <mbWritten>3399</mbWritten>
    <mountCount>3</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>
    <hourOfDay>23</hourOfDay>
    <mbRead>0</mbRead>
    <mbWritten>0</mbWritten>
    <mountCount>0</mountCount>
  </driveActivityStatistics>
  <driveActivityStatistics>

```

```
<hourOfDay>0</hourOfDay>
<mbRead>0</mbRead>
<mbWritten>0</mbWritten>
<mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>1</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>2</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>3</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>4</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>5</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>6</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>7</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>8</hourOfDay>
  <mbRead>344</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>2</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>9</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
```



```

<driveActivityStatistics>
  <hourOfDay>10</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>11</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>12</hourOfDay>
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>13</hourOfDay> <!-- 2 hours ago -->
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>14</hourOfDay> <!-- 1 hour ago -->
  <mbRead>0</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>0</mountCount>
</driveActivityStatistics>
<driveActivityStatistics>
  <hourOfDay>15</hourOfDay> <!-- Current hour of day -->
  <mbRead>23344</mbRead>
  <mbWritten>0</mbWritten>
  <mountCount>4</mountCount>
</driveActivityStatistics>
</ns2:driveActivityStatisticsList>

```

Figure 35: driveCleaningList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:driveCleaningList xmlns:ns2="http://automatedMediaLibrary/">
  <driveCleaning/> <!-- A list of driveCleaning objects -->
</ns2:driveCleaningList>

```

Figure 36: driveCleaning

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:driveCleaning xmlns:ns2="http://automatedMediaLibrary/">
  <dateTime>2001-12-31T12:00:00</dateTime>
  <barcode>barcode</barcode>
  <mediaCoordinate /> <!-- The coordinate where the media came from -->
  <driveSerialNumber>driveSerialNumber</driveSerialNumber>
  <driveCoordinate /> <!-- The coordinate of the drive that was cleaned -->
  <status>status</status> <!-- Result of the cleaning operation -->
  <cleaningType>cleaningType</cleaningType> <!-- Manual or Automatic -->
  <expired>true</expired> <!-- Is the cleaning media expired -->
  <useCount>0</useCount> <!-- How many times this media was used to clean a drive -->
</ns2:driveCleaning>

```

Figure 37: driveCleaningPolicyList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:driveCleaningPolicyList xmlns:ns2="http://automatedMediaLibrary/">
  <driveCleaningPolicy/> <!-- A list of driveCleaningPolicy objects -->
</ns2:driveCleaningPolicyList>
```

Figure 38: driveCleaningPolicy

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:driveCleaningPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partition>partition name</partition> <!-- Partition name to which the policy applies. -->
  <enabled>true</enabled> <!-- Indication whether drives in partition are being automatically cleaned or not -->
  <hostApplicationInitiated>>false</hostApplicationInitiated> <!--Indication if library or host application perform
                                                                    cleaning operation. If true, host performs
                                                                    cleaning and library suppresses drive cleaning
                                                                    request RAS tickets. -->

  <driveCleaning> <!-- Drive specific cleaning parameter options. -->
    <motionTime>100</motionTime> <!-- HP drive option: Specifies tape motion hours to elapse before re-
                                                                    requesting recommended cleaning (0, 100, 200, 400, 800 or 1000) -->
    <mountCount>0</mountCount> <!-- HP EDLM drive option: Mount count to elapse before requesting re-
                                                                    commended EDLM drive cleaning (0, 10 or 25) -->
    <errorCount>1</errorCount> <!--IBM drive option: Library detected error count total to trigger drive cleaning
                                                                    within any 24 hour time period (0,1,2,3) -->
  </driveCleaning>
  <libraryCleaning> <!-- Library configured periodic cleaning interval (currently not supported). -->
    <hour>0</hour>
    <dayOfWeek>0</dayOfWeek>
    <period>1</period>
  </libraryCleaning>
</ns2:driveCleaningPolicy>
```

Figure 39: driveLevelingPolicy

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveLevelingPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partition>LL1</partition>
  <type>2</type> <!-- 0(None), 1(Auto) and 2(Selective)
  <firmwareFile/> <!-- A list of firmwareFile objects, see Figure 100: firmwareFile -->
</ns2:driveLevelingPolicy>
```

Figure 40: driveLogList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveLogList xmlns: ns2="http://automatedMediaLibrary/">
  <driveLog/> <!-- A list of driveLog objects -->
</ns2:driveLogList>
```

Figure 41: driveLog

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveLog xmlns: ns2="http://automatedMediaLibrary/">
  <name>The log file name</name>
  <driveSerialNumber>1013000947</driveSerialNumber> <!-- The physical serial number of the drive or 'N/A' if
unknown. -->
  <created>The date and time the log file was created</created>
  <size>The log file size, in bytes</size>
</ns2:driveLog>
```

Figure 42: drivePortList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:drivePortList xmlns:ns2="http://automatedMediaLibrary/">
  <drivePorts/> <!-- A list of drivePorts objects, see Figure 43: drivePorts -->
</ns2:drivePortList>
```

Figure 43: drivePorts

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:drivePorts xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>serialNumber</serialNumber> <!-- The drives logical serial number -->
  <physicalSerialNumber>serial number</physicalSerialNumber> <!-- The drive's physical serial number -->
  <ports/> <!-- A list of port objects, see Figure 169: port -->
</ns2:drivePorts>
```

Figure 44: driveSerialNumberList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveSerialNumberList xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>F00139603D</serialNumber> <!-- one or more serialNumber elements -->
</ns2:driveSerialNumberList>
```

Figure 45: driveUtilizationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:driveUtilizationList xmlns:ns2="http://automatedMediaLibrary/">
  <driveUtilization/> <!-- A list of driveUtilization objects -->
</ns2:driveUtilizationList>
```

Figure 46: driveUtilization

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:driveUtilization xmlns:ns2="http://automatedMediaLibrary/">
  <coordinate>
    <frame>1</frame>
    <rack>0</rack>
    <section>0</section>
    <column>0</column>
    <row>0</row>
    <type>4</type>
    <relations/>
  </coordinate>
  <driveSerialNumber>the drive's physical serial number</driveSerialNumber>
  <driveLogicalSerialNumber>drive's logical serial number</driveLogicalSerialNumber> <!-- Added in 770(i6000),
  160(i3/i6/i6H)-->

  <partition>partition name</partition>
  <mountTime>2001-12-31 12:00:00</mountTime>
  <unmountTime>2001-12-31 12:02:00</unmountTime>
  <mbRead>0</mbRead>
  <mbWrite>0</mbWrite>
  <barcode>barcode</barcode>
</ns2:driveUtilization>
```

Figure 47: edlmMediaList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmMediaList xmlns:ns2="http://automatedMediaLibrary/">
  <edlmMedia/> <!-- A list of edlmMedia objects -->
```

```
<continueOnError /> <!-- Continue testing media despite media having failed already. -->
</ns2:edlmMediaList>
```

Figure 48: edlmMedia

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmMedia xmlns:ns2="http://automatedMediaLibrary/">
  <barcode>ABC123000L6</barcode>
  <resultId>19</resultId> <!-- The id of the edlmMediaResult object -->
  <coordinate>
    <frame>1</frame>
    <rack>0</rack>
    <section>0</section>
    <column>0</column>
    <row>0</row>
    <type>1</type>
  </coordinate>
  <owner>owner</owner> <!-- Partition owning this media -->
  <testType>0</testType> <!-- 0(None), 1(Quick Scan), 2(Normal Scan), 3(Full Scan) -->
  <testPriority>0</testPriority> <!-- 0(Immediate), 1(High), 2(Medium), 3(Low) -->
  <testState>1</testState> <!-- 0(Unknown), 1(Pending), 2(In Progress), 3(Complete), 4(Stopped),
    5(Paused), 6(Resume) -->
  <testResult>3</testResult> <!-- 0(Not Complete), 1(Good), 2(Unsupported), 3(Suspect), 4(Failed) -->
  <lastTested>2001-12-31T12:00:00</lastTested> <!-- When was media last tested -->
  <supported>true</supported> <!-- Is media supported for EDLM Scan Test with the EDLM drives configured
    for testing. -->
</ns2:edlmMedia>
```

Figure 49: edlmMediaResultList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:edlmMediaResultList xmlns:ns2="http://automatedMediaLibrary/">
  <edlmMediaResult /> <!-- A list of edlmMediaResult objects -->
</ns2:edlmMediaResultList>
```

Figure 50: edlmMediaResult

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmMediaResult xmlns:ns2="http://automatedMediaLibrary/">
  <id>0</id>
  <sessionId>0</sessionId>
  <barcode>barcode</barcode>
  <driveSerialNumber>driveSerialNumber</driveSerialNumber>
  <partition>LL1</partition> <!-- The partition that owns the media, if known. Otherwise 'N/A'. -->
  <mediaSerialNumber>1070748083</mediaSerialNumber>
  <testDate>2001-12-31 12:00:00</testDate>
  <startDate>2001-12-31 11:48:05</startDate>
  <testState>0</testState>
  <!--
0(Unknown) (i6000 Only),
1(Pending),
2(In Progress),
3(Complete),
4(Stopped),
5(Paused),
6(Resume) (i6000 Only)
-->
  <testType>0</testType>
  <!--
```

```

0(None),
1(Quick Scan),
2(Normal Scan),
3(Full Scan)
-->
  <testResult>0</status>
<!--
0(Not Complete) (i6000 Only),
1(Good),
2(Unsupported),
3(Suspect),
4(Failed)
-->
  <staticTestStatus>0</staticTestStatus>
<!--
512(Test Completed),
513(Test Paused),
514(Test Pending),
515(Test Not Run),
516(Test In Progress)
1030(Stopped) (i3/i6/i6H Only)
-->
  <dynamicTestStatus>0</dynamicTestStatus>
<!--
1024(Test Completed),
1025(Test Paused),
1026(Test Pending),
1027(Test Not Run),
1028(Test In Progress),
1029(Test Not Configured),
1030(Test Stopped) (i3/i6/i6H Only)
-->
  <staticTestErrorCode>0</staticTestErrorCode>
<!--
768(Good),
769(N/A),
770(Failed to get CM data),
771(CM Hardware Failure),
772(99% EOL based on thread count),
773(99% EOL based on number of writes),
774(Uncorrected errors),
775(Load failure),
776(Unload failure),
777(Tape was removed),
778(No compatible drive found),
779(Invalid EOD status)
-->
  <dynamicTestErrorCode>0</dynamicTestErrorCode>
<!--
1280(Good),
1281(N/A),
1282(Failed to communicate to IO Blade),
1283(Failed to receive scan data),
1284(Unexpected EOD, Possible corrupt CM),
1285(Unformatted tape),
1286(Failed to read tape data),
1287(Un-recovered read errors on tape),
1289(Corrupt data format),
1296(Tape experienced a mechanical error),

```

```

1297(Tape performance is severely degraded),
1298(Unable to load tape),
1299(Unable to unload tape),
1300(Tape is a cleaning cartridge),
1301(Cartridge memory fault encountered),
1302(Unknown media type detected),
1303(Scan was aborted),
1304(Drive reports no media present),
1305(Media is encrypted),
1312(Media is blank),
1313(Block size exceeds maximum),
1314(Media is a FUP tape),
1315(Failed to read the CM from the drive),
1316(Drive failure encountered while scanning the media),
1317(Drive communication failure) (i3/i6/i6H), Drive is not ready (i6000)),
1318(Test stopped) (i3/i6/i6H), Drive hardware error condition (i6000)),
1319(Uninitialized tape) (i3/i6/i6H), Illegal drive request (i6000)) -->
  <scanTrigger>1</scanTrigger>
<!-- What triggered the scan
0(Unknown),
1(Manual),
2(Import),
3(Interval),
4(Tape Alert),
5(Suspect Count)
-->
</ns2:edlmResult>

```

Figure 51: edlmMediaScanTestList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmMediaScanTestList xmlns:ns2="http://automatedMediaLibrary/">
  <edlmMediaScanTest/> A list of edlmMediaScanTest objects
</ns2: edlmMediaScanTestList>

```

Figure 52: edlmMediaScanTest

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:edlmMediaScanTest xmlns:ns2="http://automatedMediaLibrary/">
  <testDate>2016-05-25 09:53:15 -0600</testDate>
  <barcode>000340L4</barcode>
  <mediaSerialNumber>N/A</mediaSerialNumber>
  <partition>N/A</partition>
  <driveSerialNumber>GB120401FD</driveSerialNumber>
  <scanType>Quick</scanType>
  <result>Untested</result>
  <cmScanStatus>N/A</cmScanStatus>
  <cmScanAnalysis>N/A</cmScanAnalysis>
  <tapeScanStatus>Not Configured</tapeScanStatus>
  <tapeScanAnalysis>N/A</tapeScanAnalysis>
  <scanTrigger>Import</scanTrigger>
</ns2:edlmMediaScanTest>

```

Figure 53: edlmPolicyList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmPolicyList xmlns:ns2="http://automatedMediaLibrary/">
  <edlmPolicy/> A list of edlmPolicy objects
</ns2:edlmPolicyList>

```

Figure 54: edlmPolicy

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>partitionName</partitionName>
  <tapeAlert>
    <scanType>0</scanType> <!-- 0(None), 1(Quick), 2(Normal) and 3(Full) -->
    <count>0</count> <!-- The threshold count on when to do the scan -->
  </tapeAlert>
  <timeInterval> <!-- The interval is in days -->
    <quickScan>0</quickScan>
    <normalScan>0</normalScan>
    <fullScan>0</fullScan>
  </timeInterval>
  <onImport>0</onImport> <!--Perform scan when media is imported 0(No Scan), 1(Quick), 2(Normal) and
3(Full) -->
  <scanPriority>0</scanPriority> <!-- 0(Immediate), 1(High), 2(Medium), 3(Low) -->
  <concurrentScans>0</concurrentScans> <!-- The maximum number of concurrent scans allowed (depends on
the number of EDLM drives configured), 0 for No Limit and then 1 through N where N is the number of EDLM
drives installed -->
  <continueOnError>true</continueOnError>
  <disableRasTicketGeneration>true</disableRasTicketGeneration>
  <externalPolicies>
    <externalApplicationServersName>The StorNext server name</externalApplicationServersName>
    <mediaCopyPolicy>0</mediaCopyPolicy> <!-- 0(Disabled), 1(Suspect Media), 2(Bad Media), 3(Bad or
Suspect Media) -->
    <suspectCountScanType>0</suspectCountScanType> <!-- 0(None), 1(Quick), 2(Normal), 3(Full) -->
  </externalPolicies>
  <relations/>
</ns2:edlmPolicy>
```

Figure 55: edlmSessionList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmSessionList xmlns:ns2="http://automatedMediaLibrary/">
  </edlmSession> <!-- A list of edlmSession objects -->
</ns2:edlmSessionList>
```

Figure 56: edlmSession

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:edlmSession xmlns:ns2="http://automatedMediaLibrary/">
  <id>0</id>
  <startDate>2001-12-31 12:00:00</startDate>
  <endDate>2001-12-31 12:00:00</endDate>
  <state>0</state> <!-- 0(Unknown), 1(Complete), 2(Pending), 4(Paused), 8(In Progress), 16(Stopped) -->
  <goodCount>0</goodCount> <!-- The number of scans in the session that completed with good status -->
  <suspectCount>0</suspectCount> <!-- The number of scans in the session that completed with suspect status -->
  <badCount>0</badCount> <!-- The number of scans in the session that completed with bad status -->
  <notCompleteCount>0</notCompleteCount> <!-- The number of scans in the session that did not complete -->
  <unSupportedCount>0</unSupportedCount> <!-- The number of scans in the session that were not supported -->
  <continueOnError>true</continueOnError> <!--Was the continue on error flag set for this session -->
  <estimatedCompletionTime>34</estimatedCompletionTime> <!-- The estimated time in minutes it will take to
complete the session scan tests (Added in version 760(i6000)) -->
</ns2:edlmSession>
```

Figure 57: ekmMediaStatusList

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<ns2:ekmMediaStatusList xmlns:ns2="http://automatedMediaLibrary/">
  <ekmMediaStatus/> A list of ekmMediaStatus objects
</ns2:ekmMediaStatusList>
```

Figure 58: ekmMediaStatus

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:ekmMediaStatus xmlns:ns2="http://automatedMediaLibrary/">
  <driveSerialNumber>driveSerialNumber</driveSerialNumber>
  <barcode>barcode</barcode>
  <mediaSerialNumber>mediaSerialNumber</mediaSerialNumber>
  <partitionName>partitionName</partitionName>
  <encrypted>true</encrypted>
  <mountTime>2001-12-31T12:00:00</mountTime>
  <unmountTime>2001-12-31T12:00:00</unmountTime>
</ns2:ekmMediaStatus>
```

Figure 59: ekmPartitionActivityList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:ekmPartitionActivityList xmlns:ns2="http://automatedMediaLibrary/">
  <ekmPartitionActivity/> A list of ekmPartitionActivity objects
</ns2:ekmPartitionActivityList>
```

Figure 60: ekmPartitionActivity

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:ekmPartitionActivity xmlns:ns2="http://automatedMediaLibrary/">
  <partition>partition</partition>
  <method>method</method>
  <user>user</user>
  <loginFrom>loginFrom</loginFrom>
  <dateTime>2001-12-31T12:00:00</dateTime>
</ns2:ekmPartitionActivity>
```

Figure 61: ekmServersList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ekmServersList xmlns:ns2="http://automatedMediaLibrary/">
  <ekmServers/> <!-- A list of ekmServers objects -->
</ns2:ekmServersList>
```

Figure 62: ekmServers

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ekmServers xmlns:ns2="http://automatedMediaLibrary/">
  <ekmServerType> <!-- 2(RKM), 4(KMIP), 8(QEKM), 16(SKM), 32(TKLM), 2048(IBM SKLM – Added in
770(i6000))-->
    <!-- Note: RKM is no longer supported, QEKM and TKLM for i6000 only -->
    <server>
      <hostName>10.20.9.18</hostName>
      <port>3801</port>
      <status>Active</status>
    </server>
    <server>
      <hostName>10.20.9.6</hostName>
      <port>3801</port>
      <status>Standby</status>
    </server>
```



```

    <ekmPathDiagnosticsInterval>0-60</ekmPathDiagnosticsInterval> <!-- 0-60 minutes, where 0 means
    disabled -->
    <ssl>>false</ssl>
</ns2:ekmServers>

```

Figure 63: ekmServerTestResultList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:ekmServerTestResultList xmlns:ns2="http://automatedMediaLibrary/">
  </ekmServerTestResult> <!-- A list of ekmServerTestResult objects -->
</ns2:ekmServerTestResultList>

```

Figure 64: ekmServerTestResult

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:ekmServerTestResult xmlns:ns2="http://automatedMediaLibrary/">
  <server>server</server> <!-- The EKM server name/IP -->
  <test> <!-- The list of test objects -->
    <type>1</type> <!-- 1(Ping Test), 2(Path Test), 3(Configure Test) -->
    <result>1</result> <!-- 1(Passed), 2(Failed) -->
  </test>
</ns2:ekmServerTestResult>

```

Figure 65: elementList (ENUM)

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<elementList xmlns:ns2="http://automatedMediaLibrary/">
  <component name="component name">
    <element name="element name"> <!-- One or more elements -->
      <entry key="1" value="Connectivity"/> <!-- One or more key value entry pairs -->
    </element>
  </component>
</elementList>

```

Figure 66: elementList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:elementList xmlns:ns2="http://automatedMediaLibrary/">
  <element/> <!-- A list of element objects -->
</ns2:elementList>

```

Figure 67: element

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:element xmlns:ns2="http://automatedMediaLibrary/">
  <coordinate/> <!-- See Figure 26: coordinate -->
  <address>256</address> <!-- The logical SCSI element address -->
  <status>2</status>
<!--
1 (Not Installed),
2 (Accessible),
3 (Not Accessible)
-->
  <barcode></barcode>
  <owner>Test Partition</owner>
  <configuredType>0</configuredType> <!-- This field is currently not used and should be ignored. -->
  <shared>>true/false</shared> <!-- Deprecated, use ieStatus element instead. -->
  <ieStatus>0</ieStatus>
<!-- This element is not supported on the i6000

```

```
0(None),
1(Shared),
2(System Partition)
-->
</ns2:element>
```

Figure 68: email

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:email xmlns:ns2="http://automatedMediaLibrary/">
  <!-- A list of recipients -->
  <recipient>john.doe@company.com</recipient>
  <recipient>jane.doe@company.com</recipient>
  <comment>Needs your urgent attention</comment>
  </reportCriteria> <!-- Figure 182: reportCriteria -->
</ns2:email>
```

Figure 69: emailServer

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:emailServer xmlns:ns2="http://automatedMediaLibrary/">
  <server>10.20.169.2</server>
  <accountName>john.doe</accountName>
  <accountPassword>secret_password</accountPassword>
  <senderEmailAddress>dvt8@quantum.com</senderEmailAddress>
  <authorize>>true</authorize>
  <testEmailAddress>john.doe@company.com</testEmailAddress>
  <enableTLS>>false</enableTLS> <!-- Enable TLS support, added in versions 775(i6000) and 210(i3/i6/i6H) -->
  <serverPort>25</serverPort> <!-- Email server port number, added in versions 775(i6000) and 210(i3/i6/i6H) -->
</ns2:emailServer>
```

Figure 70: emailRecipientList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:emailRecipientList xmlns:ns2="http://automatedMediaLibrary/">
  <emailRecipient>
    <id>1</id> <!-- Automatically generated by the library -->
    <address>john.doe@company.com</address> <!-- e-mail address -->
  </emailRecipient>
</ns2:emailRecipientList>
```

Figure 71: emailRecipient

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:emailRecipient xmlns:ns2="http://automatedMediaLibrary/">
  <id>1</id> <!-- Automatically generated by the library -->
  <address>john.doe@company.com</address> <!-- e-mail address -->
</ns2:emailRecipient>
```

Figure 72: emmc

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:emmc xmlns:ns2="http://automatedMediaLibrary/">
  <sectorUsage>Good</sectorUsage> <!-- Good, Warning, Alert and Degraded -->
  <spareBlocksUsage>Good</spareBlocksUsage> <!-- Good, Warning and Alert -->
</ns2:emmc>
```

Figure 73: entryList (ENUM)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entryList xmlns:ns2="http://automatedMediaLibrary/">
  <component name="component name">
    <element name="element name">
      <entry key="1" value="SCSI"/> <!-- One or more key value entry pairs -->
    </element>
  </component>
</entryList>
```

Figure 74: environmentList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<environmentList xmlns:ns2="http://automatedMediaLibrary/">
  <environment/> <!-- A list of environment objects -->
</environmentList>
```

Figure 75: environment

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<environment xmlns:ns2="http://automatedMediaLibrary/">
  <dateTime>2018-03-25 19:07:44</dateTime>
  <temperature>25</temperature> <!-- Temperature in degrees Celsius -->
  <humidity>22</humidity> <!-- Humidity as a percentage -->
</environment>
```

Figure 76: ethernetExpansionBladeList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ethernetExpansionBladeList xmlns:ns2="http://automatedMediaLibrary/">
  <ethernetExpansionBlade/> A list of ethernetExpansionBlade objects, see Figure 77: ethernetExpansionBlade
</ns2:ethernetExpansionBladeList>
```

Figure 77: ethernetExpansionBlade

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ethernetExpansionBlade xmlns:ns2="http://automatedMediaLibrary/">
  <blade/> See Figure 13: blade
  <ethernetExpansionBladePort/> A list of 6 ethernetExpansionBladePort objects, see Figure 78:
ethernetExpansionBladePort
</ns2:ethernetExpansionBlade>
```

Figure 78: ethernetExpansionBladePort

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ethernetExpansionBladePort xmlns:ns2="http://automatedMediaLibrary/">
  <number>0</number>
  <linkStatus>linkStatus</linkStatus>
  <speed>0</speed>
  <duplex>duplex</duplex>
</ns2:ethernetExpansionBladePort>
```

Figure 79: externalApplicationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:externalApplicationList xmlns:ns2="http://automatedMediaLibrary/">
  </externalApplication> A list of externalApplication objects.
</ns2:externalApplicationList>
```

Figure 80: externalApplication

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:externalApplication xmlns:ns2="http://automatedMediaLibrary/">
  <name>snapi-2.0.1</name>
  <version>110i.EE002</version>
  <description>StorNext Plugin (3.5 to 4.1)</description>
</ns2:externalApplication>
```

Figure 81: externalApplicationServersList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:externalApplicationServersList xmlns:ns2="http://automatedMediaLibrary/">
  </externalApplicationServers> A list of externalApplicationServers objects
</ns2:externalApplicationServersList>
```

Figure 82: externalApplicationServers

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:externalApplicationServers xmlns:ns2="http://automatedMediaLibrary/">
  <name>StorNext</name>
  <server>
    <name>10.20.169.88</name>
    <port>61776</port>
  </server>
  <server>
    <name>10.20.9.18</name>
    <port>61776</port>
  </server>
  <externalApplicationName>snappy-2.0.1</externalApplicationName>
  <username>>false</username> <!-- The username to use with StorNext Web Services (Added in version
760(i6000), i3/i6/i6H)-->
  <password>>false</password> <!-- The password to use with StorNext Web Services (Added in version
760(i6000), i3/i6/i6H)-->
  <protocol>0</protocol> <!-- This indicates which protocol to use for Web Services communications, (added
in version 760(i6000), i3/i6/i6H)-->
  <!--
0(None),
1(HTTP),
2(HTTPS)
-->
</ns2:externalApplicationServersList>
```

Figure 83: externalApplicationServerTestResultList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:externalApplicationServerTestResultList xmlns:ns2="http://automatedMediaLibrary/">
  < externalApplicationServerTestResult/> <!-- A list of externalApplicationServerTestResult objects -->
</ns2:externalApplicationServerTestResultList>
```

Figure 84: externalApplicationServerTestResult

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:externalApplicationServerTestResult xmlns:ns2="http://automatedMediaLibrary/">
  <server>server</server> <!-- The external application server name/IP -->
  <test> <!-- The list of test objects -->
    <type>1</type> <!-- 1(Ping Test), 2(Configuration Path Test) -->
    <result>1</result> <!-- 1(Passed), 2(Failed) -->
    <details>4</details> <!-- Bit mask with the following values
```

```

0 (Good)
1 (Server Not Reachable)
2 (Web Server Connection Refused)
4 (Web Services Disabled)
8 (Authentication Failed)
16 (System Offline)
32 (DSM Offline)
64 (MSM Offline)
128 (TSM Offline)
256 (Database Offline)
512 (HTTP Protocol Not Enabled)
1024 (Unknown Error)
-->
</test>
</ns2:externalApplicationServerTestResult>

```

Figure 85: fcBladeList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladeList xmlns: ns2="http://automatedMediaLibrary/">
  <fcBlade/> A list of fcBlade objects, see Figure 86: fcBlade
</ns2:fcBladeList>

```

Figure 86: fcBlade

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBlade xmlns: ns2="http://automatedMediaLibrary/">
  <blade/> See Figure 13: blade
  <wwnn>wwnn</wwnn>
  <type>1</type> <!-- 0(Unknown), 1(6404), 2(7404) -->
  <status>1</status> <!-- 1(Unknown), 3(OK), 4(Warning), 5(Failed) Updated/Corrected in 765(i6000)-->
  <hostPortFailover>true</hostPortFailover>
  <fcBladePort/> A list of 6 fcBladePort objects, see Figure 94: fcBladePort
  <host/> A list of host objects, see Figure 105: host
</ns2:fcBlade>

```

Figure 87: fcBladeHostsList

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladeHostsList xmlns:ns2="http://automatedMediaLibrary/">
  <fcBladeHosts/> <!-- A list of fcBladeHosts objects -->
</ns2:fcBladeHostsList>

```

Figure 88: fcBladeHosts

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladeHosts xmlns:ns2="http://automatedMediaLibrary/">
  <blade/> <!-- One blade object, See Figure 13: blade for details -->
  <host/> <!-- 0-n host objects, See Figure 105: host for details -->
</ns2:fcBladeHosts>

```

Figure 89: fcBladeZoning

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladeZoning xmlns:ns2="http://automatedMediaLibrary/">
  <bladeSerialNumber>AMQ002639-0009</bladeSerialNumber>

```

```

<targetPort>
  <portNumber>1</portNumber>
  <initiatorPort>
    <portNumber>3</portNumber>
    <accessEnabled>true</accessEnabled>
  </initiatorPort>
  <initiatorPort>
    <portNumber>4</portNumber>
    <accessEnabled>true</accessEnabled>
  </initiatorPort>
  <initiatorPort>
    <portNumber>5</portNumber>
    <accessEnabled>>false</accessEnabled>
  </initiatorPort>
  <initiatorPort>
    <portNumber>6</portNumber>
    <accessEnabled>true</accessEnabled>
  </initiatorPort>
</targetPort>
<targetPort>
  <portNumber>2</portNumber>
  <initiatorPort>
    <portNumber>3</portNumber>
    <accessEnabled>true</accessEnabled>
  </initiatorPort>
  <initiatorPort>
    <portNumber>4</portNumber>
    <accessEnabled>true</accessEnabled>
  </initiatorPort>
  <initiatorPort>
    <portNumber>5</portNumber>
    <accessEnabled>>false</accessEnabled>
  </initiatorPort>
  <initiatorPort>
    <portNumber>6</portNumber>
    <accessEnabled>true</accessEnabled>
  </initiatorPort>
</targetPort>
</ns2:fcBladeZoning>

```

Figure 90: fcHostPortFailoverList

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcHostPortFailoverList xmlns:ns2="http://automatedMediaLibrary/">
  </fcHostPortFailover> <!-- A list of fcHostPortFailover objects, one for each blade configured. -->
</ns2:fcHostPortFailoverList>

```

Figure 91: fcHostPortFailover

```

<!-- Added in version 760(i6000) -->
<fcHostPortFailover>
  <bladeSerialNumber>AMQ002639-0009</bladeSerialNumber>
  <configuration>
    <enabled>true</enabled> <!-- Is host port failover enabled -->
    <linkDownDelayTime>3</linkDownDelayTime> <!-- Time in seconds before link down status applies,
    0 - 2147483648 -->
    <primaryPort>1</primaryPort> <!-- 1 or 2 -->
  </configuration>

```

```

    <port> <!-- If host port failover is enabled, 2 port objects are returned, otherwise no port objects exist -->
      <number>1</number> <!-- The host (target) port number, can be 1 or 2 -->
      <mode>0</mode> <!-- 0(Online), 1(Offline) or 2(N/A) -->
      <failureType>0</failureType> <!-- 0(None), 1(Link Down) or 2(Link Error) -->
      <intervention>false</intervention> <!-- Whether port needs intervention to be re-enabled online -->
    </port>
  </fcHostPortFailover>

```

Figure 92: fcLunMapping

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcLunMapping
  xmlns:ns2="http://automatedMediaLibrary/"
  <fcBladeHost/> <!-- See Figure 88: fcBladeHost -->
  <mapping> <!-- 0 or more mapping elements -->
    <deviceName>PartitionTest</deviceName>
    <deviceSerialNumber>273190049_LL2</deviceSerialNumber>
    <deviceType>2</deviceType>
  <!--
  0(Unknown),
  1(Drive),
  2(Partition)
  -->
    <internalLun>4</internalLun>
  <!-- The LUN number of the device that is used internally by the blade, this is not user configurable. -->
    <externalLun>1</externalLun>
  <!-- The LUN number that is used by an external host to access the device, this number is user configurable. The
  valid LUN number range is 0 to 255 -->
    </mapping>
  </ns2:fcLunMapping>

```

Figure 93: fcBladePortList

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladePortList xmlns:ns2="http://automatedMediaLibrary/"
  <bladeSerialNumber>AMQ002639-0009</ bladeSerialNumber >
  <fcBladePort/> <!-- A list (6) of fcBladePort objects -->
</ns2:fcBladePortList>

```

Figure 94: fcBladePort

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:fcBladePort xmlns:ns2="http://automatedMediaLibrary/"
  <wwpn>wwpn</wwpn>
  <number>1</number>
    <!--1 through 6, where ports 1 and 2 are target ports which can only be connected to a host or switch
    and 3,4,5 and 6 are initiator ports and can only be connected to drives. -->
  <softLoop>true</softLoop> <!-- true or false, if set to true the loop id will be automatically configured -->
  <loopId>0</loopId> <!-- 0 – 125, if softLoop is set to true, this value is ignored -->
  <mode>0</mode>
    <!-- 1(Private Target),
    2(Private Initiator),
    3(Private Target and Initiator),
    17(Public Target),
    18(Public Initiator),
    19(Public Target and Initiator) -->

```

```

<topology>0</topology> <!-- 0(Loop), 1(Point to Point), 2(Loop Preferred) -->
<autoSpeed>>false</autoSpeed> <!-- True or False -->
<speed>0</speed> <!-- 0(Auto), 1, 2 or 4 -->
<frameSize>512</frameSize> <!-- 512, 1024 or 2048 -->
<status>0</status>
    <!-- 0(Configure Wait),
           1(Loop Initiate),
           2(Login),
           3(Ready),
           4(Lost Sync),
           5(Error),
           6(Reinitiate),
           7(Non Part),
           8(Failed) -->
</ns2:fcBladePort>

```

Figure 95: firmwareList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareList xmlns:ns2="http://automatedMediaLibrary/">
  <lastInstallDate>2014-06-02 09:57:50 -0600</lastInstallDate>
  <firmware/> <!-- A list of firmware objects -->
</ns2:firmwareList>

```

Figure 96: firmware

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmware xmlns:ns2="http://automatedMediaLibrary/">
  <component>Current</component> <!-- Values are 'Current' (i6000 only), 'Rollback' and 'Uploaded' -->
  <version>665H.TS07401</version> <!-- The firmware/software version -->
  <signingStatus>Signed by Production Certificate</signingStatus>
</ns2:firmware>

```

Figure 97: firmwareFileList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:firmwareFileList xmlns:ns2="http://automatedMediaLibrary/">
  <firmwareFile/> A list of firmwareFile objects, see Figure 100: firmwareFile
</ns2:firmwareFileList>

```

Figure 98: firmwareUpdateList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareUpdateList xmlns:ns2="http://automatedMediaLibrary/">
  </firmwareUpdate> A list of firmwareUpdate objects.
</ns2:firmwareUpdateList>

```

Figure 99: firmwareUpdate

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareUpdate xmlns:ns2="http://automatedMediaLibrary/">
  <serialNumber>HU19487U51</serialNumber>
  </firmwareFile> A firmwareFile object
</ns2:firmwareUpdate>

```

Figure 100: firmwareFile

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:firmwareFile xmlns:ns2="http://automatedMediaLibrary/">

```



```

<name>name</name>
<version>version</version>
<vendor>vendor</vendor> <!-- HP or IBM -->
<type>type</type> <!-- LTO2, LTO3, LTO4, LTO5, LTO6, LTO7, LTO8, or LTO9 -->
<formFactor>HH or FH</formFactor> <!-- HH (Half Height) or FH (Full Height) -->
<interface>Fibre</interface> <!-- Fibre or SAS -->
<ibmFipsImage>false</ibmFipsImage> <!-- Is this a FIPS image (Added in version 760(i6000)) -->
</ns2:firmwareFile>

```

Figure 101: firmwareStatusList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareStatusList xmlns:ns2="http://automatedMediaLibrary/">
  <updateState>2</updateState> <!-- 0(None), 1(Pending), 2(In Progress), 3(Canceling), 4(Canceled),
5(Success), 6(Failure) -->
  <firmwareStatus/> A list of firmwareStatus objects, see Figure 102: firmwareStatus
</ns2:firmwareStatusList>

```

Figure 102: firmwareStatus

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:firmwareStatus xmlns:ns2="http://automatedMediaLibrary/">
  <component>Drive SN: HU19487U51</component> <!-- drive or device component identification -->
  <status>In Progress</status> <!-- status information, i.e. Success, Pending, In Progress, Failed -->
  <percentComplete>50%</percentComplete> <!-- update completion percentage, i.e. 15% or 100% -->
</ns2:firmwareStatus>

```

Figure 103: heartbeatNotification

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:heartbeatNotification xmlns:ns2="http://automatedMediaLibrary/">
  <id>1</id>
  <interval>60</interval> <!-- Interval in minutes -->
  <emailRecipientList/> <!-- notification recipients, See Figure 70: emailRecipientList -->
</ns2:heartbeatNotification>

```

Figure 104: hostList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:hostList xmlns:ns2="http://automatedMediaLibrary/">
  <host/> A list of host objects, see Figure 105: host
</ns2:hostList>

```

Figure 105: host

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:host xmlns:ns2="http://automatedMediaLibrary/">
  <name>Test</name> <!-- The host name cannot be more than 32 characters -->
  <type>2</type>
<!--
0(Unknown),
1(WINDOWS),
2(AIX),
3(IRIX),
4(SOLARIS),
5(HP-UX),
6(NETWARE),
7(GATEWAY),
8(SWITCH),

```

```

9(GENERIC),
10(AS400),
11(UNISYS),
12(LINUX),
13(FCR-2),
14(PV-136T-FC),
15(HP-V2) -->
    <mode>0</mode>
<!--
0(Offline),
1(Online)
-->
    <WWPN>12345678:ABCDABCD</WWPN>
<!-- The World Wide Port Name of the HBA on the host -->
    <port>Port Number</port>
<!-- The port number of HBA on the host, this will default to 0. Used by Scalar i6000 FC IO Blade hosts. -->
</ns2:host>

```

Figure 106: ieSlots

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:ieSlots xmlns:ns2="http://automatedMediaLibrary/">
    <slotCount>0</slotCount> <!-- The number of ie slots configured -->
    <assignmentMode>1</assignmentMode> <!-- 1(Manual), 2(Automatic) -->
</ns2:ieSlots>

```

Figure 107: ieStationList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ieStationList xmlns:ns2="http://automatedMediaLibrary/">
    <ieStation/> A list of ieStation objects, see Figure 108: ieStation
</ns2:ieStation>

```

Figure 108: ieStation

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ieStation xmlns:ns2="http://automatedMediaLibrary/">
    <number>0</number>
    <coordinate/> See Figure 26: coordinate
    <slotCount>0</slotCount>
    <opened>false</opened>
    <status>1</status>          <!-- 1(locked), 2(unlocked) -->
    <mode>0</mode>            <!-- 1(Online), 2(Offline) -->
    <state>1</state>          <!-- 1(Varied On), 2(Varied Off) -->
</ns2:ieStation>

```

Figure 109: internalNetwork

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:internalNetwork xmlns:ns2="http://automatedMediaLibrary/">
    <current>192.19.240.0</current>
    <options>10.247.240.0</options> <!-- One or more options elements. For I3/i6/i6H the available options are
10.247.240.0, 172.29.240.0, 192.168.240.0, 192.19.240.0 -->
</ns2:internalNetwork>

```

Figure 110: inventoryTask

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:inventoryTask xmlns:ns2="http://automatedMediaLibrary/">

```

```

<partitionName>LL1</partitionName> <!-- The partition name or NULL for physical library inventory -->
<offline>true</offline> <!-- Take the partition/physical library offline while doing the inventory. You should almost
always set this to true -->
<startElement>2048</startElement>
<elementCount>2058</elementCount>
</ns2:inventoryTask>

```

Figure 111: keySetList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:keySetList xmlns:ns2="http://automatedMediaLibrary/">
  <keyset/> <!-- A list of keyset objects.-->
</ns2:keySetList>

```

Figure 112: keySet

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:keySet xmlns:ns2="http://automatedMediaLibrary/">
  <name>KEY-GROUP1</name> <!-- The name of the keyset group -->
  <keyCount>LL1</keyCount> <!-- The number of keys in the keyset group -->
  <status>1</status>
<!--
0 (New Group),
1 (Generating Keys),
2 (Needs Backup),
3 (Ready),
4 (Missing),
5 (Error)
  <availableSequence>0</availableSequence> <!-- Currently not used -->
-->
</ns2:keySet>

```

Figure 113: latestFirmwareVersion

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:latestFirmwareVersion xmlns:ns2="http://automatedMediaLibrary/">
  <version>770G.GS15500</version> <!-- The latest firmware version -->
</ns2:latestFirmwareVersion>

```

Figure 114: ldap

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ldap
  xmlns:ns2="http://automatedMediaLibrary/"
  <enabled>true</enabled>
  <primaryServer>10.20.170.3</primaryServer>
  <alternateServer>10.20.170.4</alternateServer>
  <serverPort>389</serverPort> <!-- 389 (Standard port), 636 (Secure port) -->
  <secureMode>1</secureMode> <!-- 1(LDAP standard), 2(LDAPS, TLS connection), 3(StartTLS, start a TLS
session within an already established LDAP connection -->
  <searchUser>cn=admin,dc=hyjal,dc=com</searchUser>
  <searchUserPassword></searchUserPassword>
  <usersContext>cn=Users,dc=hyjal,dc=com</usersContext>
  <groupContext>cn=Users,dc=hyjal,dc=com</groupContext>
  <libraryAccessGroupsUser>cn=people,dc=hyjal,dc=com</libraryAccessGroupsUser>
  <libraryAccessGroupsAdmin>cn=admins,dc=hyjal,dc=com</libraryAccessGroupsAdmin>
  <!-- The following are used to support ldap-Kerberos and will only be supported on Scalar i3/i6/i6H -->

```

```

<realm>string</realm>
<keyDistributionCenter>string</keyDistributionCenter>
<domainMapping>string</domainMapping>
<keytabFile>
  <name>keyTabFile</name> <!--The name of the file -->
  <date>yyyy-dd-mm hh:mm:ss +nnnn</date> <!--The date and time the file was uploaded -->
</keytabFile>
</ns2:ldap>

```

Figure 115: ldapTest

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ldapTest xmlns:ns2="http://automatedMediaLibrary/">
  <user>JIM</user> <!-- The LDAP user -->
  <password>*****</password> <!-- The LDAP user password -->
  </ldap> <!-- The ldap object to test, Figure 114: ldap -->
</ns2:ldapTest>

```

Figure 116: libraryControlBladeList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:libraryControlBladeList xmlns: ns2="http://automatedMediaLibrary/">
  <libraryControlBlade/> A list of libraryControlBlade objects
</ns2:libraryControlBladeList>

```

Figure 117: libraryControlBlade

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2: libraryControlBlade xmlns: ns2="http://automatedMediaLibrary/">
  <blade/> See Figure 13: blade
  <fcBladePort/> A list of fcBladePort objects, see Figure 94: fcBladePort
</ns2: libraryControlBlade>

```

Figure 118: libraryDiagnosticTestList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:libraryDiagnosticTestList xmlns:ns2="http://automatedMediaLibrary/">
  <libraryDiagnosticTest /> <!-- A list of libraryDiagnosticTest objects -->
</ns2:libraryDiagnosticTestList>

```

Figure 119: libraryDiagnosticTest

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:libraryDiagnosticTest xmlns:ns2="http://automatedMediaLibrary/">
  <name>Robot Test</name>
  <type>16</type>
</ns2:libraryDiagnosticTest>

```

Figure 120: libraryDiagnosticTestResult

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:libraryDiagnosticTestResult xmlns:ns2="http://automatedMediaLibrary/">
  <testType>12</testType>
  <startTime>2001-12-31T12:00:00</startTime>
  <endTime>2001-12-31T12:00:00</endTime>
  <state>2</state> <!-- 1(In Progress), 2(Pending), 3(Stopped), 4(Terminated), 5(Complete) -->
  <!-- A List of results for the given test type -->
  <result>
    <type>16</type> <!-- The test type, can be different from libraryDiagnosticTestResult.testType for full IVT -->

```

```

<element>1,1,1,1,1</element> <!-- I3/i6/i6H only -->
<description>ALIGNMENT MAGAZINE PASSED</description>
<status>1<status> <!--0(Unknown), 1(Passed), 2(Warning), 3(Invalid), 4(Incomplete), 5(Failed), 6(Skipped) -
-->
</result>
</ns2:libraryDiagnosticTestResult>

```

Figure 121: libraryDiagnosticTestSessionList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:libraryDiagnosticTestSessionList xmlns:ns2="http://automatedMediaLibrary/">
  <libraryDiagnosticTestSession /> <!-- A list of libraryDiagnosticTestSession objects -->
</ns2:libraryDiagnosticTestSessionList>

```

Figure 122: libraryDiagnosticTestSession

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:libraryDiagnosticTestSession xmlns:ns2="http://automatedMediaLibrary/">
  <taskId>0</taskId>
  <startTime>2001-12-31T12:00:00</startTime>
  <endTime>2001-12-31T12:00:00</endTime>
  <state>5<state> <!-- 1(In Progress), 2(Pending), 3(Stopped), 4(Terminated), 5(Complete) -->
  <libraryDiagnosticTestResult /> <!-- A list of libraryDiagnosticTestResult objects -->
</ns2:libraryDiagnosticTestSession>

```

Figure 123: libraryDiagnosticTestTask

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:libraryDiagnosticTestTask xmlns:ns2="http://automatedMediaLibrary/">
  <testType>12</testType>
  <!--
12 (VT, Start Test Diagnostic Session (i6000))
13 (VT, Finish Test Diagnostic Session (i6000))
14 (VT, Robot Accessor Test (i6000))
15 (VT, Robot Picker Test (i6000))
16 (VT, Robot Assembly Test (i6000 and I3/i6/i6H))
17 (VT, IE Station Assembly Test (i6000))
18 (VT, Tower Assembly Test (i6000))
19 (VT, Tower Scanner Test (i6000))
20 (VT, Robot Scanner Test (i6000))
21 (VT, Library Get Put Test (i6000))
22 (VT, Drive Assembly Test (i6000 and I3/i6/i6H))
23 (VT, Magazine Test (I3/i6/i6H))
24 (IVT, Full Installation Verification Test (i6000 and I3/i6/i6H))
27 (VT, Library Alignment Test (i6000))
28 (VT, Barcode Label Test (i6000)) (Added in version 760(i6000))
29 (VT, Module Assembly Test (i3/i6/i6H)) (Added in version 210(i3/i6/i6H))
51 (Teach Configure/Calibrate (i6000)) (Added in version 760(i6000))
-->
  <libraryTestParameters>
    <robot>0</robot> <!-- 0(Left), 1(Right) and 2(Both) -->
    <startModule>0</startModule>
    <endModule>0</endModule>
    <startRack>0</startRack>
    <endRack>0</endRack>
    <slotLocation> <!-- Used by picker assembly test -->
      <coordinate/>
    </slotLocation>
    <mediaLocation> <!-- A list of scratch tapes, used by robot position test, picker assembly, IE assembly,

```

```

GET/PUT and drive assembly tests. -->
  <coordinate/>
</mediaLocation>
<startLocation> <!--Start coordinate -->
  <coordinate/>
</startLocation>
<endLocation> <!--End coordinate -->
  <coordinate/>
</endLocation>
<partialIvt>true</partialIvt> <! Indicates whether this is a partial IVT, this requires startModule, endModule,
startRack and endRack. (i6000 only) -->
</libraryTestParameters>
</ns2:libraryDiagnosticTestTask>

```

Figure 124: libraryStatus

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:libraryStatus xmlns:ns2="http://automatedMediaLibrary/">
  <state>1</state> <!--0(Unknown), 1(Ready), 2(Not Ready), 3(Becoming Ready) -->
  <mode>1</mode> <!-- 1(Online) 2(Offline) -->
  <ras>
    <status> <!-- See Figure 171: RASGroupStatus -->
      <group>0</group>
      <status>4</status>
    </status>
    <openedTickets>5</openedTickets>
  </ras>
  <partition> <!-- 0 or n partition entries -->
    <name>AV</name>
    <mode>1</mode> <!-- 1(Online) 2(Offline) -->
    <type>1</type> <!-- 1(Standard), 2(EDLM), 3(AMP), 4(Active Vault) -->
  </ partition >
  <drive> <!-- 0 or n drive entries -->
    <logicalSerialNumber>drive logical serial number</ logicalSerialNumber>
    <mode>1</mode> <!-- 1(Online) 2(Offline) -->
    <state>2</state> <!-- 1(Varied On), 2(Varied Off) and 3(Pending/Initializing) -->
  </drive>
  <robot> <!-- 0 or n robot entries -->
    <serialNumber>The robot serial number</serialNumber>
    <location>Right or Left robot</location> <!-- Left or Right -->
    <status>The robot status</status> <!-- 0(Unknown), 1(Good/Operational), 2(Not Installed), 3(Initializing),
      4(Failed), 5(N/A) , 6(Active Media Present (770(i6000))), 7(Failed
      Media Present (770(i6000))), 8(Inoperable(220(i3/i6/i6H), 778(i6000))) -->
    <state>2</state> <!-- 1(Varied On), 2(Varied Off) and 3(Pending/Initializing) -->
  </robot>
  <tower> <!-- 0 or n tower entries -->
    <frameNumber>The frame number the tower is in</frameNumber>
    <status>The tower status</status> <!--0(Unknown), 1(Not Present), 2(Failed), 3(Not Ready), 4(Initializing),
5(Ready/Operational)
    <state>2</state> <!-- 1(Varied On), 2(Varied Off) and 3(Pending/Initializing) -->
    <mode>1</mode> <!-- 1(Online) 2(Offline) -->
  </tower>
  <systemStatus>0</systemStatus>
<!--
0 (Unknown)
1(OK)
2 (Offline Devices)
3 (Not Ready Devices)
-->

```

```

<saveConfigurationRequired>true</saveConfigurationRequired> <!-- Was there a library configuration change
made that requires a new rescue image to be generated. -->
<time>2014-06-27 11:00:15 -0600</time> <!-- The current time on the library. -->
<timeZoneOffset> Returns the offset, measured in minutes, for the local time zone relative to
UTC</timeZoneOffset>
<timeSinceEPOC>1410958379212</timeSinceEPOC> <!-- Returns the number of milliseconds elapsed
since January 1, 1970 -->
<snmpStarted>true</snmpStarted> <!-- This element is used on the i6000 to indicate if the SNMP daemon is
running when the LMC server starts up. -->
</ns2:libraryStatus>

```

Figure 125: licenseList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:licenseList xmlns:ns2="http://automatedMediaLibrary/">
  <license/> <!-- A list of license objects. -->
</ns2:licenseList>

```

Figure 126: license

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:license xmlns:ns2="http://automatedMediaLibrary/">
  <feature>The name of the feature</feature> <!-- This element is used to install a new license key (POST
request) and it also lists the license feature names (GET request), see type element below for the list of valid
license names -->
  <quantity>1</quantity> <!-- Some licenses are controlled by a number, for instance COD, the rest will be 1
(installed) or 0 if not installed -->
  <description>6 Drives</description>
  <expiration>Permanent</expiration> <!-- "Active", 'Permanent', "Expired", "N/A" or 'Month Day, Year'
(example, Jan 12, 2015) -->
  <daysRemaining>25</daysRemaining> <!-- The number of days before the license will expire. Added in
770(i6000) and 200(i3/i6/i6H) -->
  <installed>true</installed> <!-- Is the license installed -->
  <type> License type</type>
<!--
2(Advanced Reporting),
3(Active Vault),
4(Capacity On Demand),
6(Extended Data Lifecycle Management),
7(Encryption Key Management),
8(Partition),
9(Partition Utilization),
11(Path Failover/Native Storage Networking (SNW)),
13(Service Level (i3/i6/i6H Only))
15(Path Failover (i3/i6/i6H Only))
16(Advanced Path Failover (i3/i6/i6H Only))
17(Scalar Key Manager SKM (i3/i6/i6H Only))
-->
  <usedQuantity>2</usedQuantity> <!-- This element only applies to the following license type: Capacity on
Demand, Partition, Encryption Key Management and Path Failover/Native Storage Networking -->
</license>
</ns2:license>

```

Figure 127: loginActivityList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:loginActivityList xmlns:ns2="http://automatedMediaLibrary/">
  <loginActivity /> A list of loginActivity objects
</ns2:loginActivity List>

```

Figure 128: loginActivity

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:loginActivity xmlns:ns2="http://automatedMediaLibrary/">
  <user>admin</user>
  <role>0</role> <!-- 0(Admin User), 1(Standard User), 2(Service User), 3(Guest User) -->
  <sessionId>1</sessionId>
  <command>Login</command> <!-- The command that was executed i.e. login, logout, create partition,
                               etc... -->
  <loginFrom>10.20.9.68</loginFrom>
  <time>2014-06-26 15:35:31 -0600</time>
  <description>More details of the command that was run</description>
</ns2:loginActivity>
```

Figure 129: ItfsBladeList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ItfsBladeList xmlns:ns2="http://automatedMediaLibrary/">
  <ItfsBlade/> <!-- A list of ItfsBlade objects -->
</ns2:ItfsBladeList>
```

Figure 130: ItfsBlade

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ItfsBlade xmlns:ns2="http://automatedMediaLibrary/">
  <blade/> <!-- See Figure 13: blade -->
  <ipAddress>10.60.166.130</ipAddress>
  <partition>Partition Name</partition>
  <baseVersion>The blades base firmware version</baseVersion>
  <mode>1</mode>
  <!--
0(Unknown)
1(Online)
2(Offline)
-->
  <state>1</state>
  <!--
0(Unknown)
1(Not Ready)
2(Becoming Ready)
3(Ready)
-->
  <status>1</status>
  <!--
0(Unknown)
1(Good/Operational)
2(Invalid)
3(Missing)
4(Initializing)
-->
</ns2:ItfsBlade>
```

Figure 131: LUIAccess

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:LUIAccess xmlns:ns2="http://automatedMediaLibrary/">
  <mode>1</mode> <!-- 1(Open), 2(Login required), 3(PIN Required) -->
  <pin>1234</pin> <!-- 4-digit string -->
</ns2:LUIAccess>
```


Figure 132: magazineList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:magazineList xmlns:ns2="http://automatedMediaLibrary/">
  <magazine /> <!-- A list magazine objects -->
</ns2:magazineList>
```

Figure 133: magazine

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:magazine xmlns:ns2="http://automatedMediaLibrary/">
  <coordinate /> <!-- See Figure 26: coordinate -->
  <storageSlotCount>0</storageSlotCount> <!-- The number of storage slots in the magazine -->
  <ieSlotCount>0</ieSlotCount> <!-- The number of ie slots in the magazine -->
  <mediaInStorageCount>2</mediaInStorageCount>
  <mediaInIECount>0</mediaInIECount>
  <status>1</status> <!-- 1(Good/Operational), 2(Ejected) -->
  <state>1</state> <!-- 1(Ready), 2(Not Ready) -->
  <enabledRelease>true</enabledRelease><!-- Indicates if magazine may be released. Added in 220(i3/i6/i6H) -->
  <removable>true</removable><!-- Magazine is capable of being ejected. Added in version 230(i3/i6/i6H) -->
</ns2:magazine>
```

Figure 134: mediaList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:mediaList xmlns:ns2="http://automatedMediaLibrary/">
  <media/> A list of media objects, see Figure 135: media
</ns2:mediaList>
```

Figure 135: media

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:media xmlns:ns2="http://automatedMediaLibrary/">
  <barcode>barcode</barcode>
  <mediaType>0</mediaType>
<!--
2(LTO1),
3(LTO2),
4(LTO3),
5(LTO4),
6(LTO5),
7(LTO6),
8(LTO7),
9(LTO8),
10(LTO9),
20(Cleaning)
-->
  <cartridgeType>0</cartridgeType>
<!--
0(Data),
1(Cleaning),
2(FUP),
3(Diagnostic)
This element is not supported on the i6000
-->
  <currentOwner>N/A</currentOwner>
  <previousOwner>N/A</previousOwner>
  <encryption>Unknown</encryption>
<!--
```

Unknown,
Encrypted,
Not Encrypted

-->

```
<coordinate/> See Figure 26: coordinate
<shared>true/false</shared> <!--Deprecated, use ieStatus element instead. -->
<ieStatus>0</ieStatus>
```

<!--

0(None),
1(Shared),
2(System Partition)

This element is not supported on the i6000

-->

```
<elementAddress>4096</elementAddress> <!-- The SCSI logical element address of where the media is
located -->
```

```
<accessible>false</accessible> <!-- Is the media currently accessible (media located in a varied off tower would
not be accessible (false)). Added in versions 751(i6000) and 166(i3/i6/i6H). -->
```

```
<isWorm>false</isWorm> <!--Indication whether media is WORM -->
```

```
</ns2:media>
```

Figure 136: mediaSecurityEventList

```
<?xml version='1.0' encoding='UTF-8'?>
<ns2:mediaSecurityEventList xmlns:ns2="http://automatedMediaLibrary/">
  < mediaSecurityEvent/> A list of mediaSecurityEvent objects
</ns2:mediaSecurityEventList>
```

Figure 137: mediaSecurityEvent

```
<?xml version='1.0' encoding='UTF-8'?>
<ns2:mediaSecurityEvent xmlns:ns2="http://automatedMediaLibrary/">
  <date>2001-12-31 12:00:00</date>
  <barcode>barcode</barcode>
  <coordinate/> <!-- See Figure 26: coordinate -->
  <removalExpected>true</removalExpected> <!-- Was the media removal expected or unexpected -->
</ns2:mediaSecurityEvent>
```

Figure 138: mediaSecurityPolicy

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:mediaSecurityPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <unexpectedRemovalAfterReboot>true</unexpectedRemovalAfterReboot>
  <unexpectedRemovalDuringLibraryOperation>true</unexpectedRemovalDuringLibraryOperation>
  <expectedRemovalFromle>true</expectedRemovalFromle>
  <unexpectedRemovalFromle>true</unexpectedRemovalFromle>
</ns2:mediaSecurityPolicy>
```

Figure 139: mediaUsageList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:mediaUsageList xmlns:ns2="http://automatedMediaLibrary/">
  <mediaUsage/> A list of mediaUsage objects
</ns2:mediaUsageList>
```

Figure 140: mediaUsage

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:mediaUsage xmlns:ns2="http://automatedMediaLibrary/">
  <updated>2001-12-31T12:00:00</updated>
```

```

<barcode>barcode</barcode>
<serialNumber>Media serial number</serialNumber>
<manufacturer>manufacturer</manufacturer>
<type>type</type>
<manufacturerDate>2001-12-31T12:00:00</manufacturerDate>
<threadCount>0</threadCount>
<MBread>0</MBread>
<MBwrite>0</MBwrite>
<recoveredReadErrors>0</recoveredReadErrors>
<recoveredWriteErrors>0</recoveredWriteErrors>
<unRecoveredReadErrors>0</unRecoveredReadErrors>
<unRecoveredWriteErrors>0</unRecoveredWriteErrors>
  <beginPasses>0</beginPasses><!-- How often the drive moved the tape past the beginning (LP3) of the tape.
    Added in version 785(i6000) -->
  <middlePasses>0</middlePasses><!-- How often the drive moved the tape past the middle of the tape.
    Added in version 785(i6000) -->
<encrypted>true</encrypted> <!--The media encryption state of true or false -->
<edlmScanDate></edlmScanDate> <!-- The date the media was last tested by an EDLM scan
    (added in version 760(i6000) -->
<edlmScanType></edlmScanType> <!-- The EDLM scan type "Quick", "Normal", "Full"
    (added in version 760(i6000) -->
<edlmScanResult></edlmScanResult> <!-- The EDLM scan result "Not Completed", "Good", "Untested",
    "Suspect", "Failed" (added in version 760(i6000) -->
</ns2:mediaUsage>

```

Figure 141: mfaList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:mfaList xmlns:ns2="http://automatedMediaLibrary/"><!--Added in versions 231(i3/i6/i6H), 785(i6000)-->
  <mfa/> <!-- A list of mfa objects -->
</ns2:mfaList>

```

Figure 142: mfa

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:mfa xmlns:ns2="http://automatedMediaLibrary/">
  <type>n</type><!--1(TOTP), 2(Reserved for future use), 3 (Service passcode only,
    versions 779(i6000), 260(i3/i6/i6H)) -->
  <enabled>>false</enabled>
  <authenticationCode>string</authenticationCode>
</ns2:mfa>

```

Figure 143: mfaAuthentication

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:mfaAuthentication xmlns:ns2="http://automatedMediaLibrary/"><!--Added in version 779(i6000),
    231(i3/i6/i6H)-->
  <type>n</type><!--1(TOTP, i3/i6/i6H only) 2(Reserved for future use) 3 (service passcode, i6000 only)-->
  <authenticationCode>string</authenticationCode>
</ns2:mfaAuthentication>

```

Figure 144: mfaSharedData

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:mfaSharedData xmlns:ns2="http://automatedMediaLibrary/"><!--Added in versions
    231(i3/i6/i6H), 785(i6000)-->
  <key>n</keys>
</ns2:mfaSharedData>

```

Figure 145: moduleList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:moduleList xmlns:ns2="http://automatedMediaLibrary/">
  <module/> <!-- A list of module objects -->
</ns2:moduleList>
```

Figure 146: module

For GET `/physicalLibrary/i3-i6/modules`:

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:module xmlns:ns2="http://automatedMediaLibrary/"> <!-- Added in Scalar i3/i6/i6H version 220 -->
  <number>1</number> <!-- The module number -->
  <form>3U | 6U</form> <!-- A 3U module will have 1 section, a 6U 2 sections -->
  <section/> <!-- see Figure 190: sectionFigure 192: segment -->
</ns2:module>
```

For GET `/physicalLibrary/quattro/modules` (deprecated in Scalar i3/i6/i6H version 220):

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:module xmlns:ns2="http://automatedMediaLibrary/">
  <number>1</number> <!-- The module number -->
  <type>1</type> <!-- 1(Control Module), 2 (Expansion Module), 3 (Service Module added in version 210)-->
  <section>1</section> <!-- Section coordinate number -->
</ns2:module>
```

Figure 147: moveMediumList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:moveMediumList xmlns:ns2="http://automatedMediaLibrary/">
  <moveMedium/> A list of moveMedium objects
</ns2:moveMediumList>
```

Figure 148: moveMedium

```
<ns2:moveMedium xmlns:ns2="http://automatedMediaLibrary/">
  <mode>2</mode> <!-- This is an optional field that provides the capability to take the partition(s) offline that are
    involved in the move medium, only standard partitions apply. The default behavior is to
    do nothing -->
  <type>0</type> <!-- The type element has been deprecated; use moveClass instead:
    0 (Normal, requires source and destination coordinates.),
    3 (Unload, requires source coordinate only and source must be a drive slot. The drive must
    belong to a partition. The WS will move the media to its home slot. If the home slot is
    occupied, the WS will try and move to the first available storage slot that belongs to the
    partition. If the media is not owned by a partition, i.e. library defined cleaning tape, make
    sure the tape cartridge is removed from the partition once the unload completes.) -->
  </sourceCoordinate> A coordinate object, see Figure 26: coordinate
  </destinationCoordinate> A coordinate object, see Figure 26: coordinate
  <moveClass>0</moveClass> <!-- Bit mask definitions to qualify the Move request. Support added in version
    743(i6000) and 160(i3/i6/i6H):
    0 (Normal Move. The source and destination coordinates are required and
    allow the media to be moved within a partition or across partition boundaries.)
    i3/i6/i6H: Restrictions apply to moves from IE slots; see Table 165: POST
    aml/media/operations/moveMedium.
    2 (Import Move, requires the source coordinate only, which must be an IE slot
    and the tape cartridge in the IE slot must belong to a partition, or if not
    assigned, the destinationPartition element must be specified. The WS moves
    the media to the first available storage slot in the respective destination
```

partition). *Support added in 770(i6000) and 200(i3/i6/i6H)*. i3/i6/i6H: Additional restrictions apply; see Table 165: POST aml/media/operations/moveMedium.
4 (Export Move, requires the source coordinate only, it must be a storage slot that belongs to a partition. The WS will move the media to the first available IE slot available to the partition.). *Support added in version 770(i6000) and 200(i3/i6/i6H)*.

8 (Unload Drive, requires the source coordinate of the drive. The drive must belong to a partition. The WS will move the media to its home slot. If the home slot is occupied, the WS will try and move to the first available storage slot that belongs to the partition. If the media is not owned by a partition, i.e. library defined cleaning tape, make sure the tape cartridge is removed from the partition once the unload completes.)

16 (No Eject required. By default, when moving a tape from a drive, the WS request will always issue an unload/eject request to the drive before requesting the move. By setting this flag, the move request will not perform the unload/eject operation and expect the tape as having been unloaded/ejected by a host or via the robotic setting to assist or not assist with tape cartridge unload operations. This option would be used if the tape cartridge to be moved from a drive is expected to be unloaded already by a host or robotic subsystem unload assist configuration. For example, if doing an unload and an eject is not required, the moveClass would be set to 24 (8+16).)

32 (Move to closest slot, used in conjunction with a drive unload (8). Instead of moving the media from the drive to its home slot, the media is moved to the nearest empty storage slot. *Supported by Scalar i6000 only.*

64 (simulate a destination partition IE slot placement for import by the destination partition. May be used with export or a regular move media when destination is an IE slot. It requires a <destinationPartition>. Supported by Scalar i3/i6/i6H only.)

1024 (Force LLS Move, This definition specifies that the move request not be bypassed by any Logical Library Subsystem (LLS) partition but be initiated by the respective partition so that any connected SCSI host be made aware of the media change within the partition, as well as any configured partition policy be tested and performed, such as a partition's EDLM import scan policy, which may be bypassed if a Normal Move within a partition is specified. This requires the source and destination elements to be in the same partition and is the preferred and recommended definition when performing moves within a partition. *Introduced in 765(i6000). Supported by Scalar i6000 only. -->*

<destinationPartition>P1</destinationPartition> <!-- required for import operations of unassigned tape cartridges in a shared IE slot when the Scalar i3 or Scalar i6/i6H is configured for *Remote UI/Host Assignment*. This element is optional for other import operations, but if specified, it must match the source coordinate's partition. *Supported by Scalar i3/i6/i6H only.* →

</ns2:moveMedium>

Figure 149: network

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:network xmlns:ns2="http://automatedMediaLibrary/">
  </netInterfaceList> See Figure 153: netInterfaceList
  </netConfigurationList> See Figure 151: netConfigurationList
</ns2:network>
```

Figure 150: networkAccess

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:networkAccess
  xmlns:ns2="http://automatedMediaLibrary/">
  <icmp>
```

```

    <enabled>true</enabled>
  </icmp>
  <ssh>
    <enabled>false</enabled>
  </ssh>
  <cli>
    <enabled>true</enabled>
  </cli>
  <snmp>
    <enabled>true</enabled>
    <v1v2>true</v1v2>
  </snmp>
  <smis>
    <enabled>true</enabled>
    <secure>false</secure>
  </smis>
  <cvtl>
    <enabled>false</enabled>
  </cvtl>
  <xml>
    <enabled>true</enabled>
  </xml>
</ns2:networkAccess>

```

Figure 151: netConfigurationList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netConfigurationList xmlns:ns2="http://automatedMediaLibrary/">
  </netConfiguration> A list of netConfiguration objects
</ns2:netConfigurationList>

```

Figure 152: netConfiguration

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <location>N/A</location>
  <version>1</version> <!-- 1(IPv4), 2(IPv6) -->
  <hostName>dvt4</hostName> <!-- Valid characters, regex "[a-zA-Z][a-zA-Z0-9\-\.]*$" -->
  <domainName>company.com</domainName>
  <type>1</type> <!-- 1(Unknown), 0(None), 1(Static), 2(DHCP), 3(DHCPv6), 4(Static and DHCPv6) -->
  <netMask>255.255.248.0</netMask>
  <netGateway>10.20.168.1</netGateway>
  <ipAddress>10.20.171.14</ipAddress>
</ns2:netConfiguration>

```

Figure 153: netInterfaceList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netInterfaceList xmlns:ns2="http://automatedMediaLibrary/">
  </netInterface> A list of netInterface objects, see Figure 154: netInterface
</ns2:netInterfaceList>

```

Figure 154: netInterface

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:netInterface xmlns:ns2="http://automatedMediaLibrary/">
  <name>eth0</name>
  <macAddress>00:30:8C:06:78:D7</macAddress>

```

```

    <duplexMode>full</duplexMode>
    <autoNegotiate>>false</autoNegotiate>
    <speed>1</speed>
<!--
0(Unknown),
1(10Mb),
2(100Mb)
3(1Gb),
4(10Gb)
-->
    <linkStatus>1</linkStatus> <!-- 1(Up), 2(Down) -->
</ns2:netInterface>

```

Figure 155: networkDeviceConnectivityInfoList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:networkDeviceConnectivityInfoList xmlns:ns2="http://automatedMediaLibrary/">
  <networkDeviceConnectivityInfo/> <!-- A list of networkDeviceConnectivityInfo objects -->
</ns2:networkDeviceConnectivityInfoList>

```

Figure 156: networkDeviceConnectivityInfo

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:networkDeviceConnectivityInfo xmlns:ns2="http://automatedMediaLibrary/">
  <device>CMB</device>
  <location>[1, 1, 1, 1, 2]</location>
  <pingStatus>OK</pingStatus>
  <address>192.19.0.28</address>
  <host>M0000281</host>
  <description>N/A</description>
</ns2:networkDeviceConnectivityInfo>

```

Figure 157: NTP

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:NTP xmlns:ns2="http://automatedMediaLibrary/">
  <server>0.us.pool.ntp.org</server> <!--You can have 0 or more of these -->
</ns2:NTP>

```

Figure 158: onlineHelp

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:onlineHelp xmlns:ns2="http://automatedMediaLibrary/">
  <version>200Q.G0002</version>
  <mode>1</mode> <!-- 0(Unknown), 1(Local), 2(Remote) -->
  <installDate>The date/time the help bundle was installed</installDate>
</ns2:onlineHelp>

```

Figure 159: partitionList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:partitionList xmlns:ns2="http://automatedMediaLibrary/">
  <partition/> A list of partition objects, see Figure 160: partition
</ns2:partitionList>

```

Figure 160: partition

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:partition xmlns:ns2="http://automatedMediaLibrary/">

```

```

<id>0</id>    <!-- Used internally -->
<name>name</name> <!-- The name 'System' (case-insensitive) cannot be used on I3/i6/i6H, it is a reserved
word -->
<serialNumber>serialNumber</serialNumber>
<type>1</type>
<!--
1(Standard)
2(EDLM) Not supported on i3
3(AMP) Not supported on i3/i6/i6H
4(Active Vault)
6(Linear Tape File System (LTFS)) Only supported on i3/i6/i6H
-->
<driveDomainType>554</driveDomainType>
<!--
0(Unknown)
3(LTO2)
4(LTO3)
5(LTO4)
6(LTO5)
7(LTO6)
8(LTO7)
9(LTO8)
10(LTO9)
99(None)
554(Mixed)
-->
<mode>0</mode>          <!-- 1(Online), 2(Offline) -->
<state>1</state>
<-- added in version 760 (i6000)
0(Unknown)
1(Ready)
2(Not Ready)
3(Becoming Ready)
-->
<storageSlotCount>0</storageSlotCount>
<driveCount>0</driveCount>
<ieSlotCount>0</ieSlotCount> <!-- Not supported on I3/i6/i6H -->
<xieSlotCount>0</xieSlotCount> <!-- Not supported on I3/i6/i6H -->
<ampExtensionsCount>0</ampExtensionsCount> <!-- Not supported on I3/i6/i6H -->
<mediaCount>0</mediaCount>
<sharedIEMediaCount>0<sharedIEMediaCount> <!-- I3/i6/i6H only, media in an IE slot marked 'awaiting
assignment' when the library is in automatic assignment mode -->
<barcodeReporting>4</barcodeReporting>
<!--
1(Prefix / Media ID first)
2(Suffix / Media ID last)
3(Disabled / Standard),
4(Pass Through / Extended)
5(Standard 6; i3/i6/i6H only)
6(Plus 6; i3/i6/i6H only)
-->
<mediaTypeChecking>1</mediaTypeChecking> <!-- 1(Not Required), 2(Disabled), 3(Required)
Added in version 785(i6000)-->
<vendorId>1</vendorId> <!-- 0(ADIC), 1(Quantum) -->
<productId>7</productId>
<!-- supported options depend on library model...
1((ADIC) Scalar 24)
2((ADIC) Scalar 100)
3((ADIC) Scalar 1000)

```



```

4((ADIC) Scalar 10k)
5((ADIC/Quantum) Scalar i500)
6((ADIC/Quantum) Scalar i2000)
7((ADIC/Quantum) Scalar i6000)
8((ADIC/Quantum) Scalar i40-i80)
9((Quantum) Scalar i3-i6)
-->
<controlPathProvider>0</controlPathProvider> <!-- 0(None), 1(Drive), 2(Management Control Blade) -->
<policySettings>
  <driveFirmwareLevelingEnabled>>false</driveFirmwareLevelingEnabled>
  <driveCleaningEnabled>>false</driveCleaningEnabled>
  <driveSpoofingEnabled>>true</driveSpoofingEnabled>
  <encryptionEnabled>>true</encryptionEnabled>
  <activeVaultEnabled>>false</activeVaultEnabled>
  <autoImportEnabled>>true</autoImportEnabled>
  <autoExportEnabled>>true</autoExportEnabled>
  <edlmEnabled>>false</edlmEnabled>
</policySettings>
</ns2:partition>

```

Figure 161: partitionEncryptionPolicyList

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:partitionEncryptionPolicyList xmlns:ns2="http://automatedMediaLibrary/">
  </partitionEncryptionPolicy> <!-- A list of partitionEncryptionPolicy objects -->
</ns2:partitionEncryptionPolicyList>

```

Figure 162: partitionEncryptionPolicy

```

<?xml version="1.0" encoding="UTF-8"?>
<ns2:partitionEncryptionPolicy xmlns:ns2="http://automatedMediaLibrary/">
  <partitionName>partitionName</partitionName>
  </ekmServerType> <!-- 0(None), 2(RKM), 4(KMIP), 8(QEKM), 16(SKM), 32(TKLM), 2048(IBM SKLM - Added
770(i6000)) -->
  <!-- Note: RKM is no longer supported -->
  <libraryManaged>>true</libraryManaged>
  <fipsEnabled>>true</fipsEnabled>
  <keyReuse>>true</keyReuse>
  <keyType>0</keyType> <!-- 1(Key per Media), 2(Key per Partition), 3(Key per Library) -->
  <keySetName>MAIN-KEY-SET</keySetName> <!-- The keyset group name -->
</ns2:partitionEncryptionPolicy>

```

Figure 163: physicalLibrary

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:physicalLibrary xmlns:ns2="http://automatedMediaLibrary/">
  <name>dvt4</name> <!-- The library host name -->
  <serialNumber>273190049</serialNumber> <!-- The library serial number -->
  <logicalSerialNumber>273190049</logicalSerialNumber> <!-- Scalar i3/i6/i6H : logical library serial number,
added in version 230(i3/i6/i6H) -->
  <vendorId>quantum</vendorId> <!-- The library vendor name -->
  <productId>Scalar i6000</productId> <!-- The library type, i6000, i500 etc... -->
  <mode>1</mode> <!-- 1 (Online) or 2 (Offline) -->
  <state>1</state> <!-- 0 (Unknown), 1 (Ready) or 2 (Not Ready) -->
  <mediaInStorageCount>108</mediaInStorageCount> <!-- The number of media in storage slots -->
  <mediaInDriveCount>1</mediaInDriveCount> <!-- The number of media in drives -->
  <mediaInIeCount>3</mediaInIeCount> <!-- The number of media in IE slots -->
  <storageSlotCount>756</storageSlotCount> <!-- The number of storage slots -->
  <assignedStorageSlotCount>102</assignedStorageSlotCount> <!-- The number of storage slots owned by

```

```

partitions. On the i6000 this also includes cleaning slots.-->
<ieSlotCount>24</ieSlotCount> <!-- The number of ie slots -->
<assignedIeSlotCount>6</assignedIeSlotCount> <!-- The number of ie slots owned by partitions-->
<driveCount>9</driveCount> <!--The number of drives in the library -->
<assignedDriveCount>2</assignedDriveCount> <!-- The number of drives owned by partitions -->
<ieAreaCount>2</ieAreaCount> <!-- The number of configured IE Areas, I3/i6/i6H only -->
<libraryController>MCB2B</libraryController>
<roboticController>RCU2</roboticController>
<firmwareVersion>665Q.DS02101</firmwareVersion> <!-- The library firmware version -->
<roboticsGeneration>2</roboticsGeneration> <!-- The library robot type 1 (Gen1 for i6000 or Model 1 for
I3/i6/i6H) or 2 (Gen2 for i6000 or Model 2 for i3/i6/i6H) -->
<moduleCount>3</moduleCount> <!-- The number of frames/modules in the library -->
<towerCount>0</towerCount> <!-- The number of towers in the library -->
<parkingModules>true</parkingModules> <!-- Does the library have parking modules -->
<cleaningSlotCount>0</cleaningSlotCount> <!-- The number of cleaning slots in the library -->
<cleaningMediaCount>0</cleaningMediaCount> <!-- The number of cleaning media in the library -->
<systemMediaCount>0</systemMediaCount> <!-- The number of media owned by the System partition. This
is only supported on I3/i6/i6H. -->
<libraryUpTime>6 days 18h:21m:40s</libraryUpTime> <!--How long has the library been powered up since
last power down -->
<phySettings>
  <driveSerialNumberSpoofing>
    <enabled>true</enabled>
  </driveSerialNumberSpoofing>
  </driveCleaningCount>n</driveCleaningCount><!-- (0-3) Library detected error count total to trigger drive
cleaning within any 24 hour time period. Support added
in versions 779(i6000), 260(i3/i6/i6H) -->

  <autoInventory>
    <enabled>>false</enabled>
  </autoInventory>
  <autoCalibration> <!-- Deprecated -->
    <enabled>>false</enabled>
  </autoCalibration>
  <autoConfiguration> <!-- Deprecated -->
    <enabled>>false</enabled>
  </autoConfiguration>
  <autoCleaning> <!-- Deprecated, this is now provided on a partition basis (aml/partitions/policy/driveCleaning) -->
    <enabled>true</enabled>
  </autoCleaning>
  <autoDriveUnload>
    <enabled>true</enabled>
  </autoDriveUnload>
  <autoFirmwareUpgrade> <!--support added in version 210(i3/i6/i6H) -->
    <enabled>>false</enabled>
  </autoFirmwareUpgrade>
  <ipv6>
    <enabled>true</enabled> <!-- As of I6000 i12.3 (750) IPv6 cannot be disabled, it will always be enabled -->
  </ipv6>
  <extendedIe>
    <enabled>true</enabled>
  </extendedIe>
  <sendUsageStatistics /> <!-- See Figure 193: sendUsageStatistics -->
  <healthCheck>
    <railInterval>0</railInterval> <!-- 0-180 days (0 to disable) -->
    <robotInterval>0</robotInterval> <!-- 0-180 days (0 to disable) -->
    <towerInterval>0</towerInterval> <!-- 0-180 days (0 to disable) -->
  </healthCheck>
  <aisleLights> <!-- Set the duration for aisle lighting -->
    <interval>0</interval> <!-- 0 (off), 30 minutes or 60 minutes -->

```

```

</aisleLights>
<webCamera> <!-- The IP of the host where the Camera (i6000) Application is running -->
  <ipAddress>10.20.9.1</ipAddress>
</webCamera>
<icmpService> <!-- Allow PINGing the library -->
  <enabled>true</enabled>
</icmpService>
<sshService> <!-- Secure Shell connections to the library -->
  <enabled>true</enabled>
</sshService>
<cliService> <!-- Basic CLI interface to the library -->
  <enabled>true</enabled>
</cliService>
<xmlInterfaceService> <!-- Interface used by Quantum Vision to get library information -->
  <enabled>true</enabled>
</xmlInterfaceService>
<serviceLogin> <!-- Allow/disallow service user login -->
  <enabled>true</enabled><!-- i6000 only, used to enable/disable remote service user login. -->
  <enableRemoteAccess>true</enableRemoteAccess> <!-- (i3/i6/i6H only) Enable a service user to
    login remotely -->
  <remoteAccessTimeout>0</remoteAccessTimeout> <!-- (i3/i6/i6H only) The amount of time before a
    service user's remote access will be disabled after it
    has been enabled. Values are 0 to 72 hours, where 0
    is indefinitely -->
  <enableLocalAccess>true</enableLocalAccess> <!-- (i3/i6/i6H only) Enable a service user to login from
    the local service port -->
  <localAccessTimeout>0</localAccessTimeout> <!-- (i3/i6/i6H only) The amount of time before a service
    user's local access will be disabled after it has been
    enabled. Values are 0 to 72 hours, where 0 is
    indefinitely -->
  <serviceUserSession>240</serviceUserSession> <!-- (i3/i6/i6H only) length of the service user session,
    in minutes (Not modifiable) -->
  <remoteAccessGranted>2013-05-29 13:17:36</remoteAccessGranted> <!-- (i3/i6/i6H only) date/time
    remote access was granted -->
  <localAccessGranted>2013-05-29 13:17:36</localAccessGranted> <!-- (i3/i6/i6H only) date/time local
    access was granted -->
</serviceLogin>
<sessionTimeout> <!-- The user session timeout: -->
  <minutes>30</minutes> <!-- (1 - 1440) -->
</sessionTimeout>
<snmp>
  <communityString>publicCmtyStr</communityString>
  <enabled>true</enabled>
  <enableVersion1And2>true</enableVersion1And2>
  <enableVersion3>false</enableVersion3> <!-- Not supported in Scalar i6000 -->
  <enableAuthenticationTraps>false</enableAuthenticationTraps> <!-- Not supported in Scalar i6000 -->
</snmp>
<smis>
  <enabled>false</enabled>
  <enableSecureSmis>false</enableSecureSmis>
</smis>
<autoWebRequests> <!--support added for Scalar i3/i6/i6H in version 230(i3/i6/i6H) -->
  <enabled>false</enabled>
</autoWebRequests>
<logicalSystemAddressing> <!--support added for Scalar i3/i6/i6H in version 230(i3/i6/i6H) -->
  <enabled>false</enabled>
</logicalSystemAddressing>
</phySettings>
</ns2:physicalLibrary>

```

Figure 164: physicalLibraryConfiguration

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:physicalLibraryConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <name>dvt4</name> <!-- The library host name -->
  <serialNumber>273190049</serialNumber> <!-- The library serial number -->
  <logicalSerialNumber>273190049</logicalSerialNumber> <!-- logical serial number, added in 230(i3/i6/i6H) -->
  <vendorId>quantum</vendorId> <!-- The library vendor name -->
  <productId>Scalar i6000</productId> <!-- The library type, i6000, i500, etc... -->
  <mode>1</mode> <!-- 1 (Online) or 2 (Offline) -->
  <state>1</state> <!-- 1 (Ready) or 2 (Not Ready) -->
  <libraryController>MCB2B</libraryController>
  <roboticController>RCU2</roboticController>
  <firmwareVersion>firmwareVersion</firmwareVersion>
  <roboticsGeneration>0</roboticsGeneration> <!-- The library robot type 1 or 2 -->
  <libraryUpTime>6 days 18h:21m:40s</libraryUpTime> <!--How long has the library been powered up since last
power down -->
</ns2:physicalLibraryConfiguration>
```

Figure 165: physicalLibraryRemoteAccess

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:physicalLibraryRemoteAccess xmlns:ns2="http://automatedMediaLibrary/">
  <ipv6>
    <enabled>true</enabled> <!-- As of i6000 i12.3 (750), IPv6 cannot be disabled, it will always be enabled -->
  </ipv6>
  <icmpService> <!-- Allow/disallow PINGing the library -->
    <enabled>true</enabled>
  </icmpService>
  <sshService> <!-- Secure Shell connections to the library -->
    <enabled>true</enabled>
  </sshService>
  <cliService> <!-- Basic CLI interface to the library -->
    <enabled>true</enabled>
  </cliService>
  <xmlInterfaceService> <!-- Enable Vision Interface -->
    <enabled>true</enabled>
  </xmlInterfaceService>
  <serviceLogin> <!-- Allow/disallow service user login -->
    <enabled>true</enabled>
    <enableRemoteAccess>true</enableRemoteAccess> <!-- Enable a service user to login from a remote
interface (browser) -->
      <remoteAccessTimeout>0</remoteAccessTimeout> <!-- The amount of time before a service user's
remote access will be disabled after it has been enabled. Values are 0 to 72 hours, where 0 is indefinitely -->
      <enableLocalAccess>true</enableLocalAccess> <!-- Enable a service user to login from the local user
interface -->
        <localAccessTimeout>0</localAccessTimeout> <!-- The amount of time before a service user's local
access will be disabled after it has been enabled. Values are 0 to 72 hours, where 0 is indefinitely -->
        <serviceUserSession>240</serviceUserSession> <!-- length of the service user session, in minutes (Not
modifiable) -->
        <remoteAccessGranted>2013-05-29 13:17:36</remoteAccessGranted> <!-- date/time remote access
was granted -->
        <localAccessGranted>2013-05-29 13:17:36</localAccessGranted> <!-- date/time local access was
granted -->
      </serviceLogin>
    <sessionTimeout> <!-- The user session timeout: in minutes, 1 – 1440 -->
      <minutes>0</minutes>
    </sessionTimeout>
  </ns2:physicalLibraryRemoteAccess>
```

Figure 166: physicalLibraryResources

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:physicalLibraryResources xmlns:ns2="http://automatedMediaLibrary/">
  <mediaInStorageCount>0</mediaInStorageCount>
  <mediaInDriveCount>0</mediaInDriveCount>
  <mediaInIeCount>0</mediaInIeCount>
  <storageSlotCount>0</storageSlotCount>
  <assignedStorageSlotCount>0</assignedStorageSlotCount> <!-- The number of storage slots assigned to
    partitions and cleaning slots. -->
  <ieSlotCount>0</ieSlotCount>
  <assignedIeSlotCount>0</assignedIeSlotCount>
  <driveCount>0</driveCount>
  <assignedDriveCount>0</assignedDriveCount>
  <moduleCount>0</moduleCount>
  <towerCount>0</towerCount>
  <parkingModules>true</parkingModules>
  <cleaningSlotCount>0</cleaningSlotCount>
  <cleaningMediaCount>0</cleaningMediaCount>
  <ieAreaCount>2</ieAreaCount> <!-- The number of configured IE Areas, I3/i6/i6H only -->
  <systemMediaCount>0</systemMediaCount> <!-- The number of media owned by the System partition. This
    is only supported on I3/i6/i6H. -->
</ns2:physicalLibraryResources>
```

Figure 167: physicalLibrarySettings

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:physicalLibrarySettings xmlns:ns2="http://automatedMediaLibrary/">
  <driveSerialNumberSpoofing>
    <enabled>true</enabled>
  </driveSerialNumberSpoofing>
  <driveCleaningCount>n</driveCleaningCount><!-- (0-3) Library detected error count total to trigger drive
    cleaning within any 24 hour time period. Support added
    in versions 779(i6000), 260(i3i/i6/i6H)-->
  <autoInventory>
    <enabled>true</enabled>
  </autoInventory>
  <autoCalibration> <!-- Deprecated -->
    <enabled>true</enabled>
  </autoCalibration>
  <autoConfiguration> <!-- Deprecated -->
    <enabled>true</enabled>
  </autoConfiguration>
  <autoCleaning> <!--Deprecated; now provided on a partition basis (aml/partitions/policy/driveCleaning) -->
    <enabled>true</enabled>
  </autoCleaning>
  <autoDriveUnload>
    <enabled>true</enabled>
  </autoDriveUnload>
  <extendedIe>
    <enabled>true</enabled>
  </extendedIe>
  <sendUsageStatistics /> <!-- See Figure 193: sendUsageStatistics -->
  <healthCheck>
    <raillInterval>0</raillInterval> <!-- 0-180 days (0 to disable) -->
    <robotInterval>0</robotInterval> <!-- 0-180 days (0 to disable) -->
    <towerInterval>0</towerInterval> <!-- 0-180 days (0 to disable) -->
  </healthCheck>
  <aisleLights> <!-- Set the duration for aisle lighting 0 (off), 30 minutes or 60 minutes -->
```

```

    <interval>0</interval>
</aisleLights>
<webCamera> <!-- The IP of the host where the Camera (i6000) Application is running -->
    <ipAddress>ipAddress</ipAddress>
</webCamera>
<snmp>
    <communityString>communityString</communityString>
    <enabled>true</enabled>
    <enableVersion1And2>true</enableVersion1And2>
    <enableVersion3>true</enableVersion3> <!-- Not supported in i6000 -->
    <enableAuthenticationTraps>true</enableAuthenticationTraps> <!-- Not supported in i6000 -->
</snmp>
<smis>
    <enabled>true</enabled>
    <enableSecureSmis>true</enableSecureSmis>
</smis>
<autoWebRequests> <!--support added for Scalar i3/i6/i6H in version 230(i3/i6/i6H) -->
    <enabled>false</enabled>
</autoWebRequests>
<logicalSystemAddressing> <!--support added for Scalar i3/i6/i6H in version 230(i3/i6/i6H) -->
    <enabled>false</enabled>
</logicalSystemAddressing>
</ns2:physicalLibrarySettings>

```

Figure 168: ping

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ping xmlns:ns2="http://automatedMediaLibrary/">
    <firmwareVersion>665Q.DS02401</firmwareVersion>
    <productName>Scalar i6000</productName> <!-- "Scalar i6000", "Scalar i3" or "Scalar i6" -->
    <serialNumber>273190048</serialNumber>
    <vendor>Vendor Name</vendor> <!-- "Quantum" -->
</ns2:ping>

```

Figure 169: port

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:port xmlns:ns2="http://automatedMediaLibrary/">
    <id>Port 1, Port A, Left, Right ...</id>
    <type>1</type> <!-- 1(SCSI), 2(Fibre), 3(SAS) -->
    <address>WWPN</address>
    <topology>
        <actual>2</actual> <!-- -1 and 0 (N/A), 1(Loop Preferred "LN"), 2(P2P/Fabric "N"), 3(Loop "L"), 4(P2P/Fabric
preferred "NL", only supported on i3/i6/i6H) -->
        <requested>2</requested> <!-- -1 and 0 (N/A), 1(Loop Preferred "LN"), 2(P2P/Fabric "N"), 3(Loop "L"),
4(P2P/Fabric preferred "NL", only supported on i3/i6/i6H) -->
    </topology>
    <loopId>0</loopId>
    <speed>
        <actual>4</actual> <!-- -1(N/A), 1(1Gb/s), 2(2Gb/s), 4(4Gb/s), 8(8Gb/s) -->
        <requested>4</requested> <!-- 0(Auto), 1(1Gb/s), 2(2Gb/s), 4(4Gb/s), 8(8Gb/s) -->
    </speed>
    <loop> <!-- The loop ID of the drive when configure for loop mode. This is intended to
replace the loopId element, since i3/i6/i6H libraries support both 'requested' and 'actual' loop IDs. For i6000 if this
loop element is not requested then the loopId element will be used. -->
        <actual>0</actual> <!-- This will report 0-126. On the i6000 0 and 126 indicates soft (which is
equivalent to auto), on i3/i6/i6H, 126 indicates soft. On i6000 we report -1 if we cannot determine the ID -->
        <requested>0</requested> <!-- For i6000 0 and 126 indicate soft and for i3/i6/i6H, 126 indicates soft. All
other values indicate hard (user set) loop IDs. On i6000 we report -1 if we cannot determine the ID. -->
    </loop>

```

```

</loop>
<status>0</status>          <!-- 0(N/A), 1(Down), 2(Active), 4(Passive) -->
</ns2:port>

```

Figure 170: RASGroupStatusList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASGroupStatusList xmlns:ns2="http://automatedMediaLibrary/">
  </RASGroupStatus> A list of RASGroupStatus objects
</ns2:RASGroupStatusList>

```

Figure 171: RASGroupStatus

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASGroupStatus xmlns:ns2="http://automatedMediaLibrary/">
  <group>1</group> <!--
    0 (All), i6000 and I3/i6/i6H use group 0 to represent the overall library status
    1 (Connectivity), i6000 only
    2 (Control), i6000 and I3/i6/i6H
    3 (Media), i6000 and I3/i6/i6H
    4 (Drives), i6000 and I3/i6/i6H
    5 (Power), i6000 only
    6 (Robotics) i6000 only
    7 (Library) I3/i6/i6H only.-->
  <status>1</status> <!-- 1 (Good/Operational), 2 (Failed), 3 (Degraded), 4 (Warning), 5 (Informational),
    6 (Unknown), 7 (Invalid), 8(Attention) -->
</ns2:RASGroupStatus>

```

Figure 172: RASReportList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASReportList xmlns:ns2="http://automatedMediaLibrary/">
  </RASReport> A list of RASReport objects
</ns2:RASReportList>

```

Figure 173: RASReport

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASReport xmlns:ns2="http://automatedMediaLibrary/">
  <reportId>42</reportId>
  <postedDate>2013-05-29 13:17:36 +0000</postedDate>
  <duplicates>0</duplicates>
  </RASGroupStatus> <!-- See Figure 171: RASGroupStatus -->
  <eventCode>09_09_18_00_00000000</eventCode>
  <modifier>0x0</modifier>
  <summary>Drive [1, 1, 1, 12, 1, 1] lost network link, will be unable to reconfigure</summary>
  <description>Control of Tape Drive at [1,1,1,12,1,1] communication has failed</description>
  <headReport>41</headReport>
  <keyReportId>0</keyReportId>
  <serialNumber>GB120401FD</serialNumber>
  <repairLink>09_09_18_htm</repairLink>
</ns2:RASReport>

```

Figure 174: RASTicketReports

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASTicketReports xmlns:ns2="http://automatedMediaLibrary/">
  <ticketId>15</ticketId>
  </RASReportList> A RASReportList object, see Figure 172: RASReportList

```

```
</ns2:RASTicketReports>
```

Figure 175: RASTicketList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASTicketList xmlns:ns2="http://automatedMediaLibrary/">
  <RASTicket>
    <ticketId>5</ticketId>
    <name></name>
    <description>Control of Tape Drive at [1,1,1,10,1,1] communication has failed</description>
    <closed>1970-01-01 00:00:00 +0000</closed>
    <opened>2013-05-16 20:36:43 +0000</opened>
    <eventCode>0</eventCode>
    <groupStatus>
      <group>4</group>
      <status>2</status>
    </groupStatus>
    <RASTicketState>
      <state>2</state>
    </RASTicketState>
    <duplicates>0</duplicates>
    <lastUpdate>2013-06-11 10:20:05 +0000</lastUpdate>
    <serialNumber>HU1231PJTT</serialNumber>
    <repairLink>09_09_18_htm</repairLink>
    <keyReportId>17</keyReportId>
    <rasTicketDetails/>
  </RASTicket>
</ns2:RASTicketList>
```

Figure 176: RASTicket

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASTicket xmlns:ns2="http://automatedMediaLibrary/">
  <ticketId>5</ticketId>
  <name></name>
  <description>Control of Tape Drive at [1,1,1,10,1,1] communication has failed</description>
  <closed>1970-01-01 00:00:00 +0000</closed>
  <opened>2013-05-16 20:36:43 +0000</opened>
  <eventCode>0</eventCode>
  </groupStatus> <!-- RASGroupStatus object, see Figure 171: RASGroupStatus -->
  </RASTicketState> <!-- A RASTicketState object -->
  <duplicates>0</duplicates>
  <lastUpdate>2013-06-11 10:20:05 +0000</lastUpdate>
  <serialNumber>HU1231PJTT</serialNumber>
  <powerOnHours>5912</powerOnHours><!-- i3/i6/i6H only, added in release 210 -->
  <moveCount>128183</moveCount><!-- i3/i6/i6H only, added in release 210 -->
  <temperature>26</temperature><!-- degrees Celsius; i3/i6/i6H only, added in release 210-->
  <humidity>15</humidity><!-- percentage; i3/i6/i6H only, added in release 210 -->
  <repairLink>09_09_18_htm</repairLink>
  <keyReportId>17</keyReportId>
  <serviceUser>>false</serviceUser> <!-- service was logged in when ticket opened. Added in version
    751(i6000), 210(i3/i6/i6H) -->
  <rasTicketDetails>
    <rasTicketDetails/> <!-- 0-n rasTicketDetails, basically a list of strings -->
  </rasTicketDetails>
  <severity>1</severity> <!-- 1(critical), 2(degraded), 3(warning), 4(attention) and 5(informational)
  <fruLocation>1,1,1,1,1,3</fruLocation> <!-- Where the component is location in the library. Note: This is only
supported on the i6000 -->
</ns2:RASTicket>
```


Figure 177: RASTicketState

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:RASTicketState xmlns:ns2="http://automatedMediaLibrary/">
  <state>5</state> <!-- 1 (New), 2 (Open), 3 (Suspended), 4 (Closed), 5 (Verified) -->
</ns2:RASTicketState>
```

Figure 178: rasNotificationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:rasNotificationList xmlns:ns2="http://automatedMediaLibrary/">
  </rasNotification> A list of rasNotification objects
</ns2:rasNotificationList>
```

Figure 179: rasNotification

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:rasNotification xmlns:ns2="http://automatedMediaLibrary/">
  <id>1</id> <!-- This id is generated and is used to lookup a reportNotification object. Each reportNotification
gets a unique id. -->
  <enabled>true</enabled> <!-- Enable/Disable the notification, when disabled the notification will not be sent -
-->
  <emailAddress>john.doe@acme.com</emailAddress> <!-- E-mail address -->
  <severity1>true</severity1> <!-- Send Severity 1 Tickets -->
  <severity2>true</severity2> <!-- Send Severity 2 Tickets -->
  <severity3>true</severity3> <!-- Send Severity 3 Tickets -->
  <severity4>true</severity4> <!-- Send Severity 4 Tickets -->
  <severity5>true</severity5> <!-- Send Severity 5 Tickets -->
  <includeSnapshot>>false</includeSnapshot> <!-- Do we include a snapshot with the notification. This is not
supported on the i6000 -->
  <lastSent>Date</lastSent> <!-- The last time the notification was sent -->
  <includeDriveLog>>false</includeDriveLog> <!-- Do we include a drive log with the notification. This is not
supported on the i6000 -->
  <includeResolution>>false</includeResolution> <!-- Do we include a resolution with the notification. This is not
supported on the i6000 -->
</ns2:rasNotification>
```

Figure 180: reportList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:reportList xmlns:ns2="http://automatedMediaLibrary/">
  </report> A list of report objects
</ns2:reportList>
```

Figure 181: report

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:report xmlns:ns2="http://automatedMediaLibrary/">
  <name>Drive Utilization</name> <!-- The report name -->
  <type>The Report Type</type>
<!--
1, "Drive Utilization",
2, "Media Integrity Analysis",
3, "Media Usage",
4, "Media Security",
5, "Cross Partition Media Moves",
6, "Tickets",
7, "LUN Mapping",
8, "Media Inventory",
```

```

9, "EKM Partition Activity",
10, "EKM Media Status",
11, "Login Activity",
12, "Verification Test",
13, "Library Configuration Record",
14, "Partition Utilization",
15, "Drive Cleaning",
16, "EDLM Scan Test",
17, "Blade Media Summary",
18, "Blade Volume Group Capacity",
19, "Blade Media Summary",
20, "Blade Configuration Record",
21, "Internal Network Connectivity Status",
22, "Temperature/Humidity",
23, "Library Configuration Change"

```

```
-->
```

```

<license>Advanced Reporting</license> <!-- Some reports required a license, if the report requires a
license, then the license name will be reported. If it does not require a license, then this field will be null or empty
-->

```

```

<licensed>true</licensed> <!-- If the report requires a license, the 'license' element is not null or empty, then
this field will have indicated if the license is installed, true, or false if the required license is not installed. If the
license element is null or empty, then you can ignore this element-->

```

```

<format>CSV</format> <!-- The format supported when the report is saved -->

```

```

<recordCount>123</recordCount> <!-- The number of records, or if TXT format -->

```

```

<template /> <!-- A list of reportTemplate objects, see Figure 186: reportTemplate -->

```

```
</ns2:report>
```

Figure 182: reportCriteria

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<ns2:reportCriteria xmlns:ns2="http://automatedMediaLibrary/">
```

```

<start>0</start> <!-- The start offset in the list of records, 0 is the default, the first record -->

```

```

<length>0</length> <!-- The number of records, you want to retrieve, 0 is default and means all records after
the start offset -->

```

```

<period>7</period> <!-- The last number of days to report. If I want a report for the last week, this value would
be 7. 0 is default and means report all records -->

```

```

<date>Query start date</date> <!-- At what date you want to start your query. The data returned will include all
records that are equal to or older than the date specified. When used with the period parameter, the data
returned will include all records that are equal or older than the date specified up to the period (number of days)
specified. The date format expected is "yyyy-MM-dd HH:mm:ss" or "yyyy-MM-dd HH:mm:ss Z" the Z (time zone)
field will be ignored. -->

```

```

<partition>partition name</partition> <!-- Some reports can be filtered on partition name; this field is also used
as alerts filter for Media Integrity Analysis report. -->

```

```

<driveSerialNumber>serial number</driveSerialNumber> <!-- Some reports can be filtered on the drive
physical serial number -->

```

```

<barcode>The media barcode</barcode> <!-- Some reports can be filtered on the media barcode-->

```

```

<state>1</state> <!-- Generic field used to filter on state, or overloaded to filter on some other field, must be > 0 -->

```

```

<type>1</type> <!-- Generic field used to filter on type, or overloaded to filter on some other field, must be > 0 -->

```

```

<id>1</id> <!-- Generic field used to filter on id, or overloaded to filter on some other field, must be > 0. This
was added for i6000 in version 760 -->

```

```
</ns2:reportCriteria>
```

Figure 183: reportNotificationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<ns2:reportNotificationList xmlns:ns2="http://automatedMediaLibrary/">
```

```

<reportNotification/> A list of reportNotification objects, See Figure 184: reportNotification

```

```
</ns2:reportNotificationList>
```

Figure 184: reportNotification

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:reportNotification xmlns:ns2="http://automatedMediaLibrary/">
  <id>4</id> <!-- This id is generated and is used to lookup a reportNotification object. Each reportNotification
gets a unique id. -->
  <enabled>true</enabled> <!-- Enable/Disable the notification, when disabled the notification will not be sent -
->
  <emailAddress>john.doe@company.com </emailAddress> <!-- The e-mail address where the notification will
be sent too -->
  <reportTemplateName>LoginActivity</reportTemplateName> <!-- The report template name, See Figure 186:
reportTemplate. -->
  <interval>
    <frequency>1</frequency> <!-- The frequency the report will be sent, valid values are 1 (Daily), 2 (Weekly), 3
(Monthly) and 4 (Quarterly) -->
    <dayOfWeek>4</dayOfWeek> <!-- The day of the week the report should be sent, 0 is Sunday, 6 is
Saturday -->
    <hourOfDay>0</hourOfDay> <!-- The hour of the day the report should be sent, 0 - 23 -->
  </interval>
</ns2:reportNotification>
```

Figure 185: reportTemplateList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:reportTemplateList xmlns:ns2="http://automatedMediaLibrary/">
  <reportTemplate/> A list of reportTemplate objects, see Figure 186: reportTemplate
</ns2:reportTemplateList>
```

Figure 186: reportTemplate

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:reportTemplate xmlns:ns2="http://automatedMediaLibrary/">
  <id>Template ID</id> <!-- Only used to lookup template -->
  <name>name</name> <!-- The name can only contain the following characters A-Z a-z 0-9 _ and spaces. The
maximum number of characters allowed is 64 -->
  <reportType>1</reportType> <!-- See type element of Figure 181: report -->
  <reportCriteria/> <!-- A reportCriteria object Figure 182: reportCriteria -->
</ns2:reportTemplate>
```

Figure 187: robotList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:robotList xmlns:ns2="http://automatedMediaLibrary/">
  <robot/> A list of 1 or 2 robot objects, see Figure 188: robot
</ns2:robotList>
```

Figure 188: robot

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:robot xmlns:ns2="http://automatedMediaLibrary/">
  <name>name</name>
  <status>0</status> <!-- 0(Unknown), 1(Active), 2(NotInstalled), 3(Initializing), 4(Failed), 5(N/A),
6(Active Media Present (770(i6000))), 7(Failed Media Present (770(i6000))),
8 (Inoperable (220(i3/i6/i6H). 778(i6000))) -->
  <state>0</state> <!-- 0(Unknown), 1(Varied On), 2(Varied Off) -->
  <serialNumber>serialNumber</serialNumber> <!-- Robot controller serial number -->
  <firmwareVersion>firmwareVersion</firmwareVersion>
  <parked>true</parked>
  <present>true</present>
```

```

<generation>generation</generation>
<coordinate/> <!-- See Figure 26: coordinate, added in versions 820(i6000), 220(i3/i6/i6H)-->
</ns2:robot>

```

Figure 189: robotSettings

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:robotSettings xmlns:ns2="http://automatedMediaLibrary/">
  <parkingDelay>
    <seconds>180</seconds><!-- 5-900 seconds -->
  </parkingDelay>
  <serviceTrayRelease>
    <enabled>>false</enabled>
  </serviceTrayRelease>
</robotSettings>

```

Figure 190: section

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:section xmlns:ns2="http://automatedMediaLibrary/"> <!-- added in version 220(i3/i6/i6H) -->
  <number>1</number> <!-- Section coordinate number -->
  <type>1</type> <!-- 1(Control Module), 2 (Expansion Module), 3 (Service Module)-->
  <status>1</status> <!-- 0(Unknown), 1(Operational), 2 (Receive Mode), 3 (Capture Mode), 4(Tray Missing,
5(Failed)-->
</ns2:section>

```

Figure 191: segmentList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segmentList xmlns:ns2="http://automatedMediaLibrary/">
  </segment> <!-- A list of segment objects -->
</ns2:segmentList>

```

Figure 192: segment

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:segment xmlns:ns2="http://automatedMediaLibrary/">
  <coordinate/> <!-- See Figure 26: coordinate -->
  <size>6</size>
  <owner>LL1</owner> <!-- The partition who owns the segment -->
  <configuredType>0</configuredType> <!-- Future configuration type option to allow IE to be configured as
storage -->
</ns2:segment>

```

Figure 193: sendUsageStatistics

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sendUsageStatistics xmlns:ns2="http://automatedMediaLibrary/">
  <interval/>
<!-- This has been changed to a bitmask in (760(i6000) and 150(i3/i6/i6H))
0 (Disabled (Both E-mail and Cloud))
1 (Monthly (Enabled for both E-mail and Cloud))
2 (Quarterly (Enabled for both E-mail and Cloud))
4 (Disable E-mail)
8 (Disable Cloud)

```

To just e-mail on a quarterly basis, use 10, 2 (Quarterly) + 8 (Disable cloud). The valid values are:
0 - disable both
1 - enable both monthly

- 2 - enable both quarterly
- 5 - monthly, email disabled, cloud enabled
- 6 - quarterly, email disabled, cloud enabled
- 9 - monthly cloud disabled, email enabled
- 10 - quarterly cloud disabled, email enabled

Note: sendUsageStatistics was deprecated in version 210 (i3/i6/i6H) and is no longer supported by Scalar i3 and Scalar i6. Use telemetric notifications.

```
-->
</ns2: sendUsageStatistics>
```

Figure 194: sensorList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sensorList xmlns:ns2="http://automatedMediaLibrary/">
  </sensor> A list of sensor objects
</ns2:sensorList>
```

Figure 195: sensor

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sensor xmlns:ns2="http://automatedMediaLibrary/">
  <!-- All elements are strings -->
  <name>RCS FAN1</name>
  <type>Cooling</type>
  <status>Normal</status>
  <value>5818</value>
  <unit>RPM</unit>
  <location>Library (LPC) Cooling Fan #1</location>
  <configurationType>1</configurationType> <-- 0(None) 1(Library Temperature) 2(Library Humidity)
                                     added for Scalar i3/i6/i6H in version 220(i3/i6/i6H)-->
</ns2:sensor>
```

Figure 196: sensorConfigurationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sensorConfigurationList xmlns:ns2="http://automatedMediaLibrary/">
  <serviceConfiguration/> <!-- A list of sensorConfiguration objects. See Figure 197: sensorConfiguration-->
</ns2:sensorConfigurationList>
```

Figure 197: sensorConfiguration

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sensorConfiguration xmlns:ns2="http://automatedMediaLibrary/">
  <type>1</type> <-- 1(Library Temperature) 2(Library Humidity) -->
  <minLimit>10</minLimit><!--minimum range-->
  <maxLimit>45</maxLimit> <!--maximum range-->
  <minValue>12</minValue> <-- minimum threshold -->
  <maxValue>44</maxValue><-- maximum threshold -->
  <minDefault>16</minDefault> <-- library default minimum -->
  <maxDefault>42</maxDefault><--library default maximum -->
</ns2:sensorConfiguration>
```

Figure 198: serviceLogList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:serviceLogList xmlns:ns2="http://automatedMediaLibrary/">
  <serviceLog/> <!-- A list of serviceLog objects -->
</ns2:serviceLogList>
```

Figure 199: serviceLog

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:serviceLog xmlns:ns2="http://automatedMediaLibrary/">
  <name>vt_2U31090031_2015-06-18_17.21.48.log</name> <!-- The name of the log -->
  <type>1</type> <!-- 0(N/A), 1(VT), 2(SCSI), 3(GET/PUT Statistics) -->
  <date>2015-06-18 17:22:59</date> <!-- The date the log file was last modified -->
</ns2:serviceLog>
```

Figure 200: shutdownTask

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:shutdownTask xmlns:ns2="http://automatedMediaLibrary/">
  <reboot>false</reboot> <!-- True if library should reboot, false if library needs to be power-cycled -->
  <reset>false</reset> <!-- This is used internally and is not required by any interface -->
</ns2:shutdownTask>
```

Figure 201: sysLogServerList

```
<!-- Added in version 770(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sysLogServerList xmlns:ns2="http://automatedMediaLibrary/">
  <sysLogServer/> <!-- A list of sysLogServer objects -->
</ns2:sysLogServerList>
```

Figure 202: sysLogServer

```
<!-- Added in version 770(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sysLogServer xmlns:ns2="http://automatedMediaLibrary/">
  <id>1</id>
  <enabled>true</enabled> <!-- Enable remote syslog logging -->
  <name>10.20.9.8</name> <!-- The IP/Host name of the remote syslog server -->
  <port>514</port> <!-- The port number of the syslog service -->
  <transport>1</transport>
  <!--
  1(TCP),
  2(UDP)
  -->
</ns2:sysLogServer>
```

Figure 203: teachTask

```
<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:teachTask xmlns:ns2="http://automatedMediaLibrary/">
  <type>1</type> <!-- 1(Configure) or 2(Calibrate) -->
  <range>
    <startFrame>0</startFrame> <!-- The starting frame number -->
    <endFrame>2</endFrame> <!-- The ending frame number -->
  </range>
</ns2:teachTask>
```

Figure 204: telemetricNotificationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:telemetricNotificationList xmlns:ns2="http://automatedMediaLibrary/">
  <telemetricNotification/> A list of telemetricNotification objects, See Figure 205: telemetricNotification
</ns2:telemetricNotificationList>
```

Figure 205: telemetricNotification

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:telemetricNotification xmlns:ns2="http://automatedMediaLibrary/">
  <receiver>1|2</receiver> <!-- Receiver type. 1-autosupport cloud, 2 -telemetrics E-Mail -->
  <enabled>true</enabled> <!-- When disabled, the notification will not be sent -->
  <interval>
    <frequency>1</frequency> <!-- The frequency the report will be sent, valid values are 1 (Daily), 2 (Weekly), 3
(Monthly) and 4 (Quarterly) -->
    <dayOfWeek>4</dayOfWeek> <!-- The day of the week the report should be sent, 0 is Sunday, 6 is
Saturday -->
    <hourOfDay>0</hourOfDay> <!-- The hour of the day the report should be sent, 0 - 23 -->
  </interval>
</ns2:telemetricNotification>
```

Figure 206: trapNotificationList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:trapNotificationList xmlns:ns2="http://automatedMediaLibrary/">
  <trapNotification/> A list of trapNotification objects.
</ns2:trapNotificationList>
```

Figure 207: trapNotification

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:trapNotification xmlns:ns2="http://automatedMediaLibrary/">
  <id>Unique ID</id> <!-- Used to lookup object -->
  <host>10.20.1.100</host> <!-- The host or IP of the host that will receive the trap -->
  <port>162</port>
  <transportType>1</transportType> <!-- 1(UDP IPv4), 2(UDP IPv6), 3(TCP IPv4), 4(TCP IPv6) Not supported
in i6000 -->
  <communityString>publicCmtyStr</communityString> <!-- Not required for Quantum branded i6000 libraries -
->
  <version>1</version> <!-- 1(SNMPv1), 2(SNMPv2c), 3(SNMPv3) Not supported in i6000 or i3/i6/i6H -->
</ns2:trapNotification>
```

Figure 208: taskList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:taskList xmlns:ns2="http://automatedMediaLibrary/">
  <task/> A list of task objects
</ns2:taskList>
```

Figure 209: task

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:task xmlns:ns2="http://automatedMediaLibrary/">
  <id>91</id> <!-- A unique task id number, used to look up a particular task -->
  <componentId>LL1</componentId> <!-- Drive serial number, partition name, blade coordinate, etc...-->
  <type>1</type>
<!-- 0(All types),
1 (Inventory),
2 (Library Shutdown),
3 (Library Reboot),
4 (Identify Drive),
5 (Drive Clean),
6 (Power Cycle FC IO Blade),
7 (Reset FC IO Blade),
8 (Identify FC IO Blade),
```

```

9 (Identify Ethernet Expansion Blade),
10 (Auto Import Media),
11 (Generate Command History Logs)
12 (VT, Start Test Diagnostic Session (i6000 and I3/i6/i6H))
13 (VT, Finish Test Diagnostic Session (i6000 and I3/i6/i6H))
14 (VT, Robot Accessor Test (i6000))
15 (VT, Robot Picker Test (i6000))
16 (VT, Robot Assembly Test (i6000 and I3/i6/i6H))
17 (VT, IE Station Assembly Test (i6000))
18 (VT, Tower Assembly Test (i6000))
19 (VT, Tower Scanner Test (i6000))
20 (VT, Robot Scanner Test (i6000))
21 (VT, Library Get Put Test (i6000))
22 (VT, Drive Assembly Test (i6000 and I3/i6/i6H))
23 (VT, Magazine Test (I3/i6/i6H))
24 (IVT, Full Installation Verification Test (i6000 and I3/i6/i6H))
27 (VT, Library Alignment Test (i6000))
28 (VT, Barcode Label Test (i6000)) 760(i6000)
29 (VT, Module Assembly Test (I3/i6/i6H))
51 (Teach Configure/Calibrate (i6000)) 760(i6000)
52 (Power Cycle EEB (i6000)) 760(i6000)
53 (Library Reset (i6000)) 770(i6000)
-->
  <opened>2013-12-16 17:17:55 +0000</opened> <!-- When the task was started -->
  <closed>2013-12-16 17:18:06 +0000</closed> <!-- When the task completed -->
  <state>5</state>
<!--
0 (Unknown)
1 (In Progress)
2 (Pending)
3 (Stopped)
4 (Terminated)
5 (Completed)
-->
  <status>1</status>
<!--
0 (Unknown)
1 (Success)
2 (Warning)
3 (Invalid)
4 (Incomplete)
5 (Failed)
-->
  <description>Inventory - Start Element: 4096, element count: 20, offline: true</description>
  <sessionId>15</sessionId>
</ns2:task>

```

Figure 210: ticketFilterList

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8"?>
<ns2:ticketFilterList xmlns:ns2="http://automatedMediaLibrary/">
  </ticketFilter> <!-- A list of ticketFilter objects -->
</ns2:ticketFilterList>

```

Figure 211: ticketFilter

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8"?>

```



```

<ns2:ticketFilter xmlns:ns2="http://automatedMediaLibrary/">
  <id>0</id>
  <linkId>01_09_10</linkId> <!-- The RAS ticket link ID -->
  <defaultSuppressOption>0</defaultSuppressOption>
  <!-- The library assigned default option, this cannot be modified
0(No Suppression, e-mail notifications will be sent),
1(No E-mail to Technical Support),
2(No E-mail will be sent to anybody),
3(The RAS ticket will not be generated)
-->
  <suppressOption>0</suppressOption>
  <!--
0(No Suppression, e-mail notifications will be sent),
1(No E-mail to Technical Support),
2(No E-mail will be sent to anybody),
3(The RAS ticket will not be generated)
-->
  <description>description</description> <!-- RAS Ticket description -->
  <rasGroup>1</rasGroup>
  <!--
1(Connectivity),
2(Control),
3(Media),
4(Drives),
5(Power)
6(Robotics)
-->
</ns2:ticketFilter>

```

Figure 212: timeZoneIDs

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:timeZoneIDs xmlns:ns2="http://automatedMediaLibrary/">
  <ID>(GMT-12:00) Etc/GMT+12 (GMT-12:00)</ID>
  <ID>(GMT-11:00) Etc/GMT+11 (GMT-11:00)</ID>
  <ID>(GMT+13:00) MIT (WSDT)</ID>
  <ID>(GMT+13:00) Pacific/Apia (WSDT)</ID>
  <ID>(GMT-11:00) Pacific/Midway (SDT)</ID>
  <ID>(GMT-11:00) Pacific/Niue (NUST)</ID>
  <ID>(GMT-11:00) Pacific/Pago_Pago (SDT)</ID>
  <ID>(GMT-11:00) Pacific/Samoa (SDT)</ID>
  <ID>(GMT-11:00) US/Samoa (SDT)</ID>
  <ID>(GMT-10:00) America/Adak (HADT)</ID>
  .....
</ns2:timeZoneIDs>

```

Figure 213: towerList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:towerList xmlns:ns2="http://automatedMediaLibrary/">
  <tower/> A list of tower objects, see Figure 214: tower
</ns2:tower>

```

Figure 214: tower

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:tower xmlns:ns2="http://automatedMediaLibrary/">
  <id>2</id> <!-- The tower ID -->
  <coordinate/> See Figure 26: coordinate

```

```

<serialNumber>serialNumber</serialNumber> <!-- Tower controller serial number -->
<firmwareVersion>firmwareVersion</firmwareVersion>
<scannerPresent>true</scannerPresent>
<doorOpened>true</doorOpened>
<mode>0</mode> <!-- 1(Online), 2(Offline) -->
<state>1</state> <!-- 1(Varied On), 2(Varied Off) -->
<status>0</status> <!-- 1(Not Present), 2(Failed), 3(Not Ready), 4(Initializing), 5(Ready/Operational) -->
</ns2:tower>

```

Figure 215: usb

```

<!-- Added in version 760(i6000) -->
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:usb xmlns:ns2="http://automatedMediaLibrary/">
  <state>47</state> <!-- The USB state, this is a bit mask with the following values: -->
  <!--
  0 (No Flash Drive Installed)
  1 (The device is enabled)
  2 (The device is present/physically installed)
  4 (The device belongs to this library, it did not come from another library)
  8 (The device is mounted)
  16 (The device is in a paused state)
  32 (The device is Active and ready for backups)
  64 (The device is in a ejected state. Recommended before physically remove device from the MCB controller) -->
  <description>
    <vendor>SanDisk</vendor> <!-- The USB vendor -->
    <product>Cruzer</product> <!-- The USB product type -->
    <serialNumber>123456789</serialNumber> <!-- The USB serial number -->
    <size>8.0G</size> <!-- The USB size -->
  </ description>
  <lastConfigurationBackup>2016-12-01 03.30.01</ lastConfigurationBackup> <!-- The last time a Library
Configuration backup was run. -->
  <lastDatabaseBackup>2016-12-01 03.30.01</ lastDatabaseBackup> <!-- The last time a Library Database
backup was run. -->
  <associatedLibrarySerialNumber>123456789</associatedLibrarySerialNumber> <!-- The serial number of the
library associated with this USB device -->
</ns2:usb>

```

Figure 216: userList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:userList xmlns:ns2="http://automatedMediaLibrary/">
  </user> A list of user objects
</ns2:userList>

```

Figure 217: user

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:user xmlns:ns2="http://automatedMediaLibrary/">
  <name>JohnDoe</name>
  <password>The user's password</password> <!-- This is used when logging in and when changing the user's
password -->
  <role>1</role> <!-- -1(Ignore this field), 0 (Admin), 1 (User), 2 (Service), 3 (Guest)
  <partitionAccess>Test Partition</partitionAccess>
  <partitionAccess>Sales Partition</partitionAccess>
  <activeCount>0</activeCount>
  <ldap>false</ldap>
  <protected>false</protected><!-- Indicator of default library user. Added in version 220(i3/i6/i6H) -->
</ns2:user>

```

Figure 218: userMfaList

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:userMfaList xmlns:ns2="http://automatedMediaLibrary/"> <!--Added in versions 785(i6000), 231(i3/i6/i6H) -->
  <userMfa/> <!-- A list of userMfa objects -->
</ns2:userMfaList>
```

Figure 219: userMfa

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:userMfa xmlns:ns2="http://automatedMediaLibrary/"> <!--Added in versions 785(i6000), 231(i3/i6/i6H) -->
  <type>n</type><!--0(None), 1(TOTP) -->
  <validated>>false</validated><!-- User has successfully validated using this MFA method -->
  <info>text</info><!-- info needed for MFA, such as an email address or phone number -->
</userMfa>
```

Figure 220: userSessionList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:userSessionList xmlns:ns2="http://automatedMediaLibrary/">
  </userSession> A list of userSession objects
</ns2:userSessionList>
```

Figure 221: userSession

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:userSession xmlns:ns2="http://automatedMediaLibrary/">
  <id>3</id>
  <loginTime>2013-01-10 14:43:29 -0700</loginTime>
  <name>johndoe</name>
  <role>1</role>
  <lastActivityTime>2013-01-10 14:43:29 -0700</lastActivityTime>
  <loginFrom>10.20.9.123</loginFrom>
  <self>>false</self> <!-- This is set to true if the session belongs to the requester -->
</ns2:userSession>
```

Figure 222: vtReportList

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:vtReportList xmlns:ns2="http://automatedMediaLibrary/">
  <report>vt_2U31090031_2014-06-23_16.09.52</report> <!-- The report name -->
  <report>vt_2U31090031_2014-06-23_16.49.36</report>
</ns2:vtReportList>
```

Figure 223: windowsBlade

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:windowsBlade xmlns:ns2="http://automatedMediaLibrary/">
  <blade/> <!-- See Figure 13: blade -->
  <ipAddress>10.60.166.130</ipAddress>
  <baseVersion>The blades base firmware version</baseVersion>
  <mode>1</mode>
<!--
0(Unknown)
1(Online)
2(Offline)
-->
  <state>1</state>
<!--
```

```

0(Unknown)
1(Not Ready)
2(Becoming Ready)
3(Ready)
-->
  <status>1</status>
<!--
0(Unknown)
1(Good/Operational)
2(Invalid)
3(Missing)
4(Initializing)
-->
</ns2:windowsBlade>

```

Figure 224: windowsBladeList

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:windowsBladeList xmlns:ns2="http://automatedMediaLibrary/">
  <windowsBlade/> <!-- A list of windowsBlade objects -->
</ns2:windowsBladeList>

```

Figure 225: WSResultCode

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:WSResultCode xmlns:ns2="http://automatedMediaLibrary/">
  <code>200</code> <!-- HTTP Status code -->
  <description>OK</description> <!-- A brief description of this code -->
  <summary>Operation Completed Successfully</summary> <!-- A summary of the result of the operation -->
  <action>Upload library firmware</action> <!-- A description of the action/operation that was requested -->
  <customCode>0</customCode> <!-- An optional custom code -->
</ns2:WSResultCode>

```

7. WSResultCode Custom Codes

The Scalar i6000, i3 and i6/i6H WSResultCode object contains a customCode element which may provide more information when an error occurs for any given Web Service request. On the Scalar i6000 a customCode is only used when a Web Services request encounters an error, regardless of it being a client or server problem.

The Scalar i3/i6/i6H will always return a custom code, where custom code 0 (zero) means, "Operation completed successfully".

The Scalar i6000 returns a custom code only when available. If a custom code is not available, a value of 0 (zero) will be returned.

The following tables list the custom codes and describe their meaning.

Table 472: Scalar i6000 SCSI Custom Codes 10000 – 80000

The Scalar i6000 supports few general purpose custom codes, but reports an extensive set for errors that are also reported and defined for SCSI sense data reporting. In general, custom codes above decimal 10,000, have a SCSI ASC/ASCQ code equivalent value, which can be calculated with the following formula: ASC/ASCQ=HEX (custom code – 10000).

ASC	ASCQ	Custom Code	Description
		211	File exceeded the maximum size allowed by e-mail server.
		10001	Reservation Conflict
00h	17h	10023	Drive requests cleaning
04h	00h	11024	Robotics not ready due to an unknown cause
04h	01h	11025	Robotics are becoming ready
04h	03h	11027	Robotics not ready; manual intervention required
04h	83h	11155	Robotics not ready; aisle power disabled
04h	8Dh	11165	Robotics not ready
15h	01h	15377	Robotics positioning error
15h	80h	15504	Robotics dropped a cartridge
15h	81h	15505	Robotics could not pick a cartridge
15h	83h	15507	Robotics could not place a cartridge
15h	84h	15508	Move completed with cartridge Get recoveries
15h	85h	15509	Move completed with cartridge Put recoveries
15h	86h	15510	Move completed but cartridge was placed in alternate location
15h	91h	15521	Media stranded in picker
15h	92h	15522	Media stranded in picker
15h	93h	15523	Operation needs to be retried
1Ah	00h	16656	Logic error: Parameter list length error
20h	00h	18192	Logic error: Illegal OpCode in CDB
21h	01h	18449	Logic error: Invalid element address in CDB
24h	00h	19216	Logic error: Invalid field in CDB
24h	80h	19344	Logic error: Attempt to write a read only buffer
25h	00h	19472	Logic error: Illegal LUN
26h	00h	19728	Logic error: Invalid field in Parameter List
26h	01h	19729	Logic error: Parameter not supported
26h	02h	19730	Logic error: Parameter value invalid

26h	80h	19856	Logic error: Parameter data checksum failure
26h	81h	19857	Logic error: Parameter value already in use
28h	00h	20240	Robotics transitioned to ready state: Element status may have changed.
28h	01h	20241	Insert/Eject area opened and closed: I/E element status may have changed
29h	00h	20496	Power-on or reset occurred
29h	01h	20497	Power on occurred
29h	04h	20500	Internal reset occurred
29h	81h	20625	Library reset into degraded mode of operation
2Ah	01h	20753	Mode parameters have been changed
2Ah	80h	20880	Library inventory completed
30h	00h	22288	Incompatible medium installed
30h	07h	22295	Cleaning failure
30h	82h	22418	Drive cleaning operation complete
30h	90h	22432	Drive firmware update complete
30h	91h	22433	Drive firmware update failed
30h	92h	22434	Invalid firmware image
3Bh	0Dh	25117	Destination element is full
3Bh	0Eh	25118	Source element is empty
3Bh	12h	25122	Media magazine not installed
3Bh	85h	25237	Logic Error: Destination of MOVE cannot be picker
3Bh	A0h	25264	Logic error: Media type does not match destination media type
3Eh	00h	25872	Robotics discovery/teach not complete
3Eh	03h	25875	Robotics self-test failed
3Fh	01h	26129	New firmware loaded
3Fh	04h	26132	Drive added
3Fh	80h	26256	EEPROM failed to erase
3Fh	84h	26260	EEPROM program failure
3Fh	90h	26272	Robotics status changed
3Fh	91h	26273	Robotics access timer started
3Fh	92h	26274	Robot replacement succeeded
3Fh	93h	26275	Robot replacement failed
3Fh	94h	26276	Replacement robot detected
40h	80h	26512	Component failure
40h	91h	26529	Gripper failure
40h	A0h	26544	Robotics vertical axis motion failure
40h	A1h	26545	Robotics vertical axis homing failure
40h	B0h	26560	Robotics horizontal axis motion failure
40h	B1h	26561	Robotics horizontal axis homing failure
40h	C0h	26576	Robotics motion failure
40h	E0h	26608	Robotics power failure
44h	00h	27408	Internal logic failure
44h	81h	27537	Drive communication not established
44h	82h	27538	Drive communication lost
44h	83h	27539	Drive powered off
4Ch	00h	29456	Robotics discovery/teach failure
53h	00h	31248	Drive did not load or unload a tape cartridge
53h	01h	31249	A drive did not unload a tape cartridge
53h	02h	31250	A drive is preventing media removal
53h	80h	31376	Tape cartridge in I/E station not properly inserted

53h	81h	31377	Insert/Eject station door is open
53h	82h	31378	I/E station lock failure
53h	83h	31379	I/E station unlock failure
53h	84h	31380	Medium in drive is unloaded and robot accessible
5Dh	00h	33808	Tape Alert reported or failure prediction threshold exceeded
83h	00h	43536	Barcode label too short or too long
83h	01h	43537	Cannot read a barcode label due to scanner problem
83h	02h	43538	Barcode label questionable
83h	03h	43539	Cell status and barcode label questionable
83h	04h	43540	Drive not installed
83h	05h	43541	Drive varied off and not accessible for library operations
83h	06h	43542	Element temporarily inaccessible for library operations.
83h	07h	43543	Tower is offline
83h	08h	43544	Tower transitioned to online
83h	09h	43545	Drive is offline
83h	0Ah	43546	Drive transitioned to online
83h	0Bh	43547	Drive enabled library managed encryption
83h	0Ch	43548	Drive enabled application managed encryption
83h	0Dh	43549	Drive assigned valid Ethernet IP address
83h	0Eh	43550	Drive disabled encryption

Table 473: Scalar i3/i6/i6H Custom Codes

The Scalar i3/i6/i6H return a customCode for each request. A custom code of 0-3 indicates successful completion of the request. All other custom codes denote the type of error encountered while processing the request.

Code	Supported	Description
0	i3/i6/i6H	Operation completed successfully.
1	i3/i6/i6H	Resource successfully created.
2	i3/i6/i6H	Operation to be started.
3	i3/i6/i6H	The URI is correct, but the functionality specified is not supported by the library. The summary will indicate the functionality is not supported by a Scalar i3 or both a Scalar i3 and a Scalar i6.
100	i3/i6/i6H	The functionality requested by this method and URI is not yet implemented in Scalar i3/i6/i6H.
101	i3/i6/i6H	Unable to connect to database.
110	i3/i6/i6H	The request method type was invalid for the URI. Comma delimited, valid method types ('GET', 'POST', 'PUT', 'DELETE') will be included in the summary.
120	i3/i6/i6H	The URI is invalid and included malformed syntax. It could be caused by a typo, or an invalid combination of path resource parameters. The summary attempts to identify which part of the URI is problematic. It will include the URI resource that is undefined, and for which expected resource. In some cases, the expected resource is a user defined value.
121	i3/i6/i6H	The URI is invalid. The URI path is incomplete and additional resource parameter(s) are required. The summary will include the possible resource parameters (comma delimited) for the URI received.
122	i3/i6/i6H	The URI is invalid and the Web Services cannot determine the error. This error currently occurs only on POST device blade LTFS reports requests. The summary will include the method and resource.
123	i3/i6/i6H	The web services cannot process the request, because the Content-Type

		header in the request message is invalid or missing for the method and URI. The type header expected will be included in the summary ('application/json', 'application/xml', etc.)
125	i3/i6/i6H	An invalid data object was received in the request message data. Generally, this indicates the data object is missing required elements or the combination of elements is not valid. The summary will include an indication of the error.
126	i3/i6/i6H	The request message for this method and URI requires data and none was received.
127	i3/i6/i6H	An invalid query string was given on the URI. Generally, this is indicative of a problem with the number of query parameters. The error in the summary will indicate the problem: too many query parameters, too few, parameters used together that are mutually exclusive, etc.
128	i3/i6/i6H	A URI query string parameter was found which is not valid for this method and URI. The invalid parameter and the expected parameters are included in the summary.
129	i3/i6/i6H	A value given for a URI query string parameter was invalid. The value may be undefined or out of range. The invalid value and the parameter are included in the summary.
130	i3/i6/i6H	The URI requires a query string to be appended. The summary will indicate the required parameter.
131	i3/i6/i6H	The request data contained invalid XML. The summary will include the error.
132	i3/i6/i6H	The request data contained invalid JSON. The summary will include the error.
133	i3/i6/i6H	The root node in the XML request data was invalid. The received and expected tags are included in the summary.
135	i3/i6/i6H	The operation requested for a user resource was invalid. This indicates the user specified is a protected account (i.e. service or admin). The summary includes the attempted operation and the username.
136	i3/i6/i6H	The partition specified in the request is invalid for the operation. The partition name and the reason the partition is invalid will be included in the summary.
137	i3/i6/i6H	The operation could not be completed because either no control path has been configured for the partition or the control path drive is varied off.
138	i3/i6/i6H	The slot or location specified in the request is invalid for the operation. The summary will indicate the reason the slot is invalid.
139	i3/i6/i6H	The drive included in the request was not valid for the operation. Generally, this indicates the drive was in the wrong state for the operation requested. The summary will indicate the reason the drive is invalid.
140	i3/i6/i6H	The operation could not be initiated due to an invalid state. The operation and the invalid state will be included in the summary.
141	i3/i6/i6H	Date and time values may not be updated with NTP enabled.
144	i3/i6/i6H	Server values may not be updated with NTP disabled.
146	i3/i6/i6H	A specified data element value (drive serial number, partition, etc.) included in the request data was not found. The summary will include the data element and the value that was not found.
147	i3/i6/i6H	A data value included in the request data failed validation. Typically, this error is returned to indicate a value that is out of range, is incorrectly formatted, or is not defined for the element. The summary will include the element name and either the expected value(s) or the reason the value is invalid.
148	i3/i6/i6H	The user's role does not have permission for this functionality or the user role has not been granted access to the partition. The operation will be included in the summary.
149	i3/i6/i6H	Either an invalid coordinate object was received, or the coordinate provided is of the wrong type for the operation. The summary will indicate the error and may include the type of coordinate.

153	i3/i6/i6H	An email address included in the request data has an invalid format. The e-mail address will be included in the summary.
154	i3/i6/i6H	The operation failed due to a capacity overflow error. The library encountered an error and was unable to process the request. If additional information is available for the error, it will be included in the summary.
155	i3/i6/i6H	The operation failed. If there is a reason available to the Web Services, it will be included in the summary.
156	i3/i6/i6H	A library error prevented the retrieval of the resource.
157	i3/i6/i6H	The library is not licensed for the functionality requested. The license type will be included in the summary and the operation may be included.
160	i3/i6/i6H	Close RAS ticket failed. Tickets must be in an open state to be closed. The id of the ticket is included in the summary.
164	i3/i6/i6H	A filter has been specified that is not defined by the report type. The reason will be included in the summary.
166	i3/i6/i6H	The control path drive specified for the operation is invalid. The drive's serial number and the reason the drive is invalid will be included in the summary.
167	i3/i6/i6H	The upgrade request is invalid due to the specified reason.
168	i3/i6/i6H	The data object in the request message data included an unknown data element. The element name will be included in the summary.
169	i3/i6/i6H	The IP address given in the request data was invalid.
170	i3/i6/i6H	DNS is not configured, and the request data requires a valid IP address.
171	i3/i6/i6H	A setting failed to update. The failed setting will be included in the summary. If any additional information is available on the failure it will be included in the summary.
172	i3/i6/i6H	A resource (partition, user, etc.) could not be created because a resource with the same identifier already exists. The resource and the resource's identifier will be included in the summary.
173	i3/i6/i6H	The request was attempting to delete or test one of the protected system email addresses. The summary will include the operation and the email address.
175	i3/i6/i6H	The drive log was unable to be pulled. The summary will include the drive serial number and the reason returned by the library.
177	i3/i6/i6H	The certificates uploaded were not as expected and could not be installed. The reason will be included in the summary.
178	i3/i6/i6H	The encryption certificate failed to install. The summary will include the filename and the reason for the failure.
184	i3/i6/i6H	The scratch slot received was not valid for the test. Either the slot specified was invalid, or the slot was empty. The summary will include the reason.
185	i3/i6/i6H	An EKM configuration already exists.
186	i3/i6/i6H	The server type is not configured.
187	i3/i6/i6H	No encryption certificates are installed for the currently configured encryption key server type.
188	i3/i6/i6H	One or more encryption certificates for the currently configured encryption key server type has expired.
189	i3/i6/i6H	The operation requested requires the partition to be offline. The operation will be included in the summary.
190	i3/i6/i6H	On an update of an EKM policy, the servers could not be configured. The reason is optional and will only be included in the summary for SKM servers. No reason is included for KMIP – the reason should be available in a RAS Ticket.
191	i3/i6/i6H	The request failed because one or more drives were loaded. The summary will include the operation that failed and a comma delimited list of serial numbers of the loaded drives.

192	i3/i6/i6H	The drive firmware upgrade failed for one or more drives. The summary will include a comma delimited list of drive serial numbers and the library error code.
193	i3/i6/i6H	Key file not found for CSR.
194	i3/i6/i6H	The file uploaded was not a valid certificate file. The filename will be included in the summary.
195	i3/i6/i6H	A private key for the latest generated CSR is maintained on the library and the certificate does not match this private key.
196	i3/i6/i6H	The certificate date on the uploaded file was invalid. The summary will indicate whether the start or end date is invalid and the date value of the certificate.
197	i3/i6/i6H	On an update of an EKM policy, one or more SKM servers could not be configured. The servers were not available.
198	i3/i6/i6H	The request failed due to the configuration of the drives. The operation (add drive/remove drive) and the reason will be included in the summary. If a drive is not connected to an LTFS partition, it may not be added to the partition. If the drive is connected to an LTFS partition, it may not be removed.
199	i3/i6/i6H	Invalid request due to the current FIPS configuration. The operation and the reason will be included in the summary.
200	i3/i6/i6H	The request failed because the library is not ready. The operation may be included in the summary.
201	i3/i6/i6H	The request cannot be processed until the library has completed initialization. The summary will include the operation that failed.
202	i3/i6/i6H	The server IP address or host name failed validation. The invalid value will be included in the summary.
203	i3/i6/i6H	Partitions are configured with this server type, unable to delete.
204	i3/i6/i6H	CSR was unable to be generated.
205	i3/i6/i6H	The request failed due to a configuration error. The operation and the reason for the failure will be included in the summary.
206	i3/i6/i6H	The request was found to be invalid by the library during processing. The library error is included in the summary.
207	i3/i6/i6H	Invalid request due to current key set configuration. The operation on the key set could not be initiated due to the current state. The summary will include the required state of the key set.
208	i3/i6/i6H	The e-mail server is not configured.
209	i3/i6/i6H	The diagnostic test was unable to be started while one was in progress.
210	i3/i6/i6H	An LDAP test failed verification. The reason may be included in the summary if available to the Web Services.
211	i3/i6/i6H	The file exceeded the maximum size allowed by the e-mail server.
212	i3/i6/i6H	The e-mail failed with an email server error. If a server error is available to the Web Services, it will be included in the summary.
214	i3/i6/i6H	A move including an IE reassignment failed to reassign the partition, although the move was successful. If available, the library error is included in the summary.
215	i3/i6/i6H	An update to the number of IE slots failed due to an invalid request.
216	i3/i6/i6H	This is returned on operations that consume licenses. The library may be licensed for the functionality, but the number of unused licenses is not sufficient to perform the operation. The summary may include the type of license.
217	i3/i6/i6H	Server configuration may not be changed while partitions have LME enabled.
218	i3/i6/i6H	The operation failed because the drive is currently unavailable. The drive may not be present, or it may still be initializing. The serial number will be included in the summary.

219	i3/i6/i6H	The media specified in the request is not valid for the operation. The reason will be included in the summary.
220	i3/i6/i6H	A remove blade failed because the blade was still detected in the library. The blade type (Windows/LTFS) and the section number of the blade will be included in the summary.
221	i3/i6/i6H	The operation failed; the library returned a busy error. The library error message is included in the summary.
222	i3/i6/i6H	There are insufficient slots to perform this operation
223	i3/i6/i6H	There are insufficient drives to perform this operation
224	i3/i6/i6H	The operation is unable to be performed due to an empty slot.
225	i3/i6/i6H	The operation is unable to be performed due to a full slot. The coordinate is included in the summary.
226	i3/i6/i6H	The operation is unable to be performed due to one or more full slots.
230	i3/i6/i6H	The uploaded file was invalid. The type of file (restore image, firmware file, etc.) will be included in the summary. Additional information about the failure, if available, will be also included.
231	i3/i6/i6H	A file being downloaded to the library from the website failed verification. The filename and reason are included in the summary. A checksum or file size error can occur if a network glitch interrupts the download.
234	i3/i6/i6H	A file failed to upload to the library. The upload error and error code will be returned in the summary.
240	i3/i6/i6H	The license key is invalid and unable to be installed.
241	i3/i6/i6H	The license key is a duplicate. The license has already been applied. No changes were made to the library configuration.
242	i3/i6/i6H	The license key has expired and was unable to be installed.
243	i3/i6/i6H	The license key's start date is too far in the future and was unable to be installed. Check the date on the library before trying again.
251	i3/i6/i6H	The Web Services is unable to communicate with the blade. Either the blade is offline, initializing, or is in the process of going down.
300	i3/i6/i6H	The resource specified by the URI was not found. The resource type (drive, media, partition, etc.) and the resource's identifier will be included in the summary. Note that this is returned only for resources identified by the URI or the query string on the URI. For example, /aml/partition/{partitionName} or /aml/media?partition={partitionName}.
301	i3/i6/i6H	The Web Services encountered an unexpected error and was unable to process the request. The summary will indicate the error.
302	i3/i6/i6H	The library encountered an error and was unable to complete the request. The reason will be included in the summary.
305	i3/i6/i6H	The request was an invalid for an IE slot. The reason will be included in the summary.
306	i3/i6/i6H	Cross partition moves are not supported.
307	i3/i6/i6H	The move media request was invalid. Media may not be moved from a storage slot in an LTFS partition to an IE slot.
308	i3/i6/i6H	The request attempted to perform an invalid move. The reason will be included in the summary.
309	i3/i6/i6H	Only incompatible media may be exported from an LTFS partition via a move media request. The blade is currently not in a state to determine the media's eligibility. Wait until the blade is online and ready before attempting the export.
400	i3/i6/i6H	Move media failed, cell obstructed.
401	i3/i6/i6H	Move media failed, lost tape.
402	i3/i6/i6H	Move media failed, a motion failure.
403	i3/i6/i6H	Move media failed, picker obstructed.

404	i3/i6/i6H	Move media failed, X-Axis failure.
405	i3/i6/i6H	Move media failed, Y-Axis failure.
406	i3/i6/i6H	Move media failed, Z-Axis failure.
407	i3/i6/i6H	Move media failed, Z-Axis retract failure.
408	i3/i6/i6H	Move media failed, Z-Axis extend failure.
409	i3/i6/i6H	Move media failed, Theta-Axis failure
410	i3/i6/i6H	Move media failed, X Motor fault.
411	i3/i6/i6H	Move media failed, an inaccessible slot.
412	i3/i6/i6H	Move media failed, an inaccessible slot; the magazine is open.
413	i3/i6/i6H	Move media failed, an inaccessible slot; prevent media removal is enabled.
414	i3/i6/i6H	Move media failed, an inaccessible slot; IE is missing.
415	i3/i6/i6H	Move media failed, an inaccessible slot; drive is missing.
416	i3/i6/i6H	Move media failed, picker is full.
417	i3/i6/i6H	Move media failed, duplicate move.
418	i3/i6/i6H	Move media failed, recover slot is full.
419	i3/i6/i6H	Move media failed, Robotics Control System timeout.
420	i3/i6/i6H	Move media failed, Robotics Control System device missing.
421	i3/i6/i6H	Move media failed, X home failure.
422	i3/i6/i6H	Move media failed, Y home failure.
423	i3/i6/i6H	Move media failed, Z home failure.
424	i3/i6/i6H	Move media failed, Theta home failure.
425	i3/i6/i6H	Move media failed, picker unknown.
426	i3/i6/i6H	Move media failed, picker empty.
427	i3/i6/i6H	Move media failed, picker failure.
428	i3/i6/i6H	Move media failed, Y retry.
429	i3/i6/i6H	Move media failed, no response from picker.
430	i3/i6/i6H	Move media failed, tape in drive.
431	i3/i6/i6H	Move media failed, no home slot.
432	i3/i6/i6H	Move media failed, cleaning required.
433	i3/i6/i6H	Move media failed, the destination slot is full.
434	i3/i6/i6H	Move media failed, the source slot is empty.
500	i3/i6/i6H	The operation failed. The library encountered an error (illegal state).
501	i3/i6/i6H	The operation failed. The library encountered an error (invalid opcode).
502	i3/i6/i6H	The operation failed. The library encountered an error (invalid parameter).
503	i3/i6/i6H	The operation failed. The library encountered a hardware failure.
504	i3/i6/i6H	The operation failed. The library encountered a firmware error.
505	i3/i6/i6H	The operation failed. The library encountered a subcomponent failure.
506	i3/i6/i6H	The operation failed. The drive failed to load.
507	i3/i6/i6H	The operation failed. The drive failed to unload.
508	i3/i6/i6H	The operation failed. The IE lock failed.
509	i3/i6/i6H	The operation failed. The IE unlock failed.
510	i3/i6/i6H	The operation failed. The door is open.
511	i3/i6/i6H	The operation failed. The slot has not been assigned to any library.
512	i3/i6/i6H	The operation failed. The drive unload request was rejected by the drive
513	i3/i6/i6H	The operation failed. The slot ID is invalid.
514	i3/i6/i6H	The operation failed. The source element is not ready.
515	i3/i6/i6H	The operation failed. The destination is not ready.
516	i3/i6/i6H	The operation failed. A Get failed.
517	i3/i6/i6H	The operation failed. A Put failed.
518	i3/i6/i6H	The operation failed. Robotics Control System checksum failed.
519	i3/i6/i6H	The operation failed. Robotics Control System is not ready.

520	i3/i6/i6H	The operation failed. Robotics Control System not allowed.
521	i3/i6/i6H	The operation failed. Calibration tab not found.
522	i3/i6/i6H	The operation failed. Robotics Control System unexpected reset.
523	i3/i6/i6H	The operation failed. RST failed.
524	i3/i6/i6H	The operation failed. Robotics Control System unlock failed.
525	i3/i6/i6H	The operation failed. There are not enough empty storage slots for bulk import.
526	i3/i6/i6H	The operation failed. Not enough empty I/E slots available for requested operation.
527	i3/i6/i6H	The operation failed. A limit check failed and prevented successful operation.
528	i3/i6/i6H	The operation failed. The I/E slot requested is not owned by the system.
529	i3/i6/i6H	The operation failed. The scanner failed.
530	i3/i6/i6H	The operation failed. The door is open; unable to import/export media.
531	i3/i6/i6H	The operation failed. No barcode was detected.
533	i3/i6/i6H	The operation failed. The shipping restraint is still installed.
534	i3/i6/i6H	The operation failed. The prevent media removal request is currently active for the drive and/or library.
700	i3/i6/i6H	MFA authorization failed.
705	i3/i6/i6H	The user password must be changed before continuing the user session.
706	i3/i6/i6H	The password change failed. The reason will be included in the summary.
1000	i3/i6/i6H	The user account does not exist or the password is invalid.
1001	i3/i6/i6H	Invalid credentials. The request data does not include required elements.
1004	i3/i6/i6H	Service in progress. The system is unavailable at this time.
1005	i3/i6/i6H	Already logged in on the web client -- Login not allowed.
1006	i3/i6/i6H	Unable to communicate with the LDAP server.
1025	i3/i6/i6H	A library software update is in progress. The system is unavailable at this time.
1026	i3/i6/i6H	Unable to communicate with the LDAP server.
1029	i3/i6/i6H	Diagnostics in progress. The system is unavailable at this time
1046	i3/i6/i6H	The account is locked due to the number of failed login attempts.
1099	i3/i6/i6H	The user account is disabled.

8. Appendix A – Web Service Request Examples

8.1 Linux Curl Script Example

The following script, MyWebServiceScript.sh, provides an example using curl in a bash scripted command line utility to accept a tape library IP address, login credentials and a drive coordinate to log in, check and display a drive state, then log out.

```
#!/bin/bash
#
# Copyright 2020 Quantum Corporation. All rights reserved.
#
# This script is a template to issue Quantum Scalar Automation webservice #
commands
#
#####
# Variable Definitions
#####
## Command line options
LIBRARY_ADDRESS="" # l option
LIBRARY_PASSWORD="" # p option

# options with defaults
LIBRARY_USER="admin" # u option
DRIVE_COORDINATE="1,1,5,1,1" # d option

## curl option
CURL_ALLOW_INSECURE="--insecure"

## get current directory
PATHWD=`pwd`

## The cookie file is created when the user logs in and is used for
subsequent requests
COOKIE_FILE=$PATHWD/scalarCookies.txt

## Use for debugging curl statements . The http response is captured in
this file.
OUTFILE=$PATHWD/scalarWSout.txt

## define protocol
PROTOCOL="https://"

#####
# Do not change
# Wrapper to run a cli command
# Use this runCommand function to run curl commands - it provides error
checking
#####
runCommand()
{
    local command="$1";
    echo "RUNNING COMMAND: \"$command\""
    COMMAND_OUTPUT=`eval $command 2>&1`
}
```

```

COMMAND_EXIT_STATUS=$?
    if [ $COMMAND_EXIT_STATUS -ne 0 ]; then
        echo "Exit Status: $COMMAND_EXIT_STATUS"
        echo "ERROR ON COMMAND: \"$command\""
        echo "$COMMAND_OUTPUT"
        exit $COMMAND_EXIT_STATUS
    fi
    echo "success"
}

#####
# Do not change
# This code displays help text when the '?' arg is input
#####
usage()
{
    echo "Usage: $0 [OPTIONS...]"

    OPTIONS:
        -l <library address> required. Specifies library ip address or DNS
name
        -u <user> optional. Specifies user name for library login
           defaults to "admin\"
        -p <password> required. Specifies user password
        -d <drive coordinate> required.

    Typical usage example:
        ./MyWebServiceScript.sh -l \"10.20.174.208\" -u admin -p password -
d \"1,1,1,1,1\"
        ";

    exit 1;
}

#####
# Do not change
# This code process arguments passed into the script
#####
if [ $# -eq 0 ]; then
    usage
else
    while getopts "l:p:u:d:" opt
    do
        case "$opt" in
            l) LIBRARY_ADDRESS="$OPTARG"
               ;;
            p) LIBRARY_PASSWORD="$OPTARG"
               ;;
            u) LIBRARY_USER="$OPTARG"
               ;;
            d) DRIVE_COORDINATE="$OPTARG"
               ;;
            *) usage
               ;;
        esac
    done

```

```

        esac
    done
fi

#####
# Do not change
# This function logs into the library and saves the cookie to a file
#####
doLibraryLogin()
{
    runCommand "curl -X POST -c $COOKIE_FILE -o $OUTFILE -w \"${http_code}\"
-sL -H 'Accept: application/json' -H 'content-type: application/json' -d
'{"name\":\"$LIBRARY_USER\", \"password\":\"$LIBRARY_PASSWORD\"}'
${CURL_ALLOW_INSECURE} ${PROTOCOL}${LIBRARY_ADDRESS}/aml/users/login"

    if [ "$COMMAND_OUTPUT" != "200" ]; then
        echo "Http Status Code: $COMMAND_OUTPUT"
        doLibraryLogout
        exit 1
    fi
}

#####
# Do not change
# This function logs out of the library so the session is closed on the
server
#####
doLibraryLogout()
{
    runCommand "curl -X DELETE -b $COOKIE_FILE -o $OUTFILE -w
\"${http_code}\" -sL ${CURL_ALLOW_INSECURE}
${PROTOCOL}${LIBRARY_ADDRESS}/aml/users/login"
    if [ "$COMMAND_OUTPUT" != "200" ]; then
        echo "Http Status Code: $COMMAND_OUTPUT"
        exit 1
    fi
}

#####
# Do not change
# This function displays the last REST command's output to the screen
#####
doDisplayOutput()
{
    ## Display output
    cat $OUTFILE
    printf "\n"
    printf "\n"
}

#####
##### Main Line - executes the following commands - script main line
#####

```



```

#####
# Setup the environment for the script execution
#####
## Remove the old cookie files and result files
rm $COOKIE_FILE
rm $OUTFILE

## login, get session cookie
doLibraryLogin
doDisplayOutput

#####
# Add user defined functions here
#####

doLibraryPing()
{
### http://10.20.174.208/aml
    runCommand "curl -X GET -b $COOKIE_FILE -o $OUTFILE -w \"%{http_code}\"
-sL -H 'Accept: application/json' ${CURL_ALLOW_INSECURE}
${PROTOCOL}${LIBRARY_ADDRESS}/aml"

    if [ "$COMMAND_OUTPUT" != "200" ]; then
        echo "Http Status Code: $COMMAND_OUTPUT"
        doLibraryLogout
        exit 1
    fi
}

doGetDriveState()
{
### http://10.20.174.208/aml/drive/1,1,1,1,1/operations/state
    runCommand "curl -X GET -b $COOKIE_FILE -o $OUTFILE -w \"%{http_code}\"
-sL -H 'Accept: application/json' ${CURL_ALLOW_INSECURE}
${PROTOCOL}${LIBRARY_ADDRESS}/aml/drive/${DRIVE_COORDINATE}/operations/stat
e"

    if [ "$COMMAND_OUTPUT" != "200" ]; then
        echo "Http Status Code: $COMMAND_OUTPUT"
        doLibraryLogout
        exit 1
    fi
}

#####
# Add user defined function calls AFTER this line to execute desired
webservices
#####

## discover/ping library
doLibraryPing
doDisplayOutput

## show selected drive state

```

```
doGetDriveState
doDisplayOutput

#####
# Add user defined functions BEFORE this line to execute desired
webservices
#####

#####
# Tear down the environment for the script execution
#####
## logout
doLibraryLogout
doDisplayOutput

echo "SUCCESS: Script complete"
exit 0
```

8.2 Windows PowerShell Script Example

The following PowerShell script, *Rest-Example.ps1*, provides an example for a command line utility to accept a tape library IP address, login credentials and a partition name, to perform various user session and access configurations.

```
# Powershell Script for Scalar i6000 / Scalar i3/i6/i6H Libraries
#
# Requires Powershell version 3 or greater.
#
# Script prompts for library address, user credentials, partition name
# Issues HTTPS requests to the library using Invoke-WebRequest
#
# To set ps execution policy
# Set-ExecutionPolicy Unrestricted -Scope CurrentUser
#
# Demonstrates:
# - Creating a user session with a login
# - GET, DELETE requests for all users
# - PUT, POST for admin user
# - JSON and XML formatted requests and response data examples
# - Setting request headers
# - Using Response data from JSON and XML
# - Error Handling
# - Delete Session (logoff)

[cmdletbinding()]
Param (

    [switch]$help,
    [switch]$h
)

$ProgressPreference = 'SilentlyContinue'

if ($help -OR $h){

    Write-Host "`nScalar i3/i6/i6H Library Rest Example" -ForegroundColor Yellow
    Write-Host "Prerequisite: PowerShell Version 3 `n"
    Write-Host "Usage: Rest-Example [-Help] [-Debug] "
    Write-Host "    -Help | -h: Print this usage and exit."
    Write-Host "    -Debug: enable debug logging.`n"

    exit
}

if ($DebugPreference -eq 'Inquire' )
{
    $DebugPreference = "Continue"
    Write-Host "`n"
}
}
```

```

$psMajor = $PSVersionTable.PSVersion.major
$psMinor = $PSVersionTable.PSVersion.minor

# exit if PS3 or greater is not installed
if ($psMajor -lt 3){
    Write-Host "`nPowerShell Version 3 or greater is required for this script. (Powershell Version
$psMajor.$psMinor installed.)" -ForegroundColor Red
    Write-Host "`nExiting ...`n"
    exit
}

# Function Get-WS-Error
# Param $str Exception string
# Parse an error string for the ws error
# Returns string (empty string if a ws error is not found)
function Get-WS-Error([string] $str)
{
    $errorMsg = ""
    try{

        $pos = $str.IndexOf("<ns2:WSResultCode")
        $rpos = $str.LastIndexOf("WSResultCode>")
        if ($pos -gt 0 -and $rpos -gt 0)
        {
            $last = $rpos - $pos
            $ss = $str.Substring($pos, $last+13)

Write-Host "`nWS Error Response"

                $xml = [xml]$ss
Write-XML $ss
                $errorMsg = $xml.WSResultCode.summary
            }
        }catch{}

    return $errorMsg
}

# Sends a Delete Request for a given URI
function Delete-Request ( [string] $uri, [Microsoft.PowerShell.Commands.WebRequestSession] $session)
{
    try{

Write-Host("`nDELETE: $uri")

        # Request message data with json data
        # Add an accept application/json header to get response in json
        $response = Invoke-WebRequest $uri -WebSession $session -ContentType 'application/json' -
Body $json -Method 'DELETE' -ErrorVariable RespErr
    }
}

```

Write-XML \$response

```
    }catch{
        $status = $_.Exception.Response.StatusCode.value__
        $errorMsg = "`nThe delete request failed. "
# 400 Bad Request or 500 Internal Server Error, check the response for a ws error
        if ($status -ge 400){
            $s = [string] $RespErr
            $wsErr = Get-WS-Error $s
            $errorMsg = $errorMsg + $wsErr
        }else{
            Write-Host $_.Exception
        }
        Write-Host "$errorMsg `n" -ForegroundColor Red
    }finally{
        Write-Host "`n-----`n"
    }
}
```

Sends a PUT Request with XML-formatted data

```
function Send-Put-XML-Request ([String] $uri, [String] $xmlString,
[Microsoft.PowerShell.Commands.WebRequestSession] $session)
```

```
{
    $success = $false
    try{

        Write-Host("`n-----`n`nUpdate: PUT $uri")
        # Request message data, with value to change

        Write-Host("`nPUT Request Data: $xmlString")

            $response = Invoke-WebRequest $uri -WebSession $Session -ContentType 'application/xml' -
Body $xmlString -Method 'PUT' -ErrorVariable RespErr
            $success = $true
        }catch{

            Write-Debug $_.Exception
        }

        return $success
    }
}
```

Sends a POST Request with JSON formatted data

```
function Send-Post-Json-Request ( [string] $uri, $json, [Microsoft.PowerShell.Commands.WebRequestSession]
$session)
```

```
{
    $success = $true
    try{

        Write-Host("`nPOST: $uri")
    }
}
```

```

Write-Host "`n$json"

# Request message data with json data
# Add an accept application/json header to get response in json
$response = Invoke-WebRequest $uri -WebSession $session -ContentType 'application/json' -
Body $json -Method 'POST' -ErrorVariable RespErr
Write-XML $response

}catch{
    $success = $false
    $status = $_.Exception.Response.StatusCode.value__
    $errorMsg = "`nThe request failed. "
    # 400 Bad Request or 500 Internal Server Error, check the response for a ws error
    if ($status -ge 400){
        $s = [string] $RespErr
        $wsErr = Get-WS-Error $s
        $errorMsg = $errorMsg + $wsErr
    }else{
        Write-Host $_.Exception
    }
    Write-Host "$errorMsg `n" -ForegroundColor Red
}
return $success
}

```

```

# Write-Host pretty formatted XML
# Param $xml data to write to stdout
function Write-XML ([xml]$xml, $response=$true)
{
    $indent = 2
    if ($response){
        Write-Host "`nXML Response: `n"
    }
    $StringWriter = New-Object System.IO.StringWriter
    $XmlWriter = New-Object System.Xml.XmlTextWriter $StringWriter
    $xmlWriter.Formatting = "indented"
    $xmlWriter.Indentation = $indent
    $xml.WriteContentTo($XmlWriter)
    $XmlWriter.Flush()
    $StringWriter.Flush()
    Write-Host $StringWriter.ToString()
}

```

```

#
# Rest-Example (Main)
#
# Prompts user for library IP, credentials
# Creates a user session (login) via the webservice and does the following:
# - Gets system remote access settings

```

```

# - Resets the system setting
# - Creates a partition, deletes partition
# - Deletes the user session (logoff)
#
# Prints to std out URIs, response and request data

# Ignore self-signed cert
# This is required if the client has not created/installed a signed cert

# saving user's current certificate policy and security protocol, to be reset at the end of the script
$currentCertificatePolicy = [System.Net.ServicePointManager]::CertificatePolicy
add-type @"
    using System.Net;
    using System.Security.Cryptography.X509Certificates;
    public class TrustAllCertsPolicy : ICertificatePolicy {
        public bool CheckValidationResult(
            ServicePoint srvPoint, X509Certificate certificate,
            WebRequest request, int certificateProblem) {
            return true;
        }
    }
"@

[System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicy
$certPolicy = [System.Net.ServicePointManager]::CertificatePolicy
$currentSecProtocol = [Net.ServicePointManager]::SecurityProtocol
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 -bor
[Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::Tls
$secProtocol = [Net.ServicePointManager]::SecurityProtocol

Write-Debug "Security Protocol : $secProtocol"
Write-Debug "Certificate Policy : $certPolicy"

# Get library address
Write-Host "`n---- Scalar i3/i6/i6H REST Example ----"
Write-Host "`n(Use <Ctrl>C to quit)`n`n" -ForegroundColor Yellow

Write-Host "`nEnter Library IP Address: " -ForegroundColor Yellow -NoNewline
$ip = Read-Host

try{

    # Ping library
    # /aml is a GET Request which does not require a user session (no login needed)
    # Used to detect library type, serial number
    # With no Accept header, GET requests default to XML formatted response

    Write-Host "`n`nGET https://$ip/aml"

    # No -Method on the Request, defaults to GET

```

```

$response = Invoke-WebRequest "https://$ip/aml"

$xml = [xml] $response
Write-XML ($xml)
# $library = $xml.ping.serialNumber
# $type = $xml.ping.productName

# Same ping request, JSON formatted response
# Add an Accept header
$response = Invoke-WebRequest "https://$ip/aml" -Headers @{"accept"="application/json"}
Write-Host "`n JSON Response: $response"
$json = ConvertFrom-Json -InputObject $response
$library = $json.serialNumber
$type = $json.productName
Write-Host "`nLibrary: $type Serial Number $library`n`n" -ForegroundColor Yellow

$loggedIn = $false
$url = "https://$ip/aml/users/login"
$role = 0

Write-Host "Enter User Name: " -NoNewline -ForegroundColor Yellow
$user = Read-Host

# pop up for password
$password = Read-Host "Enter Password:" -AsSecureString
$password = [Runtime.InteropServices.Marshal]::PtrToStringAuto(
    [Runtime.InteropServices.Marshal]::SecureStringToBSTR($password))

# Create a user session with a login
# If successful, check the response for the user's role

$xmlnsString = 'xmlns:ns2="http://automatedMediaLibrary/'
$xmlString = "<ns2:user
$xmlString += "<name>$user</name><password>$password</password><ldap>false</ldap></ns2:user>"

# /login may also use parameters instead of json or xml formatted strings
# Example: $params = @{ "name"=$user;"password"=$password;}
# -Body $params

$loggedIn = $false
$admin = $false
try{
    # Login
    Write-Host "`n-----`nLogin and Create Session POST https://$ip/aml/users/login`n"
    # This Request uses an xml String, but /login may also use parameters:
    # $params = @{ "name"=$user;"password"=$password;}
    # Invoke-WebRequest -Body $params
    #
    # SessionVariable handles the cookie, to maintain the session. It creates a $Session variable to be used
    # with succeeding requests

```



```
$response = Invoke-WebRequest "https://$ip/aml/users/login" -SessionVariable Session -Body
$xmlString -Method 'POST' -ContentType 'application/xml' -ErrorVariable RespErr
```

```
$xml = [xml] $response
Write-XML ($xml)
$loggedIn = $true
```

```
$role = $xml.user.role
# check the response, to determine user's role
# User roles(1) don't have permission to update/add
if ( $role -eq 0){
    Write-Host ("`nAdmin Role User ") -ForegroundColor Yellow
    $admin = $true
}
elseif ($role -eq 1){
```

```
    Write-Host "`nUser Role user" -ForegroundColor Yellow
    Write-Host "`nSkipping PUT and POST`n"
}
```

```
if ($loggedIn){
```

```
    # Get Request for remote access settings
    $uri = "https://$ip/aml/physicalLibrary/subset/remoteAccess"
    Write-Host "`n-----`n`nGet session timeout: setting GET $uri`n"
    $response = Invoke-WebRequest $uri -WebSession $Session
```

```
    $xml = [xml]$response
    Write-XML ($xml)
    $currentSessionTime = [int]$xml.physicalLibraryRemoteAccess.sessionTimeout.minutes
    Write-Host "`n Current SessionTimeout: value: $currentSessionTime`n" -ForegroundColor Yellow
```

```
# admin user, update session time & Create/delete partition
```

```
if ($admin){
    if ($currentSessionTime -eq 60){
        $newTime = 90
    }
    else{
        $newTime = 60
    }
}
```

```
$xmlString = "<ns2:physicalLibrary
$nsString><phySettings><sessionTimeout><minutes>$newTime</minutes></sessionTimeout></phySettings></
ns2:physicalLibrary>"
```

```
$reset = Send-Put-XML-Request "https://$ip/aml/physicalLibrary" $xmlString $Session
if ($reset){
```

```

        Write-Host "`nChanged library user session time from $currentSessionTime
minutes to $newTime minutes. " -ForegroundColor Yellow
        $resetSessionTime = $true
    }else{
        Write-Host "`nUnable to change library session time. "
    }
}

# Create partition
# Use JSON Formatted data
Write-host "`n-----`n"
Write-Host "`nEnter New Partition Name: " -ForegroundColor Yellow -NoNewline
$partition = Read-Host
Write-Host "`nRequest Data: `n"
$partitionData = @{name = $partition
    storageSlotCount = 3
    type = 1 } | ConvertTo-Json
Write-Host "`n-----`n`nCreate Standard Partition $partition (JSON request data) with 3 slots`n"

$partitionCreated = Send-Post-Json-Request "https://$ip/aml/partitions" $partitionData $Session

if ($partitionCreated){
    Write-Host "`n`nDelete Partition $partition `n"

    Delete-Request "https://$ip/aml/partition/$partition" $Session
}else{
    Write-Host "`n`nAdd partition failed, skip delete partition`n"
}
}
}

Write-Host "`n-----`n`nDelete Session, Logoff `n"
Delete-Request "https://$ip/aml/users/login" $Session
}

}catch{
    $err=$_.Exception
    $status = $_.Exception.Response.StatusCode.value__
    $errorMsg = "Login failed. "
    # 401s are Unauthorized requests
    # Get the error string
    if ($status -eq 401)
    {
        $s = [string] $RespErr
        $wsString = Get-WS-Error $s
        $errorMsg = $errorMsg + $wsString
    }
    Write-Host "`n$errorMsg `n" -ForegroundColor Red
}
}

```

```
}catch{
    # Ping (/aml) failed

    Write-Host ("`nFailed to connect to $ip. ") -ForegroundColor Red
    Write-Debug $_.Exception

}finally{
    Write-Host "...Exiting" -ForegroundColor Yellow
    #reset policies
    [System.Net.ServicePointManager]::CertificatePolicy = $currentCertificatePolicy
    [Net.ServicePointManager]::SecurityProtocol = $currentSecProtocol
}
}
```

9. Appendix B – Change History

9.1 Overview of Changes for revision F

9.1.1 Overall documentation differences to previous document revision E:

- 1) Added appendix with curl and PowerShell examples to login via web services
- 2) Corrected typos, misspelling, and added more detailed descriptions in some command and object definitions.
- 3) Deprecated use of dataStore parameter in various WS APIs for Scalar i6000.
- 4) Modified several resource objects
- 5) Added new APIs in support of new features
- 6) Added support in Scalar i3 for Active Vault feature and StorNext application interface configurations
- 7) Added support in Scalar i3/i6/i6H to allow default admin user to be renamed (version 220(i3/i6/i6H))

9.1.2 Specific Changes:

9.1.2.1 *Scalar i6000 and Scalar i3/i6/i6H implemented changes*

New APIs:

- GET aml/system/notifications/telemetrics
- GET aml/system/notifications/telemetric/{receiver}
- PUT aml/system/notifications/telemetric/{receiver}

Object changes

- Added telemetricNotificationList and telemetricNotification objects
- Added additional robot status types for libraryStatus object
- Modified firmwareStatus object to include new element for <percentComplete>
- Modified robot object to include coordinate object, (version 820(i6000), 220(i3/i6/i6H))
- Modified physicalLibrary object to deprecate <sendUsageStatistics> setting
- Modified emailServer object and added TLS support via setting <enableTLS>

9.1.2.2 *Scalar i3/i6/i6H specific WS API modifications*

New APIs:

- GET aml/device/settings/robot
- PUT aml/device/settings/robot
- PUT aml/devices/magazines
- PUT aml/devices/magazines/release
- GET aml/system/sensor/configurations
- PUT aml/system/sensor/configurations
- GET aml/users/service/mode
- PUT aml/users/service/mode
- GET aml/physicalLibrary/i3-i6/modules
- GET /aml/users/reports/login
- POST /aml/users/reports/login/email

Object changes

- Added sensorConfigurationList and sensorConfiguration objects
- Added configurationType to sensor object
- Added section object

- Modified drive object to report also a <driveNumber>
- Modified magazine object to indicate whether <removable> or not
- Modified physicalLibrarySettings object to include <autoWebRequests> and <logicalSystemAddressing> in support of new feature settings
- Modified physicalLibrary object to include <autoWebRequests> and <logicalSystemAddressing>
- Modified physicalLibrary and physicalLibraryConfiguration objects to include <logicalSerialNumber>
- Added support for new module type in module object

9.1.2.3 *Scalar i6000 specific WS API modifications*

New APIs:

- POST aml/drive/{identifier}/operations/configure (version 777)

9.2 Overview of Changes for revision G

9.2.1 Overall documentation differences to previous document revision F:

- 1) Corrected typos, misspelling, and added more detailed descriptions in some command and object definitions.
- 2) Added Response Time information to each command request explanations to set expectations for command response performance
- 3) Extended supported http response code and custom code listing.
- 4) Added new APIs in support of new features
- 5) Added several resource objects

9.2.2 Specific Changes:

9.2.2.1 *Scalar i6000 and Scalar i3/i6/i6H implemented changes*

New APIs:

- POST aml/users/login/mfa

Object changes

- Added mfaAuthentication object

9.2.2.2 *Scalar i3/i6/i6H specific WS API modifications*

New APIs:

- GET aml/users/login/mfa/{type}/key
- POST aml/users/login/mfa
- GET aml/users/mfa
- PUT aml/users/mfa
- GET aml/user/{name}/mfa
- GET aml/system/configurationChange/report
- POST aml/system/configurationChange/report/email

Object changes

- Added mfaList and mfa objects
- Added mfaSharedData object
- Added userMFAList and userMFA objects
- Added configurationChangeList and configurationChange objects

9.2.2.3 *Scalar i6000 specific WS API modifications*

New APIs:

- POST aml/devices/blade/fibreChannel/{serialNumber}/port/{id}/operations/reset

Object changes

- Modified physicalLibrary object and added driveCleaning element

9.3 Overview of Changes for revision H

9.3.1 Overall documentation differences to previous document revision G:

- 1) Corrected typos, misspelling, and added more detailed descriptions in some command and object definitions.
- 2) Updated Response Time information for some command requests.
- 3) Extended custom code listings.
- 4) Added new APIs in support of heartbeat notification.
- 5) Removed erroneous, non-functional heartbeat notification APIs and replaced with new ones.
- 6) Deprecated barcodeReporting and ampExtensionsCount APIs
- 7) Added media type checking element to partition object
- 8) Enabled full MFA support for Scalar i6000

9.3.2 Specific Changes:

9.3.2.1 *Scalar i6000 and Scalar i3/i6/i6H implemented changes*

New APIs:

- None

Object changes

- None

9.3.2.2 *Scalar i3/i6/i6H specific WS API modifications*

New APIs:

- POST aml/devices/blade/fibreChannel/{serialNumber}/port/{id}/operations/reset

Object changes

- Modified physicalLibrary object and added driveCleaningCount element

9.3.2.3 *Scalar i6000 specific WS API modifications*

New APIs:

- GET aml/system/notifications/heartbeat
- PUT aml/system/notifications/heartbeat
- GET aml/users/login/mfa/{type}/key
- GET aml/users/mfa
- PUT aml/users/mfa
- GET aml/user/{name}/mfa

Object changes

- Added heartbeatNotification object

- Enabled support for mfaList and mfa objects
- Enabled support for mfaSharedData object
- Enabled support for userMFAList and userMFA objects
- Extended partition object for mediTypeChecking setting
- Added elements in support for beginning of tape passes and midpoint passes to mediaUsage object

9.4 Overview of Changes for revision J

9.4.1 Overall documentation differences to previous document revision H:

- 1) Assigned new document number.
- 2) Corrected typos, misspelling, and grammar.