



Intelligent Security API (Person-Based Access Control)

Developer Guide

Legal Information

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE DOCUMENT IS PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". OUR COMPANY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IN NO EVENT WILL OUR COMPANY BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, IN CONNECTION WITH THE USE OF THE DOCUMENT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

Contents

Chapter 1 Overview	1
1.1 Introduction	1
1.2 Update History	1
Chapter 2 ISAPI Description	22
2.1 Operation Method	22
2.2 URL Format	25
2.3 Message Format	26
2.4 Others	28
Chapter 3 Security	29
3.1 Authentication	29
Chapter 4 Typical Applications	31
4.1 Data Collection	31
4.1.1 Online Collect Data	31
4.1.2 Offline Collect Data	34
4.2 Manage Person Information	37
4.3 Manage Card Information	38
4.3.1 Collect Card Information	40
4.3.2 Card Operation	41
4.4 Manage Fingerprint Information	42
4.4.1 Fingerprint Collection	44
4.5 Manage Face Information	45
4.5.1 Create Face Picture Library	45
4.5.2 Collect Face Data	46
4.5.3 Manage Face Records in Face Picture Library	47
4.5.4 Configure Facial Recognition Mode	48
4.6 Configure Access Permission Control Schedule	50

4.7 Configure Authentication Mode Control Schedule	52
4.8 Configure Door Control Schedule	54
4.9 Remotely Control Door, Elevator, and Buzzer	56
4.10 Configure Password for Remote Door Control	58
4.11 Configure Anti-Passing Back	59
4.12 Cross-Controller Anti-Passing Back Configuration	60
4.12.1 Configure Route Anti-Passing Back Based on Network	61
4.12.2 Configure Entrance/Exit Anti-Passing Back Based on Network	64
4.12.3 Configure Route Anti-Passing Back Based on Card	66
4.12.4 Configure Entrance/Exit Anti-Passing Back Based on Card	69
4.13 Alarm or Event Receiving	70
4.13.1 Supported Alarm/Event Types and Details	71
4.13.2 Configure Mask Detection Event	71
4.13.3 Configure Hard Hat Detection Event	72
4.13.4 Configure and Search for Access Control Events	72
4.13.5 Receive Alarm/Event in Arming Mode	76
4.13.6 Receive Alarm/Event in Listening Mode	77
4.13.7 Remotely Verify Access Control Events	80
4.14 Configure Attendance Status and Schedule	80
4.15 Information Release	84
4.15.1 Manage Materials	86
4.15.2 Manage Programs and Pages	86
4.15.3 Manage the Program Schedule	87
4.16 Other Applications	87
4.16.1 Device/Server Settings	87
4.16.2 Multi-Factor Authentication	90
4.16.3 Multi-Door Interlocking	91
4.16.4 M1 Card Encryption Authentication	91

4.16.5 Temperature Measurement	91
4.16.6 Configuration and Maintenance	92
Appendix A. Request URIs	101
A.1 /ISAPI/AccessControl/AcsCfg/capabilities?format=json	101
A.2 /ISAPI/AccessControl/AcsCfg?format=json	101
A.3 /ISAPI/AccessControl/AcsEvent/capabilities?format=json	102
A.4 /ISAPI/AccessControl/AcsEvent/StorageCfg/capabilities?format=json	102
A.5 /ISAPI/AccessControl/AcsEvent/StorageCfg?format=json	103
A.6 /ISAPI/AccessControl/AcsEvent?format=json	103
A.7 /ISAPI/AccessControl/AcsEventTotalNum/capabilities?format=json	105
A.8 /ISAPI/AccessControl/AcsEventTotalNum?format=json	106
A.9 /ISAPI/AccessControl/AcsWorkStatus/capabilities?format=json	106
A.10 /ISAPI/AccessControl/AcsWorkStatus?format=json	107
A.11 /ISAPI/AccessControl/AntiSneakCfg/capabilities?format=json	107
A.12 /ISAPI/AccessControl/AntiSneakCfg?format=json	108
A.13 /ISAPI/AccessControl/Attendance/planTemplate/<TemplateNo>?format=json	108
A.14 /ISAPI/AccessControl/Attendance/planTemplate/capabilities?format=json	109
A.15 /ISAPI/AccessControl/Attendance/planTemplate?format=json	110
A.16 /ISAPI/AccessControl/Attendance/weekPlan/<PlanNo>?format=json	110
A.17 /ISAPI/AccessControl/Attendance/weekPlan/capabilities?format=json	111
A.18 /ISAPI/AccessControl/blackObject/capabilities?format=json	111
A.19 /ISAPI/AccessControl/blackObject?format=json	112
A.20 /ISAPI/AccessControl/bluetooth/capabilities?format=json	112
A.21 /ISAPI/AccessControl/bluetooth?format=json	113
A.22 /ISAPI/AccessControl/bluetoothEncryptionInfo/capabilities?format=json	114
A.23 /ISAPI/AccessControl/bluetoothEncryptionInfo?format=json	114
A.24 /ISAPI/AccessControl/capabilities	115
A.25 /ISAPI/AccessControl/CaptureCardInfo/capabilities?format=json	116

A.26 /ISAPI/AccessControl/CaptureCardInfo?format=json	116
A.27 /ISAPI/AccessControl/CaptureFaceData	117
A.28 /ISAPI/AccessControl/CaptureFaceData/capabilities	120
A.29 /ISAPI/AccessControl/CaptureFaceData/Progress	120
A.30 /ISAPI/AccessControl/CaptureFaceData/Progress/capabilities	120
A.31 /ISAPI/AccessControl/CaptureFingerPrint	121
A.32 /ISAPI/AccessControl/CaptureFingerPrint/capabilities	121
A.33 /ISAPI/AccessControl/CaptureIDInfo/capabilities?format=json	122
A.34 /ISAPI/AccessControl/CaptureIDInfo?format=json	122
A.35 /ISAPI/AccessControl/CapturePresetParam/capabilities?format=json	123
A.36 /ISAPI/AccessControl/CapturePresetParam?format=json	123
A.37 /ISAPI/AccessControl/CaptureRule/capabilities?format=json	124
A.38 /ISAPI/AccessControl/CaptureRule?format=json	125
A.39 /ISAPI/AccessControl/CardInfo/capabilities?format=json	125
A.40 /ISAPI/AccessControl/CardInfo/Count?format=json	126
A.41 /ISAPI/AccessControl/CardInfo/Count?format=json&employeeNo=<ID>	127
A.42 /ISAPI/AccessControl/CardInfo/Delete?format=json	127
A.43 /ISAPI/AccessControl/CardInfo/Modify?format=json	128
A.44 /ISAPI/AccessControl/CardInfo/Record?format=json	128
A.45 /ISAPI/AccessControl/CardInfo/Search?format=json	128
A.46 /ISAPI/AccessControl/CardInfo/SetUp?format=json	129
A.47 /ISAPI/AccessControl/CardOperations/capabilities?format=json	130
A.48 /ISAPI/AccessControl/CardOperations/cardIssueStatus?format=json	130
A.49 /ISAPI/AccessControl/CardOperations/cardParam?format=json	131
A.50 /ISAPI/AccessControl/CardOperations/clearData?format=json	131
A.51 /ISAPI/AccessControl/CardOperations/controlBlock?format=json	131
A.52 /ISAPI/AccessControl/CardOperations/customData/searchTask?format=json	132
A.53 /ISAPI/AccessControl/CardOperations/customData?format=json	133

A.54 /ISAPI/AccessControl/CardOperations/dataBlock/<address>?format=json	133
A.55 /ISAPI/AccessControl/CardOperations/dataBlock/control?format=json	134
A.56 /ISAPI/AccessControl/CardOperations/dataTrans?format=json	134
A.57 /ISAPI/AccessControl/CardOperations/encryption?format=json	135
A.58 /ISAPI/AccessControl/CardOperations/localIssueCfg?format=json	135
A.59 /ISAPI/AccessControl/CardOperations/localIssueRequest?format=json	136
A.60 /ISAPI/AccessControl/CardOperations/localIssueRes?format=json	136
A.61 /ISAPI/AccessControl/CardOperations/protocol?format=json	137
A.62 /ISAPI/AccessControl/CardOperations/reset?format=json	137
A.63 /ISAPI/AccessControl/CardOperations/sectionEncryption?format=json	137
A.64 /ISAPI/AccessControl/CardOperations/verification?format=json	138
A.65 /ISAPI/AccessControl/CardReaderAntiSneakCfg/<ID>?format=json	139
A.66 /ISAPI/AccessControl/CardReaderAntiSneakCfg/capabilities?format=json	139
A.67 /ISAPI/AccessControl/CardReaderCfg/<ID>?format=json	140
A.68 /ISAPI/AccessControl/CardReaderCfg/capabilities?format=json	141
A.69 /ISAPI/AccessControl/CardReaderPlan/<CardReaderNo>?format=json	141
A.70 /ISAPI/AccessControl/CardReaderPlan/capabilities?format=json	142
A.71 /ISAPI/AccessControl/CardVerificationRule/capabilities?format=json	142
A.72 /ISAPI/AccessControl/CardVerificationRule/progress?format=json	143
A.73 /ISAPI/AccessControl/CardVerificationRule?format=json	143
A.74 /ISAPI/AccessControl/ClearAntiSneak?format=json	144
A.75 /ISAPI/AccessControl/ClearAntiSneak/capabilities?format=json	144
A.76 /ISAPI/AccessControl/ClearAntiSneakCfg/capabilities?format=json	145
A.77 /ISAPI/AccessControl/ClearAntiSneakCfg?format=json	145
A.78 /ISAPI/AccessControl/ClearAttendancePlan?format=json	146
A.79 /ISAPI/AccessControl/ClearCardRecord	146
A.80 /ISAPI/AccessControl/ClearCardRecord/capabilities	146
A.81 /ISAPI/AccessControl/ClearEventCardLinkageCfg/capabilities?format=json	147

A.82 /ISAPI/AccessControl/ClearEventCardLinkageCfg?format=json	147
A.83 /ISAPI/AccessControl/ClearGroupCfg/capabilities?format=json	148
A.84 /ISAPI/AccessControl/ClearGroupCfg?format=json	148
A.85 /ISAPI/AccessControl/ClearPictureCfg/capabilities?format=json	149
A.86 /ISAPI/AccessControl/ClearPictureCfg?format=json	149
A.87 /ISAPI/AccessControl/ClearPlansCfg/capabilities?format=json	149
A.88 /ISAPI/AccessControl/ClearPlansCfg?format=json	150
A.89 /ISAPI/AccessControl/ClearSubmarineBack	151
A.90 /ISAPI/AccessControl/ClearSubmarineBack/capabilities	151
A.91 /ISAPI/AccessControl/Configuration/attendanceMode/capabilities?format=json	151
A.92 /ISAPI/AccessControl/Configuration/attendanceMode?format=json	152
A.93 /ISAPI/AccessControl/Configuration/IRCfg/capabilities?format=json	153
A.94 /ISAPI/AccessControl/Configuration/IRCfg?format=json	153
A.95 /ISAPI/AccessControl/Configuration/lockType/capabilities?format=json	154
A.96 /ISAPI/AccessControl/Configuration/lockType?format=json	154
A.97 /ISAPI/AccessControl/Configuration/NFCCfg/capabilities?format=json	155
A.98 /ISAPI/AccessControl/Configuration/NFCCfg?format=json	155
A.99 /ISAPI/AccessControl/Configuration/RFCardCfg/capabilities?format=json	156
A.100 /ISAPI/AccessControl/Configuration/RFCardCfg?format=json	156
A.101 /ISAPI/AccessControl/Configuration/safetyHelmetDetection/capabilities?format=json	157
A.102 /ISAPI/AccessControl/Configuration/safetyHelmetDetection?format=json	158
A.103 /ISAPI/AccessControl/customAudio/addCustomAudio?format=json	158
A.104 /ISAPI/AccessControl/customAudio/capabilities?format=json	159
A.105 /ISAPI/AccessControl/customAudio/deleteCustomAudio?format=json	159
A.106 /ISAPI/AccessControl/customAudio/searchCustomAudioStatus?format=json	160
A.107 /ISAPI/AccessControl/DeployInfo	160
A.108 /ISAPI/AccessControl/DeployInfo/capabilities	161

A.109 /ISAPI/AccessControl/Door/param/<ID>	161
A.110 /ISAPI/AccessControl/Door/param/<ID>/capabilities	162
A.111 /ISAPI/AccessControl/DoorSecurityModule/moduleStatus	162
A.112 /ISAPI/AccessControl/DoorSecurityModule/moduleStatus/capabilities	163
A.113 /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/<GroupNo>?format=json	163
A.114 /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/capabilities?format=json	164
A.115 /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/<PlanNo>?format=json	165
A.116 /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/capabilities?format=json	166
A.117 /ISAPI/AccessControl/DoorStatusPlan/<DoorNo>?format=json	166
A.118 /ISAPI/AccessControl/DoorStatusPlan/capabilities?format=json	167
A.119 /ISAPI/AccessControl/DoorStatusPlanTemplate/<TemplateNo>?format=json	167
A.120 /ISAPI/AccessControl/DoorStatusPlanTemplate/capabilities?format=json	168
A.121 /ISAPI/AccessControl/DoorStatusWeekPlanCfg/<PlanNo>?format=json	169
A.122 /ISAPI/AccessControl/DoorStatusWeekPlanCfg/capabilities?format=json	169
A.123 /ISAPI/AccessControl/EventCardLinkageCfg/<ID>?format=json	170
A.124 /ISAPI/AccessControl/EventCardLinkageCfg/capabilities?format=json	171
A.125 /ISAPI/AccessControl/EventCardNoList/capabilities?format=json	171
A.126 /ISAPI/AccessControl/EventCardNoList?format=json	172
A.127 /ISAPI/AccessControl/EventOptimizationCfg/capabilities?format=json	172
A.128 /ISAPI/AccessControl/EventOptimizationCfg?format=json	172
A.129 /ISAPI/AccessControl/FaceCompareCond	173
A.130 /ISAPI/AccessControl/FaceCompareCond/capabilities	174
A.131 /ISAPI/AccessControl/FaceRecognizeMode/capabilities?format=json	174
A.132 /ISAPI/AccessControl/FaceRecognizeMode?format=json	175
A.133 /ISAPI/AccessControl/FaceTemperatureEvent/capabilities?format=json	176
A.134 /ISAPI/AccessControl/FaceTemperatureEvent?format=json	176
A.135 /ISAPI/AccessControl/FingerPrint/Count?format=json&employeeNo=	176
A.136 /ISAPI/AccessControl/FingerPrint/Delete/capabilities?format=json	177

A.137 /ISAPI/AccessControl/FingerPrint/Delete?format=json	177
A.138 /ISAPI/AccessControl/FingerPrint/DeleteProcess?format=json	178
A.139 /ISAPI/AccessControl/FingerPrint/SetUp?format=json	179
A.140 /ISAPI/AccessControl/FingerPrintCfg/capabilities?format=json	180
A.141 /ISAPI/AccessControl/FingerPrintDownload?format=json	180
A.142 /ISAPI/AccessControl/FingerPrintModify?format=json	181
A.143 /ISAPI/AccessControl/FingerPrintProgress?format=json	181
A.144 /ISAPI/AccessControl/FingerPrintUpload?format=json	182
A.145 /ISAPI/AccessControl/FingerPrintUploadAll?format=json	182
A.146 /ISAPI/AccessControl/GroupCfg/<ID>?format=json	183
A.147 /ISAPI/AccessControl/GroupCfg/capabilities?format=json	184
A.148 /ISAPI/AccessControl/healthCodeCfg/capabilities?format=json	184
A.149 /ISAPI/AccessControl/healthCodeCfg?format=json	184
A.150 /ISAPI/AccessControl/IDBlackListCfg	185
A.151 /ISAPI/AccessControl/IDBlackListCfg/capabilities	186
A.152 /ISAPI/AccessControl/IDBlackListCfg/template?format=json	186
A.153 /ISAPI/AccessControl/IDCardInfoEvent/capabilities?format=json	186
A.154 /ISAPI/AccessControl/IDCardInfoEvent?format=json	187
A.155 /ISAPI/AccessControl/IdentityTerminal	187
A.156 /ISAPI/AccessControl/IdentityTerminal/capabilities	188
A.157 /ISAPI/AccessControl/keyCfg/<ID>/attendance?format=json	188
A.158 /ISAPI/AccessControl/keyCfg/attendance/capabilities?format=json	189
A.159 /ISAPI/AccessControl/keyCfg/attendance?format=json	190
A.160 /ISAPI/AccessControl/LogModeCfg/capabilities?format=json	190
A.161 /ISAPI/AccessControl/LogModeCfg?format=json	190
A.162 /ISAPI/AccessControl/LOGOCfg/capabilities?format=json	191
A.163 /ISAPI/AccessControl/LOGOCfg?format=json	192
A.164 /ISAPI/AccessControl/M1CardEncryptCfg	192

A.165 /ISAPI/AccessControl/M1CardEncryptCfg/capabilities	193
A.166 /ISAPI/AccessControl/maintenanceData?secretkey=	193
A.167 /ISAPI/AccessControl/maskDetection/capabilities?format=json	194
A.168 /ISAPI/AccessControl/maskDetection?format=json	194
A.169 /ISAPI/AccessControl/MultiCardCfg/<ID>?format=json	195
A.170 /ISAPI/AccessControl/MultiCardCfg/capabilities?format=json	196
A.171 /ISAPI/AccessControl/MultiDoorInterLockCfg/capabilities?format=json	196
A.172 /ISAPI/AccessControl/MultiDoorInterLockCfg?format=json	197
A.173 /ISAPI/AccessControl/OfflineCapture/capabilities?format=json	197
A.174 /ISAPI/AccessControl/OfflineCapture/DataCollections/<captureNo>?format=json	198
A.175 /ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?format=json	198
A.176 /ISAPI/AccessControl/OfflineCapture/DataCollections/searchTask?format=json	201
A.177 /ISAPI/AccessControl/OfflineCapture/DataCollections?format=json	201
A.178 /ISAPI/AccessControl/OfflineCapture/dataOutput/progress?format=json	202
A.179 /ISAPI/AccessControl/OfflineCapture/dataOutput?format=json	202
A.180 /ISAPI/AccessControl/OfflineCapture/InfoFile/progress?format=json	203
A.181 /ISAPI/AccessControl/OfflineCapture/InfoFile?format=json	203
A.182 /ISAPI/AccessControl/OfflineCapture/InfoFileTemplateDownload?format=json	204
A.183 /ISAPI/AccessControl/OfflineCapture/progress?format=json	206
A.184 /ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json	206
A.185 /ISAPI/AccessControl/OfflineCapture/uploadFailedDetails?format=json	207
A.186 /ISAPI/AccessControl/OSDPMModify/<ID>?format=json	208
A.187 /ISAPI/AccessControl/OSDPMModify/capabilities?format=json	208
A.188 /ISAPI/AccessControl/OSDPStatus/<ID>?format=json	208
A.189 /ISAPI/AccessControl/OSDPStatus/capabilities?format=json	209
A.190 /ISAPI/AccessControl/personInfoExtendName/capabilities?format=json	209
A.191 /ISAPI/AccessControl/personInfoExtendName?format=json	210
A.192 /ISAPI/AccessControl/PhoneDoorRightCfg/<ID>?format=json	211

A.193 /ISAPI/AccessControl/PhoneDoorRightCfg/capabilities?format=json	211
A.194 /ISAPI/AccessControl/QRCodeEvent/capabilities?format=json	212
A.195 /ISAPI/AccessControl/QRCodeEvent?format=json	212
A.196 /ISAPI/AccessControl/ReaderAcrossHost	213
A.197 /ISAPI/AccessControl/ReaderAcrossHost/capabilities	213
A.198 /ISAPI/AccessControl/remoteCheck/capabilities?format=json	214
A.199 /ISAPI/AccessControl/remoteCheck?format=json	214
A.200 /ISAPI/AccessControl/RemoteControl/buzzer/<ID>?format=json	215
A.201 /ISAPI/AccessControl/RemoteControl/buzzer/capabilities?format=json	215
A.202 /ISAPI/AccessControl/RemoteControl/door/<ID>	216
A.203 /ISAPI/AccessControl/RemoteControl/door/capabilities	216
A.204 /ISAPI/AccessControl/remoteControlPWCheck/capabilities?format=json	217
A.205 /ISAPI/AccessControl/remoteControlPWCheck/door/<ID>?format=json	217
A.206 /ISAPI/AccessControl/remoteControlPWCfg/capabilities?format=json	218
A.207 /ISAPI/AccessControl/remoteControlPWCfg/door/<ID>?format=json	218
A.208 /ISAPI/AccessControl/ServerDevice	219
A.209 /ISAPI/AccessControl/ServerDevice/capabilities	220
A.210 /ISAPI/AccessControl/showHealthCodeCfg/capabilities?format=json	220
A.211 /ISAPI/AccessControl/showHealthCodeCfg?format=json	221
A.212 /ISAPI/AccessControl/SmsRelativeParam/capabilities?format=json	221
A.213 /ISAPI/AccessControl/SmsRelativeParam?format=json	222
A.214 /ISAPI/AccessControl/SnapConfig	223
A.215 /ISAPI/AccessControl/SnapConfig/capabilities	223
A.216 /ISAPI/AccessControl/StartReaderInfo	223
A.217 /ISAPI/AccessControl/StartReaderInfo/capabilities	224
A.218 /ISAPI/AccessControl/SubmarineBack	225
A.219 /ISAPI/AccessControl/SubmarineBack/capabilities	225
A.220 /ISAPI/AccessControl/SubmarineBackHostInfo/capabilities	226

A.221 /ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>	226
A.222 /ISAPI/AccessControl/SubmarineBackMode	227
A.223 /ISAPI/AccessControl/SubmarineBackMode/capabilities	228
A.224 /ISAPI/AccessControl/SubmarineBackReader/capabilities	228
A.225 /ISAPI/AccessControl/SubmarineBackReader/ConfigureNo/<ID>	229
A.226 /ISAPI/AccessControl/temperatureMeasureAreaCalibration/capabilities?format=json	229
A.227 /ISAPI/AccessControl/temperatureMeasureAreaCalibration?format=json	230
A.228 /ISAPI/AccessControl/temperatureMeasureAreaCfg/capabilities?format=json	231
A.229 /ISAPI/AccessControl/temperatureMeasureAreaCfg?format=json	231
A.230 /ISAPI/AccessControl/temperatureMeasureCfg/capabilities?format=json	232
A.231 /ISAPI/AccessControl/temperatureMeasureCfg?format=json	232
A.232 /ISAPI/AccessControl/userData?secretkey=	233
A.233 /ISAPI/AccessControl/UserInfo/capabilities?format=json	234
A.234 /ISAPI/AccessControl/UserInfo/Count?format=json	235
A.235 /ISAPI/AccessControl/UserInfo/Delete?format=json	235
A.236 /ISAPI/AccessControl/UserInfo/Modify?format=json	236
A.237 /ISAPI/AccessControl/UserInfo/Record?format=json	236
A.238 /ISAPI/AccessControl/UserInfo/Search?format=json	237
A.239 /ISAPI/AccessControl/UserInfo/SetUp?format=json	237
A.240 /ISAPI/AccessControl/UserInfoDetail/Delete/capabilities?format=json	238
A.241 /ISAPI/AccessControl/UserInfoDetail/Delete?format=json	239
A.242 /ISAPI/AccessControl/UserInfoDetail/DeleteProcess?format=json	239
A.243 /ISAPI/AccessControl/UserRightHolidayPlanCfg/capabilities?format=json	240
A.244 /ISAPI/AccessControl/UserRightWeekPlanCfg/capabilities?format=json	241
A.245 /ISAPI/AccessControl/UserRightHolidayGroupCfg/<GroupNo>?format=json	241
A.246 /ISAPI/AccessControl/UserRightHolidayGroupCfg/capabilities?format=json	242
A.247 /ISAPI/AccessControl/UserRightHolidayPlanCfg/<PlanNo>?format=json	243

A.248 /ISAPI/AccessControl/UserRightPlanTemplate/<TemplateNo>?format=json	244
A.249 /ISAPI/AccessControl/UserRightPlanTemplate/capabilities?format=json	245
A.250 /ISAPI/AccessControl/UserRightWeekPlanCfg/<PlanNo>?format=json	246
A.251 /ISAPI/AccessControl/Verification/ttsText/capabilities?format=json	247
A.252 /ISAPI/AccessControl/Verification/ttsText?format=json	247
A.253 /ISAPI/AccessControl/VerifyHolidayGroupCfg/<GroupNo>?format=json	248
A.254 /ISAPI/AccessControl/VerifyHolidayGroupCfg/capabilities?format=json	249
A.255 /ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json	250
A.256 /ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities?format=json	251
A.257 /ISAPI/AccessControl/VerifyPlanTemplate/<TemplateNo>?format=json	251
A.258 /ISAPI/AccessControl/VerifyPlanTemplate/capabilities?format=json	252
A.259 /ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json	252
A.260 /ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities?format=json	253
A.261 /ISAPI/AccessControl/WiegandCfg/capabilities	254
A.262 /ISAPI/AccessControl/WiegandCfg/wiegandNo/<ID>	254
A.263 /ISAPI/AccessControl/WiegandRuleCfg	255
A.264 /ISAPI/AccessControl/WiegandRuleCfg/capabilities	255
A.265 /ISAPI/Event/notification/alertStream	256
A.266 /ISAPI/Event/notification/httpHosts	257
A.267 /ISAPI/Event/notification/httpHosts/<ID>/test	258
A.268 /ISAPI/Event/notification/httpHosts/capabilities	259
A.269 /ISAPI/Intelligent/FDLib/capabilities?format=json	259
A.270 /ISAPI/Intelligent/FDLib/Count?format=json	260
A.271 /ISAPI/Intelligent/FDLib/Count?format=json&FDID=&faceLibType=	260
A.272 /ISAPI/Intelligent/FDLib/FaceDataRecord?format=json	261
A.273 /ISAPI/Intelligent/FDLib/FDModify?format=json	262
A.274 /ISAPI/Intelligent/FDLib/FDSearch/Delete?format=json&FDID=&faceLibType=	262
A.275 /ISAPI/Intelligent/FDLib/FDSearch?format=json	263

A.276 /ISAPI/Intelligent/FDLib/FDSearch?format=json&FDID=&FPID=&faceLibType=	263
A.277 /ISAPI/Intelligent/FDLib/FDSetUp?format=json	264
A.278 /ISAPI/Intelligent/FDLib?format=json	264
A.279 /ISAPI/Intelligent/FDLib?format=json&FDID=&faceLibType=	266
A.280 /ISAPI/Publish/capabilities	268
A.281 /ISAPI/Publish/material/<ID>/capabilities	268
A.282 /ISAPI/Publish/MaterialMgr/material	268
A.283 /ISAPI/Publish/MaterialMgr/material/<ID>	269
A.284 /ISAPI/Publish/MaterialMgr/material/<ID>/upload	270
A.285 /ISAPI/Publish/MaterialMgr/material/batchDelete	271
A.286 /ISAPI/Publish/MaterialMgr/materialSearch	271
A.287 /ISAPI/Publish/MaterialMgr/materialSearch/profile	271
A.288 /ISAPI/Publish/ProgramMgr/program	272
A.289 /ISAPI/Publish/ProgramMgr/program/<ID>	273
A.290 /ISAPI/Publish/ProgramMgr/program/<ID>/capabilities	274
A.291 /ISAPI/Publish/ProgramMgr/program/<ID>/page	274
A.292 /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>	275
A.293 /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>/capabilities	276
A.294 /ISAPI/Publish/ProgramMgr/program/dynamicCap	276
A.295 /ISAPI/Publish/ScheduleMgr/capabilities?format=json	277
A.296 /ISAPI/Publish/ScheduleMgr/playSchedule	277
A.297 /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>	278
A.298 /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>/capabilities	279
A.299 /ISAPI/System/capabilities	279
A.300 /ISAPI/System/PictureServer/capabilities?format=json	280
A.301 /ISAPI/System/PictureServer?format=json	280
A.302 http://<ipAddress>:<portNo>/<url>	281
Appendix B. Appendixes	282

B.1 Request and Response Messages	282
B.1.1 JSON Messages	282
B.1.2 XML Messages	522
B.2 Access Control Event Types	652
B.3 Event Linkage Types	669
B.4 Log Types for ISAPI	681
B.5 Response Codes of Text Protocol	707
B.6 Error Codes Categorized by Functional Modules	746

Chapter 1 Overview

Access Control is the selective restriction of access to a place or other resources. The access control applications integrated by Intelligent Security API (ISAPI) in this manual take the person as the management and control unit, which indicates that linking fingerprints, faces, and other attributes to a card will be replaced by linking fingerprints, cards, and other attributes to a person.

1.1 Introduction

This manual mainly introduces the integration flows and related URIs for access controller, fingerprint access control terminal, fingerprint time attendance terminal, and so on, to implement the following functions: schedule configuration, person/card/fingerprint information management, alarm/event configuration, door/elevator/buzzer control, anti-passing back, and so on.

1.2 Update History

Summary of Changes in Version 2.6_Aug., 2021

Related Product: DS-K1T673 Series Face Recognition Terminal with Software Version 3.3.1

1. Extended the message about the face picture library capability [JSON_FPLibCap](#), the condition message of adding a face record to the face picture library [JSON_AddFaceRecordCond](#), the condition message about editing a face record in a specific face picture library [JSON_EditFaceRecord](#), the condition message about editing face records in the face picture library in a batch [JSON_BatchEditFaceRecord](#), and the condition message about setting the face record in the face picture library [JSON_SetFaceRecord](#) (related URIs: [/ISAPI/Intelligent/FDLib/capabilities?format=json](#) , [/ISAPI/Intelligent/FDLib/FaceDataRecord?format=json](#) , [/ISAPI/Intelligent/FDLib/FDSearch?format=json&FDID=&FPIID=&faceLibType=](#) , [/ISAPI/Intelligent/FDLib/FDModify?format=json](#) , and [/ISAPI/Intelligent/FDLib/FDSetUp?format=json](#)): add a node **saveFacePic** (whether to save face pictures).
2. Extended the result message of searching for the face records in the a face picture library [JSON_SearchFaceRecordResult](#) (related URI: [/ISAPI/Intelligent/FDLib/FDSearch?format=json](#)): added a sub node **saveFacePic** (whether to save face pictures) to the node **MatchList**.
3. Added two URIs of configuring bluetooth parameters of access control:
Get the capability: GET [/ISAPI/AccessControl/bluetooth/capabilities?format=json](#) ;
Get or set the parameters: GET or PUT [/ISAPI/AccessControl/bluetooth?format=json](#) .
4. Extended the configuration capability message [XML_Cap_IdentityTerminal](#) and the parameter message [XML_IdentityTerminal](#) of intelligent identity recognition terminal (related URIs: [/ISAPI/AccessControl/IdentityTerminal/capabilities](#) and [/ISAPI/AccessControl/IdentityTerminal](#)): added a sub node **maskFaceMatchThreshold1** (1:1 face picture (face with mask and normal background picture) comparison threshold of ECO mode) to the node **ecoMode**.

5. Extended the configuration capability message **JSON_Cap_CardReaderCfg** and the parameter message **JSON_CardReaderCfg** of the card reader (related URIs: </ISAPI/AccessControl/CardReaderCfg/capabilities?format=json> and </ISAPI/AccessControl/CardReaderCfg/<ID>?format=json>):
added a node **maskFaceMatchThreshold1** (1:1 face picture (face with mask and normal background) comparison threshold).
6. Extended the configuration capability message **JSON_Cap_AcsCfg** and parameter message **JSON_AcsCfg** of the access controller (related URIs: </ISAPI/AccessControl/AcsCfg/capabilities?format=json> and </ISAPI/AccessControl/AcsCfg?format=json>):
added two nodes **desensitiseEmployeeNo** (whether to enable employee No. de-identification for local UI display) and **desensitiseName** (whether to enable name de-identification for local UI display).
7. Extended **Access Control Event Types**:
added two exception event types 0x44d-"MINOR_EXTEND_MODULE_ONLINE" (Extension Module Online) and 0x44e-"MINOR_EXTEND_MODULE_OFFLINE" (Extension Module Offline).

Summary of Changes in Version 2.6_June., 2021

Related Product: DS-K1T672DX-T and DS-K1T672DWX-T Face Recognition Terminal with Software Version 3.2.32

1. Extended the capability message of actively getting face temperature screening events **JSON_FaceTemperatureEventCap** (related URI: </ISAPI/AccessControl/FaceTemperatureEvent/capabilities?format=json>):
added a sub node **isAbnormalTemperature** (whether the skin-surface temperature is abnormal) to the node **FaceTemperatureEventCond**.
2. Extended the condition message of actively getting face temperature screening events **JSON_FaceTemperatureEventCond** (related URI: </ISAPI/AccessControl/FaceTemperatureEvent?format=json>):
added a node **isAbnormalTemperature** (whether the skin-surface temperature is abnormal).
3. Extended the capability message of searching for access control events **JSON_Cap_AcsEvent** (related URI: </ISAPI/AccessControl/AcsEvent/capabilities?format=json>):
added a sub node **isAbnormalTemperature** (whether the skin-surface temperature is abnormal) to the node **AcsEventCond**;
added a sub node **HealthInfo** (health information) to the node **InfoList**.
4. Extended the condition message of searching for access control events **JSON_AcsEventCond** (related URI: </ISAPI/AccessControl/AcsEvent?format=json>):
added a node **isAbnormalTemperature** (whether the skin-surface temperature is abnormal).
5. Extended the result message of searching for access control events **JSON_AcsEvent** (related URI: </ISAPI/AccessControl/AcsEvent?format=json>):
added a sub node **HealthInfo** (health information) to the node **InfoList**.
6. Extended the capability message of getting the ID card swiping events actively **JSON_IDCardInfoEventCap** (related URI: </ISAPI/AccessControl/IDCardInfoEvent/capabilities?format=json>):

- added a sub node **isAbnormalTemperature** (whether the skin-surface temperature is abnormal) to the node **IDCardInfoEventCond**;
- added a sub node **HealthInfo** (health information) to the node **InfoList**.
7. Extended the condition message of getting the ID card swiping events actively
[JSON_IDCardInfoEventCond](#) (related URI: [/ISAPI/AccessControl/IDCardInfoEvent?format=json](#)):
added a node **isAbnormalTemperature** (whether the skin-surface temperature is abnormal).
8. Extended the result message of getting the ID card swiping events actively
[JSON_IDCardInfoEvent](#) (related URI: [/ISAPI/AccessControl/IDCardInfoEvent?format=json](#)):
added a sub node **HealthInfo** (health information) to the node **InfoList**.
9. Extended the configuration capability message [JSON_Cap_AcsCfg](#) and the parameter message [JSON_AcsCfg](#) of the access controller (related URIs: [/ISAPI/AccessControl/AcsCfg/capabilities?format=json](#) and [/ISAPI/AccessControl/AcsCfg?format=json](#)):
added a verification channel type "ISAPIListen" (ISAPI listening channel) to the node **checkChannelType**;
added a node **enableCaptureCertificate** (whether to enable capturing the ID picture).
10. Extended the functional capability message of access control [XML_Cap_AccessControl](#) (related URI: [/ISAPI/AccessControl/capabilities](#)):
added three nodes <isSupportAddCustomAudio> (whether it supports importing custom audio), <isSupportDeleteCustomAudio> (whether it supports deleting custom audio), and <isSupportSearchCustomAudio> (whether it supports searching for custom audio).
11. Added URIs of managing the custom audio:
Get the configuration capability: GET [/ISAPI/AccessControl/customAudio/capabilities?format=json](#) ;
Import the custom audio file: POST [/ISAPI/AccessControl/customAudio/addCustomAudio?format=json](#) ;
Delete the custom audio file: POST [/ISAPI/AccessControl/customAudio/deleteCustomAudio?format=json](#) ;
Search for the applying status of a specified custom audio file: POST [/ISAPI/AccessControl/customAudio/searchCustomAudioStatus?format=json](#) .
12. Extended message about access control event information
[JSON_EventNotificationAlert_AccessControllerEvent](#) :
added a sub node **HealthInfo** (health information) to the node **AccessControllerEvent**.
13. Extended message about event information of swiping ID card
[JSON_EventNotificationAlert_IDCardInfoEvent](#) :
added a sub node **HealthInfo** (health information) to the node **IDCardInfoEvent**.

Summary of Changes in Version 2.6_Mar., 2021

Related Product: DS-K1T671TM-3XF, DS-K1T671M-3XF, DS-K1T671TMW-3XF, and DS-K1TA70MI-T Face Recognition Terminal with Software Version 3.2.2

1. Added functions of temperature measurement, refer to [Temperature Measurement](#) .
2. Added URIs of configuring health code parameters:

- Get configuration capability: GET [/ISAPI/AccessControl/healthCodeCfg/capabilities?format=json](#) ;
Get or set parameters: GET or PUT [/ISAPI/AccessControl/healthCodeCfg?format=json](#) .
3. Added URIs of configuring health code display parameters:
Get configuration capability: GET [/ISAPI/AccessControl/showHealthCodeCfg/capabilities?format=json](#) ;
Get or set parameters: GET or PUT [/ISAPI/AccessControl/showHealthCodeCfg?format=json](#) .
4. Added two URIs of configuring black body parameters:
Get configuration capability: GET [/ISAPI/AccessControl/blackObject/capabilities?format=json](#) ;
Get or set parameters: GET or PUT [/ISAPI/AccessControl/blackObject?format=json](#) .
5. Extended the functional capability message of access control [XML Cap AccessControl](#) (related URI: [/ISAPI/AccessControl/capabilities](#)):
added six node: **<isSupportTemperatureMeasureCfg>** (whether it supports configuring temperature measurement parameters), **<isSupportTemperatureMeasureAreaCfg>** (whether it supports configuring parameters of the temperature measurement area), **<isSupportTemperatureMeasureAreaCalibrationCfg>** (whether it supports configuring calibration parameters of the temperature measurement area), **<isSupportBlackObjectCfg>** (whether it supports configuring black body parameters), **<isSupportHealthCodeCfg>** (whether it supports configuring health code parameters), and **<isSupportShowHealthCodeCfg>** (whether it supports configuring display parameters of the health code).
6. Extended the configuration capability message [JSON Cap AcsCfg](#) and the parameter message [JSON AcsCfg](#) of the access controller (related URIs: [/ISAPI/AccessControl/AcsCfg/capabilities?format=json](#) and [/ISAPI/AccessControl/AcsCfg?format=json](#)):
added 7 nodes: **uploadVerificationPic** (whether to upload the authenticated picture), **saveVerificationPic** (whether to save the authenticated picture), **saveFacePic** (whether to save the registered face picture), **thermalUnit** (temperature unit), **highestThermalThresholdF** (the maximum value of the temperature threshold), **lowestThermalThresholdF** (the minimum value of the temperature threshold), and **thermalCompensation** (temperature compensation).
7. Extended the event information message of face temperature screening
[JSON EventNotificationAlert FaceTempScreeningEventMsg](#) :
added a sub node **helmet** (whether the person wears a hard hat) to the node **FaceTemperatureMeasurementEvent**.
8. Extended the event message of scanning QR code
[JSON EventNotificationAlert QRCodeEventMsg](#) :
added a sub node **helmet** (whether the person wears a hard hat) to the node **QRCodeEvent**.
9. Extended the event message of swiping ID card [JSON EventNotificationAlert IDCARDInfoEvent](#) :
added a sub node **helmet** (whether the person wears a hard hat) to the node **IDCardInfoEvent**.
10. Extended the configuration capability message [XML Cap IdentityTerminal](#) and the parameter message [XML IdentityTerminal](#) of the intelligent identity recognition terminal (related URIs: [/ISAPI/AccessControl/IdentityTerminal/capabilities](#) and [/ISAPI/AccessControl/IdentityTerminal](#)):
added a node <**showMode**> (display mode).

11. Extended the capability message **JSON_FaceTemperatureEventCap** and the result message **JSON_FaceTemperatureEvent** of actively getting face temperature screening events (related URIs: </ISAPI/AccessControl/FaceTemperatureEvent/capabilities?format=json> and </ISAPI/AccessControl/FaceTemperatureEvent?format=json>):
added a sub node **helmet** (whether the person wears a hard hat) to the node **InfoList**.
12. Extended the capability message **JSON_QRCodeEventCap** and the result message **JSON_QRCodeEvent** of actively getting QR code scanning events (related URIs: </ISAPI/AccessControl/QRCodeEvent/capabilities?format=json> and </ISAPI/AccessControl/QRCodeEvent?format=json>):
added a sub node **helmet** (whether the person wears a hard hat) to the node **InfoList**.
13. Extended the capability message **JSON_IDCardInfoEventCap** and the result message **JSON_IDCardInfoEvent** of actively getting ID card swiping events (related URIs: </ISAPI/AccessControl/IDCardInfoEvent/capabilities?format=json> and </ISAPI/AccessControl/IDCardInfoEvent?format=json>):
added a sub node **helmet** (whether the person wears a hard hat) to the node **InfoList**.

Summary of Changes in Version 2.6_Jan., 2021

Related Products: DS-K1T331 Series, DS-K1T341A Series, DS-K1T341M Series, DS-K1T642 Series, DS-K1T671 Series, DS-K1T672 Series, DS-K5671 Series, DS-K5672 Series, and DS-K5604A Series Face Recognition Terminal with Software Version 3.2.0; DS-K1A330 Series Face Time Attendance Terminal with Software Version 3.2.0

1. Extended face picture library capability message **JSON_FPLibCap** (related URI: </ISAPI/Intelligent/FDLib/capabilities?format=json>):
added a node **featurePointTypeList** (feature point types of face pictures supported by the device).
2. Extended the condition message of setting the face record **JSON_SetFaceRecord** (related URI: </ISAPI/Intelligent/FDLib/FDSetUp?format=json>):
added a node **PicFeaturePoints** (feature points to be applied).
3. Extended the condition message of editing face records in the face picture library in a batch **JSON_BatchEditFaceRecord** (related URI: </ISAPI/Intelligent/FDLib/FDModify?format=json>):
added a node **PicFeaturePoints** (feature points to be applied).
4. Extended the condition message of adding a face record to the face picture library **JSON_AddFaceRecordCond** (related URI: </ISAPI/Intelligent/FDLib/FaceDataRecord?format=json>):
added a node **PicFeaturePoints** (feature points to be applied).
5. Extended the condition message of editing a face record **JSON_EditFaceRecord** (related URI: </ISAPI/Intelligent/FDLib/FDSearch?format=json&FDID=&FPID=&faceLibType=>):
added a node **PicFeaturePoints** (feature points to be applied).
6. Extended the result message of searching for person information **JSON_UserInfoSearch** (related URI: </ISAPI/AccessControl/UserInfo/Search?format=json>):
added a sub node **id** (ID of the additional person information) to the node **PersonInfoExtends** of **UserInfo**;
deleted a sub node **name** from the node **PersonInfoExtends** of **UserInfo**.

7. Extended the person information message **JSON UserInfo** (related URIs: [/ISAPI/AccessControl/UserInfo/Modify?format=json](#) , [/ISAPI/AccessControl/UserInfo/Record?format=json](#) , and [/ISAPI/AccessControl/UserInfo/SetUp?format=json](#)):
added a sub node **id** (ID of the additional person information) to the node **PersonInfoExtends**; deleted a sub node **name** from the node **PersonInfoExtends**.
8. Extended the person management capability message **JSON Cap UserInfo** (related URI: [/ISAPI/AccessControl/UserInfo/capabilities?format=json](#)):
added a sub node **id** (ID of the additional person information) to the node **PersonInfoExtends**; deleted a sub node **name** from the node **PersonInfoExtends**.
9. Added two URIs of configuring the name of the additional person information:
Get configuration capability: GET [/ISAPI/AccessControl/personInfoExtendName/capabilities?format=json](#) ;
Get or set parameters: GET or PUT [/ISAPI/AccessControl/personInfoExtendName?format=json](#) .
10. Extended access control event types in **Access Control Event Types** :
added an event type 0xc1—"MINOR_FULL_STAFF" (Number of People Exceeds 90% of Capacity).
11. Extended log types in **Log Types for ISAPI** :
added 15 operation log types: "localParamFactoryDefault" (Restore to default settings locally), "remoteParamFactoryDefault" (Restore to default settings remotely), "remoteDeleteAllVerifyOrCapPics" (Delete all authenticated or captured face pictures remotely), "localDeleteAllVerifyOrCapPics" (Delete all authenticated or captured face pictures locally), "remoteDeleteEventsAtSpecTime" (Delete events by specified time remotely), "localDeleteEventsAtSpecTime" (Delete events by specified time locally), "remoteOpenSummerTime" (Enable DST remotely), "localOpenSummerTime" (Enable DST locally), "remoteCloseSummerTime" (Disable DST remotely), "localCloseSummerTime" (Disable DST locally), "remoteEZVIZUnbind" (Unbind from EZVIZ cloud remotely), "localEZVIZUnbind" (Unbind from EZVIZ cloud locally), "enterLocalUIBackground" (Enter UI background), "remoteDeleteFaceBaseMap" (Delete registered face pictures remotely), and "localDeleteFaceBaseMap" (Delete registered face pictures locally);
added four additional information log types: "addUserInfo" (Added person information (access control permission)), "modifyUserInfo" (Edit person information (access control permission)), "clearUserInfo" (Delete person information by employee No. (access control permission)), and "clearAllUser" (Delete all person information (access control permission)).

Summary of Changes in Version 2.6_Oct., 2020

Related Product: DS-K1F600U-D6E and DS-K1F600U-D6E-F Enrollment Station with Software Version 1.0.0

1. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [/ISAPI/AccessControl/CapturePresetParam?format=json](#) .
2. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [/ISAPI/AccessControl/CaptureCardInfo?format=json](#) .

3. Extended the capability message of collecting card information ***JSON_CardInfoCap*** and card information message ***JSON_CardInfo_Collection*** (related URIs: [*/ISAPI/AccessControl/CaptureCardInfo/capabilities?format=json*](#) and [*/ISAPI/AccessControl/CaptureCardInfo?format=json*](#)):
added two card types "FelicaCard" (Felica card) and "DesfireCard" (DESFire card) to the node **cardType**.
4. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [*/ISAPI/AccessControl/CaptureIDInfo?format=json*](#).
5. Added URIs of uploading the user list of offline collection:
Upload the user list: POST [*/ISAPI/AccessControl/OfflineCapture/InfoFile?format=json*](#) ;
Get the uploading progress: GET [*/ISAPI/AccessControl/OfflineCapture/InfoFile/progress?format=json*](#) ;
Get details of failing to upload: GET [*/ISAPI/AccessControl/OfflineCapture/uploadFailedDetails?format=json*](#) .
6. Extended the result message of searching for the collected data ***JSON_SearchTaskResponse*** (related URI: [*/ISAPI/AccessControl/OfflineCapture/DataCollections/searchTask?format=json*](#)):
added two sub nodes **cardNo** (card No.) and **cardType** (card type) to the node **CardNoList** of **DataCollections**;
added two sub nodes **IdentityInfo** (identity information) and **CardIssueStatus** (issuing status list of cards containing face pictures and fingerprints) to the node **DataCollections**.
7. Extended parameter message of offline collection rules ***JSON_RuleInfo*** (related URI: [*/ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json*](#)):
added two nodes **enableLocalIssueCard** (whether to enable issuing smart cards locally) and **isLocalStorage** (whether to store face picture and fingerprint information in the device locally).
8. Extended parameter message of offline collection progress ***JSON_CaptureProgress*** (related URI: [*/ISAPI/AccessControl/OfflineCapture/progress?format=json*](#)):
added two nodes **reqIssueNum** (number of persons to be issued with smart cards) and **IssuedNum** (number of persons that have been issued with smart cards).
9. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [*/ISAPI/AccessControl/OfflineCapture/dataOutput?format=json*](#) .
10. Extended parameter message for exporting offline collected data ***JSON_DataOutputCfg*** (related URI: [*/ISAPI/AccessControl/OfflineCapture/dataOutput?format=json*](#)):
added a node **type** (exporting type).
11. Added a URI of downloading the user list template of offline collection: POST [*/ISAPI/AccessControl/OfflineCapture/InfoFileTemplateDownload?format=json*](#) .
12. Added a URI of downloading data collected offline: POST [*/ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?format=json*](#) .
13. Extended the offline collection capability message ***JSON_OfflineCaptureCap*** (related URI: [*/ISAPI/AccessControl/OfflineCapture/capabilities?format=json*](#)):
added three sub nodes **maxSize** (size of the card No. list), **cardNo** (card No.), and **cardType** (card type) to the node **CardNoList** of **DataCollections** of **SearchTask**;

added two sub nodes **IdentityInfo** (identity information) and **CardIssueStatus** (issuing status list of cards containing face pictures and fingerprints) to the node **DataCollections** of **SearchTask**;

added two nodes **enableLocalIssueCard** (whether to enable issuing smart cards locally) and **isLocalStorage** (whether to store face picture and fingerprint information in the device locally) to the node **RuleInfo**;

added two nodes **reqIssueNum** (number of persons to be issued with smart cards) and **IssuedNum** (number of persons that have been issued with smart cards) to the node **CaptureProgress**.

14. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [/ISAPI/AccessControl/CardOperations/sectionEncryption?format=json](#) .
15. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [/ISAPI/AccessControl/CardOperations/verification?format=json](#) .
16. Added two query parameters **security** (the version No. of encryption scheme) and **iv** (the initialization vector) to the request URI [/ISAPI/AccessControl/CardOperations/controlBlock?format=json](#) .
17. Added a URI for sending a request for card issuing: PUT [/ISAPI/AccessControl/CardOperations/localIssueRequest?format=json](#) .
18. Added a URI of getting the current card issuing status and real-time card issuing results: GET [/ISAPI/AccessControl/CardOperations/localIssueRes?format=json](#) .
19. Added a URI of getting or setting rule parameters for issuing smart cards: GET or PUT [/ISAPI/AccessControl/CardOperations/localIssueCfg?format=json](#) .
20. Added a URI of deleting data from the card: PUT [/ISAPI/AccessControl/CardOperations/clearData?format=json](#) .
21. Added a URI of setting custom card information: PUT [/ISAPI/AccessControl/CardOperations/customData?format=json](#) .
22. Added a URI of searching for custom card information: POST [/ISAPI/AccessControl/CardOperations/customData/searchTask?format=json](#) .
23. Added a URI of getting the smart card issuing status: GET [/ISAPI/AccessControl/CardOperations/cardIssueStatus?format=json](#) .
24. Extended card operation capability message **JSON_CardOperationsCap** (related URI: [/ISAPI/AccessControl/CardOperations/capabilities?format=json](#)):
added seven nodes: **Issue** (capability of sending a request for card issuing and getting the current card issuing status and real-time card issuing results), **localIssueCfg** (capability of configuring rule parameters for issuing smart cards), **ClearData** (capability of deleting data from the card), **CustomData** (capability of setting custom card information), **CustomDataSearchCond** (condition configuration capability of searching for custom card information), **CustomDataResult** (result capability of searching for custom card information), and **CardIssueStatus** (capability of getting the smart card issuing status).

Summary of Changes in Version 2.6_Aug., 2020

Related Product: DS-K1T680DX Series Face Recognition Terminal with Software Version 3.1.2

1. Extended the functional capability message of access control **XML_Cap_AccessControl** (related URI: </ISAPI/AccessControl/capabilities>):
added 9 nodes, i.e., **<isSupportSafetyHelmetDetection>** (whether it supports configuring hard hat detection), **<isSupportKeyCfgAttendance>** (whether it supports configuring parameters of attendance check by pressing the key), **<isSupportIDBlackListTemplate>** (whether it supports downloading the ID card blocklist template), **<isSupportAttendanceWeekPlan>** (whether it supports configuring parameters of the week attendance schedule), **<isSupportClearAttendancePlan>** (whether it supports clearing the week attendance schedule), **<isSupportAttendanceMode>** (whether it supports configuring the attendance mode), **<isSupportAttendancePlanTemplate>** (whether it supports configuring the attendance schedule template), **<isSupportAttendancePlanTemplateList>** (whether it supports getting the list of attendance schedule templates), and **<isSupportCardVerificationRule>** (whether it supports configuring card No. authentication mode).
2. Extended capability message **JSON_Cap_AcsEvent** and result parameter message **JSON_AcsEvent** of searching for access control events (related URIs: </ISAPI/AccessControl/AcsEvent/capabilities?format=json> and </ISAPI/AccessControl/AcsEvent?format=json>):
added three sub nodes to the node **InfoList**, i.e., **label** (custom attendance name), **mask** (whether the person is wearing mask), and **helmet** (whether the person is wearing hard hat).
3. Extended the configuration capability message **JSON_Cap_CardReaderCfg** and the parameter message **JSON_CardReaderCfg** of the card reader (related URIs: </ISAPI/AccessControl/CardReaderCfg/capabilities?format=json> and </ISAPI/AccessControl/CardReaderCfg/<ID>?format=json>):
added three nodes: **enableReverseCardNo** (whether to enable reversing the card No.), **independSwipeIntervals** (time interval of person authentication), and **maskFaceMatchThresholdN** (1:N face picture (face with mask and normal background) comparison threshold).
4. Extended message about access control event information **JSON_EventNotificationAlert_AccessControllerEvent**:
added two sub nodes **label** (custom attendance name) and **helmet** (whether the person is wearing hard hat) to the node **AccessControllerEvent**.
5. Extended configuration capability message **XML_Cap_IdentityTerminal** and parameter message **XML_IdentityTerminal** of intelligent identity recognition terminal (related URIs: </ISAPI/AccessControl/IdentityTerminal/capabilities> and </ISAPI/AccessControl/IdentityTerminal>):
added a sub node **<maskFaceMatchThresholdN>** (1:N face picture (face with mask and normal background picture) comparison threshold of ECO mode) to the node **<ecoMode>**.
6. Extended configuration capability message **JSON_RFCardCfgCap** and parameter message **JSON_RFCardCfg** of enabling RF (Radio Frequency) card recognition (related URIs: </ISAPI/AccessControl/Configuration/RFCardCfg/capabilities?format=json> and </ISAPI/AccessControl/Configuration/RFCardCfg?format=json>):

add two card types "DesfireCard" (DESFire card) and "FelicaCard" (FeliCa card) to the node **cardType**.

7. Added the function of configuring attendance status and schedule, refer to [Configure Attendance Status and Schedule](#) .

8. Added URIs of configuring card No. authentication mode:

Get the configuration capability: GET [/ISAPI/AccessControl/CardVerificationRule/capabilities?format=json](#) ;

Get or set parameters: GET or PUT [/ISAPI/AccessControl/CardVerificationRule?format=json](#) ;

Get the switching progress and configuration result: GET [/ISAPI/AccessControl/CardVerificationRule/progress?format=json](#) .

Summary of Changes in Version 2.6_Apr., 2020

Related Product: DS-K1T671TM-3XF, DS-K1T671TMW-3XF, DS-K5671-3XF/ZU, DS-K5604A-3XF/V, and DS-K1TA70MI-T Face Recognition Terminal with Software Version 2.2.6

1. Extended message about access control event information

[JSON_EventNotificationAlert_AccessControllerEvent](#) :

added 8 sub nodes: **name** (person name), **QRCodeInfo** (QR code information), **thermometryUnit** (temperature unit), **currTemperature** (face temperature), **isAbnormalTemperature** (whether the face temperature is abnormal), **RegionCoordinates** (face temperature's coordinates), **remoteCheck** (whether remote verification is required), and **mask** (whether the person is wearing mask or not) to the node **AccessControllerEvent**.

2. Extended message about event information of swiping ID card

[JSON_EventNotificationAlert_IDCardInfoEvent](#) :

added 7 sub nodes: **QRCodeInfo** (QR code information), **thermometryUnit** (temperature unit), **currTemperature** (face temperature), **isAbnormalTemperature** (whether the face temperature is abnormal), **RegionCoordinates** (face temperature's coordinates), **remoteCheck** (whether remote verification is required), and **mask** (whether the person is wearing mask or not) to the node **IDCardInfoEvent**.

3. Added a message about event information of scanning QR code

[JSON_EventNotificationAlert_QRCodeEventMsg](#) .

4. Added a message about face temperature screening event information

[JSON_EventNotificationAlert_FaceTempScreeningEventMsg](#) .

5. Added two URIs of verifying the access control event remotely:

Get capability: GET [/ISAPI/AccessControl/remoteCheck/capabilities?format=json](#) ;

Verify the access control event remotely: PUT [/ISAPI/AccessControl/remoteCheck?format=json](#) .

6. Extended configuration capability message of the access controller [JSON_Cap_AcsCfg](#) (related URI: [/ISAPI/AccessControl/AcsCfg/capabilities?format=json](#)):

added 11 nodes: **thermalEnabled** (whether to enable temperature measurement), **thermalMode** (whether to enable temperature measurement only mode), **thermalPictureEnabled** (whether to enable uploading visible light pictures in temperature measurement only mode), **isSupportThermalIp** (whether it supports configuring IP address of the thermography device), **highestThermalThreshold** (upper limit of the temperature

threshold), **lowestThermalThreshold** (lower limit of the temperature threshold), **thermalDoorEnabled** (whether to open the door when the temperature is above the upper limit or below the lower limit of the threshold), **QRCodeEnabled** (whether to enable QR code function), **remoteCheckDoorEnabled** (whether to enable controlling the door by remote verification), **checkChannelType** (verification channel type), and **isSupportChannelp** (whether it supports configuring IP address of the verification channel).

7. Extended parameter message of the access controller **JSON_AcsCfg** (related URI: **/ISAPI/AccessControl/AcsCfg?format=json**):
added 11 nodes: **thermalEnabled** (whether to enable temperature measurement), **thermalMode** (whether to enable temperature measurement only mode), **thermalPictureEnabled** (whether to enable uploading visible light pictures in temperature measurement only mode), **thermaltip** (IP address of the thermography device), **highestThermalThreshold** (upper limit of the temperature threshold), **lowestThermalThreshold** (lower limit of the temperature threshold), **thermalDoorEnabled** (whether to open the door when the temperature is above the upper limit or below the lower limit of the threshold), **QRCodeEnabled** (whether to enable QR code function), **remoteCheckDoorEnabled** (whether to enable controlling the door by remote verification), **checkChannelType** (verification channel type), and **channelp** (IP address of the verification channel).
8. Added two URIs of configuring mask detection parameters:
Get configuration capability: GET **/ISAPI/AccessControl/maskDetection/capabilities?format=json**;
Get or set parameters: GET or PUT **/ISAPI/AccessControl/maskDetection?format=json**.
9. Extended access control capability message **XML_Cap_AccessControl** (related URI: **/ISAPI/AccessControl/capabilities**):
added two nodes: <isSupportRemoteCheck> (whether it supports verifying access control events remotely) and <isSupportMaskDetection> (whether it supports mask detection).
10. Extended device capability message **XML_DeviceCap** (related URI: **/ISAPI/System/capabilities**):
added two nodes: <isSupportFaceTemperatureMeasurementEvent> (whether it supports uploading face temperature screening events) and <isSupportQRCodeEvent> (whether it supports uploading QR code events).

Summary of Changes in Version 2.6_Feb., 2020

Related Product: DS-K1T804A Series and DS-K1T8003 Series Fingerprint Access Control Terminal with Software Version 1.3.0; DS-K1A802A Series and DS-K1A8503 Series Fingerprint Time Attendance Terminal with Software Version 1.3.0

1. Extended person management capability message **JSON_Cap_UserInfo** (related URI: **/ISAPI/AccessControl/UserInfo/capabilities?format=json**):
added a node **purePwdVerifyEnable** (whether the device supports opening the door only by password).
2. Extended message about week schedule configuration capability of card reader authentication mode **JSON_Cap_VerifyWeekPlanCfg** (related URI: **/ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities?format=json**):

- added a node **purePwdVerifyEnable** (whether the device supports opening the door only by password).
3. Extended message about holiday schedule configuration capability of card reader authentication mode **JSON_Cap_VerifyHolidayPlanCfg** (related URI: **/ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities?format=json**) :
added a node **purePwdVerifyEnable** (whether the device supports opening the door only by password).
4. Extended configuration capability message of event and card linkage **JSON_Cap_EventCardLinkageCfg** (related URI: **/ISAPI/AccessControl/EventCardLinkageCfg/capabilities?format=json**) :
added a node **purePwdVerifyEnable** (whether the device supports opening the door only by password).
5. Extended condition message of searching for access control events **JSON_AcsEventCond** (related URI: **/ISAPI/AccessControl/AcsEvent?format=json**) :
added a node **timeReverseOrder** (whether to return events in descending order of time).
6. Extended capability message of searching for access control events **JSON_Cap_AcsEvent** (related URI: **/ISAPI/AccessControl/AcsEvent/capabilities?format=json**) :
added a sub node **timeReverseOrder** (whether to return events in descending order of time) to the node **AcsEventCond**.
7. Extended message about access control event information **JSON_EventNotificationAlert_AccessControllerEvent** :
added a sub node **purePwdVerifyEnable** (whether the device supports opening the door only by password) to the node **AccessControllerEvent**.
8. Extended configuration capability message **JSON_Cap_CardReaderCfg** and parameter message **JSON_CardReaderCfg** of card reader (related URIs: **/ISAPI/AccessControl/CardReaderCfg/capabilities?format=json** and **/ISAPI/AccessControl/CardReaderCfg/<ID>?format=json**) :
added two nodes: **FPAlgorithmVersion** (fingerprint algorithm library version) and **cardReaderVersion** (card reader version).

Summary of Changes in Version 2.6_Jan., 2020

Related Product: DS-K1T341AM, DS-K1T341AMF, DS-K1T642M, DS-K1T642MF, DS-K1T642E, DS-K1T642EF, DS-K1T642MW, DS-K1T642MFW, DS-K1T642EW, and DS-K1T642EFW Face Recognition Terminal with Software Version 1.0

1. Extended person information message **JSON_UserInfo** (related URIs: **/ISAPI/AccessControl/UserInfo/Record?format=json**, **/ISAPI/AccessControl/UserInfo/Modify?format=json**, and **/ISAPI/AccessControl/UserInfo/SetUp?format=json**) :
added two nodes: **gender** (gender of the person in the face picture) and **PersonInfoExtends** (additional person information).
2. Extended result message of searching for person information **JSON_UserInfoSearch** (related URI: **/ISAPI/AccessControl/UserInfo/Search?format=json**) :
added two sub nodes: **gender** (gender of the person in the face picture) and **PersonInfoExtends** (additional person information) to the node **UserInfo**.

3. Extended person management capability message [JSON Cap UserInfo](#) (related URI: /ISAPI/AccessControl/UserInfo/capabilities?format=json):
added a sub node **fuzzySearch** (keywords for fuzzy search) to the node **UserInfoSearchCond**; added two nodes: **gender** (gender of the person in the face picture) and **PersonInfoExtends** (additional person information).
4. Added a URI of exporting or importing person permission data securely: GET or POST /ISAPI/AccessControl/userData?secretkey=.
5. Added a URI of exporting the maintenance data: GET /ISAPI/AccessControl/maintenanceData?secretkey=.
6. Added two URIs of configuring text parameters of the audio prompt for authentication results:
Get configuration capability: GET /ISAPI/AccessControl/Verification/ttsText/capabilities?format=json ;
Get or set parameters: GET or PUT /ISAPI/AccessControl/Verification/ttsText?format=json .
7. Extended configuration capability message [JSON Cap AcsCfg](#) and parameter message [JSON AcsCfg](#) of the access controller (related URIs: /ISAPI/AccessControl/AcsCfg/capabilities?format=json and /ISAPI/AccessControl/AcsCfg?format=json):
added three nodes: **showPicture** (whether to display the authenticated picture), **showEmployeeNo** (whether to display the authenticated employee ID), and **showName** (whether to display the authenticated name).
8. Extended condition configuration capability [XML Cap FaceCompareCond](#) and condition parameter message [XML FaceCompareCond](#) of face picture comparison (related URIs: /ISAPI/AccessControl/FaceCompareCond/capabilities and /ISAPI/AccessControl/FaceCompareCond):
added a node <maxDistance> (maximum recognition distance).
9. Added two URIs of configuring door lock status when the device is powered off:
Get configuration capability: GET /ISAPI/AccessControl/Configuration/lockType/capabilities?format=json ;
Get or set parameters: GET or PUT /ISAPI/AccessControl/Configuration/lockType?format=json .
10. Extended functional capability message of access control [XML Cap AccessControl](#) (related URI: /ISAPI/AccessControl/capabilities):
added six nodes: <isSupportTTSText> (whether it supports configuring the text of the audio prompt), <isSupportIDBlackListCfg> (whether it supports applying ID card blocklist), <isSupportUserDataImport> (whether it supports importing person permission data), <isSupportUserDataExport> (whether it supports exporting person permission data), <isSupportMaintenanceDataExport> (whether it supports exporting maintenance data), and <isSupportLockTypeCfg> (whether it supports configuring door lock status when the device is powered off).

Summary of Changes in Version 2.0_Aug., 2019

Related Product: DS-K1T640 Series, DS-K1T671 Series, and DS-K5671 Series Face Recognition Terminal with Software Version 2.1.1

1. Extended the capability message of collecting face data [XML Cap CaptureFaceData](#) (related URI: /ISAPI/AccessControl/CaptureFaceData/capabilities):

- added a sub node <**dataType**> (data type of collected face pictures) to the node <**CaptureFaceDataCond**>.
2. Extended the condition message of collecting face data **XML_CaptureFaceDataCond** (related URI: [/ISAPI/AccessControl/CaptureFaceData](#)):
added a node <**dataType**> (data type of collected face pictures).

Summary of Changes in Version 2.0_July, 2019

Related Products: DS-K1A802 Series, DS-K1A802A Series, and DS-K1A8503 Series Fingerprint Time Attendance Terminal; DS-K1T804 Series, DS-K1T8003 Series, and DS-K1T8004 Series Fingerprint Access Control Terminal.

1. Extended person management capability message **JSON_Cap_UserInfo** and person information message **JSON_UserInfo** (related URIs: [/ISAPI/AccessControl/UserInfo/capabilities?format=json](#) , [/ISAPI/AccessControl/UserInfo/Record?format=json](#) , and [/ISAPI/AccessControl/UserInfo/Modify?format=json](#)):
added a node **addUser** (whether to add the person if the person information being edited does not exist);
added a person authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the node **userVerifyMode**.
2. Extended person information search result message **JSON_UserInfoSearch** (related URI: [/ISAPI/AccessControl/UserInfo/Search?format=json](#)):
added a person authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the sub node **userVerifyMode** of the node **UserInfo** (person information).
3. Extended card information capability message **JSON_Cap_CardInfo** and card information message **JSON_CardInfo** (related URIs: [/ISAPI/AccessControl/CardInfo/capabilities?format=json](#) and [/ISAPI/AccessControl/CardInfo/Modify?format=json](#)):
added a node **addCard** (whether to add the card if the card information being edited does not exist).
4. Extended capability message **XML_Cap_RemoteControlDoor** and parameter message **XML_RemoteControlDoor** of remotely controlling the door or elevator (related URIs: [/ISAPI/AccessControl/RemoteControl/door/capabilities](#) and [/ISAPI/AccessControl/RemoteControl/door<ID>](#)):
added a node <**password**> (password for opening door).
5. Extended week schedule configuration capability message **JSON_Cap_VerifyWeekPlanCfg** and week schedule parameter message **JSON_VerifyWeekPlanCfg** of the card reader authentication mode (related URIs: [/ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities?format=json](#) and [/ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json](#)):
added an authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the sub node **verifyMode** of the node **WeekPlanCfg** (week schedule parameters).
6. Extended holiday schedule configuration capability message **JSON_Cap_VerifyHolidayPlanCfg** and holiday schedule parameter message **JSON_VerifyHolidayPlanCfg** of the card reader authentication mode (related URIs: [/ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities?format=json](#) and [/ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json](#)):

- added an authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the sub node **verifyMode** of the node **HolidayPlanCfg** (holiday schedule parameters).
7. Extended condition message of searching for access control events **JSON_AcsEventCond** (related URI: [/ISAPI/AccessControl/AcsEvent?format=json](#)):
added a node **eventAttribute** (event attribute).
8. Extended result message of searching for access control events **JSON_AcsEvent** (related URI: [/ISAPI/AccessControl/AcsEvent?format=json](#)):
added two sub nodes: **attendanceStatus** (attendance status) and **statusValue** (status value) to the node **InfoList** (event details);
added an authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the sub node **currentVerifyMode** of the node **InfoList** (event details).
9. Extended capability message of searching for access control events **JSON_Cap_AcsEvent** (related URI: [/ISAPI/AccessControl/AcsEvent/capabilities?format=json](#)):
added a sub node **eventAttribute** (event attribute) to the node **AcsEventCond** (search conditions);
added two sub nodes: **attendanceStatus** (attendance status) and **statusValue** (status value) to the node **InfoList** (event details);
added an authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the sub node **currentVerifyMode** of the node **InfoList** (event details).
10. Extended condition message of getting the total number of access control events by conditions **JSON_AcsEventTotalNumCond** (related URI: [/ISAPI/AccessControl/AcsEventTotalNum?format=json](#)):
added a node **eventAttribute** (event attribute).
11. Extended capability message of getting the total number of the access control events by conditions **JSON_Cap_AcsEventTotalNum** (related URI: [/ISAPI/AccessControl/AcsEventTotalNum/capabilities?format=json](#)):
added a sub node **eventAttribute** (event attribute) to the node **AcsEventTotalNumCond** (search conditions).
12. Extended message of access control event information
JSON_EventNotificationAlert_AccessControllerEvent :
added two sub nodes: **attendanceStatus** (attendance status) and **statusValue** (status value) to the node **AccessControllerEvent**;
added an authentication mode "cardOrFpOrPw" (card or fingerprint or password) to the sub node **currentVerifyMode** of the node **AccessControllerEvent**.
13. Extended capability message of getting working status of access controller
JSON_Cap_AcsWorkStatus and working status message of access controller
JSON_AcsWorkStatus (related URLs: [/ISAPI/AccessControl/AcsWorkStatus/capabilities?format=json](#) and [/ISAPI/AccessControl/AcsWorkStatus?format=json](#)):
added an authentication mode 27 (card or fingerprint or password) to the node **cardReaderVerifyMode**.
14. Extended door (floor) configuration capability message **XML_Cap_DoorParam** and door (floor) parameter message **XML_DoorParam** (related URLs: [/ISAPI/AccessControl/Door/param/<ID>/capabilities](#) and [/ISAPI/AccessControl/Door/param/<ID>](#)):

- added a node <**remoteControlPWStatus**> (whether the password has been configured for remote door control).
15. Added the function of configuring attendance status, refer to [**Configure Attendance Status and Schedule**](#) for details.
 16. Added the function of configuring password for remote door control, refer to [**Configure Password for Remote Door Control**](#) for details.
 17. Added the function of collecting card information, refer to [**Collect Card Information**](#) for details.
 18. Extended access control capability message [**XML_Cap_AccessControl**](#) (related URI: [**/ISAPI/AccessControl/capabilities**](#)):
added five nodes: <**isSupportRemoteControlPWChcek**> (whether to support verifying the password for remote door control), <**isSupportRemoteControlPWCfg**> (whether to support configuring password for remote door control), <**isSupportAttendanceStatusModeCfg**> (whether to support configuring attendance mode), <**isSupportAttendanceStatusRuleCfg**> (whether to support configuring attendance status and rule), and <**isSupportCaptureCardInfo**> (whether to support collecting card information).
 19. Extended the access control event types in [**Access Control Event Types**](#) :
added six event types to MAJOR_EVENT: "MINOR_LOCAL_UPGRADE_FAIL" (Local Upgrade Failed), "MINOR_REMOTE_UPGRADE_FAIL" (Remote Upgrade Failed), "MINOR_REMOTE_EXTEND_MODULE_UPGRADE_SUCC" (Extension Module is Remotely Upgraded), "MINOR_REMOTE_EXTEND_MODULE_UPGRADE_FAIL" (Upgrading Extension Module Remotely Failed), "MINOR_REMOTE_FINGER_PRINT_MODULE_UPGRADE_SUCC" (Fingerprint Module is Remotely Upgraded), and "MINOR_REMOTE_FINGER_PRINT_MODULE_UPGRADE_FAIL" (Upgrading Fingerprint Module Remotely Failed).

Summary of Changes in Version 2.0_July, 2019

Related Products: DS-K1T804 Series Fingerprint Access Control Terminal.

1. Added the URIs to enable or disable NFC (Near-Field Communication) function:
Get the configuration capability: GET [**/ISAPI/AccessControl/Configuration/NFCCfg/capabilities?format=json**](#) ;
Get parameters: GET [**/ISAPI/AccessControl/Configuration/NFCCfg?format=json**](#) ;
Set parameters: PUT [**/ISAPI/AccessControl/Configuration/NFCCfg?format=json**](#) .
2. Added the URIs to enable or disable RF (Radio Frequency) card recognition:
Get the configuration capability: GET [**/ISAPI/AccessControl/Configuration/RFCardCfg/capabilities?format=json**](#) ;
Get parameters: GET [**/ISAPI/AccessControl/Configuration/RFCardCfg?format=json**](#) ;
Set parameters: PUT [**/ISAPI/AccessControl/Configuration/RFCardCfg?format=json**](#) .
3. Extended access control capability message [**XML_Cap_AccessControl**](#) (related URI: [**/ISAPI/AccessControl/capabilities**](#)):
added two nodes: <**isSupportNFCCfg**> (whether the device supports enabling or disabling NFC function) and <**isSupportRFCardCfg**> (whether the device supports enabling or disabling RF card recognition).
4. Extended the access control event types in [**Access Control Event Types**](#) :

added four operation event types to MAJOR_OPERATION:
"MINOR_M1_CARD_ENCRYPT_VERIFY_OPEN" (M1 Card Encryption Verification Enabled),
"MINOR_M1_CARD_ENCRYPT_VERIFY_CLOSE" (M1 Card Encryption Verification Disabled),
"MINOR_NFC_FUNCTION_OPEN" (Opening Door with NFC Card Enabled), and
"MINOR_NFC_FUNCTION_CLOSE" (Opening Door with NFC Card Disabled);
added eight event types to MAJOR_EVENT: "MINOR_INFORMAL_MIFARE_CARD_VERIFY_FAIL"
(Authentication Failed: Invalid Mifare Card), "MINOR_CPU_CARD_ENCRYPT_VERIFY_FAIL"
(Verifying CPU Card Encryption Failed), "MINOR_NFC_DISABLE_VERIFY_FAIL" (Disabling NFC
Verification Failed), "MINOR_EM_CARD_RECOGNIZE_NOT_ENABLED" (EM Card Recognition
Disabled), "MINOR_M1_CARD_RECOGNIZE_NOT_ENABLED" (M1 Card Recognition Disabled),
"MINOR_CPU_CARD_RECOGNIZE_NOT_ENABLED" (CPU Card Recognition Disabled),
"MINOR_ID_CARD_RECOGNIZE_NOT_ENABLED" (ID Card Recognition Disabled), and
"MINOR_CARD_SET_SECRET_KEY_FAIL" (Importing Key to Card Failed).

5. Extended the event linkage types in [Event Linkage Types](#) :

added eight event linkage types of the authentication unit:
"EVENT_ACS_INFORMAL_MIFARE_CARD_VERIFY_FAIL" (Authentication Failed: Invalid Mifare
Card), "EVENT_ACS_CPU_CARD_ENCRYPT_VERIFY_FAIL" (Verifying CPU Card Encryption Failed),
"EVENT_ACS_NFC_DISABLE_VERIFY_FAIL" (Disabling NFC Verification Failed),
"EVENT_ACS_EM_CARD_RECOGNIZE_NOT_ENABLED" (EM Card Recognition Disabled),
"EVENT_ACS_M1_CARD_RECOGNIZE_NOT_ENABLED" (M1 Card Recognition Disabled),
"EVENT_ACS_CPU_CARD_RECOGNIZE_NOT_ENABLED" (CPU Card Recognition Disabled),
"EVENT_ACS_ID_CARD_RECOGNIZE_NOT_ENABLED" (ID Card Recognition Disabled), and
"EVENT_ACS_CARD_SET_SECRET_KEY_FAIL" (Importing Key to Card Failed).

Summary of Changes in Version 2.0_June, 2019

Related Products: DS-K1T607 Series, DS-K1T610 Series, and DS-K5607 Series Face Recognition
Terminal in Version 1.1

1. Extended picture storage server capability message [JSON_Cap_PictureServerInformation](#) and
picture storage server parameter message [JSON_PictureServerInformation](#) (related URIs: [/ISAPI/System/PictureServer/capabilities?format=json](#) and [/ISAPI/System/PictureServer?format=json](#)):
added a sub node **cloudPoolIdEx** (cloud storage pool ID) to the node **cloudStorage** (parameters
of the cloud storage server).
2. Extended person management capability message [JSON_Cap_UserInfo](#) (related URI: [/ISAPI/AccessControl/UserInfo/capabilities?format=json](#)):
added a sub node **searchID** (search ID) to the node **UserInfoSearchCond** (search conditions);
added a node **maxRecordNum** (supported maximum number of records (person records)).
3. Extended card information capability message [JSON_Cap_CardInfo](#) (related URI: [/ISAPI/AccessControl/CardInfo/capabilities?format=json](#)):
added a sub node **searchID** (search ID) to the node **CardInfoSearchCond** (search conditions);
added a node **maxRecordNum** (supported maximum number of records (card records)).
4. Extended fingerprint configuration capability message [JSON_Cap_FingerPrintCfg](#) (related URI: [/ISAPI/AccessControl/FingerPrintCfg/capabilities?format=json](#)):

- added a node **searchID** (search ID).
5. Added the function of managing face information (including creating face picture library, managing face records in the face picture library, and configuring facial recognition mode), refer to **Manage Face Information** for details.
6. Extended fingerprint and card reader configuration capability message **JSON_Cap_CardReaderCfg** and fingerprint and card reader parameter message **JSON_CardReaderCfg** (related URLs: [/ISAPI/AccessControl/CardReaderCfg/capabilities?format=json](#) and [/ISAPI/AccessControl/CardReaderCfg/<ID>?format=json](#)):
added two authentication modes: "cardOrFace" (card or face) and "cardOrFaceOrFp" (card or face or fingerprint) to the node **defaultVerifyMode** (default authentication mode of the fingerprint and card reader);
added a node **faceRecognizeEnable** (whether to enable facial recognition).
7. Extended configuration capability message of intelligent identity recognition terminal **XML_Cap_IdentityTerminal** and parameter message of intelligent identity recognition terminal **XML_IdentityTerminal** (related URLs: [/ISAPI/AccessControl/IdentityTerminal/capabilities](#) and [/ISAPI/AccessControl/IdentityTerminal](#)):
added a node <readCardRule> (card No. setting rule).
8. Extended access control capability message **XML_Cap_AccessControl** (related URI: [/ISAPI/AccessControl/capabilities](#)):
added three nodes: <isSupportCaptureFace> (whether to support collecting face pictures), <isSupportCaptureInfraredFace> (whether to support collecting infrared face pictures), and <isSupportFaceRecognizeMode> (whether to support configuring facial recognition mode).

Summary of Changes in Version 2.0_May, 2019

Related Products: DS-K2600 Series Access Controller in Version 2.1.0

1. Extended person information message **JSON_UserInfo** and person information search result message **JSON_UserInfoSearch** (related URLs: [/ISAPI/AccessControl/UserInfo/Record?format=json](#), [/ISAPI/AccessControl/UserInfo/Search?format=json](#), and [/ISAPI/AccessControl/UserInfo/Modify?format=json](#)):
added 11 person authentication modes "faceOrFpOrCardOrPw" (face or fingerprint or card or password), "faceAndFp" (face+fingerprint), "faceAndPw" (face+password), "faceAndCard" (face+card), "face" (face), "faceAndFpAndCard" (face+fingerprint+card), "faceAndPwAndFp" (face+password+fingerprint), "employeeNoAndFace" (employee No.+face), "faceOrfaceandCard" (face or face+card), "fpOrface" (fingerprint or face), "cardOrfaceOrPw" (card or face or password) to the sub node **userVerifyMode** in the node **UserInfo**.
2. Added a URI to set person information: PUT [/ISAPI/AccessControl/UserInfo/SetUp?format=json](#).
3. Extended person management capability message **JSON_Cap_UserInfo** (related URI: [/ISAPI/AccessControl/UserInfo/capabilities?format=json](#)):
added a function type "setUp" (set person information) to the node **supportFunction**;
added two sub nodes **timeRangeBegin** (start time that can be configured) and **timeRangeEnd** (end time that can be configured) to the node **Valid**.

4. Extended card information message [JSON_CardInfo](#) (related URI: /ISAPI/AccessControl/CardInfo/Record?format=json):
add a node **checkEmployeeNo** (whether to check the existence of the employee No. (person ID)).
5. Added a URI to set card information: PUT /ISAPI/AccessControl/CardInfo/SetUp?format=json .
6. Extended card information capability message [JSON_Cap_CardInfo](#) (related URI: /ISAPI/AccessControl/CardInfo/capabilities?format=json):
added a function type "setUp" (set card information) to the node **supportFunction**;
added a node **checkEmployeeNo** (whether to check the existence of the employee No. (person ID)).
7. Added a URI to set fingerprint parameters: PUT /ISAPI/AccessControl/FingerPrint/SetUp?format=json .
8. Extended parameter message of door control week schedule [JSON_DoorStatusWeekPlanCfg](#) (related URI: /ISAPI/AccessControl/DoorStatusWeekPlanCfg/<PlanNo>?format=json):
add two door status "sleep" and "invalid" to the sub node **doorStatus** in the node **WeekPlanCfg**.
9. Extended configuration capability message of door control week schedule
[JSON_Cap_DoorStatusWeekPlanCfg](#) (related URI: /ISAPI/AccessControl/DoorStatusWeekPlanCfg/capabilities?format=json):
added two door status "sleep" and "invalid" to the sub node **doorStatus** in the node **WeekPlanCfg**;
add a sub node **validUnit** (time accuracy) to the node **TimeSegment** in the node **WeekPlanCfg**.
10. Extended week schedule parameter message of the card reader authentication mode
[JSON_VerifyWeekPlanCfg](#) (related URI: /ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json):
added two authentication modes "sleep" and "invalid" to the sub node **verifyMode** in the node **WeekPlanCfg**.
11. Extended week schedule configuration capability of the card reader authentication mode
[JSON_Cap_VerifyWeekPlanCfg](#) (related URI: /ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities?format=json):
added two authentication modes "sleep" and "invalid" to the sub node **verifyMode** in the node **WeekPlanCfg**;
added a sub node **validUnit** (time accuracy) to the node **TimeSegment** in the node **WeekPlanCfg**.
12. Extended parameter message of door control holiday schedule
[JSON_DoorStatusHolidayPlanCfg](#) (related URI: /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/<PlanNo>?format=json):
add two door status "sleep" and "invalid" to the sub node **doorStatus** in the node **HolidayPlanCfg**.
13. Extended configuration capability message of door control holiday schedule
[JSON_Cap_DoorStatusHolidayPlanCfg](#) (related URI: /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/capabilities?format=json):
added two door status "sleep" and "invalid" to the sub node **doorStatus** in the node **HolidayPlanCfg**;

- add a sub node **validUnit** (time accuracy) to the node **TimeSegment** in the node **HolidayPlanCfg**.
14. Extended holiday schedule parameter message of the card reader authentication mode **JSON VerifyHolidayPlanCfg** (related URI: [/ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json](#)):
added two authentication modes "sleep" and "invalid" to the sub node **verifyMode** in the node **HolidayPlanCfg**.
15. Extended holiday schedule configuration capability of the card reader authentication mode **JSON Cap VerifyHolidayPlanCfg** (related URI: [/ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities?format=json](#)):
added two authentication modes "sleep" and "invalid" to the sub node **verifyMode** in the node **HolidayPlanCfg**;
added a sub node **validUnit** (time accuracy) to the node **TimeSegment** in the node **HolidayPlanCfg**.
16. Added the URIs to get the list of event and card linkage ID:
Get the capability of the list of event and card linkage ID: GET [/ISAPI/AccessControl/EventCardNoList/capabilities?format=json](#) ;
Get the list of event and card linkage ID: GET [/ISAPI/AccessControl/EventCardNoList?format=json](#) .
17. Added the URI to get the capability of clearing event and card linkage configurations:
GET [/ISAPI/AccessControl/ClearEventCardLinkageCfg/capabilities?format=json](#) .
18. Added the URIs to get the total number of access control events by specific conditions:
Get capability: GET [/ISAPI/AccessControl/AcsEventTotalNum/capabilities?format=json](#) ;
Get the total number: POST [/ISAPI/AccessControl/AcsEventTotalNum?format=json](#) .
19. Extended message of access control event information (**JSON EventNotificationAlert AccessControllerEvent**):
added 11 authentication modes "faceOrFpOrCardOrPw" (face or fingerprint or card or password), "faceAndFp" (face+fingerprint), "faceAndPw" (face+password), "faceAndCard" (face+card), "face" (face), "faceAndFpAndCard" (face+fingerprint+card), "faceAndPwAndFp" (face+password+fingerprint), "employeeNoAndFace" (employee No.+face), "faceOrfaceAndCard" (face or face+card), "fpOrface" (fingerprint or face), and "cardOrfaceOrPw" (card or face or password) to the node **currentVerifyMode** (authentication modes).
20. Added the function of configuring anti-passing back, refer to **Configure Anti-Passing Back** for details.
21. Added functions of configuring cross-controller anti-passing back, refer to **Cross-Controller Anti-Passing Back Configuration** for details.
22. Added the URIs to get access controller working status, customize Wiegand rule, configure log mode, configure SMS function, and configure event optimization, refer to **Configuration and Maintenance** for details.
23. Added the URIs to configure door (floor), reader, access controller, and OSDP card reader, refer to **Device/Server Settings** for details.
24. Added the URIs to configure M1 card encryption authentication, refer to **M1 Card Encryption Authentication** for details.

25. Added the URIs to configure multiple authentication, refer to [***Multi-Factor Authentication***](#) for details.
26. Added the URIs to configure multi-door interlocking, refer to [***Multi-Door Interlocking***](#) for details.
27. Extended access control capability message [***XML_Cap_AccessControl***](#) (related URI: [***/ISAPI/AccessControl/capabilities***](#)):
added 49 nodes from <isSupportRemoteControlDoor> to <isSupportLogModeCfg>.
28. Added a sub status code 0x60001024—"eventNotSupport" (event subscription is not supported) to status code 6 (Invalid Message Content) in [***Response Codes of Text Protocol***](#).

Summary of Changes in Version 2.0_Aug., 2018

New document.

Chapter 2 ISAPI Description

The design of Intelligent Security API (hereafter referred as to ISAPI) adopts RESTful style, so this part introduces the predefined resource operation methods, API (URL) format, interaction message format, time format, namespace, and error processing method.

2.1 Operation Method

The methods to operate resources via ISAPI are same as those of HTTP (Hyper Text Transport Protocol) and RTSP (Real Time Streaming Protocol).



The RTSP operation methods are mainly used to get the real-time stream for live view, two-way audio, and playback in this manual. For details about HTTP and RTSP, please refer to <https://tools.ietf.org/html/rfc2612> and <https://tools.ietf.org/html/rfc2326>.

Table 2-1 HTTP Operation Method

Method	Description
POST	Create resources. This method is only available for adding resource that does not exist before.
GET	Retrieve resources. This method cannot change the system status, only return data as the response to the requester.
PUT	Update resources. This method is usually for update the resource that already exists, but it can also be used to create the resource if the specific resource does not exist.
DELETE	Delete resources.

Table 2-2 RTSP Operation Method

Method	Description
OPTIONS	<p>Get the supported RTSP operation methods. See the request and response message format below when interacting between client software and server.</p> <pre> OPTIONS %s RTSP/1.0\r\n //Request URL CSeq:%u\r\n //Command No. User-Agent:%s\r\n //Client software name \r\n /*Succeeded*/ RTSP/1.0 200 OK\r\n </pre>

Method	Description
	<pre>CSeq: %u\r\n //Command No. Public: %s\r\n //Supported operation methods Date:%s\r\n //Date and time \r\n /*Failed*/ RTSP/1.0 4XX/5XX %s\r\n CSeq: %u\r\n //Command No. Date:%s\r\n //Date and time \r\n</pre>
DESCRIBE	<p>Transfer basic information by SDP (Session Description Protocol, see https://tools.ietf.org/html/rfc2327) files, such as URL with SETUP command and so on. See the request and response message format below when interacting between client software and server.</p> <pre>DESCRIBE %s RTSP/1.0\r\n //URL CSeq:%u\r\n //Command No. Accept: application/sdp\r\n //The SDP description is accepted Authorization:%s\r\n //Authentication information User-Agent:%s\r\n //Client software name \r\n /*Succeeded*/ RTSP/1.0 200 OK\r\n CSeq: %u\r\n //Command No. Content-Type: application/sdp\r\n //The SDP description exists behind the command Content-Base:%s\r\n //URL Content-Length: %d\r\n //The length of contents behind the command \r\n [content] //SDP description /*Failed*/ RTSP/1.0 4XX/5XX %s\r\n CSeq: %u\r\n //Command No. \r\n</pre>
SETUP	<p>Interact the session information, such as transmission mode, port number, and so on. See the request and response message format below when interacting between client software and server.</p> <pre>SETUP %s RTSP/1.0\r\n //URL CSeq:%u\r\n //Command No. Authorization:%s\r\n //Authentication information Session:%s\r\n //Session ID is only returned at the even number of times</pre>

Method	Description
	<pre> Transport: %s\r\n //Transmission protocol User-Agent: %s\r\n //Client software name \r\n /*Succeeded*/ RTSP/1.0 200 OK \r\n CSeq: %u\r\n Session:%s\r\n //Session ID Transport: s% //Transmission method Date: s% //Date and time /*Failed*/ RTSP/1.0 4XX/5XX %s\r\n CSeq: %u\r\n //Command No. \r\n </pre>
PLAY	<p>Start the stream transmission. See the request and response message format below when interacting between client software and server.</p> <pre> PLAY %s RTSP/1.0\r\n //URL CSeq:%u\r\n //Command No. Authorization:%s\r\n //Authentication information Session:%s\r\n //Session ID Range: npt=%f-%f\r\n //Determine the play range User-Agent:%s\r\n //Client software name \r\n /*Succeeded*/ RTSP/1.0 200 OK \r\n CSeq: %u\r\n Session:%s\r\n RTP-Info:%s Date: %s /*Failed*/ RTSP/1.0 4XX/5XX %s\r\n CSeq: %u\r\n //Command No. Session:%s\r\n \r\n </pre>
PAUSE	<p>Pause the stream transmission.</p>
TEARDOWN	<p>Stop the stream transmission. See the request and response message format below when interacting between client software and server.</p> <pre> TEARDOWN %s RTSP/1.0\r\n //URL CSeq: %u\r\n //Command No. Authorization:%s\r\n //Authentication information Session:%s\r\n //Session ID </pre>

Method	Description
	<pre>User-Agent:%s\r\n //Client software name \r\n /*Succeeded*/ RTSP/1.0 200 OK \r\n CSeq: %u\r\n Session:%s\r\n Date:%s\r\n \r\n /*Failed*/ RTSP/1.0 4XX/5XX %s\r\n CSeq: %u\r\n //Command No. Session:%s\r\n \r\n</pre>

2.2 URL Format

URL (Uniform Resource Locator) is a further class of URIs, it can identify a resource and locate the resource by describing its primary access mechanism.

The format of URL is defined as the follows: **<protocol>://<host>[:port][abs_path [?query]]**.

protocol

Protocol types, i.e., HTTP (version 1.1) and RTSP (version 1.0).

host

Host name, IP address, or the FQDN (Fully Qualified Domain Name) of network devices.

port

Port number of host service for listening the connection status of TCP (Transmission Control Protocol, see <https://tools.ietf.org/html/rfc793>) or UDP (User Datagram Protocol, see <https://tools.ietf.org/html/rfc768>). If this field is not configured, the default port number will be adopted. For HTTP, the default port number is 80, and for RTSP, the default port number is 554.

abs_path

Resource URI: /ServiceName/ResourceType/resource. Here, the **ServiceName** is ISAPI; the **ResourceType** is predefined with upper camel case according to different functions , see details in the following table; the resource is defined with lower camel case and can be extended in actual applications. E.g., /ISAPI/System/Network/interfaces.

Predefined URI Model	Description
/ISAPI/System/...	System related resources
/ISAPI/Security/...	Security related resources
/ISAPI/Event...	Event/alarm related resources
/ISAPI/Image/...	Video encoding and image related resources
/ISAPI/ContentMgmt/...	Storage management related resources

query

Strings for describing resources information, including related parameters. The parameter names and values must be listed as the following format in this field: ?p1=v1&p2=v2&...&pn=vn.



Note

- To locate the connected device, when operating lower-level device via the URL, the **query** field should be filled as ?devIndex=uuid&p1=v1&p2=v2&...&pn=vn. The uuid (or guid) is a 32-byte (128 bits) random number, which is unique and generated by operating system when adding device, and its format is "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx".
- For message in JSON format, the **query** field should be filled as ?format=json&p1=v1&p2=v2&...&pn=vn. For details about message format, refer to the next section below. E.g., http://10.17.132.22/ISAPI/System/time?format=json&devIndex=550e8400e29b41d4a716446655440000.

2.3 Message Format

During the ISAPI integration, the request and response messages generated among the interaction between devices and platform are data in XML format or JSON format.



The message format here is only available for URLs based on HTTP.

XML Format

- For the previous integration, XML is a common format which may only cause a little changes in the later integration.
- Generally, for configuration information, the **Content-Type** in the XML format message is "application/xml; charset='UTF-8'", see details below.

```
//Request Message  
GET /ISAPI/System/status HTTP/1.1  
...
```

```
//Response Message
HTTP/1.1 200 OK
...
Content-Type: application/xml; charset="UTF-8"
...
<?xml version="1.0" encoding="UTF-8"?>
<DeviceStatus version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
...
</DeviceStatus>
```

For data (e.g., firmware, configuration files), the **Content-Type** in the XML format message is "application/octet-stream", see details below.

```
//Request Message
PUT /ISAPI/System/configurationData HTTP/1.1
...
Content-Type: application/octet-stream
...
[proprietary configuration file data content]

//Response Message
HTTP/1.1 200 OK
...

Content-Type: application/xml; charset="UTF-8"
...
<?xml version="1.0" encoding="UTF-8"?>
<ResponseStatus version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
...
</ResponseStatus>
```

JSON Format Message

- The leaf node (without any sub node) in the message is named by lower camel case, while the non-leaf node in the message is named by upper camel case.
- To communicate by the messages in JSON format, the devices must support the public specifications in <http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf> and HTTP with version 1.1.



JSON is a lightweight data format which is a subset of JavaScript language and is small, fast, and easy to be parsed.

- Generally, for configuration information, the **Content-Type** of message is "application/json", see the example below:

```
//Request message
GET /ISAPI/System/status HTTP/1.1
...
//Response message
HTTP/1.1 200 OK
```

```
...
Content-Type: application/json
...
"DeviceStatus":""
```

For data (e.g., firmware, configuration files), the **Content-Type** of message is "application/octet-stream", see the example below:

```
//Request message
PUT /ISAPI/System/configurationData HTTP/1.1
...
Content-Type: application/octet-stream
...
[proprietary configuration file data content]

//Response message
HTTP/1.1 200 OK
...
Content-Type: application/json
...
"ResponseStatus":""
```

2.4 Others

Time Format

The time format during ISAPI integration adopts ISO8601 standard (see details in <http://www.w3.org/TR/NOTE-datetime-970915>), that is, YYY-MM-DDThh:mm:ss.sTZD (e.g., 2017-08-16T20:17:06+08:00).

Namespace

For message in XML format, namespace is required. The following namespaces are available:

- xmlns=http://www.isapi.org/ver20/XMLSchema
- xmlns:xs="http://www.w3.org/2001/XMLSchema"
- xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
- xmlns:xlink="http://www.w3.org/1999/xlink"

Error Processing

During the integration applications of ISAPI protocol, when the error of URL based on HTTP occurred, the ResponseStatus message (in XML or JSON format) which contains error code will be returned. If the error of URL based on RTSP occurs, the corresponding status code will directly be returned, for details, refer to <https://tools.ietf.org/html/rfc2326> .

Chapter 3 Security

This part mainly introduces the authentication, user permission, and encryption in the integration applications of ISAPI.

3.1 Authentication

When communicating via ISAPI protocol, the digest of the session must be authenticated.



Note

- The authentication must based on *HTTP Authentication: Basic and Digest Access Authentication*, see <https://tools.ietf.org/html/rfc2617> for details.
- The request session must contain authentication information, otherwise, device will return 401 error code.

The message digest, which contains user name, password, specific nonce value, HTTP or RTSP operation methods, and request URL, is generated by the MD5 algorithm, see the calculation rules below.

qop=Undefined

Digest=MD5(MD5(A1):<nonce>:MD5(A2))

qop="auth:"

Digest=MD5(MD5(A1):<nonce>:<nc>:<cnonce>:<qop>:MD5(A2))

qop="auth-int:"

Digest=MD5(MD5(A1):<nonce>:<nc>:<cnonce>:<qop>:MD5(A2))



Note

- The **qop** is a value for determining whether the authentication is required.
- A1 and A2 are two data blocks required for digest calculation.
A1: Data block about security, which contains user name, password, security domain, random number, and so on. If the digest calculation algorithm is MD5, A1=<user>:<realm>:<password>; if the algorithm is MD5-sess, A1=MD5(<user>:<realm>:<password>):<nonce>:<cnonce>.
A2: Data block about message, such as URL, repeated requests, message body, and so on, it helps to prevent repeated, and realize the resource/message tamper-proof. If the **qop** is not defined or it is "auth:", A2=<request-method>:<uri-directive-value>; if the **qop** is "auth-int:", A2=<request-method>:<uri-directive-value>:MD5(<request-entity-body>).
- The **nonce** is the random number generated by service, the following generation formula is suggested: nonce = BASE64(time-stamp MD5(time-stamp ":" ETag ":" private-key)). The **time-stamp** in the formula is the time stamp generated by service or the unique serial No.; the **ETag** is

the value of HTTP ETag header in the request message; the **private-key** is the data that only known by service.

If authentication failed, the device will return the **XMLResponseStatus.AuthenticationFailed** message, and the remaining authentication attempts will also be returned. If the remaining attempts is 0, the user will be locked at the next authentication attempt.

Chapter 4 Typical Applications

4.1 Data Collection

4.1.1 Online Collect Data

When the access control device is connected to the client software or platform via the network, you can collect data (including ID card information, card information, face data, and fingerprint) on the client software or platform remotely. The online collected data will be uploaded to the client software or platform in real time.

Steps

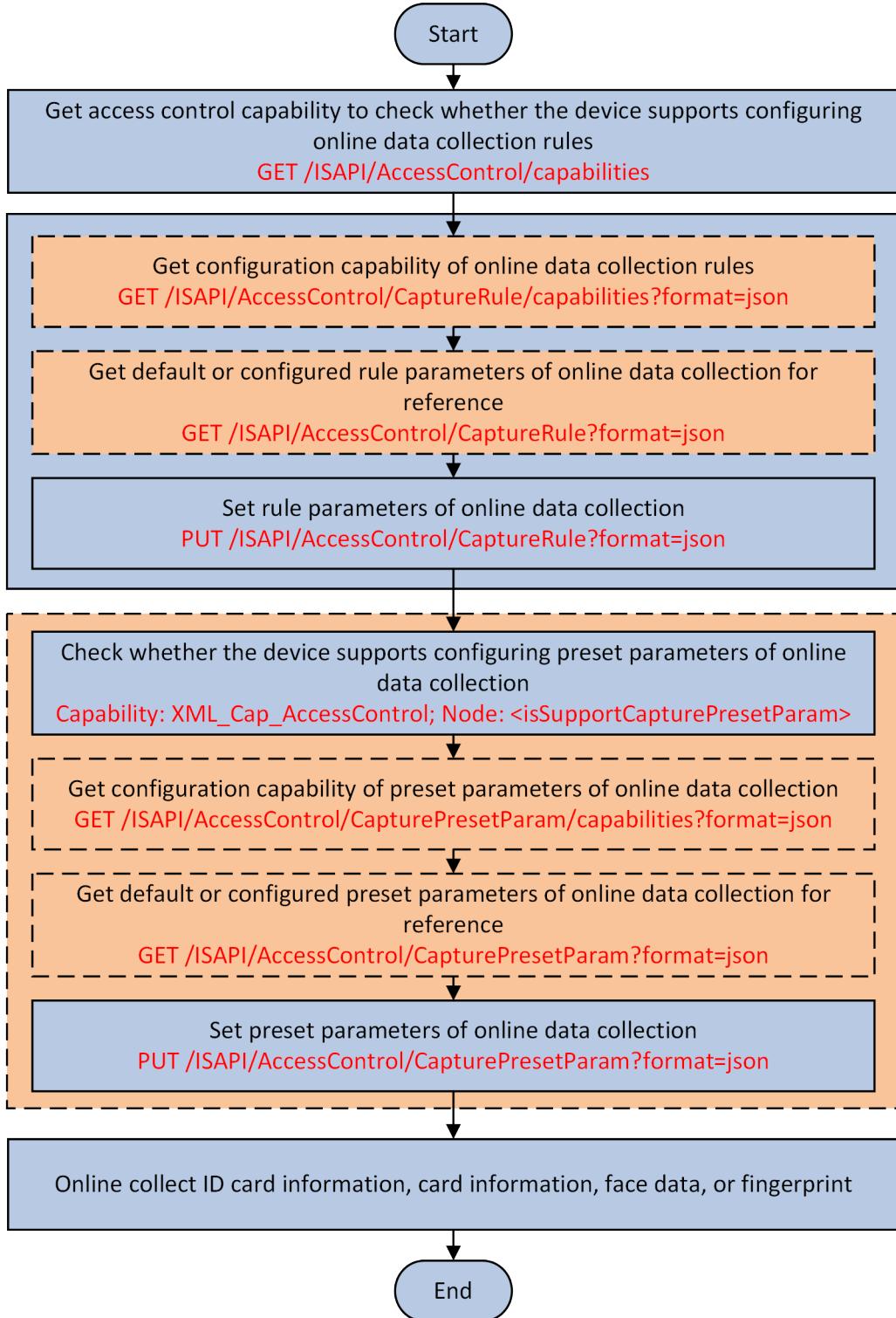


Figure 4-1 API Calling Flow of Online Collecting Data

1. Call [**/ISAPI/AccessControl/capabilities**](#) by GET method to get the access control capability and check whether the device supports configuring online data collection rules.

The access control capability is returned in the message [**XML_Cap_AccessControl**](#).

If the device supports configuring online data collection rules, the node `<isSupportCaptureRule>` will be returned in the capability message and its value is true, and then you can perform the following steps.

Otherwise, rule configuration of online data collection is not supported, please end this task.

2. Configure online data collection rules.

- 1) **Optional:** Call [**/ISAPI/AccessControl/CaptureRule/capabilities?format=json**](#) by GET method to get the configuration capability of online data collection rules.

The capability is returned in the message [**JSON_CaptureRuleCap**](#).

- 2) **Optional:** Call [**/ISAPI/AccessControl/CaptureRule?format=json**](#) by GET method to get default or configured rule parameters of online data collection for reference.

The rule parameters are returned in the message [**JSON_CaptureRule**](#).

- 3) Call [**/ISAPI/AccessControl/CaptureRule?format=json**](#) by PUT method to set rule parameters of online data collection.

3. **Optional:** Configure preset parameters of online data collection.

- 1) Check the access control capability [**XML_Cap_AccessControl**](#) to know whether the device supports configuring preset parameters of online data collection.

If the device supports configuring preset parameters of online data collection, the node `<isSupportCapturePresetParam>` will be returned in the capability message and its value is true, and then you can continue to set preset parameters.

Otherwise, preset configuration of online data collection is not supported.

- 2) **Optional:** Call [**/ISAPI/AccessControl/CapturePresetParam/capabilities?format=json**](#) by GET method to get the configuration capability of preset parameters of online data collection.

The configuration capability is returned in the message [**JSON_CapturePresetCap**](#).

- 3) **Optional:** Call [**/ISAPI/AccessControl/CapturePresetParam?format=json**](#) by GET method to get default or configured preset parameters of online data collection for reference.

The preset parameters are returned in the message [**JSON_CapturePreset**](#).

- 4) Call [**/ISAPI/AccessControl/CapturePresetParam?format=json**](#) by PUT method to set preset parameters of online data collection.



Note

The preset parameters are used to display custom information on the device UI during data collection. Currently, it only supports displaying the name of the person whose data is being collected. The preset parameters should be configured again for each collection.

4. Perform the following operation(s) to collect ID card information, card information, face data, or fingerprint online.

Collect ID Card Information

- a. Call [**/ISAPI/AccessControl/capabilities**](#) by GET method to get the access control capability and check whether the device supports online collecting ID card information.

The capability is returned in the message [XML_Cap_AccessControl](#). If it is supported, the node <isSupportCaptureIDInfo> is returned and its value is true. Otherwise, online ID card collection is not supported.

- b. Optional: Call [/ISAPI/AccessControl/CaptureIDInfo/capabilities?format=json](#) by GET method to get the capability of online collecting ID card information.
The capability is returned in the message [JSON_IdentityInfoCap](#).
- c. Call [/ISAPI/AccessControl/CaptureIDInfo?format=json](#) by POST method to online collect ID card information.
The online collected ID card information is returned in the message [JSON_IdentityInfo](#).

Collect Card Information Refer to [Collect Card Information](#)

Collect Face Data Refer to [Collect Face Data](#)

Collect Fingerprint Refer to [Fingerprint Collection](#)

4.1.2 Offline Collect Data

When the access control device is not connected to the client software or platform via the network, you can collect data (including ID card information, card information, face data, and fingerprint) locally on the stand-alone device by importing description of the information that needs to be collected. The offline collected data will be stored on the device and can also be downloaded, exported, or deleted from the device.

Steps

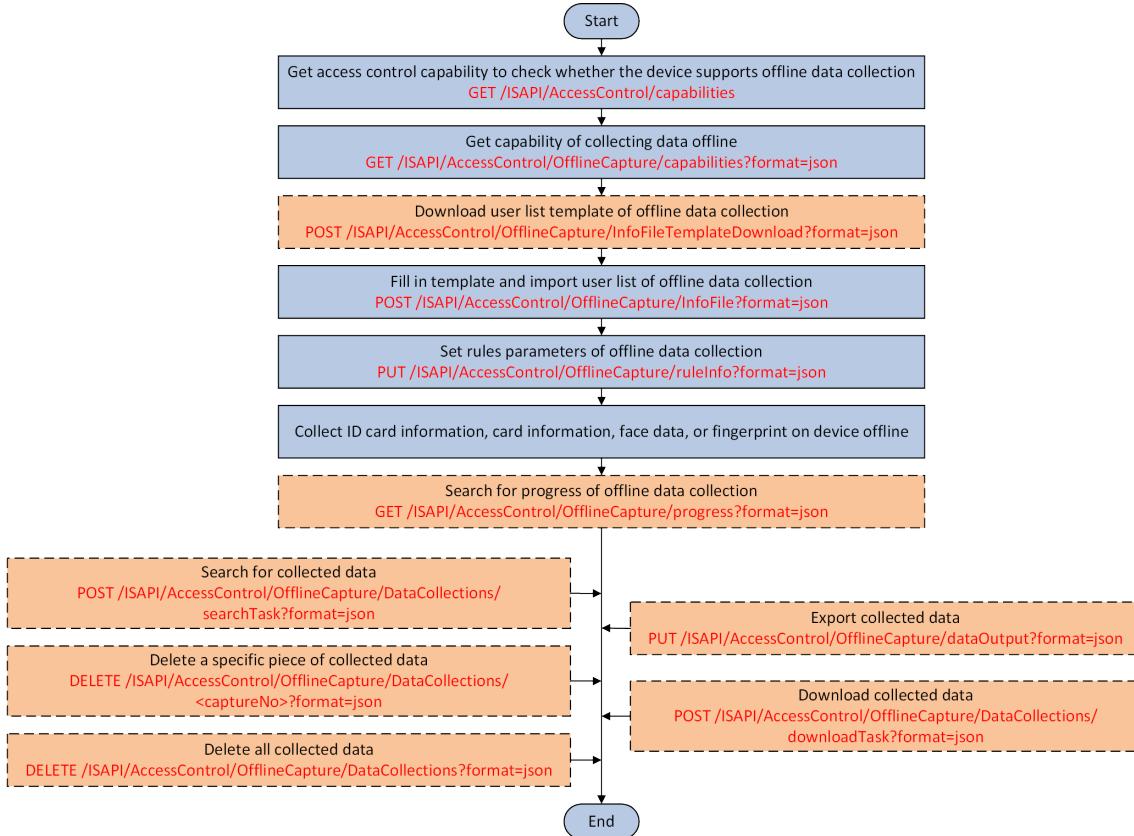


Figure 4-2 API Calling Flow of Offline Collecting Data

1. Call **/ISAPI/AccessControl/capabilities** by GET method to get the access control capability and check whether the device supports offline data collection.

The capability is returned in the message **XML_Cap_AccessControl**.

If the node <isSupportOfflineCapture> is returned in the message and its value is true, it indicates that the device supports offline data collection, and then you can continue to perform the following operations. Otherwise, please end this task.

2. Call **/ISAPI/AccessControl/OfflineCapture/capabilities?format=json** by GET method to get the capability of collecting data offline for knowing the supported parameters.

The capability is returned in the message **JSON_OfflineCaptureCap**.

3. **Optional:** Call **/ISAPI/AccessControl/OfflineCapture/InfoFileTemplateDownload?format=json** by POST method to download the user list template of offline data collection.

4. Call **/ISAPI/AccessControl/OfflineCapture/InfoFile?format=json** by POST method to import the user list of offline data collection filled in the template.



Note

- You can call [`/ISAPI/AccessControl/OfflineCapture/InfoFile/progress?format=json`](#) by GET method to get the progress of uploading the user list of offline data collection.
- If uploading failed, you can call [`/ISAPI/AccessControl/OfflineCapture/uploadFailedDetails?format=json`](#) by GET method to get the details of failing to upload the user list of offline data collection.

5. Call [`/ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json`](#) by PUT method to set rule parameters of offline data collection.



Note

Before setting rule parameters of offline data collection, you'd better call [`/ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json`](#) by GET method to get the existing or configured parameters for reference. The parameters are returned in the message [`JSON_RuleInfo`](#).

6. Collect ID card information, card information, face data, or fingerprint on the stand-alone device offline.

7. **Optional:** Call [`/ISAPI/AccessControl/OfflineCapture/progress?format=json`](#) by GET method to get the progress of offline data collection.

The collection progress is returned in the message [`JSON_CaptureProgress`](#).

8. **Optional:** Perform the following operation(s) after collecting data offline.

Export Collected Data

PUT [`/ISAPI/AccessControl/OfflineCapture/dataOutput?format=json`](#)



Note

During exporting, you can call [`/ISAPI/AccessControl/OfflineCapture/dataOutput/progress?format=json`](#) by GET method to get the progress of exporting the offline collected data.

Download Collected Data

POST [`/ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?format=json`](#)

Search for Collected Data

POST [`/ISAPI/AccessControl/OfflineCapture/DataCollections/searchTask?format=json`](#)

Delete A Specific Piece of Collected Data

DELETE [`/ISAPI/AccessControl/OfflineCapture/DataCollections/<captureNo>?format=json`](#)

Delete All Collected Data

DELETE [`/ISAPI/AccessControl/OfflineCapture/DataCollections?format=json`](#)

4.2 Manage Person Information

A person is a basic unit, which can link with multiple cards and fingerprints, for access control in this manual. So, before starting any other operations, you should add persons and apply the person information (e.g., person ID, name, organization, permissions, and so on) to access control devices.

Steps

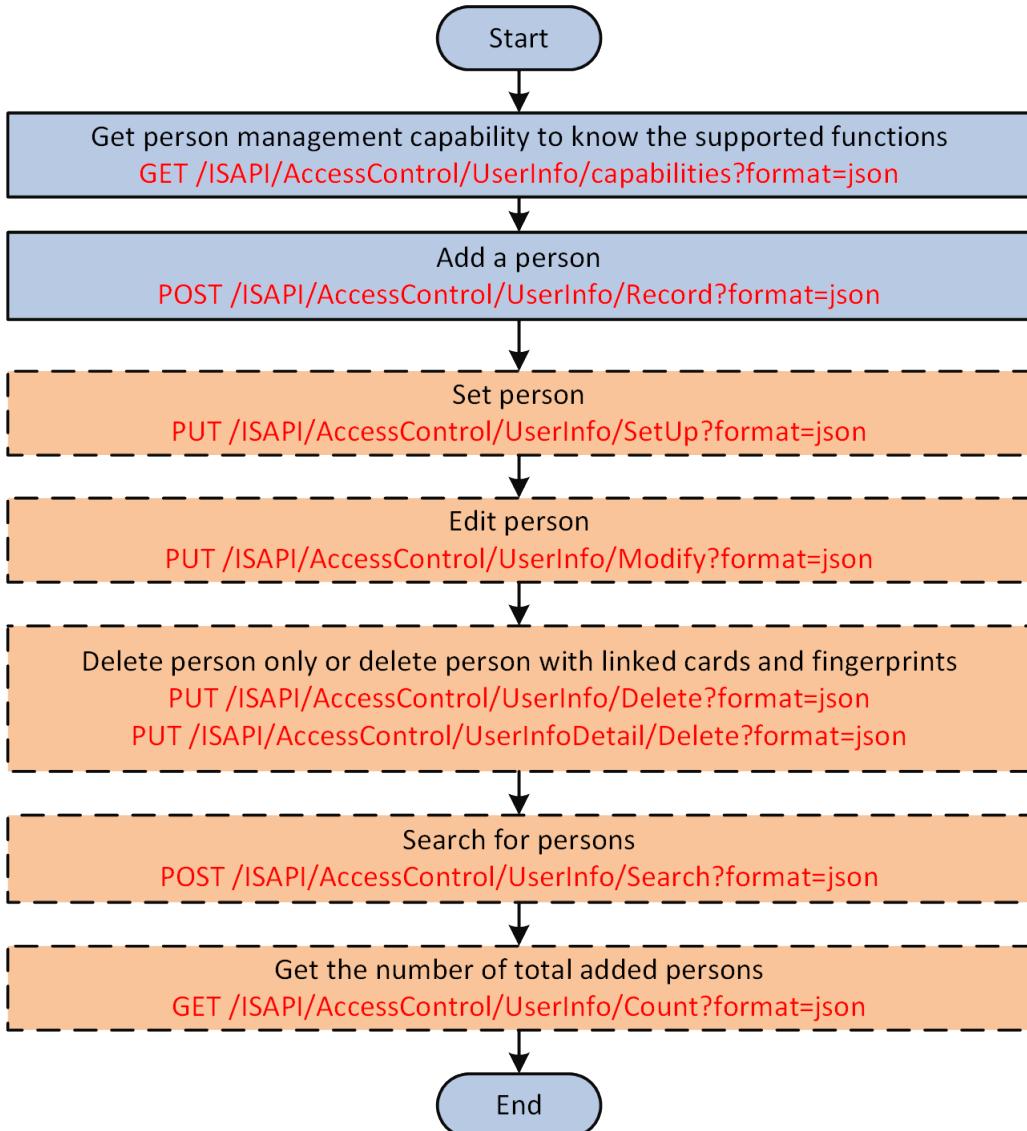


Figure 4-3 Programming Flow of Managing Person Information

1. Call `/ISAPI/AccessControl/UserInfo/capabilities?format=json` by GET method to get the person management capability to know the supported functions.

The field **supportFunction** with different values (i.e., "post"-support adding person, "delete"-support deleting person, "put"-support editing person information, "get"-support searching for persons) is returned in the **JSON_Cap_UserInfo** message.

2. Call [**/ISAPI/AccessControl/UserInfo/Record?format=json**](#) by POST method to add a person.

The person information, assigned access permission, and configured authentication mode are all added and applied to the access control device.

3. **Optional:** Perform the following operation(s) by the corresponding URIs after adding persons.

Set Person Information

PUT [**/ISAPI/AccessControl/UserInfo/SetUp?format=json**](#)

Edit Person Information

PUT [**/ISAPI/AccessControl/UserInfo/Modify?format=json**](#)

Delete Person Only

PUT [**/ISAPI/AccessControl/UserInfo/Delete?format=json**](#)



Note

The timeout of deleting person only can be configured, and setting the timeout to 60s is suggested.

Delete Person with Linked Cards, Fingerprints, and Permissions

PUT [**/ISAPI/AccessControl/UserInfoDetail/Delete?format=json**](#)



Note

- Before deleting person with linked cards, fingerprints, and permissions, you should call [**/ISAPI/AccessControl/UserInfoDetail/Delete/capabilities?format=json**](#) by GET method to get the deleting capability to know the supported deleting modes (delete all or delete by person) and other configuration details.
- You can call [**/ISAPI/AccessControl/UserInfoDetail/DeleteProcess?format=json**](#) by GET method to get the deleting status.
- For linking cards and fingerprint to the person, refer to [**Manage Card Information**](#) and [**Manage Fingerprint Information**](#).

Search for Persons

POST [**/ISAPI/AccessControl/UserInfo/Search?format=json**](#)

Get Number of Total Added Persons

GET [**/ISAPI/AccessControl/UserInfo/Count?format=json**](#)

4.3 Manage Card Information

If a person want to access by card, you should add cards and link the cards with the person for getting the access permissions, and then apply card information (e.g., card No., card type, and so on) to access control device.

Before You Start

Make sure you have collected the card information, refer to [***Collect Card Information***](#) for details.

Steps

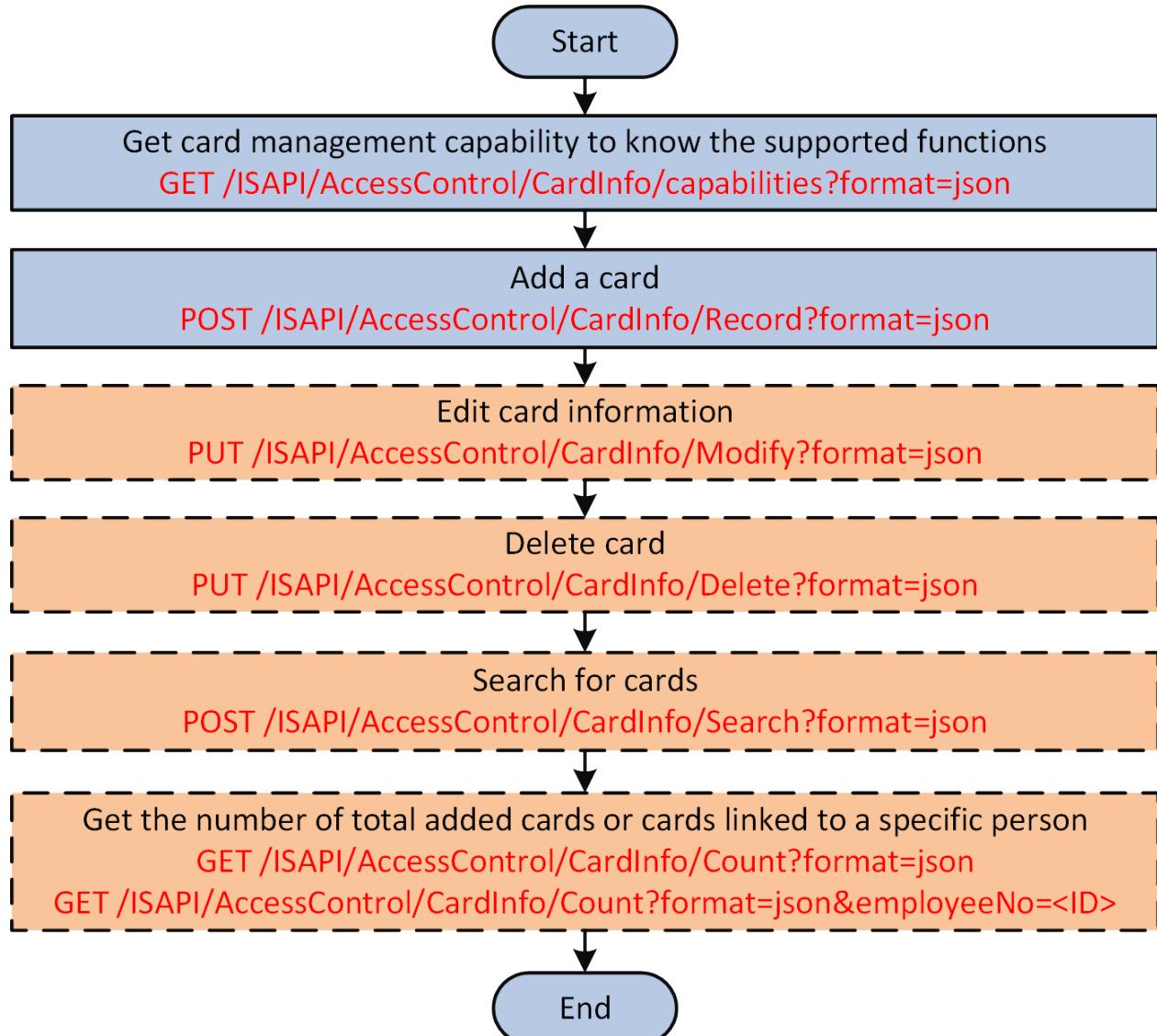


Figure 4-4 Programming Flow of Managing Card Information

1. Call [***/ISAPI/AccessControl/CardInfo/capabilities?format=json***](#) by GET method to get the card management capability for knowing the supported functions.

The field **supportFunction** with different values (i.e., "post"-support adding card, "delete"-support deleting card, "put"-support editing card information, "get"-support searching for cards) is returned in the [***JSON_Cap_CardInfo***](#) message.

2. Call [***/ISAPI/AccessControl/CardInfo/Record?format=json***](#) by POST method to add a card.

The card information (such as card No., card type, and so on) is added to the access control device and linked to the person according to the employee No.

3. **Optional:** Perform the following operation(s) by the corresponding URIs after adding cards.

Set Card Information	PUT <u>/ISAPI/AccessControl/CardInfo/SetUp?format=json</u>
Edit Card Information	PUT <u>/ISAPI/AccessControl/CardInfo/Modify?format=json</u>
Delete Card	PUT <u>/ISAPI/AccessControl/CardInfo/Delete?format=json</u>



Note

The timeout of deleting card can be configured, and setting the timeout to 60s is suggested.

Search for Cards	POST <u>/ISAPI/AccessControl/CardInfo/Search?format=json</u>
Get Number of Total Added Cards	GET <u>/ISAPI/AccessControl/CardInfo/Count?format=json</u>
Get Number of Cards Linked to A Specific Person	GET <u>/ISAPI/AccessControl/CardInfo/Count?format=json&employeeNo=<ID></u>

4.3.1 Collect Card Information

The card information for further management and applying should be collected by the card reading module of the access control device first. The following contents are about the process and parameter settings of collecting card information.

Steps

1. Call [/ISAPI/AccessControl/capabilities](#) by GET method to get the functional capability of access control and check whether the device supports collecting card information.
The capability will be returned in the message [XML_Cap_AccessControl](#).
If the device supports collecting card information, the node <isSupportCaptureCardInfo> is returned and its value is "true", and then you can perform the following steps. Otherwise, it indicates that collecting card information is not supported by the device, please end this task.
2. **Optional:** Call [/ISAPI/AccessControl/CaptureCardInfo/capabilities?format=json](#) by GET method to get the capability of collecting card information.
3. Call [/ISAPI/AccessControl/CaptureCardInfo?format=json](#) by GET method to collect the card information.

4.3.2 Card Operation

Function	Request URI
Get Card Operation Capability	GET <u>/ISAPI/AccessControl/ CardOperations/capabilities? format=json</u>
Encrypt Specific Sections (M1 Card)	PUT <u>/ISAPI/AccessControl/ CardOperations/ sectionEncryption? format=json</u>
Verify Section Password (M1 Card)	PUT <u>/ISAPI/AccessControl/ CardOperations/verification? format=json</u>
Change Control Block of Section (M1 Card)	PUT <u>/ISAPI/AccessControl/ CardOperations/controlBlock? format=json</u>
Read or Write Block Data (M1 Card)	Read Block Data GET <u>/ISAPI/AccessControl/ CardOperations/dataBlock/ <address>?format=json</u>
	Write Block Data PUT <u>/ISAPI/AccessControl/ CardOperations/dataBlock/ <address>?format=json</u>
Operate Data Block (M1 Card)	PUT <u>/ISAPI/AccessControl/ CardOperations/dataBlock/ control?format=json</u>
Set Operation Protocol Type of Card	PUT <u>/ISAPI/AccessControl/ CardOperations/protocol? format=json</u>
Set CPU Card Parameters	PUT <u>/ISAPI/AccessControl/ CardOperations/cardParam? format=json</u>
Reset CPU Card	GET <u>/ISAPI/AccessControl/ CardOperations/reset? format=json</u>
Pass Through Data Package of CPU Card	PUT <u>/ISAPI/AccessControl/ CardOperations/dataTrans? format=json</u>

Function	Request URI
Encrypt CPU Card	PUT <u>/ISAPI/AccessControl/CardOperations/encryption?format=json</u>
Send a Request for Card Issuing	PUT <u>/ISAPI/AccessControl/CardOperations/localIssueRequest?format=json</u>
Get Current Card Issuing Status and Real-time Card Issuing Results	GET <u>/ISAPI/AccessControl/CardOperations/localIssueRes?format=json</u>
Get or Set Rule Parameters for Issuing Smart Cards	GET or PUT <u>/ISAPI/AccessControl/CardOperations/localIssueCfg?format=json</u>
Delete Data from Card	PUT <u>/ISAPI/AccessControl/CardOperations/clearData?format=json</u>
Set Custom Card Information	PUT <u>/ISAPI/AccessControl/CardOperations/customData?format=json</u>
Search for Custom Card Information	POST <u>/ISAPI/AccessControl/CardOperations/customData/searchTask?format=json</u>
Get Smart Card Issuing Status	GET <u>/ISAPI/AccessControl/CardOperations/cardIssueStatus?format=json</u>

4.4 Manage Fingerprint Information

If a person wants to access by fingerprint, you should collect the fingerprint data via the fingerprint recorder first, and then apply the fingerprint data and information (e.g., fingerprint ID, type, and so on) to the fingerprint module of access control device and link the fingerprints with the person for getting the access permissions.

Before You Start

Make sure you have collected the fingerprint data, refer to [Fingerprint Collection](#) for details.

Steps

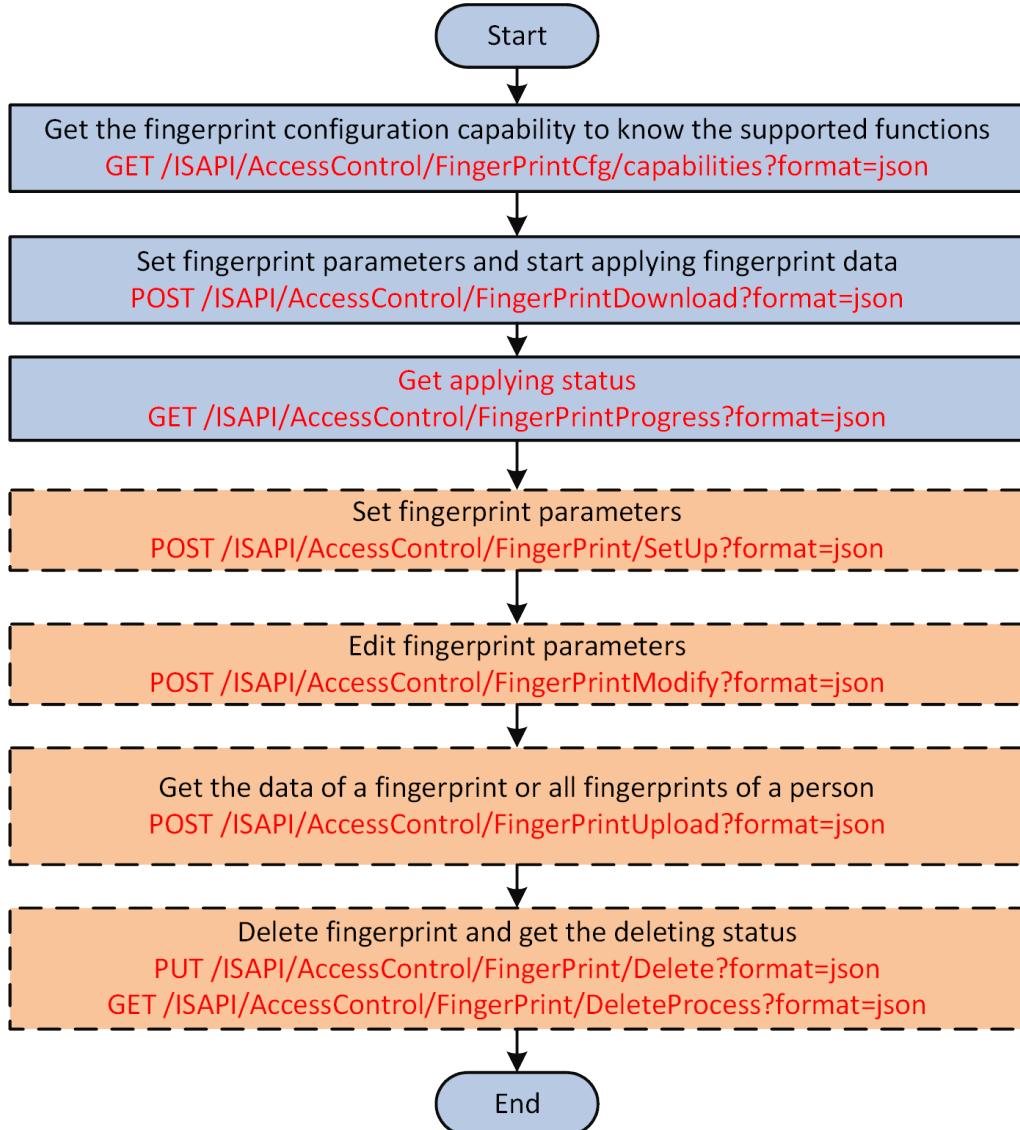


Figure 4-5 Programming Flow of Managing Fingerprint Information



To collect the fingerprint, refer to [Fingerprint Collection](#) for details.

1. Call [`/ISAPI/AccessControl/FingerPrintCfg/capabilities?format=json`](#) by GET method to get the fingerprint configuration capability for knowing the required configuration details.
2. Call [`/ISAPI/AccessControl/FingerPrintDownload?format=json`](#) by POST method to set the fingerprint parameters (e.g., an employee No. to be linked, fingerprint modules to be applied, and so on) and start applying the recorded fingerprint data.



The binary fingerprint data is collected and recorded by the fingerprint recorder.

3. Call [/ISAPI/AccessControl/FingerPrintProgress?format=json](#) by GET method to get the applying status and make sure the applying is completed.
-



The fingerprint data is linked to a person according to the configured employee No. and applied to the specified fingerprint modules only when the value of applying status (**totalStatus**) is 1.

4. **Optional:** Perform the following operation(s) after applying the recorded fingerprint data.

Set Fingerprint Parameters

POST [/ISAPI/AccessControl/FingerPrint/SetUp?format=json](#)

Edit Fingerprint Parameters

POST [/ISAPI/AccessControl/FingerPrintModify?format=json](#)

Get Fingerprint Data

POST [/ISAPI/AccessControl/FingerPrintUpload?format=json](#)

Get Data of All Fingerprints of A Person

POST [/ISAPI/AccessControl/FingerPrintUploadAll?format=json](#)

Get Total Number of Fingerprints of A Specific Person

GET [/ISAPI/AccessControl/FingerPrint/Count?format=json&employeeNo=](#)

Delete Fingerprint Data

PUT [/ISAPI/AccessControl/FingerPrint/Delete?format=json](#)



- Before deleting fingerprint data, you should call [/ISAPI/AccessControl/FingerPrint/Delete/capabilities?format=json](#) by GET method to get the deleting capability for knowing the supported deleting modes (delete by person or by fingerprint module) and other configuration details.
- This URI is only used to start deleting the fingerprint data. So, to judge whether the deleting is completed, you must repeatedly call [/ISAPI/AccessControl/FingerPrint/DeleteProcess?format=json](#) by GET method to get the fingerprint deleting status.

4.4.1 Fingerprint Collection

The fingerprint information for further management and applying should be collected by fingerprint recorder first. The following contents are about the process and parameter settings of fingerprint collection.

- a. Call [**/ISAPI/AccessControl/CaptureFingerPrint/capabilities**](#) by GET method to get the fingerprint collection capability.
- b. Call [**/ISAPI/AccessControl/CaptureFingerPrint**](#) by POST method to collect the fingerprint information.

4.5 Manage Face Information

If a person wants to access by face, you should collect face data via the face capture module of the access control device first, create face picture libraries, and then apply face records (including face record ID, information about the person in the picture, and so on) to face picture libraries for getting the access permission.

4.5.1 Create Face Picture Library

The face picture library refers to the library of face pictures, including captured picture library, resident population library, blocklist library, etc. You can create, edit, delete, and search for the face picture libraries.

Steps

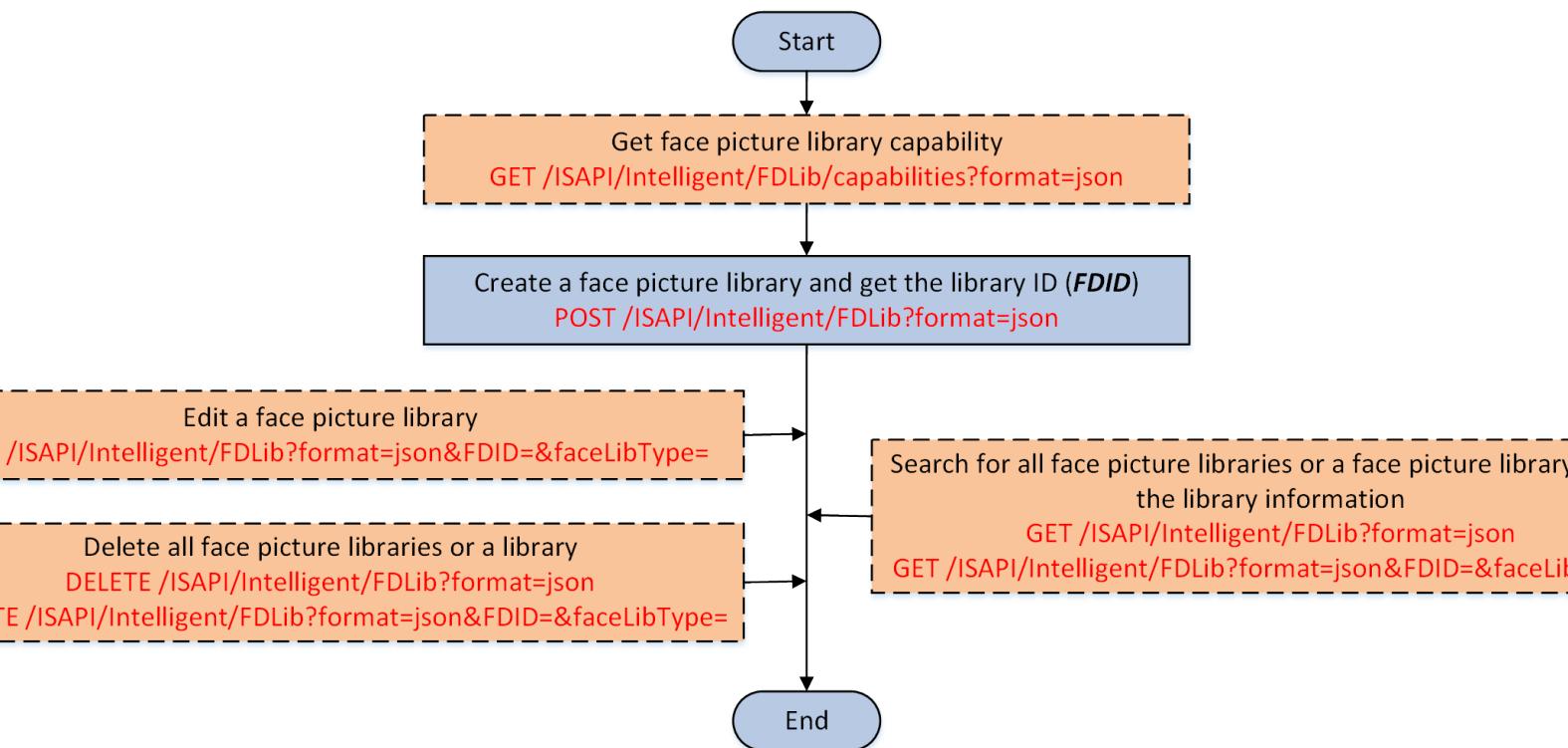


Figure 4-6 Programming Flow of Creating Face Picture Library

1. **Optional:** Call [**/ISAPI/Intelligent/FDLib/capabilities?format=json**](#) by GET method to get the face picture library capability and check the supported operations of face picture libraries.

The face picture library capability is returned in the message **JSON_FPLibCap**. If the value of the node <**supportFDFunction**> is "post, delete, put, get", it indicates that creating, editing, deleting, and searching for face picture libraries are supported, and you can perform the following steps to implement these functions.

2. Call **/ISAPI/Intelligent/FDLib?format=json** by POST method to create a face picture library.



Note

There are three types of face picture library, including infrared face picture library, list library, and static library. So if you want to specify a face picture library, you should provide the library type and library ID together.

The ID of the created face picture library (**FDID**) is returned.

3. **Optional:** Perform the following operation(s) after creating a face picture library.

Edit A Face Picture Library

PUT **/ISAPI/Intelligent/FDLib?**
format=json&FDID=&faceLibType=

Delete A Face Picture Library

DELETE **/ISAPI/Intelligent/FDLib?**
format=json&FDID=&faceLibType=

Delete All Face Picture Libraries

DELETE **/ISAPI/Intelligent/FDLib?format=json**

Search for A Specific Face Picture Library

GET **/ISAPI/Intelligent/FDLib?**
format=json&FDID=&faceLibType=

Search for All Face Picture Libraries

GET **/ISAPI/Intelligent/FDLib?format=json**



Note

In the URI, both the library ID (**FDID**) and the library type (**faceLibType**) are required to specify a face picture library, e.g., **/ISAPI/Intelligent/FDLib?**

format=json&FDID=1223344455566788&faceLibType=blackFD.

4.5.2 Collect Face Data

The face data for further management and applying should be collected by the face capture module of the access control device first. The following contents are about the process and parameter settings of face data collection.

Steps

1. **Optional:** Call **/ISAPI/AccessControl/CaptureFaceData/capabilities** by GET method to get the capability of collecting face data.
2. Call **/ISAPI/AccessControl/CaptureFaceData** by POST method to start collecting face data.
3. Call **/ISAPI/AccessControl/CaptureFaceData/Progress** by GET method to get the progress of collecting face data.

4.5.3 Manage Face Records in Face Picture Library

After creating face picture library, you can import face pictures with different types (i.e., picture URL and binary picture) to add the face records to the library. And you can also edit, delete, and search for the face records in the library for management.

Before You Start

- Make sure you have added face picture libraries and get the ID of each library. For creating face picture library, refer to [**Create Face Picture Library**](#) for details.
- Make sure you have collected the face picture data, refer to [**Collect Face Data**](#) for details.

Steps

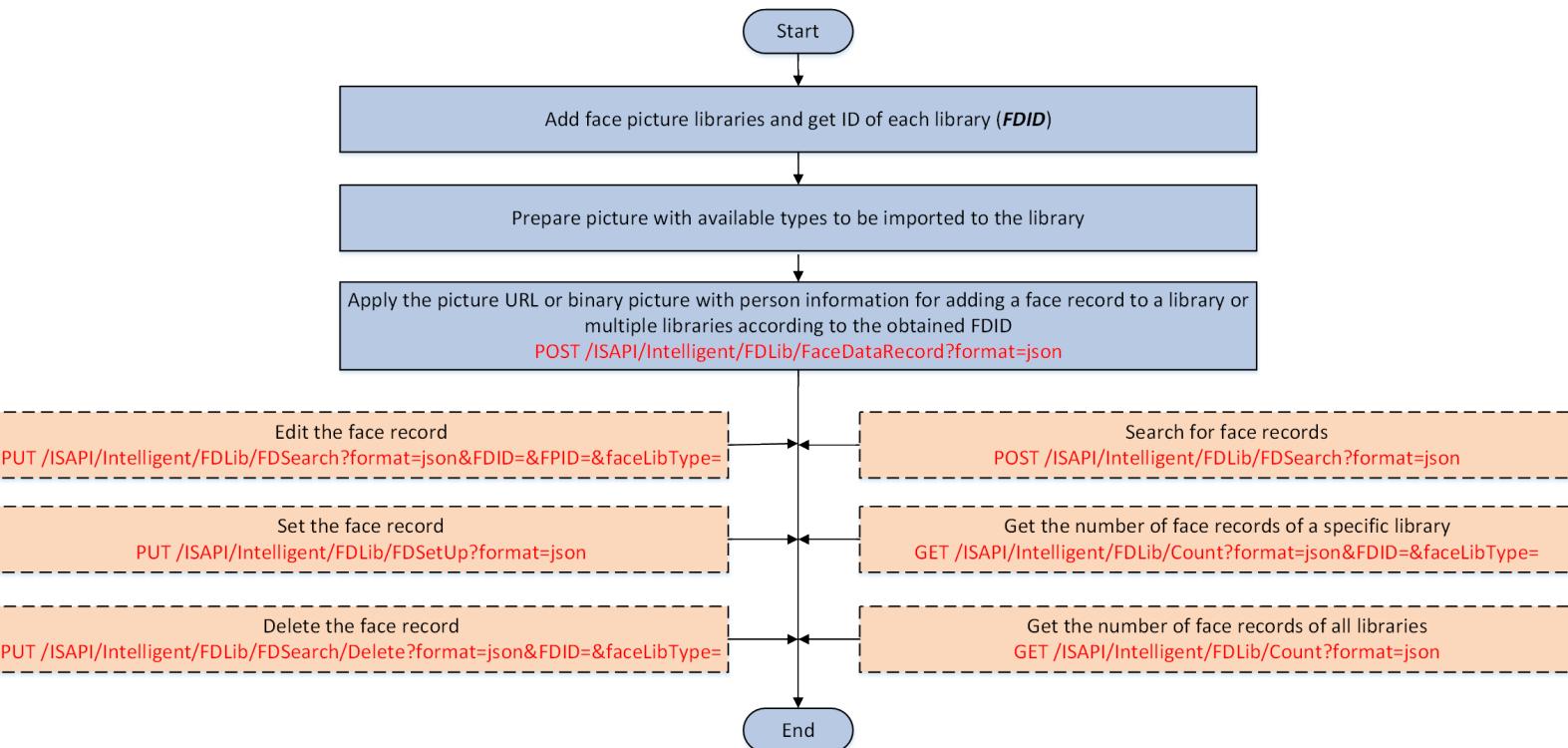


Figure 4-7 Programming Flow of Managing Face Records in Face Picture Library

1. Prepare picture URLs (picture storage location) or binary pictures in form format for being imported to the library.
 2. Call [**/ISAPI/Intelligent/FDLib/FaceDataRecord?format=json**](#) by POST method to apply the picture URL or binary picture with person information for adding a face record to the library according to the face picture library ID (**FDID**).
- The face record ID (**FPIID**) is returned in the message [**JSON AddFaceRecordResult**](#).
3. **Optional:** Perform the following operation(s) after adding face records to the face picture library.

Edit Face Record

`PUT /ISAPI/Intelligent/FDLib/FSearc?
format=json&FDID=&FPIID=&faceLibType=`

Edit Face Records in a Batch PUT [/ISAPI/Intelligent/FDLib/FDModify?format=json](#)

Set Face Record PUT [/ISAPI/Intelligent/FDLib/FDSetUp?format=json](#)

Delete Face Record(s) PUT [/ISAPI/Intelligent/FDLib/FDSearch/Delete?format=json&FDID=&faceLibType=](#)



Note

Deleting a face record or deleting face records in a batch are both supported.

Search for Face Records POST [/ISAPI/Intelligent/FDLib/FDSearch?format=json](#)



Note

Searching multiple face picture libraries at a time and fuzzy search are both supported.

Get Number of Face Records of a Face Picture Library GET [/ISAPI/Intelligent/FDLib/Count?format=json&FDID=&faceLibType=](#)

Get Number of Face Records of All Face Picture Libraries GET [/ISAPI/Intelligent/FDLib/Count?format=json](#)



In the request URI, both the library ID (**FDID**) and library type (**faceLibType**) are required to specify a face picture library, e.g., [/ISAPI/Intelligent/FDLib?format=json&FDID=1223344455566788&faceLibType=blackFD](#).

4.5.4 Configure Facial Recognition Mode

When recognizing human faces via the access control device, both the normal mode and the deep mode are available. For the normal mode, the human face is recognized via white light camera; for the deep mode, the human face is recognized by the IR light camera, which is applicable to a more complicated environment and can recognize a much wider people range than the normal mode.

Steps

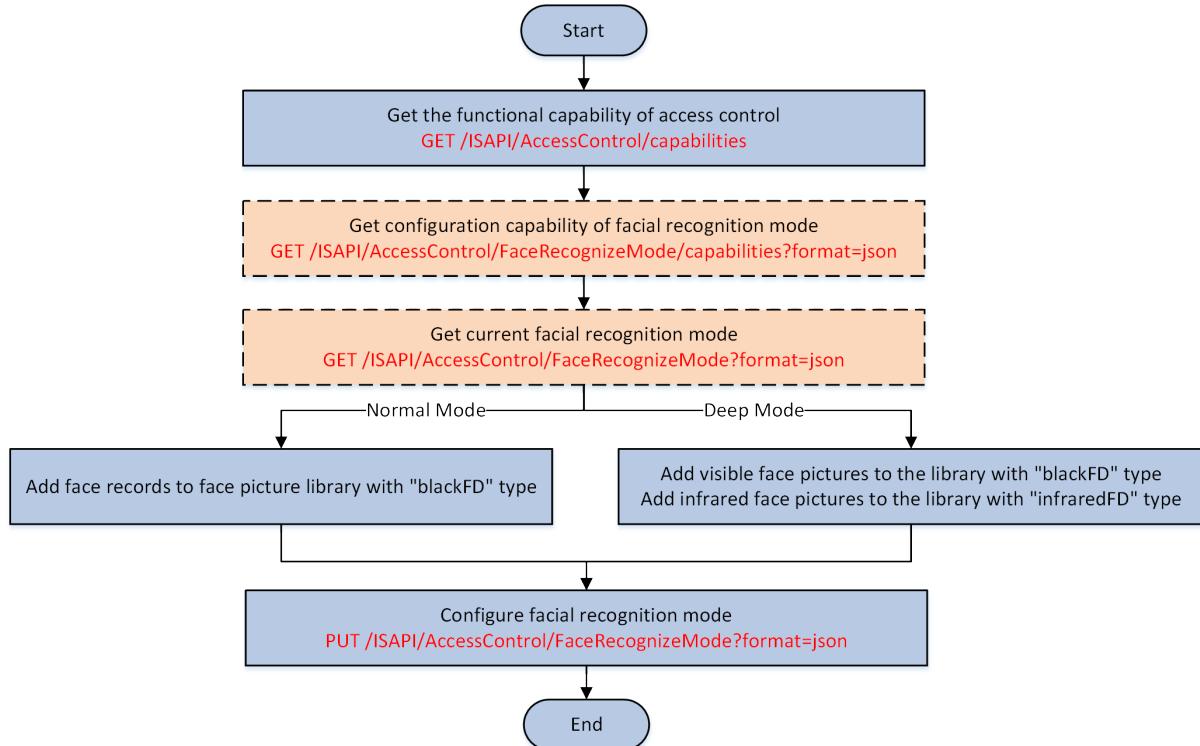


Figure 4-8 Programming Flow of Configuring Facial Recognition Mode

1. Call **/ISAPI/AccessControl/capabilities** by GET method to get the functional capability of access control and check whether the device supports configuring facial recognition mode.



The capability will be returned in the message **XML_Cap_AccessControl**.

If the device supports configuring facial recognition mode, the node

<isSupportFaceRecognizeMode> is returned and its value is "true", and then you can perform the following steps. Otherwise, it indicates that configuring facial recognition mode is not supported by the device, please end this task.

2. **Optional:** Call **/ISAPI/AccessControl/FaceRecognizeMode/capabilities?format=json** by GET method to get the configuration capability of facial recognition mode for knowing the supported facial recognition modes.
3. **Optional:** Call **/ISAPI/AccessControl/FaceRecognizeMode?format=json** by GET method to get the current facial recognition mode.
4. Perform one of the following operations to add face records to face picture libraries for setting normal or deep facial recognition mode.
 - Add face records to the default face picture library with "blackFD" type, refer to **Manage Face Records in Face Picture Library** for details.

- Add visible face pictures to the default face picture library with "blackFD" type, and add infrared face pictures to the default library with "infraredFD" type, refer to [**Manage Face Records in Face Picture Library**](#) for details.
-



Note

Generally, during the initialization of the access control device, two face picture libraries with "blackID" type (the library ID is 1) and "infraredFD" type (the library ID is 2) will be created automatically. But if the default libraries have not been created, you should create them by yourself, refer to [**Create Face Picture Library**](#) for details.

5. Call [**/ISAPI/AccessControl/FaceRecognizeMode?format=json**](#) by PUT method to configure facial recognition mode.

Result

The device will reboot automatically after configuring facial recognition mode, and permissions linked with face pictures in the library will be cleared.

4.6 Configure Access Permission Control Schedule

To regularly control the access permissions for managing the accessible time duration (by default, it is 24 hours) of some important access control points, you can configure the week or holiday schedules.

Steps

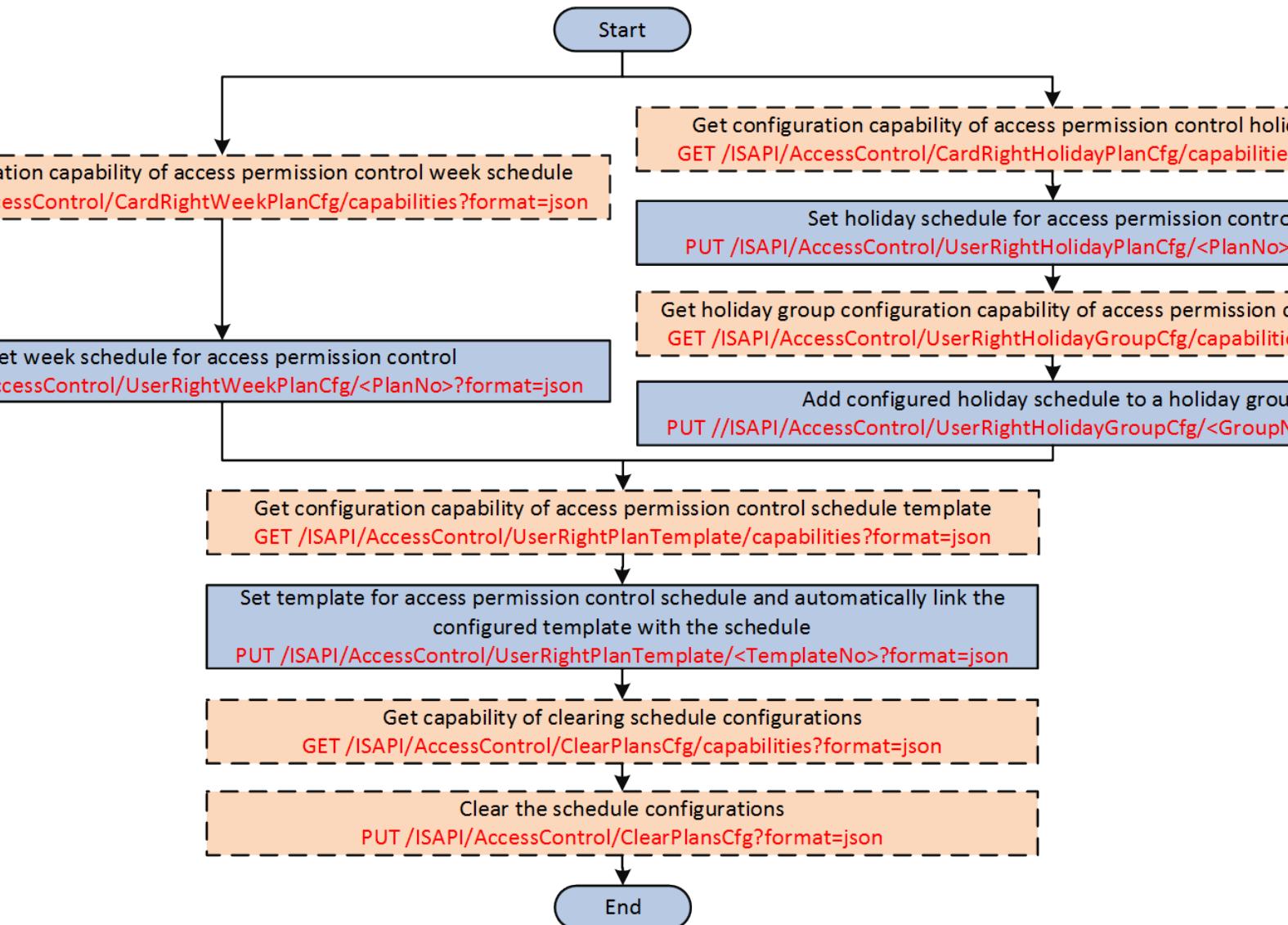


Figure 4-9 API Calling Flow of Configuring Access Permission Control Schedule

1. Perform one of the following operations to set week or holiday schedule for access permission control.
 - a. Call **/ISAPI/AccessControl/UserRightWeekPlanCfg/capabilities?format=json** by GET method to get the configuration capability of access permission control week schedule for knowing the configuration details and notices.
 - b. Call **/ISAPI/AccessControl/UserRightWeekPlanCfg/<PlanNo>?format=json** by PUT method to set the week schedule.

- a. Call [/ISAPI/AccessControl/UserRightHolidayPlanCfg/capabilities?format=json](#) by GET method to get the configuration capability of access permission control holiday schedule for knowing the configuration details and notices.
 - b. Call [/ISAPI/AccessControl/UserRightHolidayPlanCfg/<PlanNo>?format=json](#) by PUT method to set the holiday schedule.
 - c. Call [/ISAPI/AccessControl/UserRightHolidayGroupCfg/capabilities?format=json](#) by GET method to get the holiday group configuration capability of access permission control schedule for knowing the configuration details and notices.
 - d. Call [/ISAPI/AccessControl/UserRightHolidayGroupCfg/<GroupNo>?format=json](#) by PUT method to add the configured holiday schedule to a holiday group for management.
2. **Optional:** Call [/ISAPI/AccessControl/UserRightPlanTemplate/capabilities?format=json](#) by GET method to get the configuration capability of access permission control schedule template for knowing the configuration details and notices.
3. Call [/ISAPI/AccessControl/UserRightPlanTemplate/<TemplateNo>?format=json](#) by PUT method to set template for access permission control schedule and link the configured template to the schedule.



Note

For the above configuration URLs, before setting the parameters, you'd better perform GET operation to get the existing or configured parameters for reference.

1. **Optional:** Call [/ISAPI/AccessControl/ClearPlansCfg/capabilities?format=json](#) by GET method to get the capability of clearing schedule configurations for knowing the configuration details and notices.
5. **Optional:** Call [/ISAPI/AccessControl/ClearPlansCfg?format=json](#) by PUT method to clear the schedule configurations.

4.7 Configure Authentication Mode Control Schedule

You can configure the week or holiday schedule to regularly control the authentication modes (e.g., by card, by card+password, by fingerprint, by fingerprint+card, and so on) in some specific time periods.

Perform this task to configure authentication mode control schedule via ISAPI protocol.

Steps

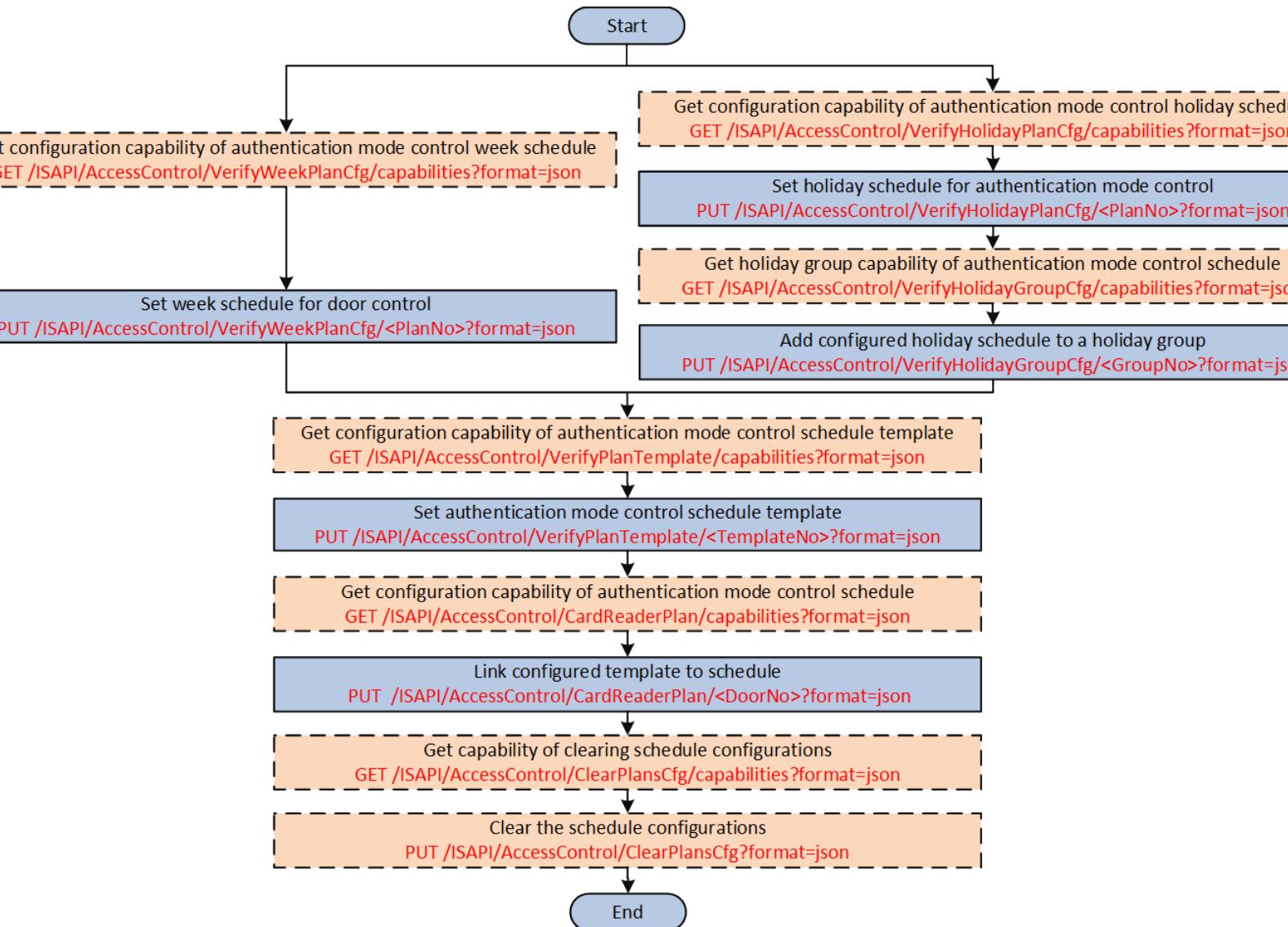


Figure 4-10 Programming Flow of Configuring Authentication Mode Control Schedule

1. Perform one of the following operations to set week or holiday schedule for authentication mode control.

- a. Call **/ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities?format=json** by GET method to get the configuration capability of authentication mode control week schedule for knowing the configuration details and notices.
- b. Call **/ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json** by PUT method to set the week schedule.

- a. Call [/ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities?format=json](#) by GET method to get the configuration capability of authentication mode control holiday schedule for knowing the configuration details and notices.
 - b. Call [/ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json](#) by PUT method to set the holiday schedule.
 - c. Call [/ISAPI/AccessControl/VerifyHolidayGroupCfg/capabilities?format=json](#) by GET method to get the holiday group configuration capability of authentication mode control schedule for knowing the configuration details and notices.
 - d. Call [/ISAPI/AccessControl/VerifyHolidayGroupCfg/<GroupNo>?format=json](#) by PUT method to add the configured holiday schedule to a holiday group for management.
2. **Optional:** Call [/ISAPI/AccessControl/VerifyPlanTemplate/capabilities?format=json](#) by GET method to get the configuration capability of authentication mode control schedule template for knowing the configuration details and notices.
3. Call [/ISAPI/AccessControl/VerifyPlanTemplate/<TemplateNo>?format=json](#) by PUT method to set template for authentication mode control schedule.
4. **Optional:** Call [/ISAPI/AccessControl/CardReaderPlan/capabilities?format=json](#) by GET method to get the configuration capability of authentication mode control schedule for knowing the configuration details and notices.
5. Call [/ISAPI/AccessControl/CardReaderPlan/<CardReaderNo>?format=json](#) by PUT method to link the configured template to the configured authentication mode control schedule.
-



Note

For the above configuration URLs, before setting the parameters, you'd better perform GET operation to get the existing or configured parameters for reference.

1. **Optional:** Call [/ISAPI/AccessControl/ClearPlansCfg/capabilities?format=json](#) by GET method to get the capability of clearing schedule configurations for knowing the configuration details and notices.
7. **Optional:** Call [/ISAPI/AccessControl/ClearPlansCfg?format=json](#) by PUT method to clear the schedule configurations.
-

4.8 Configure Door Control Schedule

You can configure the week or holiday schedule to regularly control the door statuses, including Remain Open (access without authentication), Remain Closed (access is not allowed), and Normal (access with authentication), in some specific time periods.

Perform this task to configure door control schedule via ISAPI protocol.

Steps

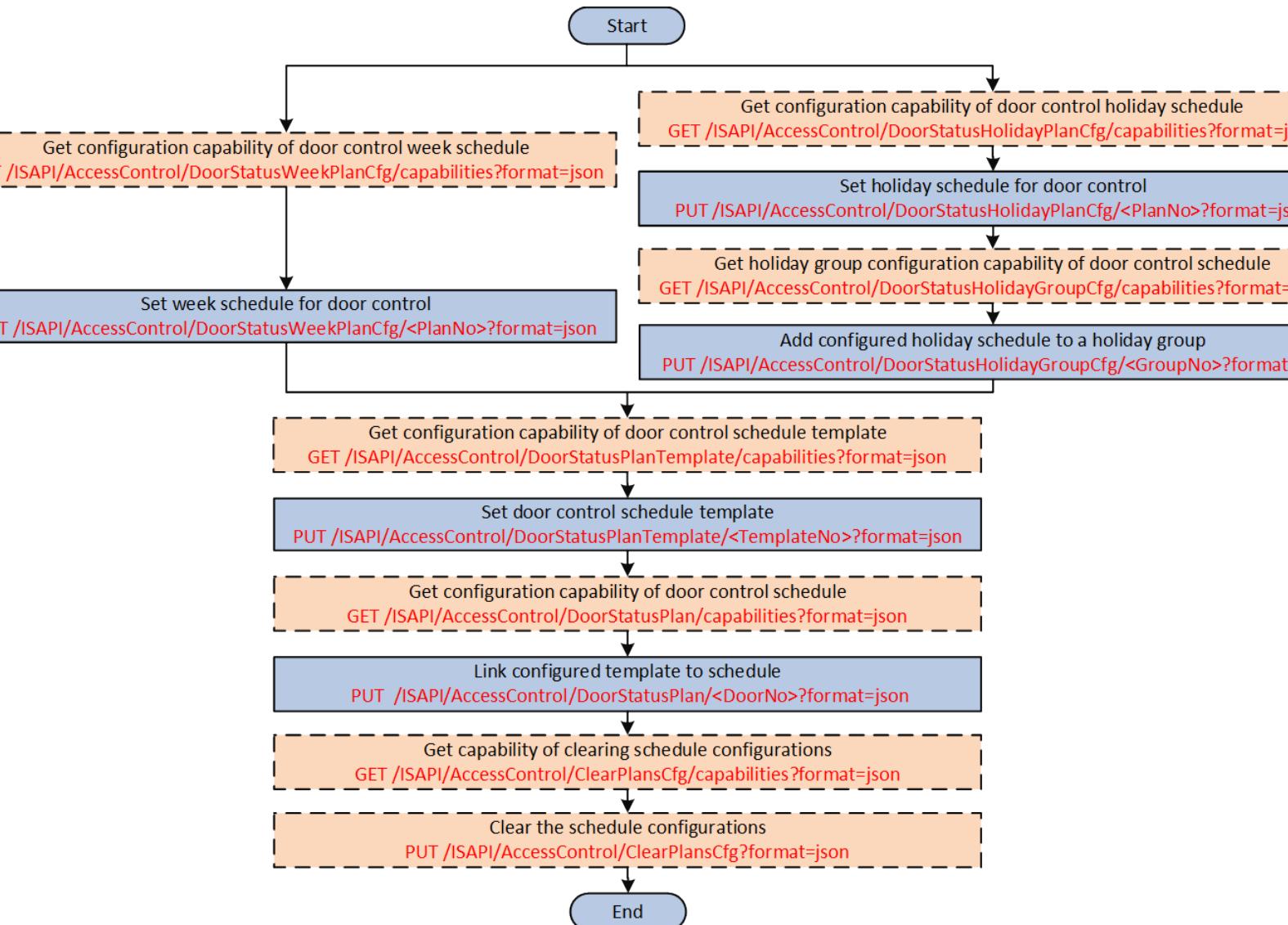


Figure 4-11 Programming Flow of Configuring Door Control Schedule

1. Perform one of the following operations to set week or holiday schedule for door control.

- a. Call **/ISAPI/AccessControl/DoorStatusWeekPlanCfg/capabilities?format=json** by GET method to get the configuration capability of door control week schedule for knowing the configuration details and notices.
- b. Call **/ISAPI/AccessControl/DoorStatusWeekPlanCfg/<PlanNo>?format=json** by PUT method to set the week schedule.

- a. Call [/ISAPI/AccessControl/DoorStatusHolidayPlanCfg/capabilities?format=json](#) by GET method to get the configuration capability of door control holiday schedule for knowing the configuration details and notices.
 - b. Call [/ISAPI/AccessControl/DoorStatusHolidayPlanCfg/<PlanNo>?format=json](#) by PUT method to set the holiday schedule.
 - c. Call [/ISAPI/AccessControl/DoorStatusHolidayPlanCfg/capabilities?format=json](#) by GET method to get the holiday group configuration capability of door control schedule for knowing the configuration details and notices.
 - d. Call [/ISAPI/AccessControl/DoorStatusHolidayGroupCfg/<GroupNo>?format=json](#) by PUT method to add the configured holiday schedule to a holiday group for management.
2. **Optional:** Call [/ISAPI/AccessControl/DoorStatusPlanTemplate/capabilities?format=json](#) by GET method to get the configuration capability of door control schedule template for knowing the configuration details and notices.
3. Call [/ISAPI/AccessControl/DoorStatusPlanTemplate/<TemplateNo>?format=json](#) by PUT method to set template for door control schedule.
4. **Optional:** Call [/ISAPI/AccessControl/DoorStatusPlan/capabilities?format=json](#) by GET method to get the configuration capability of door control schedule for knowing the configuration details and notices.
5. Call [/ISAPI/AccessControl/DoorStatusPlan/<DoorNo>?format=json](#) by PUT method to link the configured template to the configured door control schedule.
-



Note

For the above configuration URLs, before setting the parameters, you'd better perform GET operation to get the existing or configured parameters for reference.

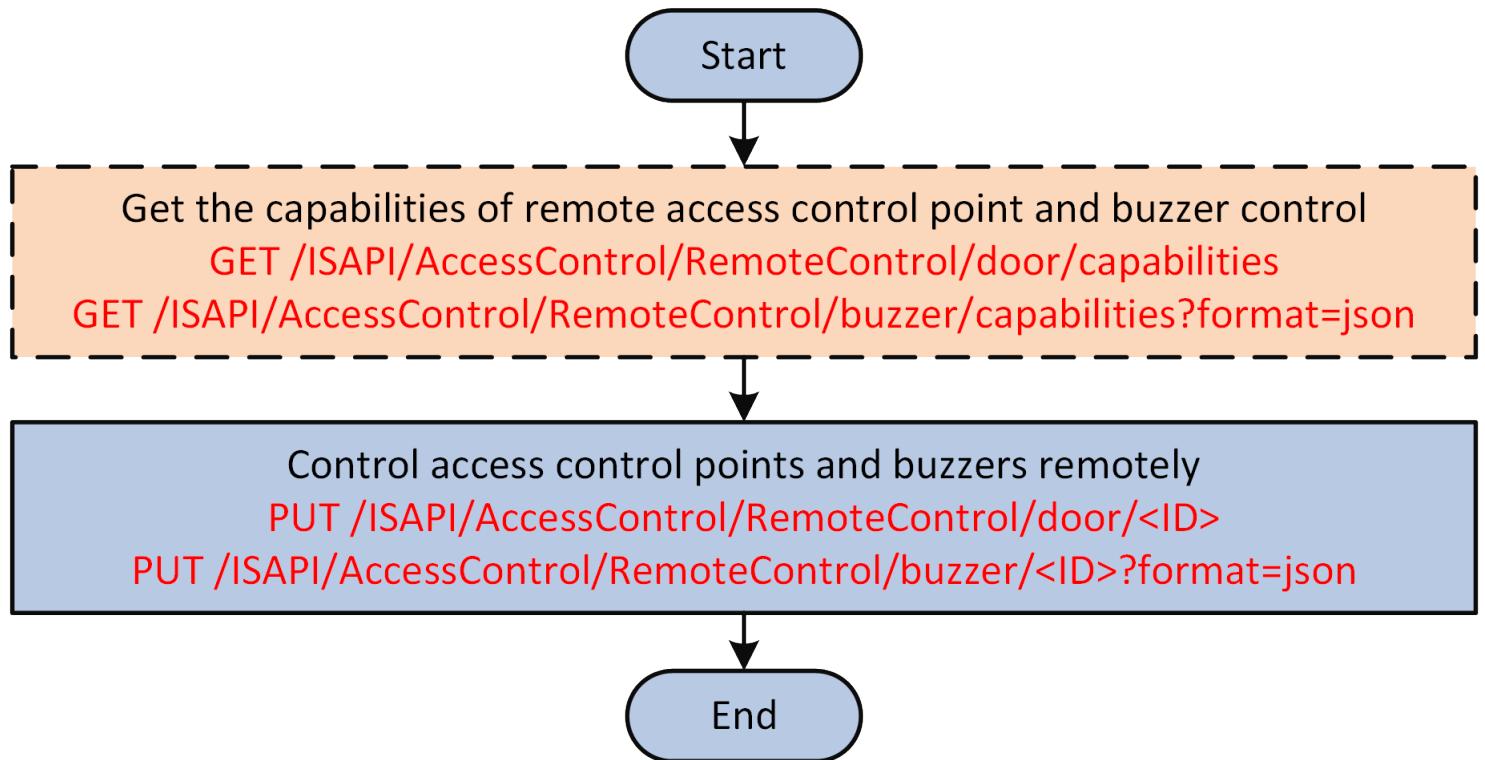
1. **Optional:** Call [/ISAPI/AccessControl/ClearPlansCfg/capabilities?format=json](#) by GET method to get the capability of clearing schedule configurations for knowing the configuration details and notices.
7. **Optional:** Call [/ISAPI/AccessControl/ClearPlansCfg?format=json](#) by PUT method to clear the schedule configurations.
-

4.9 Remotely Control Door, Elevator, and Buzzer

You can remotely control the status of doors or elevators, and buzzer (i.e., start or stop buzzing).

Perform this task to remotely control doors, elevators, and buzzers via ISAPI protocol.

Steps

**Figure 4-12 Programming Flow of Remotely Controlling Door, Elevator, and Buzzer**

1. **Optional:** Perform one of the following operations to get the capabilities of remote control to know the available configurations.
 - Call `/ISAPI/AccessControl/RemoteControl/door/capabilities` by GET method to get the capability of remote door or elevator control.
 - Call `/ISAPI/AccessControl/RemoteControl/buzzer/capabilities?format=json` by GET method to get the capability of remote buzzer control.
2. Perform one of the following operations to control the doors, elevators, or buzzers.
 - Call `/ISAPI/AccessControl/RemoteControl/door/<ID>` by PUT method to control the doors or elevators remotely.

**Note**

For doors, you can control them in **Remain Open**, **Remain Closed**, or **Normal** status; for elevators, you can control them in the status of **Elevator is Allowed to be Called by Visitor** or **Elevator is Allowed to be Called by Resident Only**.

- Call `/ISAPI/AccessControl/RemoteControl/buzzer/<ID>?format=json` by PUT method to control buzzers remotely to start or stop buzzing.

4.10 Configure Password for Remote Door Control

If you want to remotely control the door via the EZVIZ Cloud Service, the password should be verified to improve the security. You should configure the password for the door before you can remotely control the door via the EZVIZ Cloud Service.

Steps

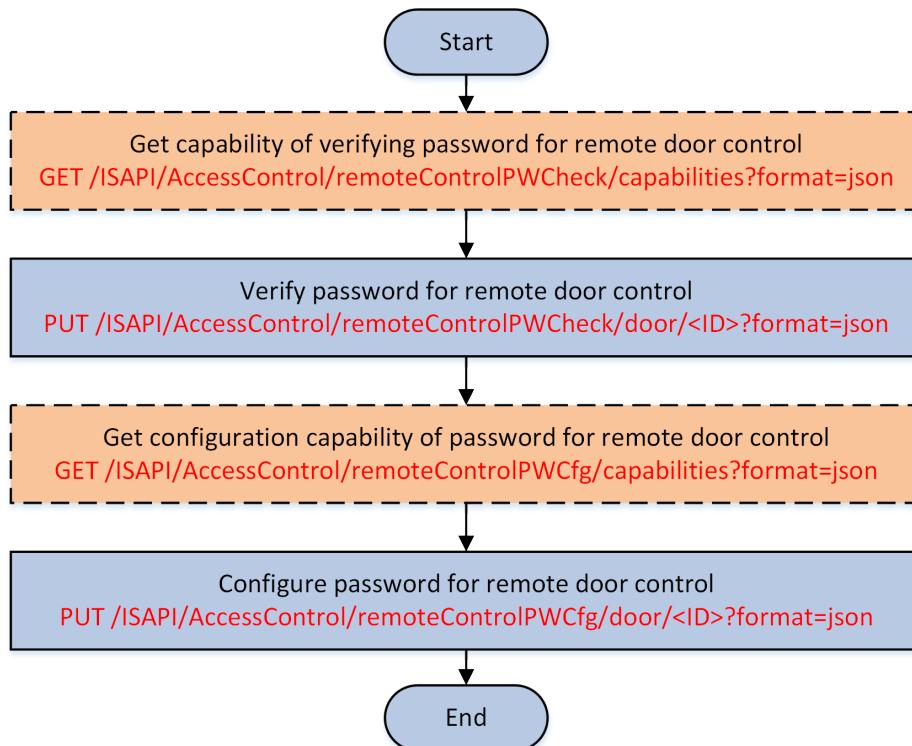


Figure 4-13 Programming Flow of Configuring Password for Remote Door Control

1. **Optional:** Call [/ISAPI/AccessControl/remoteControlPWCheck/capabilities?format=json](#) by GET method to get the capability of verifying password for remote door control.
The capability is returned in the message [JSON_Cap_RemoteControlPWCheck](#).
2. Call [/ISAPI/AccessControl/remoteControlPWCheck/door/<ID>?format=json](#) by PUT method to verify the password for remote door control.
3. **Optional:** Call [/ISAPI/AccessControl/remoteControlPWCfg/capabilities?format=json](#) by GET method to get the capability of configuring password for remote door control.
The capability is returned in the message [JSON_Cap_RemoteControlPWCfg](#).
4. Call [/ISAPI/AccessControl/remoteControlPWCfg/door/<ID>?format=json](#) by PUT method to configure the password for remote door control.

4.11 Configure Anti-Passing Back

The anti-passing back is to set the only route for passing the access control points and only one person could pass after swiping card. You can configure this function to enhance the access security of some important and specific places (e.g., laboratories, offices).

Steps

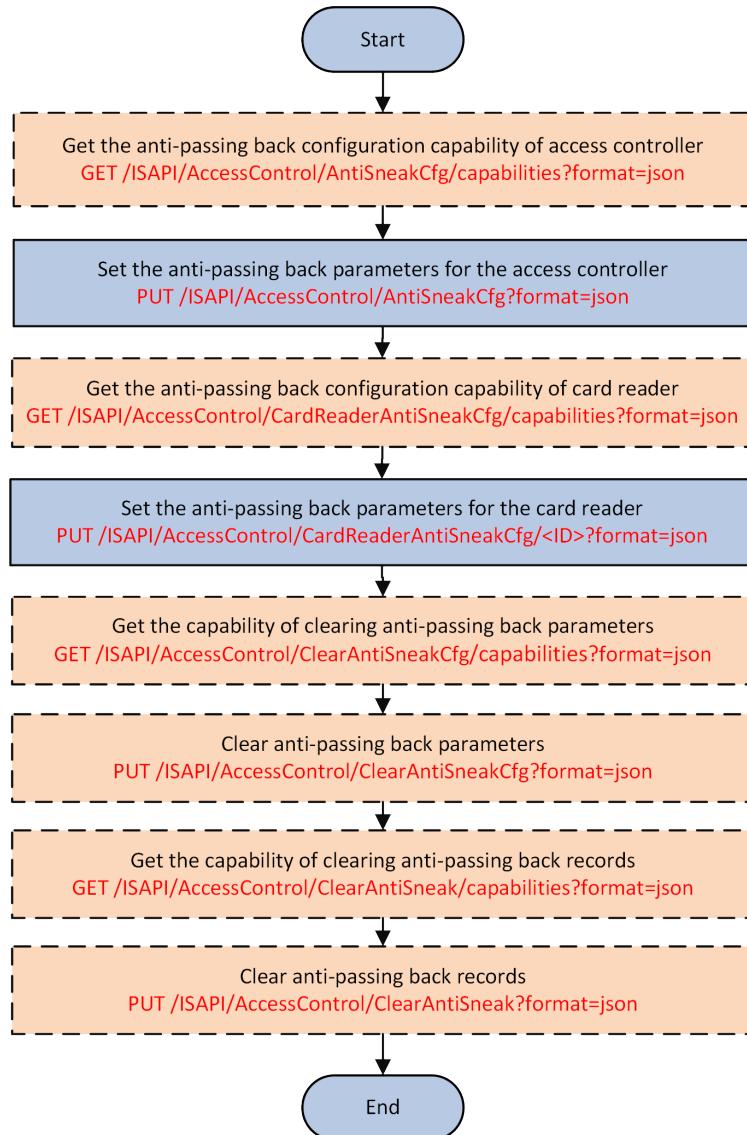


Figure 4-14 Programming Flow of Configuring Anti-Passing Back



Before setting the following parameters, you'd better get the existing or configured parameters for reference by each configuration URLs with GET method.

1. **Optional:** Call [/ISAPI/AccessControl/AntiSneakCfg/capabilities?format=json](#) by GET method to get the anti-passing back configuration capability of the access controller.
The anti-passing back configuration capability [JSON_Cap_AntiSneakCfg](#) is returned.
2. Call [/ISAPI/AccessControl/AntiSneakCfg?format=json](#) by PUT method to set the anti-passing back parameters of the access controller.
3. **Optional:** Call [/ISAPI/AccessControl/CardReaderAntiSneakCfg/capabilities?format=json](#) by GET method to get the anti-passing back configuration capability of the card reader.
4. Call [/ISAPI/AccessControl/CardReaderCfg/<ID>?format=json](#) by PUT method to set the anti-passing back parameters of the card reader.
5. Perform the following operation(s) after configuring the anti-passing back function.

Clear Anti-passing Back Parameters

PUT [/ISAPI/AccessControl/ClearAntiSneakCfg?format=json](#)



The capability of clearing anti-passing back parameters ([JSON_Cap_ClearAntiSneakCfg](#)) can be obtained by calling [/ISAPI/AccessControl/ClearAntiSneakCfg/capabilities?format=json](#) by GET method.

Clear Anti-passing Back Records

If the anti-passing back event occurred, it will be recorded in the access controller, so if needed, you can call [/ISAPI/AccessControl/ClearAntiSneak?format=json](#) by PUT method for clearing the records.



The capability of clearing anti-passing back records ([JSON_Cap_ClearAntiSneak](#)) can be obtained by calling [/ISAPI/AccessControl/ClearAntiSneak/capabilities?format=json](#) by GET method.

4.12 Cross-Controller Anti-Passing Back Configuration

You can set anti-passing for card readers in multiple access controllers. You should swipe the card according to the configured card swiping route or entrance/exit. And only one person can pass the access control point after swiping the card.

4.12.1 Configure Route Anti-Passing Back Based on Network

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards. The anti-passing back will be judged according to the entrance and exit information stored in the card readers.

Steps

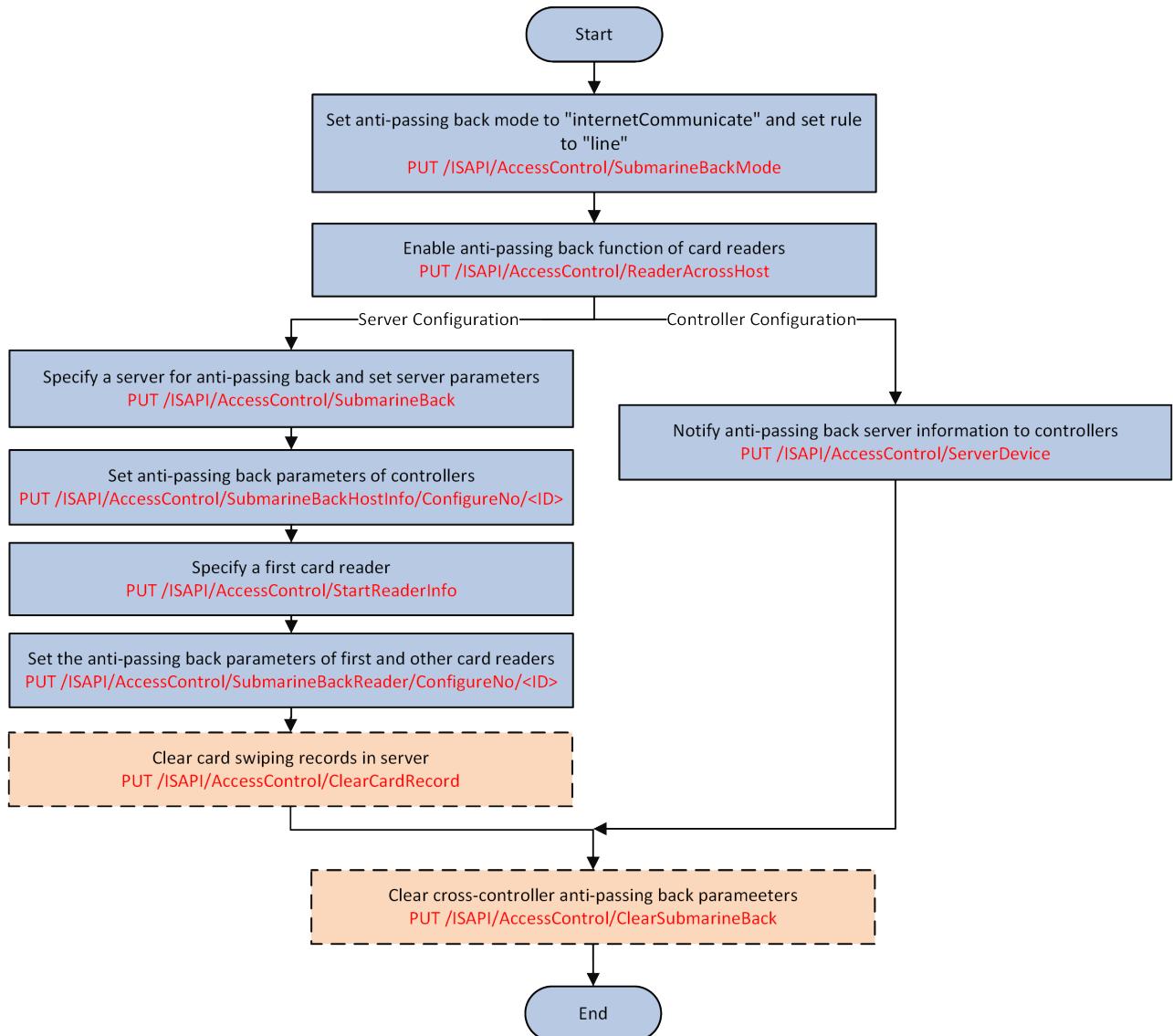


Figure 4-15 Programming Flow of Configuring Route Anti-Passing Back Based on Network



Note

Before setting the following parameters, you'd better get the existing or configured parameters for reference by each configuration URLs with GET method.

1. Call [**/ISAPI/AccessControl/SubmarineBackMode**](#) by PUT method to set the anti-passing back mode and rule.
-



Note

- For route anti-passing back based on network, the mode must be set to "internetCommunicate" and the rule should be set to "line".
- To get the capability of setting anti-passing back mode and rule, you should call [**/ISAPI/AccessControl/SubmarineBackMode/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_SubmarineBackMode**](#).

2. Call [**/ISAPI/AccessControl/ReaderAcrossHost**](#) by PUT method to enable anti-passing back of card readers.
-



Note

To get the capability of enabling anti-passing back of card readers, you should call [**/ISAPI/AccessControl/ReaderAcrossHost/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_ReaderAcrossHost**](#).

3. Perform one of the following operations to configure anti-passing back server or access controllers.

- Configure anti-passing back server:

- a. Call [**/ISAPI/AccessControl/SubmarineBack**](#) by PUT method to specify an access controller as the server for cross-controller anti-passing back and set the server parameters.
-



Note

To get the capability of specifying a server for cross-controller anti-passing back, you should call [**/ISAPI/AccessControl/SubmarineBack/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_SubmarineBack**](#).

- b. Call [**/ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>**](#) by PUT method to set anti-passing back parameters of access controllers.
-



Note

To get the capability of adding access controllers to the anti-passing back route, you should call [**/ISAPI/AccessControl/SubmarineBackHostInfo/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_SubmarineBackHostInfo**](#).

- c. Call [**/ISAPI/AccessControl/StartReaderInfo**](#) by PUT method to specify a first card reader.
-



Note

To get the capability of specifying a first card reader, you should call [/ISAPI/AccessControl/StartReaderInfo/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_StartReaderInfo](#).

- d. Call [/ISAPI/AccessControl/SubmarineBackReader/ConfigureNo/<ID>](#) by PUT method to set anti-passing back parameters of the first card reader and other card readers.
-



Note

To get the capability of setting anti-passing back parameters for card readers, you should call [/ISAPI/AccessControl/SubmarineBackReader/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_SubmarineBackReader](#).

- Configure anti-passing back access controllers:

Call [/ISAPI/AccessControl/ServerDevice](#) by PUT method to notify the anti-passing back server information to access controllers.



Note

To get the capability of notifying anti-passing back server information to access controllers, you should call [/ISAPI/AccessControl/ServerDevice/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_ServerDevice](#).

4. Perform the following operation(s) after configuring route anti-passing back based on network.

Clear Cross-Controller Anti-Passing Back Parameters

PUT [/ISAPI/AccessControl/ClearSubmarineBack](#)



Note

To get the capability of clearing the cross-controller anti-passing back parameters, you should call [/ISAPI/AccessControl/ClearSubmarineBack/capabilities](#) by GET method. And the capability is returned in message [XML_Cap_ClearSubmarineBack](#).

Clear Card Swiping Records in Server

If the card is swiped in the anti-passing back route, it will be recorded in the server. You can call [/ISAPI/AccessControl/ClearCardRecord](#) by PUT method to clear card swiping records in the server.



Note

To get the capability of clearing card swiping records in the server, you should call [/ISAPI/AccessControl/ClearCardRecord/capabilities](#) by GET method. And the capability is returned in message [XML_Cap_ClearCardRecord](#).

4.12.2 Configure Entrance/Exit Anti-Passing Back Based on Network

You can set the entrance card reader and the exit card reader only for entering and exiting, without setting the first card reader and the card readers afterwards. It will authenticate the anti-passing back according to the entrance and exit information on the card reader.

Steps

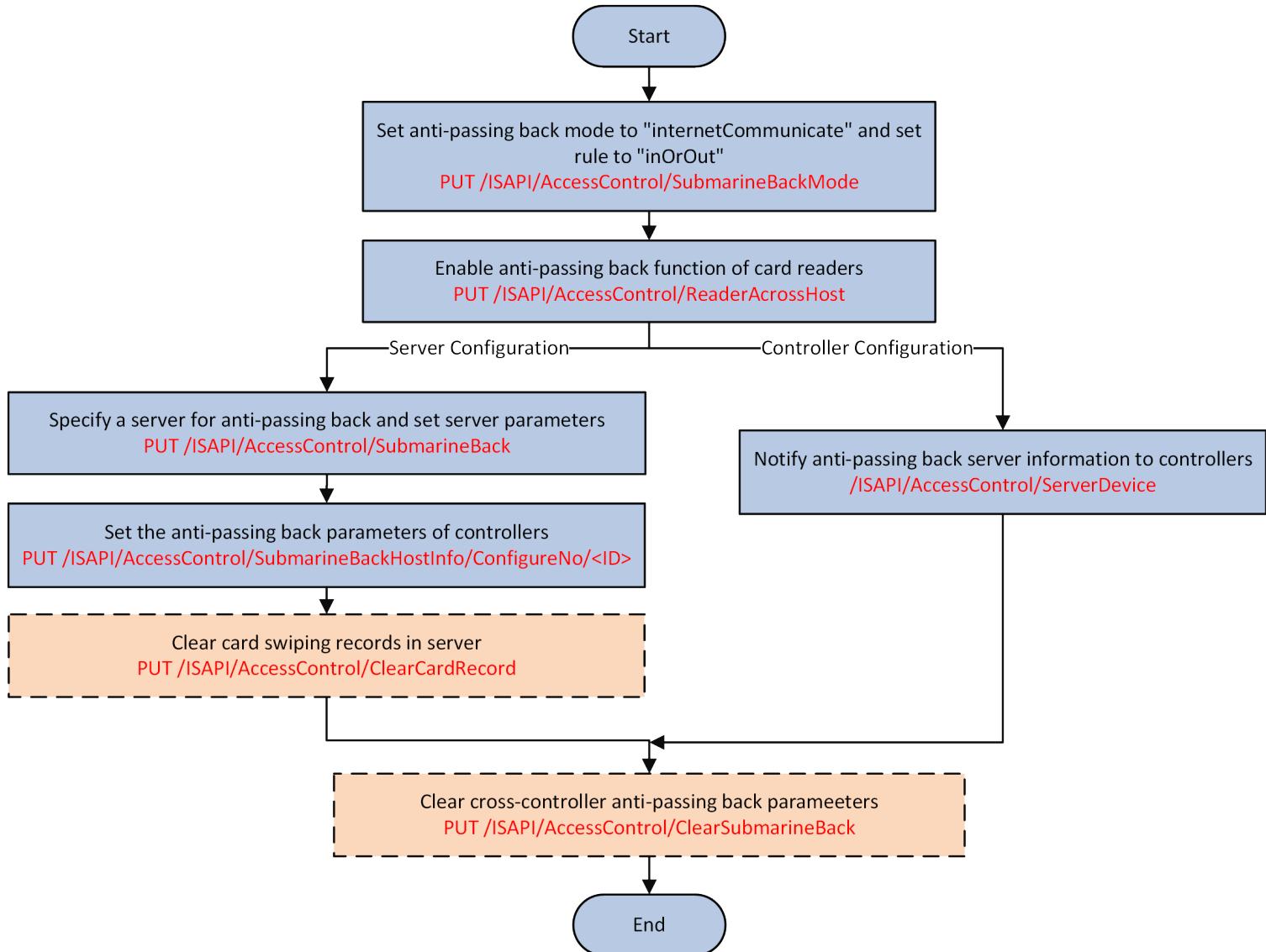


Figure 4-16 Programming Flow of Configuring Entrance/Exit Anti-Passing Back Based on Network



Note

Before setting the following parameters, you'd better get the existing or configured parameters for reference by each configuration URLs with GET method.

1. Call [**/ISAPI/AccessControl/SubmarineBackMode**](#) by PUT method to set anti-passing back mode and rule.
-



Note

- For entrance and exit anti-passing back based on network, the mode must be set to "internetCommunicate" and the rule should be set to "inOrOut".
- To get the capability of setting anti-passing back mode and rule, you should call [**/ISAPI/AccessControl/SubmarineBackMode/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_SubmarineBackMode**](#).

2. Call [**/ISAPI/AccessControl/ReaderAcrossHost**](#) by PUT method to enable anti-passing back of card readers.
-



Note

To get the capability of enabling anti-passing back of card readers, you should call [**/ISAPI/AccessControl/ReaderAcrossHost/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_ReaderAcrossHost**](#).

3. Perform one of the following operations to configure anti-passing back server or access controllers.

- Configure anti-passing back server:

- a. Call [**/ISAPI/AccessControl/SubmarineBack**](#) by PUT method to specify an access controller as the server for cross-controller anti-passing back and set the server parameters.
-



Note

To get the capability of specifying a server for anti-passing back, you should call [**/ISAPI/AccessControl/SubmarineBack/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_SubmarineBack**](#).

- b. Call [**/ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>**](#) by PUT method to set anti-passing back parameters of access controllers.
-



Note

To get the capability of adding access controllers to anti-passing back route, you should call [**/ISAPI/AccessControl/SubmarineBackHostInfo/capabilities**](#) by GET method. And the capability is returned in the message [**XML_Cap_SubmarineBackHostInfo**](#).

- Configure anti-passing access controllers:

- Call [**/ISAPI/AccessControl/ServerDevice**](#) by PUT method to notify the anti-passing back server information to access controllers.
-

-  **Note**

To get the capability of notifying anti-passing back server information to access controllers, you should call [/ISAPI/AccessControl/ServerDevice/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_ServerDevice](#).

4. Perform the following operation(s) after configuring entrance/exit anti-passing back based on network.

Clear Cross-Controller Anti-Passing Back Parameters

PUT [/ISAPI/AccessControl/ClearSubmarineBack](#)

 **Note**

To get the capability of clearing the cross-controller anti-passing back parameters, you should call [/ISAPI/AccessControl/ClearSubmarineBack/capabilities](#) by GET method. And the capability is returned in message [XML_Cap_ClearSubmarineBack](#)

Clear Card Swiping Records in Server

If the card is swiped in the anti-passing back route or entrance/exit, it will be recorded by the server. So you can call [/ISAPI/AccessControl/ClearCardRecord](#) by PUT method for clearing card swiping records in the server.

 **Note**

To get the capability of clearing card swiping records in server, you should call [/ISAPI/AccessControl/ClearCardRecord/capabilities](#) by GET method. And the capability is returned in message [XML_Cap_ClearCardRecord](#)

4.12.3 Configure Route Anti-Passing Back Based on Card

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will judge the anti-passing back according to the entrance and exit records in the card.

Steps

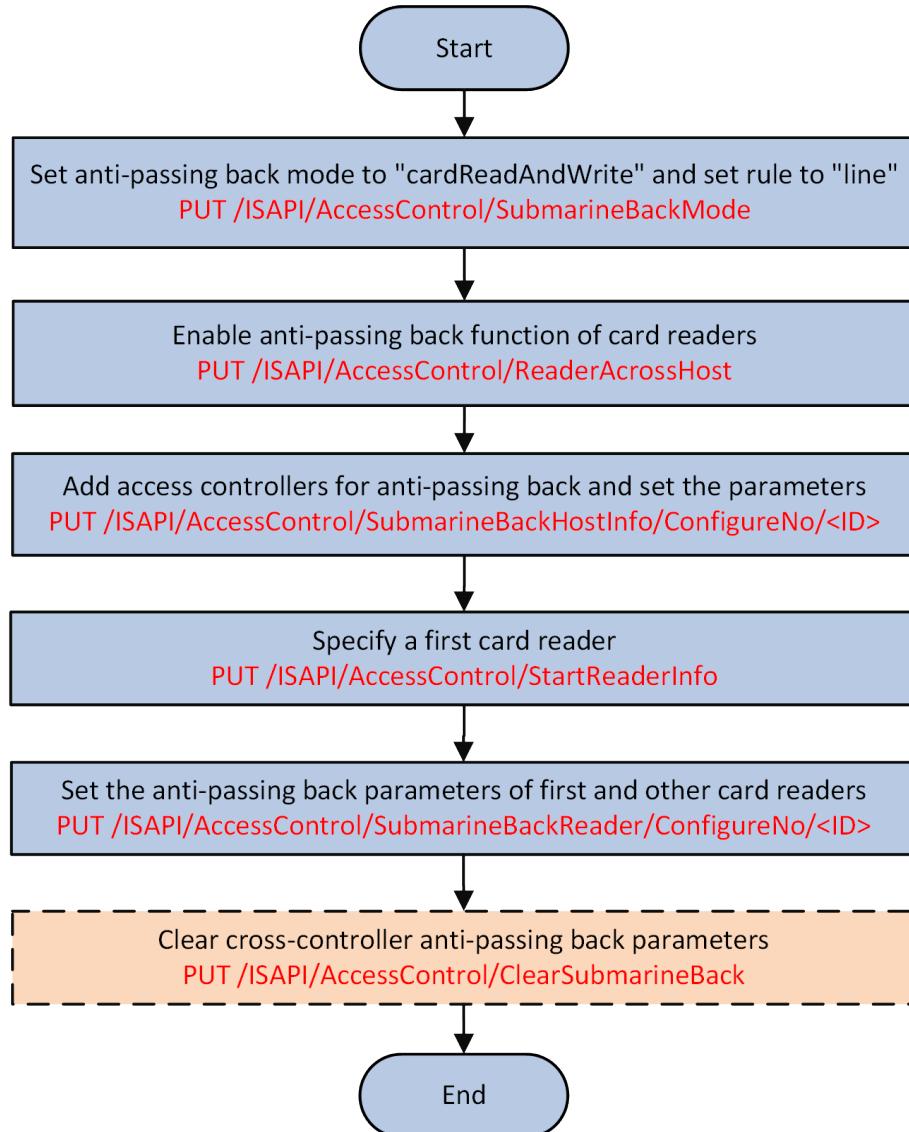


Figure 4-17 Programming Flow of Configuring Route Anti-Passing Back Based on Card



Before setting the following parameters, you'd better get the existing or configured parameters for reference by each configuration URIs with GET method.

1. Call **/ISAPI/AccessControl/SubmarineBackMode** by PUT method to set the anti-passing back mode and rule.

Note

- For route anti-passing back based on card, the mode must be set to "cardReadAndWrite" and the rule should be set to "line".
- To get the capability of setting anti-passing back mode and rule, you should call [/ISAPI/AccessControl/SubmarineBackMode/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_SubmarineBackMode](#).

2. Call [/ISAPI/AccessControl/ReaderAcrossHost](#) by PUT method to enable anti-passing back of card readers.

Note

To get the capability of enabling anti-passing back of card readers, you should call [/ISAPI/AccessControl/ReaderAcrossHost/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_ReaderAcrossHost](#).

3. Call [/ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>](#) by PUT method to add access controllers for anti-passing back and set their parameters.

Note

To get the capability of adding access controllers to anti-passing back route, you should call [/ISAPI/AccessControl/SubmarineBackHostInfo/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_SubmarineBackHostInfo](#).

4. Call [/ISAPI/AccessControl/StartReaderInfo](#) by PUT method to specify a first card reader.

Note

To get the capability of specifying a first card reader, you should call [/ISAPI/AccessControl/StartReaderInfo/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_StartReaderInfo](#).

5. Call [/ISAPI/AccessControl/SubmarineBackReader/ConfigureNo/<ID>](#) by PUT method to set the anti-passing back parameters of the first card reader and other card readers.

Note

To get the capability of setting anti-passing back parameters for card readers, you should call [/ISAPI/AccessControl/SubmarineBackReader/capabilities](#) by GET method. And the capability is returned in the message [XML_Cap_SubmarineBackReader](#).

6. **Optional:** Call [/ISAPI/AccessControl/ClearSubmarineBack](#) by PUT method to clear the cross-controller anti-passing back parameters.

Note

To get the capability of clearing the cross-controller anti-passing back parameters, you should call [/ISAPI/AccessControl/ClearSubmarineBack/capabilities](#) by GET method. And the capability is returned in message [XML_Cap_ClearSubmarineBack](#).

4.12.4 Configure Entrance/Exit Anti-Passing Back Based on Card

You can set the entrance card reader and the exit card reader only for entering and exiting without setting the first card reader and card readers afterwards. The anti-passing back will be judged according to the entrance and exit records in the card.

Steps

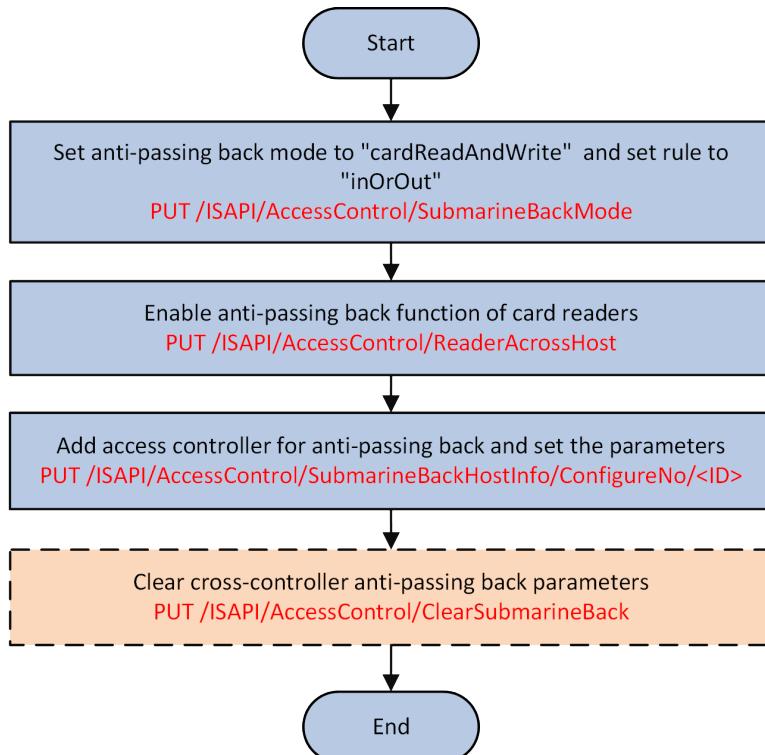


Figure 4-18 Programming Flow of Configuring Entrance/Exit Anti-Passing Back Based on Card



Before setting the following parameters, you'd better get the existing or configured parameters for reference by each configuration URLs with GET method.

1. Call **/ISAPI/AccessControl/SubmarineBackMode** by PUT method to set the anti-passing back mode and rule.



- For entrance and exit anti-passing back based on card, the mode must be set to "cardReadAndWrite" and the rule should be set to "inOrOut".
- To get the capability of setting anti-passing back mode and rule, you should call **/ISAPI/AccessControl/SubmarineBackMode/capabilities** by GET method. And the capability is returned in the message **XML_Cap_SubmarineBackMode**.

2. Call **/ISAPI/AccessControl/ReaderAcrossHost** by PUT method to enable anti-passing back of card readers.



To get the capability of enabling anti-passing back of card readers, you should call **/ISAPI/AccessControl/ReaderAcrossHost/capabilities** by GET method. And the capability is returned in the message **XML_Cap_ReaderAcrossHost**.

3. Call **/ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>** by PUT method to add access controllers for entrance and exit anti-passing back and set the parameters.



To get the capability of adding access controllers for entrance and exit anti-passing back, you should call **/ISAPI/AccessControl/SubmarineBackHostInfo/capabilities** by GET method. And the capability is returned in the message **XML_Cap_SubmarineBackHostInfo**.

4. **Optional:** Call **/ISAPI/AccessControl/ClearSubmarineBack** by PUT method to clear the cross-controller anti-passing back parameters.



To get the capability of clearing cross-controller anti-passing back parameters, you should call **/ISAPI/AccessControl/ClearSubmarineBack/capabilities** by GET method. And the capability is returned in message **XML_Cap_ClearSubmarineBack**.

4.13 Alarm or Event Receiving

When the alarm is triggered or the event occurred, if you have configured alarm/event uploading parameters, you can receive and process the alarm/event information in the third-party platform or system. Two modes are available for receiving alarms, including arming mode and listening mode.

Arming Mode

When the alarm is triggered or event occurred, the third-party platform or system can send the request URL to the device for getting the alarm/event stream, and then the device uploads the response message with alarm/event information.

Listening Mode

When alarm is triggered or event occurred, the device uploads the alarm information automatically, and then the third-party platform or system can receives the alarm/event by configuring listening port of HTTP host server.



Currently, for traffic camera or capture camera, receiving alarm or event in arming mode is not supported.

4.13.1 Supported Alarm/Event Types and Details

Event Type	Value of eventType	Event Message
Access Control Event	AccessControllerEvent	<u>JSON_EventNotificationAlert_AccessControllerEvent</u>
ID Card Swiping Event	IDCardInfoEvent	<u>JSON_EventNotificationAlert_IDCardInfoEvent</u>
QR Code Scanning Event	QRCodeEvent	<u>JSON_EventNotificationAlert_QRCodeEventMsg</u>  Note To check whether the device supports uploading QR code events, you can call <u>/ISAPI/System/capabilities</u> by GET method to get the device capability. The device capability is returned in the message <u>XML_DeviceCap</u> . If uploading QR code events is supported, the node <isSupportQRCodeEvent> will be returned and its value is true.
Face Temperature Screening Event	FaceTemperatureMeasurementEvent	<u>JSON_EventNotificationAlert_FaceTempScreeningEventMsg</u>  Note To check whether the device supports uploading face temperature screening events, you can call <u>/ISAPI/System/capabilities</u> by GET method to get the device capability. The device capability is returned in the message <u>XML_DeviceCap</u> . If uploading face temperature screening events is supported, the node <isSupportFaceTemperatureMeasurementEvent> will be returned and its value is true.

4.13.2 Configure Mask Detection Event

You can configure mask detection parameters to determine whether to open the door and whether to prompt when the person does not wear a mask.

Function	Description
Get Configuration Capability of Mask Detection	GET <u>/ISAPI/AccessControl/maskDetection/capabilities?format=json</u>
Get or Set Mask Detection Parameters	GET or PUT <u>/ISAPI/AccessControl/maskDetection?format=json</u>



To check whether the device supports mask detection, you can call [/ISAPI/AccessControl/capabilities](#)

by GET method to get the access control capability.

The access control capability is returned in the message [XML_Cap_AccessControl](#). If the device supports mask detection, the node <isSupportMaskDetection> will be returned and its value is true.

4.13.3 Configure Hard Hat Detection Event

You can configure hard hat detection parameters to determine whether to open the door when the person does not wear a hard hat.

Function	Request URI
Get Configuration Capability of Hard Hat Detection	GET <u>/ISAPI/AccessControl/Configuration/safetyHelmetDetection/capabilities?format=json</u>
Get or Set Hard Hat Detection Parameters	GET or PUT <u>/ISAPI/AccessControl/Configuration/safetyHelmetDetection?format=json</u>



To check whether the device supports hard hat detection, you can call [/ISAPI/AccessControl/capabilities](#) by GET method to get the access control capability.

The access control capability is returned in the message [XML_Cap_AccessControl](#). If the device supports hard hat detection, the node <isSupportSafetyHelmetDetection> will be returned and its value is true.

4.13.4 Configure and Search for Access Control Events

The access control events include device events, alarm input events, door events, card reader events, card swiping events, and so on. You can configure the linkage types (i.e., event linkage, card linkage, MAC linkage, and person linkage) and linkage actions (e.g., recording, alarm output, buzzing, capture, etc.) of event card linkage via ISAPI protocol to execute the linked actions when

the corresponding events occurred (e.g., door open or closed, card swiped, etc.). And then you can receive the event information from event sources and search for events via ISAPI protocol.

Perform this task to configure and search for the access control events via ISAPI protocol.

Steps

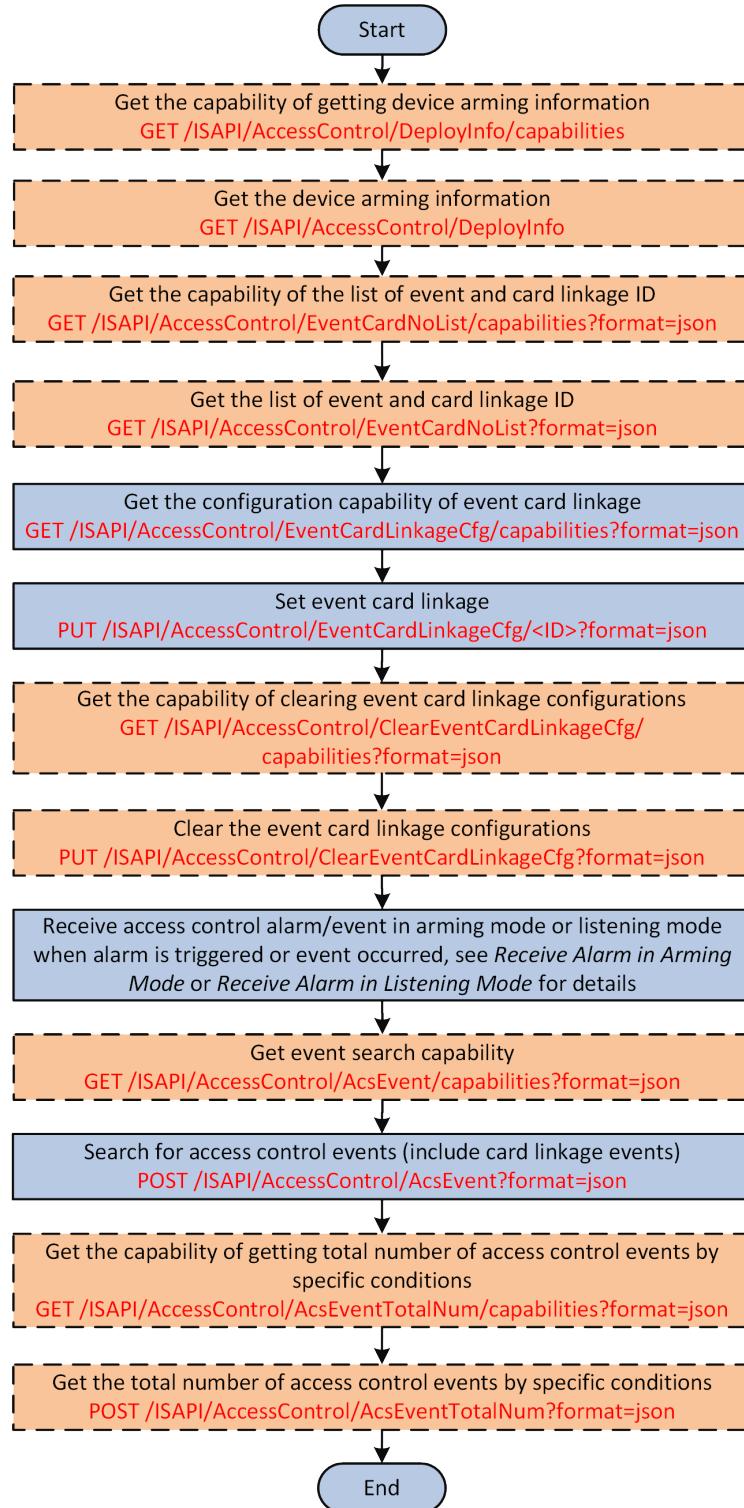


Figure 4-19 Programming Flow of Configuring and Searching for Access Control Events

1. **Optional:** Call [/ISAPI/AccessControl/DeployInfo/capabilities](#) by GET method to get the capability of getting arming information.



The available arming types, including arming via client software, real-time arming, and arming via ISAPI protocol, are returned in the capability. For arming via client software, only one channel can be armed and supports uploading offline events; for real-time arming, up to 4 channels can be armed and it is mainly used to arm the access control device via other devices, but uploading offline events is not supported.

2. **Optional:** Call [/ISAPI/AccessControl/DeployInfo](#) by GET method to get the arming information, such as arming No., arming types, and so on, for checking whether the device is armed by other platforms or systems.
3. **Optional:** Call [/ISAPI/AccessControl/EventCardNoList/capabilities?format=json](#) by GET method to get the capability of the list of event and card linkage ID for knowing the range of event ID that can be configured.
4. **Optional:** Call [/ISAPI/AccessControl/EventCardNoList?format=json](#) by GET method to get the list of configured event and card linkage ID.
5. Call [/ISAPI/AccessControl/EventCardLinkageCfg/capabilities?format=json](#) by GET method to get the configuration capability of event card linkage for knowing the configuration details and notices.
6. Call [/ISAPI/AccessControl/EventCardLinkageCfg/<ID>?format=json](#) by PUT method to set the event card linkages.
7. **Optional:** Call [/ISAPI/AccessControl/ClearEventCardLinkageCfg/capabilities?format=json](#) by GET method to get the capability of clearing event card linkage configurations.
8. **Optional:** Call [/ISAPI/AccessControl/ClearEventCardLinkageCfg?format=json](#) by PUT method to clear the event card linkage configurations.
9. Receive access control alarm/event from the event source in arming mode (see [Receive Alarm/Event in Arming Mode](#)) or listening mode (see [Receive Alarm/Event in Listening Mode](#)) when the specified alarm is triggered or event occurred.



The access control event information (`eventType: "AccessControllerEvent"`) is returned in [JSON_EventNotificationAlert_AccessControllerEvent](#).

10. **Optional:** Call [/ISAPI/AccessControl/AcsEvent/capabilities?format=json](#) by GET method to get the event search capability for knowing the supported event types and other information.
11. Call [/ISAPI/AccessControl/AcsEvent?format=json](#) by POST method to search for access control events.
12. **Optional:** Call [/ISAPI/AccessControl/AcsEventTotalNum/capabilities?format=json](#) by GET method to get the capability of getting total number of access control events by specific conditions.
13. **Optional:** Call [/ISAPI/AccessControl/AcsEventTotalNum?format=json](#) by POST method to get the total number of access control events by specific conditions.

4.13.5 Receive Alarm/Event in Arming Mode

When alarm is triggered or event occurred, and the alarm/event linkage is configured, you can send request message to device for getting the alarm/event stream, and then the device uploads the corresponding response message, which contains alarm/event information.

Before You Start

Make sure you have configured alarm/event and triggered the alarm/event. For configuring alarm/event parameters, refer to the some typical applications of alarm/event configuration.

Steps

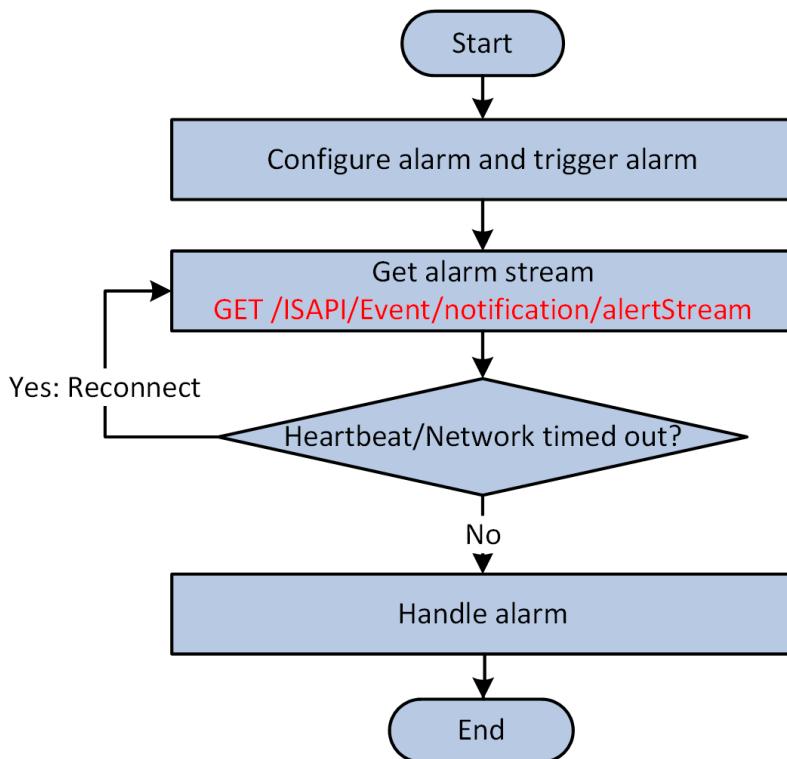


Figure 4-20 API Calling Flow of Receiving Alarm/Event in Arming Mode

1. Call **/ISAPI/Event/notification/alertStream** by GET to get the alarm/event stream.
2. Check if the heartbeat receiving timed out or network disconnected.
 - If the heartbeat keeps alive and the network still connected, perform the following step to continue.
 - If the heartbeat receiving timed out or network disconnected, perform the above step repeatedly until reconnected.
3. Receive and process the alarm/event information.

Example

Sample of Receiving Alarm/Event in Arming Mode (without Binary Picture Data)

```
GET /ISAPI/Event/notification/alertStream HTTP/1.1
Host: data_gateway_ip
Connection: Keep-Alive

HTTP/1.1 401 Unauthorized
Date: Sun, 01 Apr 2018 18:58:53 GMT
Server:
Content-Length: 178
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=10, max=99
WWW-Authenticate: Digest qop="auth",
realm="IP Camera (C2183)",
nonce="4e5468694e7a42694e7a4d364f4449354d7a6b354d54513d",
stale="FALSE"

GET /ISAPI/Event/notification/alertStream HTTP/1.1
Authorization: Digest username="admin",
realm="IP Camera (C2183)",
nonce="4e5468694e7a42694e7a4d364f4449354d7a6b354d54513d",
uri="/ISAPI/Event/notification/alertStream",
cnonce="3d183a245b8729121ae4ca3d41b90f18",
nc=00000001,
qop="auth",
response="f2e0728991bb031f83df557a8f185178"
Host: 10.6.165.192

HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type: multipart/mixed; boundary=<frontier>

--<frontier>
Content-Type: application/xml; charset="UTF-8"
Content-Length: text_length

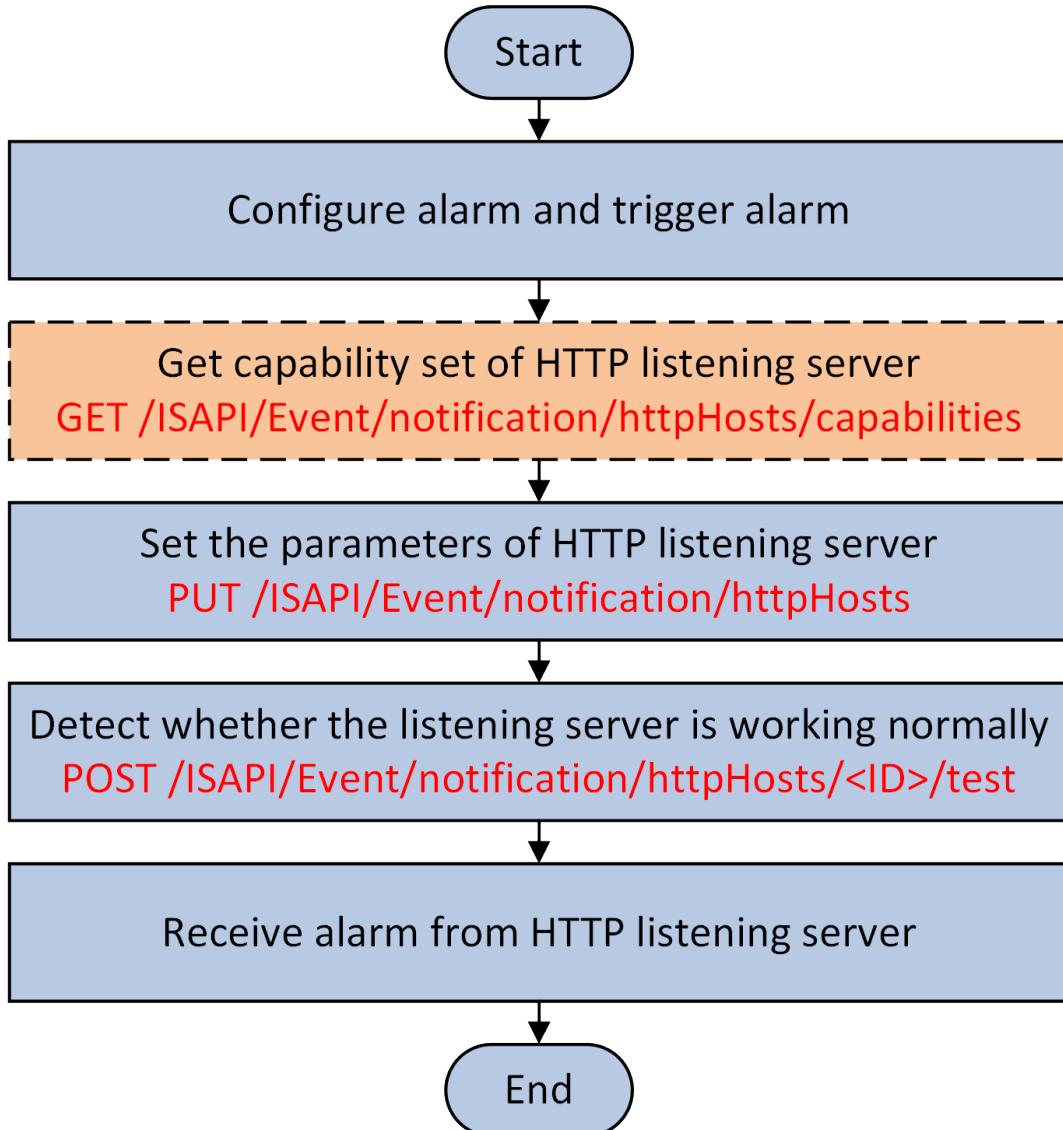
<EventNotificationAlert/>
--<frontier>
```

4.13.6 Receive Alarm/Event in Listening Mode

When alarm is triggered or event occurred, and the alarm/event linkage is configured, the device uploads the alarm/event information automatically, you can receive the alarm/event by configuring the listening port of HTTP host server.

Before You Start

Make sure you have configured alarm/event and triggered the alarm/event. For configuring alarm/event parameters, refer to the some typical applications of alarm/event configuration.

Steps**Figure 4-21 API Calling Flow of Receiving Alarm/Event in Listening Mode**

1. **Optional:** Call **/ISAPI/Event/notification/httpHosts/capabilities** by GET method to get the capability of HTTP listening server.
2. Call **/ISAPI/Event/notification/httpHosts** by PUT method to set the parameters (including listening address and listening port) of HTTP listening server.

**Note**

Before setting the listening server, you'd better call the URI by GET method to get the default or configured parameters for reference.

3. Call **/ISAPI/Event/notification/httpHosts/<ID>/test** by POST method to check if the listening server is working normally.

4. Receive the alarm/event information from the listening server.



Note

After receiving the alarm/event information uploaded by the device, you need to send a response message with the status "200 OK" to the device as the acknowledgment.

Example

Sample Code of Receiving Alarm/Event in Listening Mode

- with Binary Picture Data

```
//Request
POST requestUrl HTTP/1.1
Host: data_gateway_ip:port
Accept-Language: en-US
Date: YourDate
Content-Type: multipart/form-data;boundary=<frontier>
Content-Length: body_length
Connection: keep-alive

--<frontier>
Content-Disposition: form-data; name="Event_Type"
Content-Type: text/xml
Content-Length: xml_length

<EventNotificationAlert/>
--<frontier>
Content-Disposition: form-data; name="Picture_Name"
Content-Length: image_length
Content-Type: image/pjpeg

[binary picture data]
--<frontier>--

//Response
HTTP/1.1 HTTP statusCode
Date: YourDate
Connection: close
```

- without Binary Picture Data

```
//Request
POST requestUrl HTTP/1.1
Host: data_gateway_ip:port
Accept-Language: en-US
Date: YourDate
Content-Type: text/xml;
Content-Length: text_length
Connection: keep-alive

<EventNotificationAlert/>

//Response
HTTP/1.1 HTTP statusCode
```

Date: YourDate
Connection: close



Note

- The **Host** is the HTTP server domain name or IP address and port No.
 - Some alarm data is in JSON format, so the **Content-Type** may be "text/xml" or "text/json".
-

4.13.7 Remotely Verify Access Control Events

For the uploaded access control events, you can verify them remotely to control opening or closing the door.

Function	Description
Get Capability of Verifying Access Control Event Remotely	GET <u>/ISAPI/AccessControl/remoteCheck/capabilities?format=json</u>
Verify Access Control Event Remotely	PUT <u>/ISAPI/AccessControl/remoteCheck?format=json</u>



To check whether the device supports verifying access control events remotely, you can call [/ISAPI/AccessControl/capabilities](#) by GET method to get the access control capability.

The access control capability is returned in the message [XML_Cap_AccessControl](#). If the device supports this function, the node <isSupportRemoteCheck> will be returned and its value is true.

4.14 Configure Attendance Status and Schedule

The time and attendance refers to tracking and monitoring when employees start and stop working, and their working hours (including late arrivals, early departures, time taken on breaks and absenteeism, etc.). You can set the manual or automatic time and attendance mode, or disable the attendance mode. You can also configure the week schedule to regularly manage and control the attendance (i.e., check in, check out, break out, break in, overtime in, or overtime out) in some specific time periods.

Before You Start

Make sure you have added at least one person, refer to [Manage Person Information](#) for details.

Steps

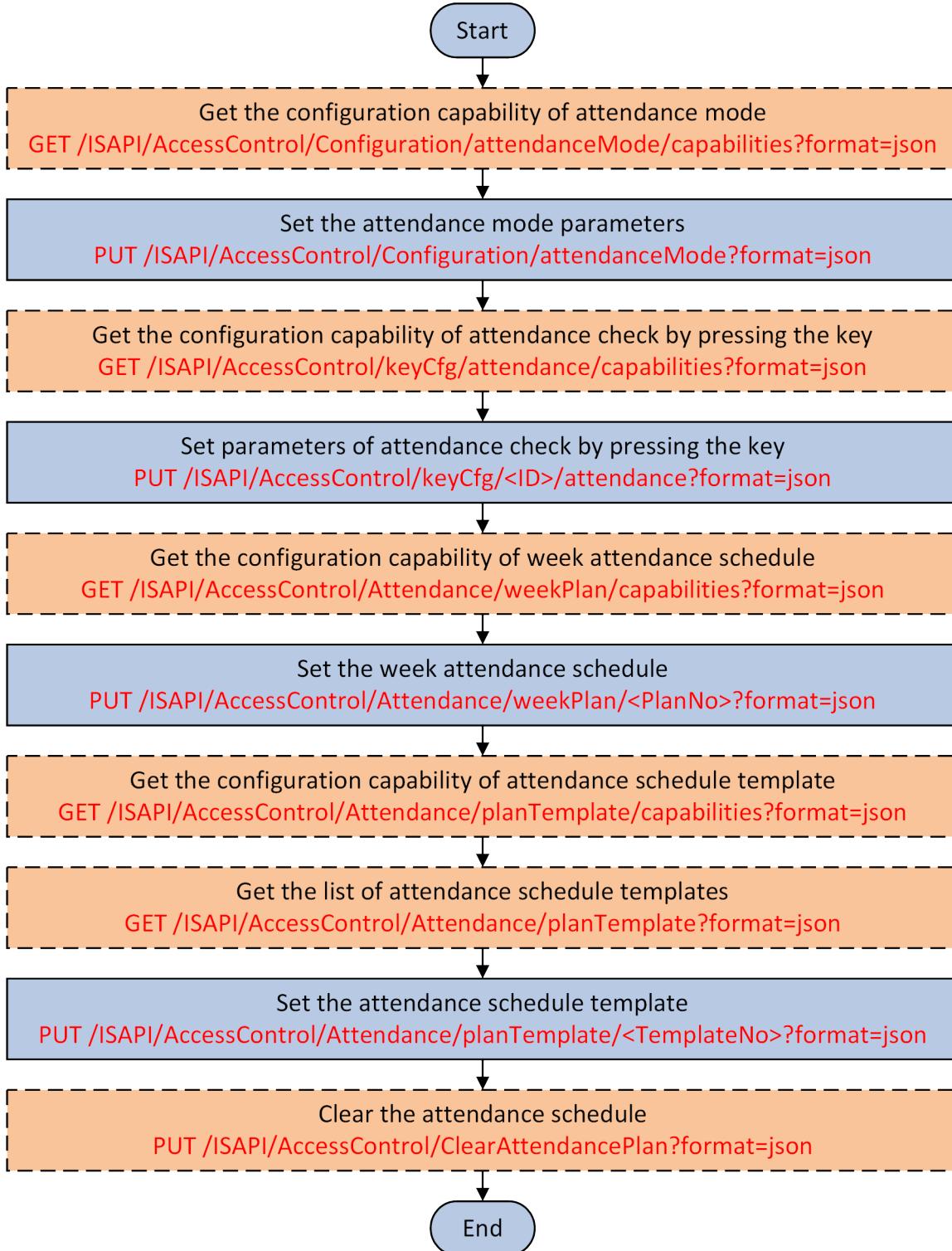


Figure 4-22 API Calling Flow of Configuring Attendance Status and Schedule

1. **Optional:** Call [*/ISAPI/AccessControl/Configuration/attendanceMode/capabilities?format=json*](#) by GET method to get the configuration capability of the attendance mode for knowing the configuration details and notices.



Note

To check whether the device supports configuring the attendance mode, you can call [*/ISAPI/AccessControl/capabilities*](#) by GET method to get the functional capability of access control.

If the node <isSupportAttendanceMode> is returned in the message [*XML_Cap_AccessControl*](#) and its value is true, it indicates that the device supports configuring the attendance mode.

2. Call [*/ISAPI/AccessControl/Configuration/attendanceMode?format=json*](#) by PUT method to set the attendance mode parameters.



Note

Before setting the attendance mode parameters, you'd better call [*/ISAPI/AccessControl/Configuration/attendanceMode?format=json*](#) by GET method to get the existing or default attendance mode parameters for reference.

3. **Optional:** Call [*/ISAPI/AccessControl/keyCfg/attendance/capabilities?format=json*](#) by GET method to get the configuration capability of attendance check by pressing the key for knowing the configuration details and notices.



Note

To check whether the device supports configuring parameters of attendance check by pressing the key, you can call [*/ISAPI/AccessControl/capabilities*](#) by GET method to get the functional capability of access control.

If the node <isSupportKeyCfgAttendance> is returned in the message [*XML_Cap_AccessControl*](#) and its value is true, it indicates that the device supports configuring parameters of attendance check by pressing the key.

4. Call [*/ISAPI/AccessControl/keyCfg/<ID>/attendance?format=json*](#) by PUT method to set the parameters of attendance check by pressing the key.



Note

Before setting the parameters, you'd better call [*/ISAPI/AccessControl/keyCfg/<ID>/attendance?format=json*](#) or [*/ISAPI/AccessControl/keyCfg/attendance?format=json*](#) by GET method to get the existing or default parameters of one or all keys for reference.

5. **Optional:** Call [*/ISAPI/AccessControl/Attendance/weekPlan/capabilities?format=json*](#) by GET method to get the configuration capability of the week attendance schedule for knowing the configuration details and notices.



Note

To check whether the device supports configuring the week attendance schedule, you can call [*/ISAPI/AccessControl/capabilities*](#) by GET method to get the functional capability of access control.

If the node <isSupportAttendanceWeekPlan> is returned in the message [XML Cap AccessControl](#) and its value is true, it indicates that the device supports configuring the week attendance schedule.

6. Call [/ISAPI/AccessControl/Attendance/weekPlan/<PlanNo>?format=json](#) by PUT method to set the parameters of the week attendance schedule.
-



Before setting the parameters, you'd better call [/ISAPI/AccessControl/Attendance/weekPlan/<PlanNo>?format=json](#) by GET method to get the existing or default parameters for reference.

7. **Optional:** Call [/ISAPI/AccessControl/Attendance/planTemplate/capabilities?format=json](#) by GET method to get the configuration capability of the attendance schedule template for knowing the configuration details and notices.
-



To check whether the device supports configuring the attendance schedule template, you can call [/ISAPI/AccessControl/capabilities](#) by GET method to get the functional capability of access control.

If the node <isSupportAttendancePlanTemplate> is returned in the message [XML Cap AccessControl](#) and its value is true, it indicates that the device supports configuring the attendance schedule template.

8. **Optional:** Call [/ISAPI/AccessControl/Attendance/planTemplate?format=json](#) by GET method to get the list of attendance schedule templates.
-



To check whether the device supports getting the list of attendance schedule templates, you can call [/ISAPI/AccessControl/capabilities](#) by GET method to get the functional capability of access control.

If the node <isSupportAttendancePlanTemplateList> is returned in the message [XML Cap AccessControl](#) and its value is true, it indicates that the device supports getting the list of attendance schedule templates.

9. Call [/ISAPI/AccessControl/Attendance/planTemplate/<TemplateNo>?format=json](#) by PUT method to set the parameters of the attendance schedule template.
-



Before setting the parameters, you'd better call [/ISAPI/AccessControl/Attendance/planTemplate/<TemplateNo>?format=json](#) by GET method to get the existing or default parameters for reference.

10. **Optional:** Call [/ISAPI/AccessControl/ClearAttendancePlan?format=json](#) by PUT method to clear the attendance schedule.
-



Note

To check whether the device supports clearing the attendance schedule, you can call [/ISAPI/AccessControl/capabilities](#) by GET method to get the functional capability of access control. If the node <isSupportClearAttendancePlan> is returned in the message [XML Cap AccessControl](#) and its value is true, it indicates that the device supports clearing the attendance schedule.

4.15 Information Release

You can create programs and manage programs according to the following flow chart.

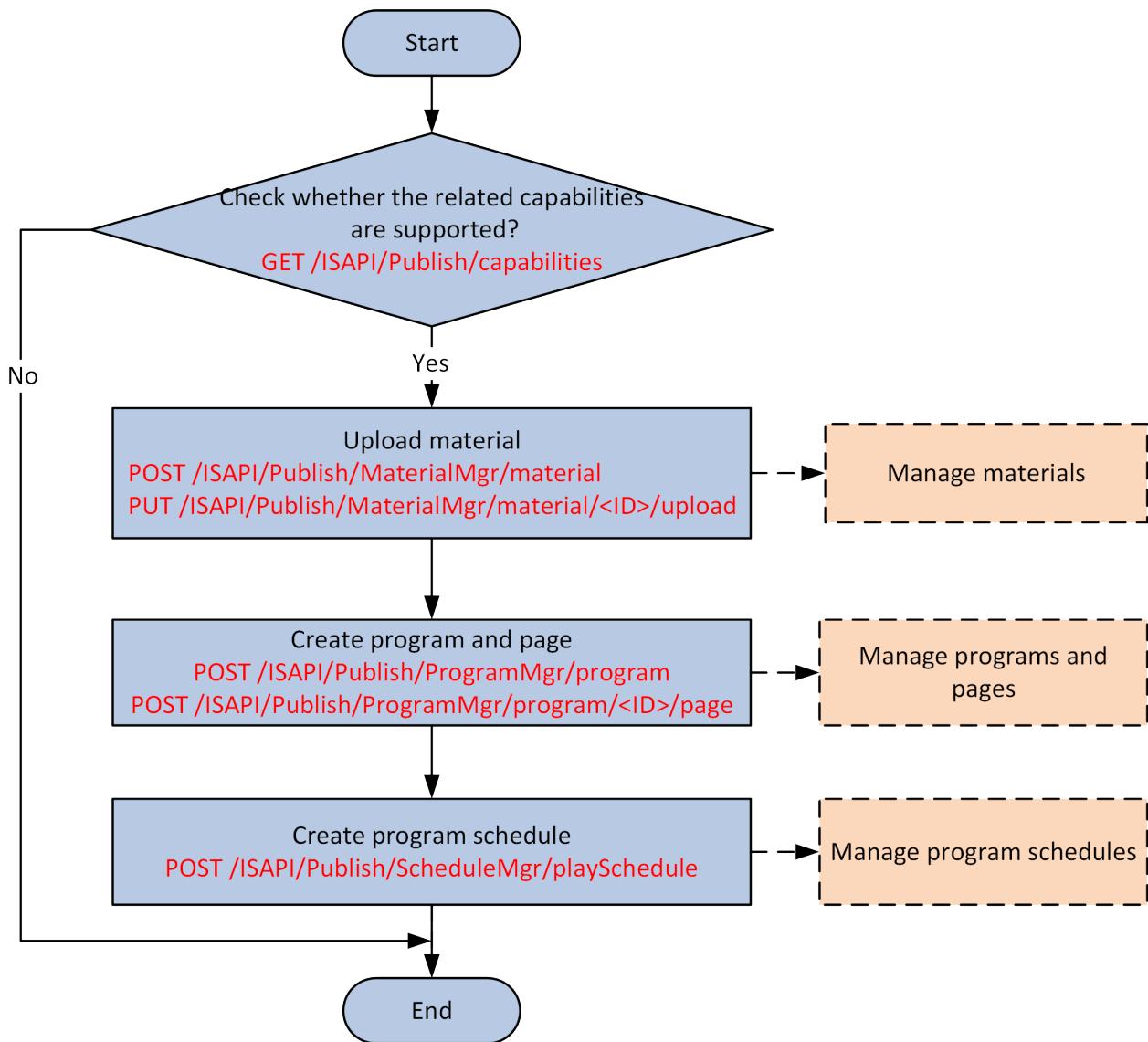


Figure 4-23 Main Flow of Information Release

- Manage materials: to upload, delete, and search to materials. For details, see [Manage Materials](#) .
- Manage programs and pages: to create the programs by customizing layout, edit and delete the programs, manage the pages. For details, see [Manage Programs and Pages](#) .
- Manage the program schedule: to play the program according to the scheduled time or mode. For details, see [Manage the Program Schedule](#) .

4.15.1 Manage Materials

**Note**

This function is supported only when `isSupportMaterialMgr` in `XML_PublishServerCap` is true (related API: [`/ISAPI/Publish/capabilities`](#)).

Function	Request URI
Get the capability of material management parameters	GET <code>/ISAPI/Publish/material/<ID>/capabilities</code>
Create a specific material	POST <code>/ISAPI/Publish/MaterialMgr/material</code>
Get, set or delete a specific material	GET, PUT, or DELETE <code>/ISAPI/Publish/MaterialMgr/material/<ID></code>
Delete multiple materials	DELETE <code>/ISAPI/Publish/MaterialMgr/material</code>
Search for materials	<ul style="list-style-type: none">Get the capability of material search parameters: GET <code>/ISAPI/Publish/MaterialMgr/materialSearch/profile</code>Search for materials: POST <code>/ISAPI/Publish/MaterialMgr/materialSearch</code>
Upload static materials	POST <code>/ISAPI/Publish/MaterialMgr/material/<ID>/upload</code>

4.15.2 Manage Programs and Pages

**Note**

This function is supported only when `isSupportProgramMgr` in `XML_PublishServerCap` is true (related API: [`/ISAPI/Publish/capabilities`](#)).

Function	Request URI
Get capability	GET <code>/ISAPI/Publish/ProgramMgr/program/dynamicCap</code>
Get all programs' parameters	GET <code>/ISAPI/Publish/ProgramMgr/program</code>
Create programs	POST <code>/ISAPI/Publish/ProgramMgr/program</code>
Configure a specific program	<ul style="list-style-type: none">Get the configuration capability of a specific program: GET <code>/ISAPI/Publish/ProgramMgr/program/<ID>/capabilities</code>Get, set or delete a specific program: GET, PUT, or DELETE <code>/ISAPI/Publish/ProgramMgr/program/<ID></code>
Configure page	Get page configuration capability:

Function	Request URI
	GET <u>/ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>/capabilities</u>
	Get information of all pages: GET <u>/ISAPI/Publish/ProgramMgr/program/<ID>/page</u>
	Create a new page: POST <u>/ISAPI/Publish/ProgramMgr/program/<ID>/page</u>
	Get a specific page of a specific program: GET <u>/ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID></u>
	Edit the information of a page: PUT <u>/ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID></u>
	Delete a page: DELETE <u>/ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID></u>

4.15.3 Manage the Program Schedule



This function is supported only when `isSupportScheduleMgr` in `XML_PublishServerCap` is true (related API: [/ISAPI/Publish/capabilities](#)).

Function	Request URI
Get schedule management capability set	GET <u>/ISAPI/Publish/ScheduleMgr/capabilities?format=json</u>
Create schedule	POST <u>/ISAPI/Publish/ScheduleMgr/playSchedule</u>
Configure a specific schedule	<ul style="list-style-type: none"> • Get the configuration capability of a specific schedule: GET <u>/ISAPI/Publish/ScheduleMgr/playSchedule/<ID>/capabilities</u> • Get, set or delete a specific schedule: GET, PUT, or DELETE <u>/ISAPI/Publish/ScheduleMgr/playSchedule/<ID></u>

4.16 Other Applications

4.16.1 Device/Server Settings

Door/Floor

Function	Description
Get door (floor) configuration capability	GET <i>/ISAPI/AccessControl/Door/param/<ID>/capabilities</i>
Get or set door (floor) parameters	GET or PUT <i>/ISAPI/AccessControl/Door/param/<ID></i>

Reader

Function	Description
Get reader configuration capability	GET <i>/ISAPI/AccessControl/CardReaderCfg/capabilities?format=json</i>
Get or set reader parameters	GET or PUT <i>/ISAPI/AccessControl/CardReaderCfg/<ID>?format=json</i>
NFC (Near-Field Communication) Function	<p>Get configuration capability of enabling or disabling NFC function Request URI: GET <i>/ISAPI/AccessControl/Configuration/NFCCfg/capabilities?format=json</i></p> <p>Get parameters of enabling or disabling NFC function Request URI: GET <i>/ISAPI/AccessControl/Configuration/NFCCfg?format=json</i></p> <p>Set parameters of enabling or disabling NFC function Request URI: PUT <i>/ISAPI/AccessControl/Configuration/NFCCfg?format=json</i></p>
RF (Radio Frequency) Card Recognition	<p>Get configuration capability of enabling or disabling RF card recognition Request URI: GET <i>/ISAPI/AccessControl/Configuration/RFCardCfg/capabilities?format=json</i></p> <p>Get parameters of enabling or disabling RF card recognition Request URI: GET <i>/ISAPI/AccessControl/Configuration/RFCardCfg?format=json</i></p> <p>Set parameters of enabling or disabling RF card recognition Request URI: PUT <i>/ISAPI/AccessControl/Configuration/RFCardCfg?format=json</i></p>

Access Controller

Function	Description
Get configuration capability of access controller	GET <i>/ISAPI/AccessControl/AcsCfg/capabilities?format=json</i>
Get or set access controller parameters	GET or PUT <i>/ISAPI/AccessControl/AcsCfg?format=json</i>

OSDP (Open Supervised Device Protocol) Card Reader

Function	Description
Get capability of getting OSDP card reader status	GET <i>/ISAPI/AccessControl/OSDPStatus/capabilities?format=json</i>
Get OSDP card reader status	GET <i>/ISAPI/AccessControl/OSDPStatus/<ID>?format=json</i>
Get capability of setting OSDP card reader ID	GET <i>/ISAPI/AccessControl/OSDPMModify/capabilities?format=json</i>
Set OSDP card reader ID	PUT <i>/ISAPI/AccessControl/OSDPMModify/<ID>?format=json</i>

Intelligent Identity Recognition Terminal

Function	Description
Get configuration capability of intelligent identity recognition terminal	GET <i>/ISAPI/AccessControl/IdentityTerminal/capabilities</i>
Get parameters of intelligent identity recognition terminal	GET <i>/ISAPI/AccessControl/IdentityTerminal</i>
Set parameters of intelligent identity recognition terminal	PUT <i>/ISAPI/AccessControl/IdentityTerminal</i>



After configuring the identity recognition parameters, when the ID card is swiped to recognize, the corresponding event information (`eventType` is "IDCardInfoEvent") will be uploaded in the message [*JSON_EventNotificationAlert_IDCardInfoEvent*](#).

Picture Storage Server

Function	Description
Get picture storage server capability	GET <i>/ISAPI/System/PictureServer/capabilities?format=json</i>
Get picture storage server parameters	GET <i>/ISAPI/System/PictureServer?format=json</i>
Set picture storage server parameters	PUT <i>/ISAPI/System/PictureServer?format=json</i>

4.16.2 Multi-Factor Authentication

Multi-factor authentication is to manage the cards by group and set the authentication for multiple cards of one access control point (door).

Mode Settings

Function	Description
Get configuration capability of multi-factor authentication mode	GET <i>/ISAPI/AccessControl/MultiCardCfg/capabilities?format=json</i>
Get or set parameters of multi-factor authentication mode	GET or PUT <i>/ISAPI/AccessControl/MultiCardCfg/<ID>?format=json</i>

Group Settings

Function	Description
Get group configuration capability	GET <i>/ISAPI/AccessControl/GroupCfg/capabilities?format=json</i>
Get or set group parameters	GET or PUT <i>/ISAPI/AccessControl/GroupCfg/<ID>?format=json</i>
Get capability of clearing group parameters	GET <i>/ISAPI/AccessControl/ClearGroupCfg/capabilities?format=json</i>
Clear group parameters	PUT <i>/ISAPI/AccessControl/ClearGroupCfg?format=json</i>

4.16.3 Multi-Door Interlocking

Multi-door interlocking is used to control the entry of persons to a secure area such as a clean room, where dust or small particles may be a problem. One rule is composed of at least two doors and only one door can be opened simultaneously.

Function	Description
Get configuration capability of multi-door interlocking	GET <u>/ISAPI/AccessControl/MultiDoorInterLockCfg/capabilities?format=json</u>
Get or set multi-door interlocking parameters	GET or PUT <u>/ISAPI/AccessControl/MultiDoorInterLockCfg?format=json</u>

4.16.4 M1 Card Encryption Authentication

M1 card encryption can improve the security level of authentication.

Function	Description
Get configuration capability of M1 card encryption authentication	GET <u>/ISAPI/AccessControl/M1CardEncryptCfg/capabilities</u>
Get or set parameters of M1 card encryption authentication	GET or PUT <u>/ISAPI/AccessControl/M1CardEncryptCfg</u>

4.16.5 Temperature Measurement

Temperature Measurement Area

Function	Request URI
Get the configuration capability of the temperature measurement area	GET <u>/ISAPI/AccessControl/temperatureMeasureAreaCfg/capabilities?format=json</u>
Get the parameters of the temperature measurement area	GET

Function	Request URI
	<u>/ISAPI/AccessControl/temperatureMeasureAreaCfg?format=json</u>
Set the parameters of the temperature measurement area	PUT <u>/ISAPI/AccessControl/temperatureMeasureAreaCfg?format=json</u>

Temperature Measurement Area Calibration

Function	Request URI
Get the calibration configuration capability of the temperature measurement area	GET <u>/ISAPI/AccessControl/temperatureMeasureAreaCalibration/capabilities?format=json</u>
Get the calibration parameters of the temperature measurement area	GET <u>/ISAPI/AccessControl/temperatureMeasureAreaCalibration?format=json</u>
Set the calibration parameters of the temperature measurement area	PUT <u>/ISAPI/AccessControl/temperatureMeasureAreaCalibration?format=json</u>

Temperature Measurement Settings

Function	Request URI
Get the configuration capability of temperature measurement parameters	GET <u>/ISAPI/AccessControl/temperatureMeasureCfg/capabilities?format=json</u>
Get temperature measurement parameters	GET <u>/ISAPI/AccessControl/temperatureMeasureCfg?format=json</u>
Set temperature measurement parameters	PUT <u>/ISAPI/AccessControl/temperatureMeasureCfg?format=json</u>

4.16.6 Configuration and Maintenance

Data Exporting and Importing

Function	Description
Export or import person permission data securely	<p>GET or POST <i>/ISAPI/AccessControl/userData?secretkey=</i></p> <p> Note To check whether the device supports exporting or importing person permission data securely, you can call <i>/ISAPI/AccessControl/capabilities</i> by GET method to get the functional capability of access control. The capability is returned in the message <i>XML Cap AccessControl</i>. If the device supports exporting person permission data securely, the node <isSupportUserDataExport> will be returned in the message and its value is "true"; if the device supports importing person permission data securely, the node <isSupportUserDataImport> will be returned in the message and its value is "true".</p>
Export maintenance data	<p>GET <i>/ISAPI/AccessControl/maintenanceData?secretkey=</i></p> <p> Note To check whether the device supports exporting the maintenance data, you can call <i>/ISAPI/AccessControl/capabilities</i> by GET method to get the functional capability of access control. The capability is returned in the message <i>XML Cap AccessControl</i>. If the device supports exporting the maintenance data, the node <isSupportMaintenanceDataExport> will be returned in the message and its value is "true".</p>

Access Control Status

Function	Description
Get capability of getting working status of access controller	GET <i>/ISAPI/AccessControl/AcsWorkStatus/capabilities?format=json</i>
Get working status of access controller	GET <i>/ISAPI/AccessControl/AcsWorkStatus?format=json</i>

Function	Description
Get capability of getting status of secure door control unit	GET <i>/ISAPI/AccessControl/DoorSecurityModule/moduleStatus/capabilities</i>
Get status of secure door control unit	GET <i>/ISAPI/AccessControl/DoorSecurityModule/moduleStatus</i>

Wiegand Settings

Function	Description
Get Wiegand configuration capability	GET <i>/ISAPI/AccessControl/WiegandCfg/capabilities</i>
Get or set Wiegand parameters	GET or PUT <i>/ISAPI/AccessControl/WiegandCfg/wiegandNo/<ID></i>
Get configuration capability of Wiegand rule	GET <i>/ISAPI/AccessControl/WiegandRuleCfg/capabilities</i>
Get or set Wiegand rule	GET or PUT <i>/ISAPI/AccessControl/WiegandRuleCfg</i>

Log Mode

Function	Description
Get configuration capability of log mode	GET <i>/ISAPI/AccessControl/LogModeCfg/capabilities?format=json</i>
Get or set log mode	GET or PUT <i>/ISAPI/AccessControl/LogModeCfg?format=json</i>

SMS (Short Message Service)

Function	Description
Get SMS configuration capability	GET <i>/ISAPI/AccessControl/SmsRelativeParam/capabilities?format=json</i>
Get or set SMS parameters	GET or PUT <i>/ISAPI/AccessControl/SmsRelativeParam?format=json</i>

Function	Description
Get capability of linking door permission to phone number	GET <u>/ISAPI/AccessControl/PhoneDoorRightCfg/capabilities?format=json</u>
Get or set parameters of linking door permission to phone number	GET or PUT <u>/ISAPI/AccessControl/PhoneDoorRightCfg/<ID>?format=json</u>

Event Optimization

Function	Description
Get configuration capability of event optimization	GET <u>/ISAPI/AccessControl/EventOptimizationCfg/capabilities?format=json</u>
Get or set event optimization parameters	GET or PUT <u>/ISAPI/AccessControl/EventOptimizationCfg?format=json</u>

Text of Audio Prompt for Authentication Results

Function	Description
Get text configuration capability of audio prompt for authentication results	GET <u>/ISAPI/AccessControl/Verification/ttsText/capabilities?format=json</u>
Get or set text parameters of audio prompt for authentication results	GET or PUT <u>/ISAPI/AccessControl/Verification/ttsText?format=json</u>

Face Picture Comparison Condition

Function	Description
Get condition configuration capability of face picture comparison	GET <u>/ISAPI/AccessControl/FaceCompareCond/capabilities</u>
Get or set condition parameters of face picture comparison	GET or PUT <u>/ISAPI/AccessControl/FaceCompareCond</u>

ID Card Blocklist

Function	Description
Get capability of applying ID card blocklist	GET <i>/ISAPI/AccessControl/IDBlackListCfg/capabilities</i>
Apply ID card blocklist	PUT <i>/ISAPI/AccessControl/IDBlackListCfg</i>
Get ID card blocklist template	GET <i>/ISAPI/AccessControl/IDBlackListCfg/template?format=json</i>

Capture Triggering Settings

Function	Description
Get capability of getting capture triggering parameters	GET <i>/ISAPI/AccessControl/SnapConfig/capabilities</i>
Get capture triggering parameters	GET <i>/ISAPI/AccessControl/SnapConfig</i>

Door Lock Status

Function	Description
Get configuration capability of door lock status when the device is powered off	GET <i>/ISAPI/AccessControl/Configuration/lockType/capabilities?format=json</i>
Get or set door lock status when the device is powered off	GET or PUT <i>/ISAPI/AccessControl/Configuration/lockType?format=json</i>

Card No. Authentication Mode

Function	Description
Get configuration capability of card No. authentication mode	GET <i>/ISAPI/AccessControl/CardVerificationRule/capabilities?format=json</i>
Get or set parameters of card No. authentication mode	GET or PUT <i>/ISAPI/AccessControl/CardVerificationRule?format=json</i>
Get switching progress and configuration result of card No. authentication mode	GET <i>/ISAPI/AccessControl/CardVerificationRule/progress?format=json</i>

Active Infrared Intrusion Detection

Function	Description
Get Configuration Capability of Active Infrared Intrusion Detection	GET <u>/ISAPI/AccessControl/Configuration/IRCfg/capabilities?format=json</u>
Get Parameters of Active Infrared Intrusion Detection	GET <u>/ISAPI/AccessControl/Configuration/IRCfg?format=json</u>
Set Parameters of Active Infrared Intrusion Detection	PUT <u>/ISAPI/AccessControl/Configuration/IRCfg?format=json</u>

Additional Person Information

Function	Request URI
Get the configuration capability of the name of the additional person information	GET <u>/ISAPI/AccessControl/personInfoExtendName/capabilities?format=json</u>
Get or set the name of the additional person information	GET or PUT <u>/ISAPI/AccessControl/personInfoExtendName?format=json</u>

Privacy Settings

Function	Request URI
Get the capability of clearing pictures in the device	GET <u>/ISAPI/AccessControl/ClearPictureCfg/capabilities?format=json</u>
Clear pictures in the device	PUT <u>/ISAPI/AccessControl/ClearPictureCfg?format=json</u>
Get the storage configuration capability of access control events	GET <u>/ISAPI/AccessControl/AcsEvent/StorageCfg/capabilities?format=json</u>
Get or set storage parameters of access control events	GET or PUT <u>/ISAPI/AccessControl/AcsEvent/StorageCfg?format=json</u>

Getting Events Actively

Function	Request URI
Get the capability of getting ID card swiping events actively	GET <i>/ISAPI/AccessControl/IDCardInfoEvent/capabilities?format=json</i>
Get ID card swiping events actively	POST <i>/ISAPI/AccessControl/IDCardInfoEvent?format=json</i>
Get the capability of getting face temperature screening events actively	GET <i>/ISAPI/AccessControl/FaceTemperatureEvent/capabilities?format=json</i>
Get face temperature screening events actively	POST <i>/ISAPI/AccessControl/FaceTemperatureEvent?format=json</i>
Get the capability of getting QR code scanning events actively	GET <i>/ISAPI/AccessControl/QRCodeEvent/capabilities?format=json</i>
Get QR code scanning events actively	POST <i>/ISAPI/AccessControl/QRCodeEvent?format=json</i>

Health Code

Function	Request URI
Get the configuration capability of the health code	GET <i>/ISAPI/AccessControl/healthCodeCfg/capabilities?format=json</i>
Get or set the health code parameters	GET or PUT <i>/ISAPI/AccessControl/healthCodeCfg?format=json</i>
Get the configuration capability of the health code display parameters	GET <i>/ISAPI/AccessControl/showHealthCodeCfg/capabilities?format=json</i>
Get or set the health code display parameters	GET or PUT <i>/ISAPI/AccessControl/showHealthCodeCfg?format=json</i>

Black Body

Function	Request URI
Get the configuration capability of the black body	GET <u>/ISAPI/AccessControl/blackObject/capabilities?format=json</u>
Get or set the black body parameters	GET or PUT <u>/ISAPI/AccessControl/blackObject?format=json</u>

Custom Audio File

Function	Request URI
Get the capability of configuring the custom audio file	GET <u>/ISAPI/AccessControl/customAudio/capabilities?format=json</u>
Import the custom audio file	POST <u>/ISAPI/AccessControl/customAudio/addCustomAudio?format=json</u>
Delete the custom audio file	POST <u>/ISAPI/AccessControl/customAudio/deleteCustomAudio?format=json</u>
Search for the applying status of a specified custom audio file	POST <u>/ISAPI/AccessControl/customAudio/searchCustomAudioStatus?format=json</u>

Logo Management

Function	Request URI
Get the capability of configuring logo parameters	GET <u>/ISAPI/AccessControl/LOGOCfg/capabilities?format=json</u>
Import the logo	POST <u>/ISAPI/AccessControl/LOGOCfg?format=json</u>
Delete the logo	DELETE <u>/ISAPI/AccessControl/LOGOCfg?format=json</u>

Access Control via Bluetooth

Function	Request URI
Get the capability of configuring bluetooth parameters of access control	GET <u>/ISAPI/AccessControl/bluetooth/capabilities?format=json</u>
Get or set the bluetooth parameters of access control	GET or PUT <u>/ISAPI/AccessControl/bluetooth?format=json</u>
Get the capability of configuring the bluetooth encryption information	GET <u>/ISAPI/AccessControl/bluetoothEncryptionInfo/capabilities?format=json</u>
Get or set the bluetooth encryption information	GET or PUT <u>/ISAPI/AccessControl/bluetoothEncryptionInfo?format=json</u>

Appendix A. Request URIs

A.1 /ISAPI/AccessControl/AcsCfg/capabilities?format=json

Get the configuration capability of the access controller.

Request URI Definition

Table A-1 GET /ISAPI/AccessControl/AcsCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the access controller.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_AcsCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.2 /ISAPI/AccessControl/AcsCfg?format=json

Operations about the configuration of the access controller.

Request URI Definition

Table A-2 GET /ISAPI/AccessControl/AcsCfg?format=json

Method	GET
Description	Get the configuration parameters of the access controller.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_AcsCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-3 PUT /ISAPI/AccessControl/AcsCfg?format=json

Method	PUT
Description	Set the parameters of the access controller.

Query	format: determine the format of request or response message.
Request	<u>JSON_AcsCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.3 /ISAPI/AccessControl/AcsEvent/capabilities?format=json

Get the capability of searching for access control events

Request URI Definition

Table A-4 GET /ISAPI/AccessControl/AcsEvent/capabilities?format=json

Method	GET
Description	Get the capability of searching for access control events.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_AcsEvent</u> Failed: <u>JSON_ResponseStatus</u>

A.4 /ISAPI/AccessControl/AcsEvent/StorageCfg/capabilities?format=json

Get the storage configuration capability of access control events.

Request URI Definition

Table A-5 GET /ISAPI/AccessControl/AcsEvent/StorageCfg/capabilities?format=json

Method	GET
Description	Get the storage configuration capability of access control events.
Query	format: determine the format of request or response message.

Request	None.
Response	Succeeded: <u>JSON_EventStorageCfgCap</u> Failed: <u>JSON_ResponseStatus</u>

A.5 /ISAPI/AccessControl/AcsEvent/StorageCfg?format=json

Get or set the storage parameters of access control events.

Request URI Definition

Table A-6 GET /ISAPI/AccessControl/AcsEvent/StorageCfg?format=json

Method	GET
Description	Get the storage parameters of access control events.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_EventStorageCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-7 PUT /ISAPI/AccessControl/AcsEvent/StorageCfg?format=json

Method	PUT
Description	Set the storage parameters of access control events.
Query	format: determine the format of request or response message.
Request	<u>JSON_EventStorageCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.6 /ISAPI/AccessControl/AcsEvent?format=json

Search for access control events.

Request URI Definition

Table A-8 POST /ISAPI/AccessControl/AcsEvent?format=json

Method	POST
Description	Search for access control events.
Query	format: determine the format of request or response message.
Request	<u>JSON_AcsEventCond</u>
Response	Succeeded: <u>JSON_AcsEvent</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- The recommended timeout of this URI is 10 seconds.
- If the response message contains picture data, the picture data will be returned by boundary method; otherwise, the response message in JSON format will be returned directly.

Example

Sample Response Message with Picture Data

```
--MIME_boundary
Content-Type: application/json
Content-Length:480

{
    "AcsEvent": {
        "searchID": "",
        "responseStatusStrg": "OK",
        "numOfMatches": 1,
        "totalMatches": 1,
        "InfoList": [
            {
                "major": 1,
                "minor": 1,
                "time": "2016-12-12T17:30:08+08:00",
                "netUser": "",
                "remoteHostAddr": "",
                "cardNo": "",
                "cardType": 1,
                "whiteListNo": 1,
                "reportChannel": 1,
                "cardReaderKind": 1,
                "cardReaderNo": 1,
                "doorNo": 1,
                "verifyNo": 1,
                "alarmInNo": 1,
                "alarmOutNo": 1,
                "caseSensorNo": 1
            }
        ]
    }
}
```

```

        "RS485No":1,
        "multiCardGroupNo":1,
        "accessChannel":1,
        "deviceNo":1,
        "distractControlNo":1,
        "employeeNoString":"",
        "localControllerID":1,
        "InternetAccess":1,
        "type":1,
        "MACAddr":"",
        "swipeCardType":1,
        "serialNo":1,
        "channelControllerID":1,
        "channelControllerLampID":1,
        "channelControllerIRAdaptorID":1,
        "channelControllerIREmitterID":1,
        "userType":"normal",
        "currentVerifyMode":"",
        "attendanceStatus":"",
        "statusValue":1,
        "pictureURL":"",
        "picturesNumber":1,
        "filename":"picture1"
    ],
}
}

--MIME_boundary
Content-Disposition: form-data; filename="picture1"; //Picture data
Content-Type:image/jpeg
Content-Length:12345

fgagashgshdasdad...
--MIME_boundary--

```

A.7 /ISAPI/AccessControl/AcsEventTotalNum/capabilities?format=json

Get the capability of getting total number of access control events by specific conditions.

Request URI Definition

Table A-9 GET /ISAPI/AccessControl/AcsEventTotalNum/capabilities?format=json

Method	GET
Description	Get the capability of getting total number of access control events by specific conditions.
Query	format: determine the format of request or response message.

	terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_AcsEventTotalNum</u> Failed: <u>JSON_ResponseStatus</u>

A.8 /ISAPI/AccessControl/AcsEventTotalNum?format=json

Get the total number of access control events by specific conditions.

Request URI Definition

Table A-10 POST /ISAPI/AccessControl/AcsEventTotalNum?format=json

Method	POST
Description	Get the total number of access control events by specific conditions.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	<u>JSON_AcsEventTotalNumCond</u>
Response	Succeeded: <u>JSON_AcsEventTotalNum</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- The recommended timeout is 30s.
- This URI is not supported by integration of information release system.

A.9 /ISAPI/AccessControl/AcsWorkStatus/capabilities?format=json

Get the capability of getting the working status of the access controller.

Request URI Definition

Table A-11 GET /ISAPI/AccessControl/AcsWorkStatus/capabilities?format=json

Method	GET
Description	Get the capability of getting the working status of the access controller.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_AcsWorkStatus</u> Failed: <u>JSON_ResponseStatus</u>

A.10 /ISAPI/AccessControl/AcsWorkStatus?format=json

Get the working status of the access controller.

Request URI Definition

Table A-12 GET /ISAPI/AccessControl/AcsWorkStatus?format=json

Method	GET
Description	Get the working status of the access controller.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_AcsWorkStatus</u> Failed: <u>JSON_ResponseStatus</u>

A.11 /ISAPI/AccessControl/AntiSneakCfg/capabilities?format=json

Get the anti-passing back configuration capability.

Request URI Definition

Table A-13 GET /ISAPI/AccessControl/AntiSneakCfg/capabilities?format=json

Method	GET
Description	Get the anti-passing back configuration capability.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_AntiSneakCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.12 /ISAPI/AccessControl/AntiSneakCfg?format=json

Operations about anti-passing back configuration.

Request URI Definition

Table A-14 GET /ISAPI/AccessControl/AntiSneakCfg?format=json

Method	GET
Description	Get the anti-passing back configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_AntiSneakCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-15 PUT /ISAPI/AccessControl/AntiSneakCfg?format=json

Method	PUT
Description	Set the anti-passing back parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_AntiSneakCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.13 /ISAPI/AccessControl/Attendance/planTemplate/<TemplateNo>?format=json

Get or set the parameters of the attendance schedule template.

Request URI Definition

Table A-16 GET /ISAPI/AccessControl/Attendance/planTemplate/<TemplateNo>?format=json

Method	GET
Description	Get the parameters of the attendance schedule template.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_AttendancePlanTemplate</i> Failed: <i>JSON_ResponseStatus</i>

Table A-17 PUT /ISAPI/AccessControl/Attendance/planTemplate/<TemplateNo>?format=json

Method	PUT
Description	Set the parameters of the attendance schedule template.
Query	format: determine the format of request or response message.
Request	<i>JSON_AttendancePlanTemplate</i>
Response	<i>JSON_ResponseStatus</i>

Remarks

The <TemplateNo> in the request URI refers to the attendance schedule template No.

A.14 /ISAPI/AccessControl/Attendance/planTemplate/capabilities? format=json

Get the configuration capability of the attendance schedule template.

Request URI Definition

Table A-18 GET /ISAPI/AccessControl/Attendance/planTemplate/capabilities?format=json

Method	GET
Description	Get the configuration capability of the attendance schedule template.
Query	format: determine the format of request or response message.

Request	None.
Response	Succeeded: <i>JSON_AttendancePlanTemplateCap</i> Failed: <i>JSON_ResponseStatus</i>

A.15 /ISAPI/AccessControl/Attendance/planTemplate?format=json

Get the list of attendance schedule templates.

Request URI Definition

Table A-19 GET /ISAPI/AccessControl/Attendance/planTemplate?format=json

Method	GET
Description	Get the list of attendance schedule templates.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_AttendancePlanTemplateList</i> Failed: <i>JSON_ResponseStatus</i>

A.16 /ISAPI/AccessControl/Attendance/weekPlan/<PlanNo>?format=json

Get or set the parameters of the week attendance schedule.

Request URI Definition

Table A-20 GET /ISAPI/AccessControl/Attendance/weekPlan/<PlanNo>?format=json

Method	GET
Description	Get the parameters of the week attendance schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_AttendanceWeekPlan</i> Failed: <i>JSON_ResponseStatus</i>

Table A-21 PUT /ISAPI/AccessControl/Attendance/weekPlan/<PlanNo>?format=json

Method	PUT
Description	Set the parameters of the week attendance schedule.
Query	format: determine the format of request or response message.
Request	<u>JSON_AttendanceWeekPlan</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <PlanNo> in the request URI refers to the attendance schedule No.

A.17 /ISAPI/AccessControl/Attendance/weekPlan/capabilities? format=json

Get the configuration capability of the week attendance schedule.

Request URI Definition

Table A-22 GET /ISAPI/AccessControl/Attendance/weekPlan/capabilities?format=json

Method	GET
Description	Get the configuration capability of the week attendance schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_AttendanceWeekPlanCap</u> Failed: <u>JSON_ResponseStatus</u>

A.18 /ISAPI/AccessControl/blackObject/capabilities?format=json

Get the configuration capability of the black body.

Request URI Definition

Table A-23 GET /ISAPI/AccessControl/blackObject/capabilities?format=json

Method	GET
Description	Get the configuration capability of the black body.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_BlackBodyCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.19 /ISAPI/AccessControl/blackObject?format=json

Get or set the black body parameters.

Request URI Definition

Table A-24 GET /ISAPI/AccessControl/blackObject?format=json

Method	GET
Description	Get the black body parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_BlackBodyCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-25 PUT /ISAPI/AccessControl/blackObject?format=json

Method	PUT
Description	Set the black body parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_BlackBodyCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.20 /ISAPI/AccessControl/bluetooth/capabilities?format=json

Get the capability of configuring bluetooth parameters of access control.

Request URI Definition

Table A-26 GET /ISAPI/AccessControl/bluetooth/capabilities?format=json

Method	GET
Description	Get the capability of configuring bluetooth parameters of access control.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_BluetoothCfg</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

To check whether the device supports bluetooth configuration of access control, you can call `/ISAPI/AccessControl/capabilities` by GET method to get the access control capability `XML_Cap_AccessControl`. If the capability message contains the node `<isSupportBluetooth>` and its value is true, it indicates that the device supports bluetooth configuration of access control.

A.21 /ISAPI/AccessControl/bluetooth?format=json

Get or set the bluetooth parameters of access control.

Request URI Definition

Table A-27 GET /ISAPI/AccessControl/bluetooth?format=json

Method	GET
Description	Get the bluetooth parameters of access control.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_BluetoothCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-28 PUT /ISAPI/AccessControl/bluetooth?format=json

Method	PUT
Description	Set the bluetooth parameters of access control.

Query	format: determine the format of request or response message.
Request	<u>JSON_BluetoothCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

To check whether the device supports bluetooth configuration of access control, you can call `/ISAPI/AccessControl/capabilities` by GET method to get the access control capability `XML_Cap_AccessControl`. If the capability message contains the node `<isSupportBluetooth>` and its value is true, it indicates that the device supports bluetooth configuration of access control.

A.22 /ISAPI/AccessControl/bluetoothEncryptionInfo/capabilities?format=json

Get the capability of configuring the bluetooth encryption information.

Request URI Definition

Table A-29 GET /ISAPI/AccessControl/bluetoothEncryptionInfo/capabilities?format=json

Method	GET
Description	Get the capability of configuring the bluetooth encryption information.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_BluetoothEncryptionInfoCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.23 /ISAPI/AccessControl/bluetoothEncryptionInfo?format=json

Get or set the bluetooth encryption information.

Request URI Definition

Table A-30 GET /ISAPI/AccessControl/bluetoothEncryptionInfo?format=json

Method	GET
Description	Get the bluetooth encryption information.

Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the response message, the node authData , vector , and employeeNo should be encrypted. iv: the initialization vector, and it is required when security is 1 or 2.
Request	None.
Response	Succeeded: <u>JSON_BluetoothEncryptionInfoCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-31 PUT /ISAPI/AccessControl/bluetoothEncryptionInfo?format=json

Method	PUT
Description	Set the bluetooth encryption information.
Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the request message, the node authData , vector , and employeeNo should be encrypted. iv: the initialization vector, and it is required when security is 1 or 2.
Request	<u>JSON_BluetoothEncryptionInfoCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

By default there is no bluetooth encryption information in the device. If the bluetooth encryption information is not configured for the device, the device cannot communicate with the mobile phone via bluetooth.

A.24 /ISAPI/AccessControl/capabilities

Get the functional capability of access control.

Request URI Definition

Table A-32 GET /ISAPI/AccessControl/capabilities

Method	GET
Description	Get the functional capability of access control.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_AccessControl</i> Failed: <i>XML_ResponseStatus</i>

A.25 /ISAPI/AccessControl/CaptureCardInfo/capabilities?format=json

Get the capability of collecting card information.

Request URI Definition

Table A-33 GET /ISAPI/AccessControl/CaptureCardInfo/capabilities?format=json

Method	GET
Description	Get the capability of collecting card information.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_CardInfoCap</i> Failed: <i>JSON_ResponseStatus</i>

A.26 /ISAPI/AccessControl/CaptureCardInfo?format=json

Collect card information.

Request URI Definition

Table A-34 GET /ISAPI/AccessControl/CaptureCardInfo?format=json

Method	GET
Description	Collect card information by the card reading module of the device.

Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the value of the field cardNo should be encrypted. iv: the initialization vector, and it is required when security is 1 or 2.
Request	None.
Response	Succeeded: <u>JSON_CardInfo_Collection</u> Failed: <u>JSON_ResponseStatus</u>

A.27 /ISAPI/AccessControl/CaptureFaceData

Collect face picture information.

Request URI Definition

Table A-35 POST /ISAPI/AccessControl/CaptureFaceData

Method	POST
Description	Collect face picture information.
Query	None.
Request	<u>XML_CaptureFaceDataCond</u>
Response	Succeeded: <u>XML_CaptureFaceData</u> Failed: <u>XML_ResponseStatus</u>

Remarks

This API is allowed to return collected face pictures directly, and the blocking time cannot be too long (the timeout value is 5s).

Example

Interaction When No Face Data is Collected

```
POST /ISAPI/AccessControl/CaptureFaceData
Accept: text/html, application/xhtml+xml,
Accept-Language: zh-CN
Content-Type: application/xml
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/
```

```
5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

<CaptureFaceDataCond version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
<captureInfrared>true</captureInfrared>
<dataType><!--input "binary" or "url" here--></dataType>
</CaptureFaceDataCond>

-----
-----

HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type: application/xml; charset="UTF-8"
Content-Length: text_length

<CaptureFaceData version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
<captureProgress>0</captureProgress>
</CaptureFaceData>
```

Example

Interaction by URI

```
POST /ISAPI/AccessControl/CaptureFaceData
Accept: text/html, application/xhtml+xml,
Accept-Language: zh-CN
Content-Type: application/xml
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

<CaptureFaceDataCond version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
<captureInfrared>true</captureInfrared>
</CaptureFaceDataCond>

-----
-----

HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type: application/xml; charset="UTF-8"
Content-Length: text_length
```

```
<CaptureFaceData version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
<faceDataURL>url_string</faceDataURL>
<captureProgress>100</captureProgress>
<infraredFaceDataURL>url_string</infraredFaceDataURL>
</CaptureFaceData>
```

Example

Interaction with Binary Data

```
POST /ISAPI/AccessControl/CaptureFaceData
Accept: text/html, application/xhtml+xml,
Accept-Language: zh-CN
Content-Type: application/xml
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

<CaptureFaceDataCond version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
<captureInfrared>true</captureInfrared>
<dataType>binary</dataType>
</CaptureFaceDataCond>

-----
-----

HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type: multipart/form-data; boundary=<frontier>
Content-Length: all_length

--<frontier>
Content-Type: application/xml; charset="UTF-8"
Content-Length: text_length

<CaptureFaceData/>
--<frontier>
Content-Disposition: form-data; name="FaceData"; filename="FaceData.jpg"
Content-Type: image/jpeg
Content-Length: image_length

[picture data]
--<frontier>
Content-Disposition: form-data; name="InfraredFaceData";
filename="InfraredFaceData.jpg"
Content-Type: image/jpeg
Content-Length: image_length
```

```
[picture data]
--<frontier>--
```

A.28 /ISAPI/AccessControl/CaptureFaceData/capabilities

Get the capability of collecting face picture information.

Request URI Definition

Table A-36 GET /ISAPI/AccessControl/CaptureFaceData/capabilities

Method	GET
Description	Get the capability of collecting face picture information.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_CaptureFaceData</u> Failed: <u>XML_ResponseStatus</u>

A.29 /ISAPI/AccessControl/CaptureFaceData/Progress

Get the progress of collecting face picture information.

Request URI Definition

Table A-37 GET /ISAPI/AccessControl/CaptureFaceData/Progress

Method	GET
Description	Get the progress of collecting face picture information.
Query	None.
Request	None.
Response	Succeeded: <u>XML_CaptureFaceData</u> Failed: <u>XML_ResponseStatus</u>

A.30 /ISAPI/AccessControl/CaptureFaceData/Progress/capabilities

Get capability of getting face picture collection progress.

Request URI Definition

Table A-38 GET /ISAPI/AccessControl/CaptureFaceData/Progress/capabilities

Method	GET
Description	Get capability of getting face picture collection progress.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_CaptureFaceData</u> Failed: <u>XML_ResponseStatus</u>

A.31 /ISAPI/AccessControl/CaptureFingerPrint

Collect fingerprint information.

Request URI Definition

Table A-39 POST /ISAPI/AccessControl/CaptureFingerPrint

Method	POST
Description	Collect fingerprint information.
Query	None.
Request	<u>XML_CaptureFingerPrintCond</u>
Response	Succeeded: <u>XML_CaptureFingerPrint</u> Failed: <u>XML_ResponseStatus</u>

A.32 /ISAPI/AccessControl/CaptureFingerPrint/capabilities

Get the fingerprint collection capability.

Request URI Definition

Table A-40 GET /ISAPI/AccessControl/CaptureFingerPrint/capabilities

Method	GET
Description	Get the fingerprint collection capability.

Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_CaptureFingerPrint</u> Failed: <u>XML_ResponseStatus</u>

A.33 /ISAPI/AccessControl/CaptureIDInfo/capabilities?format=json

Get the capability of collecting ID card information.

Request URI Definition

Table A-41 GET /ISAPI/AccessControl/CaptureIDInfo/capabilities?format=json

Method	GET
Description	Get the capability of collecting ID card information.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_IdentityInfoCap</u> Failed: <u>JSON_ResponseStatus</u>

A.34 /ISAPI/AccessControl/CaptureIDInfo?format=json

Collect ID card information.

Request URI Definition

Table A-42 POST /ISAPI/AccessControl/CaptureIDInfo?format=json

Method	POST
Description	Collect ID card information.
Query	security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the value of the field IDCardNo should be encrypted.

	iv: the initialization vector, and it is required when security is 1 or 2. format: determine the format of request or response message.
Request	<u>JSON_IdentityInfoCond</u>
Response	<u>JSON_IdentityInfo</u>

A.35 /ISAPI/AccessControl/CapturePresetParam/capabilities?format=json

Get the configuration capability of online collection preset parameters.

Request URI Definition

Table A-43 GET /ISAPI/AccessControl/CapturePresetParam/capabilities?format=json

Method	GET
Description	Get the configuration capability of online collection preset parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CapturePresetCap</u> Failed: <u>JSON_ResponseStatus</u>

A.36 /ISAPI/AccessControl/CapturePresetParam?format=json

Get or set the online collection preset parameters.

Request URI Definition

Table A-44 GET /ISAPI/AccessControl/CapturePresetParam?format=json

Method	GET
Description	Get the online collection preset parameters.
Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message

	<p>are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the value of the field name should be encrypted.</p> <p>iv: the initialization vector, and it is required when security is 1 or 2.</p>
Request	None.
Response	Succeeded: <u>JSON_CapturePreset</u> Failed: <u>JSON_ResponseStatus</u>

Table A-45 PUT /ISAPI/AccessControl/CapturePresetParam?format=json

Method	PUT
Description	Set the online collection preset parameters.
Query	<p>format: determine the format of request or response message.</p> <p>security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the value of the field name should be encrypted.</p> <p>iv: the initialization vector, and it is required when security is 1 or 2.</p>
Request	<u>JSON_CapturePreset</u>
Response	<u>JSON_ResponseStatus</u>

A.37 /ISAPI/AccessControl/CaptureRule/capabilities?format=json

Get the configuration capability of online collection rules.

Request URI Definition

Table A-46 GET /ISAPI/AccessControl/CaptureRule/capabilities?format=json

Method	GET
Description	Get the configuration capability of online collection rules.
Query	format: determine the format of request or response message.

Request	None.
Response	Succeeded: <u>JSON_CaptureRuleCap</u> Failed: <u>JSON_ResponseStatus</u>

A.38 /ISAPI/AccessControl/CaptureRule?format=json

Get or set the parameters of online collection rules.

Request URI Definition

Table A-47 GET /ISAPI/AccessControl/CaptureRule?format=json

Method	GET
Description	Get the parameters of online collection rules.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CaptureRule</u> Failed: <u>JSON_ResponseStatus</u>

Table A-48 PUT /ISAPI/AccessControl/CaptureRule?format=json

Method	PUT
Description	Set the parameters of online collection rules.
Query	format: determine the format of request or response message.
Request	<u>JSON_CaptureRule</u>
Response	<u>JSON_ResponseStatus</u>

A.39 /ISAPI/AccessControl/CardInfo/capabilities?format=json

Get the card management capability.

Request URI Definition

Table A-49 GET /ISAPI/AccessControl/CardInfo/capabilities?format=json

Method	GET
Description	Get the card management capability.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_CardInfo</u> Failed: <u>JSON_ResponseStatus</u>

A.40 /ISAPI/AccessControl/CardInfo/Count?format=json

Get the total number of the added cards.

Request URI Definition

Table A-50 GET /ISAPI/AccessControl/CardInfo/Count?format=json

Method	GET
Description	Get the total number of the added cards.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_CardInfoCount</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.41 /ISAPI/AccessControl/CardInfo/Count? format=json&employeeNo=<ID>

Get the number of cards linked with a specific person.

Request URI Definition

Table A-51 GET /ISAPI/AccessControl/CardInfo/Count?format=json&employeeNo=<ID>

Method	GET
Description	Get the number of cards linked with a specific person.
Query	format : determine the format of request or response message. employeeNo : employee No.
Request	None.
Response	Succeeded: <u>JSON_CardInfoCount</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the actual person ID or employee No.

A.42 /ISAPI/AccessControl/CardInfo/Delete?format=json

Delete cards.

Request URI Definition

Table A-52 PUT /ISAPI/AccessControl/CardInfo/Delete?format=json

Method	PUT
Description	Delete cards.
Query	format : determine the format of request or response message.
Request	<u>JSON_CardInfoDelCond</u>
Response	<u>JSON_ResponseStatus</u>

A.43 /ISAPI/AccessControl/CardInfo/Modify?format=json

Edit card information.

Request URI Definition

Table A-53 PUT /ISAPI/AccessControl/CardInfo/Modify?format=json

Method	PUT
Description	Edit card information.
Query	format: determine the format of request or response message.
Request	<u>JSON_CardInfo</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The **employeeNo** and **cardNo** in the request message [JSON_CardInfo](#) cannot be edited by calling this URI. If the **cardNo** needs to be edited, you should firstly delete this card and then create a new one.

A.44 /ISAPI/AccessControl/CardInfo/Record?format=json

Add cards and link them with a person.

Request URI Definition

Table A-54 POST /ISAPI/AccessControl/CardInfo/Record?format=json

Method	POST
Description	Add cards and link them with a person.
Query	format: determine the format of request or response message.
Request	<u>JSON_CardInfo</u>
Response	<u>JSON_ResponseStatus</u>

A.45 /ISAPI/AccessControl/CardInfo/Search?format=json

Search for cards.

Request URI Definition

Table A-55 POST /ISAPI/AccessControl/CardInfo/Search?format=json

Method	POST
Description	Search for cards.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	<u>JSON_CardInfoSearchCond</u>
Response	<u>JSON_CardInfoSearch</u>

A.46 /ISAPI/AccessControl/CardInfo/SetUp?format=json

Set card information.

Request URI Definition

Table A-56 PUT /ISAPI/AccessControl/CardInfo/SetUp?format=json

Method	PUT
Description	Set card information.
Query	format: determine the format of request or response message.
Request	<u>JSON_CardInfo</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

- If the device has checked that the card does not exist according to the card No., the card information will be added.
- If the device has checked that the card already exists according to the card No., the card information will be edited.
- If you want to delete a card for a person, you should set the **employeeNo** and **cardNo**, and set the **deleteCard** to "true" in the message [JSON_CardInfo](#). The success response message will be

returned no matter whether the card exists or not. Deleting the card will only delete the card's information and will not delete the linked person information.

- If you want to delete all cards for a person, you should set the **employeeNo**, and set the **deleteCard** to "true" in the message ***JSON_CardInfo***. The success response message will be returned no matter whether the person exists or not or whether the person has cards or not. Deleting cards will only delete the cards' information and will not delete the linked person information.

A.47 /ISAPI/AccessControl/CardOperations/capabilities?format=json

Get card operation capability.

Request URI Definition

Table A-57 GET /ISAPI/AccessControl/CardOperations/capabilities?format=json

Method	GET
Description	Get card operation capability.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_CardOperationsCap</i> Failed: <i>JSON_ResponseStatus</i>

A.48 /ISAPI/AccessControl/CardOperations/cardIssueStatus?format=json

Get the smart card issuing status.

Request URI Definition

Table A-58 GET /ISAPI/AccessControl/CardOperations/cardIssueStatus?format=json

Method	GET
Description	Get the smart card issuing status.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_CardIssueStatus</i> Failed: <i>JSON_ResponseStatus</i>

A.49 /ISAPI/AccessControl/CardOperations/cardParam?format=json

Set card parameters (only available for CPU card).

Request URI Definition

Table A-59 PUT /ISAPI/AccessControl/CardOperations/cardParam?format=json

Method	PUT
Description	Set card parameters (only available for CPU card).
Query	format: determine the format of request or response message.
Request	<u>JSON_CardParam</u>
Response	<u>JSON_ResponseStatus</u>

A.50 /ISAPI/AccessControl/CardOperations/clearData?format=json

Delete data from the card.

Request URI Definition

Table A-60 PUT /ISAPI/AccessControl/CardOperations/clearData?format=json

Method	PUT
Description	Delete data from the card.
Query	format: determine the format of request or response message.
Request	<u>JSON_ClearData</u>
Response	Succeeded: <u>JSON_ClearDataRes</u> Failed: <u>JSON_ResponseStatus</u>

A.51 /ISAPI/AccessControl/CardOperations/controlBlock?format=json

Change the control block of a specific section (only available for M1 card).

Request URI Definition

Table A-61 PUT /ISAPI/AccessControl/CardOperations/controlBlock?format=json

Method	PUT
Description	Change the control block of a specific section (only available for M1 card).
Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the values of the fields KeyA and KeyB should be encrypted. iv: the initialization vector, and it is required when security is 1 or 2.
Request	<u>JSON_ControlBlock</u>
Response	<u>JSON_ResponseStatus</u>

A.52 /ISAPI/AccessControl/CardOperations/customData/searchTask?format=json

Search for custom card information.

Request URI Definition

Table A-62 POST /ISAPI/AccessControl/CardOperations/customData/searchTask?format=json

Method	POST
Description	Search for custom card information.
Query	format: determine the format of request or response message.
Request	<u>JSON_CustomDataSearchCond</u>
Response	Succeeded: <u>JSON_CustomDataResult</u> Failed: <u>JSON_ResponseStatus</u>

A.53 /ISAPI/AccessControl/CardOperations/customData?format=json

Set custom card information.

Request URI Definition

Table A-63 PUT /ISAPI/AccessControl/CardOperations/customData?format=json

Method	PUT
Description	Set custom card information.
Query	format: determine the format of request or response message.
Request	<u>JSON_CustomData</u>
Response	Succeeded: <u>JSON_CustomDataRes</u> Failed: <u>JSON_ResponseStatus</u>

A.54 /ISAPI/AccessControl/CardOperations/dataBlock/<address>?format=json

Read or write data block (only available for M1 card).

Request URI Definition

Table A-64 GET /ISAPI/AccessControl/CardOperations/dataBlock/<address>?format=json

Method	GET
Description	Read data block (only available for M1 card).
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_DataBlock</u> Failed: <u>JSON_ResponseStatus</u>

Table A-65 PUT /ISAPI/AccessControl/CardOperations/dataBlock/<address>?format=json

Method	PUT
Description	Write data block (only available for M1 card).
Query	format: determine the format of request or response message.

Request	<u>JSON_DataBlock</u>
Response	<u>JSONResponseStatus</u>

Remarks

The <address> in the request URI refers to the block address, which is same as that in JSON_DataBlock.

A.55 /ISAPI/AccessControl/CardOperations/dataBlock/control?format=json

Do operations (i.e., plus, minus, copy, and paste) on the data block.

Request URI Definition

Table A-66 PUT /ISAPI/AccessControl/CardOperations/dataBlock/control?format=json

Method	PUT
Description	Do operations (i.e., plus, minus, copy, and paste) on the data block.
Query	format: determine the format of request or response message.
Request	<u>JSON_DataBlockCtrl</u>
Response	<u>JSONResponseStatus</u>

A.56 /ISAPI/AccessControl/CardOperations/dataTrans?format=json

Pass through the data package (only available for CPU card).

Request URI Definition

Table A-67 PUT /ISAPI/AccessControl/CardOperations/dataTrans?format=json

Method	PUT
Description	Pass through the data package (only available for CPU card).
Query	format: determine the format of request or response message.
Request	<u>JSON_DataTrans</u>
Response	<u>JSONResponseStatus</u>

A.57 /ISAPI/AccessControl/CardOperations/encryption?format=json

Set card encryption parameters (only available for CPU card).

Request URI Definition

Table A-68 PUT /ISAPI/AccessControl/CardOperations/encryption?format=json

Method	PUT
Description	Set card encryption parameters (only available for CPU card).
Query	format: determine the format of request or response message.
Request	<u>JSON_CardEncryption</u>
Response	<u>JSON_ResponseStatus</u> and tryTimes field (card encryption attempts)

A.58 /ISAPI/AccessControl/CardOperations/localIssueCfg?format=json

Get or set rule parameters for issuing smart cards.

Request URI Definition

Table A-69 GET /ISAPI/AccessControl/CardOperations/localIssueCfg?format=json

Method	GET
Description	Get rule parameters for issuing smart cards.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_localIssueCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-70 PUT /ISAPI/AccessControl/CardOperations/localIssueCfg?format=json

Method	PUT
Description	Set rule parameters for issuing smart cards.
Query	None.
Request	<u>JSON_localIssueCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.59 /ISAPI/AccessControl/CardOperations/localIssueRequest?format=json

Send a request for card issuing.

Request URI Definition

Table A-71 PUT /ISAPI/AccessControl/CardOperations/localIssueRequest?format=json

Method	PUT
Description	Send a request for card issuing.
Query	format: determine the format of request or response message.
Request	<u>JSON_LocalIssueRequest</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

- The API is not blocked and concurrently processing is not supported.
- The response message only indicates that sending the request for card issuing succeeded. The card issuing status and results are returned in the response message after the API [/ISAPI/AccessControl/CardOperations/localIssueRes?format=json](#) is called.

A.60 /ISAPI/AccessControl/CardOperations/localIssueRes?format=json

Get the current card issuing status and real-time card issuing results.

Request URI Definition

Table A-72 GET /ISAPI/AccessControl/CardOperations/localIssueRes?format=json

Method	GET
Description	Get the current card issuing status and real-time card issuing results.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_LocalIssueRes</u> Failed: <u>JSON_ResponseStatus</u>

A.61 /ISAPI/AccessControl/CardOperations/protocol?format=json

Set operation protocol type for the card (only available when applying card).

Request URI Definition

Table A-73 PUT /ISAPI/AccessControl/CardOperations/protocol?format=json

Method	PUT
Description	Set operation protocol type for the card (only available when applying card).
Query	format: determine the format of request or response message.
Request	<u>JSON_CardProto</u>
Response	<u>JSON_ResponseStatus</u>

A.62 /ISAPI/AccessControl/CardOperations/reset?format=json

Reset card parameters (only available for CPU card).

Request URI Definition

Table A-74 GET /ISAPI/AccessControl/CardOperations/reset?format=json

Method	GET
Description	Reset card parameters (only available for CPU card).
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CardResetResponse</u> Failed: <u>JSON_ResponseStatus</u>

A.63 /ISAPI/AccessControl/CardOperations/sectionEncryption? format=json

Set the encryption parameters of a specific section (only available for M1 card).

Request URI Definition

Table A-75 PUT /ISAPI/AccessControl/CardOperations/sectionEncryption?format=json

Method	PUT
Description	Set the encryption parameters of a specific section (only available for M1 card).
Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the values of the fields password , KeyA , and KeyB should be encrypted. iv: the initialization vector, and it is required when security is 1 or 2.
Request	<u>JSON_SectionEncryption</u>
Response	<u>JSON_ResponseStatus</u>

A.64 /ISAPI/AccessControl/CardOperations/verification?format=json

Verify the password of the encrypted section (only available for M1 card).

Request URI Definition

Table A-76 PUT /ISAPI/AccessControl/CardOperations/verification?format=json

Method	PUT
Description	Verify the password of the encrypted section (only available for M1 card).
Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the value of the field password should be encrypted.

	iv: the initialization vector, and it is required when security is 1 or 2.
Request	<u>JSON_Verification</u>
Response	<u>JSON_ResponseStatus</u>

A.65 /ISAPI/AccessControl/CardReaderAntiSneakCfg/<ID>?format=json

Operations about the anti-passing back configuration of a specified card reader.

Request URI Definition

Table A-77 GET /ISAPI/AccessControl/CardReaderAntiSneakCfg/<ID>?format=json

Method	GET
Description	Get the anti-passing back configuration parameters of a specified card reader.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CardReaderAntiSneakCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-78 PUT /ISAPI/AccessControl/CardReaderAntiSneakCfg/<ID>?format=json

Method	PUT
Description	Set the anti-passing back parameters of a specified card reader.
Query	format: determine the format of request or response message.
Request	<u>JSON_CardReaderAntiSneakCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the card reader No.

A.66 /ISAPI/AccessControl/CardReaderAntiSneakCfg/capabilities?format=json

Get the anti-passing back configuration capability of card readers.

Request URI Definition

Table A-79 GET /ISAPI/AccessControl/CardReaderAntiSneakCfg/capabilities?format=json

Method	GET
Description	Get the anti-passing back configuration capability of card readers.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_CardReaderAntiSneakCfg</i> Failed: <i>JSON_ResponseStatus</i>

A.67 /ISAPI/AccessControl/CardReaderCfg/<ID>?format=json

Operations about the card reader configuration.

Request URI Definition

Table A-80 GET /ISAPI/AccessControl/CardReaderCfg/<ID>?format=json

Method	GET
Description	Get the card reader configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_CardReaderCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-81 PUT /ISAPI/AccessControl/CardReaderCfg/<ID>?format=json

Method	PUT
Description	Set the card reader parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_CardReaderCfg</i>
Response	<i>JSON_ResponseStatus</i>

Remarks

The <ID> in the request URI refers to the card reader No. which starts from 1.

A.68 /ISAPI/AccessControl/CardReaderCfg/capabilities?format=json

Get the configuration capability of the card reader.

Request URI Definition

Table A-82 GET /ISAPI/AccessControl/CardReaderCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the card reader.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_CardReaderCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.69 /ISAPI/AccessControl/CardReaderPlan/<CardReaderNo>?format=json

Operations about the control schedule configuration of the card reader authentication mode.

Request URI Definition

Table A-83 GET /ISAPI/AccessControl/CardReaderPlan/<CardReaderNo>?format=json

Method	GET
Description	Get the control schedule configuration parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CardReaderPlan</u> Failed: <u>JSON_ResponseStatus</u>

Table A-84 PUT /ISAPI/AccessControl/CardReaderPlan/<CardReaderNo>?format=json

Method	PUT
Description	Set the control schedule parameters of the card reader authentication mode.

Query	format: determine the format of request or response message.
Request	<u>JSON_CardReaderPlan</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <CardReaderNo> in the request URI refers to the card reader No. which starts from 1, and you can get the maximum number of the card readers supported by the device from the control schedule configuration capability of the card reader authentication mode ([JSON_Cap_CardReaderPlan](#)).

A.70 /ISAPI/AccessControl/CardReaderPlan/capabilities?format=json

Get the control schedule configuration capability of the card reader authentication mode.

Request URI Definition

Table A-85 GET /ISAPI/AccessControl/CardReaderPlan/capabilities?format=json

Method	GET
Description	Get the control schedule configuration capability of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_CardReaderPlan</u> Failed: <u>JSON_ResponseStatus</u>

A.71 /ISAPI/AccessControl/CardVerificationRule/capabilities?format=json

Get the configuration capability of card No. authentication mode.

Request URI Definition

Table A-86 GET /ISAPI/AccessControl/CardVerificationRule/capabilities?format=json

Method	GET
Description	Get the configuration capability of card No. authentication mode.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CardVerificationRuleCap</u> Failed: <u>JSON_ResponseStatus</u>

A.72 /ISAPI/AccessControl/CardVerificationRule/progress?format=json

Get the switching progress and configuration result of card No. authentication mode.

Request URI Definition

Table A-87 GET /ISAPI/AccessControl/CardVerificationRule/progress?format=json

Method	GET
Description	Get the switching progress and configuration result of card No. authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CardVerificationRuleRes</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- This URI is used to search for the result of switching card No. authentication (comparison) mode.
- After the card No. authentication (comparison) mode is switched, the device will check whether the card No. is duplicate.

A.73 /ISAPI/AccessControl/CardVerificationRule?format=json

Get or set the parameters of card No. authentication mode.

Request URI Definition

Table A-88 GET /ISAPI/AccessControl/CardVerificationRule?format=json

Method	GET
Description	Get the parameters of card No. authentication mode.
Query	format: determine the format of request or response message.

Request	None.
Response	Succeeded: <u>JSON_CardVerificationRule</u> Failed: <u>JSON_ResponseStatus</u>

Table A-89 PUT /ISAPI/AccessControl/CardVerificationRule?format=json

Method	PUT
Description	Set the parameters of card No. authentication mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_CardVerificationRule</u>
Response	<u>JSON_ResponseStatus</u>

A.74 /ISAPI/AccessControl/ClearAntiSneak?format=json

Clear anti-passing back records.

Request URI Definition

Table A-90 PUT /ISAPI/AccessControl/ClearAntiSneak?format=json

Method	PUT
Description	Clear anti-passing back records.
Query	format: determine the format of request or response message.
Request	<u>JSON_ClearAntiSneak</u>
Response	<u>JSON_ResponseStatus</u>

A.75 /ISAPI/AccessControl/ClearAntiSneak/capabilities?format=json

Get the capability of clearing anti-passing back records.

Request URI Definition

Table A-91 GET /ISAPI/AccessControl/ClearAntiSneak/capabilities?format=json

Method	GET
Description	Get the capability of clearing anti-passing back records.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_ClearAntiSneak</u> Failed: <u>JSON_ResponseStatus</u>

A.76 /ISAPI/AccessControl/ClearAntiSneakCfg/capabilities?format=json

Get the capability of clearing anti-passing back parameters.

Request URI Definition

Table A-92 GET /ISAPI/AccessControl/ClearAntiSneakCfg/capabilities?format=json

Method	GET
Description	Get the capability of clearing anti-passing back parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_ClearAntiSneakCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.77 /ISAPI/AccessControl/ClearAntiSneakCfg?format=json

Clear anti-passing back parameters.

Request URI Definition

Table A-93 PUT /ISAPI/AccessControl/ClearAntiSneakCfg?format=json

Method	PUT
Description	Clear anti-passing back parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_ClearAntiSneakCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.78 /ISAPI/AccessControl/ClearAttendancePlan?format=json

Clear the attendance schedule.

Request URI Definition

Table A-94 PUT /ISAPI/AccessControl/ClearAttendancePlan?format=json

Method	PUT
Description	Clear the attendance schedule.
Query	format: determine the format of request or response message.
Request	<u>JSON_ClearAttendancePlan</u>
Response	<u>JSON_ResponseStatus</u>

A.79 /ISAPI/AccessControl/ClearCardRecord

Clear card swiping records in the cross-controller anti-passing back server.

Request URI Definition

Table A-95 PUT /ISAPI/AccessControl/ClearCardRecord

Method	PUT
Description	Clear card swiping records in the cross-controller anti-passing back server.
Query	None.
Request	<u>XML_ClearCardRecord</u>
Response	<u>XML_ResponseStatus</u>

Remarks

This request URI can only be used by the cross-controller anti-passing back server, and it is not supported by the cross-controller anti-passing back devices based on card mode.

A.80 /ISAPI/AccessControl/ClearCardRecord/capabilities

Get the capability of clearing card swiping records in the cross-controller anti-passing back server.

Request URI Definition

Table A-96 GET /ISAPI/AccessControl/ClearCardRecord/capabilities

Method	GET
Description	Get the capability of clearing card swiping records in the cross-controller anti-passing back server.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_ClearCardRecord</u> Failed: <u>XML_ResponseStatus</u>

A.81 /ISAPI/AccessControl/ClearEventCardLinkageCfg/capabilities?format=json

Get the capability of clearing event and card linkage configuration.

Request URI Definition

Table A-97 GET /ISAPI/AccessControl/ClearEventCardLinkageCfg/capabilities?format=json

Method	GET
Description	Get the capability of clearing event and card linkage configuration.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_ClearEventCardLinkageCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.82 /ISAPI/AccessControl/ClearEventCardLinkageCfg?format=json

Clear event and card linkage configuration.

Request URI Definition

Table A-98 PUT /ISAPI/AccessControl/ClearEventCardLinkageCfg?format=json

Method	PUT
Description	Clear event card linkage configuration parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_ClearEventCardLinkageCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.83 /ISAPI/AccessControl/ClearGroupCfg/capabilities?format=json

Get the capability of clearing group configuration.

Request URI Definition

Table A-99 GET /ISAPI/AccessControl/ClearGroupCfg/capabilities?format=json

Method	GET
Description	Get the capability of clearing group configuration.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_ClearGroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.84 /ISAPI/AccessControl/ClearGroupCfg?format=json

Clear the group configuration.

Request URI Definition

Table A-100 PUT /ISAPI/AccessControl/ClearGroupCfg?format=json

Method	PUT
Description	Clear the group configuration parameters.
Query	format: determine the format of request or response message.

Request	<i>JSON_ClearGroupCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.85 /ISAPI/AccessControl/ClearPictureCfg/capabilities?format=json

Get the capability of clearing all pictures in the device.

Request URI Definition

Table A-101 GET /ISAPI/AccessControl/ClearPictureCfg/capabilities?format=json

Method	GET
Description	Get the capability of clearing all pictures in the device.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_ClearPictureCfgCap</i> Failed: <i>JSON_ResponseStatus</i>

A.86 /ISAPI/AccessControl/ClearPictureCfg?format=json

Clear all pictures in the device.

Request URI Definition

Table A-102 PUT /ISAPI/AccessControl/ClearPictureCfg?format=json

Method	PUT
Description	Clear all pictures in the device.
Query	format: determine the format of request or response message.
Request	<i>JSON_ClearPictureCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.87 /ISAPI/AccessControl/ClearPlansCfg/capabilities?format=json

Get the capability of clearing access control schedule configuration.

Request URI Definition

Table A-103 GET /ISAPI/AccessControl/ClearPlansCfg/capabilities?format=json

Method	GET
Description	Get the capability of clearing access control schedule configuration.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_ClearPlansCfg</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.88 /ISAPI/AccessControl/ClearPlansCfg?format=json

Clear the access control schedule configuration.

Request URI Definition

Table A-104 PUT /ISAPI/AccessControl/ClearPlansCfg?format=json

Method	PUT
Description	Clear the access control schedule configuration parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_ClearPlansCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.89 /ISAPI/AccessControl/ClearSubmarineBack

Clear cross-controller anti-passing back parameters.

Request URI Definition

Table A-105 PUT /ISAPI/AccessControl/ClearSubmarineBack

Method	PUT
Description	Clear cross-controller anti-passing back parameters.
Query	None.
Request	<u>XML_ClearSubmarineBack</u>
Response	<u>XML_ResponseStatus</u>

A.90 /ISAPI/AccessControl/ClearSubmarineBack/capabilities

Get the capability of clearing cross-controller anti-passing back parameters.

Request URI Definition

Table A-106 GET /ISAPI/AccessControl/ClearSubmarineBack/capabilities

Method	GET
Description	Get the capability of clearing cross-controller anti-passing back parameters.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_ClearSubmarineBack</u> Failed: <u>XML_ResponseStatus</u>

A.91 /ISAPI/AccessControl/Configuration/attendanceMode/capabilities? format=json

Get the configuration capability of the attendance mode.

Request URI Definition

Table A-107 GET /ISAPI/AccessControl/Configuration/attendanceMode/capabilities?format=json

Method	GET
Description	Get the configuration capability of the attendance mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_AttendanceMode</i> Failed: <i>JSON_ResponseStatus</i>

A.92 /ISAPI/AccessControl/Configuration/attendanceMode?format=json

Get or set the attendance mode parameters.

Request URI Definition

Table A-108 GET /ISAPI/AccessControl/Configuration/attendanceMode?format=json

Method	GET
Description	Get the attendance mode parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_AttendanceMode</i> Failed: <i>JSON_ResponseStatus</i>

Table A-109 PUT /ISAPI/AccessControl/Configuration/attendanceMode?format=json

Method	PUT
Description	Set the attendance mode parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_AttendanceMode</i>
Response	<i>JSON_ResponseStatus</i>

A.93 /ISAPI/AccessControl/Configuration/IRCfg/capabilities?format=json

Get active infrared intrusion capability.

Request URI Definition

Table A-110 GET /ISAPI/AccessControl/Configuration/IRCfg/capabilities?format=json

Method	GET
Description	Get active infrared intrusion capability.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_IRCfgCap</i> Failed: <i>JSON_ResponseStatus</i>

A.94 /ISAPI/AccessControl/Configuration/IRCfg?format=json

Get or set active infrared intrusion parameters.

Request URI Definition

Table A-111 GET /ISAPI/AccessControl/Configuration/IRCfg?format=json

Method	GET
Description	Get active infrared intrusion parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_IRCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-112 PUT /ISAPI/AccessControl/Configuration/IRCfg?format=json

Method	PUT
Description	Set active infrared intrusion parameters.
Query	format: determine the format of request or response message.

Request	<u>JSON_IRCfq</u>
Response	<u>JSON_ResponseStatus</u>

A.95 /ISAPI/AccessControl/Configuration/lockType/capabilities?format=json

Get the configuration capability of the door lock status when the device is powered off.

Request URI Definition

Table A-113 GET /ISAPI/AccessControl/Configuration/lockType/capabilities?format=json

Method	GET
Description	Get the configuration capability of the door lock status when the device is powered off.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_LockTypeCap</u> Failed: <u>JSON_ResponseStatus</u>

A.96 /ISAPI/AccessControl/Configuration/lockType?format=json

Get or set the door lock status when the device is powered off.

Request URI Definition

Table A-114 GET /ISAPI/AccessControl/Configuration/lockType?format=json

Method	GET
Description	Get the door lock status when the device is powered off.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_LockType</u> Failed: <u>JSON_ResponseStatus</u>

Table A-115 PUT /ISAPI/AccessControl/Configuration/lockType?format=json

Method	PUT
Description	Set the door lock status when the device is powered off.
Query	format: determine the format of request or response message.
Request	<u>JSON_LockType</u>
Response	<u>JSON_ResponseStatus</u>

A.97 /ISAPI/AccessControl/Configuration/NFCCfg/capabilities?format=json

Get the configuration capability of enabling NFC (Near-Field Communication) function.

Request URI Definition

Table A-116 GET /ISAPI/AccessControl/Configuration/NFCCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of enabling NFC (Near-Field Communication) function.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_NFCCfgCap</u> Failed: <u>JSON_ResponseStatus</u>

A.98 /ISAPI/AccessControl/Configuration/NFCCfg?format=json

Operations about the configuration of enabling NFC (Near-Field Communication) function.

Request URI Definition

Table A-117 GET /ISAPI/AccessControl/Configuration/NFCCfg?format=json

Method	GET
Description	Get the parameters of enabling NFC (Near-Field Communication) function.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_NFCCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-118 PUT /ISAPI/AccessControl/Configuration/NFCCfg?format=json

Method	PUT
Description	Set the parameters of enabling NFC (Near-Field Communication) function.
Query	format: determine the format of request or response message.
Request	<u>JSON_NFCCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.99 /ISAPI/AccessControl/Configuration/RFCardCfg/capabilities?format=json

Get the configuration capability of enabling RF (Radio Frequency) card recognition.

Request URI Definition

Table A-119 GET /ISAPI/AccessControl/Configuration/RFCardCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of enabling RF (Radio Frequency) card recognition.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_RFCardCfgCap</u> Failed: <u>JSON_ResponseStatus</u>

A.100 /ISAPI/AccessControl/Configuration/RFCardCfg?format=json

Operations about the configuration of enabling RF (Radio Frequency) card recognition.

Request URI Definition

Table A-120 GET /ISAPI/AccessControl/Configuration/RFCardCfg?format=json

Method	GET
Description	Get the parameters of enabling RF (Radio Frequency) card recognition.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_RFCardCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-121 PUT /ISAPI/AccessControl/Configuration/RFCardCfg?format=json

Method	PUT
Description	Set the parameters of enabling RF (Radio Frequency) card recognition.
Query	format: determine the format of request or response message.
Request	<u>JSON_RFCardCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.101 /ISAPI/AccessControl/Configuration/safetyHelmetDetection/capabilities?format=json

Get the configuration capability of hard hat detection.

Request URI Definition

Table A-122 GET /ISAPI/AccessControl/Configuration/safetyHelmetDetection/capabilities?format=json

Method	GET
Description	Get the configuration capability of hard hat detection.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_SafetyHelmetDetectionCap</u>

	Failed: <i>JSON_ResponseStatus</i>
--	------------------------------------

A.102 /ISAPI/AccessControl/Configuration/safetyHelmetDetection?format=json

Get or set the parameters of hard hat detection.

Request URI Definition

Table A-123 GET /ISAPI/AccessControl/Configuration/safetyHelmetDetection?format=json

Method	GET
Description	Get the parameters of hard hat detection.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_SafetyHelmetDetection</i> Failed: <i>JSON_ResponseStatus</i>

Table A-124 PUT /ISAPI/AccessControl/Configuration/safetyHelmetDetection?format=json

Method	PUT
Description	Set the parameters of hard hat detection.
Query	format: determine the format of request or response message.
Request	<i>JSON_SafetyHelmetDetection</i>
Response	<i>JSON_ResponseStatus</i>

A.103 /ISAPI/AccessControl/customAudio/addCustomAudio?format=json

Import the custom audio file.

Request URI Definition

Table A-125 POST /ISAPI/AccessControl/customAudio/addCustomAudio?format=json

Method	POST
Description	Import the custom audio file.
Query	format: determine the format of request or response message.
Request	<i>JSON ImportCustomAudioFile</i> and/or Custom Audio File in Binary Format
Response	<i>JSONResponseStatus</i>

A.104 /ISAPI/AccessControl/customAudio/capabilities?format=json

Get the capability of configuring the custom audio.

Request URI Definition

Table A-126 GET /ISAPI/AccessControl/customAudio/capabilities?format=json

Method	GET
Description	Get the capability of configuring the custom audio.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON Cap_CustomAudioCfg</i> Failed: <i>JSONResponseStatus</i>

A.105 /ISAPI/AccessControl/customAudio/deleteCustomAudio? format=json

Delete the custom audio file.

Request URI Definition

Table A-127 POST /ISAPI/AccessControl/customAudio/deleteCustomAudio?format=json

Method	POST
Description	Delete the custom audio file.

Query	format: determine the format of request or response message.
Request	<u>JSON_CustomAudioFileDelCond</u>
Response	<u>JSON_ResponseStatus</u>

A.106 /ISAPI/AccessControl/customAudio/searchCustomAudioStatus? format=json

Search for the applying status of a specified custom audio file.

Request URI Definition

Table A-128 POST /ISAPI/AccessControl/customAudio/searchCustomAudioStatus?format=json

Method	POST
Description	Search for the applying status of a specified custom audio file.
Query	format: determine the format of request or response message.
Request	<u>JSON_CustomAudioFileApplyStatusSearchCond</u>
Response	Succeeded: <u>JSON_CustomAudioFileApplyStatusSearchResult</u> Failed: <u>JSON_ResponseStatus</u>

A.107 /ISAPI/AccessControl/DeployInfo

Get the arming information (e.g., arming types).

Request URI Definition

Table A-129 GET /ISAPI/AccessControl/DeployInfo

Method	GET
Description	Get the arming information (e.g., arming types).
Query	None.
Request	None.
Response	Succeeded: <u>XML_DeployInfo</u> Failed: <u>XML_ResponseStatus</u>

Remarks

The client arming supports arming of only one channel and can upload offline events. The real-time arming is used for other devices to arm the access control devices, which supports arming of up to four channels and cannot upload offline events.

A.108 /ISAPI/AccessControl/DeployInfo/capabilities

Get the capability of getting arming information.

Request URI Definition

Table A-130 GET /ISAPI/AccessControl/DeployInfo/capabilities

Method	GET
Description	Get the capability of getting arming information.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_DeployInfo</u> Failed: <u>XML_ResponseStatus</u>

A.109 /ISAPI/AccessControl/Door/param/<ID>

Operations about the door (floor) configuration.

Request URI Definition

Table A-131 GET /ISAPI/AccessControl/Door/param/<ID>

Method	GET
Description	Get the door (floor) configuration parameters.
Query	None.
Request	None.
Response	Succeeded: <u>XML_DoorParam</u> Failed: <u>XML_ResponseStatus</u>

Table A-132 PUT /ISAPI/AccessControl/Door/param/<ID>

Method	PUT
Description	Set the door (floor) parameters.
Query	None.
Request	<u>XML_DoorParam</u>
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the door No. (floor No.) which starts from 1.

A.110 /ISAPI/AccessControl/Door/param/<ID>/capabilities

Get the door (floor) configuration capability.

Request URI Definition

Table A-133 GET /ISAPI/AccessControl/Door/param/<ID>/capabilities

Method	GET
Description	Get the door (floor) configuration capability.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_DoorParam</u> Failed: <u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the door No. (floor No.) which starts from 1.

A.111 /ISAPI/AccessControl/DoorSecurityModule/moduleStatus

Get the status of the secure door control unit.

Request URI Definition

Table A-134 GET /ISAPI/AccessControl/DoorSecurityModule/moduleStatus

Method	GET
Description	Get the status of the secure door control unit.
Query	None.
Request	None.
Response	Succeeded: <i>XML_ModuleStatus</i> Failed: <i>XML_ResponseStatus</i>

A.112 /ISAPI/AccessControl/DoorSecurityModule/moduleStatus/capabilities

Get the capability of getting the status of the secure door control unit.

Request URI Definition

Table A-135 GET /ISAPI/AccessControl/DoorSecurityModule/moduleStatus/capabilities

Method	GET
Description	Get the capability of getting the status of the secure door control unit.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_ModuleStatus</i> Failed: <i>XML_ResponseStatus</i>

A.113 /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/<GroupNo>?format=json

Operations about the holiday group configuration of the door control schedule.

Request URI Definition

Table A-136 GET /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/<GroupNo>?format=json

Method	GET
Description	Get the holiday group configuration parameters of the door control schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_DoorStatusHolidayGroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-137 PUT /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/<GroupNo>?format=json

Method	PUT
Description	Set the holiday group parameters of the door control schedule.
Query	format: determine the format of request or response message.
Request	<u>JSON_DoorStatusHolidayGroupCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <GroupNo> in the request URI refers to the holiday group No. which starts from 1, and you can get the maximum number of the holiday groups supported by the device from the holiday group configuration capability of the door control schedule ([JSON_Cap_DoorStatusHolidayGroupCfg](#)).

A.114 /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/capabilities?format=json

Get the holiday group configuration capability of the door control schedule.

Request URI Definition

Table A-138 GET /ISAPI/AccessControl/DoorStatusHolidayGroupCfg/capabilities?format=json

Method	GET
Description	Get the holiday group configuration capability of the door control schedule.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_DoorStatusHolidayGroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.115 /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/<PlanNo>? format=json

Operations about the configuration of the door control holiday schedule.

Request URI Definition

Table A-139 GET /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/<PlanNo>?format=json

Method	GET
Description	Get the configuration parameters of the door control holiday schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_DoorStatusHolidayPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-140 PUT /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/<PlanNo>?format=json

Method	PUT
Description	Set the parameters of the door control holiday schedule.
Query	format: determine the format of request or response message.
Request	<u>JSON_DoorStatusHolidayPlanCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <PlanNo> in the request URI refers to the holiday schedule No. which starts from 1, and you can get the maximum number of the holiday schedules supported by the device from the configuration capability of the door control holiday schedule ([JSON_Cap_DoorStatusHolidayPlanCfg](#)).

A.116 /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/capabilities?format=json

Get the configuration capability of the door control holiday schedule.

Request URI Definition

Table A-141 GET /ISAPI/AccessControl/DoorStatusHolidayPlanCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the door control holiday schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_DoorStatusHolidayPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.117 /ISAPI/AccessControl/DoorStatusPlan/<DoorNo>?format=json

Operations about the configuration of the door control schedule.

Request URI Definition

Table A-142 GET /ISAPI/AccessControl/DoorStatusPlan/<DoorNo>?format=json

Method	GET
Description	Get the configuration parameters of the door control schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_DoorStatusPlan</u> Failed: <u>JSON_ResponseStatus</u>

Table A-143 PUT /ISAPI/AccessControl/DoorStatusPlan/<DoorNo>?format=json

Method	PUT
Description	Set the parameters of the door control schedule.
Query	format: determine the format of request or response message.

Request	<u>JSON_DoorStatusPlan</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <DoorNo> in the request URI refers to door No. which starts from 1, and you can get the maximum number of the doors supported by the device from the configuration capability of the door control schedule ([JSON_Cap_DoorStatusPlan](#)).

A.118 /ISAPI/AccessControl/DoorStatusPlan/capabilities?format=json

Get the configuration capability of the door control schedule.

Request URI Definition

Table A-144 GET /ISAPI/AccessControl/DoorStatusPlan/capabilities?format=json

Method	GET
Description	Get the configuration capability of the door control schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_DoorStatusPlan</u> Failed: <u>JSON_ResponseStatus</u>

A.119 /ISAPI/AccessControl/DoorStatusPlanTemplate/<TemplateNo>?format=json

Operations about the configuration of the door control schedule template.

Request URI Definition

Table A-145 GET /ISAPI/AccessControl/DoorStatusPlanTemplate/<TemplateNo>?format=json

Method	GET
Description	Get the configuration parameters of the door control schedule template.
Query	format: determine the format of request or response message.

Request	None.
Response	Succeeded: <u>JSON_DoorStatusPlanTemplate</u> Failed: <u>JSON_ResponseStatus</u>

Table A-146 PUT /ISAPI/AccessControl/DoorStatusPlanTemplate/<TemplateNo>?format=json

Method	PUT
Description	Set the parameters of the door control schedule template.
Query	format: determine the format of request or response message.
Request	<u>JSON_DoorStatusPlanTemplate</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <TemplateNo> in the request URI refers to door control schedule template No. which starts from 1, and you can get the maximum number of the templates supported by the device from the configuration capability of the door control schedule template ([JSON_Cap_DoorStatusPlanTemplate](#)).

A.120 /ISAPI/AccessControl/DoorStatusPlanTemplate/capabilities?format=json

Get the configuration capability of the door control schedule template.

Request URI Definition**Table A-147 GET /ISAPI/AccessControl/DoorStatusPlanTemplate/capabilities?format=json**

Method	GET
Description	Get the configuration capability of the door control schedule template.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_DoorStatusPlanTemplate</u> Failed: <u>JSON_ResponseStatus</u>

A.121 /ISAPI/AccessControl/DoorStatusWeekPlanCfg/<PlanNo>?format=json

Operations about the configuration of the door control week schedule.

Request URI Definition

Table A-148 GET /ISAPI/AccessControl/DoorStatusWeekPlanCfg/<PlanNo>?format=json

Method	GET
Description	Get the configuration parameters of the door control week schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_DoorStatusWeekPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-149 PUT /ISAPI/AccessControl/DoorStatusWeekPlanCfg/<PlanNo>?format=json

Method	PUT
Description	Set the parameters of the door control week schedule.
Query	format: determine the format of request or response message.
Request	<u>JSON_DoorStatusWeekPlanCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <PlanNo> in the request URI refers to the door control week schedule No. which starts from 1, and you can get the maximum number of week schedules supported by the device from the configuration capability of the door control week schedule ([JSON_Cap_DoorStatusWeekPlanCfg](#)).

A.122 /ISAPI/AccessControl/DoorStatusWeekPlanCfg/capabilities?format=json

Get the configuration capability of the door control week schedule.

Request URI Definition

Table A-150 GET /ISAPI/AccessControl/DoorStatusWeekPlanCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the door control week schedule.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_DoorStatusWeekPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.123 /ISAPI/AccessControl/EventCardLinkageCfg/<ID>?format=json

Operations about event and card linkage configuration.

Request URI Definition

Table A-151 GET /ISAPI/AccessControl/EventCardLinkageCfg/<ID>?format=json

Method	GET
Description	Get the event and card linkage configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_EventCardLinkageCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-152 PUT /ISAPI/AccessControl/EventCardLinkageCfg/<ID>?format=json

Method	PUT
Description	Set the event card linkage parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_EventCardLinkageCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the event No. which starts from 1, and you can get the maximum number of the events supported by the device from the configuration capability of the event and card linkage ([JSON_Cap_EventCardLinkageCfg](#)).

A.124 /ISAPI/AccessControl/EventCardLinkageCfg/capabilities?format=json

Get the configuration capability of the event and card linkage.

Request URI Definition

Table A-153 GET /ISAPI/AccessControl/EventCardLinkageCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the event and card linkage.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_EventCardLinkageCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.125 /ISAPI/AccessControl/EventCardNoList/capabilities?format=json

Get the capability of the list of event and card linkage ID.

Request URI Definition

Table A-154 GET /ISAPI/AccessControl/EventCardNoList/capabilities?format=json

Method	GET
Description	Get the capability of the list of event and card linkage ID.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_EventCardNoList</u> Failed: <u>JSON_ResponseStatus</u>

A.126 /ISAPI/AccessControl/EventCardNoList?format=json

Get the list of event and card linkage ID.

Request URI Definition

Table A-155 GET /ISAPI/AccessControl/EventCardNoList?format=json

Method	GET
Description	Get the list of event and card linkage ID.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_EventCardNoList</u> Failed: <u>JSON_ResponseStatus</u>

A.127 /ISAPI/AccessControl/EventOptimizationCfg/capabilities?format=json

Get the configuration capability of event optimization.

Request URI Definition

Table A-156 GET /ISAPI/AccessControl/EventOptimizationCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of event optimization.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_EventOptimizationCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.128 /ISAPI/AccessControl/EventOptimizationCfg?format=json

Operations about the event optimization configuration.

Request URI Definition

Table A-157 GET /ISAPI/AccessControl/EventOptimizationCfg?format=json

Method	GET
Description	Get the event optimization configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_EventOptimizationCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-158 PUT /ISAPI/AccessControl/EventOptimizationCfg?format=json

Method	PUT
Description	Set the event optimization parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_EventOptimizationCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.129 /ISAPI/AccessControl/FaceCompareCond

Get or set the condition parameters of face picture comparison.

Request URI Definition

Table A-159 GET /ISAPI/AccessControl/FaceCompareCond

Method	GET
Description	Get the condition parameters of face picture comparison.
Query	None.
Request	None.
Response	Succeeded: <i>XML_FaceCompareCond</i> Failed: <i>XML_ResponseStatus</i>

Table A-160 PUT /ISAPI/AccessControl/FaceCompareCond

Method	PUT
Description	Set the condition parameters of face picture comparison.
Query	None.
Request	<u>XML_FaceCompareCond</u>
Response	<u>XMLResponseStatus</u>

A.130 /ISAPI/AccessControl/FaceCompareCond/capabilities

Get condition configuration capability of face picture comparison.

Request URI Definition

Table A-161 GET /ISAPI/AccessControl/FaceCompareCond/capabilities

Method	GET
Description	Get condition configuration capability of face picture comparison.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_FaceCompareCond</u> Failed: <u>XMLResponseStatus</u>

A.131 /ISAPI/AccessControl/FaceRecognizeMode/capabilities? format=json

Get the configuration capability of the facial recognition mode.

Request URI Definition

Table A-162 GET /ISAPI/AccessControl/FaceRecognizeMode/capabilities?format=json

Method	GET
Description	Get the configuration capability of the facial recognition mode.
Query	format: determine the format of request or response message.

Request	None.
Response	Succeeded: <u>JSON_Cap_FaceRecognizeMode</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

Switching facial recognition mode will clear face permission information in the device.

A.132 /ISAPI/AccessControl/FaceRecognizeMode?format=json

Operations about the configuration of the facial recognition mode.

Request URI Definition

Table A-163 GET /ISAPI/AccessControl/FaceRecognizeMode?format=json

Method	GET
Description	Get the parameters of the facial recognition mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_FaceRecognizeMode</u> Failed: <u>JSON_ResponseStatus</u>

Table A-164 PUT /ISAPI/AccessControl/FaceRecognizeMode?format=json

Method	PUT
Description	Set the parameters of the facial recognition mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_FaceRecognizeMode</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

Switching facial recognition mode will clear face permission information in the device.

A.133 /ISAPI/AccessControl/FaceTemperatureEvent/capabilities?format=json

Get the capability of actively getting face temperature screening events.

Request URI Definition

Table A-165 GET /ISAPI/AccessControl/FaceTemperatureEvent/capabilities?format=json

Method	GET
Description	Get the capability of actively getting face temperature screening events.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_FaceTemperatureEventCap</i> Failed: <i>JSON_ResponseStatus</i>

A.134 /ISAPI/AccessControl/FaceTemperatureEvent?format=json

Get face temperature screening events actively.

Request URI Definition

Table A-166 POST /ISAPI/AccessControl/FaceTemperatureEvent?format=json

Method	POST
Description	Get face temperature screening events actively.
Query	format: determine the format of request or response message.
Request	<i>JSON_FaceTemperatureEventCond</i>
Response	Succeeded: <i>JSON_FaceTemperatureEvent</i> Failed: <i>JSON_ResponseStatus</i>

A.135 /ISAPI/AccessControl/FingerPrint/Count? format=json&employeeNo=

Get the total number of fingerprints of a specific person.

Request URI Definition

Table A-167 GET /ISAPI/AccessControl/FingerPrint/Count?format=json&employeeNo=

Method	GET
Description	Get the total number of fingerprints of a specific person.
Query	format: determine the format of request or response message. employeeNo: int, employee No.
Request	None.
Response	Succeeded: <u>JSON_FingerPrintCountList</u> Failed: <u>JSON_ResponseStatus</u>

A.136 /ISAPI/AccessControl/FingerPrint/Delete/capabilities? format=json

Get the capability of deleting fingerprint data.

Request URI Definition

Table A-168 GET /ISAPI/AccessControl/FingerPrint/Delete/capabilities?format=json

Method	GET
Description	Get the capability of deleting fingerprint data.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_FingerPrintDelete</u> Failed: <u>JSON_ResponseStatus</u>

A.137 /ISAPI/AccessControl/FingerPrint/Delete?format=json

Start deleting the fingerprint data.

Request URI Definition

Table A-169 PUT /ISAPI/AccessControl/FingerPrint/Delete?format=json

Method	PUT
Description	Start deleting the fingerprint data.
Query	format: determine the format of request or response message.
Request	<u>JSON_FingerPrintDelete</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

This URI is only used to start deleting. To judge whether the deleting is completed, you should call the request URI [/ISAPI/AccessControl/FingerPrint/DeleteProcess?format=json](#) by GET method to get the deleting status.

A.138 /ISAPI/AccessControl/FingerPrint/DeleteProcess?format=json

Get the progress of deleting fingerprint data.

Request URI Definition

Table A-170 GET /ISAPI/AccessControl/FingerPrint/DeleteProcess?format=json

Method	GET
Description	Get the progress of deleting fingerprint data.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_FingerPrintDeleteProcess</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

When starting deleting fingerprint data, this URI will be repeatedly called to get the deleting progress until "success" or "failed" is returned by the parameter **status** in the message [JSON_FingerPrintDeleteProcess](#).

A.139 /ISAPI/AccessControl/FingerPrint/SetUp?format=json

Set the fingerprint parameters.

Request URI Definition

Table A-171 POST /ISAPI/AccessControl/FingerPrint/SetUp?format=json

Method	POST
Description	Set the fingerprint parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_FingerPrintCfg</u>
Response	<u>JSON_FingerPrintStatus</u>

Remarks

- If the **fingerData** is not applied, it indicates editing fingerprint parameters instead of applying fingerprint data to the fingerprint module.
- If the **fingerData** is applied, the fingerprint data will be added if it does not exist in the fingerprint module, or the original fingerprint data will be overwritten if it already exists in the fingerprint module.
- There are four different methods for deleting one or more fingerprints:
 - To delete a specific fingerprint in a specific fingerprint module linked with a specific employee No., the **employeeNo**, **enableCardReader**, **fingerPrintID**, and **deleteFingerPrint** in the message [JSON_FingerPrintCfg](#) should be configured, and the success response message will be returned no matter whether the fingerprint exists or not.
 - To delete a specific fingerprint in all fingerprint modules linked with a specific employee No., the **employeeNo**, **fingerPrintID**, and **deleteFingerPrint** in the message [JSON_FingerPrintCfg](#) should be configured, and the success response message will be returned no matter whether the fingerprints exist or not.
 - To delete all fingerprints in a specific fingerprint module linked with a specific employee No., the **employeeNo**, **enableCardReader**, and **deleteFingerPrint** in the message [JSON_FingerPrintCfg](#) should be configured, and the success response message will be returned no matter whether the fingerprints exist or not.
 - To delete all fingerprints in all fingerprint modules linked with a specific employee No., the **employeeNo** and **deleteFingerPrint** in the message [JSON_FingerPrintCfg](#) should be configured, and the success response message will be returned no matter whether the fingerprints exist or not.

A.140 /ISAPI/AccessControl/FingerPrintCfg/capabilities?format=json

Get the configuration capability of fingerprint parameters.

Request URI Definition

Table A-172 GET /ISAPI/AccessControl/FingerPrintCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of fingerprint parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_FingerPrintCfg</i> Failed: <i>JSON_ResponseStatus</i>

A.141 /ISAPI/AccessControl/FingerPrintDownload?format=json

Set fingerprint parameters to link with a person, and apply the collected fingerprint data.

Request URI Definition

Table A-173 POST /ISAPI/AccessControl/FingerPrintDownload?format=json

Method	POST
Description	Set fingerprint parameters to link with a person, and apply the collected fingerprint data.
Query	format: determine the format of request or response message.
Request	<i>JSON_FingerPrintCfg</i> +fingerprint data (by boundary method)
Response	<i>JSON_ResponseStatus</i>

Remarks

This URI is only used to start applying the fingerprint data. To check whether the applying is completed, you should call the request URI **/ISAPI/AccessControl/FingerPrintProgress?format=json** by GET method to get the applying status.

A.142 /ISAPI/AccessControl/FingerPrintModify?format=json

Edit fingerprint parameters.

Request URI Definition

Table A-174 POST /ISAPI/AccessControl/FingerPrintModify?format=json

Method	POST
Description	Edit fingerprint parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_FingerPrintModify</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

Only the fingerprint parameters can be edited. The collected fingerprint data will not be edited and applied.

A.143 /ISAPI/AccessControl/FingerPrintProgress?format=json

Get the progress of applying fingerprint data.

Request URI Definition

Table A-175 GET /ISAPI/AccessControl/FingerPrintProgress?format=json

Method	GET
Description	Get the progress of applying fingerprint data.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_FingerPrintStatus</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

When starting applying fingerprint data, this URI will be repeatedly called to get the applying progress until "1" is returned by the parameter **totalStatus** in the message [JSON_FingerPrintStatus](#).

A.144 /ISAPI/AccessControl/FingerPrintUpload?format=json

Get the fingerprint information, including fingerprint parameters and data.

Request URI Definition

Table A-176 POST /ISAPI/AccessControl/FingerPrintUpload?format=json

Method	POST
Description	Get the fingerprint information, including fingerprint parameters and data.
Query	format : determine the format of request or response message.
Request	<u>JSON_FingerPrintCond</u>
Response	<u>JSON_FingerPrintInfo</u> +fingerprint data (by boundary method)

Remarks

- To get the information of a specific fingerprint, the **searchID**, **employeeNo**, **cardReaderNo**, and **fingerPrintID** in the message [JSON_FingerPrintCond](#) should be configured. If the fingerprint matching the search conditions exists, the **status** will be set to "OK" and the corresponding fingerprint information will be returned by **FingerPrintList** in the message [JSON_FingerPrintInfo](#); otherwise, the **status** will be set to "NoFP" and the **FingerPrintList** will be set to NULL in the message [JSON_FingerPrintInfo](#).
- To get all fingerprints linked with a specific employee No. (person ID), the **searchID** and **employeeNo** in the message [JSON_FingerPrintCond](#) should be configured. If the fingerprints matching the search conditions exist, the **status** will be set to "OK" and the corresponding fingerprint information will be returned by **FingerPrintList** in the message [JSON_FingerPrintInfo](#). The request URI [/ISAPI/AccessControl/FingerPrintUpload?format=json](#) will be repeatedly called by POST method to get the information of multiple fingerprints matching the search conditions until "NoFP" is returned by **status** in the message [JSON_FingerPrintInfo](#) (it indicates that information of all fingerprints matching the search conditions are obtained). If there is no fingerprint matching the search conditions, the **status** will be set to "NoFP" and the **FingerPrintList** will be set to NULL in the message [JSON_FingerPrintInfo](#).

A.145 /ISAPI/AccessControl/FingerPrintUploadAll?format=json

Get all fingerprints' information (including fingerprint parameters and data) of a specific person.

Request URI Definition

Table A-177 POST /ISAPI/AccessControl/FingerPrintUploadAll?format=json

Method	POST
Description	Get all fingerprints' information (including fingerprint parameters and data) of a specific person.
Query	format: determine the format of request or response message.
Request	<u>JSON_FingerPrintCondAll</u>
Response	<u>JSON_FingerPrintInfoAll</u> +fingerprint data (by boundary method)

A.146 /ISAPI/AccessControl/GroupCfg/<ID>?format=json

Operations about the group configuration.

Request URI Definition

Table A-178 GET /ISAPI/AccessControl/GroupCfg/<ID>?format=json

Method	GET
Description	Get the group configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_GroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-179 PUT /ISAPI/AccessControl/GroupCfg/<ID>?format=json

Method	PUT
Description	Set the group parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_GroupCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the group No. which starts from 1.

A.147 /ISAPI/AccessControl/GroupCfg/capabilities?format=json

Get the group configuration capability.

Request URI Definition

Table A-180 GET /ISAPI/AccessControl/GroupCfg/capabilities?format=json

Method	GET
Description	Get the group configuration capability.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_GroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.148 /ISAPI/AccessControl/healthCodeCfg/capabilities?format=json

Get the configuration capability of the health code.

Request URI Definition

Table A-181 GET /ISAPI/AccessControl/healthCodeCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the health code.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_HealthCodeCfg</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

The device needs to connect to the health code server for uploading the information of the person to be authenticated to the server. The health code server is provided by the third party.

A.149 /ISAPI/AccessControl/healthCodeCfg?format=json

Get or set the health code parameters.

Request URI Definition

Table A-182 GET /ISAPI/AccessControl/healthCodeCfg?format=json

Method	GET
Description	Get the health code parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_HealthCodeCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-183 PUT /ISAPI/AccessControl/healthCodeCfg?format=json

Method	PUT
Description	Set the health code parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_HealthCodeCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.150 /ISAPI/AccessControl/IDBlackListCfg

Apply ID card blocklist.

Request URI Definition

Table A-184 PUT /ISAPI/AccessControl/IDBlackListCfg

Method	PUT
Description	Apply ID card blocklist.
Query	None.
Request	<i>XML_IDBlackListCfg</i>
Response	<i>XML_ResponseStatus</i>

A.151 /ISAPI/AccessControl/IDBlackListCfg/capabilities

Get capability of applying ID card blocklist.

Request URI Definition

Table A-185 GET /ISAPI/AccessControl/IDBlackListCfg/capabilities

Method	GET
Description	Get capability of applying ID card blocklist.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_IDBlackListCfg</i> Failed: <i>XML_ResponseStatus</i>

A.152 /ISAPI/AccessControl/IDBlackListCfg/template?format=json

Get the ID card blocklist template.

Request URI Definition

Table A-186 GET /ISAPI/AccessControl/IDBlackListCfg/template?format=json

Method	GET
Description	Get the ID card blocklist template.
Query	format: determine the format of request or response message.
Request	None.
Response	Binary data (template data in binary format).

A.153 /ISAPI/AccessControl/IDCardInfoEvent/capabilities?format=json

Get the capability of getting the ID card swiping events actively.

Request URI Definition

Table A-187 GET /ISAPI/AccessControl/IDCardInfoEvent/capabilities?format=json

Method	GET
Description	Get the capability of getting the ID card swiping events actively.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_IDCardInfoEventCap</i> Failed: <i>JSON_ResponseStatus</i>

A.154 /ISAPI/AccessControl/IDCardInfoEvent?format=json

Get the ID card swiping events actively.

Request URI Definition

Table A-188 POST /ISAPI/AccessControl/IDCardInfoEvent?format=json

Method	POST
Description	Get the ID card swiping events actively.
Query	format: determine the format of request or response message.
Request	<i>JSON_IDCardInfoEventCond</i>
Response	<i>JSON_IDCardInfoEvent</i>

A.155 /ISAPI/AccessControl/IdentityTerminal

Operations about configuration of intelligent identity recognition terminal.

Request URI Definition

Table A-189 GET /ISAPI/AccessControl/IdentityTerminal

Method	GET
Description	Get the configuration parameters of intelligent identity recognition terminal.

Query	None.
Request	None.
Response	Succeeded: <u>XML_IdentityTerminal</u> Failed: <u>XML_ResponseStatus</u>

Table A-190 PUT /ISAPI/AccessControl/IdentityTerminal

Method	PUT
Description	Set the parameters of intelligent identity recognition terminal.
Query	None.
Request	<u>XML_IdentityTerminal</u>
Response	<u>XML_ResponseStatus</u>

A.156 /ISAPI/AccessControl/IdentityTerminal/capabilities

Get configuration capability of intelligent identity recognition terminal.

Request URI Definition

Table A-191 GET /ISAPI/AccessControl/IdentityTerminal/capabilities

Method	GET
Description	Get configuration capability of intelligent identity recognition terminal.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_IdentityTerminal</u> Failed: <u>XML_ResponseStatus</u>

A.157 /ISAPI/AccessControl/keyCfg/<ID>/attendance?format=json

Get or set the parameters of attendance check by pressing the key.

Request URI Definition

Table A-192 GET /ISAPI/AccessControl/keyCfg/<ID>/attendance?format=json

Method	GET
Description	Get the parameters of attendance check by pressing the key.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Attendance</i> Failed: <i>JSON_ResponseStatus</i>

Table A-193 PUT /ISAPI/AccessControl/keyCfg/<ID>/attendance?format=json

Method	PUT
Description	Set the parameters of attendance check by pressing the key.
Query	format: determine the format of request or response message.
Request	<i>JSON_Attendance</i>
Response	<i>JSON_ResponseStatus</i>

A.158 /ISAPI/AccessControl/keyCfg/attendance/capabilities? **format=json**

Get the configuration capability of attendance check by pressing the key.

Request URI Definition

Table A-194 GET /ISAPI/AccessControl/keyCfg/attendance/capabilities?format=json

Method	GET
Description	Get the configuration capability of attendance check by pressing the key.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_AttendanceCap</i> Failed: <i>JSON_ResponseStatus</i>

A.159 /ISAPI/AccessControl/keyCfg/attendance?format=json

Get the attendance parameter list.

Request URI Definition

Table A-195 GET /ISAPI/AccessControl/keyCfg/attendance?format=json

Method	GET
Description	Get the attendance parameter list.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_AttendanceList</u> Failed: <u>JSON_ResponseStatus</u>

A.160 /ISAPI/AccessControl/LogModeCfg/capabilities?format=json

Get the configuration capability of the log mode.

Request URI Definition

Table A-196 GET /ISAPI/AccessControl/LogModeCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the log mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_LogModeCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.161 /ISAPI/AccessControl/LogModeCfg?format=json

Operations about the log mode configuration.

Request URI Definition

Table A-197 GET /ISAPI/AccessControl/LogModeCfg?format=json

Method	GET
Description	Get the log mode configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_LogModeCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-198 PUT /ISAPI/AccessControl/LogModeCfg?format=json

Method	PUT
Description	Set the log mode parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_LogModeCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.162 /ISAPI/AccessControl/LOGOCfg/capabilities?format=json

Get the capability of configuring logo parameters.

Request URI Definition

Table A-199 GET /ISAPI/AccessControl/LOGOCfg/capabilities?format=json

Method	GET
Description	Get the capability of configuring logo parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_LOGOCfg</i> Failed: <i>JSON_ResponseStatus</i>

A.163 /ISAPI/AccessControl/LOGOCfg?format=json

Import or delete the logo.

Request URI Definition

Table A-200 POST /ISAPI/AccessControl/LOGOCfg?format=json

Method	POST
Description	Import the logo.
Query	format: determine the format of request or response message.
Request	Binary data (form format).
Response	<u>JSONResponseStatus</u>

Table A-201 DELETE /ISAPI/AccessControl/LOGOCfg?format=json

Method	DELETE
Description	Delete the logo.
Query	format: determine the format of request or response message.
Request	None.
Response	<u>JSONResponseStatus</u>

A.164 /ISAPI/AccessControl/M1CardEncryptCfg

Operations about the configuration of M1 card encryption verification.

Request URI Definition

Table A-202 GET /ISAPI/AccessControl/M1CardEncryptCfg

Method	GET
Description	Get the configuration parameters of M1 card encryption verification.
Query	None.
Request	None.
Response	Succeeded: <u>XML_M1CardEncryptCfg</u> Failed: <u>XMLResponseStatus</u>

Table A-203 PUT /ISAPI/AccessControl/M1CardEncryptCfg

Method	PUT
Description	Set the parameters of M1 card encryption verification.
Query	None.
Request	<u>XML_M1CardEncryptCfg</u>
Response	<u>XMLResponseStatus</u>

Remarks

This request URI is used to notify the device that data of which sector is encrypted by M1 card and will not execute the encryption function.

A.165 /ISAPI/AccessControl/M1CardEncryptCfg/capabilities

Get the configuration capability of M1 card encryption verification.

Request URI Definition

Table A-204 GET /ISAPI/AccessControl/M1CardEncryptCfg/capabilities

Method	GET
Description	Get the configuration capability of M1 card encryption verification.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_M1CardEncryptCfg</u> Failed: <u>XMLResponseStatus</u>

A.166 /ISAPI/AccessControl/maintenanceData?secretkey=

Export the maintenance data.

Request URI Definition

Table A-205 GET /ISAPI/AccessControl/maintenanceData?secretkey=

Method	GET
Description	Export the maintenance data.

Query	secretkey : the verification key, it is provided by the upper layer. It should be encrypted for exporting and recorded for importing. security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. iv : the initialization vector, and it is required when security is 1 or 2.
Request	None.
Response	Succeeded: Opaque data. Failed: <u>XML_ResponseStatus</u>

Remarks

The maintenance data include device running logs, events, and so on, and they are used for troubleshooting.

A.167 /ISAPI/AccessControl/maskDetection/capabilities?format=json

Get the configuration capability of mask detection.

Request URI Definition

Table A-206 GET /ISAPI/AccessControl/maskDetection/capabilities?format=json

Method	GET
Description	Get the configuration capability of mask detection.
Query	format : determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_MaskDetectionCap</u> Failed: <u>JSON_ResponseStatus</u>

A.168 /ISAPI/AccessControl/maskDetection?format=json

Get or set the mask detection parameters.

Request URI Definition

Table A-207 GET /ISAPI/AccessControl/maskDetection?format=json

Method	GET
Description	Get the mask detection parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_MaskDetection</i> Failed: <i>JSON_ResponseStatus</i>

Table A-208 PUT /ISAPI/AccessControl/maskDetection?format=json

Method	PUT
Description	Set the mask detection parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_MaskDetection</i>
Response	<i>JSON_ResponseStatus</i>

A.169 /ISAPI/AccessControl/MultiCardCfg/<ID>?format=json

Operations about the configuration of multi-factor authentication mode.

Request URI Definition

Table A-209 GET /ISAPI/AccessControl/MultiCardCfg/<ID>?format=json

Method	GET
Description	Get the configuration parameters of multi-factor authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_MultiCardCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-210 PUT /ISAPI/AccessControl/MultiCardCfg/<ID>?format=json

Method	PUT
Description	Set the parameters of multi-factor authentication mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_MultiCardCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the door No. which starts from 1.

A.170 /ISAPI/AccessControl/MultiCardCfg/capabilities?format=json

Get the configuration capability of multi-factor authentication mode.

Request URI Definition

Table A-211 GET /ISAPI/AccessControl/MultiCardCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of multi-factor authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_MultiCardCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.171 /ISAPI/AccessControl/MultiDoorInterLockCfg/capabilities?format=json

Get the configuration capability of the multi-door interlocking.

Request URI Definition

Table A-212 GET /ISAPI/AccessControl/MultiDoorInterLockCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the multi-door interlocking.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_MultiDoorInterLockCfg</i> Failed: <i>JSON_ResponseStatus</i>

A.172 /ISAPI/AccessControl/MultiDoorInterLockCfg?format=json

Operations about the multi-door interlocking configuration.

Request URI Definition

Table A-213 GET /ISAPI/AccessControl/MultiDoorInterLockCfg?format=json

Method	GET
Description	Get the multi-door interlocking configuration parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_MultiDoorInterLockCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-214 PUT /ISAPI/AccessControl/MultiDoorInterLockCfg?format=json

Method	PUT
Description	Set the multi-door interlocking parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_MultiDoorInterLockCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.173 /ISAPI/AccessControl/OfflineCapture/capabilities?format=json

Get the offline collection capability.

Request URI Definition

Table A-215 GET /ISAPI/AccessControl/OfflineCapture/capabilities?format=json

Method	GET
Description	Get the offline collection capability.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_OfflineCaptureCap</i> Failed: <i>JSON_ResponseStatus</i>

A.174 /ISAPI/AccessControl/OfflineCapture/DataCollections/<captureNo>?format=json

Deleted a specific piece of offline collected data.

Request URI Definition

Table A-216 DELETE /ISAPI/AccessControl/OfflineCapture/DataCollections/<captureNo>?format=json

Method	DELETE
Description	Deleted a specific piece of offline collected data.
Query	format: determine the format of request or response message.
Request	None.
Response	<i>JSON_ResponseStatus</i>

Remarks

The <captureNo> in the request URI refers to the collection No.

A.175 /ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?format=json

Download data collected offline.

Request URI Definition

Table A-217 POST /ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?format=json

Method	POST
Description	Download data collected offline.
Query	format: determine the format of request or response message.
Request	<u>JSON_DataCollectionsCond</u>
Response	Succeeded: <u>JSON_DataCollections</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- You can repeatedly call this request URI using the same ID to get the progress. The default timeout is 60s (if the device's progress is 100 and the caller does not download after 60s, this request fails and an error message will be returned).
- If the ID is different, the device will return the corresponding status according to whether it supports processing concurrently. If processing concurrently is not supported, the device will return the error "The device is busy".
- When the field **progress** in the success response message is 100, the data collected offline in binary format or the URL for downloading the data will be returned.

Example

Sample Code of Interaction in URL Format

```
POST /ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?
format=json
Accept: text/html, application/xhtml+xml,
Accept-Language: en-US
Content-Type: application/xml
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/
5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

{
  "DataCollectionsCond": {
    "dataType ":"url"
  /*required, string, data type of the file: "url"-URL, "binary"-binary data*/
  }
}
```

```
-----  
HTTP/1.1 200 OK  
MIME-Version: 1.0  
Connection: close  
Content-Type: application/xml; charset="UTF-8"  
Content-Length: text_length  
  
{  
    "DataCollections":{  
        "dataType ":"binary",  
        /*required, string, data type of the file: "url"-URL, "binary"-binary data*/  
        "fileUrl":""  
        /*dependent, string, file URL, this field is valid when dataType is "url"*/  
    }  
}
```

Example

Sample Code of Interaction in Binary Format

```
POST /ISAPI/AccessControl/OfflineCapture/DataCollections/downloadTask?  
format=json  
Accept: text/html, application/xhtml+xml,  
Accept-Language: en-US  
Content-Type: application/xml  
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/  
5.0)  
Accept-Encoding: gzip, deflate  
Host: 10.10.36.29:8080  
Content-Length: 9907  
Connection: Keep-Alive  
Cache-Control: no-cache  
  
{  
    "DataCollectionsCond":{  
        "dataType ":"binary",  
        /*required, string, data type of the file: "url"-URL, "binary"-binary data*/  
    }  
}  
-----  
-----  
HTTP/1.1 200 OK  
MIME-Version: 1.0  
Connection: close  
Content-Type: multipart/form-data; boundary=<frontier>  
Content-Length: all_length  
  
--<frontier>  
Content-Type: application/json; charset="UTF-8"  
Content-Length: text_length  
  
{DataCollections}  
--<frontier>
```

```
Content-Disposition: form-data; name="dataCollections";
filename="dataCollections.xx "
Content-Type: application/octet-stream
Content-Length: data_length

[Data]
--<frontier>--
```

A.176 /ISAPI/AccessControl/OfflineCapture/DataCollections/searchTask?format=json

Search for the collected data.

Request URI Definition

Table A-218 POST /ISAPI/AccessControl/OfflineCapture/DataCollections/searchTask?format=json

Method	POST
Description	Search for the collected data.
Query	format: determine the format of request or response message.
Request	<u>JSON_SearchTaskCond</u>
Response	Succeeded: <u>JSON_SearchTaskResponse</u> Failed: <u>JSON_ResponseStatus</u>

A.177 /ISAPI/AccessControl/OfflineCapture/DataCollections?format=json

Delete all offline collected data.

Request URI Definition

Table A-219 DELETE /ISAPI/AccessControl/OfflineCapture/DataCollections?format=json

Method	DELETE
Description	Delete all offline collected data.
Query	format: determine the format of request or response message.
Request	None.
Response	<u>JSON_ResponseStatus</u>

A.178 /ISAPI/AccessControl/OfflineCapture/dataOutput/progress? format=json

Get the progress of exporting the offline collected data.

Request URI Definition

Table A-220 GET /ISAPI/AccessControl/OfflineCapture/dataOutput/progress?format=json

Method	GET
Description	Get the progress of exporting the offline collected data.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_DataOutputProgress</u> Failed: <u>JSON_ResponseStatus</u>

A.179 /ISAPI/AccessControl/OfflineCapture/dataOutput?format=json

Export the offline collected data.

Request URI Definition

Table A-221 PUT /ISAPI/AccessControl/OfflineCapture/dataOutput?format=json

Method	PUT
Description	Export the offline collected data.
Query	format: determine the format of request or response message. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. In the message of this request URI, the value of the field password should be encrypted. iv: the initialization vector, and it is required when security is 1 or 2.
Request	<u>JSON_DataOutputCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.180 /ISAPI/AccessControl/OfflineCapture/InfoFile/progress?format=json

Get the progress of uploading the user list of offline collection.

Request URI Definition

Table A-222 GET /ISAPI/AccessControl/OfflineCapture/InfoFile/progress?format=json

Method	GET
Description	Get the progress of uploading the user list of offline collection.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_InfoFileProgress</u> Failed: <u>JSON_ResponseStatus</u>

A.181 /ISAPI/AccessControl/OfflineCapture/InfoFile?format=json

Upload the user list of offline collection.

Request URI Definition

Table A-223 POST /ISAPI/AccessControl/OfflineCapture/InfoFile?format=json

Method	POST
Description	Upload the user list of offline collection.
Query	format: determine the format of request or response message.
Request	<u>JSON_InfoFile</u> (opaque data (MIME data)).
Response	<u>JSON_ResponseStatus</u>

Example

Sample Code of Interaction in Form Format

```
POST /ISAPI/AccessControl/OfflineCapture/infoFile?format=json
Accept: text/html, application/xhtml+xml,
Accept-Language: zh-CN
Content-Type: multipart/form-data;
boundary=-----7e13971310878
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

```
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

-----7e13971310878
Content-Type: application/json
Content-Length: 9907

{JSON_InfoFile}
-----7e13971310878
Content-Disposition: form-data; name="infoFile";
Content-Type: application/octet-stream
Content-Length: 9907

.....`..C.....
..
..... $.' ",#..(7),01444.'9=82<.342...C. ....
-----7e13971310878--
```

A.182 /ISAPI/AccessControl/OfflineCapture/InfoFileTemplateDownload? format=json

Download the user list template of offline collection.

Request URI Definition

Table A-224 POST /ISAPI/AccessControl/OfflineCapture/InfoFileTemplateDownload?format=json

Method	POST
Description	Download the user list template of offline collection.
Query	format: determine the format of request or response message.
Request	<u>JSON_InfoFileTemplateCond</u>
Response	Succeeded: <u>JSON_InfoFileTemplate</u> (opaque data (MIME data)) Failed: <u>JSONResponseStatus</u>

Example

Sample Code of Interaction in URL Format

```
POST /ISAPI/AccessControl/OfflineCapture/InfoFileTemplate/DownloadTask?
format=json
Accept: text/html, application/xhtml+xml,
Accept-Language: en-US
Content-Type: application/xml
```

```
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

{
  "InfoFileTemplateCond": {
    "dataType ":"binary"
  /*required, string, data type of the file: "url"-URL, "binary"-binary data*/
  }
}

-----
HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type: application/xml; charset=UTF-8
Content-Length: text_length

{
  "InfoFileTemplate": {
    "dataType ":"binary",
  /*required, string, data type of the file: "url"-URL, "binary"-binary data*/
    "fileUrl": ""
  /*dependent, string, file URL, this field is valid when dataType is "url"*/
  }
}
```

Example

Sample Code of Interaction in Binary Format

```
POST /ISAPI/AccessControl/OfflineCapture/InfoFileTemplate/DownloadTask?
format=json
Accept: text/html, application/xhtml+xml,
Accept-Language: en-US
Content-Type: application/xml
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.36.29:8080
Content-Length: 9907
Connection: Keep-Alive
Cache-Control: no-cache

{
  "InfoFileTemplateCond": {
    "dataType ":"binary"
  /*required, string, data type of the file: "url"-URL, "binary"-binary data*/
  }
```

```
}

-----
-----
HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type: multipart/form-data; boundary=<frontier>
Content-Length: all_length

--<frontier>
Content-Type: application/json; charset="UTF-8"
Content-Length: text_length

{JSON_InfoFileTemplate}
--<frontier>
Content-Disposition: form-data; name="infoFileTemplate";
filename="infoFileTemplate.xx "
Content-Type: image/jpeg //The Content-Type can be defined according to the
file and standard MIME type
Content-Length: image_length

[File Data]
--<frontier>--
```

A.183 /ISAPI/AccessControl/OfflineCapture/progress?format=json

Get the offline collection progress.

Request URI Definition

Table A-225 GET /ISAPI/AccessControl/OfflineCapture/progress?format=json

Method	GET
Description	Get the offline collection progress.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_CaptureProgress</u> Failed: <u>JSON_ResponseStatus</u>

A.184 /ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json

Get or set the parameters of offline collection rules.

Request URI Definition

Table A-226 GET /ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json

Method	GET
Description	Get the parameters of offline collection rules.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_RuleInfo</i> Failed: <i>JSON_ResponseStatus</i>

Table A-227 PUT /ISAPI/AccessControl/OfflineCapture/ruleInfo?format=json

Method	PUT
Description	Set the parameters of offline collection rules.
Query	format: determine the format of request or response message.
Request	<i>JSON_RuleInfo</i>
Response	<i>JSON_ResponseStatus</i>

A.185 /ISAPI/AccessControl/OfflineCapture/uploadFailedDetails? format=json

Get the details of failing to upload the user list of offline collection.

Request URI Definition

Table A-228 GET /ISAPI/AccessControl/OfflineCapture/uploadFailedDetails?format=json

Method	GET
Description	Get the details of failing to upload the user list of offline collection.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_UploadFailedDetails</i> Failed: <i>JSON_ResponseStatus</i>

A.186 /ISAPI/AccessControl/OSDPMModify/<ID>?format=json

Set the OSDP (Open Supervised Device Protocol) card reader ID.

Request URI Definition

Table A-229 PUT /ISAPI/AccessControl/OSDPMModify/<ID>?format=json

Method	PUT
Description	Set the OSDP (Open Supervised Device Protocol) card reader ID.
Query	format: determine the format of request or response message.
Request	<u>JSON OSDPModify</u>
Response	<u>JSONResponseStatus</u>

Remarks

The <ID> in the request URI refers to the original OSDP card reader ID which is between 0 and 126, and 127 refers to broadcast.

A.187 /ISAPI/AccessControl/OSDPMModify/capabilities?format=json

Get the capability of editing the OSDP (Open Supervised Device Protocol) card reader ID.

Request URI Definition

Table A-230 GET /ISAPI/AccessControl/OSDPMModify/capabilities?format=json

Method	GET
Description	Get the capability of editing the OSDP (Open Supervised Device Protocol) card reader ID.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap OSDPModify</u> Failed: <u>JSONResponseStatus</u>

A.188 /ISAPI/AccessControl/OSDPStatus/<ID>?format=json

Get the OSDP (Open Supervised Device Protocol) card reader status.

Request URI Definition

Table A-231 GET /ISAPI/AccessControl/OSDPStatus/<ID>?format=json

Method	GET
Description	Get the OSDP (Open Supervised Device Protocol) card reader status.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_OSDPStatus</i> Failed: <i>JSONResponseStatus</i>

Remarks

The <ID> in the request URI refers to the OSDP card reader ID which is between 0 and 126, and 127 refers to broadcast. Limited by the device, the OSDP card reader status can only be obtained one by one.

A.189 /ISAPI/AccessControl/OSDPStatus/capabilities?format=json

Get the capability of getting the OSDP (Open Supervised Device Protocol) card reader status.

Request URI Definition

Table A-232 GET /ISAPI/AccessControl/OSDPStatus/capabilities?format=json

Method	GET
Description	Get the capability of getting the OSDP (Open Supervised Device Protocol) card reader status.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_OSDPStatus</i> Failed: <i>JSONResponseStatus</i>

A.190 /ISAPI/AccessControl/personInfoExtendName/capabilities?format=json

Get the configuration capability of the name of the additional person information.

Request URI Definition

Table A-233 GET /ISAPI/AccessControl/personInfoExtendName/capabilities?format=json

Method	GET
Description	Get the configuration capability of the name of the additional person information.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_PersonInfoExtendNameCap</u> Failed: <u>JSONResponseStatus</u>

A.191 /ISAPI/AccessControl/personInfoExtendName?format=json

Get or set the parameters of the name of the additional person information.

Request URI Definition

Table A-234 GET /ISAPI/AccessControl/personInfoExtendName?format=json

Method	GET
Description	Get the parameters of the name of the additional person information.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_PersonInfoExtendName</u> Failed: <u>JSONResponseStatus</u>

Table A-235 PUT /ISAPI/AccessControl/personInfoExtendName?format=json

Method	PUT
Description	Set the parameters of the name of the additional person information.
Query	format: determine the format of request or response message.
Request	<u>JSON_PersonInfoExtendName</u>
Response	<u>JSONResponseStatus</u>

A.192 /ISAPI/AccessControl/PhoneDoorRightCfg/<ID>?format=json

Operations about the configuration of the door permission linked to the mobile phone number.

Request URI Definition

Table A-236 GET /ISAPI/AccessControl/PhoneDoorRightCfg/<ID>?format=json

Method	GET
Description	Get the configuration parameters of the door permission linked to the mobile phone number.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_PhoneDoorRightCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-237 PUT /ISAPI/AccessControl/PhoneDoorRightCfg/<ID>?format=json

Method	PUT
Description	Set the parameters of the door permission linked to the mobile phone number.
Query	format: determine the format of request or response message.
Request	<u>JSON_PhoneDoorRightCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the No. of the mobile phone number allowlist.

A.193 /ISAPI/AccessControl/PhoneDoorRightCfg/capabilities? format=json

Get the configuration capability of the door permission linked to the mobile phone number.

Request URI Definition

Table A-238 GET /ISAPI/AccessControl/PhoneDoorRightCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the door permission linked to the mobile phone number.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_PhoneDoorRightCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.194 /ISAPI/AccessControl/QRCodeEvent/capabilities?format=json

Get the capability of actively getting QR code scanning events.

Request URI Definition

Table A-239 GET /ISAPI/AccessControl/QRCodeEvent/capabilities?format=json

Method	GET
Description	Get the capability of actively getting QR code scanning events.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_QRCodeEventCap</u> Failed: <u>JSON_ResponseStatus</u>

A.195 /ISAPI/AccessControl/QRCodeEvent?format=json

Get QR code scanning events actively.

Request URI Definition

Table A-240 POST /ISAPI/AccessControl/QRCodeEvent?format=json

Method	POST
Description	Get QR code scanning events actively.

Query	format: determine the format of request or response message.
Request	<u>JSON_QRCodeEventCond</u>
Response	Succeeded: <u>JSON_QRCodeEvent</u> Failed: <u>JSON_ResponseStatus</u>

A.196 /ISAPI/AccessControl/ReaderAcrossHost

Operations about the cross-controller anti-passing back configuration of card readers.

Request URI Definition

Table A-241 GET /ISAPI/AccessControl/ReaderAcrossHost

Method	GET
Description	Get the cross-controller anti-passing back parameters of card readers.
Query	None.
Request	None.
Response	Succeeded: <u>XML_ReaderAcrossHost</u> Failed: <u>XML_ResponseStatus</u>

Table A-242 PUT /ISAPI/AccessControl/ReaderAcrossHost

Method	PUT
Description	Set the cross-controller anti-passing back parameters of card readers.
Query	None.
Request	<u>XML_ReaderAcrossHost</u>
Response	<u>XML_ResponseStatus</u>

A.197 /ISAPI/AccessControl/ReaderAcrossHost/capabilities

Get the configuration capability of cross-controller anti-passing back status of card readers.

Request URI Definition

Table A-243 GET /ISAPI/AccessControl/ReaderAcrossHost/capabilities

Method	GET
Description	Get the configuration capability of cross-controller anti-passing back status of card readers.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_ReaderAcrossHost</u> Failed: <u>XML_ResponseStatus</u>

A.198 /ISAPI/AccessControl/remoteCheck/capabilities?format=json

Get the capability of verifying the access control event remotely.

Request URI Definition

Table A-244 GET /ISAPI/AccessControl/remoteCheck/capabilities?format=json

Method	GET
Description	Get the capability of verifying the access control event remotely.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_RemoteCheck</u> Failed: <u>JSON_ResponseStatus</u>

A.199 /ISAPI/AccessControl/remoteCheck?format=json

Verify the access control event remotely.

Request URI Definition

Table A-245 PUT /ISAPI/AccessControl/remoteCheck?format=json

Method	PUT
Description	Verify the access control event remotely to control opening or closing the door.
Query	format: determine the format of request or response message.
Request	<u>JSON_RemoteCheck</u>
Response	<u>JSON_ResponseStatus</u>

A.200 /ISAPI/AccessControl/RemoteControl/buzzer/<ID>?format=json

Remotely control the buzzer of the card reader.

Request URI Definition

Table A-246 PUT /ISAPI/AccessControl/RemoteControl/buzzer/<ID>?format=json

Method	PUT
Description	Remotely control the buzzer of the card reader.
Query	format: determine the format of request or response message.
Request	<u>JSON_RemoteControlBuzzer</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the buzzer No., which is also the No. of the card reader. If the <ID> is 65535, it refers to all buzzers (card readers).

A.201 /ISAPI/AccessControl/RemoteControl/buzzer/capabilities? format=json

Get the capability of remotely controlling the buzzer of the card reader.

Request URI Definition

Table A-247 GET /ISAPI/AccessControl/RemoteControl/buzzer/capabilities?format=json

Method	GET
Description	Get the capability of remotely controlling the buzzer of the card reader.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_RemoteControlBuzzer</u> Failed: <u>JSON_ResponseStatus</u>

A.202 /ISAPI/AccessControl/RemoteControl/door/<ID>

Remotely control the door or elevator.

Request URI Definition

Table A-248 PUT /ISAPI/AccessControl/RemoteControl/door/<ID>

Method	PUT
Description	Remotely control the door or elevator.
Query	None.
Request	<u>XML_RemoteControlDoor</u>
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the door No. If the <ID> is 65535, it refers to all doors.

A.203 /ISAPI/AccessControl/RemoteControl/door/capabilities

Get the capability of remotely controlling the door or elevator.

Request URI Definition

Table A-249 GET /ISAPI/AccessControl/RemoteControl/door/capabilities

Method	GET
Description	Get the capability of remotely controlling the door or elevator.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_RemoteControlDoor</u> Failed: <u>XML_ResponseStatus</u>

A.204 /ISAPI/AccessControl/remoteControlPWCheck/capabilities? format=json

Get the capability of verifying the password for remote door control.

Request URI Definition

Table A-250 GET /ISAPI/AccessControl/remoteControlPWCheck/capabilities?format=json

Method	GET
Description	Get the capability of verifying the password for remote door control.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_RemoteControlPWCheck</u> Failed: <u>JSON_ResponseStatus</u>

A.205 /ISAPI/AccessControl/remoteControlPWCheck/door/<ID>? format=json

Verify the password for remote door control.

Request URI Definition

Table A-251 PUT /ISAPI/AccessControl/remoteControlPWCheck/door/<ID>?format=json

Method	PUT
Description	Verify the password for remote door control.
Query	format: determine the format of request or response message.
Request	<u>JSON_RemoteControlPWCheck</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the door No.

A.206 /ISAPI/AccessControl/remoteControlPWCfg/capabilities? format=json

Get the capability of configuring password for remote door control.

Request URI Definition

Table A-252 GET /ISAPI/AccessControl/remoteControlPWCfg/capabilities?format=json

Method	GET
Description	Get the capability of configuring password for remote door control.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_RemoteControlPWCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.207 /ISAPI/AccessControl/remoteControlPWCfg/door/<ID>? format=json

Configure the password for remote door control.

Request URI Definition

Table A-253 PUT /ISAPI/AccessControl/remoteControlPWCfg/door/<ID>?format=json

Method	PUT
Description	Configure the password for remote door control.
Query	format: determine the format of request or response message.
Request	<u>JSON_RemoteControlPWCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

- The <ID> in the request URI refers to the door No.
- The password for remote door control can be configured only after the password is verified by the request URI: [PUT /ISAPI/AccessControl/remoteControlPWCheck/door/<ID>?format=json](#).

A.208 /ISAPI/AccessControl/ServerDevice

Operation about the configuration of cross-controller anti-passing back server information.

Request URI Definition

Table A-254 GET /ISAPI/AccessControl/ServerDevice

Method	GET
Description	Get the information (i.e., IP address and port No.) of the cross-controller anti-passing back server.
Query	None.
Request	None.
Response	Succeeded: <u>XML_ServerDevice</u> Failed: <u>XML_ResponseStatus</u>

Table A-255 PUT /ISAPI/AccessControl/ServerDevice

Method	PUT
Description	Set the information (i.e., IP address and port No.) of the cross-controller anti-passing back server.
Query	None.

Request	<u>XML_ServerDevice</u>
Response	<u>XML_ResponseStatus</u>

A.209 /ISAPI/AccessControl/ServerDevice/capabilities

Get the configuration capability of cross-controller anti-passing back server information.

Request URI Definition

Table A-256 GET /ISAPI/AccessControl/ServerDevice/capabilities

Method	GET
Description	Get the configuration capability of cross-controller anti-passing back server information.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_ServerDevice</u> Failed: <u>XML_ResponseStatus</u>

A.210 /ISAPI/AccessControl/showHealthCodeCfg/capabilities?format=json

Get the configuration capability of health code display parameters.

Request URI Definition

Table A-257 GET /ISAPI/AccessControl/showHealthCodeCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of health code display parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_HealthCodeDisplayCfg</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

When the device does not display the health code for privacy reasons after getting it, whether to open the door for the person is determined by the health code type.

A.211 /ISAPI/AccessControl/showHealthCodeCfg?format=json

Get or set the health code display parameters.

Request URI Definition

Table A-258 GET /ISAPI/AccessControl/showHealthCodeCfg?format=json

Method	GET
Description	Get the health code display parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_HealthCodeDisplayCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-259 PUT /ISAPI/AccessControl/showHealthCodeCfg?format=json

Method	PUT
Description	Set the health code display parameters.
Query	format: determine the format of request or response message.
Request	<u>JSON_HealthCodeDisplayCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.212 /ISAPI/AccessControl/SmsRelativeParam/capabilities?format=json

Get the configuration capability of the SMS (Short Message Service) function.

Request URI Definition

Table A-260 GET /ISAPI/AccessControl/SmsRelativeParam/capabilities?format=json

Method	GET
Description	Get the configuration capability of the SMS (Short Message Service) function.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_SmsRelativeParam</u> Failed: <u>JSON_ResponseStatus</u>

A.213 /ISAPI/AccessControl/SmsRelativeParam?format=json

Operations about the SMS (Short Message Service) function configuration.

Request URI Definition

Table A-261 GET /ISAPI/AccessControl/SmsRelativeParam?format=json

Method	GET
Description	Get the configuration parameters of the SMS (Short Message Service) function.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_SmsRelativeParam</u> Failed: <u>JSON_ResponseStatus</u>

Table A-262 PUT /ISAPI/AccessControl/SmsRelativeParam?format=json

Method	PUT
Description	Set the parameters of the SMS (Short Message Service) function.
Query	format: determine the format of request or response message.
Request	<u>JSON_SmsRelativeParam</u>
Response	<u>JSON_ResponseStatus</u>

A.214 /ISAPI/AccessControl/SnapConfig

Get capture triggering parameters.

Request URI Definition

Table A-263 GET /ISAPI/AccessControl/SnapConfig

Method	GET
Description	Get capture triggering parameters.
Query	None
Request	None
Response	Succeeded: <i>XML_SnapConfig</i> Failed: <i>XML_ResponseStatus</i>

A.215 /ISAPI/AccessControl/SnapConfig/capabilities

Get capability of getting capture triggering parameters.

Request URI Definition

Table A-264 GET /ISAPI/AccessControl/SnapConfig/capabilities

Method	GET
Description	Get capability of getting capture triggering parameters.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_SnapConfig</i> Failed: <i>XML_ResponseStatus</i>

A.216 /ISAPI/AccessControl/StartReaderInfo

Operations about first card reader configurations.

Request URI Definition

Table A-265 GET /ISAPI/AccessControl/StartReaderInfo

Method	GET
Description	Get the configuration parameters of first card reader.
Query	None.
Request	None.
Response	<u>XML_StartReaderInfo</u>

Table A-266 PUT /ISAPI/AccessControl/StartReaderInfo

Method	PUT
Description	Set the parameters of first card reader.
Query	None.
Request	<u>XML_StartReaderInfo</u>
Response	<u>XML_ResponseStatus</u>

A.217 /ISAPI/AccessControl/StartReaderInfo/capabilities

Get the configuration capability of the first card reader.

Request URI Definition

Table A-267 GET /ISAPI/AccessControl/StartReaderInfo/capabilities

Method	GET
Description	Get the configuration capability of the first card reader.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_StartReaderInfo</u> Failed: <u>XML_ResponseStatus</u>

A.218 /ISAPI/AccessControl/SubmarineBack

Operations about the configuration of the cross-controller anti-passing back server.

Request URI Definition

Table A-268 GET /ISAPI/AccessControl/SubmarineBack

Method	GET
Description	Get the configuration parameters of the cross-controller anti-passing back server.
Query	None.
Request	None.
Response	Succeeded: <i>XML_SubmarineBack</i> Failed: <i>XML_ResponseStatus</i>

Table A-269 PUT /ISAPI/AccessControl/SubmarineBack

Method	PUT
Description	Set the parameters of the cross-controller anti-passing back server.
Query	None.
Request	<i>XML_SubmarineBack</i>
Response	<i>XML_ResponseStatus</i>

A.219 /ISAPI/AccessControl/SubmarineBack/capabilities

Get the configuration capability of the cross-controller anti-passing back server.

Request URI Definition

Table A-270 GET /ISAPI/AccessControl/SubmarineBack/capabilities

Method	GET
Description	Get the configuration capability of the cross-controller anti-passing back server.
Query	None.

Request	None.
Response	Succeeded: <u>XML_Cap_SubmarineBack</u> Failed: <u>XML_ResponseStatus</u>

A.220 /ISAPI/AccessControl/SubmarineBackHostInfo/capabilities

Get the configuration capability of access controllers for cross-controller anti-passing back.

Request URI Definition

Table A-271 GET /ISAPI/AccessControl/SubmarineBackHostInfo/capabilities

Method	GET
Description	Get the configuration capability of access controllers for cross-controller anti-passing back.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_SubmarineBackHostInfo</u> Failed: <u>XML_ResponseStatus</u>

A.221 /ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>

Operations about the configuration of access controllers for cross-controller anti-passing back.

Request URI Definition

Table A-272 GET /ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>

Method	GET
Description	Get the parameters of access controllers for cross-controller anti-passing back.
Query	None.
Request	None.
Response	Succeeded: <u>XML_SubmarineBackHostInfo</u> Failed: <u>XML_ResponseStatus</u>

Table A-273 PUT /ISAPI/AccessControl/SubmarineBackHostInfo/ConfigureNo/<ID>

Method	PUT
Description	Set the parameters of access controllers for cross-controller anti-passing back.
Query	None.
Request	<u>XML_SubmarineBackHostInfo</u>
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the configuration No., which is between 1 and 4. More specifically, 1 refers to device No.1 to device No.16, 2 refers to device No.17 to device No.32, 3 refers to device No.33 to device No.48, and 4 refers to device No.49 to device No.64.

A.222 /ISAPI/AccessControl/SubmarineBackMode

Operations about the configuration of cross-controller anti-passing back mode and rule.

Request URI Definition

Table A-274 GET /ISAPI/AccessControl/SubmarineBackMode

Method	GET
Description	Get the parameters of cross-controller anti-passing back mode and rule.
Query	None.
Request	None.
Response	Succeeded: <u>XML_SubmarineBackMode</u> Failed: <u>XML_ResponseStatus</u>

Table A-275 PUT /ISAPI/AccessControl/SubmarineBackMode

Method	PUT
Description	Set the parameters of cross-controller anti-passing back mode and rule.
Query	None.

Request	<u>XML_SubmarineBackMode</u>
Response	<u>XML_ResponseStatus</u>

A.223 /ISAPI/AccessControl/SubmarineBackMode/capabilities

Get the configuration capability of cross-controller anti-passing back mode and rule.

Request URI Definition

Table A-276 GET /ISAPI/AccessControl/SubmarineBackMode/capabilities

Method	GET
Description	Get the configuration capability of cross-controller anti-passing back mode and rule.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_SubmarineBackMode</u> Failed: <u>XML_ResponseStatus</u>

A.224 /ISAPI/AccessControl/SubmarineBackReader/capabilities

Get the configuration capability of card readers for cross-controller anti-passing back.

Request URI Definition

Table A-277 GET /ISAPI/AccessControl/SubmarineBackReader/capabilities

Method	GET
Description	Get the configuration capability of card readers for cross-controller anti-passing back.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_SubmarineBackReader</u> Failed: <u>XML_ResponseStatus</u>

A.225 /ISAPI/AccessControl/SubmarineBackReader/ConfigureNo/<ID>

Operations about the configuration of card readers for cross-controller anti-passing back.

Request URI Definition

Table A-278 GET /ISAPI/AccessControl/SubmarineBackReader/ConfigureNo/<ID>

Method	GET
Description	Get the parameters of card readers for cross-controller anti-passing back.
Query	None.
Request	None.
Response	Succeeded: <i>XML_SubmarineBackReader</i> Failed: <i>XML_ResponseStatus</i>

Table A-279 PUT /ISAPI/AccessControl/SubmarineBackReader/ConfigureNo/<ID>

Method	PUT
Description	Set the parameters of card readers for cross-controller anti-passing back.
Query	None.
Request	<i>XML_SubmarineBackReader</i>
Response	<i>XML_ResponseStatus</i>

Remarks

The <ID> in the request URI refers to the configuration No., which is between 1 and 128.

A.226 /ISAPI/AccessControl/temperatureMeasureAreaCalibration/capabilities?format=json

Get the calibration configuration capability of the temperature measurement area.

Request URI Definition

Table A-280 GET /ISAPI/AccessControl/temperatureMeasureAreaCalibration/capabilities?format=json

Method	GET
Description	Get the calibration configuration capability of the temperature measurement area.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_Cap_RegionCalibrationCfg</i> Failed: <i>JSON_ResponseStatus</i>

Remarks

Calibrating the temperature measurement area can be used to check whether the face position located by the rectangle frame is accurate during thermography.

A.227 /ISAPI/AccessControl/temperatureMeasureAreaCalibration?format=json

Get or set the calibration parameters of the temperature measurement area.

Request URI Definition

Table A-281 GET /ISAPI/AccessControl/temperatureMeasureAreaCalibration?format=json

Method	GET
Description	Get the calibration parameters of the temperature measurement area.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_RegionCalibrationCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-282 PUT /ISAPI/AccessControl/temperatureMeasureAreaCalibration?format=json

Method	PUT
Description	Set the calibration parameters of the temperature measurement area.
Query	format: determine the format of request or response message.
Request	<u>JSON_RegionCalibrationCfg</u>
Response	<u>JSON_ResponseStatus</u>

A.228 /ISAPI/AccessControl/temperatureMeasureAreaCfg/capabilities?format=json

Get the configuration capability of the temperature measurement area.

Request URI Definition

Table A-283 GET /ISAPI/AccessControl/temperatureMeasureAreaCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of the temperature measurement area.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_RegionCoordinate</u> Failed: <u>JSON_ResponseStatus</u>

A.229 /ISAPI/AccessControl/temperatureMeasureAreaCfg?format=json

Get or set the parameters of the temperature measurement area.

Request URI Definition

Table A-284 GET /ISAPI/AccessControl/temperatureMeasureAreaCfg?format=json

Method	GET
Description	Get the parameters of the temperature measurement area.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_RegionCoordinate</u> Failed: <u>JSON_ResponseStatus</u>

Table A-285 PUT /ISAPI/AccessControl/temperatureMeasureAreaCfg?format=json

Method	PUT
Description	Set the parameters of the temperature measurement area.
Query	format: determine the format of request or response message.
Request	<u>JSON_RegionCoordinate</u>
Response	<u>JSON_ResponseStatus</u>

A.230 /ISAPI/AccessControl/temperatureMeasureCfg/capabilities?format=json

Get the configuration capability of temperature measurement parameters.

Request URI Definition

Table A-286 GET /ISAPI/AccessControl/temperatureMeasureCfg/capabilities?format=json

Method	GET
Description	Get the configuration capability of temperature measurement parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_TemperatureMeasurementCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.231 /ISAPI/AccessControl/temperatureMeasureCfg?format=json

Get or set the temperature measurement parameters.

Request URI Definition

Table A-287 GET /ISAPI/AccessControl/temperatureMeasureCfg?format=json

Method	GET
Description	Get the temperature measurement parameters.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <i>JSON_TemperatureMeasurementCfg</i> Failed: <i>JSON_ResponseStatus</i>

Table A-288 PUT /ISAPI/AccessControl/temperatureMeasureCfg?format=json

Method	PUT
Description	Set the temperature measurement parameters.
Query	format: determine the format of request or response message.
Request	<i>JSON_TemperatureMeasurementCfg</i>
Response	<i>JSON_ResponseStatus</i>

A.232 /ISAPI/AccessControl/userData?secretkey=

Import or export person permission data securely.

Request URI Definition

Table A-289 GET /ISAPI/AccessControl/userData?secretkey=

Method	GET
Description	Export person permission data securely.
Query	secretkey: the verification key, it is provided by the upper layer. It should be encrypted for exporting and recorded for importing. security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode.

	iv : the initialization vector, and it is required when security is 1 or 2.
Request	None.
Response	Succeeded: Opaque data. Failed: <u>XMLResponseStatus</u>

Table A-290 POST /ISAPI/AccessControl/userData?secretkey=

Method	POST
Description	Import person permission data securely.
Query	secretkey : the verification key, it must be the same as the exported one and should be encrypted for importing. security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. iv : the initialization vector, and it is required when security is 1 or 2.
Request	Opaque data.
Response	<u>XMLResponseStatus</u>

Remarks

The person permission data include permission data of the person's card, face, fingerprint, etc.

A.233 /ISAPI/AccessControl/UserInfo/capabilities?format=json

Get the person management capability.

Request URI Definition

Table A-291 GET /ISAPI/AccessControl/UserInfo/capabilities?format=json

Method	GET
Description	Get the person management capability.
Query	format : determine the format of request or response message. terminalNo : dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after

	information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_UserInfo</u> Failed: <u>JSON_ResponseStatus</u>

A.234 /ISAPI/AccessControl/UserInfo/Count?format=json

Get the total number of the added persons.

Request URI Definition

Table A-292 GET /ISAPI/AccessControl/UserInfo/Count?format=json

Method	GET
Description	Get the total number of the added persons.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_UserInfoCount</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.235 /ISAPI/AccessControl/UserInfo/Delete?format=json

Delete person information only.

Request URI Definition

Table A-293 PUT /ISAPI/AccessControl/UserInfo/Delete?format=json

Method	PUT
Description	Delete person information only.
Query	format: determine the format of request or response message.
Request	<u>JSON_UserInfoDelCond</u>
Response	<u>JSON_ResponseStatus</u>

A.236 /ISAPI/AccessControl/UserInfo/Modify?format=json

Edit person information.

Request URI Definition

Table A-294 PUT /ISAPI/AccessControl/UserInfo/Modify?format=json

Method	PUT
Description	Edit person information.
Query	format: determine the format of request or response message.
Request	<u>JSON_UserInfo</u>
Response	<u>JSON_ResponseStatus</u>

A.237 /ISAPI/AccessControl/UserInfo/Record?format=json

Add a person.

Request URI Definition

Table A-295 POST /ISAPI/AccessControl/UserInfo/Record?format=json

Method	POST
Description	Add a person.
Query	format: determine the format of request or response message.

Request	<u>JSON_UserInfo</u>
Response	<u>JSON_ResponseStatus</u>

A.238 /ISAPI/AccessControl/UserInfo/Search?format=json

Search for person information.

Request URI Definition

Table A-296 POST /ISAPI/AccessControl/UserInfo/Search?format=json

Method	POST
Description	Search for person information.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	<u>JSON_UserInfoSearchCond</u>
Response	<u>JSON_UserInfoSearch</u>

Remarks

The Request (user information search condition JSON_UserInfoSearchCond) depends on the user information capability JSON_Cap_UserInfo (related node: <UserInfoSearchCond>).

A.239 /ISAPI/AccessControl/UserInfo/SetUp?format=json

Set person information.

Request URI Definition

Table A-297 PUT /ISAPI/AccessControl/UserInfo/SetUp?format=json

Method	PUT
Description	Set person information.
Query	format: determine the format of request or response message.

Request	<u>JSON.UserInfo</u>
Response	<u>JSONResponseStatus</u>

Remarks

- If the device has checked that the person does not exist according to the employee No. (person ID), the person information will be added.
- If the device has checked that the person already exists according to the employee No. (person ID), the person information will be edited.
- If a person needs to be deleted, the **deleteUser** in the message JSON.UserInfo should be set to "true", and the success response message will be returned no matter whether the person information exists or not. Deleting the person will only delete the person's information and will not delete the linked cards, fingerprints, and face information.

A.240 /ISAPI/AccessControl/UserInfoDetail/Delete/capabilities?format=json

Get the capability of deleting person information (including linked cards, fingerprints, and faces) and permissions.

Request URI Definition

Table A-298 GET /ISAPI/AccessControl/UserInfoDetail/Delete/capabilities?format=json

Method	GET
Description	Get the capability of deleting person information (including linked cards, fingerprints, and faces) and permissions.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap.UserInfoDetail</u> Failed: <u>JSONResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.241 /ISAPI/AccessControl/UserInfoDetail/Delete?format=json

Start deleting all person information and permissions by employee No.

Request URI Definition

Table A-299 PUT /ISAPI/AccessControl/UserInfoDetail/Delete?format=json

Method	PUT
Description	Start deleting all person information (including linked cards, fingerprints, and faces) and permissions by employee No.
Query	format: determine the format of request or response message.
Request	<u>JSON.UserInfoDetail</u>
Response	<u>JSON.ResponseStatus</u>

Remarks

- This URI is only used to start deleting. To check whether the deleting is completed, you should call the request URI [/ISAPI/AccessControl/UserInfoDetail/DeleteProcess?format=json](#) by GET method to get the deleting status.
- This URI is not supported by integration of information release system.

A.242 /ISAPI/AccessControl/UserInfoDetail/DeleteProcess?format=json

Get the status of deleting all person information and permissions by employee No.

Request URI Definition

Table A-300 GET /ISAPI/AccessControl/UserInfoDetail/DeleteProcess?format=json

Method	GET
Description	Get the status of deleting all person information (including linked cards, fingerprints, and faces) and permissions by employee No.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.

Request	None.
Response	Succeeded: <u>JSON_UserInfoDetailDeleteProcess</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- When starting deleting all person information (including linked cards, fingerprints, and faces) and permissions by employee No., this URI will be repeatedly called to get the deleting status until "success" or "failed" is returned by the parameter **status** in the message [JSON_UserInfoDetailDeleteProcess](#).
- This URI is not supported by integration of information release system.

A.243 /ISAPI/AccessControl/UserRightHolidayPlanCfg/capabilities?format=json

Get the holiday schedule configuration capability of the access permission control.

Request URI Definition

Table A-301 GET /ISAPI/AccessControl/UserRightHolidayPlanCfg/capabilities?format=json

Method	GET
Description	Get the holiday schedule configuration capability of the access permission control.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_UserRightHolidayPlanCfa</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.244 /ISAPI/AccessControl/UserRightWeekPlanCfg/capabilities? format=json

Get the week schedule configuration capability of the access permission control.

Request URI Definition

Table A-302 GET /ISAPI/AccessControl/UserRightWeekPlanCfg/capabilities?format=json

Method	GET
Description	Get the week schedule configuration capability of the access permission control.
Query	format : determine the format of request or response message. terminalNo : dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_UserRightWeekPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.245 /ISAPI/AccessControl/UserRightHolidayGroupCfg/<GroupNo> format=json

Operations about the holiday group configuration of the access permission control schedule.

Request URI Definition

Table A-303 GET /ISAPI/AccessControl/UserRightHolidayGroupCfg/<GroupNo>?format=json

Method	GET
Description	Get the holiday group configuration parameters of the access permission control schedule.

Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No. <GroupNo>: int, holiday group ID, start from 1.
Request	None.
Response	Succeeded: <u>JSON UserRightHolidayGroupCfg</u> Failed: <u>JSON ResponseStatus</u>

Table A-304 PUT /ISAPI/AccessControl/UserRightHolidayGroupCfg/<GroupNo>?format=json

Method	PUT
Description	Set the holiday group parameters of the access permission control schedule.
Query	format: determine the format of request or response message. <GroupNo>: int, holiday group ID, start from 1.
Request	<u>JSON UserRightHolidayGroupCfg</u>
Response	<u>JSON ResponseStatus</u>

Remarks

- The **<GroupNo>** in the request URI refers to the holiday group No. which starts from 1, and you can get the maximum number of the holiday groups supported by the device from the holiday group configuration capability of the access permission control schedule ([JSON Cap UserRightHolidayGroupCfg](#)).
- This URI is not supported by integration of information release system.

A.246 /ISAPI/AccessControl/UserRightHolidayGroupCfg/capabilities?format=json

Get the holiday group configuration capability of the access permission control schedule.

Request URI Definition

Table A-305 GET /ISAPI/AccessControl/UserRightHolidayGroupCfg/capabilities?format=json

Method	GET
Description	Get the holiday group configuration capability of the access permission control schedule.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_UserRightHolidayGroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.247 /ISAPI/AccessControl/UserRightHolidayPlanCfg/<PlanNo>?format=json

Operations about the holiday schedule configuration of the access permission control.

Request URI Definition

Table A-306 GET /ISAPI/AccessControl/UserRightHolidayPlanCfg/<PlanNo>?format=json

Method	GET
Description	Get the holiday schedule configuration parameters of the access permission control.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.

	<PlanNo>: int, holiday schedule ID.
Request	None.
Response	Succeeded: <u>JSON_UserRightHolidayPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-307 PUT /ISAPI/AccessControl/UserRightHolidayPlanCfg/<PlanNo>?format=json

Method	PUT
Description	Set the holiday schedule parameters of the access permission control.
Query	format: determine the format of request or response message. <PlanNo>: int, holiday schedule ID.
Request	<u>JSON_UserRightHolidayPlanCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

- The <PlanNo> in the request URI refers to the holiday schedule No. which starts from 1, and you can get the maximum number of the holiday schedules supported by the device from the holiday schedule configuration capability of the access permission control ([JSON_Cap_UserRightHolidayPlanCfg](#)).
- This URI is not supported by integration of information release system.

A.248 /ISAPI/AccessControl/UserRightPlanTemplate/<TemplateNo>?format=json

Operations about the schedule template configuration of the access permission control.

Request URI Definition

Table A-308 GET /ISAPI/AccessControl/UserRightPlanTemplate/<TemplateNo>?format=json

Method	GET
Description	Get the schedule template configuration parameters of the access permission control.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management

	server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No. <TemplateNo> : int, schedule template ID, start from 1.
Request	None.
Response	Succeeded: <u>JSON_UserRightPlanTemplate</u> Failed: <u>JSON_ResponseStatus</u>

Table A-309 PUT /ISAPI/AccessControl/UserRightPlanTemplate/<TemplateNo>?format=json

Method	PUT
Description	Set the schedule template parameters of the access permission control.
Query	format : determine the format of request or response message. <TemplateNo> : int, schedule template ID, start from 1.
Request	<u>JSON_UserRightPlanTemplate</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

- The **<TemplateNo>** in the request URI refers to the schedule template No. which starts from 1, and you can get the maximum number of the templates supported by the device from the schedule template configuration capability of the access permission control ([JSON_Cap_UserRightPlanTemplate](#)).
- This URI is not supported by integration of information release system.

A.249 /ISAPI/AccessControl/UserRightPlanTemplate/capabilities? format=json

Get the schedule template configuration capability of the access permission control.

Request URI Definition

Table A-310 GET /ISAPI/AccessControl/UserRightPlanTemplate/capabilities?format=json

Method	GET
Description	Get the schedule template configuration capability of the access permission control.
Query	format : determine the format of request or response message.

	terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_Cap_UserRightPlanTemplate</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.250 /ISAPI/AccessControl/UserRightWeekPlanCfg/<PlanNo>?format=json

Operations about the week schedule configuration of the access permission control.

Request URI Definition

Table A-311 GET /ISAPI/AccessControl/UserRightWeekPlanCfg/<PlanNo>?format=json

Method	GET
Description	Get the week schedule configuration parameters of the access permission control.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No. <PlanNo>: int, week schedule ID.
Request	None.
Response	Succeeded: <u>JSON_UserRightWeekPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-312 PUT /ISAPI/AccessControl/UserRightWeekPlanCfg/<PlanNo>?format=json

Method	PUT
Description	Set the week schedule parameters of the access permission control.
Query	format: determine the format of request or response message. <PlanNo>: int, week schedule ID.
Request	<u>JSON UserRightWeekPlanCfg</u>
Response	<u>JSON ResponseStatus</u>

Remarks

- The **<PlanNo>** in the request URI refers to the week schedule No. which starts from 1, and you can get the maximum number of the week schedules supported by the device from the week schedule configuration capability of the access permission control ([JSON Cap UserRightWeekPlanCfg](#)).
- This URI is not supported by integration of information release system.

A.251 /ISAPI/AccessControl/Verification/ttsText/capabilities? format=json

Get the text configuration capability of the audio prompt for the authentication results.

Request URI Definition

Table A-313 GET /ISAPI/AccessControl/Verification/ttsText/capabilities?format=json

Method	GET
Description	Get the text configuration capability of the audio prompt for the authentication results.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON TTSTextCap</u> Failed: <u>JSON ResponseStatus</u>

A.252 /ISAPI/AccessControl/Verification/ttsText?format=json

Get or set the text parameters of the audio prompt for the authentication results.

Request URI Definition

Table A-314 GET /ISAPI/AccessControl/Verification/ttsText?format=json

Method	GET
Description	Get the text parameters of the audio prompt for the authentication results.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_TTSText</u> Failed: <u>JSON_ResponseStatus</u>

Table A-315 PUT /ISAPI/AccessControl/Verification/ttsText?format=json

Method	PUT
Description	Set the text parameters of the audio prompt for the authentication results.
Query	format: determine the format of request or response message.
Request	<u>JSON_TTSText</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The configured text will be converted to a audio prompt.

A.253 /ISAPI/AccessControl/VerifyHolidayGroupCfg/<GroupNo>?format=json

Operations about the holiday group configuration of the control schedule of the card reader authentication mode.

Request URI Definition

Table A-316 GET /ISAPI/AccessControl/VerifyHolidayGroupCfg/<GroupNo>?format=json

Method	GET
Description	Get the holiday group configuration parameters of the control schedule of the card reader authentication mode.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_VerifyHolidayGroupCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-317 PUT /ISAPI/AccessControl/VerifyHolidayGroupCfg/<GroupNo>?format=json

Method	PUT
Description	Set the holiday group parameters of the control schedule of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_VerifyHolidayGroupCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <GroupNo> in the request URI refers to the holiday group No. which starts from 1, and you can get the maximum number of the holiday groups supported by the device from the holiday group configuration capability of the control schedule of the card reader authentication mode ([JSON_Cap_VerifyHolidayGroupCfg](#)).

A.254 /ISAPI/AccessControl/VerifyHolidayGroupCfg/capabilities? format=json

Get the holiday group configuration capability of the control schedule of the card reader authentication mode.

Request URI Definition

Table A-318 GET /ISAPI/AccessControl/VerifyHolidayGroupCfg/capabilities?format=json

Method	GET
Description	Get the holiday group configuration capability of the control schedule of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_VerifyHolidayGroupCfg</u>

	Failed: <u>JSONResponseStatus</u>
--	---

A.255 /ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json

Operations about the holiday schedule configuration of the card reader authentication mode.

Request URI Definition

Table A-319 GET /ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json

Method	GET
Description	Get the holiday schedule configuration parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_VerifyHolidayPlanCfg</u> Failed: <u>JSONResponseStatus</u>

Table A-320 PUT /ISAPI/AccessControl/VerifyHolidayPlanCfg/<PlanNo>?format=json

Method	PUT
Description	Set the holiday schedule parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_VerifyHolidayPlanCfg</u>
Response	<u>JSONResponseStatus</u>

Remarks

The <PlanNo> in the request URI refers to the holiday schedule No. which starts from 1, and you can get the maximum number of the holiday schedules supported by the device from the holiday schedule configuration capability of the card reader authentication mode ([JSON_Cap_VerifyHolidayPlanCfg](#)).

A.256 /ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities? format=json

Get the holiday schedule configuration capability of the card reader authentication mode.

Request URI Definition

Table A-321 GET /ISAPI/AccessControl/VerifyHolidayPlanCfg/capabilities?format=json

Method	GET
Description	Get the holiday schedule configuration capability of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_VerifyHolidayPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.257 /ISAPI/AccessControl/VerifyPlanTemplate/<TemplateNo> format=json

Operations about the schedule template configuration of the card reader authentication mode.

Request URI Definition

Table A-322 GET /ISAPI/AccessControl/VerifyPlanTemplate/<TemplateNo>?format=json

Method	GET
Description	Get the schedule template configuration parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_VerifyPlanTemplate</u> Failed: <u>JSON_ResponseStatus</u>

Table A-323 PUT /ISAPI/AccessControl/VerifyPlanTemplate/<TemplateNo>?format=json

Method	PUT
Description	Set the schedule template parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_VerifyPlanTemplate</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <TemplateNo> in the request URI refers to the schedule template No. which starts from 1, and you can get the maximum number of the templates supported by the device from the schedule template configuration capability of the card reader authentication mode ([JSON_Cap_VerifyPlanTemplate](#)).

A.258 /ISAPI/AccessControl/VerifyPlanTemplate/capabilities? format=json

Get the schedule template configuration capability of the card reader authentication mode.

Request URI Definition**Table A-324 GET /ISAPI/AccessControl/VerifyPlanTemplate/capabilities?format=json**

Method	GET
Description	Get the schedule template configuration capability of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_VerifyPlanTemplate</u> Failed: <u>JSON_ResponseStatus</u>

A.259 /ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json

Operations about the week schedule configuration of the card reader authentication mode.

Request URI Definition

Table A-325 GET /ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json

Method	GET
Description	Get the week schedule configuration parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_VerifyWeekPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

Table A-326 PUT /ISAPI/AccessControl/VerifyWeekPlanCfg/<PlanNo>?format=json

Method	PUT
Description	Set the week schedule parameters of the card reader authentication mode.
Query	format: determine the format of request or response message.
Request	<u>JSON_VerifyWeekPlanCfg</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

The <PlanNo> in the request URI refers to the week schedule No. which starts from 1, and you can get the maximum number of the week schedules supported by the device from the week schedule configuration capability of the card reader authentication mode ([JSON_Cap_VerifyWeekPlanCfg](#)).

A.260 /ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities? format=json

Get the week schedule configuration capability of the card reader authentication mode.

Request URI Definition

Table A-327 GET /ISAPI/AccessControl/VerifyWeekPlanCfg/capabilities?format=json

Method	GET
Description	Get the week schedule configuration capability of the card reader authentication mode.

Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_VerifyWeekPlanCfg</u> Failed: <u>JSON_ResponseStatus</u>

A.261 /ISAPI/AccessControl/WiegandCfg/capabilities

Get the Wiegand configuration capability.

Request URI Definition

Table A-328 GET /ISAPI/AccessControl/WiegandCfg/capabilities

Method	GET
Description	Get the Wiegand configuration capability.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_WiegandCfg</u> Failed: <u>XML_ResponseStatus</u>

A.262 /ISAPI/AccessControl/WiegandCfg/wiegandNo/<ID>

Get or set Wiegand parameters.

Request URI Definition

Table A-329 GET /ISAPI/AccessControl/WiegandCfg/wiegandNo/<ID>

Method	GET
Description	Get Wiegand parameters.
Query	None.
Request	None.
Response	Succeeded: <u>XML_WiegandCfg</u> Failed: <u>XML_ResponseStatus</u>

Table A-330 PUT /ISAPI/AccessControl/WiegandCfg/wiegandNo/<ID>

Method	PUT
Description	Set Wiegand parameters.
Query	None.
Request	<u>XML_WiegandCfg</u>
Response	<u>XML_ResponseStatus</u>

A.263 /ISAPI/AccessControl/WiegandRuleCfg

Operations about the configuration of the custom Wiegand rule.

Request URI Definition

Table A-331 GET /ISAPI/AccessControl/WiegandRuleCfg

Method	GET
Description	Get the configuration parameters of the custom Wiegand rule.
Query	None.
Request	None.
Response	Succeeded: <u>XML_WiegandRuleCfg</u> Failed: <u>XML_ResponseStatus</u>

Table A-332 PUT /ISAPI/AccessControl/WiegandRuleCfg

Method	PUT
Description	Set the parameters of the custom Wiegand rule.
Query	None.
Request	<u>XML_WiegandRuleCfg</u>
Response	<u>XML_ResponseStatus</u>

A.264 /ISAPI/AccessControl/WiegandRuleCfg/capabilities

Get the configuration capability of the custom Wiegand rule.

Request URI Definition

Table A-333 GET /ISAPI/AccessControl/WiegandRuleCfg/capabilities

Method	GET
Description	Get the configuration capability of the custom Wiegand rule.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_WiegandRuleCfg</u> Failed: <u>XML_ResponseStatus</u>

A.265 /ISAPI/Event/notification/alertStream

Get the uploaded heartbeat or alarm/event information.

Request URI Definition

Table A-334 GET /ISAPI/Event/notification/alertStream

Method	GET
Description	Get the heartbeat or uploaded alarm/event information.
Query	None.
Request	None.
Response	Option 1: <u>XML_EventNotificationAlert_AlarmEventInfo</u> or <u>XML_EventNotificationAlert_HeartbeatInfo</u> Option 2: <u>JSON_EventNotificationAlert_Alarm/EventInfo</u>  Note The messages here only show the format of alarm/event information to be uploaded. For details, refer to the corresponding alarm/event configuration chapters.

Remarks

- After calling this URI, a persistent connection is set up between the device and the platform, and the alarm or event information will be uploaded from device continuously once the alarm is triggered or event occurred.
- You can check if the XML response message is the heartbeat information according to the nodes `<eventType>` and `<eventState>`. If the values of these two node are "videoloss" and "inactive", respectively, the returned message is the heartbeat information.

A.266 /ISAPI/Event/notification/httpHosts

Get or set parameters of all HTTP listening servers, add a HTTP listening server, and delete all HTTP listening servers.

Request URI Definition

Table A-335 GET /ISAPI/Event/notification/httpHosts

Method	GET
Description	Get parameters of all HTTP listening servers.
Query	security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode.
Request	None
Response	Succeeded: <u>XML HttpHostNotificationList</u> Failed: <u>XML ResponseStatus</u>

Table A-336 PUT /ISAPI/Event/notification/httpHosts

Method	PUT
Description	Set parameters of all HTTP listening servers.
Query	security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode.

Request	<u>XML_HttpHostNotificationList</u>
Response	<u>XML_ResponseStatus</u>

Table A-337 POST /ISAPI/Event/notification/httpHosts

Method	POST
Description	Add a HTTP listening server.
Query	security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode.
Request	<u>XML_HttpHostNotification</u>
Response	<u>XML_ResponseStatus</u>

Table A-338 DELETE /ISAPI/Event/notification/httpHosts

Method	DELETE
Description	Delete all HTTP listening servers.
Query	None
Request	None
Response	<u>XML_ResponseStatus</u>

A.267 /ISAPI/Event/notification/httpHosts/<ID>/test

Check whether the HTTP listening server is working normally.

Request URI Definition

Table A-339 POST /ISAPI/Event/notification/httpHosts/<ID>/test

Method	POST
Description	Check whether the HTTP listening server is working normally.
Query	None

Request	<u>XML_HttpHostNotification</u>
Response	Succeeded: <u>XML_HttpHostTestResult</u> Failed: <u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the HTTP listening server ID.

A.268 /ISAPI/Event/notification/httpHosts/capabilities

Get the configuration capabilities of all HTTP listening servers.

Request URI Definition

Table A-340 GET /ISAPI/Event/notification/httpHosts/capabilities

Method	GET
Description	Get the configuration capabilities of all HTTP listening servers.
Query	None
Request	None
Response	Succeeded: <u>XML_HttpHostNotificationCap</u> Failed: <u>XML_ResponseStatus</u>

A.269 /ISAPI/Intelligent/FDLib/capabilities?format=json

Get face picture library capability.

Request URI Definition

Table A-341 GET /ISAPI/Intelligent/FDLib/capabilities?format=json

Method	GET
Description	Get face picture library capability.
Query	format: determine the format of request or response message. terminalNo: int, terminal No., starts from 1.
Request	None.
Response	Succeeded: <u>JSON_FPLibCap</u>

	Failed: <u>JSONResponseStatus</u>
--	---

A.270 /ISAPI/Intelligent/FDLib/Count?format=json

Get the total number of face records in all face picture libraries.

Request URI Definition

Table A-342 GET /ISAPI/Intelligent/FDLib/Count?format=json

Method	GET
Description	Get the total number of face records in all face picture libraries.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None
Response	Succeeded: <u>JSON_FaceRecordNumInAllFPLib</u> Failed: <u>JSONResponseStatus</u>

Remarks

This URI is not supported by integration of information release system.

A.271 /ISAPI/Intelligent/FDLib/Count? format=json&FDID=&faceLibType=

Get the number of face records in a specific face picture library.

Request URI Definition

Table A-343 GET /ISAPI/Intelligent/FDLib/Count?format=json&FDID=&faceLibType=

Method	GET
Description	Get the number of face records in a specific face picture library.
Query	format: determine the format of request or response message.

	FDID : face picture library ID. faceLibType : face picture library type, which can equal to "blackFD" (list library) and "staticFD" (static library). terminalNo : dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None
Response	Succeeded: <u>JSON_FaceRecordNumInOneFPLib</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- In the URI, to specify a face picture library, both the library ID (**FDID**) and library type (**faceLibType**) are required, e.g., /ISAPI/Intelligent/FDLib/Count?format=json&FDID=1223344455566788&faceLibType=blackFD.
- This URI is not supported by integration of information release system.

A.272 /ISAPI/Intelligent/FDLib/FaceDataRecord?format=json

Add the face record (face picture and person information) to a face picture library or multiple face picture libraries.

Request URI Definition

Table A-344 POST /ISAPI/Intelligent/FDLib/FaceDataRecord?format=json

Method	POST
Description	Add a face record (including face picture and person information) to the face picture library.
Query	format : determine the format of request or response message.
Request	<u>JSON_AddFaceRecordCond</u>
Response	Succeeded: <u>JSON_AddFaceRecordResult</u> Failed: <u>JSON_ResponseStatus</u>

Remarks

- The face picture in the face record supports URL and binary data format. If the JSON message about adding condition parameters (**JSON_AddFaceRecordCond**) contains node "faceURL", the

picture should be uploaded in URL format; otherwise, the picture should be uploaded in binary data format.

- Currently, the picture URL refers to the URL generated when the picture is stored in the storage server of central management server. Before using picture URL, you should generate the URL via the cloud storage server of storage service component of ISUP (Intelligent Security Uplink Protocol).

A.273 /ISAPI/Intelligent/FDLib/FDModify?format=json

Edit face records in the face picture library in a batch.

Request URI Definition

Table A-345 PUT /ISAPI/Intelligent/FDLib/FDModify?format=json

Method	PUT
Description	Edit face records in the face picture library in a batch.
Query	format: determine the format of request or response message.
Request	<u>JSON_BatchEditFaceRecord</u>
Response	<u>JSON_ResponseStatus</u>

A.274 /ISAPI/Intelligent/FDLib/FDSearch/Delete? format=json&FDID=&faceLibType=

Delete the face record(s) in a specific face picture library.

Request URI Definition

Table A-346 PUT /ISAPI/Intelligent/FDLib/FDSearch/Delete?format=json&FDID=&faceLibType=

Method	PUT
Description	Delete the face record(s) in the face picture library.
Query	format: determine the format of request or response message. FDID: face picture library ID faceLibType: face picture library type
Request	<u>JSON_DelFaceRecord</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

In the URI, to specify a face picture library, both the library ID (**FDID**) and library type (**faceLibType**) are required.

A.275 /ISAPI/Intelligent/FDLib/FDSearch?format=json

Search for the face records in the face picture library.

Request URI Definition

Table A-347 POST /ISAPI/Intelligent/FDLib/FDSearch?format=json

Method	POST
Description	Search for the face records in the a face picture library or multiple face picture libraries. Fuzzy search is also supported.
Query	format : determine the format of request or response message. terminalNo : int, terminal No., starts from 1.
Request	<u>JSON_SearchFaceRecordCond</u>
Response	Succeeded: <u>JSON_SearchFaceRecordResult</u> Failed: <u>JSON_ResponseStatus</u>

A.276 /ISAPI/Intelligent/FDLib/FDSearch? format=json&FDID=&FPID=&faceLibType=

Edit a face record in a specific face picture library.

Request URI Definition

Table A-348 PUT /ISAPI/Intelligent/FDLib/FDSearch?format=json&FDID=&FPID=&faceLibType=

Method	PUT
Description	Edit a face record in a specific face picture library.
Query	format : determine the format of request or response message. FDID : face picture library ID FPID : face record ID faceLibType : face picture library type, which can be "blackFD" (list library) or "staticFD" (static library).

Request	<u>JSON_EditFaceRecord</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

In the URI, to specify a face picture library, both the library ID (**FDID**) and library type (**faceLibType**) are required.

A.277 /ISAPI/Intelligent/FDLib/FDSetUp?format=json

Set the face record (including face picture, person information, etc.) in the face picture library.

Request URI Definition

Table A-349 PUT /ISAPI/Intelligent/FDLib/FDSetUp?format=json

Method	PUT
Description	Set the face record (including face picture, person information, etc.) in the face picture library.
Query	format: determine the format of request or response message.
Request	<u>JSON_SetFaceRecord</u>
Response	<u>JSON_ResponseStatus</u>

Remarks

- If the face picture with the employee No. (person ID) does not exist, the face record will be added.
- If the face picture with the employee No. (person ID) exists, the face record will be overwritten.
- When deleting the face record, the **faceLibType**, **FDID**, **FPID**, and **deleteFP** in the request message JSON_SetFaceRecord should be configured, and the success response message will be returned no matter whether deleting succeeded or not.
- The employee No. is required.

A.278 /ISAPI/Intelligent/FDLib?format=json

Operations about the face picture library.

Request URI Definition

Table A-350 POST /ISAPI/Intelligent/FDLib?format=json

Method	POST
Description	Create a face picture library
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	<u>JSON_CreateFPLibCond</u>
Response	Succeeded: <u>JSON_CreateFPLibResult</u> Failed: <u>JSON_ResponseStatus</u>

Table A-351 GET /ISAPI/Intelligent/FDLib?format=json

Method	GET
Description	Get the information, including library ID, library type, name, and custom information, of all face picture libraries.
Query	format: determine the format of request or response message. terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None
Response	Succeeded: <u>JSON_FPLibListInfo</u> Failed: <u>JSON_ResponseStatus</u>

Table A-352 DELETE /ISAPI/Intelligent/FDLib?format=json

Method	DELETE
Description	Delete all face picture libraries.
Query	format: determine the format of request or response message.

	terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None
Response	<u>JSON_ResponseStatus</u>

Remarks

- After a face picture library is created, the face picture library ID will be returned. Each face picture library ID of the same library type is unique.
- The POST and DELETE operation methods are not supported by integration of information release system.

A.279 /ISAPI/Intelligent/FDLib?format=json&FDID=&faceLibType=

Operations about the management of a specific face picture library.

Request URI Definition

Table A-353 GET /ISAPI/Intelligent/FDLib?format=json&FDID=&faceLibType=

Method	GET
Description	Get the information, including library ID, library type, name, and custom information, of a specific face picture library.
Query	format: determine the format of request or response message. FDID: optional, string, face picture library ID. faceLibType: optional, string, face picture library type, which can be "blackFD" (list library) or "staticFD" (static library). terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	Succeeded: <u>JSON_SingleFPLibInfo</u> Failed: <u>JSON_ResponseStatus</u>

Table A-354 PUT /ISAPI/Intelligent/FDLib?format=json&FDID=&faceLibType=

Method	PUT
Description	Edit the information of a specific face picture library information, including name and custom information.
Query	format: determine the format of request or response message. FDID: optional, string, face picture library ID faceLibType: optional, string, face picture library type, which can be "blackFD" (list library) or "staticFD" (static library). terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	<u>JSON_EditFplibInfo</u>
Response	<u>JSON_ResponseStatus</u>

Table A-355 DELETE /ISAPI/Intelligent/FDLib?format=json&FDID=&faceLibType=

Method	DELETE
Description	Delete a specific face picture library.
Query	format: determine the format of request or response message. FDID: face picture library ID faceLibType: face picture library type terminalNo: dependent, int, terminal No., starts from 1. It is required for information release system integration. The No. is generated after information release terminal is registered to the central management server, and you can call "/ISAPI/Publish/TerminalMgr/terminalSearch" by POST method to get the generated terminal No.
Request	None.
Response	<u>JSON_ResponseStatus</u>

Remarks

- In the URI, to specify a face picture library, both the library ID (**FDID**) and library type (**faceLibType**) are required.
- This URI is not supported by integration of information release system.

A.280 /ISAPI/Publish/capabilities

Get information release capabilities to see the functions supported by the system.

Request URI Definition

Table A-356 GET /ISAPI/Publish/capabilities

Method	GET
Description	Get information release capabilities to see the functions supported by the system.
Query	None.
Request	None.
Response	Succeeded: <i>XML_PublishServerCap</i> Failed: <i>XML_ResponseStatus</i>

A.281 /ISAPI/Publish/material/<ID>/capabilities

Get the capability of material management parameters.

Request URI Definition

Table A-357 GET /ISAPI/Publish/material/<ID>/capabilities

Method	GET
Description	Get the capability of material management parameters.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_Material</i> Failed: <i>XML_ResponseStatus</i>

Remarks

The <ID> in the request URI refers to the material ID.

A.282 /ISAPI/Publish/MaterialMgr/material

Get information of all materials, or add a material.

Request URI Definition

Table A-358 GET /ISAPI/Publish/MaterialMgr/material

Method	GET
Description	Get information of all materials.
Query	None.
Request	None.
Response	Succeeded: <i>XML_MaterialList</i> Failed: <i>XML_ResponseStatus</i>

Table A-359 POST /ISAPI/Publish/MaterialMgr/material

Method	POST
Description	Add a material.
Query	None.
Request	<i>XML_Material</i>
Response	Succeeded: <ID> (material ID) + <i>XML_ResponseStatus</i> Failed: <i>XML_ResponseStatus</i>

A.283 /ISAPI/Publish/MaterialMgr/material/<ID>

Get, set, or delete a specific material.

Request URI Definition

Table A-360 GET /ISAPI/Publish/MaterialMgr/material/<ID>

Method	GET
Description	Get information of a specific material.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Material</i> Failed: <i>XML_ResponseStatus</i>

Table A-361 PUT /ISAPI/Publish/MaterialMgr/material/<ID>

Method	PUT
Description	Set information of a specific material.
Query	None.
Request	<u>XML_Material</u>
Response	<u>XML_ResponseStatus</u>

Table A-362 DELETE /ISAPI/Publish/MaterialMgr/material/<ID>

Method	DELETE
Description	Delete a specific material.
Query	None.
Request	None.
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the material ID.

A.284 /ISAPI/Publish/MaterialMgr/material/<ID>/upload

Upload static materials.

Request URI Definition

Table A-363 PUT /ISAPI/Publish/MaterialMgr/material/<ID>/upload

Method	PUT
Description	Upload static materials.
Query	None.
Request	Opaque data
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the static materials ID, which is valid when the material is uploaded.

A.285 /ISAPI/Publish/MaterialMgr/material/batchDelete

Batch delete the materials.

Request URI Definition

Table A-364 PUT /ISAPI/Publish/MaterialMgr/material/batchDelete

Method	PUT
Description	Batch delete the materials.
Query	None
Request	<u>XML_MaterialIdList</u>
Response	<u>XML_ResponseStatus</u>

A.286 /ISAPI/Publish/MaterialMgr/materialSearch

Search materials.

Request URI Definition

Table A-365 POST /ISAPI/Publish/MaterialMgr/materialSearch

Method	POST
Description	Search materials.
Query	None
Request	<u>XML_MaterialSearchDescription</u>
Response	Succeeded: <u>XML_MaterialSearchResult</u> Failed: <u>XML_ResponseStatus</u>

A.287 /ISAPI/Publish/MaterialMgr/materialSearch/profile

Get the capability of material search parameters.

Request URI Definition

Table A-366 GET /ISAPI/Publish/MaterialMgr/materialSearch/profile

Method	GET
Description	Get the capability of material search parameters.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_MaterialSearchProfile</i> Failed: <i>XML_ResponseStatus</i>

A.288 /ISAPI/Publish/ProgramMgr/program

Get all programs' parameters or add a new program.

Request URI Definition

Table A-367 GET /ISAPI/Publish/ProgramMgr/program

Method	GET
Description	Get all programs' parameters.
Query	None.
Request	None.
Response	Succeeded: <i>XML_ProgramList</i> Failed: <i>XML_ResponseStatus</i>

Table A-368 POST /ISAPI/Publish/ProgramMgr/program

Method	POST
Description	Add a new program.
Query	None.
Request	<i>XML_Program</i>
Response	Succeeded: <ID> (program ID) + <i>XML_ResponseStatus</i> Failed: <i>XML_ResponseStatus</i>

A.289 /ISAPI/Publish/ProgramMgr/program/<ID>

Get, set or delete a specific program.

Request URI Definition

Table A-369 GET /ISAPI/Publish/ProgramMgr/program/<ID>

Method	GET
Description	Get a specific program.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Program</u> Failed: <u>XML_ResponseStatus</u>

Table A-370 PUT /ISAPI/Publish/ProgramMgr/program/<ID>

Method	PUT
Description	Set a specific program.
Query	None.
Request	<u>XML_Program</u>
Response	<u>XML_ResponseStatus</u>

Table A-371 DELETE /ISAPI/Publish/ProgramMgr/program/<ID>

Method	DELETE
Description	Delete a specific program.
Query	None.
Request	None.
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the program ID.

A.290 /ISAPI/Publish/ProgramMgr/program/<ID>/capabilities

Get program parameter capabilities.

Request URI Definition

Table A-372 GET /ISAPI/Publish/ProgramMgr/program/<ID>/capabilities

Method	GET
Description	Get program parameter capabilities.
Query	None.
Request	None.
Response	Succeeded: <i>XML_Cap_Program</i> Failed: <i>XML_ResponseStatus</i>

Remarks

The <ID> in the request URI refers to the program ID.

A.291 /ISAPI/Publish/ProgramMgr/program/<ID>/page

Get information of all pages, or create a new page.

Request URI Definition

Table A-373 GET /ISAPI/Publish/ProgramMgr/program/<ID>/page

Method	GET
Description	Get information of all pages.
Query	None.
Request	None.
Response	Succeeded: <i>XML_PageList</i> Failed: <i>XML_ResponseStatus</i>

Table A-374 POST /ISAPI/Publish/ProgramMgr/program/<ID>/page

Method	POST
Description	Create a new page.

Query	None.
Request	<u>XML_Page</u>
Response	<u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the program ID.

A.292 /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>

Get, edit, or delete a page.

Request URI Definition

Table A-375 GET /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>

Method	GET
Description	Get a specific page of a specific program.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Page</u> Failed: <u>XML_ResponseStatus</u>

Table A-376 PUT /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>

Method	PUT
Description	Edit the information of a page.
Query	None.
Request	<u>XML_Page</u>
Response	<u>XML_ResponseStatus</u>

Table A-377 DELETE /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>

Method	DELETE
Description	Delete a page.
Query	None.

Request	None.
Response	<u>XML_ResponseStatus</u>

Remarks

The first <ID> in the request URI refers to the program ID, and the second one refers to the page ID.

A.293 /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>/capabilities

Get the page configuration capability.

Request URI Definition

Table A-378 GET /ISAPI/Publish/ProgramMgr/program/<ID>/page/<ID>/capabilities

Method	GET
Description	Get the page configuration capability.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_Page</u> Failed: <u>XML_ResponseStatus</u>

Remarks

The first <ID> in the request URI refers to the program ID, and the second one refers to the page ID.

A.294 /ISAPI/Publish/ProgramMgr/program/dynamicCap

Get program dynamic capability.

Request URI Definition

Table A-379 GET /ISAPI/Publish/ProgramMgr/program/dynamicCap

Method	GET
Description	Get program dynamic capability.
Query	None.

Request	None.
Response	Succeeded: <u>XML_ProgramDynamicCap</u> Failed: <u>XML_ResponseStatus</u>

A.295 /ISAPI/Publish/ScheduleMgr/capabilities?format=json

Get the schedule management capability set.

Request URI Definition

Table A-380 GET /ISAPI/Publish/ScheduleMgr/capabilities?format=json

Method	GET
Description	Get the schedule management capability set.
Query	format: determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_ScheduleMgrCap</u> Failed: <u>JSON_ResponseStatus</u>

A.296 /ISAPI/Publish/ScheduleMgr/playSchedule

Add a new program schedule, or get all program schedules.

Request URI Definition

Table A-381 POST /ISAPI/Publish/ScheduleMgr/playSchedule

Method	POST
Description	Add a new program schedule.
Query	None.
Request	<u>XML_PlaySchedule</u>
Response	Succeeded: <ID> (program schedule ID) + <u>XML_ResponseStatus</u> Failed: <u>XML_ResponseStatus</u>

Table A-382 GET /ISAPI/Publish/ScheduleMgr/playSchedule

Method	GET
Description	Get all program schedules.
Query	None.
Request	None.
Response	Succeeded: <u>XML_PlayScheduleList</u> Failed: <u>XML_ResponseStatus</u>

A.297 /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>

Get, set, or delete a specific program schedule.

Request URI Definition

Table A-383 GET /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>

Method	GET
Description	Get a specific program schedule.
Query	None.
Request	None.
Response	Succeeded: <u>XML_PlaySchedule</u> Failed: <u>XML_ResponseStatus</u>

Table A-384 PUT /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>

Method	PUT
Description	Set a specific program schedule.
Query	None.
Request	<u>XML_PlaySchedule</u>
Response	<u>XML_ResponseStatus</u>

Table A-385 DELETE /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>

Method	DELETE
Description	Delete a specific program schedule.

Query	None.
Request	None.
Response	<u>XML_ResponseStatus</u>

A.298 /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>/capabilities

Get the program schedule configuration capability.

Request URI Definition

Table A-386 GET /ISAPI/Publish/ScheduleMgr/playSchedule/<ID>/capabilities

Method	GET
Description	Get the program schedule configuration capability.
Query	None.
Request	None.
Response	Succeeded: <u>XML_Cap_PlaySchedule</u> Failed: <u>XML_ResponseStatus</u>

Remarks

The <ID> in the request URI refers to the program schedule ID.

A.299 /ISAPI/System/capabilities

Get device capability.

Request URI Definition

Table A-387 GET /ISAPI/System/capabilities

Method	GET
Description	Get device capability.
Query	None
Request	None.
Response	Succeeded: <u>XML_DeviceCap</u> Failed: <u>XML_ResponseStatus</u>

A.300 /ISAPI/System/PictureServer/capabilities?format=json

Get the picture storage server capability.

Request URI Definition

Table A-388 GET /ISAPI/System/PictureServer/capabilities?format=json

Method	GET
Description	Get the picture storage server capability.
Query	format : determine the format of request or response message.
Request	None.
Response	Succeeded: <u>JSON_Cap_PictureServerInformation</u> Failed: <u>JSON_ResponseStatus</u>

A.301 /ISAPI/System/PictureServer?format=json

Operations about the picture storage server configuration parameters.

Request URI Definition

Table A-389 GET /ISAPI/System/PictureServer?format=json

Method	GET
Description	Get the picture storage server parameters.
Query	format : determine the format of request or response message. security : the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode. iv : the initialization vector, and it is required when security is 1 or 2.
Request	None.
Response	Succeeded: <u>JSON_PictureServerInformation</u> Failed: <u>JSON_ResponseStatus</u>

Table A-390 PUT /ISAPI/System/PictureServer?format=json

Method	PUT
Description	Set the picture storage server parameters.
Query	<p>format: determine the format of request or response message.</p> <p>security: the version No. of encryption scheme. When security does not exist, it indicates that the data is not encrypted; when security is 1, it indicates that the nodes of sensitive information in the message are encrypted in AES128 CBC mode; when security is 2, it indicates that the nodes of sensitive information in the message are encrypted in AES256 CBC mode.</p> <p>iv: the initialization vector, and it is required when security is 1 or 2.</p>
Request	<u>JSON_PictureServerInformation</u>
Response	<u>JSON_ResponseStatus</u>

A.302 http://<ipAddress>:<portNo>/<url>

HTTP listening sever sends alarm information to alarm center.

Request URL Definition

Table A-391 POST http://<ipAddress>:<portNo>/<url>

Method	POST
Description	HTTP listening sever sends alarm information to alarm center.
Query	None
Request	None
Response	<p>Succeeded: <u>XML_EventNotificationAlert_AlarmEventInfo</u> or <u>JSON_EventNotificationAlert_Alarm/EventInfo</u></p> <p>Failed: <u>XML_ResponseStatus</u></p>

Remarks

- The <ipAddress> in the request URL refers to the IP address or domain name of HTTP listening server, the <portNo> is the port No. of HTTP listening server, and the <url> represents the streaming URL, which is configured via the HTTP listening server.
- The default port No. is 80, so the request URL without port No. is also valid.

Appendix B. Appendixes

B.1 Request and Response Messages

B.1.1 JSON Messages

JSON_AcsCfg

AcsCfg message in JSON format

```
{  
    "AcsCfg": {  
        "RS485Backup": ,  
        /*optional, boolean, whether to enable downstream RS-485 communication  
        redundancy: "true"-yes, "false"-no*/  
        "showCapPic": ,  
        /*optional, boolean, whether to display the captured picture: "true"-yes,  
        "false"-no*/  
        "showUserInfo": ,  
        /*optional, boolean, whether to display user information: "true"-yes, "false"-  
        no*/  
        "overlayUserInfo": ,  
        /*optional, boolean, whether to overlay user information: "true"-yes, "false"-  
        no*/  
        "voicePrompt": ,  
        /*optional, boolean, whether to enable audio announcement: "true"-yes, "false"-  
        no*/  
        "uploadCapPic": ,  
        /*optional, boolean, whether to upload the picture from linked capture: "true"-  
        yes, "false"-no*/  
        "saveCapPic": ,  
        /*optional, boolean, whether to save the captured picture: "true"-yes, "false"-  
        no*/  
        "inputCardNo": ,  
        /*optional, boolean, whether to allow inputting card No. on keypad: "true"-yes,  
        "false"-no*/  
        "enableWifiDetect": ,  
        /*optional, boolean, whether to enable Wi-Fi probe: "true"-yes, "false"-no*/  
        "enable3G4G": ,  
        /*optional, boolean, whether to enable 3G/4G: "true"-yes, "false"-no*/  
        "protocol": "",  
        /*optional, string, communication protocol type of the card reader: "Private"-  
        private protocol, "OSDP"-OSDP protocol*/  
        "enableCaptureCertificate": true,  
        /*optional, boolean, whether to enable capturing the ID picture: true (yes),  
        false (no). The captured ID picture will be compared with the captured face
```

```
picture to check whether it is the same person. If this node does not exist, it
indicates that this function is not supported*/
    "showPicture": ,
/*optional, boolean, whether to display the authenticated picture: true-
display, false-not display*/
    "showEmployeeNo": ,
/*optional, boolean, whether to display the authenticated employee ID: true-
display, false-not display*/
    "showName": ,
/*optional, boolean, whether to display the authenticated name: true-display,
false-not display*/
    "desensitiseEmployeeNo": ,
/*dependent, boolean, whether to enable employee No. de-identification for
local UI display: true (yes), false (no). This node is valid when the value of
the node showEmployeeNo is true*/
    "desensitiseName": ,
/*dependent, boolean, whether to enable name de-identification for local UI
display: true (yes), false (no). This node is valid when the value of the node
showName is true*/
    "thermalEnabled": true,
/*optional, boolean, whether to enable temperature measurement: true-enable
(default), false-disable*/
    "thermalMode": true,
/*optional, boolean, whether to enable temperature measurement only mode: true-
enable (only for temperature measurement), false-disable (default)*/
    "thermalPictureEnabled": true,
/*optional, boolean, whether to enable uploading visible light pictures in
temperature measurement only mode: true-enable, false-disable (default). This
field is used to control uploading captured pictures and visible light
pictures*/
    "thermalIp": "192.168.1.1",
/*optional, string, IP address of the thermography device. For access control
devices, each device only requires one IP address; for metal detector doors,
this field does not need to be configured*/
    "highestThermalThreshold": 37.3,
/*optional, float, upper limit of the temperature threshold which is accurate
to one decimal place, unit: Celsius. The default value of this field is
37.3 °C. This field is used to check whether to open the door when the
temperature is above the upper limit*/
    "lowestThermalThreshold": ,
/*optional, float, lower limit of the temperature threshold which is accurate
to one decimal place, unit: Celsius. This field is used to check whether to
open the door when the temperature is below the lower limit*/
    "thermalDoorEnabled": false,
/*optional, boolean, whether to open the door when the temperature is above the
upper limit (highestThermalThreshold) or below the lower limit
(lowestThermalThreshold) of the threshold: true-open the door, false-not open
the door (default)*/
    "QRCodeEnabled": false,
/*optional, boolean, whether to enable QR code function: true-enable, false-
disable (default)*/
    "remoteCheckDoorEnabled": false,
```

```
/*optional, boolean, whether to enable controlling the door by remote verification: true-control, false-not control (default)*/
    "checkChannelType": "",
/*dependent, string, verification channel type: "Ezviz"-EZVIZ channel, "ISUP"-ISUP channel, "ISAPI"-ISAPI channel, "PrivateSDK"-private SDK channel, "ISAPIListen"-ISAPI listening channel. This field is valid when remoteCheckDoorEnabled is true*/
    "channelIp": "",
/*dependent, string, IP address of the verification channel. This field is valid when checkChannelType is "PrivateSDK"*/
    "uploadVerificationPic": ,
/*optional, boolean, whether to upload the authenticated picture: true, false*/
    "saveVerificationPic": ,
/*optional, boolean, whether to save the authenticated picture: true, false*/
    "saveFacePic": ,
/*optional, boolean, whether to save the registered face picture: true, false*/
    "thermalUnit": "",
/*optional, string, temperature unit: "celsius" (default), "fahrenheit". If this node does not exist, the default unit is Celsius*/
    "highestThermalThresholdF": ,
/*optional, float, the maximum value of the temperature threshold. The value is accurate to one decimal place, and the unit is Fahrenheit. This node is used to check whether to open the door when the temperature is higher than the threshold*/
    "lowestThermalThresholdF": ,
/*optional, float, the minimum value of the temperature threshold. The value is accurate to one decimal place, and the unit is Fahrenheit. This node is used to check whether to open the door when the temperature is lower than the threshold*/
    "thermalCompensation": ,
/*optional, float, temperature compensation, the value is accurate to one decimal place. The unit depends on the node thermalUnit. If the node thermalUnit does not exist, the default unit is Celsius*/
}
```

JSON_AcsEvent

AcsEvent message in JSON format

```
{
    "AcsEvent":{
        "searchID": "",
/*required, string type, search ID, which is used to confirm the upper-level platform or system. If the platform or the system is the same one during two searching, the search history will be saved in the memory to speed up next searching*/
        "responseStatusStrg": "",
/*required, string, search status: "OK"-searching completed, "MORE"-searching for more results, "NO MATCH"-no matched results*/
        "numOfMatches": ,
```

```
/*required, integer, number of returned results*/
    "totalMatches": ,
/*required, integer, total number of matched results*/
    "InfoList": [
/*optional, event details*/
        "major": ,
/*required, integer, major alarm/event types (the type value should be
transformed to the decimal number), see Access Control Event Types for details*/
        "minor": ,
/*required, integer, minor alarm/event types (the type value should be
transformed to the decimal number), see Access Control Event Types for details*/
        "time": "",
/*required, string, time (UTC time), e.g., "2016-12-12T17:30:08+08:00"*/
        "netUser": "",
/*optional, string, user name*/
        "remoteHostAddr": "",
/*optional, string, remote host address*/
        "cardNo": "",
/*optional, string, card No.*/
        "cardType": ,
/*optional, integer, card types: 1-normal card, 2-disabled card, 3-blocklist
card, 4-patrol card, 5-duress card, 6-super card, 7-visitor card, 8-dismiss
card*/
        "name": "",
/*optional, string, person name*/
        "whiteListNo": ,
/*optional, integer, allowlist No., which is between 1 and 8*/
        "reportChannel": ,
/*optional, integer, channel type for uploading alarm/event: 1-for uploading
arming information, 2-for uploading by central group 1, 3-for uploading by
central group 2*/
        "cardReaderKind": ,
/*optional, integer, authentication unit type: 1-IC card reader, 2-ID card
reader, 3-QR code scanner, 4-fingerprint module*/
        "cardReaderNo": ,
/*Optional, integer, authentication unit No.*/
        "doorNo": ,
/*optional, integer, door or floor No.*/
        "verifyNo": ,
/*optional, integer, multiple authentication No.*/
        "alarmInNo": ,
/*optional, integer, alarm input No.*/
        "alarmOutNo": ,
/*optional, integer, alarm output No.*/
        "caseSensorNo": ,
/*optional, integer, event trigger No.*/
        "RS485No": ,
/*optional, integer, RS-485 channel No.*/
        "multiCardGroupNo": ,
/*optional, integer, group No.*/
        "accessChannel": ,
/*optional, integer, swing barrier No.*/

```

```
    "deviceNo": ,
/*optional, integer, device No.*/
    "distractControlNo": ,
/*optional, integer, distributed controller No.*/
    "employeeNoString": "",
/*optional, integer, employee No. (person ID)*/
    "localControllerID": ,
/*optional, integer, distributed access controller No.: 0-access controller, 1
to 64-distributed access controller No.1 to distributed access controller No.
64*/
    "InternetAccess": ,
/*optional, integer, network interface No.: 1-upstream network interface No.1,
2-upstream network interface No.2, 3-downstream network interface No.1*/
    "type": ,
/*optional, integer, zone type: 0-instant alarm zone, 1-24-hour alarm zone, 2-
delayed zone, 3-internal zone, 4-key zone, 5-fire alarm zone, 6-perimeter
protection, 7-24-hour silent alarm zone, 8-24-hour auxiliary zone, 9-24-hour
shock alarm zone, 10-emergency door open alarm zone, 11-emergency door closed
alarm zone, 255-none*/
    "MACAddr": "",
/*optional, string, physical address*/
    "swipeCardType": ,
/*optional, integer, card swiping types: 0-invalid, 1-QR code*/
    "serialNo": ,
/*optional, integer, event serial No., which is used to judge whether the event
loss occurred*/
    "channelControllerID": ,
/*optional, integer, lane controller No.: 1-main lane controller, 2-sub lane
controller*/
    "channelControllerLampID": ,
/*optional, integer, light board No. of lane controller, which is between 1 and
255*/
    "channelControllerIRAdaptorID": ,
/*optional, integer, IR adapter No. of lane controller, which is between 1 and
255*/
    "channelControllerIREmitterID": ,
/*optional, integer, active infrared intrusion detector No. of lane controller,
which is between 1 and 255*/
    "userType": "",
/*optional, string, person type: "normal"-normal person (household), "visitor"-_
visitor, "blacklist"-person in blocklist, "administrators"-administrator*/
    "currentVerifyMode": "",
/*optional, string, authentication mode: "cardAndPw"-card+password, "card",
"cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password,
"fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-_
fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or
password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password,
"faceAndCard"-face+card, "face", "employeeNoAndPw"-employee No.+password,
"fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint,
"employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-_
face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint,
"employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card,
```

```
"fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password,  
"cardOrFpOrPw"-card or fingerprint or password*/  
    "QRCodeInfo":"test",  
/*optional, string, QR code information*/  
    "thermometryUnit": "",  
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-  
Fahrenheit, "kelvin"-Kelvin*/  
    "currTemperature": ,  
/*optional, float, face temperature which is accurate to one decimal place*/  
    "isAbnormalTemperature": ,  
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-  
no*/  
    "RegionCoordinates": {  
/*optional, face temperature's coordinates*/  
        "positionX": ,  
/*optional, int, normalized X-coordinate which is between 0 and 1000*/  
        "positionY":  
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/  
        },  
        "mask": "",  
/*optional, string, whether the person is wearing mask: "unknown", "yes"-  
wearing mask, "no"-not wearing mask*/  
        "pictureURL": "",  
/*optional, string, picture URL*/  
        "filename": "",  
/*optional, string, file name. If multiple pictures are returned at a time,  
filename of each picture should be unique*/  
        "attendanceStatus": "",  
/*optional, string, attendance status: "undefined", "checkIn"-check in,  
"checkOut"-check out, "breakOut"-break out, "breakIn"-break in, "overtimeIn"-  
overtime in, "overTimeOut"-overtime out*/  
        "label": "",  
/*optional, string, custom attendance name*/  
        "statusValue": ,  
/*optional, integer, status value*/  
        "helmet": "",  
/*optional, string, whether the person is wearing hard hat: "unknown", "yes"-  
wearing hard hat, "no"-not wearing hard hat*/  
        "visibleLightPicUrl": "test",  
/*optional, string, URL of the visible light picture*/  
        "thermalPicUrl": "test",  
/*optional, string, URL of the thermal picture*/  
        "appType": "attendance",  
/*optional, string, application type: "attendance" (attendance application),  
"signIn" (check-in application, which is only used for information release  
products)*/  
        "HealthInfo": {  
/*optional, object, health information*/  
            "healthCode": 1,  
/*optional, int, health code status: 0 (no request), 1 (no health code), 2  
(green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6  
(other error, e.g., searching failed due to API exception), 7 (searching for
```

```
the health code timed out)*/
    "NADCode": 1,
/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/
    "travelCode": 1,
/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3 (other)*/
    "vaccineStatus": 1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1 (vaccinated)*/
},
    "meetingID": "test",
/*required, string, meeting number, range:[1,32]*/
    "PersonInfoExtends": [
/*optional, array, extended person information*/
{
    "id": 1,
/*optional, integer, extended person ID, range:[1,32]*/
        "value": "test"
/*optional, string, content of extended person information*/
    ],
    "name": "test",
/*optional, string, name*/
    "FaceRect": {
/*optional, object, rectangle for face picture*/
        "height": 1.000,
/*optional, float, height, range:[0.000,1.000]*/
        "width": 1.000,
/*optional, float, width, range:[0.000,1.000]*/
        "x": 0.000,
/*optional, float, horizontal coordinate in the upper-left corner, range:[0.000,1.000]*/
        "y": 0.000
/*optional, float, vertical coordinate in the upper-left corner, range:[0.000,1.000]*/
    }
},
    }
}
```

JSON_AcsEventCond

AcsEventCond message in JSON format

```
{
    "AcsEventCond": {
        "searchID": "",
/*required, string type, search ID, which is used to confirm the upper-level platform or system. If the platform or the system is the same one during two searching, the search history will be saved in the memory to speed up next
```

```
searching*/,
    "searchResultPosition": ,
/*required, integer, the start position of the search result in the result
list. When there are multiple records and you cannot get all search results at
a time, you can search for the records after the specified position next time*/
    "maxResults": ,
/*required, integer, maximum number of search results. If maxResults exceeds
the range returned by the device capability, the device will return the maximum
number of search results according to the device capability and will not return
error message*/
    "major": ,
/*required, integer, major alarm/event types (the type value should be
transformed to the decimal number), see Access Control Alarm Types for details*/
    "minor": ,
/*required, integer, minor alarm/event types (the type value should be
transformed to the decimal number), see Access Control Alarm Types for details*/
    "startTime": "",
/*optional, string, start time (UTC time), e.g., 2016-12-12T17:30:08+08:00*/
    "endTime": "",
/*optional, string, end time (UTC time), e.g., 2017-12-12T17:30:08+08:00*/
    "cardNo": "",
/*optional, string, card No.*/
    "name": "",
/*optional, string, cardholder name*/
    "picEnable": ,
/*optional, boolean, whether to contain pictures: "false"-no, "true"-yes*/
    "beginSerialNo": ,
/*optional, integer, start serial No.*/
    "endSerialNo": ,
/*optional, integer, end serial No.*/
    "employeeNoString": "",
/*optional, string, employee No. (person ID)*/
    "eventAttribute": "",
/*optional, string, event attribute: "attendance"-valid authentication,
"other"*/
    "employeeNo": "",
/*optional, string, employee No. (person ID)*/
    "timeReverseOrder": ,
/*optional, boolean, whether to return events in descending order of time
(later events will be returned first): true-yes, false or this node is not
returned-no*/
    "isAbnormalTemperature": true
/*optional, boolean, whether the skin-surface temperature is abnormal*/
    "temperatureSearchCond": "all"
/*optional, string, temperature search conditions, all (events with temperature
information), normal (events with normal temperature), abnormal (events with
abnormal temperature), if it exists with isAbnormalTemperature, then the latter
will be invalid.*/
}
```

JSON_AcsEventTotalNum

AcsEventTotalNum message in JSON format

```
{  
    "AcsEventTotalNum": {  
        "totalNum":  
/*required, integer, total number of events that match the search conditions*/  
    }  
}
```

JSON_AcsEventTotalNumCond

AcsEventTotalNumCond message in JSON format

```
{  
    "AcsEventTotalNumCond": {  
        "major": ,  
/*required, integer, major type (the type value should be transformed to the  
decimal number), refer to Access Control Event Types for details*/  
        "minor": ,  
/*required, integer, minor type (the type value should be transformed to the  
decimal number), refer to Access Control Event Types for details*/  
        "startTime": "",  
/*optional, string, start time (UTC time), e.g., "2016-12-12T17:30:08+08:00"*/  
        "endTime": "",  
/*optional, string, end time (UTC time), e.g., "2017-12-12T17:30:08+08:00"*/  
        "cardNo": "",  
/*optional, string, card No.*/  
        "name": "",  
/*optional, string, cardholder name*/  
        "picEnable": ,  
/*optional, boolean, whether to contain pictures: "true"-yes, "false"-no*/  
        "beginSerialNo": ,  
/*optional, integer, start serial No.*/  
        "endSerialNo": ,  
/*optional, integer, end serial No.*/  
        "employeeNoString": "",  
/*optional, string, employee No. (person ID)*/  
        "eventAttribute": ""  
/*optional, string, event attribute: "attendance"-valid authentication,  
"other"*/  
    }  
}
```

See Also

[Access Control Event Types](#)

JSON_AcsWorkStatus

AcsWorkStatus message in JSON format

```
{  
    "AcsWorkStatus":{  
        "doorLockStatus": ,  
        /*optional, array, door lock status (relay status): 0-normally close, 1-normally open, 2-short-circuit alarm, 3-broken-circuit alarm, 4-exception alarm. For example, [1,2,1,2] indicates that door lock 1 is normally open, door lock 2 triggers short-circuit alarm, door lock 3 is normally open, and door lock 4 triggers short-circuit alarm*/  
        "doorStatus": ,  
        /*optional, array, door (floor) status: 1-sleep, 2-remain unlocked (free), 3-remain locked (disabled), 4-normal status (controlled). For example, [1,2,1,2] indicates that door 1 is sleeping, door 2 remains unlocked, door 3 is sleeping, and door 4 remains unlocked*/  
        "magneticStatus": ,  
        /*optional, array, magnetic contact status: 0-normally close, 1-normally open, 2-short-circuit alarm, 3-broken-circuit alarm, 4-exception alarm. For example, [1,2,1,2] indicates that magnetic contact No.1 is normally open, magnetic contact No.2 triggers short-circuit alarm, magnetic contact No.3 is normally open, and magnetic contact No.4 triggers short-circuit alarm*/  
        "caseStatus": ,  
        /*optional, array, event trigger status, e.g., [1,3,5] indicates that event trigger No.1, No.3, and No.5 have input*/  
        "batteryVoltage": ,  
        /*optional, integer, storage battery power voltage, the actual value will be 10 times of this value, unit: Volt*/  
        "batteryLowVoltage": ,  
        /*optional, boolean, whether the storage battery is in low voltage status:  
        "true"-yes, "false"-no*/  
        "powerSupplyStatus": "",  
        /*optional, string, device power supply status: "ACPowerSupply"-alternative current, "BatteryPowerSupply"-storage battery power supply*/  
        "multiDoorInterlockStatus": "",  
        /*optional, string, multi-door interlocking status: "close"-disabled, "open"-enabled/  
        "antiSneakStatus": "",  
        /*optional, string, anti-passback status: "close"-disabled, "open"-enabled*/  
        "hostAntiDismantleStatus": "",  
        /*optional, string, tampering status of the access control device: "close"-disabled, "open"-enabled*/  
        "indicatorLightStatus": "",  
        /*optional, string, indicator status: "offLine"-offline, "onLine"-online*/  
        "cardReaderOnlineStatus": ,  
        /*optional, array, online status of the authentication unit, e.g., [1,3,5] indicates that authentication unit No.1, No.3, and No.5 are online*/  
        "cardReaderAntiDismantleStatus": ,  
        /*optional, array, tampering status of the authentication unit, e.g., [1,3,5] indicates that the tampering function of authentication unit No.1, No.3, and No.
```

```
5 is enabled*/
    "cardReaderVerifyMode": ,
/*optional, array, current authentication mode of the authentication unit: 1-
sleep, 2-card+password, 3-card, 4-card or password, 5-fingerprint, 6-fingerprint
+password, 7-fingerprint or card, 8-fingerprint+card, 9-fingerprint+card
+password, 10-face or fingerprint or card or password, 11-face+fingerprint, 12-
face+password, 13-face+card, 14-face, 15-employee No.+password, 16-fingerprint
or password, 17-employee No.+fingerprint, 18-employee No.+fingerprint+password,
19-face+fingerprint+card, 20-face+password+fingerprint, 21-employee No.+face,
22-face or face+card, 23-fingerprint or face, 24-card or face or password, 25-
card or face, 26-card or face or fingerprint, 27-card or fingerprint or
password. For example, [3,5,3,5] indicates that the authentication mode of
authentication unit 1 is "card", the authentication mode of authentication unit
2 is "fingerprint", the authentication mode of authentication unit 3 is "card",
and the authentication mode of authentication unit 4 is "fingerprint"*/
    "setupAlarmStatus": ,
/*optional, array, No. of armed input port, e.g., [1,3,5] indicates that input
port No.1, No.3, and No.5 are armed*/
    "alarmInStatus": ,
/*optional, array, No. of input port with alarms, e.g., [1,3,5] indicates that
input port No.1, No.3, and No.5 trigger alarms*/
    "alarmOutStatus": ,
/*optional, array, No. of output port with alarms, e.g., [1,3,5] indicates that
output port No.1, No.3, and No.5 trigger alarms*/
    "cardNum": ,
/*optional, integer, number of added cards*/
    "fireAlarmStatus":"",
/*optional, string, fire alarm status: "normal", "shortCircuit"-short-circuit
alarm, "brokenCircuit"-broken-circuit alarm*/
    "batteryChargeStatus":"",
/*optional, string, battery charging status: "charging", "uncharged"*/
    "masterChannelControllerStatus":"",
/*optional, string, online status of the main lane controller: "offLine"-_
offline, "onLine"-online*/
    "slaveChannelControllerStatus":"",
/*optional, string, online status of the sub lane controller: "offLine"-_
offline, "onLine"-online*/
    "antiSneakServerStatus":""
/*optional, string, anti-passback server status: "disable"-disabled, "normal",
"disconnect"-disconnected*/
}
}
```

JSON_AddFaceRecordCond

Message about conditions of adding a face record, it is in JSON format

```
{
    "faceURL": "",
/*optional, string type, picture storage URL inputted when uploading the face
picture by URL, the maximum length is 256 bytes*/
```

```
"faceLibType": "",  
/*required, face picture library type: "blackFD"-list library, "staticFD"-  
static library, string type, the maximum size is 32 bytes*/  
"FDID": "",  
/*required, face picture library ID, string type, the maximum size is 63  
bytes*/  
"FPID": "",  
/*optional, string type, face record ID, which is the same as the employee No.  
(person ID), and the maximum length is 63 bytes*/  
"name": "",  
/*required, name of person in the face picture, string type, the maximum size  
is 96 bytes*/  
"gender": "",  
/*optional, gender of person in the face picture: male, female, unknown, string  
type, the maximum size is 32 bytes*/  
"bornTime": "",  
/*required, birthday of person in the face picture, ISO8601 time format, string  
type, the maximum size is 20 bytes*/  
"city": "",  
/*optional, city code of birth for the person in the face picture, string type,  
the maximum size is 32 bytes*/  
"certificateType": "",  
/*optional, string type, the max. size is 10 bytes, certificate type:  
"officerID"-officer ID, "ID"-identify card, passport, other*/  
"certificateNumber": "",  
/*optional, certificate No., string, the max. size is 32 bytes*/  
"caseInfo": "",  
/*optional, case information, string type, the max. size is 192 bytes, it is  
valid when faceLibType is "blackFD".*/  
"tag": "",  
/*optional, custom tag, up to 4 tags, which are separated by commas, string  
type, the max. size is 195 bytes, it is valid when faceLibType is "blackFD".*/  
"address": "",  
/*optional, person address, string type, the max. size is 192 bytes, it is  
valid when faceLibType is "staticFD".*/  
"customInfo": "",  
/*optional, custom information, string type, the max. size is 192 bytes, it is  
valid when faceLibType is "staticFD".*/  
"modelData": ""  
/*optional, string type, target model data, non-modeled binary data needs to be  
encrypted by Base64 during transmission*/  
"transfer":true,  
/*optional, boolean, whether to enable transfer*/  
"operateType": "byTerminal",  
/*optional, string, operation type: "byTerminal"-by terminal*/  
"terminalNoList": [1],  
/*optional, array, terminal ID list, this node is required when operation type  
is "byTerminal"; currently, only one terminal is supported*/  
"PicFeaturePoints":[]  
/*optional, array of object, feature points to be applied. If the device only  
supports three types of feature points, when the platform applies more than  
three types of feature points, the device will not return error information*/
```

```
    "featurePointType": "face",
/*required, string, feature point type: "face", "leftEye" (left eye),
"rightEye" (right eye), "leftMouthCorner" (left corner of mouth),
"rightMouthCorner" (right corner of mouth), "nose"*/
    "coordinatePoint": {
/*required, object, coordinates of the feature point*/
        "x": 1,
/*required, int, normalized X-coordinate which is between 0 and 1000*/
        "y": 1,
/*required, int, normalized Y-coordinate which is between 0 and 1000*/
        "width": 1,
/*required, int, width which is between 0 and 1000. This node is required when
featurePointType is "face"*/
        "height": 1
/*required, int, height which is between 0 and 1000. This node is required when
featurePointType is "face"*/
    }
},
"saveFacePic": true
/*optional, boolean, whether to save face pictures*/
}
```

Remarks

If the field "faceURL" exists in the message, it indicates that the picture is uploaded via URL, and the "faceURL" of message should be set to picture URL. Otherwise, the picture is uploaded as binary data, which can be followed the message in JSON format, and separated by "boundary". See the example below.

Example

Add Face Record When Binary Picture is Uploaded in Form Format

```
1) POST /ISAPI/Intelligent/FDLib/FaceDataRecord?format=json
2) Accept: text/html, application/xhtml+xml,
3) Accept-Language: us-EN
4) Content-Type: multipart/form-data;
boundary=-----7e13971310878
5) User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0)
6) Accept-Encoding: gzip, deflate
7) Host: 10.10.36.29:8080
8) Content-Length: 9907
9) Connection: Keep-Alive
10) Cache-Control: no-cache
11)
12) -----7e13971310878
13) Content-Disposition: form-data; name="FaceDataRecord";
14) Content-Type: application/json
15) Content-Length: 9907
16)
17) {
a) "faceLibType": "blackFD",
```

```
b) "FDID": "122334455566788",
c) "FPID": "11111aa",
d) "name": "Eric",
e) "gender": "male",
f) "bornTime": "2004-05-03",
g) "city": "130100",
h) "certificateType": "officerID",
i) "certificateNumber": "",
j) "caseInfo": "",
k) "tag": "aa,bb,cc,dd",
l) "address": "",
m) "customInfo": ""
18)
19) -----7e13971310878
20) Content-Disposition: form-data; name="FaceImage";
21) Content-Type: image/jpeg
22) Content-Length: 9907
23)
24) .....JFIF.....`..`.....C..... .
25) ..
26) .....$.' ",#..(7),01444.'9=82<.342...C. ....
27) -----7e13971310878--
```



Note

- In line 4, "Content-Type: multipart/form-data" indicates that the data is sent in form format. The "boundary" is a delimiter, you can assign value to it for distinguishing other ones.
- In line 12, the request body consists of multiple same parts, and each part starts with "-" and from the customized "boundary" delimiter, the contents after the delimiter is the description of this part.
- In line 13, "Content-Disposition" refers to condition parameters, when adding face record, the "name" must be set to "FaceDataRecord".
- In line 14, "Content-Type" refers to JSON format, which based on UTF-8 character set.
- In line 15, "Content-Length" refers to the size of data (contains the "\r\n" escape characters) from line 16 to line 18.
- In line 16, the "\r\n\r\n" escape characters must be entered.
- Line 19 is the start delimiter of next part.
- Line 20 is the binary picture data, and the "name" must be set to "FaceImage".
- Line 21 is the format of the binary picture data. Here, "image/jpeg" indicates that the following contents are JPEG format picture data.
- In line 23, the "\r\n\r\n" escape characters must be entered.
- In line 27, the customized "boundary" indicates the end of request body.

JSON_AddFaceRecordResult

Message about the result of adding the face record to face picture library, it is in JSON format.

```
{  
    "requestURL": "",  
    "statusCode": "",  
    "statusString": "",  
    "subStatusCode": "",  
    "errorCode": "",  
    "errorMsg": "",  
    /*see the description of this node and above nodes in the message of  
    JSON_ResponseStatus*/  
    "FPID": ""  
    /*optional, string type, face record ID returned when the face record is added,  
    it is unique, and the maximum size is 63 bytes. This node is valid when  
    errorCode is "1" and errorMsg is "ok"*/  
}
```

See Also

[JSON_ResponseStatus](#)

JSON_AntiSneakCfg

AntiSneakCfg message in JSON format

```
{  
    "AntiSneakCfg": {  
        "enable": ,  
        /*required, boolean, whether to enable anti-passing back*/  
        "startCardReaderNo":  
        /*optional, integer, first card reader No., 0-no first card reader*/  
    }  
}
```

JSON_Attendance

JSON message about the parameters of attendance check by pressing the key

```
{  
    "Attendance": {  
        "enable": true,  
        /*required, boolean, whether to enable*/  
        "attendanceStatus": "",  
        /*optional, string, attendance status: "checkIn"-check in, "checkOut"-check  
        out, "breakOut"-break out, "breakIn"-break in, "overtimeIn"-overtime in,  
        "overtimeOut"-overtime out*/  
        "label": ""  
        /*optional, string, custom name*/  
    }  
}
```

JSON_AttendanceCap

JSON message about the configuration capability of attendance check by pressing the key

```
{  
    "AttendanceCap":{  
        "id":{  
/*required, int, key No. range*/  
            "@min":0,  
            "@max":0  
        },  
        "enable":{  
/*required, boolean, whether to enable*/  
            "@opt":[true, false]  
        },  
        "label":{  
/*optional, string, custom name*/  
            "@min":0,  
            "@max":0  
        },  
        "attendanceStatus":{  
/*optional, string, attendance status*/  
            "@opt":["checkIn", "checkOut", "breakOut", "breakIn", "overtimeIn",  
"overtimeOut"]  
        }  
    }  
}
```

JSON_AttendanceList

JSON message about the attendance parameter list

```
{  
    "AttendanceList": [ {  
        "enable":true,  
/*required, boolean, whether to enable*/  
        "attendanceStatus":"",  
/*optional, string, attendance status: "checkIn"-check in, "checkOut"-check  
out, "breakOut"-break out, "breakIn"-break in, "overtimeIn"-overtime in,  
"overtimeOut"-overtime out*/  
        "label":""  
/*optional, string, custom name*/  
    } ]  
}
```

JSON_AttendanceMode

JSON message about the attendance mode parameters

```
{  
    "AttendanceMode":{  
        "mode":"" ,  
        /*optional, string, attendance mode: "disable", "manual", "auto"-automatic,  
        "manualAndAuto"-manual and automatic*/  
        "attendanceStatusTime": 0,  
        /*optional, int, attendance status duration, unit: second. This node is valid  
        when mode is "manual" or "manualAndAuto"*/  
        "reqAttendanceStatus": true  
        /*optional, boolean, whether the attendance status is required*/  
    }  
}
```

JSON_AttendancePlanTemplate

JSON message about the parameters of the attendance schedule template

```
{  
    "AttendancePlanTemplate":{  
        "enable":true,  
        /*required, boolean, whether to enable: true-enable, false-disable*/  
        "property":"check",  
        /*required, string, attendance attribute: "check"-check in and check out,  
        "break"-break out and break in, "overtime"-overtime in and overtime out. Only  
        one attendance attribute can be configured for each template*/  
        "templateName":"" ,  
        /*required, string, template name*/  
        "weekPlanNo":1  
        /*required, int, week schedule No.*/  
    }  
}
```

JSON_AttendancePlanTemplateCap

JSON message about the configuration capability of the attendance schedule template

```
{  
    "AttendancePlanTemplateCap":{  
        "templateNo ":{  
            /*schedule template No.*/  
            "@min":1,  
            "@max":16  
        },  
        "property":{  
    }
```

```
/*required, attendance attribute: "check"-check in and check out, "break"-break out and break in, "overtime"-overtime in and overtime out*/
    "@opt":["check", "break", "overtime"]
},
"enable":{
/*whether to enable: true-enable, false-disable*/
    "@opt":[true, false]
},
"templateName":{
/*template name*/
    "@min":1,
    "@max":32
},
"weekPlanNo":{
/*week schedule No.*/
    "@min":1,
    "@max":16
},
"holidayGroupNo":{
/*holiday group No.*/
    "@min":1,
    "@max":16
}
}
```

JSON_AttendancePlanTemplateList

JSON message about the list of attendance schedule templates

```
{
    "AttendancePlanTemplateList":[{
        "templateNo":1,
/*required, int, schedule template No.*/
        "enable":true,
/*required, boolean, whether to enable: true-enable, false-disable*/
        "templateName":"",
/*required, string, template name*/
        "weekPlanNo":1
/*required, int, week schedule No.*/
    }]
}
```

JSON_AttendanceWeekPlan

JSON message about the parameters of the week attendance schedule

```
{
    "AttendanceWeekPlan":{
```

```
"enable":true,  
/*required, boolean, whether to enable: true-enable, false-disable*/  
    "WeekPlanCfg":[{
/*required, week schedule parameters*/  
        "id":1,  
/*required, int, time period No.*/  
        "week":"Monday",  
/*required, string, day of the week: "Monday", "Tuesday", "Wednesday",  
"Thursday", "Friday", "Saturday", "Sunday"*/  
        "enable":true,  
/*required, boolean, whether to enable: true-enable, false-disable*/  
        "TimeSegment":{
            "beginTime":"10:10:00",  
/*required, string, start time (device's local time)*/  
            "endTime":"12:10:00"  
/*required, string, end time (device's local time)*/  
        }
    }]
}
```

JSON_AttendanceWeekPlanCap

JSON message about the configuration capability of the week attendance schedule

```
{
    "AttendanceWeekPlanCap": {
        "planNo": {
/*week attendance schedule No.*/
            "@min":1,
            "@max":16
        },
        "enable": {
/*boolean, whether to enable: true-enable, false-disable*/
            "@opt":[true, false]
        },
        "WeekPlanCfg": {
/*week schedule parameters*/
            "maxSize":5,
            "id":{
                "@min":1,
                "@max":8
            },
            "week":{
                "@opt":["Monday", "Tuesday", "Wednesday", "Thursday", "Friday",
"Saturday", "Sunday"]
            },
            "enable": {
/*boolean, whether to enable: true-enable, false-disable*/
                "@opt":[true, false]
            },

```

```
    "TimeSegment": {
        "beginTime": "",
        /*start time (device's local time)*/
        "endTime": "",
        /*end time (device's local time)*/
        "validUnit": "second"
        /*time accuracy: "hour", "minute", "second". If this node is not returned, the
        time accuracy is "minute"*/
    }
}
}
```

JSON_BatchEditFaceRecord

Message about the condition of editing face records in the face picture library in a batch, and it is in JSON format.

```
{
    "faceURL": "",  

    /*optional, string type, picture storage URL inputted when uploading the face  

    picture by URL, the maximum length is 256 bytes*/  

    "faceLibType": "",  

    /*required, string type, face picture library type: "blackFD"-list library,  

    "staticFD"-static library, the maximum length is 32 bytes*/  

    "FDID": "",  

    /*required, string type, face picture library ID, the maximum length is 63  

    bytes, multiple face picture libraries should be separated by commas*/  

    "FPID": "",  

    /*optional, string type, face record ID, it can be generated by the device or  

    inputted. If it is inputted, it should be the unique ID with the combination of  

    letters and digits, and the maximum length is 63 bytes; if it is generated by  

    the device automatically, it is the same as the employee No. (person ID)*/  

    "name": "",  

    /*required, string type, name of the person in the face picture, the maximum  

    length is 96 bytes*/  

    "gender": "",  

    /*optional, string type, gender of the person in the face picture: "male",  

    "female", "unknown", the maximum length is 32 bytes*/  

    "bornTime": "",  

    /*required, string type, date of birth of the person in the face picture in  

    ISO8601 time format, the maximum length is 20 bytes*/  

    "city": "",  

    /*optional, string type, code of the city of birth for the person in the face  

    picture, the maximum length is 32 bytes*/  

    "certificateType": "",  

    /*optional, string type, ID type: "officerID"-officer ID, "ID"-ID card. The  

    maximum length is 10 bytes*/  

    "certificateNumber": "",  

    /*optional, string type, ID No., the maximum length is 32 bytes*/
```

```
    "caseInfo":"",
/*optional, string type, case information, the maximum length is 192 bytes, it
is valid when faceLibType is "blackFD"*/
    "tag":"",
/*optional, string type, custom tag, up to 4 tags can be added and they should
be separated by commas, the maximum length of each tag is 48 bytes, and the
maximum length of this node is 195 bytes. It is valid when faceLibType is
"blackFD"*/
    "address":"",
/*optional, string type, person address, the maximum length is 192 bytes, it is
valid when faceLibType is "staticFD"*/
    "customInfo":"",
/*optional, string type, custom information, the maximum length is 192 bytes,
it is valid when faceLibType is "staticFD"*/
    "modelData":"",
/*optional, string type, target model data, non-modeled binary data needs to be
encrypted by base64 during transmission*/
    "operateType": "byTerminal",
/*optional, string, operation type: "byTerminal"-by terminal*/
    "terminalNoList": [1],
/*optional, array, terminal ID list, this node is required when operation type
is "byTerminal"; currently, only one terminal is supported*/
    "PicFeaturePoints": [
/*optional, array of object, feature points to be applied. If the device only
supports three types of feature points, when the platform applies more than
three types of feature points, the device will not return error information*/
        "featurePointType": "face",
/*required, string, feature point type: "face", "leftEye" (left eye),
"rightEye" (right eye), "leftMouthCorner" (left corner of mouth),
"rightMouthCorner" (right corner of mouth), "nose"*/
        "coordinatePoint": {
/*required, object, coordinates of the feature point*/
            "x":1,
/*required, int, normalized X-coordinate which is between 0 and 1000*/
            "y":1,
/*required, int, normalized Y-coordinate which is between 0 and 1000*/
            "width":1,
/*required, int, width which is between 0 and 1000. This node is required when
featurePointType is "face"*/
            "height":1
/*required, int, height which is between 0 and 1000. This node is required when
featurePointType is "face"*/
        }
    ],
    "saveFacePic": true
/*optional, boolean, whether to save face pictures*/
}
```

JSON_BlackBodyCfg

JSON message about the black body parameters

```
{  
    "enabled":true,  
    /*required, boolean, whether to enable the black body*/  
    "Position":{  
        /*optional, object, black body position (coordinate), the value is normalized  
        to a number between 0 and 1000*/  
        "x":1,  
        /*optional, int, X-coordinate, value range: [0,1000]*/  
        "y":1  
        /*optional, int, Y-coordinate, value range: [0,1000]*/  
    },  
    "distance":1.0,  
    /*optional, float, distance between the black body and the lens, the value is  
    accurate to one decimal place, value range: [0.0,10.0], unit: meter*/  
    "emissivity":0.10,  
    /*optional, float, emissivity, the value is accurate to two decimal places,  
    value range: [0.00,1.00]*/  
    "unit":"celsius",  
    /*optional, string, temperature unit: "celsius", "fahrenheit"*/  
    "temperature":30.0  
    /*optional, float, black body temperature. When the value of the node unit is  
    "celsius", the value of this node is between 30.0 and 50.0; when the value of  
    the node unit is "fahrenheit", the value of this node is between 86.0 and  
    122.0. The value is accurate to one decimal place*/  
}
```

JSON_BluetoothCfg

JSON message about the bluetooth parameters of access control

```
{  
    "openDoorEnabled":true  
    /*optional, boolean, whether to enable opening the door via bluetooth*/  
}
```

JSON_BluetoothEncryptionInfoCfg

JSON message about the bluetooth encryption information

```
{  
    "encryptType": "",  
    /*required, string, encryption type: "AES128_CBC" (AES128 encryption in CBC  
    mode) */  
    "authData": "",
```

```
/*required, string, authentication information used for encryption, which is 32-byte hexadecimal data, e.g., "00112233445566778899aabbccddeeff"*/
    "vector": "",
/*required, string, initialization vector used for encryption, which is 32-byte hexadecimal data, e.g., "00112233445566778899aabbccddeeff"*/
    "loopCount": ,
/*required, int, repetition times for generating the key*/
    "employeeNo": ""
/*optional, string, employee No. (person ID). When you get the bluetooth encryption information, this node will only be returned by indoor stations. Door stations and MinMoe face recognition terminals will not return this node*/
}
```

JSON_Cap_AcsCfg

AcsCfg capability message in JSON format

```
{
    "AcsCfg": {
        "RS485Backup": "true,false",
/*optional, boolean, whether to enable downstream RS-485 communication redundancy: "true"-yes, "false"-no*/
        "showCapPic": "true,false",
/*optional, boolean, whether to display the captured picture: "true"-yes, "false"-no*/
        "showUserInfo": "true,false",
/*optional, boolean, whether to display user information: "true"-yes, "false"-no*/
        "overlayUserInfo": "true,false",
/*optional, boolean, whether to overlay user information: "true"-yes, "false"-no*/
        "voicePrompt": "true,false",
/*optional, boolean, whether to enable audio announcement: "true"-yes, "false"-no*/
        "uploadCapPic": "true,false",
/*optional, boolean, whether to upload the picture from linked capture: "true"-yes, "false"-no*/
        "saveCapPic": "true,false",
/*optional, boolean, whether to save the capture picture: "true"-yes, "false"-no*/
        "inputCardNo": "true,false",
/*optional, boolean, whether to allow inputting card No. on keypad: "true"-yes, "false"-no*/
        "enableWifiDetect": "true,false",
/*optional, boolean, whether to enable Wi-Fi probe: "true"-yes, "false"-no*/
        "enable3G4G": "true,false",
/*optional, boolean, whether to enable 3G/4G: "true"-yes, "false"-no*/
        "protocol": {
/*optional, string, communication protocol type of the card reader: "Private"-private protocol, "OSDP"-OSDP protocol*/
            "@opt": "Private,OSDP"
        }
    }
}
```

```

},
"enableCaptureCertificate": "true,false",
/*optional, string, whether to enable capturing the ID picture: true (yes),  

false (no). The captured ID picture will be compared with the captured face  

picture to check whether it is the same person. If this node does not exist, it  

indicates that this function is not supported*/
"showPicture":"true,false",
/*optional, boolean, whether to display the authenticated picture: "true"-  

display, "false"-not display*/
"showEmployeeNo":"true,false",
/*optional, boolean, whether to display the authenticated employee ID: "true"-  

display, "false"-not display*/
"showName":"true,false",
/*optional, boolean, whether to display the authenticated name: "true"-display,  

"false"-not display*/
"desensitiseEmployeeNo": {
/*dependent, boolean, whether to enable employee No. de-identification for  

local UI display: true (yes), false (no). This node is valid when the value of  

the node showEmployeeNo is true*/
    "@opt": [true,false]
},
"desensitiseName": {
/*dependent, boolean, whether to enable name de-identification for local UI  

display: true (yes), false (no). This node is valid when the value of the node  

showName is true*/
    "@opt": [true,false]
},
"thermalEnabled": {
/*optional, boolean, whether to enable temperature measurement: true-enable  

(default), false-disable*/
    "@opt": [true,false]
},
"thermalMode": {
/*optional, boolean, whether to enable temperature measurement only mode: true-  

enable (only for temperature measurement), false-disable (default)*/
    "@opt": [true,false]
},
"thermalPictureEnabled": {
/*optional, boolean, whether to enable uploading visible light pictures in  

temperature measurement only mode: true-enable, false-disable (default). This  

field is used to control uploading captured pictures and visible light  

pictures*/
    "@opt": [true,false]
},
"isSupportThermalIp": true,
/*optional, boolean, whether it supports configuring IP address of the  

thermography device: true-yes, this field is not returned-no*/
"highestThermalThreshold": {
/*optional, float, upper limit of the temperature threshold which is accurate  

to one decimal place, unit: Celsius*/
    "@min": ,
    "@max": 
}

```

```

},
"lowestThermalThreshold": {
/*optional, float, lower limit of the temperature threshold which is accurate
to one decimal place, unit: Celsius*/
    "@min": ,
    "@max": ,
},
"thermalDoorEnabled": {
/*optional, boolean, whether to open the door when the temperature is above the
upper limit (highestThermalThreshold) or below the lower limit
(lowestThermalThreshold) of the threshold: true-open the door, false-not open
the door (default)*/
    "@opt": [true,false]
},
"QRCodeEnabled": {
/*optional, boolean, whether to enable QR code function: true-enable, false-
disable (default)*/
    "@opt": [true,false]
},
"remoteCheckDoorEnabled": {
/*optional, boolean, whether to enable controlling the door by remote
verification: true-control, false-not control (default)*/
    "@opt": [true,false]
},
"checkChannelType": {
/*dependent, string, verification channel type: "Ezviz"-EZVIZ channel, "ISUP"-ISUP
channel, "ISAPI"-ISAPI channel, "PrivateSDK"-private SDK channel,
"ISAPIListen"-ISAPI listening channel. This field is valid when
remoteCheckDoorEnabled is true*/
    "@opt": ["Ezviz","ISUP","ISAPI","PrivateSDK","ISAPIListen"]
},
"isSupportChannelIp": true,
/*optional, boolean, whether it supports configuring IP address of the
verification channel: true-yes, this field is not returned-no*/
"uploadVerificationPic":"",
/*optional, boolean, whether to upload the authenticated picture: true, false*/
"saveVerificationPic":"",
/*optional, boolean, whether to save the authenticated picture: true, false*/
"saveFacePic":"",
/*optional, boolean, whether to save the registered face picture: true, false*/
"thermalUnit":{
/*optional, object, temperature unit: "celsius" (default), "fahrenheit"*/
    "@opt":["celsius", "fahrenheit"]
},
"highestThermalThresholdF": {
/*optional, object, the maximum value of the temperature threshold. The value
is accurate to one decimal place, and the unit is Fahrenheit*/
    "@min":1.0,
    "@max":1.0
},
"lowestThermalThresholdF": {
/*optional, object, the minimum value of the temperature threshold. The value

```

```
is accurate to one decimal place, and the unit is Fahrenheit*/
    "@min":1.0,
    "@max":1.0
},
"thermalCompensation":{
/*optional, object, temperature compensation, the value is accurate to one
decimal place. The unit depends on the node thermalUnit. If the node
thermalUnit does not exist, the default unit is Celsius*/
    "@min":-99.9,
    "@max":99.9
}
}
```

JSON_Cap_AcsEvent

AcsEvent capability message in JSON format

```
{
  "AcsEvent": {
    "AcsEventCond": {
      /*optional, search conditions*/
      "searchID": {
        /*required, string type, search ID, which is used to confirm the upper-level
        platform or system. If the platform or the system is the same one during two
        searching, the search history will be saved in the memory to speed up next
        searching*/
        "@min": ,
        "@max":
      },
      "searchResultPosition": {
        /*required, integer, the start position of the search result in the result
        list. When there are multiple records and you cannot get all search results at
        a time, you can search for the records after the specified position next time*/
        "@min": ,
        "@max":
      },
      "maxResults": {
        /*required, integer, maximum number of search results*/
        "@min": ,
        "@max":
      },
      "major": {
        /*required, integer, major alarm/event types (the type value should be
        transformed to the decimal number), refer to Access Control Event Types for
        details*/
        "@opt": "0,1,2,3,5"
      },
      "minorAlarm": {
        /*required, integer, minor alarm type (the type value should be transformed to
        the decimal number), refer to Access Control Event Types for details*/
      }
    }
  }
}
```

```
        "@opt": "1024,1025,1026,1027..."  
    },  
    "minorException":{  
/*required, integer, minor exception type (the type value should be transformed  
to the decimal number), refer to Access Control Event Types for details*/  
        "@opt": "39,58,59,1024..."  
    },  
    "minorOperation":{  
/*required, integer, minor operation type (the type value should be transformed  
to the decimal number), refer to Access Control Event Types for details*/  
        "@opt": "80,90,112,113..."  
    },  
    "minorEvent":{  
/*required, integer, minor event type (the type value should be transformed to  
the decimal number), refer to Access Control Event Types for details*/  
        "@opt": "1,2,3,4..."  
    },  
    "startTime":{  
/*optional, string, start time (UTC time)*/  
        "@min": ,  
        "@max":  
    },  
    "endTime":{  
/*optional, string, end time (UTC time)*/  
        "@min": ,  
        "@max":  
    },  
    "cardNo":{  
/*optional, string, card No.*/  
        "@min": ,  
        "@max":  
    },  
    "name":{  
/*optional, string, cardholder name*/  
        "@min": ,  
        "@max":  
    },  
    "picEnable": "true,false",  
/*optional, boolean, whether to contain pictures: "false"-no, "true"-yes*/  
    "beginSerialNo":{  
/*optional, integer, start serial No.*/  
        "@min": ,  
        "@max":  
    },  
    "endSerialNo":{  
/*optional, integer, end serial No.*/  
        "@min": ,  
        "@max":  
    },  
    "employeeNoString":{  
/*optional, string, employee No. (person ID)*/  
        "@min": ,
```

```

        "@max":  
    },  
    "eventAttribute":{  
/*optional, string, event attribute: "attendance"-valid authentication,  
"other"*/  
        "@opt":"attendance,other"  
    },  
    "employeeNo": {  
/*optional, string, employee No. (person ID)*/  
        "@min": ,  
        "@max":  
    },  
    "timeReverseOrder": "true,false",  
/*optional, boolean, whether to return events in descending order of time  
(later events will be returned first): true-yes, false or this node is not  
returned-no*/  
    "isAbnormalTemperature":{  
/*optional, object, whether the skin-surface temperature is abnormal*/  
        "@opt": [true, false]  
/*optional, array of boolean, options: true (yes), false (no)*/  
    }  
},  
    "InfoList":{  
/*optional, event details*/  
        "maxSize": 10,  
        "time":{  
/*required, string, time (UTC time)*/  
            "@min": ,  
            "@max":  
        },  
        "netUser":{  
/*optional, string, user name*/  
            "@min": ,  
            "@max":  
        },  
        "remoteHostAddr":{  
/*optional, string, remote host address*/  
            "@min": ,  
            "@max":  
        },  
        "cardNo":{  
/*optional, string, card No.*/  
            "@min": ,  
            "@max":  
        },  
        "cardType":{  
/*optional, integer, card type: "1"-normal card, "2"-disabled card, "3"-  
blocklist card, "4"-patrol card, "5"-duress card, "6"-super card, "7"-visitor  
card, "8"-dismiss card*/  
            "@opt": "1,2,3,4,5,6,7,8"  
        },  
        "whiteListNo":{  
/*optional, string, white list No.*/  
            "@min": ,  
            "@max":  
        }  
}  
}

```

```
/*optional, integer, allowlist No., which is between 1 and 8*/
    "@min": ,
    "@max": ,
},
"reportChannel":{

/*optional, integer, channel type for uploading alarm/event: "1"-for uploading arming information, "2"-for uploading by central group 1, "3"-for uploading by central group 2*/
    "@opt": "1,2,3"
},
"cardReaderKind":{

/*optional, integer, authentication unit type: "1"-IC card reader, "2"-ID card reader, "3"-QR code scanner, "4"-fingerprint module*/
    "@opt": "1,2,3,4"
},
"cardReaderNo":{

/*Optional, integer, authentication unit No.*/
    "@min": ,
    "@max": ,
},
"doorNo":{

/*optional, integer, door or floor No.*/
    "@min": ,
    "@max": ,
},
"verifyNo":{

/*optional, integer, multiple authentication No.*/
    "@min": ,
    "@max": ,
},
"alarmInNo":{

/*optional, integer, alarm input No.*/
    "@min": ,
    "@max": ,
},
"alarmOutNo":{

/*optional, integer, alarm output No.*/
    "@min": ,
    "@max": ,
},
"caseSensorNo":{

/*optional, integer, event trigger No.*/
    "@min": ,
    "@max": ,
},
"RS485No":{

/*optional, integer, RS-485 channel No.*/
    "@min": ,
    "@max": ,
},
"multiCardGroupNo":{

/*optional, integer, group No.*/
}
```

```

        "@min": ,
        "@max":
    },
    "accessChannel":{
/*optional, integer, swing barrier No.*/
        "@min": ,
        "@max":
    },
    "deviceNo":{
/*optional, integer, device No.*/
        "@min": ,
        "@max":
    },
    "distractControlNo":{
/*optional, integer, distributed access controller No.*/
        "@min": ,
        "@max":
    },
    "employeeNo":{
/*optional, string, employee No. (person ID)*/
        "@min": ,
        "@max":
    },
    "localControllerID":{
/*optional, integer, distributed access controller No.: "0"-access controller,
"1" to "64"-distributed access controller No.1 to distributed access controller
No.64*/
        "@min": ,
        "@max":
    },
    "InternetAccess":{
/*optional, integer, network interface No.: "1"-upstream network interface No.
1, "2"-upstream network interface No.2, "3"-downstream network interface No.1*/
        "@min": ,
        "@max":
    },
    "type":{
/*optional, integer, zone type: "0"-instant alarm zone, "1"-24-hour alarm zone,
"2"-delayed zone, "3"-internal zone, "4"-key zone, "5"-fire alarm zone, "6"-perimeter protection, "7"-24-hour slient alarm zone, "8"-24-hour auxiliary
zone, "9"-24-hour shock alarm zone, "10"-emergency door open alarm zone, "11"-emergency door closed alarm zone, "255"-none*/
        "@opt": "0,1,2,3,4,5,6,7,8,9,10,11,255"
    },
    "MACAddr":{
/*optional, string, physical address*/
        "@min": ,
        "@max":
    },
    "swipeCardType":{
/*optional, integer, card swiping type: "0"-invalid, "1"-QR code*/
        "@opt": "0,1"
}

```

```

    },
    "serialNo": {
        /*optional, integer, event serial No., which is used to judge whether the event
        loss occurred*/
        "@min": ,
        "@max":
    },
    "channelControllerID": {
        /*optional, integer, lane controller No.: "1"-main lane controller, "2"-sub
        lane controller*/
        "@opt": "0,1"
    },
    "channelControllerLampID": {
        /*optional, integer, light board No. of lane controller, which is between 1 and
        255*/
        "@min": ,
        "@max":
    },
    "channelControllerIRAdaptorID": {
        /*optional, integer, IR adapter No. of lane controller, which is between 1 and
        255*/
        "@min": ,
        "@max":
    },
    "channelControllerIREmitterID": {
        /*optional, integer, active infrared intrusion detector No. of lane controller,
        which is between 1 and 255*/
        "@min": ,
        "@max":
    },
    "userType": {
        /*optional, string, person types: "normal"-normal person (household), "visitor"-visitor,
        "blacklist"-person in blocklist, "administrators"-administrator*/
        "@opt": "normal,visitor,blackList,administrators"
    },
    "currentVerifyMode": {
        /*optional, string, authentication modes: "cardAndPw"-card+password, "card",
        "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password,
        "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password,
        "faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password,
        "faceAndCard"-face+card, "face", "employeeNoAndPw"-employee No.+password,
        "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint,
        "employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card,
        "faceAndPwAndFp"-face+password+fingerprint,
        "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card,
        "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password,
        "cardOrFpOrPw"-card or fingerprint or password*/
        "@opt":
    }
}

```

```

OrfaceAndCard, fpOrface, cardOrfaceOrPw, cardOrFpOrPw"
    },
    "QRCodeInfo": {
/*optional, object, QR code information*/
        "@min":1,
        "@max":1
    },
    "thermometryUnit": {
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
        "@opt": ["celsius","fahrenheit","kelvin"]
    },
    "currTemperature": {
/*optional, float, face temperature which is accurate to one decimal place*/
        "@min":1 ,
        "@max":1
    },
    "isAbnormalTemperature": {
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
        "@opt": [true,false]
    },
    "RegionCoordinates": {
/*optional, face temperature's coordinates*/
        "positionX": {
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
            "@min": 0,
            "@max": 1000
        },
        "positionY": {
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
            "@min": 0,
            "@max": 1000
        }
    },
    "picEnable": "true,false",
/*optional, boolean, whether to contain pictures*/
    "picturesNumber":{
/*optional, integer, number of captured pictures if the capture linkage action is configured. This node will be 0 or not be returned if there is no picture*/
        "@min": ,
        "@max": 
    },
    "filename": {
/*optional, string, file name. If multiple pictures are returned at a time, the file name of each picture should be unique, and the value of this node should be the same as the following one*/
        "@min": ,
        "@max": 
    },
    "attendanceStatus":{
/*optional, string, attendance status: "undefined", "checkIn"-check in,

```

```
"checkOut"-check out, "breakOut"-break out, "breakIn"-break in, "overtimeIn"-overtime in, "overTimeOut"-overtime out*/  
  
"@opt":"undefined,checkIn,checkOut,breakOut,breakIn,overtimeIn,overtimeOut"  
},  
"label":{  
/*optional, string, custom attendance name*/  
    "@min": ,  
    "@max":  
},  
"statusValue":{  
/*optional, integer, status value*/  
    "@min":0,  
    "@max":255  
},  
"mask": {  
/*optional, string, whether the person is wearing mask: "unknown", "yes"-wearing mask, "no"-not wearing mask*/  
    "@opt": "unknown,yes,no"  
},  
"pictureURL":{  
/*optional, object, URL of the captured picture*/  
    "@min":1,  
    "@max":1  
},  
"helmet": {  
/*optional, string, whether the person is wearing hard hat: "unknown", "yes"-wearing hard hat, "no"-not wearing hard hat*/  
    "@opt": "unknown,yes,no"  
},  
"visibleLightPicUrl":{  
/*optional, object, URL of the visible light picture*/  
    "@min":1,  
    "@max":1  
},  
"thermalPicUrl":{  
/*optional, object, URL of the thermal picture*/  
    "@min":1,  
    "@max":1  
},  
"HealthInfo":{  
/*optional, object, health information*/  
    "healthCode":{  
/*optional, object, health code status*/  
        "@opt": [0, 1, 2, 3, 4, 5, 6]  
/*optional, array of int, options: 0 (no request), 1 (no health code), 2 (green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6 (other error, e.g., searching failed due to API exception), 7 (searching for the health code timed out)*/  
    },  
    "NADCode":{  
/*optional, object, nucleic acid test result: 0 (no result), 1 (negative, which
```

```
means normal), 2 (positive, which means diagnosed), 3 (the result has expired) */
        "@opt": [0, 1, 2, 3]
    },
    "travelCode": {
        /*optional, object, trip code: 0 (no trip in the past 14 days), 1 (once left in
        the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3
        (other)*/
        "@opt": [0, 1, 2, 3]
    },
    "vaccineStatus": {
        /*optional, object, whether the person is vaccinated: 0 (not vaccinated), 1
        (vaccinated)*/
        "@opt": [0, 1]
    }
}
}
}
```

See Also

Access Control Event Types

JSON_Cap_AcsEventTotalNum

AcsEventTotalNum capability message in JSON format

```
{  
    "AcsEvent":{  
        "AcsEventTotalNumCond":{  
/*optional, search conditions*/  
            "major":{  
/*required, integer type, major type (the type value should be transformed to  
the decimal number): 0-all, 1-major alarm type, 2-major exception type, 3-major  
operation type, 5-major event type, refer to  
                "Access Control Event Types  
for details*/  
                "@opt":"0,1,2,3,5"  
            },  
            "minorAlarm":{  
/*required, integer, minor alarm type (the type value should be transformed to  
the decimal number), refer to Access Control Event Types for details*/  
                "@opt":"1024,1025,1026,1027..."  
            },  
            "minorException":{  
/*required, integer, minor exception type (the type value should be transformed  
to the decimal number), refer to Access Control Event Types for details*/  
                "@opt":"39,58,59,1024..."  
            },  
            "minorOperation":{  
/*required, integer, minor operation type (the type value should be transformed
```

```
to the decimal number), refer to Access Control Event Types for details*/
    "@opt":"80,90,112,113..."  
},  
    "minorEvent":{  
/*required, integer, minor event type (the type value should be transformed to  
the decimal number), refer to Access Control Event Types for details*/  
    "@opt":"1,2,3,4..."  
},  
    "startTime":{  
/*optional, string, start time (UTC time)*/  
    "@min": ,  
    "@max":  
},  
    "endTime":{  
/*optional, string, end time (UTC time)*/  
    "@min": ,  
    "@max":  
},  
    "cardNo":{  
/*optional, string, card No.*/  
    "@min": ,  
    "@max":  
},  
    "name":{  
/*optional, string, cardholder name*/  
    "@min": ,  
    "@max":  
},  
    "picEnable":"true,false",  
/*optional, boolean, whether to contain pictures: "false"-no, "true"-yes*/  
    "beginSerialNo":{  
/*optional, integer, start serial No.*/  
    "@min": ,  
    "@max":  
},  
    "endSerialNo":{  
/*optional, integer, end serial No.*/  
    "@min": ,  
    "@max":  
},  
    "employeeNoString":{  
/*optional, string, employee No. (person ID)*/  
    "@min": ,  
    "@max":  
},  
    "eventAttribute":{  
/*optional, string, event attribute: "attendance"-valid authentication,  
"other"*/  
    "@opt":"attendance,other"  
}  
},  
    "totalNum":{
```

```
/*required, integer, total number of events that match the search conditions*/
    "@min": ,
    "@max":
  }
}
}
```

See Also

[Access Control Event Types](#)

JSON_Cap_AcsWorkStatus

AcsWorkStatus capability message in JSON format

```
{
  "AcsWorkStatus": {
    "doorLockStatus": {
      /*optional, array, door lock status (relay status): 0-normally close, 1-normally open, 2-short-circuit alarm, 3-broken-circuit alarm, 4-exception alarm*/
        "@opt":"0,1,2,3,4"
      },
      "doorStatus": {
        /*optional, array, door (floor) status: 1-sleep, 2-remain unlocked (free), 3-remain locked (disabled), 4-normal status (controlled)*/
          "@opt":"1,2,3,4"
        },
        "magneticStatus": {
          /*optional, array, magnetic contact status: 0-normally close, 1-normally open, 2-short-circuit alarm, 3-broken-circuit alarm, 4-exception alarm*/
            "@opt":"0,1,2,3,4"
          },
          "caseStatus": {
            /*optional, array, event trigger status*/
              "@min": ,
              "@max":
            },
            "batteryVoltage": {
              /*optional, integer, storage battery power voltage, the actual value will be 10 times of this value, unit: Volt*/
                "@min": ,
                "@max":
              },
              "batteryLowVoltage": "true,false",
            /*optional, boolean, whether the storage battery is in low voltage status: "true"-yes, "false"-no*/
              "powerSupplyStatus": {
                /*optional, string, device power supply status: "ACPowerSupply"-alternative current, "BatteryPowerSupply"-storage battery power supply*/
                  "@opt": "ACPowerSupply,BatteryPowerSupply"
                }
              }
            }
          }
        }
```

```
},
"multiDoorInterlockStatus":{
/*optional, string, multi-door interlocking status: "close"-disabled, "open"-enabled*/
    "@opt":"close,open"
},
"antiSneakStatus":{
/*optional, string, anti-passback status: "close"-disabled, "open"-enabled*/
    "@opt":"close,open"
},
"hostAntiDismantleStatus":{
/*optional, string, tampering status of the access control device: "close"-disabled, "open"-enabled*/
    "@opt":"close,open"
},
"indicatorLightStatus":{
/*optional, string, indicator status: "offLine"-offline, "onLine"-online*/
    "@opt":"offLine,onLine"
},
"cardReaderOnlineStatus":{
/*optional, array, online status of the authentication unit*/
    "@min": ,
    "@max":
},
"cardReaderAntiDismantleStatus":{
/*optional, array, tampering status of the authentication unit*/
    "@min": ,
    "@max":
},
"cardReaderVerifyMode":{
/*optional, array, current authentication mode of the authentication unit: 1-sleep, 2-card+password, 3-card, 4-card or password, 5-fingerprint, 6-fingerprint+password, 7-fingerprint or card, 8-fingerprint+card, 9-fingerprint+card+password, 10-face or fingerprint or card or password, 11-face+fingerprint, 12-face+password, 13-face+card, 14-face, 15-employee No.+password, 16-fingerprint or password, 17-employee No.+fingerprint, 18-employee No.+fingerprint+password, 19-face+fingerprint+card, 20-face+password+fingerprint, 21-employee No.+face, 22-face or face+card, 23-fingerprint or face, 24-card or face or password, 25-card or face, 26-card or face or fingerprint, 27-card or fingerprint or password*/
    "@opt":"1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27"
},
"setupAlarmStatus":{
/*optional, array, No. of armed input port*/
    "@min": ,
    "@max":
},
"alarmInStatus":{
/*optional, array, No. of input port with alarms*/
    "@min": ,
    "@max":
```

```

},
"alarmOutStatus":{
/*optional, array, No. of output port with alarms*/
    "@min": ,
    "@max": 
},
"cardNum":{
/*optional, integer, number of added cards*/
    "@min": ,
    "@max": 
},
"fireAlarmStatus":{
/*optional, string, fire alarm status: "normal", "shortCircuit"-short-circuit
alarm, "brokenCircuit"-broken-circuit alarm*/
    "@opt":"normal,shortCircuit,brokenCircuit"
},
"batteryChargeStatus":{
/*optional, string, battery charging status: "charging", "uncharged"*/
    "@opt":"charging,uncharged"
},
"masterChannelControllerStatus":{
/*optional, string, online status of the main lane controller: "offLine"-offline,
"onLine"-online*/
    "@opt":"offLine,onLine"
},
"slaveChannelControllerStatus":{
/*optional, string, online status of the sub lane controller: "offLine"-offline,
"onLine"-online*/
    "@opt":"offLine,onLine"
},
"antiSneakServerStatus":{
/*optional, string, anti-passback server status: "disable"-disabled, "normal",
"disconnect"-disconnected*/
    "@opt":"disable,normal,disconnect"
}
}
}

```

JSON_Cap_AntiSneakCfg

AntiSneakCfg capability message in JSON format

```
{
"AntiSneakCfg": {
    "enable": "true,false",
/*required, boolean, whether to enable anti-passing back*/
    "startCardReaderNo": {
/*optional, integer, first card reader No., 0-no first card reader*/
        "@min": 1,
        "@max": 4
    }
}
```

```
    }
}
```

JSON_Cap_AttendanceMode

JSON message about the configuration capability of the attendance mode

```
{
  "AttendanceMode": {
    "mode": {
      /*optional, string, attendance mode: "disable", "manual", "auto"-automatic,
      "manualAndAuto"-manual and automatic*/
      "@opt": ["disable", "manual", "auto", "manualAndAuto"]
    },
    "attendanceStatusTime": {
      /*optional, int, attendance status duration, unit: second. This node is valid
      when mode is "manual" or "manualAndAuto"*/
      "@min": 0,
      "@max": 0
    }
  }
}
```

JSON_Cap_BlackBodyCfg

JSON message about the configuration capability of the black body

```
{
  "enabled": {
    /*required, object, whether to enable the black body. The black body is used to
    calibrate the temperature of the thermography module. You need to put the black
    body with fixed temperature in front of the device and calibrate the
    temperature of the thermography module according to the black body in the
    image*/
    "@opt": [true, false]
  },
  "Position": {
    /*optional, object, black body position (coordinate), the value is normalized
    to a number between 0 and 1000*/
    "x": {
      /*optional, object, X-coordinate*/
      "@min": 0,
      "@max": 1000
    },
    "y": {
      /*optional, object, Y-coordinate*/
      "@min": 0,
      "@max": 1000
    }
  }
}
```

```
},
"distance": {
/*optional, object, distance between the black body and the lens, the value is
accurate to one decimal place, unit: meter*/
    "@min":0.0,
    "@max":10.0
},
"emissivity": {
/*optional, object, emissivity, the value is accurate to two decimal places.
The emissivity is applied from the system or platform to the device and is
transmitted to the thermography module by the device for temperature
measurement*/
    "@min":0.00,
    "@max":1.00
},
"TemperatureList": [
/*optional, array of object, temperature list of the black body. The second
decimal place of the black body's temperature will be rounded to eliminate the
error. For example, 0.95 will be input as 1.0*/
    "unit":"celsius",
/*optional, string, temperature unit: "celsius", "fahrenheit"*/
    "temperature": {
/*optional, object, black body temperature. When the unit is "celsius", the
value of this node is between 30.0 and 50.0; when the unit is "fahrenheit", the
value of this node is between 86.0 and 122.0*/
        "@min":30.0,
        "@max":50.0
    }
}
}
```

JSON_Cap_BluetoothCfg

JSON message about the capability of configuring bluetooth parameters of access control

```
{
    "openDoorEnabled": {
/*optional, object, whether to enable opening the door via bluetooth*/
        "@opt": [true, false]
    }
}
```

JSON_Cap_BluetoothEncryptionInfoCfg

JSON message about the capability of configuring the bluetooth encryption information

```
{
    "encryptType": {
/*required, object, encryption type: "AES128_CBC" (AES128 encryption in CBC
```

```
mode) */
    "@opt": ["AES128_CBC"]
},
"authData": {
/*required, object, authentication information used for encryption, which is 32-byte hexadecimal data*/
    "@min":32,
    "@max":32
},
"vector": {
/*required, object, initialization vector used for encryption, which is 32-byte hexadecimal data*/
    "@min":32,
    "@max":32
},
"loopCount": ,
/*required, int, repetition times for generating the key*/
"employeeNo": {
/*optional, object, employee No. (person ID)*/
    "@min": ,
    "@max": 
}
}
```

JSON_Cap_CardInfo

CardInfo capability message in JSON format

```
{
    "CardInfo": {
        "supportFunction": {
/*required, supported functions of adding, editing, deleting, searching for card information, and getting the total number of added cards: "post"-add, "delete", "put"-edit, "get"-search, "setUp"-set*/
            "@opt": "post,delete,put,get,setUp"
        },
        "CardInfoSearchCond": {
/*optional, search conditions*/
            "searchID": {
/*required, string type, search ID, which is used to check the upper-level platform or system. If the platform or the system is the same one during two searching, the search history will be saved in the memory to speed up next searching*/
                "@min":1,
                "@max":36
            },
            "maxResults": {
/*required, integer32, maximum number of obtained records*/
                "@min":1,
                "@max":30
            }
        }
    }
}
```

```
"EmployeeNoList":{  
/*optional, person ID list*/  
    "maxSize":56,  
    "employeeNo":{  
/*optional, string, employee No. (person ID)*/  
        "@min": ,  
        "@max":  
    }  
},  
"CardNoList":{  
/*optional, card No. list*/  
    "maxSize":56,  
    "cardNo":{  
/*optional, string, card No.*/  
        "@min":1,  
        "@max":32  
    }  
},  
"CardInfoDelCond":{  
/*optional, deleting conditions*/  
    "EmployeeNoList":{  
/*optional, person ID list*/  
        "maxSize":56,  
        "employeeNo":{  
/*optional, string, employee No. (person ID)*/  
            "@min": ,  
            "@max":  
        }  
},  
    "CardNoList":{  
/*optional, card No. list*/  
        "maxSize":56,  
        "cardNo":{  
/*optional, string, card No.*/  
            "@min":1,  
            "@max":32  
        }  
},  
    "cardNo":{  
/*required, string, card No.*/  
        "@min":1,  
        "@max":32  
},  
    "employeeNo":{  
/*required, string, employee No. (person ID)*/  
        "@min": ,  
        "@max":  
},  
    "cardType":{  
/*required, string, card type: "normalCard"-normal card, "patrolCard"-patrol
```

```
card, "hijackCard"-duress card, "superCard"-super card, "dismissingCard"-  
dismiss card, "emergencyCard"-emergency card (it is used to assign permission  
to a temporary card, but it cannot open the door)*/  
  
"@opt":"normalCard,patrolCard,hijackCard,superCard,dismissingCard,emergencyCard"  
},  
"leaderCard":{  
/*optional, string, whether to support first card authentication function*/  
    "@min":1,  
    "@max":32  
},  
"checkCardNo":"true,false",  
/*optional, boolean, whether to enable duplicated card verification: "false"-  
disable, "true"-enable. If this node is not configured, the device will verify  
the duplicated card by default. When there is no card information, you can set  
checkCardNo to "false" to speed up data applying; otherwise, it is not  
recommended to configure this node*/  
"checkEmployeeNo":"true,false",  
/*optional, boolean, whether to check the existence of the employee No. (person  
ID): "false"-no, "true"-yes. If this node is not configured, the device will  
judge the existence of the employee No. (person ID) by default. If this node is  
set to "false", the device will not judge the existence of the employee No.  
(person ID) to speed up data applying; if this node is set to "true" or NULL,  
the device will judge the existence of the employee No. (person ID), and it is  
recommended to set this node to "true" or NULL if there is no need to speed up  
data applying*/  
"addCard":"true,false",  
/*optional, boolean type, whether to add the card if the card information being  
edited does not exist: "false"-no (if the device has checked that the card  
information being edited does not exist, the failure response message will be  
returned along with the error code), "true"-yes (if the device has checked that  
the card information being edited does not exist, the success response message  
will be returned, and the card will be added). If this node is not configured,  
the card will not be added by default*/  
"maxRecordNum":  
/*required, integer type, supported maximum number of records (card records)*/  
}  
}
```

JSON_Cap_CardReaderAntiSneakCfg

CardReaderAntiSneakCfg capability message in JSON format

```
{  
    "CardReaderAntiSneakCfg": {  
        "cardReaderNo": {  
            /*optional, string, card reader No.*/  
            "@min": ,  
            "@max":  
        }  
        "enable": "true,false",  
    }  
}
```

```
/*required, boolean, whether to enable the anti-passing back function of the
card reader: "true"-enable, "false"-disable*/
    "followUpCardReader": {
/*optional, array, following card reader No. after the first card reader*/
        "@min": ,
        "@max":
    }
}
```

JSON_Cap_CardReaderCfg

CardReaderCfg capability message in JSON format

```
{
    "CardReaderCfg": {
        "cardReaderNo": {
/*optional, integer, card reader No.*/
            "@min": ,
            "@max":
        },
        "enable": "true, false",
/*required, boolean, whether to enable: "true"-yes, "false"-no*/
        "okLedPolarity": {
/*optional, string, OK LED polarity: "cathode", "anode"*/
            "@opt": "cathode, anode"
        },
        "errorLedPolarity": {
/*optional, string, error LED polarity: "cathode", "anode"*/
            "@opt": "cathode, anode"
        },
        "buzzerPolarity": {
/*optional, string, buzzer polarity: "cathode", "anode"*/
            "@opt": "cathode, anode"
        },
        "swipeInterval": {
/*optional, integer, time interval of repeated authentication, which is valid
for authentication modes such as fingerprint, card, face, etc., unit: second*/
            "@min": 1,
            "@max": 255
        },
        "pressTimeout": {
/*optional, integer, timeout to reset entry on keypad, unit: second*/
            "@min": 1,
            "@max": 255
        },
        "enableFailAlarm": "true, false",
/*optional, boolean, whether to enable excessive failed authentication attempts
alarm*/
        "maxReadCardFailNum": {
/*optional, integer, maximum number of failed authentication attempts*/
    }
```

```

        "@min":1,
        "@max":255
    },
    "enableTamperCheck":"true,false",
/*optional, boolean, whether to enable tampering detection*/
    "offlineCheckTime":{
/*optional, integer, time to detect after the card reader is offline, unit:
second*/
        "@min":1,
        "@max":255
    },
    "fingerPrintCheckLevel":{
/*optional, integer, fingerprint recognition level: 1-1/10 false acceptance
rate (FAR), 2-1/100 false acceptance rate (FAR), 3-1/1000 false acceptance rate
(FAR), 4-1/10000 false acceptance rate (FAR), 5-1/100000 false acceptance rate
(FAR), 6-1/1000000 false acceptance rate (FAR), 7-1/10000000 false acceptance
rate (FAR), 8-1/100000000 false acceptance rate (FAR), 9-3/100 false acceptance
rate (FAR), 10-3/1000 false acceptance rate (FAR), 11-3/10000 false acceptance
rate (FAR), 12-3/100000 false acceptance rate (FAR), 13-3/1000000 false
acceptance rate (FAR), 14-3/10000000 false acceptance rate (FAR),
15-3/100000000 false acceptance rate (FAR), 16-Automatic Normal, 17-Automatic
Secure, 18-Automatic More Secure (currently not support)*/
        "@opt":"1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18"
    },
    "useLocalController":"true,false",
/*ro, opt, boolean, whether it is connected to the distributed controller*/
    "localControllerID":{
/*ro, opt, integer, distributed controller No., which is between 1 and 64, 0-
unregistered. This field is valid only when useLocalController is "true"*/
        "@min":0,
        "@max":64
    },
    "localControllerReaderID":{
/*ro, opt, integer, card reader ID of the distributed controller, 0-
unregistered. This field is valid only when useLocalController is "true"*/
        "@min":0,
        "@max":4
    },
    "cardReaderChannel":{
/*ro, opt, integer, communication channel No. of the card reader: 0-Wiegand or
offline, 1-RS-485A, 2-RS-485B. This field is valid only when useLocalController
is "true"*/
        "@opt":"0,1,2"
    },
    "fingerPrintImageQuality":{
/*opt, integer, fingerprint image quality: 1-low quality (V1), 2-medium quality
(V1), 3-high quality (V1), 4-highest quality (V1), 5-low quality (V2), 6-medium
quality (V2), 7-high quality (V2), 8-highest quality (V2)*/
        "@opt":"1,2,3,4,5,6,7,8"
    },
    "fingerPrintContrastTimeOut":{
/*optional, integer, fingerprint comparison timeout, which is between 1 and 20,

```

```
unit: second, 255-infinite*/
    "@min":0,
    "@max":20
},
"fingerPrintRecognizeInterval":{
/*optional, integer, fingerprint scanning interval, which is between 1 and 10,
unit: second, 255-no delay*/
    "@min":0,
    "@max":10
},
"fingerPrintMatchFastMode":{
/*optional, integer, fingerprint matching quick mode: 1-quick mode 1, 2-quick
mode 2, 3-quick mode 3, 4-quick mode 4, 5-quick mode 5, 255-automatic*/
    "@min":0,
    "@max":5
},
"fingerPrintModuleSensitive":{
/*optional, integer, fingerprint module sensitivity, which is between 1 and 8*/
    "@min":1,
    "@max":8
},
"fingerPrintModuleLightCondition":{
/*optional, string, fingerprint module light condition: "outdoor", "indoor"*/
    "@opt":"outdoor,indoor"
},
"faceMatchThresholdN":{
/*optional, integer, threshold of face picture 1:N comparison, which is between
0 and 100*/
    "@min":0,
    "@max":100
},
"faceQuality":{
/*optional, integer, face picture quality, which is between 0 and 100*/
    "@min":0,
    "@max":100
},
"faceRecognizeTimeOut":{
/*optional, integer, face recognition timeout, which is between 1 and 20, unit:
second, 255-infinite*/
    "@min":0,
    "@max":20
},
"faceRecognizeInterval":{
/*optional, integer, face recognition interval, which is between 1 and 10,
unit: second, 255-no delay*/
    "@min":0,
    "@max":10
},
"cardReaderFunction":{
/*ro, opt, array, card reader type: "fingerPrint"-fingerprint, "face",
"fingerVein"-finger vein*/
    "@opt":"fingerPrint,face,fingerVein"
```

```
},
"cardReaderDescription":{

/*ro, opt, card reader description. If the card reader is the Wiegand card
reader or if offline, this field will be set to "Wiegand" or "485Offline"*/
    "@min":1,
    "@max":16
},
"faceImageSensitometry":{

/*ro, opt, integer, face picture exposure, which is between 0 and 65535*/
    "@min":0,
    "@max":65535
},
"livingBodyDetect":"true,false",
/*optional, boolean, whether to enable human detection*/
"faceMatchThreshold1":{

/*optional, integer, threshold of face picture 1:1 comparison, which is between
0 and 100*/
    "@min":0,
    "@max":100
},
"buzzerTime":{

/*optional, integer, buzzing duration, which is between 0 and 5999, unit:
second, 0-long buzzing*/
    "@min":0,
    "@max":5999
},
"faceMatch1SecurityLevel":{

/*optional, integer, security level of face 1:1 recognition: 1-normal, 2-high,
3-higher*/
    "@opt":"1,2,3"
},
"faceMatchNSecurityLevel":{

/*optional, integer, security level of face 1:N recognition: 1-normal, 2-high,
3-higher*/
    "@opt":"1,2,3"
},
"envirMode":{

/*optional, string, environment mode of face recognition: "indoor", "other"*/
    "@opt":"indoor,other"
},
"liveDetLevelSet":{

/*optional, string, threshold level of liveness detection: "low", "middle"-medium,
 "high"*/
    "@opt":"low,middle,high"
},
"liveDetAntiAttackCntLimit":{

/*optional, integer, number of anti-attacks of liveness detection, which is
between 1 and 255. This value should be configured as the same one on both
client and device*/
    "@min":1,
    "@max":255
},
```

```

    "enableLiveDetAntiAttack": "true, false",
/*optional, boolean, whether to enable anti-attack for liveness detection*/
    "supportDelFPByID": "true, false",
/*ro, opt, boolean, whether the card reader supports deleting fingerprint by
fingerprint ID: "true"-yes, "false"-no*/
    "fingerPrintCapacity": {
/*ro, opt, integer, maximum number of fingerprints that can be added*/
        "@min": ,
        "@max": ,
    },
    "fingerPrintNum": {
/*ro, opt, integer, number of added fingerprints*/
        "@min": ,
        "@max": ,
    },
    "defaultVerifyMode": {
/*ro, opt, string, default authentication mode of the card reader (factory
defaults): "cardAndPw"-card+password, "card", "cardOrPw"-card or password, "fp"-fingerprint,
"fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card,
"fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password,
"faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face
+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face",
"employeeNoAndPw"-employee No.+password, "fpOrPw"-fingerprint or password,
"employeeNoAndFp"-employee No.+fingerprint, "employeeNoAndFpAndPw"-employee No.
+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card,
"faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee No.
+face, "faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face,
"cardOrfaceOrPw"-card or face or password, "cardOrFace"-card or face,
"cardOrFaceOrFp"-card or face or fingerprint*/
    },
    "@opt": "cardAndPw, card, cardOrPw, fp, fpAndPw, fpOrCard, fpAndCard, fpAndCardAndPw, fac
eOrFpOrCardOrPw, faceAndFp, faceAndPw, faceAndCard, face, employeeNoAndPw, fpOrPw, empl
oyeeNoAndFp, employeeNoAndFpAndPw, faceAndFpAndCard, faceAndPwAndFp, employeeNoAndFa
ce, faceOrfaceAndCard, fpOrface, cardOrfaceOrPw, cardOrFace, cardOrFaceOrFp"
},
    "faceRecognizeEnable": {
/*optional, integer, whether to enable facial recognition: 1-enable, 2-disable,
3-attendance checked in/out by recognition of multiple faces*/
        "@opt": "1, 2, 3"
},
    "FPAlgorithmVersion": {
/*optional, string, read-only, fingerprint algorithm library version*/
        "@min": ,
        "@max": ,
    },
    "cardReaderVersion": {
/*optional, string, read-only, card reader version*/
        "@min": ,
        "@max": ,
    }
    "enableReverseCardNo": "true, false",
/*optional, boolean, whether to enable reversing the card No.*/

```

```
"independSwipeIntervals": {  
/*optional, int, time interval of person authentication, unit: second. This  
time interval is calculated for each person separately and is different from  
swipeInterval*/  
    "@min": ,  
    "@max":  
},  
"maskFaceMatchThresholdN":{  
/*optional, int, 1:N face picture (face with mask and normal background)  
comparison threshold, value range: [0,100]*/  
    "@min": ,  
    "@max":  
},  
"maskFaceMatchThreshold1":{  
/*optional, int, 1:1 face picture (face with mask and normal background)  
comparison threshold, value range: [0,100]*/  
    "@min":0,  
    "@max":100  
}  
}  
}
```

JSON_Cap_CardReaderPlan

CardReaderPlan capability message in JSON format

```
{  
    "CardReaderPlan": {  
        "cardReaderNo": {  
/*authentication unit (card reader, fingerprint module, etc.) No.*/  
            "@min": 1,  
            "@max": 4  
        },  
        "templateNo": {  
/*required, integer, schedule template No.: 0-cancel linking the template to the  
schedule and restore to the default status (normal status)*/  
            "@min": 1,  
            "@max": 16  
        }  
    }  
}
```

JSON_Cap_ClearAntiSneak

ClearAntiSneak capability message in JSON format

```
{  
    "ClearAntiSneak": {  
        "clearAll": "true,false",  
    }  
}
```

```
/*required, boolean, whether to clear all anti-passing back records: "true"-yes, "false"-no. Clearing all anti-passing back records is not supported by access control devices version 2.1*/
    "EmployeeNoList" : {
/*optional, person ID list, this node is valid when clearAll is "false"*/
        "maxSize": ,
        "employeeNo": {
/*optional, string, employee No. (person ID)*/
            "@min": ,
            "@max":
        }
    }
}
```

JSON_Cap_ClearAntiSneakCfg

ClearAntiSneakCfg capability message in JSON format

```
{
    "ClearAntiSneakCfg": {
        "ClearFlags": {
            "antiSneak": "true,false"
/*required, boolean, whether to clear the anti-passing back parameter*/
        }
    }
}
```

JSON_Cap_ClearEventCardLinkageCfg

ClearEventCardLinkageCfg capability message in JSON format

```
{
    "ClearEventCardLinkageCfg": {
        "ClearFlags": {
            "eventCardLinkage": "true,false"
/*required, boolean, whether to clear event and card linkage parameters: "true"-yes, "false"-no*/
        }
    }
}
```

JSON_Cap_ClearGroupCfg

ClearGroupCfg capability message in JSON format

```
{  
    "ClearGroupCfg": {  
        "ClearFlags": {  
            "groupCfg": "true, false"  
        /*required, boolean, group parameters*/  
        }  
    }  
}
```

JSON_Cap_ClearPlansCfg

ClearPlansCfg capability message in JSON format

```
{  
    "ClearPlansCfg": {  
        "ClearFlags": {  
            "doorStatusWeekPlan": "true, false",  
        /*optional, boolean, whether to clear the week schedule of the door control*/  
            "cardReaderWeekPlan": "true, false",  
        /*optional, boolean, whether to clear the week schedule of the card reader  
        authentication mode control*/  
            "userRightWeekPlan": "true, false",  
        /*optional, boolean, whether to clear the week schedule of the access  
        permission control*/  
            "doorStatusHolidayPlan": "true, false",  
        /*optional, boolean, whether to clear the holiday schedule of the door control*/  
            "cardReaderHolidayPlan": "true, false",  
        /*optional, boolean, whether to clear the holiday schedule of the card reader  
        authentication mode control*/  
            "userRightHolidayPlan": "true, false",  
        /*optional, boolean, whether to clear the holiday schedule of the access  
        permission control*/  
            "doorStatusHolidayGroup": "true, false",  
        /*optional, boolean, whether to clear the holiday group of the door control*/  
            "cardReaderHolidayGroup": "true, false",  
        /*optional, boolean, whether to clear the holiday group of the card reader  
        authentication mode control*/  
            "userRightHolidayGroup": "true, false",  
        /*optional, boolean, whether to clear the holiday group of the access  
        permission control*/  
            "doorStatusTemplate": "true, false",  
        /*optional, boolean, whether to clear the schedule template of the door  
        control*/  
            "cardReaderTemplate": "true, false",  
        /*optional, boolean, whether to clear the control schedule template of the card  
        reader authentication mode*/  
            "userRightTemplate": "true, false"  
        /*optional, boolean, whether to clear the schedule template of the access  
        permission control*/  
        }  
    }
```

```
    }
}
```

JSON_Cap_CustomAudioCfg

JSON message about the capability of configuring the custom audio

```
{
    "customAudioType": {
        /*required, object, type of the custom audio file: "callCenter" (calling the center), "centerBusy" (the line is busy), "centerRefused" (the call is declined), "centerOverTime" (unanswered), "swipeCard" (please swipe the card), "thanks", "callAgain" (try again later), "verifyFailed" (authentication failed), "verifySuccess" (authentication succeeded), "doorOpened" (the door is opened), "wearSafetyHelmet" (please wear a hard hat), "wearMask" (please wear a mask), "abnormalTemperature" (the skin-surface temperature is abnormal)*/
        "@opt": ["callCenter", "centerBusy", "centerRefused", "centerOverTime",
            "swipeCard", "thanks", "callAgain", "verifyFailed", "verifySuccess",
            "doorOpened", "wearSafetyHelmet", "wearMask", "abnormalTemperature"]
    },
    "filePathType": {
        /*required, object, file path type: "simpleStorage" (simple storage), "URL",
        "localPath" (local storage), "binary"*/
        "@opt": ["simpleStorage", "URL", "localPath", "binary"]
    },
    "customAudioURL": {
        /*optional, object, URL of the custom audio file. This node is valid when the value of the node filePathType is "URL"*/
        "@min": 1,
        "@max": 256
    },
    "customAudioFormat": {
        /*optional, object, format of the custom audio file: "wav"*/
        "@opt": ["wav"]
    },
    "customAudioSize": {
        /*optional, object, size of the custom audio file, unit: KB*/
        "@min": 0,
        "@max": 512
    },
    "customAudioSearchType": {
        /*optional, object, status searching type of the custom audio file*/
        "@size": 13,
        /*optional, int, the maximum number of searching types. The value of this node will increase with the increasing of the custom audio file types*/
        "@opt": ["all", "callCenter", "centerBusy", "centerRefused",
            "centerOverTime", "swipeCard", "thanks", "callAgain", "verifyFailed",
            "verifySuccess", "doorOpened", "wearSafetyHelmet", "wearMask",
            "abnormalTemperature"]
        /*optional, array of string, options: "all" (searching for all types),
        "callCenter" (calling the center), "centerBusy" (the line is busy),
        "centerRefused" (the call is declined), "centerOverTime" (unanswered),
        "swipeCard" (please swipe the card), "thanks" (thank you), "callAgain" (try again later),
        "verifyFailed" (authentication failed), "verifySuccess" (authentication succeeded),
        "doorOpened" (the door is opened), "wearSafetyHelmet" (please wear a hard hat),
        "wearMask" (please wear a mask), "abnormalTemperature" (the skin-surface temperature is abnormal)*/
```

```
"centerRefused" (the call is declined), "centerOverTime" (unanswered),
"swipeCard" (please swipe the card), "thanks", "callAgain" (try again later),
"verifyFailed" (authentication failed), "verifySuccess" (authentication
succeeded), "doorOpened" (the door is opened), "wearSafetyHelmet" (please wear
a hard hat), "wearMask" (please wear a mask), "abnormalTemperature" (the skin-
surface temperature is abnormal) */
    }
}
```

JSON_Cap_DoorStatusHolidayGroupCfg

DoorStatusHolidayGroupCfg capability message in JSON format

```
{
  "DoorStatusHolidayGroupCfg": {
    "groupNo": {
      /*holiday group No.*/
      "@min": 1,
      "@max": 16
    },
    "enable": "true,false",
    /*whether to enable: "true"-enable, "false"-disable*/
    "groupName": {
      /*holiday group name*/
      "@min": 1,
      "@max": 32
    },
    "holidayPlanNo" : {
      /*holiday group schedule No.*/
      "@min": 1,
      "@max": 16
    }
  }
}
```

JSON_Cap_DoorStatusHolidayPlanCfg

DoorStatusHolidayPlanCfg capability message in JSON format

```
{
  "DoorStatusHolidayPlanCfg": {
    "planNo": {
      /*holiday schedule No.*/
      "@min": 1,
      "@max": 16
    },
    "enable": "true,false",
    /*whether to enable: "true"-enable, "false"-disable*/
    "beginDate": ""
  }
}
```

```

/*start date of the holiday*/
    "endDate": "",
/*end date of the holiday*/
    "HolidayPlanCfg" : {
/*holiday schedule parameters*/
        "maxSize": 8,
        "id": {
/*time period No.*/
            "@min": 1,
            "@max": 8
        },
        "enable": "true,false",
/*whether to enable: "true"-enable, "false"-disable*/
        "doorStatus": {
/*door status: "remainOpen"-remain open (access without authentication),
"remainClosed"-remain closed (access is not allowed), "normal"-access by
authentication, "sleep", "invalid"*/
            "@opt": "remainOpen,remainClosed,normal,sleep,invalid"
        },
        "TimeSegment": {
            "beginTime": ""
/*start time of the time period (device local time)*/
            "endTime": "",
/*end time of the time period (device local time)*/
            "validUnit":
/*time accuracy: "hour", "minute", "second". If this node is not returned, it
indicates that the time accuracy is "minute"*/
            }
        }
    }
}

```

JSON_Cap_DoorStatusPlan

DoorStatusPlan capability message in JSON format

```

{
    "DoorStatusPlan": {
        "doorNo": {
/*door No.*/
            "@min": 1,
            "@max": 4
        },
        "templateNo": {
/*required, integer, schedule template No.: 0-cancel linking the template with
the schedule and restore to the default status (normal status)*/
            "@min": 1,
            "@max": 16
        }
    }
}

```

```
    }
}
```

JSON_Cap_DoorStatusPlanTemplate

DoorStatusPlanTemplate capability message in JSON format

```
{
  "DoorStatusPlanTemplate": {
    "templateNo": {
      /*schedule template No.*/
      "@min": 1,
      "@max": 16
    },
    "enable": "true,false",
    /*required, boolean, whether to enable: "true"-enable, "false"-disable*/
    "templateName": {
      /*required, string, template name*/
      "@min": 1,
      "@max": 32
    },
    "weekPlanNo": {
      /*required, integer, week schedule No.*/
      "@min": 1,
      "@max": 16
    },
    "holidayGroupNo": {
      /*required, integer, holiday group No.*/
      "@min": 1,
      "@max": 16
    }
  }
}
```

JSON_Cap_DoorStatusWeekPlanCfg

DoorStatusWeekPlanCfg capability message in JSON format

```
{
  "DoorStatusWeekPlanCfg": {
    "planNo": {
      /*week schedule No.*/
      "@min": 1,
      "@max": 16
    },
    "enable": "true,false",
    /*whether to enable: "true"-enable, "false"-disable*/
    "WeekPlanCfg": {
      /*week schedule parameters*/
    }
  }
}
```

```

    "maxSize":56,
    "week":{
        "@opt":"Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday"
    },
    "id":{
        "@min":1,
        "@max":8
    },
    "enable":"true,false",
/*whether to enable: "true"-enable, "false"-disable*/
    "doorStatus":{
/*door status: "remainOpen"-remain open (access without authentication),
"remainClosed"-remain closed (access is not allowed), "normal"-access by
authentication, "sleep", "invalid"*/
        "@opt":"remainOpen,remainClosed,normal,sleep,invalid"
    },
    "TimeSegment":{
        "beginTime":"",
/*start time of the time period (device local time)*/
        "endTime":"",
/*end time of the time period (device local time)*/
        "validUnit":
/*time accuracy: "hour", "minute", "second". If this node is not returned, it
indicates that the time accuracy is "minute"*/
    }
}
}
}

```

JSON_Cap_EventCardLinkageCfg

EventCardLinkageCfg capability message in JSON format

```

{
    "EventCardLinkageCfg":{
        "eventID":{
/*optional, integer, event ID*/
            "@min": ,
            "@max":
        },
        "proMode":{
/*required, string, linkage type: "event"-event linkage, "card"-card linkage,
"mac"-MAC address linkage, "employee"-employee No. (person ID)*/
            "@opt": "event,card,mac,employee"
        },
        "EventLinkageInfo":{
/*optional, event linkage parameters, it is valid when proMode is "event"*/
            "mainEventType":{
/*optional, integer, major event type: 0-device event, 1-alarm input event, 2-
access control point event, 3-authentication unit (card reader, fingerprint
module) event*/

```

```

        "@opt": "0,1,2,3"
    },
    "devSubEventType":{
/*optional, integer, minor type of device event, refer to Event Linkage Types
for details*/
        "@opt": "0,1,2,3..."
    },
    "alarmSubEventType": {
/*optional, integer, minor type of alarm input event, refer to Event Linkage
Types for details*/
        "@opt": "0,1,2,3..."
    },
    "doorSubEventType": {
/*optional, integer, minor type of access control point event, refer to Event
Linkage Types for details*/
        "@opt": "0,1,2,3..."
    },
    "cardReaderSubEventType":{
/*optional, integer, minor type of authentication unit event, refer to Event
Linkage Types for details*/
        "@opt": "0,1,2,3..."
    }
},
"CardNoLinkageInfo":{
/*optional, card linkage parameters, it is valid when proMode is "card"*/
    "cardNo":{
/*optional, string, card No.*/
        "@min": ,
        "@max":
    }
},
"MacAddrLinkageInfo":{
/*optional, MAC address linkage parameters, it is valid when proMode is "mac"*/
    "MACAddr":{
/*optional, string, physical MAC address*/
        "@min": ,
        "@max":
    }
},
"EmployeeInfo":{
/*optional, employee No. (person ID) linkage parameters, it is valid when
proMode is "employee"*/
    "employeeNo":{
/*optional, string, employee ID (person ID)*/
        "@min": ,
        "@max":
    }
},
"eventSourceID":{
/*optional, integer, event source ID, it is valid when proMode is "event",
65535-all. For device event (mainEventType is 0), this field is invalid; for
access control point event (mainEventType is 2), this field refers to the
*/
}
}

```

```

access control point No.; for authentication unit event (mainEventType is 3,
this field refers to the authentication unit No.; for alarm input event
(mainEventType is 1), this field refers to the zone alarm input ID or the event
alarm input ID*/
    "@min": ,
    "@max": ,
},
"alarmout":{
/*optional, array, linked alarm output No.*/
    "@min": ,
    "@max": ,
},
"openDoor":{
/*optional, array, linked door No. to open*/
    "@min": ,
    "@max": ,
},
"closeDoor":{
/*optional, array, linked door No. to close*/
    "@min": ,
    "@max": ,
},
"alwaysOpen":{
/*optional, array, linked door No. to remain unlocked*/
    "@min": ,
    "@max": ,
},
"alwaysClose":{
/*optional, array, linked door No. to remain locked*/
    "@min": ,
    "@max": ,
},
"mainDevBuzzer": "true,false",
/*optional, boolean, whether to enable buzzer linkage of the access controller
(start buzzing): "false"-no, "true"-yes*/
    "capturePic": "true,false",
/*optional, boolean, whether to enable capture linkage: "false"-no, "true"-yes*/
    "recordVideo": "true,false",
/*optional, boolean, whether to enable recording linkage: "false"-no, "true"-yes*/
    "mainDevStopBuzzer": "true,false",
/*optional, boolean, whether to enable buzzer linkage of the access controller
(stop buzzing): "false"-no, "true"-yes*/
    "audioDisplayID": {
/*optional, integer, linked audio announcement ID, which is between 1 and 32: 0-
not link*/
        "@min": ,
        "@max": ,
},
"audioDisplayMode": {
/*optional, integer, linked audio announcement mode: "close", "single", "loop"*/
    "@min": "close,single,loop"
}

```

```
},
  "readerBuzzer": {
/*optional, array, linked buzzer No.*/
    "@min": ,
    "@max": ,
  },
  "alarmOutClose": {
/*optional, array, linked alarm output No.*/
    "@min": ,
    "@max": ,
  },
  "alarmInSetup": {
/*optional, array, linked zone No. to arm*/
    "@min": ,
    "@max": ,
  },
  "alarmInClose": {
/*optional, array, linked zone No. to disarm*/
    "@min": ,
    "@max": ,
  },
  "readerStopBuzzer": {
/*optional, array, linked buzzer No. to stop buzzing*/
    "@min": ,
    "@max": ,
  },
  "purePwdVerifyEnable": ,
/*optional, boolean, whether the device supports opening the door only by password: true-yes, this node is not returned-no. The password used to open the door is the value of the node password in the message JSON_UserInfo.*/
/*For opening the door only by password: 1. The password in "XXX or password" in the authentication mode refers to the person's password (the value of the node password in JSON_UserInfo); 2. The device will not check the duplication of the password, and the upper platform should ensure that the password is unique; 3. The password cannot be added, deleted, edited, or searched for on the device locally.*/
  }
}
```

See Also

[Event Linkage Types](#)

JSON_Cap_EventCardNoList

EventCardNoList capability message in JSON format

```
{
  "EventCardNoList":{
    "id":{
/*optional, range of event ID that can be configured*/
  }}
```

```
    "@min": ,
    "@max":
}
}
}
```

JSON_Cap_EventOptimizationCfg

EventOptimizationCfg capability message in JSON format

```
{
  "EventOptimizationCfg": {
    "enable": "true, false",
    /*optional, boolean, whether to enable event optimization: "true"-yes
    (default), "false"-no*/
    "isCombinedLinkageEvents": "true, false"
    /*optional, boolean, whether to enable linked event combination: "true"-yes
    (default), "false"-no*/
  }
}
```

JSON_Cap_FaceRecognizeMode

FaceRecognizeMode capability message in JSON format

```
{
  "FaceRecognizeMode": {
    "mode": {
      /*optional, string type, facial recognition mode: "normalMode"-normal mode,
      "deepMode"-deep mode*/
      "@opt": "normalMode, deepMode"
    }
  }
}
```

JSON_Cap_FingerPrintCfg

FingerPrintCfg capability message in JSON format

```
{
  "FingerPrintCfg": {
    "searchID": {
      /*required, string type, search ID*/
      "@min": 1,
      "@max": 36
    },
    "employeeNo": {

```

```
/*required, string, employee No. (person ID) linked with the fingerprint*/
    "@min": ,
    "@max": ,
},
"enableCardReader":{
/*required, array, fingerprint module to apply fingerprint data to*/
    "@min": ,
    "@max": ,
},
"fingerPrintID":{
/*required, integer, fingerprint No., which is between 1 and 10*/
    "@min":1,
    "@max":10
},
"fingerType":{
/*required, string, fingerprint type: "normalFP"-normal fingerprint, "hijackFP"-duress fingerprint, "patrolFP"-patrol fingerprint, "superFP"-super fingerprint, "dismissingFP"-dismiss fingerprint*/
    "@opt":"normalFP,hijackFP,patrolFP,superFP,dismissingFP"
},
"leaderFP":{
/*optional, array, whether to support first time authentication function*/
    "@min":1,
    "@max":32
},
"checkEmployeeNo":"true,false",
/*optional, boolean, whether to judge the existence of the employee No. (person ID): "false"-no, "true"-yes. If this node is not configured, the device will judge the existence of the employee No. (person ID) by default. If this node is set to "false", the device will not judge the existence of the employee No. (person ID) to speed up data applying; if this node is set to "true" or NULL, the device will judge the existence of the employee No. (person ID), and it is recommended to set this node to "true" or NULL if there is no need to speed up data applying*/
    "callbackMode":"allRetrun,partReturn",
/*optional, string, device callback mode: "allRetrun"-return when applying to all fingerprint modules completed (blocking); "partReturn"-return when applying to a part of fingerprint modules completed (unblocking). If this node is set to NULL, blocking mode will be adopted*/
/*when blocking mode is adopted, the totalStatus must be 1 after FingerPrintStatus is returned, which indicates that the fingerprint information is applied; when unblocking mode is adopted, if the totalStatus is 0 after FingerPrintStatus is returned, you should repeatedly call the URI /ISAPI/AccessControl/FingerPrintProgress?format=json to get the applying progress (which is also returned in FingerPrintStatus) until totalStatus equals to 1 (the fingerprint information is applied)*/
    "StatusList":{
/*optional, status list*/
        "id":{
/*optional, integer, fingerprint module No.*/
            "@min": ,
            "@max": ,
        }
    }
}
```

```

    },
    "cardReaderRecvStatus":{
/*optional, integer, fingerprint module status: 0-connecting failed, 1-
connected, 2-the fingerprint module is offline, 3-the fingerprint quality is
poor, try again, 4-the memory is full, 5-the fingerprint already exists, 6-the
fingerprint ID already exists, 7-invalid fingerprint ID, 8-this fingerprint
module is already configured, 10-the fingerprint module version is too old to
support the employee No.*/
        "@opt": "0,1,2,3,4,5,6,7,8,10"
    },
    "errorMsg":{
/*optional, string, error information*/
        "@min": ,
        "@max":
    }
},
    "totalStatus":{
/*required, integer, applying status: 0-applying, 1-applied*/
        "@opt":"0,1"
},
    "isSupportFingerCover":true,
/*whether to support overwriting the original fingerprint when applying new
fingerprint linked with the same person ID or employee No. If it is supported,
this node will be set to "true"; otherwise, this node will not be returned*/
    "isSupportSetUp":true
/*whether to support setting fingerprint parameters. If it is supported, this
node will be set to "true"; otherwise, this node will not be returned*/
}
}

```

JSON_Cap_FingerPrintDelete

FingerPrintDelete capability message in JSON format

```

{
    "FingerPrintDelete":{
        "mode":{
/*required, string, deleting mode: "byEmployeeNo"-delete by employee No.
(person ID), "byCardReader"-delete by fingerprint module*/
            "@opt":"byEmployeeNo,byCardReader"
        },
        "EmployeeNoDetail":{
/*optional, delete by employee No. (person ID), this node is valid when mode is
"byEmployeeNo"*/
            "employeeNo":{
/*optional, string, employee No. (person ID) linked with the fingerprint*/
                "@min": ,
                "@max":
            },
            "enableCardReader":{
/*optional, array, fingerprint module whose fingerprints should be deleted*/

```

```

        "@min": ,
        "@max": ,
    },
    "fingerPrintID":{
/*optional, array, No. of fingerprint to be deleted*/
        "@min": ,
        "@max": ,
    },
    "CardReaderDetail":{
/*optional, delete by fingerprint module, this node is valid when mode is
"byCardReader"*/
        "cardReaderNo":{
/*optional, integer, fingerprint module No.*/
            "@min": ,
            "@max": ,
        },
        "clearAllCard":"true,false",
/*optional, boolean, whether to delete the fingerprint information of all
cards: "false"-no (delete by employee No.), "true"-yes (delete the fingerprint
information of all employee No.)*/
        "employeeNo":{
/*optional, string, employee No. (person ID) linked with the fingerprint, this
node is valid when clearAllCard is "false"*/
            "@min": ,
            "@max": ,
        }
    }
}
}

```

JSON_Cap_GroupCfg

GroupCfg capability message in JSON format

```

{
    "GroupCfg":{
        "groupNo":{
/*optional, integer, group No.*/
            "@min": ,
            "@max": ,
        },
        "enable":"true,false",
/*required, boolean, whether to enable the group*/
        "ValidPeriodCfg":{
/*required, effective period parameters of the group*/
            "enable":"true,false",
/*required, boolean, whether to enable the effective period: "true"-yes,
>false"-no. If the effective period is not enabled, it indicates that the group
is permanently valid*/
            "beginTime":{

```

```
/*required, start time of the effective period (UTC time)*/
    "@min":1,
    "@max":32
},
"endTime":{
/*required, end time of the effective period (UTC time)*/
    "@min":1,
    "@max":32
}
},
"groupName":{
/*optional, string, group name*/
    "@min":1,
    "@max":32
}
}
```

JSON_Cap_HealthCodeCfg

JSON message about the configuration capability of the health code

```
{
  "enabled":{
/*required, object, whether to enable: true, false*/
    "@opt":[true, false]
},
  "serverAddress":{
/*optional, object, address of the health code server. The value is a string,
which means that configuring IP address and port No. separately is not
supported*/
    "@min":1,
    "@max":128
}
}
```

JSON_Cap_HealthCodeDisplayCfg

JSON message about the configuration capability of health code display

```
{
  "showHealthCode":{
/*required, object, whether to display the health code information: true,
false*/
    "@opt":[true, false]
}
}
```

JSON_Cap_LogModeCfg

LogModeCfg capability message in JSON format

```
{  
    "LogModeCfg":{  
        "type":{  
            /*optional, integer, log mode: 1-16 bytes (the host log can be stored by 25w,  
            and the employee No. can be stored by 16 bytes), 2-12 bytes (the host log can  
            be stored by 25w, and the employee No. can be stored by 12 bytes). This node  
            will be set to 1 by default*/  
            "@opt":"1,2"  
        }  
    }  
}
```

JSON_Cap_LOGOCfg

JSON message about the capability of configuring logo parameters

```
{  
    "fileSize":{  
        /*optional, object, size of the logo picture file, unit: KB*/  
        "@min":0,  
        /*optional, int, the minimum value*/  
        "@max":100  
        /*optional, int, the maximum value*/  
    },  
    "isSupportImportLOGO":true,  
    /*optional, boolean, whether it supports importing the logo*/  
    "isSupportDeleteLOGO":true  
    /*optional, boolean, whether it supports deleting the logo*/  
}
```

JSON_Cap_MultiCardCfg

MultiCardCfg capability message in JSON format

```
{  
    "MultiCardCfg":{  
        "doorNo":{  
            /*optional, integer, door No.*/  
            "@min": ,  
            "@max":  
        },  
        "enable":"true,false",  
        /*required, boolean, whether to enable multi-factor authentication*/  
        "swipeIntervalTimeout":{  
    }
```

```
/*optional, integer, timeout of swiping (authentication) interval, which is
between 1 and 255, and the default value is 10, unit: second*/
    "@min":1,
    "@max":255
},
"GroupCfg":{
/*optional, multi-factor authentication parameters*/
    "maxSize":20,
    "id":{
/*optional, integer, multi-factor authentication No., which is between 1 and
20*/
        "@min":1,
        "@max":20
    },
    "enable":"true,false",
/*optional, boolean, whether to enable the multi-factor authentication*/
    "enableOfflineVerifyMode":"true,false",
/*optional, boolean, whether to enable verification mode when the access
control device is offline (the super password will replace opening door
remotely)*/
    "templateNo":{
/*optional, integer, schedule template No. to enable the multi-factor
authentication*/
        "@min":1,
        "@max":20
    },
    "GroupCombination":{
/*optional, parameters of the multi-factor authentication group*/
        "maxSize":8,
        "enable":"true,false",
/*optional, integer, whether to enable the multi-factor authentication group*/
        "memberNum":{
/*optional, integer, number of members swiping cards*/
            "@min":1,
            "@max":20
        },
        "sequenceNo":{
/*optional, integer, serial No. of swiping cards of the multi-factor
authentication group, which is between 1 and 8*/
            "@min":1,
            "@max":8
        },
        "groupNo":{
/*optional, integer, group No., 65534-super password, 65535-remotely open door.
65534 and 65535 do not need to be returned by the device capability. If the
device returns groupNo node, it indicates that the device supports 65534 and
65535*/
            "@min":1,
            "@max":20
        }
    }
}
```

```
    }
}
```

JSON_Cap_MultiDoorInterLockCfg

MultiDoorInterLockCfg capability message in JSON format

```
{
    "MultiDoorInterLockCfg": {
        "enable": "true, false",
        /*required, boolean, whether to enable multi-door interlocking: "true"-yes,
        "false"-no*/
        "MultiDoorGroup": {
            /*optional, parameters of the multi-door interlocking group*/
            "maxSize": 8,
            "id": {
                /*optional, integer, multi-door interlocking No., which is between 1 and 8*/
                "@min": 1,
                "@max": 8
            },
            "doorNoList": {
                /*optional, array, door No. list of multi-door interlocking (range of each door
                No. in the list), which is between 1 and 8*/
                "@min": 1,
                "@max": 8
            },
            "doorNoListLen": {
                /*optional, range of the list length of multi-door interlocking, e.g., the list
                length of [1,3,5] is 3*/
                "@min": 1,
                "@max": 8
            }
        }
    }
}
```

JSON_Cap OSDPModify

OSDPModify capability message in JSON format

```
{
    "OSDPModify": {
        "id": {
            /*required, integer, range of the original OSDP card reader ID*/
            "@min": ,
            "@max":
        },
        "newID": {
            /*required, integer, new ID of the OSDP card reader*/
        }
    }
}
```

```
    "@min": ,
    "@max":
  }
}
}
```

JSON_Cap OSDPStatus

OSDPStatus capability message in JSON format

```
{
  "OSDPStatus": {
    "id": {
      /*required, integer, range of the OSDP card reader ID*/
      "@min": ,
      "@max":
    },
    "status": "online,offline"
    /*required, string, online status: "online", "offline"*/
  }
}
```

JSON_Cap PhoneDoorRightCfg

PhoneDoorRightCfg capability message in JSON format

```
{
  "PhoneDoorRightCfg": {
    "phoneNo": {
      /*optional, integer, No. of the mobile phone number allowlist*/
      "@min": ,
      "@max":
    },
    "openRight": {
      /*optional, array, whether to have permission to open the door*/
      "@min": ,
      "@max":
    },
    "closeRight": {
      /*optional, array, whether to have permission to close the door*/
      "@min": ,
      "@max":
    },
    "alwaysOpenRight": {
      /*optional, array, whether to have permission to remain the door unlocked*/
      "@min": ,
      "@max":
    },
    "alwaysCloseRight": {

```

```
/*optional, array, whether to have permission to remain the door locked*/
    "@min": ,
    "@max": ,
},
"armRight":{

/*optional, array, whether to have permission to arm the alarm input port*/
    "@min": ,
    "@max": ,
},
"disarmRight":{

/*optional, array, whether to have permission to disarm the alarm input port*/
    "@min": ,
    "@max": ,
}
}
```

JSON_Cap_PictureServerInformation

PictureServerInformation capability message in JSON format

```
{
  "PictureServerInformation":{

    "pictureServerType":{

      /*required, string type, picture storage server type: "tomact", "VRB",
      "cloudStorage"-cloud storage, "KMS"*/
        "@opt":"tomact,VRB,cloudStorage,KMS",
        "#text":""


    },
    "addressingFormatType":{

      /*required, string type, format type of the picture storage server address:
      "ipaddress"-IP address (default), "hostname"-host name*/
        "@opt":"ipaddress,hostname",
        "#text":""


    },
    "hostName":{

      /*string type, domain name of the picture storage server, the string length is
      between 0 and 64. This field is valid when addressingFormatType is "hostname"*/
        "@min":0,
        "@max":64,
        "#text":""


    },
    "ipv4Address":{

      /*string type, IPv4 address of the picture storage server, the string length is
      between 0 and 64. This field is valid when addressingFormatType is "ipaddress"*/
        "@min":0,
        "@max":64,
        "#text":""


    },
    "ipv6Address":{

      /*string type, IPv6 address of the picture storage server, the string length is
```

```
between 0 and 128. This field is valid when addressingFormatType is
"ipaddress"*/
    "@min":0,
    "@max":128,
    "#text":"""
},
"portNo":{
/*required, integer type, port No. of the picture storage server, which is
between 1024 and 65535*/
    "@min":1024,
    "@max":65535,
    "#text":
},
"underlyingProtocol":{
/*optional, string, bottom-level protocol of the picture storage server:
"HTTP", "HTTPS". This field is valid when pictureServerType contains
"cloudStorage"*/
    "@opt":["http","https"]
},
"cloudStorage":{
/*parameters of the cloud storage server, which is valid when
pictureServerType is "cloudStorage"*/
    "cloudManageHttpPort":{
/*required, integer type, HTTP port No. for central management of the cloud
storage server, which is between 1024 and 65535*/
        "@min":1024,
        "@max":65535,
        "#text":
},
    "cloudTransDataPort":{
/*required, integer type, data transmission port No. of the cloud storage
server, which is between 1024 and 65535*/
        "@min":1024,
        "@max":65535,
        "#text":
},
    "cloudCmdPort":{
/*required, integer type, signaling port No. of the cloud storage server, which
is between 1024 and 65535*/
        "@min":1024,
        "@max":65535,
        "#text":
},
    "cloudHeartBeatPort":{
/*required, integer type, heartbeat port No. of the cloud storage server, which
is between 1024 and 65535*/
        "@min":1024,
        "@max":65535,
        "#text":
},
    "cloudStorageHttpPort":{
/*required, integer type, HTTP port No. of the cloud storage server, which is
```

```
between 1024 and 65535*/
    "@min":1024,
    "@max":65535,
    "#text":
},
"cloudUsername":{
/*required, string type, user name of the cloud storage server, the string
length is between 0 and 32*/
    "@min":0,
    "@max":32,
    "#text":""
},
"cloudPassword":{
/*required, string type, password of the cloud storage server, the string
length is between 0 and 32*/
    "@min":0,
    "@max":32,
    "#text":""
},
"cloudPoolId":{
/*required, integer type, cloud storage pool ID, which is between 1 and
4294967295. If this field is not configured by the upper-level, this field will
be set to 1 by default*/
    "@min":1,
    "@max":4294967295,
    "#text":
},
"cloudPoolIdEx":{
/*optional, string, cloud storage pool ID, this node is valid when cloud
storage pool ID of type string is supported*/
    "@min":0,
    "@max":0,
    "#text":""
},
"cloudProtocolVersion":{
/*required, string type, protocol version of the cloud storage server, the
string length is between 0 and 32*/
    "@min":0,
    "@max":32,
    "#text":""
},
"cloudAccessKey":{
/*string type, cloud storage server access_key, the string length is between 0
and 64. This field is valid when cloudProtocolVersion is "V2.0"*/
    "@min":0,
    "@max":64
},
"cloudSecretKey":{
/*string type, cloud storage server secret_key, the string length is between 0
and 64. This field is valid when cloudProtocolVersion is "V2.0"*/
    "@min":0,
    "@max":64
```

```
        }
    }
}
```

JSON_Cap_PrinterCfg

PrinterCfg capability message in JSON format

```
{
    "PrinterCfg": {
        "enable": {
            /*required, boolean, whether to enable the printer*/
            "@opt": "true, false"
        },
        "printFormat": {
            "vistorPic": {
                /*optional, visitor picture*/
                "enable": {
                    /*required, boolean, whether to print visitor picture*/
                    "@opt": "true, false"
                },
                "lineNo": {
                    /*required, integer, line No.*/
                    "@min": 1,
                    "@max": 255,
                }
            },
            "vistorName": {
                /*optional, visitor name*/
                "enable": {
                    /*required, boolean, whether to print visitor name*/
                    "@opt": "true, false"
                },
                "lineNo": {
                    /*required, integer, line No.*/
                    "@min": 1,
                    "@max": 255,
                }
            },
            "certificateNumber": {
                /*optional, visitor's certificate No.*/
                "enable": {
                    /*required, boolean, whether to print visitor's certificate No.*/
                    "@opt": "true, false"
                },
                "lineNo": {
                    /*required, integer, line No.*/
                    "@min": 1,
                    "@max": 255,
                }
            }
        }
    }
}
```

```
        },
        "address": {
/*optional, visitor's address*/
            "enable": {
/*required, boolean, whether to print visitor's address*/
                "@opt": "true, false"
            },
            "lineNo": {
/*required, integer, line No.*/
                "@min": 1,
                "@max": 255,
            }
        },
        "validity": {
/*optional, expiry date*/
            "enable": {
/*required, whether to print the expiry date*/
                "@opt": "true, false"
            },
            "lineNo": {
/*required, integer, line No.*/
                "@min": 1,
                "@max": 255,
            }
        },
        "receptionDepartment": {
/*optional, reception department*/
            "enable": {
/*required, boolean, whether to print the reception department*/
                "@opt": "true, false"
            },
            "lineNo": {
/*required, integer, line No.*/
                "@min": 1,
                "@max": 255,
            }
        },
        "receptionStaff": {
/*optional, receptionist information*/
            "enable": {
/*required, boolean, whether to print the receptionist information*/
                "@opt": "true, false"
            },
            "lineNo": {
/*required, integer, line No.*/
                "@min": 1,
                "@max": 255,
            }
        },
        "registrationTime": {
/*optional, registered time*/
            "enable": {
```

```
/*optional, whether to print the registered time*/
    "@opt":"true,false"
},
"lineNo":{

/*required, integer, line No.*/
    "@min": 1,
    "@max": 255,
}
},
}
}
```

JSON_Cap_RegionCalibrationCfg

JSON message about the calibration configuration capability of the temperature measurement area

```
{
    "enabled":{

/*required, object, whether to enable the calibration: true, false*/
        "@opt": [true, false]
},
    "FaceFrameCoordinate":{

/*optional, object, face frame coordinate, the value is normalized to a number between 0 and 1000*/
        "height":{

/*optional, object, height*/
            "@min":0,
            "@max":1000
},
        "width":{

/*optional, object, width*/
            "@min":0,
            "@max":1000
},
        "x":{

/*optional, object, X-coordinate*/
            "@min":0,
            "@max":1000
},
        "y":{

/*optional, object, Y-coordinate*/
            "@min":0,
            "@max":1000
}
}
}
```

JSON_Cap_RegionCoordinate

JSON message about the configuration capability of the temperature measurement area

```
{  
    "uniqueItems":{  
        /*required, object, range of the number of vertexes of the polygon, read-only*/  
        "@min":3,  
        "@max":10  
    },  
    "RegionCoordinate":{  
        /*optional, object, coordinate of the vertexes of the polygon, read-only*/  
        "x":{  
            /*optional, object, X-coordinate, read-only*/  
            "@min":0,  
            "@max":1000  
        },  
        "y":{  
            /*optional, object, Y-coordinate, read-only*/  
            "@min":0,  
            "@max":1000  
        }  
    }  
}
```

JSON_Cap_RemoteCheck

Message about the capability of verifying the access control event remotely in JSON format.

```
{  
    "RemoteCheck":{  
        "serialNo":{  
            /*required, int, event serial No. which should be the same as that in the event  
information message for uploading*/  
            "@min":1,  
            "@max":2000000000  
        },  
        "checkResult":{  
            /*required, string, verification result: "success"-verified, "failed"-  
verification failed*/  
            "@opt":["success", "failed"]  
        },  
        "info":{  
            /*optional, string, additional information*/  
            "@min":1,  
            "@max":  
        }  
    }  
}
```

JSON_Cap_RemoteControlBuzzer

RemoteControlBuzzer capability message in JSON format

```
{  
    "RemoteControlBuzzer":{  
        "cardReaderNo":{  
            /*optional, integer, card reader No. (buzzer No.)*/  
            "@min": ,  
            "@max":  
        },  
        "cmd":{  
            /*required, string, command: "start"-start buzzing, "stop"-stop buzzing*/  
            "@opt":"start,stop"  
        }  
    }  
}
```

JSON_Cap_RemoteControlPWCfg

RemoteControlPWCfg capability message in JSON format

```
{  
    "RemoteControlPWCfg":{  
        "password":{  
            /*optional, string type, password for remote door control. The password must  
            contain 6 digits and it ranges from 000000 to 999999*/  
            "@min":000000,  
            "@max":999999  
        }  
    }  
}
```

JSON_Cap_RemoteControlPWCheck

RemoteControlPWCheck capability message in JSON format

```
{  
    "RemoteControlPWCfg":{  
        "password":{  
            /*optional, string type, password for remote door control (or EZVIZ  
            verification code). The password must contain 6 digits and it ranges from  
            000000 to 999999*/  
            "@min":000000,  
            "@max":999999  
        }  
    }  
}
```

```
    }
}
```

JSON_Cap_SmsRelativeParam

SmsRelativeParam capability message in JSON format

```
{
  "SmsRelativeParam": {
    "WhiteList": {
      /*required, mobile phone number allowlist*/
      "maxSize": 32,
      /*maximum number of mobile phone number allowlists*/
      "id": {
        /*required, integer, No. of mobile phone number allowlist*/
        "@min": ,
        "@max":
      },
      "phoneNo": {
        /*required, string, mobile phone number*/
        "@min": ,
        "@max":
      },
      "doorControl": "true, false",
      /*optional, boolean, whether to support door operation control: "true"-yes, "false"-no*/
      "acsPassword": {
        /*optional, string, command to open the door*/
        "@min": ,
        "@max":
      }
    }
  }
}
```

JSON_Cap_TemperatureMeasurementCfg

JSON message about the configuration capability of the temperature measurement parameters

```
{
  "showTemperatureInfo": {
    /*optional, object, whether to display the temperature information: true, false*/
    "@opt": [true, false]
  },
  "saveThermalPicture": {
    /*optional, object, whether to save the thermal picture: true, false*/
    "@opt": [true, false]
  },
}
```

```
"uploadThermalPicture":{  
/*optional, object, whether to upload the thermal picture: true, false*/  
    "@opt": [true, false]  
,  
    "lowTemperatureEnabled":{  
/*optional, boolean, whether to enable temperature measurement in the low-  
temperature environment: true, false. When this function is enabled, if the  
face temperature is lower than 36 °C, the measured temperature will be mapped  
to that higher than 36 °C; temperatures higher than 36 °C will not be mapped*/  
    "@opt": [true, false]  
}  
}
```

JSON_Cap_UserInfo

UserInfo capability message in JSON format

```
{  
    "UserInfo":{  
        "supportFunction":{  
/*required, supported function of adding, deleting, editing, searching for  
person information, and getting total number of the added persons: "post"-add,  
"delete", "put"-edit, "get"-search, "setUp"-set*/  
            "@opt": "post,delete,put,get,setUp"  
,  
            "UserInfoSearchCond":{  
/*optional, search conditions*/  
                "searchID":{  
/*required, string type, search ID, which is used to check the upper-level  
platform or system. If the platform or the system is the same one during two  
searching, the search history will be saved in the memory to speed up next  
searching*/  
                    "@min":1,  
                    "@max":36  
,  
                    "maxResults":{  
/*required, integer32, maximum number of search results*/  
                        "@min":1,  
                        "@max":30  
,  
                        "EmployeeNoList":{  
/*optional, person ID list*/  
                            "maxSize":56,  
                            "employeeNo":{  
/*optional, string, employee No. (person ID)*/  
                                "@min": ,  
                                "@max":  
                            }  
,  
                            "fuzzySearch":{  
/*optional, string, keywords for fuzzy search*/  
                    }
```

```

        "@min": ,
        "@max":
    },
    "isSupportNumOfFace":0,
/*optional, integer, whether it supports number of linked face pictures when
searching. If this field is not returned, it indicates that this function is
not supported*/
    "isSupportNumOfFP":0,
/*optional, integer, whether it supports number of linked fingerprints when
searching. If this field is not returned, it indicates that this function is
not supported*/
    "isSupportNumOfCard":0,
/*optional, integer, whether it supports number of linked cards when searching.
If this field is not returned, it indicates that this function is not
supported*/
    "groupIdList":{
/*optional, object, range of the department No. of local time and attendance*/
        "@size":1,
/*required, int, the maximum number of lists supported by the device*/
        "@min":1,
/*required, int, the minimum value among elements of the array*/
        "@max":1
/*required, int, the maximum value among elements of the array*/
    },
    "arrangeType":{
/*optional, object, shift schedule type: "" (shift schedule by individual).
Currently only the shift schedule by individual is supported. If this node
exists, it indicates searching for all persons with shift schedule by
individual*/
        "@opt":["personal"]
    }
},
    "UserInfoDelCond":{
/*optional, deleting conditions*/
        "EmployeeNoList":{
/*optional, person ID list (if this node does not exist, it indicates deleting
all person information)*/
            "maxSize":56,
            "employeeNo":{
/*optional, string, employee No. (person ID)*/
                "@min": ,
                "@max":
            }
        }
},
    "employeeNo":{
/*required, string, employee No. (person ID)*/
        "@min": ,
        "@max":
    },
    "name":{
/*optional, string, name*/

```

```

        "@min":1,
        "@max":32
    },
    "userType":{
/*required, string, person type: "normal"-normal person (household), "visitor",
"blackList"-person in blocklist/
        "@opt":"normal,visitor,blackList"
    },
    "closeDelayEnabled":"true,false",
/*optional, boolean, whether to enable door close delay: "true"-yes, "false"-no*/
    "Valid":{
/*required, parameters of the effective period/
        "enable":"true, false",
/*required, boolean, whether to enable the effective period: "false"-disable,
"true"-enable. If this node is set to "false", the effective period is
permanent/
        "beginTime":{
/*required, start time of the effective period (if timeType does not exist or
is "local", the beginTime is the device local time, e.g.,: 2017-08-01T17:30:08;
if timeType is "UTC", the beginTime is UTC time, e.g.,:
2017-08-01T17:30:08+08:00)*/
            "@min":1,
            "@max":32
        },
        "endTime":{
/*required, end time of the effective period (if timeType does not exist or is
"local", the endTime is the device local time, e.g.,: 2017-08-01T17:30:08; if
timeType is "UTC", the endTime is UTC time, e.g.,: 2017-08-01T17:30:08+08:00)*/
            "@min":1,
            "@max":32
        },
        "timeRangeBegin":"",
/*optional, string, start time that can be configured for beginTime. If the
device does not return this node, the default start time that can be configured
for beginTime is "1970-01-01T00:00:00"*/
        "timeRangeEnd":"",
/*optional, string, end time that can be configured for endTime. If the device
does not return this node, the default end time that can be configured for
endTime is "2037-12-31T23:59:59"*/
        "timeType":{
/*optional, string, time type: "local"- device local time, "UTC"- UTC time*/
            "@opt":"local,UTC"
        }
    },
    "maxBelongGroup":4,
/*optional, integer, maximum number of groups that a person can belong to*/
    "belongGroup":{
/*optional, string, group*/
        "@min":1,
        "@max":32
    },

```

```
"password":{  
/*optional, string, password*/  
    "@min":1,  
    "@max":32  
},  
"doorRight":{  
/*optional, string, No. of door or lock that has access permission*/  
    "@min":1,  
    "@max":32  
},  
"RightPlan":{  
/*optional, door permission schedule (lock permission schedule)*/  
    "maxSize":32,  
    "doorNo":{  
/*optional, integer, door No. (lock ID)*/  
        "@min":1,  
        "@max":32  
    },  
    "maxPlanTemplate":4,  
/*optional, integer, maximum number of schedule templates that can be  
configured for one door*/  
    "planTemplateNo":{  
/*optional, string, schedule template No.*/  
        "@min":1,  
        "@max":32  
    }  
},  
"maxOpenDoorTime":{  
/*optional, integer, maximum authentication attempts, 0-unlimited*/  
    "@min":0,  
    "@max":100  
},  
"openDoorTime":{  
/*optional, integer, read-only, authenticated attempts*/  
    "@min":0,  
    "@max":100  
},  
"roomNumber":{  
/*optional, integer, room No.*/  
    "@min":0,  
    "@max":100  
},  
"floorNumber":{  
/*optional, integer, floor No.*/  
    "@min":0,  
    "@max":100  
},  
"doubleLockRight":"true, false",  
/*optional, boolean, whether to have the permission to open the double-locked  
door: "true"-yes, "false"-no*/  
    "localUIRight":"true, false",  
/*optional, boolean, whether to have the permission to access the device local
```

```

UI: "true"-yes, "false"-no*/
    "localUIUserType":{
/*optional, object, user type of device local UI: "admin" (administrator),
"operator", "viewer" (normal user). This node is used to distinguish different
users with different operation permissions of device local UI*/
        "@opt":["admin","operator","viewer"]
    },
    "userVerifyMode":{
/*optional, string, person authentication mode: "cardAndPw"-card+password,
"card"-card, "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-  

fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint  

+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or  

fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face  

+password, "faceAndCard"-face+card, "face"-face, "employeeNoAndPw"-employee No.  

+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.  

+fingerprint, "employeeNoAndFpAndPw"-employee No.+fingerprint+password,  

"faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password  

+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face  

or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or  

password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or  

fingerprint, "cardOrFpOrPw"-card or fingerprint or password. The priority of  

the person authentication mode is higher than that of the card reader  

authentication mode*/
    "@opt":"cardAndPw,card,cardOrPw,fp,fpAndPw,fpOrCard,fpAndCard,fpAndCardAndPw,fac  

eOrFpOrCardOrPw,faceAndFp,faceAndPw,faceAndCard,face,employeeNoAndPw,fpOrPw,empl  

oyeeNoAndFp,employeeNoAndFpAndPw,faceAndFpAndCard,faceAndPwAndFp,employeeNoAndFa  

ce,faceOrfaceAndCard,fpOrface,cardOrfaceOrPw,cardOrFace,cardOrFaceOrFp,cardOrFpO  

rPw"
    },
    "checkUser":"true, false",
/*optional, boolean, whether to verify the duplicated person information:  

"false"-no, "true"-yes. If checkUser is not configured, the device will verify  

the duplicated person information by default. When there is no person  

information, you can set checkUser to "false" to speed up data applying;  

otherwise, it is not recommended to configure this node*/
    "addUser": "true, false",
/*optional, boolean type, whether to add the person if the person information  

being edited does not exist: "false"-no (if the device has checked that the  

person information being edited does not exist, the failure response message  

will be returned along with the error code), "true"-yes (if the device has  

checked that the person information being edited does not exist, the success  

response message will be returned, and the person will be added). If this node  

is not configured, the person will not be added by default*/
    "maxRecordNum": ,
/*required, integer type, supported maximum number of records (person records)*/
    "callNumbers": {
/*optional, string type, room No. list to be called, which is extended from  

roomNumber and it is in higher priority; by default, the No. format is X-X-X-X,  

e.g., 1-1-1-401, and for standard SIP, it can be the SIP number; this node must  

be configured together with roomNumber*/
        "maxSize": ,

```

```

/*range of members in the array*/
    "@min": 0,
/*minimum string length*/
    "@max": 100
/*maximum string length*/
},
"floorNumbers": {
/*optional, integer type, floor No. list, which is extended from floorNumber
and it is in higher priority; this node must be configured together with
floorNumber*/
    "maxSize": ,
/*range of members in the array*/
    "@min": 0,
/*minimum floor No.*/
    "@max": 100
/*maximum floor No.*/
},
"gender":{
/*optional, string, gender of the person in the face picture: "male", "female",
"unknown"*/
    "@opt":"male,female,unknown"
},
"PersonInfoExtends": {
/*optional, object, extended fields for the additional person information*/
    "maxSize":3,
/*required, integer, supported maximum number of extension fields*/
    "id":{
/*optional, object, extended ID of the additional person information*/
        "@min": 1,
        "@max": 1
    },
    "value":{
/*optional, object, extended content of the additional person information*/
        "@min": 0,
        "@max": 100
    }
},
"purePwdVerifyEnable": ,
/*optional, boolean, whether the device supports opening the door only by
password: true-yes, this node is not returned-no. The password used to open the
door is the value of the node password in the message JSON_UserInfo.*/
/*For opening the door only by password: 1. The password in "XXX or password"
in the authentication mode refers to the person's password (the value of the
node password in JSON_UserInfo); 2. The device will not check the duplication
of the password, and the upper platform should ensure that the password is
unique; 3. The password cannot be added, deleted, edited, or searched for on
the device locally.*/
    "groupId":{
/*optional, object, department No. of local time and attendance*/
        "@min": 0,
        "@max": 0
    },
}

```

```
"localAtndPlanTemplateId":{  
/*optional, object, schedule template of local time and attendance. If this  
node exist, it indicates that there are shift schedule settings by individual*/  
    "@min": 0,  
    "@max": 0  
}  
}  
}
```

JSON_Cap_UserInfoDetail

UserInfoDetail capability message in JSON format

```
{  
    "UserInfoDetail":{  
        "mode":{  
            "@opt":"all,byEmployeeNo"  
/*required, string type, deleting mode: "all"-delete all, "byEmployeeNo"-delete  
by employee No. (person ID)*/  
        },  
        "EmployeeNoList":{  
/*optional, person ID list*/  
            "maxSize": ,  
            "employeeNo":{  
/*optional, string type, employee No. (person ID), it is valid when mode is  
"byEmployeeNo"*/  
                "@min": ,  
                "@max":  
            }  
        }  
    }  
}
```

JSON_Cap_UserRightHolidayGroupCfg

UserRightHolidayGroupCfg capability message in JSON format

```
{  
    "UserRightHolidayGroupCfg": {  
        "groupNo": {  
/*holiday group No.*/  
            "@min": 1,  
            "@max": 16  
        },  
        "enable": "true,false",  
/*whether to enable: "true"-enable, "false"-disable*/  
        "groupName": {  
/*holiday group name*/  
            "@min": 1,
```

```
    "@max": 32
  },
  "holidayPlanNo": {
/*holiday group schedule No.*/
    "@min": 1,
    "@max": 16
  }
}
```

JSON_Cap_UserRightHolidayPlanCfg

UserRightHolidayPlanCfg capability message in JSON format

```
{
  "UserRightHolidayPlanCfg": {
    "planNo": {
/*holiday schedule No.*/
      "@min": 1,
      "@max": 16
    },
    "enable": "true,false",
/*whether to enable: "true"-enable, "false"-disable*/
    "beginDate": "",
/*start date of the holiday (device local time)*/
    "endDate": "",
/*end date of the holiday (device local time)*/
    "HolidayPlanCfg": {
/*holiday schedule parameter*/
      "maxSize": 8,
      "id": {
/*time period No.*/
        "@min": 1,
        "@max": 8
      },
      "enable": "true,false",
/*whether to enable: "true"-enable, "false"-disable*/
      "TimeSegment": {
        "beginTime": "",
/*start time of the time period (device local time)*/
        "endTime": "",
/*end time of the time period (device local time)*/
        "validUnit": /*time accuracy: "hour", "minute", "second". If this node is not returned, it indicates that the time accuracy is "minute"*/
      }
    }
  }
}
```

JSON_Cap_UserRightPlanTemplate

UserRightPlanTemplate capability message in JSON format

```
{  
    "UserRightPlanTemplate": {  
        "templateNo": {  
/*schedule template No.*/  
            "@min": 1,  
            "@max": 16  
        },  
        "enable": "true,false",  
/*whether to enable: "true"-enable, "false"-disable*/  
        "templateName": {  
/*template name*/  
            "@min": 1,  
            "@max": 32  
        },  
        "weekPlanNo" : {  
/*week schedule No.*/  
            "@min": 1,  
            "@max": 16  
        },  
        "holidayGroupNo": {  
/*holiday group No.*/  
            "@min": 1,  
            "@max": 16  
        }  
    }  
}
```

JSON_Cap_UserRightWeekPlanCfg

UserRightWeekPlanCfg capability message in JSON format

```
{  
    "UserRightWeekPlanCfg":{  
        "planNo":{  
/*week schedule No.*/  
            "@min":1,  
            "@max":16  
        },  
        "enable":"true,false",  
/*whether to enable: "true"-enable, "false"-disable*/  
        "WeekPlanCfg":{  
/*week schedule parameter*/  
            "maxSize":56,  
            "week":{  
                "@opt":"Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday"  
            }  
        }  
    }  
}
```

```
        },
        "id": {
            "@min": 1,
            "@max": 8
        },
        "enable": "true, false",
/*whether to enable: "true"-enable, "false"-disable*/
        "TimeSegment": {
            "beginTime": "",
/*start time of the time period (device local time)*/
            "endTime": "",
/*end time of the time period (device local time)*/
            "validUnit": /*time accuracy: "hour", "minute", "second". If this node is not returned, it indicates that the time accuracy is "minute"*/
                }
        }
    }
}
```

JSON_Cap_VerifyHolidayGroupCfg

VerifyHolidayGroupCfg capability message in JSON format

```
{
    "VerifyHolidayGroupCfg": {
        "groupNo": {
/*holiday group No.*/
            "@min": 1,
            "@max": 16
        },
        "enable": "true, false",
/*whether to enable: "true"-enable, "false"-disable*/
        "groupName": {
/*holiday group name*/
            "@min": 1,
            "@max": 32
        },
        "holidayPlanNo": {
/*holiday group schedule No.*/
            "@min": 1,
            "@max": 16
        }
    }
}
```

JSON_Cap_VerifyHolidayPlanCfg

VerifyHolidayPlanCfg capability message in JSON format

```
{
    "VerifyHolidayPlanCfg": {
        "planNo": {
            /*holiday schedule template No.*/
            "@min": 1,
            "@max": 16
        },
        "enable": "true,false",
        /*whether to enable: "true"-enable, "false"-disable*/
        "beginDate": "",
        /*start date of the holiday (device local time)*/
        "endDate": "",
        /*end date of the holiday (device local time)*/
        "HolidayPlanCfg": {
            /*holiday schedule parameters*/
            "maxSize": 8,
            "id": {
                /*time period No.*/
                "@min": 1,
                "@max": 8
            },
            "enable": "true, false",
            /*whether to enable: "true"-enable, "false"-disable*/
            "verifyMode": {
                /*authentication mode: "cardAndPw"-card+password, "card", "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face", "employeeNoAndPw"-employee No.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint, "employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint, "cardOrFpOrPw"-card or fingerprint or password, "sleep", "invalid"*/
                "@opt":
                "cardAndPw,card,cardOrPw,fp,fpAndPw,fpOrCard,fpAndCard,fpAndCardAndPw,faceOrFpOrCardOrPw,faceAndFp,faceAndPw,faceAndCard,face,employeeNoAndPw,fpOrPw,employeeNoAndFp,employeeNoAndFpAndPw,faceAndFpAndCard,faceAndPwAndFp,employeeNoAndFace,faceOrfaceAndCard,fpOrface,cardOrfaceOrPw,cardOrFace,cardOrFaceOrFp,cardOrFpOrPw,sleep,invalid"
            },
            "TimeSegment": {
                "beginTime": ""
            }
        }
        /*start time of the time period (device local time)*/
    }
}
```

```
        "endTime": "",  
        /*end time of the time period (device local time)  
         "validUnit":  
        /*time accuracy: "hour", "minute", "second". If this node is not returned, it  
        indicates that the time accuracy is "minute"*/  
        }  
    },  
    "purePwdVerifyEnable":  
    /*optional, boolean, whether the device supports opening the door only by  
    password: true-yes, this node is not returned-no. The password used to open the  
    door is the value of the node password in the message JSON_UserInfo.*/  
    /*For opening the door only by password: 1. The password in "XXX or password"  
    in the authentication mode refers to the person's password (the value of the  
    node password in JSON_UserInfo); 2. The device will not check the duplication  
    of the password, and the upper platform should ensure that the password is  
    unique; 3. The password cannot be added, deleted, edited, or searched for on  
    the device locally.*/  
    }  
}
```

JSON_Cap_VerifyPlanTemplate

VerifyPlanTemplate capability message in JSON format

```
{  
    "VerifyPlanTemplate": {  
        "templateNo": {  
            /*schedule template No.*/  
            "@min": 1,  
            "@max": 16  
        },  
        "enable": "true,false",  
        /*whether to enable: "true"-enable, "false"-disable*/  
        "templateName": {  
            /*template name*/  
            "@min": 1,  
            "@max": 32  
        },  
        "weekPlanNo": {  
            /*week schedule No.*/  
            "@min": 1,  
            "@max": 16  
        },  
        "holidayGroupNo": {  
            /*holiday group No.*/  
            "@min": 1,  
            "@max": 16  
        }  
    }  
}
```

JSON_Cap_VerifyWeekPlanCfg

VerifyWeekPlanCfg capability message in JSON format

```
{
    "VerifyWeekPlanCfg": {
        "planNo": {
            /*week schedule No.*/
            "@min": 1,
            "@max": 16
        },
        "enable": "",
        /*whether to enable: "true"-enable, "false"-disable*/
        "WeekPlanCfg": {
            /*week schedule parameters*/
            "maxSize": 56,
            "week": {
                "@opt": "Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday"
            },
            "id": {
                "@min": 1,
                "@max": 8
            },
            "enable": "true, false",
            /*whether to enable: "true"-enable, "false"-disable*/
            "verifyMode": {
                /*authentication mode: "cardAndPw"-card+password, "card", "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face", "employeeNoAndPw"-employee No.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint, "employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrFaceAndCard"-face or face+card, "fpOrFace"-fingerprint or face, "cardOrFaceOrPw"-card or face or password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint, "cardOrFpOrPw"-card or fingerprint or password, "sleep", "invalid"*/
                "@opt": "cardAndPw, card, cardOrPw, fp, fpAndPw, fpOrCard, fpAndCard, fpAndCardAndPw, faceOrFpOrCardOrPw, faceAndFp, faceAndPw, faceAndCard, face, employeeNoAndPw, fpOrPw, employeeNoAndFp, employeeNoAndFpAndPw, faceAndFpAndCard, faceAndPwAndFp, employeeNoAndFace, faceOrFaceAndCard, fpOrFace, cardOrFaceOrPw, cardOrFace, cardOrFaceOrFp, cardOrFpOrPw, sleep, invalid"
            },
            "TimeSegment": {
                "beginTime": "",
                /*start time of the time period (device local time)*/
                "endTime": "",
                /*end time of the time period (device local time)*/
            }
        }
    }
}
```

```
        "validUnit":  
/*time accuracy: "hour", "minute", "second". If this node is not returned, it  
indicates that the time accuracy is "minute"*/  
    }  
},  
"purePwdVerifyEnable":  
/*optional, boolean, whether the device supports opening the door only by  
password: true-yes, this node is not returned-no. The password used to open the  
door is the value of the node password in the message JSON_UserInfo.*/  
/*For opening the door only by password: 1. The password in "XXX or password"  
in the authentication mode refers to the person's password (the value of the  
node password in JSON_UserInfo); 2. The device will not check the duplication  
of the password, and the upper platform should ensure that the password is  
unique; 3. The password cannot be added, deleted, edited, or searched for on  
the device locally.*/  
}
```

JSON_CapturePreset

CapturePreset message in JSON format

```
{  
    "CapturePreset":{  
        "name":""  
/*optional, string, name, the maximum size is 128 bytes by default. This field  
is NULL by default*/  
    }  
}
```

JSON_CapturePresetCap

CapturePresetCap capability message in JSON format

```
{  
    "CapturePresetCap":{  
        "name":{  
/*optional, string, name*/  
            "@min":0,  
            "@max":0  
        }  
    }  
}
```

JSON_CaptureProgress

CaptureProgress message in JSON format

```
{  
    "CaptureProgress":{  
        "reqCaptureNum": ,  
/*optional, integer, total number of person to be collected*/  
        "completelyCaptureNum": ,  
/*optional, integer, number of completely collected persons*/  
        "partiallyCaptureNum": ,  
/*optional, integer, number of partially collected persons*/  
        "reqFaceNum": ,  
/*optional, integer, number of faces to be collected*/  
        "faceNum": ,  
/*optional, integer, number of collected faces*/  
        "reqFingerprintNum": ,  
/*optional, integer, number of fingerprints to be collected*/  
        "fingerprintNum": ,  
/*optional, integer, number of collected fingerprints*/  
        "reqCardNum": ,  
/*optional, integer, number of cards to be collected*/  
        "cardNum": ,  
/*optional, integer, number of collected cards*/  
        "reqIDCardNum": ,  
/*optional, integer, number of ID cards to be collected*/  
        "IDCardNum": ,  
/*optional, integer, number of collected ID cards*/  
        "reqIssueNum": ,  
/*optional, int, number of persons to be issued with smart cards*/  
        "IssuedNum":  
/*optional, int, number of persons that have been issued with smart cards*/  
    }  
}
```

JSON_CaptureRule

CaptureRule message in JSON format

```
{  
    "CaptureRule":{  
        "enableCardNoLenAuto": ,  
/*optional, boolean, whether to enable length self-adaption of the card serial  
No.*/  
        "cardNoLen": ,  
/*dependency, integer, length of the card serial No.: 3, 4, 7, 10, unit: byte.  
This field is valid when enableCardNoLenAuto is "false". If this field is set  
to 3, it refers to Wiegand 26*/  
        "cardTimeout":  
/*optional, integer, card collection timeout, unit: ms*/  
    }  
}
```

JSON_CaptureRuleCap

CaptureRuleCap capability message in JSON format

```
{  
    "CaptureRuleCap": {  
        "enableCardNoLenAuto": [true, false],  
        /*optional, boolean, whether to enable length self-adaption of the card serial  
        No.*/  
        "cardNoLen": {  
            /*dependency, integer, length of the card serial No.: 3, 4, 7, 10*/  
            "@opt": [3, 4, 7, 10]  
        },  
        "cardTimeout": {  
            /*optional, integer, card collection timeout, unit: ms*/  
            "@min": 0,  
            "@max": 0  
        }  
    }  
}
```

JSON_CardEncryption

JSON message about card encryption parameters

```
{  
    "CardEncryption": {  
        "cardType": "",  
        /*required, string type, card types: "blank"-blank card, "private"-private CPU  
        card, encrypted-other encrypted cards*/  
        "keyLen":,  
        /*depend, integer, size of key for external authentication, this field is valid  
        only when cardType is set to "encrypted"*/  
        "key": ""  
        /*required, hexadecimal string, a 16-byte key content for external  
        authentication*/  
    }  
}
```

JSON_CardInfo

JSON message about card information

```
{  
    "CardInfo": {  
        "employeeNo": "",  
        /*required, string, employee No. (person ID)*/  
        "cardNo": "",  
    }  
}
```

```
/*required, string, card No.*/
    "deleteCard": ,
/*optional, boolean, whether to delete the card: "true"-yes. This node is required only when the card needs to be deleted; for adding or editing card information, this node can be set to NULL*/
    "cardType":"",
/*optional, string, card type: "normalCard"-normal card, "patrolCard"-patrol card, "hijackCard"-duress card, "superCard"-super card, "dismissingCard"-dismiss card, "emergencyCard"-emergency card (it is used to assign permission to a temporary card, but it cannot open the door)*/
    "leaderCard":"",
/*optional, string, whether to support first card authentication function, e.g., the value "1,3,5" indicates that the access control points No.1, No.3, and No.5 support first card authentication function*/
    "checkCardNo":"",
/*optional, boolean, whether to enable duplicated card verification: "false"-disable, "true"-enable. If this node is not configured, the device will verify the duplicated card by default. When there is no card information, you can set checkCardNo to "false" to speed up data applying; otherwise, it is not recommended to configure this node*/
    "checkEmployeeNo": ,
/*optional, boolean, whether to check the existence of the employee No. (person ID): "false"-no, "true"-yes. If this node is not configured, the device will check the existence of the employee No. (person ID) by default. If this node is set to "false", the device will not check the existence of the employee No. (person ID) to speed up data applying; if this node is set to "true" or NULL, the device will check the existence of the employee No. (person ID), and it is recommended to set this node to "true" or NULL if there is no need to speed up data applying*/
    "addCard": ,
/*optional, boolean, whether to add the card if the card information being edited does not exist: "false"-no (if the device has checked that the card information being edited does not exist, the failure response message will be returned along with the error code), "true"-yes (if the device has checked that the card information being edited does not exist, the success response message will be returned, and the card will be added). If this node is not configured, the card will not be added by default*/
    "operateType": "byTerminal",
/*optional, string, operation type: "byTerminal"-by terminal*/
    "terminalNoList": [1]
/*optional, array, terminal ID list, this node is required when operation type is "byTerminal"; currently, only one terminal is supported*/
}
```

Remarks

The **employeeNo** and **cardNo** cannot be edited. If you need to edit the **cardNo**, you should delete the previous card and create a new card.

JSON_CardInfo_Collection

CardInfo message in JSON format

```
{  
    "CardInfo":{  
        "cardNo":"",
/*required, string, card No.*/
        "cardType":""
/*optional, string, card type: "TypeA_M1", "TypeA_CPU", "TypeB", "ID_125K",
"FelicaCard"-Felica card, "DesfireCard"-DESFire card*/
    }
}
```

JSON_CardInfoCap

CardInfoCap capability message in JSON format

```
{  
    "CardInfoCap":{  
        "cardNo":{  
/*required, string, card No.*/
            "@min":1,
            "@max":32
        },
        "cardType":  
["TypeA_M1","TypeA_CPU","TypeB","ID_125K","FelicaCard","DesfireCard"]
/*optional, string, card type: "TypeA_M1", "TypeA_CPU", "TypeB", "ID_125K",
"FelicaCard"-Felica card, "DesfireCard"-DESFire card*/
    }
}
```

JSON_CardInfoCount

CardInfoCount message in JSON format

```
{  
    "CardInfoCount":{  
        "cardNumber":
/*number of cards*/
    }
}
```

JSON_CardInfoDelCond

JSON message about card information to be deleted

```
{  
    "CardInfoDelCond": {  
        "EmployeeNoList" : [{  
            /*optional, person ID list, if this node does not exist or is set to NULL, it  
            indicates deleting all cards*/  
            "employeeNo":""  
        },  
        /*optional, string, employee No. (person ID)*/  
        "CardNoList": [{  
            /*optional, card No. list (this node cannot exist together with the  
            EmployeeNoList, and if this node does not exist or is set to NULL, it indicates  
            deleting all cards)*/  
            "cardNo":""  
        },  
        /*optional, string, card No.*/  
        "operateType": "byTerminal",  
        /*optional, string, operation type: "byTerminal"-by terminal*/  
        "terminalNoList": [1]  
        /*optional, array, terminal ID list, this node is required when operation type  
        is "byTerminal"; currently, only one terminal is supported*/  
    }  
}
```

JSON_CardInfoSearch

CardInfoSearch message in JSON format

```
{  
    "CardInfoSearch": {  
        "searchID": "",  
        /*required, string, search ID, which is used to confirm the upper-level  
        platform or system. If the platform or the system is the same one during two  
        searching, the search history will be saved in the memory to speed up next  
        searching*/  
        "responseStatusStrg": "",  
        /*required, string, search status: "OK"-searching completed, "NO MATCH"-no  
        matched results, "MORE"-searching for more results*/  
        "numOfMatches": ,  
        /*required, integer32, number of returned results*/  
        "totalMatches": ,  
        /*required, integer32, total number of matched results*/  
        "CardInfo": [{  
            /*optional, person information*/  
            "employeeNo": "",  
            /*required, string, employee No. (person ID)*/  
            "cardNo": "",  
            /*required, string, card No.*/  
            "cardType": "",  
            /*required, string, card type: "normalCard"-normal card, "patrolCard"-patrol  
            card, "hijackCard"-duress card, "superCard"-super card, "dismissingCard"-
```

```
dismiss card, "emergencyCard"-emergency card (it is used to assign permission  
to a temporary card, but it cannot open the door)*/  
    "leaderCard":""},  
/*optional, string, whether to support first card authentication function,  
e.g., the value "1,3,5" indicates that the access control points No.1, No.3,  
and No.5 support first card authentication function*/  
    []  
}  
}
```

JSON_CardInfoSearchCond

CardInfoSearchCond message in JSON format

```
{  
    "CardInfoSearchCond":{  
        "searchID":""},  
/*required, string, search ID, which is used to confirm the upper-level  
platform or system. If the platform or the system is the same one during two  
searching, the search history will be saved in the memory to speed up next  
searching*/  
        "searchResultPosition": ,  
/*required, integer32, the start position of the search result in the result  
list. When there are multiple records and you cannot get all search results at  
a time, you can search for the records after the specified position next time.  
For example, if the maximum total number of matched results (totalMatches)  
supported by the device is M and the total number of matched results  
(totalMatches) stored in the device currently is N (here N is smaller than M),  
the valid range of this field is from 0 to N-1*/  
        "maxResults": ,  
/*required, integer32, maximum number of search results. If maxResults exceeds  
the range returned by the device capability, the device will return the maximum  
number of search results according to the device capability and will not return  
error message*/  
        "EmployeeNoList":[]  
/*optional, person ID list (if this node does not exist or is set to NULL, it  
indicates searching for all cards)*/  
        "employeeNo":""  
/*optional, string, employee No. (person ID)*/  
    },  
        "CardNoList":[]  
/*optional, card No. list (this node cannot exist together with EmployeeNoList,  
and if this node does not exist or is set to NULL, it indicates searching for  
all cards)*/  
        "cardNo":""  
/*optional, string, card No.*/  
    }  
}
```

JSON_CardIssueStatus

JSON message about the smart card issuing status

```
{  
    "CardIssueStatus":{  
        "status":"ok",  
        /*required, string, card issuing status: "ok"-succeeded, "failed"-operation failed, "timeout"-timed out, "verifyFailure"-authentication failed, "noCard"-no card detected, "processing"*/  
        "cardNo": "",  
        /*optional, string, issued card No.*/  
        "cardErrorCode": 0,  
        /*dependent, int, internal error code of card operation. This node is valid when the value of status is "failed"*/  
        "face": true,  
        /*optional, boolean, issuing status of the card containing the face picture: true-issued, false-not issued*/  
        "fingerprint1": true,  
        /*optional, boolean, issuing status of the card containing fingerprint 1: true-issued, false-not issued*/  
        "fingerprint2": true,  
        /*optional, boolean, issuing status of the card containing fingerprint 2: true-issued, false-not issued*/  
        "customData": true  
        /*optional, boolean, issuing status of the card containing custom information: true-issued, false-not issued*/  
    }  
}
```

JSON_CardOperationsCap

JSON message about card operation capability

```
{  
    "CardOperationsCap":{  
        "SectionEncryption":{  
            "supportFunction":{  
                /*required, string, supported methods*/  
                "@opt": ["put", "get", "delete", "post"]  
            },  
            "sectionNo": {  
                /*required, integer, section No.*/  
                "@min": 0,  
                "@max": 0  
            },  
            "keyType": {  
                /*required, string, verification key types: "private"-private key, "normal"-other valid keys*/  
            }  
        }  
    }  
}
```

```
    "@opt": ["private", "normal"]
},
"password":{
/*optional, string, a hexadecimal verification key, this field is valid only
when keyType is set to "nomal"*/
    "@min": 0,
    "@max": 0
},
"newKeyType":{
/*required, string, new key types: "private"-private key, "normal"-other valid
keys*/
    "@opt": ["private", "normal"]
},
"KeyA":{
/*optional, string, a hexadecimal key A password*/
    "@min": 0,
    "@max": 0
},
"KeyB":{
/*optional, string, a hexadecimal key B password*/
    "@min": 0,
    "@max": 0
},
"controlBits":{
/*optional, string, a hexadecimal control bit*/
    "@min": 0,
    "@max": 0
},
},
"Verification":{
    "supportFunction":{
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
},
"sectionNo":{
/*required, integer, section No.*/
    "@min": 0,
    "@max": 0
},
"passwordType":{
/*optional, password types: "KeyA" (default), "KeyB"*/
    "@opt": ["KeyA", "KeyB"]
},
"password":{
/*optional, string, a hexadecimal password*/
    "@min": 0,
    "@max": 0
},
},
"DataBlock":{
    "supportFunction":{
/*required, string, supported methods*/

```

```

        "@opt": ["put", "get", "delete", "post"]
    },
    "addressOfBlock":{
/*optional, integer, block address*/
        "@min": 0,
        "@max": 0
    },
    "data":{
/*required, a hexBinary string, e.g., "f2345678abf2345678abf2345678abf2"*/
        "@min": 0,
        "@max": 0
    },
},
"DataBlockCtrl":{
    "supportFunction":{
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "addressOfBlock":{
/*required, integer, block address*/
        "@min": 0,
        "@max": 0
    },
    "command":{
/*required, string, control commands*/
        "@opt": ["add", "minus", "copy", "paste"]
    },
    "value":{
/*depend, integer, relative value to be changed, this field is valid only when
the command is set to "add" or "minus"*/
        "@min": 0,
        "@max": 0
    },
},
"ControlBlock":{
    "supportFunction":{
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "sectionNo":{
/*required, integer, section No.*/
        "@min": 0,
        "@max": 0
    },
    "KeyA":{
/*optional, string, a hexadecimal key A*/
        "@min": 0,
        "@max": 0
    },
    "KeyB":{
/*optional, string, a hexadecimal key B*/
        "@min": 0,
        "@max": 0
    }
}

```

```

        "@max": 0
    },
    "controlBits": {
/*optional, string, a hexadecimal control bit*/
        "@min": 0,
        "@max": 0
    }
},
"CardProto": {
    "supportFunction": {
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "protocol": {
/*required, string, operation protocol types*/
        "@opt": ["TypeA", "TypeB", "TypeAB", "125K", "all"]
    }
},
"CardEncryption": {
    "supportFunction": {
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "cardType": {
/*required, string, card types: "blank"-blank card, "private"-private CPU card,
"encrypted"-other encrypted card*/
        "@opt": [ "blank", "private", "encrypted" ]
    }
},
"keyLen": {
/*depend, integer, size of key for external authentication, this field is valid
only when cardType is set to "encrypted"*/
    "@min": 0,
    "@max": 0
},
"key": {
/*required, hexadeciml string, a 16-byte key content for external
authentication*/
    "@min": 0,
    "@max": 0
},
"CardParam": {
    "supportFunction": {
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "type": {
/*required, string, card types*/
        "@opt": ["CPU1356", "PSAM1", "PSAM2", "PSAM3", "PSAM4"]
    },
    "protocol": {
/*required, string, card protocol types*/

```

```

        "@opt": ["T0", "T1"]
    }
},
"CardResetResponse":{
    "supportFunction":{
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "data":{
/*required, string, resetting response information (usually, it is
manufacturer, which is encoded by Base64 and specified by device*/
        "@min": 0,
        "@max": 0
    }
},
"DataTrans":{
    "supportFunction":{
/*required, string, supported methods*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "content":{
/*required, string, data to be passed through, which is encoded in Base64*/
        "@min": 0,
        "@max": 0
    }
},
"Issue":{
/*capability of sending a request for card issuing and getting the current card
issuing status and real-time card issuing results, related URIs: /ISAPI/
AccessControl/CardOperations/localIssueRequest?format=json and /ISAPI/
AccessControl/CardOperations/localIssueStatus?format=json*/
    "supportFunction":{
/*required, string, supported methods. The actually supported methods will be
returned*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "LocalIssueRequest":{
        "operation":{
/*required, string, operation type: "face"-issue card to be enrolled with face
picture, "fingerprint"-issue card to be enrolled with fingerprint*/
            "@opt": ["face", "fingerprint"]
        },
        "FPIIndex":{
/*optional, int, fingerprint storage index (card storage area). This field is
valid when operation is "fingerprint"*/
            "@min":0,
            "@max":0
        },
        "facePic":{
/*optional, string, face picture type: "visible"-visible light picture,
"infrared"-IR light picture. This field is valid when operation is "face"*/
            "@opt": ["visible", "infrared"]
        }
    }
}
}

```

```

        }
    },
    "LocalIssueRes": {
        "status": {
/*required, string, card issuing status: "ok"-succeeded, "failed"-card
operation failed, "timeout"-timed out, "verifiyFailure"-authentication failed,
"noCard"-no card detected, "processing"-processing*/
            "@opt": ["ok", "failed", "processing", "timeout", "verifiyFailure",
"noCard"]
        },
        "cardNo": {
/*optional, string, issued card No.*/
            "@min": 0
        },
        "cardErrorCode": {
/*dependent, string, internal error code of card operation returned by the
device*/
            "@opt":
        }
    },
    "localIssueCfg": {
/*capability of configuring rule parameters for issuing smart cards, related
URI: /ISAPI/AccessControl/CardOperations/localIssueCfg?format=json*/
        "validFP": {
/*optional, array of int, valid fingerprint ID. This field is valid for
applying fingerprint to the card*/
            "@size": 2,
            "@min": 1,
            "@max": 10
        },
        "validFacePicture": {
/*optional, string, valid face picture type: "visible"-visible light picture,
"infrared"-IR light picture. This field is valid for applying face picture to
the card*/
            "@opt": ["visible", "infrared"]
        }
    },
    "ClearData": {
/*capability of deleting data from the card, related URI: /ISAPI/AccessControl/
CardOperations/clearData?format=json*/
        "supportFunction": {
/*required, string, supported methods. The actually supported methods will be
returned*/
            "@opt": ["put", "get", "delete", "post"]
        },
        "checkAll": {
/*optional, boolean, whether to delete all data*/
            "@opt": [true, false]
        },
        "checkFingerprint": {
/*optional, boolean, whether to delete fingerprint data. This field is valid

```

```
when checkAll is false or does not exist*/
    "@opt": [true, false]
},
    "fingerprints": {
/*optional, array of int, list of addresses whether the fingerprints to be
deleted are stored. This field is valid when checkFingerprint exists. If this
field does not exist, it indicates deleting all fingerprints*/
    "@size": 2,
    "@min": 0,
    "@max": 0
},
    "checkFacePicture": {
/*optional, boolean, whether to delete face data. This field is valid when
checkAll is false or does not exist*/
    "@opt": [true, false]
},
    "checkCustom": {
/*optional, boolean, whether to delete custom data. This field is valid when
checkAll is false or does not exist*/
    "@opt": [true, false]
},
    "ClearDataRes": {
        "status": {
/*required, string, card issuing status: "ok"-succeeded, "failed"-operation
failed, "timeout"-timed out, "verifyFailure"-authentication failed, "noCard"-no
card detected, "processing"-processing*/
        "@opt": ["ok", "failed", "processing", "timeout", "verifyFailure",
"noCard"]
},
        "cardErrorCode": {
/*dependent, int, internal error code of card operation*/
        "@opt":
        }
},
    "CustomData": {
/*capability of setting custom card information, related URI: /ISAPI/
AccessControl/CardOperations/customData?format=json*/
        "supportFunction": {
/*required, string, supported methods. The actually supported methods will be
returned*/
        "@opt": ["put", "get", "delete", "post"]
},
        "address": {
/*optional, int, start address for writing. By default the data will be written
from the start address*/
        "@min": 0,
        "@max": 0
},
        "length": {
/*optional, int, length of source data to be written, it is 0 by default, unit:
byte*/
}
```

```
        "@min":0,
        "@max":0
    },
    "data":{
/*required, string, custom information encoded by Base64*/
        "@min":0,
        "@max":0
    },
    "CustomDataRes":{
        "status":{

/*required, string, card issuing status: "ok"-succeeded, "failed"-operation failed, "timeout"-timed out, "verifiyFailure"-authentication failed, "noCard"-no card detected, "processing"-processing*/
            "@opt":["ok", "failed", "processing", "timeout", "verifiyFailure",
"noCard"]
        },
        "cardErrorCode":{

/*dependent, int, internal error code of card operation*/
            "@opt":
        }
    },
    "CustomDataSearchCond":{

/*condition configuration capability of searching for custom card information, related URI: /ISAPI/AccessControl/CardOperations/customData/searchTask?format=json*/
        "address":{

/*optional, int, start address for reading. By default the data will be read from the start address*/
            "@min":0,
            "@max":0
        },
        "length":{

/*optional, int, length of data to be read, it is 0 by default, unit: byte*/
            "@min":0,
            "@max":0
        }
    },
    "CustomDataResult":{

/*result capability of searching for custom card information, related URI: /ISAPI/AccessControl/CardOperations/customData/searchTask?format=json*/
        "length":{

/*required, int, length of data that has been read, unit: byte*/
            "@min":0,
            "@max":0
        },
        "data":{

/*required, string, card information encoded by Base64*/
            "@min":0,
            "@max":0
        },
        "status":{


```

```
/*required, string, card issuing status: "ok"-succeeded, "failed"-operation failed, "timeout"-timed out, "verifiyFailure"-authentication failed, "noCard"-no card detected, "processing"-processing*/
    "@opt": ["ok", "failed", "processing", "timeout", "verifiyFailure",
"noCard"]
},
"cardErrorCode":{
/*required, int, internal error code of card operation*/
    "@opt":
}
},
"CardIssueStatus":{
/*capability of getting the smart card issuing status, related URI: /ISAPI/
AccessControl/CardOperations/cardIssueStatus?format=json*/
    "status":{
/*required, string, card issuing status: "ok"-succeeded, "failed"-operation failed, "timeout"-timed out, "verifiyFailure"-authentication failed, "noCard"-no card detected, "processing"-processing*/
        "@opt": ["ok", "failed", "processing", "timeout", "verifiyFailure",
"noCard"]
},
"cardNo":{
/*optional, string, issued card No.*/
    "@min":0,
    "@max":0
},
"cardErrorCode":{
/*dependent, int, internal error code of card operation*/
    "@opt":
}
},
"face":{
/*optional, boolean, issuing status of the card containing the face picture:
true-issued, false-not issued*/
    "@opt": [true, false]
},
"fingerprint1":{
/*optional, boolean, issuing status of the card containing fingerprint 1: true-issued, false-not issued*/
    "@opt": [true, false]
},
"fingerprint2":{
/*optional, boolean, issuing status of the card containing fingerprint 2: true-issued, false-not issued*/
    "@opt": [true, false]
},
"customData":{
/*optional, boolean, issuing status of the card containing custom information:
true-issued, false-not issued*/
    "@opt": [true, false]
}
}
```

```
    }  
}
```

JSON_CardParam

JSON message about card parameters

```
{  
    "CardParam": {  
        "type": ""  
/*required, string, card types: " CPU1356,PSAM1,PSAM2,PSAM3,PSAM4"*/  
        "protocol": ""  
/*required, string, card protocol types: "T0,T1"*/  
    }  
}
```

JSON_CardProto

JSON message about operation protocol types of card

```
{  
    "CardProto": {  
        "protocol": "TypeA"  
/*required, string, operation protocol types: "TypeA,TypeB,TypeAB,125K,all"*/  
    }  
}
```

JSON_CardReaderAntiSneakCfg

CardReaderAntiSneakCfg message in JSON format

```
{  
    "CardReaderAntiSneakCfg": {  
        "enable": ,  
/*required, boolean, whether to enable the anti-passing back function of the  
card reader: "true"-enable, "false"-disable*/  
        "followUpCardReader":  
/*optional, array, following card reader No. after the first card reader, e.g.,  
[2,3,4] indicates that card reader No. 2, No. 3, and No. 4 can be swiped after  
the first card reader*/  
    }  
}
```

JSON_CardReaderCfg

CardReaderCfg message in JSON format

```
{
    "CardReaderCfg": {
        "enable": ,
        /*required, boolean, whether to enable: "true"-yes, "false"-no*/
        "okLedPolarity": "",
        /*optional, string, OK LED polarity: "cathode", "anode"*/
        "errorLedPolarity": "",
        /*optional, string, error LED polarity: "cathode", "anode"*/
        "buzzerPolarity": "",
        /*optional, string, buzzer polarity: "cathode", "anode"*/
        "swipeInterval": ,
        /*optional, integer, time interval of repeated authentication, which is valid
        for authentication modes such as fingerprint, card, face, etc., unit: second*/
        "pressTimeout": ,
        /*optional, integer, timeout to reset entry on keypad, unit: second*/
        "enableFailAlarm": ,
        /*optional, boolean, whether to enable excessive failed authentication attempts
        alarm*/
        "maxReadCardFailNum": ,
        /*optional, integer, maximum number of failed authentication attempts*/
        "enableTamperCheck": ,
        /*optional, boolean, whether to enable tampering detection*/
        "offlineCheckTime": ,
        /*optional, integer, time to detect after the card reader is offline, unit:
        second*/
        "fingerPrintCheckLevel": ,
        /*optional, integer, fingerprint recognition level: 1-1/10 false acceptance
        rate (FAR), 2-1/100 false acceptance rate (FAR), 3-1/1000 false acceptance rate
        (FAR), 4-1/10000 false acceptance rate (FAR), 5-1/100000 false acceptance rate
        (FAR), 6-1/1000000 false acceptance rate (FAR), 7-1/10000000 false acceptance
        rate (FAR), 8-1/100000000 false acceptance rate (FAR), 9-3/100 false acceptance
        rate (FAR), 10-3/1000 false acceptance rate (FAR), 11-3/10000 false acceptance
        rate (FAR), 12-3/100000 false acceptance rate (FAR), 13-3/1000000 false
        acceptance rate (FAR), 14-3/10000000 false acceptance rate (FAR),
        15-3/100000000 false acceptance rate (FAR), 16-Automatic Normal, 17-Automatic
        Secure, 18-Automatic More Secure (currently not support)*/
        "useLocalController": ,
        /*ro, opt, boolean, whether it is connected to the distributed controller*/
        "localControllerID": ,
        /*ro, opt, integer, distributed controller No., which is between 1 and 64, 0-
        unregistered. This field is valid only when useLocalController is "true"*/
        "localControllerReaderID": ,
        /*ro, opt, integer, card reader ID of the distributed controller, 0-
        unregistered. This field is valid only when useLocalController is "true"*/
        "cardReaderChannel": ,
        /*ro, opt, integer, communication channel No. of the card reader: 0-Wiegand or
        offline, 1-RS-485A, 2-RS-485B. This field is valid only when useLocalController
```

```
is "true"*/
    "fingerPrintImageQuality": ,
/*opt, integer, fingerprint image quality: 1-low quality (V1), 2-medium quality
(V1), 3-high quality (V1), 4-highest quality (V1), 5-low quality (V2), 6-medium
quality (V2), 7-high quality (V2), 8-highest quality (V2)*/
    "fingerPrintContrastTimeOut": ,
/*optional, integer, fingerprint comparison timeout, which is between 1 and 20,
unit: second, 255-infinite*/
    "fingerPrintRecognizeInterval": ,
/*optional, integer, fingerprint scanning interval, which is between 1 and 10,
unit: second, 255-no delay*/
    "fingerPrintMatchFastMode": ,
/*optional, integer, fingerprint matching quick mode: 1-quick mode 1, 2-quick
mode 2, 3-quick mode 3, 4-quick mode 4, 5-quick mode 5, 255-automatic*/
    "fingerPrintModuleSensitive": ,
/*optional, integer, fingerprint module sensitivity, which is between 1 and 8*/
    "fingerPrintModuleLightCondition": "",
/*optional, string, fingerprint module light condition: "outdoor", "indoor"*/
    "faceMatchThresholdN": ,
/*optional, integer, threshold of face picture 1:N comparison, which is between
0 and 100*/
    "faceQuality": ,
/*optional, integer, face picture quality, which is between 0 and 100*/
    "faceRecognizeTimeOut": ,
/*optional, integer, face recognition timeout, which is between 1 and 20, unit:
second, 255-infinite*/
    "faceRecognizeInterval": ,
/*optional, integer, face recognition interval, which is between 1 and 10,
unit: second, 255-no delay*/
    "cardReaderFunction": ,
/*ro, opt, array, card reader type: "fingerPrint"-fingerprint, "face",
"fingerVein"-finger vein. For example, ["fingerPrint","face"] indicates that
the card reader supports both fingerprint and face*/
    "cardReaderDescription": "",
/*ro, opt, string, card reader description. If the card reader is the Wiegand
card reader or if offline, this field will be set to "Wiegand" or "485Offline"*/
    "faceImageSensitometry": ,
/*ro, opt, integer, face picture exposure, which is between 0 and 65535*/
    "livingBodyDetect": ,
/*optional, boolean, whether to enable human detection*/
    "faceMatchThreshold1": ,
/*optional, integer, threshold of face picture 1:1 comparison, which is between
0 and 100*/
    "buzzerTime": ,
/*optional, integer, buzzing duration, which is between 0 and 5999, unit:
second, 0-long buzzing*/
    "faceMatch1SecurityLevel": ,
/*optional, integer, security level of face 1:1 recognition: 1-normal, 2-high,
3-higher*/
    "faceMatchNSecurityLevel": ,
/*optional, integer, security level of face 1:N recognition: 1-normal, 2-high,
3-higher*/
```

```
"envirMode":"",
/*optional, string, environment mode of face recognition: "indoor", "other"*/
"liveDetLevelSet":"",
/*optional, string, threshold level of liveness detection: "low", "middle"-medium, "high"*/
"liveDetAntiAttackCntLimit": ,
/*optional, integer, number of anti-attacks of liveness detection, which is between 1 and 255. This value should be configured as the same one on both client and device*/
"enableLiveDetAntiAttack": ,
/*optional, boolean, whether to enable anti-attack for liveness detection*/
"supportDelFPByID": ,
/*ro, opt, boolean, whether the card reader supports deleting fingerprint by fingerprint ID: "true"-yes, "false"-no*/
"fingerPrintCapacity": ,
/*ro, opt, integer, fingerprint capacity, which is the maximum number of fingerprints that can be added*/
"fingerPrintNum": ,
/*ro, opt, integer, number of added fingerprints*/
"defaultVerifyMode":"",
/*ro, opt, string, default authentication mode of the fingerprint and card reader (factory defaults): "cardAndPw"-card+password, "card", "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face", "employeeNoAndPw"-employee No.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint, "employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint*/
"faceRecognizeEnable": ,
/*optional, integer, whether to enable facial recognition: 1-enable, 2-disable, 3-attendance checked in/out by recognition of multiple faces*/
"FPAlgorithmVersion":"",
/*optional, string, read-only, fingerprint algorithm library version*/
"cardReaderVersion":"",
/*optional, string, read-only, card reader version*/
"enableReverseCardNo": true,
/*optional, boolean, whether to enable reversing the card No.*/
"independSwipeIntervals": 0,
/*optional, int, time interval of person authentication, unit: second. This time interval is calculated for each person separately and is different from swipeInterval*/
"maskFaceMatchThresholdN":1,
/*optional, int, 1:N face picture (face with mask and normal background) comparison threshold, value range: [0,100]*/
"maskFaceMatchThreshold1":1
/*optional, int, 1:1 face picture (face with mask and normal background) comparison threshold, value range: [0,100]*/
```

```
    }  
}
```

JSON_CardReaderPlan

CardReaderPlan message in JSON format

```
{  
    "CardReaderPlan": {  
        "templateNo":  
/*required, integer, schedule template No.: 0-cancel linking the template to the  
schedule and restore to the default status (normal status)*/  
    }  
}
```

JSON_CardResetResponse

JSON message about card resetting response

```
{  
    "CardResetResponse": {  
        "data": ""  
/*required, string, resetting response information (usually, it is  
manufacturer, which is encoded by Base64 and specified by device)*/  
    }  
}
```

JSON_CardVerificationRule

JSON message about the parameters of card No. authentication mode

```
{  
    "CardVerificationRule":{  
        "cardNoLenMode":"full"  
/*required, string, length mode of card No. authentication (comparison):  
"full", "3Bytes", "4Bytes". After the card No. authentication (comparison) mode  
is switched, the device should check the card No. compatibility*/  
    }  
}
```

JSON_CardVerificationRuleCap

JSON message about the configuration capability of the card No. authentication mode

```
{  
    "CardVerificationRuleCap":{
```

```
"cardNoLenMode": {
/*required, string, length mode of card No. authentication (comparison):
"full", "3Bytes", "4Bytes". After the card No. authentication (comparison) mode
is switched, the device should check the compatibility of the card No.*/
    "@opt":["full", "3Bytes", "4Bytes"]
},
"CardVerificationRuleRes": {
    "checkStatus": {
/*required, string, status of switching card No. authentication (comparison)
mode: "continue"-switching result can be searched for later, "ok"-switching
completed, "duplicate"-duplicate data exist and switching failed*/
        "@opt":["continue", "ok", "duplicate"]
    },
    "progress": {
/*optional, int, switching progress in percentage which is between 0 and 100,
and 100 indicates that the card No. authentication (comparison) mode is
switched*/
        "@min":0,
        "@max":0
    }
}
}
```

JSON_CardVerificationRuleRes

JSON message about the switching progress and configuration result of card No. authentication mode

```
{
    "CardVerificationRuleRes": {
        "checkStatus":"continue",
/*required, string, status of switching card No. authentication (comparison)
mode: "continue"-switching result can be searched for later, "ok"-switching
succeeded, "duplicate"-duplicate data exist and switching failed*/
        "progress":0
/*optional, int, switching progress in percentage which is between 0 and 100,
and 100 indicates that card No. authentication (comparison) mode is switched*/
    }
}
```

JSON_ClearAntiSneak

ClearAntiSneak message in JSON format

```
{
    "ClearAntiSneak": {
        "clearAll": ,
/*required, boolean, whether to clear all anti-passing back records: "true"-*/
    }
}
```

```
yes, "false"-no. Clearing all anti-passing back records is not supported by  
access control devices version 2.1*/  
    "EmployeeNoList" : [{}  
/*optional, person ID list, this node is valid when clearAll is "false". For  
access control devices version 2.1, if this node is not configured, failure  
response message will be returned*/  
    "employeeNo":""  
/*optional, string, employee No. (person ID)*/  
    }]  
}  
}
```

JSON_ClearAntiSneakCfg

ClearAntiSneakCfg message in JSON format

```
{  
    "ClearAntiSneakCfg":{  
        "ClearFlags":{  
            "antiSneak":  
/*required, boolean, whether to clear the anti-passing back parameters*/  
            }  
        }  
    }  
}
```

JSON_ClearAttendancePlan

JSON message about the parameters for clearing the attendance schedule

```
{  
    "ClearAttendancePlan":{  
        "ClearFlags":{  
            "attendanceWeekPlan":true,  
/*optional, boolean, whether to clear the week attendance schedule*/  
            "attendanceTemplate":true  
/*optional, boolean, whether to clear the parameters of the attendance schedule  
template*/  
            }  
        }  
    }  
}
```

JSON_ClearData

JSON message about the conditions of deleting data from the card

```
{  
    "ClearData":{  
        }
```

```
    "checkAll":true,  
    /*optional, boolean, whether to delete all data*/  
    "checkFingerprint":true,  
    /*optional, boolean, whether to delete fingerprint data. This node is valid  
when the value of checkAll is false or the node checkAll does not exist*/  
    "fingerprints":[1, 2],  
    /*optional, array of int, address list of storage areas where the fingerprints  
to be deleted are stored. This node is valid when the node checkFingerprint  
exists. If this node does not exist, it indicates deleting all fingerprints*/  
    "checkFacePicture":true,  
    /*optional, boolean, whether to delete face data. This node is valid when the  
value of checkAll is false or the node checkAll does not exist*/  
    "checkCustom":true  
    /*optional, boolean, whether to delete custom data. This node is valid when the  
value of checkAll is false or the node checkAll does not exist*/  
}  
}
```

JSON_ClearDataRes

JSON message about the result parameters of deleting data from the card

```
{  
    "ClearDataRes":{  
        "status":"ok",  
        /*required, string, card issuing status: "ok"-succeeded, "failed"-operation  
failed, "timeout"-timed out, "verifiyFailure"-authentication failed, "noCard"-  
no card detected, "processing"-processing*/  
        "cardErrorCode":  
        /*dependent, int, internal error code of card operation*/  
    }  
}
```

JSON_ClearEventCardLinkageCfg

ClearEventCardLinkageCfg message in JSON format

```
{  
    "ClearEventCardLinkageCfg":{  
        "ClearFlags":{  
            "eventCardLinkage":  
            /*required, boolean, whether to clear event and card linkage parameters: "true"-  
yes, "false"-no*/  
        }  
    }  
}
```

JSON_ClearGroupCfg

ClearGroupCfg message in JSON format

```
{  
    "ClearGroupCfg":{  
        "ClearFlags":{  
            "groupCfg":  
/*required, boolean, group parameters*/  
        }  
    }  
}
```

JSON_ClearPictureCfg

JSON message about the parameters of clearing all pictures in the device

```
{  
    "ClearPictureCfg":{  
        "ClearFlags":{  
            "facePicture":true,  
/*optional, boolean, whether it supports clearing registered face pictures in  
the device*/  
            "capOrVerifyPicture":true  
/*optional, boolean, whether it supports clearing authenticated or captured  
face pictures in the device*/  
        }  
    }  
}
```

JSON_ClearPictureCfgCap

JSON message about the capability of clearing all pictures in the device

```
{  
    "ClearPictureCfgCap":{  
        "ClearFlags":{  
            "facePicture":{  
/*optional, boolean, whether it supports clearing registered face pictures*/  
                "@opt":[true, false]  
            },  
            "capOrVerifyPicture":{  
/*optional, boolean, whether it supports clearing authenticated or captured  
face pictures*/  
                "@opt":[true, false]  
            }  
        }  
    }  
}
```

```
    }
}
```

JSON_ClearPlansCfg

ClearPlansCfg message in JSON format

```
{
  "ClearPlansCfg": {
    "ClearFlags": {
      "doorStatusWeekPlan": ,
      /*optional, boolean, whether to clear the week schedule of the door control:
      "true"-yes, "false"-no*/
      "cardReaderWeekPlan": ,
      /*optional, boolean, whether to clear the week schedule of the card reader
      authentication mode control: "true"-yes, "false"-no*/
      "userRightWeekPlan": ,
      /*optional, boolean, whether to clear the week schedule of the access
      permission control: "true"-yes, "false"-no*/
      "doorStatusHolidayPlan": ,
      /*optional, boolean, whether to clear the holiday schedule of the door control:
      "true"-yes, "false"-no*/
      "cardReaderHolidayPlan": ,
      /*optional, boolean, whether to clear the holiday schedule of the card reader
      authentication mode control: "true"-yes, "false"-no*/
      "userRightHolidayPlan": ,
      /*optional, boolean, whether to clear the holiday schedule of the access
      permission control: "true"-yes, "false"-no*/
      "doorStatusHolidayGroup": ,
      /*optional, boolean, whether to clear the holiday group of the door control:
      "true"-yes, "false"-no*/
      "cardReaderHolidayGroup": ,
      /*optional, boolean, whether to clear the holiday group of the card reader
      authentication mode control: "true"-yes, "false"-no*/
      "userRightHolidayGroup": ,
      /*optional, boolean, whether to clear the holiday group of the access
      permission control: "true"-yes, "false"-no*/
      "doorStatusTemplate": ,
      /*optional, boolean, whether to clear the schedule template of the door
      control: "true"-yes, "false"-no*/
      "cardReaderTemplate": ,
      /*optional, boolean, whether to clear the control schedule template of card
      reader authentication mode: "true"-yes, "false"-no*/
      "userRightTemplate": ,
      /*optional, boolean, whether to clear the schedule template of access
      permission control: "true"-yes, "false"-no*/
    }
  }
}
```

JSON_ControlBlock

JSON message about the control block parameters of a specific section.

```
{  
    "ControlBlock": {  
        "sectionNo": ,  
/*required, integer, section No.*/  
        "KeyA": "",  
/*optional, string type, a hexadecimal key A password*/  
        "KeyB": "",  
/*optional, string type, a hexadecimal key B password*/  
        "controlBits":""  
/*optional, string type, a hexadecimal control bit*/  
    }  
}
```

JSON_CreateFPLibCond

Message about the conditions of creating face picture library, and it is in JSON format.

```
{  
    "faceLibType": "",  
/*required, string type, face picture library type: "infraredFD"-infrared face  
picture library, "blackFD"-list library, "staticFD"-static library, the maximum  
size is 32 bytes*/  
    "name": "",  
/*required, string type, face picture library name, it cannot be duplicated,  
the maximum size is 48 bytes*/  
    "customInfo": "",  
/*optional, string type, custom information, it is used to indicate the data  
property or uniqueness, the maximum size is 192 bytes*/  
}
```

JSON_CreateFPLibResult

Message about the results of creating face picture library, and it is in JSON format.

```
{  
    "requestURL": "",  
    "statusCode": "",  
    "statusString": "",  
    "subStatusCode": "",  
    "errorCode": "",  
    "errorMsg": "",  
/*see the description of this node and above nodes in the message of  
JSON_ResponseStatus*/  
    "FDID": ""
```

```
/*optional, string type, returned face picture library ID when it created, the  
library ID of the same type is unique, the maximum length is 63 bytes. This  
node is valid when errorCode is 1 and errorMsg is "ok"*/  
}
```

See Also

[JSONResponseStatus](#)

JSON_CustomAudioFileApplyStatusSearchCond

JSON message about the condition of searching for the applying status of specified custom audio files

```
{  
    "customAudioSearchType": ["callCenter", "centerBusy"]  
/*required, array of string, searching type of the custom audio file: "all"  
(searching for all types), "callCenter" (calling the center), "centerBusy" (the  
line is busy), "centerRefused" (the call is declined), "centerOverTime"  
(unanswered), "swipeCard" (please swipe the card), "thanks", "callAgain" (try  
again later), "verifyFailed" (authentication failed), "verifySuccess"  
(authentication succeeded), "doorOpened" (the door is opened),  
"wearSafetyHelmet" (please wear a hard hat), "wearMask" (please wear a mask),  
"abnormalTemperature" (the skin-surface temperature is abnormal)*/  
}
```

JSON_CustomAudioFileApplyStatusSearchResult

JSON message about the result of searching for the applying status of specified custom audio files

```
{  
    "CustomAudioStatusList": [  
        /*required, array of object, status list of the custom audio files*/  
        {"customAudioType": "callCenter",  
        /*required, string, type of the custom audio file: "callCenter" (calling the  
center), "centerBusy" (the line is busy), "centerRefused" (the call is  
declined), "centerOverTime" (unanswered), "swipeCard" (please swipe the card),  
"thanks", "callAgain" (try again later), "verifyFailed" (authentication  
failed), "verifySuccess" (authentication succeeded), "doorOpened" (the door is  
opened), "wearSafetyHelmet" (please wear a hard hat), "wearMask" (please wear a  
mask), "abnormalTemperature" (the skin-surface temperature is abnormal)*/  
        "status": "normal"  
        /*required, string, status: "normal" (applied), "abnormal" (not applied)*/  
    ]  
}
```

JSON_CustomAudioFileDelCond

JSON message about the condition of deleting the custom audio file

```
{  
    "customAudioType": "callCenter"  
    /*required, string, type of the custom audio file: "callCenter" (calling the  
    center), "centerBusy" (the line is busy), "centerRefused" (the call is  
    declined), "centerOverTime" (unanswered), "swipeCard" (please swipe the card),  
    "thanks", "callAgain" (try again later), "verifyFailed" (authentication  
    failed), "verifySuccess" (authentication succeeded), "doorOpened" (the door is  
    opened), "wearSafetyHelmet" (please wear a hard hat), "wearMask" (please wear a  
    mask), "abnormalTemperature" (the skin-surface temperature is abnormal)*/  
}
```

JSON_CustomData

JSON message about the conditions of setting custom card information

```
{  
    "CustomData": {  
        "address": 1,  
        /*optional, int, start address for writing. By default the data will be written  
        from the start address*/  
        "length": 1,  
        /*optional, int, length of the source data to be written, it is 0 by default,  
        unit: byte*/  
        "data": ""  
        /*required, string, custom information encoded by Base64*/  
    }  
}
```

JSON_CustomDataRes

JSON message about the result parameters of setting custom card information

```
{  
    "CustomDataRes": {  
        "status": "ok",  
        /*required, string, card issuing status: "ok"-succeeded, "failed"-operation  
        failed, "timeout"-timed out, "verifyFailure"-authentication failed, "noCard"-  
        no card detected, "processing"-processing*/  
        "cardErrorCode":  
        /*dependent, int, internal error code of card operation*/  
    }  
}
```

JSON_CustomDataResult

JSON message about the results of searching for custom card information

```
{  
    "CustomDataResult":{  
        "status":"ok",  
        /*required, string, card issuing status: "ok"-succeeded, "failed"-operation  
        failed, "timeout"-timed out, "verifyFailure"-authentication failed, "noCard"-  
        no card detected, "processing"-processing*/  
        "cardErrorCode":0,  
        /*dependent, int, internal error code of card operation. This node is valid  
        when the value of status is "failed"*/  
        "length":1,  
        /*dependent, int, length of the source data that has been read, unit: byte.  
        This node is valid when the value of status is "ok"*/  
        "data":""  
        /*dependent, string, card information encoded by Base64. This node is valid  
        when the value of status is "ok"*/  
    }  
}
```

JSON_CustomDataSearchCond

JSON message about condition parameters of searching for custom card information

```
{  
    "CustomDataSearchCond":{  
        "address":1,  
        /*optional, int, start address for reading data. By default the data will be  
        read from the start address*/  
        "length":1  
        /*optional, int, length of the data that can be read, it is 0 by default, unit:  
        byte*/  
    }  
}
```

JSON_DataBlock

JSON message about data block details

```
{  
    "DataBlock": {  
        "addressOfBlock": ,  
        /*optional, integer, block address*/  
        "data": "",  
        /*required, string, a hexBinary character string, i.e.,  
        "f2345678abf2345678abf2345678abf2"*/  
    }  
}
```

```
    }
}
```

JSON_DataBlockCtrl

JSON message about operation parameters of data block

```
{
  "DataBlockCtrl": {
    "addressOfBlock": ,
    /*required, integer, block address*/
    "command":"",
    /*required, string, control commands: "add, minus, copy, paste"*/
    "value":,
    /*depend, integer, relative value to be changed, this field is value only when
the command is set to "add" or "minus"*/
  }
}
```

JSON_DataCollections

JSON message about the parameters of downloaded data collected offline

```
{
  "DataCollections":{
    "dataType ":"binary",
    /*required, string, data type of the file: "url"-URL, "binary"-binary data*/
    "progress":0,
    /*required, int, file preparation progress. When it is 100, the data or the
field fileUrl will be parsed*/
    "fileUrl": ""
    /*dependent, string, file URL, this field is valid when the value of dataType
is "url"*/
  }
}
```

JSON_DataCollectionsCond

JSON message about the conditions of downloading data collected offline

```
{
  "DataCollectionsCond":{
    "id":"",
    /*required, string, downloading ID, which is used to check whether it is the
same request*/
    "dataType ":"binary",
    /*required, string, data type of the file: "url", "binary"-binary data*/
  }
}
```

```
    "password ":""
/*required, string, password*/
}
}
```

JSON_DataOutputCfg

DataOutputCfg message in JSON format

```
{
  "DataOutputCfg":{
    "password":"",
/*required, string, password for exporting*/
    "type":""
/*optional, string, exporting type: "UsbDisk"-exporting via USB flash drive,
"UsbPrivate"-exporting via private USB, "ISAPI"-exporting via ISAPI*/
  }
}
```

JSON_DataOutputProgress

DataOutputProgress message in JSON format

```
{
  "DataOutputProgress":{
    "progress":
/*required, integer, exporting progress*/
  }
}
```

JSON_DataTrans

JSON message about data package to be passed through

```
{
  "DataTrans": {
    "content": ""
/*required, string, data to be passed through, which is encoded by Base64*/
  }
}
```

JSON_RuleInfo

RuleInfo message in JSON format

```
{  
    "RuleInfo": {  
        "reqAdminRights": ,  
        /*required, boolean, whether the administrator permission is required: "true"-yes, "false"-no*/  
        "enableCardNoLenAuto": ,  
        /*optional, boolean, whether to enable length self-adaption of the card serial No. The priority of this field is higher than len*/  
        "RuleList": [{  
            /*rule list, which contains rules for collecting different types of data*/  
            "dataType": "",  
            /*required, string, data type: "name", "employeeNo"-employee No., "IDCardNo"-ID card No., "IDCardSerialNo"-ID card serial No., "IDCardDetails"-ID card details, "card", "fingerprint"-fingerprint, "face"*/  
            "enable": ,  
            /*required, boolean, whether to collect and display: "true"-collect and display, "false"-not collect and display*/  
            "uniqueCheck": ,  
            /*dependency, boolean, whether to enable uniqueness verification: "true"-yes, "false" (default) or this field is not returned-no. This field is valid when dataType is "name". For other data types, this field is the read-only optional parameter*/  
            "len": ,  
            /*dependency, integer, data length, this field is valid when dataType is "name", "employeeNo" or "card". The default data length of name is 128. For other data types, this field is the read-only optional parameter. If it is not supported, this field will not be returned*/  
            "num": ,  
            /*dependency, integer, number of collected data, this field is valid when dataType is "fingerprint" or "card"*/  
            "fingerprintIDs":  
            /*dependency, integer, ID list of fingerprints that need to be collected, this field is valid when dataType is "fingerprint"*/  
        }],  
        "enableLocalIssueCard": true,  
        /*optional, boolean, whether to enable issuing smart cards locally*/  
        "isLocalStorage": false  
        /*optional, boolean, whether to store face picture and fingerprint information in the device locally*/  
    }  
}
```

JSON_DelFaceRecord

JSON message about the parameters of deleting face records

```
{  
    "FPID": [  
        /*array, list of face record ID, it is the same as the employee No. (person ID). Deleting multiple face records in a batch is supported*/
```

```
    "value":""  
/*required, string type, face record ID, the maximum length is 63 bytes*/  
    }]  
    "operateType": "byTerminal",  
/*optional, string, operation type: "byTerminal"-by terminal*/  
    "terminalNoList": [1]  
/*optional, array, terminal ID list, this node is required when operation type  
is "byTerminal"; currently, only one terminal is supported*/  
}
```

JSON_DoorStatusHolidayGroupCfg

DoorStatusHolidayGroupCfg message in JSON format

```
{  
    "DoorStatusHolidayGroupCfg": {  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "groupName": "",  
/*required, string, holiday group name*/  
        "holidayPlanNo" : ""  
/*required, string, holiday group schedule No.*/  
    }  
}
```

JSON_DoorStatusHolidayPlanCfg

DoorStatusHolidayPlanCfg message in JSON format

```
{  
    "DoorStatusHolidayPlanCfg":{  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "beginDate": "",  
/*required, start date of the holiday*/  
        "endDate": "",  
/*required, end data of the holiday*/  
        "HolidayPlanCfg":[]  
/*required, holiday schedule parameters*/  
        "id": ,  
/*required, integer, time period No., which is between 1 and 8*/  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "doorStatus": "",  
/*required, string, door status: "remainOpen"-remain open (access without  
authentication), "remainClosed"-remain closed (access is not allowed), "normal"-  
access by authentication, "sleep", "invalid"*/  
        "TimeSegment":{  
            "beginTime": "",  
            "endTime": "",  
            "interval": "",  
            "repeat": "",  
            "repeatCount": "",  
            "repeatUnit": ""  
        }  
    }  
}
```

```
/*required, start time of the time period (device local time)*/  
    "endTime":""  
/*required, end time of the time period (device local time)*/  
    }  
    }]  
}  
}
```

JSON_DoorStatusPlan

DoorStatusPlan message in JSON format

```
{  
    "DoorStatusPlan": {  
        "templateNo":  
/*required, integer, schedule template No.: 0-cancel linking the template with  
the schedule and restore to the default status (normal status)*/  
    }  
}
```

JSON_DoorStatusPlanTemplate

DoorStatusPlanTemplate message in JSON format

```
{  
    "DoorStatusPlanTemplate": {  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "templateName": "",  
/*required, string, template name*/  
        "weekPlanNo" : ,  
/*required, integer, week schedule No.*/  
        "holidayGroupNo" : ""  
/*required, string, holiday group No.*/  
    }  
}
```

JSON_DoorStatusWeekPlanCfg

DoorStatusWeekPlanCfg message in JSON format

```
{  
    "DoorStatusWeekPlanCfg":{  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "WeekPlanCfg":[]  
/*required, week schedule parameters*/  
}
```

```
        "week": "",  
/*required, string, days of the week: "Monday", "Tuesday", "Wednesday",  
"Thursday", "Friday", "Saturday", "Sunday"*/  
        "id": ,  
/*required, integer, time period No., which is between 1 and 8*/  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "doorStatus": "",  
/*required, sting, door status: "remainOpen"-remain open (access without  
authentication), "remainClosed"-remain closed (access is not allowed), "normal"-  
access by authentication, "sleep", "invalid"*/  
        "TimeSegment": {  
            "beginTime": "",  
/*required, start time of the time period (device local time)*/  
            "endTime": ""  
/*required, end time of the time period (device local time)*/  
        }  
    }  
}
```

JSON_EditFaceRecord

Message about the condition message of editing a face record, and it is in JSON format.

```
{  
    "faceURL": "",  
/*optional, face picture URL, string type, the maximum size is 256 bytes*/  
    "name": "",  
/*required, name of person in the face picture, string type, the maximum size  
is 96 bytes*/  
    "gender": "",  
/*optional, gender of person in the face picture: male, female, unknown, string  
type, the maximum size is 32 bytes*/  
    "bornTime": "",  
/*required, birthday of person in the face picture, ISO8601 time format, string  
type, the maximum size is 20 bytes*/  
    "city": "",  
/*optional, city code of birth for the person in the face picture, string type,  
the maximum size is 32 bytes*/  
    "certificateType": "",  
/*optional, string type, the maximum size is 10 bytes, certificate type:  
"officerID"-officer ID, "ID"-identify card, passport, other*/  
    "certificateNumber": "",  
/*optional, certificate No., string, the maximum size is 32 bytes*/  
    "caseInfo": "",  
/*optional, case information, string type, the maximum size is 192 bytes, it is  
valid when faceLibType is blackFD*/  
    "tag": "",  
/*optional, custom tag, up to 4 tags, which are separated by commas, string  
type, the maximum size is 195 bytes. It is valid when faceLibType is blackFD*/
```

```
    "address": "",  
    /*optional, person address, string type, the maximum size is 192 bytes, it is  
    valid when faceLibType is staticFD.*/  
    "customInfo": "",  
    /*optional, custom information, string type, the maximum size is 192 bytes, it  
    is valid when faceLibType is staticFD.*/  
    "modelData": ""  
    /*optional, string type, target model data, non-modeled binary data needs to be  
    encrypted by base64 during transmission*/  
    "rowKey ":"",  
    /*optional, string type, face picture library main key. Search by rowKey can be  
    more efficient, the maximum size is 64 bytes*/  
    "transfer":true,  
    /*optional, boolean type, whether to enable transfer*/  
    "PicFeaturePoints":[]  
    /*optional, array of object, feature points to be applied. If the device only  
    supports three types of feature points, when the platform applies more than  
    three types of feature points, the device will not return error information*/  
        "featurePointType":"face",  
        /*required, string, feature point type: "face", "leftEye" (left eye),  
        "rightEye" (right eye), "leftMouthCorner" (left corner of mouth),  
        "rightMouthCorner" (right corner of mouth), "nose"*/  
        "coordinatePoint":{  
            /*required, object, coordinates of the feature point*/  
            "x":1,  
            /*required, int, normalized X-coordinate which is between 0 and 1000*/  
            "y":1,  
            /*required, int, normalized Y-coordinate which is between 0 and 1000*/  
            "width":1,  
            /*required, int, width which is between 0 and 1000. This node is required when  
            featurePointType is "face"*/  
            "height":1  
            /*required, int, height which is between 0 and 1000. This node is required when  
            featurePointType is "face"*/  
        }  
    },  
    "saveFacePic": true  
    /*optional, boolean, whether to save face pictures*/  
}
```

JSON_EditFPlibInfo

Message about the editing information of face picture library, and it is in JSON format.

```
{  
    "name": "",  
    /*optional, face picture library name, string type, the max. string length is  
    48 bytes*/  
    "customInfo": "",  
    /*optional, custom information, it is used to indicate the data property or  
    uniqueness, string type, the max. string length is 192 bytes*/
```

```
    "libArmingType": "armingLib",
/*optional, string, arming type of the list library: "armingLib" (armed face
picture library), "nonArmingLib" (not armed face picture library). The default
value is "armingLib"*/
    "libAttribute": "blackList"
/*optional, string, library type: "blackList" (blocklist library), "VIP" (VIP
library), "passerby" (passerby library). The passerby library cannot be
deleted*/
}
```

JSON_EventCardLinkageCfg

EventCardLinkageCfg message in JSON format

```
{
    "EventCardLinkageCfg": {
        "proMode": "",
/*required, string, linkage type: "event"-event linkage, "card"-card linkage,
"mac"-MAC address linkage, "employee"-employee No. (person ID)*/
        "EventLinkageInfo":{
/*optional, event linage parameters, it is valid when proMode is "event"*/
            "mainEventType": ,
/*optional, integer, major event type: 0-device event, 1-alarm input event, 2-
access control point event, 3-authentication unit (card reader, fingerprint
module) event*/
            "subEventType": ,
/*optional, integer, minor event type, refer to Event Linkage Types for
details*/
            },
        "CardNoLinkageInfo": {
/*optional, card linkage parameters, it is valid when proMode is "card"*/
            "cardNo": ""
/*optional, string, card No.*/
            },
        "MacAddrLinkageInfo": {
/*optional, MAC address linkage parameters, it is valid when proMode is "mac"*/
            "MACAddr": ""
/*optional, string, physical MAC address*/
            },
        "EmployeeInfo": {
/*optional, employee No. (person ID) linkage parameters, it is valid when
proMode is "employee"*/
            "employeeNo": ""
/*optional, string, employee No. (person ID)*/
            },
        "eventSourceID": ,
/*optional, integer, event source ID, it is valid when proMode is "event",
65535-all. For device event (mainEventType is 0), this field is invalid; for
access control point event (mainEventType is 2), this field refers to the
access control point No.; for authentication unit event (mainEventType is 3,
this field refers to the authentication unit No.; for alarm input event
            }
    }
}
```

```
(mainEventType is 1), this field refers to the zone alarm input ID or the event
alarm input ID*/
    "alarmout": ,
/*optional, array, linked alarm output No., e.g., [1,3,5]: 1-linked alarm
output No.1; 3-linked alarm output No.3; 5-linked alarm output No.5*/
    "openDoor": ,
/*optional, array, linked door No. to open, e.g., [1,3,5]: 1-linked door No.1;
3-linked door No.3; 5-linked door No.5*/
    "closeDoor": ,
/*optional, array, linked door No. to close, e.g., [1,3,5]: 1-linked door No.1;
3-linked door No.3; 5-linked door No.5*/
    "alwaysOpen": ,
/*optional, array, linked door No. to remain unlocked, e.g., [1,3,5]: 1-linked
door No.1; 3-linked door No.3; 5-linked door No.5*/
    "alwaysClose": ,
/*optional, array, linked door No. to remain locked, e.g., [1,3,5]: 1-linked
door No.1; 3-linked door No.3; 5-linked door No.5*/
    "mainDevBuzzer": ,
/*optional, boolean, whether to enable buzzer linkage of the access controller
(start buzzing): "false"-no, "true"-yes*/
    "capturePic": ,
/*optional, boolean, whether to enable capture linkage: "false"-no, "true"-yes*/
    "recordVideo": ,
/*optional, boolean, whether to enable recording linkage: "false"-no, "true"-yes*/
    "mainDevStopBuzzer": ,
/*optional, boolean, whether to enable buzzer linkage of access controller
(stop buzzing): "false"-no, "true"-yes*/
    "audioDisplayID": ,
/*optional, integer, linked audio announcement ID, which is between 1 and 32: 0-
not link*/
    "audioDisplayMode": "",
/*optional, integer, linked audio announcement mode: "close", "single", "loop"*/
    "readerBuzzer": ,
/*optional, array, linked buzzer No., e.g, [1,3,5]: 1-buzzer No.1, 3-buzzer No.
3, 5-buzzer No.5*/
    "alarmOutClose": ,
/*optional, array, linked alarm output No. to disable, e.g, [1,3,5]: 1-alarm
output No.1, 3-alarm output No.3, 5-alarm output No.5*/
    "alarmInSetup": ,
/*optional, array, linked zone No. to arm, e.g, [1,3,5]: 1-zone No.1, 3-zone No.
3, 5-zone No.5*/
    "alarmInClose": ,
/*optional, array, linked zone No. to disarm, e.g, [1,3,5]: 1-zone No.1, 3-zone
No.3, 5-zone No.5*/
    "readerStopBuzzer": ,
/*optional, array, linked buzzer No. to stop buzzing, e.g, [1,3,5]: 1-buzzer No.
1, 3-buzzer No.3, 5-buzzer No.*/
}
```

See Also

[Event Linkage Types](#)

JSON_EventCardNoList

EventCardNoList message in JSON format

```
{  
    "EventCardNoList":{  
        "id":  
/*required, array, list of configured event and card linkage ID, e.g., [1,2,3]  
indicates that the device is configured with event linkage 1, 2, and 3*/  
    }  
}
```

JSON_EventNotificationAlert_AccessControllerEvent

The access control event information is uploaded in JSON format of EventNotificationAlert message.

Access Control Event Message With Binary Picture Data

```
Content-Type:multipart/form-data;boundary=MIME_boundary  
--MIME_boundary  
Content-Type: application/json  
Content-Length:480  
{  
    "ipAddress": "",  
/*required, string, IP address of the alarm device, the maximum size is 32  
bytes*/  
    "ipv6Address": "",  
/*optional, string, IPv6 address of the alarm device, the maximum size is 128  
bytes*/  
    "portNo": ,  
/*optional, integer32, port No. of the alarm device*/  
    "protocol": "",  
/*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32  
bytes*/  
    "macAddress": "",  
/*optional, string, MAC address, the maximum size is 32 bytes*/  
    "channelID": ,  
/*optional, integer32, device channel No. that triggered the alarm*/  
    "dateTime": "",  
/*required, string, time when the alarm is triggered (UTC time), the maximum  
size is 32 bytes*/  
    "activePostCount": ,  
/*required, integer32, number of times that the same alarm has been uploaded*/
```

```
"eventType": "",  
/*required, string, triggered event type, here it should be set to  
"AccessControllerEvent", and the maximum size is 128 bytes*/  
"eventState": "",  
/*required, string, event triggering status: "active"-triggered, "inactive"-not  
triggered, the maximum size is 32 bytes*/  
"eventDescription": "",  
/*required, string, event description*/  
"deviceID": "",  
/*optional, string, device No.*/  
"AccessControllerEvent":{  
    "deviceName": "",  
/*optional, string, device name*/  
    "majorEventType": ,  
/*required, int, major alarm/event types (the type value should be converted to  
a decimal number for transmission), see Access Control Event Types for details*/  
    "subEventType": ,  
/*required, int, minor alarm/event types (the type value should be converted to  
a decimal number for transmission), see Access Control Event Types for details*/  
    "inductiveEventType": "",  
/*optional, string, inductive event type. This field is used by storage  
devices; for access control devices, this field is invalid*/  
    "netUser": "",  
/*optional, string, user name for network operations*/  
    "remoteHostAddr": "",  
/*optional, string, remote host address*/  
    "cardNo": "",  
/*optional, string, card No.*/  
    "cardType": ,  
/*optional, int, card type: 1-normal card, 2-disability card, 3-blocklist card,  
4-patrol card, 5-duress card, 6-super card, 7-visitor card, 8-dismiss card*/  
    "name": "",  
/*optional, string, person name*/  
    "whiteListNo": ,  
/*optional, int, allowlist No., which is between 1 and 8*/  
    "reportChannel": ,  
/*optional, int, alarm/event uploading channel type: 1-uploading in arming  
mode, 2-uploading by central group 1, 3-uploading by central group 2*/  
    "cardReaderKind": ,  
/*optional, int, reader type: 1-IC card reader, 2-ID card reader, 3-QR code  
scanner, 4-fingerprint module*/  
    "cardReaderNo": ,  
/*optional, int, reader No.*/  
    "doorNo": ,  
/*optional, int, door or floor No.*/  
    "verifyNo": ,  
/*optional, int, multiple authentication No.*/  
    "alarmInNo": ,  
/*optional, int, alarm input No.*/  
    "alarmOutNo": ,  
/*optional, int, alarm output No.*/  
    "caseSensorNo": ,
```

```
/*optional, int, event trigger No.*/
    "RS485No": ,
/*optional, int, RS-485 channel No.*/
    "multiCardGroupNo": ,
/*optional, int, group No.*/
    "accessChannel": ,
/*optional, int, turnstile No.*/
    "deviceNo": ,
/*optional, int, device No.*/
    "distractControlNo": ,
/*optional, int, distributed access controller No.*/
    "employeeNo": ,
/*optional, int, employee No. (person ID)*/
    "employeeNoString": "",
/*optional, string, employee No. (person ID). If the field employeeNo exists or
the value of employeeNoString can be converted to that of employeeNo, this
field is required. For the upper-layer platform or client software, the field
employeeNoString will be parsed in prior; if employeeNoString is not
configured, the field employeeNo will be parsed*/
    "localControllerID": ,
/*optional, int, distributed access controller No.: 0-access controller, 1 to
64-distributed access controller No. 1 to distributed access controller No. 64*/
    "InternetAccess": ,
/*optional, int, network interface No.: 1-upstream network interface No. 1, 2-
upstream network interface No. 2, 3-downstream network interface No. 1*/
    "type": ,
/*optional, int, zone type: 0-instant zone, 1-24-hour zone, 2-delayed zone, 3-
internal zone, 4-key zone, 5-fire alarm zone, 6-perimeter zone, 7-24-hour
silent zone, 8-24-hour auxiliary zone, 9-24-hour shock zone, 10-emergency door
open zone, 11-emergency door closed zone, 255-none*/
    "MACAddr": "",
/*optional, string, physical address*/
    "swipeCardType": ,
/*optional, int, card swiping types: 0-invalid, 1-QR code*/
    "serialNo": ,
/*optional, int, event serial No., which is used to check whether the event
loss occurred*/
    "channelControllerID": ,
/*optional, int, lane controller ID: 1-main lane controller, 2-sub-lane
controller*/
    "channelControllerLampID": ,
/*optional, int, light board ID of the lane controller, which is between 1 and
255*/
    "channelControllerIRAdaptorID": ,
/*optional, int, IR adaptor ID of the lane controller, which is between 1 and
255*/
    "channelControllerIREmitterID": ,
/*optional, int, active infrared intrusion detector No. of the lane controller,
which is between 1 and 255*/
    "userType": "",
/*optional, string, person type: "normal"-normal person (resident), "visitor"-_
visitor, "blacklist"-person in the blocklist, "administrators"-administrator*/
```

```
"currentVerifyMode": ,  
/*optional, string, current authentication mode of the reader: "cardAndPw"-card  
+password, "card"-card, "cardOrPw"-card or password, "fp"-fingerprint,  
"fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-  
fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password,  
"faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face  
+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face"-face,  
"employeeNoAndPw"-employee No.+password, "fpOrPw"-fingerprint or password,  
"employeeNoAndFp"-employee No.+fingerprint, "employeeNoAndFpAndPw"-employee No.  
+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card,  
"faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee No.  
+face, "faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face,  
"cardOrfaceOrPw"-card or face or password, "cardOrFace"-card or face,  
"cardOrFaceOrFp"-card or face or fingerprint, "cardOrFpOrPw"-card or  
fingerprint or password*/  
    "currentEvent": ,  
/*optional, boolean, whether it is a real-time event: true-yes (real-time  
event), false-no (offline event)*/  
    "QRCodeInfo": "",  
/*optional, string, QR code information*/  
    "thermometryUnit": "",  
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheith"-  
Fahrenheit, "kelvin"-Kelvin*/  
    "currTemperature": ,  
/*optional, float, face temperature which is accurate to one decimal place*/  
    "isAbnormalTemperature": ,  
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-  
no*/  
    "RegionCoordinates": {  
/*optional, face temperature's coordinates*/  
        "positionX": ,  
/*optional, int, normalized X-coordinate which is between 0 and 1000*/  
        "positionY":  
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/  
        },  
    "remoteCheck": ,  
/*optional, boolean, whether remote verification is required: true-yes, false-  
no (default)*/  
    "mask": "",  
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-  
wearing mask, "no"-not wearing mask*/  
    "helmet": "",  
/*optional, string, whether the person is wearing hard hat: "unknown", "yes"-  
wearing hard hat, "no"-not wearing hard hat*/  
    "frontSerialNo": ,  
/*optional, int, the previous event's serial No. If this field does not exist,  
the platform will check whether the event loss occurred according to the field  
serialNo. If both the serialNo and frontSerialNo are returned, the platform  
will check whether the event loss occurred according to both fields. It is  
mainly used to solve the problem that the serialNo is inconsistent after  
subscribing events or alarms*/  
    "deviceId": ,
```

```
/*optional, string, device's long No., e.g., "10000000101"*/
    "attendanceStatus": "",  
/*optional, string, attendance status: "undefined", "checkIn"-check in,
"checkOut"-check out, "breakOut"-break out, "breakIn"-break in, "overtimeIn"-
overtime in, "overTimeOut"-overtime out*/
    "statusValue": ,  
/*optional, int, status value*/
    "label": "",  
/*optional, string, custom attendance name*/
    "pictureURL": "test",
/*optional, string, captured picture URL, size range: [0,256]*/
    "visibleLightURL": "test",
/*optional, string, URL of picture captured by visible light channel, size
range: [0,256]*/
    "thermalURL": "test",
/*optional, string, URL of picture captured by thermal imaging channel, size
range: [0,256]*/
    "picturesNumber": ,
/*optional, int, number of captured pictures if the capture linkage action is
configured. This field will be 0 or not be returned if there is no picture*/
    "purePwdVerifyEnable": ,
/*optional, boolean, whether the device supports opening the door only by
password: true-yes, this field is not returned-no. The password used to open
the door is the value of the field password in the message
JSON UserInfo
*/
/*For opening the door only by password: 1. The password in "XXX or password"
in the authentication mode refers to the person's password (the value of the
field password in
JSON UserInfo
);
2. The device will not check
the duplication of the password, and the upper platform should ensure that the
password is unique; 3. The password cannot be added, deleted, edited, or
searched for on the device locally*/
    "HealthInfo": {
/*optional, object, health information*/
        "healthCode": 1,
/*optional, int, health code status: 0 (no request), 1 (no health code), 2
(green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6
(other error, e.g., searching failed due to API exception), 7 (searching for
the health code timed out)*/
        "NADCode": 1,
/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which
means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/
        "travelCode": 1,
/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in
the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3
(other)*/
        "vaccineStatus": 1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1
(vaccinated)*/
    }
```

```
}

--MIME_boundary
Content-Disposition: form-data; name="Picture"; filename="Picture.jpg";  //
Captured picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: pictureImage

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="VisibleLight";
filename="VisibleLight.jpg"; //Data of the visible light picture captured by
the thermal camera
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: visibleLight_image

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="Thermal"; filename="Thermal.jpg"; //
Thermal picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: thermal_image

fefefwageegfqaeg...
--MIME_boundary
```

Access Control Event Message With Picture URL

```
{
    "ipAddress": "",  
/*required, string, IP address of the alarm device, the maximum size is 32  
bytes*/
    "ipv6Address": "",  
/*optional, string, IPv6 address of the alarm device, the maximum size is 128  
bytes*/
    "portNo": ,  
/*optional, integer32, port No. of the alarm device*/
    "protocol": "",  
/*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32  
bytes*/
    "macAddress": "",  
/*optional, string, MAC address, the maximum size is 32 bytes*/
    "channelID": ,  
/*optional, integer32, device channel No. that triggered the alarm*/
    "dateTime": "",  
/*required, string, time when the alarm is triggered (UTC time), the maximum  
size is 32 bytes*/
    "activePostCount": ,  
/*required, integer32, number of times that the same alarm has been uploaded*/
```

```
"eventType": "",  
/*required, string, triggered event type, here it should be set to  
"AccessControllerEvent", and the maximum size is 128 bytes*/  
"eventState": "",  
/*required, string, event triggering status: "active"-triggered, "inactive"-not  
triggered, the maximum size is 32 bytes*/  
"eventDescription": "",  
/*required, string, event description*/  
"deviceID": "",  
/*optional, string, device No.*/  
"AccessControllerEvent":{  
    "deviceName": "",  
/*optional, string, device name*/  
    "majorEventType": ,  
/*required, int, major alarm/event types (the type value should be converted to  
a decimal number for transmission), see Access Control Event Types for details*/  
    "subEventType": ,  
/*required, int, minor alarm/event types (the type value should be converted to  
a decimal number for transmission), see Access Control Event Types for details*/  
    "inductiveEventType": "",  
/*optional, string, inductive event type. This field is used by back-end  
devices; for access control devices, this field is invalid*/  
    "netUser": "",  
/*optional, string, user name for network operations*/  
    "remoteHostAddr": "",  
/*optional, string, remote host address*/  
    "cardNo": "",  
/*optional, string, card No.*/  
    "cardType": ,  
/*optional, int, card type: 1-normal card, 2-disability card, 3-blocklist card,  
4-patrol card, 5-duress card, 6-super card, 7-visitor card, 8-dismiss card*/  
    "name": "",  
/*optional, string, person name*/  
    "whiteListNo": ,  
/*optional, int, allowlist No., which is between 1 and 8*/  
    "reportChannel": ,  
/*optional, int, alarm/event uploading channel type: 1-uploading in arming  
mode, 2-uploading by central group 1, 3-uploading by central group 2*/  
    "cardReaderKind": ,  
/*optional, int, reader type: 1-IC card reader, 2-ID card reader, 3-QR code  
scanner, 4-fingerprint module*/  
    "cardReaderNo": ,  
/*optional, int, reader No.*/  
    "doorNo": ,  
/*optional, int, door or floor No.*/  
    "verifyNo": ,  
/*optional, int, multiple authentication No.*/  
    "alarmInNo": ,  
/*optional, int, alarm input No.*/  
    "alarmOutNo": ,  
/*optional, int, alarm output No.*/  
    "caseSensorNo": ,
```

```
/*optional, int, event trigger No.*/
    "RS485No": ,
/*optional, int, RS-485 channel No.*/
    "multiCardGroupNo": ,
/*optional, int, group No.*/
    "accessChannel": ,
/*optional, int, turnstile No.*/
    "deviceNo": ,
/*optional, int, device No.*/
    "distractControlNo": ,
/*optional, int, distributed access controller No.*/
    "employeeNo": ,
/*optional, int, employee No. (person ID)*/
    "employeeNoString": "",
/*optional, string, employee No. (person ID). If the field employeeNo exists or
the value of employeeNoString can be converted to that of employeeNo, this
field is required. For the upper-layer platform or client software, the field
employeeNoString will be parsed in prior; if employeeNoString is not
configured, the field employeeNo will be parsed*/
    "employeeName": "test",
/*optional, string, employee name. This node is only used for information
release devices, and both this node and the node name should be uploaded*/
    "localControllerID": ,
/*optional, int, distributed access controller No.: 0-access controller, 1 to
64-distributed access controller No. 1 to distributed access controller No. 64*/
    "InternetAccess": """",
/*optional, string, network interface No.: "1"-upstream network interface No.
1, "2"-upstream network interface No. 2, "3"-downstream network interface No.
1*/
    "type": ,
/*optional, int, zone type: 0-instant zone, 1-24-hour zone, 2-delayed zone, 3-
internal zone, 4-key zone, 5-fire alarm zone, 6-perimeter zone, 7-24-hour
client zone, 8-24-hour auxiliary zone, 9-24-hour shock zone, 10-emergency door
open zone, 11-emergency door closed zone, 255-none*/
    "MACAddr": "",
/*optional, string, physical address*/
    "swipeCardType": ,
/*optional, int, card swiping types: 0-invalid, 1-QR code*/
    "serialNo": ,
/*optional, int, event serial No., which is used to check whether the event
loss occurred*/
    "channelControllerID": ,
/*optional, int, lane controller ID: 1-main lane controller, 2-sub lane
controller*/
    "channelControllerLampID": ,
/*optional, int, light board ID of the lane controller, which is between 1 and
255*/
    "channelControllerIRAdaptorID": ,
/*optional, int, IR adaptor ID of the lane controller, which is between 1 and
255*/
    "channelControllerIREmitterID": ,
/*optional, int, active infrared intrusion detector No. of the lane controller,
```

```
which is between 1 and 255*/
    "userType": "",  
/*optional, string, person type: "normal"-normal person (resident), "visitor"-visitor, "blacklist"-person in the blocklist, "administrators"-administrator*/
    "currentVerifyMode": "",  
/*optional, string, current authentication mode of the reader: "cardAndPw"-card+password, "card"-card, "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password, "faceAndCard"-face+card, "face"-face, "employeeNoAndPw"-employee No.+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint, "employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint, "cardOrFpOrPw"-card or fingerprint or password*/
    "currentEvent": ,  
/*optional, boolean, whether it is a real-time event: true-yes (real-time event), false-no (offline event)*/
    "QRCodeInfo": "",  
/*optional, string, QR code information*/
    "thermometryUnit": "",  
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
    "currTemperature": ,  
/*optional, float, face temperature which is accurate to one decimal place*/
    "isAbnormalTemperature": ,  
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
    "RegionCoordinates": {
/*optional, face temperature's coordinates*/
        "positionX": ,  
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
        "positionY": ,  
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
        },
    "remoteCheck": ,  
/*optional, boolean, whether remote verification is required: true-yes, false-no (default)*/
    "mask": "",  
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
    "helmet": "",  
/*optional, string, whether the person is wearing hard hat: "unknown", "yes"-wearing hard hat, "no"-not wearing hard hat*/
    "frontSerialNo": ,  
/*optional, int, the previous event's serial No. If this field does not exist, the platform will check whether the event loss occurred according to the field serialNo. If both the serialNo and frontSerialNo are returned, the platform
```

```

will check whether the event loss occurred according to both fields. It is
mainly used to solve the problem that the serialNo is inconsistent after
subscribing events or alarms*/
    "attendanceStatus": "",  

/*optional, string, attendance status: "undefined", "checkIn"-check in,  

"checkOut"-check out, "breakOut"-break out, "breakIn"-break in, "overtimeIn"-  

overtime in, "overTimeOut"-overtime out*/
    "statusValue": ,  

/*optional, int, status value*/
    "label": "",  

/*optional, string, custom attendance name*/
    "pictureURL": "",  

/*optional, string, captured picture URL*/
    "deviceId": ,  

/*optional, string, device's long No., e.g., "10000000101"*/
    "visibleLightURL": "",  

/*optional, string, URL of the visible light picture captured by the thermal  

camera*/
    "thermalURL": "",  

/*optional, string, thermal picture URL*/
    "picturesNumber": ,  

/*optional, int, number of captured pictures if the capture linkage action is  

configured. This field will be 0 or not be returned if there is no picture*/
    "purePwdVerifyEnable": ,  

/*optional, boolean, whether the device supports opening the door only by  

password: true-yes, this field is not returned-no. The password used to open  

the door is the value of the field password in the message

```

JSON UserInfo

*/

/*For opening the door only by password: 1. The password in "XXX or password" in the authentication mode refers to the person's password (the value of the field **password** in

JSON UserInfo

); 2. The device will not check the duplication of the password, and the upper platform should ensure that the password is unique; 3. The password cannot be added, deleted, edited, or searched for on the device locally*/

```

    "HealthInfo": {
/*optional, object, health information*/
        "healthCode": 1,  

/*optional, int, health code status: 0 (no request), 1 (no health code), 2  

(green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6  

(other error, e.g., searching failed due to API exception), 7 (searching for  

the health code timed out)*/
        "NADCode": 1,  

/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which  

means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/
        "travelCode": 1,  

/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in  

the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3  

(other)*/
        "vaccineStatus": 1
    }

```

```
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1  
(vaccinated)*/
    }
}
}
```

See Also

[Access Control Event Types](#)

Example

Interaction Example of Uploading Access Control Event with Pictures in Arming Mode

```
HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type:multipart/form-data;boundary=MIME_boundary

--MIME_boundary
Content-Type: application/json
Content-Length:480

<alarm message in JSON format>
--MIME_boundary
Content-Disposition: form-data; name="Picture"; filename="Picture.jpg"; //
Captured picture data
Content-Type:image/jpeg
Content-Length:516876
Content-ID: pictureImage

fefefwageegfqaeg...
--MIME_boundary
Content-Type: application/json
Content-Length:480

<next alarm message in JSON format>
--MIME_boundary
Content-Disposition: form-data; name="Picture"; filename="Picture.jpg"
Content-Type:image/jpeg
Content-Length:516876

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="VisibleLight";
filename="VisibleLight.jpg"; //Data of the visible light picture captured by
the thermal camera
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: visibleLight_image

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="Thermal"; filename="Thermal.jpg"; //
```

```
Thermal picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: thermal_image

fefefwageegfqaeg...
--MIME_boundary
```

JSON_EventNotificationAlert_Alarm/EventInfo

EventNotificationAlert message with alarm or event information in JSON format.

```
{
    "ipAddress": "",  
/*required, device IPv4 address , string, the maximum size is 32 bytes*/
    "ipv6Address": "",  
/*optional, device IPv6 address, string, the maximum size is 128 bytes*/
    "portNo": ,  
/*optional, device port No., integer32*/
    "protocol": "",  
/*optional, protocol type, "HTTP, HTTPS", string, the maximum size is 32 bytes*/
    "macAddress": "",  
/*optional, MAC address, string, the maximum size is 32 bytes, e.g.,
01:17:24:45:D9:F4*/
    "channelID": "",  
/*optional, device channel No., integer32*/
    "dateTime": "",  
/*optional, string, alarm/event triggered or occurred time based on ISO8601,
the maximum size is 32 bytes, e.g., 2009-11-14T15:27Z*/
    "activePostCount": "",  
/*required, alarm/event frequency, integer32*/
    "eventType": "",  
/*required, alarm/event type, "captureResult, faceCapture,...", string, the
maximum size is 128 bytes*/
    "eventState": "",  
/*required, string, the maximum size is 32 bytes, durative alarm/event status:
"active"-valid, "inactive"-invalid*/
    "eventDescription": "",  
/*required, event description, string, the maximum size is 128 bytes*/
    "deviceID": "",  
/*string type, device ID*/
    "uuid": "",  
/*string type, event UUID, which is used to uniquely identify an event, the
standard UUID format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx*/
    ...
/*optional, for different alarm/event types, the nodes are different, see the
message examples in different applications*/
}
```

JSON_EventNotificationAlert_FaceTempScreeningEventMsg

The event information of face temperature screening is uploaded in JSON format of EventNotificationAlert message.

Event Message of Face Temperature Screening with Binary Picture Data

```
{  
    "ipAddress": "",  
    /*required, string, IP address of the alarm device, the maximum size is 32  
    bytes*/  
    "ipv6Address": "",  
    /*optional, string, IPv6 address of the alarm device, the maximum size is 128  
    bytes*/  
    "portNo": ,  
    /*optional, integer32, port No. of the alarm device*/  
    "protocol": "",  
    /*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32  
    bytes*/  
    "macAddress": "",  
    /*optional, string, MAC address, the maximum size is 32 bytes*/  
    "channelID": ,  
    /*optional, integer32, device channel No. that triggered the alarm*/  
    "dateTime": "",  
    /*required, string, time when the alarm is triggered (UTC time), the maximum  
    size is 32 bytes*/  
    "activePostCount": ,  
    /*required, integer32, number of times that the same alarm has been uploaded*/  
    "eventType": "",  
    /*required, string, triggered event type, here it should be set to  
    "FaceTemperatureMeasurementEvent", the maximum size is 128 bytes*/  
    "eventState": "",  
    /*required, string, event triggering status: "active"-triggered, "inactive"-not  
    triggered, the maximum size is 32 bytes*/  
    "eventDescription": "",  
    /*required, string, event description*/  
    "FaceTemperatureMeasurementEvent": {  
        "deviceName": "",  
        /*optional, string, device name*/  
        "serialNo": ,  
        /*optional, int, event serial No.*/  
        "currentEvent": ,  
        /*optional, boolean, whether it is a real-time event: true-yes (real-time  
        event), false-no (offline event)*/  
        "thermometryUnit": "",  
        /*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-  
        Fahrenheit, "kelvin"-Kelvin*/  
        "currTemperature": ,  
        /*optional, float, face temperature which is accurate to one decimal place*/  
        "isAbnormalTemperature": ,  
    }  
}
```

```
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
    "RegionCoordinates": {
/*optional, face temperature's coordinates*/
        "positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
        "positionY": ,
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
        },
        "remoteCheck": ,
/*optional, boolean, whether remote verification is required: true-yes, false-no (default)*/
        "mask": "",
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
        "helmet": ""
/*optional, string, whether the person wears a hard hat: "yes", "no",
"unknown"*/
        }
    }
--MIME_boundary
Content-Disposition: form-data; name="VisibleLight";
filename="VisibleLight.jpg"; //Data of the visible light picture captured by
the thermal camera
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: visibleLight_image

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="Thermal"; filename="Thermal.jpg"; //
Thermal picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: thermal_image

fefefwageegfqaeg...
--MIME_boundaryContent-Disposition: form-data; name="Picture";
filename="Picture.jpg"; //Captured picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: picture_image

fefefwageegfqaeg...
--MIME_boundary
```

Event Message of Face Temperature Screening with Picture URL

```
{
    "ipAddress": "",  
/*required, string, IP address of the alarm device, the maximum size is 32  
bytes*/
```

```
    "ipv6Address":"",
/*optional, string, IPv6 address of the alarm device, the maximum size is 128 bytes*/
    "portNo": ,
/*optional, integer32, port No. of the alarm device*/
    "protocol":"",
/*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32 bytes*/
    "macAddress":"",
/*optional, string, MAC address, the maximum size is 32 bytes*/
    "channelID": ,
/*optional, integer32, device channel No. that triggered the alarm*/
    "dateTime":"",
/*required, string, time when the alarm is triggered (UTC time), the maximum size is 32 bytes*/
    "activePostCount": ,
/*required, integer32, number of times that the same alarm has been uploaded*/
    "eventType":"",
/*required, string, triggered event type, here it should be set to "FaceTemperatureMeasurementEvent", the maximum size is 128 bytes*/
    "eventState":"",
/*required, string, event triggering status: "active"-triggered, "inactive"-not triggered, the maximum size is 32 bytes*/
    "eventDescription":"",
/*required, string, event description*/
    "deviceID": "test0123",
/*optional, string, device ID (PUID), which should be returned when the event message is uploaded via ISUP*/
    "FaceTemperatureMeasurementEvent":{
        "deviceName":"",
/*optional, string, device name*/
        "serialNo": ,
/*optional, int, event serial No.*/
        "currentEvent": ,
/*optional, boolean, whether it is a real-time event: true-yes (real-time event), false-no (offline event)*/
        "thermometryUnit":"",
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
        "currTemperature": ,
/*optional, float, face temperature which is accurate to one decimal place*/
        "isAbnormalTemperature": ,
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
        "RegionCoordinates":{
/*optional, face temperature's coordinates*/
            "positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
            "positionY": ,
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
        },
        "remoteCheck": ,
    }
}
```

```
/*optional, boolean, whether remote verification is required: true-yes, false-no (default)*/
    "mask":"",
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
    "visibleLightURL": "",
/*optional, string, URL of the visible light picture captured by the thermal camera*/
    "thermalURL": "",
/*optional, string, thermal picture URL*/
    "pictureURL": "",
/*optional, string, captured picture URL*/
    "helmet": ""
/*optional, string, whether the person wears a hard hat: "yes", "no",
"unknown"*/
}
}
```

JSON_EventNotificationAlert_IDCardInfoEvent

The event information of swiping ID card is uploaded in JSON format of EventNotificationAlert message.

Event Message of Swiping ID Card with Binary Picture Data

```
{
    "ipAddress":"",
/*required, string, IPv4 address of the alarm device, the maximum size is 32 bytes*/
    "ipv6Address":"",
/*optional, string, IPv6 address of the alarm device, the maximum size is 128 bytes*/
    "portNo": ,
/*optional, integer32, port No. of the alarm device*/
    "protocol":"",
/*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32 bytes*/
    "macAddress":"",
/*optional, string, MAC address, the maximum size is 32 bytes*/
    "channelID": ,
/*optional, integer32, device channel No. that triggered alarm*/
    "dateTime":"",
/*required, string, time when the alarm is triggered (UTC time), the maximum size is 32 bytes*/
    "activePostCount": ,
/*required, integer32, times that the same alarm has been uploaded*/
    "eventType":"",
/*required, string, triggered event type, here it should be set to "IDCardInfoEvent", the maximum size is 128 bytes*/
    "eventState": "",
```

```
/*required, string, event triggering status: "active"-triggered, "inactive"-not triggered, the maximum size is 32 bytes*/
    "eventDescription":"",
/*required, event description*/
    "IDCardInfoEvent":{
        "deviceName":"",
/*optional, string, device name*/
        "major": ,
/*required, int, major alarm type, the type value should be converted to a decimal number, see Access Control Event Types for details*/
        "minor": ,
/*required, int, minor alarm type, the type value should be converted to a decimal number, see Access Control Event Types for details*/
        "inductiveEventType":"",
/*optional, string, inductive event type. This field is used by back-end devices; for access control devices, this field is invalid*/
        "netUser":"",
/*optional, string, user name for network operations*/
        "remoteHostAddr":"",
/*optional, string, remote host address*/
        "cardType": ,
/*optional, int, card type: 1-normal card, 2-disability card, 3-blocklist card, 4-patrol card, 5-duress card, 6-super card, 7-visitor card, 8-dismiss card*/
        "cardReaderNo": ,
/*optional, int, card reader No.*/
        "doorNo": ,
/*optional, int, door No. (floor No)*/
        "deviceNo": ,
/*optional, int, device No.*/
        "serialNo": ,
/*optional, int, event serial No.*/
        "currentEvent": ,
/*optional, boolean, whether it is a real-time event: true-yes (real-time event), false-no (offline event)*/
        "QRCodeInfo":"",
/*optional, string, QR code information*/
        "thermometryUnit":"",
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
        "currTemperature": ,
/*optional, float, face temperature which is accurate to one decimal place*/
        "isAbnormalTemperature": ,
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
        "RegionCoordinates":{
/*optional, face temperature's coordinates*/
            "positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
            "positionY": ,
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
        },
        "remoteCheck": ,
```

```
/*optional, boolean, whether remote verification is required: true, false
(default)*/
    "mask":"",
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
    "frontSerialNo": ,
/*optional, int, the previous event's serial No. If this field does not exist, the platform will check whether the event loss occurred according to the field serialNo. If both the serialNo and frontSerialNo are returned, the platform will check whether the event loss occurred according to both fields. It is mainly used to solve the problem that the serialNo is inconsistent after subscribing events or alarms*/
    "IDCardInfo":{
        "name":"",
/*optional, string, name*/
        "sex":"",
/*optional, string, gender: "male", "female"*/
        "birth":"",
/*optional, string, date of birth, e.g., "1990-02-24"*/
        "addr":"",
/*optional, string, address*/
        "IDCardNo":"",
/*optional, string, ID card No.*/
        "issuingAuthority":"",
/*optional, string, issuing authority*/
        "startDate":"",
/*optional, string, start date of the effective period*/
        "endDate":"",
/*optional, string, end date of the effective period*/
        "isLongTermEffective":
/*optional, boolean, whether the effective period is permanent*/
        },
    "picturesNumber": ,
/*optional, int, number of pictures. If there is no picture, this node is set to 0 or is not returned*/
    "helmet": "",

/*optional, string, whether the person wears a hard hat: "yes", "no", "unknown"*/
    "HealthInfo": {
/*optional, object, health information*/
        "healthCode": 1,
/*optional, int, health code status: 0 (no request), 1 (no health code), 2 (green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6 (other error, e.g., searching failed due to API exception), 7 (searching for the health code timed out)*/
        "NADCode": 1,
/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/
        "travelCode": 1,
/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3 (other)*/
    }
```

```
        "vaccineStatus": 1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1
(vaccinated)*/
    }
}
--MIME_boundary
Content-Disposition: form-data; name="Picture"; filename="Picture.jpg"; //
Captured picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: pictureImage

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="IDCardPic";
filename="IDCardPic.jpg"; //ID card picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: IDCardPicImage

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="VisibleLight";
filename="VisibleLight.jpg"; //Data of the visible light picture captured by
the thermal camera
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: visibleLight_image

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="Thermal"; filename="Thermal.jpg"; //
Thermal picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: thermal_image

fefefwageegfqaeg...
--MIME_boundary
```

Event Message of Swiping ID Card with Picture URL

```
{
    "ipAddress":"",
/*required, string, IPv4 address of the alarm device, the maximum size is 32
bytes*/
    "ipv6Address":"",
/*optional, string, IPv6 address of the alarm device, the maximum size is 128
bytes*/
    "portNo": ,
/*optional, integer32, port No. of the alarm device*/
```

```
    "protocol":"",
/*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32
bytes*/
    "macAddress":"",
/*optional, string, MAC address, the maximum size is 32 bytes*/
    "channelID": ,
/*optional, integer32, device channel No. that triggered alarm*/
    "dateTime":"",
/*required, string, time when the alarm is triggered (UTC time), the maximum
size is 32 bytes*/
    "activePostCount": ,
/*required, integer32, times that the same alarm has been uploaded*/
    "eventType":"",
/*required, string, triggered event type, here it should be set to
"IDCardInfoEvent", the maximum size is 128 bytes*/
    "eventState":"",
/*required, string, event triggering status: "active"-triggered, "inactive"-not
triggered, the maximum size is 32 bytes*/
    "eventDescription":"",
/*required, event description*/
    "deviceID": "test0123",
/*optional, string, device ID (PUID), which should be returned when the event
message is uploaded via ISUP*/
    "IDCardInfoEvent":{
        "deviceName":"",
/*optional, string, device name*/
        "major": ,
/*required, int, major alarm type, the type value should be converted to a
decimal number, see Access Control Event Types for details*/
        "minor": ,
/*required, int, minor alarm type, the type value should be converted to a
decimal number, see Access Control Event Types for details*/
        "inductiveEventType":"",
/*optional, string, inductive event type. This field is used by back-end
devices; for access control devices, this field is invalid*/
        "netUser":"",
/*optional, string, user name for network operations*/
        "remoteHostAddr":"",
/*optional, string, remote host address*/
        "cardType": ,
/*optional, int, card type: 1-normal card, 2-disability card, 3-blocklist card,
4-patrol card, 5-duress card, 6-super card, 7-visitor card, 8-dismiss card*/
        "cardReaderNo": ,
/*optional, int, card reader No.*/
        "doorNo": ,
/*optional, int, door No. (floor No.)*/
        "deviceNo": ,
/*optional, int, device No.*/
        "serialNo": ,
/*optional, int, event serial No.*/
        "currentEvent": ,
/*optional, boolean, whether it is a real-time event: true-yes (real-time
```

```
event), false-no (offline event)*/  
    "QRCodeInfo": "",  
/*optional, string, QR code information*/  
    "thermometryUnit": "",  
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-  
Fahrenheit, "kelvin"-Kelvin*/  
    "currTemperature": ,  
/*optional, float, face temperature which is accurate to one decimal place*/  
    "isAbnormalTemperature": ,  
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-  
no*/  
    "RegionCoordinates": {  
/*optional, face temperature's coordinates*/  
        "positionX": ,  
/*optional, int, normalized X-coordinate which is between 0 and 1000*/  
        "positionY":  
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/  
        },  
    "remoteCheck": ,  
/*optional, boolean, whether remote verification is required: true, false  
(default)*/  
    "mask": "",  
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-  
wearing mask, "no"-not wearing mask*/  
    "frontSerialNo": ,  
/*optional, int, the previous event's serial No. If this field does not exist,  
the platform will check whether the event loss occurred according to the field  
serialNo. If both the serialNo and frontSerialNo are returned, the platform  
will check whether the event loss occurred according to both fields. It is  
mainly used to solve the problem that the serialNo is inconsistent after  
subscribing events or alarms*/  
    "IDCardInfo": {  
        "name": "",  
/*optional, string, name*/  
        "sex": "",  
/*optional, string, gender: "male", "female"*/  
        "birth": "",  
/*optional, string, date of birth, e.g., "1990-02-24"*/  
        "addr": "",  
/*optional, string, address*/  
        "IDCardNo": "",  
/*optional, string, ID card No.*/  
        "issuingAuthority": "",  
/*optional, string, issuing authority*/  
        "startDate": "",  
/*optional, string, start date of the effective period*/  
        "endDate": "",  
/*optional, string, end date of the effective period*/  
        "isLongTermEffective":  
/*optional, boolean, whether the effective period is permanent*/  
        },  
    "pictureURL": "",
```

```
/*optional, string, captured picture URL*/
    "IDCardPicURL": "",
/*optional, string, ID card picture URL*/
    "visibleLightURL": "",
/*optional, string, URL of the visible light picture captured by the thermal
camera*/
    "thermalURL": "",
/*optional, string, thermal picture URL*/
    "picturesNumber": ,
/*optional, int, number of pictures. If there is no picture, this node is set
to 0 or is not returned*/
    "helmet": "",
/*optional, string, whether the person wears a hard hat: "yes", "no",
"unknown)*/
    "HealthInfo": {
/*optional, object, health information*/
        "healthCode": 1,
/*optional, int, health code status: 0 (no request), 1 (no health code), 2
(green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6
(other error, e.g., searching failed due to API exception), 7 (searching for
the health code timed out)*/
        "NADCode": 1,
/*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which
means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/
        "travelCode": 1,
/*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in
the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3
(other)*/
        "vaccineStatus": 1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1
(vaccinated)*/
    }
}
```

See Also

[Access Control Event Types](#)

Example

Interaction Example of Uploading ID Card Swiping Event with Binary Picture Data in Arming Mode

```
HTTP/1.1 200 OK
MIME-Version: 1.0
Connection: close
Content-Type:multipart/form-data;boundary=MIME_boundary

--MIME_boundary
Content-Type: application/json
Content-Length:480

<alarm message in JSON format>
--MIME_boundary
```

```
Content-Disposition: form-data; name="Picture"; filename="Picture.jpg"; //  
Captured picture data  
Content-Type:image/jpeg  
Content-Length:516876  
Content-ID: pictureImage  
  
fefefwageegfqaeg...  
--MIME_boundary  
Content-Disposition: form-data; name="IDCardPic"; filename="IDCardPic.jpg";//ID  
card picture data  
Content-Type:image/jpeg  
Content-Length:516876  
Content-ID: IDCardPicImage  
  
fefefwageegfqaeg...  
--MIME_boundary  
Content-Type: application/json  
Content-Length:480  
  
<next alarm message in JSON format>  
--MIME_boundary  
Content-Disposition: form-data; name="Picture"; filename="Picture.jpg"  
Content-Type:image/jpeg  
Content-Length:516876  
  
fefefwageegfqaeg...  
--MIME_boundary  
Content-Disposition: form-data; name="IDCardPic"; filename="IDCardPic.jpg"  
Content-Type:image/jpeg  
Content-Length:516876  
  
fefefwageegfqaeg...  
--MIME_boundary  
Content-Disposition: form-data; name="VisibleLight";  
filename="VisibleLight.jpg"; //Data of the visible light picture captured by  
the thermal camera  
Content-Type: image/jpeg  
Content-Length: 516876  
Content-ID: visibleLight_image  
  
fefefwageegfqaeg...  
--MIME_boundary  
Content-Disposition: form-data; name="Thermal"; filename="Thermal.jpg"; //  
Thermal picture data  
Content-Type: image/jpeg  
Content-Length: 516876  
Content-ID: thermal_image  
  
fefefwageegfqaeg...  
--MIME_boundary
```

JSON_EventNotificationAlert_QRCodeEventMsg

The event information of scanning QR code is uploaded in JSON format of EventNotificationAlert message.

Event Message of Scanning QR Code with Binary Picture Data

After registering personal information by scanning a fixed QR code using mobile APP, the registered information will be sent to the central storage of the platform, and then the person information URL will be returned which will be used to generate a dynamic QR code in the mobile APP. When a person scans the dynamic QR code on the access control device, the QR code and temperature information will be sent to the platform.

```
{  
    "ipAddress": "",  
    /*required, string, IP address of the alarm device, the maximum size is 32 bytes*/  
    "ipv6Address": "",  
    /*optional, string, IPv6 address of the alarm device, the maximum size is 128 bytes*/  
    "portNo": ,  
    /*optional, integer32, port No. of the alarm device*/  
    "protocol": "",  
    /*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32 bytes*/  
    "macAddress": "",  
    /*optional, string, MAC address, the maximum size is 32 bytes*/  
    "channelID": ,  
    /*optional, integer32, device channel No. that triggered the alarm*/  
    "dateTime": "",  
    /*required, string, time when the alarm is triggered (UTC time), the maximum size is 32 bytes*/  
    "activePostCount": ,  
    /*required, integer32, number of times that the same alarm has been uploaded*/  
    "eventType": "",  
    /*required, string, triggered event type, here it should be set to "QRCodeEvent", the maximum size is 128 bytes*/  
    "eventState": "",  
    /*required, string, event triggering status: "active"-triggered, "inactive"-not triggered, the maximum size is 32 bytes*/  
    "eventDescription": "",  
    /*required, event description*/  
    "deviceID": "test0123",  
    /*optional, string, device ID (PUID), which should be returned when the event message is uploaded via ISUP*/  
    "QRCodeEvent": {  
        "deviceName": "",  
        /*optional, string, device name*/  
        "serialNo": ,  
        /*optional, int, event serial No.*/
```

```
"currentEvent": ,
/*optional, boolean, whether it is a real-time event: true-yes (real-time
event), false-no (offline event)*/
"QRCodeInfo":"",
/*required, string, QR code information*/
"thermometryUnit":"",
/*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/
"currTemperature": ,
/*optional, float, face temperature which is accurate to one decimal place*/
"isAbnormalTemperature": ,
/*optional, boolean, whether the face temperature is abnormal: true-yes, false-no*/
"RegionCoordinates":{
/*optional, face temperature's coordinates*/
"positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
"positionY": ,
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
},
"remoteCheck": ,
/*optional, boolean, whether remote verification is required: true-yes, false-no (default)*/
"mask":"",
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
"helmet": ""
/*optional, string, whether the person wears a hard hat: "yes", "no",
"unknown"*/
}
--MIME_boundary
Content-Disposition: form-data; name="VisibleLight";
filename="VisibleLight.jpg"; //Data of the visible light picture captured by
the thermal camera
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: visibleLight_image

fefefwageegfqaeg...
--MIME_boundary
Content-Disposition: form-data; name="Thermal"; filename="Thermal.jpg"; //
Thermal picture data
Content-Type: image/jpeg
Content-Length: 516876
Content-ID: thermal_image

fefefwageegfqaeg...
--MIME_boundary
```

Event Message of Scanning QR Code with Picture URL

```
{  
    "ipAddress": "",  
    /*required, string, IP address of the alarm device, the maximum size is 32 bytes*/  
    "ipv6Address": "",  
    /*optional, string, IPv6 address of the alarm device, the maximum size is 128 bytes*/  
    "portNo": ,  
    /*optional, integer32, port No. of the alarm device*/  
    "protocol": "",  
    /*optional, string, protocol type: "HTTP", "HTTPS", the maximum size is 32 bytes*/  
    "macAddress": "",  
    /*optional, string, MAC address, the maximum size is 32 bytes*/  
    "channelID": ,  
    /*optional, integer32, device channel No. that triggered the alarm*/  
    "dateTime": "",  
    /*required, string, time when the alarm is triggered (UTC time), the maximum size is 32 bytes*/  
    "activePostCount": ,  
    /*required, integer32, number of times that the same alarm has been uploaded*/  
    "eventType": "",  
    /*required, string, triggered event type, here it should be set to "QRCodeEvent", the maximum size is 128 bytes*/  
    "eventState": "",  
    /*required, string, event triggering status: "active"-triggered, "inactive"-not triggered, the maximum size is 32 bytes*/  
    "eventDescription": "",  
    /*required, event description*/  
    "deviceID": "test0123",  
    /*optional, string, device ID (PUID), which should be returned when the event message is uploaded via ISUP*/  
    "QRCodeEvent": {  
        "deviceName": "",  
        /*optional, string, device name*/  
        "serialNo": ,  
        /*optional, int, event serial No.*/  
        "currentEvent": ,  
        /*optional, boolean, whether it is a real-time event: true-yes (real-time event), false-no (offline event)*/  
        "QRCodeInfo": "",  
        /*required, string, QR code information*/  
        "thermometryUnit": "",  
        /*optional, string, temperature unit: "celsius"-Celsius (default), "fahrenheit"-Fahrenheit, "kelvin"-Kelvin*/  
        "currTemperature": ,  
        /*optional, float, face temperature which is accurate to one decimal place*/  
        "isAbnormalTemperature": ,  
        /*optional, boolean, whether the face temperature is abnormal: true-yes, false-
```

```
no*/
    "RegionCoordinates": {
/*optional, face temperature's coordinates*/
        "positionX": ,
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
        "positionY": ,
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
        },
        "remoteCheck": ,
/*optional, boolean, whether remote verification is required: true-yes, false-
no (default)*/
        "mask": "",
/*optional, string, whether the person is wearing mask or not: "unknown", "yes"-wearing mask, "no"-not wearing mask*/
        "visibleLightURL": "",
/*optional, string, URL of the visible light picture captured by the thermal
camera*/
        "thermalURL": "",
/*optional, string, thermal picture URL*/
        "helmet": ""
/*optional, string, whether the person wears a hard hat: "yes", "no",
"unknown"*/
    }
}
```

JSON_EventOptimizationCfg

EventOptimizationCfg message in JSON format

```
{
    "EventOptimizationCfg": {
        "enable": ,
/*optional, boolean, whether to enable event optimization: true-yes (default),
false-no*/
        "isCombinedLinkageEvents": ,
/*optional, boolean, whether to enable linked event combination: true-enable
(default), false-disable*/
    }
}
```

JSON_EventStorageCfg

JSON message about the storage parameters of access control events

```
{
    "EventStorageCfg": {
        "mode": "regular",
/*required, string, event storage method: "regular" (delete old events
periodically), "time" (delete old events by specified time), "cycle"
```

```
(overwriting) */
    "checkTime": "",
/*dependent, string, check time. Events that occurred before the check time
will be deleted. The maximum size is 32 bytes. This node is valid when mode is
"time"*/
    "period":10
/*dependent, int, time period for deleting old events, unit: minute. This node
is valid when mode is "regular"*/
}
}
```

JSON_EventStorageCfgCap

JSON message about the storage configuration capability of access control events

```
{
    "EventStorageCfgCap": {
        "mode": {
/*required, string, event storage method: "regular" (delete old events
periodically), "time" (delete old events by specified time), "cycle"
(overwriting)*/
            "@opt": ["regular", "time", "cycle"]
        },
        "checkTime": {
/*dependent, string, check time. Events that occurred before the check time
will be deleted. The maximum size is 32 bytes. This node is valid when mode is
"time"*/
            "@min":0,
            "@max":0
        },
        "period": {
/*dependent, int, time period for deleting old events, unit: minute. This node
is valid when mode is "regular"*/
            "@min":10,
            "@max":10
        }
    }
}
```

JSON_FaceRecognizeMode

FaceRecognizeMode message in JSON format

```
{
    "FaceRecognizeMode": {
/*required, facial recognition mode: "normalMode"-normal mode, "deepMode"-deep
mode*/
        "mode": ""
    }
}
```

```
    }
}
```

JSON_FaceRecordNumInAllFPLib

Message about the total number of face records in all face picture libraries, and it is in JSON format.

```
{
  "requestURL": "",
  "statusCode": "",
  "statusString": "",
  "subStatusCode": "",
  "errorCode": "",
  "errorMsg": "",
  /*see the description of this node and above nodes in the message of
  JSON_ResponseStatus*/
  "FDRecordDataInfo": [
    /*optional, string type, information of face records in face picture library,
    this node is valid when errorCode is 1 and errorMsg is "ok"*/
    "FDID": "",
    /*optional, face picture library ID, string type, the maximum size is 63 bytes*/
    "faceLibType": "",
    /*optional, face picture library type: "blackFD"-list library, "staticFD"-static
    library, string type, the maximum size is 32 bytes*/
    "name": "",
    /*optional, face picture library name, string type, the maximum size is 48
    bytes*/
    "recordDataNumber": ""
    /*optional, number of records, integer32 type*/
  ]
}
```

See Also

[JSON_ResponseStatus](#)

JSON_FaceRecordNumInOneFPLib

Message about the number of face records in a specific face picture library, and it is in JSON format.

```
{
  "requestURL": "",
  "statusCode": "",
  "statusString": "",
  "subStatusCode": "",
  "errorCode": "",
  "errorMsg": "",
```

```
/*see the description of this node and above nodes in the message of
JSON_ResponseStatus*/
    "FDID": "",
/*optional, face picture library ID, string type, the max. string length is 63
bytes*/
    "faceLibType": "",
/*optional, face picture library type: "blackFD"-list library, "staticFD"-static
library, string type, the max. string length is 32 bytes*/
    "name": "",
/*optional, face picture library name, string type, the max. string length is
48 bytes*/
    "recordDataNumber": ""
/*optional, number of records, integer32 type*/
}
```

See Also

[JSON_ResponseStatus](#)

JSON_FaceTemperatureEvent

JSON message about the result of actively getting face temperature screening events

```
{
    "FaceTemperatureEvent" : {
        "searchID": "",
/*required, string, search ID, which is used to check whether the current
search requester is the same as the previous one. If they are the same, the
search record will be stored in the device to speed up the next search*/
        "responseStatusStrg": "OK",
/*required, string, search status: "OK"(searching completed), "MORE"(searching
for more results), "NO MATCH"(no matched results)*/
        "numOfMatches": 1,
/*required, int, the number of the returned records*/
        "totalMatches": 1,
/*required, int, the total number of the matched records*/
        "InfoList": [
/*optional, event information*/
            "deviceName": "",
/*optional, string, device name*/
            "serialNo": 1,
/*optional, int, event serial No.*/
            "thermometryUnit": "",
/*required, string, temperature unit: "celsius" (Celsius), "fahrenheit"
(Fahrenheit), "kelvin" (Kelvin), the default value is "celsius"*/
            "currTemperature": 1.0,
/*required, float, face temperature, the value is accurate to one decimal
place*/
            "isAbnormalTemperature": true,
/*optional, boolean, whether the face temperature is abnormal: true (abnormal),
false (normal)*/
        ]
    }
}
```

```
        "RegionCoordinates": {
            /*optional, coordinates of the face temperature*/
            "positionX": 1,
            /*optional, int, X-coordinate, which is normalized to a number between 0 and 1000*/
            "positionY": 1
            /*optional, int, Y-coordinate, which is normalized to a number between 0 and 1000*/
        },
        "mask": "",
        /*optional, string, whether the person wears a mask: "unknown" (unknown), "yes" (wearing a mask), "no" (no mask)*/
        "capturePicUrl":"",
        /*optional, string, the URL of the captured picture*/
        "visibleLightPicUrl":"",
        /*optional, string, the URL of the visible light picture*/
        "thermalPicUrl":"",
        /*optional, string, the URL of the thermal picture*/
        "helmet": "",
        /*optional, string, whether the person wears a hard hat: "unknown" (unknown), "yes" (wearing a hard hat), "no" (no hard hat)*/
        "dateTime": "2016-12-12T17:30:08+08:00"
        /*required, string, the time (UTC time) when the alarm is triggered, the maximum size is 32 bytes*/
    }
}
```

JSON_FaceTemperatureEventCap

JSON message about the capability of actively getting face temperature screening events

```
{
    "FaceTemperatureEventCap" : {
        "FaceTemperatureEventCond": {
            "searchID": {
                /*required, string, search ID, which is used to check whether the current search requester is the same as the previous one. If they are the same, the search record will be stored in the device to speed up the next search*/
                "@min":1,
                "@max":1
            },
            "searchResultPosition": {
                /*required, int, the start position of search result in the result list. In a single search, if you cannot get all the records in the result list, you can mark the end position and get the following records after the marked position in the next search. If the maximum number of totalMatches supported by the device is M and the number of totalMatches stored in the device now is N (N<=M), the valid range of this node is 0 to N-1*/
                "@min":1,
                "@max":1
            }
        }
    }
}
```

```

    },
    "maxResults": {
/*required, int, the maximum number of search results that can be obtained by
calling the URI this time. If the value of maxResults is greater than that
defined in the device capability, the value in the capability will be returned.
In this case, the device will not return error*/
        "@min":1,
        "@max":1
    },
    "startTime": "1970-01-01T00:00:00+00:00",
/*optional, string, start time (UTC time)*/
    "endTime": "2017-12-12T17:30:08+08:00",
/*optional, string, end time (UTC time)*/
    "picEnable": {
/*optional, boolean, whether to upload the picture along with the event
information: true (all matched events will be uploaded with pictures if there
are any), false (all matched events will be uploaded without pictures). If this
node is not configured, the default value is true*/
        "@opt": [true, false]
    },
    "beginSerialNo": {
/*optional, int, start serial No.*/
        "@min":1,
        "@max":1
    },
    "endSerialNo": {
/*optional, int, end serial No.*/
        "@min":1,
        "@max":1
    },
    "isAbnormalTemperature": {
/*optional, object, whether the skin-surface temperature is abnormal*/
        "@opt": [true, false]
/*optional, array of boolean, options: true (yes), false (no)*/
    }
},
    "InfoList" : {
/*optional, event information*/
        "deviceName": {
/*optional, string, device name*/
            "@min":1,
            "@max":1
        },
        "serialNo": {
/*optional, int, event serial No.*/
            "@min":1,
            "@max":1
        },
        "thermometryUnit": {
/*required, string, temperature unit: "celsius" (Celsius), "fahrenheit"
(Fahrenheit), "kelvin" (Kelvin), the default value is "celsius"*/
            "@opt": ["celsius", "fahrenheit", "kelvin"]
        }
    }
}

```

```
        },
        "currTemperature": {
/*required, float, face temperature, the value is accurate to one decimal
place*/
            "@min":1.0,
            "@max":1.0
        },
        "isAbnormalTemperature": {
/*optional, boolean, whether the face temperature is abnormal: true (abnormal),
false (normal)*/
            "@opt": [true, false]
        },
        "RegionCoordinates": {
/*optional, coordinates of the face temperature*/
            "positionX": {
/*optional, int, X-coordinate, which is normalized to a number between 0 and
1000*/
                "@min":1,
                "@max":1
            },
            "positionY": {
/*optional, int, Y-coordinate, which is normalized to a number between 0 and
1000*/
                "@min":1,
                "@max":1
            }
        },
        "mask": {
/*optional, string, whether the person wears a mask: "unknown" (unknown), "yes"
(wearing a mask), "no" (no mask)*/
            "@opt": ["unknown", "yes", "no"]
        },
        "capturePicUrl": {
/*optional, string, the URL of the captured picture*/
            "@min":1,
            "@max":1
        },
        "visibleLightPicUrl": {
/*optional, string, the URL of the visible light picture*/
            "@min":1,
            "@max":1
        },
        "thermalPicUrl": {
/*optional, string, the URL of the thermal picture*/
            "@min":1,
            "@max":1
        },
        "helmet": {
/*optional, string, whether the person wears a hard hat: "unknown" (unknown),
"yes" (wearing a hard hat), "no" (no hard hat)*/
            "@opt": ["unknown", "yes", "no"]
        },
    },
}
```

```
        "dateTime": "2016-12-12T17:30:08+08:00"
/*required, string, the time (UTC time) when the alarm is triggered, the
maximum size is 32 bytes*/
    }
}
}
```

JSON_FaceTemperatureEventCond

JSON message about the condition of actively getting face temperature screening events

```
{
  "FaceTemperatureEventCond": {
    "searchID": "",
    /*required, string, search ID, which is used to check whether the current
    search requester is the same as the previous one. If they are the same, the
    search record will be stored in the device to speed up the next search*/
    "searchResultPosition": 0,
    /*required, int, the start position of search result in the result list. In a
    single search, if you cannot get all the records in the result list, you can
    mark the end position and get the following records after the marked position
    in the next search. If the maximum number of totalMatches supported by the
    device is M and the number of totalMatches stored in the device now is N
    (N<=M), the valid range of this node is 0 to N-1*/
    "maxResults": 30,
    /*required, int, the maximum number of search results that can be obtained by
    calling the URI this time. If the value of maxResults is greater than that
    defined in the device capability, the value in the capability will be returned.
    In this case, the device will not return error*/
    "startTime": "2016-12-12T17:30:08+08:00",
    /*optional, string, start time (UTC time)*/
    "endTime": "2017-12-12T17:30:08+08:00",
    /*optional, string, end time (UTC time)*/
    "picEnable": true,
    /*optional, boolean, whether to upload the picture along with the event
    information: true (all matched events will be uploaded with pictures if there
    are any), false (all matched events will be uploaded without pictures). If this
    node is not configured, the default value is true*/
    "beginSerialNo": 1,
    /*optional, int, start serial No.*/
    "endSerialNo": 1,
    /*optional, int, end serial No.*/
    "isAbnormalTemperature": true
    /*optional, boolean, whether the skin-surface temperature is abnormal*/
  }
}
```

JSON_FingerPrintCfg

FingerPrintCfg message in JSON format

```
{  
    "FingerPrintCfg": {  
        "employeeNo": "",  
        /*required, string, employee No. (person ID) linked with the fingerprint*/  
        "enableCardReader": ,  
        /*required, array, fingerprint modules to apply fingerprint data to, e.g.,  
        [1,3,5] indicates applying fingerprint data to fingerprint modules No.1, No.3,  
        and No.5*/  
        "fingerPrintID": ,  
        /*required, integer, fingerprint No., which is between 1 and 10*/  
        "deleteFingerPrint": ,  
        /*optional, boolean, whether to delete the fingerprint: "true"-yes. This node  
        is required only when the fingerprint needs to be deleted; for adding or  
        editing fingerprint information, this node can be set to NULL*/  
        "fingerType": "",  
        /*required, string, fingerprint type: "normalFP"-normal fingerprint, "hijackFP"-  
        duress fingerprint, "patrolFP"-patrol fingerprint, "superFP"-super fingerprint,  
        "dismissingFP"-dismiss fingerprint*/  
        "fingerData": "",  
        /*required, string, fingerprint data encoded by Base64*/  
        "leaderFP": ,  
        /*optional, array, whether the access control points support first fingerprint  
        authentication function, e.g., [1,3,5] indicates that access control points No.  
        1, No.3, and No.5 support first fingerprint authentication function*/  
        "checkEmployeeNo":  
        /*optional, boolean, whether to check the existence of the employee No. (person  
        ID): "false"-no, "true"-yes. If this node is not configured, the device will  
        check the existence of the employee No. (person ID) by default. If this node is  
        set to "false", the device will not check the existence of the employee No.  
        (person ID) to speed up data applying; if this node is set to "true" or NULL,  
        the device will check the existence of the employee No. (person ID), and it is  
        recommended to set this node to "true" or NULL if there is no need to speed up  
        data applying*/  
    }  
}
```

JSON_FingerPrintCond

FingerPrintCond message in JSON format

```
{  
    "FingerPrintCond": {  
        "searchID": "",  
        /*required, string, search ID, which is used to confirm the upper-level  
        platform or system. If the platform or the system is the same one during two
```

```
searching, the search history will be saved in the memory to speed up next
searching*/
    "employeeNo":"",
/*required, string, employee No. (person ID) linked with the fingerprint*/
    "cardReaderNo": ,
/*optional, integer, fingerprint module No.*/
    "fingerPrintID":
/*optional, integer, fingerprint No., which is between 1 and 10*/
}
}
```

JSON_FingerPrintCondAll

FingerPrintCondAll message in JSON format.

```
{
  "FingerPrintCondAll": {
    "employeeNo": ,
/*required, integer, employee ID (person ID), which is linked with the
fingerprint*/
    "cardReaderNo":
/*required, integer, fingerprint module No.*/
  }
}
```

JSON_FingerPrintCountList

JSON message about the total number of fingerprints

```
{
  "FingerPrintCountList": [
    "cardReaderNo":1,
/*optional, int, fingerprint and card reader No.*/
    "numberOffP":3,
/*required, int, number of fingerprints*/
    "fingerPrintIDs":
/*optional, array, finger number, which is between 1 and 10*/
  ]
}
```

JSON_FingerPrintDelete

FingerPrintDelete message in JSON format

```
{
  "FingerPrintDelete":{
    "mode":"",

```

```
/*required, string, deleting mode: "byEmployeeNo"-delete by employee No.  
(person ID), "byCardReader"-delete by fingerprint module*/  
    "EmployeeNoDetail":{  
/*optional, delete by employee No. (person ID), this node is valid when mode is  
"byEmployeeNo"*/  
    "employeeNo":"" ,  
/*optional, string, employee No. (person ID) linked with the fingerprint*/  
    "enableCardReader": ,  
/*optional, array, fingerprint module whose fingerprints should be deleted,  
e.g., [1,3,5] indicates that the fingerprints of fingerprint modules No.1, No.  
3, and No.5 are deleted*/  
    "fingerPrintID":  
/*optional, array, No. of fingerprint to be deleted, e.g., [1,3,5] indicates  
deleting fingerprint No.1, No.3, and No.5*/  
    },  
    "CardReaderDetail":{  
/*optional, delete by fingerprint module, this node is valid when mode is  
"byCardReader"*/  
    "cardReaderNo": ,  
/*optional, integer, fingerprint module No.*/  
    "clearAllCard": ,  
/*optional, boolean, whether to delete the fingerprint information of all  
cards: "false"-no (delete by employee No.), "true"-yes (delete the fingerprint  
information of all employee No.)*/  
    "employeeNo":""  
/*optional, string, employee No. (person ID) linked with the fingerprint, this  
node is valid when clearAllCard is "false"*/  
    }  
}  
}
```

JSON_FingerPrintDeleteProcess

FingerPrintDeleteProcess message in JSON format

```
{  
    "FingerPrintDeleteProcess":{  
        "status":""  
/*required, string, deleting status: "processing"-deleting, "success"-deleted,  
"failed"-deleting failed*/  
    }  
}
```

JSON_FingerPrintInfo

FingerPrintInfo message in JSON format

```
{  
    "FingerPrintInfo":{
```

```
"searchID":"",
/*required, string, search ID, which is used to confirm the upper-level
platform or system. If the platform or the system is the same one during two
searching, the search history will be saved in the memory to speed up next
searching*/
"status":"",
/*required, string, status: "OK"-the fingerprint exists, "NoFP"-the fingerprint
does not exist*/
"FingerPrintList": [
    "cardReaderNo": ,
/*required, integer, fingerprint module No.*/
    "fingerPrintID": ,
/*required, integer, fingerprint No., which is between 1 and 10*/
    "fingerType":"",
/*required, string, fingerprint type: "normalFP"-normal fingerprint, "hijackFP"-duress
fingerprint, "patrolFP"-patrol fingerprint, "superFP"-super fingerprint,
"dismissingFP"-dismiss fingerprint*/
    "fingerData":"",
/*required, string, fingerprint data encoded by Base64*/
    "leaderFP":
/*optional, array, whether the access control points support first fingerprint
authentication function, e.g., [1,3,5] indicates that access control points No.
1, No.3, and No.5 support first fingerprint authentication function*/
    []
}
}
```

JSON_FingerPrintInfoAll

FingerPrintInfoAll message in JSON format.

```
{
    "FingerPrintInfoAll": {
        "FingerPrintList": [
            {
                "fingerPrintID": ,
/*required, integer, fingerprint No., which is between 1 and 10*/
                "fingerType": "",
/*required, string, fingerprint type: "normalFP"-normal fingerprint, "hijackFP"-duress
fingerprint, "patrolFP"-patrol fingerprint, "superFP"-super fingerprint,
"dismissingFP"-dismiss fingerprint*/
                "leaderFP": ,
/*optional, array, whether the access control points support first fingerprint
authentication function, e.g., [1,3,5], access control point No.1, No.3, and No.
5 support first fingerprint authentication function*/
                "picEnable": ,
/*optional, boolean, whether contains fingerprint data*/
            ],
            "picturesNumber": ,
/*optional, integer, number of fingerprint, if there is no fingerprint data,
this node will be set to 0 or not be returned*/
        ]
    }
}
```

```
    }
}
```

JSON_FingerPrintModify

FingerPrintModify message in JSON format

```
{
  "FingerPrintModify": {
    "employeeNo": "",
    /*required, string, employee No. (person ID) linked with the fingerprint*/
    "cardReaderNo": ,
    /*required, integer, fingerprint module No.*/
    "fingerPrintID": ,
    /*required, integer, fingerprint No., which is between 1 and 10*/
    "fingerType": "",
    /*required, string, fingerprint type: "normalFP"-normal fingerprint, "hijackFP"-duress fingerprint, "patrolFP"-patrol fingerprint, "superFP"-super fingerprint, "dismissingFP"-dismiss fingerprint. If this node is not configured, the fingerprint type will be the original type*/
    "leaderFP": ,
    /*optional, array, whether the access control points support first fingerprint authentication function, e.g., [1,3,5] indicates that access control points No. 1, No.3, and No.5 support first fingerprint authentication function. If this node is not configured, the first fingerprint authentication function will remain unchanged*/
  }
}
```

JSON_FingerPrintStatus

FingerPrintStatus message in JSON format

```
{
  "FingerPrintStatus": {
    "status": "",
    /*optional, string, status: "success", "failed". This node will be returned only when editing fingerprint parameters or deleting fingerprints; for applying fingerprint data to the fingerprint module, this node will not be returned*/
    "StatusList": [
      /*optional, status list. This node will be returned only when applying fingerprint data to the fingerprint module; for editing fingerprint parameters or deleting fingerprints, this node will not be returned*/
      "id": ,
      /*optional, integer, fingerprint module No.*/
      "cardReaderRecvStatus": ,
      /*optional, integer, fingerprint module status: 0-connecting failed, 1-connected, 2-the fingerprint module is offline, 3-the fingerprint quality is poor, try again, 4-the memory is full, 5-the fingerprint already exists, 6-the
    ]
  }
}
```

```
fingerprint ID already exists, 7-invalid fingerprint ID, 8-this fingerprint
module is already configured, 10-the fingerprint module version is too old to
support the employee No.*/
    "errorMsg":"",
/*optional, string, error information*/
    ],
    "totalStatus":
/*required, integer, applying status: 0-applying, 1-applied*/
}
}
```

JSON_FPLibCap

Face picture library capability message, and it is in JSON format.

```
{
    "requestURL":"",
    "statusCode": ,
    "statusString":"",
    "subStatusCode":"",
    "errorCode": ,
    "errorMsg": " ",
/*see the description of this node and the above nodes in the message of
JSON_ResponseStatus*/
    "FDNameMaxLen": ,
/*required, integer32 type, maximum length of face picture library name, the
default value is 64 bytes*/
    "customInfoMaxLen": ,
/*required, int, maximum length of custom information, the default value is 256
bytes, read-only*/
    "FDMaxNum": ,
/*required, integer32 type, maximum number of face picture libraries, the
default value is 3*/
    "FDRecordDataMaxNum": ,
/*required, integer type, maximum face records supported by face picture
library*/
    "supportFDFunction":"post,delete,put,get,setUp",
/*required, the supported operations on face picture library: "post"-create,
"delete"-delete, "put"-edit, "get"-search, "setUp"-set*/
    "isSupportFDSearch": ,
/*required, boolean type, whether supports searching in face picture library:
"true"-yes, "false"-no*/
    "isSupportFDSearchDataPackage": ,
/*required, boolean type, whether supports packaging the found data in the face
picture library: "true"-yes, "false"-no*/
    "isSupportFSsearchByPic": ,
/*required, boolean type, whether supports searching by picture in the face
picture library: "true"-yes, "false"-no*/
    "isSupportFSsearchByPicGenerate": ,
/*required, boolean type, whether supports exporting search by picture results
from the face picture library: "true"-yes, "false"-no*/
```

```
"isSupportFDSearchDuplicate": ,  
/*required, boolean type, whether supports duplication checking: "true"-yes,  
"false"-no*/  
"isSupportFDSearchDuplicateGenerate": ,  
/*required, boolean type, whether supports exporting the duplication checking  
results: "true"-yes, "false"-no*/  
"isSupportFCSearch": ,  
/*required, boolean type, whether supports searching face picture comparison  
alarms: "true"-yes, "false"-no*/  
"isSupportFCSearchDataPackage": ,  
/*required, boolean, whether supports packaging the search results of face  
picture comparison alarms: "true"-yes, "false"-no*/  
"isSupportFDExecuteControl": ,  
/*required, boolean, whether supports creating relation between face picture  
libraries and cameras: "true"-yes, "false"-no*/  
"generateMaxNum": ,  
/*required, integer32 type, maximum face records can be exported from face  
picture library*/  
"faceLibType":"blackFD,staticFD,infraredFD",  
/*optional, string type, face picture library types: "blackFD"-list library,  
"staticFD"-static library, "infraredFD"-infrared face picture library, the  
maximum size of value can be assigned to this node is 32 bytes*/  
"modelMaxNum": ,  
/*optional, integer type, the maximum number of search results, the default  
value is 100*/  
"isSupportModelData":true,  
/*optional, boolean type, whether to support applying model data: "true"-yes,  
this node is not returned-no*/  
"isSupportFDLibArmingType": ,  
/*optional, boolean, whether it supports face picture library arming type:  
true, false*/  
"isSupportFDLibSearch": ,  
/*optional, boolean, whether it supports searching face picture library: true,  
false*/  
"FDArmingRecordDataMaxNum": ,  
/*optional, integer32, the supported maximum number of face records in the face  
picture arming library*/  
"isSupportControlPersonRecordByHumanId": ,  
/*optional, boolean, whether it supports modifying and deleting the face record  
by humanId: true, false*/  
"isSupportControlPersonRecordByRowKey": ,  
/*optional, boolean, whether it supports modifying and deleting the face record  
by rowKey: true, false*/  
"isSupportFaceLibRebuildCfg": ,  
/*optional, boolean, whether it supports recreating face picture library  
information and configuration: true, false*/  
"isSupportFDMove": ,  
/*optional, boolean, whether it supports moving face data in the face picture  
library in a batch: true, false. The related URI is /ISAPI/Intelligent/FDLib/  
FDMove/capabilities?format=json*/  
"faceURLLen": ,  
/*optional, int, the maximum size of the face picture URL. If this node is not
```

```
returned, the default size of the face picture URL supported by the device is
256 bytes; otherwise, the device should support that the value of this node is
greater than or equal to 256*/
    "featurePointTypeList":
["face","leftEye","rightEye","leftMouthCorner","rightMouthCorner","nose"],
/*optional, array of string, feature point types of face pictures supported by
the device. If this node exists, it indicates that the device supports applying
feature points of pictures, and the returned values are feature point types
supported by the device*/
    "isSupportArmingLibCfg":true,
/*optional, boolean, whether it supports configuring parameters of the armed
face picture library, read-only, related URI: /ISAPI/Intelligent/FDLib/
armingLibCfg/capabilities?format=json*/
    "isSupportModelTransformation":true,
/*optional, boolean, whether it supports converting face picture models in the
face picture list library, read-only, related URI: /ISAPI/Intelligent/FDLib/
model/transformation/capabilities?format=json*/
    "libAttribute":{
/*optional, object, library type: "general" (general library), "blackList"
(blocklist library), "VIP" (VIP library), "passerby" (strange library which
cannot be deleted)*/
        "@opt":["general", "blackList", "VIP", "passerby"]
/*optional, array of string, options*/
    },
    "faceType":{
/*optional, object, face type*/
        "@opt":["normalFace", "patrolFace", "hijackFace", "superFace"]
    },
    "saveFacePic": {
/*optional, object, whether to save face pictures*/
        "@opt": [true, false]
    },
    "leaderPermission":{
/*optional, object, first authentication permission*/
        "@size":4,
/*optional, int, the maximum number of elements in the array, value range:
[1,4]*/
        "@min":1,
/*optional, int, the minimum value of the element, value range: [1,4]*/
        "@max":4
/*optional, int, the maximum value of the element, value range: [1,4]*/
    }
}
```

See Also

[JSON ResponseStatus](#)

JSON_FPLibListInfo

Message about the list of face picture libraries, and it is in JSON format.

```
{  
    "requestURL": "",  
    "statusCode": "",  
    "statusString": "",  
    "subStatusCode": "",  
    "errorCode": "",  
    "errorMsg": "",  
    /*see the description of this node and above nodes in the message of  
    JSON_ResponseStatus*/  
    "FDLib": [  
        /*optional, face picture library information, string type, this node is valid  
        when errorCode is 1 and errorMsg is "ok"*/  
        {  
            "FDID": "",  
            /*optional, face picture library ID, string type, the maximum size is 63 bytes*/  
            "faceLibType": "",  
            /*optional, face picture library type: "blackFD"-list library, "staticFD"-  
            static library, string type, the maximum size is 32 bytes*/  
            "name": "",  
            /*optional, face picture library name, string type, the maximum size is 48  
            bytes*/  
            "customInfo": ""  
            /*optional, custom information, string type, the maximum size is 192 bytes*/  
        }  
    ]  
}
```

See Also

[JSON_ResponseStatus](#)

JSON_GroupCfg

GroupCfg message in JSON format

```
{  
    "GroupCfg": {  
        "enable": ,  
        /*required, boolean, whether to enable the group*/  
        "ValidPeriodCfg": {  
            /*required, effective period parameters of the group*/  
            "enable": ,  
            /*required, boolean, whether to enable the effective period: "true"-yes,  
            "false"-no. If the effective period is not enabled, it indicates that the group  
            is permanently valid*/  
            "beginTime": "",  
            "endT
```

```
/*required, start time of the effective period (UTC time)*/
    "endTime":""
/*required, end time of the effective period (UTC time)*/
    },
    "groupName ":""
/*optional, string, group name*/
}
}
```

JSON_HealthCodeCfg

JSON message about the health code parameters

```
{
    "enabled":true,
/*required, boolean, whether to enable the health code*/
    "serverAddress":"test"
/*optional, string, address of the health code server, the maximum string size
is 128 bytes*/
}
```

JSON_HealthCodeDisplayCfg

JSON message about the health code display parameters

```
{
    "showHealthCode":true
/*required, boolean, whether to display the health code: true, false*/
}
```

JSON_IDCardInfoEvent

JSON message about the result of getting ID card swiping events actively

```
{
    "IDCardInfoEvent":{
        "searchID":"",
/*required, string, search ID, which is used to check whether the current
search requester is the same as the previous one. If they are the same, the
search record will be stored in the device to speed up the next search*/
        "responseStatusStrg":"OK",
/*required, string, searching status: "OK" (searching completed), "MORE"
(search for more data), "NO MATCH" (no matched data)*/
        "numOfMatches":1,
/*required, int, number of records returned this time*/
        "totalMatches":1,
/*required, int, total number of matched records*/
    }
}
```

```

"InfoList": [
    /*optional, event information*/
    "deviceName":"",
    /*optional, string, device name*/
    "major":1,
    /*required, int, major event type, 0 means all event types. For details, refer
    to Access Control Event Types. The value of this node is in decimal format
    instead of hexadecimal format (for example, 1 refers to 0x1 which indicates
    that the major type is MAJOR_ALARM)*/
    "minor":1,
    /*required, int, minor event type, 0 means all event types. For details, refer
    to Access Control Event Types. The value of this node is in decimal format
    instead of hexadecimal format (for example, 1024 refers to 0x400 which
    indicates that the minor type is MINOR_ALARMIN_SHORT_CIRCUIT)*/
    "inductiveEventType":"",
    /*optional, string, inductive event type (only valid for rear-end devices)*/
    "netUser":"",
    /*optional, string, user name for network operation*/
    "remoteHostAddr":"",
    /*optional, string, remote host address*/
    "cardType":1,
    /*optional, int, card type: 1 (normal card), 2 (disability card), 3 (blocklist
    card), 4 (patrol card), 5 (duress card), 6 (super card), 7 (visitor card), 8
    (dismiss card)*/
    "cardReaderNo":1,
    /*optional, int, card reader No.*/
    "doorNo":1,
    /*optional, int, door (floor) No.*/
    "deviceNo":1,
    /*optional, int, device No.*/
    "serialNo":1,
    /*optional, int, event serial No.*/
    "QRCodeInfo":"",
    /*optional, string, QR code information*/
    "thermometryUnit":"",
    /*optional, string, temperature unit: "celsius", "fahrenheit", "kelvin"*/
    "currTemperature":1.0,
    /*optional, float, face temperature which is accurate to one decimal place*/
    "isAbnormalTemperature":true,
    /*optional, boolean, whether the face temperature is abnormal: true, false*/
    "RegionCoordinates":{
        /*optional, coordinates of the face temperature*/
        "positionX":1,
        /*optional, int, normalized X-coordinate which is between 0 and 1000*/
        "positionY":1
    },
    /*optional, int, normalized Y-coordinate which is between 0 and 1000*/
    "mask":"",
    /*optional, string, whether the person is wearing a mask: "unknown", "yes",
    "no"*/
    "frontSerialNo":1,
    /*optional, int, serial No. of the previous event. If this node is not returned
    */
]

```

by the device, the platform will check whether the event is lost by **serialNo**; if this node is returned by the device, the platform will check whether the event is lost by both this node and **serialNo**. This node is used for the problem that the **serialNo** is not continuous after alarm subscription*/

```
"IDCardInfo":{  
    "name": "",  
    /*optional, string, name*/  
    "sex": "",  
    /*optional, string, gender: "male", "female"*/  
    "birth": "",  
    /*optional, string, date of birth, e.g., "1990-02-24"*/  
    "addr": "",  
    /*optional, string, address*/  
    "IDCardNo": "",  
    /*optional, string, ID card No.*/  
    "issuingAuthority": "",  
    /*optional, string, issuing authority*/  
    "startDate": "",  
    /*optional, string, start date of the validity period*/  
    "endDate": "",  
    /*optional, string, end date of the validity period*/  
    "isLongTermEffective": false  
    /*optional, boolean, whether it is permanently valid*/  
    },  
    "capturePicUrl": "",  
    /*optional, string, captured picture URL*/  
    "IDCardPic": "",  
    /*optional, string, ID card picture URL*/  
    "visibleLightPicUrl": "",  
    /*optional, string, visible light picture URL*/  
    "thermalPicUrl": "",  
    /*optional, string, thermal picture URL*/  
    "helmet": "",  
    /*optional, string, whether the person wears a hard hat: "unknown", "yes",  
    "no"*/  
    "dateTime": "2016-12-12T17:30:08+08:00",  
    /*required, string, alarm triggering time (UTC time), the maximum size is 32  
    bytes*/  
    "HealthInfo": {  
        /*optional, object, health information*/  
        "healthCode": 1,  
        /*optional, int, health code status: 0 (no request), 1 (no health code), 2  
        (green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6  
        (other error, e.g., searching failed due to API exception), 7 (searching for  
        the health code timed out)*/  
        "NADCode": 1,  
        /*optional, int, nucleic acid test result: 0 (no result), 1 (negative, which  
        means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/  
        "travelCode": 1,  
        /*optional, int, trip code: 0 (no trip in the past 14 days), 1 (once left in  
        the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3  
        (other)*/
```

```
        "vaccineStatus": 1
/*optional, int, whether the person is vaccinated: 0 (not vaccinated), 1
(vaccinated)*/
    }
}
}
```

See Also

[Access Control Event Types](#)

JSON_IDCardInfoEventCap

JSON message about the capability of getting the ID card swiping events actively

```
{
  "IDCardInfoEventCap": {
    "IDCardInfoEventCond": {
      "searchID": {
        /*required, string, search ID, which is used to check whether the current
        search requester is the same as the previous one. If they are the same, the
        search record will be stored in the device to speed up the next search*/
        "@min": 1,
        "@max": 1
      },
      "searchResultPosition": {
        /*required, int, the end position of search result in result list. In a single
        search, if you cannot get all the records in the result list, you can mark the
        end position and get the following records after the marked position in the
        next search. For example, if the maximum value of totalMatches supported by the
        device is M, but there are N matched results stored in the device currently
        (N<=M), the valid range of this node is 0 to N-1*/
        "@min": 1,
        "@max": 1
      },
      "maxResults": {
        /*required, int, maximum number of records that can be obtained after the URI
        is called this time. If the value of maxResults is larger than the value
        returned by the device capability, the device will return according to the
        maximum value in the capability and will not return error information*/
        "@min": 1,
        "@max": 1
      },
      "major": {
        /*required, int, major event type: 0-all, 1-alarm, 2-exception, 3-operaiton, 5-
        event. For details, refer to Access Control Event Types. The value of this node
        is in decimal format instead of hexadecimal format*/
        "@opt": [0, 1, 2, 3, 5]
      },
      "minorAlarm": {

```

```
/*required, int, minor alarm type. For details, refer to Access Control Event
Types. The value of this node is in decimal format instead of hexadecimal
format*/
    "@opt": [1024, 1025, 1026, 1027]
},
    "minorException":{

/*required, int, minor exception type. For details, refer to Access Control
Event Types. The value of this node is in decimal format instead of hexadecimal
format*/
    "@opt": [39, 58, 59, 1024]
},
    "minorOperation":{

/*required, int, minor operation type. For details, refer to Access Control Event
Types. The value of this node is in decimal format instead of hexadecimal
format*/
    "@opt": [80, 90, 112, 113]
},
    "minorEvent":{

/*required, int, minor event type. For details, refer to Access Control Event
Types. The value of this node is in decimal format instead of hexadecimal
format*/
    "@opt": [1, 2, 3, 4]
},
    "startTime": "1970-01-01T00:00:00+00:00",
/*optional, string, start time (UTC time)*/
    "endTime": "2017-12-12T17:30:08+08:00",
/*optional, string, end time (UTC time)*/
    "picEnable":{

/*optional, boolean, whether to upload events with pictures: true (yes), false
(no). The default value is true*/
        "@opt": [true, false]
},
    "beginSerialNo":{

/*optional, int, start serial No.*/
        "@min": 1,
        "@max": 1
},
    "endSerialNo":{

/*optional, int, end serial No.*/
        "@min": 1,
        "@max": 1
},
    "isAbnormalTemperature":{

/*optional, object, whether the skin-surface temperature is abnormal*/
        "@opt": [true, false]
},
/*optional, array of boolean, options: true (yes), false (no)*/
    }
},
    "InfoList":{

/*optional, event information*/
        "deviceName":{

/*optional, string, device name*/

```

```

        "@min":1,
        "@max":1
    },
    "inductiveEventType":{
/*optional, string, inductive event type (only valid for rear-end devices)*/
        "@min":1,
        "@max":1
    },
    "netUser":{
/*optional, string, user name for network operation*/
        "@min":1,
        "@max":1
    },
    "remoteHostAddr":{
/*optional, string, remote host address*/
        "@min":1,
        "@max":1
    },
    "cardType":{
/*optional, int, card type: 1 (normal card), 2 (disability card), 3 (blocklist
card), 4 (patrol card), 5 (duress card), 6 (super card), 7 (visitor card), 8
(dismiss card)*/
        "@opt":[1, 2, 3, 4, 5, 6, 7, 8]
    },
    "cardReaderNo":{
/*optional, int, card reader No.*/
        "@min":1,
        "@max":1
    },
    "doorNo":{
/*optional, int, door (floor) No.*/
        "@min":1,
        "@max":1
    },
    "deviceNo":{
/*optional, int, device No.*/
        "@min":1,
        "@max":1
    },
    "serialNo":{
/*optional, int, event serial No.*/
        "@min":1,
        "@max":1
    },
    "QRCodeInfo":{
/*optional, string, QR code information*/
        "@min":1,
        "@max":1
    },
    "thermometryUnit":{
/*optional, string, temperature unit: "celsius", "fahrenheit", "kelvin"*/
        "@opt":["celsius", "fahrenheit", "kelvin"]
    }
}

```

```

    },
    "currTemperature":{
/*optional, float, face temperature which is accurate to one decimal place*/
        "@min":1.0,
        "@max":1.0
    },
    "isAbnormalTemperature":{
/*optional, boolean, whether the face temperature is abnormal: true, false*/
        "@opt":[true, false]
    },
    "RegionCoordinates":{
/*optional, coordinates of the face temperature*/
        "positionX":{
/*optional, int, normalized X-coordinate which is between 0 and 1000*/
            "@min":1,
            "@max":1
        },
        "positionY":{
/*optional, int, normalized Y-coordinate which is between 0 and 1000*/
            "@min":1,
            "@max":1
        }
    },
    "mask":{
/*optional, string, whether the person is wearing a mask: "unknown", "yes",
"no"*/
        "@opt":["unknown", "yes", "no"]
    },
    "frontSerialNo":{
/*optional, int, serial No. of the previous event. If this node is not returned
by the device, the platform will check whether the event is lost by serialNo;
if this node is returned by the device, the platform will check whether the
event is lost by both this node and serialNo. This node is used for the problem
that the serialNo is not continuous after alarm subscription*/
        "@min":1,
        "@max":1
    },
    "IDCardInfo":{
        "name":{
/*optional, string, name*/
            "@min":1,
            "@max":1
        },
        "sex":{
/*optional, string, gender: "male", "female"*/
            "@min":1,
            "@max":1
        },
        "birth":{
/*optional, string, date of birth, e.g., "1990-02-24"*/
            "@min":1,
            "@max":1
        }
    }
}

```

```
        },
        "addr": {
/*optional, string, address*/
            "@min":1,
            "@max":1
        },
        "IDCardNo": {
/*optional, string, ID card No.*/
            "@min":1,
            "@max":1
        },
        "issuingAuthority": {
/*optional, string, issuing authority*/
            "@min":1,
            "@max":1
        },
        "startDate": {
/*optional, string, start date of the validity period*/
            "@min":1,
            "@max":1
        },
        "endDate": {
/*optional, string, end date of the validity period*/
            "@min":1,
            "@max":1
        },
        "isLongTermEffective": {
/*optional, boolean, whether it is permanently valid*/
            "@opt": [true, false]
        },
        "capturePicUrl": {
/*optional, string, captured picture URL*/
            "@min":1,
            "@max":1
        },
        "IDCardPic": {
/*optional, string, ID card picture URL*/
            "@min":1,
            "@max":1
        },
        "visibleLightPicUrl": {
/*optional, string, visible light picture URL*/
            "@min":1,
            "@max":1
        },
        "thermalPicUrl": {
/*optional, string, thermal picture URL*/
            "@min":1,
            "@max":1
        },
        "helmet": {
```

```
/*optional, string, whether the person wears a hard hat: "unknown", "yes", "no"*/
    "@opt": ["unknown", "yes", "no"]
},
"dateTime": "2016-12-12T17:30:08+08:00",
/*required, string, alarm triggering time (UTC time), the maximum size is 32 bytes*/
    "HealthInfo": {
/*optional, object, health information*/
        "healthCode": {
/*optional, object, health code status*/
            "@opt": [0, 1, 2, 3, 4, 5, 6]
/*optional, array of int, options: 0 (no request), 1 (no health code), 2 (green QR code), 3 (yellow QR code), 4 (red QR code), 5 (no such person), 6 (other error, e.g., searching failed due to API exception), 7 (searching for the health code timed out)*/
            },
        "NADCCode": {
/*optional, object, nucleic acid test result: 0 (no result), 1 (negative, which means normal), 2 (positive, which means diagnosed), 3 (the result has expired)*/
            "@opt": [0, 1, 2, 3]
        },
        "travelCode": {
/*optional, object, trip code: 0 (no trip in the past 14 days), 1 (once left in the past 14 days), 2 (has been to the high-risk area in the past 14 days), 3 (other)*/
            "@opt": [0, 1, 2, 3]
        },
        "vaccineStatus": {
/*optional, object, whether the person is vaccinated: 0 (not vaccinated), 1 (vaccinated)*/
            "@opt": [0, 1]
        }
    }
}
```

See Also

[Access Control Event Types](#)

JSON_IDCardInfoEventCond

JSON message about the condition of getting ID card swiping events actively

```
{
    "IDCardInfoEventCond": {
        "searchID": "",
/*required, string, search ID, which is used to check whether the current search requester is the same as the previous one. If they are the same, the
```

```
search record will be stored in the device to speed up the next search*/
    "searchResultPosition":0,
/*required, int, the end position of search result in result list. In a single
search, if you cannot get all the records in the result list, you can mark the
end position and get the following records after the marked position in the
next search. For example, if the maximum value of totalMatches supported by the
device is M, but there are N matched results stored in the device currently
(N<=M), the valid range of this node is 0 to N-1*/
    "maxResults":30,
/*required, int, maximum number of records that can be obtained after the URI
is called this time. If the value of maxResults is larger than the value
returned by the device capability, the device will return according to the
maximum value in the capability and will not return error information*/
    "major":1,
/*optional, int, major event type, 0 means all event types. For details, refer
to Access Control Event Types. The value of this node is in decimal format
instead of hexadecimal format (for example, 1 refers to 0x1 which indicates
that the major type is MAJOR_ALARM)*/
    "minor":1024,
/*optional, int, minor event type, 0 means all event types. For details, refer
to Access Control Event Types. The value of this node is in decimal format
instead of hexadecimal format (for example, 1024 refers to 0x400 which
indicates that the minor type is MINOR_ALARMIN_SHORT_CIRCUIT)*/
    "startTime":"2016-12-12T17:30:08+08:00",
/*optional, string, start time (UTC time)*/
    "endTime":"2017-12-12T17:30:08+08:00",
/*optional, string, end time (UTC time)*/
    "picEnable":true,
/*optional, boolean, whether to upload events with pictures: true (yes), false
(no). The default value is true*/
    "beginSerialNo":1,
/*optional, int, start serial No.*/
    "endSerialNo":1,
/*optional, int, end serial No.*/
    "isAbnormalTemperature":true
/*optional, boolean, whether the skin-surface temperature is abnormal*/
}
```

See Also

[Access Control Event Types](#)

JSON_IdentityInfo

IdentityInfo message in JSON format

```
{
    "IdentityInfo":{
        "chnName":"",
/*optional, string, reserved*/
```

```
"enName":"",
/*optional, string, English name*/
"sex":"",
/*optional, string, gender: "male", "female"*/
"birth":"",
/*optional, string, date of birth, e.g., 1990-02-24*/
"addr":"",
/*optional, string, address*/
"IDCardNo":"",
/*optional, string, ID card No., it is the sensitive information that should be
encrypted*/
"issuingAuthority":"",
/*optional, string, authority*/
"startDate":"",
/*optional, string, start time of the validity period*/
"endDate":"",
/*optional, string, end time of the validity period*/
"passNo":"",
/*optional, string, entry-exit permit No.*/
"issueNumber":"",
/*optional, string, issuing times*/
"certificateType":"",
/*optional, string, certificate type*/
"permanentResidenceCardNo":"",
/*optional, string, permanent resident card No.*/
"nationalityOrAreaCode":"",
/*optional, string, country or region code*/
"version":"",
/*optional, string, certificate version No.*/
"receivingAuthorityCode":"",
/*optional, string, acceptance authority code*/
"FingerprintList": [
    "fingerprint"
]
/*optional, string, fingerprint information, it is encoded using base64*/
],
"pic"
/*optional, string, ID photo information, it is encoded using base64. The
encrypted data should be decrypted using the specific decryption library*/
}
```

JSON_IdentityInfoCap

IdentityInfoCap capability message in JSON format

```
{
    "IdentityInfoCap": {
        "IdentityInfoCond": { },
    }
/*optional, conditions of collecting ID card information*/
    "chnName": {
    }
/*optional, string, reserved*/
```

```
        "@min":0,
        "@max":0
    },
    "enName":{
/*optional, string, English name*/
        "@min":0,
        "@max":0
    },
    "sex":{
/*optional, string, gender: "male", "female"*/
        "@opt":["male", "female"]
    },
    "birth":{
/*optional, string, date of birth, e.g., 1990-02-24*/
        "@min":0,
        "@max":0
    },
    "addr":{
/*optional, string, address*/
        "@min":0,
        "@max":0
    },
    "IDCardNo":{
/*optional, string, ID card No.*/
        "@min":0,
        "@max":0
    },
    "issuingAuthority":{
/*optional, string, authority*/
        "@min":0,
        "@max":0
    },
    "startDate":{
/*optional, string, start time of the validity period*/
        "@min":0,
        "@max":0
    },
    "endDate":{
/*optional, string, end time of the validity period*/
        "@min":0,
        "@max":0
    },
    "passNo":{
/*optional, string, entry-exit permit No.*/
        "@min":0,
        "@max":0
    },
    "issueNumber:{
/*optional, string, issuing times*/
        "@min":0,
        "@max":0
    },

```

```
"certificateType":{  
/*optional, string, certificate type*/  
    "@min":0,  
    "@max":0  
},  
"permanentResidenceCardNo":{  
/*optional, string, permanent resident card No.*/  
    "@min":0,  
    "@max":0  
},  
"nationalityOrAreaCode":{  
/*optional, string, country or region code*/  
    "@min":0,  
    "@max":0  
},  
"version":{  
/*optional, string, certificate version No.*/  
    "@min":0,  
    "@max":0  
},  
"receivingAuthorityCode":{  
/*optional, string, acceptance authority code*/  
    "@min":0,  
    "@max":0  
},  
"FingerprintList":{  
    "maxSize":0,  
    "fingerprint":{  
/*optional, string, fingerprint information, it is encoded using base64. This  
field is the data size capability*/  
        "@min":0,  
        "@max":0  
    }  
},  
"pic":{  
/*optional, string, ID photo information, it is encoded using base64. This  
field is the data size capability*/  
    "@min":0,  
    "@max":0  
}  
}
```

JSON_IdentityInfoCond

IdentityInfoCond message in JSON format

```
{  
    "IdentityInfoCond":{ }  
/*currently there are no condition parameters, so this field can be set to
```

```
NULL*/  
}
```

JSON_ImportCustomAudioFile

JSON message about the custom audio file to be imported

```
{  
    "customAudioType": "callCenter",  
    /*required, string, type of the custom audio file: "callCenter" (calling the  
    center), "centerBusy" (the line is busy), "centerRefused" (the call is  
    declined), "centerOverTime" (unanswered), "swipeCard" (please swipe the card),  
    "thanks", "callAgain" (try again later), "verifyFailed" (authentication  
    failed), "verifySuccess" (authentication succeeded), "doorOpened" (the door is  
    opened), "wearSafetyHelmet" (please wear a hard hat), "wearMask" (please wear a  
    mask), "abnormalTemperature" (the skin-surface temperature is abnormal)*/  
    "filePathType": "URL",  
    /*required, string, file path type: "simpleStorage" (simple storage), "URL",  
    "localPath" (local storage), "binary"*/  
    "customAudioURL": "test"  
    /*optional, string, URL of the custom audio file, the maximum string size is  
    256 bytes. This node is required when the value of the node filePathType is  
    "URL"*/  
}
```

JSON_InfoFile

JSON message about the parameters of the user list file for offline collection

```
{  
    "InfoFile": {  
        "dataType": "binary",  
        /*required, string, data type of the file: "url", "binary"-binary data*/  
        "fileUrl": ""  
        /*dependent, string, file URL. This node is valid when the value of dataType is  
        "url"*/  
    }  
}
```

JSON_InfoFileProgress

JSON message about the progress of uploading the user list of offline collection

```
{  
    "InfoFileProgress": {  
        "percent":  
        /*required, int, percentage of the uploading progress*/  
    }
```

```
    }  
}
```

JSON_InfoFileTemplate

JSON message about parameters of the user list template of offline collection

```
{  
    "InfoFileTemplate":{  
        "dataType ":"binary",  
/*required, string, data type of the file: "url", "binary"-binary data*/  
        "fileUrl":""  
/*dependent, string, file URL, this field is valid when the value of dataType  
is "url"*/  
    }  
}
```

JSON_InfoFileTemplateCond

JSON message about the condition parameters of downloading the user list template of offline collection

```
{  
    "InfoFileTemplateCond":{  
        "dataType ":"binary"  
/*required, string, data type of the file: "url"-URL, "binary"-binary data*/  
    }  
}
```

JSON_IRCfg

JSON message about active infrared intrusion parameters

```
{  
    "IRCfg": {  
        "enable": ,  
/*required, boolean, whether to enable: true (yes), false (no)*/  
        "distance":  
/*optional, float, distance, unit: m*/  
    }  
}
```

JSON_IRCfgCap

JSON message about active infrared intrusion capability

```
{  
    "IRCfgCap": {  
        "enable": [true, false],  
        /*required, boolean, whether to enable*/  
        "distance": {  
            "@opt": [0.5, 1, 1.5]  
        }  
    }  
}
```

JSON_localIssueCfg

JSON message about rules for issuing smart cards

```
{  
    "localIssueCfg": {  
        "validFP": [1, 2],  
        /*optional, array of int, ID list of valid fingerprints. This node is valid for  
        applying fingerprint(s) to the card*/  
        "validFacePicture": "visible"  
        /*optional, string, type of valid face pictures: "visible"-face picture(s) in  
        visible light, "infrared"-face picture(s) in infrared light. This node is valid  
        for applying face picture(s) to the card*/  
    }  
}
```

JSON_LocalIssueRequest

JSON message about the parameters of sending a request for card issuing

```
{  
    "LocalIssueRequest": {  
        "operation": "face",  
        /*required, string, operation type: "face"-issue card containing face picture  
        information, "fingerprint"-issue card containing fingerprint information*/  
        "FPIIndex": 1,  
        /*optional, int, fingerprint storage index (in the card storage area). This  
        node is valid when the value of operation is "fingerprint"*/  
        "facePic": "visible"  
        /*optional, string, face picture type: "visible"-face picture in visible light,  
        "infrared"-face picture in infrared light. This node is valid when the value of  
        operation is "face"*/  
    }  
}
```

JSON_LocalIssueRes

JSON message about the current card issuing status and real-time card issuing results

```
{  
    "LocalIssueRes":{  
        "status":"ok",  
        /*required, string, card issuing status: "ok"-succeeded, "failed"-operation failed, "timeout"-timed out, "verifyFailure"-authentication failed, "noCard"-no card detected, "processing"*/  
        "cardNo": "",  
        /*optional, string, issued card No.*/  
        "cardErrorCode":  
        /*dependent, int, internal error code of card operation. This node is valid when the value of status is "failed"*/  
    }  
}
```

JSON_LockType

JSON message about the door lock status when the device is powered off

```
{  
    "LockType":{  
        "status":""  
        /*required, string, door lock status when the device is powered off:  
        "alwaysOpen"-remain open, "alwaysClose"-remain closed*/  
    }  
}
```

JSON_LockTypeCap

JSON message about the configuration capability of the door lock status when the device is powered off

```
{  
    "LockTypeCap":{  
        "status":{  
            /*required, string, door lock status when the device is powered off:  
            "alwaysOpen"-remain open, "alwaysClose"-remain closed*/  
            "@opt":["alwaysOpen", "alwaysClose"]  
        }  
    }  
}
```

JSON_LogModeCfg

LogModeCfg message in JSON format

```
{  
    "LogModeCfg":{  
        "type":  
            /*optional, integer, log mode: 1-16 bytes (the host log can be stored by 25w,  
            and the employee No. can be stored by 16 bytes), 2-12 bytes (the host log can  
            be stored by 25w, and the employee No. can be stored by 12 bytes). This node  
            will be set to 1 by default*/  
    }  
}
```

JSON_MaskDetection

Message about the mask detection parameters in JSON format.

```
{  
    "MaskDetection":{  
        "enable": ,  
        /*optional, boolean, whether to enable mask detection: true-enable, false-  
        disable*/  
        "noMaskStrategy":""  
        /*optional, string, door control strategy when not wearing mask is detected:  
        "noTipsAndOpenDoor"-open the door without prompt, "tipsAndOpenDoor"-prompt and  
        open the door (default), "tipsAndNotOpenDoor"-prompt and not open the door.  
        This field is valid when enable is true*/  
    }  
}
```

JSON_MaskDetectionCap

Message about the configuration capability of mask detection in JSON format.

```
{  
    "MaskDetectionCap":{  
        "enable":{  
            /*optional, boolean, whether to enable mask detection: true-enable, false-  
            disable*/  
            "@opt": [true, false]  
        },  
        "noMaskStrategy":{  
            /*optional, string, door control strategy when not wearing mask is detected:  
            "noTipsAndOpenDoor"-open the door without prompt, "tipsAndOpenDoor"-prompt and  
            open the door (default), "tipsAndNotOpenDoor"-prompt and not open the door.  
            This field is valid when enable is true*/  
            "@opt": ["noTipsAndOpenDoor", "tipsAndOpenDoor", "tipsAndNotOpenDoor"]  
        }  
    }  
}
```

```
    }
}
}
```

JSON_MultiCardCfg

MultiCardCfg message in JSON format

```
{
  "MultiCardCfg": {
    "enable": ,
    /*required, boolean, whether to enable multi-factor authentication*/
    "swipeIntervalTimeout": ,
    /*optional, integer, timeout of swiping (authentication) interval, which is
    between 1 and 255, and the default value is 10, unit: second*/
    "GroupCfg": [
      /*optional, multi-factor authentication parameters*/
      {
        "id": ,
        /*optional, integer, multi-factor authentication No., which is between 1 and
        20*/
        "enable": ,
        /*optional, boolean, whether to enable the multi-factor authentication*/
        "enableOfflineVerifyMode": ,
        /*optional, boolean, whether to enable verification mode when the access
        control device is offline (the super password will replace opening door
        remotely)*/
        "templateNo": ,
        /*optional, integer, schedule template No. to enable the multi-factor
        authentication*/
        "GroupCombination": [
          /*optional, parameters of the multi-factor authentication group*/
          {
            "enable": ,
            /*optional, integer, whether to enable the multi-factor authentication group*/
            "memberNum": ,
            /*optional, integer, number of members swiping cards*/
            "sequenceNo": ,
            /*optional, integer, serial No. of swiping cards of the multi-factor
            authentication group, which is between 1 and 8*/
            "groupNo": ,
            /*optional, integer, group No., 65534-super password, 65535-remotely open door*/
            " ]"
          }
        ]
      }
    }
}
```

JSON_MultiDoorInterLockCfg

MultiDoorInterLockCfg message in JSON format

```
{  
    "MultiDoorInterLockCfg": {  
        "enable": ,  
        /*required, boolean, whether to enable multi-door interlocking: "true"-yes,  
        "false"-no*/  
        "MultiDoorGroup": [{  
            /*optional, parameters of the multi-door interlocking group*/  
            "id": ,  
            /*optional, integer, multi-door interlocking No., which is between 1 and 8*/  
            "doorNoList":  
                /*optional, array, door No. list of multi-door interlocking, which is between 1  
                and 8. For example, [1,3,5] indicates that door No. 1, No. 3 and No. 5 will be  
                interlocked*/  
                []  
        }]  
    }  
}
```

JSON_NFCCfg

NFCCfg message in JSON format

```
{  
    "NFCCfg": {  
        "enable":  
        /*required, boolean, whether to enable NFC function: "true"-yes, "false"-no*/  
    }  
}
```

JSON_NFCCfgCap

NFCCfgCap capability message in JSON format

```
{  
    "NFCCfgCap": {  
        "enable": "true, false"  
        /*required, whether to enable NFC function: "true"-yes, "false"-no (default)*/  
    }  
}
```

JSON_OfflineCaptureCap

OfflineCaptureCap capability message in JSON format

```
{  
    "OfflineCaptureCap": {  
        "isSuportDownloadOfflineCaptureInfoTemplate": true,  
        /*optional, whether it supports downloading template of offline user list:  
        */  
    }  
}
```

```
"true"-yes, this node is not returned-no/
    "isSuportUploadOfflineCaptureInfo":true,
/*optional, whether it supports uploading offline user list: "true"-yes, this
node is not returned-no/
    "isSupportDownloadCaptureData":true,
/*optional, whether it supports downloading collected data: "true"-yes, this
node is not returned-no/
    "isSupportDeleteAllData":true,
/*optional, whether it supports deleting all collected data: "true"-yes, this
node is not returned-no/
    "isSupportDeleteTheData":true,
/*optional, whether it supports deleting specific collected data: "true"-yes,
this node is not returned-no/
    "SearchTask":{
        "supportFunction":{
/*required, string, supported methods, actually supported methods will be
returned*/
            "@opt":["put", "get", "delete", "post"]
        },
        "searchID":{
/*required, string, search ID which is used to check whether the upper-layer
clients are the same one/
            "@min":0,
            "@max":0
        },
        "maxResults":{
            "@min":0,
            "@max":0
        },
        "captureNoList":{
            "maxSize":0,
            "@min":0,
            "@max":0
        },
        "searchType":{
            "@opt":["new", "modified"]
        },
        "DataCollections":{
/*optional, array, matched data information that has been searched*/
            "maxSize":0,
            "captureNo":{
/*optional, integer, collection No.*/
                "@min":0,
                "@max":0
            },
            "name":{
/*optional, string, name*/
                "@min":0,
                "@max":0
            },
            "employeeNo":{
/*optional, string, employee No.*/

```

```

        "@min":0,
        "@max":0
    },
    "CardNoList":{
/*optional, string, card No. list*/
        "maxSize":0,
        "cardNo":{
            "@min": 0,
            "@max": 0
        },
        "cardType": {
/*optional, string, card type: "TypeA_M1", "TypeA_CPU", "TypeB", "ID_125K",
"FelicaCard", "DesfireCard"*/
            "@opt":
["TypeA_M1","TypeA_CPU","TypeB","ID_125K","FelicaCard","DesfireCard"]
        }
    },
    "IDCardNo":{
/*optional, string, ID card No.*/
        "@min":0,
        "@max":0
    },
    "FingerprintList":{
        "fingerprintID":{
            "@min":0,
            "@max":0
        },
        "fingerprint":{
/*optional, fingerprint information, it is encoded using base64*/
            "@min":0,
            "@max":0
        }
    },
    "FaceFeature":{
/*optional, string, facial feature information*/
        "isSupportFaceRegion":true,
/*optional, whether it supports facial feature area*/
        "isSupportCommonPoint":true
/*optional, whether it supports feature point coordinates (e.g., left eye,
right eye, left mouth corner, right mouth corner, nose)*/
    },
    "isSupportRiskMark":true,
/*optional, whether it supports risk data mark*/
    "dataType":{
/*optional, data type*/
        "@opt":["new", "modified", "normal"]
    },
    "IdentityInfo":{
/*identity information*/
        "chnName":{
/*optional, string, Chinese name*/
            "@min":0,

```

```
        "@max":0
    },
    "enName":{
/*optional, string, English name*/
        "@min":0,
        "@max":0
    },
    "sex":{
/*optional, string, gender: "male", "female"*/
        "@opt":["male", "female"]
    },
    "birth":{
/*optional, string, data of birth, e.g., "1990-02-24"*/
        "@min":0,
        "@max":0
    },
    "addr":{
/*optional, string, address*/
        "@min":0,
        "@max":0
    },
    "IDCardNo":{
/*optional, string, ID card No.*/
        "@min":0,
        "@max":0
    },
    "issuingAuthority":{
/*optional, string, issuing authority*/
        "@min":0,
        "@max":0
    },
    "startDate":{
/*optional, string, start date of validity period*/
        "@min":0,
        "@max":0
    },
    "endDate":{
/*optional, string, end date of validity period*/
        "@min":0,
        "@max":0
    },
    "passNo":{
/*optional, string, entry-exit permit No.*/
        "@min":0,
        "@max":0
    },
    "issueNumber":{
/*optional, string, issued times*/
        "@min":0,
        "@max":0
    },
    "certificateType":{
```

```

/*optional, string, certificate type*/
    "@min":0,
    "@max":0
},
"permanentResidenceCardNo":{
/*optional, string, permanent resident visa No.*/
    "@min":0,
    "@max":0
},
"nationalityOrAreaCode":{
/*optional, string, country/region code*/
    "@min":0,
    "@max":0
},
"version":{
/*optional, string, certificate version No.*/
    "@min":0,
    "@max":0
},
"receivingAuthorityCode":{
/*optional, string, acceptance authority code*/
    "@min":0,
    "@max":0
},
"FingerprintList":{
    "maxSize":0,
    "fingerprint":{
/*optional, string, fingerprint information, which should be encoded by Base64*/
        "@min":0,
        "@max":0
    }
},
"pic":{
/*optional, string, certificate picture information, which should be encoded by
Base64, encrypted and decrypted by a specific decryption library*/
    "@min":0,
    "@max":0
},
"CardIssueStatus":{
/*optional, issuing status list of cards containing face pictures and
fingerprints*/
    "@size":0,
/*optional, capability of number of elements in the array*/
    "face":{
/*optional, boolean, card issuing status of the face picture: true-with card
issued, false-without card issued*/
        "@opt": [true, false]
    },
    "fingerprint1":{
/*optional, boolean, card issuing status of the fingerprint 1: true-with card
issued, false-without card issued*/
    }
}
}

```

```

        "@opt": [true, false]
    },
    "fingerprint2": {
/*optional, boolean, card issuing status of the fingerprint 2: true-with card
issued, false-without card issued*/
        "@opt": [true, false]
    }
}
},
"RuleInfo": {
/*rule list, which lists rules for collecting different types of data*/
    "reqAdminRights": [true, false],
/*required, boolean, whether the administrator permission is required: "true"-yes, "false"-no*/
    "enableCardNoLenAuto": [true, false],
/*optional, boolean, whether to enable length self-adaption of the card serial
No.*/
    "maxSize": 0,
    "supportFunction": {
/*required, string, supported methods, actually supported methods will be
returned*/
        "@opt": ["put", "get", "delete", "post"]
    },
    "dataType": {
/*required, string, data type: "name", "employeeNo"-employee No., "IDCardNo"-ID
card No., "IDCardSerialNo"-ID card serial No., "IDCardDetails"-ID card
details, "card", "fingerprint"-fingerprint, "face"*/
        "@opt": ["name", "employeeNo", "IDCardNo", "IDCardSerialNo",
"IDCardDetails", "card", "fingerprint", "face"]
    },
    "enable": [true, false],
/*required, string, whether to collect and display: "true"-collect and display,
"false"-not collect and display*/
    "uniqueCheck": [true, false],
/*dependency, boolean, whether to enable uniqueness verification: "true"-yes,
"false" (default) or this node is not returned-no. This field is valid when
dataType is "name". For other data types, the field is the read-only optional
parameter*/
    "len": [
/*dependency, integer, data length. If dataType is "name", it refers to the
name length and the default value is 128. For other data types, this field is
the read-only optional parameter. This node will not be returned if it is not
supported. The capability list will be returned according to the data type*/
        "dataType": "",
        "@min": 0,
        "@max": 0
    ],
    "num": [
/*dependency, integer, number of collected data, this field is valid when
dataType is "fingerprint" or "card". The capability list will be returned
according to the data type*/

```

```

        "dataType":"",
        "@min":0,
        "@max":0
    }],
    "fingerprintIDs":{
/*dependency, integer, No. list of collected fingerprints, this field is valid
when dataType is "fingerprint"*/
        "maxSize":0,
        "@min":0,
        "@max":0
    },
    "enableLocalIssueCard": {
/*optional, boolean, whether to enable issuing smart cards locally*/
        "@opt": [true, false]
    },
    "isLocalStorage": {
/*optional, boolean, whether to store face picture and fingerprint information
in the device locally*/
        "@opt": [true, false]
    }
},
"CaptureProgress":{
    "supportFunction":{
/*required, string, supported methods, actually supported methods will be
returned*/
        "@opt":["put", "get", "delete", "post"]
    },
    "reqCaptureNum":{
/*optional, integer, total number of persons to be collected*/
        "@min":0,
        "@max":0
    },
    "completelyCaptureNum":{
/*optional, integer, number of completely collected persons*/
        "@min":0,
        "@max":0
    },
    "partiallyCaptureNum":{
/*optional, integer, number of partially collected persons*/
        "@min":0,
        "@max":0
    },
    "reqFaceNum":{
/*optional, integer, number of faces to be collected*/
        "@min":0,
        "@max":0
    },
    "faceNum":{
/*optional, integer, number of collected faces*/
        "@min":0,
        "@max":0
    }
},

```

```
"reqFingerprintNum":{  
/*optional, integer, number of fingerprints to be collected*/  
    "@min":0,  
    "@max":0  
},  
"fingerprintNum":{  
/*optional, integer, number of collected fingerprints*/  
    "@min":0,  
    "@max":0  
},  
"reqCardNum":{  
/*optional, integer, number of cards to be collected*/  
    "@min":0,  
    "@max":0  
},  
"cardNum":{  
/*optional, integer, number of collected cards*/  
    "@min":0,  
    "@max":0  
},  
"reqIDCardNum":{  
/*optional, integer, number of ID cards to be collected*/  
    "@min":0,  
    "@max":0  
},  
"IDCardNum":{  
/*optional, integer, number of collected ID cards*/  
    "@min":0,  
    "@max":0  
},  
"reqIssueNum":{  
/*optional, int, number of persons to be issued with smart cards*/  
    "@min": 0,  
    "@max": 0  
},  
"IssuedNum":{  
/*optional, int, number of persons that have been issued with smart cards*/  
    "@min": 0,  
    "@max": 0  
},  
"DataOutput":{  
    "supportFunction":{  
/*required, string, supported methods, actually supported methods will be  
returned*/  
        "@opt":["put", "get", "delete", "post"]  
    },  
    "password":{  
/*required, string, password for exporting*/  
        "@min":0,  
        "@max":0  
    },
```

```
"type": {
/*optional, string, exporting method, the default method is "USB"*/
    "@opt":"USB"
},
"progress": {
/*required, integer, exporting progress*/
    "@min":0,
    "@max":0
}
}
```

JSON_OSDPModify

OSDPModify message in JSON format

```
{
    "OSDPModify": {
        "newID": {
/*required, integer, new ID of the OSDP card reader*/
        }
    }
}
```

JSON_OSDPStatus

OSDPStatus message in JSON format

```
{
    "OSDPStatus": {
        "status": ""
/*required, string, online status: "online", "offline"*/
    }
}
```

JSON_PersonInfoExtendName

JSON message about the parameters of the name of the additional person information

```
{
    "PersonInfoExtendName": {
        "NameList": [
            {
                "id":1,
/*required, int, ID of the additional person information, it corresponds to the
id of PersonInfoExtends in the message JSON_UserInfo*/
                "name": "Student ID"
/*required, string, name of the additional person information*/
            }
        ]
    }
}
```

```
        }]
    }
}
```

See Also

[JSON UserInfo](#)

JSON_PersonInfoExtendNameCap

JSON message about the configuration capability of the name of the additional person information

```
{
  "PersonInfoExtendNameCap": {
    "NameList": {
      "@size": 1,
      /*required, int, maximum number of names that can be configured*/
      "id": {
        "@min": 1,
        "@max": 1
      },
      "name": {
        /*required, string, name of the additional person information*/
        "@min": 1,
        "@max": 1
      }
    }
  }
}
```

See Also

[JSON_Cap_UserInfo](#)

JSON_PhoneDoorRightCfg

PhoneDoorRightCfg message in JSON format

```
{
  "PhoneDoorRightCfg": {
    "openRight": ,
    /*optional, array, whether to have permission to open the door. For example,
    [1,3,5] indicates having permission to open the door No. 1, No. 3, and No. 5*/
    "closeRight": ,
    /*optional, array, whether to have permission to close the door. For example,
    [1,3,5] indicates having permission to close the door No. 1, No. 3, and No. 5*/
    "alwaysOpenRight": ,
    /*optional, array, whether to have permission to remain the door unlocked. For
    [1,3,5] indicates having permission to remain the door unlocked No. 1, No. 3, and No. 5*/
  }
}
```

```
example, [1,3,5] indicates having permission to remain the door No. 1, No. 3, and No. 5 unlocked*/  
    "alwaysCloseRight": ,  
/*optional, array, whether to have permission to remain the door locked. For example, [1,3,5] indicates having permission to remain the door No. 1, No. 3, and No. 5 locked*/  
    "armRight": ,  
/*optional, array, whether to have permission to arm the alarm input port. For example, [1,3,5] indicates having permission to arm the alarm input port No. 1, No. 3, and No. 5*/  
    "disarmRight":  
/*optional, array, whether to have permission to disarm the alarm input port. For example, [1,3,5] indicates having permission to disarm the alarm input port No. 1, No. 3, and No. 5*/  
    }  
}
```

JSON_PictureServerInformation

PictureServerInformation message in JSON format

```
{  
    "PictureServerInformation":{  
        "pictureServerType": "",  
/*required, string type, picture storage server type:  
"tomact,VRB,cloudStorage,KMS"*/  
        "addressingFormatType": "",  
/*required, string type, format type of the picture storage server address:  
"ipaddress"-IP address (default), "hostname"-host name*/  
        "hostName": "",  
/*string type, domain name of the picture storage server, the string length is between 0 and 64. This field is valid when addressingFormatType is "hostname"*/  
        "ipv4Address": "",  
/*string type, IPv4 address of the picture storage server, the string length is between 0 and 64. This field is valid when addressingFormatType is "ipaddress"*/  
        "ipv6Address": "",  
/*string type, IPv6 address of the picture storage server, the string length is between 0 and 128. This field is valid when addressingFormatType is "ipaddress"*/  
        "ipaddress": /  
        "portNo": ,  
/*required, integer type, port No. of the picture storage server, which is between 1024 and 65535*/  
        "underlyingProtocol": "",  
/*optional, string, bottom-level protocol of the picture storage server:  
"HTTP", "HTTPS". This field is valid when pictureServerType contains "cloudStorage". If this field does not exist, the default bottom-level protocol is HTTP*/  
        "cloudStorage": {  
/*parameters of the cloud storage server, which is valid when pictureServerType is "cloudStorage"*/  
            "cloudManageHttpPort": ,
```

```
/*required, integer type, HTTP port No. for central management of the cloud storage server, which is between 1024 and 65535*/
    "cloudTransDataPort": ,
/*required, integer type, data transmission port No. of the cloud storage server, which is between 1024 and 65535. This field is not supported by access control devices*/
    "cloudCmdPort": ,
/*required, integer type, signaling port No. of the cloud storage server, which is between 1024 and 65535*/
    "cloudHeartBeatPort": ,
/*required, integer type, heartbeat port No. of the cloud storage server, which is between 1024 and 65535. This field is not supported by access control devices*/
    "cloudStorageHttpPort": ,
/*required, integer type, HTTP port No. of the cloud storage server, which is between 1024 and 65535. This field is not supported by access control devices*/
    "cloudUsername":"",
/*required, string type, user name of the cloud storage server, the string length is between 0 and 32. This field is not supported by access control devices*/
    "cloudPassword":"",
/*required, string type, password of the cloud storage server, the string length is between 0 and 32. This field is not supported by access control devices*/
    "cloudPoolId": ,
/*required, integer type, cloud storage pool ID, which is between 1 and 4294967295. If this field is not configured by the upper-level, this field will be set to 1 by default*/
    "cloudPoolIdEx":"",
/*optional, string type, cloud storage pool ID, this node is valid when cloud storage pool ID of type string (cloud storage protocol in version 3.0) is supported*/
    "cloudProtocolVersion":"",
/*required, string type, protocol version of the cloud storage server, the string length is between 0 and 32*/
    "cloudAccessKey":"",
/*string type, cloud storage server access_key, the string length is between 0 and 64. This field is valid when cloudProtocolVersion is "V2.0"*/
    "cloudSecretKey":""
/*string type, cloud storage server secret_key, the string length is between 0 and 64. This field is valid when cloudProtocolVersion is "V2.0"*/
}
}
```

JSON_PrinterCfg

PrinterCfg message in JSON format

```
{
  "PrinterCfg": {
```

```
/*required, boolean, whether to enable the printer*/
    "enable": ,
    "printFormat": {
        "vistorPic": {
/*optional, visitor picture*/
            "enable": ,
/*required, boolean, whether to print visitor picture*/
            "lineNo": 
/*required, integer, line No.*/
            },
            "vistorName": {
/*optional, visitor name*/
                "enable": ,
/*required, boolean, whether to print visitor name*/
                "lineNo": 
/*required, integer, line No.*/
                },
                "certificateNumber": {
/*optional, visitor's certificate No.*/
                    "enable": ,
/*required, boolean, whether to print visitor's certificate No.*/
                    "lineNo": 
/*required, integer, line No.*/
                    },
                    "address": {
/*optional, visitor's address*/
                        "enable": ,
/*required, boolean, whether to print visitor's address*/
                        "lineNo": 
/*required, integer, line No.*/
                        },
                        "validity": {
/*optional, expiry date*/
                            "enable": ,
/*required, whether to print the expiry date*/
                            "lineNo": 
/*required, integer, line No.*/
                            },
                            "receptionDepartment": {
/*optional, reception department*/
                                "enable": ,
/*required, boolean, whether to print the reception department*/
                                "lineNo": 
/*required, integer, line No.*/
                                },
                                "receptionStaff": {
/*optional, receptionist information*/
                                    "enable": ,
/*required, boolean, whether to print the receptionist information*/
                                    "lineNo": 
/*required, integer, line No.*/
                                    },
```

```
        "registrationTime": {
/*optional, registered time*/
            "enable": ,
/*optional, whether to print the registered time*/
            "lineNo":
/*required, integer, line No.*/
        },
    }
}
```

JSON_QRCodeEvent

JSON message about the result of actively getting QR code scanning events

```
{
    "QRCodeEvent" : {
        "searchID": "",

/*required, string, search ID, which is used to check whether the current
search requester is the same as the previous one. If they are the same, the
search record will be stored in the device to speed up the next search*/
        "responseStatusStrg": "OK",
/*required, string, search status: "OK"(searching completed), "MORE"(searching
for more results), "NO MATCH"(no matched results)*/
        "numOfMatches": 1,
/*required, int, the number of the returned records*/
        "totalMatches": 1,
/*required, int, the total number of the matched records*/
        "InfoList" : [
/*optional, event information*/
            "deviceName": "",
/*optional, string, device name*/
            "serialNo": 1,
/*optional, int, event serial No.*/
            "QRCodeInfo": "",
/*required, string, QR code information*/
            "thermometryUnit": "",
/*optional, string, temperature unit: "celsius" (Celsius), "fahrenheit"
(Fahrenheit), "kelvin" (Kelvin), the default value is "celsius"*/
            "currTemperature": 1.0,
/*optional, float, face temperature, the value is accurate to one decimal
place*/
            "isAbnormalTemperature": true,
/*optional, boolean, whether the face temperature is abnormal: true (abnormal),
false (normal)*/
            "RegionCoordinates": {
/*optional, coordinates of the face temperature*/
                "positionX": 1,
/*optional, int, X-coordinate, the value is normalized to a number between 0
and 1000*/
                "positionY": 1
            }
        ]
    }
}
```

```
/*optional, int, Y-coordinate, the value is normalized to a number between 0  
and 1000*/
    },
    "mask": "",  
/*optional, string, whether the person wears a mask: "unknown" (unknown), "yes"  
(wearing a mask), "no" (no mask)*/
    "visibleLightPicUrl":"",
/*optional, string, the URL of the visible light picture*/
    "thermalPicUrl":"",
/*optional, string, the URL of the thermal picture*/
    "helmet": "",  
/*optional, string, whether the person wears a hard hat: "unknown" (unknown),  
"yes" (wearing a hard hat), "no" (no hard hat)*/
    "dateTime": "2016-12-12T17:30:08+08:00"
/*required, string, the time (UTC time) when the alarm is triggered, the  
maximum size is 32 bytes*/
    []
}
}
```

JSON_QRCodeEventCap

JSON message about the capability of actively getting QR code scanning events

```
{
    "QRCodeEventCap": {
        "QRCodeEventCond": {
            "searchID": {
/*required, string, search ID, which is used to check whether the current  
search requester is the same as the previous one. If they are the same, the  
search record will be stored in the device to speed up the next search*/
                "@min":1,
                "@max":1
            },
            "searchResultPosition": {
/*required, int, the start position of search result in the result list. In a  
single search, if you cannot get all the records in the result list, you can  
mark the end position and get the following records after the marked position  
in the next search. If the maximum number of totalMatches supported by the  
device is M and the number of totalMatches stored in the device now is N  
(N<=M), the valid range of this node is 0 to N-1*/
                "@min":1,
                "@max":1
            },
            "maxResults": {
/*required, int, the maximum number of search results that can be obtained by  
calling the URI this time. If the value of maxResults is greater than that  
defined in the device capability, the value in the capability will be returned.  
In this case, the device will not return error*/
                "@min":1,
                "@max":1
            }
        }
    }
}
```

```
        },
        "startTime": "1970-01-01T00:00:00+00:00",
/*optional, string, start time (UTC time)*/
        "endTime": "2017-12-12T17:30:08+08:00",
/*optional, string, end time (UTC time)*/
        "picEnable": {
/*optional, boolean, whether to upload the picture along with the event
information: true (all matched events will be uploaded with pictures if there
are any), false (all matched events will be uploaded without pictures). If this
node is not configured, the default value is true*/
            "@opt": [true, false]
        },
        "beginSerialNo": {
/*optional, int, start serial No.*/
            "@min": 1,
            "@max": 1
        },
        "endSerialNo": {
/*optional, int, end serial No.*/
            "@min": 1,
            "@max": 1
        }
    },
    "InfoList" : {
/*optional, event information*/
        "deviceName": {
/*optional, string, device name*/
            "@min": 1,
            "@max": 1
        },
        "serialNo": {
/*optional, int, event serial No.*/
            "@min": 1,
            "@max": 1
        },
        "QRCodeInfo": {
/*required, string, QR code information*/
            "@min": 1,
            "@max": 1
        },
        "thermometryUnit": {
/*optional, string, temperature unit: "celsius" (Celsius), "fahrenheitz"
(Fahrenheit), "kelvin" (Kelvin), the default value is "celsius"*/
            "@opt": ["celsius", "fahrenheitz", "kelvin"]
        },
        "currTemperature": {
/*optional, float, face temperature, the value is accurate to one decimal
place*/
            "@min": 1.0,
            "@max": 1.0
        },
        "isAbnormalTemperature": {
```

```
/*optional, boolean, whether the face temperature is abnormal: true (abnormal),  
false (normal)*/  
    "@opt": [true, false]  
,  
    "RegionCoordinates": {  
/*optional, coordinates of the face temperature*/  
        "positionX": {  
/*optional, int, X-coordinate, the value is normalized to a number between 0  
and 1000*/  
            "@min": 1,  
            "@max": 1  
,  
        "positionY": {  
/*optional, int, Y-coordinate, the value is normalized to a number between 0  
and 1000*/  
            "@min": 1,  
            "@max": 1  
,  
        }  
    },  
    "mask": {  
/*optional, string, whether the person wears a mask: "unknown" (unknown), "yes"  
(wearing a mask), "no" (no mask)*/  
        "@opt": ["unknown", "yes", "no"]  
,  
        "visibleLightPicUrl": {  
/*optional, string, the URL of the visible light picture*/  
            "@min": 1,  
            "@max": 1  
,  
        "thermalPicUrl": {  
/*optional, string, the URL of the thermal picture*/  
            "@min": 1,  
            "@max": 1  
,  
        "helmet": {  
/*optional, string, whether the person wears a hard hat: "unknown" (unknown),  
"yes" (wearing a hard hat), "no" (no hard hat)*/  
            "@opt": ["unknown", "yes", "no"]  
,  
            "dateTime": "2016-12-12T17:30:08+08:00"  
/*required, string, the time (UTC time) when the alarm is triggered, the  
maximum size is 32 bytes*/  
        }  
    }  
}
```

JSON_QRCodeEventCond

JSON message about the condition of actively getting QR code scanning events

```
{  
    "QRCodeEventCond": {  
        "searchID": "",  
        /*required, string, search ID, which is used to check whether the current  
        search requester is the same as the previous one. If they are the same, the  
        search record will be stored in the device to speed up the next search*/  
        "searchResultPosition": 0,  
        /*required, int, the start position of search result in the result list. In a  
        single search, if you cannot get all the records in the result list, you can  
        mark the end position and get the following records after the marked position  
        in the next search. If the maximum number of totalMatches supported by the  
        device is M and the number of totalMatches stored in the device now is N  
        (N<=M), the valid range of this node is 0 to N-1*/  
        "maxResults": 30,  
        /*required, int, the maximum number of search results that can be obtained by  
        calling the URI this time. If the value of maxResults is greater than that  
        defined in the device capability, the value in the capability will be returned.  
        In this case, the device will not return error*/  
        "startTime": "2016-12-12T17:30:08+08:00",  
        /*optional, string, start time (UTC time)*/  
        "endTime": "2017-12-12T17:30:08+08:00",  
        /*optional, string, end time (UTC time)*/  
        "picEnable": true,  
        /*optional, boolean, whether to upload the picture along with the event  
        information: true (all matched events will be uploaded with pictures if there  
        are any), false (all matched events will be uploaded without pictures). If this  
        node is not configured, the default value is true*/  
        "beginSerialNo": 1,  
        /*optional, int, start serial No.*/  
        "endSerialNo": 1  
        /*optional, int, end serial No.*/  
    }  
}
```

JSON_RegionCalibrationCfg

JSON message about the calibration parameters of the temperature measurement area

```
{  
    "enabled":true,  
    /*required, boolean, whether to enable calibration: true, false*/  
    "FaceFrameCoordinate":{  
        /*optional, object, coordinate of the face frame, the value is normalized to a  
        number between 0 and 1000*/  
        "height":1,  
        /*optional, int, height, value range: [0,1000]*/  
        "width":2,  
        /*optional, int, width, value range: [0,1000]*/  
        "x":5,  
        /*optional, int, X-coordinate, value range: [0,1000]*/  
    }  
}
```

```
    "y":10
/*optional, int, Y-coordinate, value range: [0,1000]*/
}
}
```

JSON_RegionCoordinate

JSON message about the parameters of the temperature measurement area

```
{
  "RegionCoordinate":[{
    /*required, array of object, coordinates of vertexes of the polygon. The number
    of vertexes of the polygon is between 3 and 10*/
    "x":1,
    /*optional, int, X-coordinate, the value is between 0 and 1000*/
    "y":2
    /*optional, int, Y-coordinate, the value is between 0 and 1000*/
  }]
}
```

JSON_RemoteCheck

Message about the parameters of verifying the access control event remotely in JSON format.

```
{
  "RemoteCheck":{
    "serialNo": ,
    /*required, int, event serial No. which should be the same as that in the event
    information message for uploading*/
    "checkResult":"",
    /*required, string, verification result: "success"-verified, "failed"-
    verification failed*/
    "info":""
    /*optional, string, additional information*/
  }
}
```

JSON_RemoteControlBuzzer

RemoteControlBuzzer message in JSON format

```
{
  "RemoteControlBuzzer":{
    "cmd":""
    /*required, string, command: "start"-start buzzing, "stop"-stop buzzing*/
  }
}
```

JSON_RemoteControlPWCfg

RemoteControlPWCfg message in JSON format

```
{  
    "RemoteControlPWCfg":{  
        "password":""  
    /*optional, string type, password for remote door control*/  
    }  
}
```

JSON_RemoteControlPWCheck

RemoteControlPWCheck message in JSON format

```
{  
    "RemoteControlPWCheck":{  
        "password":""  
    /*optional, string type, password for remote door control (or EZVIZ  
    verification code)*/  
    }  
}
```

JSON_ResponseStatus

ResponseStatus message in JSON format.

```
{  
    "requestURL":"",
/*optional, string type, request URL*/
    "statusCode": ,
/*required, integer type, status code*/
    "statusString":"",
/*required, string type, status description*/
    "subStatusCode":"",
/*required, string type, sub status code*/
    "errorCode": ,
/*optional, integer type, error code, which corresponds to subStatusCode, this
field is required when statusCode is not 1*/
    "errorMsg":"",
/*optional, string type, error details, this field is required when statusCode
is not 1*/
    "tryTimes":
/*optional, integer, number of retry attempts, it is returned when configuring
card encryption*/
}
```



See [**Response Codes of Text Protocol**](#) for details about the status codes, sub status codes, error codes, and error descriptions.

JSON_RFCardCfg

RFCardCfg message in JSON format

```
{  
    "RFCardCfg": [  
        {  
            "cardType": "",  
            /*required, string, card type: "EMCard"-EM card, "M1Card"-M1 card, "CPUCard"-  
            CPU card, "IDCard"-ID card, "DesfireCard"-DESFire card, "FelicaCard"-Felica  
            card*/  
            "enabled":  
            /*required, boolean, whether to enable RF card recognition: "true"-yes, "false"-  
            no*/  
        }  
    ]  
}
```

JSON_RFCardCfgCap

RFCardCfgCap capability message in JSON format

```
{  
    "RFCardCfgCap": {  
        "cardType": {  
            /*required, string, card type: "EMCard"-EM card, "M1Card"-M1 card, "CPUCard"-  
            CPU card, "IDCard"-ID card, "DesfireCard"-DESFire card, "FelicaCard"-Felica  
            card*/  
            "@opt": ["EMCard", "M1Card", "CPUCard", "IDCard"]  
        },  
        "enabled": {  
            /*required, boolean, whether to enable RF card recognition: "true"-yes, "false"-  
            no*/  
            "@opt": [true, false]  
        }  
    }  
}
```

JSON_RuleInfo

RuleInfo message in JSON format

```
{  
    "RuleInfo": {
```

```
"reqAdminRights": ,
/*required, boolean, whether the administrator permission is required: "true"-yes, "false"-no*/
"enableCardNoLenAuto": ,
/*optional, boolean, whether to enable length self-adaption of the card serial No. The priority of this field is higher than len*/
"RuleList":[{
/*rule list, which contains rules for collecting different types of data*/
    "dataType":"",
/*required, string, data type: "name", "employeeNo"-employee No., "IDCardNo"-ID card No., "IDCardSerialNo"-ID card serial No., "IDCardDetails"-ID card details, "card", "fingerprint"-fingerprint, "face"*/
    "enable": ,
/*required, boolean, whether to collect and display: "true"-collect and display, "false"-not collect and display*/
    "uniqueCheck": ,
/*dependency, boolean, whether to enable uniqueness verification: "true"-yes, "false" (default) or this field is not returned-no. This field is valid when dataType is "name". For other data types, this field is the read-only optional parameter*/
    "len": ,
/*dependency, integer, data length, this field is valid when dataType is "name", "employeeNo" or "card". The default data length of name is 128. For other data types, this field is the read-only optional parameter. If it is not supported, this field will not be returned*/
    "num": ,
/*dependency, integer, number of collected data, this field is valid when dataType is "fingerprint" or "card"*/
    "fingerprintIDs": 
/*dependency, integer, ID list of fingerprints that need to be collected, this field is valid when dataType is "fingerprint"*/
},
"enableLocalIssueCard": true,
/*optional, boolean, whether to enable issuing smart cards locally*/
"localStorage": false
/*optional, boolean, whether to store face picture and fingerprint information in the device locally*/
}
}]
```

JSON_SafetyHelmetDetection

JSON message about parameters of hard hat detection

```
{
    "SafetyHelmetDetection":{
        "enable":true,
/*optional, boolean, whether to enable hard hat detection: true-yes, false-no (default)*/
        "noHelmetStrategy":"" 
/*optional, string, door control strategy when not wearing hard hat is
```

```
detected: "normal"-open the door to allow access, "forbidden"-access is
prohibited*/
    }
}
```

JSON_SafetyHelmetDetectionCap

JSON message about the configuration capability of hard hat detection

```
{
  "SafetyHelmetDetectionCap": {
    "enable": {
      /*optional, boolean, whether to enable hard hat detection: true-yes, false-no
      (default)*/
      "@opt": [true, false]
    },
    "noHelmetStrategy": {
      /*optional, string, door control strategy when not wearing hard hat is
      detected: "normal"-open the door to allow access, "forbidden"-access is
      prohibited*/
      "@opt": ["normal", "forbidden"]
    }
  }
}
```

JSON_ScheduleMgrCap

JSON message about the schedule management capability set

```
{
  "ScheduleMgrCap": {
    "isSupportPostSchedule": true
    /*optional, boolean, whether it supports releasing program schedules*/
  }
}
```

JSON_SearchFaceRecordCond

Message about conditions of searching for face records, and it is in JSON format.

```
{
  "searchResultPosition": "",
  /*required, initial position of search result list, integer32 type. When there
  are multiple records, and cannot get all records in one time searching, you can
  search the records followed specified position for next search. For video
  intercom devices, this field can only be set to 0 as the picture will be
  returned along with the message*/
```

```
"maxResults": "",  
/*required, int32 type, maximum number of records for single searching. If  
maxResults exceeds the range defined by the device capability, the device will  
return the maximum number of records according to the device capability and  
will not return error. For video intercom devices, this field can only be set  
to 1 as the picture will be returned along with the message*/  
"faceLibType": "",  
/*required, face picture library type: "blackFD"-list library, "staticFD"-  
static library, string type, the maximum size is 32 bytes*/  
"FDID": "",  
/*required, face picture library ID, string type, the maximum size is 63*/  
"FPID": "",  
/*optional, string type, face record ID, it can be generated by device or  
inputted. If it is inputted, it should be the unique ID with the combination of  
letters and digits, and the maximum length is 63 bytes; if it is generated by  
the device automatically, it is the same as the employee No. (person ID)*/  
"startTime": "",  
/*optional, start time, ISO8601 time format, string type, the maximum size is  
32 bytes*/  
"endTime": "",  
/*optional, end time, ISO8601 time format, string type, the maximum size is 32  
bytes*/  
"name": "",  
/*optional, name, string type, the maximum size is 96 bytes*/  
"gender": "",  
/*optional, gender: male, female, unknown, string type, the maximum size is 10*/  
"city": "",  
/*optional, city code of birth for the person in the face picture, string type,  
the maximum size is 32 bytes*/  
"certificateType": "",  
/*optional, string type, the maximum size is 10 bytes, certificate type:  
"officerID"-officer ID, "ID"-identify card, passport, other*/  
"certificateNumber": ""  
/*optional, certificate No., string, the maximum size is 32 bytes*/  
"isInLibrary": "yes",  
/*optional, string type, whether the picture is in library (whether modeling is  
successful): unknown, no, yes*/  
"isDisplayCaptureNum": true,  
/*optional, boolean type, whether to display number of captured pictures, true:  
display, false: hide, by default it is false*/  
"rowKey ":"",  
/*optional, string type, face picture library main key. Search by rowKey can be  
more efficient, the maximum size is 64 bytes*/  
"transfer":true  
/*optional, boolean type, whether to enable transfer*/  
}
```

JSON_SearchFaceRecordResult

Message about result of searching for face record.

```
{
    "requestURL": "",
    "statusCode": ,
    "statusString": "",
    "subStatusCode": "",
    "errorCode": ,
    "errorMsg": "",

    /*see the description of this node and above nodes in the message of
    JSON_ResponseStatus*/
    "responseStatusStrg": "",

    /*optional, searching status: "OK"-searching ended, "NO MATCHES"-no data found,
    "MORE"-searching, string type, the max. size is 32 bytes. It is valid only when
    errorCode is 1 and errorMsg is ok*/
    "searchResultPosition": "",

    /*optional, initial position of search result list, integer32 type. It is valid
    only when errorCode is 1 and errorMsg is ok*/
    "numOfMatches": ,

    /*optional, returned number of results for current search, integer32. It is
    valid only when errorCode is 1 and errorMsg is ok*/
    "totalMatches": ,

    /*optional, total number of matched results, integer32. It is valid only when
    errorCode is 1 and errorMsg is ok*/
    "MatchList": [
        /*optional, searched matched data information, array. It is valid only when
        errorCode is 1 and errorMsg is ok*/
        {
            "FPID": "",

            /*optional, string type, face record ID (it is the same as the employee No.
            (person ID)), the maximum length is 63 bytes*/
            "FDID": "test",

            /*optional, string, face picture library ID, read-only*/
            "FDName": "List Library A",

            /*optional, string, face picture library name, read-only*/
            "faceURL": "",

            /*optional, face picture URL, string type, the maximum size is 128 bytes*/
            "name": "",

            /*required, name of person in the face picture, string type, the maximum size
            is 96 bytes*/
            "gender": "",

            /*optional, gender of person in the face picture: male, female, unknown, string
            type, the maximum size is 32 bytes*/
            "bornTime": "",

            /*required, birthday of person in the face picture, ISO8601 time format, string
            type, the maximum size is 20 bytes*/
            "city": "",

            /*optional, city code of birth for the person in the face picture, string type,
            the maximum size is 32 bytes*/
            "certificateType": "",

            /*optional, string type, the max. size is 10 bytes, certificate type:
            "officerID"-officer ID, "ID"-identify card, passport, other*/
            "certificateNumber": "",

            /*optional, certificate No., string, the max. size is 32 bytes*/
        }
    ]
}
```

```
    "caseInfo": "",  
    /*optional, case information, string type, the max. size is 192 bytes, it is  
    valid when faceLibType is blackFD.*/  
    "tag": "",  
    /*optional, custom tag, up to 4 tags, which are separated by commas, string  
    type, the max. size is 195 bytes, it is valid when faceLibType is blackFD.*/  
    "address": "",  
    /*optional, person address, string type, the max. size is 192 bytes, it is  
    valid when faceLibType is staticFD.*/  
    "customInfo": "",  
    /*optional, custom information, string type, the max. size is 192 bytes, it is  
    valid when faceLibType is staticFD.*/  
    "modelData":""  
    /*optional, string type, target model data, non-modeled binary data needs to be  
    encrypted by base64 during transmission*/  
    "isInLibrary": "yes",  
    /*optional, string type, whether the picture is in library (whether modeling is  
    successful): unknown, no, yes*/  
    "captureNum": 12,  
    /*optional, int, number of captured pictures*/  
    "rowKey": "",  
    /*optional, string type, face picture library main key. Search by rowKey can be  
    more efficient, the maximum size is 64 bytes*/  
    "saveFacePic": true  
    /*optional, boolean, whether to save face pictures*/  
    }  
]  
}
```

See Also

[JSONResponseStatus](#)

JSON_SearchTaskCond

SearchTaskCond message in JSON format

```
{  
    "SearchTaskCond":{  
        "searchID": "",  
        /*required, string, search ID which is used to check whether the upper-layer  
        clients are the same one*/  
        "searchResultPosition": ,  
        /*required, integer32, the start position of the search result in the result  
        list. When there are multiple records and you cannot get all search results at  
        a time, you can search for the records after the specified position next time.  
        If the device returns the picture along with the response message, this field  
        should be between 0 and totalMatches*/  
        "maxResults": ,  
        /*required, integer32, the maximum number of results that can be obtained by  
        calling the URL at a time. If the device returns the picture along with the
```

```
response message, this field can only be set to 1*/
    "captureNoList": ,
/*optional, integer, collection No. list. If the collection No. is not
configured, it will search all data according to searchResultPosition*/
    "searchType":""
/*optional, search type: "new"-search and only return newly added data,
"modified"-search and only return edited data. By default all data will be
searched*/
}
}
```

JSON_SearchTaskResponse

SearchTaskResponse message in JSON format

```
{
  "SearchTaskResponse": {
    "searchID": "",
/*required, string, search ID which is used to check whether the upper-layer
clients are the same one*/
    "responseStatusStrg": "",
/*optional, string, searching status: "OK"-searching completed, "NO MATCH"-no
matched results, "MORE"-searching for more results*/
    "numOfMatches": ,
/*optional, integer32, number of returned results this time*/
    "totalMatches": ,
/*optional, integer32, total number of matched results*/
    "DataCollections": [
/*optional, array, searched matched data information*/
      "lastCaptureNo": ,
/*required, integer, last collection No., it is used to check whether there is
data lost*/
      "captureNo": ,
/*required, integer, current collection No.*/
      "name": "",
/*optional, string, name*/
      "employeeNo": "",
/*optional, string, employee No.*/
      "IDCardNo": "",
/*optional, string, ID card No.*/
      "CardNoList": [
/*optional, string, card No. list*/
        "cardNo": "",
        "cardType": "TypeA_M1"
/*optional, string, card type: "TypeA_M1", "TypeA_CPU", "TypeB", "ID_125K",
"FelicaCard", "DesfireCard"*/
      ],
      "FingerprintList": [
        "fingerprintID": ,
/*optional, integer, fingerprint No.*/
        "fingerprint": ""
      ]
    ]
  }
}
```

```
/*optional, string, fingerprint information which is encoded using base64*/
    }],
    "FaceFeature":{
/*optional, feature information of face picture matting*/
    "Region":{
/*required, area coordinates of face picture matting, it is a rectangle*/
        "height": ,
/*required, float, height*/
        "width": ,
/*required, float, width*/
        "x": ,
/*required, float, X-coordinate of the left corner*/
        "y": ,
/*required, float, Y-coordinate of the left corner*/
        },
    "LeftEyePoint":{
/*optional, coordinates of the left eye*/
        "x": ,
/*required, float, X-coordinate, it is between 0.000 and 1*/
        "y": ,
/*required, float, Y-coordinate, it is between 0.000 and 1*/
        },
    "RightEyePoint":{
/*optional, coordinates of the right eye*/
        "x": ,
/*required, float, X-coordinate, it is between 0.000 and 1*/
        "y": ,
/*required, float, Y-coordinate, it is between 0.000 and 1*/
        },
    "LeftMouthPoint":{
/*optional, coordinates of the left mouth corner*/
        "x": ,
/*required, float, X-coordinate, it is between 0.000 and 1*/
        "y": ,
/*required, float, Y-coordinate, it is between 0.000 and 1*/
        },
    "RightMouthPoint":{
/*optional, coordinates of the right mouth corner*/
        "x": ,
/*required, float, X-coordinate, it is between 0.000 and 1*/
        "y": ,
/*required, float, Y-coordinate, it is between 0.000 and 1*/
        },
    "NoseTipPoint":{
/*optional, coordinates of the nose*/
        "x": ,
/*required, float, X-coordinate, it is between 0.000 and 1*/
        "y": ,
/*required, float, Y-coordinate, it is between 0.000 and 1*/
        }
    },
    "riskDataMark": ,
```

```
/*optional, boolean, whether to mark risk data: "true"-mark the data as the  
risk data and person and ID comparison failed, "false" or this field is not  
returned-the data is normal*/  
    "dataType": "",  
/*optional, string, data type and status: "new"-newly added data, "modified"-  
edited data, "normal"-unchanged data*/  
    "IdentityInfo": {  
/*identity information*/  
        "chnName": "",  
/*optional, string, Chinese name*/  
        "enName": "",  
/*optional, string, English name*/  
        "sex": "",  
/*optional, string, gender: "male", "female"*/  
        "birth": "",  
/*optional, string, data of birth, e.g., "1990-02-24"*/  
        "addr": "",  
/*optional, string, address*/  
        "IDCardNo": "",  
/*optional, string, ID card No.*/  
        "issuingAuthority": "",  
/*optional, string, issuing authority*/  
        "startDate": "",  
/*optional, string, start date of validity period*/  
        "endDate": "",  
/*optional, string, end date of validity period*/  
        "passNo": "",  
/*optional, string, entry-exit permit No.*/  
        "issueNumber": "",  
/*optional, string, issued times*/  
        "certificateType": "",  
/*optional, string, certificate type*/  
        "permanentResidenceCardNo": "",  
/*optional, string, permanent resident visa No.*/  
        "nationalityOrAreaCode": "",  
/*optional, string, country/region code*/  
        "version": "",  
/*optional, string, certificate version No.*/  
        "receivingAuthorityCode": "",  
/*optional, string, acceptance authority code*/  
        "FingerprintList": [{  
            "fingerprint": ""  
/*optional, string, fingerprint information, which should be encoded by Base64*/  
        }],  
        "pic": ""  
/*optional, string, certificate picture information, which should be encoded by  
Base64, encrypted and decrypted by a specific decryption library*/  
    },  
    "CardIssueStatus": [  
/*optional, issuing status list of cards containing face pictures and  
fingerprints*/  
        "cardNo": "",
```

```
/*optional, string, card information*/
    "face":true,
/*optional, boolean, card issuing status of the face picture: true-with card
issued, false-without card issued*/
    "fingerprint1":true,
/*optional, boolean, card issuing status of the fingerprint 1: true-with card
issued, false-without card issued*/
    "fingerprint2":true
/*optional, boolean, card issuing status of the fingerprint 2: true-with card
issued, false-without card issued*/
    }
}
}
}
```

JSON_SectionEncryption

JSON message about section encryption parameters

```
{
  "SectionEncryption": {
    "sectionNo": ,
/*required, integer, section No.*/
    "keyType": "",
/*required, string, key types: "private"-private key, "normal"-other valid
keys*/
    "password": ""
/*depend, string, a hexadecimal verification key, this field is valid only when
the keyType is "normal"*/
    "newKeyType": "",
/*required, string, new key types: "private"-private key, "normal"-other valid
keys*/
    "KeyA": "",
/*depend, string, a hexadecimal password of key A, this field is valid only
when the keyType is "normal"*/
    "KeyB": "",
/*depend, string, a hexadecimal password of key B, this field is valid only
when the keyType is "normal"*/
    "controlBits":
/*depend, a hexadecimal control bit, this field is valid only when the keyType
is "normal"*/
  }
}
```

JSON_SetFaceRecord

Message about the condition of setting the face record, and it is in JSON format.

```
{
    "faceURL":"",
    /*optional, string type, picture storage URL inputted when uploading the face
picture by URL, the maximum length is 256 bytes*/
    "faceLibType":"",
    /*required, string type, face picture library type: "blackFD"-list library,
"staticFD"-static library, the maximum length is 32 bytes*/
    "FDID":"",
    /*required, string type, face picture library ID, the maximum length is 63
bytes*/
    "FPID":"",
    /*optional, string type, face record ID, it can be generated by the device or
inputted. If it is inputted, it should be the unique ID with the combination of
letters and digits, and the maximum length is 63 bytes; if it is generated by
the device automatically, it is the same as the employee No. (person ID)*/
    "deleteFP": ,
    /*optional, boolean type, whether to delete the face record: "true"-yes. This
node is required when the face record needs to be deleted; for adding or
editing the face record, this node should be set to NULL*/
    "name":"",
    /*required, string type, name of the person in the face picture, the maximum
length is 96 bytes*/
    "gender":"",
    /*optional, string type, gender of the person in the face picture: "male",
"female", "unknown", the maximum length is 32 bytes*/
    "bornTime":"",
    /*required, string type, date of birth of the person in the face picture in
ISO8601 time format, the maximum length is 20 bytes*/
    "city":"",
    /*optional, string type, code of the city of birth for the person in the face
picture, the maximum length is 32 bytes*/
    "certificateType":"",
    /*optional, string type, ID type: "officerID"-officer ID, "ID"-ID card. The
maximum length is 10 bytes*/
    "certificateNumber":"",
    /*optional, string type, ID No., the maximum length is 32 bytes*/
    "caseInfo":"",
    /*optional, string type, case information, the maximum length is 192 bytes, it
is valid when faceLibType is "blackFD"*/
    "tag":"",
    /*optional, string type, custom tag, up to 4 tags can be added and they should
be separated by commas, the maximum length of each tag is 48 bytes, and the
maximum length of this node is 195 bytes. It is valid when faceLibType is
"blackFD"*/
    "address":"",
    /*optional, string type, person address, the maximum length is 192 bytes, it is
valid when faceLibType is "staticFD"*/
    "customInfo":"",
    /*optional, string type, custom information, the maximum length is 192 bytes,
it is valid when faceLibType is "staticFD"*/
    "modelData":"",
    /*optional, string type, target model data, non-modeled binary data needs to be

```

```
encrypted by base64 during transmission*/
    "PicFeaturePoints": [
/*optional, array of object, feature points to be applied. If the device only
supports three types of feature points, when the platform applies more than
three types of feature points, the device will not return error information*/
        "featurePointType": "face",
/*required, string, feature point type: "face", "leftEye" (left eye),
"rightEye" (right eye), "leftMouthCorner" (left corner of mouth),
"rightMouthCorner" (right corner of mouth), "nose"*/
        "coordinatePoint": {
/*required, object, coordinates of the feature point*/
            "x": 1,
/*required, int, normalized X-coordinate which is between 0 and 1000*/
            "y": 1,
/*required, int, normalized Y-coordinate which is between 0 and 1000*/
            "width": 1,
/*required, int, width which is between 0 and 1000. This node is required when
featurePointType is "face"*/
            "height": 1
/*required, int, height which is between 0 and 1000. This node is required when
featurePointType is "face"*/
        }
    ],
    "saveFacePic": true
/*optional, boolean, whether to save face pictures*/
}
```

JSON_SingleFPLibInfo

Message about the information of a face picture library, and it is in JSON format.

```
{
    "requestURL": "",
    "statusCode": "",
    "statusString": "",
    "subStatusCode": "",
    "errorCode": "",
    "errorMsg": "",
/*see the description of this node and above nodes in the message of
JSON_ResponseStatus*/
    "faceLibType": "",
/*optional, face picture library type: "blackFD"-list library, "staticFD"-static
library, string type, the max. string length is 32 bytes*/
    "name": "",
/*optional, face picture library name, string type, the max. string length is
48 bytes*/
    "customInfo": "",
/*optional, custom information, string type, the max. string length is 192
bytes*/
    "libArmingType": "armingLib",
/*optional, string, arming type of the list library: "armingLib" (armed face
```

```
picture library), "nonArmingLib" (not armed face picture library). The default
value is "armingLib"*/
    "libAttribute": "blackList",
/*optional, string, library type: "blackList" (blocklist library), "VIP" (VIP
library), "passerby" (passerby library). The passerby library cannot be
deleted*/
    "personnelFileEnabled": true
/*optional, boolean, whether to enable personnel archive configuration, read-
only*/
}
```

See Also

[JSON ResponseStatus](#)

JSON_SmsRelativeParam

SmsRelativeParam message in JSON format

```
{
  "SmsRelativeParam": {
    "WhiteList": [
      /*required, mobile phone number allowlist*/
      "id": ,
      /*required, integer, No. of mobile phone number allowlist*/
      "phoneNo": "",
      /*required, string, mobile phone number*/
      "doorControl": ,
      /*optional, boolean, whether to support door operation control: "true"-yes,
      "false"-no*/
      "acsPassword": ""
      /*optional, string, command to open the door*/
    ]
  }
}
```

JSON_TemperatureMeasurementCfg

JSON message about the temperature measurement parameters

```
{
  "showTemperatureInfo":true,
/*optional, boolean, whether to display the temperature information: true,
false*/
  "saveThermalPicture":true,
/*optional, boolean, whether to save the thermal picture: true, false*/
  "uploadThermalPicture":true,
/*optional, boolean, whether to upload the thermal picture: true, false*/
  "lowTemperatureEnabled":true
}
```

```
/*optional, boolean, whether to enable temperature measurement in the low-  
temperature environment: true, false*/  
}
```

JSON_TTSText

JSON message about the text parameters of the audio prompt for the authentication results

```
{  
    "TTSText":{  
        "enable": ,  
/*required, boolean, whether to enable: true-enable, false-disable*/  
        "prefix": "",  
/*optional, string, whether to play the audio with "user name" or "honorific  
and last name of the user" as the prefix: "name"-play the audio with "user  
name" (e.g., "Jack Smith" will be played), "lastname"-play the audio with  
"honorific and last name of the user" (e.g., "Mr. Smith" will be played),  
"none" (default)*/  
        "Success":[] {  
            "TimeSegment":{  
/*optional, time period*/  
                "beginTime": "",  
/*required, string, start time, which is between 00:00:00 and 23:59:59*/  
                "endTime": ""  
/*required, string, end time, which is between 00:00:00 and 23:59:59*/  
            },  
            "language": "",  
/*optional, string, language: "SimChinese,TraChinese,English"*/  
            "text": ""  
/*required, string, text of the audio prompt*/  
        },  
        "Failure":[] {  
            "TimeSegment":{  
/*optional, time period*/  
                "beginTime": "",  
/*required, string, start time, which is between 00:00:00 and 23:59:59*/  
                "endTime": ""  
/*required, string, end time, which is between 00:00:00 and 23:59:59*/  
            },  
            "language": "",  
/*optional, string, language: "SimChinese,TraChinese,English"*/  
            "text": ""  
/*required, string, text of the audio prompt*/  
        }  
    }  
}
```

JSON_TTSTextCap

JSON message about the text configuration capability of the audio prompt for the authentication results

```
{  
    "TTSTextCap":{  
        "enable":[true, false],  
        /*required, boolean, whether to enable: true-enable, false-disable*/  
        "prefix":["name", "lastname", "none"],  
        /*optional, string, whether to play the audio with "user name" or "honorific  
        and last name of the user" as the prefix: "name"-play the audio with "user  
        name" (e.g., "Jack Smith" will be played), "lastname"-play the audio with  
        "honorific and last name of the user" (e.g., "Mr. Smith" will be played),  
        "none" (default)*/  
        "Success":{  
            "maxSize":4,  
            "TimeSegment":{  
                "beginTime": "",  
                /*required, string, start time, which is between 00:00:00 and 23:59:59*/  
                "endTime": "",  
                /*required, string, end time, which is between 00:00:00 and 23:59:59*/  
                "validUnit":""  
                /*optional, string, time accuracy: "hour", "minute", "second". If this field is  
                not returned, it indicates that the default time accuracy is "minute"*/  
            },  
            "language":{  
                /*optional, string, language: "SimChinese", "TraChinese", "English"*/  
                "@opt":["SimChinese", "TraChinese", "English"]  
            },  
            "text":{  
                /*required, string, text of the audio prompt*/  
                "@min": ,  
                "@max":  
            }  
        },  
        "Failure":{  
            "maxSize":4,  
            "TimeSegment":{  
                "beginTime": "",  
                /*required, string, start time, which is between 00:00:00 and 23:59:59*/  
                "endTime": "",  
                /*required, string, end time, which is between 00:00:00 and 23:59:59*/  
                "validUnit":""  
                /*optional, string, time accuracy: "hour", "minute", "second". If this field is  
                not returned, it indicates that the default time accuracy is "minute"*/  
            },  
            "language":{  
                /*optional, string, language: "SimChinese", "TraChinese", "English"*/  
                "@opt":["SimChinese", "TraChinese", "English"]  
            },  
        }  
    }  
}
```

```
        "text":{  
/*required, string, text of the audio prompt*/  
        "@min": ,  
        "@max":  
    }  
}  
}  
}
```

JSON_UploadFailedDetails

JSON message about the details of failing to upload the user list of offline collection

```
{  
    "UploadFailedDetails":{  
        "description":""  
/*required, string, details of failing to uploading the user list of offline  
collection, including detailed error descriptions and reports*/  
    }  
}
```

JSON_UserInfo

JSON message about the person information

```
{  
    "UserInfo":{  
        "employeeNo":"",
/*required, string, employee No. (person ID)*/
        "deleteUser": ,
/*optional, boolean, whether to delete the person: "true"-yes. This node is  
required only when the person needs to be deleted; for adding or editing person  
information, this node can be set to NULL*/
        "name":"",
/*optional, string, person name*/
        "userType":"",
/*required, string, person type: "normal"-normal person (household), "visitor",  
"blackList"-person in blocklist*/
        "closeDelayEnabled": ,
/*optional, boolean, whether to enable door close delay: "true"-yes, "false"-  
no*/
        "Valid":{  
/*required, parameters of the effective period, the effective period can be a  
period of time between 1970-01-01 00:00:00 and 2037-12-31 23:59:59*/
            "enable": ,
/*required, boolean, whether to enable the effective period: "false"-disable,  
"true"-enable. If this node is set to "false", the effective period is  
permanent*/
            "beginTime":"",

```

```

/*required, start time of the effective period (if timeType does not exist or
is "local", the beginTime is the device local time, e.g., 2017-08-01T17:30:08;
if timeType is "UTC", the beginTime is UTC time, e.g.,
2017-08-01T17:30:08+08:00)*/
    "endTime":"",
/*required, end time of the effective period (if timeType does not exist or is
"local", the endTime is the device local time, e.g., 2017-08-01T17:30:08; if
timeType is "UTC", the endTime is UTC time, e.g., 2017-08-01T17:30:08+08:00)*/
    "timeType":"",
/*optional, string, time type: "local"- device local time, "UTC"- UTC time*/
},
"belongGroup":"",
/*optional, string, group*/
"password":"",
/*optional, string, password*/
"doorRight":"",
/*optional, string, No. of the door or lock that has access permission, e.g.,
"1,3" indicates having permission to access door (lock) No. 1 and No. 3*/
    "RightPlan":{},
/*optional, door permission schedule (lock permission schedule)*/
    "doorNo": ,
/*optional, integer, door No. (lock ID)*/
    "planTemplateNo":"",
/*optional, string, schedule template No.*/
},
"maxOpenDoorTime": ,
/*optional, integer, maximum authentication attempts, 0-unlimited*/
    "openDoorTime": ,
/*optional, integer, read-only, authenticated attempts*/
    "roomNumber": ,
/*optional, integer, room No.*/
    "floorNumber": ,
/*optional, integer, floor No.*/
    "doubleLockRight": ,
/*optional, boolean, whether to have the permission to open the double-locked
door: "true"-yes, "false"-no*/
    "localUIRight": ,
/*optional, boolean, whether to have the permission to access the device local
UI: "true"-yes, "false"-no*/
    "localUIUserType":"",
/*optional, string, user type of device local UI: "admin" (administrator),
"operator", "viewer" (normal user). This node is used to distinguish different
users with different operation permissions of device local UI*/
    "userVerifyMode":"",
/*optional, string, person authentication mode: "cardAndPw"-card+password,
"card"-card, "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password,
"fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password,
"faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint,
"faceAndPw"-face+password, "faceAndCard"-face+card, "face"-face, "employeeNoAndPw"-employee No.+password,
"fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint,
"employeeNoAndFpAndPw"-employee No.+fingerprint+password,

```

```
"faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password
+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face
or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or
password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or
fingerprint, "cardOrFpOrPw"-card or fingerprint or password. The priority of
the person authentication mode is higher than that of the card reader
authentication mode*/
    "checkUser": ,
/*optional, boolean, whether to verify the duplicated person information:
"false"-no, "true"-yes. If checkUser is not configured, the device will verify
the duplicated person information by default. When there is no person
information, you can set checkUser to "false" to speed up data applying;
otherwise, it is not recommended to configure this node*/
    "addUser": ,
/*optional, boolean type, whether to add the person if the person information
being edited does not exist: "false"-no (if the device has checked that the
person information being edited does not exist, the failure response message
will be returned along with the error code), "true"-yes (if the device has
checked that the person information being edited does not exist, the success
response message will be returned, and the person will be added). If this node
is not configured, the person will not be added by default*/
    "dynamicCode": "123456",
/*optional, string, dynamic permission code, this node is write-only*/
    "callNumbers": [ "", "", "" ],
/*optional, string type, room No. list to be called, by default, its format is
X-X-X-X (e.g., 1-1-1-401), which is extended from roomNumber; for standard SIP,
it can be the SIP number*/
    "floorNumbers": [ , ],
/*optional, integer type, floor No. list, which is extended from floorNumber*/
    "numOfFace": ,
/*optional, read-only, number of linked face pictures. If this field is not
returned, it indicates that this function is not supported*/
    "numOfFP": ,
/*optional, read-only, number of linked fingerprints. If this field is not
returned, it indicates that this function is not supported*/
    "numOfCard": ,
/*optional, read-only, number of linked cards. If this field is not returned,
it indicates that this function is not supported*/
    "gender": "",
/*optional, string, gender of the person in the face picture: "male", "female",
"unknown"*/
    "PersonInfoExtends": [
/*optional, array of object, extended fields for the additional person
information. This node is used to configure the extended person information
displayed on the device's UI. For MinMoe series facial recognition terminals,
currently only one value node can be supported for displaying the employee No.
and the node id is not supported*/
        "id":1,
/*optional, int, extended ID of the additional person information, value range:
[1,32]. It corresponds to the id in the message of the request URI /ISAPI/
AccessControl/personInfoExtendName?format=json and is used to link the value of
the node value and its name (the node name in the message of the request URI /
```

```
ISAPI/AccessControl/personInfoExtendName?format=json). If the node id does not exist, the ID will start from 1 by default according to the array order*/
    "value": ""
/*optional, string, extended content of the additional person information*/
    }],
    "operateType": "byTerminal",
/*optional, string, operation type: "byTerminal"-by terminal*/
    "terminalNoList": [1],
/*optional, array, terminal ID list, this node is required when operation type is "byTerminal"; currently, only one terminal is supported*/
    "groupId":1,
/*optional, int, department No. of local time and attendance*/
    "localAtndPlanTemplateId":1
/*optional, int, schedule template of local time and attendance. If this node exist, it indicates that there are shift schedule settings by individual. If id is 0, it indicates canceling the shift schedule of the person*/
    }
}
```

JSON_UserInfoCount

UserInfoCount message in JSON format

```
{
  "UserInfoCount": {
    "userNumber": 0
  }
}
```

JSON_UserInfoDelCond

JSON message about user information to be deleted

```
{
  "UserInfoDelCond": {
    "EmployeeNoList": [
      /*optional, person ID list (if this node does not exist or is set to NULL, it indicates deleting all person information)*/
      "employeeNo": ""
    ],
    "operateType": "byTerminal",
    /*optional, string, operation type: "byTerminal"-by terminal*/
    "terminalNoList": [1]
  }
}
```

```
    }
}
```

JSON_UserInfoDetail

JSON message about user information

```
{
  "UserInfoDetail": {
    "mode": "",
    /*required, string, deleting mode: "all"-delete all, "byEmployeeNo"-delete by
employee No. (person ID)*/
    "EmployeeNoList": [
      /*optional, person ID list, if this node does not exist or is null, it
indicates deleting all person information (including linked cards and
fingerprints) and permissions*/
      "employeeNo": ""
      /*optional, string, employee No. (person ID), it is valid when mode is
"byEmployeeNo"*/
    ],
    "operateType": "byTerminal",
    /*optional, string, operation type: "byTerminal"-by terminal, "byOrg"-by
organization, "byTerminalOrg"-by terminal organization*/
    "terminalNoList": [ 1, 2, 3, 4 ],
    /*optional, array, terminal ID list, this node is required when operation type
is "byTerminal" or "byTerminalOrg"*/
    "orgNoList": [ 1, 2, 3, 4 ]
    /*optional, array, organization ID list, this node is required when operation
type is "byOrg" or "byTerminalOrg"*/
  }
}
```

JSON_UserInfoDetailDeleteProcess

UserInfoDetailDeleteProcess message in JSON format

```
{
  "UserInfoDetailDeleteProcess": {
    "status": ""
    /*required, string type, status: "processing", "success", "failed"*/
  }
}
```

JSON_UserInfoSearch

UserInfoSearch message in JSON format

```
{
    "UserInfoSearch": {
        "searchID": "",  

        /*required, string type, search ID, which is used to confirm the upper-level  

        platform or system. If the platform or the system is the same one during two  

        searching, the search history will be saved in the memory to speed up next  

        searching*/
        "responseStatusStrg": "",  

        /*required, string, search status: "OK"-searching completed, "NO MATCH"-no  

        matched results, "MORE"-searching for more results*/
        "numOfMatches": ,  

        /*required, integer32, number of returned results this time*/
        "totalMatches": ,  

        /*required, integer32, total number of matched results*/
        "UserInfo": [{  

            /*optional, person information*/
            "employeeNo": "",  

            /*required, string, employee No. (person ID)*/
            "name": "",  

            /*optional, string, person name*/
            "userType": "",  

            /*required, string, person type: "normal"-normal person (household), "visitor",  

            "blackList"-person in blocklist*/
            "closeDelayEnabled": ,  

            /*optional, boolean, whether to enable door close delay: "true"-yes, "false"-  

            no*/
            "Valid": {  

                /*required, parameters of the effective period*/
                "enable": "",  

                /*required, boolean, whether to enable the effective period: "false"-disable,  

                "true"-enable. If this node is set to "false", the effective period is  

                permanent*/
                "beginTime": "",  

                /*required, start time of the effective period (if timeType does not exist or  

                is "local", the beginTime is the device local time, e.g., 2017-08-01T17:30:08;  

                if timeType is "UTC", the beginTime is UTC time, e.g.,  

                2017-08-01T17:30:08+08:00)*/
                "endTime": "",  

                /*required, end time of the effective period (if timeType does not exist or is  

                "local", the endTime is the device local time, e.g., 2017-08-01T17:30:08; if  

                timeType is "UTC", the endTime is UTC time, e.g., 2017-08-01T17:30:08+08:00)*/
                "timeType": ""  

            },  

            "belongGroup": "",  

            /*optional, string, group*/
            "password": "",  

            /*optional, string, password*/
            "doorRight": "",  

            /*optional, string, No. of door or lock that has access permission, e.g., "1,3"  

            indicates having permission to access door (lock) No. 1 and No. 3*/
            "RightPlan": [{  

        }
    }
}
```

```
/*optional, access permission schedule of the door or lock*/
    "doorNo": ,
/*optional, integer, door No. (lock ID)*/
    "planTemplateNo":"""
/*optional, string, schedule template No.*/
    ],
    "maxOpenDoorTime": ,
/*optional, integer, the maximum authentication attempts, 0-unlimited*/
    "openDoorTime": ,
/*optional, integer, read-only, authenticated attempts*/
    "roomNumber": ,
/*optional, integer, room No.*/
    "floorNumber": ,
/*optional, integer, floor No.*/
    "doubleLockRight": ,
/*optional, boolean, whether to have the permission to open the double-locked
door: "true"-yes, "false"-no*/
    "localUIRight": ,
/*optional, boolean, whether to have the permission to access the device local
UI: "true"-yes, "false"-no*/
    "localUIUserType":"",
/*optional, string, user type of device local UI: "admin" (administrator),
"operator", "viewer" (normal user). This node is used to distinguish different
users with different operation permissions of device local UI*/
    "userVerifyMode":"",
/*optional, string, person authentication mode: "cardAndPw"-card+password,
"card"-card, "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password,
"fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-fingerprint+card+password,
"faceOrFpOrCardOrPw"-face or fingerprint or card or password, "faceAndFp"-face+fingerprint,
"faceAndPw"-face+password, "faceAndCard"-face+card, "face"-face, "employeeNoAndPw"-employee No.+password,
"fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint,
"employeeNoAndFpAndPw"-employee No.+fingerprint+password,
"faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint,
"employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card,
"fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password,
"cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint,
"cardOrFpOrPw"-card or fingerprint or password. The priority of the person authentication mode is higher than that of the card reader authentication mode*/
    "dynamicCode": "123456",
/*optional, string, dynamic permission code, this node is write-only*/
    "callNumbers": ["","",""],
/*optional, array of string, list of called numbers, the default rule is "X-X-X-X",
e.g., "1-1-1-401". This node is the extension of the node roomNumber. When
the number list is supported, you need to use this node to configure
parameters*/
    "floorNumbers": [1,2],
/*optional, array of int, floor No. list. This node is the extension of
floorNumber. When the number list is supported, you need to use this node to
configure parameters*/
    "numOfFace":0,
```

```
/*optional, int, number of linked face pictures. This node is read-only and if
it is not returned, it indicates that this function is not supported*/
    "numOfFP":0,
/*optional, int, number of linked fingerprints. This node is read-only and if
it is not returned, it indicates that this function is not supported*/
    "numOfCard":0,
/*optional, int, number of linked cards. This node is read-only and if it is
not returned, it indicates that this function is not supported*/
    "gender":"",
/*optional, string, gender of the person in the face picture: "male", "female",
"unknown"*/
    "PersonInfoExtends":{},
/*optional, array of object, extended fields for the additional person
information. This node is used to configure the extended person information
displayed on the device's UI. For MinMoe series facial recognition terminals,
currently only one value node can be supported for displaying the employee No.
and the node id is not supported*/
    "id":1,
/*optional, int, extended ID of the additional person information, value range:
[1,32]. It corresponds to the id in the message of the request URI /ISAPI/
AccessControl/personInfoExtendName?format=json and is used to link the value of
the node value and its name (the node name in the message of the request URI /
ISAPI/AccessControl/personInfoExtendName?format=json). If the node id does not
exist, the ID will start from 1 by default according to the array order*/
    "value":""
/*optional, string, extended content of the additional person information*/
},
    "groupName": "test",
/*optional, string. group name, range:[1,64]*/
    "age": 0,
/*optional, integer, age, range:[0,120]*/
    "PatientInfos": {
/*optional, object, patient infomation*/
        "deviceID": "test",
/*optional, string, device number*/
        "admissionTime": "1970-01-01T00:00:00+08:00",
/*optional, datetime, hospitalized date*/
        "chargeNurse": "test",
/*optional, string, nurse in charge, range:[0,32]*/
        "chargeDoctor": "test",
/*optional, string, doctor in charge, range:[0,32]*/
        "nursingLevel": "tertiary",
/*optional, enumerate, nursing level*/
        "doctorsAdvice": "test",
/*optional, string, advice from doctor, range:[0,128]*/
        "allergicHistory ": "test"
/*optional, string, allergy, range:[0,128]*/
},
    "TromboneRule": {
/*optional, object, trombone rule*/
        "industryType": "builidings",
/*optional, string, industry type*/

```

```
        "unitType": "indoor",
/*optional, string, device type, indoor (idoor station), villa (villa outdoor
station), confirm (double confirm), outdoor (outdoor station), fence (outer
door station), doorbell (doorbell), manage (master station), acs (access
control device), wardStation (ward extension), bedheadExtension (bedhead
extension), bedsideExtension (bedside extension), terminal (terminal), netAudio
(network audio), interactive (interactive terminal), amplifier (amplifier)*/
        "SIPVersion": "V10"
/*optional, string, private SIP version, range:[0,32]*/
    },
    "ESDType": "handAndFoot"
/*optional, enumerate, ESD detection type: handAndFoot (detect both hand and
foot), no (no detection), hand (detect hand), foot (detect foot)*/
}
}
```

JSON_UserInfoSearchCond

UserInfoSearchCond message in JSON format

```
{
    "UserInfoSearchCond":{
        "searchID":"",
/*required, string type, search ID, which is used to confirm the upper-level
platform or system. If the platform or the system is the same one during two
searching, the search history will be saved in the memory to speed up next
searching*/
        "searchResultPosition": ,
/*required, integer32 type, the start position of the search result in the
result list. When there are multiple records and you cannot get all search
results at a time, you can search for the records after the specified position
next time*/
        "maxResults": ,
/*required, integer32 type, maximum number of search results. If maxResults
exceeds the range returned by the device capability, the device will return the
maximum number of search results according to the device capability and will
not return error message*/
        "EmployeeNoList":{},
/*optional, person ID list (if this node does not exist or is empty, it
indicates searching for all person information)*/
        "employeeNo":""
/*optional, string type, employee No. (person ID)*/
    },
    "fuzzySearch":"",
/*optional, string, key words for fuzzy search*/
    "userType": "normal",
/*optional, string, normal (normal user), visitor (visitor), blockList (person
in blocklist), patient (patient), maintenance (maintenance people)*/
    "deviceIDList": [1, 2]
/*optional, array, device ID list*/
```

```
    }  
}
```

JSON_UserRightHolidayGroupCfg

UserRightHolidayGroupCfg message in JSON format

```
{  
    "UserRightHolidayGroupCfg": {  
        "enable": ,  
        /*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "groupName": "",  
        /*required, string, holiday group name*/  
        "holidayPlanNo": "",  
        /*required, string, holiday group schedule No.*/  
        "operateType": "byTerminal",  
        /*optional, string, operation type: "byTerminal"-by terminal, "byOrg"-by  
        organization, "byTerminalOrg"-by terminal organization*/  
        "terminalNoList": [ 1, 2, 3, 4 ],  
        /*optional, array, terminal ID list, this node is required when operation type  
        is "byTerminal" or "byTerminalOrg"*/  
        "orgNoList": [ 1, 2, 3, 4 ]  
        /*optional, array, organization ID list, this node is required when operation  
        type is "byOrg" or "byTerminalOrg"*/  
    }  
}
```

JSON_UserRightHolidayPlanCfg

JSON message about holiday schedule parameters of the access permission control

```
{  
    "UserRightHolidayPlanCfg": {  
        "enable": ,  
        /*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "beginDate": "",  
        /*start date of the holiday (device local time)*/  
        "endDate": "",  
        /*end date of the holiday (device local time)*/  
        "HolidayPlanCfg" : [ {  
            /*holiday schedule parameters*/  
            "id": ,  
            /*required, integer, time period No., which is between 1 and 8*/  
            "enable": ,  
            /*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
            "TimeSegment": {  
                "beginTime": "",  
                /*required, start time of the time period (device local time)*/  
                "endTime": ""  
            }  
        } ]  
    }  
}
```

```
/*required, end time of the time period (device local time)*/
    }
},
"operateType": "byTerminal",
/*optional, string, operation type: "byTerminal"-by terminal, "byOrg"-by
organization, "byTerminalOrg"-by terminal organization*/
"terminalNoList": [ 1, 2, 3, 4 ],
/*optional, array, terminal ID list, this node is required when operation type
is "byTerminal" or "byTerminalOrg"*/
"orgNoList": [ 1, 2, 3, 4 ]
/*optional, array, organization ID list, this node is required when operation
type is "byOrg" or "byTerminalOrg"*/
}
}
```

JSON_UserRightPlanTemplate

JSON message about schedule template configuration parameters of the access permission control

```
{
  "UserRightPlanTemplate": {
    "enable": ,
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/
    "templateName": "",
/*required, string, template name*/
    "weekPlanNo": ,
/*required, integer, week schedule No.*/
    "holidayGroupNo": "",
/*required, string, holiday group No.*/
    "operateType": "byTerminal",
/*optional, string, operation type: "byTerminal"-by terminal, "byOrg"-by
organization, "byTerminalOrg"-by terminal organization*/
    "terminalNoList": [ 1, 2, 3, 4 ],
/*optional, array, terminal ID list, this node is required when operation type
is "byTerminal" or "byTerminalOrg"*/
    "orgNoList": [ 1, 2, 3, 4 ]
/*optional, array, organization ID list, this node is required when operation
type is "byOrg" or "byTerminalOrg"*/
  }
}
```

JSON_UserRightWeekPlanCfg

JSON message about week schedule parameters of the access permission control

```
{
  "UserRightWeekPlanCfg": {
    "enable": ,
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/
  }
}
```

```
"WeekPlanCfg": [ {
    /*required, week schedule parameters*/
    "week": "",
    /*required, string, day of the week: "Monday", "Tuesday", "Wednesday",
    "Thursday", "Friday", "Saturday", "Sunday"*/
    "id": ,
    /*required, integer, time period No., which is between 1 and 8*/
    "enable": ,
    /*required, boolean, whether to enable: "true"-enable, "false"-disable*/
    "TimeSegment": {
        "beginTime": "",
        /*required, start time of the time period (device local time)*/
        "endTime": ""
        /*required, end time of the time period (device local time)*/
        }
    },
    "operateType": "byTerminal",
    /*optional, string, operation type: "byTerminal"-by terminal, "byOrg"-by
    organization, "byTerminalOrg"-by terminal organization*/
    "terminalNoList": [ 1, 2, 3, 4 ],
    /*optional, array, terminal ID list, this node is required when operation type
    is "byTerminal" or "byTerminalOrg"*/
    "orgNoList": [ 1, 2, 3, 4 ]
    /*optional, array, organization ID list, this node is required when operation
    type is "byOrg" or "byTerminalOrg"*/
    }
}
```

JSON_Verification

JSON message about verification parameters of section password.

```
{
    "Verification": {
        "sectionNo": ,
        /*requiried, integer, section No.*/
        "passwordType": "",
        /*optional, string, password types: "KeyA" (default), "KeyB"*/
        "password": ""
        /*optional, string, a hexadecimal key, which depends on the password type*/
        }
}
```

JSON_VerifyHolidayGroupCfg

VerifyHolidayGroupCfg message in JSON format

```
{
    "VerifyHolidayGroupCfg": {
```

```
"enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
    "groupName": "",  
/*required, string, holiday group name*/  
    "holidayPlanNo": ""  
/*required, string, holiday group schedule No.*/  
    }  
}
```

JSON_VerifyHolidayPlanCfg

VerifyHolidayPlanCfg message in JSON format

```
{  
    "VerifyHolidayPlanCfg": {  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "beginDate": "",  
/*required, start date of the holiday (device local time)*/  
        "endDate": "",  
/*required, end date of the holiday (device local time)*/  
        "HolidayPlanCfg": [{}  
/*required, holiday schedule parameters*/  
        "id": ,  
/*required, integer, time period No., which is between 1 and 8*/  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "verifyMode": "",  
/*required, string, authentication mode: "cardAndPw"-card+password, "card",  
"cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint+password,  
"fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card, "fpAndCardAndPw"-  
fingerprint+card+password, "faceOrFpOrCardOrPw"-face or fingerprint or card or  
password, "faceAndFp"-face+fingerprint, "faceAndPw"-face+password,  
"faceAndCard"-face+card, "face", "employeeNoAndPw"-employee No.+password,  
"fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.+fingerprint,  
"employeeNoAndFpAndPw"-employee No.+fingerprint+password, "faceAndFpAndCard"-  
face+fingerprint+card, "faceAndPwAndFp"-face+password+fingerprint,  
"employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face or face+card,  
"fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or password,  
"cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or fingerprint,  
"cardOrFpOrPw"-card or fingerprint or password, "sleep", "invalid"*/  
        "TimeSegment": {  
            "beginTime": "",  
/*required, start time of the time period (device local time)*/  
            "endTime": "",  
/*required, end time of the time period (device local time)*/  
        }  
    }  
}
```

JSON_VerifyPlanTemplate

VerifyPlanTemplate message in JSON format

```
{  
    "VerifyPlanTemplate": {  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "templateName": "",  
/*required, string, template name*/  
        "weekPlanNo": ,  
/*required, integer, week schedule No.*/  
        "holidayGroupNo": ""  
/*required, string, holiday group No.*/  
    }  
}
```

JSON_VerifyWeekPlanCfg

VerifyWeekPlanCfg message in JSON format

```
{  
    "VerifyWeekPlanCfg":{  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "WeekPlanCfg":[]  
/*required, week schedule parameters*/  
        "week": "",  
/*required, string, days of the week: "Monday", "Tuesday", "Wednesday",  
"Thursday", "Friday", "Saturday", "Sunday"*/  
        "id": ,  
/*required, integer, time period No., which is between 1 and 8*/  
        "enable": ,  
/*required, boolean, whether to enable: "true"-enable, "false"-disable*/  
        "verifyMode": "",  
/*required, string, authentication mode: "cardAndPw"-card+password, "card"-  
card, "cardOrPw"-card or password, "fp"-fingerprint, "fpAndPw"-fingerprint  
+password, "fpOrCard"-fingerprint or card, "fpAndCard"-fingerprint+card,  
"fpAndCardAndPw"-fingerprint+card+password, "faceOrFpOrCardOrPw"-face or  
fingerprint or card or password, "faceAndFp"-face+fingerprint, "faceAndPw"-face  
+password, "faceAndCard"-face+card, "face"-face, "employeeNoAndPw"-employee No.  
+password, "fpOrPw"-fingerprint or password, "employeeNoAndFp"-employee No.  
+fingerprint, "employeeNoAndFpAndPw"-employee No.+fingerprint+password,  
"faceAndFpAndCard"-face+fingerprint+card, "faceAndPwAndFp"-face+password  
+fingerprint, "employeeNoAndFace"-employee No.+face, "faceOrfaceAndCard"-face  
or face+card, "fpOrface"-fingerprint or face, "cardOrfaceOrPw"-card or face or  
password, "cardOrFace"-card or face, "cardOrFaceOrFp"-card or face or  
fingerprint, "cardOrFpOrPw"-card or fingerprint or password, "sleep",  
"invalid"*/
```

```
        "TimeSegment": {
            "beginTime": "",
            /*required, start time of the time period (device local time)*/
            "endTime": ""
            /*required, end time of the time period (device local time)*/
        }
    }
}
```

B.1.2 XML Messages

XML_CaptureFaceData

CaptureFaceData message in XML format

```
<CaptureFaceData version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <faceDataUrl>
        <!--dep, xs: string, face data URL, if this node does not exist, it
indicates that there is no face data-->
    </faceDataUrl>
    <captureProgress>
        <!--req, xs: integer, collection progress, which is between 0 and 100, 0-no
face data collected, 100-collected, the face data URL can be parsed only when
the progress is 100-->
    </captureProgress>
    <isCurRequestOver>
        <!--opt, xs:boolean, whether the current collection request is completed:
"true"-yes, "false"-no-->
    </isCurRequestOver>
    <infraredFaceDataURL>
        <!--dep, xs:string, infrared face data URL, if this node does not exist, it
indicates that there is no infrared face data-->
    </infraredFaceDataURL>
</CaptureFaceData>
```

XML_CaptureFaceDataCond

CaptureFaceDataCond message in XML format

```
<CaptureFaceDataCond version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <captureInfrared>
        <!--opt, xs:boolean, whether to collect infrared face pictures
simultaneously: "true"-yes, "false"-no-->
    </captureInfrared>
    <dataType><!--opt, xs:string, data type of collected face pictures: "url"

```

```
(default), "binary"--></dataType>  
</CaptureFaceDataCond>
```

XML_CaptureFingerPrint

CaptureFingerPrint message in XML format

```
<CaptureFingerPrint version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <fingerData><!--dep, xs:string, fingerprint data, which is between 1 and 768,  
    and it should be encoded by Base64--></fingerData>  
    <fingerNo><!--req, xs:integer, finger No., which is between 1 and 10--></  
    fingerNo>  
    <fingerPrintQuality><!--req, xs:integer, fingerprint quality, which is  
    between 1 and 100--></fingerPrintQuality>  
</CaptureFingerPrint>
```

XML_CaptureFingerPrintCond

CaptureFingerPrintCond message in XML format

```
<CaptureFingerPrintCond version="2.0" xmlns="http://www.isapi.org/ver20/  
    XMLSchema">  
    <fingerNo><!--req, xs: integer, finger No., which is between 1 and 10--></  
    fingerNo>  
</CaptureFingerPrintCond>
```

XML_Cap_AccessControl

AccessControl capability message in XML format

```
<AccessControl version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <isSupportWiegandCfg>  
        <!--optional, xs:boolean, whether it supports Wiegand configuration-->  
    </isSupportWiegandCfg>  
    <isSupportModuleStatus>  
        <!--optional, xs:boolean, whether it supports getting the status of secure  
        door control unit-->  
    </isSupportModuleStatus>  
    <isSupportSNAPConfig>  
        <!--optional, xs:boolean, whether it supports getting capture linkage  
        parameters-->  
    </isSupportSNAPConfig>  
    <LocalController><!--opt-->  
        <isSupportLocalControllerManage>  
            <!--optional, xs:boolean, whether it supports distributed access  
            controller management-->  
        </isSupportLocalControllerManage>
```

```
<isSupportLocalControllerControl>
    <!--optional, xs:boolean, whether it supports distributed access
controller control-->
</isSupportLocalControllerControl>
</LocalController>
<isSupportUSBManage>
    <!--optional, xs:boolean, whether it supports USB management of access
control device-->
</isSupportUSBManage>
<isSupportIdentityTerminal>
    <!--optional, xs:boolean, whether it supports face recognition terminal
configuration-->
</isSupportIdentityTerminal>
<isSupportDepartmentParam>
    <!--optional, xs:boolean, whether it supports setting department
parameters-->
</isSupportDepartmentParam>
<isSupportSchedulePlan>
    <!--optional, xs:boolean, whether it supports setting shift schedule-->
</isSupportSchedulePlan>
<isSupportAttendanceRule>
    <!--optional, xs:boolean, whether it supports setting time and attendance
rule-->
</isSupportAttendanceRule>
<isSupportOrdinaryClass>
    <!--optional, xs:boolean, whether it supports setting normal shift
parameters-->
</isSupportOrdinaryClass>
<isSupportWorkingClass>
    <!--optional, xs:boolean, whether it supports setting man-hour shift
parameters-->
</isSupportWorkingClass>
<isSupportAttendanceHolidayGroup>
    <!--optional, xs:boolean, whether it supports setting holiday group for
time and attendance-->
</isSupportAttendanceHolidayGroup>
<isSupportAttendanceHolidayPlan>
    <!--optional, xs:boolean, whether it supports setting holiday schedule for
time and attendance-->
</isSupportAttendanceHolidayPlan>
<isSupportLadderControlRelay>
    <!--optional, xs:boolean, whether it supports setting elevator controller
relay-->
</isSupportLadderControlRelay>
<isSupportWiegandRuleCfg>
    <!--optional, xs:boolean, whether it supports setting Wiegand rule-->
</isSupportWiegandRuleCfg>
<isSupportM1CardEncryptCfg>
    <!--optional, xs:boolean, whether it supports M1 card encryption
authentication-->
</isSupportM1CardEncryptCfg>
<isSupportDeployInfo>
```

```
<!--optional, xs:boolean, whether it supports getting arming information-->
</isSupportDeployInfo>
<isSupportSubmarineBack>
    <!--optional, xs:boolean, whether it supports specifying anti-passing back
server-->
    </isSupportSubmarineBack>
    <isSupportSubmarineBackHostInfo>
        <!--optional, xs:boolean, whether it supports setting access controllers
with anti-passing back enabled-->
        </isSupportSubmarineBackHostInfo>
        <isSupportStartReaderInfo>
            <!--optional, xs:boolean, whether it supports setting first card reader-->
            </isSupportStartReaderInfo>
            <isSupportSubmarineBackReader>
                <!--optional, xs:boolean, whether it supports setting anti-passing back
card reader-->
                </isSupportSubmarineBackReader>
                <isSupportServerDevice>
                    <!--optional, xs:boolean, whether it supports setting anti-passing back
server information-->
                    </isSupportServerDevice>
                    <isSupportReaderAcrossHost>
                        <!--optional, xs:boolean, whether it supports enabling cross-controller
anti-passing back function of card reader-->
                        </isSupportReaderAcrossHost>
                        <isSupportClearCardRecord>
                            <!--optional, xs:boolean, whether it supports clearing card swiping records
in anti-passing back server-->
                            </isSupportClearCardRecord>
                            <isSupportSubmarineBackMode>
                                <!--optional, xs:boolean, whether it supports setting anti-passing back
mode-->
                                </isSupportSubmarineBackMode>
                                <isSupportClearSubmarineBack>
                                    <!--optional, xs:boolean, whether it supports clearing cross-controller
anti-passing back information-->
                                    </isSupportClearSubmarineBack>
                                    <isSupportFaceCompareCond><!--optional, xs:boolean, whether it supports
configuring restriction condition parameters of face picture comparison--></
isSupportFaceCompareCond>
                                    <isSupportRemoteControlDoor>
                                        <!--optional, xs:boolean, whether it supports remote door, elevator, and
lock control: "true"-yes, this node is not returned-no-->
                                        </isSupportRemoteControlDoor>
                                        <isSupportUserInfo><!--optional, xs:boolean, whether it supports person
management based on person--></isSupportUserInfo>
                                        <EmployeeNoInfo><!--dep, employee No. (person ID) information, this node is
valid only when the isSupportUserInfo is "true"-->
                                            <employeeNo min="" max=""><!--optional, employee No. (person ID)--></
employeeNo>
                                            <characterType opt="any,number">
                                                <!--optional, employee No. (person) ID type: "any"-any characters
```

```
(default), "number"-digits (from 0 to 9), only one value can be returned-->
    </characterType>
    <isSupportCompress>
        <!--optional, xs:boolean, whether it supports compressing employee No.
(person ID) for storage: "true"-yes, this node is not returned-no-->
    </isSupportCompress>
</EmployeeNoInfo>
<isSupportCardInfo><!--optional, xs:boolean, whether it supports card
management based on person: "true"-yes, this node is not returned-no--></
isSupportCardInfo>
<isSupportFDLib><!--optional, xs:boolean, whether it supports face picture
library management--></isSupportFDLib>
<isSupportUserInfoDetailDelete><!--optional, xs:boolean, whether it supports
deleting person information and permission: "true"-yes, this node is not
returned-no--></isSupportUserInfoDetailDelete>
<isSupportAuthCodeInfo>
    <!--optional, xs:boolean, whether it supports authentication password
management: "true"-yes, this node is not returned-no-->
</isSupportAuthCodeInfo>
<isSupportFingerPrintCfg>
    <!--optional, xs:boolean, whether it supports configuring fingerprint
parameters: "true"-yes, this node is not returned-no-->
</isSupportFingerPrintCfg>
<isSupportFingerPrintDelete>
    <!--optional, xs:boolean, whether it supports deleting fingerprint: "true"-yes,
this node is not returned-no-->
</isSupportFingerPrintDelete>
<isSupportCaptureFingerPrint>
    <!--optional, xs:boolean, whether it supports collecting fingerprint
information: "true"-yes, this node is not returned-no-->
</isSupportCaptureFingerPrint>
<isSupportDoorStatusWeekPlanCfg>
    <!--optional, xs:boolean, whether it supports configuring door control week
schedule: "true"-yes, this node is not returned-no-->
</isSupportDoorStatusWeekPlanCfg>
<isSupportVerifyWeekPlanCfg>
    <!--optional, xs:boolean, whether it supports configuring week schedule of
the card reader authentication mode: "true"-yes, this node is not returned-no-->
</isSupportVerifyWeekPlanCfg>
<isSupportCardRightWeekPlanCfg>
    <!--optional, xs:boolean, whether it supports configuring week schedule of
the access permission control: "true"-yes, this node is not returned-no-->
</isSupportCardRightWeekPlanCfg>
<isSupportDoorStatusHolidayPlanCfg>
    <!--optional, xs:boolean, whether it supports configuring door control
holiday schedule: "true"-yes, this node is not returned-no-->
</isSupportDoorStatusHolidayPlanCfg>
<isSupportVerifyHolidayPlanCfg>
    <!--optional, xs:boolean, whether it supports configuring holiday schedule
of the card reader authentication mode: "true"-yes, this node is not returned-
no-->
</isSupportVerifyHolidayPlanCfg>
```

```
<isSupportCardRightHolidayPlanCfg>
    <!--optional, xs:boolean, whether it supports configuring holiday schedule
of the access permission control: "true"-yes, this node is not returned-no-->
</isSupportCardRightHolidayPlanCfg>
<isSupportDoorStatusHolidayGroupCfg>
    <!--optional, xs:boolean, whether it supports configuring holiday group of
the door control schedule: "true"-yes, this node is not returned-no-->
</isSupportDoorStatusHolidayGroupCfg>
<isSupportVerifyHolidayGroupCfg>
    <!--optional, xs:boolean, whether it supports configuring holiday group of
the control schedule of the card reader authentication mode: "true"-yes, this
node is not returned-no-->
</isSupportVerifyHolidayGroupCfg>
<isSupportUserRightHolidayGroupCfg>
    <!--optional, xs:boolean, whether it supports configuring holiday group of
the access permission control schedule: "true"-yes, this node is not returned-
no-->
</isSupportUserRightHolidayGroupCfg>
<isSupportDoorStatusPlanTemplate>
    <!--optional, xs:boolean, whether it supports configuring door control
schedule template: "true"-yes, this node is not returned-no-->
</isSupportDoorStatusPlanTemplate>
<isSupportVerifyPlanTemplate>
    <!--optional, xs:boolean, whether it supports configuring schedule template
of the card reader authentication mode: "true"-yes, this node is not returned-
no-->
</isSupportVerifyPlanTemplate>
<isSupportUserRightPlanTemplate>
    <!--optional, xs:boolean, whether it supports configuring schedule template
of the access permission control: "true"-yes, this node is not returned-no-->
</isSupportUserRightPlanTemplate>
<isSupportDoorStatusPlan>
    <!--optional, xs:boolean, whether it supports configuring door control
schedule: "true"-yes, this node is not returned-no-->
</isSupportDoorStatusPlan>
<isSupportCardReaderPlan>
    <!--optional, xs:boolean, whether it supports configuring control schedule
of the card reader authentication mode: "true"-yes, this node is not returned-
no-->
</isSupportCardReaderPlan>
<isSupportClearPlansCfg>
    <!--optional, xs:boolean, whether it supports clearing the access control
schedule parameters: "true"-yes, this node is not returned-no-->
</isSupportClearPlansCfg>
<isSupportRemoteControlBuzzer>
    <!--optional, xs:boolean, whether it supports remotely controlling the
buzzer of the card reader: "true"-yes, this node is not returned-no-->
</isSupportRemoteControlBuzzer>
<isSupportEventCardNoList>
    <!--optional, xs:boolean, whether it supports getting the list of event and
card linkage ID: "true"-yes, this node is not returned-no-->
</isSupportEventCardNoList>
```

```
<isSupportEventCardLinkageCfg>
    <!--optional, xs:boolean, whether it supports configuring event and card
linkage parameters: "true"-yes, this node is not returned-no-->
</isSupportEventCardLinkageCfg>
<isSupportClearEventCardLinkageCfg>
    <!--optional, xs:boolean, whether it supports clearing event and card
linkage parameters: "true"-yes, this node is not returned-no-->
</isSupportClearEventCardLinkageCfg>
<isSupportAcsEvent>
    <!--optional, xs:boolean, whether it supports searching for access control
events: "true"-yes, this node is not returned-no-->
</isSupportAcsEvent>
<isSupportAcsEventTotalNum>
    <!--optional, xs:boolean, whether it supports getting total number of
access control events by specific conditions: "true"-yes, this node is not
returned-no-->
</isSupportAcsEventTotalNum>
<isSupportDeployInfo>
    <!--optional, xs:boolean, whether it supports getting the arming
information: "true"-yes, this node is not returned-no-->
</isSupportDeployInfo>
<isSupportEventOptimizationCfg>
    <!--optional, xs:boolean, whether it supports configuring event
optimization: "true"-yes, this node is not returned-no-->
</isSupportEventOptimizationCfg>
<isSupportAcsWorkStatus>
    <!--optional, xs:boolean, whether it supports getting working status of the
access control device: "true"-yes, this node is not returned-no-->
</isSupportAcsWorkStatus>
<isSupportDoorCfg>
    <!--optional, xs:boolean, whether it supports configuring door parameters:
"true"-yes, this node is not returned-no-->
</isSupportDoorCfg>
<isSupportCardReaderCfg>
    <!--optional, xs:boolean, whether it supports configuring card reader
parameters: "true"-yes, this node is not returned-no-->
</isSupportCardReaderCfg>
<isSupportAcsCfg>
    <!--optional, xs:boolean, whether it supports configuring parameters of
access control device: "true"-yes, this node is not returned-no-->
</isSupportAcsCfg>
<isSupportRemoteCheck>
    <!--optional, xs:boolean, whether it supports verifying access control
events remotely: true-yes, this field is not returned-no-->
</isSupportRemoteCheck>
<isSupportMaskDetection>
    <!--optional, xs:boolean, whether it supports mask detection: true-yes,
this field is not returned-no-->
</isSupportMaskDetection>
<isSupportGroupCfg>
    <!--optional, xs:boolean, whether it supports configuring group parameters:
"true"-yes, this node is not returned-no-->
```

```
</isSupportGroupCfg>
<isSupportClearGroupCfg>
    <!--optional, xs:boolean, whether it supports clearing group parameters:
"true"--yes, this node is not returned-no-->
</isSupportClearGroupCfg>
<isSupportMultiCardCfg>
    <!--optional, xs:boolean, whether it supports configuring multiple
authentication mode: "true"--yes, this node is not returned-no-->
</isSupportMultiCardCfg>
<isSupportMultiDoorInterLockCfg>
    <!--optional, xs:boolean, whether it supports configuring multi-door
interlocking parameters: "true"--yes, this node is not returned-no-->
</isSupportMultiDoorInterLockCfg>
<isSupportAntiSneakCfg>
    <!--optional, xs:boolean, whether it supports configuring anti-passing back
parameters in the device: "true"--yes, this node is not returned-no-->
</isSupportAntiSneakCfg>
<isSupportCardReaderAntiSneakCfg>
    <!--optional, xs:boolean, whether it supports configuring anti-passing back
parameters for the card reader in the device: "true"--yes, this node is not
returned-no-->
</isSupportCardReaderAntiSneakCfg>
<isSupportClearAntiSneakCfg>
    <!--optional, xs:boolean, whether it supports clearing anti-passing back
parameters: "true"--yes, this node is not returned-no-->
</isSupportClearAntiSneakCfg>
<isSupportClearAntiSneak>
    <!--optional, xs:boolean, whether it supports clearing anti-passing back
records in the device: "true"--yes, this node is not returned-no-->
</isSupportClearAntiSneak>
<isSupportSmsRelativeParam>
    <!--optional, xs:boolean, whether it supports configuring message function:
"true"--yes, this node is not returned-no-->
</isSupportSmsRelativeParam>
<isSupportPhoneDoorRightCfg>
    <!--optional, xs:boolean, whether it supports configuring the door
permission linked to the mobile phone number: "true"--yes, this node is not
returned-no-->
</isSupportPhoneDoorRightCfg>
<isSupportOSDPStatus>
    <!--optional, xs:boolean, whether it supports searching for OSDP card
reader status: "true"--yes, this node is not returned-no-->
</isSupportOSDPStatus>
<isSupportOSDPMModify>
    <!--optional, xs:boolean, whether it supports editing OSDP card reader ID:
"true"--yes, this node is not returned-no-->
</isSupportOSDPMModify>
<isSupportLogModeCfg>
    <!--optional, xs:boolean, whether it supports configuring log mode: "true"--yes,
this node is not returned-no-->
</isSupportLogModeCfg>
<FactoryReset>
```

```
<isSupportFactoryReset><!--optional, xs: boolean, whether it supports  
restoring to default settings by condition--></isSupportFactoryReset>  
    <mode opt="full,basic,part"><!--optional, xs: string, conditions for  
restoring to default settings--></mode>  
    </FactoryReset>  
    <isSupportNFCCfg><!--optional, xs:boolean, whether it supports enabling or  
disabling NFC function: "true"-yes, this node is not returned-no--></  
isSupportNFCCfg>  
    <isSupportRFCardCfg><!--optional, xs:boolean, whether it supports enabling or  
disabling RF card recognition: "true"-yes, this node is not returned-no--></  
isSupportRFCardCfg>  
    <isSupportCaptureFace>  
        <!--optional, xs:boolean, whether it supports collecting face pictures:  
"true"-yes, this node is not returned-no-->  
    </isSupportCaptureFace>  
    <isSupportCaptureInfraredFace>  
        <!--optional, xs:boolean, whether it supports collecting infrared face  
pictures: "true"-yes, this node is not returned-no-->  
    </isSupportCaptureInfraredFace>  
    <isSupportFaceRecognizeMode>  
        <!--optional, xs:boolean, whether it supports configuring facial  
recognition mode: "true"-yes, this node is not returned-no-->  
    </isSupportFaceRecognizeMode>  
    <isSupportRemoteControlPWChcek>  
        <!--optional, xs:boolean, whether it supports verifying the password for  
remote door control: "true"-yes, this node is not returned-no-->  
    </isSupportRemoteControlPWChcek>  
    <isSupportRemoteControlPWCfg>  
        <!--optional, xs:boolean, whether it supports configuring the password for  
remote door control: "true"-yes, this node is not returned-no-->  
    </isSupportRemoteControlPWCfg>  
    <isSupportAttendanceStatusModeCfg>  
        <!--optional, xs:boolean, whether it supports configuring attendance mode:  
"true"-yes, this node is not returned-no-->  
    </isSupportAttendanceStatusModeCfg>  
    <isSupportAttendanceStatusRuleCfg>  
        <!--optional, xs:boolean, whether it supports configuring attendance status  
and rule: "true"-yes, this node is not returned-no-->  
    </isSupportAttendanceStatusRuleCfg>  
    <isSupportCaptureCardInfo>  
        <!--optional, xs:boolean, whether it supports collecting card information:  
"true"-yes, this node is not returned-no-->  
    </isSupportCaptureCardInfo>  
    <isSupportCaptureIDInfo>  
        <!--optional, xs:boolean, whether it supports collecting ID card  
information: "true"-yes, this node is not returned-no-->  
    </isSupportCaptureIDInfo>  
    <isSupportCaptureRule>  
        <!--optional, xs:boolean, whether it supports configuring online collection  
rules: "true"-yes, this node is not returned-no-->  
    </isSupportCaptureRule>  
    <isSupportCapturePresetParam>
```

```
<!--optional, xs:boolean, whether it supports configuring preset parameters  
of online collection: "true"--yes, this node is not returned-->  
</isSupportCapturePresetParam>  
<isSupportOfflineCapture>  
    <!--optional, xs:boolean, whether it supports offline collection: "true"--  
yes, this node is not returned-->  
</isSupportOfflineCapture>  
<isSupportCardOperations>  
    <!--optional, xs:boolean, whether it supports card operation: "true"--yes,  
this node is not returned-->  
</isSupportCardOperations>  
<isSupportRightControllerAudio>  
    <!--optional, xs:boolean, whether it supports configuring audio file  
parameters of the main controller-->  
</isSupportRightControllerAudio>  
<isSupportChannelControllerCfg>  
    <!--optional, xs:boolean, whether it supports configuring lane controller-->  
</isSupportChannelControllerCfg>  
<isSupportGateDialAndInfo>  
    <!--optional, xs:boolean, whether it supports getting local DIP and  
information of the turnstile-->  
</isSupportGateDialAndInfo>  
<isSupportGateStatus>  
    <!--optional, xs:boolean, whether it supports getting turnstile status-->  
</isSupportGateStatus>  
<isSupportGateIRStatus>  
    <!--optional, xs:boolean, whether it supports getting the status of the  
active infrared intrusion detector of the turnstile-->  
</isSupportGateIRStatus>  
<isSupportGateRelatedPartsStatus>  
    <!--optional, xs:boolean, whether it supports getting related components'  
status of the turnstile-->  
</isSupportGateRelatedPartsStatus>  
<isSupportChannelControllerAlarmLinkage>  
    <!--optional, xs:boolean, whether it supports configuring alarm linkage of  
the lane controller-->  
</isSupportChannelControllerAlarmLinkage>  
<isSupportChannelControllerAlarmOut>  
    <!--optional, xs:boolean, whether it supports configuring alarm output of  
the lane controller-->  
</isSupportChannelControllerAlarmOut>  
<isSupportChannelControllerAlarmOutControl>  
    <!--optional, xs:boolean, whether it supports controlling alarm output of  
the lane controller-->  
</isSupportChannelControllerAlarmOutControl>  
<isSupportChannelControllerTypeCfg>  
    <!--optional, xs:boolean, whether it supports configuring device type of  
the lane controller-->  
</isSupportChannelControllerTypeCfg>  
<isSupportRemoteCtrlrModeCfg>  
    <!--optional, xs:boolean, whether it supports configuring parameters of the  
keyfob control mode-->
```

```
</isSupportRemoteControllerModeCfg>
<isSupportTTSText><!--optional, xs:boolean, whether it supports configuring the text of the audio prompt: true-yes. If this function is not supported, this node will be not returned--></isSupportTTSText>
<isSupportIDBlackListCfg><!--optional, xs:boolean, whether it supports applying ID card blocklist: true-yes. If this function is not supported, this node will be not returned--></isSupportIDBlackListCfg>
<isSupportUserDataImport><!--optional, xs:boolean, whether it supports importing person permission data: true-yes. If this function is not supported, this node will be not returned--></isSupportUserDataImport>
<isSupportUserDataExport><!--optional, xs:boolean, whether it supports exporting person permission data: true-yes. If this function is not supported, this node will be not returned--></isSupportUserDataExport>
<isSupportMaintenanceDataExport><!--optional, xs:boolean, whether it supports exporting maintenance data: true-yes. If this function is not supported, this node will be not returned--></isSupportMaintenanceDataExport>
<isSupportLockTypeCfg><!--optional, xs:boolean, whether it supports configuring door lock status when the device is powered off: true-yes. If this function is not supported, this node will be not returned--></isSupportLockTypeCfg>
<isSupportSafetyHelmetDetection><!--optional, xs:boolean, whether it supports configuring hard hat detection: true-yes, this node is not returned-no--></isSupportSafetyHelmetDetection>
<isSupportKeyCfgAttendance><!--optional, xs:boolean, whether it supports configuring parameters of attendance check by pressing the key: true-yes, this node is not returned-no--></isSupportKeyCfgAttendance>
<isSupportIDBlackListTemplate><!--optional, xs:boolean, whether it supports downloading the ID card blocklist template: true-yes, this node is not returned-no--></isSupportIDBlackListTemplate>
<isSupportAttendanceWeekPlan><!--optional, xs:boolean, whether it supports configuring parameters of the week attendance schedule: true-yes, this node is not returned-no--></isSupportAttendanceWeekPlan>
<isSupportClearAttendancePlan><!--optional, xs:boolean, whether it supports clearing the week attendance schedule: true-yes, this node is not returned-no--></isSupportClearAttendancePlan>
<isSupportAttendanceMode><!--optional, xs:boolean, whether it supports configuring the attendance mode: true-yes, this node is not returned-no--></isSupportAttendanceMode>
<isSupportAttendancePlanTemplate><!--whether it supports configuring the attendance schedule template: true-yes, this node is not returned-no--></isSupportAttendancePlanTemplate>
<isSupportAttendancePlanTemplateList><!--optional, xs:boolean, whether it supports getting the list of attendance schedule templates: true-yes, this node is not returned-no--></isSupportAttendancePlanTemplateList>
<isSupportCardVerificationRule><!--optional, xs:boolean, whether it supports configuring card No. authentication mode: true-yes, this node is not returned-no--></isSupportCardVerificationRule>
<isSupportTemperatureMeasureCfg><!--optional, xs:boolean, whether it supports configuring temperature measurement parameters: true (support), this node is not returned (not support)--></isSupportTemperatureMeasureCfg>
<isSupportTemperatureMeasureAreaCfg><!--optional, xs:boolean, whether it supports configuring parameters of the temperature measurement area: true
```

```
(support), this node is not returned (not support)--></
isSupportTemperatureMeasureAreaCfg>
<isSupportTemperatureMeasureAreaCalibrationCfg><!--optional, xs:boolean,
whether it supports configuring calibration parameters of the temperature
measurement area: true (support), this node is not returned (not support)--></
isSupportTemperatureMeasureAreaCalibrationCfg>
<isSupportBlackObjectCfg><!--optional, xs:boolean, whether it supports
configuring black body parameters: true (support), this node is not returned
(not support)--></isSupportBlackObjectCfg>
<isSupportHealthCodeCfg><!--optional, xs:boolean, whether it supports
configuring health code parameters: true (support), this node is not returned
(not support)--></isSupportHealthCodeCfg>
<isSupportShowHealthCodeCfg><!--optional, xs:boolean, whether it supports
configuring display parameters of the health code: true (support), this node is
not returned (not support)--></isSupportShowHealthCodeCfg>
<isSupportAddCustomAudio><!--optional, boolean, whether it supports importing
custom audio, related URI: /ISAPI/AccessControl/customAudio/addCustomAudio?
format=json--></isSupportAddCustomAudio>
<isSupportDeleteCustomAudio><!--optional, boolean, whether it supports
deleting custom audio, related URI: /ISAPI/AccessControl/customAudio/
deleteCustomAudio?format=json--></isSupportDeleteCustomAudio>
<isSupportSearchCustomAudio><!--optional, boolean, whether it supports
searching for custom audio, related URI: /ISAPI/AccessControl/customAudio/
searchCustomAudioStatus?format=json--></isSupportSearchCustomAudio>
<isSupportBluetoothEncryptionInfo><!--optional, xs:boolean, whether it
supports configuring bluetooth encryption information: true (support). If this
function is not supported, this node will not be returned--></
isSupportBluetoothEncryptionInfo>
<isSupportBluetoothEncryptionVersion><!--optional, xs:boolean, whether it
supports configuring bluetooth encryption version: true (support). If this
function is not supported, this node will not be returned--></
isSupportBluetoothEncryptionVersion>
<isSupportBluetooth><!--optional, xs:boolean, whether it supports bluetooth
configuration--></isSupportBluetooth>
</AccessControl>
```

XML_Cap_CaptureFaceData

CaptureFaceData capability message in XML format

```
<CaptureFaceData version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <CaptureFaceDataCond>
    <captureInfrared opt="true,false"><!--req, xs:boolean, whether to collect
infrared face data--></captureInfrared>
    <dataType opt="url,binary"><!--opt, xs:string, data type of collected face
pictures: "url" (default), "binary"--></dataType>
  </CaptureFaceDataCond>
  <faceDataUrl min="1" max="768">
    <!--dep, xs:string, face data URL, if this node does not exist, it
indicates that there is no face data-->
  </faceDataUrl>
```

```
<captureProgress min="0" max="100">
    <!--req, xs:integer, collection progress, which is between 0 and 100, 0-no
face data collected, 100-collected, the face data URL can be parsed only when
the progress is 100-->
</captureProgress>
<isCurRequestOver opt="true,false">
    <!--opt, xs:boolean, whether the current collection request is completed:
"true"-yes, "false"-no-->
</isCurRequestOver>
<infraredFaceDataUrl min="1" max="100">
    <!--req, xs:string, infrared face picture URL, if this node does not exist,
it indicates that there is no infrared face data-->
</infraredFaceDataUrl>
</CaptureFaceData>
```

XML_Cap_CaptureFingerPrint

CaptureFingerPrint capability message in XML format

```
<CaptureFingerPrint version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <CaptureFingerPrintCond><!--req, xs: integer, finger No.-->
        <fingerNo min="1" max="10"></fingerNo>
    </CaptureFingerPrintCond>
    <fingerData min="1" max="768"><!--dep, xs:string, fingerprint data--></
fingerData>
    <fingerNo min="1" max="10"><!--req, xs:integer, finger No.--></fingerNo>
    <fingerPrintQuality min="1" max="100"><!--req, xs:integer, fingerprint
quality--></fingerPrintQuality>
</CaptureFingerPrint>
```

XML_Cap_ClearCardRecord

ClearCardRecord capability message in XML format

```
<ClearCardRecord version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <clearAllCard opt="true,false">
        <!--req, xs: boolean, whether to clear all card swiping records in the
cross-controller anti-passing back server-->
    </clearAllCard>
    <CardList size="32">
        <cardNo min="1" max="32"><!--opt, xs: string, card No.--></cardNo>
    </CardList>
    <EmployeeNoList size="32">
        <employeeNo min="" max=""><!--opt, xs:string, employee No. (person ID)--></
employeeNo>
    </EmployeeNoList>
</ClearCardRecord>
```

XML_Cap_ClearSubmarineBack

ClearSubmarineBack capability message in XML format

```
<ClearSubmarineBack version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <clearHostInfo opt="true,false"><!--opt, xs: boolean, whether to clear access controller information--></clearHostInfo>
    <clearReaderInfo opt="true,false"><!--opt, xs: boolean, whether to clear card reader information--></clearReaderInfo>
    <clearSubmarineBack opt="true,false"><!--opt, xs: boolean, whether to clear anti-passing back server parameters--></clearSubmarineBack>
    <clearSubmarineBackHostInfo opt="true,false">
        <!--opt, xs: boolean, whether to clear cross-controller anti-passing back parameters of access controllers-->
    </clearSubmarineBackHostInfo>
    <clearStartReaderInfo opt="true,false"><!--opt, xs: boolean, whether to clear first card reader parameters--></clearStartReaderInfo>
    <clearSubmarineBackReader opt="true,false">
        <!--opt, xs: boolean, whether to clear cross-controller anti-passing back parameters of card readers-->
    </clearSubmarineBackReader>
    <clearSubmarineBackMode opt="true,false">
        <!--opt, xs: boolean, whether to clear the cross-controller anti-passing back mode parameters-->
    </clearSubmarineBackMode>
    <clearServerDevice opt="true,false"><!--opt, xs: boolean, whether to clear the parameters of cross-controller anti-passing back server--></clearServerDevice>
    <clearReaderAcrossHost opt="true,false">
        <!--opt, xs: boolean, whether to clear the cross-controller anti-passing back status of card readers-->
    </clearReaderAcrossHost>
</ClearSubmarineBack>
```

XML_Cap_DeployInfo

DeployInfo capability message in XML format

```
<DeployInfo version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <DeployList size="5">
        <Content>
            <deployNo min="" max=""><!--req, xs: integer, arming No.--></deployNo>
            <deployType opt="0,1,2"><!--req, xs: integer, arming type: 0-client arming to receive real-time or offline events via platform or system (based on Hikvision private protocol), 1-real-time arming to receive real-time events (based on Hikvision private protocol), 2-arm based on ISAPI protocol--></deployType>
            <ipAddr min="" max=""><!--req, xs: string, IP address--></ipAddr>
        </Content>
    </DeployList>
</DeployInfo>
```

```
</DeployList>  
</DeployInfo>
```

XML_Cap_DoorParam

DoorParam capability message in XML format

```
<DoorParam version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <doorNo min="" max="">  
        <!--opt, xs:integer, door No.-->  
    </doorNo>  
    <doorName min="1" max="32">  
        <!--opt, xs:string, door name-->  
    </doorName>  
    <magneticType opt="alwaysClose,alwaysOpen">  
        <!--opt, xs:string, magnetic contact type: "alwaysClose"-remain locked,  
        "alwaysOpen"-remain unlocked-->  
    </magneticType>  
    <openButtonType opt="alwaysClose,alwaysOpen">  
        <!--opt, xs:string, door button type: "alwaysClose"-remain locked,  
        "alwaysOpen"-remain unlocked-->  
    </openButtonType>  
    <openDuration min="1" max="255">  
        <!--opt, xs:integer, door open duration (floor relay action time), unit:  
        second-->  
    </openDuration>  
    <disabledOpenDuration min="1" max="255">  
        <!--opt, xs:integer, door open duration by disability card (delay duration  
        of closing the door), unit: second-->  
    </disabledOpenDuration>  
    <magneticAlarmTimeout min="0" max="255">  
        <!--opt, xs:integer, alarm time of magnetic contact detection timeout,  
        which is between 0 and 255, 0 refers to not triggering alarm, unit: second-->  
    </magneticAlarmTimeout>  
    <enableDoorLock opt="true,false">  
        <!--opt, xs:boolean, whether to enable locking door when the door is  
        closed-->  
    </enableDoorLock>  
    <enableLeaderCard opt="true,false">  
        <!--opt, xs:boolean, whether to enable remaining open with first card. This  
        node is invalid when leaderCardMode is configured-->  
    </enableLeaderCard>  
    <leaderCardMode opt="disable,alwaysOpen,authorize">  
        <!--opt, xs:string, first card mode: "disable", "alwaysOpen"-remain open  
        with first card, "authorize"-first card authentication. If this node is  
        configured, the node <b>enableLeaderCard    </leaderCardMode>  
    <leaderCardOpenDuration min="1" max="1440">  
        <!--opt, xs:integer, duration of remaining open with first card, unit:  
        second-->  
    </leaderCardOpenDuration>
```

```

<stressPassword min="1" max="8">
    <!--wo, opt, xs:string, duress password, the maximum length is 8 bytes, and
the duress password should be encoded by Base64 for transmission-->
</stressPassword>
<superPassword min="1" max="8">
    <!--wo, opt, xs:string, super password, the maximum length is 8 bytes, and
the super password should be encoded by Base64 for transmission-->
</superPassword>
<unlockPassword min="1" max="8">
    <!--wo, opt, xs:string, dismiss password, the maximum length is 8 bytes,
and the dismiss password should be encoded by Base64 for transmission-->
</unlockPassword>
<useLocalController opt="true,false">
    <!--ro, opt, xs:boolean, whether it is connected to the distributed
controller-->
</useLocalController>
<localControllerID min="0" max="64">
    <!--ro, opt, xs:integer, distributed controller No., which is between 1 and
64, 0-unregistered-->
</localControllerID>
<localControllerDoorNumber min="0" max="4">
    <!--ro, opt, xs:integer, distributed controller door No., which is between
1 and 4, 0-unregistered-->
</localControllerDoorNumber>
<localControllerStatus opt="0,1,2,3,4,5,6,7,8,9">
    <!--ro, opt, xs:integer, online status of the distributed controller: 0-
offline, 1-network online, 2-RS-485 serial port 1 on loop circuit 1, 3-RS-485
serial port 2 on loop circuit 1, 4-RS-485 serial port 1 on loop circuit 2, 5-
RS-485 serial port 2 on loop circuit 2, 6-RS-485 serial port 1 on loop circuit
3, 7-RS-485 serial port 2 on loop circuit 3, 8-RS-485 serial port 1 on loop
circuit 4, 9-RS-485 serial port 2 on loop circuit 4-->
</localControllerStatus>
<lockInputCheck opt="true,false">
    <!--opt, xs:boolean, whether to enable door lock input detection-->
</lockInputCheck>
<lockInputType opt="alwaysClose,alwaysOpen">
    <!--opt, xs:string, door lock input type: "alwaysClose"-remain locked
(default), "alwaysOpen"-remain unlocked-->
</lockInputType>
<doorTerminalMode opt="preventCutAndShort,preventCutAndShort,common">
    <!--opt, xs:string, working mode of door terminal: "preventCutAndShort"-_
prevent from broken-circuit and short-circuit (default), "common"-->
</doorTerminalMode>
<openButton opt="true,false">
    <!--opt, xs:boolean, whether to enable door button: "true"-yes (default),
"false"-no-->
</openButton>
<ladderControlDelayTime min="1" max="255">
    <!--opt, xs:integer, elevator control delay time (for visitor), which is
between 1 and 255, unit: minute-->
</ladderControlDelayTime>
<remoteControlPWStatus opt="true,false">

```

```
<!--ro, opt, xs:boolean, whether the password has been configured for  
remote door control-->  
</remoteControlPWStatus>  
</DoorParam>
```

XML_Cap_FaceCompareCond

XML message about condition configuration capability of face picture comparison

```
<FaceCompareCond version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <faceWidthLowerLimit min="" max=""><!--optional, xs:integer, face width  
threshold with highest priority, value range: [0, 100], when the detected face  
width is larger than this threshold, the following conditions will be ignored  
and the face comparison will be executed--></faceWidthLowerLimit>  
    <pitch min="" max=""><!--optional, xs:integer, face raising or bowing angle,  
value range: [0, 90], unit: degree, the smaller the better--></pitch>  
    <yaw min="" max=""><!--optional, xs:integer, face siding left or right angle,  
value range: [0, 90], unit: degree, the smaller the better--></yaw>  
    <width min="" max=""><!--optional, xs:integer, face width, value range: [0,  
100]--></width>  
    <height min="" max=""><!--optional, xs:integer, face height, value range: [0,  
100]--></height>  
    <leftBorder min="" max=""><!--optional, xs:integer, left border of face,  
value range: [0, 100]--></leftBorder>  
    <rightBorder min="" max=""><!--optional, xs:integer, right border of face,  
value range: [0, 100]--></rightBorder>  
    <upBorder min="" max=""><!--optional, xs:integer, top border of face, value  
range: [0, 100]--></upBorder>  
    <bottomBorder min="" max=""><!--optional, xs:integer, bottom border of face,  
value range: [0, 100]--></bottomBorder>  
    <interorbitalDistance min="" max=""><!--optional, xs:integer, pupil distance,  
value range: [0, 100]--></interorbitalDistance>  
    <faceScore min="" max=""><!--optional, xs:integer, face score, value range:  
[0, 100], the valid face score must be larger than this score--></faceScore>  
    <maxDistance opt="0.5,1,1.5,2:auto"><!--optional, xs:string, maximum  
recognition distance: "0.5,1,1.5,2:auto", unit: m. This node has higher  
priority over <interorbitalDistance>--></maxDistance>  
    <similarity min="0.0" max="1.0"><!--optional, xs:float, face comparison  
similarity--></similarity>  
</FaceCompareCond>
```

XML_Cap_IDBlackListCfg

XML message about the parameters of ID card blocklist

```
<IDBlackListCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <blackListValid opt ="0,1">  
        <!--required, xs:integer, ID card blocklist status: 0-invalid, 1-valid.  
This node is used to delete the ID card blocklist by ID card number. If it is
```

```

0, it indicates deleting the blocklist-->
</blackListValid>
<IDCardInfo><!--dependent-->
  <name min="" max=""><!--optional, xs:string, name--></name>
  <birth><!--optional, xs:string, date of birth--></birth>
  <addr min="" max=""><!--optional, xs:string, address--></addr>
  <IDNum min="" max=""><!--required, xs:string, ID card number--></IDNum>
  <issuingAuthority min="" max=""><!--optional, xs:string, issuing authority-->
</issuingAuthority>
  <startDate><!--optional, xs:string, start date of expiry date--></startDate>
  <endDate><!--optional, xs:string, end date of expiry date--></endDate>
  <termOfValidity opt ="true,false">
    <!--optional, xs:boolean, whether it is permanently valid: false-no, true-yes (the <endDate> is invalid)-->
  </termOfValidity>
  <sex opt ="male,female"><!--optional, xs:string, gender: "male" or "female"--></sex>
</IDCardInfo>
</IDBlackListCfg>
```

XML_Cap_IdentityTerminal

IdentityTerminal capability message in XML format

```

<IdentityTerminal version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <terminalMode opt="authMode,registerMode">
    <!--req, xs: string, terminal mode: "authMode"-authentication mode,
"registerMode"-registration mode-->
  </terminalMode>
  <idCardReader opt="iDR210,DS-K1F110-I,DS-K1F1110-B, DS-K1F1110-AB, none">
    <!--req, xs: string, ID card reader model-->
  </idCardReader>
  <camera opt="C270,DS-2CS5432B-S"><!--req, xs: string, camera--></camera>
  <fingerPrintModule opt="ALIWARD,HikModule"><!--req, xs: string, fingerprint
module--></fingerPrintModule>
  <videoStorageTime min="0" max="10"><!--req, xs: integer, time for saving
video (unit: second)--></videoStorageTime>
  <faceContrastThreshold min="0" max="100"><!--req, xs: integer, face picture
comparison threshold--></faceContrastThreshold>
  <twoDimensionCode opt="enable,disable"><!--req, xs: string, whether to enable
QR code recognition--></twoDimensionCode>
  <blackListCheck opt="enable,disable"><!--req, xs: string, whether to enable
blocklist verification--></blackListCheck>
  <idCardCheckCenter opt="local,server">
    <!--req, xs: string, ID card comparison mode: local-compare with ID card of
local storage, server-compare with ID card of remote server storage-->
  </idCardCheckCenter>
  <faceAlgorithm opt="HIK-Z,HIK-H">
    <!--req, xs: string, face picture algorithm: HIK-Z-Hikvision algorithm, HIK-
H-third-party algorithm-->
  </faceAlgorithm>
```

```

<comNo min="1" max="9"><!--req, xs: integer, COM No.--></comNo>
<memoryLearning opt="enable,disable"><!--req, xs: string, whether to enable
learning and memory function--></memoryLearning>
<saveCertifiedImage opt="enable,disable"><!--req, xs: string, whether to
enable saving authenticated picture--></saveCertifiedImage>
<MCUVersion min="" max=""><!--opt, xs: string, MCU version information--></
MCUVersion>
<usbOutput opt="enable,disable"><!--req, xs: string, whether to enable USB
output of ID card reader--></usbOutput>
<serialOutput opt="enable,disable"><!--req, xs: string, whether to enable
serial port output of ID card reader--></serialOutput>
<readInfoOfCard opt="serialNo,file"><!--opt, xs: string, set content to be
read from CPU card--></readInfoOfCard>
<workMode opt="passMode,accessControlMode"><!--opt, xs: string,
authentication mode--></workMode>
<ecoMode>
  <eco opt="enable,disable"><!--opt, xs: string, whether to enable ECO mode-->
</eco>
  <faceMatchThreshold1 min="" max=""><!--req, xs: integer, 1V1 face picture
comparison threshold of ECO mode, which is between 0 and 100--></
faceMatchThreshold1>
  <faceMatchThresholdN min="" max=""><!--req, xs: integer, 1:N face picture
comparison threshold of ECO mode, which is between 0 and 100--></
faceMatchThresholdN>
  <changeThreshold min="" max=""><!--opt, xs: string, switching threshold of
ECO mode, which is between 0 and 8--></changeThreshold>
  <maskFaceMatchThresholdN min="0" max="100"><!--req, xs:integer, 1:N face
picture (face with mask and normal background picture) comparison threshold of
ECO mode, value range: [0,100]--></maskFaceMatchThresholdN>
  <maskFaceMatchThreshold1 min="0" max="100"><!--req, xs:integer, 1:1 face
picture (face with mask and normal background picture) comparison threshold of
ECO mode, value range: [0,100]--></maskFaceMatchThreshold1>
</ecoMode>
<readCardRule opt="wiegand26,wiegand34"><!--opt, xs: string, card No. setting
rule: "wiegand26", "wiegand34"--></readCardRule>
<enableScreenOff opt="true,false"><!--optional, xs:boolean, whether the
device enters the sleep mode when there is no operation after the configured
sleep time--></enableScreenOff>
<screenOffTimeout min="" max=""><!--dependent, xs:integer, sleep time, unit:
second--></screenOffTimeout>
<enableScreensaver opt="true,false"><!--optional, xs:boolean, whether to
enable the screen saver function--></enableScreensaver>
<showMode opt="concise,normal"><!--optional, xs:string, display mode:
"concise" (simple mode, only the authentication result will be displayed),
"normal" (normal mode). The default mode is normal mode. If this node does not
exist, the default mode is normal mode--></showMode>
<menuTimeout min="" max=""><!--dependent, xs:integer, timeout period to exit,
unit: second--></menuTimeout>
</IdentityTerminal>

```

XML_Cap_M1CardEncryptCfg

M1CardEncryptCfg capability message in XML format

```
<M1CardEncryptCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <enable opt="true,false"><!--req, xs:boolean, whether to enable--></enable>
    <sectionID min="0" max="100"><!--req, xs:integer, sector ID--></sectionID>
</M1CardEncryptCfg>
```

XML_Cap_Material

XML message about material management parameter capability

```
<Material version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <id><!--required, xs:integer, material ID--></id>
    <seq min="" max=""><!--optional, xs:integer, material serial No., which
changes every time the material is modified; this field is only valid on the
link between the server and the terminal--></seq>
    <materialName max=""><!--required, xs:string, material name--></
materialName>
    <materialRemarks max=""><!--required, xs:string, material description--></
materialRemarks>
    <materialType opt="static,dynamic"><!--required, xs:string, material type:
"static"-local material, "dynamic"-dynamic material--></materialType>
    <approveState opt="approved,notPass,notApprove"><!--optional, xs:string,
approval status: "approved"-pass, "notPass"-not pass, "notApprove"-not
approved--></approveState>
    <approveRemarks max=""><!--optional, xs:string, approval remarks--></
approveRemarks>
    <shareProperty opt="static,dynamic"><!--optional, xs:string, shared
property: public, private--></shareProperty>
    <uploadUser max=""><!--ro, required, xs:string, uploader, read-only--></
uploadUser>
    <uploadTime><!--read-only, required, xs:time, upload time (ISO 8601
format)--></uploadTime>
    <materialEncrypt min="" max=""><!--optional, xs:integer, material secret
key, which can be used for verifying the correctness of materials received by
the terminal; this field is only valid on the link between the server and the
terminal, e.g.,
JjEmNTA3NDg5NCY0JjI3OTM5MjAmYWEmMzYyOTM5OCZhMCY0MjAzMDQwJmI1JjQzMzc3ODgmNDg=--></materialEncrypt>
    <orgNo><!--optional, xs:integer, organization No.--></orgNo>
    <orgName><!--optional, xs:string, read-only--></orgName>
    <replaceTerminal opt="true,false"><!--optional, xs:boolean, whether to
update the material to the terminal, this field is valid only when replacing
materials--></replaceTerminal>
    <StorageInfo><!--optional, this field is valid only when the materials
saved on the storage server-->
        <storageType min="" max=""><!--optional, xs:string, storage mode,
```

```

"fms,kms,cloud,minio"--></storageType>
    <host min="" max=""><!--optional, xs:string, storage mode, https://[ip]:[port] [coded string]--></host>
        <accountName min="" max=""><!--optional, xs:string, account name, which should be encrypted--></accountName>
            <accountPasswd min="" max=""><!--optional, xs:string, account password, which should be encrypted--></accountPasswd>
                <bucket min="" max=""><!--optional, xs:string, bucket , this field is valid only when storageType is "minio"--></bucket>
            </StorageInfo>
            <StaticMaterial
opt="picture,flash,audio,video,document,ppt,doc,excel, pdf,web"><!--dep-->
                <staticMaterialType
opt="picture,flash,audio,video,document,ppt,doc,excel, pdf,web">
                    <!--dependent, xs:string, local material type-->
                </staticMaterialType>
                <picFormat opt="gif,bmp,jpg,png"><!--dependent, xs:string, image format--></picFormat>
                    <flashFormat opt="swf"><!--dependent, xs:string, flash format--></flashFormat>
                        <audioFormat opt="mp3,wav,wma"><!--dependent, xs:string, audio format--></audioFormat>
                            <videoFormat opt="rm,rmvb,asf,avi,mpg,3gp,mov,mkv,wmv,flv,mp4"><!--dependent, xs:string, video format--></videoFormat>
                                <documentFormat opt="txt"><!--dependent, xs:string, document format--></documentFormat>
                                    <pptFormat opt="ppt,pptx"><!--dependent, xs:string, slide format--></pptFormat>
                                        <docFormat opt="doc,docx"><!--dependent, xs:string, word document format--></docFormat>
                                            <excelFormat opt="xls,xlsx"><!--dependent, xs:string, table format--></excelFormat>
                                                <pdfFormat opt="pdf"><!--dependent, xs:string, PDF--></pdfFormat>
                                                <webFormat opt="html,htm"><!--dependent, xs:string, web file format--></webFormat>
                                                    <fileSize max=""><!--required, xs:integer, unit:byte, file size--></fileSize>
                                                        <duration max=""><!--optional, xs:integer, unit:seconds, material playing duration, this field is valid only when the material is a video or slide--></duration>
                                                            <uuid min="" max=""><!--dependent, xs:string, UUID provided by the server to identify the material, this field is valid only when StorageInfo exists; only 8520 platform saves materials on the storage server--></uuid>
                                                                <staticMaterialUrl min="" max=""><!--dependent, xs:string, material URL, this field is valid only when StorageInfo exists; only 8520 platform saves materials on the storage server--></staticMaterialUrl>
                                                            </StaticMaterial>
                                                            <DynamicMaterial><!--dependent-->
                                                                <dynamicMaterialType
opt="web,socket,rss,realStream,generalData,picUrl,dataSource"><!--dependent, xs:string, dynamic material type--></dynamicMaterialType>
                                                                <webUrl><!--dependent, xs:string, web URL--></webUrl>

```

```

<rssUrl><!--dependent, xs:string, RSS URL--></rssUrl>
<picUrl><!--dependent, xs:string, picture URL--></picUrl>
<RealStream><!--dependent, real stream-->
    <destionType opt="streamMedia,normalIPC"><!--required, xs:string,
streaming terminal type: Stream Media Server, normal network camera--></
destionType>
    <streamMediaUrl><!--dependent, xs:string, streaming server URL--></
streamMediaUrl>
        <NormalIPC><!--dep-->
            <IpAddress><!--dep-->
                <ipVersion opt="v4,v6,dual"><!--required, xs:string--></
ipVersion>
                    <ipAddress><!--dependent, xs:string--></ipAddress>
                    <ipv6Address><!--dependent, xs:string--></ipv6Address>
                </IpAddress>
                <portNo><!--required, xs:integer--></portNo>
                <channelNo><!--required, xs:integer, channel No.--></channelNo>
                <userName min="" max=""><!--required, xs:string, user name for
logging to devices, which is write-only and must be encrypted when
transmission--></userName>
                    <passWord min="" max=""><!--required, xs:string, password for
logging to devices, which is write-only and must be encrypted when
transmission--></passWord>
                    <transmitProtocol opt="tcp,udp,mcast"><!--optional, xs:string,
transmission protocol--></transmitProtocol>
                    <streamType opt="main,sub,third"><!--optional, xs:string,
stream type--></streamType>
                </NormalIPC>
                <dataType opt="capture,liveVideo"><!--optional, xs:string, data
type: capture, "liveVideo"-live video--></dataType>
            </RealStream>
            <GeneralData><!--dependent, third-party data-->
                <SrcAddress><!--IP address of data source -->
                    <ipVersion opt="v4,v6,dual"><!--required, xs:string, IP address
type--></ipVersion>
                        <ipAddress><!--dependent, xs:string--></ipAddress>
                        <ipv6Address><!--dependent, xs:string, IPv6 address--></
ipv6Address>
                    </SrcAddress>
                    <dataType opt="popPic,call"><!--optional, xs:string, third-party
data type: "popPic"-pop-up image, call--></dataType>
                </GeneralData>
                <dataSourceUrl min="" max=""><!--dependent, xs:string, data source URL,
this field is valid only when the material is data source and StorageInfo
exists; only 8520 platform saves materials on the storage server--></
dataSourceUrl>
            </DynamicMaterial>
        </Material>

```

XML_Cap_MaterialSearchProfile

XML message about capability of parameters of searching for materials

```
<MaterialSearchProfile version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <maxTimeSpansNum><!--required, xs:integer, maximum play duration--></maxTimeSpansNum>
    <maxMatchResults><!--required, xs:integer, maximum matched results returned per search--></maxMatchResults>
    <maxSearchTimeout><!--optional, xs:integer, timeout period of search--></maxSearchTimeout>
    <maxConcurrentSearches><!--optional, xs:integer, maximum number of concurrent searches--></maxConcurrentSearches>
    <approveState opt="approved,notPass,notApprove,all"><!--optional, xs:string, approval status--></approveState>
    <materialType opt="static,dynamic,all"><!--optional, xs:string, material type--></materialType>
        <staticMaterialType
            opt="picture,flash,audio,video,document,ppt,doc,excel,pdf,web,app,all"><!--optional, xs:string, local material type--></staticMaterialType>
        <dynamicMaterialType
            opt= "web,socket,rss,realStream,generalData,
            picUrl,all"><!--optional, xs:string, dynamic material type--></dynamicMaterialType>
        <realStreamType
            opt="streamMedia,normalIPC,all"><!--optional, xs:string, real-time stream--></realStreamType>
        <shareProperty opt="public,private,all"><!--optional, xs:string, shared property--></shareProperty>
        <isSupportUploader><!--optional, xs:boolean, whether it supports searching by uploader--></isSupportUploader>
        <isSupportMaterialName><!--optional, xs:boolean, whether it supports searching by material name--></isSupportMaterialName>
        <isSupportMaterialNameLike><!--optional, xs:boolean, whether it supports fuzzy search by material name--></isSupportMaterialNameLike>
        <isSupportMaterialRemarksLike><!--optional, xs:boolean, whether it supports fuzzy search by material description--></isSupportMaterialRemarksLike>
        <isSupportOrgName><!--optional, xs:boolean, whether it supports searching by material organization--></isSupportOrgName>
        <isSupportSubOrg><!--optional, xs:boolean, whether it supports searching by its lower-level organization--></isSupportSubOrg>
        <isSupportSort><!--optional, xs:boolean, whether it supports sort--></isSupportSort>
        <isSupportKeyword><!--optional, xs:boolean, whether it supports searching by keyword--></isSupportKeyword>
        <generalDataType><!--optional, xs:string, general data type: pop-up image, call, all; this field is valid only when the dynamic material is general data--></generalDataType>
        <streamDataType><!--optional, xs:string, stream data type: capture, live view, all; this field is valid only when the real-time stream is normal network camera--></streamDataType>
    </MaterialSearchProfile>
```

XML_Cap_ModuleStatus

Capability message about getting the status of the secure door control unit in XML format

```
<ModuleStatus version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <securityModuleNo min="1" max="256"><!--required, xs:string, secure door
control unit No.--></securityModuleNo>
    <onlineStatus opt="0,1"><!--required, xs:integer, online status: 0-offline, 1-
online--></onlineStatus>
    <desmantelStatus opt="0,1"><!--required, xs:integer, tampering status: 0-not
tampered, 1-tampered--></desmantelStatus>
</ModuleStatus>
```

XML_Cap_Page

XML message about the page configuration capability

```
<Page version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <id><!--required, int, page No.--></id>
    <PageBasicInfo><!--required, basic page information-->
        <pageName max=""><!--required, string, page name--></pageName>
        <BackgroundColor><!--required, background color-->
            <RGB><!--required, int, three primary colors in decimal format, e.g.,
16777215 indicates 0xFFFF--></RGB>
        </BackgroundColor>
        <playDurationMode opt="selfDefine,auto"><!--required, string, page playing
time mode: "selfDefine,auto". When the value of this node is selfDefine, the
node <playDuration> is valid; when the value is auto, it will be calculated
according to the content playing time--></playDurationMode>
        <playDuration min="" max="" default=""><!--dependent, int, playing
duration, unit: second--></playDuration>
        <switchDuration min="" max=""><!--required, int, switching duration, unit:
second--></switchDuration>
        <switchEffect opt=
"none,random,boxShrink,boxSpread,cycleShrink,cycSpread,eraseUp,eraseDown,eraseLe
ft,eraseRight,verticalShelter,horizontalShelter,verticalChessboard,horizontalChe
ssboard,dissolve,leftRightToCenter,ceterToLeftRight,upDownToCenter,centerToUpDow
n,drawOutLeftDown,drawOutLeftUp,drawOutRightDown,drawOutRightUp,verticalLine,hor
izontalLine"><!--required, string, switching effect:
"none,random,boxShrink,boxSpread,cycleShrink,cycSpread,eraseUp,eraseDown,eraseLe
ft,eraseRight,verticalShelter,horizontalShelter,verticalChessboard,horizontalChe
ssboard,dissolve,leftRightToCenter,ceterToLeftRight,upDownToCenter,centerToUpDow
n,drawOutLeftDown,drawOutLeftUp,drawOutRightDown,drawOutRightUp,verticalLine,hor
izontalLine"--></switchEffect>
        <backgroundPic><!--optional, int, background picture which is the picture
material ID--></backgroundPic>
    </PageBasicInfo>
    <characterMode opt="mode1,mode2,mode3"><!--optional, xs:string, welcome word
mode on the page: mode1, mode2, mode3. For access control devices, the position
```

```

of the welcome words is fixed and can be in three modes--></characterMode>
<WindowsList size=""><!--optional, window information-->
    <Windows>
        <id><!--required, int, content No.--></id>
        <Position><!--required, content's position. The upper-left corner is the
origin, and the size of the full screen is 1920*1920-->
            <positionX min="" max=""><!--required, int, X-coordinate of upper-left
corner of the content's rectangle frame--></positionX>
            <positionY min="" max=""><!--required, int, Y-coordinate of upper-left
corner of the content's rectangle frame--></positionY>
            <height min="" max=""><!--required, int, height of the content's
rectangle frame--></height>
            <width min="" max=""><!--required, int, width of the content's
rectangle frame--></width>
        </Position>
        <layerNo min="" max=""><!--required, int, layer No.--></layerNo>
        <WinMaterialInfo><!--dependent, window material information-->
            <materialType><!--required, string, window material type: static,
dynamic, other--></materialType>
            <staticMaterialType
opt="picture,flash,audio,video,document,ppt,doc,excel, pdf, web, app, "><!--
dependent, string, local material type. This node is valid when <materialType>
is static--></staticMaterialType>
            <dynamicType opt="
web,socket,rss,call,dynamicPic,realStream,capturePic, character "><!--
dependent, string, dymanic window material type:
"web,socket,rss,call,dynamicPic,realStream,capturePic, character". This node is
valid when <materialType> is dynamic--></dynamicType>
            <otherType opt="clock,weather,countdown,localInput,hyperlinkBtn"><!--
dependent, hyperlinkBtn"string, other type:
"clock,weather,countdown,localInput,hyperlinkBtn"--></otherType>
        </WinMaterialInfo>
        <TouchProperty><!--optional, touching attributes-->
            <windType opt="popup,page"><!--optional, string, window type: pop-up
window, page window--></windType>
            <hyperlinkType opt="window,page"><!--optional, string, hyperlink type:
>window,page". This node is valid when <windType> is popup--></hyperlinkType>
            <windowId><!--dependent, int, window No. (window of current page). This
node is valid when <hyperlinkType> is window--></windowId>
            <pageId><!--dependent, int, page No. This node is valid when
<hyperlinkType> is page--></pageId>
        </TouchProperty>
        <PlayItemList size=""><!--dependent, window playing list-->
            <PlayItem><!--req-->
                <id><!--required, int, playing No.--></id>
                <materialNo><!--dependent, int, material index No.--></materialNo>
                <inputChannel min="" max=""><!--optional, string, linked channel No.
of the network camera--></inputChannel>
                <playEffect><!--required, string, playing effect: none, scroller--></
playEffect>
                <MarqueeInfo><!--dependent-->
                    <scrollType><!--required, string, scroller scrolling type: not

```

```

scroll, scroll circularly, scroll once, scroll backwards and forwards--></
scrollType>
    <scrollDeriction><!--required, string, scroller scrolling
direction: none, from top to bottom, from bottom to top, from left to right,
from right to left--></scrollDeriction>
    <scrollSpeed><!--required, int, scroller scrolling speed--></
scrollSpeed>
    </MarqueeInfo>
    <PlayDuration><!--material playing duration. This node can be
configured for local materials, live video, and network camera channels-->
        <durationType><!--required, string, playing duration type, custom--></
durationType>
        <duration min="" max=""><!--required, int, material playing
duration, unit: second--></duration>
    </PlayDuration>
    <CharactersEffect><!--required, character display effect. This node
is valid when the material type is text or TXT file-->
        <fontSize min="" max=""><!--required, int, font size--></fontSize>
        <FontColor><!--required, font color-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </FontColor>
        <BackColor><!--required, background color-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackColor>
        <backTransparent min="" max=""><!--required, int, background
transparency--></backTransparent>
        <subtitlesEnabled><!--required, boolean, whether to enable
character display mode--></subtitlesEnabled>
        <scrollDirection opt="left,right,up,down"><!--required, string,
character scrolling direction: "left,right,up,down"--></scrollDirection>
        <scrollSpeed min="" max=""><!--required, int, text scrolling
speed--></scrollSpeed>
    </CharactersEffect>
    <switchEffect><!--optional, string, switching effect of the window
material: from left to right, from right to left, from bottom to top, from top
to bottom, fade in and fade out, exit from the middle, pop down from the top,
enter from the lower-right corner, enter from the upper-left corner, blind
horizontally, blind vertically, random effect. This node is valid for picture
materials--></switchEffect>
    <pageTime min="" max=""><!--dependent, int, paging interval, unit:
second. This node is valid when the material is a word, ppt, pdf, or excel
file--></pageTime>
        <scrollSpeed min="" max=""><!--dependent, int, scrolling speed. This
node is valid when the material is a static web--></scrollSpeed>
        <CharactersAttribute><!--dependent, character attribute, this node is
valid when <b><dynamicType></dynamicType></b> is character-->
            <fontSize min="" max=""><!--optional, int, font size--></fontSize>
            <FontColor><!--optional, font color-->
                <RGB><!--optional, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>

```

```

        </FontColor>
        <BackColor><!--optional, background color-->
            <RGB><!--optional, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackColor>
        <backTransparent min="" max=""><!--optional, int, background
transparency--></backTransparent>
        <alignType
opt="left,right,middle,top,bottom,verticalCenter,horizontallyCenter"><!--
optional, string, alignment mode:
"left,right,middle,top,bottom,verticalCenter,horizontallyCenter"--></alignType>
            <characterContent max=""><!--optional, string, text content whose
maximum size is 512 bytes. This node is valid when <b>dynamicType</b> is character--></characterContent>
            </CharactersAttribute>
        </PlayItem>
    </PlayItemList>
    <enabledAudio opt="true,false"><!--dependent, boolean, whether to enable
the audio--></enabledAudio>
    <enableHide opt="true,false"><!--optional, boolean, whether to enable
hiding--></enableHide>
    <enableLock opt="true,false"><!--optional, boolean, whether to enable the
clock--></enableLock>
    <AppWindow><!--dependent-->
        <WindowInfoList size=""><!--required-->
            <WindowInfo><!--required, -->
                <id><!--required, int, No.--></id>
                <materialNo><!--required, int, material No.--></materialNo>
            </WindowInfo>
        </WindowInfoList>
    </AppWindow>
    <DataSource><!--dependent, data source. This node is valid when it is a
calling or pop-up window-->
        <materialNo><!--required, int, material No.--></materialNo>
    </DataSource>
    <Call><!--dependent, calling data-->
        <tableRow min="" max=""><!--required, int, row of the table--></
tableRow>
        <tableColumn min="" max=""><!--required, int, column of the table--></
tableColumn>
        <tableDirection opt="vertical,horizontal"><!--required, int, table
direction: "vertical,horizontal"--></tableDirection >
            <tableType><!--required, xs:string, table template:
"template1,template2,template3,template4,template5,template6"--></tableType>
            <backPicId
opt="template1,template2,template3,template4,template5,template6"><!--optional,
int, control's background picture--></backPicId>
            <alignType opt="left,right,middle"><!--required, string, alignment
mode: "left,right,middle"--></alignType>
            <refreshDirection opt="upTodown,downToup,leftToright,rightToleft"><!--
required, string, refreshing direction: "upTodown"-from top to bottom,
"downToup"-from bottom to top--></refreshDirection>

```

```

<HeadDataList size=""><!--optional-->
    <HeadData><!--optional, table head data (calling data)-->
        <id><!--required, int, No.--></id>
        <data min="" max=""><!--required, string, data--></data>
    </HeadData>
</HeadDataList>
<ItemStyleList size="">
    <ItemStyle><!--style of the table's row or column-->
        <id><!--required, int, No.--></id>
        <width min="" max=""><!--required, int, width of each column
(percentage)--></width>
        <fontSize min="" max=""><!--required, int, font size--></fontSize>
        <FontColor min="" max=""><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </FontColor>
        <BackColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackColor>
    </ItemStyle>
</ItemStyleList>
</Call>
<DynamicPic><!--dependent, dynamic pop-up window parameters-->
    <backPicId><!--optional, int, ID of the control's background picture--></backPicId>
</DynamicPic>
<CapturePic><!--dependent-->
    <backPicId><!--optional, int, ID of the control's background picture--></backPicId>
    <ipcMaterialNo><!--required, int--></ipcMaterialNo>
    <cancelType opt="auto,manual"><!--required, int, cancellling type:
"auto,manual"--></cancelType>
    <duration min="" max=""><!--dependent, int, material playing duration,
unit: second--></duration>
</CapturePic>
<ClockParam><!--dependent, clock parameters-->
    <backPicId><!--optional, int, ID of the control's background picture--></backPicId>
    <ClockIcon><!--required, clock icon paameters-->
        <enabled><!--required, boolean--></enabled>
        <type opt="clock1,clock2,..."><!--dependent, string, type:
"clock1,clock2,..."--></type>
        <Position><!--dependent-->
            <positionX min="" max=""><!--required, int,X-coordinate of the
content's position--></positionX>
            <positionY min="" max=""><!--required, int,Y-coordinate of the
content's position--></positionY>
            <height min="" max=""><!--required, int, height--></height>
            <width min="" max=""><!--required, int, width--></width>
        </Position>
    </ClockIcon>

```

```

<YmdParam><!--required, parameters of year, month, and day in the
clock-->
    <enabled><!--required, boolean, whether to enable--></enabled>
    <fontSize min="" max=""><!--required, int, font size--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
        <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
        <height min="" max=""><!--required, int, height--></height>
        <width min="" max=""><!--required, int, width--></width>
    </Position>
</YmdParam>
<HmsParam><!--required, parameters of hour, minute, and second in the
clock-->
    <enabled><!--required, boolean--></enabled>
    <fontSize min="" max=""><!--required, int, font size--></fontSize>
    <FontColor><!--required, font color-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
        <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
        <height min="" max=""><!--required, int, height--></height>
        <width min="" max=""><!--required, int, width--></width>
    </Position>
</HmsParam>
<WeekParam><!--required, week parameters-->
    <enabled><!--required, boolean--></enabled>
    <fontSize min="" max=""><!--required, int--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>

```

```

        </BackColor>
        <Position><!--dependent-->
            <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
            <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
            <height min="" max=""><!--required, int, height--></height>
            <width min="" max=""><!--required, int, width--></width>
        </Position>
        </WeekParam>
    </ClockParam>
    <WeatherParam><!--dependent, weather parameters-->
        <backPicId><!--optional, int, ID of the weather's background picture--></backPicId>
        <WeatherIcon><!--optional, weather icon parameters-->
            <enabled><!--required, boolean, whether to enable--></enabled>
            <Position><!--dependent-->
                <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
                <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
                <height min="" max=""><!--required, int, height--></height>
                <width min="" max=""><!--required, int, width--></width>
            </Position>
        </WeatherIcon>
        <Date><!--optional, date parameters-->
            <enabled><!--required, boolean, whether to enable--></enabled>
            <fontSize min="" max=""><!--required, int, font size--></fontSize>
            <FontColor><!--required, font color-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFF--></RGB>
            </FontColor>
            <BackColor><!--required-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFF--></RGB>
            </BackColor>
            <Position><!--dependent-->
                <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
                <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
                <height min="" max=""><!--required, int, height--></height>
                <width min="" max=""><!--required, int, width--></width>
            </Position>
        </Date>
        <Temperature><!--optional, temperature parameters-->
            <enabled><!--required, boolean, whether to enable--></enabled>
            <fontSize min="" max=""><!--required, int, font size--></fontSize>
            <FontColor><!--required, font color-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFF--></RGB>
            </FontColor>

```

```

<BackColor><!--required-->
    <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
</BackColor>
<Position><!--dependent-->
    <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
    <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
    <height min="" max=""><!--required, int, height--></height>
    <width min="" max=""><!--required, int, width--></width>
</Position>
</Temperature>
<WeatherContent><!--optional, weather parameters-->
    <enabled><!--required, boolean, whether to enable--></enabled>
    <fontSize min="" max=""><!--required, int, font size--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
        <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
        <height min="" max=""><!--required, int, height--></height>
        <width min="" max=""><!--required, int, width--></width>
    </Position>
</WeatherContent>
<City><!--optional, city parameters-->
    <enabled><!--required, boolean, whether to enable--></enabled>
    <cityId><!--required, string, city No.--></cityId>
    <cityName><!--required, string, city name--></cityName>
    <fontSize min="" max=""><!--required, int--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
        <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
        <height min="" max=""><!--required, int, height--></height>

```

```

<width min="" max=""><!--required, int, width--></width>
</Position>
</City>
<Humidity><!--optional, humidity parameters-->
<enabled><!--required, boolean, whether to enable--></enabled>
<fontSize min="" max=""><!--required, int--></fontSize>
<FontColor><!--required-->
<RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
</FontColor>
<BackColor><!--required-->
<RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
</BackColor>
<Position><!--dependent-->
<positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
<positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
<height min="" max=""><!--required, int, height--></height>
<width min="" max=""><!--required, int, width--></width>
</Position>
</Humidity>
<AirQuality><!--optional, air quality parameters-->
<enabled><!--required, boolean--></enabled>
<fontSize min="" max=""><!--required, int--></fontSize>
<FontColor><!--required-->
<RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
</FontColor>
<BackColor><!--required-->
<RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
</BackColor>
<Position><!--dependent-->
<positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
<positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
<height min="" max=""><!--required, int, height--></height>
<width min="" max=""><!--required, int, width--></width>
</Position>
</AirQuality>
<UpdateTime><!--optional, update time parameters-->
<enabled><!--required, boolean, whether to enable--></enabled>
<refreshTime><!--required, xs:time, refreshing time in ISO8601 time
format--></refreshTime>
<updateInterval><!--required, int, updating interval, unit: minute--></updateInterval>
<fontSize min="" max=""><!--required, int--></fontSize>
<FontColor><!--required-->
<RGB><!--required, int, three primary colors in decimal format,

```

```

e.g., 16777215 indicates 0xFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
        <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
        <height min="" max=""><!--required, int, height--></height>
        <width min="" max=""><!--required, int, width--></width>
    </Position>
    </UpdateTime>
    <Wind><!--optional, wind power parameters-->
        <enabled><!--required, boolean, whether to enable--></enabled>
        <fontSize min="" max=""><!--required, int--></fontSize>
        <FontColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </FontColor>
        <BackColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackColor>
        <Position><!--dependent-->
            <positionX min="" max=""><!--required, int, X-coordinate of the
content's position--></positionX>
            <positionY min="" max=""><!--required, int, Y-coordinate of the
content's position--></positionY>
            <height min="" max=""><!--required, int, height--></height>
            <width min="" max=""><!--required, int, width--></width>
        </Position>
        </Wind>
    </WeatherParam>
    <Countdown><!--dependent, countdown material-->
        <endTime><!--required, xs:time, countdown time in ISO8601 time format--></endTime>
            <template opt="template1,template2..."><!--required, string, tempalte:
"template1" (template 1), "template2..." (template 2)--></template>
            <timeUnit opt="year,month,day,week,hour,minute,second"><!--required,
string, time unit: "year,month,day,week,hour,minute,second"--></timeUnit>
            <backPicId><!--optional, int--></backPicId>
            <TimeFontCfg><!--optional-->
                <fontSize min="" max=""><!--required, int--></fontSize>
                <FontColor><!--required-->
                    <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
                </FontColor>
                <Position><!--required, content's position. The upper-left corner is
the origin, and the size of the full screen is 1920*1920-->

```

```
<positionX min="" max=""><!--required, int, X-coordinate of upper-left corner of the content's rectangle frame--></positionX>
<positionY min="" max=""><!--required, int, Y-coordinate of upper-left corner of the content's rectangle frame--></positionY>
<height min="" max=""><!--required, int, height of the content's rectangle frame--></height>
<width min="" max=""><!--required, int, width of the content's rectangle frame--></width>
</Position>
</TimeFontCfg>
</Countdown>
<localInputNo opt="VGA,HDMI"><!--dependent, string, local input No.--></localInputNo>
<HyperlinkBtn><!--dependent-->
<backPicId><!--optional, int, ID of the control's background picture--></backPicId>
</HyperlinkBtn>
</Windows><!--optional-->
</WindowsList>
</Page>
```

XML_Cap_PlaySchedule

XML message about the program schedule configuration capability

```
<PlaySchedule version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
<id><!--required, xs:integer, program schedule ID--></id>
<scheduleName max=""><!--required, xs:string, program schedule name--></scheduleName>
<scheduleRemarks max=""><!--optional, xs:string, program schedule description--></scheduleRemarks>
<approveState opt="approved,notPass,notApprove"><!--optional, xs:string, approval status: "approved"-pass, "notPass"-not pass, "notApprove"-not approved--></approveState>
<approveRemarks max=""><!--optional, xs:string, approval remarks--></approveRemarks>
<scheduleMode opt="normal,decode,touch,decodeTouch"><!--optional, xs:string, program schedule mode: mormal, decode and touch--></scheduleMode>
<orgNo><!--optional, xs:integer, organization No.--></orgNo>
<scheduleType opt="selfDefine,daily,weekly,loop,defaultSchedule"><!--optional, xs:string, program schedule type: "daily"-daily schedule, "weekly"-weekly schedule, "selfDefine"-custom schedule, loop-loop schedule, "defaultSchedule"-default schedule--></scheduleType>
<shareProperty opt="public,private"><!--optional, xs:string, shared property: public, private--></shareProperty>
<DailySchedule><!--dependent, daily schedule-->
<PlaySpanList size=""><!--required-->
<PlaySpan><!--required-->
<id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
<programNo><!--required, xs:integer, No. of the shown program--></programNo>
```

```

<TimeRange><!--required, play duration-->
    <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
    <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
</TimeRange>
</PlaySpan>
</PlaySpanList>
</DailySchedule>
<WeeklySchedule><!--dependent, weekly schedule-->
    <DayList size=""><!--required-->
        <Day><!--required-->
            <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
            <dayOfWeek opt="monday,tuesday,...,sunday"><!--required, xs:string, day
of a week --></dayOfWeek>
                <PlaySpanList size=""><!--required, play schedule-->
                    <PlaySpan><!--required-->
                        <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
                        <programNo><!--required, xs:integer, No. of the looped program--></
programNo>
                        <TimeRange><!--required, play duration-->
                            <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
                            <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
                        </TimeRange>
                    </PlaySpan>
                </PlaySpanList>
            </Day>
        </DayList>
    </WeeklySchedule>
<LoopSchedule><!--dependent, loop schedule-->
    <ProgramNoList size=""><!--required, list of looping programs, normal mode-->
        <programNo><!--required, xs:integer, No. of the looped program--></
programNo>
        </ProgramNoList>
        <LoopTimeSpanList size=""><!--dependent-->
            <LoopTimeSpan><!--optional-->
                <TimeRange><!--required, play duration-->
                    <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
                    <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
                </TimeRange>
            </LoopTimeSpan>
        </LoopTimeSpanList>
    </LoopSchedule>
<SelfDefineSchedule><!--dependent-->

```

```

<SelfDefineList size=""><!--required-->
    <SelfDefine><!--required, custom play duration-->
        <id><!--required, xs:integer, custom play duration No.--></id>
        <programNo><!--required, xs:integer, program No.--></programNo>
        <TimeRange><!--required, play duration-->
            <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
            <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
        </TimeRange>
    </SelfDefine>
</SelfDefineList>
</SelfDefineSchedule>
<DefaultSchedule><!--dependent, default program schedule-->
    <programNo><!--required, xs:integer, program No.--></programNo>
</DefaultSchedule>
<HolidaySchedule><!--optional, holiday schedule, which can be attached to the
daily or weekly schedule-->
    <PlaySpanList><!--required, daily schedule-->
        <PlaySpan><!--required, daily schedule-->
            <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
            <programNo><!--required, xs:integer, program No.--></programNo>
            <TimeRange><!--required, duration-->
                <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
                <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
            </TimeRange>
        </PlaySpan>
    </PlaySpanList>
</HolidaySchedule>
</PlaySchedule>

```

XML_Cap_Program

XML message about capability of program parameters

```

<Program version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <id><!--required, xs:integer, program ID--></id>
    <programName max=""><!--required, xs:string, program name--></programName>
    <programRemarks max=""><!--required, xs:string, program description--></
programRemarks>
    <shareProperty opt="public,private"><!--optional, xs:string, shared property:
public, private--></shareProperty>
    <approveState opt="approved,notPass,notApprove"><!--optional, xs:string,
approval status: "approved"-pass, "notPass"-not pass, "notApprove"-not
approved--></approveState>
    <approveRemarks max=""><!--optional, xs:string, approval remarks--></
approveRemarks>
    <programType opt="normal,decode,touch,decodeTouch"><!--optional, xs:string,
program type: normal, decode, touch, "decodeTouch"-decode and touch, character

```

```
(welcome words, which is used for access control devices)--></programType>
<orgNo><!--optional, xs:integer, organization No.--></orgNo>
<Resolution><!--required-->
    <resolutionName opt="1920*1080,1080*1920"><!--optional, xs:string,
resolution --></resolutionName>
    <imageWidth min="" max=""><!--required, xs:integer, resolution width--></
imageWidth>
    <imageHeight min="" max=""><!--required, xs:integer, resolution height--></
imageHeight>
</Resolution>
<PageList size="" /><!--required, page list-->
<programSize><!--read-only, optional, xs:integer, page list, unit: byte--></
programSize>
<programLength><!--read-only, optional, xs:integer, program duration, unit:
second--></programLength>
</Program>
```

See Also

[XML_PageList](#)

XML_Cap_ReaderAcrossHost

ReaderAcrossHost capability message in XML format

```
<ReaderAcrossHost version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <AcrossHostList size="8">
        <AcrossHostAction>
            <readerNo min="1" max="8"><!--req, xs: integer, card reader No.--></
readerNo>
            <submarineBackEnabled opt="true,false">
                <!--req, xs: boolean, whether to enable the cross-controller anti-
passing back function of the card reader-->
            </submarineBackEnabled>
        </AcrossHostAction>
    </AcrossHostList>
</ReaderAcrossHost>
```

XML_Cap_RemoteControlDoor

RemoteControlDoor capability message in XML format

```
<RemoteControlDoor version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <doorNo min="" max=""><!--opt, xs:integer, range of the door No.--></doorNo>
    <cmd
opt="open,close,alwaysOpen,alwaysClose,visitorCallLadder,householdCallLadder">
        <!--req, xs:string, command: "open"-open the door, "close"-close the door
(controlled), "alwaysOpen"-remain unlocked (free), "alwaysClose"-remain locked
(disabled), "visitorCallLadder"-call elevator (visitor), "householdCallLadder"->
```

```
call elevator (resident)-->
  </cmd>
  <password min="" max="">
    <!--opt, xs:string, password for opening door-->
  </password>
</RemoteControlDoor>
```

XML_Cap_ServerDevice

ServerDevice capability message in XML format

```
<ServerDevice version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <ipAddr min="" max=""><!--req, xs: string, IP address of the cross-controller
anti-passing back server--></ipAddr>
  <port min="" max=""><!--req, xs: string, port No. of the cross-controller
anti-passing back server--></port>
</ServerDevice>
```

XML_Cap_SnapConfig

SnapConfig capability message in XML format

```
<SnapConfig version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <snapTimes min="0" max="5"><!--required, xs: integer, capture times
triggered by loop, the value is between 0 and 5--></snapTimes>
  <snapWaitTime min="0" max="6000">
    <!--required, xs: integer, capture waiting time, the value is between 0 and
6,000, currently, this node is reserved-->
  </snapWaitTime>
  <intervalTimeList size="4"><!--req-->
    <intervalTime min="0" max="6000"><!--required, xs: integer, time interval
of continuous capture, the value is between 0 and 6,000--></intervalTime>
  </intervalTimeList>
  <JPEGParam>
    <pictureSize>
      <!--required, xs: string, picture resolution: 0-CIF, 1-QCIF, 2-D1, 3-UXGA
(1600 × 1200), 4-SVGA(800 × 600), 5-HD720p(1280 × 720), 6-VGA, 7-XVGA, 8-
HD900p, 9-HD1080, 10 (2560 × 1920), 11 (1600 × 304), 12 (2048 × 1536), 13 (2448
× 2048), 14 (2448 × 1200), 15 (2448 × 800), 16-XGA (1024 × 768), 17-SXGA(1280 ×
1024), 18-WD1(960 × 576/960 × 480), 19 (1080i), 20 (576 × 576), 21 (1536 ×
1536), 22 (1920 × 1920), 161 (288 × 320), 162 (144 × 176), 163 (480 × 640), 164
(240 × 320), 165 (120 × 160), 166 (576 × 720), 167 (720 × 1280), 168 (576 ×
960), 180 (180*240), 181 (360*480), 182 (540*720), 183 (720*960), 184
(960*1280), 185 (1080*1440), 0xff (auto)-->
    </pictureSize>
    <pictureQuality opt="best, better, general"><!--required, xs: string,
picture quality: "best", "better", "general"--></pictureQuality>
```

```
</JPEGParam>  
</SnapConfig>
```

XML_Cap_StartReaderInfo

StartReaderInfo capability message in XML format

```
<StartReaderInfo version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <hostNo min="1" max="64"><!--req, xs: integer, access controller No.--></hostNo>  
    <readerNo min="1" max="8"><!--req, xs: integer, card reader No.--></readerNo>  
</StartReaderInfo>
```

XML_Cap_SubmarineBack

SubmarineBack capability message in XML format

```
<SubmarineBack version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <enabled opt="true,false"><!--req, xs: boolean, whether to specify this  
access controller as the cross-controller anti-passing back server--></enabled>  
</SubmarineBack>
```

XML_Cap_SubmarineBackHostInfo

SubmarineBackHostInfo capability message in XML format

```
<SubmarineBackHostInfo version="2.0" xmlns="http://www.isapi.org/ver20/  
XMLSchema">  
    <ID min="1" max="4"><!--req, xs: integer, configuration No.--></ID>  
    <HostInfoList size="16">  
        <Action>  
            <deviceNo min="1" max="64"><!--req, xs: integer, device No.--></deviceNo>  
            <serial min="9" max="9"><!--req, xs: string, device serial No.--></serial>  
        </Action>  
    </HostInfoList>  
</SubmarineBackHostInfo>
```

XML_Cap_SubmarineBackMode

SubmarineBackMode capability message in XML format

```
<SubmarineBackMode version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <mode opt="disable,internetCommunicate,cardReadAndWrite"><!--req, xs:string,  
anti-passing back mode--></mode>  
    <rule opt="line,inOrOut">  
        <!--req, xs:string, anti-passing back rule, this node is invalid when the
```

```
mode is set to "disable"-->
</rule>
<sectionID min="1" max="100">
    <!--req, xs:integer, section ID, this node is valid when mode is
"cardReadAndWrite", and only one section ID can be configured for one
configuration-->
</sectionID>
</SubmarineBackMode>
```

XML_Cap_SubmarineBackReader

SubmarineBackReader capability message in XML format

```
<SubmarineBackReader version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <ID min="1" max="128"><!--req, xs:integer, configuration No.--></ID>
        <selfHostNo min="1" max="64"><!--req, xs:integer, access control No. of the
configuration object--></selfHostNo>
        <selfReaderNo min="1" max="8"><!--req, xs:integer, card reader No. of the
configuration object--></selfReaderNo>
        <FollowReaderList size="16">
            <Action>
                <followHostNo min="1" max="64"><!--req, xs:integer, following access
controller No.--></followHostNo>
                <followReaderNo min="1" max="8"><!--req, xs:integer, following card
reader No.--></followReaderNo>
            </Action>
        </FollowReaderList>
    </SubmarineBackReader>
```

XML_Cap_WiegandCfg

WiegandCfg capability message in XML format

```
<WiegandCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <wiegandNo min="1" max="64"><!--required, xs:integer, Wiegand interface No.--></wiegandNo>
        <communicateDirection opt="receive,send"><!--required, xs:string,
communication direction: "receive", "send"--></communicateDirection>
        <wiegandMode opt="wiegand26,wiegand34,wiegand27,wiegand35"><!--dependent,
xs:string, Wiegand mode: "wiegand26", "wiegand34", "wiegand27", "wiegand35".
This node is valid when <communicateDirection> is "send"--></wiegandMode>
        <signalInterval min="1" max="20"><!--optional, xs:integer, interval of
sending Wiegand signals, it is between 1 and 20, unit: ms--></signalInterval>
        <enable opt="true,false"><!--optional, xs:boolean, whether to enable Wiegand
parameters: true, false--></enable>
    </WiegandCfg>
```

XML_Cap_WiegandRuleCfg

WiegandRuleCfg capability message in XML format

```

<WiegandRuleCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <name min="" max="">
        <!--req, xs:string, Wiegand name-->
    </name>
    <CustomerCardIn>
        <totalLength min="" max="">
            <!--req, xs:integer, total Wiegand length. When this node is set to 0,
the custom Wiegand rule settings will be cleared-->
        </totalLength>
        <checkMethod opt="parityCheck,xorCheck,noCheck">
            <!--req, xs:string, parity mode: "parityCheck,xorCheck,noCheck"-->
        </checkMethod>
        <ParityCheck>
            <!--dep, configuration rule of odd-even parity, this node is valid when
<checkMethod> is "parityCheck"-->
            <oddBeginBit min="" max="">
                <!--dep, xs:integer, start bit of odd parity-->
            </oddBeginBit>
            <oddLength min="" max="">
                <!--dep, xs:integer, odd parity length-->
            </oddLength>
            <evenBeginBit min="" max="">
                <!--dep, xs:integer, start bit of even parity-->
            </evenBeginBit>
            <evenLength min="" max="">
                <!--dep, xs:integer, even parity length-->
            </evenLength>
        </ParityCheck>
        <XorCheck>
            <!--dep, configuration rule of XOR parity, this node is valid when
<checkMethod> is "xorCheck"-->
            <xorBeginBit min="" max="">
                <!--dep, xs:integer, start bit of XOR parity-->
            </xorBeginBit>
            <xorPerLength min="" max="">
                <!--dep, xs:integer, length of each XOR parity group-->
            </xorPerLength>
            <xorTotalLength min="" max="">
                <!--dep, xs:integer, total length of XOR parity data-->
            </xorTotalLength>
        </XorCheck>
        <cardIdBeginBit min="" max="">
            <!--req, xs:integer, start bit of the card No.-->
        </cardIdBeginBit>
        <cardIdLength min="" max="">
            <!--req, xs:integer, card No. length-->
        </cardIdLength>
    
```

```

<siteCodeBeginBit min="" max="">
    <!--req, xs:integer, start bit of the site code-->
</siteCodeBeginBit>
<siteCodeLength min="" max="">
    <!--req, xs:integer, site code length-->
</siteCodeLength>
<oemBeginBit min="" max="">
    <!--req, xs:integer, start bit of OEM-->
</oemBeginBit>
<oemLength min="" max="">
    <!--req, xs:integer, OEM length-->
</oemLength>
<manufacturerCodeBeginBit min="" max="">
    <!--req, xs:integer, start bit of the manufacturer code-->
</manufacturerCodeBeginBit>
<manufacturerCodeLength min="" max="">
    <!--req, xs:integer, manufacturer code length-->
</manufacturerCodeLength>
</CustomerCardIn>
<CustomerCardOut>
    <CardContentList size="4">
        <!--This node contains multiple <Action> nodes, and the <type> node in
each <Action> node can only be set to one type. The order of the types will
determine the combination order of the rules-->
        <Action>
            <No min="" max="">
                <!--req, xs:integer, No.-->
            </No>
            <type opt="cardId,siteCode,oem,manufacturerCode">
                <!--req, xs:string, type: "cardId"-card ID, "siteCode"-site code,
"oem"-OEM No., "manufacturerCode"-manufacturer code-->
            </type>
            <length min="" max="">
                <!--req, xs:integer, length of the corresponding decimal data-->
            </length>
        </Action>
    </CardContentList>
</CustomerCardOut>
</WiegandRuleCfg>

```

XML_ClearCardRecord

ClearCardRecord message in XML format

```

<ClearCardRecord version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <clearAllCard>
        <!--req, xs: boolean, whether to clear all card swiping records in the
cross-controller anti-passing back server: "true"-yes, "false"-no. If this node
is set to "false", either CardList or EmployeeNoList is required. If CardList
is configured, it indicates clearing card swiping records by card No.; if
EmployeeNoList is configured, it indicates clearing card swiping records by

```

```
employee No.-->
  </clearAllCard>
  <CardList size="32">
    <cardNo><!--opt, xs: string, card No., min="1" max="32"--></cardNo>
  </CardList>
  <EmployeeNoList size="32">
    <employeeNo><!--opt, xs:string, employee No. (person ID)--></employeeNo>
  </EmployeeNoList>
</ClearCardRecord>
```

XML_ClearSubmarineBack

ClearSubmarineBack message in XML format

```
<ClearSubmarineBack version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <clearHostInfo><!--opt, xs: boolean, whether to clear access controller
information: "true,false"--></clearHostInfo>
  <clearReaderInfo><!--opt, xs: boolean, whether to clear card reader
information: "true,false"--></clearReaderInfo>
  <clearSubmarineBack><!--opt, xs: boolean, whether to clear anti-passing back
server parameters: "true,false"--></clearSubmarineBack>
  <clearSubmarineBackHostInfo>
    <!--opt, xs: boolean, whether to clear cross-controller anti-passing back
parameters of access controllers: "true,false"-->
  </clearSubmarineBackHostInfo>
  <clearStartReaderInfo><!--opt, xs: boolean, whether to clear first card
reader parameters: "true,false"--></clearStartReaderInfo>
  <clearSubmarineBackReader>
    <!--opt, xs: boolean, whether to clear cross-controller anti-passing back
parameters of card readers: "true,false"-->
  </clearSubmarineBackReader>
  <clearSubmarineBackMode>
    <!--opt, xs: boolean, whether to clear the cross-controller anti-passing
back mode parameters: "true,false"-->
  </clearSubmarineBackMode>
  <clearServerDevice>
    <!--opt, xs: boolean, whether to clear the parameters of cross-controller
anti-passing back server: "true,false"-->
  </clearServerDevice>
  <clearReaderAcrossHost>
    <!--opt, xs: boolean, whether to clear the cross-controller anti-passing
back status of card readers: "true,false"-->
  </clearReaderAcrossHost>
</ClearSubmarineBack>
```

XML_DeployInfo

DeployInfo message in XML format

```
<DeployInfo version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <DeployList size="5">
    <Content>
      <deployNo><!--req, xs: integer, arming No.--></deployNo>
      <deployType><!--req, xs: integer, arming type: 0-client arming to receive real-time or offline events via platform or system (based on Hikvision private protocol), 1-real-time arming to receive real-time events (based on Hikvision private protocol), 2-arm based on ISAPI protocol, opt="0,1,2"--></deployType>
      <ipAddr><!--req, xs: string, IP address--></ipAddr>
    </Content>
  </DeployList>
</DeployInfo>
```

XML_DeviceCap

XML message about device capability

```
<DeviceCap version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <SysCap><!--optional-->
    <isSupportDst><!--optional, xs: boolean, whether it supports daylight saving time--></isSupportDst>
    <NetworkCap/><!--optional, xs: boolean, network capability-->
    <IOCap/><!--optional, IO capability-->
    <SerialCap/><!--optional, serial port capability-->
    <VideoCap/><!--optional, video capability, see details in the message of XML_VideoCap-->
    <AudioCap/><!--optional, audio capability-->
    <isSupportHolidy><!--optional, xs:boolean--></isSupportHolidy>
    <RebootConfigurationCap>
      <Genetec><!--optional, xs:boolean--></Genetec>
      <ONVIF><!--optional, xs:boolean--></ONVIF>
      <RTSP><!--optional, xs:boolean--></RTSP>
      <HTTP><!--optional, xs:boolean--></HTTP>
      <SADP>
        <ISDiscoveryMode><!--optional, xs:boolean--></ISDiscoveryMode>
        <PcapMode><!--optional, xs:boolean--></PcapMode>
      </SADP>
      <IPCAAddStatus><!--optional, xs:boolean--></IPCAAddStatus>
    </RebootConfigurationCap>
    <isSupportExternalDevice><!--optional, xs:boolean--></isSupportExternalDevice>
    <isSupportChangedUpload>
      <!--optional, xs: boolean, whether it supports uploading status changes-->
    </isSupportChangedUpload>
    <isSupportGettingWorkingStatus>
      <!--optional, xs:boolean, whether it supports getting device status-->
    </isSupportGettingWorkingStatus>
    <isSupportGettingChannelInfoByCondition>
      <!--optional, xs:boolean-->
    </isSupportGettingChannelInfoByCondition>
```

```

<isSupportDiagnosedDataParameter>
    <!--optional, xs:boolean-->
</isSupportDiagnosedDataParameter>
<isSupportSimpleDevStatus>
    <!--optional, xs: boolean, whether it supports getting device working
status-->
</isSupportSimpleDevStatus>
<isSupportFlexible>
    <!--optional, xs: boolean, whether it supports getting channel status by
condition-->
</isSupportFlexible>
<isSupportPTZChannels>
    <!--optional, xs:boolean, whether it supports returning PTZ channel
(which is different from the video channel)-->
</isSupportPTZChannels>
<isSupportSubscribeEvent>
    <!--optional, xs:boolean, whether it supports alarm or event
subscription: "true,false"-->
</isSupportSubscribeEvent>
<isSupportDiagnosedData>
    <!--optional, xs:boolean, "true,false", whether it supports diagnosis
data-->
</isSupportDiagnosedData>
<isSupportTimeCap>
    <!--optional, xs:boolean, whether it supports time capability-->
</isSupportTimeCap>
<isSupportThermalStreamData>
    <!--optional, xs:boolean, whether it supports uploading thermal stream
data in real-time. If it is supported, the returned value is "true"; otherwise,
this node will not be returned-->
</isSupportThermalStreamData>
<isSupportPostUpdateFirmware>
    <!--optional, xs:boolean, "true,false", whether it supports upgrading the
firmware-->
</isSupportPostUpdateFirmware>
<isSupportPostConfigData>
    <!--optional, xs:boolean, "true,false", whether it supports importing or
exporting the configuration file-->
</isSupportPostConfigData>
<isSupportUserLock>
    <!--optional, xs:boolean, "true,false", whether it supports locking user-->
</isSupportUserLock>
<isSupportModuleLock><!--optional, xs:boolean, whether it supports locking
the module: "true,false"--></isSupportModuleLock>
<isSupportSoundCfg><!--optional, xs:boolean--></isSupportSoundCfg>
<isSupportMetadata>
    <!--optional, xs:boolean, if it is supported, return "true", otherwise,
this node will not be returned-->
</isSupportMetadata>
<isSupportShutdown><!--optional, xs:boolean, whether it supports shutdown
configuration--></isSupportShutdown>
<supportSmartOverlapChannles opt="1"/><!--optional, xs:boolean, whether it

```

```
supports stream configuration of smart events. If this function is supported,  
this node and the corresponding channel ID will be returned; otherwise, this  
node will not be returned-->  
    <isSupportConsumptionMode><!--optional, xs:boolean, whether it supports  
switching power consumption mode:true (yes), this node is not returned (no).  
Related URI: /ISAPI/System/consumptionMode/capabilities?format=json--></  
isSupportConsumptionMode>  
    <isSupportManualPowerConsumption><!--optional, xs:boolean, whether it  
supports control the power consumption mode manually: true (yes), this node is  
not returned (no)--></isSupportManualPowerConsumption>  
    </SysCap>  
    <voicetalkNums><!--optional, xs:integer, the number of two-way audio  
channels--></voicetalkNums>  
    <isSupportSnapshot><!--optional, xs:boolean, whether it supports capture:  
"true, false"--></isSupportSnapshot>  
    <SecurityCap/><!--optional, security capability-->  
    <EventCap/><!--optional, event capability-->  
    <ITCCap><!--optional--></ITCCap>  
    <ImageCap/><!--optional, image capability-->  
    <RacmCap/><!--optional, storage capability-->  
    <PTZCtrlCap>  
        <isSupportPatrols><!--optional, xs:boolean--></isSupportPatrols>  
        <isSupportCombinedPath><!--optional, xs:boolean, whether the device  
supports the PTZ combined path-->true</isSupportCombinedPath>  
    </PTZCtrlCap>  
    <SmartCap/><!--optional, intelligent capability-->  
    <isSupportEhome><!--optional, xs:boolean--></isSupportEhome>  
    <isSupportStreamingEncrypt><!--optional, xs:boolean--></  
isSupportStreamingEncrypt>  
    <TestCap>  
        <isSupportEmailTest><!--optional, xs:boolean--></isSupportEmailTest>  
    </TestCap>  
    <ThermalCap/><!--optional, temperature measurement capability-->  
    <WLAlarmCap/><!--optional, wireless alarm capability-->  
    <SecurityCPCapabilities/><!--optional, security control panel capability-->  
    <isSupportGIS>  
        <!--optional, xs:boolean, whether it supports GIS capability-->  
    </isSupportGIS>  
    <isSupportCompass>  
        <!--optional, xs:boolean-->  
    </isSupportCompass>  
    <isSupportRoadInfoOverlays>  
        <!--optional, xs:boolean-->  
    </isSupportRoadInfoOverlays>  
    <isSupportFaceCaptureStatistics>  
        <!--optional, xs:boolean-->  
    </isSupportFaceCaptureStatistics>  
    <isSupportExternalDevice>  
        <!--optional, xs:boolean-->  
    </isSupportExternalDevice>  
    <isSupportElectronicsEnlarge>  
        <!--optional, xs:boolean, whether it supports digital zoom-->
```

```
</isSupportElectronicsEnlarge>
<isSupportRemoveStorage>
    <!--optional, xs:boolean-->
</isSupportRemoveStorage>
<isSupportCloud>
    <!--optional, xs:boolean-->
</isSupportCloud>
<isSupportRecordHost>
    <!--optional, xs:boolean-->
</isSupportRecordHost>
<isSupportEagleEye>
    <!--optional, xs:boolean, whether it supports PanoVu series camera-->
</isSupportEagleEye>
<isSupportPanorama>
    <!--optional, xs:boolean, whether it supports panorama-->
</isSupportPanorama>
<isSupportFirmwareVersionInfo>
    <!--optional, xs:boolean, whether it supports displaying firmware version
information-->
</isSupportFirmwareVersionInfo>
<isSupportExternalWirelessServer>
    <!--optional, xs: boolean-->
</isSupportExternalWirelessServer>
<isSupportSetupCalibration>
    <!--optional, xs:boolean, whether it supports setting calibration-->
</isSupportSetupCalibration>
<isSupportGetmutexFuncErrMsg>
    <!--optional, xs:boolean, whether it supports getting mutex information-->
</isSupportGetmutexFuncErrMsg>
<isSupportTokenAuthenticate><!--optional, xs:boolean--></
isSupportTokenAuthenticate>
<isSupportStreamDualVCA><!--optional, xs:boolean--></isSupportStreamDualVCA>
<isSupportlaserSpotManual>
    <!--optional, boolean, whether it supports laser spot configuration-->
</isSupportlaserSpotManual>
<isSupportRTMP><!--optional, xs:boolean--></isSupportRTMP>
<isSupportTraffic><!--optional, xs:boolean--></isSupportTraffic>
<isSupportLaserSpotAdjustment>
    <!--optional, boolean, whether it supports adjusting laser spot size-->
</isSupportLaserSpotAdjustment>
<VideoIntercomCap/><!--optional, video intercom capability-->
<isSupportSafetyCabin>
    <!--optional, xs:boolean-->
</isSupportSafetyCabin>
<isSupportPEA>
    <!--optional, xs:boolean, whether it supports one-touch security control
panel capability-->
</isSupportPEA>
<isSupportCurrentLock>
    <!--optional, xs:boolean, whether it supports locking current
configuration-->
</isSupportCurrentLock>
```

```

<isSupportGuardAgainstTheft>
    <!--optional, xs:boolean, whether it supports device anti-theft
configuration-->
</isSupportGuardAgainstTheft>
<isSupportPicInfoOverlap>
    <!--optional, xs:boolean, whether it supports picture information overlay-->
</isSupportPicInfoOverlap>
<isSupportPlay>
    <!--optional, xs: boolean, whether it supports live view: "true,false"-->
</isSupportPlay>
<isSupportPlayback>
    <!--optional, xs: boolean, whether it supports playback: "true,false"-->
</isSupportPlayback>
<UHFRFIDReader>
    <!--optional, supported capability of UHF RFID card reader-->
    <isSupportBasicInformation>
        <!--optional, xs:boolean, whether it supports basic parameters of UHF
RFID card reader-->
    </isSupportBasicInformation>
    <isSupportHardDiskStorageTest>
        <!--optional, xs:boolean, whether it supports hard disk storage test of
UHF RFID card reader-->
    </isSupportHardDiskStorageTest>
</UHFRFIDReader>
<isSupportIntelligentStructureAnalysis>
    <!--optional, xs:boolean, whether it supports structured VCA-->
</isSupportIntelligentStructureAnalysis>
<isSupportIntelligentAnalysisEngines>
    <!--optional, xs:boolean, whether it supports VCA engine configuration-->
</isSupportIntelligentAnalysisEngines>
<PreviewDisplayNum>
    <!--optional, xs:integer, the number of live view windows, which is the
number of simultaneous live view windows controlled by the device. Limited by
the performance of DeepinMind series network video recorder, currently only
live view of a network camera is supported, and playback is not supported-->
</PreviewDisplayNum>
<isSupportBoard opt="true,false">
    <!--optional, xs:boolean, whether it supports protocol related to sub-
board-->
</isSupportBoard>
<ResourceSwitch>
    <workMode opt="4KPreview,educationRecord">
        <!--req, xs:string, device working mode: "4KPreview"-4K live view mode,
"educationRecord"-education recording mode-->
    </workMode>
</ResourceSwitch>
<isSupportCustomStream><!--optional, xs:boolean--></isSupportCustomStream>
<isSupportTriggerCapCheck>
    <!--optional, xs:boolean, whether it supports verifying capability of alarm
linkage actions-->
</isSupportTriggerCapCheck>
<isSupportActiveMulticast>

```

```

<!--optional, xs: boolean, whether it supports active multicast-->
</isSupportActiveMulticast>
<isSupportChannelEventCap>
    <!--optional, xs:boolean, whether it supports getting event capability by
channel-->
    </isSupportChannelEventCap>
    <isSupportPictureServer>
        <!-- opt, xs:boolean, whether it supports picture storage server-->
    </isSupportPictureServer>
    <isSupportVideoCompositeAlarm>
        <!--optional, xs:boolean, whether it supports video double check alarm-->
    </isSupportVideoCompositeAlarm>
    <isSupportSensorCalibrating>
        <!--optional, xs:boolean, whether it supports double sensor calibration-->
    </isSupportSensorCalibrating>
    <isSupportChannelEventListCap>
        <!--optional, xs:boolean, whether it supports getting event capability of
all channels-->
    </isSupportChannelEventListCap>
    <VCAResourceChannelsCap>
        <!--optional, whether it supports independently switching to another VCA
resource by channel-->
        <ChannelsList>
            <channelsID>
                <!--req, xs:integer, channel No. supported by the device-->
            </channelsID>
        </ChannelsList>
    </VCAResourceChannelsCap>
    <SensorCap/><!--optional, intelligent cabinet capability-->
    <isSupportSecurityCP/>
        <!--optional, xs:boolean, whether it supports the applications of security
control panel: "true, false"-->
    </isSupportSecurityCP>
    <isSupportClientProxyWEB>
        <!--optional, xs:boolean, whether it supports the function that the client
proxy passes through the remote web configuration: "true"-->
    </isSupportClientProxyWEB>
    <WEBLocation>
        <!--optional, string type, web page location: "local"-local device,
"remote"-remote location. If this node is not returned, the web page will be in
the local device by default-->
    </WEBLocation>
    <isSupportTime/>
        <!--optional, xs:boolean, "true, false", whether it supports time
configuration-->
    </isSupportTime>
    <isSupportTimeZone/>
        <!--optional, xs:boolean, "true, false", whether it supports daylight
saving time (DST) configuration-->
    </isSupportTimeZone>
    <isSupportCityManagement>
        <!--optional, boolean, ro, whether it supports intelligent city management-->
    </isSupportCityManagement>

```

```

>true
</isSupportCityManagement>
<isSupportMixedTargetDetection>
    <!--optional, xs:boolean, "true, false", whether it supports multi-target-
type detection-->
</isSupportMixedTargetDetection>
<isSupportFaceContrastMode>
    <!--optional, xs:boolean, whether it supports face picture comparison mode-->
</isSupportFaceContrastMode>
<isSupportPictureCaptureComparision>
    <!--optional, xs:boolean, whether it supports face picture N:1 comparison
between face pictures captured by the camera and imported face pictures-->
</isSupportPictureCaptureComparision>
<isSupportGPSCalibration>
    <!--optional, xs:boolean, whether it supports GPS calibration capability-->
</isSupportGPSCalibration>
<isSupportChannelFullEventListCap>
    <!--optional, xs:boolean, whether it supports getting event list capability
of all channels-->
</isSupportChannelFullEventListCap>
<isSupportAUXInfoCap>
    <!--optional, xs:boolean, whether it supports getting property capability
of all channels-->
</isSupportAUXInfoCap>
<isSupportCalibrationFile>
    <!--optional, xs:boolean, whether it supports importing calibration file-->
</isSupportCalibrationFile>
<isSupportDisplayTrajectory>
    <!--optional, xs:boolean, whether it supports displaying trajectory-->
</isSupportDisplayTrajectory>
<maximumSuperPositionTime opt="5,10,20,30">
    <!--dep, xs:integer, the maximum time of trajectory displaying, unit:
second, it is valid only when displaying trajectory is supported-->
</maximumSuperPositionTime>
<isSupportUnitConfig>
    <!--optional, xs:boolean, whether it supports unit configuration-->
</isSupportUnitConfig>
<isSupportAutoMaintenance>
    <!--optional, xs:boolean, whether it supports automatic maintenance. When
this node exists and values "true", it indicates support-->
</isSupportAutoMaintenance>
<isSupportGetLinkSocketIP>
    <!--optional, xs: boolean, "true, false", whether it supports getting the
SocketIP of current connection-->
</isSupportGetLinkSocketIP>
<isSupportIntelligentSearch>
    <!--optional, xs:boolean, whether it supports intelligent search-->
</isSupportIntelligentSearch>
<IOTCap><!--optional, xs:boolean, IoT device access capability-->
<supportChannelNum>
    <!--req, xs:integer, number of supported channels of IoT device-->

```

```

</supportChannelNum>
<startChannelNo>
    <!--optional, xs:integer, initial channel ID, if this node is not
inputted, it indicates that the initial channel ID is 1-->
</startChannelNo>
<isSupportlinkageChannelsSearch>
    <!--optional, boolean, returns "true" if support, returns "false" if not
support-->
</isSupportlinkageChannelsSearch>
</IOTCap>
<isSupportEncryption>
    <!--optional, xs: boolean, stream encryption capability-->
</isSupportEncryption>
<AIDEEventSupport opt="abandonedObject, pedestrian, congestion, roadBlock,
construction, trafficAccident, fogDetection, wrongDirection, illegalParking,
SSharpDriving, lowSpeed, dragRacing">
    <!--optional, xs:string, supported traffic incident type: "abandonedObject"-objects dropped down, "pedestrian"-pedestrian, "congestion"-congestion, "roadBlock"-roadblock, "construction"-construction, "trafficAccident"-traffic accident, "fogDetection"-fog, "wrongDirection"-wrong-way driving, "illegalParking"-illegal parking, "SSharpDriving"-slalom driving, "lowSpeed"-driving in low speed, "dragRacing"-street racing-->
</AIDEEventSupport>
<TFSEventSupport
opt="illegalParking ,wrongDirection,crossLane,laneChange,vehicleExist,turnRound,
parallelParking,notKeepDistance,notSlowZebraCrossing,overtakeRightSide,lowSpeed,
dragRacing,changeLaneContinuously,SSharpDriving,largeVehicleOccupyLine,jamCrossL
ine">
    <!--optional, xs:string, supported enforcement event type: "illegalParking"-illegal parking, "wrongDirection"-wrong-way driving, "crossLane"-driving on the lane line, "laneChange"-illegal lane change, "vehicleExist"-motor vehicle on non-motor vehicle lane, "turnRound"-illegal U-turn, "parallelParking"-parallel parking, "notKeepDistance"-not keeping vehicle distance, "notSlowZebraCrossing"-not slowing down at zebra corssing, "overtakeRightSide"-overtaking on the right, "lowSpeed"-driving in low speed, "dragRacing"-street racing, "changeLaneContinuously"-continuous lane change, "SSharpDriving"-slalom driving, "largeVehicleOccupyLine"-lane occupation by large-sized vehicle, "jamCrossLine"-queue jumping-->
</TFSEventSupport>
<isVehicleStatisticsSupport>
    <!--optional, xs: boolean, whether it supports setting parameters for
traffic data collection-->
</isVehicleStatisticsSupport>
<isSupportIntersectionAnalysis>
    <!--optional, xs: boolean, whether it supports intersection analysis-->
</isSupportIntersectionAnalysis>
<supportRemoteCtrl
opt="up,down,left,right,enter,menu,num,power,esc,edit,F1,.prev,rec,play,stop,not
Support"/><!--whether it supports remote control-->
<isSptDiagnosis>
    <!--optional, xs:boolean, whether it supports device diagnosis: "true",
"false"-->

```

```

</isSptDiagnosis>
<isSptSerialLogCfg>
    <!--optional, xs:boolean, whether it supports configuring serial port log
 redirection: "true", "false"-->
</isSptSerialLogCfg>
<isSptFileExport>
    <!--optional, xs:boolean, whether it supports exporting files from the
device: "true", "false"-->
</isSptFileExport>
<isSptCertificationStandard>
    <!--optional, xs:boolean, whether it supports configuring authentication
standard for security control panel: "true", "false"-->
</isSptCertificationStandard>
<isSptKeypadLock>
    <!--optional, xs:boolean, whether it supports locking keypad: "true",
"false"-->
</isSptKeypadLock>
<MixedTargetDetection><!--optional, whether the device supports recognizing
specific target among mixed targets-->
    <isSupportFaceRecognition><!--optional, xs:boolean, whether it supports
face recognition--></isSupportFaceRecognition>
    <isSupportHumanRecognition><!--optional, xs:boolean, whether it supports
human body recognition--></isSupportHumanRecognition>
    <isSupportVehicleRecognition><!--optional, xs:boolean, whether it supports
vehicle recognition--></isSupportVehicleRecognition>
</MixedTargetDetection>
<isSupportDiscoveryMode><!--optional, xs:boolean--></isSupportDiscoveryMode>
<streamEncryptionType>
    <!--dep, xs:string, stream encryption type: "RTP/TLS", "SRTP/UDP", "SRTP/
MULTICAST". This node is valid when <isSupportEncryption> is "true", and the
device can support one or more stream encryption types-->
</streamEncryptionType>
<isSupportLms><!--optional, xs:boolean, whether it supports laser--></
isSupportLms>
<isSupportLCDScreen><!--optional, xs:boolean, whether it supports LCD screen-->
</isSupportLCDScreen>
<isSupportBluetooth><!--optional, xs:boolean, whether it supports bluetooth-->
</isSupportBluetooth>
<isSupportAcsUpdate>
    <!--optional, whether it supports upgrading sub access control devices or
peripheral modules: "true"-yes, this node is not returned-no-->
</isSupportAcsUpdate>
<isSupportAccessControlCap>
    <!--optional, whether it supports access control capability: "true"-yes,
this node is not returned-no-->
</isSupportAccessControlCap>
<isSupportIDCardInfoEvent><!--optional, whether it supports ID card swiping
event: "true"-yes. This node will not be returned if this function is not
supported--></isSupportIDCardInfoEvent>
<OpenPlatformCap><!--optional, embedded open platform capability, refer to
the message XML_OpenPlatformCap for details-->
<isSupportInstallationAngleCalibration>

```

```

    <!--optional, xs:boolean, whether it supports installation angle
calibration-->
</isSupportInstallationAngleCalibration>
<isSupportZeroBiasCalibration>
    <!--optional, xs:boolean, whether it supports zero bias calibration-->
</isSupportZeroBiasCalibration>
<isSupportDevStatus><!--optional, xs:boolean, whether device supports getting
device status--></isSupportDevStatus>
<isSupportRadar><!--optional, xs:boolean, whether it supports the security
radar--></isSupportRadar>
<isSupportRadarChannels><!--optional, xs:boolean, whether it supports getting
radar channels--></isSupportRadarChannels>
<radarIPDForm><!--optional, xs:string, radar form: "single"-single radar,
"double_diagonal"-two radars forming an 180° diagonal, "double_vertical"-two
radars forming a 90° vertical angle--></radarIPDForm>
<isSupportRadarFieldDetection><!--optional, xs:boolean, whether it supports
intrusion detection (radar)--></isSupportRadarFieldDetection>
<isSupportRadarLineDetection><!--optional, xs:boolean, whether it supports
line crossing detection (radar)--></isSupportRadarLineDetection>
<mixedTargetDetectionWebNoDisplay><!--optional, xs:boolean, whether to enable
not displaying multi-target-type recognition--><
mixedTargetDetectionWebNoDisplay>
<SHMCap><!--opt-->
    <isSupportHighHDTemperature><!--optional, xs:boolean, whether it supports
HDD high temperature detection--></isSupportHighHDTemperature>
    <isSupportLowHDTemperature><!--optional, xs:boolean, whether it supports
HDD low temperature detection--></isSupportLowHDTemperature>
    <isSupportHDImpact><!--optional, xs:boolean, whether it supports HDD impact
detection--></isSupportHDImpact>
    <isSupportHDBadBlock><!--optional, xs:boolean, whether it supports HDD bad
sector detection--></isSupportHDBadBlock>
    <isSupportSevereHDFailure><!--optional, xs:boolean, whether it supports HDD
severe fault detection--></isSupportSevereHDFailure>
</SHMCap>
<isSupportBVCorrect><!--optional, xs:boolean, whether it supports configuring
camera correction parameters--></isSupportBVCorrect>
<guideEventSupport opt="linkageCapture">
    <!--optional,xs:string, events which support quick setup by instruction,
"linkageCapture"-capture by linkage-->
</guideEventSupport>
<isSupportAutoSwitch><!--optional, xs:boolean, whether it supports auto
switch--> true</isSupportAutoSwitch>
<isSupportDataPrealarm><!--optional,xs:boolean, whether it supports traffic
pre-alarm event--></isSupportDataPrealarm>
<supportGISEvent opt="AID,TPS,ANPR,mixedTargetDetection">
    <!--optional, xs:string, event types that support GIS information access:
AID (corresponding SDK event: COMM_ALARM_AID_V41), TPS (corresponding SDK
event: COMM_ALARM_TPS_REAL_TIME), ANPR (corresponding SDK event:
COMM_ITS_PLATE_RESULT), mixedTargetDetection-mixed targets detection-->
</supportGISEvent>
<isSupportIntelligentMode><!--optional, xs:boolean, whether it supports
intelligent scene switch (related URI:/ISAPI/System/IntelligentSceneSwitch?

```

```
format=json)--></isSupportIntelligentMode>
<isSupportCertificateCaptureEvent><!--optional, xs:boolean, whether it
supports certificate capture and comparison events: true-yes. If this function
is not supported, this node will not be returned--></
isSupportCertificateCaptureEvent>
<isSupportAlgorithmsInfo><!--optional, xs:boolean, whether it supports
getting the algorithm library version information: true-yes. If this function
is not supported, this node will not be returned--></isSupportAlgorithmsInfo>
<isSupportVibrationDetection><!--optional, xs:boolean, whether it supports
vibration detection--></isSupportVibrationDetection>
<isSupportFaceTemperatureMeasurementEvent><!--optional, xs:boolean, whether
it supports uploading face thermography events (eventType:
"FaceTemperatureMeasurementEvent")--></isSupportFaceTemperatureMeasurementEvent>
<isSupportQRCodeEvent><!--optional, xs:boolean, whether it supports uploading
QR code events (eventType: "QRCodeEvent")--></isSupportQRCodeEvent>
<isSupportPersonArmingTrack><!--optional, xs:boolean, whether device supports
person arming (related URI: /ISAPI/Intelligent/channels/<ID>/personArmingTrack/
capabilities?format=json)--></isSupportPersonArmingTrack>
<isSupportManualPersonArmingTrack><!--optional, xs:boolean, whether device
supports manual person arming (related URI: /ISAPI/Intelligent/channels/<ID>/
manualPersonArmingTrack?format=json)--></isSupportManualPersonArmingTrack>
<isSupportGPSCalibrationMode><!--optional, xs:boolean, whether device
supports GPS calibration (related URI: /ISAPI/System/GPSCalibration/channels/
<ID>/mode?format=json)--></isSupportGPSCalibrationMode>
<isSupportGPSVerification><!--optional, xs:boolean, whether device supports
GPS verification (related URI: /ISAPI/System/GPSVerification/channels/<ID>/
points?format=json)--></isSupportGPSVerification>
<isSupportHBDLib><!--optional, xs:boolean, whether device supports human body
picture library (related URI: /ISAPI/Intelligent/HBDLib/capabilities?
format=json)--></isSupportHBDLib>
<isSupportFireEscapeDetection><!--optional, xs:boolean, whether the device
supports fire engine access detection (related URI: /ISAPI/Intelligent/channels/
<ID>/fireEscapeDetection/capabilities?format=json)--></
isSupportFireEscapeDetection>
<isSupportTakingElevatorDetection><!--optional, xs:boolean, whether the device
supports elevator detection (related URI: /ISAPI/Intelligent/channels/
<ID>/takingElevatorDetection/capabilities?format=json)--></
isSupportTakingElevatorDetection>
<isSupportSSDFileSystemUpgrade><!--optional, xs:boolean, whether the device
supports SSD file system upgrade (related URI: /ISAPI/System/SSDFileSystem/
upgrade?format=json)--></isSupportSSDFileSystemUpgrade>
<isSupportSSDFileSystemFormat><!--optional, xs:boolean, whether the device
supports SSD file system formatting (related URI: /ISAPI/System/SSDFileSystem/
format?format=json)--></isSupportSSDFileSystemFormat>
<isSupportSSDFileSystemCapacity><!--optional, xs:boolean, whether the device
supports getting space distribution information of SSD file system (related
URI: /ISAPI/System/SSDFileSystem/capacity?format=json)--></
isSupportSSDFileSystemCapacity>
<isSupportAIOpenPlatform><!--optional, xs:boolean, whether the device
supports AI open platform capabilities; if supports, this node will be returned
and its value is true; if not, this node will not be returned--></
isSupportAIOpenPlatform>
```

```
<isSupportPictureDownloadError><!--optional, xs:boolean, whether the device  
supports reporting picture download failure--></isSupportPictureDownloadError>  
  <characteristicCode min="1" max="128"><!--optional, xs:string, device  
attribute code (related URI: /ISAPI/System/deviceInfo/characteristicCode?  
format=json)--></characteristicCode>  
  <isSupportContainerDetection><!--optional, xs:boolean, whether the device  
supports container detection (if this node is not returned, refer to the value  
returned by /ISAPI/Traffic/ContentMgmt/InputProxy/channels/<ID>/ocrScene/  
capabilities to find whether the device supports container detection)--></  
isSupportContainerDetection>  
  <isSupportLensParamFile><!--optional, xs:boolean, whether the device supports  
exporting and importing the lens parameters file--></isSupportLensParamFile>  
  <isSupportCounting><!--optional, xs:boolean, ro, whether it supports people  
counting--></isSupportCounting>  
  <isSupportFramesPeopleCounting><!--optional, xs:boolean, ro, whether it  
supports regional people counting--></isSupportFramesPeopleCounting>  
  <zoomFocusWebDisplay  
opt="ROI,roadTrafficDetection,SMD,mixedTargetDetection,faceCapture"><!--  
optional, string, zoom and focus page supported by the Web Client--></  
zoomFocusWebDisplay>  
  <isSupportDebugLogModuleType  
opt="playService,communicationService,attendanceService,faceService"><!--  
optional, xs:boolean, whether to export the debugging logs by module type; the  
value of <moduleType> in the URI (/ISAPI/System/debugLog?  
format=json&moduleType=<moduleType>) can be: "playService",  
"communicationService", "attendanceService", "faceService"--></  
isSupportDebugLogModuleType>  
  </isSupportPlateQuaAlarm>  
  <isSupportWiegand><!--optional, xs:boolean, ro, whether it supports the  
Wiegand protocol (related URI: /ISAPI/System/Wiegand/<wiegandID>/capabilities?  
format=json)-->true</isSupportWiegand>  
  <isSupportChannelOccupy><!--optional, xs:boolean, whether it supports  
detection of outdoor fire escape occupied by vehicle--></isSupportChannelOccupy>  
  <isSupportOffDuty><!--optional, xs:boolean, whether it supports detection of  
person absent in fire control room--></isSupportOffDuty>  
  <isSupportNoCertificate><!--optional, xs:boolean, whether it supports  
detection of authenticated staff not enough in fire control room--></  
isSupportNoCertificate>  
  <isSupportSmokeAlarm><!--optional, xs:boolean, whether it supports smoke  
alarm--></isSupportSmokeAlarm>  
  <isSupportBatteryCarDisobey><!--optional, xs:boolean, whether it supports  
electric scooter parking violation detection--></isSupportBatteryCarDisobey>  
  <isSupportNoFireExtinguisherRecog><!--optional, xs:boolean, whether it  
supports fire extinguisher missing detection--></  
isSupportNoFireExtinguisherRecog>  
  <isSupportIndoorPasswayBlock><!--optional, xs:boolean, whether it supports  
indoor channel blockage detection--></isSupportIndoorPasswayBlock>  
  <isSupportFireSmartFireDetect><!--optional, xs:boolean, whether it supports  
fire source detection--></isSupportFireSmartFireDetect>  
  <isSupportDetectorRunningStatus><!--optional, xs:boolean, whether it supports  
detector running status--></isSupportDetectorRunningStatus>  
  <isSupportDetectorOperationStatus><!--optional, xs:boolean, whether it
```

```
supports detector operation status--></isSupportDetectorOperationStatus>
    <isSupportDetectorTemperatureAlarm
opt="highTemperature,riseTemperature,flame"><!--optional, xs:boolean, whether
it supports temperature alarm: "highTemperature" (high temperature alarm),
"riseTemperature" (temperature rising alarm), "flame" (flame alarm)--></
isSupportDetectorTemperatureAlarm>
    <isSupportDetectorShelterAlarm><!--optional, xs:boolean, whether it supports
detector video tampering alarm--></isSupportDetectorShelterAlarm>
    <isSupportDetectorMotionAlarm><!--optional, xs:boolean, whether it supports
detector movement alarm--></isSupportDetectorMotionAlarm>
    <isSupportDetectorTamperAlarm><!--optional, xs:boolean, whether it supports
detector tampering alarm--></isSupportDetectorTamperAlarm>
    <isSupportDetectorEmergencyAlarm><!--optional, xs:boolean, whether it
supports detector emergency alarm--></isSupportDetectorEmergencyAlarm>
    <isSupportSmokingDetectAlarm><!--optional, xs:boolean, whether it supports
smoking alarm--></isSupportSmokingDetectAlarm>
    <isSupportDetectorSmokeAlarm><!--optional, xs:boolean, whether it supports
smoke alarm--></isSupportDetectorSmokeAlarm>
    <isSupportDetectorCombustibleGasAlarm><!--optional, xs:boolean, whether it
supports gas alarm--></isSupportDetectorCombustibleGasAlarm>
    <isSupportFireControlData><!--optional, xs:boolean, whether it supports
uploading real-time fire protection data--></isSupportFireControlData>
    <isSupportFireNoRegulation><!--optional, xs:boolean, whether it supports fire
no regulation alarm--></isSupportFireNoRegulation>
    <isSupportSmokeFireRecognize><!--optional, xs:boolean, whether it supports
uploading the smoke and fire detection event--></isSupportSmokeFireRecognize>
</DeviceCap>
```

XML_DoorParam

DoorParam message in XML format

```
<DoorParam version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <doorName>
        <!--opt, xs:string, door name-->
    </doorName>
    <magneticType>
        <!--opt, xs:string, magnetic contact type: "alwaysClose"-remain locked,
"alwaysOpen"-remain unlocked-->
    </magneticType>
    <openButtonType>
        <!--opt, xs:string, door button type: "alwaysClose"-remain locked,
"alwaysOpen"-remain unlocked-->
    </openButtonType>
    <openDuration>
        <!--opt, xs:integer, door open duration (floor relay action time), which is
between 1 and 255, unit: second-->
    </openDuration>
    <disabledOpenDuration>
        <!--opt, xs:integer, door open duration by disability card (delay duration
of closing the door), which is between 1 and 255, unit: second-->
    </disabledOpenDuration>
</DoorParam>
```

```
</disabledOpenDuration>
<magneticAlarmTimeout>
    <!--opt, xs:integer, alarm time of magnetic contact detection timeout,
which is between 0 and 255, 0 refers to not triggering alarm, unit: second-->
</magneticAlarmTimeout>
<enableDoorLock>
    <!--opt, xs:boolean, whether to enable locking door when the door is
closed-->
</enableDoorLock>
<enableLeaderCard>
    <!--opt, xs:boolean, whether to enable remaining open with first card. This
node is invalid when leaderCardMode is configured-->
</enableLeaderCard>
<leaderCardMode>
    <!--opt, xs:string, first card mode: "disable", "alwaysOpen"-remain open
with first card, "authorize"-first card authentication. If this node is
configured, the node <enableLeaderCard> is invalid-->
</leaderCardMode>
<leaderCardOpenDuration>
    <!--opt, xs:integer, duration of remaining open with first card, which is
between 1 and 1440, unit: second-->
</leaderCardOpenDuration>
<stressPassword>
    <!--wo, opt, xs:string, duress password, the maximum length is 8 bytes, and
the duress password should be encoded by Base64 for transmission-->
</stressPassword>
<superPassword>
    <!--wo, opt, xs:string, super password, the maximum length is 8 bytes, and
the super password should be encoded by Base64 for transmission-->
</superPassword>
<unlockPassword>
    <!--wo, opt, xs:string, dismiss password, the maximum length is 8 bytes,
and the dismiss password should be encoded by Base64 for transmission-->
</unlockPassword>
<useLocalController>
    <!--ro,opt, xs:boolean, whether it is connected to the distributed
controller-->
</useLocalController>
<localControllerID>
    <!--ro, opt, xs:integer, distributed controller No., which is between 1 and
64, 0-unregistered-->
</localControllerID>
<localControllerDoorNumber>
    <!--ro, opt, xs:integer, distributed controller door No., which is between
1 and 4, 0-unregistered-->
</localControllerDoorNumber>
<localControllerStatus>
    <!--ro, opt, xs:integer, online status of the distributed controller: 0-
offline, 1-network online, 2-RS-485 serial port 1 on loop circuit 1, 3-RS-485
serial port 2 on loop circuit 1, 4-RS-485 serial port 1 on loop circuit 2, 5-
RS-485 serial port 2 on loop circuit 2, 6-RS-485 serial port 1 on loop circuit
3, 7-RS-485 serial port 2 on loop circuit 3, 8-RS-485 serial port 1 on loop
```

```
circuit 4, 9-RS-485 serial port 2 on loop circuit 4-->
</localControllerStatus>
<lockInputCheck>
    <!--opt, xs:boolean, whether to enable door lock input detection-->
</lockInputCheck>
<lockInputType>
    <!--opt, xs:string, door lock input type: "alwaysClose"-remain locked
(default), "alwaysOpen"-remain unlocked-->
</lockInputType>
<doorTerminalMode>
    <!--opt, xs:string, working mode of door terminal: "preventCutAndShort"- prevent
from broken-circuit and short-circuit (default), "common"-->
</doorTerminalMode>
<openButton>
    <!--opt, xs:boolean, whether to enable door button: "true"-yes (default),
"false"-no-->
</openButton>
<ladderControlDelayTime>
    <!--opt, xs:integer, elevator control delay time (for visitor), which is
between 1 and 255, unit: minute-->
</ladderControlDelayTime>
<remoteControlPWStatus>
    <!--ro, opt, xs:boolean, whether the password has been configured for
remote door control-->
</remoteControlPWStatus>
</DoorParam>
```

XML_EventCap

EventCap capability message in XML format

```
<EventCap version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <isSupportHDFull><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportHDFull>
    <isSupportHDError><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportHDError>
    <isSupportNicBroken><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportNicBroken>
    <isSupportIpConflict><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportIpConflict>
    <isSupportIILAccess><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportIILAccess>
    <isSupportViException><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportViException>
    <isSupportViMismatch><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportViMismatch>
    <isSupportRecordException><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportRecordException>
    <isSupportTriggerFocus><!--optional, xs:boolean, "true"-support, "false"-not
support--></isSupportTriggerFocus>
    <isSupportMotionDetection><!--optional, xs:boolean, "true"-support, "false"-
```

```

not support--></isSupportMotionDetection>
<isSupportVideoLoss><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportVideoLoss>
<isSupportTamperDetection><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportTamperDetection>
<isSupportStudentsStoodUp><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportStudentsStoodUp>
<isSupportFramesPeopleCounting><!--optional, xs:boolean, "true"--support,
"false"--not support--></isSupportFramesPeopleCounting>
<isSupportRaidException><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportRaidException>
<isSupportSpareException><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportSpareException>
<isSupportPoePowerException><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportPoePowerException>
<isSupportRegionEntrance><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportRegionEntrance>
<isSupportRegionExiting><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportRegionExiting>
<isSupportLoitering><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportLoitering>
<isSupportGroup><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportGroup>
<isSupportRapidMove><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportRapidMove>
<isSupportFireDetection><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportFireDetection>
<isSupportIllegalParking><!--optional, xs:boolean, whether it supports
illegal parking detection: "true"--support, "false"--not support--></
isSupportIllegalParking>
<isSupportUnattendedBaggage><!--optional, xs:boolean --></
isSupportUnattendedBaggage>
<isSupportAttendedBaggage><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportAttendedBaggage>
<isSupportHumanAttribute><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportHumanAttribute>
<isSupportFaceContrast><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportFaceContrast>
<isSupportFaceLib><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportFaceLib>
<isSupportWhiteListFaceContrast><!--opt, xs:boolean, "true"--support, "false"--not
support--></isSupportWhiteListFaceContrast>
<isSupportBlackListFaceContrast><!--opt, xs:boolean, whether it supports
blocklist face comparison: "true"--support, "false"--not support--></
isSupportBlackListFaceContrast>
<isSupportFramesPeopleCounting><!--optional, xs:boolean, whether it supports
regional people counting--></isSupportFramesPeopleCounting>
<isSupportHumanRecognition><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportHumanRecognition>
<isSupportFaceSnap><!--optional, xs:boolean, "true"--support, "false"--not
support--></isSupportFaceSnap>
<isSupportPersonDensityDetection><!--optional, xs:boolean, "true"--support,

```

```
"false"--not support--></isSupportPersonDensityDetection>
  <isSupportMixedTargetDetection><!--optional, xs:boolean, whether it supports
multi-target-type detection alarm: "true"--support, "false"--not support--></
isSupportMixedTargetDetection>
  <isSupportPedestrian><!--optional, xs:boolean, whether it supports pedestrian
detection: "true"--support, "false"--not support--></isSupportPedestrian>
  <isSupportTrafficAccident><!--optional, xs:boolean, whether it supports
traffic accident detection: "true"--support, "false"--not support--></
isSupportTrafficAccident>
  <isSupportConstruction><!--optional, xs:boolean, whether it supports
construction detection: "true"--support, "false"--not support--></
isSupportConstruction>
  <isSupportRoadBlock><!--optional, xs:boolean, whether it supports roadblock
detection: "true"--support, "false"--not support--></isSupportRoadBlock>
  <isSupportAbandonedObject><!--optional, xs:boolean, whether it supports
thrown object detection: "true"--support, "false"--not support--></
isSupportAbandonedObject>
  <isSupportParallelParking><!--optional, xs:boolean, whether it supports
parallel parking detection: "true"--support, "false"--not support--></
isSupportParallelParking>
  <isSupportParkingState><!--optional, xs:boolean, whether it supports parking
space status detection: "true"--support, "false"--not support, currently this
node is not supported--></isSupportParkingState>
  <isSupportCongestion><!--optional, xs:boolean, whether it supports congestion
detection: "true"--support, "false"--not support--></isSupportCongestion>
  <isSupportVehicleStatistics><!--optional, xs:boolean, whether it supports
data collection: "true"--support, "false"--not support--></
isSupportVehicleStatistics>
  <isSupportWrongDirection><!--optional, xs:boolean, whether it supports wrong-
way driving detection: "true"--support, "false"--not support--></
isSupportWrongDirection>
  <isSupportTrunRound><!--optional, xs:boolean, whether it supports U-turning
detection: "true"--support, "false"--not support--></isSupportTrunRound>
  <isSupportCrossLane><!--optional, xs:boolean, whether it supports driving on
the lane line detection: "true"--support, "false"--not support--></
isSupportCrossLane>
  <isSupportLaneChange><!--optional, xs:boolean, whether it supports illegal
lane change detection: "true"--support, "false"--not support--></
isSupportLaneChange>
  <isSupportVehicleExist><!--optional, xs:boolean, whether it supports motor
vehicle on non-motor vehicle lane detection: "true"--support, "false"--not
support--></isSupportVehicleExist>
  <isSupporFogDetection><!--optional, xs:boolean, whether it supports fog
detection: "true"--support, "false"--not support--></isSupporFogDetection>
  <isSupportIntersectionAnalysis><!--optional, xs: boolean, whether it supports
configuring intersection analysis alarm: "true"--support, "false"--not support--
></isSupportIntersectionAnalysis>
  <isSupportVoltageInstable><!--optional, xs:boolean, whether it supports supply
voltage exception alarm: "true"--support, "false"--not support--></
isSupportVoltageInstable>
  <isSupportSafetyHelmetDetection><!--optional, xs:boolean, whether it supports
hard hat detection: "true"--support, "false"--not support--></
```

```
isSupportSafetyHelmetDetection>
    <isSupportCertificateRevocation><!--optional, xs:boolean, whether it supports certificate expiry alarm--></isSupportCertificateRevocation>
    <isSupportNoMaskDetection><!--optional, xs:boolean, whether device supports no wearing mask detection--></isSupportNoMaskDetection>
    <isSupportTMPA><!--optional, xs:boolean, whether device supports temperature measurement pre-alarm--></isSupportTMPA>
    <RuleScheduleCap><!--optional, capability of setting arming schedule by rule-->
        <isSupportCityManagement>
            <!--optional, xs:boolean, whether the device supports setting arming schedule by rule for intelligent city management; if supports, the value is true, otherwise, this node will not be returned-->
        </isSupportCityManagement>
    </RuleScheduleCap>
    <isSupportThermalCalibrationFileException><!--optional, xs:boolean, whether the device supports alarm of thermography calibration file exception--></isSupportThermalCalibrationFileException>
    <isSupportTemperatureIntervalMeasurement><!--optional, xs:boolean, whether the device supports interval temperature measurement--></isSupportTemperatureIntervalMeasurement>
    <isSupportPTEventCfg><!--optional, xs:boolean, whether the device supports event transmission, related URI (/ISAPI/Event/PTEventCfg/capabilities?format=json)-->true</isSupportPTEventCfg>
</EventCap>
```

XML_EventNotificationAlert_HeartbeatInfo

EventNotificationAlert message with heartbeat information (when there is no alarm is triggered) in XML format

```
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <ipv6Address><!--dep, xs:string, device IPv6 address--></ipv6Address>
    <portNo><!--opt, xs:integer, device port number--></portNo>
    <protocol><!--opt, xs:string, protocol type for uploading alarm/event information, "HTTP,HTTPS"--></protocol>
    <macAddress><!--opt, xs:string, MAC address--></macAddress>
    <channelID><!--dep, xs:string, device channel No., starts from 1--></channelID>
    <dateTime><!--req, heartbeat uploaded time, format: 2017-07-19T10:06:41+08:00--></dateTime>
    <activePostCount><!--req, xs:integer, heartbeat frequency, starts from 1--></activePostCount>
    <eventType><!--req, xs:string, for heartbeat, it is "videoloss"--></eventType>
    <eventState>
        <!--req, xs:string, for heartbeat, it is "inactive"-->
    </eventState>
    <eventDescription><!--req, xs: string, description--></eventDescription>
</EventNotificationAlert>
```

Remarks

- For network camera or network speed dome with the version 5.5.0 and lower, the heartbeat frequency is 300 ms per heartbeat.
- For network camera or network speed dome with the version 5.5.0 and higher, the heartbeat frequency is 10 s per heartbeat. If no heartbeat received for continuous 30 s, it indicates that the heartbeat is timed out.

Example

Message Example of Heartbeat

```
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.com/ver20/XMLSchema">
  <ipAddress>10.17.133.46</ipAddress>
  <portNo>80</portNo>
  <protocol>HTTP</protocol>
  <macAddress>44:19:b6:6d:24:85</macAddress>
  <channelID>1</channelID>
  <dateTime>2017-05-04T11:20:02+08:00</dateTime>
  <activePostCount>0</activePostCount>
  <eventType>videoloss</eventType>
  <eventState>inactive</eventState>
  <eventDescription>videoloss alarm</eventDescription>
</EventNotificationAlert>
```

XML_EventNotificationAlert_AlarmEventInfo

EventNotificationAlert message with alarm/event information in XML format.

```
<EventNotificationAlert version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <ipAddress><!--dep, xs:string, device IPv4 address--></ipAddress>
  <ipv6Address><!--dep, xs:string, device IPv6 address--></ipv6Address>
  <portNo><!--opt, xs:integer, device port number--></portNo>
  <protocol><!--opt, xs:string, protocol type for uploading alarm/event
information, "HTTP, HTTPS"--></protocol>
  <macAddress><!--opt, xs:string, MAC address--></macAddress>
  <channelID><!--dep, xs:string, device channel No., starts from 1--></
channelID>
  <dateTime><!--req, alarm/event triggered or occurred time, format:
2017-07-19T10:06:41+08:00--></dateTime>
  <activePostCount><!--req, xs:integer, alarm/event frequency, starts from 1--
></activePostCount>
  <eventType><!--req, xs:string, alarm/event type, "peopleCounting, ANPR,..."-->
  <eventState>
    <!--req, xs:string, durative alarm/event status: "active"-valid, "inactive"-
invalid, e.g., when a moving target is detected,
      the alarm/event information will be uploaded continuously until the status
is set to "inactive"-->
```

```
</eventState>
<eventDescription><!--req, xs:string, alarm/event description--></
eventDescription>
<...><!--opt, for different alarm/event types, the nodes are different, see
the message examples in different applications--><...>
</EventNotificationAlert>
```

XML_EventTrigger

Linkage parameter message in XML format

```
<EventTrigger version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <id><!--required, xs:string, ID--></id>
  <eventType>
    <!--required, xs:string, see details in the "Remarks" below-->
  </eventType>
  <eventDescription><!--optional, xs:string--></eventDescription>
  <inputIOPortID><!--dependent, xs:string, alarm input ID--></inputIOPortID>
  <dynInputIOPortID><!--dependent, xs:string, dynamic alarm input ID--></
dynInputPortID>
  <videoInputChannelID>
    <!--dependent, xs:string, video input channel ID, it is valid when
<eventType> is "VMD, videoloss, tamperdetection, regionEntrance, regionExiting,
loitering, group, rapidMove, parking, unattendedBaggage, attendedBaggage"-->
  </videoInputChannelID>
  <dynVideoInputChannelID><!--dependent, xs:string, dynamic video input channel
ID--></dynVideoInputChannelID>
  <intervalBetweenEvents><!--optional, xs:integer, event time interval, unit:
second--></intervalBetweenEvents>
  <WLSensorID><!--dependent, xs:string, ID--></WLSensorID>
  <EventTriggerNotificationList/><!--optional, alarm/event linkage actions, see
details in the message of XML_EventTriggerNotificationList-->
</EventTrigger>
```

Remarks

The node **<eventType>** can be the following values: IO, VMD, videoloss, raidfailure, recordingfailure, badvideo, POS, analytics, fanfailure, overheat, tamperdetection, diskfull, diskerror, nicbroken, ipconflict, illaccess, videomismatch, resolutionmismatch, radifailure, PIR, WLSensor, spareException, poePowerException, heatmap, counting, linedetection, fielddetection, regionEntrance, regionExiting, loitering, group, rapidMove, parking, unattendedBaggage, attendedBaggage, HUMANATTRIBUTE, blackList, whitelist, peopleDetection, allVehicleList, otherVehicleList, vehicledetection, storageDetection, shipsDetection, humanAttribute, faceContrast, blackListFaceContrast, whiteListFaceContrast, faceSnap, faceLib, personDensityDetection, personQueueDetecton, mixedTargetDetection, HVTVehicleDetection, illegalParking, pedestrian, trafficAccident, construction, roadblock, abandonedObject, parallelParking, parkingState, congestion, intersectionAnalysis, heatMap, thermometry, shipsFlowDetection, dredgerDetection, reverseEntrance, luma, highHDTemperature,

lowHDTemperature, hdImpact, hdBadBlock, SevereHDFailure, safetyHelmetDetection, vibrationDetection, HBDLib, TMPA, faceThermometry, noMaskDetection, detectorTemp, detectorSmoke, detectorTamper, smokeFireRecognize, indoorPasswayBlock, detectorShelter, detectorMotion, fireNoRegulation.

See Also

[XML_EventTriggerNotificationList](#)

XML_EventTriggerCapType

XML message about capability of alarm linkage action types

```
<EventTriggerCapType version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <isSupportCenter><!--optional, xs:boolean--></isSupportCenter>
    <isSupportRecord><!--optional, xs:boolean--></isSupportRecord>
    <isSupportMonitorAlarm><!--optional, xs:boolean--></isSupportMonitorAlarm>
    <isSupportBeep><!--optional, xs: boolean, whether it supports audible
warning--></isSupportBeep>
    <isSupportIO><!--optional, xs:boolean--></isSupportIO>
    <isSupportFTP><!--optional, xs:boolean--></isSupportFTP>
    <isSupportEmail><!--optional, xs:boolean--></isSupportEmail>
    <isSupportLightAudioAlarm><!--optional, xs:boolean--></
isSupportLightAudioAlarm>
    <isSupportFocus><!--optional, xs:boolean--></isSupportFocus>
    <isSupportPTZ><!--optional, xs:boolean--></isSupportPTZ>
    <maxPresetActionNum>
        <!--dependent, xs:integer, it is valid only when <isSupportPTZ> is "true"-->
    </maxPresetActionNum>
    <maxPatrolActionNum>
        <!--dependent, xs:integer, it is valid only when <isSupportPTZ> is "true"-->
    </maxPatrolActionNum>
    <maxPatternActionNum>
        <!--dependent, xs:integer, it is valid only when <isSupportPTZ> is "true"-->
    </maxPatternActionNum>
    <isSupportTrack><!--optional, xs:boolean, whether it supports PTZ linked
tracking--></isSupportTrack>
    <isSupportWhiteLight>
        <!--optional, xs: boolean, whether it supports supplement light alarm
linkage-->
    </isSupportWhiteLight>
    <isSupportCloud><!--optional, xs:boolean, whether it supports upload to the
cloud--></isSupportCloud>
    <targetNotificationInterval max="1000" min="0" default="30"><!--xs:integer,
range: [0, 1000], the default value is 30, unit: seconds, this node is valid
for <MotionDetectionTriggerCap> and <TamperDetectionTriggerCap> and this node
is valid when <isSupportPTZ> is "true"--></targetNotificationInterval>
    <direction opt="both,forward,reverse"><!--xs:string, triggering direction,
this node is valid for the node <BlackListTriggerCap>, <WhiteListTriggerCap>,
and <VehicleDetectionTriggerCap>--></direction>
    <presetDurationTime min="" max=""><!--dependent, xs:integer--></
```

```


presetDurationTime>



  <isSupportSMS><!--optional, xs:boolean, whether to support SMS (Short Message Service)--></isSupportSMS>



  <maxCellphoneNum><!--dependent, xs:integer, the maximum number of cellphones, which is node is valid only when <isSupportSMS> is "true"--></maxCellphoneNum>



  <isSupportOSD><!--optional, xs:boolean--></isSupportOSD>



  <isSupportAudio><!--optional, xs:boolean, whether it supports setting audio alarm independently. If this node is set to "true", audio alarm and buzzer alarm can be linked separately, and the linage method is audio--></isSupportAudio>



  <AudioAction><!--dependent, this node is valid when <isSupportBeep> is "true" or <isSupportAudio> is "true"-->



    <audioTypeList>



      <audioType><!--list-->



        <audioID><!--required, xs:integer, alarm sound type--></audioID>



        <audioDescription><!--required, xs:string, alarm sound description, it should correspond to the alarm sound type--></audioDescription>



      </audioType>



    </audioTypeList>



    <alarmTimes opt="0,1,2,3,4,5,6,7,8,9,255"><!--required, xs:integer, alarm times, it is between 0 and 9, 255-continuous alarm, unit: time--></alarmTimes>



  </AudioAction>



  <isSupportSMS><!--optional, xs:boolean --></isSupportSMS>



  <maxCellphoneNum><!--dependent, if <isSupportSMS> is true, xs:integer--></maxCellphoneNum>



  <isNotSupportCenterModify><!--optional, xs:boolean, whether editing configuration parameters of the monitoring center is not supported: "true"-yes (configuration parameters of the monitoring center cannot be edited), "false" or this node is not returned-no (configuration parameters of the monitoring center can be edited)--></isNotSupportCenterModify>



  <isSupportMessageConfig>



    <!--optional, xs:boolean, whether it supports SMS configuration, if supports, set cellphoneNumber to null-->



  </isSupportMessageConfig>



  <isSupportAnalogOutput><!--optional, xs:boolean, whether it supports IO output of linkage analog channel--></isSupportAnalogOutput>



  <isSupportIOOutputUnify><!--optional, xs:boolean, whether it supports configuration of IO output--></isSupportIOOutputUnify>



  <isSupportFaceContrast><!--optional, xs:boolean, whether it supports face picture comparison linkage--></isSupportFaceContrast>



  <isSupportSiren><!--optional, xs:boolean, whether it supports siren linkage--></isSupportSiren>



  <isSupportOutput><!--optional, xs:boolean, whether it supports relay linkage--></isSupportOutput>


</EventTriggerCapType>

```

XML_EventTriggerList

EventTriggerList message in XML format

```
<EventTriggerList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <EventTrigger/><!--opt, see details in the message of XML_EventTrigger-->
</EventTriggerList>
```

See Also

[XML_EventTrigger](#)

Example

XML_EventTriggerList Message Example of Linkage Configurations of Multiple Alarms

```
<EventTriggerList version="2.0" xmlns="http://www.hikvision.com/ver20/
XMLSchema">
    <EventTrigger>
        <id>VMD-1</id>
        <eventType>VMD</eventType>
        <eventDescription>VMD Event trigger Information</eventDescription>
        <videoInputChannelID>1</videoInputChannelID>
        <dynVideoInputChannelID>1</dynVideoInputChannelID>
        <EventTriggerNotificationList></EventTriggerNotificationList>
    </EventTrigger>
    <EventTrigger>
        <id>tamper-1</id>
        <eventType>tamperedetection</eventType>
        <eventDescription>shelteralarm Event trigger Information</eventDescription>
        <videoInputChannelID>1</videoInputChannelID>
        <dynVideoInputChannelID>1</dynVideoInputChannelID>
        <EventTriggerNotificationList></EventTriggerNotificationList>
    </EventTrigger>
    <EventTrigger>
        <id>diskfull</id>
        <eventType>diskfull</eventType>
        <eventDescription>exception Information</eventDescription>
        <videoInputChannelID>1</videoInputChannelID>
        <dynVideoInputChannelID>1</dynVideoInputChannelID>
        <EventTriggerNotificationList></EventTriggerNotificationList>
    </EventTrigger>
    <EventTrigger>
        <id>diskerror</id>
        <eventType>diskerror</eventType>
        <eventDescription>exception Information</eventDescription>
        <videoInputChannelID>1</videoInputChannelID>
        <dynVideoInputChannelID>1</dynVideoInputChannelID>
        <EventTriggerNotificationList>
            <EventTriggerNotification>
                <id>beep</id>
                <notificationMethod>beep</notificationMethod>
                <notificationRecurrence>beginning</notificationRecurrence>
            </EventTriggerNotification>
        </EventTriggerNotificationList>
    </EventTrigger>
    <EventTrigger>
```

```
<id>nicbroken</id>
<eventType>nicbroken</eventType>
<eventDescription>exception Information</eventDescription>
<videoInputChannelID>1</videoInputChannelID>
<dynVideoInputChannelID>1</dynVideoInputChannelID>
<EventTriggerNotificationList></EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>ipconflict</id>
  <eventType>ipconflict</eventType>
  <eventDescription>exception Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList></EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>illaccess</id>
  <eventType>illaccess</eventType>
  <eventDescription>exception Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList></EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>videomismatch</id>
  <eventType>videomismatch</eventType>
  <eventDescription>exception Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList>
    <EventTriggerNotification>
      <id>beep</id>
      <notificationMethod>beep</notificationMethod>
      <notificationRecurrence>beginning</notificationRecurrence>
    </EventTriggerNotification>
  </EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>badvideo</id>
  <eventType>badvideo</eventType>
  <eventDescription>exception Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList></EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>storageDetection-1</id>
  <eventType>storageDetection</eventType>
  <eventDescription>storageDetection Event trigger Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
```

```
<EventTriggerNotificationList></EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>illegalParking-1</id>
  <eventType>illegalParking</eventType>
  <eventDescription>illegalParking Event trigger Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList>
    <EventTriggerNotification>
      <id>center</id>
      <notificationMethod>center</notificationMethod>
      <notificationRecurrence>beginning</notificationRecurrence>
    </EventTriggerNotification>
  </EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>pedestrian-1</id>
  <eventType>pedestrian</eventType>
  <eventDescription>pedestrian Event trigger Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList>
    <EventTriggerNotification>
      <id>center</id>
      <notificationMethod>center</notificationMethod>
      <notificationRecurrence>beginning</notificationRecurrence>
    </EventTriggerNotification>
  </EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>trafficAccident-1</id>
  <eventType>trafficAccident</eventType>
  <eventDescription>trafficAccident Event trigger Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
  <EventTriggerNotificationList>
    <EventTriggerNotification>
      <id>center</id>
      <notificationMethod>center</notificationMethod>
      <notificationRecurrence>beginning</notificationRecurrence>
    </EventTriggerNotification>
  </EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
  <id>construction-1</id>
  <eventType>construction</eventType>
  <eventDescription>construction Event trigger Information</eventDescription>
  <videoInputChannelID>1</videoInputChannelID>
  <dynVideoInputChannelID>1</dynVideoInputChannelID>
```

```
<EventTriggerNotificationList>
    <EventTriggerNotification>
        <id>center</id>
        <notificationMethod>center</notificationMethod>
        <notificationRecurrence>beginning</notificationRecurrence>
    </EventTriggerNotification>
</EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
    <id>roadBlock-1</id>
    <eventType>roadBlock</eventType>
    <eventDescription>roadBlock Event trigger Information</eventDescription>
    <videoInputChannelID>1</videoInputChannelID>
    <dynVideoInputChannelID>1</dynVideoInputChannelID>
    <EventTriggerNotificationList>
        <EventTriggerNotification>
            <id>center</id>
            <notificationMethod>center</notificationMethod>
            <notificationRecurrence>beginning</notificationRecurrence>
        </EventTriggerNotification>
    </EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
    <id>abandonedObject-1</id>
    <eventType>abandonedObject</eventType>
    <eventDescription>abandonedObject Event trigger Information</eventDescription>
    <videoInputChannelID>1</videoInputChannelID>
    <dynVideoInputChannelID>1</dynVideoInputChannelID>
    <EventTriggerNotificationList>
        <EventTriggerNotification>
            <id>center</id>
            <notificationMethod>center</notificationMethod>
            <notificationRecurrence>beginning</notificationRecurrence>
        </EventTriggerNotification>
    </EventTriggerNotificationList>
</EventTrigger>
<EventTrigger>
    <id>parallelParking-1</id>
    <eventType>parallelParking</eventType>
    <eventDescription>parallelParking Event trigger Information</eventDescription>
    <videoInputChannelID>1</videoInputChannelID>
    <dynVideoInputChannelID>1</dynVideoInputChannelID>
    <EventTriggerNotificationList>
        <EventTriggerNotification>
            <id>center</id>
            <notificationMethod>center</notificationMethod>
            <notificationRecurrence>beginning</notificationRecurrence>
        </EventTriggerNotification>
    </EventTriggerNotificationList>
</EventTrigger>
```

```

<EventTrigger>
    <id>trafficJam-1</id>
    <eventType>trafficJam</eventType>
    <eventDescription>trafficJam Event trigger Information</eventDescription>
    <videoInputChannelID>1</videoInputChannelID>
    <dynVideoInputChannelID>1</dynVideoInputChannelID>
    <EventTriggerNotificationList>
        <EventTriggerNotification>
            <id>center</id>
            <notificationMethod>center</notificationMethod>
            <notificationRecurrence>beginning</notificationRecurrence>
        </EventTriggerNotification>
    </EventTriggerNotificationList>
</EventTrigger>
</EventTriggerList>

```

XML_EventTriggerNotification

Event linkage notification message in XML format

```

<EventTriggerNotification><!--opt-->
    <id><!--required, xs:string, device ID--></id>
    <notificationMethod>
        <!--required, xs:string, linkage actions,
        opt="email,IM,IO,syslog,HTTP,FTP,beep,ptz,record, monitorAlarm, center,
        LightAudioAlarm, focus, trace, cloud, SMS, whiteLight, audio, whiteLight, faceContrast, s
        iren, output"-->
    </notificationMethod>
    <notificationRecurrence>
        <!--optional, xs:string, "beginning,beginningandend,recurring"-->
    </notificationRecurrence>
    <notificationInterval><!--dependent, xs:integer, unit: millisecond--></
    notificationInterval>
        <outputIOPortID><!--dependent, xs:string, video output No., it is required
        only when notificationMethod is "IO"--></outputIOPortID>
        <dynOutputIOPortID><!--dependent, xs:string, dynamic video output No., it is
        required only when notificationMethod is "IO"--></dynOutputIOPortID>
        <videoInputID><!--dependent, xs:string, video input No., it is required only
        when notificationMethod is "record"--></videoInputID>
        <dynVideoInputID><!--dependent, xs:string, dynamic video input No., it is
        required only when notificationMethod is "record"--></dynVideoInputID>
        <ptzAction><!--dependent, it is required only when notificationMethod is
        "ptz"-->
            <ptzChannelID><!--required, xs:string, PTZ channel ID--></ptzChannelID>
            <actionName><!--required, xs:string, PTZ control type: "preset", "pattern",
            "patrol"--></actionName>
            <actionNum><!--dependent, xs:integer--></actionNum>
        </ptzAction>
        <WhiteLightAction><!--dependent, white light linkage parameters, this node is
        valid when notificationMethod is "whiteLight"-->
            <whiteLightDurationTime><!--required, xs:integer, white light flashing

```

```
duration, it is between 1 and 60, unit: second--></whiteLightDurationTime>
</WhiteLightAction>
<cellphoneNumber><!--dependent, xs:string, min="0" max="11", cellphone number--></cellphoneNumber-->
</EventTriggerNotification>
```

XML_EventTriggerNotificationList

EventTriggerNotificationList message in XML format

```
<EventTriggerNotificationList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <EventTriggerNotification/><!--opt, see details in the message of
  XML_EventTriggerNotification-->
</EventTriggerNotificationList>
```

See Also

XML_EventTriggerNotification

XML_EventTriggersCap

XML message about linkage capabilities of different alarm categories

```
<EventTriggersCap version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <DiskfullTriggerCap><!--optional, xs: EventTriggerCapType--></
  DiskfullTriggerCap>
  <DiskerrorTriggerCap><!--optional, xs: EventTriggerCapType--></
  DiskerrorTriggerCap>
  <NicbrokenTriggerCap><!--optional, xs: EventTriggerCapType--></
  NicbrokenTriggerCap>
  <IpconflictTriggerCap><!--optional, xs: EventTriggerCapType--></
  IpconflictTriggerCap>
  <IllaccesTriggerCap><!--optional, xs: EventTriggerCapType--></
  IllaccesTriggerCap>
  <BadvideoTriggerCap><!--optional, xs: EventTriggerCapType--></
  BadvideoTriggerCap>
  <VideomismatchTriggerCap><!--optional, xs: EventTriggerCapType--></
  VideomismatchTriggerCap>
  <IOTTriggerCap><!--optional, xs: EventTriggerCapType--></
  IOTTriggerCap>
  <LineDetectTriggerCap><!--optional, xs: EventTriggerCapType--></
  LineDetectTriggerCap>
  <RegionEntranceTriggerCap><!--optional, xs: EventTriggerCapType--></
  RegionEntranceTriggerCap>
  <RegionExitingTriggerCap><!--optional, xs: EventTriggerCapType--></
  RegionExitingTriggerCap>
  <LoiteringTriggerCap><!--optional, xs: EventTriggerCapType--></
  LoiteringTriggerCap>
  <GroupDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
  GroupDetectionTriggerCap>
```

```
GroupDetectionTriggerCap>
  <RapidMoveTriggerCap><!--optional, xs: EventTriggerCapType--></
RapidMoveTriggerCap>
  <ParkingTriggerCap><!--optional, xs: EventTriggerCapType--></
ParkingTriggerCap>
  <UnattendedBaggageTriggerCap><!--optional, xs: EventTriggerCapType--></
UnattendedBaggageTriggerCap>
  <AttendedBaggageTriggerCap><!--optional, xs: EventTriggerCapType--></
AttendedBaggageTriggerCap>
  <FireDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
FireDetectionTriggerCap>
  <FireDetectionCap><!--optional, xs: EventTriggerCapType--></FireDetectionCap>
  <StorageDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
StorageDetectionTriggerCap>
  <ShipsDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
ShipsDetectionTriggerCap>
  <ThermometryCap><!--optional, xs: EventTriggerCapType--></ThermometryCap>
  <VandalProofTriggerCap><!--optional, xs: EventTriggerCapType--></
VandalProofTriggerCap>
  <BlackListTriggerCap><!--opt, xs: EventTriggerCapType, configuration
capability of blocklist arming linkage--></BlackListTriggerCap>
  <WhiteListTriggerCap><!--opt, xs: EventTriggerCapType, configuration
capability of allowlist arming linkage--></WhiteListTriggerCap>
  <AllVehicleListTriggerCap><!--optional, xs: EventTriggerCapType, configuration
capability of other list arming linkage--></AllVehicleListTriggerCap>
  <OtherVehicleListTriggerCap><!--optional, xs: EventTriggerCapType--></
OtherVehicleListTriggerCap>
  <PeopleDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
PeopleDetectionTriggerCap>
  <PIRALarmCap><!--optional, xs: EventTriggerCapType--></PIRALarmCap>
  <TamperDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
TamperDetectionTriggerCap>
  <DefocusDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
DefocusDetectionTriggerCap>
  <FaceDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
FaceDetectionTriggerCap>
  <SceneChangeDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
SceneChangeDetectionTriggerCap>
  <VandalProofAlarmCap><!--optional, xs: EventTriggerCapType--></
VandalProofAlarmCap>
  <JudgmentTriggerCap><!--optional, xs: EventTriggerCapType--></
JudgmentTriggerCap>
  <FightingTriggerCap><!--optional, xs: EventTriggerCapType--></
FightingTriggerCap>
  <RisingTriggerCap><!--optional, xs: EventTriggerCapType--></RisingTriggerCap>
  <DozingTriggerCap><!--optional, xs: EventTriggerCapType--></DozingTriggerCap>
  <CountingTriggerCap><!--optional, xs: EventTriggerCapType--></
CountingTriggerCap>
  <VideoLossTriggerCap><!--optional, xs: EventTriggerCapType--></
VideoLossTriggerCap>
  <HideTriggerCap><!--optional, xs: EventTriggerCapType--></HideTriggerCap>
  <AlarmInTriggerCap><!--optional, xs: EventTriggerCapType--></
```

```

AlarmInTriggerCap>
    <VehicleDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
VehicleDetectionTriggerCap>
    <AudioExceptionCap><!--optional, xs: EventTriggerCapType--></
AudioExceptionCap>
    <FiledDetectTriggerCap><!--optional, xs: EventTriggerCapType--></
FiledDetectTriggerCap>
    <MotionDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
MotionDetectionTriggerCap>
    <TemperatureCap><!--optional, xs: EventTriggerCapType--></TemperatureCap>
    <IntelligentTriggerCap><!--optional, xs: EventTriggerCapType--></
IntelligentTriggerCap>
    <FaceContrastTriggerCap><!--optional, xs: EventTriggerCapType, face picture
comparison alarm linkage--></FaceContrastTriggerCap>
    <PersonDensityDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
PersonDensityDetectionTriggerCap>
    <PersonQueueDetectionTriggerCap><!--optional, xs: EventTriggerCapType, queue
management alarm linkage--></PersonQueueDetectionTriggerCap>
    <HumanRecognitionTriggerCap><!--optional, xs: EventTriggerCapType--></
HumanRecognitionTriggerCap>
    <FaceSnapTriggerCap><!--optional, xs: EventTriggerCapType--></
FaceSnapTriggerCap>
    <isSupportWhiteLightAction>
        <!--dependent, xs: boolean, see details in EventTriggerCapType, it is valid
when isSupportWhiteLight is "true"-->
    </isSupportWhiteLightAction>
    <isSupportAudioAction>
        <!--dependent, xs: boolean, see details in EventTriggerCapType, it is valid
when isSupportBeep is "true"-->
    </isSupportAudioAction>
    <HFPDTriggerCap><!--optional, xs: EventTriggerCapType--></HFPDTriggerCap>
    <MixedTargetDetectionCap><!--optional, xs: EventTriggerCapType--></
MixedTargetDetectionCap>
    <HVTVehicleDetectionTriggerCap><!--optional, xs: EventTriggerCapType--></
HVTVehicleDetectionTriggerCap>
    <VCATriggerCap><!--optional, xs: EventTriggerCapType--></VCATriggerCap>
    <PIRCap><!--optional, xs: EventTriggerCapType--></PIRCap>
    <IllegalParkingTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports illegal parking detection--></IllegalParkingTriggerCap>
    <PedestrianTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports pedestrian detection--></PedestrianTriggerCap>
    <TrafficAccidentTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports traffic accident detection--></TrafficAccidentTriggerCap>
    <ConstructionTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports construction detection--></ConstructionTriggerCap>
    <RoadBlockTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports roadblock detection--></RoadBlockTriggerCap>
    <AbandonedObjectTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports objects dropped down detection--></AbandonedObjectTriggerCap>
    <ParallelParkingTriggerCap><!--optional, xs: EventTriggerCapType, whether it
supports parallel parking detection--></ParallelParkingTriggerCap>
    <ParkingStateTriggerCap><!--optional, xs: EventTriggerCapType, whether it

```

```
supports parking space status detection, currently this node is not supported--></ParkingStateTriggerCap>
    <CongestionTriggerCap><!--optional, xs: EventTriggerCapType, whether it supports congestion detection--></CongestionTriggerCap>
    <IntersectionAnalysisCap><!--optional, xs: EventTriggerCapType, whether it supports intersection analysis--></IntersectionAnalysisCap>
    <ShipsFlowDetectionTriggerCap><!--optional, xs: EventTriggerCapType, ship flow detection--></ShipsFlowDetectionTriggerCap>
    <dredgerDetectionTriggerCap><!--optional, xs: EventTriggerCapType, dredger detection--></dredgerDetectionTriggerCap>
    <voltageInstableTriggerCap><!--optional, xs: EventTriggerCapType, supply voltage exception--></voltageInstableTriggerCap>
    <HighHDTemperatureTriggerCap><!--optional, xs: EventTriggerCapType, HDD high temperature detection--></HighHDTemperatureTriggerCap>
    <LowHDTemperatureTriggerCap><!--optional, xs: EventTriggerCapType, HDD low temperature detection--></LowHDTemperatureTriggerCap>
    <HDImpactTriggerCap><!--optional, xs: EventTriggerCapType, HDD impact detection--></HDImpactTriggerCap>
    <HDBadBlockTriggerCap><!--optional, xs: EventTriggerCapType, HDD bad sector detection--></HDBadBlockTriggerCap>
    <SevereHDFailureTriggerCap><!--optional, xs: EventTriggerCapType, HDD severe fault detection--></SevereHDFailureTriggerCap>
    <HUMANATTRIBUTECap><!--optional, xs: EventTriggerCapType--></HUMANATTRIBUTECap>
    <HumanAttributeTriggerCap><!--optional, xs: EventTriggerCapType, human body attribute--></HumanAttributeTriggerCap>
    <BlackListFaceContrastTriggerCap><!--opt, xs: EventTriggerCapType, alarm linkage capability of blocklist face comparison--></BlackListFaceContrastTriggerCap>
    <FaceLibTriggerCap><!--optional, xs: EventTriggerCapType--></FaceLibTriggerCap>
    <SafetyHelmetDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of hard hat detection--></SafetyHelmetDetectionTriggerCap>
    <VibrationDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of vibration detection--></VibrationDetectionTriggerCap>
    <RadarLineDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of radar line crossing detection--></RadarLineDetectionTriggerCap>
    <RadarFieldDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of radar intrusion detection--></RadarFieldDetectionTriggerCap>
    <HBDLibTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of human body picture library--></HBDLibTriggerCap>
    <FaceThermometryCap><!--optional, xs: EventTriggerCapType--></FaceThermometryCap>
    <NoMaskDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of no wearing mask detection--></NoMaskDetectionTriggerCap>
    <TMPATriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of temperature measurement pre-alarm--></TMPATriggerCap>
    <FireEscapeDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of fire engine access detection--></FireEscapeDetectionTriggerCap>
    <TakingElevatorDetectionTriggerCap><!--optional, xs: EventTriggerCapType, alarm linkage capability of elevator detection--></
```

```
TakingElevatorDetectionTriggerCap>
  <RuleTriggerCap><!--optional, linkage capability of rule triggered alarm -->
    <isSupportCityManagement>
      <!--optional, xs:boolean, whether the city management supports setting
linkage actions by area; if supports, the value is true, otherwise, this node
will not be returned-->
    </isSupportCityManagement>
  </RuleTriggerCap>
  <ThermalCalibrationFileExceptionCap><!--optional, xs:EventTriggerCapType,
alarm linkage capability of thermography calibration file exception--></
ThermalCalibrationFileExceptionCap>
</EventTriggersCap>
```

See Also

[XML_EventTriggerCapType](#)

XML_FaceCompareCond

XML message about condition parameters of face picture comparison

```
<FaceCompareCond version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <faceWidthLowerLimit><!--optional, xs:integer, face width threshold with
highest priority, value range: [0, 100], when the detected face width is larger
than this threshold, the following conditions will be ignored and the face
comparison will be executed--></faceWidthLowerLimit>
  <pitch><!--optional, xs:integer, face raising or bowing angle, value range:
[0, 90], unit: degree, the smaller the better--></pitch>
  <yaw><!--optional, xs:integer, face siding left or right angle, value range:
[0, 90], unit: degree, the smaller the better--></yaw>
  <width><!--optional, xs:integer, face width, value range: [0, 100]--></width>
  <height><!--optional, xs:integer, face height, value range: [0, 100]--></
height>
  <leftBorder><!--optional, xs:integer, left border of face, value range: [0,
100]--></leftBorder>
  <rightBorder><!--optional, xs:integer, right border of face, value range: [0,
100]--></rightBorder>
  <upBorder><!--optional, xs:integer, top border of face, value range: [0,
100]--></upBorder>
  <bottomBorder><!--optional, xs:integer, bottom border of face, value range:
[0, 100]--></bottomBorder>
  <interorbitalDistance><!--optional, xs:integer, pupil distance, value range:
[0, 100]--></interorbitalDistance>
  <faceScore><!--optional, xs:integer, face score, value range: [0, 100], the
valid face score must be larger than this score--></faceScore>
  <maxDistance><!--optional, xs:string, maximum recognition distance:
"0.5,1,1.5,2,auto", unit: m. This node has higher priority over
<interorbitalDistance>--></maxDistance>
  <similarity><!--optional, xs:float, face comparison similarity, value range:
[0.0,1.0]--></similarity>
</FaceCompareCond>
```

XML_HttpHostNotification

XML message about parameters of a HTTP listening server

```
<HttpHostNotification version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <id><!--required, xs:string, ID--></id>
    <url><!--required, xs:string, the absolute path, e.g., http://</url>
    <ipAddress>:<portNo>/<uri>--></url>
        <protocolType><!--required, xs:string, "HTTP,HTTPS,EHome". When the value of this node is EHome, this message can be used to configure the information (such as IP address and port No.) for the AMS (Alarm Management Server) of ISUP 5.0 to listen on. For communication via ISUP 5.0 (MQTT), the listening parameters can be configured and obtained; For other communication methods (such as communication via HTTP, HTTPS, EZVIZ Open Platform, etc.), the listening parameters can only be obtained and cannot be configured--></protocolType>
        <parameterFormatType><!--required, xs:string, alarm/event information format, "XML,JSON"--></parameterFormatType>
        <addressingFormatType><!--required, xs:string, "ipaddress,hostname"--></addressingFormatType>
            <hostName><!--dependent, xs:string--></hostName>
            <ipAddress><!--dependent, xs:string--></ipAddress>
            <ipv6Address><!--dependent, xs:string--></ipv6Address>
            <portNo><!--optional, xs:integer--></portNo>
            <userName><!--dependent, xs:string--></userName>
            <password><!--dependent, xs:string--></password>
            <httpAuthenticationMethod><!--required, xs:string, "MD5digest,none"--></httpAuthenticationMethod>
            <ANPR><!--optional-->
                <detectionUpLoadPicturesType>
                    <!--optional, xs:string, types of alarm picture to be uploaded: "all", "licensePlatePicture", "detectionPicture". When configuring the types of captured pictures to be uploaded to the HTTP listening server, the node detectionUpLoadPicturesType supported to be configured with the following values: "licensePlatePicture", "detectionPicture", and "all"-->
                    <!--The picture type configured for this node must be included in that configured for the node capturePicType in XML_PicParam. For example, if the values of the node capturePicType are "licensePlatePicture", "vehiclePicture", and "detectionPicture", the value of this node can be any; if the value of the node capturePicType is "licensePlatePicture", the value of this node can only be "licensePlatePicture"; if the values of the node capturePicType are "licensePlatePicture" and "vehiclePicture", the value of this node can be "licensePlatePicture" or "all"; if the values of the node capturePicType are "detectionPicture" and "vehiclePicture", the value of this node can be "detectionPicture" or "all"-->
                </detectionUpLoadPicturesType>
            </ANPR>
        <eventType optional="AID,TFS,TPS"><!--required, xs:string--></eventType>
        <uploadImagesDataType>
            <!--optional, xs:string, "URL", "binary" (default), for cloud storage, only "URL" is supported-->
```

```
</uploadImagesDataType>
<httpBroken>
    <!--optional, xs:boolean, automatic network replenishment (ANR). The ANR
function will be applied to all events once enabled-->true
</httpBroken>
<eventMode><!--optional, xs:string, "all,list"--></eventMode>
<EventList><!--dependent, it is valid only when eventMode is "list"-->
    <Event><!--required-->
        <type><!--required, xs:string--></type>
    </Event>
</EventList>
<channels><!--optional, xs:string, "1,2,3,4..."--></channels>
<SubscribeEvent/><!--optional, event subscription parameters, see details in
the message of XML_SubscribeEvent-->
</HttpHostNotification>
```

XML_HttpHostNotificationCap

XML message about capability of HTTP listening server

```
<HttpHostNotificationCap version="2.0" xmlns="http://www.isapi.org/ver20/
XMLSchema">
    <hostNumber>2</hostNumber>
    <urlLen max="" />
    <protocolType opt="HTTP,HTTPS,EHome" />
    <parameterFormatType opt="XML,querystring,JSON" />
    <addressingFormatType opt="ipaddress,hostname" />
    <ipAddress opt="ipv4,ipv6" />
    <portNo min="" max="" />
    <userNameLen min="" max="" />
    <passwordLen min="" max="" />
    <httpAuthenticationMethod opt="MD5digest,none" />
    <Extensions>
        <intervalBetweenEvents min="" max="" />
    </Extensions>
    <uploadImagesDataType opt="URL,binary" />
    <ANPR><!--optional-->
        <detectionUpLoadPicturesType
opt="all,licensePlatePicture,detectionPicture..."/><!--optional, xs:string, types
of alarm pictures to be uploaded-->
        <alarmHttpPushProtocol opt="baseline,custom" />
    </ANPR>
    <httpBroken opt="true,false" def="true"><!--optional, xs:boolean, whether to
enable global ANR: true, false--></httpBroken>
    <SubscribeEventCap>
        <heartbeat min="" max="" /><!--optional, heartbeat time interval, unit:
second-->
            <channelMode opt="all,list"/><!--required, all-subscribe events of all
channels, list-subscribe event by channel-->
            <eventMode opt="all,list"/><!--required, event subscription mode: all-
subscribe all events of all channels, list-subscribe events by type, channel,
```

```
and target-->
    <!--if the values of the two nodes channelMode and eventMode are both
    "all", it indicates that the device does not support subscribe events by type
    and channel-->
    <EventList><!--dependent, alarm uploading mode, this node is valid only
when eventMode is "list"-->
        <Event><!--required-->
            <type><!--required, xs:string, event types--></type>
                <pictureURLType opt="binary,localURL,cloudStorageURL" def="" />
                <!--optional, xs:string, transmission format of alarm picture: "binary"->
                    <!--picture binary data, "localURL"-picture URL from local device,
                    "cloudStorageURL"-picture URL from cloud storage-->
                </Event>
            </EventList>
            <pictureURLType opt="binary,localURL,cloudStorageURL" def="" />
            <!--optional, xs:string, transmission format of all alarm pictures:
            "binary"-picture binary data (default for camera), "localURL"-picture URL from
            local device (default for NVR/DVR), "cloudStorageURL"-picture URL from cloud
            storage; this node is in highest priority-->
            <ChangedUploadSub>
                <interval/><!--optional, xs:integer, the life cycle of arming GUID, unit:
                second, the default life cycle is 5 minutes; if the reconnection is not started
                during the life cycle, a new GUID will be generated-->
                <StatusSub>
                    <all/><!--optional, xs:boolean, whether to subscribe all-->
                    <channel/><!--optional, xs:boolean, subscribe channel status, this node is
                    not required when the node all is "true"-->
                    <hd/><!--optional, xs:boolean, subscribe the HDD status, this node is not
                    required when the node all is "true"-->
                    <capability/><!--optional, xs:boolean, subscribe the capability changed
                    status, this node is not required when the node all is "true"-->
                </StatusSub>
            </ChangedUploadSub>
        </SubscribeEventCap>
    </HttpHostNotificationCap>
```

XML_HttpHostNotificationList

HttpHostNotificationList message in XML format

```
<HttpHostNotificationList version="2.0" xmlns="http://www.isapi.org/ver20/
XMLSchema">
    <HttpHostNotification>
        <id><!--req, xs:string, ID--></id>
        <url><!--req, xs:string--></url>
        <protocolType><!--req, xs:string, "HTTP,HTTPS,EHome". When the value of
        this node is EHome, this message can be used to configure the information (such
        as IP address and port No.) for the AMS (Alarm Management Server) of ISUP 5.0
        to listen on. For communication via ISUP 5.0 (MQTT), the listening parameters
        can be configured and obtained; For other communication methods (such as
        communication via HTTP, HTTPS, EZVIZ Open Platform, etc.), the listening
```

```
parameters can only be obtained and cannot be configured--></protocolType>
    <parameterFormatType><!--req, xs:string, alarm/event information format,
"XML, JSON"--></parameterFormatType>
    <addressingFormatType><!--req, xs:string, "ipaddress,hostname"--></
addressingFormatType>
        <hostName><!--dep, xs:string--></hostName>
        <ipAddress><!--dep, xs:string--></ipAddress>
        <ipv6Address><!--dep, xs:string--></ipv6Address>
        <portNo><!--opt, xs:integer--></portNo>
        <userName><!--dep, xs:string--></userName>
        <password><!--dep, xs:string--></password>
        <httpAuthenticationMethod><!--req, xs:string, "MD5digest,none"--></
httpAuthenticationMethod>
        <uploadImagesDataType>
            <!--opt, xs:string, "URL", "binary" (default), for cloud storage, only
"URL" is supported-->
        </uploadImagesDataType>
        <eventMode><!--opt, xs:string, "all,list"--></eventMode>
        <EventList><!--dep, it is valid only when eventMode is "list"-->
            <Event><!--req-->
                <type><!--req, xs:string--></type>
            </Event>
        </EventList>
        <channels><!--opt, xs:string, "1,2,3,4..."--></channels>
    </HttpHostNotification>
</HttpHostNotificationList>
```

Example

HttpHostNotificationList Message Example

```
<HttpHostNotificationList version="2.0" xmlns="http://www.isapi.org/ver20/
XMLSchema">
    <HttpHostNotification>
        <id>1</id>
        <url></url>
        <protocolType>HTTP</protocolType>
        <parameterFormatType>XML</parameterFormatType>
        <addressingFormatType>ipaddress</addressingFormatType>
        <ipAddress>0.0.0.0</ipAddress>
        <portNo>80</portNo>
        <userName></userName>
        <httpAuthenticationMethod>none</httpAuthenticationMethod>
    </HttpHostNotification>
</HttpHostNotificationList>
```

XML_HttpHostTestResult

HttpHostTestResult message in XML format.

```
<HttpHostTestResult version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <errorDescription>
```

```
<!--req, xs:string-->
</errorDescription>
</HttpHostTestResult>
```

XML_IDBlackListCfg

XML message about the ID card blocklist parameters

```
<IDBlackListCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <blackListValid>
    <!--required, xs:integer, ID card blocklist status: 0-invalid, 1-valid.
This node is used to delete the ID card blocklist by ID card number. If it is
0, it indicates deleting the blocklist-->
  </blackListValid>
  <IDCardInfo><!--dependent-->
    <name><!--optional, xs:string, name--></name>
    <birth><!--optional, xs:string, date of birth--></birth>
    <addr><!--optional, xs:string, address--></addr>
    <IDNum><!--required, xs:string, ID card number--></IDNum>
    <issuingAuthority><!--optional, xs:string, issuing authority--></
issuingAuthority>
    <startDate><!--optional, xs:string, start date of expiry date--></startDate>
    <endDate><!--optional, xs:string, end date of expiry date--></endDate>
    <termOfValidity>
      <!--optional, xs:boolean, whether it is permanently valid: false-no, true-
yes (the <endDate> is invalid)-->
    </termOfValidity>
    <sex><!--optional, xs:string, gender: "male" or "female"--></sex>
  </IDCardInfo>
</IDBlackListCfg>
```

XML_IdentityTerminal

IdentityTerminal message in XML format

```
<IdentityTerminal version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <terminalMode>
    <!--req, xs: string, terminal mode: "authMode"-authentication mode,
"registerMode"-registration mode-->
  </terminalMode>
  <idCardReader>
    <!--req, xs: string, ID card reader model: iDR210, DS-K1F110-I, DS-K1F1110-
B, DS-K1F1110-AB, none, DS-K1F1001-I(USB), DS-K1F1002-I(USB), none-->
  </idCardReader>
  <camera><!--req, xs: string, camera model: C270, DS-2CS5432B-S--></camera>
  <fingerPrintModule><!--req, xs: string, fingerprint module type: ALIWARD,
HikModule--></fingerPrintModule>
  <videoStorageTime><!--req, xs: integer, time for saving video (unit: second),
which is between 0 and 10--></videoStorageTime>
```

```
<faceContrastThreshold><!--req, xs: integer, face picture comparison threshold, which is between 0 and 100--></faceContrastThreshold>
<twoDimensionCode><!--req, xs: string, whether to enable QR code recognition: enable, disable--></twoDimensionCode>
<blackListCheck><!--req, xs: string, whether to enable blocklist verification: enable, disable--></blackListCheck>
<idCardCheckCenter>
    <!--req, xs: string, ID card comparison mode: local-compare with ID card of local storage, server-compare with ID card of remote server storage-->
</idCardCheckCenter>
<faceAlgorithm>
    <!--req, xs: string, face picture algorithm: HIK-Z-Hikviison algorithm, HIK-H-third-party algorithm-->
</faceAlgorithm>
<comNo><!--req, xs: integer, COM No., which is between 1 and 9--></comNo>
<memoryLearning><!--req, xs: string, whether to enable learning and memory function: enable, disable--></memoryLearning>
<saveCertifiedImage><!--req, xs: string, whether to enable saving authenticated picture: enable, disable--></saveCertifiedImage>
<MCUVersion><!--opt, xs: string, MCU version information, read-only--></MCUVersion>
<usbOutput><!--opt, xs: string, whether to enable USB output of ID card reader: enable, disable--></usbOutput>
<serialOutput><!--opt, xs: string, whether to enable serial port output of ID card reader: enable, disable--></serialOutput>
<readInfoOfCard><!--opt, xs: string, set content to be read from CPU card: serialNo-read serial No., file-read file--></readInfoOfCard>
<workMode><!--opt, xs: string, authentication mode: passMode, accessControlMode--></workMode>
<ecoMode>
    <eco><!--opt, xs: string, whether to enable ECO mode: enable, disable--></eco>
        <faceMatchThreshold1><!--req, xs: integer, 1V1 face picture comparison threshold of ECO mode, which is between 0 and 100--></faceMatchThreshold1>
        <faceMatchThresholdN><!--req, xs: integer, 1:N face picture comparison threshold of ECO mode, which is between 0 and 100--></faceMatchThresholdN>
        <changeThreshold><!--opt, xs: string, switching threshold of ECO mode, which is between 0 and 8--></changeThreshold>
        <maskFaceMatchThresholdN><!--req, xs:integer, 1:N face picture (face with mask and normal background picture) comparison threshold of ECO mode, value range: [0,100]--></maskFaceMatchThresholdN>
        <maskFaceMatchThreshold1><!--req, xs:integer, 1:1 face picture (face with mask and normal background picture) comparison threshold of ECO mode, value range: [0,100]--></maskFaceMatchThreshold1>
    </ecoMode>
    <readCardRule><!--opt, xs: string, card No. setting rule: "wiegand26", "wiegand34"--></readCardRule>
    <enableScreenOff><!--optional, xs:boolean, whether the device enters the sleep mode when there is no operation after the configured sleep time--></enableScreenOff>
    <screenOffTimeout><!--dependent, xs:integer, sleep time, unit: second--></screenOffTimeout>
```

```
<enableScreensaver><!--optional, xs:boolean, whether to enable the screen  
saver function--></enableScreensaver>  
<showMode><!--optional, xs:string, display mode: "concise" (simple mode, only  
the authentication result will be displayed), "normal" (normal mode). The  
default mode is normal mode. If this node does not exist, the default mode is  
normal mode--></showMode>  
<menuTimeout><!--dependent, xs:integer, timeout period to exit, unit: second-->  
</menuTimeout>  
</IdentityTerminal>
```

XML_M1CardEncryptCfg

M1CardEncryptCfg message in XML format

```
<M1CardEncryptCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <enable><!--req, xs: boolean, whether to enable--></enable>  
    <sectionID><!--req, xs:integer, sector ID, only one sector can be configured  
at a time--></sectionID>  
</M1CardEncryptCfg>
```

XML_Material

XML message about material information

```
<Material version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <id><!--required, xs:integer, material ID--></id>  
    <seq><!--optional, xs:integer, material serial No., which changes every  
time the material is modified; this field is only valid on the link between the  
server and the terminal--></seq>  
        <materialName><!--required, xs:string, material name--></materialName>  
        <materialRemarks><!--required, xs:string, material description--></  
materialRemarks>  
            <materialType><!--required, xs:string, material type: "static"-local  
material, "dynamic"-dynamic material--></materialType>  
            <approveState><!--optional, xs:string, approval status: "approved"-pass,  
"notPass"-not pass, "notApprove"-not approved--></approveState>  
            <approveRemarks><!--optional, xs:string, approval remarks--></  
approveRemarks>  
                <shareProperty><!--optional, xs:string, shared property: public, private-->  
</shareProperty>  
                <uploadUser><!--read-only, required, xs:string, uploader, read-only--></  
uploadUser>  
                <uploadTime><!--read-only, required, xs:time, upload time (ISO 8601  
format)--></uploadTime>  
                <materialEncrypt><!--optional, xs:integer, material secret key, which can  
be used for verifying the correctness of materials received by the terminal;  
this field is only valid on the link between the server and the terminal, e.g.,  
JjEmNTA3NDg5NCY0JjI3OTM5MjAmYWEmMzYyOTM5OCZhMCY0MjAzMDQwJmI1JjQzMzc3ODgmNDg--></materialEncrypt>
```

```
<orgNo><!--optional, xs:integer, organization No.--></orgNo>
<orgName><!--optional, xs:string, read-only--></orgName>
<replaceTerminal><!--optional, xs:boolean, whether the material is updated
to the terminal, this field is valid only when replacing materials--></
replaceTerminal>
    <StaticMaterial><!--dep-->
        <staticMaterialType>
            <!--dependent, xs:string, local material type-->
        </staticMaterialType>
            <picFormat><!--dependent, xs:string, image format: GIF, BMP, JPG, PNG-->
        </picFormat>
            <flashFormat><!--dependent, xs:string, flash format: SWF--></
        flashFormat>
            <audioFormat><!--dependent, xs:string, audio format: MP3, WAV, WMA--></
        audioFormat>
            <videoFormat><!--dependent, xs:string, video format: RM, RMVB, ASF,
AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4--></videoFormat>
            <documentFormat><!--dependent, xs:string, document format: TXT--></
        documentFormat>
            <pptFormat><!--dependent, xs:string, slide format: PPT, PPTX--></
        pptFormat>
            <docFormat><!--dependent, xs:string, word document format: DOC, DOCX-->
        </docFormat>
            <excelFormat><!--dependent, xs:string, table format: XLS, XLSX--></
        excelFormat>
            <pdfFormat><!--dependent, xs:string, PDF--></pdfFormat>
            <webFormat><!--dependent, xs:string, web format: HTML, HTM--></
        webFormat>
            <appFormat><!--dependent, xs:string, application format: APK--></
        appFormat>
                <fileSize><!--required, xs:integer, file size, unit: byte--></fileSize>
                <duration><!--optional, xs:integer, playing duration, this filed is
valid only when the material is a video or slide file, unit: second--></
        duration>
                    <uuid><!--dependent, xs:string, UUID provided by the server to identify
the material, this field is valid only when StorageInfo exists; only 8520
platform sava materials on the storage server--></uuid>
                    <staticMaterialUrl><!--dependent, xs:string, material URL, this field
is valid only when StorageInfo exists; only 8520 platform sava materials on the
storage server--></staticMaterialUrl>
                    <materialURL><!--optional, xs:string, material storage URL. If this
node is returned, the device will synchronize these data automatically until
synchronization succeeded or failed due to exception (during synchronization,
the API cannot be blocked), and there is no need to call the API of uploading
materials--></materialURL>
                    <!--Note: 1. For a local material, you need to upload a file. If
uploading this file failed, the material ID is invalid (only for Web). 2. If
this node is returned, the material ID will be valid after synchronizing data
succeeded and the asynchronous status event (eventType: asyncNotification) is
uploaded-->
                </StaticMaterial>
                <DynamicMaterial><!--dependent-->
```

```

<dynamicMaterialType
opt="web,socket,rss,realStream,generalData,picUrl,dataSource"><!--dependent,
xs:string, dynamic material type--></dynamicMaterialType>
    <webUrl><!--dependent, xs:string, web URL--></webUrl>
    <rssUrl><!--dependent, xs:string, RSS URL--></rssUrl>
    <picUrl><!--dependent, xs:string, picture URL--></picUrl>
    <RealStream><!--dependent, real-time stream-->
        <destionType opt="streamMedia,normalIPC"><!--required, xs:string,
streaming terminal type: Stream Media Server, normal network camera--></
destionType>
        <streamMediaUrl><!--dependent, xs:string, streaming server URL--></
streamMediaUrl>
            <NormalIPC><!--dep-->
                <IpAddress><!--dep-->
                    <ipVersion opt="v4,v6,dual"><!--required, xs:string--></
ipVersion>
                        <ipAddress><!--dependent, xs:string--></ipAddress>
                        <ipv6Address><!--dependent, xs:string--></ipv6Address>
                    </IpAddress>
                    <portNo><!--required, xs:integer--></portNo>
                    <channelNo><!--required, xs:integer, channel No.--></channelNo>
                    <userName><!--required, xs:string, user name for logging to
deivces, which is write-only and must be encrypted when transmission--></
userName>
                        <passWord><!--required, xs:string, password for logging to
devices, which is write-only and must be encrypted when transmission--></
passWord>
                        <transmitProtocol opt="tcp,udp,mcast"><!--optional, xs:string,
transmission protocol--></transmitProtocol>
                        <streamType opt="main,sub,third"><!--optional, xs:string,
stream type--></streamType>
                    </NormalIPC>
                    <privateStreamMediaUrl><!--dependent, xs:string, private stream
data of hikvision--></privateStreamMediaUrl>
                        <dataType opt="capture,liveVideo"><!--optional, xs:string, data
type: capture, "liveVideo"-live video--></dataType>
                    </RealStream>
                    <GeneralData><!--dependent, third-party data-->
                        <SrcAddress><!--IP address of data source -->
                            <ipVersion opt="v4,v6,dual"><!--required, xs:string, IP address
type--></ipVersion>
                            <ipAddress><!--dependent, xs:string--></ipAddress>
                            <ipv6Address><!--dependent, xs:string, IPv6 address--></
ipv6Address>
                        </SrcAddress>
                        <dataType opt="popPic,call"><!--optional, xs:string, third-party
data type: "popPic"-pop-up image, call--></dataType>
                    </GeneralData>
                    <dataSourceUrl><!--dependent, xs:string, data source URL, this field is
valid only when the dynamic material is data source and StorageInfo exists; only
8520 platform has the data source material--></dataSourceUrl>

```

```
</DynamicMaterial>  
</Material>
```

XML_MaterialIdList

XML message about material ID list

```
<MaterialIdList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
    <materialId><!--required, xs:integer--></materialId>  
</MaterialIdList>
```

XML_MaterialList

XML message about material information list

```
<MaterialList><!--optional-->  
    <Material/><!--required-->  
</MaterialList>
```

See Also

[XML_Material](#)

XML_MaterialSearchDescription

XML message about material search parameters

```
<MaterialSearchDescription version="2.0" xmlns="http://www.isapi.org/ver20/  
XMLSchema">  
    <searchID><!--required, xs:string, search ID, which is used to check whether  
the current search requester is the same; the search ID is valid for 5 minutes  
--></searchID>  
    <approveState><!--optional, xs:string, approval status: "approved"-pass,  
"notPass"-not pass, "notApprove"-not approved, all--></approveState>  
    <materialType><!--required, xs:string, material type: "static"-local  
material, "dynamic"-dynamic material, all--></materialType>  
    <shareProperty><!--required, xs:string, shared property: public, private,  
all--></shareProperty>  
    <uploader><!--optional, xs:string, uploader name--></uploader>  
    <staticMaterialType><!--required, xs:string, local material type: image,  
flash, video, audio, file, template, document, table, PDF, web, all--></  
staticMaterialType>  
    <minStaticMaterialSize><!--required, xs:integer, the minimum size of a local  
material, unit: byte--></minStaticMaterialSize>  
    <maxStaticMaterialSize><!--dependent, xs:integer, the maximum size of a local  
material, unit: byte--></maxStaticMaterialSize>  
    <dynamicMaterialType><!--dependent, xs:string, dynamic material type: "web"-  
web URL, socket, RSS, "realStream"-real-time stream, "generalData"-general data
```

```
type, all-->/dynamicMaterialType>
  <realStreamType><!--optional, xs:string, real-time stream material type:
stream media server, normal network camera, all-->/</realStreamType>
<TimeSpanList><!--optional-->
  <TimeSpan>
    <startTime><!--required, xs:time, start time (ISO 860 format)--></
startTime>
      <endTime><!--required, xs:time, end time (ISO 860 format)--></endTime>
    </TimeSpan>
  </TimeSpanList>
  <maxResults><!--optional, xs:integer, maximum number of returned results per
search--></maxResults>
  <searchResultsPosition><!--optional, xs:integer, the end position of search
result in result list--></searchResultsPosition>
  <generalDataType><!--optional, xs:string, third-party data type: "popPic"-pop-
up image, call, all; this field is valid only when dynamicMaterialType is
"generalData"--></generalDataType>
  <streamDataType><!--optional, xs:string, real-time stream type: capture,
"liveVideo"-live video, all; this field is valid only when dynamicMaterialType
is "normalIPC"--></streamDataType>
</MaterialSearchDescription>
```

XML_MaterialSearchResult

XML message about search results of materials

```
<MaterialSearchResult version="2.0" xmlns="http://www.isapi.org/ver20/
XMLSchema">
  <searchID><!--required, xs:string, search ID, which is used to check whether
the current search request is the same as the previous one.; searchID is valid
for 5 minutes--></searchID>
  <responseStatus><!--required, xs:boolean, whether it is searched: "true"-yes,
"false"-no--></responseStatus>
  <responseStatusString><!--required, xs:string, search status: "true+OK"-no
more results, "true+MORE"-there are more results not returned, "FAILED"-search
failed, "PARAM ERROR"incorrect parameters, "TIMEOUT"-timed out--></
responseStatusString>
  <totalMatches><!--required, xs:integer, total number of returned results--></
totalMatches>
  <numOfMatches><!--required, xs:integer, number of matched results--></
numOfMatches>
  <MaterialList><!--optional, matched material list-->
    </Material><!--required-->
  </MaterialList>
</MaterialSearchResult>
```

XML_ModuleStatus

Message about the status of the secure door control unit in XML format

```
<ModuleStatus version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <onlineStatus><!--required, xs:string, online status, the value of each bit from the first one indicates the online status of the secure door control unit with the corresponding door No. For each bit, 0 indicates that the unit is offline, and 1 indicates that the unit is online. The maximum size of this node is 256 bytes--></onlineStatus>
    <desmantelStatus><!--required, xs:string, tampering status, the value of each bit from the first one indicates the tampering status of the secure door control unit with the corresponding door No. For each bit, 0 indicates that the unit is not tampered, and 1 indicates that the unit is tampered. The maximum size of this node is 256 bytes--></desmantelStatus>
</ModuleStatus>
```

XML_Page

XML message about parameters of a page

```
<Page>
    <id><!--required, int, page No.--></id>
    <PageBasicInfo><!--required, basic page information-->
        <pageName><!--required, string, page name--></pageName>
        <BackgroundColor><!--required, background color-->
            <RGB><!--required, int, three primary colors in decimal format, e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackgroundColor>
        <playDurationMode><!--required, string, page playing time mode: "selfDefine,auto". When the value of this node is selfDefine, the node <playDuration> is valid; when the value is auto, it will be calculated according to the content playing time--></playDurationMode>
            <playDuration><!--dependent, int, playing duration, unit: second--></playDuration>
            <switchDuration><!--required, int, switching duration, unit: second--></switchDuration>
                <switchEffect><!--required, string, switching effect: "none,random,boxShrink,boxSpread,cycleShrink,cycSpread,eraseUp,eraseDown,eraseLeft,eraseRight,verticalShelter,horizontalShelter,verticalChessboard,horizontalChessboard,dissolve,leftRightToCenter,ceterToLeftRight,upDownToCenter,centerToUpDown,drawOutLeftDown,drawOutLeftUp,drawOutRightDown,drawOutRightUp,verticalLine,horizontalLine"--></switchEffect>
                <backgroundPic><!--optional, int, background picture which is the picture material ID--></backgroundPic>
            </PageBasicInfo>
            <characterMode><!--optional, xs:string, welcome word mode on the page: mode1, mode2, mode3. For access control devices, the position of the welcome words is fixed and can be in three modes--></characterMode>
```

```

<WindowsList><!--optional, window information-->
    <Windows>
        <id><!--required, int, content No.--></id>
        <Position><!--required, content's position. The upper-left corner is the
origin, and the size of the full screen is 1920*1920-->
            <positionX><!--required, int, X-coordinate of upper-left corner of the
content's rectangle frame--></positionX>
            <positionY><!--required, int, Y-coordinate of upper-left corner of the
content's rectangle frame--></positionY>
            <height><!--required, int, height of the content's rectangle frame--></
height>
            <width><!--required, int, width of the content's rectangle frame--></
width>
        </Position>
        <layerNo><!--required, int, layer No.--></layerNo>
        <WinMaterialInfo><!--dependent, window material information-->
            <materialType><!--required, string, window material type: static,
dynamic, other--></materialType>
            <staticMaterialType><!--dependent, string, local material type. This
node is valid when <materialType> is static--></staticMaterialType>
            <dynamicType><!--dependent, string, dynamic window material type:
"web,socket,rss,call,dynamicPic,realStream,capturePic, character". This node is
valid when <materialType> is dynamic--></dynamicType>
            <otherType><!--dependent, hyperlinkBtn"string, other type:
"clock,weather,countdown,localInput,hyperlinkBtn"--></otherType>
        </WinMaterialInfo>
        <TouchProperty><!--optional, touching attributes-->
            <windType><!--optional, string, window type: pop-up window, page
window--></windType>
            <hyperlinkType><!--optional, string, hyperlink type: "window,page".
This node is valid when <windType> is popup--></hyperlinkType>
            <>windowId><!--dependent, int, window No. (window of current page). This
node is valid when <hyperlinkType> is window--></windowId>
            <pageId><!--dependent, int, page No. This node is valid when
<hyperlinkType> is page--></pageId>
        </TouchProperty>
        <PlayItemList><!--dependent, window playing list-->
            <PlayItem><!--required-->
                <id><!--required, int, playing No.--></id>
                <materialNo><!--dependent, int, material index No.--></materialNo>
                <inputChannel><!--optional, string, linked channel No. of the network
camera--></inputChannel>
                <playEffect><!--required, string, playing effect: none, scroller--></
playEffect>
                <MarqueeInfo><!--dependent-->
                    <scrollType><!--required, string, scroller scrolling type: not
scroll, scroll circularly, scroll once, scroll backwards and forwards--></
scrollType>
                    <scrollDeriction><!--required, string, scroller scrolling
direction: none, from top to bottom, from bottom to top, from left to right,
from right to left--></scrollDeriction>
                    <scrollSpeed><!--required, int, scroller scrolling speed--></

```

```

scrollSpeed>
    </MarqueeInfo>
    <PlayDuration><!--material playing duration. This node can be
configured for local materials, live video, and network camera channels-->
        <durationType><!--required, string, playing duration type, custom-->
    </durationType>
        <duration><!--required, int, material playing duration, unit:
second--></duration>
    </PlayDuration>
    <CharactersEffect><!--required, character display effect. This node
is valid when the material type is text or TXT file-->
        <fontSize><!--required, int, font size--></fontSize>
        <FontColor><!--required, font color-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </FontColor>
        <BackColor><!--required, background color-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackColor>
        <backTransparent><!--required, int, background transparency--></
backTransparent>
        <subtitlesEnabled><!--required, boolean, whether to enable
character display mode--></subtitlesEnabled>
        <scrollDirection><!--required, string, character scrolling
direction: "left,right,up,down"--></scrollDirection>
        <scrollSpeed><!--required, int, text scrolling speed--></
scrollSpeed>
    </CharactersEffect>
    <switchEffect><!--optional, string, switching effect of the window
material: from left to right, from right to left, from bottom to top, from top
to bottom, fade in and fade out, exit from the middle, pop down from the top,
enter from the lower-right corner, enter from the upper-left corner, blind
horizontally, blind vertically, random effect. This node is valid for picture
materials--></switchEffect>
        <pageTime><!--dependent, int, paging interval, unit: second. This
node is valid when the material is a word, ppt, pdf, or excel file--></pageTime>
        <scrollSpeed><!--dependent, int, scrolling speed. This node is valid
when the material is a static web--></scrollSpeed>
    <CharactersAttribute><!--dependent, character attribute, this node is
valid when <b>dynamicType

```

```

<alignType><!--optional, string, alignment mode:  

"left,right,middle,top,bottom,verticalCenter,horizontallyCenter"--></alignType>  

<characterContent><!--optional, string, text content whose maximum  

size is 512 bytes. This node is valid when <b>dynamicType
characterContent>  

</CharactersAttribute>  

</PlayItem>  

</PlayItemList>  

<enabledAudio><!--dependent, boolean, whether to enable the audio--></  

enabledAudio>  

<enableHide><!--optional, boolean, whether to enable hiding--></  

enableHide>  

<enableLock><!--optional, boolean, whether to enable the clock--></  

enableLock>  

<AppWindow><!--dependent-->  

<WindowInfoList><!--required-->  

<WindowInfo><!--required, -->  

<id><!--required, int, No.--></id>  

<materialNo><!--required, int, material No.--></materialNo>  

</WindowInfo>  

</WindowInfoList>  

</AppWindow>  

<DataSource><!--dependent, data source. This node is valid when it is a  

calling or pop-up window-->  

<materialNo><!--required, int, material No.--></materialNo>  

</DataSource>  

<Call><!--dependent, calling data-->  

<tableRow><!--required, int, row of the table--></tableRow>  

<tableColumn><!--required, int, column of the table--></tableColumn>  

<tableDirection><!--required, int, table direction:  

"vertical, horizontal"--></tableDirection>  

<tableType><!--required, xs:string, table template:  

"template1,template2,template3,template4,template5,template6"--></tableType>  

<backPicId><!--optional, int, control's background picture--></  

backPicId>  

<alignType><!--required, string, alignment mode: "left,right,middle"-->  

</alignType>  

<refreshDirection><!--required, string, refreshing direction:  

"upTodown"-from top to bottom, "downToup"-from bottom to top--></  

refreshDirection>  

<HeadDataList><!--optional-->  

<HeadData><!--optional, table head data (calling data)-->  

<id><!--required, int, No.--></id>  

<data><!--required, string, data--></data>  

</HeadData>  

</HeadDataList>  

<ItemStyleList>  

<ItemStyle><!--style of the table's row or column-->  

<id><!--required, int, No.--></id>  

<width><!--required, int, width of each column (percentage)--></  

width>  

<fontSize min="" max=""><!--required, int, font size--></fontSize>

```

```

<FontColor><!--required-->
    <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
</FontColor>
<BackColor><!--required-->
    <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
</BackColor>
</ItemStyle>
</ItemStyleList>
</Call>
<DynamicPic><!--dependent, dynamic pop-up window parameters-->
    <backPicId><!--optional, int, ID of the control's background picture--></backPicId>
    </DynamicPic>
    <CapturePic><!--dependent-->
        <backPicId><!--optional, int, ID of the control's background picture--></backPicId>
        <ipcMaterialNo><!--required, int--></ipcMaterialNo>
        <cancelType><!--required, int, cancelling type: "auto,manual"--></cancelType>
            <duration><!--dependent, int, material playing duration, unit: second--></duration>
            </CapturePic>
            <ClockParam><!--dependent, clock parameters-->
                <backPicId><!--optional, int, ID of the control's background picture--></backPicId>
                <ClockIcon><!--required, clock icon paameters-->
                    <enabled><!--required, boolean--></enabled>
                    <type><!--dependent, string, type: "clock1,clock2,..."--></type>
                    <Position><!--dependent-->
                        <positionX><!--required, int, X-coordinate of the content's position--></positionX>
                        <positionY><!--required, int, Y-coordinate of the content's position--></positionY>
                        <height><!--required, int, height--></height>
                        <width><!--required, int, width--></width>
                    </Position>
                </ClockIcon>
                <YmdParam><!--required, parameters of year, month, and day in the clock-->
                    <enabled><!--required, boolean, whether to enable--></enabled>
                    <fontSize><!--required, int, font size--></fontSize>
                    <FontColor><!--required-->
                        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
                    </FontColor>
                    <BackColor><!--required-->
                        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
                    </BackColor>
                    <Position><!--dependent-->

```

```

<positionX><!--required, int, X-coordinate of the content's
position--></positionX>
    <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
        <height><!--required, int, height--></height>
        <width><!--required, int, width--></width>
    </Position>
</YmdParam>
<HmsParam><!--required, parameters of hour, minute, and second in the
clock-->
    <enabled><!--required, boolean--></enabled>
    <fontSize><!--required, int, font size--></fontSize>
    <FontColor><!--required, font color-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX><!--required, int, X-coordinate of the content's
position--></positionX>
            <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
                <height><!--required, int, height--></height>
                <width><!--required, int, width--></width>
            </Position>
        </HmsParam>
        <WeekParam><!--required, week parameters-->
            <enabled><!--required, boolean--></enabled>
            <fontSize><!--required, int--></fontSize>
            <FontColor><!--required-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
            </FontColor>
            <BackColor><!--required-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
            </BackColor>
            <Position><!--dependent-->
                <positionX><!--required, int, X-coordinate of the content's
position--></positionX>
                    <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
                        <height><!--required, int, height--></height>
                        <width><!--required, int, width--></width>
                    </Position>
            </WeekParam>
        </ClockParam>
        <WeatherParam><!--dependent, weather parameters-->
            <backPicId><!--optional, int, ID of the weather's background picture-->

```

```

></backPicId>
    <WeatherIcon><!--optional, weather icon parameters-->
        <enabled><!--required, boolean, whether to enable--></enabled>
        <Position><!--dependent-->
            <positionX><!--required, int,X-coordinate of the content's
position--></positionX>
            <positionY><!--required, int,Y-coordinate of the content's
position--></positionY>
                <height><!--required, int, height--></height>
                <width><!--required, int, width--></width>
            </Position>
        </WeatherIcon>
    <Date><!--optional, date parameters-->
        <enabled><!--required, boolean, whether to enable--></enabled>
        <fontSize><!--required, int, font size--></fontSize>
        <FontColor><!--required, font color-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
        </FontColor>
        <BackColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
        </BackColor>
        <Position><!--dependent-->
            <positionX><!--required, int,X-coordinate of the content's
position--></positionX>
            <positionY><!--required, int,Y-coordinate of the content's
position--></positionY>
                <height><!--required, int, height--></height>
                <width><!--required, int, width--></width>
            </Position>
        </Date>
    <Temperature><!--optional, temperature parameters-->
        <enabled><!--required, boolean, whether to enable--></enabled>
        <fontSize><!--required, int, font size--></fontSize>
        <FontColor><!--required, font color-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
        </FontColor>
        <BackColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFFFFFF--></RGB>
        </BackColor>
        <Position><!--dependent-->
            <positionX><!--required, int,X-coordinate of the content's
position--></positionX>
            <positionY><!--required, int,Y-coordinate of the content's
position--></positionY>
                <height><!--required, int, height--></height>
                <width><!--required, int, width--></width>
            </Position>
        </Temperature>

```

```

<WeatherContent><!--optional, weather parameters-->
    <enabled><!--required, boolean, whether to enable--></enabled>
    <fontSize><!--required, int, font size--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX><!--required, int,X-coordinate of the content's
position--></positionX>
        <positionY><!--required, int,Y-coordinate of the content's
position--></positionY>
        <height><!--required, int, height--></height>
        <width><!--required, int, width--></width>
    </Position>
</WeatherContent>
<City><!--optional, city parameters-->
    <enabled><!--required, boolean, whether to enable--></enabled>
    <cityId><!--required, string, city No.--></cityId>
    <cityName><!--required, string, city name--></cityName>
    <fontSize><!--required, int--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </BackColor>
    <Position><!--dependent-->
        <positionX><!--required, int,X-coordinate of the content's
position--></positionX>
        <positionY><!--required, int,Y-coordinate of the content's
position--></positionY>
        <height><!--required, int, height--></height>
        <width><!--required, int, width--></width>
    </Position>
</City>
<Humidity><!--optional, humidity parameters-->
    <enabled><!--required, boolean, whether to enable--></enabled>
    <fontSize><!--required, int--></fontSize>
    <FontColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
    </FontColor>
    <BackColor><!--required-->
        <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>

```

```

        </BackColor>
        <Position><!--dependent-->
            <positionX><!--required, int, X-coordinate of the content's
position--></positionX>
            <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
                <height><!--required, int, height--></height>
                <width><!--required, int, width--></width>
            </Position>
        </Humidity>
        <AirQuality><!--optional, air quality parameters-->
            <enabled><!--required, boolean--></enabled>
            <fontSize><!--required, int--></fontSize>
            <FontColor><!--required-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
            </FontColor>
            <BackColor><!--required-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
            </BackColor>
            <Position><!--dependent-->
                <positionX><!--required, int, X-coordinate of the content's
position--></positionX>
                <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
                    <height><!--required, int, height--></height>
                    <width><!--required, int, width--></width>
                </Position>
            </AirQuality>
            <UpdateTime><!--optional, update time parameters-->
                <enabled><!--required, boolean, whether to enable--></enabled>
                <refreshTime><!--required, xs:time, refreshing time in ISO8601 time
format--></refreshTime>
                    <updateInterval><!--required, int, updating interval, unit: minute-->
                </updateInterval>
                <fontSize><!--required, int--></fontSize>
                <FontColor><!--required-->
                    <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
                </FontColor>
                <BackColor><!--required-->
                    <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
                </BackColor>
                <Position><!--dependent-->
                    <positionX><!--required, int, X-coordinate of the content's
position--></positionX>
                    <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
                        <height><!--required, int, height--></height>
                        <width><!--required, int, width--></width>
                    </Position>
                </AirQuality>
            </UpdateTime>
        </Position>
    </Content>
</Image>

```

```

        </Position>
    </UpdateTime>
    <Wind><!--optional, wind power parameters-->
        <enabled><!--required, boolean, whether to enable--></enabled>
        <fontSize><!--required, int--></fontSize>
        <FontColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </FontColor>
        <BackColor><!--required-->
            <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
        </BackColor>
        <Position><!--dependent-->
            <positionX><!--required, int, X-coordinate of the content's
position--></positionX>
            <positionY><!--required, int, Y-coordinate of the content's
position--></positionY>
            <height><!--required, int, height--></height>
            <width><!--required, int, width--></width>
        </Position>
    </Wind>
</WeatherParam>
<Countdown><!--dependent, countdown material-->
    <endTime><!--required, xs:time, countdown time in ISO8601 time format--></endTime>
        <template><!--required, string, template: "template1" (template 1),
"template2..." (template 2)--></template>
        <timeUnit><!--required, string, time unit:
"year,month,day,week,hour,minute,second"--></timeUnit>
        <backPicId><!--optional, int--></backPicId>
        <TimeFontCfg><!--optional-->
            <fontSize><!--required, int--></fontSize>
            <FontColor><!--required-->
                <RGB><!--required, int, three primary colors in decimal format,
e.g., 16777215 indicates 0xFFFF--></RGB>
            </FontColor>
            <Position><!--required, content's position. The upper-left corner is
the origin, and the size of the full screen is 1920*1920-->
                <positionX><!--required, int, X-coordinate of upper-left corner of
the content's rectangle frame--></positionX>
                <positionY><!--required, int, Y-coordinate of upper-left corner of
the content's rectangle frame--></positionY>
                <height><!--required, int, height of the content's rectangle frame--></height>
                <width><!--required, int, width of the content's rectangle frame--></width>
            </Position>
        </TimeFontCfg>
    </Countdown>
    <localInputNo><!--dependent, string, local input No.--></localInputNo>
    <HyperlinkBtn><!--dependent-->

```

```
<backPicId><!--optional, int, ID of the control's background picture-->
</backPicId>
</HyperlinkBtn>
</Windows>
</WindowsList>
</Page>
```

XML_PageList

XML message about page information

```
<PageList xmlns="http://www.isapi.org/ver20/XMLSchema" version="2.0" >
<Page>
    <!--list-->
    <id>
        <!--required, xs:integer, page No.-->
    </id>
    <PageBasicInfo>
        <!--required, page basic information-->
        <pageName>
            <!--required, xs:string, page name-->
        </pageName>
        <BackgroundColor>
            <!--required, background color-->
            <RGB>
                <!--required, xs:integer, RGB-->
            </RGB>
        </BackgroundColor>
        <playDurationMode>
            <!--required, xs:string, play mode: custom, auto, or auto-switch, this field is valid only when playDuration exists-->
        </playDurationMode>
        <playDuration>
            <!--dependent, xs:integer, play duration, unit: second-->
        </playDuration>
        <playCount>
            <!--optional, xs:integer-->
        </playCount>
        <switchDuration>
            <!--required, xs:integer, switch interval, unit: second-->
        </switchDuration>
        <switchEffect>
            <!--required, xs:string, switch effect, opt="none,random,boxShrink,boxSpread,cycleShrink,cycSpread,eraseUp,eraseDown,era seLeft,eraseRight,verticalShelter,horizontalShelter,verticalChessboard,horizontalChessboard,dissolve,leftRightToCenter,ceterToLeftRight,upDownToCenter,centerToUpDown,drawOutLeftDown,drawOutLeftUp,drawOutRightDown,drawOutRightUp,verticalLine,horizontalLine"-->
        </switchEffect>
        <backgroundPic>
```

```
<!--optional, xs:integer, background picture-->
</backgroundPic>
</PageBasicInfo>
<WindowsList>
    <!--optional, window information-->
    <Windows>
        <!--list-->
        <id>
            <!--required, xs:integer, content No.-->
        </id>
        <Position>
            <!--required, content position-->
            <positionX>
                <!--required, xs:integer-->
            </positionX>
            <positionY>
                <!--required, xs:integer-->
            </positionY>
            <height>
                <!--required, xs:integer-->
            </height>
            <width>
                <!--required, xs:integer-->
            </width>
        </Position>
        <layerNo>
            <!--required, xs:integer, layer No.-->
        </layerNo>
        <WinMaterialInfo>
            <!--dependent, material information-->
            <materialType>
                <!--required, xs:string, material type: "static"-local material,
"dynamic"-dynamic material, other-->
            </materialType>
            <staticMaterialType>
                <!--dependent, xs:string, local material type:
"picture,flash,audio,video,document,ppt,doc,excel,pdf,web,app"; this field is
valid only when materialType is "static"-->
            </staticMaterialType>
            <dynamicType>
                <!--dependent, xs:string, local material type:
"web,socket,rss,call,dynamicPic,realStream,capturePic,character"; this field is
valid only when materialType is "dynamic"-->
            </dynamicType>
            <otherType>
                <!--dependent,
xs:string,"clock,weather,countdown,localInput,hyperlinkBtn"-->
            </otherType>
        </WinMaterialInfo>
        <TouchProperty>
            <!--optional, touch attribute-->
            <windType>
```

```
<!--optional, xs:string, window type: "popup"-pop-up, page-->
</windType>
<hyperlinkType>
    <!--optional, xs:string, hyperlink type: "window,page"; this field
is valid only when windType is "popup"-->
    </hyperlinkType>
    <windowId>
        <!--dependent, xs:integer, window No.; this field is valid only
when hyperlinkType is "window"-->
        </windowId>
        <pageId>
            <!--dependent, xs:integer, page No.; this field is valid only when
hyperlinkType is "page"-->
            </pageId>
        </TouchProperty>
        <PlayItemList>
            <!--dependent, playing list-->
            <PlayItem>
                <!--required-->
                <id>
                    <!--required, xs:integer, playing No.-->
                </id>
                <materialNo>
                    <!--dependent, xs:integer, material No., which can be obtained by
calling /ISAPI/Publish/MaterialMgr/material by PUT method-->
                    </materialNo>
                    <inputChannel>
                        <!--optional, xs:integer, channel No. of bound IPC (network
camera)-->
                        </inputChannel>
                        <playEffect>
                            <!--required, xs:string, playing effect, "none,marquee"-->
                        </playEffect>
                        <MarqueeInfo>
                            <!--dep-->
                            <scrollType>
                                <!--required, xs:string, marquee scrolling type: none, loops,
"once"-scroll once, "backAndForth"-scroll back and forth-->
                                </scrollType>
                                <scrollDeriction>
                                    <!--required, xs:string, scrolling direction,
"none,up,down,left,right"-->
                                    </scrollDeriction>
                                    <scrollSpeed>
                                        <!--required, xs:integer, scrolling speed-->
                                    </scrollSpeed>
                                </MarqueeInfo>
                                <PlayDuration>
                                    <!--playing duration of material-->
                                    <durationType>
                                        <!--required, xs:string, "materialTime,selfDefine"-->
                                    </durationType>
                                </PlayDuration>
                            </MarqueeInfo>
                        </scrollDeriction>
                    </inputChannel>
                </materialNo>
            </PlayItem>
        </PlayItemList>
    </windowId>
</hyperlinkType>
```

```

<duration>
    <!--required, xs:integer, unit: second-->
</duration>
</PlayDuration>
<CharactersEffect>
    <!--dependent, character display effect, which is valid only when
material type is text-->
    <fontSize>
        <!--required, xs:integer, font size -->
    </fontSize>
    <FontColor>
        <!--required, font color-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </FontColor>
    <BackColor>
        <!--required, background color-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </BackColor>
    <backTransparent>
        <!--required, xs:integer, background transparency-->
    </backTransparent>
    <subtitlesEnabled>
        <!--required, xs:boolean, whether to enable preview-->
    </subtitlesEnabled>
    <scrollDirection>
        <!--required, xs:string, scrolling direction,
"left,right,up,down"-->
    </scrollDirection>
    <scrollSpeed>
        <!--required, xs:integer, scrolling speed-->
    </scrollSpeed>
</CharactersEffect>
<switchEffect>
    <!--optional, window switch effect, "
xs:string,none,leftInRightOut,rightInLeftOut,bottomInTopOut,topInBottomOut,fadeInFadeOut,middleExit,topPop,rightBottomIn,leftTopIn,horizontalOpen,verticalOpen,random"-->
</switchEffect>
<pageTime>
    <!--dependent, xs:integer, flip interval, which is invalid only
when the staticMaterialType is "word", "ppt", "pdf", or "excel", unit: second -->
</pageTime>
<scrollSpeed>
    <!--dependent, xs:integer, scrolling speed, which is invalid when
staticMaterialType is "web"-->
</scrollSpeed>
<CharactersAttribute>

```

```
<!--dependent, character attribute, which is valid only when
dynamicType is "character"-->
<fontSize>
    <!--optional, xs:integer, font size-->
</fontSize>
<FontColor>
    <!--optional, font color-->
<RGB>
    <!--optional, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--optional, background color-->
<RGB>
    <!--optional, xs:integer, RGB-->
</RGB>
</BackColor>
<backTransparent>
    <!--optional, xs:integer, background transparency-->
</backTransparent>
<alignType>
    <!--optional, xs:string, alignment,
"left,right,middle,top,bottom,verticalCenter,horizontallyCenter"-->
</alignType>
<characterContent>
    <!--optional, xs:string, content, which is valid only when
dynamicType is "character"; the maximum size is 512 bytes-->
</characterContent>
</CharactersAttribute>
</PlayItem>
</PlayItemList>
<enabledAudio>
    <!--dependent, xs:boolean, whether to enable playing audio -->
</enabledAudio>
<enableHide>
    <!--optional, xs:boolean-->
</enableHide>
<enableLock>
    <!--optional, xs:boolean, whether to display to enable locking-->
</enableLock>
<AppWindow>
    <!--dependent-->
<WindowInfoList>
    <!--required-->
<WindowInfo>
    <!--required-->
<id>
    <!--required, xs:integer-->
</id>
<materialNo>
    <!--required, xs:integer-->
</materialNo>
```

```
</WindowInfo>
</WindowInfoList>
</AppWindow>
<DataSource>
    <!--dependent, data source, which is valid only when the window type
is call or pop-up-->
    <materialNo>
        <!--required, xs:integer-->
    </materialNo>
</DataSource>
<Call>
    <!--dependent, call data-->
    <tableRow>
        <!--required, xs:integer, row-->
    </tableRow>
    <tableColumn>
        <!--required, xs:integer, column-->
    </tableColumn>
    <tableDirection>
        <!--required, xs:string, table direction,
opt="vertical,horizontal"-->
    </tableDirection>
    <tableType>
        <!--required,
xs:string,opt="template1,template2,template3,template4,template5,template6"-->
    </tableType>
    <backPicId>
        <!--optional, xs:integer, it can be obtained by calling /ISAPI/
Publish/MaterialMgr/material by PUT method-->
    </backPicId>
    <alignType>
        <!--required, xs:string, alignment type, "left,right,middle"-->
    </alignType>
    <refreshDirection>
        <!--required, xs:string, refresh mode,
"upTodown,downToup,leftToright,rightToleft"-->
    </refreshDirection>
    <HeadDataList>
        <!--optional-->
        <HeadData>
            <!--optional,header of call data-->
            <id>
                <!--required, xs:integer-->
            </id>
            <data>
                <!--required, xs:string-->
            </data>
        </HeadData>
    </HeadDataList>
    <ItemStyleList>
        <ItemStyle>
            <!--style of rows and columns in a table-->
        </ItemStyle>
    </ItemStyleList>

```

```
<id>
    <!--required, xs:integer-->
</id>
<width>
    <!--required, xs:integer, column width (%)-->
</width>
<fontSize min="" max="" >
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
</ItemStyle>
</ItemStyleList>
</Call>
<DynamicPic>
    <!--dependent, pop-up window configuration-->
<backPicId>
    <!--optional, xs:integer-->
</backPicId>
</DynamicPic>
<CapturePic>
    <!--dep-->
<backPicId>
    <!--optional, xs:integer-->
</backPicId>
<ipcMaterialNo>
    <!--required, xs:integer-->
</ipcMaterialNo>
<cancelType>
    <!--required, xs:string,"auto,manual"-->
</cancelType>
<duration>
    <!--dependent, xs:integer, unit: second-->
</duration>
</CapturePic>
<ClockParam>
    <!--dependent, clock parameters-->
<backPicId>
    <!--optional, xs:integer, background picture ID of control-->
</backPicId>
<ClockIcon>
    <!--required, icon parameters of clock-->
```

```
<enabled>
    <!--required, xs:boolean, whether to enable clock icon-->
</enabled>
<type>
    <!--dependent, xs:string, opt="clock1,clock2,..."-->
</type>
<Position>
    <!--dependent, position-->
    <positionX>
        <!--required, xs:integer-->
    </positionX>
    <positionY>
        <!--required, xs:integer-->
    </positionY>
    <height>
        <!--required, xs:integer-->
    </height>
    <width>
        <!--required, xs:integer-->
    </width>
</Position>
</ClockIcon>
<YmdParam>
    <!--required, YY/MM/DD parameters-->
<enabled>
    <!--required, xs:boolean, whether to display YY/MM/DD -->
</enabled>
<fontSize>
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
    <RGB>
        <!--required, xs:integer, RGB-->
    </RGB>
</FontColor>
<BackColor>
    <!--required-->
    <RGB>
        <!--required, xs:integer, RGB-->
    </RGB>
</BackColor>
<Position>
    <!--dep-->
    <positionX>
        <!--required, xs:integer-->
    </positionX>
    <positionY>
        <!--required, xs:integer-->
    </positionY>
    <height>
        <!--required, xs:integer-->
    </height>
```

```
</height>
<width>
    <!--required, xs:integer-->
</width>
</Position>
</YmdParam>
<HmsParam>
    <!--required, time parameters of clock, -->
<enabled>
    <!--required, xs:boolean, whether to display time-->
</enabled>
<fontSize>
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
    <!--dep-->
<positionX>
    <!--required, xs:integer-->
</positionX>
<positionY>
    <!--required, xs:integer-->
</positionY>
<height>
    <!--required, xs:integer-->
</height>
<width>
    <!--required, xs:integer-->
</width>
</Position>
</HmsParam>
<WeekParam>
    <!--required, week parameters of clock -->
<enabled>
    <!--required, xs:boolean, whether to display week -->
</enabled>
<fontSize>
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
```

```
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
    <!--dep-->
    <positionX>
        <!--required, xs:integer-->
    </positionX>
    <positionY>
        <!--required, xs:integer-->
    </positionY>
    <height>
        <!--required, xs:integer-->
    </height>
    <width>
        <!--required, xs:integer-->
    </width>
    </Position>
</WeekParam>
</ClockParam>
<WeatherParam>
    <!--dependent, weather parameters-->
    <backPicId>
        <!--optional, xs:integer, background picture ID-->
    </backPicId>
    <WeatherIcon>
        <!--optional, weather icon information-->
        <enabled>
            <!--required, xs:boolean, -->
        </enabled>
        <Position>
            <!--dep-->
            <positionX>
                <!--required, xs:integer-->
            </positionX>
            <positionY>
                <!--required, xs:integer-->
            </positionY>
            <height>
                <!--required, xs:integer-->
            </height>
            <width>
                <!--required, xs:integer-->
            </width>
        </Position>
    </WeatherIcon>
</WeatherParam>
```

```
</WeatherIcon>
<Date>
    <!--optional, date parameters of weather window -->
    <enabled>
        <!--required, xs:boolean, whether to display date -->
    </enabled>
    <fontSize>
        <!--required, xs:integer-->
    </fontSize>
    <FontColor>
        <!--required-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </FontColor>
    <BackColor>
        <!--required-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </BackColor>
    <Position>
        <!--dep-->
        <positionX>
            <!--required, xs:integer-->
        </positionX>
        <positionY>
            <!--required, xs:integer-->
        </positionY>
        <height>
            <!--required, xs:integer-->
        </height>
        <width>
            <!--required, xs:integer-->
        </width>
    </Position>
</Date>
<Temperature>
    <!--optional, temperature parameters of weather window -->
    <enabled>
        <!--required, xs:boolean, whether to display temperature -->
    </enabled>
    <fontSize>
        <!--required, xs:integer-->
    </fontSize>
    <FontColor>
        <!--required-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </FontColor>
    <BackColor>
```

```
<!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
    <!--dep-->
    <positionX>
        <!--required, xs:integer-->
    </positionX>
    <positionY>
        <!--required, xs:integer-->
    </positionY>
    <height>
        <!--required, xs:integer-->
    </height>
    <width>
        <!--required, xs:integer-->
    </width>
</Position>
</Temperature>
<WeatherContent>
    <!--optional, weather condition parameters of weather window -->
    <enabled>
        <!--required, xs:boolean, whether to display weather condition -->
    </enabled>
    <fontSize>
        <!--required, xs:integer-->
    </fontSize>
    <FontColor>
        <!--required-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </FontColor>
    <BackColor>
        <!--required-->
        <RGB>
            <!--required, xs:integer, RGB-->
        </RGB>
    </BackColor>
    <Position>
        <!--dep-->
        <positionX>
            <!--required, xs:integer-->
        </positionX>
        <positionY>
            <!--required, xs:integer-->
        </positionY>
        <height>
            <!--required, xs:integer-->
        </height>
    </Position>
```

```
<width>
    <!--required, xs:integer-->
</width>
</Position>
</WeatherContent>
<City>
    <!--optional, city parameters of weather window -->
<enabled>
    <!--required, xs:boolean, whether to display city parameters -->
</enabled>
<cityId>
    <!--required, xs:string-->
</cityId>
<cityName>
    <!--required, xs:string-->
</cityName>
<fontSize>
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
    <!--dep-->
<positionX>
    <!--required, xs:integer-->
</positionX>
<positionY>
    <!--required, xs:integer-->
</positionY>
<height>
    <!--required, xs:integer-->
</height>
<width>
    <!--required, xs:integer-->
</width>
</Position>
</City>
<Humidity>
    <!--optional, humidity parameters of weather window -->
<enabled>
    <!--required, xs:boolean, whether to display humidity -->
</enabled>
```

```
<fontSize>
  <!--required, xs:integer-->
</fontSize>
<FontColor>
  <!--required-->
<RGB>
  <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
  <!--required-->
<RGB>
  <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
  <!--dep-->
<positionX>
  <!--required, xs:integer-->
</positionX>
<positionY>
  <!--required, xs:integer-->
</positionY>
<height>
  <!--required, xs:integer-->
</height>
<width>
  <!--required, xs:integer-->
</width>
</Position>
</Humidity>
<AirQuality>
  <!--optional, air quality parameters of weather window -->
<enabled>
  <!--required, xs:boolean, whether to display air quality -->
</enabled>
<fontSize>
  <!--required, xs:integer-->
</fontSize>
<FontColor>
  <!--required-->
<RGB>
  <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
  <!--required-->
<RGB>
  <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
```

```
<!--dep-->
<positionX>
    <!--required, xs:integer-->
</positionX>
<positionY>
    <!--required, xs:integer-->
</positionY>
<height>
    <!--required, xs:integer-->
</height>
<width>
    <!--required, xs:integer-->
</width>
</Position>
</AirQuality>
<UpdateTime>
    <!--optional, updating time parameters -->
<enabled>
    <!--required, xs:boolean, whether to display updating time -->
</enabled>
<refreshTime>
    <!--required, xs:time, updating time (ISO 8601 format)-->
</refreshTime>
<updateInterval>
    <!--required, xs:integer, updating interval, unit: minute -->
</updateInterval>
<fontSize>
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
    <!--dep-->
<positionX>
    <!--required, xs:integer-->
</positionX>
<positionY>
    <!--required, xs:integer-->
</positionY>
<height>
    <!--required, xs:integer-->
</height>
```

```
<width>
    <!--required, xs:integer-->
</width>
</Position>
</UpdateTime>
<Wind>
    <!--optional, wind power parameters -->
<enabled>
    <!--required, xs:Boolean, whether to display wind power-->
</enabled>
<fontSize>
    <!--required, xs:integer-->
</fontSize>
<FontColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</FontColor>
<BackColor>
    <!--required-->
<RGB>
    <!--required, xs:integer, RGB-->
</RGB>
</BackColor>
<Position>
    <!--dep-->
<positionX>
    <!--required, xs:integer-->
</positionX>
<positionY>
    <!--required, xs:integer-->
</positionY>
<height>
    <!--required, xs:integer-->
</height>
<width>
    <!--required, xs:integer-->
</width>
</Position>
</Wind>
</WeatherParam>
<Countdown>
    <!--dependent, countdown -->
<endTime>
    <!--required, xs:time, countdown time (ISO 8601 format)-->
</endTime>
<template>
    <!--required, xs:string,"template1,template2..."-->
</template>
<timeUnit>
    <!--required, xs:string, time unit,
```

```
"year,month,day,hour,minute,second" -->
    </timeUnit>
    <backPicId>
        <!--optional, xs:integer-->
    </backPicId>
    <TimeFontCfg>
        <!--optional-->
        <fontSize>
            <!--required, xs:integer-->
        </fontSize>
        <FontColor>
            <!--required, font color-->
            <RGB>
                <!--required, xs:integer, RGB-->
            </RGB>
        </FontColor>
        <Position>
            <!--required-->
            <positionX>
                <!--required, xs:integer-->
            </positionX>
            <positionY>
                <!--required, xs:integer-->
            </positionY>
            <height>
                <!--required, xs:integer-->
            </height>
            <width>
                <!--required, xs:integer-->
            </width>
        </Position>
    </TimeFontCfg>
</Countdown>
<localInputNo>
    <!--dependent, xs:string-->
</localInputNo>
<HyperlinkBtn>
    <!--dep-->
    <backPicId>
        <!--optional, xs:integer-->
    </backPicId>
</HyperlinkBtn>
<CharactersAttribute>
    <!--dependent, this field is valid only when dynamicType is
"character"-->
    <fontSize>
        <!--optional, xs:integer, font size-->
    </fontSize>
    <FontColor>
        <!--optional, font color-->
        <RGB>
            <!--optional, xs:integer, RGB-->
```

```
</RGB>
</FontColor>
<fontType>
    <!--optional, xs:string, font, "normal,bold" -->
</fontType>
<BackColor>
    <!-->
<RGB>
    <!--optional, xs:integer, RGB-->
</RGB>
</BackColor>
<backTransparent>
    <!--optional, xs:integer, background transparency-->
</backTransparent>
<alignType>
    <!--optional, xs:string, alignment, "left,right,middle" -->
</alignType>
<verticalAlignType>
    <!--optional, xs:string, vertical alignment,
"top,bottom,verticalCenter" -->
</verticalAlignType>
<characterContent>
    <!--optional, xs:string, content, the maximum size is 512 bytes -->
</characterContent>
</CharactersAttribute>
</Windows>
</WindowsList>
</Page>
</PageList>
```

XML_PlaySchedule

XML message about parameters of a specific program schedule

```
<PlaySchedule version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <id><!--required, xs:integer, program schedule No.--></id>
    <scheduleName><!--required, xs:string, program schedule name--></scheduleName>
    <scheduleRemarks><!--optional, xs:string, program schedule description--></
scheduleRemarks>
    <approveState><!--optional, xs:string, approval status: "approved"-pass,
"notPass"-not pass, "notApprove"-not approved--></approveState>
    <approveRemarks><!--optional, xs:string, approval remarks--></approveRemarks>
    <scheduleMode><!--optional, xs:string, program schedule mode: mormal, decode
and touch--></scheduleMode>
    <orgNo><!--optional, xs:integer, organization No.--></orgNo>
    <scheduleType><!--optional, xs:string, program schedule type: "daily"-daily
schedule, "weekly"-weekly schedule, "selfDefine"-custom schedule, "loop"-loop
schedule, "defaultSchedule"-default schedule--></scheduleType>
    <shareProperty><!--optional, xs:string, shared property: public, private--></
shareProperty>
    <DailySchedule><!--dependent, daily schedule-->
```

```

<PlaySpanList><!--required-->
    <PlaySpan><!--required-->
        <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
        <programNo><!--required, xs:integer, No. of the shown program--></
programNo>
        <TimeRange><!--required, play duration-->
            <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
            <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
        </TimeRange>
    </PlaySpan>
</PlaySpanList>
</DailySchedule>
<WeeklySchedule><!--dependent, weekly schedule-->
    <DayList><!--required-->
        <Day><!--required-->
            <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
            <dayOfWeek><!--required, xs:string, day of a week --></dayOfWeek>
            <PlaySpanList><!--required, play schedule-->
                <PlaySpan><!--required-->
                    <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
                    <programNo><!--required, xs:integer, No. of the looped program--></
programNo>
                    <TimeRange><!--required, play duration-->
                        <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
                        <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
                    </TimeRange>
                </PlaySpan>
            </PlaySpanList>
        </Day>
    </DayList>
</WeeklySchedule>
<LoopSchedule><!--dependent, loop schedule-->
    <ProgramNoList><!--required, list of loop programs, normal mode-->
        <programNo><!--required, xs:integer, No. of the looped program--></
programNo>
    </ProgramNoList>
    <LoopTimeSpanList><!--dependent-->
        <LoopTimeSpan><!--optional-->
            <TimeRange><!--required, play duration-->
                <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
                <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
            </TimeRange>
        </LoopTimeSpan>
    </LoopTimeSpanList>
</LoopSchedule>

```

```
</LoopTimeSpanList>
</LoopSchedule>
<SelfDefineSchedule><!--dependent-->
<SelfDefineList><!--required-->
    <SelfDefine><!--required, custom period-->
        <id><!--required, xs:integer, custom period No.--></id>
        <programNo><!--required, xs:integer, program No., which is returned by
calling the API /ISAPI/Publish/ProgramMgr/program--></programNo>
        <TimeRange><!--required, play duration-->
            <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
            <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
        </TimeRange>
    </SelfDefine>
</SelfDefineList>
</SelfDefineSchedule>
<DefaultSchedule><!--dependent, default program schedule-->
    <programNo><!--required, xs:integer, program No.--></programNo>
</DefaultSchedule>
<HolidaySchedule><!--optional, holiday schedule-->
    <PlaySpanList><!--required, daily schedule-->
        <PlaySpan><!--required, daily schedule-->
            <id><!--required, xs:integer, day of a month, "1,2,3..."--></id>
            <programNo><!--required, xs:integer, program No.--></programNo>
            <TimeRange><!--required, play duration-->
                <beginTime><!--required, xs:time, start time (ISO 8601 format)--></
beginTime>
                <endTime><!--required, xs:time, end time (ISO 8601 format)--></
endTime>
            </TimeRange>
        </PlaySpan>
    </PlaySpanList>
</HolidaySchedule>
</PlaySchedule>
```

XML_PlayScheduleList

XML message about information of all program schedules

```
<?xml version="1.0" encoding="utf-8"?>
<PlayScheduleList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <PlaySchedule/><!--program schedule information-->
</PlayScheduleList>
```

See Also

XML_PlaySchedule

XML_Program

XML message about program parameters

```
<Program version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <id><!--required, xs:integer, program ID--></id>
  <programName><!--required, xs:string, program name--></programName>
  <programRemarks><!--required, xs:string, program description--></
programRemarks>
  <shareProperty><!--optional, xs:string, shared property: public, private--></
shareProperty>
  <approveState><!--optional, xs:string, approval status: "approved"-pass,
"notPass"-not pass, "notApprove"-not approved--></approveState>
  <approveRemarks><!--optional, xs:string, approval remarks--></approveRemarks>
  <programType><!--optional, xs:string, program type: normal, decode, touch,
"decodeTouch"-decode and touch, character (welcome words, which is used for
access control devices)--></programType>
  <orgNo><!--optional, xs:integer, organization No.--></orgNo>
  <Resolution><!--required-->
    <resolutionName><!--optional, xs:string, resolution --></resolutionName>
      <imageWidth><!--required, xs:integer, resolution width--></imageWidth>
      <imageHeight><!--required, xs:integer, resolution height--></imageHeight>
    </Resolution>
  <PageList/><!--required, page list-->
  <programSize><!--read-only, optional, xs:integer, page list, unit: byte--></
programSize>
  <programLength><!--read-only, optional, xs:integer, program duration, unit:
second--></programLength>
</Program>
```

See Also

[XML_PageList](#)

XML_ProgramDynamicCap

XML message about capabilities of program dynamic parameters

```
<ProgramDynamicCap xmlns="http://www.isapi.org/ver20/XMLSchema" version="2.0" >
  <ProgramCapList>
    <!--required, program capability list-->
    <ProgramCap>
      <!--required-->
      <id>
        <!--required, xs:integer, program No.-->
      </id>
      <programType>
        <!--required, xs:string, program type: normal, decode, touch, character
(welcome words, which is used for access control devices)-->
      </programType>
```

```

<maxPageNum>
    <!--required, xs:integer, maximum number of pages-->
</maxPageNum>
<maxWinNum>
    <!--required, xs:integer, maximum number of windows per page-->
</maxWinNum>
<maxMaterialNum>
    <!--required, xs:integer, maximum number of materials per window-->
</maxMaterialNum>
<isSupportTouch>
    <!--required, xs:boolean, whether it supports touch screen; if so, you
can configure the touch properties for the program-->
</isSupportTouch>
<WinCapList><!--optional, object, window capability list-->
    <WinCap><!--optional, object, window capability-->
        <id><!--required, xs:integer, serial No.--></id>
        <BaseRes><!--required, object, basic resolution-->
            <resWidth><!--required, xs:integer, width of the resolution--></
resWidth>
            <resHeight><!--required, xs:integer, height of the resolution--></
resHeight>
        </BaseRes>
        <WinSizeList><!--required, object, window size list-->
            <WinSize><!--optional, object, range of the window height-->
                <id><!--required, xs:integer, index--></id>
                <WinMaterialInfo><!--required, object, window material
information-->
                    <materialType opt="static,dynamic"><!--required, string,
material type: static, dynamic--></materialType>
                    <staticMaterialType
opt="picture,flash,audio,video,document,ppt,doc,excel,pdf,web"><!--optional,
string, static material type: picture, flash, audio, video, document, ppt, doc,
excel, pdf, web--></staticMaterialType>
                    <dynamicType
opt="web,socket,rss,call,dynamicPic,realStream,capturePic"><!--optional,
string, dynamic material type: web, socket, rss, realStream, call, dynamicPic,
capturePic--></dynamicType>
                    <otherType
opt="clock,weather,countdown,localInput,hyperlinkBtn,callBtn,openDoorBtn,QRCodeB
tn,authenticationSuccess,authenticationFail,statusBar"><!--optional, string,
other material type: clock, weather, countdown, localInput (local input),
hyperlinkBtn (hyperlink button), callBtn (calling button), openDoorBtn (door
opening button), QRCodeBtn (QR code button), authenticationSuccess
(authenticated), authenticationFail (authentication failed), statusBar (status
bar)--></otherType>
                    </WinMaterialInfo>
                    <maxWinNum><!--optional, xs:integer, the maximum number of
windows with specific resolution--></maxWinNum>
                    <!--optional, xs:integer, range of the
window width. For access control devices, the values of min and max are the
same. The value of this node is calculated by the unified coordinate type,
which means that the value of this node is converted by the base coordinate
-->
                <min><!--optional, xs:integer, minimum value of the
range-->
                <max><!--optional, xs:integer, maximum value of the
range-->
            </width>
        </resHeight>
    </WinSize>
</WinSizeList>
</WinCap>
</WinCapList>

```

1920. For example, if the actual resolution width of the screen is 1080 px and the window width is 540 px, the value of this node is $540/1080*1920$ --></width>

```
<height min="1" max="10"><!--optional, xs:integer, range of the window height. For access control devices, the values of min and max are the same. The value of this node is calculated by the unified coordinate type, which means that the value of this node is converted by the base coordinate 1920. For example, if the actual resolution height of the screen is 1080 px and the window height is 540 px, the value of this node is  $540/1080*1920$ --></height>
```

<DefaultSize><!--optional, object, default window size-->

```
<defaultWidth><!--required, xs:integer, width of the default window size--></defaultWidth>
```

<defaultHeight><!--required, xs:integer, height of the default window size--></defaultHeight>

```
</DefaultSize>
```

<x min="0" max="10"><!--optional, xs:integer, X-coordinate of the window's upper-left corner. For access control devices, the values of min and max are the same. The value of this node is calculated by the unified coordinate type. If this node is not returned, there is no limit to min and max--></x>

<y min="0" max="10"><!--optional, xs:integer, Y-coordinate of the window's upper-left corner. For access control devices, the values of min and max are the same. The value of this node is calculated by the unified coordinate type. If this node is not returned, there is no limit to min and max--></y>

<characterType><!--optional, string, character type: mainTitle (main title), subTitle (sub title), subTitle2 (sub title 2). This node is valid and optional when the material type is character and is used for access control devices to return the fixed position of different titles displayed on the device--></characterType>

<characterMode><!--optional, string, character mode: mode1, mode2, mode3. This node is valid and optional when the material type is character and is used for access control devices to return the window position of the main title, sub title, and sub title 2 in different character modes--></characterMode>

<fontSize min="1" max="10"><!--optional, xs:integer, font size, unit: px. This node is valid and optional when the material type is character and is used for access control devices to return the font size range of different fonts in different character modes--></fontSize>

<characterContent min="1" max="512"><!--optional, string, text content, the maximum string size is 512 bytes. This node is valid and optional when the material type is character and is used for access control devices to return the content size range of different character types in different character modes--></characterContent>

```
</WinSize>
</WinSizeList>
```

<maxCharacterWinNum><!--optional, xs:integer, maximum number of windows with characters--></maxCharacterWinNum>

```
</WinCap>
</WinCapList>
</ProgramCap>
</ProgramCapList>
</ProgramDynamicCap>
```

See Also

[XML_WinDynamicCap](#)

XML_ProgramList

XML message about parameters of all programs

```
<ProgramList version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <Program/><!--see details in the message XML_Program-->
</ProgramList>
```

See Also

[XML_Program](#)

XML_PublishServerCap

XML message about capabilities of information release

```
<PublishServerCap version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <maxStaticMaterialNum><!--required, xs:integer, maximum number of local
materials--></maxStaticMaterialNum>
    <maxDynamicMaterialNum><!--required, xs:integer, maximum number of dynamic
materials--></maxDynamicMaterialNum>
    <maxProgramNum><!--required, xs:integer, maximum number of programs--></
maxProgramNum>
    <maxScheduleNum><!--required, xs:integer, maximum number of program
schedules--></maxScheduleNum>
    <maxTerminalNum><!--required, xs:integer, maximum number of terminals--></
maxTerminalNum>
    <maxTerminalGroupNum><!--required, xs:integer, maximum number of terminal
groups--></maxTerminalGroupNum>
    <maxSchedulePlanNum><!--optional, xs:integer, maximum number of release
schedules--></maxSchedulePlanNum>
    <maxOrgNum><!--optional, xs:integer, maximum number of organizations--></
maxOrgNum>
    <maxPackLength><!--optional, xs:integer, unit:KB --></maxPackLength>
    <isSupportMaterialMgr><!--required, xs:boolean, whether it supports material
management--></isSupportMaterialMgr>
    <isSupportProgramMgr><!--required, xs:boolean, whether it supports program
management--></isSupportProgramMgr>
    <isSupportScheduleMgr><!--required, xs:boolean, whether it supports program
schedule management--></isSupportScheduleMgr>
    <isSupportTerminalMgr><!--required, xs:boolean, whether it supports terminal
schedule configuration--></isSupportTerminalMgr>
    <isSupportSwitchPlan><!--required, xs:boolean, whether it supports startup or
shutdown schedule configuration--></isSupportSwitchPlan>
    <isSupportVolumePlan><!--required, xs:boolean, whether it supports volume
```

```
adjustment schedule configuration--></isSupportVolumePlan>
  <isSupportServerAddr><!--required, xs:boolean, whether it supports
configuring terminal registration server address--></isSupportServerAddr>
  <isSupportBusinessIntelligence><!--required, xs:boolean, whether it supports
business intelligence--></isSupportBusinessIntelligence>
  <isSupportTerminalPreview><!--required, xs:boolean, whether it supports
terminal live view--></isSupportTerminalPreview>
  <isSupportTemplateMgr><!--optional, xs:boolean, whether it supports template
management--></isSupportTemplateMgr>
  <isSupportGerDataTrans><!--optional, xs:boolean, whether it supports third-
party data transmission--></isSupportGerDataTrans>
  <isSupportThridPartyFile><!--optional, xs:boolean, whether it supports
uploading third-party files--></isSupportThridPartyFile>
  <isSupportXmlUserMgr><!--optional, xs:boolean, whether it supports user
management--></isSupportXmlUserMgr>
  <isSupportUserPermissionCfg><!--optional, xs:boolean, whether it supports
user permission configuration--></isSupportUserPermissionCfg>
  <isSupportOrgMgr><!--optional, xs:boolean, whether it supports organization
management--></isSupportOrgMgr>
  <isSupportRetransmitPack><!--optional, xs:boolean, whether it supports packet
retransmission--></isSupportRetransmitPack>
  <isSupportWeatherFactory><!--optional, xs:boolean, whether it supports
configuring weather manufacture information--></isSupportWeatherFactory>
  <isSupportScheduleExport><!--optional, xs:boolean, whether it supports
exporting program schedules--></isSupportScheduleExport>
  <isSupportInputPlan><!--optional, xs:boolean, --></isSupportInputPlan>
  <isSupportInsertCharacter><!--optional, xs:boolean--></
isSupportInsertCharacter>
  <isSupportHdInit><!--optional, xs:boolean, whether it supports disk
initialization--></isSupportHdInit>
  <isSupportSSH><!--optional, xs:boolean, whether it supports SSH
configuration--></isSupportSSH>
  <isSupportTerminalAdbDebug><!--optional, xs:boolean, whether it supports
terminal ADB debugging configuration--></isSupportTerminalAdbDebug>
  <isSupportBackupData><!--optional, xs:boolean, whether it supports data
backup--></isSupportBackupData>
  <isSupportServerTimeZone><!--optional, xs:boolean, whether it supports
server time zone configuration--></isSupportServerTimeZone>
  <isSupportTerminalTimeZone><!--optional, xs:boolean, whether it supports
terminal time zone configuration--></isSupportTerminalTimeZone>
  <isSupportTerminalDiscovery><!--optional, xs:boolean, whether it supports
searching for terminals--></isSupportTerminalDiscovery>
  <isSupportScheduleUtcTime><!--optional, xs:boolean, whether it supports UTC
time schedule--></isSupportScheduleUtcTime>
  <isSupportAdditionModule><!--optional, xs:boolean, whether it supports add-
ons--></isSupportAdditionModule>
  <isSupportTerminalMgrCap><!--optional, xs:boolean, whether it supports
getting terminal management capability set--></isSupportTerminalMgrCap>
  <isSupportMaterialThumbnailDownload><!--optional, xs:boolean, whether it
supports downloading material thumbnails--></isSupportMaterialThumbnailDownload>
  <isSupportProgramThumbnailUpload><!--optional, xs:boolean, whether it
supports uploading program thumbnails--></isSupportProgramThumbnailUpload>
```

```
<isSupportprogramThumbnailDownload><!--optional, xs:boolean, whether it
supports downloading program thumbnails--></isSupportprogramThumbnailDownload>
<isSupportRePublish><!--optional, xs:boolean, whether it supports re-
releasing--></isSupportRePublish>
<isSupportTemplateThumbnailUpload><!--optional, xs:boolean, whether it
supports uploading template thumbnails--></isSupportTemplateThumbnailUpload>
<isSupportTemplateThumbnailDownload><!--optional, xs:boolean, whether it
supports downloading template thumbnails--></isSupportTemplateThumbnailDownload>
<isSupportSchedulePlanIDSearch><!--optional, xs:boolean, whether it supports
searching for a single schedule of program schedule--></
isSupportSchedulePlanIDSearch>
<isSupportTemplateBaseInfoSearch><!--optional, xs:boolean, whether it
supports searching for template basic information--></
isSupportTemplateBaseInfoSearch>
<maxDelSchedulePlanNum><!--required, xs:integer, the maximum number of
terminal deleted schedules of releasing program schedules in a batch--></
maxDelSchedulePlanNum>
<maxDelMaterialNum><!--required, xs:integer, the maximum number of materials
deleted in a batch--></maxDelMaterialNum>
<maxDelProgramNum><!--required, xs:integer, the maximum number of programs
deleted in a batch--></maxDelProgramNum>
<maxDelTerminalNum><!--required, xs:integer, the maximum number of terminals
deleted in a batch--></maxDelTerminalNum>
</PublishServerCap>
```

XML_ReaderAcrossHost

ReaderAcrossHost message in XML format

```
<ReaderAcrossHost version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <AcrossHostList size="8">
    <AcrossHostAction>
      <readerNo><!--req, xs: integer, card reader No., which is between 1 and
8--></readerNo>
      <submarineBackEnabled>
        <!--req, xs: boolean, whether to enable the cross-controller anti-
passing back function of the card reader-->
      </submarineBackEnabled>
    </AcrossHostAction>
  </AcrossHostList>
</ReaderAcrossHost>
```

XML_ResponseStatus

XML message about response status

```
<?xml version="1.0" encoding="utf-8"?>
<ResponseStatus version="2.0" xmlns="http://www.std-cgi.org/ver20/XMLSchema">
  <requestURL>
```

```
<!--required, read-only, xs:string, request URL-->
</requestURL>
<statusCode>
    <!--required, read-only, xs:integer, status code: 0,1-OK, 2-Device Busy, 3-
Device Error, 4-Invalid Operation, 5-Invalid XML Format, 6-Invalid XML Content,
7-Reboot Required, 9-Additional Error-->
</statusCode>
<statusString>
    <!--required, read-only, xs:string, status description: OK, Device Busy,
Device Error, Invalid Operation, Invalid XML Format, Invalid XML Content,
Reboot, Additional Error-->
</statusString>
<subStatusCode>
    <!--required, read-only, xs:string, describe the error reason in detail-->
</subStatusCode>
<MErrCode>
    <!--optional, xs:string, error code categorized by functional modules,
e.g., 0x12345678-->
</MErrCode>
<MErrDevSelfEx>
    <!--optional, xs:string, extension field of MErrCode. It is used to define
the custom error code, which is categorized by functional modules-->
</MErrDevSelfEx>
</ResponseStatus>
```



- See [**Response Codes of Text Protocol**](#) for details about sub status codes and corresponding error codes.
 - See [**Error Codes Categorized by Functional Modules**](#) for details about the error codes, error descriptions, and debugging suggestions.
-

XML_StatusResponse_ErrorAuthenticationFailed

StatusResponse message in XML format for failed authentication.

```
<ResponseStatus version="1.0" xmlns="http://www.std-cgi.org/ver20/XMLSchema">
    <requestURL><!-- req, ro,xs:string --></requestURL>
    <statusCode><!-- req, ro,xs:integer --></statusCode>
    <statusString><!-- req, ro,xs:string --></statusString>
    <subStatusCode><!-- req, ro,xs:string --></subStatusCode>
    <lockStatus><!-- opt, ro,xs:string , "unlock,locked", locking status--></
lockStatus>
    <retryTimes><!-- opt, ro,xs:integer, remaining authentication attempts--></
retryTimes>
    <resLockTime><!-- opt, ro,xs:integer, remaining locking time, unit: second-->
    </resLockTime>
</ResponseStatus>
```

XML_RemoteControlDoor

RemoteControlDoor message in XML format

```
<RemoteControlDoor version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <cmd>
    <!--req, xs:string, command: "open"-open the door, "close"-close the door
    (controlled), "alwaysOpen"-remain unlocked (free), "alwaysClose"-remain open
    (disabled), "visitorCallLadder"-call elevator (visitor), "householdCallLadder"-call
    elevator (resident)-->
  </cmd>
  <password>
    <!--opt, xs:string, password for opening door. This node is not required
    for access control devices to remotely control the door in the LAN. For EZVIZ
    Cloud Service, this node is required and access control devices will verify the
    inputted password-->
  </password>
</RemoteControlDoor>
```

XML_ServerDevice

ServerDevice message in XML format

```
<ServerDevice version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <ipAddr><!--req, xs: string, IP address of the cross-controller anti-passing
  back server--></ipAddr>
  <port><!--req, xs: string, port No. of the cross-controller anti-passing back
  server--></port>
</ServerDevice>
```

XML_SnapConfig

SnapConfig message in XML format

```
<SnapConfig version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
  <snapTimes><!--req, xs: integer, capture times triggered by loop, the value
  is between 0 and 5--></snapTimes>
  <snapWaitTime>
    <!--req, xs: integer, capture waiting time, the value is between 0 and
    6,000, currently, this node is reserved-->
  </snapWaitTime>
  <intervalTimeList><!--req, the list size is 4-->
    <intervalTime>
      <!--req, xs: integer, time interval of continuous capture, the value is
      between 0 and 6,000-->
    </intervalTime>
  </intervalTimeList>
  <JPEGParam>
```

```
<pictureSize>
    <!--req, xs: string, picture resolution: 0-CIF, 1-QCIF, 2-D1, 3-UXGA
(1600 × 1200), 4-SVGA(800 × 600), 5-HD720p(1280 × 720), 6-VGA, 7-XVGA, 8-
HD900p, 9-HD1080, 10-2560 × 1920, 11-1600 × 304, 12-2048 × 1536,
13-2448 × 2048, 14-2448 × 1200, 15-2448 × 800, 16-XGA(1024 × 768), 17-
SXGA(1280 × 1024), 18-WD1(960 × 576/960 × 480), 19-1080i, 20-576 × 576, 21-1536
× 1536, 22-1920 × 1920, 161-288 × 320, 162-144 × 176, 163-480 × 640, 164-240 ×
320, 165-120 × 160, 166-576 × 720, 167-720 × 1280, 168-576 × 960, 180-180*240,
181-360*480, 182-540*720, 183-720*960, 184-960*1280, 185-1080*1440, 0xff-auto-->
</pictureSize>
<pictureQuality><!--req, xs: string, picture quality: "best", "better",
"general"--></pictureQuality>
</JPEGParam>
</SnapConfig>
```

XML_StartReaderInfo

StartReaderInfo message in XML format

```
<StartReaderInfo version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <hostNo><!--req, xs: integer, access controller No., min="1" max="64"--></
hostNo>
    <readerNo><!--req, xs: integer, card reader No., min="1" max="8"--></readerNo>
</StartReaderInfo>
```

XML_SubmarineBack

SubmarineBack message in XML format

```
<SubmarineBack version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <enabled><!--req, xs: boolean, whether to specify this access controller as
the cross-controller anti-passing back server--></enabled>
</SubmarineBack>
```

XML_SubmarineBackHostInfo

SubmarineBackHostInfo message in XML format

```
<SubmarineBackHostInfo version="2.0" xmlns="http://www.isapi.org/ver20/
XMLSchema">
    <HostInfoList size="16">
        <Action>
            <deviceNo><!--req, xs: integer, device No., which is between 1 and 64--></
deviceNo>
            <serial><!--req, xs: string, device serial No., min="9" max="9"--></
serial>
        </Action>
```

```
</HostInfoList>  
</SubmarineBackHostInfo>
```

XML_SubmarineBackMode

SubmarineBackMode message in XML format

```
<SubmarineBackMode version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
  <mode>  
    <!--req, xs:string, anti-passing back mode: "disable"-anti-passing back is  
    disabled, "internetCommunicate"-based on network, "cardReadAndWrite"-based on  
    card-->  
  </mode>  
  <rule>  
    <!--req, xs:string, anti-passing back rule: "line"-route anti-passing back,  
    "inOrOut"-entrance/exit anti-passing back. This node is invalid when the mode  
    is set to "disable"-->  
  </rule>  
  <sectionID>  
    <!--req, xs:integer, section ID, which is between 1 and 100. This node is  
    valid when mode is "cardReadAndWrite", and only one section ID can be  
    configured for one configuration-->  
  </sectionID>  
</SubmarineBackMode>
```

XML_SubmarineBackReader

SubmarineBackReader message in XML format

```
<SubmarineBackReader version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">  
  <selfHostNo><!--req, xs:integer, access controller No. of the configuration  
  object, which is between 1 and 64--></selfHostNo>  
  <selfReaderNo><!--req, xs:integer, card reader No. of the configuration  
  object, which is between 1 and 8--></selfReaderNo>  
  <FollowReaderList size="16">  
    <Action>  
      <followHostNo><!--req, xs:integer, following access controller No., which  
      is between 1 and 64--></followHostNo>  
      <followReaderNo><!--req, xs:integer, following card reader No., which is  
      between 1 and 8--></followReaderNo>  
    </Action>  
  </FollowReaderList>  
</SubmarineBackReader>
```

XML_WiegandCfg

WiegandCfg message in JSON format

```
<WiegandCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <communicateDirection><!--required, xs:string, communication direction:
"receive", "send"--></communicateDirection>
    <wiegandMode><!--dependent, xs:string, Wiegand mode: "wiegand26",
"wiegand34", "wiegand27", "wiegand35". This node is valid when
<communicateDirection> is "send"--></wiegandMode>
    <signalInterval><!--optional, xs:integer, interval of sending Wiegand
signals, it is between 1 and 20, unit: ms--></signalInterval>
    <enable><!--optional, xs:boolean, whether to enable Wiegand parameters: true,
false--></enable>
</WiegandCfg>
```

XML_WiegandRuleCfg

WiegandRuleCfg message in XML format

```
<WiegandRuleCfg version="2.0" xmlns="http://www.isapi.org/ver20/XMLSchema">
    <name>
        <!--req, xs:string, Wiegand name-->
    </name>
    <CustomerCardIn>
        <totalLength>
            <!--req, xs:integer, total Wiegand length. When this node is set to 0,
the custom Wiegand rule settings will be cleared-->
        </totalLength>
        <checkMethod>
            <!--req, xs:string, parity mode: "parityCheck,xorCheck,noCheck"-->
        </checkMethod>
        <ParityCheck>
            <!--dep, configuration rule of odd-even parity, this node is valid when
<checkMethod> is "parityCheck"-->
            <oddBeginBit>
                <!--dep, xs:integer, start bit of odd parity-->
            </oddBeginBit>
            <oddLength>
                <!--dep, xs:integer, odd parity length-->
            </oddLength>
            <evenBeginBit>
                <!--dep, xs:integer, start bit of even parity-->
            </evenBeginBit>
            <evenLength>
                <!--dep, xs:integer, even parity length-->
            </evenLength>
        </ParityCheck>
        <XorCheck>
            <!--dep, configuration rule of XOR parity, this node is valid when
<checkMethod> is "xorCheck"-->
            <xorBeginBit>
                <!--dep, xs:integer, start bit of XOR parity-->
            </xorBeginBit>
        </XorCheck>
    </CustomerCardIn>
</WiegandRuleCfg>
```

```

<xorPerLength>
    <!--dep, xs:integer, length of each XOR parity group-->
</xorPerLength>
<xorTotalLength>
    <!--dep, xs:integer, total length of XOR parity data-->
</xorTotalLength>
</XorCheck>
<cardIdBeginBit>
    <!--req, xs:integer, start bit of the card No.-->
</cardIdBeginBit>
<cardIdLength>
    <!--req, xs:integer, card No. length-->
</cardIdLength>
<siteCodeBeginBit>
    <!--req, xs:integer, start bit of the site code-->
</siteCodeBeginBit>
<siteCodeLength>
    <!--req, xs:integer, site code length-->
</siteCodeLength>
<oemBeginBit>
    <!--req, xs:integer, start bit of OEM-->
</oemBeginBit>
<oemLength>
    <!--req, xs:integer, OEM length-->
</oemLength>
<manufacturerCodeBeginBit>
    <!--req, xs:integer, start bit of the manufacturer code-->
</manufacturerCodeBeginBit>
<manufacturerCodeLength>
    <!--req, xs:integer, manufacturer code length-->
</manufacturerCodeLength>
</CustomerCardIn>
<CustomerCardOut>
    <CardContentList size="4">
        <!--This node contains multiple <Action> nodes, and the <type> node in
each <Action> node can only be set to one type. The order of the types will
determine the combination order of the rules-->
        <Action>
            <No>
                <!--req, xs:integer, No.-->
            </No>
            <type>
                <!--req, xs:string, type: "cardId"-card ID, "siteCode"-site code,
"oem"-OEM No., "manufacturerCode"-manufacturer code-->
            </type>
            <length>
                <!--req, xs:integer, length of the corresponding decimal data-->
            </length>
        </Action>
    </CardContentList>
</CustomerCardOut>
</WiegandRuleCfg>

```

XML_WinDynamicCap

XML message about window capabilities at different resolutions

```
<WinDynamicCap xmlns="http://www.isapi.org/ver20/XMLSchema" version="2.0" >
  <WinCapList>
    <!--required, window capability list-->
    <WinCap>
      <!--list-->
      <id>
        <!--required, xs:integer, window No.-->
      </id>
      <BaseRes>
        <!--required, basic resolution, and the size range of each type of
window is listed-->
        <resWidth>
          <!--required, xs:integer-->
        </resWidth>
        <resHeight>
          <!--required, xs:integer-->
        </resHeight>
      </BaseRes>
      <WinSizeList>
        <!--required, window size list-->
        <WinSize>
          <!--list-->
          <id>
            <!--required, xs:integer-->
          </id>
          <WinMaterialInfo>
            <!--required, window material information-->
            <materialType>
              <!--required, xs:string, material type: "static"-local material,
"dynamic"-dynamic material, other-->
            </materialType>
            <staticMaterialType
opt="picture,flash,audio,video,document,ppt,doc,excel, pdf, web" >
              <!--dependent, xs:string, local material type-->
            </staticMaterialType>
            <dynamicType
opt="web,socket,rss,call,dynamicPic,realStream,capturePic" >
              <!--dependent, xs:string, dynamic material type-->
            </dynamicType>
            <otherType opt="clock,weather,countdown,localInput,hyperlinkBtn" >
              <!--dependent, xs:string, other type-->
            </otherType>
          </WinMaterialInfo>
          <maxWinNum>
            <!--optional, xs:integer, maximum number of windows of a specific
type at a certain resolution-->
          </maxWinNum>
        </WinSize>
      </WinSizeList>
    </WinCap>
  </WinCapList>
</WinDynamicCap>
```

```

<!--range of window width-->
<!--range of window height-->
<DefaultSize>
    <!--optional-->
    <defaultWidth>
        <!--required, xs:integer, default width-->
    </defaultWidth>
    <defaultHeight>
        <!--required, xs:integer, default height-->
    </defaultHeight>
</DefaultSize>
</WinSize>
</WinSizeList>
<maxCharacterWinNum>
    <!--optional, xs:integer, maximum number of text windows-->
</maxCharacterWinNum>
</WinCap>
</WinCapList>
<MuteWinList>
    <!--optional, capability of mutually exclusive window-->
<WinList>
    <!--list, required, window list, only one window can exist at a time-->
    <WinMaterialInfo>
        <!--required-->
        <materialType>
            <!--required, xs:string,"static,dynamic,other"-->
        </materialType>
        <staticMaterialType
opt="picture,flash,audio,video,document,ppt,doc,excel, pdf, web" >
            <!--dependent, xs:string, static windows-->
        </staticMaterialType>
        <dynamicType opt="web,socket,rss,call,dynamicPic,realStream,capturePic"
>
            <!--dependent, xs:string, dynamic windows: web, call, "dynamicPic"-pop-up image, "realStream"-stream media, "capturePic"-captured picture-->
        </dynamicType>
        <otherType opt="clock,weather,countdown,localInput,hyperlinkBtn" >
            <!--dependent, xs:string, other windows: clock, weather, countdown,
"localInpu"-video input, "hyperlinkBtn"-hyperlink-->
        </otherType>
    </WinMaterialInfo>
</WinList>
</MuteWinList>
</WinDynamicCap>

```

B.2 Access Control Event Types

The access control events are classified as four major types, i.e., alarm events (MAJOR_ALARM-0x1), exception events (MAJOR_EXCEPTION-0x2), operation events (MAJOR_OPERATION-0x3), and other events (MAJOR_EVENT-0x5). Each major type corresponds to multiple minor types, see details below.

MAJOR_ALARM

Event Minor Type	Value	Description
MINOR_ALARMIN_SHORT_CIRCUIT	0x400	Zone Short Circuit Attempts Alarm
MINOR_ALARMIN_BROKEN_CIRCUIT	0x401	Zone Disconnected Alarm
MINOR_ALARMIN_EXCEPTION	0x402	Zone Exception Alarm
MINOR_ALARMIN_RESUME	0x403	Zone Restored
MINOR_HOST_DESMANTLE_ALARM	0x404	Zone Tampering Alarm
MINOR_HOST_DESMANTLE_RESUME	0x405	Zone Tampering Restored
MINOR_CARD_READER_DESMANTLE_ALARM	0x406	Card Reader Tampering Alarm
MINOR_CARD_READER_DESMANTLE_RESUME	0x407	Card Reader Tampering Restored
MINOR_CASE_SENSOR_ALARM	0x408	Alarm Input Alarm Triggered
MINOR_CASE_SENSOR_RESUME	0x409	Alarm Input Restored
MINOR_STRESS_ALARM	0x40a	Duress Alarm
MINOR_OFFLINE_ECENT_NEARLY_FULL	0x40b	No Memory Alarm for Offline Events
MINOR_CARD_MAX_AUTHENTICATE_FAIL	0x40c	Maximum Failed Card Authentications Alarm
MINOR_SD_CARD_FULL	0x40d	SD Card Full Alarm
MINOR_LINKAGE_CAPTURE_PIC	0x40e	Capture Linkage Alarm

Event Minor Type	Value	Description
MINOR_SECURITY_MODULE_DESMANTLE_ALARM	0x40f	Secure Door Control Unit Tampering Alarm
MINOR_SECURITY_MODULE_DESMANTLE_RESUME	0x410	Secure Door Control Unit Tampering Restored
MINOR_FIRE_IMPORT_SHORT_CIRCUIT	0x415	Fire Input Short Circuit Attempts Alarm
MINOR_FIRE_IMPORT_BROKEN_CIRCUIT	0x416	Fire Input Open Circuit Attempts Alarm
MINOR_FIRE_IMPORT_RESUME	0x417	Fire Input Restored
MINOR_FIRE_BUTTON_TRIGGER	0x418	Fire Button Triggered
MINOR_FIRE_BUTTON_RESUME	0x419	Fire Button Resumed
MINOR_MAINTENANCE_BUTTON_TRIGGER	0x41a	Maintenance Button Triggered
MINOR_MAINTENANCE_BUTTON_RESUME	0x41b	Maintenance Button Resumed
MINOR_EMERGENCY_BUTTON_TRIGGER	0x41c	Panic Button Triggered
MINOR_EMERGENCY_BUTTON_RESUME	0x41d	Panic Button Resumed
MINOR_DISTRACT_CONTROLLER_ALARM	0x41e	Distributed Elevator Controller Tampering Alarm
MINOR_DISTRACT_CONTROLLER_RESUME	0x41f	Distributed Elevator Controller Tampering Restored
MINOR_CHANNEL_CONTROLLER_DESMANTLE_ALARM	0x422	Lane Controller Tampering Alarm
MINOR_CHANNEL_CONTROLLER_DESMANTLE_RESUME	0x423	Lane Controller Tampering Alarm Restored

Event Minor Type	Value	Description
MINOR_CHANNEL_CONTROLLER_FIRE_IMPORT_ALARM	0x424	Lane Controller Fire Input Alarm
MINOR_CHANNEL_CONTROLLER_FIRE_IMPORT_RESUME	0x425	Lane Controller Fire Input Alarm Restored
MINOR_PRINTER_OUT_OF_PAPER	0x440	No Paper in Printer Alarm
MINOR_LEGAL_EVENT_NEARLY_FULL	0x442	No Memory Alarm for Valid Offline Events
MINOR_ALARM_CUSTOM1 to MINOR_ALARM_CUSTOM64	0x900 to 0x93f	Access Control: Custom Alarm Event 1 to Custom Alarm Event 64

MAJOR_EXCEPTION

Event Minor Type	Value	Description
MINOR_NET_BROKEN	0x27	Network Disconnected
MINOR_RS485_DEVICE_ABNORMAL	0x3a	RS485 Connection Exception
MINOR_RS485_DEVICE_REVERT	0x3b	RS485 Connection Restored
MINOR_DEV_POWER_ON	0x400	Power on
MINOR_DEV_POWER_OFF	0x401	Power off
MINOR_WATCH_DOG_RESET	0x402	Watchdog Reset
MINOR_LOW_BATTERY	0x403	Low Battery Voltage
MINOR_BATTERY_RESUME	0x404	Battery Voltage Restored
MINOR_AC_OFF	0x405	AC Power Disconnected
MINOR_AC_RESUME	0x406	AC Power Restored
MINOR_NET_RESUME	0x407	Network Restored
MINOR_FLASH_ABNORMAL	0x408	Flash Reading and Writing Exception

Event Minor Type	Value	Description
MINOR_CARD_READER_OFFLINE	0x409	Card Reader Offline
MINOR_CAED_READER_RESUME	0x40a	Card Reader Online
MINOR_INDICATOR_LIGHT_OFF	0x40b	Indicator Turns off
MINOR_INDICATOR_LIGHT_RESUME	0x40c	Indicator Resumed
MINOR_CHANNEL_CONTROLLER_OFF	0x40d	Lane Controller Offline
MINOR_CHANNEL_CONTROLLER_RESUME	0x40e	Lane Controller Online
MINOR_SECURITY_MODULE_OFF	0x40f	Secure Door Control Unit Offline
MINOR_SECURITY_MODULE_RESUME	0x410	Secure Door Control Unit Online
MINOR_BATTERY_ELECTRIC_LOW	0x411	Low Battery Voltage (Only for Face Recognition Terminal)
MINOR_BATTERY_ELECTRIC_RESUME	0x412	Battery Voltage Recovered (Only for Face Recognition Terminal)
MINOR_LOCAL_CONTROL_NET_BROKEN	0x413	Network of Distributed Access Controller Disconnected
MINOR_LOCAL_CONTROL_NET_RSUME	0x414	Network of Distributed Access Controller Restored
MINOR_MASTER_RS485_LOOPNODE_BROKEN	0x415	RS485 Loop of Main Access Controller Disconnected
MINOR_MASTER_RS485_LOOPNODE_RESUME	0x416	RS485 Loop of Main Access Controller Connected
MINOR_LOCAL_CONTROL_OFFLINE	0x417	Distributed Access Controller Offline
MINOR_LOCAL_CONTROL_RESUME	0x418	Distributed Access Controller Online

Event Minor Type	Value	Description
MINOR_LOCAL_DOWNSIDE_RS485_LOOPNODE_BROKEN	0x419	Downstream RS485 Loop of Distributed Access Control Disconnected
MINOR_LOCAL_DOWNSIDE_RS485_LOOPNODE_RESUME	0x41a	Downstream RS485 Loop of Distributed Access Control Connected
MINOR_DISTRACT_CONTROLLER_ONLINE	0x41b	Distributed Elevator Controller Online
MINOR_DISTRACT_CONTROLLER_OFFLINE	0x41c	Distributed Elevator Controller Offline
MINOR_ID_CARD_READER_NOT_CONNECT	0x41d	ID Card Reader Disconnected
MINOR_ID_CARD_READER_RESUME	0x41e	ID Card Reader Connected
MINOR_FINGER_PRINT_MODULE_NOT_CONNECT	0x41f	Fingerprint Module Disconnected
MINOR_FINGER_PRINT_MODULE_RESUME	0x420	Fingerprint Module Connected
MINOR_CAMERA_NOT_CONNECT	0x421	Camera Disconnected
MINOR_CAMERA_RESUME	0x422	Camera Connected
MINOR_COM_NOT_CONNECT	0x423	COM Port Disconnected
MINOR_COM_RESUME	0x424	COM Port Connected
MINOR_DEVICE_NOT_AUTHORIZE	0x425	Device Unauthorized
MINOR_PEOPLE_AND_ID_CARD_DEVICE_ONLINE	0x426	Face Recognition Terminal Online
MINOR_PEOPLE_AND_ID_CARD_DEVICE_OFFLINE	0x427	Face Recognition Terminal Offline
MINOR_LOCAL_LOGIN_LOCK	0x428	Local Login Lock
MINOR_LOCAL_LOGIN_UNLOCK	0x429	Local Login Unlock

Event Minor Type	Value	Description
MINOR_SUBMARINEBACK_COMM_BREAK	0x42a	Communication with Anti-passing Back Server Failed
MINOR_SUBMARINEBACK_COMM_RESUME	0x42b	Communication with Anti-passing Back Server Restored
MINOR_MOTOR_SENSOR_EXCEPTION	0x42c	Motor or Sensor Exception
MINOR_CAN_BUS_EXCEPTION	0x42d	CAN Bus Exception
MINOR_CAN_BUS_RESUME	0x42e	CAN Bus Exception Restored
MINOR_GATE_TEMPERATURE_OVERRUN	0x42f	Too High Pedestal Temperature
MINOR_IR_EMITTER_EXCEPTION	0x430	Active Infrared Intrusion Detector Exception
MINOR_IR_EMITTER_RESUME	0x431	Active Infrared Intrusion Detector Restored
MINOR_LAMP_BOARD_COMM_EXCEPTION	0x432	Communication with Light Board Failed
MINOR_LAMP_BOARD_COMM_RESUME	0x433	Communication with Light Board Restored
MINOR_IR_ADAPTOR_COMM_EXCEPTION	0x434	Communication with IR Adaptor Failed
MINOR_IR_ADAPTOR_COMM_RESUME	0x435	Communication with IR Adaptor Restored
MINOR_PRINTER_ONLINE	0x436	Printer Online
MINOR_PRINTER_OFFLINE	0x437	Printer Offline
MINOR_4G_MOUDLE_ONLINE	0x438	4G Module Online
MINOR_4G_MOUDLE_OFFLINE	0x439	4G Module Offline
MINOR_AUXILIARY_BOARD_OFFLINE	0x43c	Auxiliary Board Disconnected
MINOR_AUXILIARY_BOARD_RESUME	0x43d	Auxiliary Board Connected
MINOR_IDCARD_SECURITY_MOUDLE_EXCEPTION	0x43e	Secure ID Card Unit Exception

Event Minor Type	Value	Description
MINOR_IDCARD_SECURITY_MOODULE_RESUME	0x43f	Secure ID Card Unit Restored
MINOR_FP_PERIPHERAL_EXCEPTION	0x440	Fingerprint Collection Peripheral Exception
MINOR_FP_PERIPHERAL_RESUME	0x441	Fingerprint Collection Peripheral Restored
MINOR_EXTEND_MODULE_ONLINE	0x44d	Extension Module Online
MINOR_EXTEND_MODULE_OFFLINE	0x44e	Extension Module Offline
MINOR_EXCEPTION_CUSTOM1 to MINOR_EXCEPTION_CUSTOM64	0x900 to 0x93f	Access Control: Custom Exception Event 1 to Custom Exception Event 64

MAJOR_OPERATION

Alarm Minor Types	Value	Description
MINOR_LOCAL_LOGIN	0x50	Local Login
MINOR_LOCAL_LOGOUT	0x51	Local Logout
MINOR_LOCAL_UPGRADE	0x5a	Local Upgrade
MINOR_REMOTE_LOGIN	0x70	Remote Login
MINOR_REMOTE_LOGOUT	0x71	Remote Logout
MINOR_REMOTE_ARM	0x79	Remote Arming
MINOR_REMOTE_DISARM	0x7a	Remote Disarming
MINOR_REMOTE_REBOOT	0x7b	Remote Reboot
MINOR_REMOTE_UPGRADE	0x7e	Remote Upgrade
MINOR_REMOTE_CFGFILE_OUTPUT	0x86	Remote Operation: Export Configuration File
MINOR_REMOTE_CFGFILE_INPUT	0x87	Remote Operation: Import Configuration File
MINOR_REMOTE_ALARMOUT_OPEN_MAN	0xd6	Remote Operation: Enable Alarm Output Manually

Alarm Minor Types	Value	Description
MINOR_REMOTE_ALARMOUT_CLOSE_MAN	0xd7	Remote Operation: Disable Alarm Output Manually
MINOR_REMOTE_OPEN_DOOR	0x400	Door Remotely Open
MINOR_REMOTE_CLOSE_DOOR	0x401	Door Remotely Closed
MINOR_REMOTE_ALWAYS_OPEN	0x402	Remain Open Remotely
MINOR_REMOTE_ALWAYS_CLOSE	0x403	Remain Closed Remotely
MINOR_REMOTE_CHECK_TIME	0x404	Remote: Manual Time Sync
MINOR_NTP_CHECK_TIME	0x405	Network Time Protocol Synchronization
MINOR_REMOTE_CLEAR_CARD	0x406	Remote Operation: Clear All Card No.
MINOR_REMOTE_RESTORE_CFG	0x407	Remote Operation: Restore Defaults
MINOR_ALARMIN_ARM	0x408	Zone Arming
MINOR_ALARMIN_DISARM	0x409	Zone Disarming
MINOR_LOCAL_RESTORE_CFG	0x40a	Local Operation: Restore Defaults
MINOR_REMOTE_CAPTURE_PIC	0x40b	Remote Operation: Capture
MINOR_MOD_NET_REPORT_CFG	0x40c	Edit Network Parameters
MINOR_MOD_GPRS_REPORT_PARAM	0x40d	Edit GPRS Parameters
MINOR_MOD_REPORT_GROUP_PARAM	0x40e	Edit Control Center Parameters
MINOR_UNLOCK_PASSWORD_OPEN_DOOR	0x40f	Enter Dismiss Code
MINOR_AUTO_RENUMBER	0x410	Auto Renumber

Alarm Minor Types	Value	Description
MINOR_AUTO_COMPLEMENT_NUMBER	0x411	Auto Supplement Number
MINOR_NORMAL_CFGFILE_INPUT	0x412	Import Configuration File
MINOR_NORMAL_CFGFILE_OUTPUT	0x413	Export Configuration File
MINOR_CARD_RIGHT_INPUT	0x414	Import Card Permission Parameters
MINOR_CARD_RIGHT_OUTPUT	0x415	Export Card Permission Parameters
MINOR_LOCAL_USB_UPGRADE	0x416	Upgrade Device via USB flash Drive
MINOR_REMOTE_VISITOR_CALL_LADDER	0x417	Visitor Calling Elevator
MINOR_REMOTE_HOUSEHOLD_CALL_LADDER	0x418	Resident Calling Elevator
MINOR_REMOTE_ACTUAL_GUARD	0x419	Remotely Arming
MINOR_REMOTE_ACTUAL_UNGUARD	0x41a	Remotely Disarming
MINOR_REMOTE_CONTROL_NOT_CODE_OPER_FAILED	0x41b	Operation Failed: Keyfob Not Pairing
MINOR_REMOTE_CONTROL_CLOSE_DOOR	0x41c	Keyfob Operation: Close Door
MINOR_REMOTE_CONTROL_OPEN_DOOR	0x41d	Keyfob Operation: Open Door
MINOR_REMOTE_CONTROL_ALWAYS_OPEN_DOOR	0x41e	Keyfob Operation: Remain Door Open
MINOR_M1_CARD_ENCRYPT_VERIFY_OPEN	0x41f	M1 Card Encryption Verification Enabled
MINOR_M1_CARD_ENCRYPT_VERIFY_CLOSE	0x420	M1 Card Encryption Verification Disabled

Alarm Minor Types	Value	Description
MINOR_NFC_FUNCTION_OPEN	0X421	Opening Door with NFC Card Enabled
MINOR_NFC_FUNCTION_CLOSE	0X422	Opening Door with NFC Card Disabled
MINOR_OFFLINE_DATA_OUTPUT	0x423	Export Offline Collected Data
MINOR_CREATE_SSH_LINK	0x42d	Establish SSH Connection
MINOR_CLOSE_SSH_LINK	0x42e	Disconnect SSH Connection
MINOR_BLUETOOTH_KEY MODIFY	/	Bluetooth Key Modified
MINOR_OPERATION_CUSTOM1 to MINOR_OPERATION_CUSTOM64	0x900-0x93f	Access Control: Custom Operation Event 1 to Custom Operation Event 64

MAJOR_EVENT

Event Minor Types	Value	Description
MINOR_LEGAL_CARD_PASS	0x01	Valid Card Authentication Completed
MINOR_CARD_AND_PSW_PASS	0x02	Card and Password Authentication Completed
MINOR_CARD_AND_PSW_FAIL	0x03	Card and Password Authentication Failed
MINOR_CARD_AND_PSW_TIMEOUT	0x04	Card and Password Authentication Timed Out
MINOR_CARD_AND_PSW_OVER_TIME	0x05	Card and Password Authentication Timed Out
MINOR_CARD_NO_RIGHT	0x06	No Permission
MINOR_CARD_INVALID_PERIOD	0x07	Invalid Card Swiping Time Period
MINOR_CARD_OUT_OF_DATE	0x08	Expired Card
MINOR_INVALID_CARD	0x09	Card No. Not Exist

Event Minor Types	Value	Description
MINOR_ANTI_SNEAK_FAIL	0x0a	Anti-passing Back Authentication Failed
MINOR_INTERLOCK_DOOR_NOT_CLOSE	0x0b	Interlocking Door Not Closed
MINOR_NOT_BELONG_MULTI_GROUP	0x0c	Card Not in Multiple Authentication Group
MINOR_INVALID_MULTI_VERIFY_PERIOD	0x0d	Card Not in Multiple Authentication Duration
MINOR_MULTI_VERIFY_SUPER_RIGHT_FAIL	0x0e	Multiple Authentications: Super Password Authentication Failed
MINOR_MULTI_VERIFY_REMOTE_RIGHT_FAIL	0x0f	Multiple Authentication Completed
MINOR_MULTI_VERIFY_SUCCESS	0x10	Multiple Authenticated
MINOR_LEADER_CARD_OPEN_BEGIN	0x11	Open Door with First Card Started
MINOR_LEADER_CARD_OPEN_END	0x12	Open Door with First Card Stopped
MINOR_ALWAYS_OPEN_BEGIN	0x13	Remain Open Started
MINOR_ALWAYS_OPEN_END	0x14	Remain Open Stopped
MINOR_LOCK_OPEN	0x15	Door Unlocked
MINOR_LOCK_CLOSE	0x16	Door Locked
MINOR_DOOR_BUTTON_PRESS	0x17	Exit Button Pressed
MINOR_DOOR_BUTTON_RELEASE	0x18	Exit Button Released
MINOR_DOOR_OPEN_NORMAL	0x19	Door Open (Contact)
MINOR_DOOR_CLOSE_NORMAL	0x1a	Door Closed (Contact)
MINOR_DOOR_OPEN_ANORMAL	0x1b	Door Abnormally Open (Contact)

Event Minor Types	Value	Description
MINOR_DOOR_OPEN_TIMEOUT	0x1c	Door Open Timed Out (Contact)
MINOR_ALARMOUT_ON	0x1d	Alarm Output Enabled
MINOR_ALARMOUT_OFF	0x1e	Alarm Output Disabled
MINOR_ALWAYS_CLOSE_BEGIN	0x1f	Remain Closed Started
MINOR_ALWAYS_CLOSE_END	0x20	Remain Closed Stopped
MINOR_MULTI_VERIFY_NEED_REMOTE_OPEN	0x21	Multiple Authentications: Remotely Open Door
MINOR_MULTI_VERIFY_SUPERPASSWD_VERIFY_SUCCESS	0x22	Multiple Authentications: Super Password Authentication Completed
MINOR_MULTI_VERIFY_REPEAT_VERIFY	0x23	Multiple Authentications: Repeated Authentication
MINOR_MULTI_VERIFY_TIMEOUT	0x24	Multiple Authentications Timed Out
MINOR_DOORBELL_RINGING	0x25	Doorbell Ring
MINOR_FINGERPRINT_COMPARE_PASS	0x26	Fingerprint Matched
MINOR_FINGERPRINT_COMPARE_FAIL	0x27	Fingerprint Mismatched
MINOR_CARD_FINGERPRINT_VERIFY_PASS	0x28	Card and Fingerprint Authentication Completed
MINOR_CARD_FINGERPRINT_VERIFY_FAIL	0x29	Card and Fingerprint Authentication Failed
MINOR_CARD_FINGERPRINT_VERIFY_TIMEOUT	0x2a	Card and Fingerprint Authentication Timed Out
MINOR_CARD_FINGERPRINT_PASSWD_VERIFY_PASS	0x2b	Card and Fingerprint and Password Authentication Completed
MINOR_CARD_FINGERPRINT_PASSWD_VERIFY_FAIL	0x2c	Card and Fingerprint and Password Authentication Failed

Event Minor Types	Value	Description
MINOR_CARD_FINGERPRINT_PASSWD_VERIFY_TIMEOUT	0x2d	Card and Fingerprint and Password Authentication Timed Out
MINOR_FINGERPRINT_PASSWD_VERIFY_PASS	0x2e	Fingerprint and Password Authentication Completed
MINOR_FINGERPRINT_PASSWD_VERIFY_FAIL	0x2f	Fingerprint and Password Authentication Failed
MINOR_FINGERPRINT_PASSWD_VERIFY_TIMEOUT	0x30	Fingerprint and Password Authentication Timed Out
MINOR_FINGERPRINT_INEXISTENCE	0x31	Fingerprint Not Exists
MINOR_CARD_PLATFORM_VERIFY	0x32	Card Platform Authentication
MINOR_CALL_CENTER	0x33	Call Center
MINOR_FIRE_RELAY_TURN_ON_DOOR_ALWAYS_OPEN	0x34	Fire Relay Closed: Door Remains Open
MINOR_FIRE_RELAY_RECOVER_DOOR_RECOVER_NORMAL	0x35	Fire Relay Opened: Door Remains Closed
MINOR_EMPLOYEEENO_AND_FP_VERIFY_PASS	0x45	Employee ID and Fingerprint Authentication Completed
MINOR_EMPLOYEEENO_AND_FP_VERIFY_FAIL	0x46	Employee ID and Fingerprint Authentication Failed
MINOR_EMPLOYEEENO_AND_FP_VERIFY_TIMEOUT	0x47	Employee ID and Fingerprint Authentication Timed Out
MINOR_EMPLOYEEENO_AND_FP_AND_PW_VERIFY_PASS	0x48	Employee ID and Fingerprint and Password Authentication Completed
MINOR_EMPLOYEEENO_AND_FP_AND_PW_VERIFY_FAIL	0x49	Employee ID and Fingerprint and Password Authentication Failed
MINOR_EMPLOYEEENO_AND_FP_AND_PW_VERIFY_TIMEOUT	0x4a	Employee ID and Fingerprint and Password Authentication Timed Out

Event Minor Types	Value	Description
MINOR_FACE_VERIFY_PASS	0x4b	Face Authentication Completed
MINOR_FACE_VERIFY_FAIL	0x4c	Face Authentication Failed
MINOR_EMPLOYEEENO_AND_FACE_VERIFY_PASS	0x4d	Employee ID and Face Authentication Completed
MINOR_EMPLOYEEENO_AND_FACE_VERIFY_FAIL	0x4e	Employee ID and Face Authentication Failed
MINOR_EMPLOYEEENO_AND_FACE_VERIFY_TIMEOUT	0x4f	Employee ID and Face Authentication Timed Out
MINOR_FACE_RECOGNIZE_FAIL	0x50	Face Recognition Failed
MINOR_FIRSTCARD_AUTHORIZE_BEGIN	0x51	First Card Authorization Started
MINOR_FIRSTCARD_AUTHORIZE_END	0x52	First Card Authorization Ended
MINOR_DOORLOCK_INPUT_SHORT_CIRCUIT	0x53	Lock Input Short Circuit Attempts Alarm
MINOR_DOORLOCK_INPUT_BROKEN_CIRCUIT	0x54	Lock Input Open Circuit Attempts Alarm
MINOR_DOORLOCK_INPUT_EXCEPTION	0x55	Lock Input Exception Alarm
MINOR_DOORCONTACT_INPUT_SHORT_CIRCUIT	0x56	Contact Input Short Circuit Attempts Alarm
MINOR_DOORCONTACT_INPUT_BROKEN_CIRCUIT	0x57	Contact Input Open Circuit Attempts Alarm
MINOR_DOORCONTACT_INPUT_EXCEPTION	0x58	Contact Input Exception Alarm
MINOR_OPENBUTTON_INPUT_SHORT_CIRCUIT	0x59	Exit Button Input Short Circuit Attempts Alarm
MINOR_OPENBUTTON_INPUT_BROKEN_CIRCUIT	0x5a	Exit Button Input Open Circuit Attempts Alarm
MINOR_OPENBUTTON_INPUT_EXCEPTION	0x5b	Exit Button Input Exception Alarm
MINOR_DOORLOCK_OPEN_EXCEPTION	0x5c	Unlocking Exception

Event Minor Types	Value	Description
MINOR_DOORLOCK_OPEN_TIMEOUT	0x5d	Unlocking Timed Out
MINOR_FIRSTCARD_OPEN_WITHOUT_AUTHORIZE	0x5e	Unauthorized First Card Opening Failed
MINOR_CALL_LADDER_RELAY_BREAK	0x5f	Call Elevator Relay Open
MINOR_CALL_LADDER_RELAY_CLOSE	0x60	Call Elevator Relay Closed
MINOR_AUTO_KEY_RELAY_BREAK	0x61	Auto Button Relay Open
MINOR_AUTO_KEY_RELAY_CLOSE	0x62	Auto Button Relay Closed
MINOR_KEY_CONTROL_RELAY_BREAK	0x63	Button Relay Open
MINOR_KEY_CONTROL_RELAY_CLOSE	0x64	Button Relay Closed
MINOR_EMPLOYEEENO_AND_PW_PASS	0x65	Employee ID and Password Authentication Completed
MINOR_EMPLOYEEENO_AND_PW_FAIL	0x66	Employee ID and Password Authentication Failed
MINOR_EMPLOYEEENO_AND_PW_TIMEOUT	0x67	Employee ID and Password Authentication Timed Out
MINOR_HUMAN_DETECT_FAIL	0x68	Human Detection Failed
MINOR_PEOPLE_AND_ID_CARD_COMPARE_PASS	0x69	Person and ID Card Matched
MINOR_PEOPLE_AND_ID_CARD_COMPARE_FAIL	0x70	Person and ID Card Mismatched
MINOR_CERTIFICATE_BLOCKLIST	0x71	Blocklist Event
MINOR_LEGAL_MESSAGE	0x72	Valid Message
MINOR_ILLEGAL_MESSAGE	0x73	Invalid Message

Event Minor Types	Value	Description
MINOR_DOOR_OPEN_OR_DORMANT_FAIL	0x75	Authentication Failed: Door Remain Closed or Door in Sleeping Mode
MINOR_AUTH_PLAN_DORMANT_FAIL	0x76	Authentication Failed: Authentication Schedule in Sleeping Mode
MINOR_CARD_ENCRYPT_VERIFY_FAIL	0x77	Card Encryption Verification Failed
MINOR_SUBMARINEBACK_REPLY_FAIL	0x78	Anti-passing Back Server Response Failed
MINOR_DOOR_OPEN_OR_DORMANT_OPEN_FAIL	0x82	Open Door via Exit Button Failed When Door Remain Closed or in Sleeping Mode
MINOR_DOOR_OPEN_OR_DORMANT_LINKAGE_OPEN_FAIL	0x84	Door Linkage Open Failed During Door Remain Close or Sleeping
MINOR_TRAILING	0x85	Tailgating
MINOR_REVERSE_ACCESS	0x86	Reverse Passing
MINOR_FORCE_ACCESS	0x87	Force Accessing
MINOR_CLIMBING_OVER_GATE	0x88	Climb Over
MINOR_PASSING_TIMEOUT	0x89	Passing Timed Out
MINOR_INTRUSION_ALARM	0x8a	Intrusion Alarm
MINOR_FREE_GATE_PASS_NOT_AUTH	0x8b	Authentication Failed When Free Passing
MINOR_DROP_ARM_BLOCK	0x8c	Barrier Obstructed
MINOR_DROP_ARM_BLOCK_RESUME	0x8d	Barrier Restored
MINOR_PASSWORD_MISMATCH	0x97	Passwords Mismatched
MINOR_EMPLOYEE_NO_NOT_EXIST	0x98	Employee ID Not Exists

Event Minor Types	Value	Description
MINOR_COMBINED_VERIFY_PASS	0x99	Combined Authentication Completed
MINOR_COMBINED_VERIFY_TIMEOUT	0x9a	Combined Authentication Timed Out
MINOR_VERIFY_MODE_MISMATCH	0x9b	Authentication Type Mismatched
MINOR_BLUETOOTH_VERIFY_PASS	0x9f	Authenticated via Bluetooth
MINOR_BLUETOOTH_VERIFY_FAIL	0xa0	Authentication via Bluetooth Failed
MINOR_INFORMAL_MIFARE_CARD_VERIFY_FAIL	0xa2	Authentication Failed: Invalid Mifare Card
MINOR_CPU_CARD_ENCRYPT_VERIFY_FAIL	0xa3	Verifying CPU Card Encryption Failed
MINOR_NFC_DISABLE_VERIFY_FAIL	0xa4	Disabling NFC Verification Failed
MINOR_EM_CARD_RECOGNIZE_NOT_ENABLED	0xa8	EM Card Recognition Disabled
MINOR_M1_CARD_RECOGNIZE_NOT_ENABLED	0xa9	M1 Card Recognition Disabled
MINOR_CPU_CARD_RECOGNIZE_NOT_ENABLED	0xaa	CPU Card Recognition Disabled
MINOR_ID_CARD_RECOGNIZE_NOT_ENABLED	0xab	ID Card Recognition Disabled
MINOR_CARD_SET_SECRET_KEY_FAIL	0xac	Importing Key to Card Failed
MINOR_LOCAL_UPGRADE_FAIL	0xad	Local Upgrade Failed
MINOR_REMOTE_UPGRADE_FAIL	0xae	Remote Upgrade Failed
MINOR_REMOTE_EXTEND_MODULE_UPGRADE_SUCC	0xaf	Extension Module is Remotely Upgraded
MINOR_REMOTE_EXTEND_MODULE_UPGRADE_FAIL	0xb0	Upgrading Extension Module Remotely Failed

Event Minor Types	Value	Description
MINOR_REMOTE_FINGER_PRINT_MODULE_UPGRADE_SUCC	0xb1	Fingerprint Module is Remotely Upgraded
MINOR_REMOTE_FINGER_PRINT_MODULE_UPGRADE_FAIL	0xb2	Upgrading Fingerprint Module Remotely Failed
MINOR_DYNAMICCODE_VERIFY_PASS	0xb3	Dynamic Verification Code Authenticated
MINOR_DYNAMICCODE_VERIFY_FAIL	0xb4	Authentication with Verification Code Failed
MINOR_PASSWD_VERIFY_PASS	0xb5	Password Authenticated
MINOR_FULL_STAFF	0xc1	Number of People Exceeds 90% of Capacity
MINOR_BLUETOOTH_KEY_VERIFY_FAIL	/	Verifying Bluetooth Key Failed
MINOR_EVENT_CUSTOM1 to MINOR_EVENT_CUSTOM64	0x500 to 0x53f	Access Control: Custom Event 1 to Custom Event 64

B.3 Event Linkage Types

For event card linkages, if the linkage type is event, four major event linkage types are available: 0-device event linkage, 1-alarm input event linkage, 2-access control point (e.g., doors, elevators, etc.) event linkage, and 3-authentication unit (e.g., card reader, fingerprint module, etc.) event linkage. Each major event linkage type corresponds multiple minor types of event linkage, see details in the following content.

Device Event Linkage

Minor Type	Value	Description
EVENT_ACS_HOST_ANTI_DISMANTLE	0	Access Controller Tampering Alarm
EVENT_ACS_OFFLINE_ECENT_NEARLY_FULL	1	No Memory Alarm
EVENT_ACS_NET_BROKEN	2	Network Disconnected

Minor Type	Value	Description
EVENT_ACS_NET_RESUME	3	Network Connected
EVENT_ACS_LOW_BATTERY	4	Low Battery Voltage
EVENT_ACS_BATTERY_RESUME	5	Battery Fully Charged
EVENT_ACS_AC_OFF	6	AC Power Off
EVENT_ACS_AC_RESUME	7	AC Power On
EVENT_ACS_SD_CARD_FULL	8	SD Card Full Alarm
EVENT_ACS_LINKAGE_CAPTURE_PIC	9	Capture Linkage Event Alarm
EVENT_ACS_IMAGE_QUALITY_LOW	10	Low Face Picture Quality
EVENT_ACS_FINGER_PRINT_QUALITY_LOW	11	Low Fingerprint Picture Quality
EVENT_ACS_BATTERY_ELECTRIC_LOW	12	Low Battery Voltage
EVENT_ACS_BATTERY_ELECTRIC_RESUME	13	Battery Fully Charged
EVENT_ACS_FIRE_IMPORT_SHORT_CIRCUIT	14	Fire Input Short Circuit Attempts Alarm
EVENT_ACS_FIRE_IMPORT_BROKEN_CIRCUIT	15	Fire Input Open Circuit Attempts Alarm
EVENT_ACS_FIRE_IMPORT_RESUME	16	Fire Input Alarm Restored
EVENT_ACS_MASTER_RS485_LOOPNODE_BROKEN	17	RS485 Loop of Main Access Controller Disconnected
EVENT_ACS_MASTER_RS485_LOOPNODE_RESUME	18	RS485 Loop of Main Access Controller Connected
EVENT_ACS_LOCAL_CONTROL_OFFLINE	19	Distributed Access Controller Offline
EVENT_ACS_LOCAL_CONTROL_RESUME	20	Distributed Access Controller Online

Minor Type	Value	Description
EVENT_ACS_LOCAL_DOWNSIDE_RS485_LOOPNODE_BROKEN	21	Downstream RS485 Loop of Distributed Access Control Disconnected
EVENT_ACS_LOCAL_DOWNSIDE_RS485_LOOPNODE_RESUME	22	Downstream RS485 Loop of Distributed Access Control Connected
EVENT_ACS_DISTRACT_CONTROLLER_ONLINE	23	Distributed Elevator Controller Online
EVENT_ACS_DISTRACT_CONTROLLER_OFFLINE	24	Distributed Elevator Controller Offline
EVENT_ACS_FIRE_BUTTON_TRIGGER	25	Fire Button Pressed
EVENT_ACS_FIRE_BUTTON_RESUME	26	Fire Button Released
EVENT_ACS_MAINTENANCE_BUTTON_TRIGGER	27	Maintenance Button Pressed
EVENT_ACS_MAINTENANCE_BUTTON_RESUME	28	Maintenance Button Released
EVENT_ACS_EMERGENCY_BUTTON_TRIGGER	29	Panic Button Pressed
EVENT_ACS_EMERGENCY_BUTTON_RESUME	30	Panic Button Released
EVENT_ACS_SUBMARINEBACK_COMM_BREAK	32	Communication with Anti-passing Back Server Failed
EVENT_ACS_SUBMARINEBACK_COMM_RESUME	33	Communication with Anti-passing Back Server Restored
EVENT_ACS_REMOTE_ACTUAL_GUARD	34	Remotely Armed
EVENT_ACS_REMOTE_ACTUAL_UNGUARD	35	Remotely Disarmed
EVENT_ACS_MOTOR_SENSOR_EXCEPTION	36	Motor or Sensor Exception

Minor Type	Value	Description
EVENT_ACS_CAN_BUS_EXCEPTION	37	CAN Bus Exception
EVENT_ACS_CAN_BUS_RESUME	38	CAN Bus Restored
EVENT_ACS_GATE_TEMPERATURE_OVERRUN	39	Too High Pedestal Temperature
EVENT_ACS_IR_EMITTER_EXCEPTION	40	Active Infrared Intrusion Detector Exception
EVENT_ACS_IR_EMITTER_RESUME	41	Active Infrared Intrusion Detector Restored
EVENT_ACS_LAMP_BOARD_COMM_EXCEPTION	42	Communication with Light Board Failed
EVENT_ACS_LAMP_BOARD_COMM_RESUME	43	Communication with Light Board Restored
EVENT_ACS_IR_ADAPTOR_BOARD_COMM_EXCEPTION	44	Communication with IR Adaptor Failed
EVENT_ACS_IR_ADAPTOR_BOARD_COMM_RESUME	45	Communication with IR Adaptor Restored
EVENT_ACS_CHANNEL_CONTROLLER_DESMANTLE_ALARM	46	Lane Controller Tampering Alarm
EVENT_ACS_CHANNEL_CONTROLLER_DESMANTLE_RESUME	47	Lane Controller Tampering Alarm Restored
EVENT_ACS_CHANNEL_CONTROLLER_FIRE_IMPORT_ALARM	48	Lane Controller Fire Input Alarm
EVENT_ACS_CHANNEL_CONTROLLER_FIRE_IMPORT_RESUME	49	Lane Controller Fire Input Alarm Restored
EVENT_ACS_STAY_EVENT	/	Staying Event
EVENT_ACS_LEGAL_EVENT_NEARLY_FULL	/	No Memory Alarm for Valid Offline Event Storage

Alarm Input Event Linkage

Minor Type	Value	Description
EVENT_ACS_ALARMIN_SHORT_CIRCUIT	0	Zone Short Circuit Attempts Alarm
EVENT_ACS_ALARMIN_BROKEN_CIRCUIT	1	Zone Open Circuit Attempts Alarm
EVENT_ACS_ALARMIN_EXCEPTION	2	Zone Exception Alarm
EVENT_ACS_ALARMIN_RESUME	3	Zone Alarm Restored
EVENT_ACS_CASE_SENSOR_ALARM	4	Alarm Input Alarm
EVENT_ACS_CASE_SENSOR_RESUME	5	Alarm Input Alarm Restored

Access Control Point Event Linkage

Minor Type	Value	Description
EVENT_ACS_LEADER_CARD_OPEN_BEGIN	0	Open Door with First Card Started
EVENT_ACS_LEADER_CARD_OPEN_END	1	Open Door with First Card Ended
EVENT_ACS_ALWAYS_OPEN_BEGIN	2	Remain Open Started
EVENT_ACS_ALWAYS_OPEN_END	3	Remain Open Ended
EVENT_ACS_ALWAYS_CLOSE_BEGIN	4	Remain Closed Started
EVENT_ACS_ALWAYS_CLOSE_END	5	Remain Closed Ended
EVENT_ACS_LOCK_OPEN	6	Door Unlocked
EVENT_ACS_LOCK_CLOSE	7	Door Locked
EVENT_ACS_DOOR_BUTTON_PRESS	8	Exit Button Pressed

Minor Type	Value	Description
EVENT_ACS_DOOR_BUTTON_RELEASE	9	Exit Button Released
EVENT_ACS_DOOR_OPEN_NORMAL	10	Door Open (Contact)
EVENT_ACS_DOOR_CLOSE_NORMAL	11	Door Closed (Contact)
EVENT_ACS_DOOR_OPEN_ANORMAL	12	Door Abnormally Open (Contact)
EVENT_ACS_DOOR_OPEN_TIMEOUT	13	Door Open Timed Out (Contact)
EVENT_ACS_REMOTE_OPEN_DOOR	14	Door Remotely Open
EVENT_ACS_REMOTE_CLOSE_DOOR	15	Door Remotely Closed
EVENT_ACS_REMOTE_ALWAYS_OPEN	16	Remain Open Remotely
EVENT_ACS_REMOTE_ALWAYS_CLOSE	17	Remain Closed Remotely
EVENT_ACS_NOT_BELONG_MULTI_GROUP	18	Card Not in Multiple Authentication Group
EVENT_ACS_INVALID_MULTI_VERIFY_PERIOD	19	Card Not in Multiple Authentication Duration
EVENT_ACS_MULTI_VERIFY_SUPER_RIGHT_FAIL	20	Multiple Authentication Mode: Super Password Authentication Failed
EVENT_ACS_MULTI_VERIFY_REMOTE_RIGHT_FAIL	21	Multiple Authentication Mode: Remote Authentication Failed
EVENT_ACS_MULTI_VERIFY_SUCCESS	22	Multiple Authentication Completed
EVENT_ACS_MULTI_VERIFY_NEED_REMOTE_OPEN	23	Multiple Authentication: Remotely Open Door
EVENT_ACS_MULTI_VERIFY_SUPERPASSWD_VERIFY_SUCCESS	24	Multiple Authentication: Super Password Authentication Completed

Minor Type	Value	Description
EVENT_ACS_MULTI_VERIFY_REPEAT_VERIFY_FAIL	25	Multiple Authentication: Repeated Authentication Failed
EVENT_ACS_MULTI_VERIFY_TIMEOUT	26	Multiple Authentication Timed Out
EVENT_ACS_REMOTE_CAPTURE_PIC	27	Remote Capture
EVENT_ACS_DOORBELL_RINGING	28	Doorbell Ring
EVENT_ACS_SECURITY_MODULE_DESMANTLE_ALARM	29	Secure Door Control Unit Tampering Alarm
EVENT_ACS_CALL_CENTER	30	Center Event
EVENT_ACS_FIRSTCARD_AUTHORIZE_BEGIN	31	First Card Authentication Started
EVENT_ACS_FIRSTCARD_AUTHORIZE_END	32	First Card Authentication End
EVENT_ACS_DOORLOCK_INPUT_SHORT_CIRCUIT	33	Lock Input Short Circuit Attempts Alarm
EVENT_ACS_DOORLOCK_INPUT_BROKEN_CIRCUIT	34	Lock Input Open Circuit Attempts Alarm
EVENT_ACS_DOORLOCK_INPUT_EXCEPTION	35	Lock Input Exception Alarm
EVENT_ACS_DOORCONTACT_INPUT_SHORT_CIRCUIT	36	Contact Input Short Circuit Attempts Alarm
EVENT_ACS_DOORCONTACT_INPUT_BROKEN_CIRCUIT	37	Contact Input Open Circuit Attempts Alarm
EVENT_ACS_DOORCONTACT_INPUT_EXCEPTION	38	Contact Input Exception Alarm
EVENT_ACS_OPENBUTTON_INPUT_SHORT_CIRCUIT	39	Exit Button Input Short Circuit Attempts Alarm
EVENT_ACS_OPENBUTTON_INPUT_BROKEN_CIRCUIT	40	Exit Button Input Open Circuit Attempts Alarm
EVENT_ACS_OPENBUTTON_INPUT_EXCEPTION	41	Exit Button Input Exception Alarm

Minor Type	Value	Description
EVENT_ACS_DOORLOCK_OPEN_EXCEPTION	42	Unlocking Exception
EVENT_ACS_DOORLOCK_OPEN_TIMEOUT	43	Unlocking Timed Out
EVENT_ACS_FIRSTCARD_OPEN_WITHOUT_AUTHORIZE	44	Unauthorized First Card Opening Failed
EVENT_ACS_CALL_LADDER_RELAY_BREAK	45	Call Elevator Relay Open
EVENT_ACS_CALL_LADDER_RELAY_CLOSE	46	Call Elevator Relay Closed
EVENT_ACS_AUTO_KEY_RELAY_BREAK	47	Auto Button Relay Open
EVENT_ACS_AUTO_KEY_RELAY_CLOSE	48	Auto Button Relay Closed
EVENT_ACS_KEY_CONTROL_RELAY_BREAK	49	Button Relay Open
EVENT_ACS_KEY_CONTROL_RELAY_CLOSE	50	Button Relay Closed
EVENT_ACS_REMOTE_VISITOR_CALL_LADDER	51	Visitor Calling Elevator
EVENT_ACS_REMOTE_HOUSEHOLD_CALL_LADDER	52	Resident Calling Elevator
EVENT_ACS_LEGAL_MESSAGE	52	Valid Message
EVENT_ACS_ILLEGAL_MESSAGE	53	Invalid Message
EVENT_ACS_TRAILING	54	Tailgating
EVENT_ACS_REVERSE_ACCESS	55	Reverse Passing
EVENT_ACS_FORCE_ACCESS	56	Force Collision
EVENT_ACS_CLIMBING_OVER_GATE	57	Climbing Over
EVENT_ACS_PASSING_TIMEOUT	58	Passing Timed Out

Minor Type	Value	Description
EVENT_ACS_INTRUSION_ALARM	59	Intrusion Alarm
EVENT_ACS_FREE_GATE_PASS_NOT_AUTH	60	Authentication Failed When Free Passing
EVENT_ACS_DROP_ARM_BLOCK	61	Barrier Obstructed
EVENT_ACS_DROP_ARM_BLOCK_RESUME	62	Barrier Restored
EVENT_ACS_REMOTE_CONTROL_CLOSE_DOOR	63	Door Closed via Keyfob
EVENT_ACS_REMOTE_CONTROL_OPEN_DOOR	64	Door Opened via Keyfob
EVENT_ACS_REMOTE_CONTROL_ALWAYS_OPEN_DOOR	65	Remain Open via Keyfob

Authentication Unit Event Linkage

Minor Type	Value	Description
EVENT_ACS_STRESS_ALARM	0	Duress Alarm
EVENT_ACS_CARD_READER_DESMANTLE_ALARM	1	Card Reader Tampering Alarm
EVENT_ACS_LEGAL_CARD_PASS	2	Valid Card Authentication Completed
EVENT_ACS_CARD_AND_PSW_PASS	3	Card and Password Authentication Completed
EVENT_ACS_CARD_AND_PSW_FAIL	4	Card and Password Authentication Failed
EVENT_ACS_CARD_AND_PSW_TIMEOUT	5	Card and Password Authentication Timed Out
EVENT_ACS_CARD_MAX_AUTHENTICATE_FAIL	6	Card Authentication Attempts Reach Limit
EVENT_ACS_CARD_NO_RIGHT	7	No Permission for Card

Minor Type	Value	Description
EVENT_ACS_CARD_INVALID_PERIOD	8	Invalid Card Swiping Time Period
EVENT_ACS_CARD_OUT_OF_DATE	9	Expired Card
EVENT_ACS_INVALID_CARD	10	Card No. Not Exist
EVENT_ACS_ANTI_SNEAK_FAIL	11	Anti-passing Back Authentication Failed
EVENT_ACS_INTERLOCK_DOOR_NOT_CLOSE	12	Interlocking Door Not Closed
EVENT_ACS_FINGERPRINT_COMPARE_PASS	13	Fingerprint Matched
EVENT_ACS_FINGERPRINT_COMPARE_FAIL	14	Fingerprint Mismatched
EVENT_ACS_CARD_FINGERPRINT_VERIFY_PASS	15	Card and Fingerprint Authentication Completed
EVENT_ACS_CARD_FINGERPRINT_VERIFY_FAIL	16	Card and Fingerprint Authentication Failed
EVENT_ACS_CARD_FINGERPRINT_VERIFY_TIMEOUT	17	Card and Fingerprint Authentication Timed Out
EVENT_ACS_CARD_FINGERPRINT_PASSWD_VERIFY_PASS	18	Card, Fingerprint, and Password Authentication Completed
EVENT_ACS_CARD_FINGERPRINT_PASSWD_VERIFY_FAIL	19	Card and Fingerprint Authentication Failed
EVENT_ACS_CARD_FINGERPRINT_PASSWD_VERIFY_TIMEOUT	20	Card and Fingerprint Authentication Timed Out
EVENT_ACS_FINGERPRINT_PASSWD_VERIFY_PASS	21	Fingerprint and Password Authentication Completed
EVENT_ACS_FINGERPRINT_PASSWD_VERIFY_FAIL	22	Fingerprint and Password Authentication Failed

Minor Type	Value	Description
EVENT_ACS_FINGERPRINT_PASSWD_VERIFY_TIMEOUT	23	Fingerprint and Password Authentication Timed Out
EVENT_ACS_FINGERPRINT_INEXISTENCE	24	Fingerprint Not Exist
EVENT_ACS_EMPLOYEEENO_AND_FP_VERIFY_PASS	42	Employee ID and Fingerprint Authentication Completed
EVENT_ACS_EMPLOYEEENO_AND_FP_VERIFY_FAIL	43	Employee ID and Fingerprint Authentication Failed
EVENT_ACS_EMPLOYEEENO_AND_FP_VERIFY_TIMEOUT	44	Employee ID and Fingerprint Authentication Timed Out
EVENT_ACS_EMPLOYEEENO_AND_FP_AND_PW_VERIFY_PASS	45	Employee ID, Fingerprint, and Password Authentication Completed
EVENT_ACS_EMPLOYEEENO_AND_FP_AND_PW_VERIFY_FAIL	46	Employee ID, Fingerprint, and Password Authentication Failed
EVENT_ACS_EMPLOYEEENO_AND_FP_AND_PW_VERIFY_TIMEOUT	47	Employee ID, Fingerprint, and Password Authentication Timed Out
EVENT_ACS_EMPLOYEEENO_AND_PW_PASS	52	Employee ID and Password Authentication Completed
EVENT_ACS_EMPLOYEEENO_AND_PW_FAIL	52	Employee ID and Password Authentication Failed
EVENT_ACS_EMPLOYEEENO_AND_PW_TIMEOUT	53	Employee ID and Password Authentication Timed Out
EVENT_ACS_DOOR_OPEN_OR_DORMANT_FAIL	57	Authentication Failed When Door Remain Closed or Door in Sleeping Mode
EVENT_ACS_AUTH_PLAN_DORMANT_FAIL	58	Authentication Failed When Authentication Schedule in Sleeping Mode
EVENT_ACS_CARD_ENCRYPT_VERIFY_FAIL	59	Card Encryption Verification Failed

Minor Type	Value	Description
EVENT_ACS_SUBMARINEBACK_REPLY_FAIL	60	Anti-passing Back Server Response Failed
EVENT_ACS_PASSWORD_MISMATCH	61	Password Mismatched
EVENT_ACS_EMPLOYEE_NO_NOT_EXIST	62	Employee ID Not Exist
EVENT_ACS_COMBINED_VERIFY_PASS	63	Combined Authentication Completed
EVENT_ACS_COMBINED_VERIFY_TIMEOUT	64	Combined Authentication Timed Out
EVENT_ACS_VERIFY_MODE_MISMATCH	65	Authentication Type Mismatched
EVENT_ACS_PSW_ERROR_OVER_TIMES	67	Maximum Password Authentication Failure Attempts
EVENT_ACS_PSW_VERIFY_PASS	68	Password Authenticated
EVENT_ACS_PSW_VERIFY_FAIL	69	Password Authentication Failed
EVENT_ACS_ORCODE_VERIFY_PASS	70	QR Code Authenticated
EVENT_ACS_ORCODE_VERIFY_FAIL	71	QR Code Authentication Failed
EVENT_ACS_HOUSEHOLDER_AUTHORIZE_PASS	72	Resident Authorization Authenticated
EVENT_ACS_BLUETOOTH_VERIFY_PASS	73	Bluetooth Authenticated
EVENT_ACS_BLUETOOTH_VERIFY_FAIL	74	Bluetooth Authentication Failed
EVENT_ACS_INFORMAL_MIFARE_CARD_VERIFY_FAIL	/	Authentication Failed: Invalid Mifare Card
EVENT_ACS_CPU_CARD_ENCRYPT_VERIFY_FAIL	/	Verifying CPU Card Encryption Failed
EVENT_ACS_NFC_DISABLE_VERIFY_FAIL	/	Disabling NFC Verification Failed

Minor Type	Value	Description
EVENT_ACS_EM_CARD_RECOGNIZE_NOT_ENABLED	/	EM Card Recognition Disabled
EVENT_ACS_M1_CARD_RECOGNIZE_NOT_ENABLED	/	M1 Card Recognition Disabled
EVENT_ACS_CPU_CARD_RECOGNIZE_NOT_ENABLED	/	CPU Card Recognition Disabled
EVENT_ACS_ID_CARD_RECOGNIZE_NOT_ENABLED	/	ID Card Recognition Disabled
EVENT_ACS_CARD_SET_SECRET_KEY_FAIL	/	Importing Key to Card Failed

B.4 Log Types for ISAPI

There are four major log types, i.e., alarm log, exception log, operation log, event log, and information log. And each major type contains multiple minor types, see details in the following contents.

Alarm Logs

Log Type	Description
shortCircuit	Short Circuit Alarm
dataPrealarm	Data warning
vehicleMonitor	Vehicle arming alarm
peopleCounting	People counting alarm
framesPeopleCounting	Regional people counting alarm
brokenCircuit	Open Circuit Alarm
alarmReset	Alarm Reset
alarmNormal	Return to Normal
passwordError	Incorrect Password (3 Times in a Row)
idCardIllegally	Invalid Card ID
keyPADRemove	Keypad Tampered
keyPADRemoveRestore	Keypad Restored

Log Type	Description
devRemove	Device Tampered
devRemoveRestore	Device Restored
belowAlarmLimit1	Sensor Value is Lower than Alarm Limit Value 1
belowAlarmLimit2	Sensor Value is Lower than Alarm Limit Value 2
belowAlarmLimit3	Sensor Value is Lower than Alarm Limit Value 3
belowAlarmLimit4	Sensor Value is Lower than Alarm Limit Value 4
aboveAlarmLimit1	Sensor Value is Higher than Alarm Limit Value 1
aboveAlarmLimit2	Sensor Value is Higher than Alarm Limit Value 2
aboveAlarmLimit3	Sensor Value is Higher than Alarm Limit Value 3
aboveAlarmLimit4	Sensor Value is Higher than Alarm Limit Value 4
UrgencyBtnON	Panic Button Triggered
UrgencyBtnOFF	Panic Button Restored
virtualDefenceBandit	Virtual Zone Burglary Alarm
virtualDefenceFire	Virtual Zone Fire Alarm
virtualDefenceUrgent	Virtual Zone Panic Alarm
motDetStart	Motion Detection Alarm Started
motDetStop	Motion Detection Alarm Stopped
hideAlarmStart	Device Blocked
hideAlarmStop	Device Blocking Alarm Restored
UPSAlarm	UPS Alarm
electricityMeterAlarm	Coulombmeter Alarm
switchPowerAlarm	Switch Power Supply Alarm
GasDetectSys	Gas Detection Alarm
transformerTempAlarm	Transformer Temperature Alarm
tempHumiAlarm	Temperature and Humidity Sensor Alarm
UPSAlarmRestore	UPS Alarm Restored
electricityMeterAlarmRestore	Coulombmeter Alarm Restored
switchPowerAlarmRestore	Switch Power Supply Alarm Restored

Log Type	Description
GasDetectSysRestore	Gas Detection Alarm Restored
transformerTempAlarmRestore	Transformer Temperature Alarm Restored
tempHumiAlarmRestore	Temperature-Humidity Sensor Alarm Restored
waterLevelSensorAlarm	Temperature-Humidity Sensor Alarm Restored
waterLevelSensorAlarmRestore	Flood Sensor Restored
dustNoiseAlarm	Dust and Noise Sensor Alarm
dustNoiseAlarmRestore	Dust and Noise Sensor Alarm Restored
environmentalLogger	Environmental Data Collector Alarm
environmentalLoggerAlarm	Environmental Data Collector Restored
triggerTemper	Detector Tampered
triggerTemperRestore	Detector Restored
emergencyCallHelp	Panic Alarm
emergencyCallHelpRestore	Panic Alarm Restored
consult	Consultation Alarm
consultRestore	Consultation Alarm Restored
deviceMoveAlarm	Device Motion Alarm
deviceMoveAlarmRestore	Device Motion Alarm Restored
earlyWarningAlarm	Early Warning Zone Alarm
earlyWarningAlarmRestore	Early Warning Zone Restored
warningAlarm	Warning Zone Alarm
warningAlarmRestore	Warning Zone Restored
wirelessOutputModTamperEvident	Wireless Output Expander Tampered
wirelessOutputModTamperEvidentReset	Wireless Output Expander tamper Restored
wirelessRepeaterTamperEvident	Wireless Repeater Tampered
wirelessRepeaterTamperEvidentReset	Wireless Repeater tamper Restored
wirelessSirenTamperEvident	Wireless Siren Tampered
wirelessSirenTamperEvidentReset	Wireless Siren Tamper Restored
wirelessKeypadTamperEvident	Wireless Keypad Tampered

Log Type	Description
wirelessKeypadTamperEvidentReset	Wireless Keypad Tamper Restored
wirelessCardReaderTamperEvident	Wireless Card Reader Tampered
wirelessCardReaderTamperEvidentReset	Wireless Card Reader Tamper Restored
softZoneMedicalAlarm	Virtual Zone Medical Alarm
accessControllerEvent	Access Controller Event
videoIntercomEvent	Video Intercom Event
GJDEvent	GJD Security Control Panel Event
LuminateEvent	LUMINITE Security Control Panel Event
OPTEXEvent	OPTEX Security Control Panel Event
cameraDetectorEvent	Detector Event
securityControlPanelEvent	Security Control Panel Event
RS-485AlarmInputModuleEvident	RS-485 Zone Module Tampered
RS-485AlarmInputModuleTamperReset	RS-485 Zone Module Tampering Reset
RS-485WirelessReceiverTamperEvident	RS-485 Wireless Receiver Module Tampered
RS-485WirelessReceiverTamperEvidentReset	RS-485 Wireless Receiver Module Tampering Reset
dredgerDetectionAlarm	Dredger Detection Alarm
crossLineAlarm	Line Crossing Alarm
crossLineAlarmRestore	Line Crossing Alarm Restored
HFPDAckStart	High Frequently Appeared Person Alarm Started
HFPDAckStop	High Frequently Appeared Person Alarm Stopped
LFPDAckStart	Low Frequency Person Alarm Started
LFPDAckStop	Low Frequency Person Alarm Stopped
safetyHelmetAckStart	Hard Hat Detection Alarm Started
safetyHelmetAckStop	Hard Hat Detection Alarm Stopped
dataPrealarm	Traffic Pre-alarm
playCellphoneStart	Playing Cellphone Alarm Started
playCellphoneStop	Playing Cellphone Alarm Stopped

Log Type	Description
sleepOnDutyStart	Sleeping on Duty Alarm Started
sleepOnDutyStop	Sleeping on Duty Alarm Stopped
vibrationDetectionStart	Vibration Detection Alarm Started
vibrationDetectionStop	Vibration Detection Alarm Stopped
fireEscapeDetectionStart	Fire Engine Access Detection Started
fireEscapeDetectionStop	Fire Engine Access Detection Ended
takingElevatorDetectionStart	Elevator Detection Started
takingElevatorDetectionStop	Elevator Detection Ended
unregisteredStreetVendorStart	Unlicensed Business Vendor Detection Started
unregisteredStreetVendorStop	Unlicensed Business Vendor Detection Ended
stallOutsideShopStart	Business Outside Store Detection Started
stallOutsideShopStop	Business Outside Store Detection Ended
stallOccupyingRoadStart	Business on Sidewalk Detection Started
stallOccupyingRoadStop	Business on Sidewalk Detection Ended
illegalHeapStart	Pile Goods or Materials in Chaos Detection Started
illegalHeapStop	Pile Goods or Materials in Chaos Detection Ended
illParkofNonMotorVehicleStart	Non-Motor Vehicles Parking in Chaos Detection Started
illParkofNonMotorVehicleStop	Non-Motor Vehicles Parking in Chaos Detection Ended
illegalOutdoorAdvertisementStart	Unauthorized Outdoor Advertisement Detection Started
illegalOutdoorAdvertisementStop	Unauthorized Outdoor Advertisement Detection Ended
packGarbageStart	Packaged Garbage Detection Started
packGarbageStop	Packaged Garbage Detection Ended
stallUnderUmbrellaStart	Running Business with Patio Umbrella Detection Started
stallUnderUmbrellaStop	Running Business with Patio Umbrella Detection Ended

Log Type	Description
dustbinOverflowStart	Overflowing Dustbin Detection Started
dustbinOverflowStop	Overflowing Dustbin Detection Ended
exposeGarbageStart	Exposed Garbage Detection Started
exposeGarbageStop	Exposed Garbage Detection Ended
hangClothingAlongStreetStart	Hanging Clothes On Street Detection Started
hangClothingAlongStreetStop	Hanging Clothes On Street Detection Ended
ATMPanelStart	ATM Panel Alarm Started
ATMPanelStop	ATM Panel Alarm Ended
ATMSurroundStart	ATM Surround Alarm Started
ATMSurroundStop	ATM Surround Alarm Ended
ATMFaceStart	ATM Face Alarm Started
ATMFaceStop	ATM Face Alarm Ended
ATMSafetyCabinStart	ATM Safety Cabin Alarm Started
ATMSafetyCabinStop	ATM Safety Cabin Alarm Ended
soundIntensityMutation	Sudden Increase of Sound Intensity Detection
soundIntensityMutationStop	Sudden Increase of Sound Intensity Detection Ended
soundIntensitySteepFall	Sudden Decrease of Sound Intensity Detection
soundIntensitySteepFallStop	Sudden Decrease of Sound Intensity Detection Ended
moveAlarm	Motion Alarm
moveAlarmRestored	Motion Alarm Restored
lowTemperatureAlarm	Low Temperature Alarm
lowTemperatureAlarmRestored	Low Temperature Alarm Restored
highTemperatureAlarm	High Temperature Alarm
highTemperatureAlarmRestored	High Temperature Alarm Restored
TemperatureIntervalMeasurementStart	Interval Temperature Measurement Started
TemperatureIntervalMeasurementStop	Interval Temperature Measurement Stopped
laneOccupationbyMotorVehicleStart	Lane Occupation by Motor Vehicle Detection Started
humanBodyStart	Mass Incident Detection Started

Log Type	Description
hangingOutdoorBannerStart	Hanging Banner Outdoors Detection Started
illegalAdvertisementStart	Illegal Advertisement Detection Started
illegalAdvertisementBannerStart	Illegal Advertisement Banner Detection Started
dirtyWaterbodyStart	Dirty Waters Detection Started
puttingTemporaryShelterIllegallyStart	Illegally Putting Temporary Shelter Detection Started
dirtyRoadStart	Dirty Road Detection Started
heapingWasteIllegallyStart	Illegally Heaping Waste Detection Started
stagnantRoadStart	Stagnant Road Detection Started
burningRubbishandLeavesStart	Burning Garbage and Leaves Detection Started
destroyingandOccupyingGreenBeltStart	Destroying and Occupying the Green Belt Detection Started
laneOccupationbyConstructionStart	Lane Occupation by Construction Detection Started
improperRubbishBinStart	Improper Dustbin Detection Started
abandonedFurnitureStart	Abandoned Furniture Detection Started
outsideAirConditionerHangingLowStart	Hanging the Air Conditioner Lowly Outside Detection Started
puttingInflatableArchIllegallyStart	Illegally Putting Inflatable Arch Detection Started
roadDamagedStart	Road Damaged Detection Started
constructionMaterialsMisplacedStart	Construction Materials Misplaced Detection Started
settingUpSlopeIllegallyStart	Illegally Setting Up Slope Detection Started
laneOccupationbyWasteRecyclingStart	Lane Occupation by Waste Recycling Detection Started
wasteWaterDischargedonRoadStart	Waste Water Discharged on Road Detection Started
barbecueStallinPublicSitesStart	Barbecue Stall in Public Sites Detection Started
litteringWasteonRoadStart	Littering Waste on Road Detection Started
distributingFlyersinPublicSitesStart	Distributing Flyers in Public Sites Detection Started
roadCollapsedStart	Road Collapsed Detection Started
constructionWasteMisplacedStart	Construction Water Misplaced Detection Started
greeningWasteStart	Greening Waste Detection Started

Log Type	Description
nonDecorativeHangingonTreeStart	Non-Decorative Tree Hangings Detection Started
installingWiresandPipesIllegallyStart	Illegally Installing Wires and Pipes Detection Started
raisingDomesticAnimalsStart	Raising Domestic Animals Detection Started
carcassNotClearedStart	Carcass Not Cleared Detection Started
streetSlaughterStart	Slaughtering Animals Along the Street Detection Started
vagrantsBegginginPublicSitesStart	Vagrant and Beggar in Public Sites Detection Started
dustbinExceptionStart	Dustbin Exception Detection Started
shortcutIsolationPileExceptionStart	Shortcut Isolation Pile Exception Detection Started
laneSeparatorDamagedStart	Lane Separator Damaged Detection Started
antiCollisionBarrelDamagedStart	Anti-Collision Barrel Damaged Detection Started
fireFightingFacilityDamagedStart	Fire Facility Damaged Detection Started
electricPowerFacilityExceptionStart	Power Facility Damaged Detection Started
transformerTankExceptionStart	Transformer Box Exception Detection Started
streetTreeExceptionStart	Street Tree Exception Detection Started
treeProtectionFacilityDamagedStart	Tree-Protection Facility Damaged Detection Started
manholeCoverExceptionStart	Manhole Cover Exception Detection Started
drainGratingDamagedStart	Drain Grating Damaged Detection Started
billboardDamagedStart	Billboard Damaged Detection Started
advertisingSignDamagedStart	Advertising Sign Damaged Detection Started
laneOccupationbyMotorVehicleStop	Lane Occupation by Motor Vehicle Detection Ended
humanBodyStop	Mass Incident Detection Ended
hangingOutdoorBannerStop	Hanging Banner Outdoors Detection Ended
illegalAdvertisementStop	Illegal Advertisement Detection Ended
illegalAdvertisementBannerStop	Illegal Advertisement Banner Detection Ended
dirtyWaterbodyStop	Dirty Waters Detection Ended
puttingTemporaryShelterIllegallyStop	Illegally Putting Temporary Shelter Detection Ended
dirtyRoadStop	Dirty Road Detection Ended

Log Type	Description
heapingWasteIllegallyStop	Illegally Heaping Waste Detection Ended
stagnantRoadStop	Stagnant Road Detection Ended
burningRubbishandLeavesStop	Burning Garbage and Leaves Detection Ended
destroyingandOccupyingGreenBeltStop	Destroying and Occupying the Green Belt Detection Ended
laneOccupationbyConstructionStop	Lane Occupation by Construction Detection Ended
improperRubbishBinStop	Improper Dustbin Detection Ended
abandonedFurnitureStop	Abandoned Furniture Detection Ended
outsideAirConditionerHangingLowStop	Hanging the Air Conditioner Lowly Outside Detection Ended
puttingInflatableArchIllegallyStop	Illegally Putting Inflatable Arch Detection Ended
roadDamagedStop	Road Damaged Detection Ended
constructionMaterialsMisplacedStop	Construction Materials Misplaced Detection Ended
settingUpSlopeIllegallyStop	Illegally Setting Up Slope Detection Ended
laneOccupationbyWasteRecyclingStop	Lane Occupation by Waste Recycling Detection Ended
wasteWaterDischargedonRoadStop	Waste Water Discharged on Road Detection Ended
barbecueStallinPublicSitesStop	Barbecue Stall in Public Sites Detection Ended
litteringWasteonRoadStop	Littering Waste on Road Detection Ended
distributingFlyersinPublicSitesStop	Distributing Flyers in Public Sites Detection Ended
roadCollapsedStop	Road Collapsed Detection Ended
constructionWasteMisplacedStop	Construction Water Misplaced Detection Ended
greeningWasteStop	Greening Waste Detection Ended
nonDecorativeHangingonTreeStop	Non-Decorative Tree Hangings Detection Ended
installingWiresandPipesIllegallyStop	Illegally Installing Wires and Pipes Detection Ended
raisingDomesticAnimalsStop	Raising Domestic Animals Detection Ended
carcassNotClearedStop	Carcass Not Cleared Detection Ended
streetSlaughterStop	Slaughtering Animals Along the Street Detection Ended
vagrantsBegginginPublicSitesStop	Vagrant and Beggar in Public Sites Detection Ended

Log Type	Description
dustbinExceptionStop	Dustbin Exception Detection Ended
shortcutIsolationPileExceptionStop	Shortcut Isolation Pile Exception Detection Ended
laneSeparatorDamagedStop	Lane Separator Damaged Detection Ended
antiCollisionBarrelDamagedStop	Anti-Collision Barrel Damaged Detection Ended
fireFightingFacilityDamagedStop	Fire Facility Damaged Detection Ended
electricPowerFacilityExceptionStop	Power Facility Damaged Detection Ended
transformerTankExceptionStop	Transformer Box Exception Detection Ended
streetTreeExceptionStop	Street Tree Exception Detection Ended
treeProtectionFacilityDamagedStop	Tree-Protection Facility Damaged Detection Ended
manholeCoverExceptionStop	Manhole Cover Exception Detection Ended
drainGratingDamagedStop	Drain Grating Damaged Detection Ended
billboardDamagedStop	Billboard Damaged Detection Ended
advertisingSignDamagedStop	Advertising Sign Damaged Detection Ended
thermalCalibrationFileExceptionStart	Calibration file exception alarm started
thermalCalibrationFileExceptionStop	Calibration file exception alarm ended

Exception Logs

Log Type	Description
powerOn	Power on
powerOff	Power off
AIOPDetResolutionOverflow	Resolution of the detection stream in AI open platform exceeds the limit
HEOPDetResolutionOverflow	Resolution of the detection stream in Hikvision Embedded Open Platform exceeds the limit
WDTReset	WDT Reset
lowBatteryVoltage	Low Battery Voltage
ACLoss	AC Power Disconnected
ACRestore	AC Power Restored

Log Type	Description
RTCException	RTC Real-time Clock Exception
netFailure	Network Disconnected
netRestore	Network Connected
telLineBroken	Telephone Line Disconnected
telLineRestore	Telephone Line Connected
expanderBusLoss	Bus Expander Disconnected
expanderBusRestore	Bus Expander Connected
keypadBusLoss	Keypad Expander Disconnected
keypadBusRestore	Keypad Expander Connected
sensorFailure	Analog Sensor Fault
sensorRestore	Analog Sensor Restored
RS485DisConnect	RS-485 Channel Disconnected
RS485Connect	RS-486 Channel Connected
batteryVoltageRestore	Battery Voltage Restored
wiredNetAbnormal	Wired Network Exception
wiredNetRestore	Wired Network Restored
GPRSAbnormal	GPRS Exception
GPRSRestore	GPRS Restored
3GAbnormal	3G Network Exception
3GRestore	3G Network Restored
SIMCardAbnormal	SIM Card Exception
SIMCardRestore	SIM Card Restored
VILost	Video Loss
illegalAccess	Illegal Login
HDFull	HDD Full
HDError	HDD Error
DCDLost	MODEM Disconnected
IPConflict	IP Address Conflicted

Log Type	Description
netbroken	Network Disconnected
recError	Recording Error
VIError	Video Input Exception(Only for Analog Channel)
formatHDDError	Remote HDD Formatting Failed
USBError	USB Communication Error
USBRestore	USB Communication Error Restored
printError	Printer Error
printRestore	Printer Error Restored
subsystemCommunicationError	Sub-board Communication Error
IPCIIPconflict	Network Camera IP Address Conflicted
VIMisMatch	Video Standard Mismatches
MCURestart	MCU Restarted
GprsMouleFault	GPRS Module Fault
telephoneFault	Telephone Module Fault
wifiAbnormal	Wi-Fi Exception
wifiRestore	Wi-Fi Restored
RFAbornal	RF Exception
RFRestore	RF Restored
detectorOnline	Detector Connected
detectorOffline	Detector Disconnected
detectorBatteryNormal	Detector Battery Restored
detectorBatteryLow	Detector Battery Low
dataTrafficOverflow	Cellular Network Data Exceeded
radarSignalFault	Radar Transmitter Fault
radarSignalFaultRestore	Radar Transmitter Restored
wirelessOutputModOffline	Wireless Output Expander Disconnected
wirelessOutputModOnline	Wireless Output Expander Connected
wirelessRepeaterOffline	Wireless Repeater Disconnected

Log Type	Description
wirelessRepeaterOnline	Wireless Repeater Connected
triggerOffline	Trigger Disconnected
triggerOnline	Trigger Connected
wirelessSirenOffline	Wireless Siren Disconnected
wirelessSirenOnline	Wireless Siren Connected
sirenLowPower	Siren Battery Low
sirenPowerRecovery	Siren Battery Restored
ipcDisconnect	Network Camera Disconnected
ipcConnectRecovery	Network Camera Connected
sendMailFailed	Sending Email Failed
eventUploadException	Uploading Event Failed or Uploaded Event Lost
keyfobLowPower	Low Keyfob Battery
keyfobPowerRecovery	Normal Keyfob Battery
detectorOvertime	Detector Heartbeat Timed Out
detectorOvertimeRecovery	Detector Heartbeat Timeout Restored
wSirenOvertime	Wireless Siren Heartbeat Timed Out
wSirenOvertimeRecovery	Wireless Siren Heartbeat Timeout Restored
wOutputOvertime	Wireless Output Module Heartbeat Timed Out
wOutputOvertimeRecovery	Wireless Output Module Heartbeat Timeout Restored
wRepeaterOvertime	Wireless Repeater Heartbeat Timed Out
wRepeaterOvertimeRecovery	Wireless Repeater Heartbeat Timeout Restored
rfJamming	RF Wireless Communication Blocked
rfJammingRecovery	RF Wireless Communication Blocking Restored
batteryMiss	Storage Battery Loss
batteryMissRecovery	Storage Battery Restored
ARCUploadFailed	Uploading to ARC Failed
ARCUploadSuccessed	Uploaded to ARC

Log Type	Description
ARCUploadRecovery	Uploading to ARC Restored
wirelessKeypadOffline	Wireless Keypad Disconnected
wirelessKeypadOnline	Wireless Keypad Connected
wirelessCardReaderOffline	Wireless Card Reader Disconnected
wirelessCardReaderOnline	Wireless Card Reader Connected
keypadLowPower	Low Keypad Battery
keypadLowPowerRecovery	Low Keypad Battery Recovered
cardReaderLowPower	Low Card Reader Battery
cardReaderLowPowerRecovery	Low Card Reader Battery Recovered
wKeypadOvertime	Wireless Keypad Heartbeat Timed Out
wKeypadOvertimeRecovery	Wireless Keypad Heartbeat Timeout Recovered
wCardReaderOvertime	Wireless Card Reader Heartbeat Timed Out
wCardReaderOvertimeRecovery	Wireless Card Reader Heartbeat Timeout Recovered
ATSFailed	ATS Failed
ATSRecovery	ATS Recovered
LANPathFailed	Wired or Wireless Connection Failed
LANPathRecovery	Wired or Wireless Connection Recovered
mobileNetPathFailed	Mobile Network Connection Failed
mobileNetPathRecovery	Mobile Network Connection Recovered
RS-485AlarmInputModuleDisconnected	RS-485 Zone Module Offline
RS-485AlarmInputModuleConnected	RS-485 Zone Module Online
RS-485WirelessReceiverDisconnected	RS-485 Wireless Receiver Module Offline
RS-485WirelessReceiverConnected	RS-485 Wireless Receiver Module Online
keypadDisconnected	Keypad Offline
keypadConnected	Keypad Online
overvoltage	High Supply Voltage
undervoltage	Low Supply Voltage
highHDTemperature	HDD High Temperature

Log Type	Description
lowHDTemperature	HDD Low Temperature
hdImpact	HDD Impact
hdBadBlock	HDD Bad Sector
severeHDFailure	HDD Severe Fault
safetyHelmetException	Hard Hat Detection Exception
ezvizUpgradeException	Hik-Connect Upgrade Exception

Operation Logs

Log Type	Description
guard	Normal Arming
unguard	Normal Disarming
bypass	Bypass
duressAccess	Duress
localReboot	Local Reboot
remoteReboot	Remote Reboot
localUpgrade	Local Upgrade
remoteUpgrade	Remote Upgrade
recoveryDefaultParam	Restore Default Settings
outputAlarm	Remote Alarm Output Control
accessOpen	Access Control: Open
accessClose	Access Control : Closed
sirenOpen	Siren: On
sirenClose	Siren: Off
modZoneConfig	Zone Settings
modAlarmoutConfig	Alarm Output Settings
modAnalogConfig	Sensor Settings
RS485Config	RS-485 Channel Settings
phoneConfig	Dialing Settings

Log Type	Description
addAdmin	Added Administrator
modAdminParam	Edited Administrator
delAdmin	Deleted Administrator
addNetUser	Added DVR/NVR Operator
modNetUserParam	Edited DVR/NVR Operator
delNetUser	Deleted DVR/NVR Operator
addOperator	Added Camera Operator
modOperatorPw	Edited Camera Operator Password
delOperator	Deleted Camera Operator Password
addKeyPadUser	Added Keypad/Card Reader User
delKeyPadUser	Deleted Keyboard/Card Reader User
remoteUserLogin	Remote Login
remoteUserLogout	Remote Logout
remoteGuard	Remote Arming
remoteUnguard	Remote Disarming
modHostConfig	Edited Control Panel Settings
restoreBypass	Bypass Restored
alarmOutOpen	Turned on Output
alarmOutClose	Turned off Output
modSubsystemParam	Edited Subsystem Parameters
groupBypass	Group Bypass
groupBypassRestore	Group Bypass Restored
modGprsParam	Edited GPRS Parameters
modNetReportParam	Edited Network Report Settings
modReportMode	Edited Uploading Mode
modGatewayParam	Edited Access Control Settings
remoteStartRec	Remote: Started Recording
remoteStopRec	Remote: Stopped Recording

Log Type	Description
transChanStart	Transparent Transmission Started
transChanStop	Transparent Transmission Stopped
startVoiceTalk	Two-way Audio Started
stopVoiceTalk	Two-way Audio Terminated
remotePlayByFile	Remote: Playback or Downloaded by File
remotePlayByTime	Remote: Playback by Time
remotePTZCtrl	Remote: PTZ Control
remoteLockFile	Remote: Locked File
remoteUnlockFile	Remote: Unlocked File
remoteFormatHd	Remote: Formatted HDD
remoteDownloadCfgFile	Remote: Exported Configuration Files
remoteUploadCfgFile	Remote: Imported Configuration Files
remoteDownloadRecFile	Remote: Exported File
stayArm	Stay Arming
quickArm	Instant Arming
keyswitchArm	Key Zone Arming
keyswitchDisarm	Key Zone Disarming
clearAlarm	Alarm Cleared
modFaultConfig	Edited System Fault Settings
modAlarmOutConfig	Edited Event Alarm Output Settings
searchExternalModule	Searched for External Module
registerExternalModule	Re-registered External Module
closeKeypadAlarm	Disabled Keypad Beep
mod3GConfig	Edited Mobile Parameters
modPrintConfig	Edited Printer Parameters
SDCardFormat	Formatted SD Card
upgradeSubsystem	Upgraded Sub-board
planArmConfig	Arming/Disarming Schedule Configuration

Log Type	Description
phoneArm	SMS Arming
phoneStayArm	SMS Stay Arming
phoneQuickArm	SMS Instant Arming
phoneDisarm	SMS Disarming
phoneClearAlarm	SMS Alarm Cleared
whiteConfig	Allowlist Settings
timeTriggerConfig	Enabled/Disabled Trigger Configuration by Schedule
pictureConfig	Capture Settings
tamperConfig	Zone Tamper-Proof Settings
remoteKeypadUpgrade	Remote: Upgraded Keypad
singlePartitionArmORDisarm	Single-Zone Arming/Disarming
cardConfiguration	Card Settings
cardAramORDisarm	Arming/Disarming by Card
expendNetCenterConfig	Extension Network Center Settings
netCardConfig	NIC Settings
DDNSConfig	DDNS Settings
RS485BusConfig	RS-485 Bus Settings
RS485BusReRegistration	RS-485 Bus Re-registration
remoteOpenElectricLock	Remote: Unlocked
remoteCloseElectricLock	Remote: Locked
localOpenElectricLock	Local: Unlocked
localCloseElectricLock	Local: Locked
openAlarmLamp	Remote: Turned On Alarm Lamp
closeAlarmLamp	Remote: Turned Off Strobe
temporaryPassword	Operation Record of Temporary Password
oneKeyAwayArm	One-Push Away Arming
oneKeyStayArm	One-Push Stay Arming
remoteDelAllVideoAnalysisTask	Empty All Video Analysis Tasks Remotely

Log Type	Description
singleZoneArm	Single-Zone Arming
singleZoneDisarm	Single-Zone Disarming
HIDDNSConfig	HiDDNS Settings
remoteKeypadUpdata	Remote: Upgraded Keypad
zoneAddDetector	Added Detector
zoneDelDetector	Deleted Detector
queryDetectorSignal	Checked Detector Signal Strength on Security Control Panel
queryDetectorBattery	Checked Detector Remaining Battery on Security Control Panel
setDetectorGuard	Detector Arming
setDetectorUnguard	Detector Disarming
setWifiParm	Wi-Fi Settings
voiceOpen	Audio On
voiceClose	Mute
functionKeyEnable	Enabled Function Key
functionKeyDisable	Disabled Panel Function Button
readCard	Swiped Patrol Card
localDeviceActive	Activated Device Remotely
localFactoryDefault	Restored Factory Settings Locally
remoteFactoryDefault	Restored Factory Settings Remotely
addWirelessOutputMod	Added Wireless Output Module
delWirelessOutputMod	Deleted Wireless Output Module
addWirelessRepeater	Added Wireless Repeater
delWirelessRepeater	Deleted Wireless Repeater
telListConfig	Mobile Phone Number Settings
searchRFSignal	Checked RF Signal
addWirelessSiren	Added Wireless Siren
delWirelessSiren	Deleted Wireless Siren

Log Type	Description
flowConfig	Cellular Data Limit Settings
addRemoter	Added Keyfob
delRemoter	Deleted Keyfob
addCard	Added Card
delCard	Deleted Card
remoteAddIpc	Added Network Camera
remoteDelIpc	Deleted Network Camera
remoteSetIpc	Edited Network Camera
localAddressFilterConfig/ remoteAddressFilterConfig	Local/Remote Address Filter Configuration
enterProgramMode	Programming Mode Enabled for Keypad
existProgramMode	Programming Mode Disabled for Keypad
localIOTCfgFileInput	Local operation: import IoT configuration file
localIOTCfgFileOutput	Local operation: export IoT configuration file
remoteIOTCfgFileInput	Remote operation: import IoT configuration file
remoteIOTCfgFileOutput	Remote operation: export IoT configuration file
localIOTAdd	Local operation: add IoT channel
remoteIOTAdd	Remote operation: add IoT channel
localIOTDelete	Local operation: delete IoT channel
remoteIOTDelete	Remote operation: delete IoT channel
localIOTSet	Local operation: configure IoT channel
remoteIOTSet	Remote operation: configure IoT channel
armWithFault	Armed with Fault
entryDelay	Entering and Exiting Delay
modArmConfig	Edit Arming Parameters
modCertificateStandard	Edit Authentication Standard
entryPaceTest	Pacing Mode Entered
exitPaceTest	Pacing Mode Exited

Log Type	Description
addNetOperator	Add Operator
modNetOperator	Edit Operator Information
delNetOperator	Delete Operator
addNetInstaller	Add Installer
modNetInstaller	Edit Installer Information
delNetInstaller	Delete Installer
addManufacturer	Add Manufacturer
modManufacturer	Edit Manufacturer Information
delManufacturer	Delete Manufacturer
upgradeSuccessed	Upgraded
upgradeFailed	Upgrading Failed
zoneDisabled	Zone Shielded
localCfgSecurity	Security Parameter Configured Locally
remoteCfgSecurity	Security Parameter Configured Remotely
remoteGetParaSecurity	Security Parameters Obtained Remotely
delRS-485InputModule	RS-485 Zone Module Deleted
delRS-485OutputModule	RS-485 Output Module Deleted
delRS-485WirelessReceiver	RS-485 Wireless Receiver Module Deleted
enrollRS-485InputModule	RS-485 Zone Module Registered
enrollRS-485OutputModule	RS-485 Output Module Registered
delRS-485OutputModule	RS-485 Output Module Deleted
enrollRS-485WirelessReceiver	RS-485 Wireless Receiver Module Registered
enrollKeypad	Keypad Registered
delKeypad	Keypad Deleted
scheduledAngleCalibration	Scheduled Angle Calibration
addZone	Added Zone
modZone	Edited Zone
delZone	Deleted Zone

Log Type	Description
addAlarmLine	Added Trigger Line
modAlarmLine	Edited Trigger Line
delAlarmLine	Deleted Trigger Line
remoteHFPDconfig/localHFPDconfig	Remote/Local Configuration of Frequently Appeared Person Detection
remoteLFPDconfig	Remote Configuration of Low Frequency Person Detection
modifyUserPassword	Password Changed
logOut	Logged Out
indicatorStatusSettings	Indicator Switch Settings
wiredNetworkSettings	Wired Network Settings
notificationSettings	Message Notification Settings
alarmCenterSettings	Alarm Receiving Center Settings
videoRecordStrategySettings	Video Recording Strategy Settings
cameraLinkageSettings	Camera Linkage Settings
armingDisarmingScheduleSettings	Arming and Disarming Schedule Settings
alarmSpeedSettings	Speed Threshold Settings for Triggering Alarms
videoTrackingSwitchSettings	Video Tracking Switching Settings
frequencySettings	Frequency Band Settings
masterSlaveTrackingSettings	Smart Linkage Settings
parkingPointSettings	Parking Point Settings
administratorEdited	Administrator Parameters Edited
securityConfigured	Security Settings
relayParametersEdited	Relay Parameters Edited
radarSensitivitySettings	Radar Sensitivity Settings
detectAngandDistanceSettings	Detector Angle and Range Settings
masterSlaveRadarSettings	Main Radar and Sub Radar Settings
remoteCheckTime	Remote: Manual Time Synchronization
remoteParamSimpleDefault	Remote: Partly Restore to Default Settings

Log Type	Description
remoteParamFactoryDefault	Remote: Restore All to Default Settings
localAutoSwitchConfig	Configure Auto Power On or Off Locally
remoteAutoSwitchConfig	Configure Auto Power On or Off Remotely
remoteCfgWirelessDialParam	Configure wireless dial-up parameters remotely
localCfgWirelessDialParam	Configure wireless dial-up parameters locally
remoteCfgWirelessSmsParam	Configure wireless message parameters remotely
localCfgWirelessSmsParam	Configure wireless message parameters locally
remoteCfgWirelessSmsSelfHelp	Configure SMS self-service parameters remotely
localCfgWirelessSmsSelfHelp	Configure SMS self-service parameters locally
remoteCfgWirelessNetFlowParam	Configure wireless traffic parameters remotely
localCfgWirelessNetFlowParam	Configure wireless traffic parameters locally
scaleCfg	Scale Settings
radarTrailCfg	Radar Pattern Settings
MapImportCfg	Map Importing Settings
radarCalibrationCfg	Radar Calibration Settings
LocalEzvizOperation	Local EZVIZ Operations
RemoteEzvizOperation	Remote EZVIZ Operations
SSHEnabled	SSH Enabled
SSHDisabled	SSH Disabled
installationModeEntered	Installation Mode Enabled
installationModeExited	Installation Mode Disabled
diagnosisModeConfigured	Diagnosis Mode Configured
fileExported	File Exported
audioFileUploaded	Audio File Uploaded
audioFileDeleted	Audio File Deleted
PIRCAMCapture	PIRCAM Captured
SIPIntercomStarted	SIP Intercom Started
SIPIntercomEnded	SIP Intercom Ended

Log Type	Description
enrollmentModeEntered	Registration Mode Enabled
enrollmentModeExited	Registration Mode Disabled
videoAudioSelfCheckStarted	Self-Test of Audio and Video Started
videoAudioSelfCheckStopped	Self-Test of Audio and Video Stopped
cardReaderunlocked	Card Reader Unlocked
cardReaderlocked	Card Reader Locked
videoAudioSelfCheckEnded	Self-Test of Audio and Video Ended
previewStart	Live View Started
previewStop	Live View Stopped
remoteDelAllVideoAnalysisTask	All Video Analysis Tasks Cleared (One-Touch)
localSSDOperateStart	Local SSD operation (firmware operations) started
localSSDOperateStop	Local SSD operation (firmware operations) ended
remoteSSDOperateStart	Remote SSD operation (firmware operations) started
remoteSSDOperateStop	Remote SSD operation (firmware operations) ended
AITargetBPAdd	Reference picture for AI target comparison added
AITargetBPDelete	Reference picture for AI target comparison deleted
AITargetBPSearch	Reference picture for AI target comparison AI searched for
AITargetBPUpdate	Reference picture for AI target comparison updated
AIRuleConfigTrigger	AI rule linkage configured
AudioFileImport	Audio file imported
AudioFileDownLoad	Audio file downloaded
cardNoNotRegistered	Card No. not registered
LocalBackupConfig	Local hot spare device configuration
RemoteBackupConfig	Remote hot spare device configuration
remoteAIModelAdd	Model package added
remoteAIModelQuery	Model package searched
remoteAIModelDelete	Model package deleted

Log Type	Description
remoteAIModelUpdate	Model package updated
remoteAIPicturePollingTaskAdd	Picture polling analysis task added
remoteAIPicturePollingTaskQuery	Picture polling analysis task searched
remoteAIPicturePollingTaskDelete	Picture polling analysis task deleted
remoteAIPicturePollingTaskModify	Picture polling analysis task edited
remoteAIVideoTaskAdd	Video analysis task added
remoteAIVideoTaskQuery	Video analysis task searched
remoteAIVideoTaskDelete	Video analysis task deleted
remoteAIVideoTaskModify	Video analysis task edited
remoteAIPictureTaskAdd	Picture analysis task added
remoteAIPictureTaskQuery	Picture analysis task searched
remoteAIPictureTaskDelete	Picture analysis task deleted
remoteAIPictureTaskModify	Picture analysis task edited
remoteAIVideoPollingTaskAdd	Video polling analysis task added
remoteAIVideoPollingTaskQuery	Video polling analysis task searched
remoteAIVideoPollingTaskDelete	Video polling analysis task deleted
remoteAIVideoPollingTaskModify	Video polling analysis task edited
AIRuleConfig	AI rule configuration
localParamFactoryDefault	Restore to default settings locally
remoteParamFactoryDefault	Restore to default settings remotely
remoteDeleteAllVerifyOrCapPics	Delete all authenticated or captured face pictures remotely
localDeleteAllVerifyOrCapPics	Delete all authenticated or captured face pictures locally
remoteDeleteEventsAtSpecTime	Delete events by specified time remotely
localDeleteEventsAtSpecTime	Delete events by specified time locally
remoteOpenSummerTime	Enable DST remotely
localOpenSummerTime	Enable DST locally
remoteCloseSummerTime	Disable DST remotely

Log Type	Description
localCloseSummerTime	Disable DST locally
remoteEZVIZUnbind	Unbind from EZVIZ cloud remotely
localEZVIZUnbind	Unbind from EZVIZ cloud locally
enterLocalUIBackground	Enter UI background
remoteDeleteFaceBaseMap	Delete registered face pictures remotely
localDeleteFaceBaseMap	Delete registered face pictures locally
SVCEnhanced	Enhance SVC
remoteImportEventTableFile	Remotely import the customized list of events
remoteExportEventTableFile	Remotely export the customized list of events
remoteEventTypeCfg	Remotely configure event type

Event Logs

Log Type	Description
SDKSchool	SDK Synchronization
presetsSatatusChange	Status of preset changed
selfTimeSchool	Time Synchronization by Schedule
insertSubsystem	Plugged in Sub-board
pullOutSubsystem	Pulled out Sub-board
autoArm	Auto Arming
autoDisarm	Auto Disarming
triggerOn	Activated Trigger by Schedule
triggerOff	Deactivated Trigger by Schedule
autoArmFailed	Auto Arming Failed
autoDisarmFailed	Auto Disarming Failed
triggerOnFailed	Activating Trigger Failed
triggerOffFailed	Deactivating Trigger Failed
mandatoryAlarm	Forced Arming
keyPADlocked	Keypad Locked

Log Type	Description
keyPADUnlocked	Keypad Unlocked
insetUSB	Plugged in USB Flash Drive
pulloutUSB	Removed USB Flash Drive
lateRemind	Late to Disarm
keypadUnlocked	Unlocked Keypad
timeSynchronization	Time Synchronization
armFailed	Arming Failed
ARCStart	ARC Connected
locked	Locked

Information Logs

Log Type	Description
doubleVerificationPass	Double Verification Completed
hdFormatStart	Formatting HDD Started
hdFormatStop	Formatting HDD Stopped
wirelessRunningStatus	Wireless Network Running Status
BackupInfo	Hot Spare Information
addUserInfo	Added person information (access control permission)
modifyUserInfo	Edit person information (access control permission)
clearUserInfo	Delete person information by employee No. (access control permission)
clearAllUser	Delete all person information (access control permission)
ezvizLinkageInfo	EZVIZ linkage information

B.5 Response Codes of Text Protocol

The response codes returned during the text protocol integration is based on the status codes of HTTP. 7 kinds of status codes are predefined, including 1 (OK), 2 (Device Busy), 3 (Device Error), 4

(Invalid Operation), 5 (Invalid Message Format), 6 (Invalid Message Content), and 7 (Reboot Required). Each kind of status code contains multiple sub status codes, and the response codes are in a one-to-one correspondence with the sub status codes.

StatusCode=1

SubStatusCode	Error Code	Description
ok	0x1	Operation completed.
riskPassword	0x10000002	Risky password.
armProcess	0x10000005	Arming process.

StatusCode=2

Sub Status Code	Error Code	Description
noMemory	0x20000001	Insufficient memory.
serviceUnavailable	0x20000002	The service is not available.
upgrading	0x20000003	Upgrading.
deviceBusy	0x20000004	The device is busy or no response.
reConnectIpc	0x20000005	The video server is reconnected.
transferUpgradePackageFailed	0x20000006	Transmitting device upgrade data failed.
startUpgradeFailed	0x20000007	Starting upgrading device failed.
getUpgradeProcessfailed.	0x20000008	Getting upgrade status failed.
certificateExist	0x2000000B	The Authentication certificate already exists.

StatusCode=3

Sub Status Code	Error Code	Description
deviceError	0x30000001	Hardware error.
badFlash	0x30000002	Flash operation error.

Sub Status Code	Error Code	Description
28181Uninitialized	0x30000003	The 28181 configuration is not initialized.
socketConnectError	0x30000005	Connecting to socket failed.
receiveError	0x30000007	Receive response message failed.
deletePictureError	0x3000000A	Deleting picture failed.
pictureSizeExceedLimit	0x3000000C	Too large picture size.
clearCacheError	0x3000000D	Clearing cache failed.
updateDatabaseError	0x3000000F	Updating database failed.
searchDatabaseError	0x30000010	Searching in the database failed.
writeDatabaseError	0x30000011	Writing to database failed.
deleteDatabaseError	0x30000012	Deleting database element failed.
searchDatabaseElementError	0x30000013	Getting number of database elements failed.
cloudAutoUpgradeException	0x30000016	Downloading upgrade packet from cloud and upgrading failed.
HBPException	0x30001000	HBP exception.
UDEPException	0x30001001	UDEP exception
elasticSearchException	0x30001002	Elastic exception.
kafkaException	0x30001003	Kafka exception.
HBaseException	0x30001004	Hbase exception.
sparkException	0x30001005	Spark exception.
yarnException	0x30001006	Yarn exception.
cacheException	0x30001007	Cache exception.
trafficException	0x30001008	Monitoring point big data server exception.
faceException	0x30001009	Human face big data server exception.

Sub Status Code	Error Code	Description
SSDFileSystemIsError	0x30001013	SSD file system error (Error occurs when it is non-Ext4 file system)
insufficientSSDCapacityForFPD	0x30001014	Insufficient SSD space for person frequency detection.
wifiException	0x3000100A	Wi-Fi big data server exception
structException	0x3000100D	Video parameters structure server exception.
noLinkageResource	0x30001015	Insufficient linkage resources.
engineAbnormal	0x30002015	Engine exception.
engineInitialization	0x30002016	Initializing the engine.
algorithmLoadingFailed	0x30002017	Loading the model failed.
algorithmDownloadFailed	0x30002018	Downloading the model failed.
algorithmDecryptionFailed	0x30002019	Decrypting the model failed.
unboundChannel	0x30002020	Delete the linked channel to load the new model.
unsupportedResolution	0x30002021	Invalid resolution.
unsupportedSteamType	0x30002022	Invalid stream type.
insufficientDecRes	0x30002023	Insufficient decoding resources.
insufficientEnginePerformance	0x30002024	Insufficient engine performance (The number of channels to be analyzed exceeds the engine's capability).
improperResolution	0x30002025	Improper resolution (The maximum resolution allowed is 4096×4096).
improperPicSize	0x30002026	Improper picture size (The maximum size allowed is 5MB).
URLDownloadFailed	0x30002027	Downloading the picture via the URI failed.

Sub Status Code	Error Code	Description
unsupportedImageFormat	0x30002028	Invalid picture format (Only JPG is supported currently).
unsupportedPollingIntervalTime	0x30002029	Invalid polling interval (The interval should be more than 10s).
exceedImagesNumber	0x30002030	The number of pictures exceeds the limit (The platform can apply 1 to 100 picture URIs per time, the maximum number allowed is 100).
unsupportedMPID	0x30002031	The applied MPID does not exist in the device, so updating this MPID is not supported.
modelPackageNotMatchLabel	0x30002032	The model and the description file mismatch.
modelPackageNotMatchTask	0x30002033	The task and the model type mismatch.
insufficientSpace	0x30002034	Insufficient space (When the number of model packages does not reach the maximum number allowed but their size together exceeds the free space, the model packages cannot be added).
engineUnLoadingModelPackage	0x30002035	Applying the task failed. This engine is not linked to a model package (Canceling the linkage failed, this engine is not linked to a model package).
engineWithModelPackage	0x30002036	Linking the engine to this model package failed. The engine has been linked to another model package. Please cancel their linkage first.

Sub Status Code	Error Code	Description
modelPackageDelete	0x30002037	Linking the model package failed. The model package has been deleted.
deleteTaskFailed	0x30002038	Deleting the task failed (It is returned when the user fails to end a task).
modelPackageNumberslimited	0x30002039	Adding the model package failed. The number of model package has reached the maximum number allowed.
modelPackageDeleteFailed	0x30002040	Deleting the model package failed.
noArmingResource	0x30001016	Insufficient arming resources.
calibrationTimeout	0x30002051	Calibration timed out.
captureTimeout	0x30006000	Data collection timed out.
lowScore	0x30006001	Low quality of collected data.
uploadingFailed	0x30007004	Uploading failed.

StatusCode=4

Sub Status Code	Error Code	Description
notSupport	0x40000001	Not supported.
lowPrivilege	0x40000002	No permission.
badAuthorization	0x40000003	Authentication failed.
methodNotAllowed	0x40000004	Invalid HTTP method.
notSetHdiskRedund	0x40000005	Setting spare HDD failed.
invalidOperation	0x40000006	Invalid operation.
notActivated	0x40000007	Inactivated.
hasActivated	0x40000008	Activated.
certificateAlreadyExist	0x40000009	The certificate already exists.
operateFailed	0x4000000F	Operation failed.

Sub Status Code	Error Code	Description
USBNotExist	0x40000010	USB device is not connected.
upgradePackageMorethan2GB	0x40001000	Up to 2GB upgrade package is allowed to be uploaded.
IDNotExist	0x40001001	The ID does not exist.
interfaceOperationError	0x40001002	API operation failed.
synchronizationError	0x40001003	Synchronization failed.
synchronizing	0x40001004	Synchronizing.
importError	0x40001005	Importing failed.
importing	0x40001006	Importing.
fileAlreadyExists	0x40001007	The file already exists.
invalidID	0x40001008	Invalid ID.
backupnodeNotAllowed	0x40001009	Accessing to backup node is not allowed.
exportingError	0x4000100A	Exporting failed.
exporting	0x4000100B	Exporting.
exportEnded	0x4000100C	Exporting stopped.
exported	0x4000100D	Exported.
IPOccupied	0x4000100E	The IP address is already occupied.
IDAlreadyExists	0x4000100F	The ID already exists.
exportItemsExceedLimit	0x40001010	No more items can be exported.
noFiles	0x40001011	The file does not exist.
beingExportedByAnotherUser	0x40001012	Being exported by others.
needReAuthentication	0x40001013	Authentication is needed after upgrade.
unitAddNotOnline	0x40001015	The added data analysis server is offline.
unitControl	0x40001016	The data analysis server is already added.
analysis unitFull	0x40001017	No more data analysis server can be added.

Sub Status Code	Error Code	Description
unitIDError	0x40001018	The data analysis server ID does not exist.
unitExit	0x40001019	The data analysis server already exists in the list.
unitSearch	0x4000101A	Searching data analysis server in the list failed.
unitNotOnline	0x4000101B	The data analysis server is offline.
unitInfoEror	0x4000101C	Getting data analysis server information failed.
unitGetNodeInfoError	0x4000101D	Getting node information failed.
unitGetNetworkInfoErr or	0x4000101E	Getting the network information of data analysis server failed
unitSetNetworkInfoErr or	0x4000101F	Setting the network information of data analysis server failed
setSmartNodeInfoError	0x40001020	Setting node information failed.
setUnitNetworkInfoErr or	0x40001021	Setting data analysis server network information failed.
unitRestartCloseError	0x40001022	Rebooting or shutting down data analysis server failed.
virtualIPnotAllowed	0x40001023	Adding virtual IP address is not allowed.
unitInstalled	0x40001024	The data analysis server is already installed.
badSubnetMask	0x40001025	Invalid subnet mask.
uintVersionMismatche d	0x40001026	Data analysis server version mismatches.
deviceMOdelMismatch ed	0x40001027	Adding failed. Device model mismatches.
unitAddNotSelf	0x40001028	Adding peripherals is not allowed.
noValidUnit	0x40001029	No valid data analysis server.
unitNameDuplicate	0x4000102A	Duplicated data analysis server name.
deleteUnitFirst	0x4000102B	Delete the added data analysis server of the node first.
getLocallInfoFailed	0x4000102C	Getting the server information failed.
getClientAddedNodeFa iled	0x4000102D	Getting the added node information of data analysis server failed.

Sub Status Code	Error Code	Description
taskExit	0x4000102E	The task already exists.
taskInitError	0x4000102F	Initializing task failed.
taskSubmitError	0x40001030	Submitting task failed.
taskDelError	0x40001031	Deleting task failed.
taskPauseError	0x40001032	Pausing task failed.
taskContinueError	0x40001033	Starting task failed.
taskSeverNoCfg	0x40001035	Full-text search server is not configured.
taskPicSeverNoCfg	0x40001036	The picture server is not configured.
taskStreamError	0x40001037	Streaming information exception.
taskRecSDK	0x40001038	History recording is not supported.
taskCasaError	0x4000103A	Cascading is not supported.
taskVCARuleError	0x4000103B	Invalid VCA rule.
taskNoRun	0x4000103C	The task is not executed.
unitLinksNoStorageNode	0x4000103D	No node is linked with the data analysis server. Configure the node first.
searchFailed	0x4000103E	Searching video files failed.
searchNull	0x4000103F	No video clip.
userScheOffline	0x40001040	The task scheduler service is offline.
updateTypeUnmatched	0x40001041	The upgrade package type mismatches.
userExist	0x40001043	The user already exists.
userCannotDelAdmin	0x40001044	The administrator cannot be deleted.
userInexistence	0x40001045	The user name does not exist.
userCannotCreateAdmin	0x40001046	The administrator cannot be created.
monitorCamExceed	0x40001048	Up to 3000 cameras can be added.
monitorCunitOverLimit	0x40001049	Adding failed. Up to 5 lower-levels are supported by the control center.

Sub Status Code	Error Code	Description
monitorReginOverLimit	0x4000104A	Adding failed. Up to 5 lower-levels are supported by the area.
monitorArming	0x4000104B	The camera is already armed. Disarm the camera and try again.
monitorSyncCfgNotSet	0x4000104C	The system parameters are not configured.
monitorFdSyncing	0x4000104E	Synchronizing. Try again after completing the synchronization.
monitorParseFailed	0x4000104F	Parsing camera information failed.
monitorCreatRootFailed	0x40001050	Creating resource node failed.
deleteArmingInfo	0x40001051	The camera is already . Disarm the camera and try again.
cannotModify	0x40001052	Editing is not allowed. Select again.
cannotDel	0x40001053	Deletion is not allowed. Select again.
deviceExist	0x40001054	The device already exists.
IPErrorConnectFailed	0x40001056	Connection failed. Check the network port.
cannotAdd	0x40001057	Only the capture cameras can be added.
serverExist	0x40001058	The server already exists.
fullTextParamError	0x40001059	Incorrect full-text search parameters.
storParamError	0x4000105A	Incorrect storage server parameters.
picServerFull	0x4000105B	The storage space of picture storage server is full.
NTPUnconnect	0x4000105C	Connecting to NTP server failed. Check the parameters.
storSerConnectFailed	0x4000105D	Connecting to storage server failed. Check the network port.
storSerLoginFailed	0x4000105E	Logging in to storage server failed. Check the user name and password.
searchSerConnectFailed	0x4000105F	Connecting to full-text search server failed. Check the network port.

Sub Status Code	Error Code	Description
searchSerLoginFailed	0x40001060	Logging in to full-text search server failed. Check the user name and password.
kafkaConnectFailed	0x40001061	Connecting to Kafka failed. Check the network port.
mgmtConnectFailed	0x40001062	Connecting to system failed. Check the network port.
mgmtLoginFailed	0x40001063	Logging in to system failed. Check the user name and password.
TDAConnectFailed	0x40001064	Connecting to traffic data access server failed. Checking the server status.
86sdkConnectFailed	0x40001065	Connecting to listening port of iVMS-8600 System failed. Check the parameters.
nameExist	0x40001066	Duplicated server name.
batchProcessFailed	0x40001067	Processing in batch failed.
IDNotExist	0x40001068	The server ID does not exist.
serviceNumberReache sLimit	0x40001069	No more service can be added.
invalidServiceType.	0x4000106A	Invalid service type.
clusterGetInfo	0x4000106B	Getting cluster group information failed.
clusterDelNode	0x4000106C	Deletion node failed.
clusterAddNode	0x4000106D	Adding node failed.
clusterInstalling	0x4000106E	Creating cluster...Do not operate.
clusterUninstall	0x4000106F	Reseting cluster...Do not operate.
clusterInstall	0x40001070	Creating cluster failed.
clusterIpError	0x40001071	Invalid IP address of task scheduler server.
clusterNotSameSeg	0x40001072	The main node and sub node must be in the same network segment.
clusterVirIpError	0x40001073	Automatically getting virtual IP address failed. Enter manually.
clusterNodeUnadd	0x40001074	The specified main (sub) node is not added.
clusterNodeOffline	0x40001075	The task scheduler server is offline.

Sub Status Code	Error Code	Description
nodeNotCurrentIP	0x40001076	The analysis node of the current IP address is required when adding main and sub nodes.
addNodeNetFailed	0x40001077	Adding node failed. The network disconnected.
needTwoMgmtNode	0x40001078	Two management nodes are required when adding main and sub nodes.
ipConflict	0x40001079	The virtual IP address and data analysis server's IP address conflicted.
ipUsed	0x4000107A	The virtual IP address has been occupied.
cloudAlalyseOnline	0x4000107B	The cloud analytic server is online.
virIP&mainIPnotSameNetSegment	0x4000107C	The virtual IP address is not in the same network segment with the IP address of main/sub node.
getNodeDispatchInfoFailed	0x4000107D	Getting node scheduler information failed.
unableModifyManagementNetworkIP	0x4000107E	Editing management network interface failed. The analysis board is in the cluster.
notSpecifyVirtualIP	0x4000107F	Virtual IP address should be specified for main and sub cluster.
armingFull	0x40001080	No more device can be armed.
armingNoFind	0x40001081	The arming information does not exist.
disArming	0x40001082	Disarming failed.
getArmingError	0x40001084	Getting arming information failed.
refreshArmingError	0x40001085	Refreshing arming information failed.
ArmingPlateSame	0x40001086	The license plate number is repeatedly armed.
ArmingParseXLSError	0x40001087	Parsing arming information file failed.
ArmingTimeError	0x40001088	Invalid arming time period.
ArmingSearchTimeError	0x40001089	Invalid search time period.
armingRelationshipReachesLimit	0x4000108A	No more relation can be created.

Sub Status Code	Error Code	Description
duplicateAarmingName	0x4000108B	The relation name already exists.
noMoreArmingListAdded	0x4000108C	No more blocklist library can be armed.
noMoreCamerasAdded	0x4000108D	No more camera can be armed.
noMoreArmingListAddedWithCamera	0x4000108E	No more library can be linked to the camera.
noMoreArmingPeriodAdded	0x4000108F	No more time period can be added to the arming schedule.
armingPeriodsOverlapped	0x40001090	The time periods in the arming schedule are overlapped.
noArmingAlarmInfo	0x40001091	The alarm information does not exist.
armingAlarmUnRead	0x40001092	Getting number of unread alarms failed.
getArmingAlarmError	0x40001093	Getting alarm information failed.
searchByPictureTimedOut	0x40001094	Searching picture by picture timeout. Search again.
comparisonTimeRangeError	0x40001095	Comparison time period error.
selectMonitorNumberUpperLimit	0x40001096	No more monitoring point ID can be filtered.
noMoreComparisonTasksAdded	0x40001097	No more comparison task can be executed at the same time.
GetComparisonResultFailed	0x40001098	Getting comparison result failed.
comparisonTypeError	0x40001099	Comparison type error.
comparisonUnfinished	0x4000109A	The comparison is not completed.
facePictureModelInvalid	0x4000109B	Invalid face model.
duplicateLibraryName.	0x4000109C	The library name already exists.
noRecord	0x4000109D	No record found.
countingRecordsFailed.	0x4000109E	Calculate the number of records failed.

Sub Status Code	Error Code	Description
getHumanFaceFrameFailed	0x4000109F	Getting face thumbnail from the picture failed.
modelingFailed.	0x400010A0	Modeling face according to picture URL failed.
1V1FacePictureComparisonFailed	0x400010A1	Comparison 1 VS 1 face picture failed.
libraryArmed	0x400010A2	The blocklist library is armed.
licenseExceedLimit	0x400010A3	Dongle limited.
licenseExpired	0x400010A4	Dongle expired.
licenseDisabled	0x400010A5	Unavailable dongle.
licenseNotExist	0x400010A6	The dongle does not exist.
SessionExpired	0x400010A7	Session expired .
beyondConcurrentLimit	0x400010A8	Out of concurrent limit.
stopSync	0x400010A9	Synchronization stopped.
getProgressFaild	0x400010AA	Getting progress failed.
uploadExtraCaps	0x400010AB	No more files can be uploaded.
timeRangeError	0x400010AC	Time period error.
dataPortNotConnected	0x400010AD	The data port is not connected.
addClusterNodeFailed	0x400010AE	Adding to the cluster failed. The device is already added to other cluster.
taskNotExist	0x400010AF	The task does not exist.
taskQueryFailed	0x400010B0	Searching task failed.
modifyTimeRuleFailed	0x400010B2	The task already exists. Editing time rule is not allowed.
modifySmartRuleFailed	0x400010B3	The task already exists. Editing VAC rule is not allowed.
queryHistoryVideoFailed	0x400010B4	Searching history video failed.
addDeviceFailed	0x400010B5	Adding device failed.
addVideoFailed	0x400010B6	Adding video files failed.

Sub Status Code	Error Code	Description
deleteAllVideoFailed	0x400010B7	Deleting all video files failed.
createVideoIndexFailed	0x400010B8	Indexing video files failed.
videoCheckTypeFailed	0x400010B9	Verifying video files types failed.
configStructuredAddressesFailed	0x400010BA	Configuring IP address of structured server failed.
configPictureServerAddressFailed	0x400010BB	Configuring IP address of picture storaged server failed.
storageServiceIPNotExist	0x400010BD	The storage server IP address does not exist.
syncBackupDatabaseFailed	0x400010BE	Synchronizing sub database failed. Try again.
syncBackupNTPTimeFailed	0x400010BF	Synchronizing NTP time of sub server failed.
clusterNotSelectLoopbackAddress	0x400010C0	Loopbacl address is not supported by the main or sub cluster.
addFaceRecordFailed	0x400010C1	Adding face record failed.
deleteFaceRecordFailed	0x400010C2	Deleting face record failed.
modifyFaceRecordFailed	0x400010C3	Editing face record failed.
queryFaceRecordFailed	0x400010C4	Searching face record failed.
faceDetectFailed	0x400010C5	Detecting face failed.
libraryNotExist	0x400010C6	The library does not exist.
blackListQueryExporting	0x400010C7	Exporting matched blocklists.
blackListQueryExported	0x400010C8	The matched blocklists are exported.
blackListQueryStopExporting	0x400010C9	Exporting matched blocklists is stopped.
blackListAlarmQueryExporting	0x400010CA	Exporting matched blocklist alarms.

Sub Status Code	Error Code	Description
blackListAlarmQueryExported	0x400010CB	The matched blocklists alarms are exported.
blackListAlarmQueryStopExporting	0x400010CC	Exporting matched blocklist alarms is stopped.
getBigDataCloudAnalysisFailed	0x400010CD	Getting big data cloud analytic information failed.
setBigDataCloudAnalysisFailed	0x400010CE	Configuring big data cloud analytic failed.
submitMapSearchFailed	0x400010CF	Submitting search by picture task failed.
controlRelationshipNotExist	0x400010D0	The relation does not exist.
getHistoryAlarmInfoFailed	0x400010D1	Getting history alarm information failed.
getFlowReportFailed	0x400010D2	Getting people counting report failed.
addGuardFailed	0x400010D3	Adding arming configuration failed.
deleteGuardFailed	0x400010D4	Deleting arming configuration failed.
modifyGuardFailed	0x400010D5	Editing arming configuration failed.
queryGuardFailed	0x400010D6	Searching arming configurations failed.
uploadUserSuperCaps	0x400010D7	No more user information can be uploaded.
bigDataServerConnectFailed	0x400010D8	Connecting to big data server failed.
microVideoCloudRequestInfoBuildFailed	0x400010D9	Adding response information of micro video cloud failed.
microVideoCloudResponseInfoBuildFailed	0x400010DA	Parsing response information of micro video cloud failed.
transcodingServerRequestInfoBuildFailed	0x400010DB	Adding response information of transcoding server failed.
transcodingServerResponseInfoParseFailed	0x400010DC	Parsing response information of transcoding server failed.
transcodingServerOffline	0x400010DD	Transcoding server is offline.

Sub Status Code	Error Code	Description
microVideoCloudOffline	0x400010DE	Micro video cloud is offline.
UPSServerOffline	0x400010DF	UPS monitor server is offline.
statisticReportRequestInfoBuildFailed	0x400010E0	Adding response information of statistics report failed.
statisticReportResponseInfoParseFailed	0x400010E1	Parsing response information of statistics report failed.
DisplayConfigInfoBuildFailed	0x400010E2	Adding display configuration information failed.
DisplayConfigInfoParseFailed	0x400010E3	Parsing display configuration information failed.
DisplayConfigInfoSaveFailed	0x400010E4	Saving display configuration information failed.
notSupportDisplayConfigType	0x400010E5	The display configuration type is not supported.
passError	0x400010E7	Incorrect password.
upgradePackageLarge	0x400010EB	Too large upgrade package.
sessionUserReachesLimit	0x400010EC	No more user can log in via session.
ISO8601TimeFormatError	0x400010ED	Invalid ISO8601 time format.
clusterDissolutionFailed	0x400010EE	Deleting cluster failed.
getServiceNodeInfoFailed	0x400010EF	Getting service node information failed.
getUPSInfoFailed	0x400010F0	Getting UPS configuration information failed.
getDataStatisticsReportFailed	0x400010F1	Getting data statistic report failed.
getDisplayConfigInfoFailed	0x400010F2	Getting display configuration failed.
namingAnalysisBoardNotAllowed	0x400010F3	Renaming analysis board is not allowed.

Sub Status Code	Error Code	Description
onlyDrawRegionsOfConvexPolygon	0x400010F4	Only drawing convex polygon area is supported.
bigDataServerResponseInfoParseFailed	0x400010F5	Parsing response message of big data service failed.
bigDataServerReturnFailed	0x400010F6	No response is returned by big data service.
microVideoReturnFailed	0x400010F7	No response is returned by micro video cloud service.
transcodingServerReturnFailed	0x400010F8	No response is returned by transcoding service.
UPSServerReturnFailed	0x400010F9	No response is returned by UPS monitoring service.
forwardingServerReturnFailed	0x400010FA	No response is returned by forwarding service.
storageServerReturnFailed	0x400010FB	No response is returned by storage service.
cloudAnalysisServerReturnFailed	0x400010FC	No response is returned by cloud analytic service.
modelEmpty	0x400010FD	No model is obtained.
mainAndBackupNodeCannotModifyManagementNetworkInterfaceIP	0x400010FE	Editing the management interface IP address of main node and backup node is not allowed.
IDTooLong	0x400010FF	The ID is too long.
pictureCheckFailed	0x40001100	Detecting picture failed.
pictureModelingFailed	0x40001101	Modeling picture failed.
setCloudAnalysisDefaultProvinceFailed	0x40001102	Setting default province of cloud analytic service failed.
InspectionAreasNumberExceedLimit	0x40001103	No more detection regions can be added.
picturePixelsTooLarge	0x40001105	The picture resolution is too high.
picturePixelsTooSmall	0x40001106	The picture resolution is too low.
storageServiceIPEmpty	0x40001107	The storage server IP address is required.

Sub Status Code	Error Code	Description
bigDataServerRequestInfoBuildFail	0x40001108	Creating request message of big data service failed.
analysisTimedOut	0x40001109	Analysis time out.
high-performanceModeDisabled	0x4000110A	Please enable high-performance mode.
configuringUPSMonitoringServerTimedOut	0x4000110B	Configuring the UPS monitoring server time out. Check IP address.
cloudAnalysisRequestInformationBuildFailed	0x4000110C	Creating request message of cloud analytic service failed.
cloudAnalysisResponseInformationParseFailed	0x4000110D	Parsing response message of cloud analytic service failed.
allCloudAnalysisInterfaceFailed	0x4000110E	Calling API for cloud analytic service failed.
cloudAnalysisModelCompareFailed	0x4000110F	Model comparison of cloud analytic service failed.
cloudAnalysisFacePictureQualityRatingFailed	0x40001110	Getting face quality grading of cloud analytic service failed.
cloudAnalysisExtractFeaturePointsFailed	0x40001111	Extracting feature of cloud analytic service failed.
cloudAnalysisExtractPropertyFailed	0x40001112	Extracting property of cloud analytic service failed.
getAddedNodeInformationFailed	0x40001113	Getting the added nodes information of data analysis server failed.
noMoreAnalysisUnitsAdded	0x40001114	No more data analysis servers can be added.
detectionAreaInvalid	0x40001115	Invalid detection region.
shieldAreaInvalid	0x40001116	Invalid shield region.
noMoreShieldAreasAdded	0x40001117	No more shield region can be drawn.
onlyAreaOfRectangleShapeAllowed	0x40001118	Only drawing rectangle is allowed in detection area.
numberReachedLlimit	0x40001119	Number reached the limit.

Sub Status Code	Error Code	Description
wait1~3MinutesGetIPAfterSetupDHCP	0x4000111A	Wait 1 to 3 minutes to get IP address after configuring DHCP.
plannedTimeMustbeHalfAnHour	0x4000111B	Schedule must be half an hour.
oneDeviceCannotBuildCluster	0x4000111C	Creating main and backup cluster requires at least two devices.
updatePackageFileNotUploaded	0x4000111E	Upgrade package is not uploaded.
highPerformanceTasksNotSupportDrawingDetectionRegions	0x4000111F	Drawing detection area is not allowed under high-performance mode.
controlCenterIDDoesNotExist	0x40001120	The control center ID does not exist.
regionIDDoesNotExist	0x40001121	The area ID does not exist.
licensePlateFormatError	0x40001122	Invalid license plate format.
managementNodeDoesNotSupportThisOperation	0x40001123	The operation is not supported.
searchByPictureResourceNotConfiged	0x40001124	The conditions for searching picture by picture are not configured.
videoFileEncapsulationFormatNotSupported	0x40001125	The video container format is not supported.
videoPackageFailure	0x40001126	Converting video container format failed.
videoCodingFormatNotSupported	0x40001127	Video coding format is not supported.
monitorOfDeviceArmingDeleteArmingInfo	0x40001129	The camera is armed. Disarm it and try again.
getVideoSourceTypeFailed	0x4000112A	Getting video source type failed.
smartRulesBuildFailed	0x4000112B	Creating VAC rule failed.
smartRulesParseFailed	0x4000112C	Parsing VAC rule failed.
timeRulesBuildFailed	0x4000112D	Creating time rule failed.

Sub Status Code	Error Code	Description
timeRulesParseFailed	0x4000112E	Parsing time rule failed.
monitoInfoInvalid	0x4000112F	Invalid camera information.
addingFailedVersionMismatch	0x40001130	Adding failed. The device version mismatches.
theInformationReturnedAfterCloudAnalysisIsEmpty	0x40001131	No response is returned by the cloud analytic service.
selectingIpAddressOfHostAndSpareNodeFailedCheckTheStatus	0x40001132	Setting IP address for main node and backup node failed. Check the node status.
theSearchIdDoesNotExist	0x40001133	The search ID does not exist.
theSynchronizationIdDoesNotExist	0x40001134	The synchronization ID does not exist.
theUserIdDoesNotExist	0x40001136	The user ID does not exist.
theIndexCodeDoesNotExist	0x40001138	The index code does not exist.
theControlCenterIdDoesNotExist	0x40001139	The control center ID does not exist.
theAreaIdDoesNotExist	0x4000113A	The area ID does not exist.
theArmingLinkagIdDoesNotExist	0x4000113C	The arming relationship ID does not exist.
theListLibraryIdDoesNotExist	0x4000113D	The list library ID does not exist.
invalidCityCode	0x4000113E	Invalid city code.
synchronizingThePasswordOfSpareServerFailed	0x4000113F	Synchronizing backup system password failed.
editingStreamingTypeIsNotSupported	0x40001140	Editing streaming type is not supported.
switchingScheduledTaskToTemporaryTaskIsNotSupported	0x40001141	Switching scheduled task to temporary task is not supported.

Sub Status Code	Error Code	Description
switchingTemporaryTaskToScheduledTaskIsNotSupported	0x40001142	Switching temporary task to scheduled task is not supported.
theTaskIsNotDispatchedOrItIsUpdating	0x40001143	The task is not dispatched or is updating.
thisTaskDoesNotExist	0x40001144	This task does not exist in the cloud analytic service.
duplicatedSchedule	0x40001145	Schedule period cannot be overlapped.
continuousScheduleWithSameAlgorithmTypeShouldBeMerged	0x40001146	The continuous schedule periods with same algorithm type should be merged.
invalidStreamingTimeRange	0x40001147	Invalid streaming time period.
invalidListLibraryType	0x40001148	Invalid list library type.
theNumberOfMatchedResultsShouldBeLargerThan0	0x40001149	The number of search results should be larger than 0.
invalidValueRangeOfSimilarity	0x4000114A	Invalid similarity range.
invalidSortingType	0x4000114B	Invalid sorting type.
noMoreListLibraryCanBeLinkedToTheDevice	0x4000114C	No more lists can be added to one device.
InvalidRecipientAddressFormat	0x4000114D	Invalid address format of result receiver.
creatingClusterFailedTheDongleIsNotPluggedIn	0x4000114E	Insert the dongle before creating cluster.
theURLIsTooLong	0x4000114F	No schedule configured for the task.
noScheduleIsConfiguredForTheTask	0x40001150	No schedule configured for the task.
theDongleIsExpired	0x40001151	Dongle has expired.
dongleException	0x40001152	Dongle exception.
invalidKey	0x40001153	Invalid authorization service key.

Sub Status Code	Error Code	Description
decryptionFailed	0x40001154	Decrypting authorization service failed.
encryptionFailed	0x40001155	Encrypting authorization service failed.
AuthorizeServiceResponseError	0x40001156	Authorization service response exception.
incorrectParameter	0x40001157	Authorization service parameters error.
operationFailed	0x40001158	Operating authorization service error.
noAnalysisResourceOrNoDataInTheListLibrary	0x40001159	No cloud analytic resources or no data in the list library.
calculationException	0x4000115A	Calculation exception.
allocatingList	0x4000115B	Allocating list.
thisOperationIsNotSupportedByTheCloudAnalytics	0x4000115C	This operation is not supported by the cloud analytic serice.
theCloudAnalyticsIsInterrupted	0x4000115D	The operation of cloud analytic serice is interrupted.
theServiceIsNotReady	0x4000115E	The service is not ready.
searchingForExternalAPIFailed	0x4000115F	Searching external interfaces failed.
noOnlineNode	0x40001160	No node is online.
noNodeAllocated	0x40001161	No allocated node.
noMatchedList	0x40001162	No matched list.
allocatingFailedTooManyFacePictureLists	0x40001163	Allocation failed. Too many lists of big data service.
searchIsNotCompletedSearchAgain	0x40001164	Current searching is not completed. Search again.
allocatingListIsNotCompleted	0x40001165	Allocating list is not completed.
searchingForCloudAnalyticsResultsFailed	0x40001166	Searching cloud analytic serice overtime.
noDataOfTheCurrentLibraryFound	0x40001167	No data in the current library. Make sure there is data in the Hbase.

Sub Status Code	Error Code	Description
noFacePictureLibraryIsArmed	0x40001168	No face picture library is armed for big data service.
noAvailableDataSlicingVersionInformationArmFirstAndSliceTheData	0x40001169	Invalid standard version information.
duplicatedOperationDataSlicingIsExecuting	0x4000116A	Slicing failed. Duplicated operation.
slicinDataFailedNoArmedFacePictureLibrary	0x4000116B	Slicing failed. No arming information in the face big data.
GenerateBenchmarkFileFailedSlicingAgain	0x4000116C	Generating sliced file failed. Slice again.
NonprimaryNodesProhibitedFromSlicingData	0x4000116D	Slicing is not allowed by the backup node.
NoReadyNodeToClusterServers	0x4000116E	Creating the cluster failed. No ready node.
NodeManagementServicesOffline	0x4000116F	The node management server is offline.
theCamera(s)OfTheControlCenterAreAlreadyArmed.DisarmThemFirst	0x40001170	Some cameras in control center are already armed. Disarm them and try again.
theCamera(s)OfTheAreaAreAlreadyArmed.DisarmThemFirst	0x40001171	Some cameras in this area are already armed. Disarm them and try again.
configuringHigh-frequencyPeopleDetectionFailed	0x40001172	Configuring high frequency people detection failed.
searchingForHigh-frequencyPeopleDetectionLogsFailed.	0x40001173	Searching detection event logs of high-frequency people detection failed.
gettingDetailsOfSearchedHigh-frequencyPeopleDetectionLogsFailed.	0x40001174	Getting the search result details of frequently appeared person alarms failed.

Sub Status Code	Error Code	Description
theArmedCamerasAlreadyExistInTheControlCenter	0x40001175	Some cameras in control center are already armed.
disarmingFailedTheCamerasNotArmed	0x40001177	Disarming failed. The camera is not armed.
noDataReturned	0x40001178	No response is returned by the big data service.
preallocFailure	0x40001179	Pre-allocating algorithm resource failed.
overDogLimit	0x4000117A	Configuration failed. No more resources can be pre-allocated.
analysisServicesDoNotSupport	0x4000117B	Not supported.
commandAndDispatchServiceError	0x4000117C	Scheduling service of cloud analytic serice error.
engineModuleError	0x4000117D	Engine module of cloud analytic serice error.
streamingServiceError	0x4000117E	Streaming component of cloud analytic serice error.
faceAnalysisModuleError	0x4000117F	Face analysis module of cloud analytic serice error.
vehicleAnalysisModuleError	0x40001180	Vehicle pictures analytic module of cloud analytic serice error.
videoStructuralAnalysisModuleError	0x40001181	Video structuring module of cloud analytic serice error.
postprocessingModuleError	0x40001182	Post-processing module of cloud analytic serice error.
frequentlyAppearedPersonAlarmIsAlreadyConfiguredForListLibrary	0x40001183	Frequently appeared person alarm is already armed for blocklist library.
creatingListLibraryFailed	0x40001184	Creating list library failed.
invalidIdentityKeyOfListLibrary	0x40001185	Invalid identity key of list library.
noMoreDevicesCanBeArmed	0x40001186	No more camera can be added.

Sub Status Code	Error Code	Description
settingAlgorithmTypeForDeviceFailed	0x40001187	Allocating task resource failed.
gettingHighFrequencyPersonDetectionAlarmInformationFailed	0x40001188	Setting frequently appeared person alarm failed.
invalidSearchConfiton	0x40001189	Invalid result.
theTaskIsNotCompleted	0x4000118B	The task is not completed.
resourceOverRemainLimit	0x4000118C	No more resource can be pre-allocated.
frequentlyAppearedPersonAlarmsAlreadyConfiguredForTheCameraDisarmFirstAndTryAgain	0x4000118D	The frequently appeared person alarm of this camera is configured. Delete the arming information and try again.
switchtimedifflesslimit	0x4000123b	Time difference between power on and off should be less than 10 minutes.
associatedFaceLibNumOverLimit	0x40001279	Maximum number of linked face picture libraries reached.
noMorePeopleNumChangeRulesAdded	0x4000128A	Maximum number of people number changing rules reached.
noMoreViolentMotionRulesAdded	0x4000128D	Maximum number of violent motion rules reached.
noMoreLeavePositionRulesAdded	0x4000128E	Maximum number of leaving position rules reached.
SMRDiskNotSupportRa id	0x40001291	SMR disk does not support RAID.
OnlySupportHikAndCustomProtocol	0x400012A3	IPv6 camera can only be added via Device Network SDK or custom protocols.
vehicleEnginesNoResource	0x400012A6	Insufficient vehicle engine resources.
noMoreRunningRulesAdded	0x400012A9	Maximum number of running rules reached.

Sub Status Code	Error Code	Description
noMoreGroupRulesAdded	0x400012AA	Maximum number of people gathering rules reached.
noMoreFailDownRulesAdded	0x400012AB	Maximum number of people falling down rules reached.
noMorePlayCellphoneRulesAdded	0x400012AC	Maximum number of playing cellphone rules reached.
ruleEventTypeDuplicate	0x400012C8	Event type duplicated.
noMoreRetentionRulesAdded	0x400015AD	Maximum number of people retention rules reached.
noMoreSleepOnDutyRulesAdded	0x400015AE	Maximum number of sleeping on duty rules reached.
polygonNotAllowCrossing	0x400015C2	Polygons are not allowed to cross.
configureRuleBeforeAdvanceParam	0x400015F8	Advanced parameters fail to be configured as no rule is configured, please configure rule information first.
behaviorCanNotPackToPic	0x40001603	The behavior model cannot be packaged as a picture algorithm.
noCluster	0x40001608	No cluster created.
NotAssociatedWithOwnChannel	0x400019C1	Current channel is not linked.
AITargetBPCaptureFail	0x400019C5	Capturing reference picture for AI target comparison failed.
AITargetBPToDSPFail	0x400019C6	Sending reference picture to DSP for AI target comparison failed.
AITargetBDuplicateName	0x400019C7	Duplicated name of reference picture for AI target comparison.
audioFileNameWrong	0x400019D0	Incorrect audio file name.
audioFileImportFail	0x400019D1	Importing audio file failed.
NonOperationalStandbyMachine	0x400019F0	Non-operational hot spare.

Sub Status Code	Error Code	Description
MaximumNumberOfDevices	0x400019F1	The maximum number of devices reached.
StandbyMachineCannotBeDeleted	0x400019F2	The hot spare cannot be deleted.
alreadyRunning	0x40002026	The application program is running.
notRunning	0x40002027	The application program is stopped.
packetNotFound	0x40002028	The software packet does not exist.
alreadyExist	0x40002029	The application program already exists.
noMemory	0x4000202A	Insufficient memory.
invalidLicense	0x4000202B	Invalid License.
noClientCertificate	0x40002036	The client certificate is not installed.
noCACertificate	0x40002037	The CA certificate is not installed.
authenticationFailed	0x40002038	Authenticating certificate failed. Check the certificate.
clientCertificateExpired	0x40002039	The client certificate is expired.
clientCertificateRevocation	0x4000203A	The client certificate is revoked.
CACertificateExpired	0x4000203B	The CA certificate is expired.
CACertificateRevocation	0x4000203C	The CA certificate is revoked.
connectFail	0x4000203D	Connection failed.
loginNumExceedLimit	0x4000203F	No more user can log in.
HDMIResolutionIllegal	0x40002040	The HDMI video resolution cannot be larger than that of main and sub stream.
hdFormatFail	0x40002049	Formatting HDD failed.
formattingFailed	0x40002056	Formatting HDD failed.
encryptedFormattingFailed	0x40002057	Formatting encrypted HDD failed.
wrongPassword	0x40002058	Verifying password of SD card failed. Incorrect password.

Sub Status Code	Error Code	Description
audioIsPlayingPleaseWait	0x40002067	Audio is playing. Please wait.
twoWayAudioInProgressPleaseWait	0x40002068	Two-way audio in progress. Please wait.
calibrationPointNumFull	0x40002069	The maximum number of calibration points reached.
completeTheLevelCalibrationFirst	0x4000206A	The level calibration is not set.
completeTheRadarCameraCalibrationFirst	0x4000206B	The radar-camera calibration is not set.
pointsOnStraightLine	0x4000209C	Calibrating failed. The calibration points cannot be one the same line.
TValueLessThanOrEqualZero	0x4000209D	Calibration failed. The T value of the calibration points should be larger than 0.
HBDLibNumOverLimit	0x40002092	The number of human body picture libraries reaches the upper limit
theShieldRegionError	0x40002093	Saving failed. The shielded area should be the ground area where the shielded object is located.
theDetectionAreaError	0x40002094	Saving failed. The detection area should only cover the ground area.
invalidLaneLine	0x40002096	Saving failed. Invalid lane line.
enableITSFunctionOfThisChannelFirst	0x400020A2	Enable ITS function of this channel first.
noCloudStorageServer	0x400020C5	No cloud storage server
NotSupportWithVideoTask	0x400020F3	This function is not supported.
noDetectionArea	0x400050df	No detection area
armingFailed	0x40008000	Arming failed.
disarmingFailed	0x40008001	Disarming failed.
clearAlarmFailed	0x40008002	Clearing alarm failed.
bypassFailed	0x40008003	Bypass failed.

Sub Status Code	Error Code	Description
bypassRecoverFailed	0x40008004	Bypass recovery failed.
outputsOpenFailed	0x40008005	Opening relay failed.
outputsCloseFailed	0x40008006	Closing relay failed.
registerTimeOut	0x40008007	Registering timed out.
registerFailed	0x40008008	Registering failed.
addedByOtherHost	0x40008009	The peripheral is already added by other security control panel.
alreadyAdded	0x4000800A	The peripheral is already added.
armedStatus	0x4000800B	The partition is armed.
bypassStatus	0x4000800C	Bypassed.
zoneNotSupport	0x4000800D	This operation is not supported by the zone.
zoneFault	0x4000800E	The zone is in fault status.
pwdConflict	0x4000800F	Password conflicted.
audioTestEntryFailed	0x40008010	Enabling audio test mode failed.
audioTestRecoveryFailed	0x40008011	Disabling audio test mode failed.
addCardMode	0x40008012	Adding card mode.
searchMode	0x40008013	Search mode.
addRemoterMode	0x40008014	Adding keyfob mode.
registerMode	0x40008015	Registration mode.
exDevNotExist	0x40008016	The peripheral does not exist.
theNumberOfExDevLimited	0x40008017	No peripheral can be added.
sirenConfigFailed	0x40008018	Setting siren failed.
chanCannotRepeatedBinded	0x40008019	This channel is already linked by the zone.
inProgramMode	0x4000801B	The keypad is in programming mode.
inPaceTest	0x4000801C	In pacing mode.
arming	0x4000801D	Arming.

Sub Status Code	Error Code	Description
masterSlavesEnable	0x4000802c	The main-sub relationship has taken effect, the sub radar does not support this operation.
forceTrackNotEnabled	0x4000802d	Mandatory tracking is disabled.
isNotSupportZoneConfigByLocalArea	0x4000802e	This area does not support the zone type.
alarmLineCross	0x4000802f	Trigger lines are overlapped.
zoneDrawingOutOfRange	0x40008030	The drawn zone is out of detection range.
alarmLineDrawingOutOfRange	0x40008031	The drawn alarm trigger line is out of detection range.
hasTargetInWarningArea	0x40008032	The warning zone already contains targets. Whether to enable mandatory arming?
radarModuleConnectFail	0x40008033	Radar module communication failed.
importCfgFilePasswordErr	0x40008034	Incorrect password for importing configuration files.
overAudioFileNumLimit	0x40008038	The number of audio files exceeds the limit.
audioFileNameIsLong	0x40008039	The audio file name is too long.
audioFormatIsWrong	0x4000803a	The audio file format is invalid.
audioFileIsLarge	0x4000803b	The size of the audio file exceeds the limit.
pircamCapTimeOut	0x4000803c	Capturing of pircam timed out.
pircamCapFail	0x4000803d	Capturing of pircam failed.
pircamIsCaping	0x4000803e	The pircam is capturing.
audioFileHasExisted	0x4000803f	The audio file already exists.
subscribeTypeErr	0x4000a016	This metadata type is not supported to be subscribed.
EISError	0x4000A01C	Electronic image stabilization failed. The smart event function is enabled.
jpegPicWithAppendDataError	0x4000A01D	Capturing the thermal graphic failed. Check if the temperature measurement parameters

Sub Status Code	Error Code	Description
		(emissivity, distance, reflective temperature) are configured correctly.
startAppFail	/	Starting running application program failed.
yuvconflict	/	The raw video stream conflicted.
overMaxAppNum	/	No more application program can be uploaded.
noFlash	/	Insufficient flash.
platMismatch	/	The platform mismatches.
emptyEventName	0x400015E0	Event name is empty.
sameEventName	0x400015E1	A same event name already exists.
emptyEventType	0x400015E2	Event type is required.
sameEventType	0x400015E3	A same event type already exists.
maxEventNameReached	0x400015E4	Maximum of events reached.
hotSpareNotAllowedExternalStorage	0x400015FC	External storage is not allowed when hot spare is enabled.
sameCustomProtocolName	0x400015FD	A same protocol name already exists.
maxPTZTriggerChannelReached	0x400015FE	Maximum of channels linked with PTZ reached.
POSCanotAddHolidayPlan	0x400015FF	No POS events during holidays.
eventTypeIsTooLong	0x40001600	Event type is too long.
eventNameIsTooLong	0x40001601	Event name is too long.
PerimeterEnginesNoResource	0x40001602	No more perimeter engines.
invalidProvinceCode	0x40001607	Invalid province code.

StatusCode=5

Sub Status Code	Error Code	Description
badXmlFormat	0x50000001	Invalid XML format.

StatusCode=6

Sub Status Code	Error Code	Description
badParameters	0x60000001	Invalid parameter.
badHostAddress	0x60000002	Invalid host IP address.
badXmlContent	0x60000003	Invalid XML content.
badIPv4Address	0x60000004	Invalid IPv4 address.
badIPv6Address	0x60000005	Invalid IPv6 address.
conflictIPv4Address	0x60000006	IPv4 address conflicted.
conflictIPv6Address	0x60000007	IPv6 address conflicted.
badDomainName	0x60000008	Invalid domain name.
connectSreverFail	0x60000009	Connecting to server failed.
conflictDomainName	0x6000000A	Domain name conflicted.
badPort	0x6000000B	Port number conflicted.
portError	0x6000000C	Port error.
exportErrorData	0x6000000D	Importing data failed.
badNetMask	0x6000000E	Invalid sub-net mask.
badVersion	0x6000000F	Version mismatches.
badDevType	0x60000010	Device type mismatches.
badLanguage	0x60000011	Language mismatches.
incorrectUserNameOrPassword	0x60000012	Incorrect user name or password.
invalidStoragePoolOfCloudServer	0x60000013	Invalid storage pool. The storage pool is not configured or incorrect ID.
noFreeSpaceOfStoragePool	0x60000014	Storage pool is full.
riskPassword	0x60000015	Risky password.
UnSupportCapture	0x60000016	Capturing in 4096*2160 or 3072*2048 resolution is not supported when H.264+ is enabled.

Sub Status Code	Error Code	Description
userPwdLenUnder8	0x60000023	At least two kinds of characters, including digits, letters, and symbols, should be contained in the password.
userPwdNameSame	0x60000025	Duplicated password.
userPwdNameMirror	0x60000026	The password cannot be the reverse order of user name.
beyondARGSRangeLimit	0x60000027	The parameter value is out of limit.
DetectionLineOutofDetectionRegion	0x60000085	The rule line is out of region.
DetectionRegionError	0x60000086	Rule region error. Make sure the rule region is convex polygon.
DetectionRegionOutOfCountingRegion	0x60000087	The rule region must be marked as red frame.
PedalAreaError	0x60000088	The pedal area must be in the rule region.
DetectionAreaABError	0x60000089	The detection region A and B must be in the a rule frame.
ABRegionCannotIntersect	0x6000008a	Region A and B cannot be overlapped.
customHBPIDError	0x6000008b	Incorrect ID of custom human body picture library
customHBPIDRepeat	0x6000008c	Duplicated ID of custom human body picture library
dataVersionsInHBDLibMismatches	0x6000008d	Database versions mismatches of human body picture library
invalidHBPID	0x6000008e	Invalid human body picture PID
invalidHBDID	0x6000008f	Invalid ID of human body picture library
humanLibraryError	0x60000090	Error of human body picture library

Sub Status Code	Error Code	Description
humanLibraryNumError	0x60000091	No more human body picture library can be added
humanImagesNumError	0x60000092	No more human body picture can be added
noHumanInThePicture	0x60000093	Modeling failed, no human body in the picture
analysisEnginesNoResourceErr or	0x60001000	No analysis engine.
analysisEnginesUsageExced	0x60001001	The engine usage is overloaded.
PicAnalysisNoResourceError	0x60001002	No analysis engine provided for picture secondary recognition.
analysisEnginesLoadingError	0x60001003	Initializing analysis engine.
analysisEnginesAbnormaError	0x60001004	Analysis engine exception.
analysisEnginesFacelibImporting	0x60001005	Importing pictures to face picture library. Failed to edit analysis engine parameters.
analysisEnginesAssociatedChannel	0x60001006	The analysis engine is linked to channel.
smdEncodingNoResource	0x60001007	Insufficient motion detection encoding resources.
smdDecodingNoResource	0x60001008	Insufficient motion detection decoding resources.
diskError	0x60001009	HDD error.
diskFull	0x6000100a	HDD full.
facelibDataProcessing	0x6000100b	Handling face picture library data.
capturePackageFailed	0x6000100c	Capturing packet failed.
capturePackageProcessing	0x6000100d	Capturing packet.
noSupportWithPlaybackAbstract	0x6000100e	This function is not supported. Playback by video synopsis is enabled.

Sub Status Code	Error Code	Description
insufficientNetworkBandwidth	0x6000100f	Insufficient network bandwidth.
tapeLibNeedStopArchive	0x60001010	Stop the filing operation of tape library first.
identityKeyError	0x60001011	Incorrect interaction command.
identityKeyMissing	0x60001012	The interaction command is lost.
noSupportWithPersonDensityDetect	0x60001013	This function is not supported. The people density detection is enabled.
ipcResolutionOverflow	0x60001014	The configured resolution of network camera is invalid.
ipcBitrateOverflow	0x60001015	The configured bit rate of network camera is invalid.
tooGreatTimeDifference	0x60001016	Too large time difference between device and server.
noSupportWithPlayback	0x60001017	This function is not supported. Playback is enabled.
channelNoSupportWithSMD	0x60001018	This function is not supported. Motion detection is enabled.
channelNoSupportWithFD	0x60001019	This function is not supported. Face capture is enabled.
illegalPhoneNumber	0x6000101a	Invalid phone number.
illegalCertificateNumber	0x6000101b	Invalid certificate No.
linkedCameraOutLimit	0x6000101c	Connecting camera timed out.
achieveMaxChannelLimit	0x6000101e	No more channels are allowed.
humanMisInfoFilterEnabledChanNumError	0x6000101f	No more channels are allowed to enable preventing false alarm.
humanEnginesNoResource	0x60001020	Insufficient human body analysis engine resources.
taskNumberOverflow	0x60001021	No more tasks can be added.

Sub Status Code	Error Code	Description
collisionTimeOverflow	0x60001022	No more comparison duration can be configured.
invalidTaskID	0x60001023	Invalid task ID.
eventNotSupport	0x60001024	Event subscription is not supported.
invalidEZVIZSecretKey	0x60001034	Invalid verification code for Hik-Connect.
needDoubleVerification	0x60001042	Double verification required
noDoubleVerificationUser	0x60001043	No double verification user
timeSpanNumOverLimit	0x60001044	Max. number of time buckets reached
channelNumOverLimit	0x60001045	Max. number of channels reached
noSearchIDResource	0x60001046	Insufficient searchID resources
noSupportDeleteStrangerLib	0x60001051	Deleting stranger library is not supported
noSupportCreateStrangerLib	0x60001052	Creating stranger library is not supported
behaviorAnalysisRuleInfoError	0x60001053	Behavior analysis rule parameters error.
safetyHelmetParamError	0x60001054	Hard hat parameters error.
OneChannelOnlyCanBindOneEngine	0x60001077	No more engines can be bound.
engineTypeMismatch	0x60001079	Engine type mismatched.
badUpgradePackage	0x6000107A	Invalid upgrade package.
AudioFileNameDuplicate	0x60001135	Duplicated audio file name.
CurrentAudioFileAIRuleInUseAIreadyDelete	0x60001136	The AI rule linkage related to current audio file has been deleted.
TransitionUseEmmc	0x60002000	Starting device failed. The EMMC is overused.

Sub Status Code	Error Code	Description
AdaptiveStreamNotEnabled	0x60002001	The stream self-adaptive function is not enabled.
AdaptiveStreamAndVariableBitRateEnabled	0x60002002	Stream self-adaptive and variable bitrate function cannot be enabled at the same time.
noSafetyHelmetRegion	0x60002023	The hard hat detection area is not configured (if users save their settings without configuring the arming area, they should be prompted to configure one).
unclosedSafetyHelmet	0x60002024	The hard hat detection is enabled (If users save their settings after deleting the arming area, they should be prompted to disable hard hat detection first and then delete the arming area).
width/heightRatioOfPictureError	0x6000202C	The width/height ratio of the uploaded picture should be in the range from 1:2 to 2:1.
PTZNotInitialized	0x6000202E	PTZ is not initialized.
PTZSelfChecking	0x6000202F	PTZ is self-checking.
PTZLocked	0x60002030	PTZ is locked.
advancedParametersError	0x60002031	Auto-switch interval in advanced parameters cannot be shorter than parking tolerance for illegal parking detection in speed dome rule settings.
resolutionError	0x60005003	Invalid resolution
deployExceedMax	0x60006018	The arming connections exceed the maximum number.
detectorTypeMismatch	0x60008000	The detector type mismatched.
nameExist	0x60008001	The name already exists.

Sub Status Code	Error Code	Description
uploadImageSizeError	0x60008016	The size of the uploaded picture is larger than 5 MB.
laneAndRegionOverlap	/	The lanes are overlapped.
unitConfigurationNotInEffect	/	Invalid unit parameter.
ruleAndShieldingMaskConflict	/	The line-rule region overlaps with the shielded area.
wholeRuleInShieldingMask	/	There are complete temperature measurement rules in the shielded area.
LogDiskNotSetReadOnlyInGroupMode	0x60001100	The log HDD in the HDD group cannot be set to read-only.
LogDiskNotSetReDundancyInGroupMode	0x60001101	The log HDD in the HDD group cannot be set to redundancy.
holidayNameContainChineseOrSpecialChar	0x60001080	No Chinese and special characters allowed in holiday name.
genderValueError	0x60001081	Invalid gender.
certificateTypeValueError	0x60001082	Invalid identification type.
personInfoExtendValueIsTooLong	0x60001083	The length of customized tags exceeds limit.
personInfoExtendValueContainsInvalidChar	0x60001084	Invalid characters are not allowed in customized tags of the face picture library.
excelHeaderError	0x60001085	Excel header error.
intelligentTrafficMutexWithHighFrames	0x60008014	Please disable all functions of traffic incident detection, violation enforcement, and traffic data collection, or adjust the video frame rate to that lower than 50 fps.
intelligentTrafficMutexWithHighFramesEx	0x60008018	Please disable all functions of traffic incident detection, violation enforcement, traffic data collection, and vehicle

Sub Status Code	Error Code	Description
		detection, or adjust the video frame rate to that lower than 50 fps.

StatusCode=7

SubStatusCode	Error Code	Description
rebootRequired	0x70000001	Reboot to take effect.

B.6 Error Codes Categorized by Functional Modules

The error codes returned during the text protocol integration is categorized by different functional modules. See the error codes, error descriptions, and debugging suggestions in the table below.

Public Function Module (Error Codes Range: 0x00000000, from 0x00100001 to 0x001fffff)

Error String	Error Code	Description	Debugging Suggestion
success	0x00000000	Succeeded.	
deviceNotActivate d	0x00100001	The device is not activated.	Activate the device.
deviceNoPermission	0x00100002	Device operation failed. No permission.	Update user's permission.
deviceNotSupport	0x00100003	This function is not supported.	Check the device capability set and call the API corresponding to supported function.
deviceResourceNotEnough	0x00100004	Insufficient resources.	Release resources.
dataFormatError	0x00100005	Invalid message format.	
resetError	0x00100006	Restoring to factory settings failed. Reactivating device is required after the device is	

Error String	Error Code	Description	Debugging Suggestion
		reboot as the Reset button may be stuck.	
parameterError	0x00100007	Incorrect parameter	
	0x00100100	Invalid channel	Check if the channel is valid.
	0x00100101	NPQ live view is not supported for stream encryption.	Replace streaming mode for stream encryption.
	0x00100102	No more channels are allowed for NPQ streaming.	Reduce NPQ streaming channels and try again.
	0x00100103	The stream type is not supported.	Check the requested stream type.
	0x00100104	The number of connections exceeded limit.	Reduce the number of streaming clients and try again.
	0x00100105	Not enough bandwidth.	Reduce the number of remote streaming channels.

User Function Module (Error Codes Range: from 0x00200001 to 0x002fffff)

Error String	Error Code	Description	Debugging Suggestion
passwordError	0x00200001	Incorrect user name or password.	Check if the password is correct.
userNameNotExist	0x00200002	The account does not exist.	Check if the account exists, or add the account.
userNameLocked	0x00200003	The account is locked.	Wait for the device to unlock.
userNumLimited	0x00200004	The number of users allowed to log in exceeded the upper limit.	Log out.
lowPrivilege	0x00200005	No permissions for this operation	For users operations, check the following situations: <ul style="list-style-type: none"> • Deleting your own account is not allowed. • Editing your own level or permission is not allowed.

Error String	Error Code	Description	Debugging Suggestion
			<ul style="list-style-type: none"> Getting information about users with higher permission is not allowed. Elevating the user's level or permission is not allowed. <p>For other operations, check according to the following measures: If operations unrelated to user's permission configuration failed, you can check the user type and permission, if not solved, contact the developers.</p>
incorrectUserNameOrPassword	0x00200006	Incorrect user name or password	Check if the configured user name and password are matched. If not, contact the administrator to configure again. If the administrator forgets the password, reset the password of the device.
riskPassword	0x00200007	Risk password	Low password strength. Change password again.
passwordMustContainMorethan8Characters	0x00200008	The password length must be greater than or equal to 8.	Check if the password length is greater than or equal to 8. If not, change password again.
passwordLenNoMoreThan16	0x00200009	The password length cannot be greater than 16.	Check if the password length is greater than 16. If yes, change password again.
adminUserNotAllowedModify	0x0020000a	Editing admin information is not allowed.	Check if the edited account is admin.
confirmPasswordError	0x0020000b	Incorrect confirm password.	Check the confirm password.
passwordMustContainMorethan2Types	0x0020000c	The password must contain at least two or more of followings: numbers, lowercase,	Check if the configured password conforms the requirements.

Error String	Error Code	Description	Debugging Suggestion
		uppercase, and special characters.	
passwordContainUserName	0x0020000d	The password cannot contain the user name.	Check if the password contains the user name.
userPwdNameMirror	0x0020000e	The password cannot be reversed user name.	Check if the password is reversed user name.

Time Function Module (Error Codes Range: from 0x00300001 to 0x003fffff)

Error String	Error Code	Description	Debugging Suggestion
manualAdjustmentFailed	0x00300001	Time synchronization failed.	
NTPError	0x00300002	Invalid NTP server address.	Check if the NTP server address is valid.
timeFormatError	0x00300003	Incorrect time format during time calibration. For example, the time in ISO 8601 format should be "2018-02-01T19:54:04", but the applied time is "2018-02-01 19:54:04".	Incorrect message format or incorrect time format.
beyondTimeRangeLimit	0x00300004	The calibration time is not within the time range supported by the device.	Get the device capability and check if the configured time is within the time range supported by the device.
endtimeEarlierThanBeginTime	0x00300005	The start time of the validity period cannot be later than the end time.	Check if the start time and end time are valid.

Network Function Module (Error Codes Range: from 0x00400001 to 0x004ffff)

Error String	Error Code	Description	Debugging Suggestion
domainNameParseFailed	0x00400001	Parsing domain name failed.	
PPPOEConnectedFailed	0x00400002	Connecting PPPOE to the network failed.	
FTPConnectedFailed	0x00400003	The FTP server is disconnected.	
deviceIPConflicted	0x00400004	IP addresses of devices conflicted.	
libraryConnectedFailed	0x00400005	The image and video library is disconnected.	
fileUploadFailed	0x00400006	Uploading failed.	Check if the network connection is normal. If yes, contact after-sales.
storSerDownloadFileFailed	0x00400007	Downloading failed.	Check if the network connection is normal. If yes, contact after-sales.
storSerDownloadFileSizeZero	0x00400008	The size of file downloaded from the storage service is 0.	Check if the network connection is normal. If yes, contact after-sales.
storSerNotConfig	0x00400009	Storage service is not configured.	Check if the configuration is correct.
badHostAddress	0x0040000a	Host address error	Check if the configuration is correct.
badIPv4Address	0x0040000b	Incorrect IPv4 address.	Check if the configuration is correct.
badIPv6Address	0x0040000c	Incorrect IPv6 address.	Check if the configuration is correct.
conflictIPv4Address	0x0040000d	IPv4 address conflict.	Check the configuration status of IPV4 in the network.
conflictIPv6Address	0x0040000e	IPv6 address conflict	Check the configuration status of IPV6 in the network.

Error String	Error Code	Description	Debugging Suggestion
badDomainName	0x0040000f	Incorrect domain name.	Check if the configuration is correct.
connectSreverFail	0x00400010	Connecting to server failed.	Check if the network is normal and check if the configuration is correct.
conflictDomainNa me	0x00400011	Domain name conflict.	Check if the configuration is correct.
badPort	0x00400012	Port conflict.	Check if the configuration is correct.
portError	0x00400013	Port error	Check if the configuration is correct.
badNetMask	0x00400014	Subnet mask error	Check if the configuration is correct.
badVersion	0x00400015	Version mismatch	Check if the version is correct.
badDns	0x00400016	DNS error	Check if the configuration is correct.
badMTU	0x00400017	MTU error	Check if the configuration is correct.
badGateway	0x00400018	Wrong gateway	Check if the configuration is correct.
urlDownloadFail	0x00400019	Downloading via URL failed.	Check if the network is normal and check if the URL is correct.
deployExceedMax	0x0040001a	The number of armed channels exceeds the maximum number of connections.	Get the supported maximum number of arming and the number of armed channels.

Maintenance Function Module (Error Codes Range: from 0x00500001 to 0x005ffff)

Error String	Error Code	Description	Debugging Suggestion
upgradeXMLForm atError	0x00500001	Incorrect XML upgrading request.	Check if the upgrade file is correct. If the file is correct, try the local upgrade.
upgradeContentEr ror	0x00500002	Incorrect upgrading request content.	Check if the upgrade file is correct. If the file is correct, try the local upgrade.
noUpgradePermis sion	0x00500003	No upgrade permission.	Switch to admin account or ask admin for advanced operation permission.
upgrading	0x00500004	Upgrading...	Wait for the upgrade to complete.
receiveUpgradePa ckageError	0x00500005	Receiving upgrade package failed.	Check if the network is normal.
upgradePackageL anguageMismatch	0x00500006	Upgrade package language mismatch.	Check the language type of upgrade package and the device.
upgradePackageM ismatch	0x00500007	Upgrade file does not match with the device type.	Check the type of upgrade package and device.
OEMCodeMismat ch	0x00500008	Upgrade package error. The OEM code mismatch.	Contact after-sales to get the correct upgrade package.
versionMismatch	0x00500009	Upgrade file version mismatch.	Contact after-sales to get the correct upgrade package.
upgradeHalfFailed	0x0050000c	Error occurred in the halfway of device upgrading. Flash error or cache error.	
deviceParameterI mportFailed	0x0050000d	Importing device parameters failed. Device model, version, or platform mismatches.	

Error String	Error Code	Description	Debugging Suggestion
deviceEncryptionError	0x0050000e	Upgrade package mismatches. Device encryption error.	
SDCardFormatError	0x00500025	Formatting SD card failed.	
SDCardLoadFailed	0x00500026	Loading page failed after the SD card is inserted.	
NASFailed	0x00500027	Mounting NAS failed.	
hardDiskError	0x00500028	HDD exception (possible reasons: HDD does not exist, incompatible, encrypted, insufficient capacity, formatting exception, array exception, array incompatible, etc.)	
upgradeError	0x00500030	Upgrade error	
upgradePackageSizeMismath	0x00500032	Mismatch between the actual size of the downloaded upgrade package and the size in the upgrading request.	
upgradePackageSizeExceeded	0x00500033	The size of the package exceeded that of the partition.	
domainNameParseExceptionFailedForDownload	0x00500034	Parsing the domain name of the address for downloading failed.	
netWorkUnstable	0x00500035	Unstable network. Downloading timed out or the maximum number of attempts reached.	
digestValueMismatch	0x00500036	Mismatched digest value.	
signatureVerifyFailed	0x00500037	Verifying the signature failed.	

Error String	Error Code	Description	Debugging Suggestion
innerFormatError	0x00500038	Incorrect inner format of the upgrade package.	
memoryNotEnough	0x00500039	Insufficient memory.	
burnFailed	0x0050003a	Burning firmware failed.	
unknownError	0x0050003b	Unknown error occurred in the underlying APIs.	
userCancel	0x0050003c	User requested cancel of current operation.	
systemResume	0x0050003d	Upgrading failed. You can resume via the backup system or minimum system.	
	0x00500080	Upgrade file is not found.	Check if the upgrade package path is too long or if there is a correct upgrade package under the upgrade package path.
	0x00500081	Upgrade file does not match with the engine type.	Select the upgrade package matched with the device engine type.
	0x00500082	Parsing camera domain name failed.	Confirm if the device is correctly configured DNS service and if the camera domain is valid.
	0x00500083	Camera network is unreachable.	Confirm if the local network can access the network where the added channel located.

Live View Module (Error Codes Range: from 0x00600001 to 0x006fffff)

Error String	Error Code	Description	Debugging Suggestion
liveViewFailed	0x00600001	Live view failed. The number of streaming channels exceeded limit.	
	0x00600002	Request packaging format exception.	Check the packaging format of requested live view.
	0x00600003	NPQ will be unavailable after enabling EHome 2.x.	When EHome 2.x is enable, use other live view mode.
	0x00600005	NPQ live view is not supported for channel-zero.	User other live view mode for channel-zero.
	0x00600007	Only virtual stream supports NPQ live view.	Switch to virtual strem.
	0x0060000A	The IP channel is offline.	Check if the IP channel is online and try again.
	0x0060000B	Live view transcoding is not supported by the device.	Use other stream type for live view.
	0x0060000C	Channel-zero is not enabled.	Enable channel-zero before starting live view of channel-zero.
	0x0060000D	Transcoding capability exceeded limit.	Reduce camera resolution or the number of transcoding channels.
	0x00600010	The channel does not have sub-stream.	Use main stream mode for live view.
	0x00600011	NPQ live view is not supported by the device.	Switch to other live view mode.
	0x00600012	NPQ function is disabled.	Enable NPQ function or switch to other live view mode.

Playback Module (Error Codes Range: from 0x00700001 to 0x007fffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00700001	Playback failed. Up to one channel's playback is supported.	
	0x00700002	The speed of playback displayed on video wall is not supported.	Reduce the playback speed.
	0x00700003	The transmission rate of playback stream is too high.	Reduce the transmission rate of playback stream.
	0x00700004	The encoding type of playback stream is not supported.	Provide the stream with encoding type supported by device.
	0x00700005	The container format of playback stream is not supported.	Provide the stream with container format supported by device.
	0x00700007	Exception occurred when decoding playback stream Possible reasons: displaying on video wall exception, image exception, display exception, decoding exception, image is stuck, black screen, invalid stream type, live view is stuck, audio decoding exception, and blurred screen.	
	0x00700008	Playback video does not exit, or searching failed.	Search again or check if HDD is normal.
	0x00700009	Playback time parameter error.	Check if the time period of searched video is correct and try again.
	0x0070000A	Invalid video type.	Select the correct video type to search.
	0x0070000B	Invalid time type.	Select the correct time type to search.

Error String	Error Code	Description	Debugging Suggestion
	0x0070000C	Invalid event parameter.	Select the correct event parameter to search.
	0x0070000D	Invalid event type.	Select the correct event type to search.
	0x0070000E	The device does not support smart search.	Select the non smart search mode to search.
	0x0070000F	Invalid smart event type.	Select the correct smart event type to search.
	0x00700010	Invalid dynamic analysis sensitivity.	Select the correct sensitivity to search video.
	0x00700011	Reverse playback is not supported.	Select the correct playback mode.
	0x00700012	Invalid file status.	Select the correct file status to search.
	0x00700013	Invalid searching start position.	Use the correct searching start position to search.
	0x00700014	Invalid maximum number of searching.	Use the correct maximum number of searching to search.

Capture Module (Error Codes Range: from 0x00800001 to 0x008fffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00800001	Manual capture failed.	

Two-Way Audio Module (Error Codes Range: from 0x00900001 to 0x009fffff)

Error String	Error Code	Description	Debugging Suggestion
startFailed	0x00900001	Starting two-way audio failed. Audio loss or driver error.	
codingFormatNot Match	0x00900002	The encoding format of the intercom is inconsistent, and the negotiation fails	Check or capture the packets on the platform, then analyze if the audio

Error String	Error Code	Description	Debugging Suggestion
			encoding formats negotiated by both sides are consistent.
dialedIsBusy	0x00900003	The intercom party is already in the intercom and can no longer respond to the intercom	Check if the intercom party is already in the intercom, if not, get the protocol message and analyze the response message.
destinationLongNumberError	0x00900004	The requested destination long number is wrong	Check or capture the packets on the platform, then analyze the long number.

Video Storage Module (Error Codes Range: from 0x00a00001 to 0x00afffff)

Error String	Error Code	Description	Debugging Suggestion
videoSearchFailed	0x00a00001	Searching videos failed.	No resource stored in the device.
notFindStorageMedium	0x00a00002	No storage medium found.	
videoDownloadFailed	0x00a00003	Downloading videos failed.	

Picture Storage Module (Error Codes Range: from 0x00b00001 to 0x00bfffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00b00001	Searching pictures failed.	No picture resource.

IO Function Model (Error Codes Range: from 0x00c00001 to 0x00cfffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00c00001	Invalid alarm input No.	
	0x00c00002	Invalid alarm output No.	

Event Function Module (Error Codes Range: from 0x00d00001 to 0x00dfffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00d00001	Incorrect event rule.	Refer to the manual for correct configuration.

Parking Service Module (Error Codes Range: from 0x00e00001 to 0x00efffff)

Error String	Error Code	Description	Debugging Suggestion
	0x00e00001	The vehicle with parking pass already exists.	Parking pass is created by license plate, you need to check if the parking pass for this license plate already created.
	0x00e00002	The license plate number is required.	

General Function Module (Error Codes Range: from 0x00f00001 to 0x00fffff)

Error String	Error Code	Description	Debugging Suggestion
noMemory	0x00f00001	Insufficient device memory (heap space allocation failed).	Check the free memory and send logs to the developer for analysis.
deviceBusy	0x00f00002	The device is busy or the device is not responding.	Send logs to the developers for analysis. For fingerprint collection, face collection, file application, and file uploading services, check if the last operation is completed.
notSupport	0x00f00003	The URL is not supported by the device.	Capture the packets, check if the applied URL exists in the PMP platform. If yes, send the URL to the developer for analysis.

Error String	Error Code	Description	Debugging Suggestion
methodNotAllowed	0x00f00004	HTTP method is not allowed.	Capture the packets, check the method corresponding to the URL in the PMP platform.
invalidOperation	0x00f00005	Invalid operation of API command.	
IDNotExist	0x00f00006	The ID does not exist (the URL should contain ID, but the actual URL does not contain the ID).	Capture the packets and check if the ID included in the URL is correct.
invalidID	0x00f00007	Invalid ID (the ID in the URL exceeds the capability set or the ID format is invalid).	Capture the packets and check if the ID included in the URL is correct. Get the capabilities of URL and check the ID range.
invalidIURL	0x00f00008	The content after the "?" in the URL is wrong.	Capture the packets and check if the URL is correct.
deviceAckTimeOut	0x00f00009	Device response timed out.	If the communication with the external module timed out, check if the external module is offline. When the above situation is eliminated, send logs to the developer for analysis.
badXmlFormat	0x00f0000a	XML format error	
badJsonFormat	0x00f0000b	JSON format error	
badURLFormat	0x00f0000c	URL format error	Get the URL and check if it is correct.
badXmlContent	0x00f0000d	XML message error:	

Error String	Error Code	Description	Debugging Suggestion
		<ul style="list-style-type: none"> The message contains only URL but no message body The required node is not configured. Node value exceeds the range limit (incorrect node value). 	
badJsonContent	0x00f0000e	<p>JSON message error:</p> <ul style="list-style-type: none"> The message contains only URL but no message body The required node is not configured. Node value exceeds the range limit (incorrect node value). 	
messageParametersLack	0x00f0000f	The required node does not exists.	
invalidSearchConditions	0x00f00010	Invalid search condition, search again.	Check if searchID is correct.
operObjectNotExist	0x00f00011	The object does not exist (for the operations about door, alarm IO, the object is not added).	Check if door lock is connected.

Door Control Module (Error Codes Range: from 0x01000001 to 0x010fffff)

Error String	Error Code	Description	Debugging Suggestion
multiAuthentication Failed	0x01000001	Multi-factor authentication status operation failed.	
securityModuleOffline	0x01000002	The safety door control module is offline and fails to open the door.	Check if the safety door control is offline.

Schedule Template Module (Error Codes Range: from 0x01100001 to 0x011ffff)

Error String	Error Code	Description	Debugging Suggestion
planNumberConflict	0x01100001	Plan number conflict.	
timeOverlap	0x01100002	Time period conflict.	Check the message to find out if there is a time overlap of different time periods in one day.

Person Information Module (Error Codes Range: from 0x01200001 to 0x012ffff)

Error String	Error Code	Description	Debugging Suggestion

Certificate Module (Error Codes Range: from 0x01300001 to 0x013ffff)

Error String	Error Code	Description	Debugging Suggestion

Security Function Module (Error Codes Range: from 0x01400001 to 0x014ffff)

Error String	Error Code	Description	Debugging Suggestion
decryptFailed	0x01400001	Decryption failed, when decrypting sensitive information fields or importing data files.	The import secret key should be consistent with the export.
certificateNotmatch	0x01400003	Certificates mismatched, SSL/TLS public and private keys need to be matched in pairs.	The public and private keys need to be generated at the same time.
notActivated	0x01400004	Device is not activated.	Activate the device by tools such as SADP before use.
hasActivated	0x01400005	Device has been activated.	
forbiddenIP	0x01400006	IP address is banned	IP address is banned when illegal login attempts exceed the upper limit.

Error String	Error Code	Description	Debugging Suggestion
bondMacAddressNotMatch	0x01400007	The MAC address does not match the user.	Check if the specific MAC address has linked to the user.
bondIpAddressNotMatch	0x01400008	IP address does not match the user.	Check if the specific IP address has linked to the user.
badAuthorization	0x01400009	Triggered by illegal login	Incorrect password triggered the illegal login.

Advertising Function Module (Error Codes Range: from 0x01500001 to 0x015ffff)

Error String	Error Code	Description	Debugging Suggestion
materialDownloadFailed	0x01500001	Material download failed.	<ul style="list-style-type: none"> • Check if the network connection is normal. • Check if the device is running normally. • Check the log print.
materialNumberIsOver	0x01500002	The number of materials in the program list reached the upper limit.	Check if the number of materials in applied program list exceeded the limit.

