

GDS371X Firmware Release Notes

Table of Content

Table of Content.....	1
FIRMWARE VERSION 1.0.13.15	16
PRODUCT NAME.....	16
DATE	16
FIRMWARE FILE INFORMATION	16
SUMMARY OF UPDATE	16
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	17
FIRMWARE VERSION 1.0.13.10	19
PRODUCT NAME.....	19
DATE	19
FIRMWARE FILE INFORMATION	19
SUMMARY OF UPDATE	19
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	20
ENHANCEMENT	20
BUG FIX	20
KNOWN ISSUES.....	20
NEW P-VALUE	21
NEW HTTP API:	21
NEW FEATURES OVERVIEW.....	22
<i>SIP Calling Trigger Alarm Output.....</i>	<i>22</i>
<i>Alarm Out Status Icon in WebUI.....</i>	<i>23</i>
FIRMWARE VERSION 1.0.13.9	25
PRODUCT NAME.....	25
DATE	25
FIRMWARE FILE INFORMATION	25
SUMMARY OF UPDATE	25
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	26
ENHANCEMENT	26
BUG FIX	26
KNOWN ISSUES.....	27
NEW P-VALUE	28

NEW HTTP API:	28
NEW FEATURES OVERVIEW	29
<i>SCHEDULE FOR ENABLE BACKGROUND LIGHT</i>	29

FIRMWARE VERSION 1.0.13.531

PRODUCT NAME.....	31
DATE	31
SUMMARY OF UPDATE	31
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	31
ENHANCEMENT	32
BUG FIX	32
KNOWN ISSUES.....	32
NEW P-VALUE	33
UPDATED P-VALUE.....	34
NEW HTTP API:	34
NEW FEATURES OVERVIEW	35
<i>CHANGED “ZERO CONFIG” TO “3CX AUTO PROVISION”</i>	35
<i>ENHANCE ALARM OUTPUT DURATION</i>	36
<i>LIGHT BRIGHTNESS ADJUSTABLE AT KEYPAD BLUE LED</i>	37
<i>SEND SIP LOG</i>	38
<i>802.1X SUPPORT</i>	39
<i>SEND “ENVET TYPE”, “USERNAME”, “CARD ID” IN EMAIL WITH OPEN DOOR EVENT</i>	40

FIRMWARE VERSION 1.0.13.242

PRODUCT NAME.....	42
DATE	42
SUMMARY OF UPDATE	42
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	42
ENHANCEMENT	43
BUG FIX	43
KNOWN ISSUES.....	43
NEW P-VALUE	44
NEW HTTP API:	45
NEW FEATURES OVERVIEW	46
<i>HTTPS AS DEFAULT CFG PROVISIONING METHOD (ZOOM COMPATIBLE)</i>	46
<i>INTERVAL OF “ONHOOK TIMER AFTER REMOTE OPEN DOOR(S)” CONFIGURABLE</i>	47
<i>DELAY FOR SNAPSHOTS TAKEN WHEN “DOOR OPENED” OR “DOORBELL PRESSED”</i> ...	48
<i>ADMIN AUDIT LOGGING TO THE EVENT LOG FUNCTIONALITY [ITSP: MASERGY]</i>	49
<i>DEFINE THE TLS PROTOCOL LEVEL</i>	50
<i>IMPROVED ALARM EMAIL SUBJECT AND TEXT</i>	51
<i>EMERGENCY PIN TO RE-ENABLE KEEP DOOR OPEN</i>	52

WEBUI DISPLAY CERTIFICATE TYPE INFORMATION	53
ACCESS WITH RTSP PASSWORD IN ONVIF	54
SNI EXTENSION ON TLS [ITSP NETIA]	55
BIRGHTNESS/CONTRAST/SATURATION ADJUSTMENT IN LIVEVIEW PAGE	56

FIRMWARE VERSION 1.0.11.23..... 58

PRODUCT NAME	58
DATE	58
SUMMARY OF UPDATE	58
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	58
ENHANCEMENT	59
BUG FIX	59
KNOWN ISSUES	59
NEW P-VALUE	60
UPDATED P-VALUE	60
NEW HTTP API:	60
NEW FEATURES OVERVIEW	61
<i>DISABLE ALARM SIREN IN TRIGGERED ALARM CALL</i>	61
<i>MULTPLE SCHEDULES FOR "KEEP DOOR OPEN"</i>	62
<i>GRANULAR TIME DURATION OF DITITAL OUTPUT</i>	64
<i>SEND PIN VIA WIEGAND WHEN HTTP API OPEN DOOR EXECUTED</i>	65
<i>NO "#" REQUIRED AFTER PIN INPUT WHEN "DISABLE KEYPAD SIP NUMBER DIALING"</i> ..	67
<i>FIRMWARE UPGRADE VIA LOCAL FILE UPLOAD</i>	69

FIRMWARE VERSION 1.0.11.18..... 72

PRODUCT NAME	72
DATE	72
SUMMARY OF UPDATE	72
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	72
ENHANCEMENT	73
BUG FIX	73
KNOWN ISSUES	73
NEW P-VALUE	74
NEW HTTP API:	75
NEW FEATURES OVERVIEW	76
<i>SNMP SUPPORT</i>	76

FIRMWARE VERSION 1.0.11.15..... 78

PRODUCT NAME	78
DATE	78
SUMMARY OF UPDATE	78

FIRMWARE APPLIES TO BELOW HW VERSION ONLY	78
ENHANCEMENT	79
BUG FIX	79
KNOWN ISSUES.....	79
NEW P-VALUE	80
NEW HTTP API:	80
NEW FEATURES OVERVIEW	81
<i>DOORBELL CALL DIFFERENT NUMBERS BASED ON DIFFERENT SCHEDULE</i>	<i>81</i>

FIRMWARE VERSION 1.0.11.13..... 84

PRODUCT NAME.....	84
DATE	84
SUMMARY OF UPDATE	84
WARNING:	84
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	85
ENHANCEMENT	86
BUG FIX	86
KNOWN ISSUES.....	86
UPDATED P-VALUE.....	87
NEW HTTP API:	87
NEW FEATURES OVERVIEW	88
<i>LOG NON-SCHEDULED ACCESS ALARM IN EVENT LOG</i>	<i>88</i>

FIRMWARE VERSION 1.0.9.9 92

PRODUCT NAME.....	92
DATE	92
SUMMARY OF UPDATE	92
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	92
ENHANCEMENT	93
BUG FIX	93
KNOWN ISSUES.....	93
NEW P-VALUE	94
NEW HTTP API:	94
NEW FEATURES OVERVIEW	95
<i>CISCO WEBEX IOT: SIP URI SCHEME WHEN USING TLS</i>	<i>95</i>
<i>CISCO WEBEX IOT: SIP INSTANCE ID</i>	<i>96</i>
<i>ADDED TIPS FOR OPENVPN PORT</i>	<i>97</i>

FIRMWARE VERSION 1.0.9.6 99

PRODUCT NAME.....	99
DATE	99

SUMMARY OF UPDATE	99
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	99
ENHANCEMENT	100
BUG FIX	100
KNOWN ISSUES.....	100
NEW P-VALUE	101
DIRECT LOGIN HTTP API:	101
NEW HTTP API:	102
NEW FEATURES OVERVIEW	103
<i>SECONDARY SIP SERVER SUPPORT</i>	<i>103</i>
<i>UNIFIED "PIN#" for ALL WHEN ENABLE "DISABLE KEYPAD SIP NUMBER DIALING"</i>	<i>104</i>

FIRMWARE VERSION 1.0.7.26 107

PRODUCT NAME.....	107
DATE	107
SUMMARY OF UPDATE	107
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	107
ENHANCEMENT	108
BUG FIX	108
KNOWN ISSUES.....	108
UPDATED P-VALUE.....	109
NEW FEATURES OVERVIEW	110
<i>BASIC AUTHENTICATION OF HTTP API REMOTE OPEN DOOR</i>	<i>110</i>

FIRMWARE VERSION 1.0.7.24 112

PRODUCT NAME.....	112
DATE	112
SUMMARY OF UPDATE	112
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	112
ENHANCEMENT	113
BUG FIX	113
KNOWN ISSUES.....	113
NEW P-VALUE	114
NEW HTTP API:	114
NEW FEATURES OVERVIEW	115
<i>ADD MAC IN USER-AGENT.....</i>	<i>115</i>
<i>IMPROVED PIN MANAGEMENT AT CARD MANAGEMENT</i>	<i>116</i>
<i>MORE TEMPLATE VARIABLES IN EVENT NOTIFICATION</i>	<i>118</i>

FIRMWARE VERSION 1.0.7.23 120

PRODUCT NAME.....	120
-------------------	-----

DATE	120
SUMMARY OF UPDATE	120
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	120
ENHANCEMENT	121
BUG FIX	121
KNOWN ISSUES.....	121
NEW P-VALUE	122
UPDATED P-VALUE.....	122
NEW HTTP API:	122
NEW FEATURES OVERVIEW	123
<i>KEY SENSITIVITY OPTION</i>	123
<i>ONE-WAY INTERLOCKING MODE</i>	125
<i>PAIR WITH GSC3570 OPEN DOOR W/O SIP CALL</i>	129
<i>SCHEDULED AUTO REBOOT</i>	132
<i>INCREASED WHITELIST</i>	133
<i>MODIFIED TIPS AT CARD MANAGEMENT PAGE</i>	134
<i>WEBUI PASSWORD DISPLAY WITH SECURITY AND CONVENIENCE</i>	135
FIRMWARE VERSION 1.0.7.19	137
PRODUCT NAME.....	137
DATE	137
SUMMARY OF UPDATE	137
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	137
ENHANCEMENT	138
BUG FIX	138
KNOWN ISSUES.....	138
NEW P-VALUE	139
UPDATED P-VALUE.....	139
NEW HTTP API:	140
NEW FEATURES OVERVIEW	141
<i>ALARM ACTION WHEN ILLEGAL CARD SWIPED</i>	141
<i>NEWFOUNDLAND/CANADA TIME ZONE</i>	142
<i>GSC3570 SECURE OPEN DOOR VIA GDS37XX/GSC3570 PEERING</i>	143
<i>ENHANCED OPEN DOOR VIA 3RD PARTY WEBRELAY</i>	146
FIRMWARE VERSION 1.0.7.14	148
PRODUCT NAME.....	148
DATE	148
SUMMARY OF UPDATE	148
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	148
ENHANCEMENT	149

BUG FIX	149
KNOWN ISSUES.....	149
NEW P-VALUE	150
NEW HTTP API:	151
NEW FEATURES OVERVIEW	152
<i>OPEN VPN SUPPORT</i>	152
<i>CALL TERMINATION BUTTON IN WEBUI</i>	153
<i>REBOOT/RESYNC VIA SIP NOTIFY</i>	155
<i>OPEN DOOR VIA WEBRELAY</i>	156
<i>ENABLE PIN/PASSWORD DISPLAY</i>	157
<i>SUPPORT "USERNAME" IN HTTP EVENT NOTIFICATION</i>	158
<i>LOG & DISPLAY "UNAUTHORIZED DOOR OPENING ATTEMPT" IN EVENT LOG</i>	159

FIRMWARE VERSION 1.0.7.11..... 161

PRODUCT NAME.....	161
DATE	161
SUMMARY OF UPDATE	161
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	161
ENHANCEMENT	162
BUG FIX	162
KNOWN ISSUES.....	162
NEW P-VALUE	163
NEW HTTP API:	163
NEW FEATURES OVERVIEW	164
<i>REVISED SIP ACCOUNT NAME TO DISPLAY NAME</i>	164
<i>SUPORT FOR CISCO QUOVADIS/HYDRANTID CA</i>	165

FIRMWARE VERSION 1.0.7.10 167

PRODUCT NAME.....	167
DATE	167
SUMMARY OF UPDATE	167
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	167
ENHANCEMENT	168
BUG FIX	168
KNOWN ISSUES.....	168
NEW P-VALUE	169
MODIFIED P-VALUE	169
NEW FEATURES OVERVIEW	170
<i>INCREASE UNLOCK HOLDING TIME</i>	170
<i>ANONYMOUS MJPEG STREAM VIEWING FOR EACH STREAM</i>	171
<i>DEDICATED PASSWORD FOR RTSP STREAM</i>	174

FIRMWARE VERSION 1.0.7.8 177

PRODUCT NAME.....	177
DATE	177
SUMMARY OF UPDATE	177
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	177
ENHANCEMENT	178
BUG FIX	178
KNOWN ISSUES.....	178

FIRMWARE VERSION 1.0.7.7 179

PRODUCT NAME.....	179
DATE	179
SUMMARY OF UPDATE	179
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	179
ENHANCEMENT	180
BUG FIX	180
KNOWN ISSUES.....	180
NEW P-VALUE	181
MODIFIED P-VALUE	181
NEW HTTP API	181
NEW FEATURES OVERVIEW	182
<i>SUPPORT FAILOVER MECHANISM ON DNS SRV</i>	<i>182</i>
<i>SIREN ALARMING WHEN DOOR OPENED ABNORMALLY (SPECIAL WIRING REQUIRED)</i>	
.....	184
<i>ONLY ACCEPT INCOMING SIP CALL FROM PROXY/SERVER</i>	<i>188</i>
<i>SUPPORT HOLIDAYS IN KEEP DOOR OPEN SCHEDULE</i>	<i>189</i>
<i>RESET FACTORY PASSWORD VIA SPECIAL KEY COMBINATION OPERATION.....</i>	<i>190</i>

FIRMWARE VERSION 1.0.7.4 192

PRODUCT NAME.....	192
DATE	192
SUMMARY OF UPDATE	192
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	192
ENHANCEMENT	193
BUG FIX	194
KNOWN ISSUES.....	194
NEW P-VALUE	195
MODIFIED P-VALUE	196
NEW HTTP API	196
NEW FEATURES OVERVIEW.....	199

<i>SUPPORT DNS SRV</i>	<i>199</i>
<i>SUPPORT SPECIAL FEATURE - TELEFONICA.....</i>	<i>200</i>
<i>SEPARATE CREDENTIALS FOR GDSMANAGER.....</i>	<i>201</i>
<i>G.729 AND MULTIPLE AUDIO CODECS SIMULTANEOUSLY WITH PRIORITY.....</i>	<i>203</i>
<i>SCHEDULE FOR FIRMWARE UPGRADE AND PROVISIONING, DHCP OPTION 120.....</i>	<i>204</i>
<i>REREGISTER BEFORE EXPIRATION AND VOICE FRAME PER TX.....</i>	<i>205</i>
<i>KEYPAD BLUE LIGHT ON/OFF ON SCHEDULE.....</i>	<i>206</i>
<i>ADJUST SYTEM DEFAULT VOLUME TO LEVER 2</i>	<i>207</i>
<i>SUPPORT ANONYMOUSE RTSP LIVE VIEW.....</i>	<i>208</i>

FIRMWARE VERSION 1.0.5.6210

PRODUCT NAME.....	210
DATE	210
SUMMARY OF UPDATE	210
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	210
ENHANCEMENT	211
BUG FIX	212
KNOWN ISSUES.....	213
NEW P-VALUE	214
MODIFIED P-VALUE.....	216
NEW HTTP API	216
NEW FEATURES OVERVIEW	217
<i>SUPPORT 4 SIP ACCOUNTS.....</i>	<i>217</i>
<i>CONFIGURE H.264, DTMF PAYLOAD AND PROXY ROUTE VALUE</i>	<i>219</i>
<i>ADD OR DELETE CUSTOMIZED DOORBELL TONE</i>	<i>220</i>
<i>SYSTEM HEALTH ALERTS VIA EMAIL.....</i>	<i>221</i>
<i>SET SCHEDULE FOR LOCAL PIN TO OPEN DOOR.....</i>	<i>222</i>
<i>SUPPORT PACKKETIZATION MODE 0.....</i>	<i>223</i>
<i>SUPPORT CSV FORMAT WHEN IMPORT/EXPORT CARD DATA FILE</i>	<i>224</i>
<i>SUPPORT ANONYMOUSE SNAPSHOT.....</i>	<i>225</i>
<i>NORMAL OPEN/CLOSE IN ALARM_OUT1 (COM1) OPEN DOOR CONTROL.....</i>	<i>226</i>
<i>ADDED BOOT VERSION IN "STATUS" PAGE</i>	<i>227</i>

FIRMWARE VERSION 1.0.5.2228

PRODUCT NAME.....	228
DATE	228
SUMMARY OF UPDATE	228
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	228
ENHANCEMENT	229
BUG FIX	230
KNOWN ISSUES.....	231

NEW P-VALUE	232
NEW HTTP API	233
NEW FEATURES OVERVIEW	235
<i>CONTROL DOOR2 VIA ALARM_OUT (COM1) INTERFACE.....</i>	<i>235</i>
<i>ENABLE / DISABLE WEB UI ACCESS.....</i>	<i>240</i>
<i>DEFINE NUMBER OF SNAPSHOT UPLOADED WHEN OPEN DOOR.....</i>	<i>241</i>
<i>DEFINE DIGIT INPUT INTERFACE TO BE NORMAL OPEN OR CLOSE.....</i>	<i>242</i>
<i>SET SCHEDULE FOR ALARM IN OPEN DOOR</i>	<i>243</i>
<i>OPEN DOOR VIA DIGIT ONLY PRIVATE PIN.....</i>	<i>244</i>
<i>SET "NO KEY ENTRY TIMEOUT"</i>	<i>245</i>
<i>EMAIL SNAPSHOTS WHEN DOOR OPENED.....</i>	<i>246</i>
<i>ALLOW ANONYMOUS VIEWING.....</i>	<i>247</i>
<i>DISPLAY MOTION DETECTION REGION CONFIGURATON WITHOUT PLUGIN.....</i>	<i>248</i>
<i>EMERGENCY PIN TO OVERWRITE "KEEP DOOR OPEN" (LOCKDOWN).....</i>	<i>249</i>
<i>CHECK/UPGRADE FIRMWARE AND DISPLAY DEVICE TEMPERATURE.....</i>	<i>250</i>
<i>SUPPORT SIP NOTIFY AND SET H.264 PAYLOAD TYPE</i>	<i>252</i>
<i>DISPLAY USER OPEN DOOR VIA PIN OVER EVENT LOG</i>	<i>253</i>
<i>CONFIG FIRMWARE OR CONFIGURATION SERVER PATH AND PING TEST VIA SSH.....</i>	<i>254</i>

FIRMWARE VERSION 1.0.4.9256

PRODUCT NAME.....	256
DATE	256
SUMMARY OF UPDATE	256
WARNING:	256
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	257
ENHANCEMENT	257
BUG FIX	257
KNOWN ISSUES.....	257
NEW P-VALUE	257
NEW HTTP API	257

FIRMWARE VERSION 1.0.4.5 (REMOVED)258

PRODUCT NAME.....	258
DATE	258
SUMMARY OF UPDATE	258
WARNING:	258
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	259
ENHANCEMENT	259
BUG FIX	259
KNOWN ISSUES.....	259
NEW P-VALUE	260

NEW HTTP API	260
NEW FEATURES OVERVIEW	261
<i>PARELLEL HUNTING/SIMUTANEOUS RINGING WHEN DOORBELL PRESSED</i>	261
<i>EVENT NOTIFICATION</i>	262

FIRMWARE VERSION 1.0.3.35264

PRODUCT NAME.....	264
DATE	264
SUMMARY OF UPDATE	264
IMPORTANT UPGRADING NOTE	264
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	264
ENHANCEMENT	265
BUG FIX	265
KNOWN ISSUES.....	265
NEW FUNCTIONS	266
NEW P-VALUE	266
NEW HTTP API	266
NEW FEATURES OVERVIEW	267
<i>ASSIGN SCHEDULE TO DOOR BELL</i>	267
<i>MAXIMUM NUMBER OF DIGIT DIALED</i>	268

FIRMWARE VERSION 1.0.3.34269

PRODUCT NAME.....	269
DATE	269
SUMMARY OF UPDATE	269
IMPORTANT UPGRADING NOTE	269
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	269
ENHANCEMENT	270
BUG FIX	270
KNOWN ISSUES.....	270
NEW FUNCTIONS	271
NEW P-VALUE	272
NEW HTTP API	272
NEW FEATURES OVERVIEW	273
<i>CHROME/FIREFOX NO PLUGIN REQUIRED FOR VIDEO LIVEVIEW</i>	273
<i>BASIC AUTHENTICATION of MJPEG VIDEO OR SNAPSHOT VIA HTTP API</i>	274
<i>OPEN DOOR BY CONFIGURED SCHEDULE OR TIME WINDOW</i>	276
<i>ALARM NOTIFICATION OF ACCESS BY USERS OUT OF SCHEDULE</i>	277
<i>SEND SNAPSHOT VIA EMAIL WHEN DOORBELL PRESSED</i>	278
<i>RTCP/RTCP-XR SIP CALL FOR ITSP/CLOUD SOLUTION</i>	279
<i>IMPROVED EVENT LOG UI LAYOUT</i>	280

FIRMWARE VERSION 1.0.3.32281

PRODUCT NAME.....	281
DATE	281
SUMMARY OF UPDATE	281
IMPORTANT UPGRADING NOTE	281
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	281
ENHANCEMENT	282
BUG FIX	283
KNOWN ISSUES.....	283
NEW FUNCTIONS	284
NEW P-VALUE	284
NEW HTTP API	285
NEW FEATURES OVERVIEW	286
<i>HTTP OPEN DOOR</i>	286
<i>SELF-DEFIND EVENT NOTIFICATION MESSAGE</i>	287

FIRMWARE VERSION 1.0.3.31288

PRODUCT NAME.....	288
DATE	288
SUMMARY OF UPDATE	288
IMPORTANT UPGRADING NOTE	288
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	288
ENHANCEMENT	288
BUG FIX	289
KNOWN ISSUES.....	289
NEW FUNCTIONS	290
NEW P-VALUE	290
NEW HTTP API	291
NEW FEATURES OVERVIEW	291
<i>DOOR SYSTEM SETTINGS</i>	291
<i>MULTI-CHANNEL CALL MODE</i>	292

FIRMWARE VERSION 1.0.3.23293

PRODUCT NAME.....	293
DATE	293
SUMMARY OF UPDATE	293
IMPORTANT UPGRADING NOTE	293
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	293
ENHANCEMENT	293
BUG FIX	293

KNOWN ISSUES.....	294
NEW P-VALUE	294
NEW HTTP API	295
NEW FEATURES OVERVIEW	296
<i>CENTRAL MODE</i>	296
<i>BROADSOFT MODE</i>	296
<i>CLICK TO DIAL</i>	297
FIRMWARE VERSION 1.0.3.13	299
PRODUCT NAME.....	299
DATE	299
SUMMARY OF UPDATE	299
IMPORTANT UPGRADING NOTE	299
FIRMWARE APPLIES TO BELOW HW VERSION ONLY	299
NEW P-VALUE	299
ENHANCEMENT	300
BUG FIX	300
KNOWN ISSUES.....	301
NEW FEATURES OVERVIEW	302
<i>CENTRAL MODE</i>	302
<i>DISABLE ALARM SOUND AT PHONE SIDE FOR TRIGERED SIP CALL</i>	302
<i>CAPTURE IMAGE WHEN DOOR BELL PRESSED</i>	303
<i>DISABLE KEYPAD</i>	303
<i>ENABLE REMOTE UNLOCK TO ON HOOK</i>	304
<i>DISABLE AUTO ANSWER</i>	304
<i>ENABLE DOORBELL BUTTON TO HANG UP CALL</i>	305
<i>CARD ISSUING STATE EXPIRED TIME</i>	305
<i>LIGHT SETTINGS</i>	306
<i>ENABLE DOORBELL BLUE LIGHT PER SETTINGS</i>	307
<i>ENABLE LOG REPORT</i>	307
FIRMWARE VERSION 1.0.2.25	309
PRODUCT NAME.....	309
DATE	309
SUMMARY OF UPDATE	309
IMPORTANT UPGRADING NOTE	309
NEW P-VALUE	309
ENHANCEMENT	309
BUG FIX	310
FIRMWARE VERSION 1.0.2.22	311

PRODUCT NAME.....	311
DATE	311
SUMMARY OF UPDATE	311
IMPORTANT UPGRADING NOTE.....	311
BUG FIX	311

FIRMWARE VERSION 1.0.2.21312

PRODUCT NAME.....	312
DATE	312
SUMMARY OF UPDATE	312
IMPORTANT UPGRADING NOTE.....	312
ENHANCEMENT	312
BUG FIX	313

FIRMWARE VERSION 1.0.2.13314

PRODUCT NAME.....	314
DATE	314
SUMMARY OF UPDATE	314
IMPORTANT UPGRADING NOTE.....	314
ENHANCEMENT	314
BUG FIX	315

FIRMWARE VERSION 1.0.2.9316

PRODUCT NAME.....	316
DATE	316
SUMMARY OF UPDATE	316
IMPORTANT UPGRADING NOTE.....	316
ENHANCEMENT	316
BUG FIX	316

FIRMWARE VERSION 1.0.2.5317

PRODUCT NAME.....	317
DATE	317
SUMMARY OF UPDATE	317
IMPORTANT UPGRADING NOTE.....	317
ENHANCEMENT	317
BUG FIX	318

FIRMWARE VERSION 1.0.1.19319

PRODUCT NAME.....	319
DATE	319

SUMMARY OF UPDATE	319
ENHANCEMENT	319
BUG FIX	320

FIRMWARE VERSION 1.0.13.15

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A, 2.2A, 3.0A, 3.1A)

GDS3712 (HW Supported: 1.0A, 1.1A, 1.2A)

DATE

07/07/2025

FIRMWARE FILE INFORMATION

- Firmware file name: **gds37xx_fw.bin**
MD5: **5575cd334aaef17aca1edc17d8b42042**

SUMMARY OF UPDATE

This release is for HW3.1A support, based on 1.0.13.10

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior like WebUI missing some parameters or settings, factory reset is required. Please backup the configuration file and database file of RFID cards before factory reset, and import them back or configure them again after factory reset.

NOTES:

- Once upgraded, device can NOT downgrade to FW1.0.11.23 or below, due to the new firmware is using 2nd generation certificate
- This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.XA, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW3.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW3.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.2A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	
GDS3712 HW1.1A	YES	
GDS3712 HW1.0A	YES	

For detailed information about GDS371X, please refer to User Manual and Resource Center:

- **GDS371X User Manual:**
<https://documentation.grandstream.com/article-categories/facility-access-systems/>
- **HOW-TO Guide**
<https://documentation.grandstream.com/article-categories/interconnection-facility/>
- **HTTP API** documentation can be downloaded from here:
<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

FIRMWARE VERSION 1.0.13.10

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A, 2.2A, 3.0A)

GDS3712 (HW Supported: 1.0A, 1.1A, 1.2A)

DATE

08/28/2024

FIRMWARE FILE INFORMATION

- Firmware file name: **gds37xx_fw.bin**
MD5: **381c0aa636739cc576ee8020bd348053**

SUMMARY OF UPDATE

This release is for bug fixes (IOT) and new feature enhancements.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior like WebUI missing some parameters or settings, factory reset is required. Please backup the configuration file and database file of RFID cards before factory reset, and import them back or configure them again after factory reset.

NOTES:

- Once upgraded, device can NOT downgrade to FW1.0.11.23 or below, due to the new firmware is using 2nd generation certificate
- This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.XA, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW3.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.2A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	
GDS3712 HW1.1A	YES	
GDS3712 HW1.0A	YES	

ENHANCEMENT

- Added an Alarm-Out Event when receiving/performing a call [ITSP]
- Added option to disable the weak TLS ciphers.
- Added alarm out status icon in the webUI.

BUG FIX

- Fixed video call fails with Yealink T58W [IOT]
- Fixed basic call feature one case failure [IOT]

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing keypad the response will be abnormal till the call time out (about 2 minute).

NEW P-VALUE

P8536	System_Settings.Access_Settings.Enable_Disable_Weak_Ciphers (Value: 0, 1, 2, 3, 4, 5)
P15610	Alarm_Settings.Alarm_Events_Config.Enable_SIP_Calling_Trigger_Alarm_Output (Value: 0, 1)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=access
- SET:[http|https]://<servername>/goform/config?cmd=set&P8536=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=event
- SET:[http|https]://<servername>/goform/config?cmd=set&P15610=<value>

Released HTTP API documentation can be downloaded from here:

<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

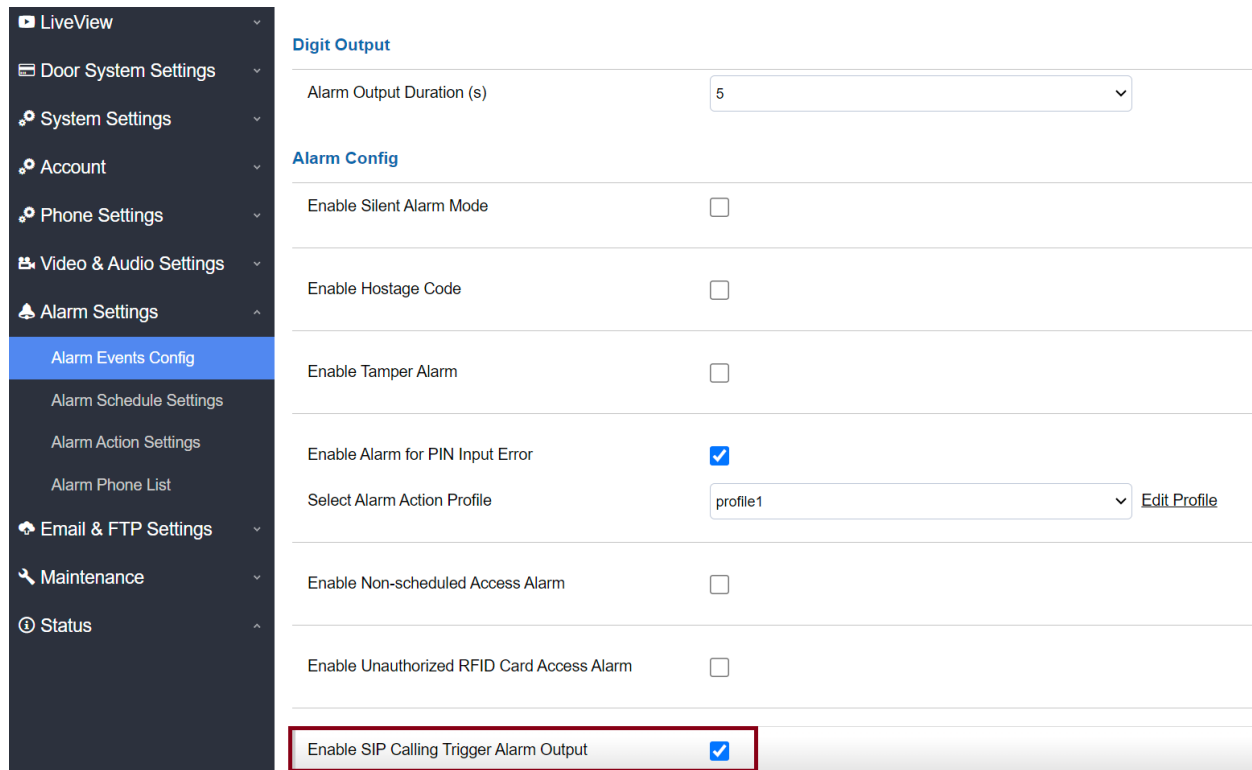
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

SIP Calling Trigger Alarm Output

- Web Configuration**

This feature can be found under device web UI: Alarm Settings → Alarm Events Config:



Digit Output	
Alarm Output Duration (s)	5

Alarm Config	
Enable Silent Alarm Mode	<input type="checkbox"/>
Enable Hostage Code	<input type="checkbox"/>
Enable Tamper Alarm	<input type="checkbox"/>
Enable Alarm for PIN Input Error	<input checked="" type="checkbox"/>
Select Alarm Action Profile	profile1 Edit Profile
Enable Non-scheduled Access Alarm	<input type="checkbox"/>
Enable Unauthorized RFID Card Access Alarm	<input type="checkbox"/>
Enable SIP Calling Trigger Alarm Output	<input checked="" type="checkbox"/>

- Functionality**

This feature is implemented by ITSP customer's request.

With this feature enabled, the calls in/out of the GDS37xx will trigger Alarm Output, where 3rd party devices are connected.

This feature is especially useful where the usage scene requires loud sound or visual effect when GDS37xx is called or when visitors press doorbell or call designated phone number asking for open door.

For example, senior houses, or rehab center, or disabled person (e.g.: deaf person) residence place, or places like drive-in banks or restaurants, etc., where requires those loud audio (siren) or visual effect (strike light) reminding there is a call asking for open door.

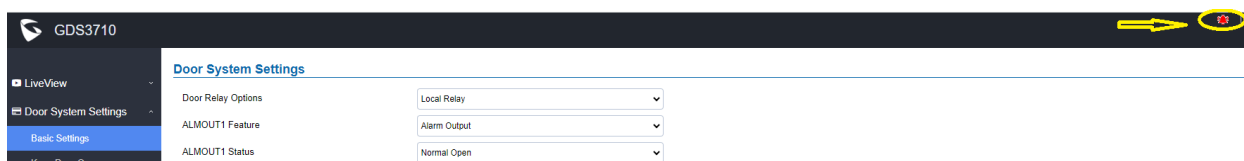
Alarm Out Status Icon in WebUI

- Web Configuration**

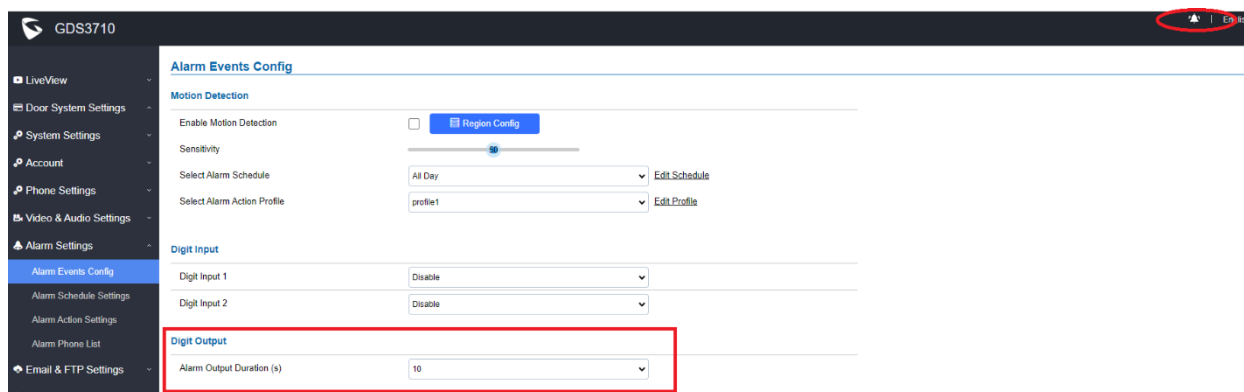
This feature is combined side function with above “SIP Calling Trigger Alarm Output” feature enabled.

When the “SIP Calling Trigger Alarm Output” feature enabled, if there is incoming or outgoing call or from the GDS37xx, the top right corner “Bell Icon” will become red and be flashing. The triggered alarm can be stopped in below two ways:

1. Click that flashing icon will stop the alarm:



2. Automatically stop based on configured “Alarm Output Duration” timer (below sample is 10 seconds):



- Functionality**

With the alarm status icon on the webUI, the user can either manually stops the alarm by log into the GDS37xx (if the configured timer is long for example); or let it stop automatically based on the timer in configuration.

These functions allow users to control the 3rd party alarm devices basoed on their usage scene.

For detailed information about GDS371X, please refer to User Manual and Resource Center:

- **GDS371X User Manual:**
<https://documentation.grandstream.com/article-categories/facility-access-systems/>
- **HOW-TO Guide**
<https://documentation.grandstream.com/article-categories/interconnection-facility/>
- **HTTP API** documentation can be downloaded from here:
<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

FIRMWARE VERSION 1.0.13.9

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A, 2.2A, 3.0A)

GDS3712 (HW Supported: 1.0A, 1.1A, 1.2A)

DATE

06/24/2024

FIRMWARE FILE INFORMATION

- Firmware file name: **gds37xx_fw.bin**
MD5: **69e87ad992c7d75c3fc870ac9b2b83f3**

SUMMARY OF UPDATE

This release is for bug fixes and new feature enhancements.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior like WebUI missing some parameters or settings, factory reset is required. Please backup the configuration file and database file of RFID cards before factory reset, and import them back or configure them again after factory reset.

NOTES:

- Once upgraded, device can NOT downgrade to FW1.0.11.23 or below, due to the new firmware is using 2nd generation certificate
- This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.XA, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW3.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.2A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	
GDS3712 HW1.1A	YES	
GDS3712 HW1.0A	YES	

ENHANCEMENT

- Added schedule for “Enable Background Light”
- Added 802.1X support.
- Updated gs_cpe to V1.0.5.7 (not displayed in webUI)

BUG FIX

- Fixed issue the first key pressed no key sound heard when pressing the keys.
- Fixed DUT not sending config file request to updated config server after GDMS redirection.
- Fixed DUT does not respect schedule
- Fixed no startup event log after the DUT restarted.
- Fixed after answering automatic callback there is no audio.
- Fixed P value update not requiring reboot would not be found in configuration upate.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing keypad the response will be abnormal till the call time out (about 2 minute).

NEW P-VALUE

P15594	DoorSysteemSettings.BasicSettings.EnableWhiteBacklightonTimeInterval (Value: 0:Disable, Default: 1:Enable)
P15595	DoorSysteemSettings.BasicSettings.WhiteBacklightonTimeIntervalStart (Value: Digital String)
P15596	DoorSysteemSettings.BasicSettings.WhiteBacklightonTimeIntervalEnd (Value: Digital String)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15594=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15595=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15596=<value>

Released HTTP API documentation can be downloaded from here:

<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

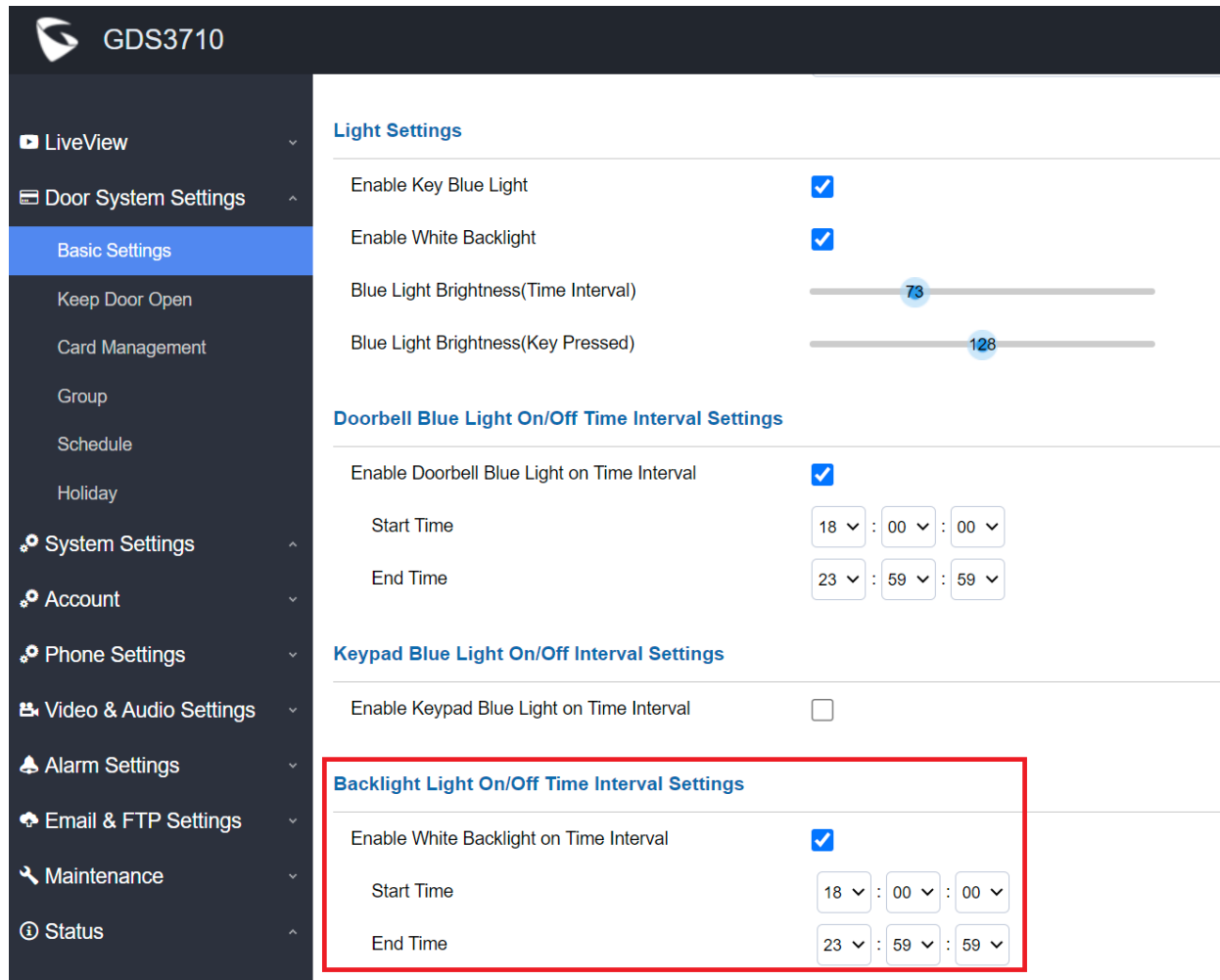
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

SCHEDULE FOR ENABLE BACKGROUND LIGHT

- **Web Configuration**

This feature can be found under device web UI: Door System Settings → Basic Settings:



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
- System Settings
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status

Light Settings

- Enable Key Blue Light ☒
- Enable White Backlight ☒
- Blue Light Brightness(Time Interval)
- Blue Light Brightness(Key Pressed)

Doorbell Blue Light On/Off Time Interval Settings

- Enable Doorbell Blue Light on Time Interval ☒
- Start Time : :
- End Time : :

Keypad Blue Light On/Off Interval Settings

- Enable Keypad Blue Light on Time Interval ☐

Backlight Light On/Off Time Interval Settings

- Enable White Backlight on Time Interval ☒
- Start Time : :
- End Time : :

- **Functionality**

This feature is implemented by customer's request.

With configurable schedule, user can turn ON/OFF the white background LED to light up the keypad as well as illuminate nearby area around the GDS3710.

NOTE: This feature is applied to GDS3710 Only, because GDS3712 does not have keypad therefore without the background LED light.

For detailed information about GDS371X, please refer to User Manual and Resource Center:

- **GDS371X User Manual:**
<https://documentation.grandstream.com/article-categories/facility-access-systems/>
- **HOW-TO Guide**
<https://documentation.grandstream.com/article-categories/interconnection-facility/>
- **HTTP API** documentation can be downloaded from here:
<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

FIRMWARE VERSION 1.0.13.5

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A, 2.2A, 3.0A)

GDS3712 (HW Supported: 1.0A, 1.1A, 1.2A)

DATE

04/24/2024

SUMMARY OF UPDATE

This release is for bug fixes and new feature enhancements, and GDS3710 HW3.0A support.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior like WebUI missing some parameters or settings, factory reset is required. Please backup the configuration file and database file of RFID cards before factory reset, and import them back after factory reset.

NOTES:

- **Once upgraded, device can NOT downgrade to FW1.0.11.23 or below, due to the new firmware is using 2nd generation certificate**
- **This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.XA, except for HW1.7A or below.**

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW3.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.2A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	
GDS3712 HW1.1A	YES	
GDS3712 HW1.0A	YES	

ENHANCEMENT

- Initial firmware for GDS3710 HW3.0A
- Optimized webUI language translation
- Changed “Zero Config” option wording to “3CX Auto Provision”
- Added feature to allow device sending syslog debug messages after reset [IOT]
- Added SRTP requirement [IOT]
- Enhanced syslog to be more user friendly [IOT]
- Added SSL Key Log File [IOT]
- Added support for DHCP Option 2 [IOT]
- Added feature for packet capture [IOT]
- Enhanced Alarm Output duration to last longer or unlimited
- Enhanced keypad blue LED light brightness can be adjusted
- Added feature to “Send SIP Log”
- Added feature to send “event type”, “username” and “card ID” in the email with opendoor event
- Added support for 802.1X

BUG FIX

- Fixed video call not working when SRTP set to “Enabled and forced” [IOT]
- Fixed device got blocked randomly
- Fixed video feed got dark sometimes
- Fixed device not sending email notification after doorbell pressed
- Fixed call disconnected with WebEx hunting group
- Fixed local feature code cannot be disabled [IOT]
- Fixed TLS SRTP call 500 response from server [IOT]
- Fixed audio got cutoff in the beginning of call [IOT]
- Fixed registration failure and retry timer not being followed [IOT]
- Fixed device not followup on HTTP config file download after receiving 401 response [IOT]
- Fixed device randomly stops sending email or feeding video stream
- Fixed SIP process cannot be started sometimes
- Fixed device swiping card failed to open door when in call with GSC3570
- Fixed device SMTP configuration fail to work with Office365 Exchange account

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing keypad the response will be abnormal till the call time out (about 2 minute).

NEW P-VALUE

P15591	DoorSystemSettings.BasicSettings.BlueLightBrightness(Time Interval) (Value: 1 – 255)
P15592	DoorSystemSettings.BasicSettings.BlueLightBrightness(Key Pressed) (Value: 1 - 255)
P143	SystemSettings.DateTime.AllowDHCPOption2toOverrideTimeZoneSetting (Value: 0:Disable; 1:Enable)
P7901	SystemSettings.NetworkSettings.802.1XMode (Value: 0:Disabled; 1:EAP_MD5; 2:EAP-TLS; 3:EAP-PEAPv0/MSCHAPv2)
P7902	SystemSettings.NetworkSettings.802.1XIdentity (Value: String, Max.length=512)
P7903	SystemSettings.NetworkSettings.MD5Password (Value: String, Max.length=8912)
P8439	SystemSettings.NetworkSettings.802.1XCACertificate (Value: String, Max.length=8912)
P8440	SystemSettings.NetworkSettings.802.1XClientCertificate (Value: String, Max.length=8912)
P2383	Account.Account.1.SRTPKeyLength (Value: 0:AES 128&256 bit; 1:AES 128 bit; 2:AES 256 bit)
P191	Account.Account.1.EnableLocalCallFeatures (Value: 0:Disable; 1:Enable)
P2483	Account.Account.2.SRTPKeyLength (Value: 0:AES 128&256 bit; 1:AES 128 bit; 2:AES 256 bit)
P420	Account.Account.2.EnableLocalCallFeatures (Value: 0:Disable; 1:Enable)
P2583	Account.Account.3.SRTPKeyLength (Value: 0:AES 128&256 bit; 1:AES 128 bit; 2:AES 256 bit)
P520	Account.Account.3.EnableLocalCallFeatures (Value: 0:Disable; 1:Enable)
P2683	Account.Account.4.SRTPKeyLength (Value: 0:AES 128&256 bit; 1:AES 128 bit; 2:AES 256 bit)
P620	Account.Account.4.EnableLocalCallFeatures (Value: 0:Disable; 1:Enable)
P1387	Maintenance.PacketCapture.SendSIPLog (Value: 0:Disable; 1:Enable)
P6008	Maintenance.PacketCapture.WithRTTPackets (Value: 0:No; 1:Yes)
P22419	Maintenance.PacketCapture.WithSecretKeyInformation (Value: 0:No; 1:Yes)
P82307	Send Syslog Debug Messages After Reset (Value: 0:Disable; 1:Enable)

UPDATED P-VALUE

P198	Account.Account.1.SpecialFeature (Value added: 122: Metaswitch)
P424	Account.Account.2.SpecialFeature (Value added: 122: Metaswitch)
P524	Account.Account.3.SpecialFeature (Value added: 122: Metaswitch)
P624	Account.Account.4.SpecialFeature (Value added: 122: Metaswitch)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15591=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15592=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=date
- SET:[http|https]://<servername>/goform/config?cmd=set&P143=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=net
- SET:[http|https]://<servername>/goform/config?cmd=set&P7901=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P7902=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P7903=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P8439=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P8440=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P2383=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2483=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2583=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2683=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P191=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P420=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P520=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P620=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=debug
- SET:[http|https]://<servername>/goform/config?cmd=set&P1387=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=capture
- SET:[http|https]://<servername>/goform/config?cmd=set&P6008=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P22419=<value>

Released HTTP API documentation can be downloaded from here:

<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

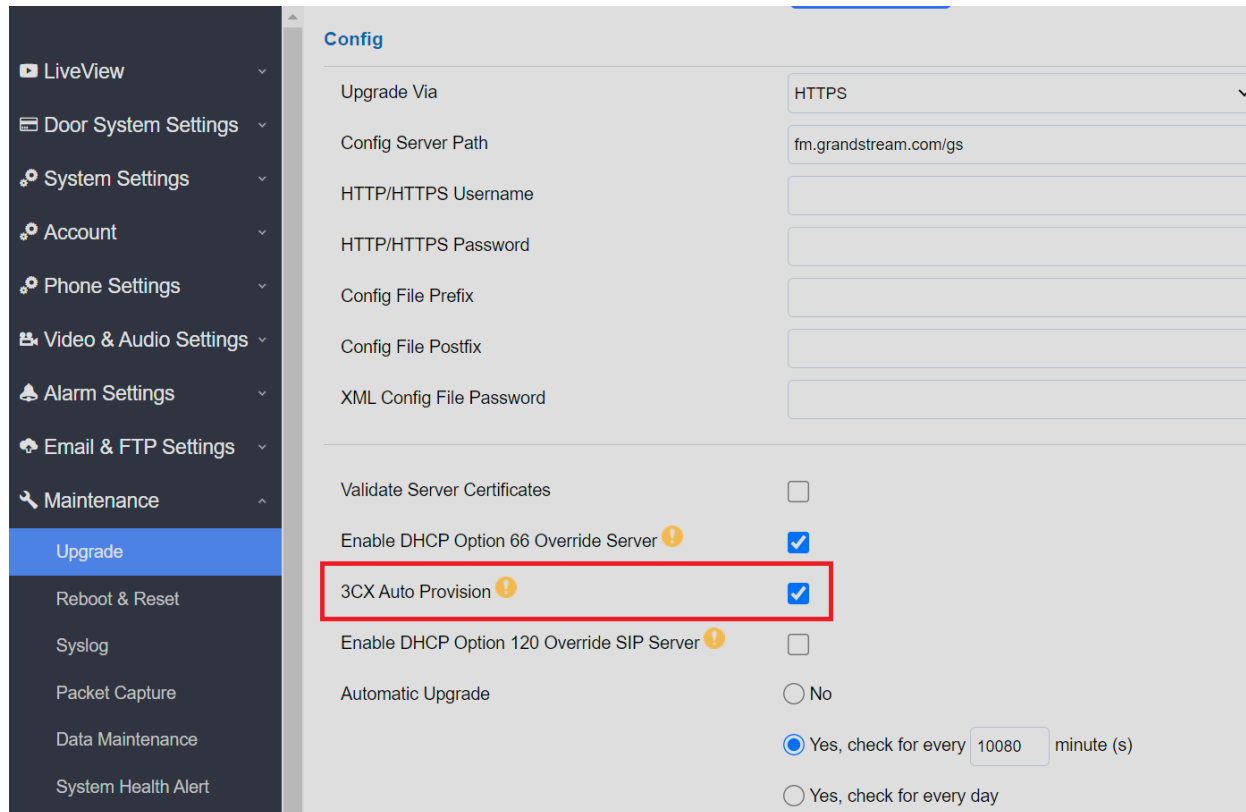
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

CHANGED “ZERO CONFIG” TO “3CX AUTO PROVISION”

- **Web Configuration**

This feature can be found under device web UI: Maintenance → Upgrade:



The screenshot shows the 'Upgrade' configuration page in the Grandstream device web UI. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Upgrade (highlighted), Reboot & Reset, Syslog, Packet Capture, Data Maintenance, and System Health Alert. The main content area is titled 'Config' and contains the following settings:

Setting	Value
Upgrade Via	HTTPS
Config Server Path	fm.grandstream.com/gs
HTTP/HTTPS Username	
HTTP/HTTPS Password	
Config File Prefix	
Config File Postfix	
XML Config File Password	
Validate Server Certificates	<input type="checkbox"/>
Enable DHCP Option 66 Override Server	<input checked="" type="checkbox"/>
3CX Auto Provision	<input checked="" type="checkbox"/>
Enable DHCP Option 120 Override SIP Server	<input type="checkbox"/>
Automatic Upgrade	<input type="radio"/> No
	<input checked="" type="radio"/> Yes, check for every 10080 minute (s)
	<input type="radio"/> Yes, check for every day

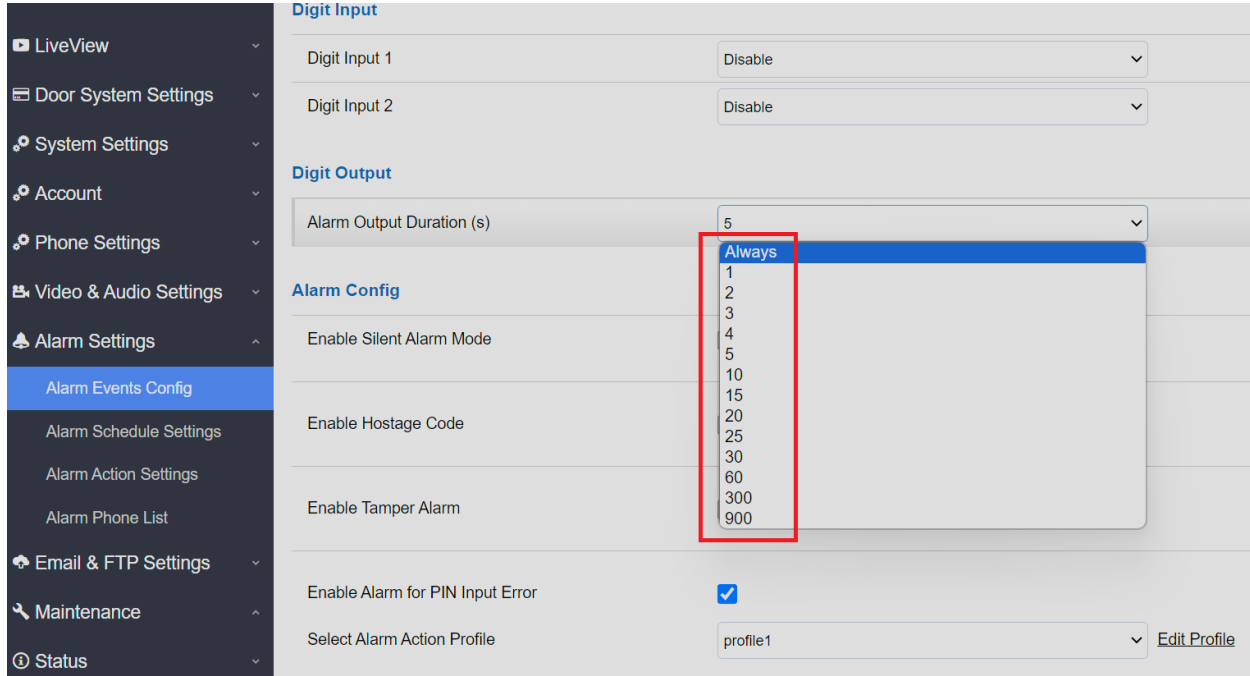
- **Functionality**

This feature previously marked as “Zero Config”, it is working with 3CX Auto Provisioning, therefore changed the wording to “3CX Auto Provision” to be more specific and clear to users.

ENHANCE ALARM OUTPUT DURATION

- **Web Configuration**

This feature can be found under device webUI: Alarm Settings → Alarm Events Config → Digit Output:



The screenshot shows the 'Alarm Events Config' page in the Grandstream webUI. The left sidebar contains navigation links: LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings (expanded), Alarm Events Config (selected), Alarm Schedule Settings, Alarm Action Settings, Alarm Phone List, Email & FTP Settings, Maintenance, and Status. The main content area is divided into three sections: 'Digit Input' with two 'Disable' dropdowns, 'Digit Output' with an 'Alarm Output Duration (s)' dropdown menu, and 'Alarm Config' with several toggle and selection options. The 'Alarm Output Duration (s)' dropdown is open, showing a list of options: 5, Always, 1, 2, 3, 4, 5, 10, 15, 20, 25, 30, 60, 300, and 900. The 'Always' option is highlighted in blue and is enclosed in a red rectangular box. The 'Alarm Config' section includes 'Enable Silent Alarm Mode', 'Enable Hostage Code', 'Enable Tamper Alarm', 'Enable Alarm for PIN Input Error' (checked), and 'Select Alarm Action Profile' (set to 'profile1').

- **Functionality**

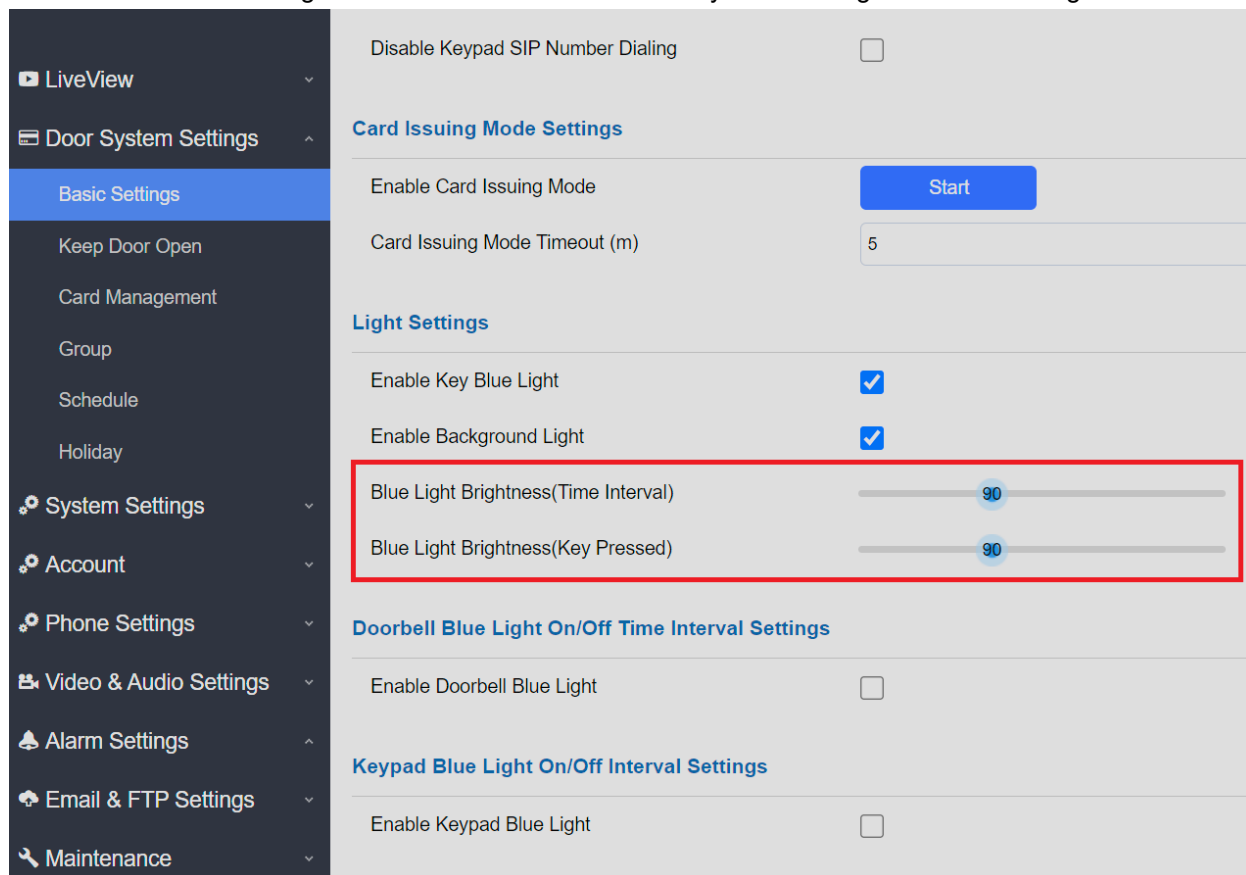
This feature enhancement is implemented based on feedback from field.

The alarm output duration now increased to 900 seconds or 15 minutes. When “Always” is selected in the pull-down menu, the alarm output will be forever until administrator to disable or reset it.

LIGHT BRIGHTNESS ADJUSTABLE AT KEYPAD BLUE LED

- **Web Configuration**

This feature can be configured under device webUI: Door System Settings → Basic Settings:



The screenshot shows the webUI configuration page for Door System Settings. The left sidebar contains a menu with options: LiveView, Door System Settings (expanded), Basic Settings (selected), Keep Door Open, Card Management, Group, Schedule, Holiday, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, and Maintenance. The main content area is titled 'Basic Settings' and includes sections for Card Issuing Mode Settings, Light Settings, Doorbell Blue Light On/Off Time Interval Settings, and Keypad Blue Light On/Off Interval Settings. The 'Light Settings' section is highlighted with a red box and contains two adjustable sliders: 'Blue Light Brightness(Time Interval)' and 'Blue Light Brightness(Key Pressed)', both set to 90.

- **Functionality**

This feature enhancement is implemented based on feedback from the field. Customers want to be able to adjust the brightness of keypad blue LED to meet the application environment.

Now customer can now adjust the keypad blue LED brightness by moving the bar in the webUI.

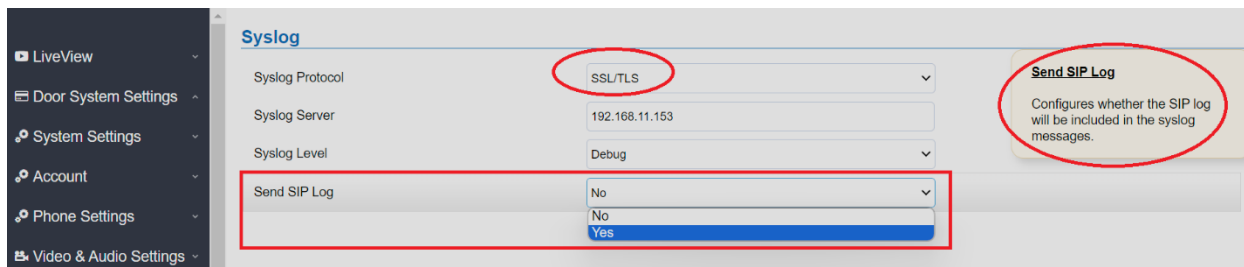
There are two adjustable bars or choices:

- “Blue Light Brightness(Time Interval):
This bar adjusts the brightness when blue LED is configured to light up at configured On/Off intervals.
- “Blue Light Brightness(Key Pressed):
This bar adjusts the brightness of blue LED when keypad is pressed

SEND SIP LOG

- **Web Configuration**

This feature can be found under device webUI: Maintenance → Syslog:



- **Functionality**

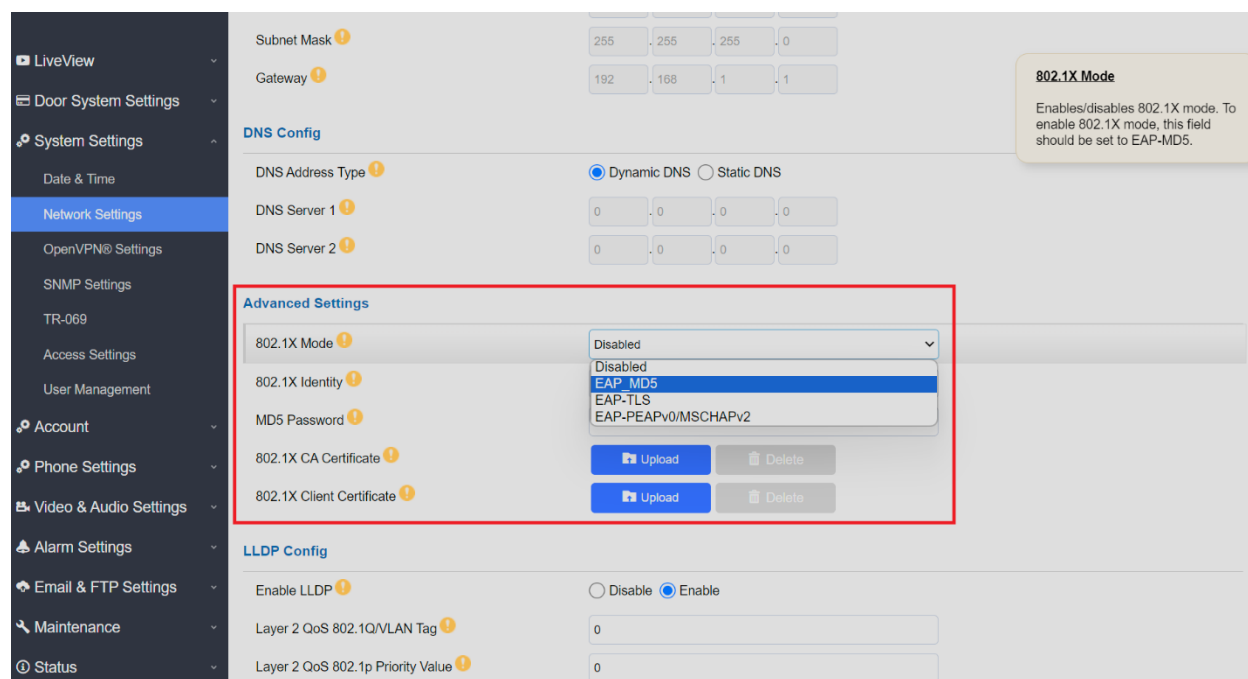
This feature enhancement is implemented based on customer's request.

When enabled by choosing "Yes" in the pull down menu, the SIP log will be included in the syslog message. This is particularly useful when secure link is used (e.g.: SSL/TLS used)

802.1X SUPPORT

- **Web Configuration**

This feature can be configured under device web UI: System Settings → Network Settings → Advanced Settings:



802.1X Mode
Enables/disables 802.1X mode. To enable 802.1X mode, this field should be set to EAP-MD5.

DNS Config

DNS Address Type ☒ Dynamic DNS ☐ Static DNS

DNS Server 1 0 0 0 0

DNS Server 2 0 0 0 0

Advanced Settings

802.1X Mode
 Disabled
 EAP_MD5
 EAP-TLS
 EAP-PEAPv0/MSCHAPv2

802.1X Identity

MD5 Password

802.1X CA Certificate

802.1X Client Certificate

LLDP Config

Enable LLDP ☐ Disable ☒ Enable

Layer 2 QoS 802.1Q/VLAN Tag 0

Layer 2 QoS 802.1p Priority Value 0

- **Functionality**

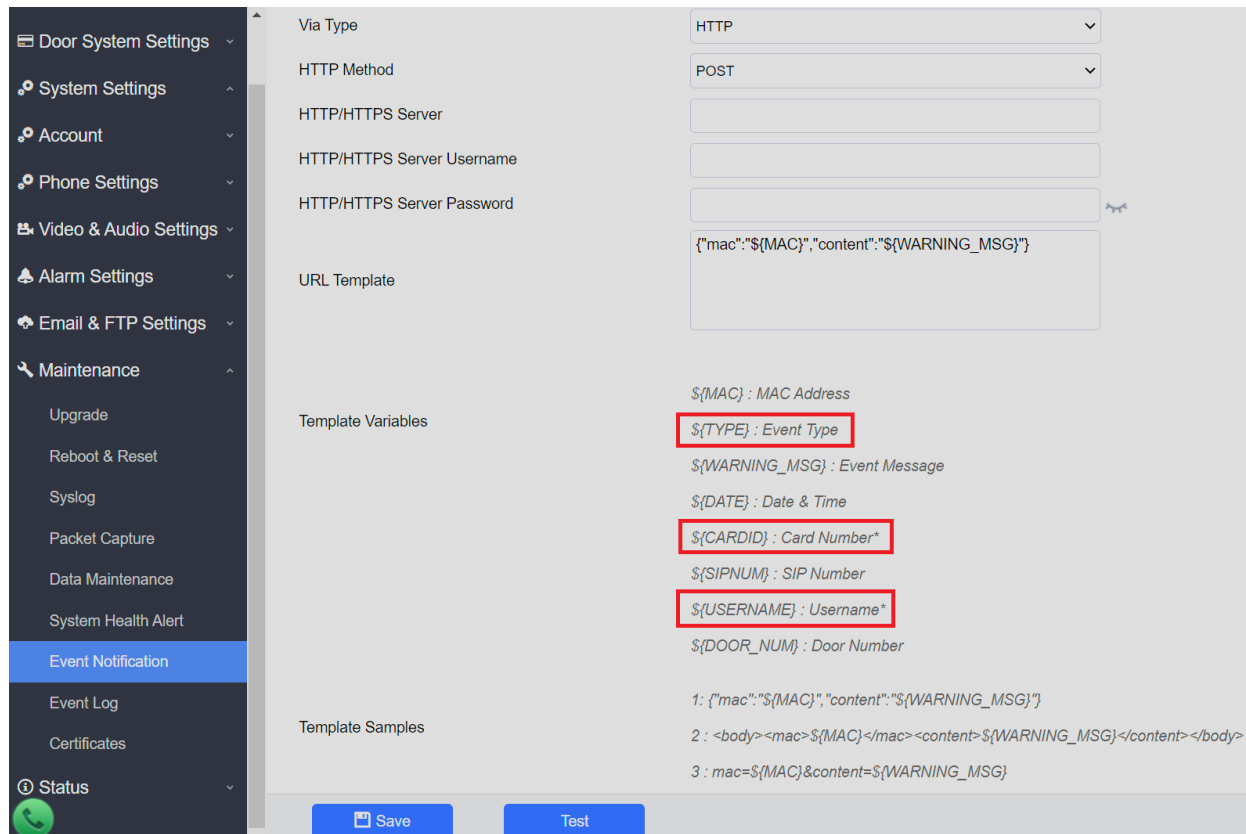
This feature enhancement is implemented based on customer's request.

User can now support the network by filling in the parameters of 802.1X

SEND “ENVET TYPE”, “USERNAME”, “CARD ID” IN EMAIL WITH OPEN DOOR EVENT

- **Web Configuration**

This feature can be found under device webUI: Maintenance → Event Notification:



Via Type: HTTP

HTTP Method: POST

HTTP/HTTPS Server:

HTTP/HTTPS Server Username:

HTTP/HTTPS Server Password:

URL Template: `{"mac":"${MAC}","content":"${WARNING_MSG}"}`

Template Variables:

- `${MAC}` : MAC Address
- `${TYPE}` : Event Type
- `${WARNING_MSG}` : Event Message
- `${DATE}` : Date & Time
- `${CARDID}` : Card Number*
- `${SIPNUM}` : SIP Number
- `${USERNAME}` : Username*
- `${DOOR_NUM}` : Door Number

Template Samples:

- `1: {"mac":"${MAC}","content":"${WARNING_MSG}"}`
- `2: <body><mac>${MAC}</mac><content>${WARNING_MSG}</content></body>`
- `3: mac=${MAC}&content=${WARNING_MSG}`

Buttons: Save, Test

- **Functionality**

This feature enhancement is implemented based on feedback from the field.

Customers can now fill in the Event Notification template with more information like Event Type, Card ID, Username, etc, together with the snapshots when door opened.

More detailed information in the email together with the snapshot, will help the management of the door access events more successfully.

This is especially useful for customers with the implementation site where many doors exist, like but not limited to: Schools, Gym, Hospitals, Office Buildings, etc.

For detailed information about GDS371X, please refer to User Manual and Resource Center:

- **GDS371X User Manual:**
<https://documentation.grandstream.com/article-categories/facility-access-systems/>
- **HOW-TO Guide**
<https://documentation.grandstream.com/article-categories/interconnection-facility/>
- **HTTP API** documentation can be downloaded from here:
<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

FIRMWARE VERSION 1.0.13.2

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A, 2.2A)

GDS3712 (HW Supported: 1.0A, 1.1A, 1.2A)

DATE

11/22/2023

SUMMARY OF UPDATE

This release is major security upgrade, bug fixes and new features enhancements.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior, or Web UI display missing some parameters or settings, factory reset is MANDATORY.

Please backup the configuration file and database file of RFID cards before factory reset, and import them back after factory reset.

NOTES:

- Once upgraded, device can NOT downgrade to FW1.0.11.23 or below, due to the new firmware is using 2nd generation certificate
- This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.XA, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW2.2A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	
GDS3712 HW1.1A	YES	
GDS3712 HW1.0A	YES	

ENHANCEMENT

- Use HTTPS as default CFG file download method to update gen2 cert without manual configuration
- Added support for HTTP API request when web access is set to HTTPS
- Added support to edit the interval of “Onhook Timer After Remote Open Door(s)”
- Added the ability to configure delay for the snapshots taken when “Door Opened” or “Doorbell Pressed”
- Added admin audit logging to the event log functionality [ITSP]
- Added ability to define the TLS protocol level
- Added support for System Temperature object identifier in the MIB file
- Added improvement for Alarm Email Subject and Text in GDS37xx
- Added Emergency PIN to Re-enable Keep Door Open
- Added in WebUI the Certificate Type Information
- Added support for access with RTSP password in ONVIF
- Added support for 2nd generation certificate
- Added support for SNI extension on TLS [ITSP]
- Added support for SNMP trap when doorbell button pressed
- Added “BRIGHTNESS/CONTRAST/SATURATION” setting bar at LiveView page on WebUI

BUG FIX

- Fixed under SNMP settings, some key-related parameters configured and set are inconsistent with actual delivered parameters locally
- Fixed UCM cannot discover GDS37xx through zero config when GDS is in another subnet
- Fixed device doorbell blue light turning OFF after open door event.
- Fixed device not playing the ring group prompt
- Fixed “Send Wiegand Code on Remote Open Door Action” feature is not working
- Fixed device not be redirected to the final provisioning server
- Fixed the anonymous call issue reported by user
- Fixed video re-invite fails to GDS device in WAVE
- Fixed device does NOT trigger alarms for PIN Input Error
- Fixed device does not send Request GET cfggds3710.xml
- Fixed device video failed randomly after several hours
- Fixed when creating a new card with name contains non alphanumeric characters (e.g.: O'Brian) the card is NOT created when clicking “Save”

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing keypad the response will be abnormal till the call time out (about 2 minute).

NEW P-VALUE

P15582	DoorSystemSettings.BasicSettings.OnhookTimerAfterRemoteOpenDoor (Value: 3 – 1800)
P15584	DoorSystemSettings.BasicSettings.SnapshotDelayWhenDoorbellPressed (Value: 0 – 10)
P22293	SystemSettings.AccessSettings.MinimumTLSVersion (Value: 10/11/12 10:TLS 1.0 11:TLS 1.1 12:TLS 1.2)
P22294	SystemSettings.AccessSettings.MaximumTLSVersion (Value: 99/10/11/12 99:Unlimited 10:TLS 1.0 11:TLS 1.1 12:TLS 1.2)
P15585	SystemSettings.KeepDoorOpen.EmergencyPINtoReenableKeepDoor1Open (Value: String, max.length = 8)
P15586	SystemSettings.KeepDoorOpen.EmergencyPINtoReenableKeepDoor2Open (Value: String, max.length = 8)
P2311	Account.Account_1.Check_Domain_Certificates (Value: 0, 1 0: Disable 1: Enable)
P2411	Account.Account_2.Check_Domain_Certificates (Value: 0, 1 0: Disable 1: Enable)
P2511	Account.Account_3.Check_Domain_Certificates (Value: 0, 1 0: Disable 1: Enable)
P2611	Account.Account_4.Check_Domain_Certificates (Value: 0, 1 0: Disable 1: Enable)
P15520	ISP.BRIGHTNESS (Value: 0 – 128)
P15521	ISP.CONTRAST (Value: 0 – 128)
P15522	ISP.SATURATION (Value: 0 – 128)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15582=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15584=<value>

- GET:[http|https]://<servername>/goform/config?cmd=get&type=access
- SET:[http|https]://<servername>/goform/config?cmd=set&P22293=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P22294=<value>

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sch_open_door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15585=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15586=<value>

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P2311=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2411=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2511=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2611=<value>

- GET:[http|https]://<servername>/goform/config?cmd=get&type=play
- SET:[http|https]://<servername>/goform/config?cmd=set&P15520=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15521=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15522=<value>

Released HTTP API documentation can be downloaded from here:

<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

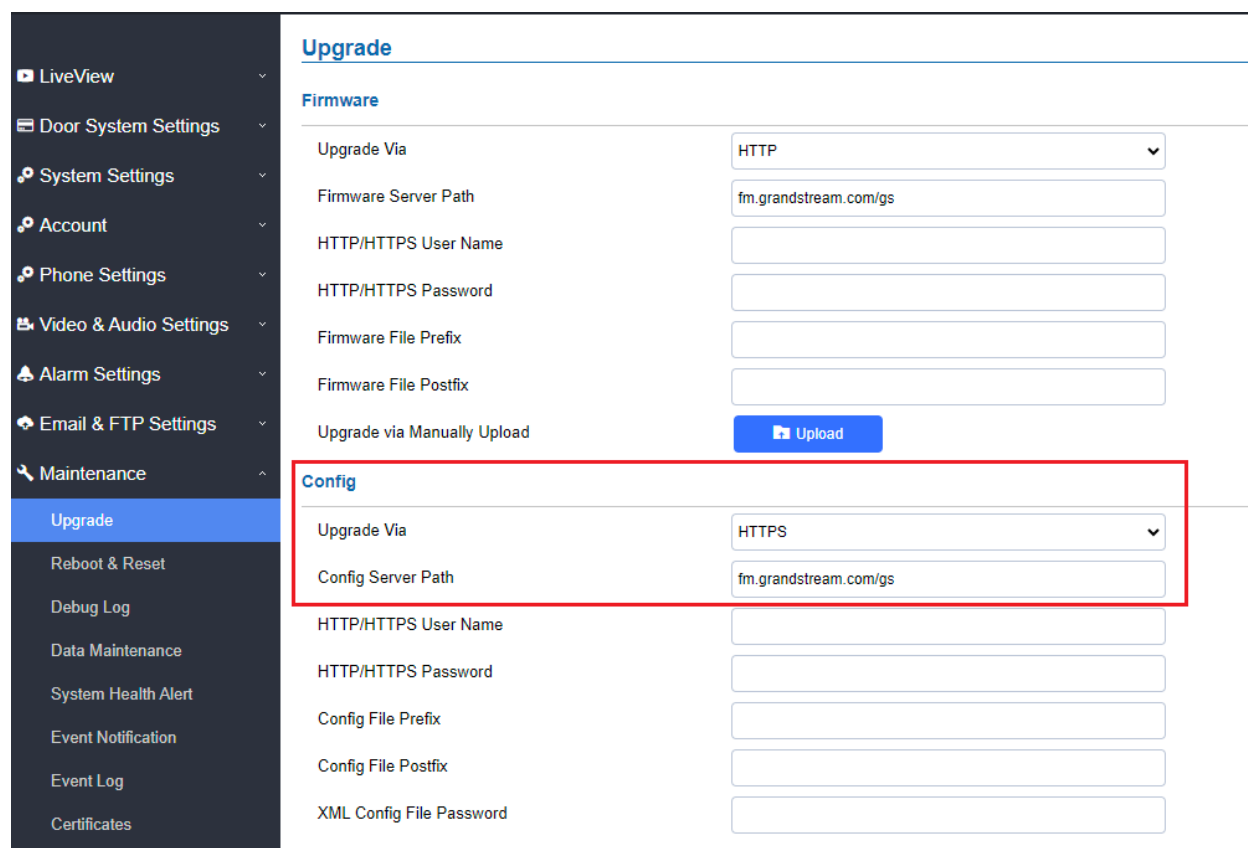
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

HTTPS AS DEFAULT CFG PROVISIONING METHOD (ZOOM COMPATIBLE)

- Web Configuration**

This feature can be found under device web UI: Maintenance → Upgrade → Config:



The screenshot displays the Grandstream device web UI. On the left is a dark sidebar with a menu. The 'Upgrade' option is selected and highlighted in blue. The main content area is divided into two sections: 'Upgrade' and 'Config'. The 'Upgrade' section contains fields for 'Upgrade Via' (set to HTTP), 'Firmware Server Path' (fm.grandstream.com/gs), 'HTTP/HTTPS User Name', 'HTTP/HTTPS Password', 'Firmware File Prefix', 'Firmware File Postfix', and an 'Upload' button. The 'Config' section, which is highlighted with a red rectangular box, contains fields for 'Upgrade Via' (set to HTTPS), 'Config Server Path' (fm.grandstream.com/gs), 'HTTP/HTTPS User Name', 'HTTP/HTTPS Password', 'Config File Prefix', 'Config File Postfix', and 'XML Config File Password'.

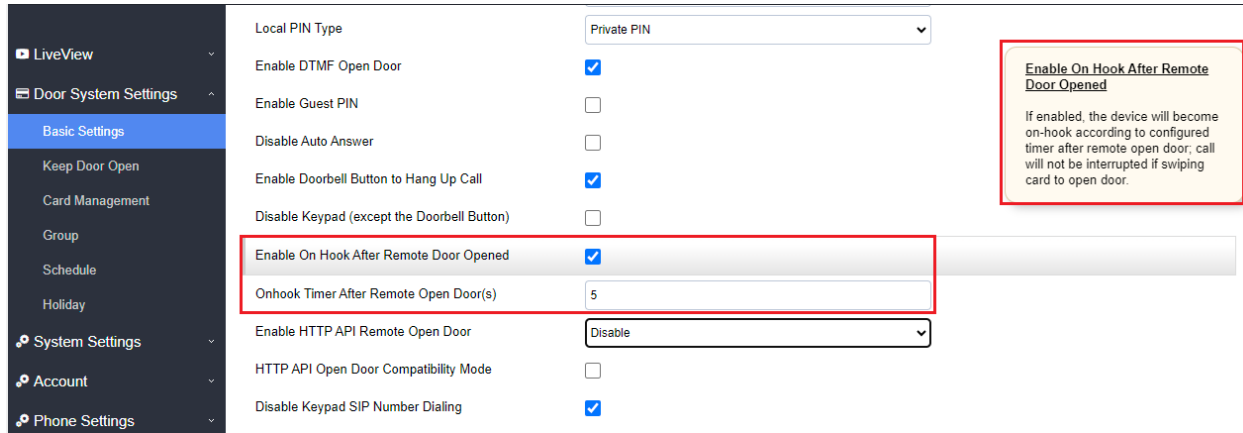
- Functionality**

Factory reset after upgrading to this firmware, the Config path will be changed from previous HTTP to HTTPS. This feature enhancement is implemented based on Zoom IOT. With such a change, device will be provisioned using HTTPS instead of HTTP, to meet the security requirement of Zoom or related ITSP service providers.

INTERVAL OF “ONHOOK TIMER AFTER REMOTE OPEN DOOR(S)” CONFIGURABLE

- **Web Configuration**

This feature can be found under device webUI: Door System Settings → Basic Settings:



Local PIN Type	Private PIN
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>
Disable Auto Answer	<input type="checkbox"/>
Enable Doorbell Button to Hang Up Call	<input checked="" type="checkbox"/>
Disable Keypad (except the Doorbell Button)	<input type="checkbox"/>
Enable On Hook After Remote Door Opened	<input checked="" type="checkbox"/>
Onhook Timer After Remote Open Door(s)	5
Enable HTTP API Remote Open Door	Disable
HTTP API Open Door Compatibility Mode	<input type="checkbox"/>
Disable Keypad SIP Number Dialing	<input checked="" type="checkbox"/>

Enable On Hook After Remote Door Opened

If enabled, the device will become on-hook according to configured timer after remote open door; call will not be interrupted if swiping card to open door.

- **Functionality**

This feature enhancement is implemented based on feedback from field.

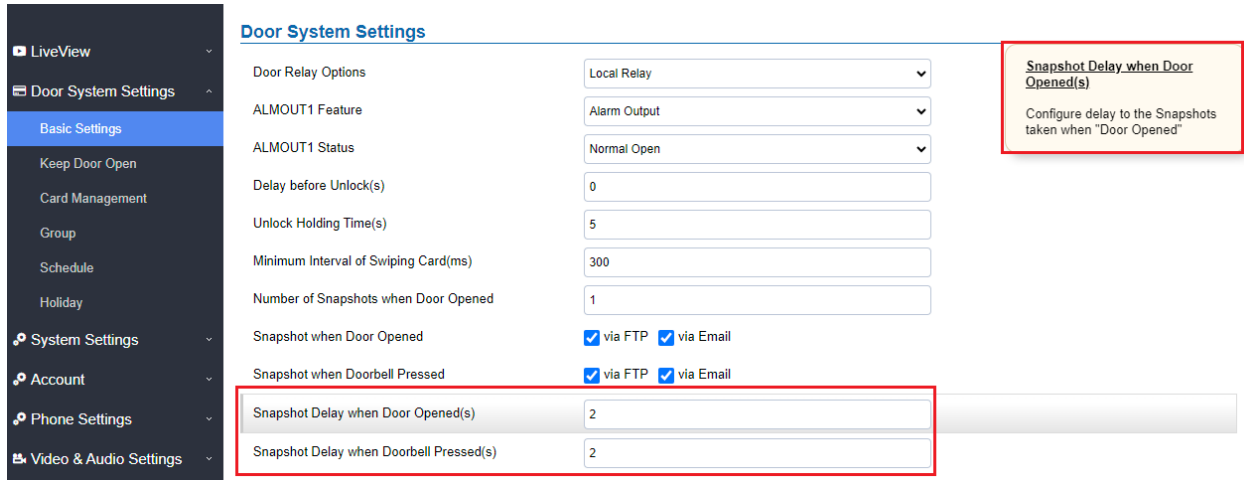
When enabled, user can configure the “Onhook Timer After Remote Open Door(s)” instead of hard coded 3 seconds.

This will help customers check and monitor what’s happening in the application scene after door opened before the call automatically cleared and GDS back to normal idle state.

DELAY FOR SNAPSHOTS TAKEN WHEN “DOOR OPENED” OR “DOORBELL PRESSED”

- **Web Configuration**

This feature can be configured under device webUI: Door System Settings → Basic Settings:



Door System Settings	
Door Relay Options	Local Relay
ALMOUT1 Feature	Alarm Output
ALMOUT1 Status	Normal Open
Delay before Unlock(s)	0
Unlock Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Number of Snapshots when Door Opened	1
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email
Snapshot Delay when Door Opened(s)	2
Snapshot Delay when Doorbell Pressed(s)	2

Snapshot Delay when Door Opened(s)
 Configure delay to the Snapshots taken when "Door Opened"

- **Functionality**

This feature enhancement is implemented based on feedback from the field. Customers want to take snapshots AFTER door opened or doorbell pressed.

This new feature allows customers to configure this Delay Timer instead of previous snapshots taken immediately when door opened or doorbell pressed.

With such configurable timer, customers can get the desired delay snapshots after door opened or doorbell pressed, to meet the exactly needs in the installation environment.

ADMIN AUDIT LOGGING TO THE EVENT LOG FUNCTIONALITY [ITSP: MASERGY]

- **Web Configuration**

This feature can be found under device webUI: Maintenance → Event Log:

<ul style="list-style-type: none"> LiveView Door System Settings System Settings Account Phone Settings Video & Audio Settings Alarm Settings Email & FTP Settings Maintenance <ul style="list-style-type: none"> Upgrade Reboot & Reset Debug Log Data Maintenance System Health Alert Event Notification Event Log 	Event Log		
	Start Time <input type="text" value="2023-11-29 00:00:00"/> End Time <input type="text" value="2023-11-29 15:53:47"/> All <input type="button" value="Search"/>		
	No.	Date & Time	Event Type
	1	2023-11-29 08:49:20	Call In Log
	2	2023-11-29 13:10:59	admin log in success
	3	2023-11-29 13:13:11	Firmware Update(1.0.13.2)
	4	2023-11-29 13:13:11	Reboot
	5	2023-11-29 13:30:43	admin log in success
	6	2023-11-29 13:47:37	admin log off due to timeout
	7	2023-11-29 14:43:07	admin log in success
	8	2023-11-29 14:58:24	admin log off due to timeout

- **Functionality**

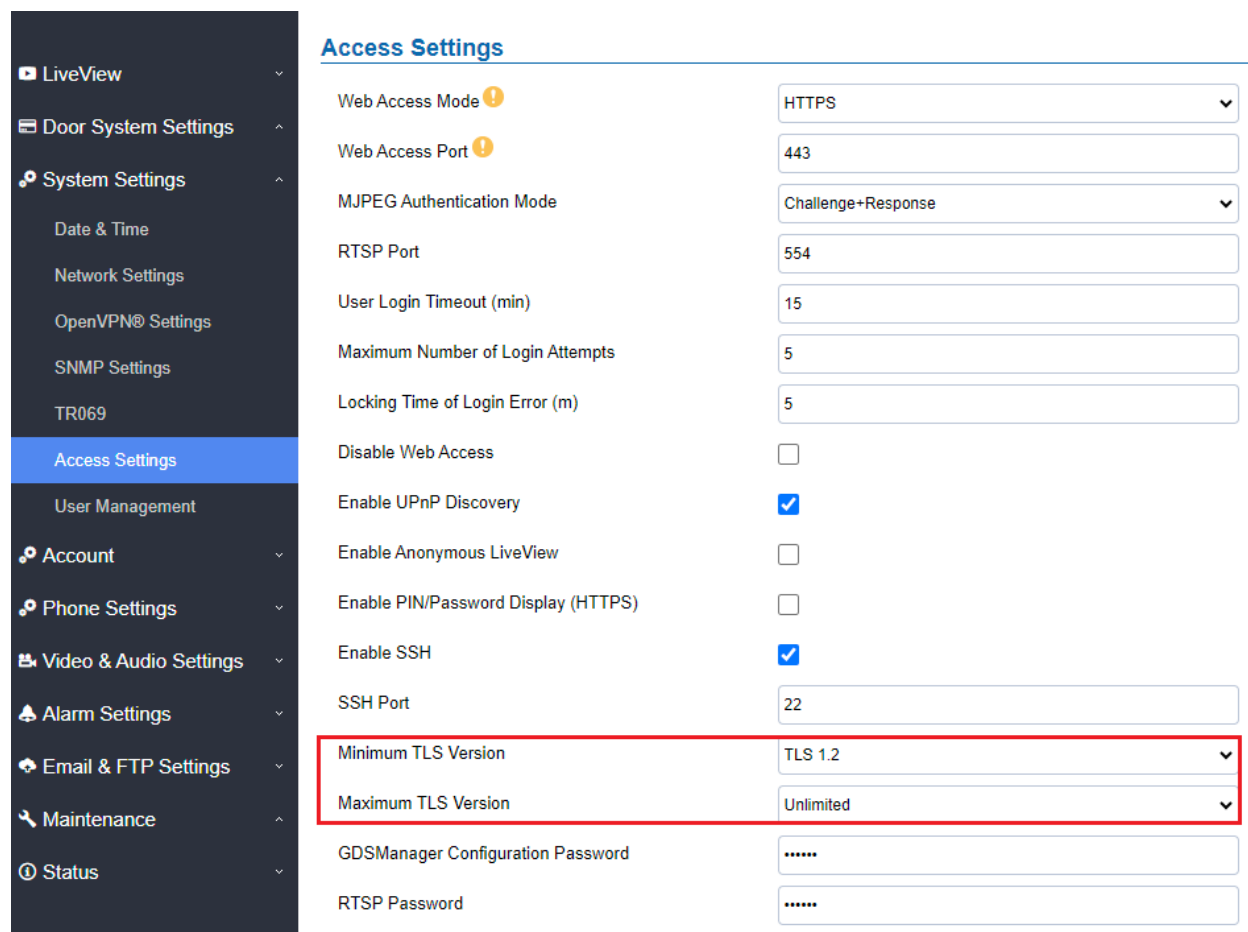
This feature enhancement is implemented based on the requirement of ITSP (MASERGY)

This new feature allows admin activities to be logged in the Event Log table, as seen in the above screenshot.

DEFINE THE TLS PROTOCOL LEVEL

- Web Configuration**

This feature can be configured under device web UI: System Settings → Access Settings:



Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	554
User Login Timeout (min)	15
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
Minimum TLS Version	TLS 1.2
Maximum TLS Version	Unlimited
GDSManager Configuration Password	*****
RTSP Password	*****

- Functionality**

This feature enhancement is implemented based on ITSP requirement.

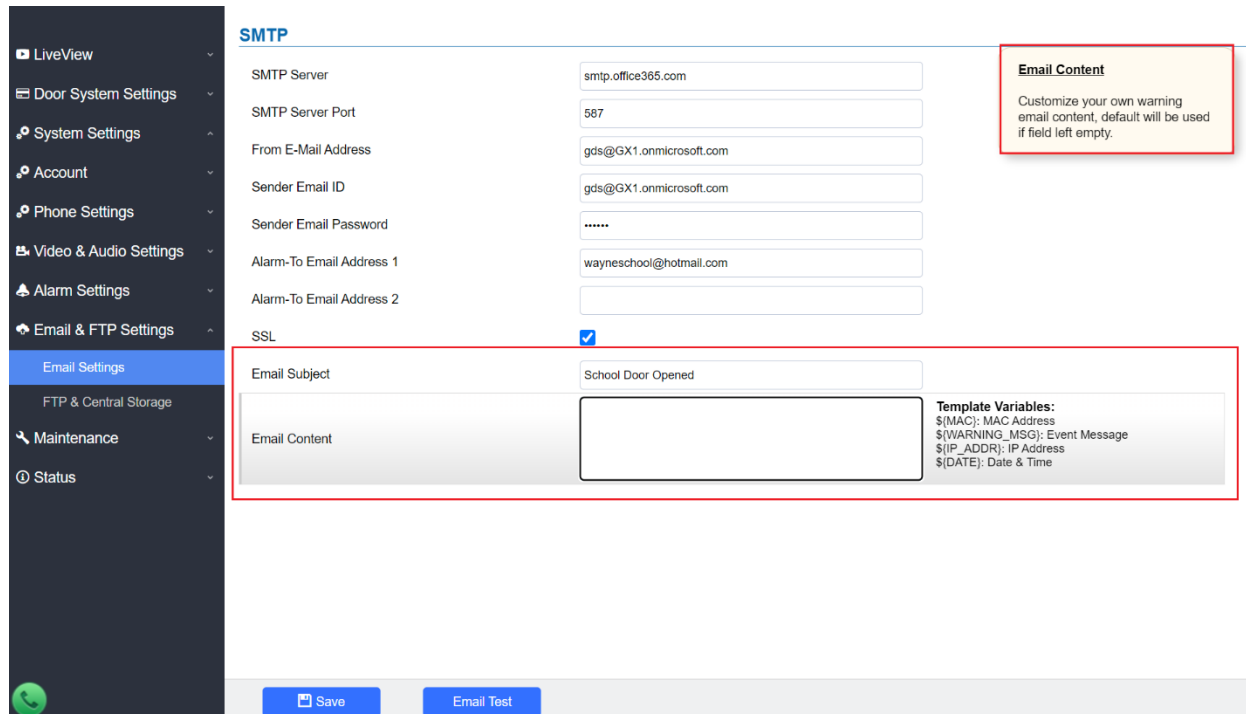
Some ITSPs only allow in their network infrastructure the devices support some particular TLS lever. (For example, only TLS 1.2 allowed and older versions of the protocol have been forbidden)

This feature will allow those ITSP customers to define the level of the TLS protocol they want to enforce in the network deployment environment.

IMPROVED ALARM EMAIL SUBJECT AND TEXT

- Web Configuration**

This feature can be found under device webUI: Email & FTP Settings → Email Settings:



- Functionality**

This feature enhancement is implemented based on feedback from the field.

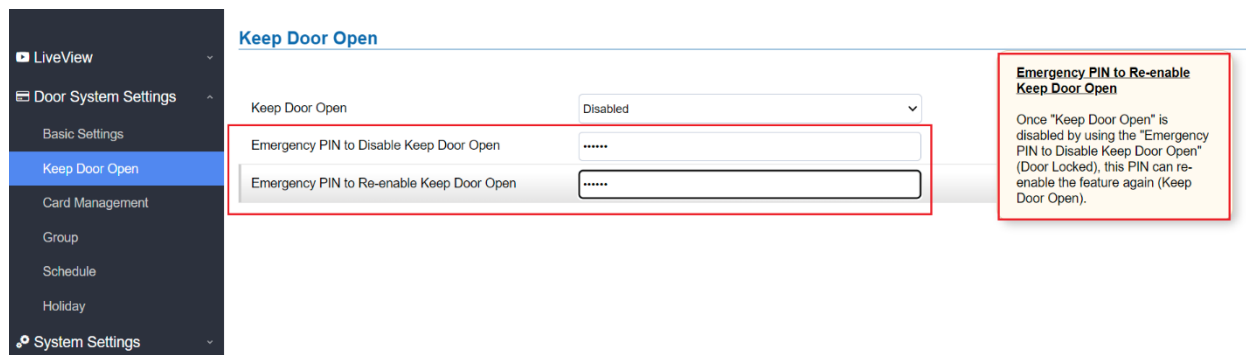
Customers can now customize the Email Subject and Email Content, based on the installation or implementation scene of the GDS, just like the what they can do in the Grandstream IP Cameras.

This is especially useful for customers with the implementation site where many doors exist, like but not limited to: Schools, Gym, Hospitals, Office Buildings, etc.

EMERGENCY PIN TO RE-ENABLE KEEP DOOR OPEN

• Web Configuration

This feature can be configured under device webUI: Door System Settings → Keep Door Open:



• Functionality

This feature enhancement is implemented based on feedback from the field, especially for K-12 school system which the feature “Keep Door Open” is designed for.

During the scheduled “Keep Door Open” period, if emergency (like lock-down) happened the user can enter the emergency PIN (locally from GDS keypad or remotely call into it) to disable the “Keep Door Open” (Lock the Door) ; if emergency is gone, user can do the same thing by re-enable the “Keep Door Open” (Open the Door) locally from keypad of GDS or remotely by calling into GDS then entering the PIN remotely.

This feature is mainly developed and implemented for users like the K-12 school system, library, gym, club, etc., where doors need to open to public at some time but locked later on.

NOTES:

- For locally at GDS keypad, the PIN input format is: *PIN#
- For remotely operation during call with GDS, just like DTMF open door with PIN format: PIN#
- The two emergency PINs must be different.
- The two PINs recommended to be different in length with other normal Open Door PINs
- The phones used to input emergency PINs must be inside card database or white list, just like authorized phones capable of doing normal DTMF open door.

For example, normal (private or DTMF open door) PIN is 3 digits (e.g.: 123), the emergency PIN to “Disable Keep Door Open” is 4 digits (e.g.: 9999), and emergency PIN to “Re-enable Keep Door Open” is also 4 digits (e.g.: 6666). If there is a lock down and must “Disable Keep Door Open”, related personal can do operation in below two scene:

- 1) If at the door beside the GDS, just input emergency PIN like: *9999#
- 2) Make a call from authorized phone to GDS and input emergency PIN like: 9999#

WEBUI DISPLAY CERTIFICATE TYPE INFORMATION

- **Web Configuration**

This feature can be found under device webUI: Status → System Info:

- LiveView
- Door System Settings
- System Settings
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status
- Account Status
- System Info
- Network Info

System Info

Product Model	GDS3710
Hardware Version	V1.6A
Part Number	9650001416A
Boot Version	1.0.0.59
Core Version	1.0.13.2
Base Version	1.0.13.2
Prog Version	1.0.13.2
Certificate Type	RSA+SHA256
System Uptime	19 hours 49 minutes

Firmware Status

UP TO DATE: 1.0.13.2

Check

System Temperature	37°C (98.6°F)
Tamper Sensor	Triggered
Door Ctrl	Untriggered
Digit Output	Untriggered
Digit Input 1	Untriggered

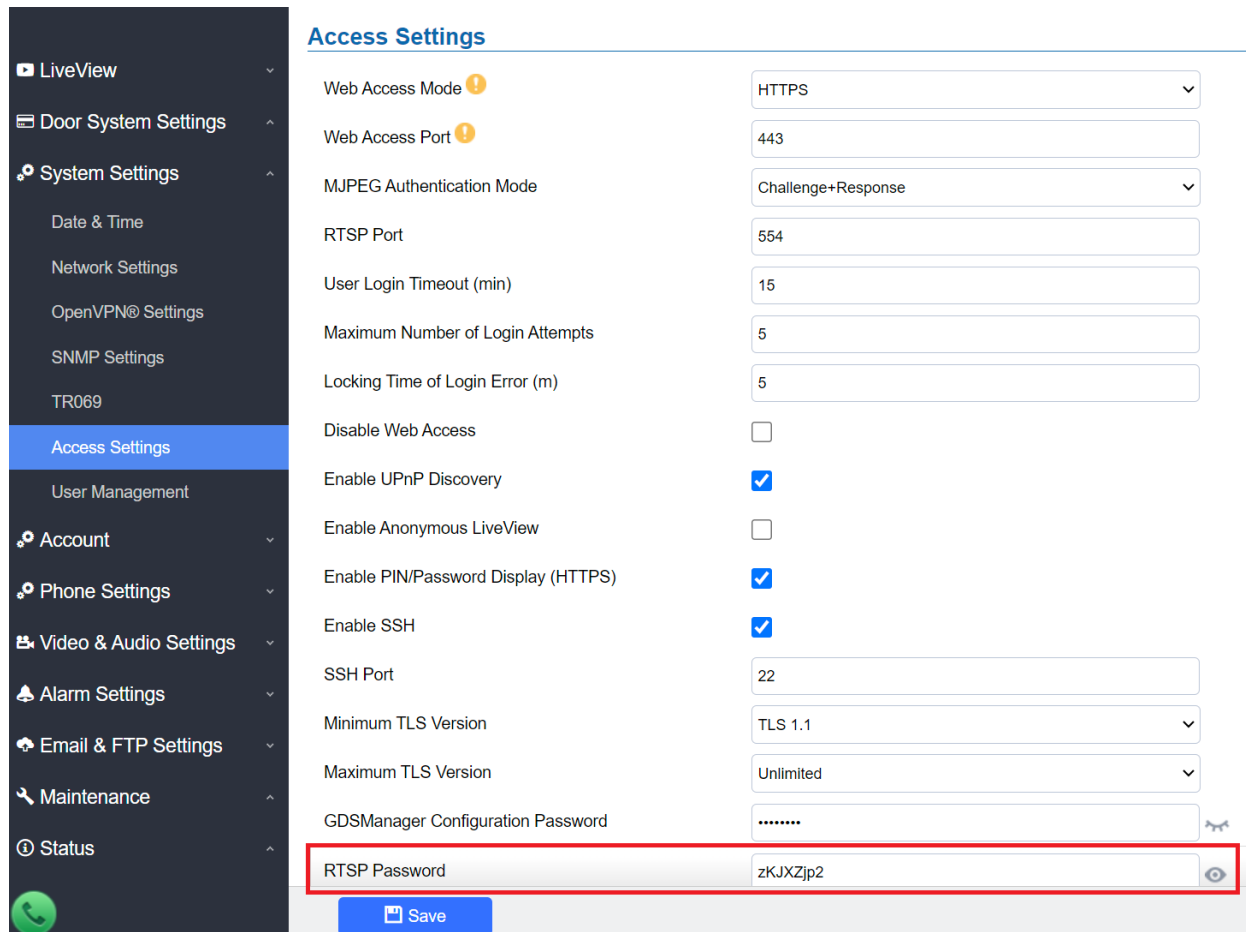
- **Functionality**

This feature enhancement is implemented based on ITSP requirement.

ACCESS WITH RTSP PASSWORD IN ONVIF

- Web Configuration**

This feature can be found under device webUI: System Settings → Access Settings:



Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	554
User Login Timeout (min)	15
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
Minimum TLS Version	TLS 1.1
Maximum TLS Version	Unlimited
GDSManager Configuration Password
RTSP Password	zKJXZjp2

Save

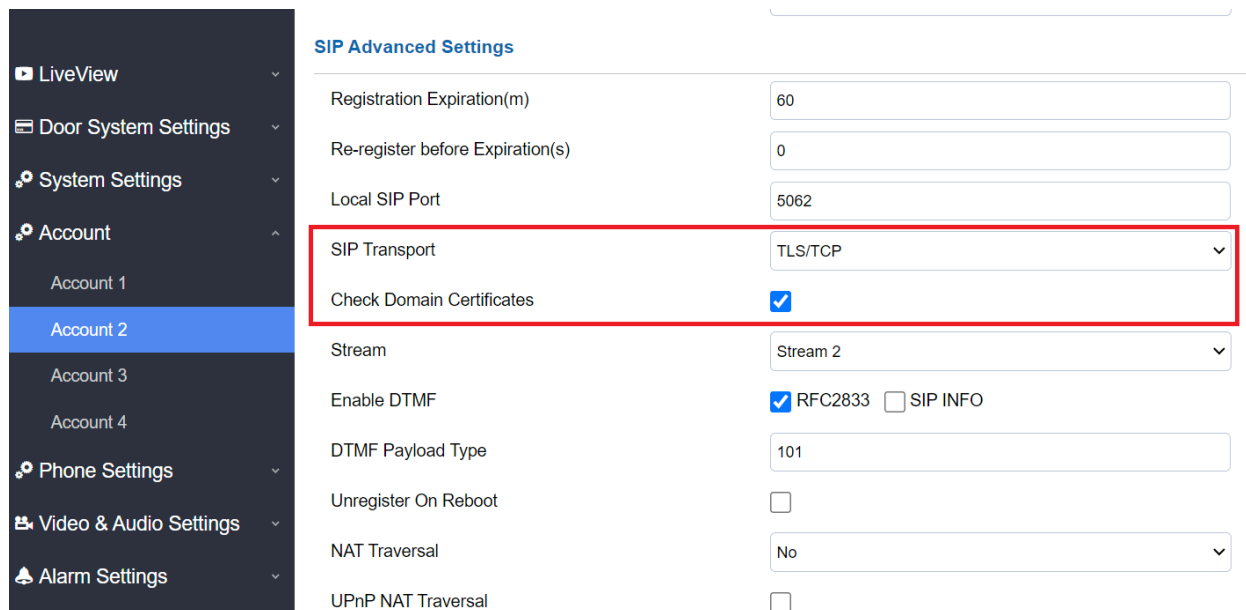
- Functionality**

This feature enhancement will allow user to add and use the RTSP password when interoperating with ONVIF certified device for video recording, instead of using admin password.

SNI EXTENSION ON TLS [ITSP NETIA]

- Web Configuration**

This feature can be configured under device webUI: Account → Account X → SIP Advanced Settings:



SIP Advanced Settings	
Registration Expiration(m)	60
Re-register before Expiration(s)	0
Local SIP Port	5062
SIP Transport	TLS/TCP
Check Domain Certificates	<input checked="" type="checkbox"/>
Stream	Stream 2
Enable DTMF	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
DTMF Payload Type	101
Unregister On Reboot	<input type="checkbox"/>
NAT Traversal	No
UPnP NAT Traversal	<input type="checkbox"/>

- Functionality**

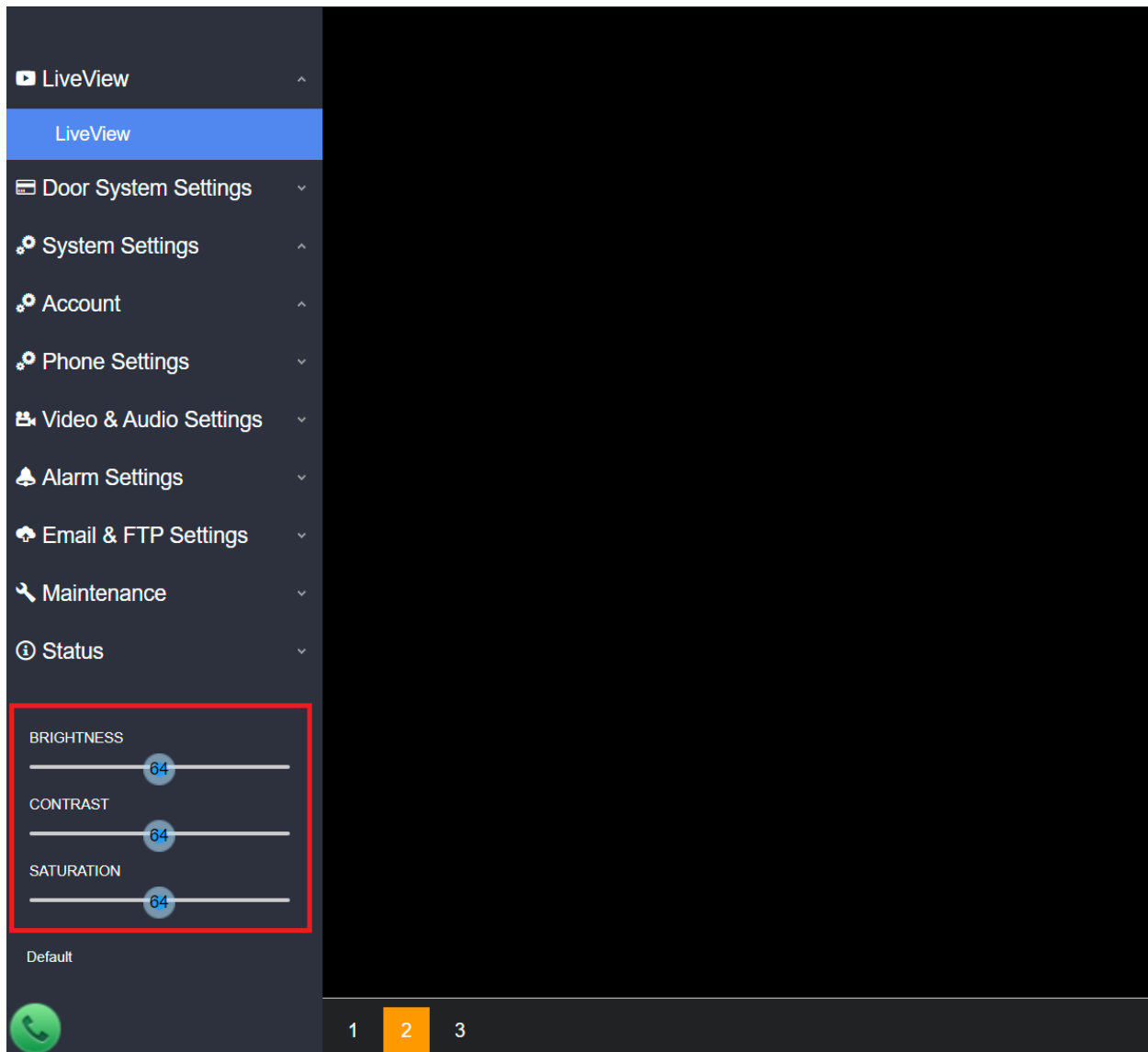
This feature enhancement is implemented based on requirement from ITSP NETIA.

Under Account X configured, in the SIP Advanced Settings, choose “TLS/TCP” in the SIP Transport, the choose “Check Domain Certificates” choice will show up, click to check and select it, the device will then following ITSP’s security requirement to check the certificate before connecting to SIP Server.

BRIGHTNESS/CONTRAST/SATURATION ADJUSTMENT IN LIVEVIEW PAGE

- **Web Configuration**

This feature can be found under device webUI: LiveView → LiveView:



- **Functionality**

This feature enhancement is implemented based on requirement from customers.

Go to the LiveView page, there are bars displayed under “BRIGHTNESS, CONTRAST, SATURATION”, drag and bar left or right the displayed number will change, therefore dynamically adjust those values to meet the image/video quality expectation by users.

For detailed information about GDS371X, please refer to User Manual and Resource Center:

- **GDS371X User Manual:**
<https://documentation.grandstream.com/article-categories/facility-access-systems/>
- **HOW-TO Guide**
<https://documentation.grandstream.com/article-categories/interconnection-facility/>
- **HTTP API** documentation can be downloaded from here:
<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

FIRMWARE VERSION 1.0.11.23

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A, 2.2A)

GDS3712 (HW Supported: 1.0A, 1.1A, 1.2A)

DATE

08/28/2022

SUMMARY OF UPDATE

The main purpose of this release is bug fixes, features enhancement and new HW support.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior, or Web UI display missing some parameters or settings, factory reset is MANDATORY.

Please backup the configuration file and database file of RFID cards before factory reset, and import them back after factory reset.

This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.XA, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW2.2A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	
GDS3712 HW1.1A	YES	
GDS3712 HW1.0A	YES	

ENHANCEMENT

- Added ability to disable alarm siren sound in triggered alarm call.
- Added "Keep Door Open" could be configured to use multiple schedules and allow users to choose and apply which schedule to use.
- Added granular DIGITAL OUTPUT time duration (1s to 4s).
- Added sending PIN via Wiegand when HTTP API open door executed.
- Added option that no "#" required after PIN input to make device behave like traditional access controller when "Disable Keypad SIP Number Dialing" selected.
- Added firmware upgrade via manually upload firmware file from computer.
- Optimized speaker via OQA testing
- Updated CPE version to 1.0.5.5

BUG FIX

- Fixed alarm phone list 1 not used if alarm phone list 2 is empty.
- Fixed MJPEG video cannot be previewed via API if the authentication mode is basic mode.
- Fixed SNMP settings some key-related parameters configured, the local value is inconsistent with the delivered value.
- Fixed unable to pass video from GDS371X to remote RC Wave client
- Fixed no INVITE to 2nd SIP Server if primary SIP Server no response.
- Fixed device should unregister first when changing SIP transport mode [3CX IOT]
- Fixed wrong profile-lever-id at INVITE after changing video parameters of the device.
- Fixed device security vulnerabilities reported by security agents.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing keypad the response will be abnormal till the call time out (about 2 minute).

NEW P-VALUE

P15571	Door_System_Settings.Keep_Door_Open.Door_1.Schdule (Value: 0 – 10)
P15572	Door_System_Settings.Keep_Door_Open.Door_2.Schdule (Value: 0 – 10)
P15575	Alarm_Settings.Alarm_Phone_List_2.Alarm_Call_Out_Account (Value: 0/1/2/3/4)
P15576	Alarm_Settings.Alarm_Phone_List_2.Alarm_Phone (Value: String, Max. Length = 1024)

UPDATED P-VALUE

P15540	Door_System_Settings.Bassic_Settingsgs.Door_relay_Options (Value: 0/1/2 → 0/1/2/3)
P15541	Alarm_Settings.Alarm_Events_Config.Aarm_Output_Duration (Value: 5/10/15/20/25/3 → 1/2/3/4/5/10/15/20/25/30)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sch_open_door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15571=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15572=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P15575=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15576=<value>

Released HTTP API documentation can be downloaded from here:

<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

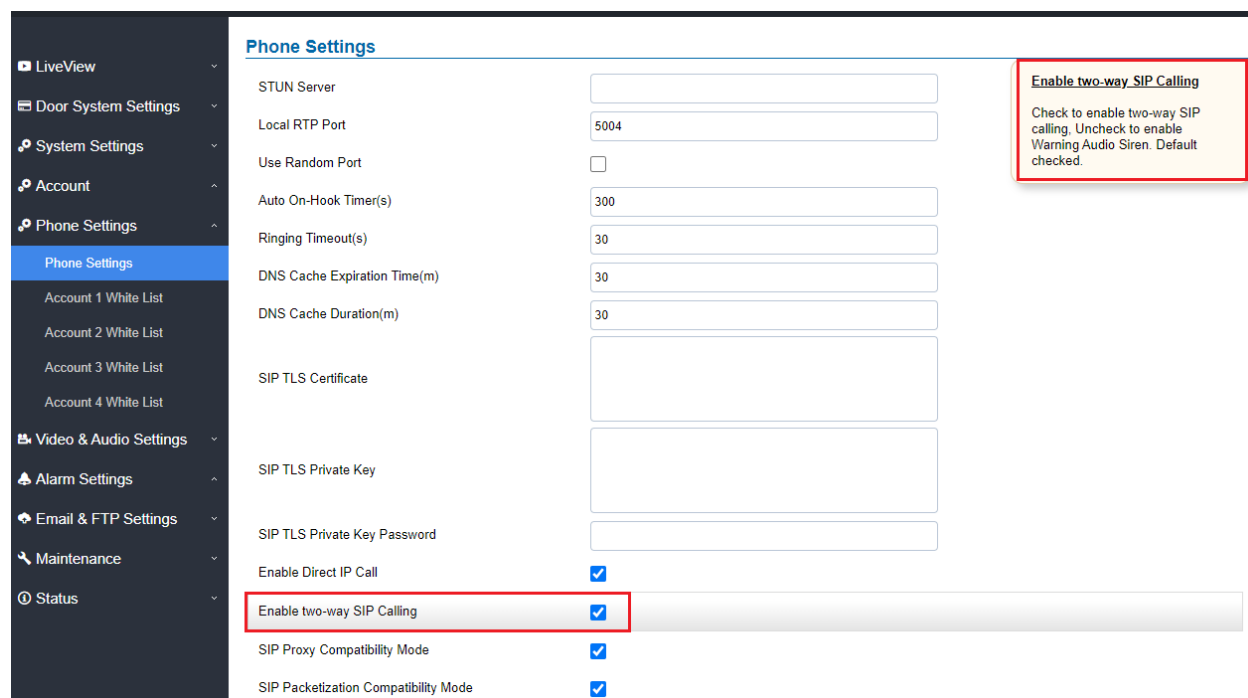
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

DISABLE ALARM SIREN IN TRIGGERED ALARM CALL

- **Web Configuration**

This feature can be configured under device web UI → Phone Settings:



Phone Settings

STUN Server	<input type="text"/>
Local RTP Port	5004
Use Random Port	<input type="checkbox"/>
Auto On-Hook Timer(s)	300
Ringing Timeout(s)	30
DNS Cache Expiration Time(m)	30
DNS Cache Duration(m)	30
SIP TLS Certificate	<input type="text"/>
SIP TLS Private Key	<input type="text"/>
SIP TLS Private Key Password	<input type="text"/>
Enable Direct IP Call	<input checked="" type="checkbox"/>
Enable two-way SIP Calling	<input checked="" type="checkbox"/>
SIP Proxy Compatibility Mode	<input checked="" type="checkbox"/>
SIP Packetization Compatibility Mode	<input checked="" type="checkbox"/>

Enable two-way SIP Calling

Check to enable two-way SIP calling. Uncheck to enable Warning Audio Siren. Default checked.

- **Functionality**

This feature enhancement is implemented based on feedback from field. Customers want to install button as Alarm Input, press the button trigger emergence call to special configured number.

Previously the triggered call will have siren audio (although the callee press any key in the phone's keypad will stop the siren, but still some first time users are confused with it).

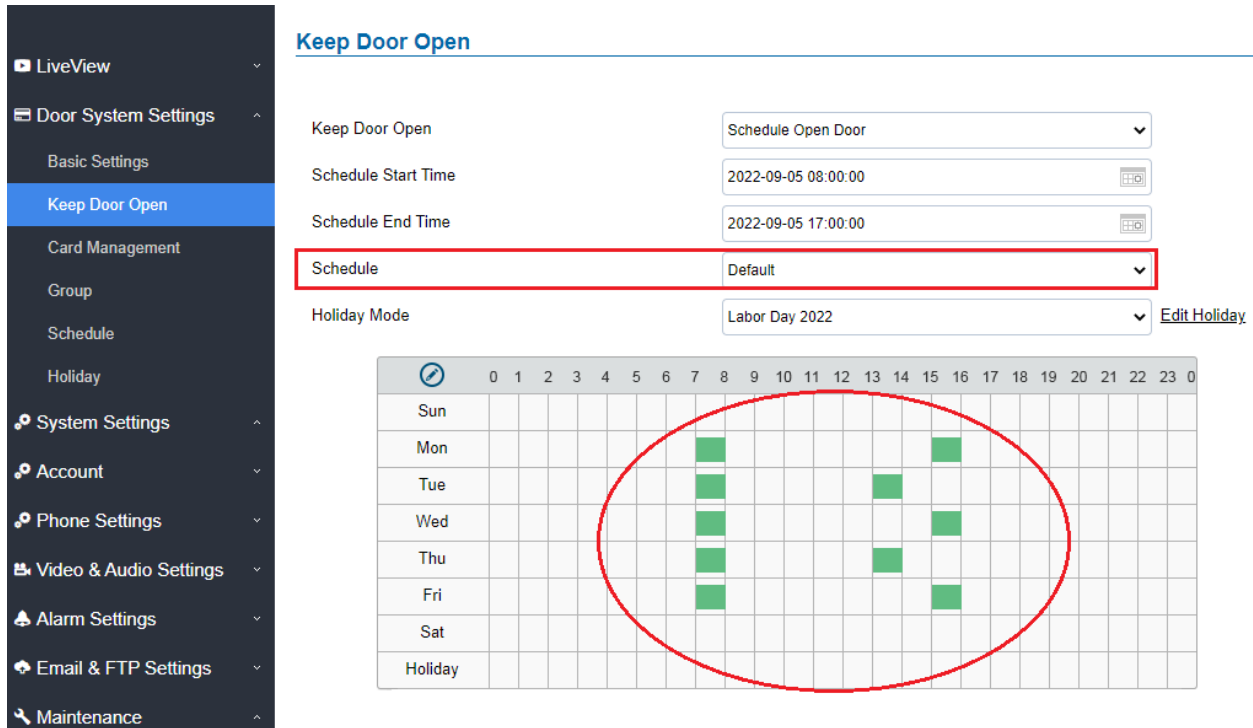
The new firmware default disabled the siren and triggered call will be two-way audio (with video if video phone used as callee).

This feature is requested in application scene like nursing call, clinic, hospital, etc., where buttons are installed as Alarm Input, pressed the button will call out to pre-programmed number (or IP address if no SIP Proxy) based on configured "Alarm Schedule" and "Alarm Action Profile" configured.

MULTIPLE SCHEDULES FOR “KEEP DOOR OPEN”

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Keep Door Open:



Keep Door Open

Keep Door Open: Schedule Open Door

Schedule Start Time: 2022-09-05 08:00:00

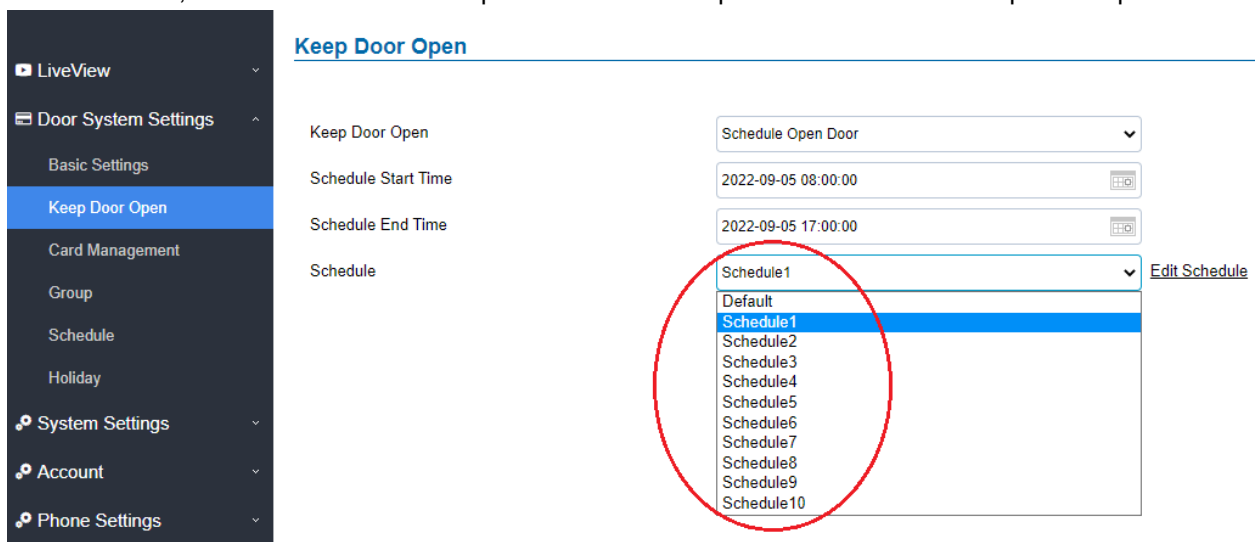
Schedule End Time: 2022-09-05 17:00:00

Schedule: Default

Holiday Mode: Labor Day 2022 [Edit Holiday](#)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0
Sun																									
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Holiday																									

With this new feature, customers can pre-configure the “Default” schedule, as well as other 10 schedules into the device, then based on actual requirement to select specific schedule for “Keep Door Open”.



Keep Door Open


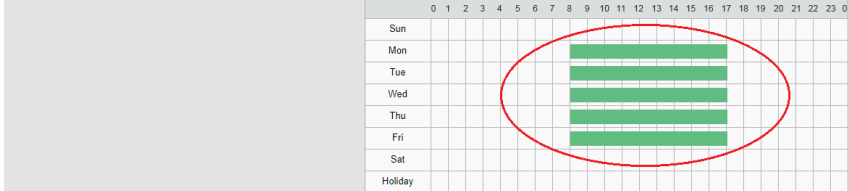









Keep Door Open: Schedule Open Door

Schedule Start Time: 2022-09-05 08:00:00

Schedule End Time: 2022-09-05 17:00:00

Schedule: Schedule1

[Edit Schedule](#)

No.	Schedule Name	Holiday Name	Detail
1	Weekday_Working_Hours	Disabled	
			
2	Weekday_Non_Working_Hours	Disabled	
3	Weekend_Day_Hours	Disabled	
4	Weekend_Night_Hours	Disabled	
5	schedule5	Disabled	
6	schedule6	Disabled	
7	schedule7	Disabled	
8	schedule8	Disabled	
9	schedule9	Disabled	
10	schedule10	Disabled	

NOTES:

- Maximum 11 different “Schedule” can be configured including the “Default” one.
- For this feature to work properly, customers need to pre-configure the “Schedule” accordingly:

• Functionality

This feature enhancement is implemented based on feedback from field.

For example, device installed at public schools could have different “Holidays” and “Keep Door Open” schedules. Customers could pre-program or pre-configure based on “Holidays” of each school semester and select the related “schedule” accordingly when it comes.

This will help school management as once pre-programmed, the door will just automatic open or close based on the configured time schedule or holidays, like early-release, snow or storm day or late opening, etc.

GRANULAR TIME DURATION OF DIGITAL OUTPUT

- Web Configuration**

This feature can be configured under device web UI → Alarm Settings → Alarm Events Config:

Alarm Settings

- Alarm Events Config**
- Alarm Schedule Settings
- Alarm Action Settings
- Alarm Phone List
- Email & FTP Settings
- Maintenance
- Status

Digit Input

Digit Input 1: Disable

Digit Input 2: Disable

Digit Output

Alarm Output Duration(s): 5

Alarm Config

Enable Silent Alarm Mode: ☐

Enable Hostage Code: ☐

Enable Tamper Alarm: ☐

- Functionality**

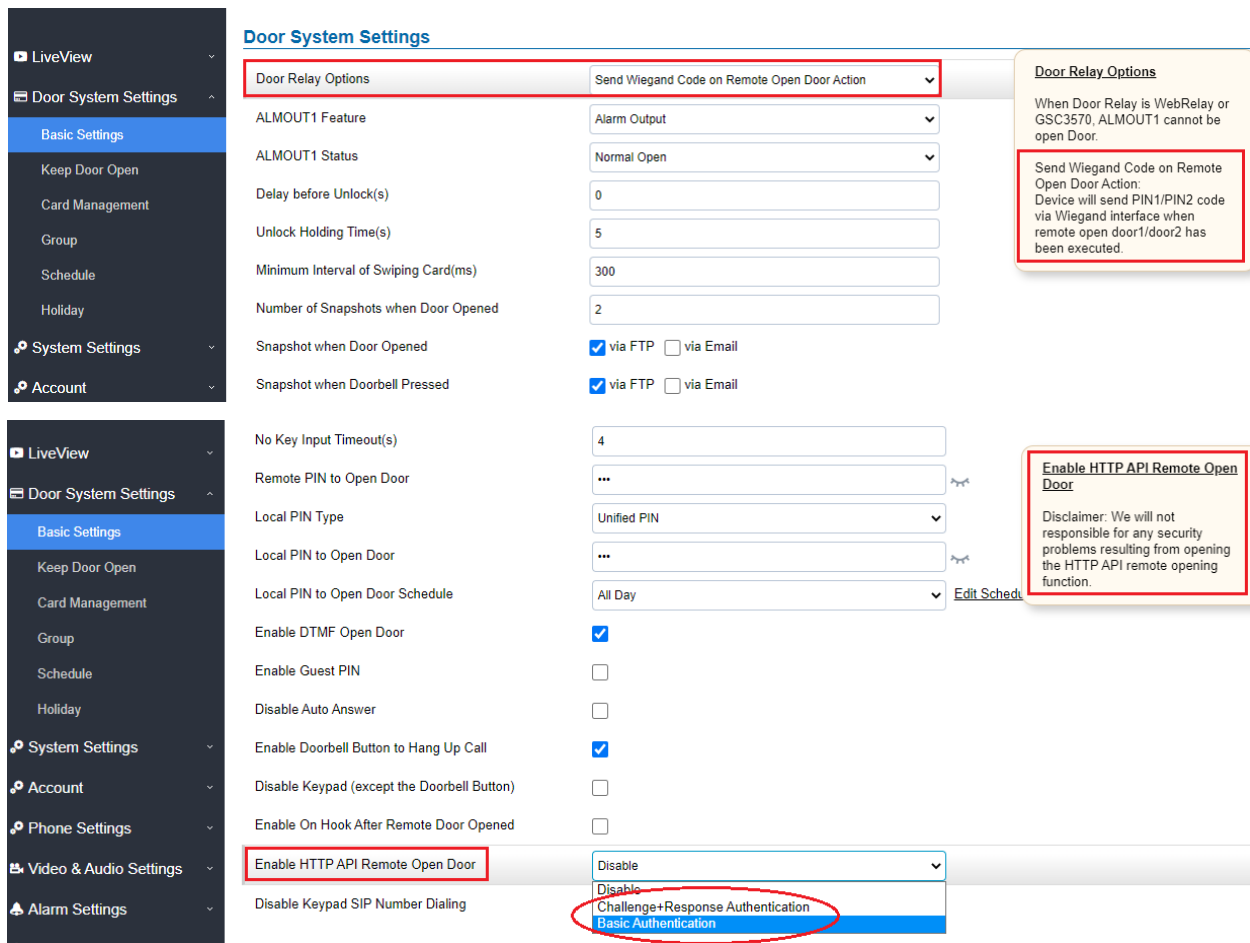
This feature enhancement is implemented based on feedback from field. Customers want to reduce the Alarm Output Duration, which previously the minimum value is 5 seconds.

Now new value of 1, 2, 3, 4 seconds added, see the pull-down selection, customers can not choose specific alarm duration second based on application scene.

SEND PIN VIA WIEGAND WHEN HTTP API OPEN DOOR EXECUTED

• Web Configuration

This feature can be configured under device web UI → Door System Settings → Basic Settings → Door Relay Options:



Door System Settings

Door Relay Options

Send Wiegand Code on Remote Open Door Action ▼

ALMOUT1 Feature: Alarm Output ▼

ALMOUT1 Status: Normal Open ▼

Delay before Unlock(s): 0

Unlock Holding Time(s): 5

Minimum Interval of Swiping Card(ms): 300

Number of Snapshots when Door Opened: 2

Snapshot when Door Opened: ☒ via FTP ☐ via Email

Snapshot when Doorbell Pressed: ☒ via FTP ☐ via Email

No Key Input Timeout(s): 4

Remote PIN to Open Door: ...

Local PIN Type: Unified PIN ▼

Local PIN to Open Door: ...

Local PIN to Open Door Schedule: All Day ▼ [Edit Schedule](#)

Enable DTMF Open Door: ☒

Enable Guest PIN: ☐

Disable Auto Answer: ☐

Enable Doorbell Button to Hang Up Call: ☒

Disable Keypad (except the Doorbell Button): ☐

Enable On Hook After Remote Door Opened: ☐

Enable HTTP API Remote Open Door ▼

Disable Keypad SIP Number Dialing

Door Relay Options

When Door Relay is WebRelay or GSC3570, ALMOUT1 cannot be open Door.

Send Wiegand Code on Remote Open Door Action: Device will send PIN1/PIN2 code via Wiegand interface when remote open door1/door2 has been executed.

Enable HTTP API Remote Open Door

Disclaimer: We will not responsible for any security problems resulting from opening the HTTP API remote opening function.

Disable
Challenge+Response Authentication
Basic Authentication

NOTES:

- “Send Wiegand Code on Remote Open Door Action” need to be selected in the “Door Relay Options” pull-down menu.
- “Enable HTTP API Remote Open Door” need to be selected and related authentication method also need to be selected from the pull-down menu.
- By default the HTTP API Remote Open Door is Disabled for security reason, and system integrators need to enable this option for integration solution.

Output example with 3rd party power supply for Wiegand device

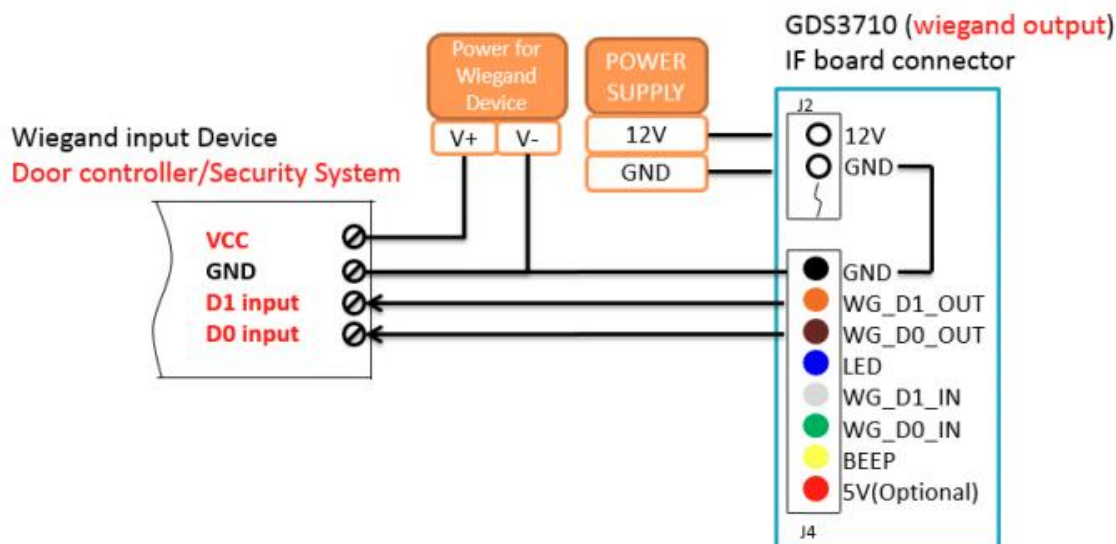


Figure 28: Wiegand Output Wiring Example

Functionality

This feature enhancement is implemented based on feedback from forum/field from Europe region.

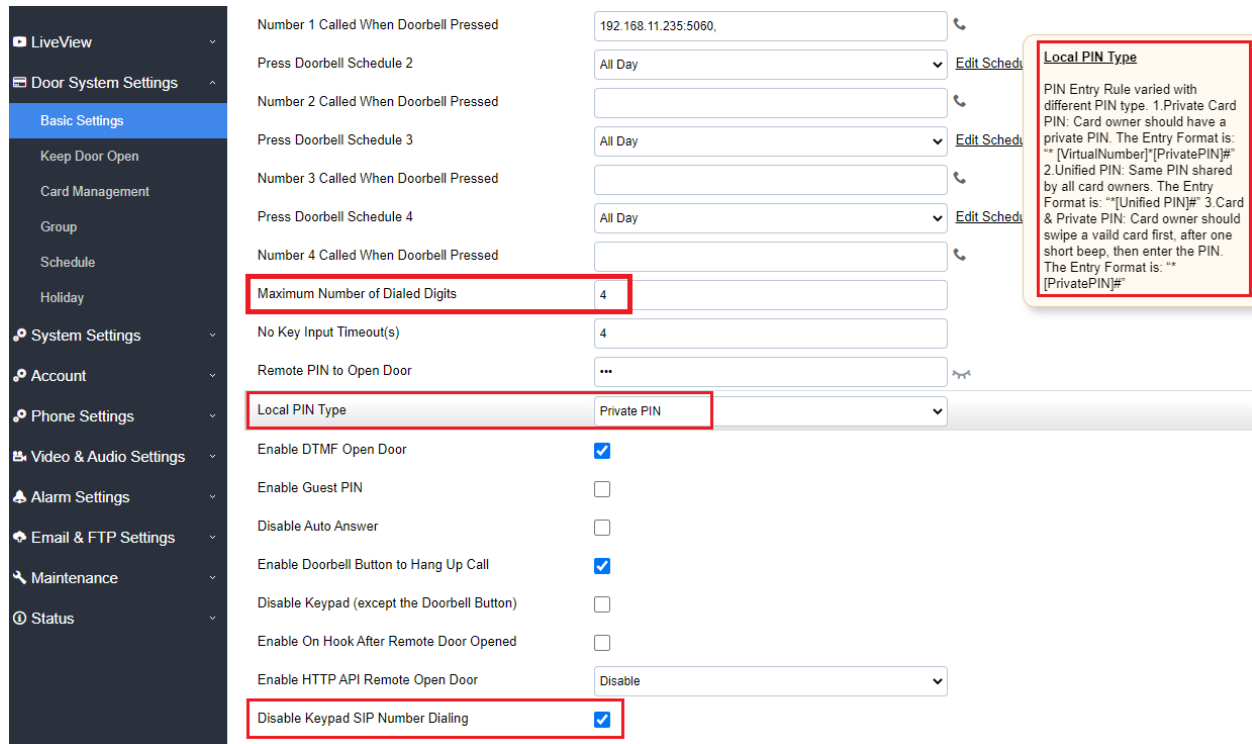
System integrators want use HTTP API to trigger open door event, and the related open door PIN (Door1 or Door2) will be sent out via the Wiegand Interface of GDS37xx (Wiegand Output, see the related wiring diagram in [Page 50](#) of [User Manual](#)) to connected 3rd party Door Controller to execute Remote Open Door, based on the correct PIN used.

Also, when GSC3570 used in this application scene, once the “Virtual Open Door” icon pressed, the PIN of related Door (Door1 or Door2) will be sent out via the Wiegand Interface to 3rd party Door Controller, similar to the HTTP API, to execute remote open door by the 3rd party Door Controller.

NO “#” REQUIRED AFTER PIN INPUT WHEN “DISABLE KEYPAD SIP NUMBER DIALING”

• Web Configuration

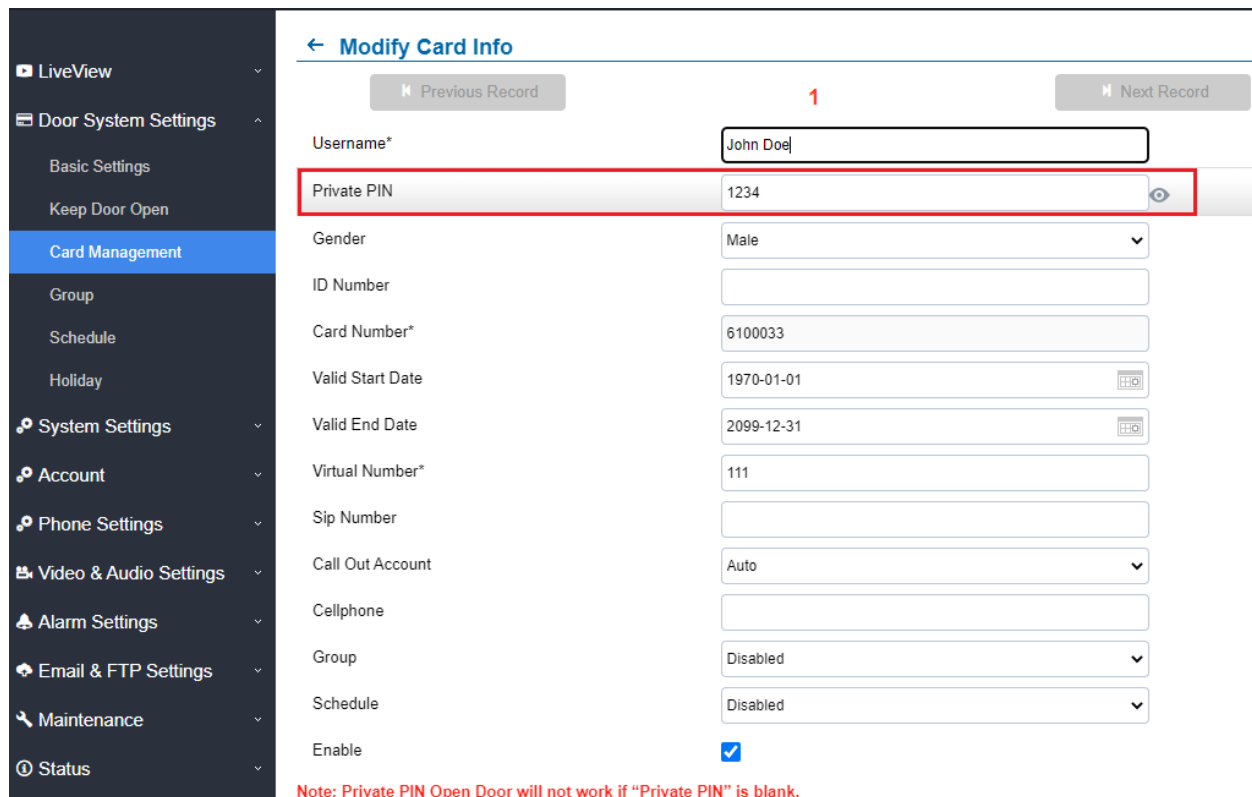
This feature can be configured under device web UI → Door System Settings → Basic Settings:



Local PIN Type

PIN Entry Rule varied with different PIN type. 1. Private Card PIN: Card owner should have a private PIN. The Entry Format is: "[VirtualNumber]"[PrivatePIN]#. 2. Unified PIN: Same PIN shared by all card owners. The Entry Format is: "[UnifiedPIN]#. 3. Card & Private PIN: Card owner should swipe a valid card first, after one short beep, then enter the PIN. The Entry Format is: "[PrivatePIN]#"

Number 1 Called When Doorbell Pressed	192.168.11.235:5060,
Press Doorbell Schedule 2	All Day
Number 2 Called When Doorbell Pressed	
Press Doorbell Schedule 3	All Day
Number 3 Called When Doorbell Pressed	
Press Doorbell Schedule 4	All Day
Number 4 Called When Doorbell Pressed	
Maximum Number of Dialed Digits	4
No Key Input Timeout(s)	4
Remote PIN to Open Door	...
Local PIN Type	Private PIN
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>
Disable Auto Answer	<input type="checkbox"/>
Enable Doorbell Button to Hang Up Call	<input checked="" type="checkbox"/>
Disable Keypad (except the Doorbell Button)	<input type="checkbox"/>
Enable On Hook After Remote Door Opened	<input type="checkbox"/>
Enable HTTP API Remote Open Door	Disable
Disable Keypad SIP Number Dialing	<input checked="" type="checkbox"/>



← Modify Card Info

Previous Record 1 Next Record

Username*	John Doe
Private PIN	1234
Gender	Male
ID Number	
Card Number*	6100033
Valid Start Date	1970-01-01
Valid End Date	2099-12-31
Virtual Number*	111
Sip Number	
Call Out Account	Auto
Cellphone	
Group	Disabled
Schedule	Disabled
Enable	<input checked="" type="checkbox"/>

Note: Private PIN Open Door will not work if "Private PIN" is blank.

- **Functionality**

This feature enhancement is implemented based on feedback from field. Customers who using “Disable Keypad SIP Number Dialing” want the device behave like traditional access control device, just input private PIN to open door, **no “#” required** after input the PIN, because users are get used to the behavior of open door via analogue device or door controller.

“Maximum Number of Dialed Digits” has to be configured in order to use this new feature. By default the value is “0” and the feature is disabled. If this field is NOT configured, user still have to add “#” after input PIN to open door, as previous firmware. When this feature is enabled, ALL PIN should be the same length, as the number configured in this field.

Users have to configure the PIN in “Card Management” and input the “Private PIN” in related card/user, and match the PIN length to the “Maximum Number of Dialed Digits” configured.

In below example, the length of the “Maximum Number of Dialed Digits” is “4”, then in the “Private PIN” field, the PIN “1234” is configured with PIN length as 4.

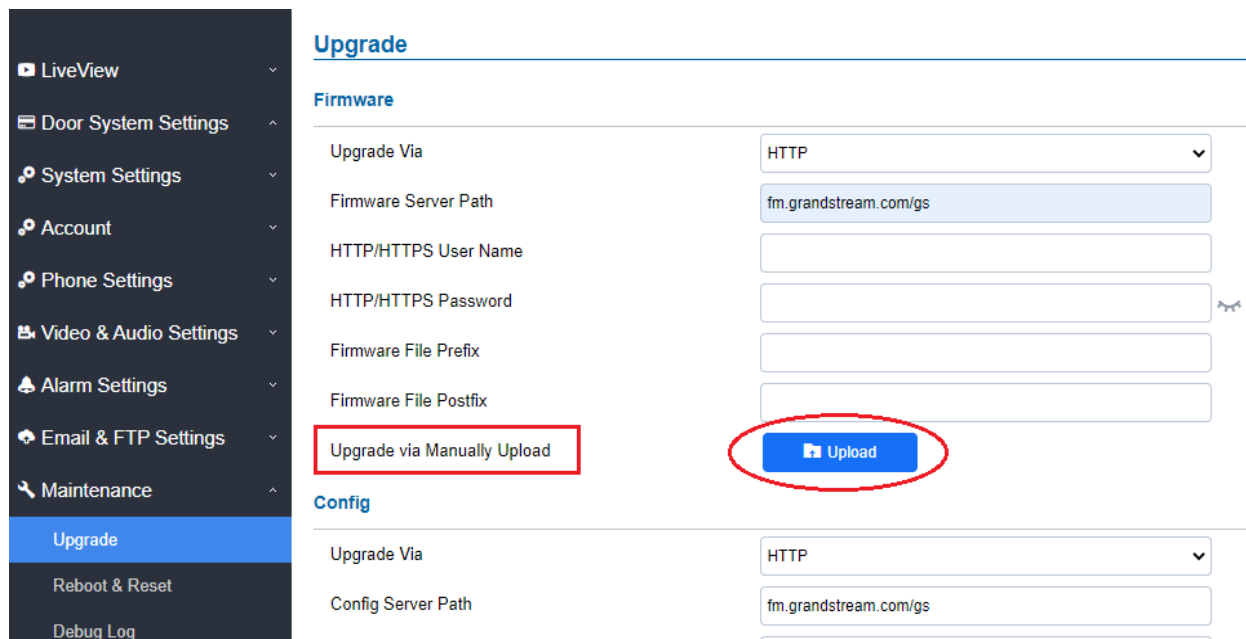
NOTES:

- “Maximum Number of Dialed Digits” is the length of PIN.
- For this feature to work properly, customers need to pre-configure the “PIN” in the “Card Management” field under RFID card’s “Private PIN”, and PIN length should use the same length as configured in the specified in “Maximum Number of Dialed Digits”.
- “Local PIN Type” recommended using “Private PIN” so each card user will have own PIN, and the GDManager will generate report of who and when opened the door, different PIN is also more safe. “Unified PIN” only advise when door opened and cannot tell who because everybody share the same PIN, also less safe therefore not suggested for usage in this application scenario.

FIRMWARE UPGRADE VIA LOCAL FILE UPLOAD

- **Web Configuration**

This feature can be found under device web UI → Maintenance → Upgrade:



The screenshot displays the 'Upgrade' page in the device web UI. On the left is a dark sidebar menu with options: LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Upgrade (highlighted), Reboot & Reset, and Debug Log. The main content area is titled 'Upgrade' and contains two sections: 'Firmware' and 'Config'. In the 'Firmware' section, there are input fields for 'Upgrade Via' (set to HTTP), 'Firmware Server Path' (fm.grandstream.com/gs), 'HTTP/HTTPS User Name', 'HTTP/HTTPS Password', 'Firmware File Prefix', and 'Firmware File Postfix'. Below these is a red-bordered box containing the text 'Upgrade via Manually Upload'. To the right of this box is a blue 'Upload' button with a folder icon, which is circled in red. The 'Config' section below has similar fields for 'Upgrade Via' and 'Config Server Path'.

- **Functionality**

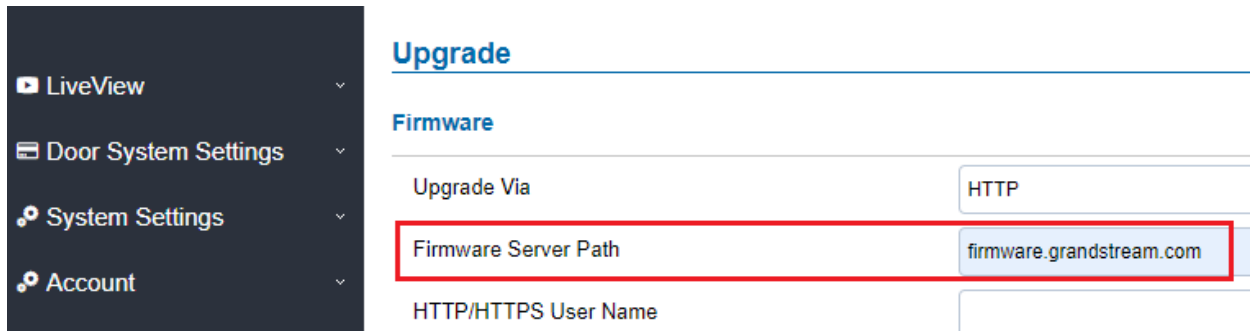
This feature enhancement is implemented based on feedback from field.

Technicians on the field can now download the firmware file into computer before heading to the field. Once on site, technician can log in to the device and upload the firmware file from computer to flash and upgrade the firmware of the device.

This is especially useful for site with limited internet access or no internet access, also for customers without access to HTTP/TFTP firmware server.

NOTES:

- For device with firmware later than 1.0.4.5, or just purchased new device, customer can use “firmware.grandstream.com” to upgrade firmware if having good Internet connection.
- The related configuration is like below by pointing the “Firmware Server Path” to “firmware.grandstream.com”



The screenshot displays the 'Upgrade' section of the Grandstream web interface. On the left is a dark sidebar with navigation links: LiveView, Door System Settings, System Settings, and Account. The main content area is titled 'Upgrade' and 'Firmware'. It contains three configuration fields: 'Upgrade Via' set to 'HTTP', 'Firmware Server Path' set to 'firmware.grandstream.com' (highlighted with a red border), and 'HTTP/HTTPS User Name' which is empty.

Upgrade	
Firmware	
Upgrade Via	HTTP
Firmware Server Path	firmware.grandstream.com
HTTP/HTTPS User Name	

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS371X User Manual:**
<https://documentation.grandstream.com/article-categories/facility-access-systems/>
- **HOW-TO Guide**
<https://documentation.grandstream.com/article-categories/interconnection-facility/>
- **HTTP API** documentation can be downloaded from here:
<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

FIRMWARE VERSION 1.0.11.18

PRODUCT NAME

GDS3710 (HW Supported: **1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A**)

GDS3712 (HW Supported: **1.0A, 1.1A**) – **Initial Launching Firmware**

DATE

05/26/2022

SUMMARY OF UPDATE

The main purpose of this release is bug fixes, features enhancement and new HW support.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior, or Web UI display missing some parameters or settings, factory reset is MANDATORY.

Please backup the configuration file and database file of RFID cards before factory reset, and import them back after factory reset.

This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.0A and HW2.1A, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade
GDS3712 HW1.2A	YES	Initial version 1.0.11.18
GDS3712 HW1.1A	YES	Initial version 1.0.11.18
GDS3712 HW1.0A	YES	Initial version 1.0.11.18

ENHANCEMENT

- Added ability to disable config download with password (ITSP Telefonica)
- Added support for SNMP.
- Disabled dialing Error Beep Tone when making SIP Direct IP Calls.

BUG FIX

- Fixed login timeout range prompts an error.
- Fixed serial hunting doorbell call in probability may not continue when some extension reject the call.
- Fixed card management page remains in loading state after adding a user.
- Fixed Privacy Mask dragging might cause other masks edition and frozen the process.
- Fixed “Enable password display (HTTPS)” prompt not accurate.
- Fixed registration failure when DNS mode is NAPTR and primary Outbound Proxy domain unavailable.
- Fixed registration sending to both primary and secondary SIP servers simultaneously.
- Fixed when alarm call configured as extension and IP address mixed, the alarm call will not ring in configured order but call IP address.
- Fixed enable blue keypad light with wrong time schedule configuration the display would abnormal.
- Fixed not able to use private PIN to open door if adding the RFID card via HTTP API.
- Fixed adding RFID card via HTTP API with valid end date end up with blank in web display.
- Fixed device not working with static IP in VLAN.
- Fixed HTTP access mode cannot revise and save port 80 when using P value.
- Fixed Event Notification HTTP POST method using wrong Content-Type for Template Sample 1 & 2.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing keypad the response will be abnormal till the call time out (about 2 minute).

NEW P-VALUE

P21896	System_Settings.SNMP_Settings.Enable_SNMP (Value: 0 / 1)
P21904	System_Settings.SNMP_Settings.Version (Value: 1 – Version 1; 2 – Version 2; 3 – Version 3)
P21903	System_Settings.SNMP_Settings.SNMP_Port (Value: 161 or 1025 ~ 65535)
P21902	System_Settings.SNMP_Settings.Community (Value: String, Max. Length = 64)
P21899	System_Settings.SNMP_Settings.SNMP_Trapping_Version (Value: 1 – Version 1; 2 – Version 2; 3 – Version 3)
P21897	System_Settings.SNMP_Settings.SNMP_Trapping_IP (Value: String, Max. Length = 16)
P21898	System_Settings.SNMP_Settings.SNMP_Trapping_Port (Value: 162 or 1025 ~ 65535)
P21901	System_Settings.SNMP_Settings.SNMP_Trapping_Interval (Value: 1 ~ 1440)
P21900	System_Settings.SNMP_Settings.SNMP_Trapping_Community (Value: String, Max. Length = 64)
P21905	System_Settings.SNMP_Settings.SNMP_Username (Value: String, Max. Length = 128)
P21910	System_Settings.SNMP_Settings.Security_Level (Value: 0 – noAuthUser; 1 – authUser; 2 – privUser)
P21906	System_Settings.SNMP_Settings.Authentication_Protocol (Value: 0 – None; 1 – MD5; 2 – SHA)
P21907	System_Settings.SNMP_Settings.Privacy_Protocol (Value: 0 – None; 1 – DES; 2 – AES)
P21908	System_Settings.SNMP_Settings.Authentication_Key (Value: String, Max. Length = 2048)
P21909	System_Settings.SNMP_Settings.Privacy_Key (Value: String, Max. Length = 2048)
P21911	System_Settings.SNMP_Settings.SNMP_Trapping_Username (Value: String, Max. Length = 128)
P21916	System_Settings.SNMP_Settings.Trapping_Security_Level (Value: 0 – noAuthUser; 1 – authUser; 2 – privUser)
P21912	System_Settings.SNMP_Settings.Trapping_Authentication_Protocol (Value: 0 – None; 1 – MD5; 2 – SHA)
P21913	System_Settings.SNMP_Settings.Trapping_Privacy_Protocol (Value: 0 – None; 1 – DES; 2 – AES)
P21914	System_Settings.SNMP_Settings.Trapping_Authentication_Key (Value: String, Max. Length = 2048)
P21915	System_Settings.SNMP_Settings.Trapping_Privacy_Key (Value: String, Max. Length = 2048)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=snmp
- SET:[http|https]://<servername>/goform/config?cmd=set&P21896=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21904=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21903=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21902=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21899=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21897=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21898=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21901=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21900=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21905=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21910=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21906=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21907=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21908=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21909=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21911=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21916=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21912=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21913=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21914=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P21915=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

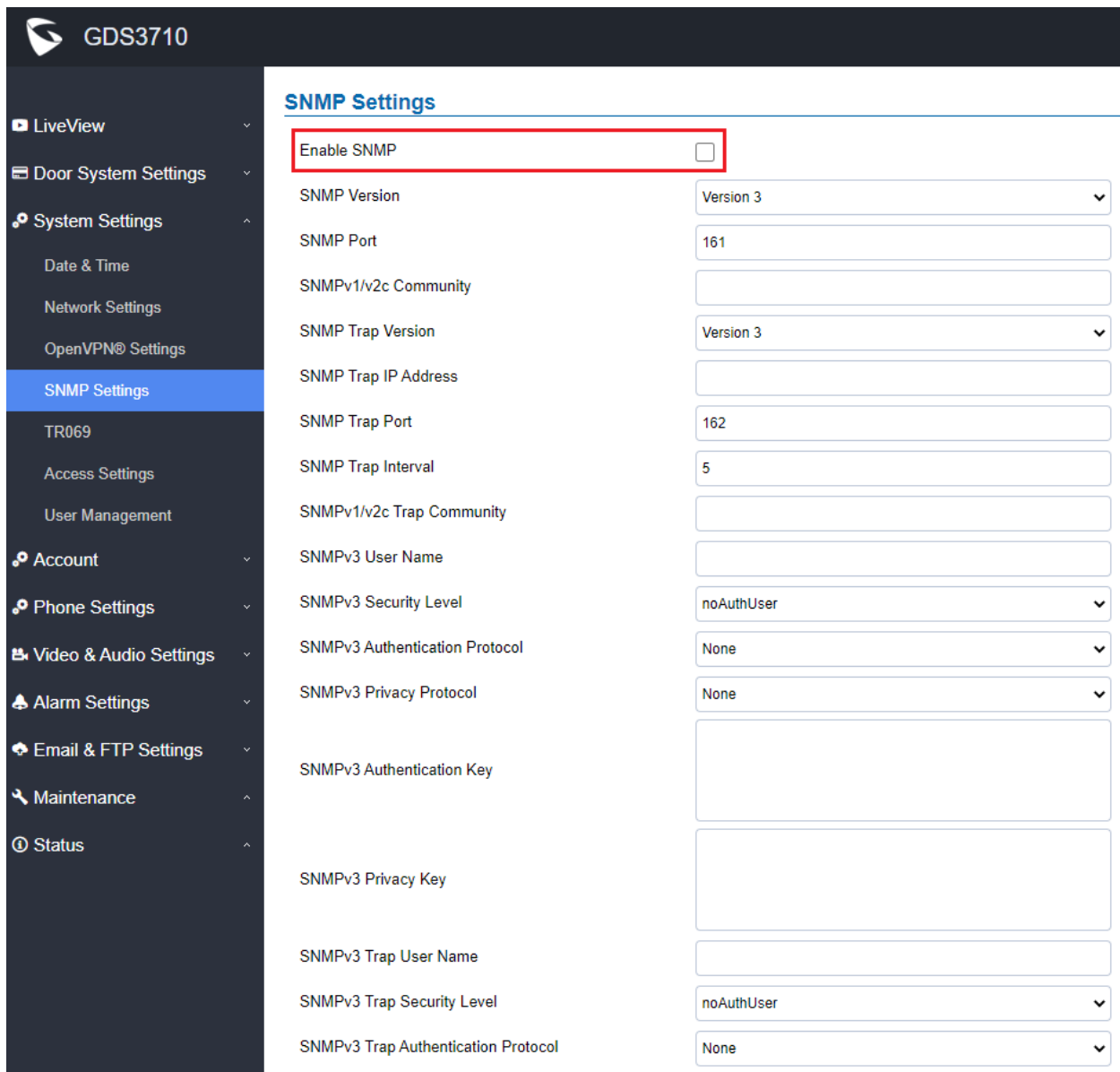
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

SNMP SUPPORT

- **Web Configuration**

This feature can be configured under device web UI → System Settings → SNMP Settings:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, OpenVPN® Settings, SNMP Settings (highlighted), TR069, Access Settings, User Management, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'SNMP Settings' and contains the following configuration options:

Configuration Option	Value
Enable SNMP	<input type="checkbox"/>
SNMP Version	Version 3
SNMP Port	161
SNMPv1/v2c Community	
SNMP Trap Version	Version 3
SNMP Trap IP Address	
SNMP Trap Port	162
SNMP Trap Interval	5
SNMPv1/v2c Trap Community	
SNMPv3 User Name	
SNMPv3 Security Level	noAuthUser
SNMPv3 Authentication Protocol	None
SNMPv3 Privacy Protocol	None
SNMPv3 Authentication Key	
SNMPv3 Privacy Key	
SNMPv3 Trap User Name	
SNMPv3 Trap Security Level	noAuthUser
SNMPv3 Trap Authentication Protocol	None

NOTES:

- By default the SNMP feature is not enabled.
- Related parameters need to be configured according to the SNMP requirement.

- **Functionality**

This feature enhancement is implemented based on feedback from field. Customers want to manage and monitor the GDS3710 via SNMP

This new feature helps to resolve customers with such requirement.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.11.15

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A*)

DATE

04/10/2022

SUMMARY OF UPDATE

The main purpose of this release is bug fixes, features enhancement and new HW support.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior, or Web UI display missing some parameters or settings, factory reset is MANDATORY.

Please backup the configuration file and database file of RFID cards before factory reset, and import them back after factory reset.

This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.0A and HW2.1A, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW2.1A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW2.0A	YES	Not able downgrade to 1.0.9.x
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Added support of configure different “Number Called When Door Bell Pressed” entries depending on the time frame or schedule.

BUG FIX

- Fixed DNS server 2 displayed as “null” under DHCP mode
- Fixed using Chrome to see “LiveView”, when 1st and 2nd streams configured MJPEG while 3rd H.264, no video displayed in the browser
- Fixed switching from MJPEG to H.264 video codec, SIP call no video stream sometimes.
- Fixed in card management the card SIP number is IP (not extension) then manually input PIN to remote open door would fail.
- Fixed illegal card swipe event displayed in “Event Log” incorrectly.
- Fixed swiping legal card in unauthorized schedule will trigger both Non-scheduled Access Alarm and Non-authorized RFID Card Access Alarm (this one should not be triggered).
- Fixed when “Disable Keypad SIP Number Dialing” enabled, device cannot open door when private PIN is more than 9 digits.
- Fixed device falling in looped downloading if firmware file downloaded is incomplete.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.

NEW P-VALUE

P15557	Door_System_Settings.Basic_Settings.Press_Doorbell_Schedule_2 (Value: 0 - 10)
P15556	Door_System_Settings.Basic_Settings.Number_2_Called_When_Doorbell_Pressed (Value: String, Max. Length = 255)
P15559	Door_System_Settings.Basic_Settings.Press_Doorbell_Schedule_3 (Value: 0 - 10)
P15558	Door_System_Settings.Basic_Settings.Number_3_Called_When_Doorbell_Pressed (Value: String, Max. Length = 255)
P15561	Door_System_Settings.Basic_Settings.Press_Doorbell_Schedule_4 (Value: 0 - 10)
P15560	Door_System_Settings.Basic_Settings.Number_4_Called_When_Doorbell_Pressed (Value: String, Max. Length = 255)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15556=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15557=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15558=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15559=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15560=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15561=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

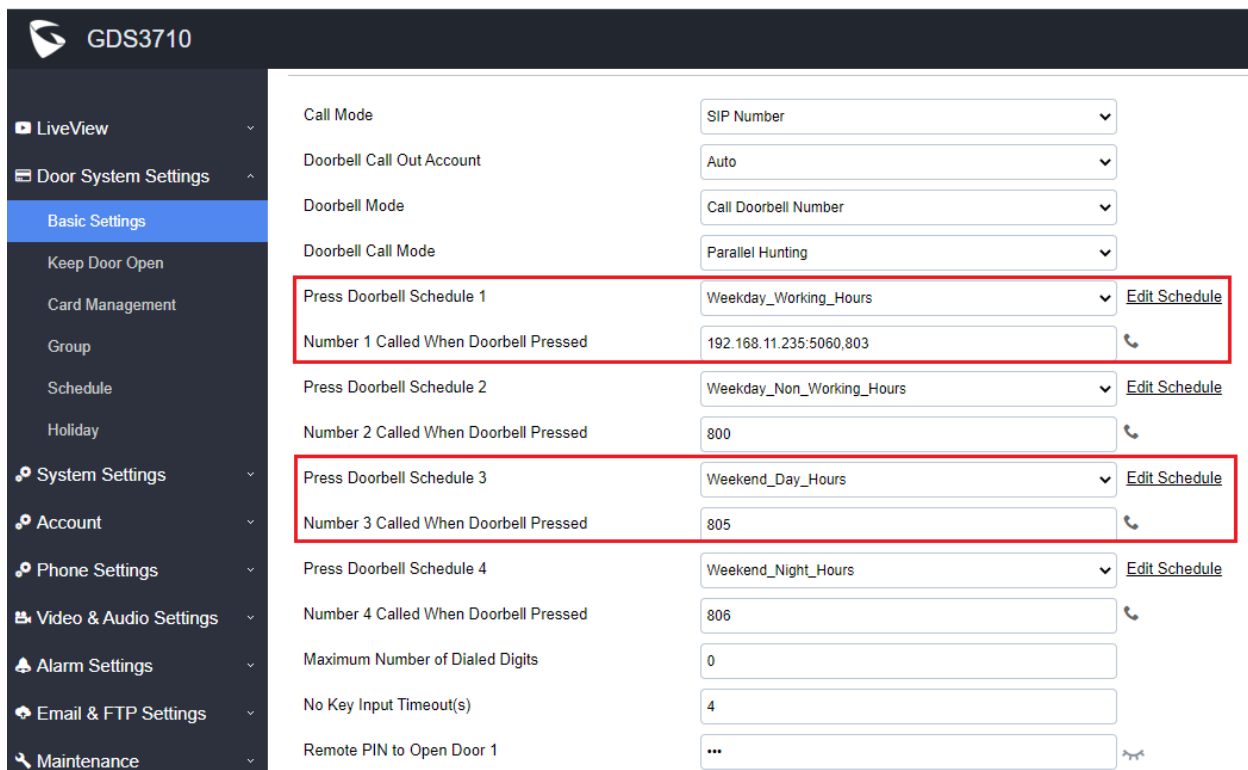
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

DOORBELL CALL DIFFERENT NUMBERS BASED ON DIFFERENT SCHEDULE

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:

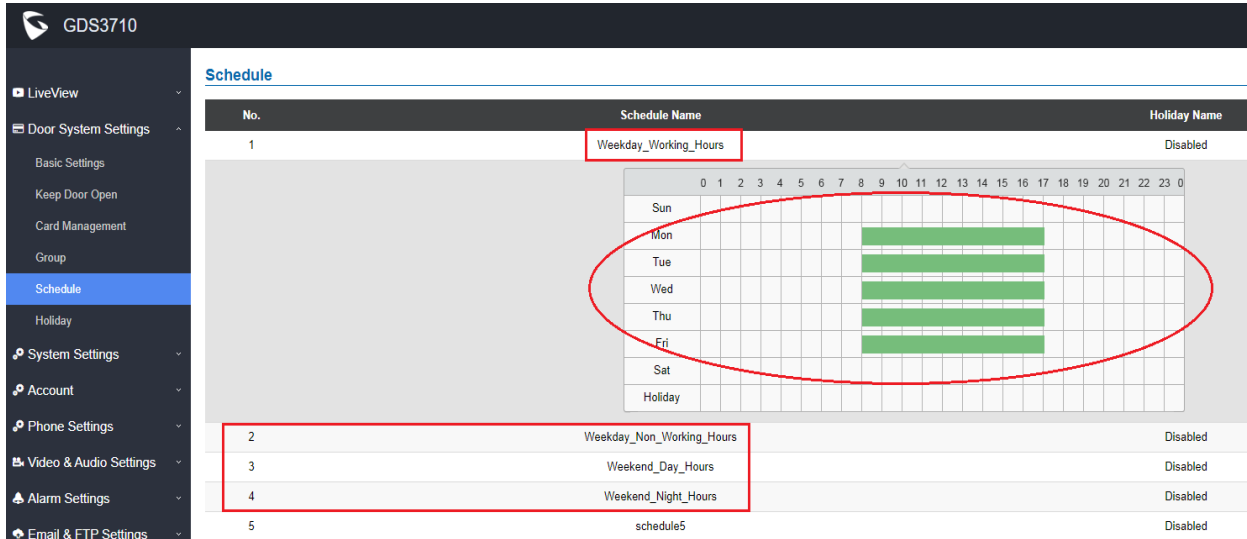


Setting	Value	Action
Call Mode	SIP Number	
Doorbell Call Out Account	Auto	
Doorbell Mode	Call Doorbell Number	
Doorbell Call Mode	Parallel Hunting	
Press Doorbell Schedule 1	Weekday_Working_Hours	Edit Schedule
Number 1 Called When Doorbell Pressed	192.168.11.235:5060,803	
Press Doorbell Schedule 2	Weekday_Non_Working_Hours	Edit Schedule
Number 2 Called When Doorbell Pressed	800	
Press Doorbell Schedule 3	Weekend_Day_Hours	Edit Schedule
Number 3 Called When Doorbell Pressed	805	
Press Doorbell Schedule 4	Weekend_Night_Hours	Edit Schedule
Number 4 Called When Doorbell Pressed	806	
Maximum Number of Dialed Digits	0	
No Key Input Timeout(s)	4	
Remote PIN to Open Door 1	...	

NOTES:

- Maximum 4 different “Schedule” can be configured.
- “Doorbell” Call Number or IP address must be configured in related “Schedule”.
- The priority order of schedule is “Schedule 1, 2, 3, 4”. The device will first check and verify current time fits in “Schedule 1”, if yes it will dial out using the configured number in Number 1; if not it will check “Schedule 2” and dial out using the configured number in Number 2 if result matched, and continue to do such checking and verification in loop till end.

For this feature to work properly, customers also need to pre-configure the “Schedule” accordingly:



No.	Schedule Name	Holiday Name
1	Weekday_Working_Hours	Disabled
2	Weekday_Non_Working_Hours	Disabled
3	Weekend_Day_Hours	Disabled
4	Weekend_Night_Hours	Disabled
5	schedule5	Disabled

• Functionality

This feature enhancement is implemented based on feedback from field. Customers want doorbell call to directed to different extensions or IP address based on different time schedule.

For example, Weekly Office Hour to ring at Front Desk; Off office hour ring at person in charge, etc.

This new feature helps to resolve customers with such requirement.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.11.13

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A, 2.0A, 2.1A)

DATE

01/12/2022

SUMMARY OF UPDATE

The main purpose of this release is bug fixes, features enhancement and new HW support.

This is **MAJOR UPDATE** with purpose of bug fixes and feature enhancement. Please read below WARNING carefully before upgrading.

WARNING:

- **TWO self-reboot** required to finish the whole upgrade process, it could take time for about **20 minutes**. Please be patient and **DO NOT interrupt power** during the process. Lost power or network during the process can brick the device.
- When Blue light of the keypad displaying “1, 2, 3”, “4, 5, 6” **animating the bar movement**, the device is erasing/writing flash. Lost power will damage the device.
- After 20 minutes, please press any button on the keypad, If having Beep sound and Blue light when button pressed, it means the device finished upgrading and booted successfully. If no Beep sound and Blue light, it means the device has not finished upgrade yet, **DO NOT** unplug power otherwise it would damage the device.
- Once finished upgrade, please download and run **GS Search** in the PC to search the device in LAN. The device must be displayed in the result of “search” and showing correct firmware version. Double clicking it will open browser to get into device log in web UI successfully. That indicates upgrading process successfully completed.
- **Local upgrade strongly recommended**. Please download and use **GS Upgrade Tool** provided by Grandstream or own local HTTP/TFTP server to upgrade firmware, avoid network or power interruption to brick the device.
- For old 1.0.1.xx and 1.0.2.xx firmware, all the unzipped binary files are required for successful upgrade. Please allow at least **30 minutes** in local upgrade process before log in back to check the status and reboot the device.
- **Factory Reset** is recommended after upgrading from previous lower lever firmware. Please backup data before performing factory reset and then restore back the data.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal behavior, or having missed web UI configuration parameters or settings, factory reset is MANDATORY.

Please backup the configuration file and database file of RFID cards before factory reset, and import them back after factory reset.

This firmware would not be able to downgrade to previous version 1.0.9.X or below for HW2.0A and HW2.1A, except for HW1.7A or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW2.1A	YES	Initial FW, not able to downgrade
GDS3710 HW2.0A	YES	Initial FW, not able to downgrade
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Updated non-scheduled access alarm event log.

BUG FIX

- Fixed streaming request causes SIP lost registration.
- Fixed wrong time display for Israel.
- ITSP - Fixed under Special Mode (Telefonica) the Proxy SVR1 not response to Invite the device will not immediately send request to Proxy SVR2.
- Fixed soft phone the video will take 3 ~ 5 seconds to be displayed.
- Fixed if alarm number set to mixed SIP number and IP address, the alarm output is abnormal and device key panel light will be on steadily.
- Fixed when stream 1 set to 1080p, the frame rate is inaccurate for all streams.
- Fixed some SIP servers (e.g.: WebEx) cannot be saved from webUI.
- Fixed remote open door will fail randomly if set SIP transport mode to TLS/TCP.
- Fixed device as callee will not do stream negotiation during handshaking.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.

UPDATED P-VALUE

P12312	Video_Audio_Settings.Stream_1.I-frame_Interval (New default value: 60)
P12712	Video_Audio_Settings.Stream_2.I-frame_Interval (New default value: 50)
P13112	Video_Audio_Settings.Stream_3.I-frame_Interval (New default value: 60)
P14003	Video_Audio_Settings.Audio_Settings.System_Volume (New default value: Lever 4)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sips
- SET:[http|https]://<servername>/goform/config?cmd=set&P2329=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2429=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2529=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2629=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P288=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P489=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P589=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P689=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

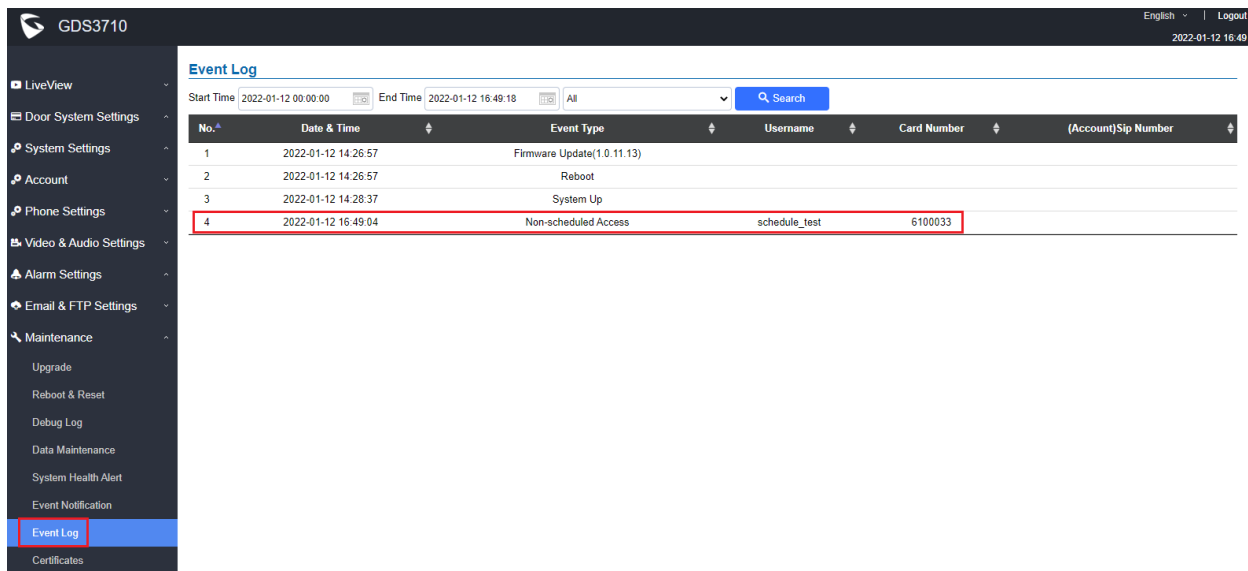
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

LOG NON-SCHEDULED ACCESS ALARM IN EVENT LOG

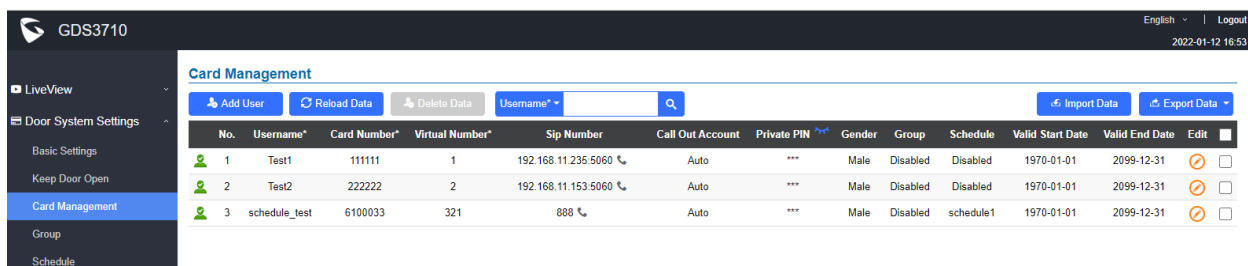
- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Log:




No.	Date & Time	Event Type	Username	Card Number	(Account)Sip Number
1	2022-01-12 14:26:57	Firmware Update(1.0.11.13)			
2	2022-01-12 14:26:57	Reboot			
3	2022-01-12 14:28:37	System Up			
4	2022-01-12 16:49:04	Non-scheduled Access	schedule_test	6100033	

For this feature to work properly, customers also need to pre-configure the “Schedule” and “Card Management” under “Door System Settings” correctly:



No.	Username	Card Number	Virtual Number	Sip Number	Call Out Account	Private PIN	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	Test1	111111	1	192.168.11.235:5060	Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	<input checked="" type="checkbox"/>
2	Test2	222222	2	192.168.11.153:5060	Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	<input checked="" type="checkbox"/>
3	schedule_test	6100033	321	888	Auto	***	Male	Disabled	schedule1	1970-01-01	2099-12-31	<input checked="" type="checkbox"/>


GDS3710

English | Logout
2022-01-12 16:57

LiveView

Door System Settings

Basic Settings

Keep Door Open

Card Management

Group

Schedule

Holiday

System Settings

Account

Phone Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status

← Modify Card Info

Previous Record
3
Next Record

Username*
 Private PIN
 Gender
 ID Number
 Card Number*
 Valid Start Date
 Valid End Date
 Virtual Number*
 Sip Number
 Call Out Account
 Cellphone
 Group

Schedule

 Enable

Male ▼

Auto ▼

Disabled ▼

schedule1 ▼

☒

Note: Private PIN Open Door will not work if "Private PIN" is blank.

Save
Back

GDS3710

English

Logout

2022-01-12 16:57

LiveView

Door System Settings

Basic Settings

Keep Door Open

Card Management

Group

Schedule

Holiday

System Settings

Account

Phone Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status

No.

Schedule Name

Holiday Name

Detail

Edit

1

schedule1

Disabled

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

0

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Holiday

2

schedule2

Disabled

3

schedule3

Disabled

4

schedule4

Disabled

5

schedule5

Disabled

6

schedule6

Disabled

7

schedule7

Disabled

8

schedule8

Disabled

9

schedule9

Disabled

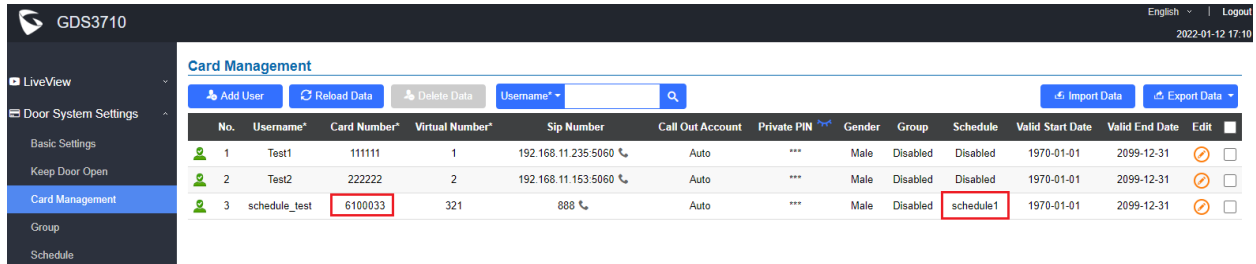
10

schedule10

Disabled

- **Functionality**

This feature enhancement is implemented based on feedback from field. Customers enabled RFID card access based on schedule need the system to log the access attempt out of the pre-programmed schedule to ensure better security and management.



No.	Username	Card Number	Virtual Number	Sip Number	Call Out Account	Private PIN	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	Test1	111111	1	192.168.11.235:5060	Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>
2	Test2	222222	2	192.168.11.153:5060	Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>
3	schedule_test	6100033	321	888	Auto	***	Male	Disabled	schedule1	1970-01-01	2099-12-31	<input type="checkbox"/>

In this example with above screenshot, RFID card number “6100033” is a legal user, but pre-programmed to be allowed to get into building except Wednesday and Thursday, Therefore if this card is swiped at unauthorized day, the RFID card will be rejected to open door and alarm will be logged and reported for HR or Management.

This application scene is very useful for healthcare industry, like hospital, clinic, senior home, etc., or other industry customers who have similar requirement.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.9.9

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

09/28/2021

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal or missed configuration settings in the web UI, factory reset is MANDATORY. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Cisco WebEx IOT: Added WebUI option “SIP URI scheme When using TLS”
- Cisco WebEx IOT: fAdded WebUI option “Support SIP Instance ID”
- Increased OSD text length to 32
- Added tips for OpenVPN Port.

BUG FIX

- Fixed some SIP servers with long domain name cannot be saved
- Fixed device abnormal when connecting to NVR via ONVIF for the 1st time after factory reset
- Fixed no prompt when configure local SIP port less than 80
- Fixed prompt box not obvious when the ACS connection request port is wrong
- Fixed some parameter values delivered from GDMS not applied to the device
- Fixed multi-channel call mode switching between two video calls would end up with audio calls
- Fixed distorted image when turning on LDC (Lens Distortion Correction) under CMOS setting

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P2329	Account.Account_1.SIP_URI_Scheme_When_Using_TLS (Value: 0/1; 0: sip 1: sips)
P2429	Account.Account_2.SIP_URI_Scheme_When_Using_TLS (Value: 0/1; 0: sip 1: sips)
P2529	Account.Account_3.SIP_URI_Scheme_When_Using_TLS (Value: 0/1; 0: sip 1: sips)
P2629	Account.Account_4.SIP_URI_Scheme_When_Using_TLS (Value: 0/1; 0: sip 1: sips)
P288	Account.Account_1.Support_SIP_Instance_ID (Value: 0/1; 0:Disable 1:Enable)
P489	Account.Account_2.Support_SIP_Instance_ID (Value: 0/1; 0:Disable 1:Enable)
P589	Account.Account_3.Support_SIP_Instance_ID (Value: 0/1; 0:Disable 1:Enable)
P689	Account.Account_4.Support_SIP_Instance_ID (Value: 0/1; 0:Disable 1:Enable)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sips
- SET:[http|https]://<servername>/goform/config?cmd=set&P2329=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2429=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2529=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2629=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P288=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P489=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P589=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P689=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

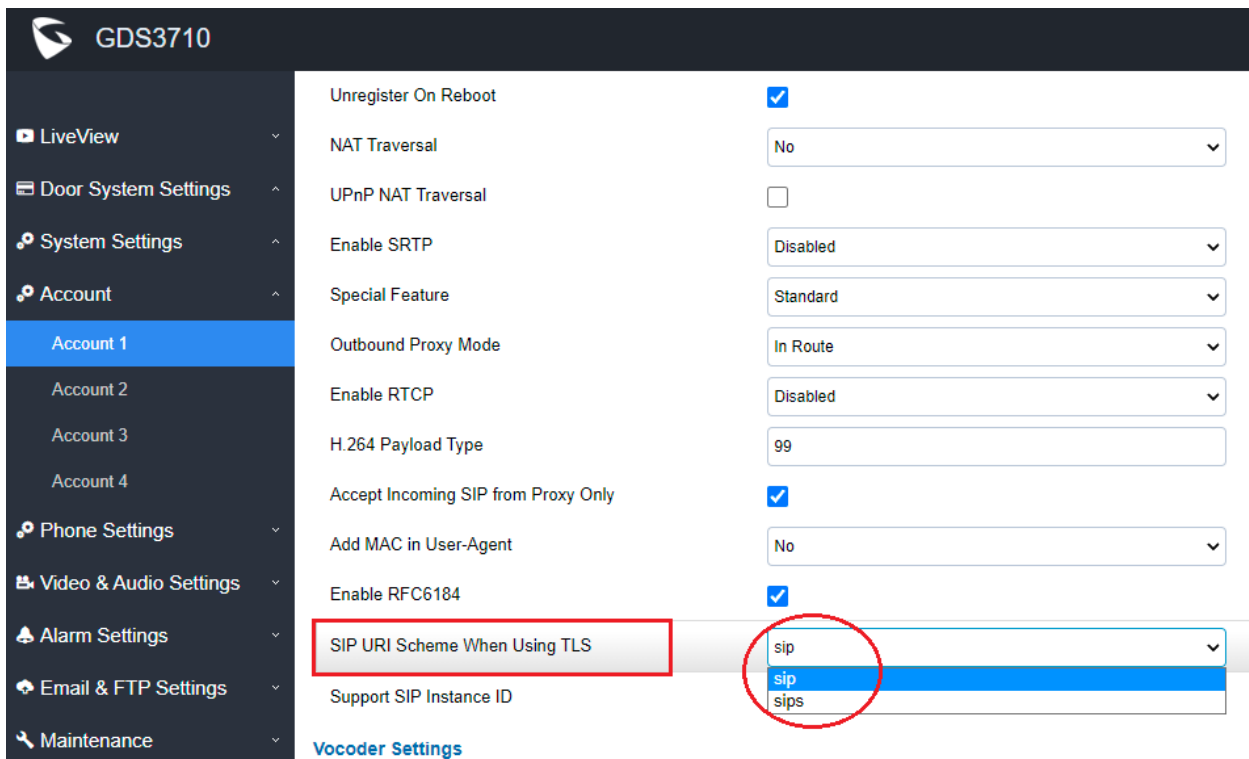
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

CISCO WEBEX IOT: SIP URI SCHEME WHEN USING TLS

- Web Configuration**

This option can be found under device web UI → Account → Account X:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Account 1 (selected), Account 2, Account 3, Account 4, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, and Maintenance. The main content area displays various settings for the selected account. The 'SIP URI Scheme When Using TLS' setting is highlighted with a red box. Its value is set to 'sip', which is also circled in red. Other settings include 'Unregister On Reboot' (checked), 'NAT Traversal' (No), 'UPnP NAT Traversal' (unchecked), 'Enable SRTP' (Disabled), 'Special Feature' (Standard), 'Outbound Proxy Mode' (In Route), 'Enable RTCP' (Disabled), 'H.264 Payload Type' (99), 'Accept Incoming SIP from Proxy Only' (checked), 'Add MAC in User-Agent' (No), and 'Enable RFC6184' (checked). A 'Vocoder Settings' link is visible at the bottom.

Setting	Value
Unregister On Reboot	<input checked="" type="checkbox"/>
NAT Traversal	No
UPnP NAT Traversal	<input type="checkbox"/>
Enable SRTP	Disabled
Special Feature	Standard
Outbound Proxy Mode	In Route
Enable RTCP	Disabled
H.264 Payload Type	99
Accept Incoming SIP from Proxy Only	<input checked="" type="checkbox"/>
Add MAC in User-Agent	No
Enable RFC6184	<input checked="" type="checkbox"/>
SIP URI Scheme When Using TLS	sip
Support SIP Instance ID	

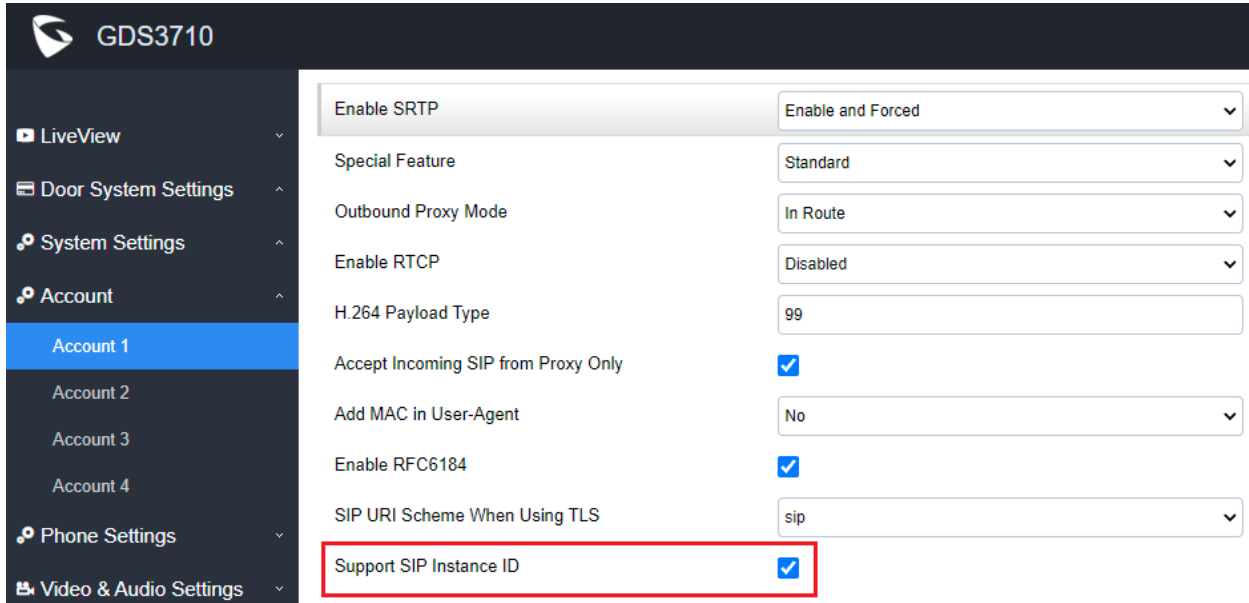
- Functionality**

This feature enhancement is implemented based on IOT with Cisco WebEx service. With correct configuration, the GDS3710 will work with Cisco WebEX server as SIP client.

CISCO WEBEX IOT: SIP INSTANCE ID

- Web Configuration**

This option can be found under device web UI → Account → Account X:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Account 1 (selected), Account 2, Account 3, Account 4, Phone Settings, and Video & Audio Settings. The main content area displays various settings for the selected account. The 'Support SIP Instance ID' option is highlighted with a red box and is checked.

Setting	Value
Enable SRTP	Enable and Forced
Special Feature	Standard
Outbound Proxy Mode	In Route
Enable RTCP	Disabled
H.264 Payload Type	99
Accept Incoming SIP from Proxy Only	<input checked="" type="checkbox"/>
Add MAC in User-Agent	No
Enable RFC6184	<input checked="" type="checkbox"/>
SIP URI Scheme When Using TLS	sip
Support SIP Instance ID	<input checked="" type="checkbox"/>

- Functionality**

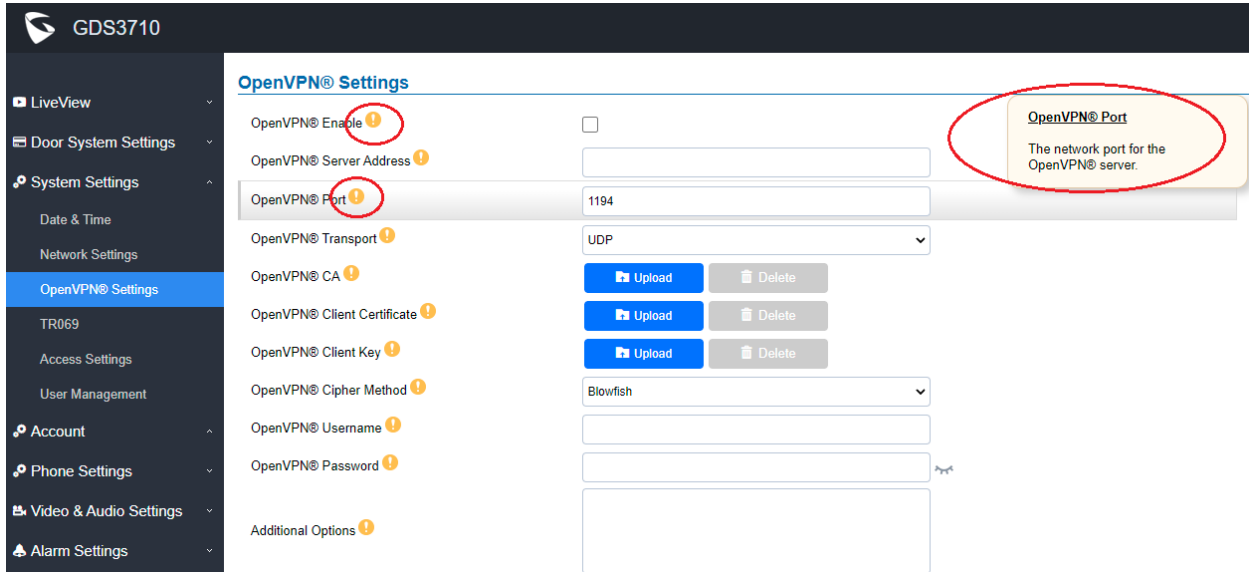
This feature enhancement is implemented based on IOT with Cisco WebEx service.

When checked and enabled, the GDS3710 will work with Cisco WebEX server as SIP client.

ADDED TIPS FOR OPENVPN PORT

- **Web Configuration**

This option can be found under device web UI → System Settings → OpenVPN Settings:



GDS3710

OpenVPN® Settings

OpenVPN® Enable ⓘ ☐

OpenVPN® Server Address ⓘ

OpenVPN® Port ⓘ

OpenVPN® Transport ⓘ

OpenVPN® CA ⓘ

OpenVPN® Client Certificate ⓘ

OpenVPN® Client Key ⓘ

OpenVPN® Cipher Method ⓘ

OpenVPN® Username ⓘ

OpenVPN® Password ⓘ

Additional Options ⓘ

OpenVPN® Port
The network port for the OpenVPN® server.

- **Functionality**

This feature enhancement is implemented based on feedbacks from customers.

Added tips in the webUI will help users to configure OpenVPN correctly and avoid wrong configuration.

This user friendly improvement will help to increase the usability of OpenVPN.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.9.6

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

08/10/2021

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal or missed configuration settings in the web UI, factory reset is MANDATORY. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Added GDMS Support.
- Added HW V1.8A Support.
- TR069 enabled by default.
- Allow using "PIN#" format for Unified PIN when "Disable Keypad SIP Number Dialing" is enabled.
- Added support to automatically log in webUI from server interface (3CX feature).
- Added support for Secondary SIP Server.

BUG FIX

- Fixed some parameter values delivered from GDMS not applied by the device.
- Fixed as callee will not do stream negotiation.
- Fixed Wave audio call established trying turn on video the screen is black.
- Fixed device registered to secondary SIP server the GSC3570 one button open door would fail.
- Fixed doorbell blue light will not turn on if set 00:00–00:00 at the very first time.
- Fixed enabled LLDP the QoS related value cannot be configured.
- Fixed displaying not in Chinese when log in page selected Chinese
- Fixed special characters "&" in the edit name will cause the interface abnormal.
- Fixed import the exported data causing no sound when pressing button and talking.
- Fixed no default value for HTTP Event Notification.
- Fixed GDMS configuration template issue.
- Fixed alert email not send to updated email address when Door Opened or Doorbell Pressed.
- Fixed video not disconnected after changing password in GDSManager.
- Fixed no model and manufacture information in the UPnP Search.
- Fixed enable Privacy Masks then adjust audio and video parameters will trigger MD alarm.
- Fixed select G.722 as vocoder then the call would have no video displayed.
- Fixed modifying the 10th holiday name and time period cannot be saved.
- Fixed only 29 groups can be saved if group name using maximum 64 characters.
- Fixed 3CX provision SIP Notify Event Header "check-sync-reboot=false" still cause reboot.
- Fixed device randomly stops sending video.
- Fixed distorted audio in auxiliary equipment when using G.722 vocoder.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P2327	Account.Account_1.Enable_RFC6184 (Value: 0/1; 0: Disable 1: Enable)
P2427	Account.Account_2.Enable_RFC6184 (Value: 0/1; 0: Disable 1: Enable)
P2527	Account.Account_3.Enable_RFC6184 (Value: 0/1; 0: Disable 1: Enable)
P2627	Account.Account_4.Enable_RFC6184 (Value: 0/1; 0: Disable 1: Enable)
P2312	Account.Account_1.Secondary_SIP_Server (Value: String; Max. Length = 255)
P2412	Account.Account_2.Secondary_SIP_Server (Value: String; Max. Length = 255)
P2512	Account.Account_3.Secondary_SIP_Server (Value: String; Max. Length = 255)
P2612	Account.Account_4.Secondary_SIP_Server (Value: String; Max. Length = 255)
P1409	System_Settings.TR069.Enable_TR-069 (Value: 0/1; 0: Disable 1: Enable)
P4503	System_Settings.TR069.ACS_URL (Value: String; Max. Length = 1024)
P4504	System_Settings.TR069.ACS_User_Name (Value: String; Max. Length = 512)
P4505	System_Settings.TR069.ACS_Password (Value: String; Max. Length = 512)
P4506	System_Settings.TR069.Periodic_Inform_Enable (Value: 0/1; 0: Disable 1: Enable)
P4507	System_Settings.TR069.Periodic_Inform_Interval (Value: integer; Range: 1 ~ 4294967295)
P4511	System_Settings.TR069.Connection_Request_User_Name (Value: String; Max. Length = 256)
P4512	System_Settings.TR069.Connection_Request_User_Password (Value: String; Max. Length = 256)
P4518	System_Settings.TR069.Connection_Request_Port (Value: integer; Range: 0 ~ 65535)
P8220	System_Settings.TR069.CPE_Cert_File (Value: String; Max. Length = 8192)
P8221	System_Settings.TR069.CPE_Cert_Key (Value: String; Max. Length = 8192)

DIRECT LOGIN HTTP API:

- <http|https>://username:password@<servername>/direct-login

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P2327=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2427=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2527=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2627=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P2312=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2412=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2512=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P2612=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=tr069
- SET:[http|https]://<servername>/goform/config?cmd=set&P1409=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4503=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4504=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4505=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4506=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4507=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4511=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4512=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P4518=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P8220=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P8221=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

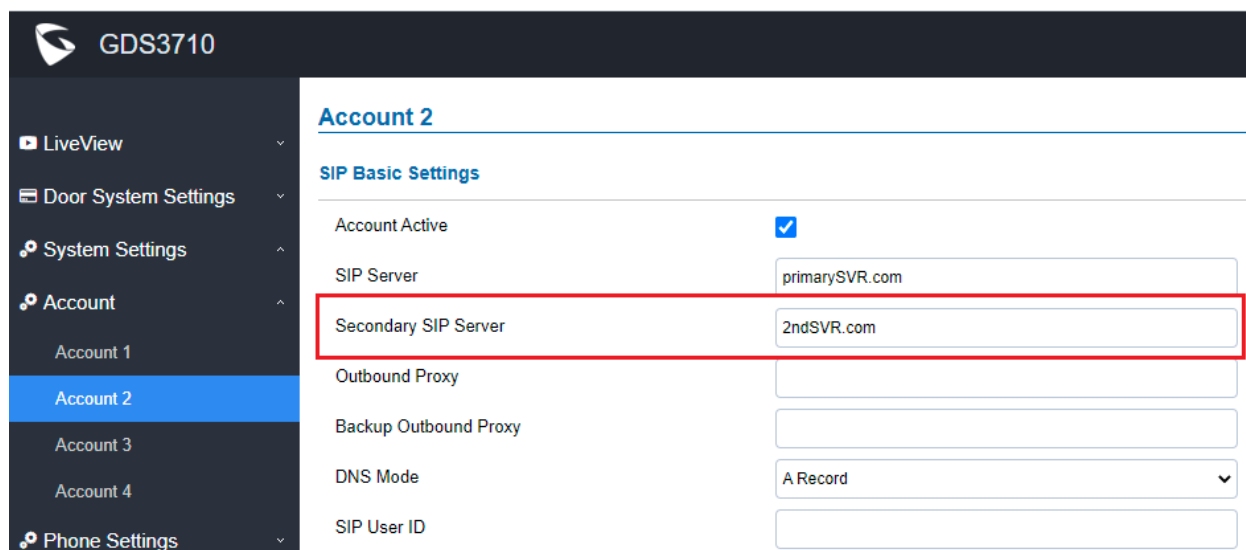
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

SECONDARY SIP SERVER SUPPORT

- **Web Configuration**

This option can be found under device web UI → Account → Account X:



The screenshot shows the web configuration interface for a Grandstream GDS3710 device. The left sidebar contains navigation options: LiveView, Door System Settings, System Settings, Account (selected), Account 1, Account 2 (highlighted), Account 3, Account 4, and Phone Settings. The main content area displays the 'Account 2' settings under 'SIP Basic Settings'. The 'Account Active' checkbox is checked. The 'SIP Server' field contains 'primarySVR.com'. The 'Secondary SIP Server' field, which is highlighted with a red box, contains '2ndSVR.com'. Other fields include 'Outbound Proxy', 'Backup Outbound Proxy', 'DNS Mode' (set to 'A Record'), and 'SIP User ID'.

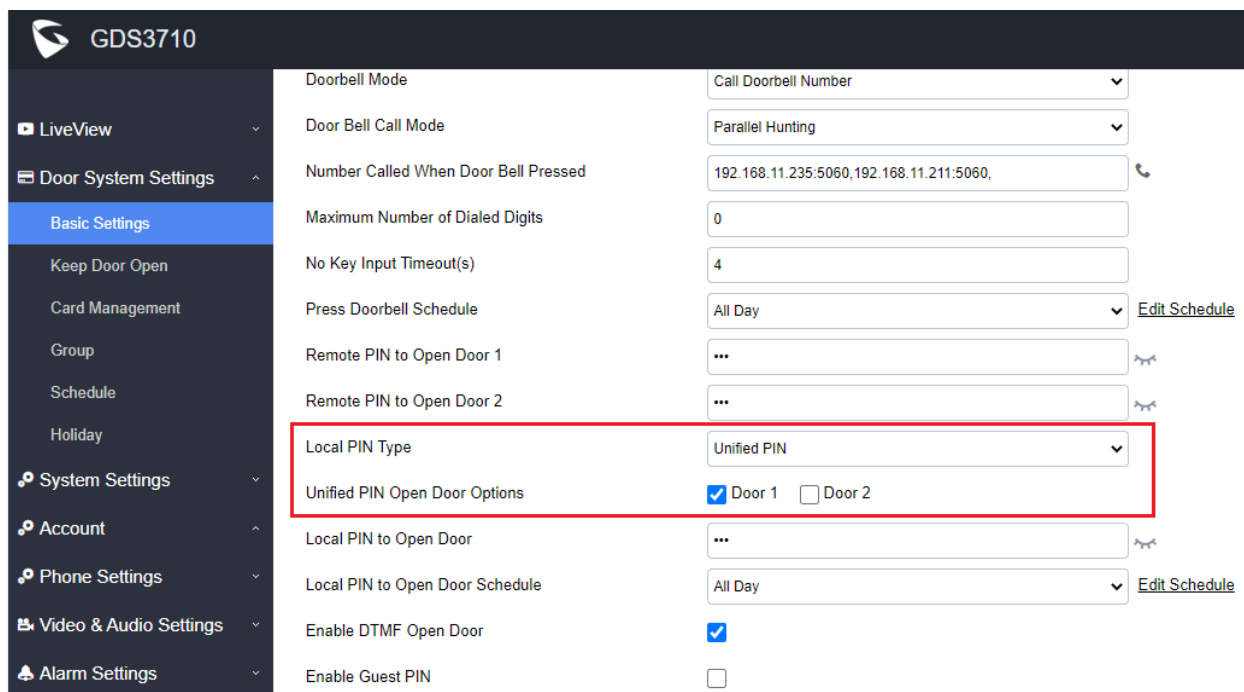
- **Functionality**

This feature enhancement is implemented based on request from field by customers. The “Second SIP Server” allows customers with such network environment to use secondary SIP server if primary SIP server having problems to ensure service availability.

UNIFIED "PIN#" for ALL WHEN ENABLE "DISABLE KEYPAD SIP NUMBER DIALING"

- **Web Configuration**

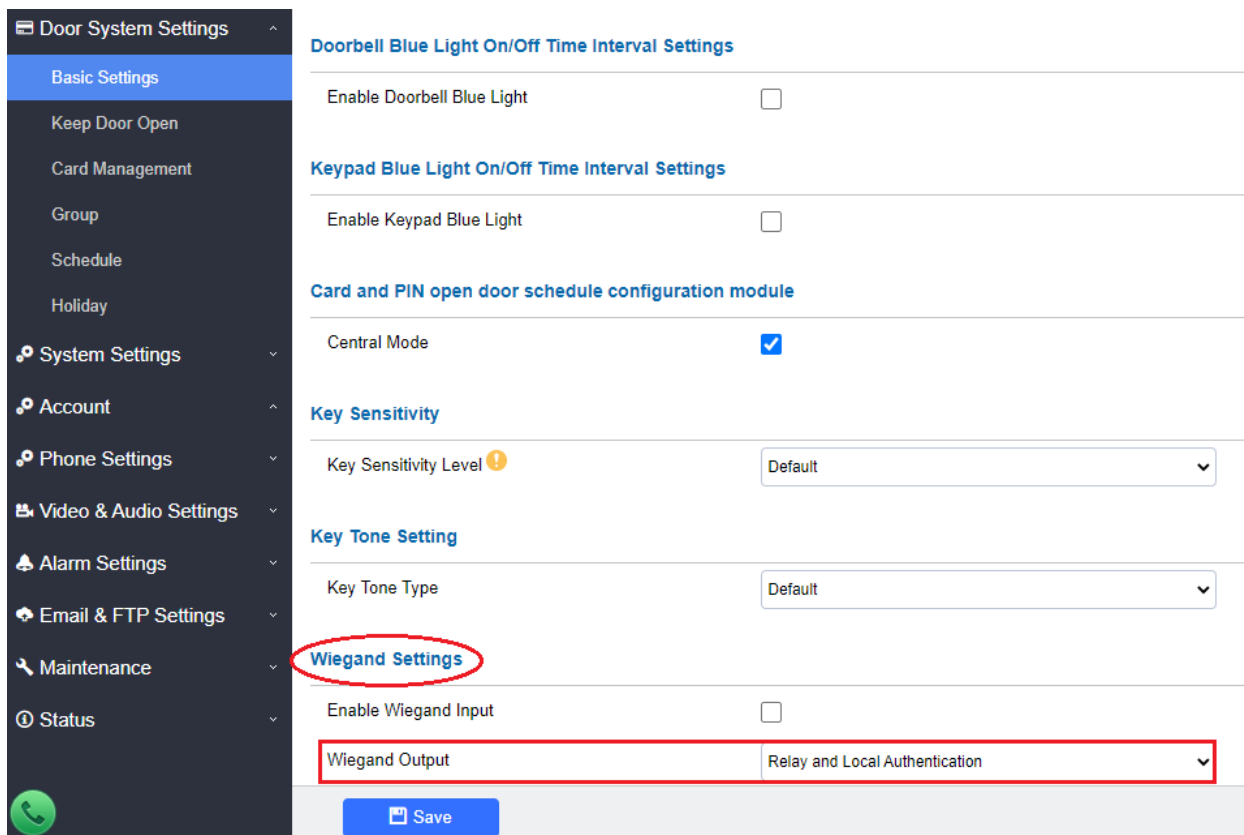
This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
- System Settings
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings

Doorbell Mode	Call Doorbell Number
Door Bell Call Mode	Parallel Hunting
Number Called When Door Bell Pressed	192.168.11.235:5060, 192.168.11.211:5060,
Maximum Number of Dialed Digits	0
No Key Input Timeout(s)	4
Press Doorbell Schedule	All Day Edit Schedule
Remote PIN to Open Door 1	...
Remote PIN to Open Door 2	...
Local PIN Type	Unified PIN
Unified PIN Open Door Options	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2
Local PIN to Open Door	...
Local PIN to Open Door Schedule	All Day Edit Schedule
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>



Door System Settings

- Basic Settings**
- Keep Door Open
- Card Management
- Group
- Schedule
- Holiday
- System Settings
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status

Doorbell Blue Light On/Off Time Interval Settings

Enable Doorbell Blue Light ☐


Keypad Blue Light On/Off Time Interval Settings

Enable Keypad Blue Light ☐

Card and PIN open door schedule configuration module

Central Mode ☒

Key Sensitivity

Key Sensitivity Level  Default

Key Tone Setting

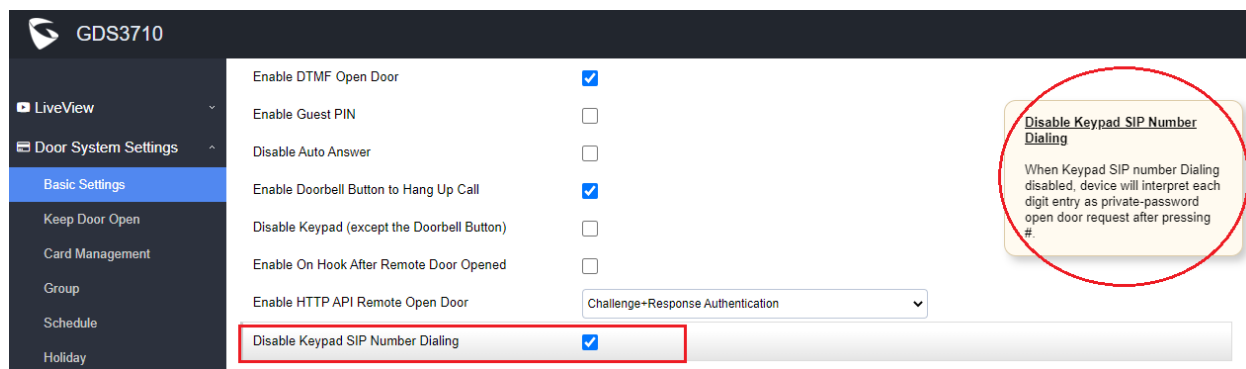
Key Tone Type Default

Wiegand Settings

Enable Wiegand Input ☐

Wiegand Output Relay and Local Authentication

[Save](#)



- 1) First in the “Local PIN Type” to choose “Unified PIN” as open door method and which door.
- 2) Fill in the PIN in the “Local PIN to Open Door” field.
- 3) Select and edit the “Local PIN to Open Door Schedule” to specify the open door schedule.
- 4) Select “Disable Keypad SIP Number Dialing” to tell system that all input should be treated as PIN input and NOT SIP number to call (only Doorbell button can make pre-programmed SIP call when this feature enabled).
- 5) If “Wiegand Output” enabled and 3rd party Wiegand input device connected to GDS3710, select “Relay and Bypass” or “Relay and Local Authentication” depending on how the 3rd party Wiegand device handling the data. Here the example is “Relay and Bypass” selected.

• **Functionality**

This feature enhancement is implemented based on request from field by customers.

When “Disable Keypad SIP Number Dialing” enabled, the GDS3710 will simply function like traditional door access device, only input PIN following by # to decide whether door open or not.

When wired 3rd party Wiegand device as output to control door, now input the same “PIN#” from the connected 3rd party Wiegand device will also open door.

This feature is not implemented before firmware 1.0.9.6

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.26

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

07/20/2021

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal or missed configuration settings in the web UI, factory reset is MANDATORY. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Added support for HW1.8A
- Added support for Basic Authentication of HTTP API Remote Open Door

BUG FIX

- Fixed incorrect prompt when enable HTTP API Remote Open Door
- Fixed 10th Holiday Schedule cannot be saved in Door System Settings

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

UPDATED P-VALUE

P15424	Enable HTTP API Remote Open Door (0:Disable 1:Challenge+Response Authentication 2: Basic Authentication)
--------	---

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

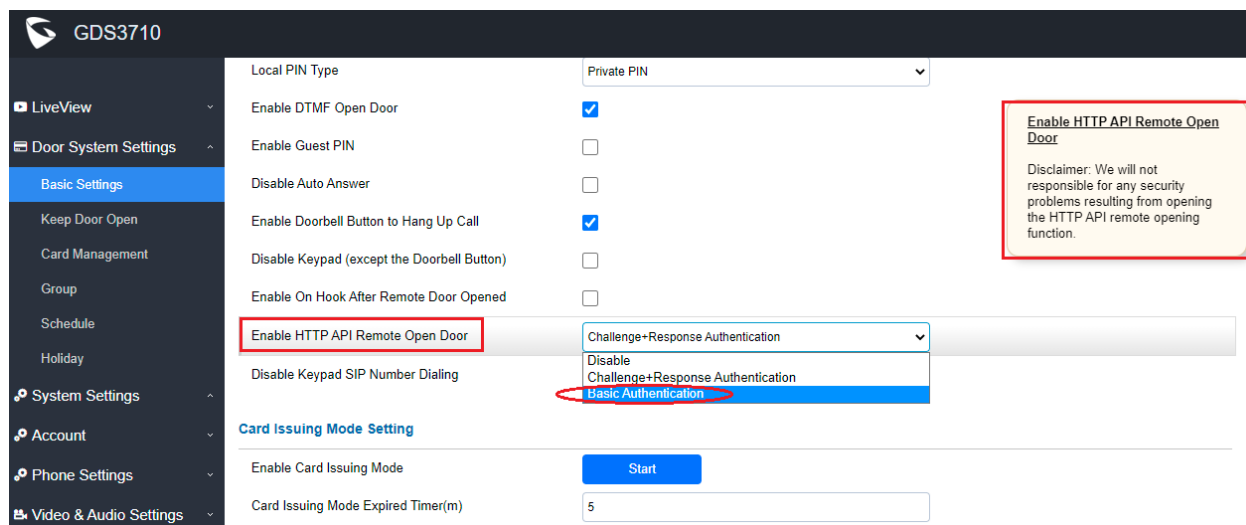
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

BASIC AUTHENTICATION OF HTTP API REMOTE OPEN DOOR

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Local PIN Type: Private PIN

Enable DTMF Open Door: ☒

Enable Guest PIN: ☐

Disable Auto Answer: ☐

Enable Doorbell Button to Hang Up Call: ☒

Disable Keypad (except the Doorbell Button): ☐

Enable On Hook After Remote Door Opened: ☐

Enable HTTP API Remote Open Door: Challenge+Response Authentication

Disable Keypad SIP Number Dialing: Disable

Card Issuing Mode Setting

Enable Card Issuing Mode: Start

Card Issuing Mode Expired Timer(m): 5

Enable HTTP API Remote Open Door

Disclaimer: We will not be responsible for any security problems resulting from opening the HTTP API remote opening function.

- **Functionality**

This feature enhancement is implemented based on request from field by customers. The “Basic Authentication” gives the convenience for 3rd party system integration and 2nd stage application development, with the risk of security.

NOTES:

- Grandstream will not be responsible for any issue resulting from using HTTP API Remote Open Door. Users should take full responsibility for the (network) system security by using this feature.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.24

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

05/6/2021

SUMMARY OF UPDATE

The main purpose of this release is for 3CX compatibility, bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal or missed configuration settings in the web UI, factory reset is MANDATORY. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- [3CX IoT]: Added MAC in User-Agent configuration.
- Added unauthorized card swiped on wired external Wiegand reader will also have alert message in event Log
- Added prompt to prevent when alarm action profile name is empty.
- Added more template variables in Event Notification.
- Improved private PIN management at Card Management Web UI.
- Added option to choose HTTP method to either POST or GET in Event Notification.

BUG FIX

- [3CX IoT]: Fixed not negotiating codec in configured order as callee.
- [3CX IoT]: Fixed audio distortion when answering IVR via SRTP.
- [3CX IoT]: Fixed provision with SIP NOTIFY event header “check-sync: reboot=false” cause reboot.
- [3CX IoT]: Fixed continuous ringing after Yealink T58V answered.
- Fixed editing alarm area via Firefox browser the previously configured area will be overlapped.
- Fixed private PIN cannot open door if the card information is added via HTTP API.
- Fixed switching streams at Live View in Firefox video will not play.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P26061	Account.Account_1.Add_MAC_in_User-Agent (Value: 0/1/2; 0: No 1: Yes except REGISTER 2: Yes to all SIP)
P26161	Account.Account_2.Add_MAC_in_User-Agent (Value: 0/1/2; 0: No 1: Yes except REGISTER 2: Yes to all SIP)
P26261	Account.Account_3.Add_MAC_in_User-Agent (Value: 0/1/2; 0: No 1: Yes except REGISTER 2: Yes to all SIP)
P26361	Account.Account_4.Add_MAC_in_User-Agent (Value: 0/1/2; 0: No 1: Yes except REGISTER 2: Yes to all SIP)
P29061	Account.Account_1.Codec_Negotiation_Priority (Value: 0/1; 0: Caller 1: Callee)
P29161	Account.Account_2.Codec_Negotiation_Priority (Value: 0/1; 0: Caller 1: Callee)
P29261	Account.Account_3.Codec_Negotiation_Priority (Value: 0/1; 0: Caller 1: Callee)
P29361	Account.Account_4.Codec_Negotiation_Priority (Value: 0/1; 0: Caller 1: Callee)
P15553	Maintenance.Event_Notification.HTTP_Method (Value: 0/1 0:POST 1:GET)

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P26061=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P26161=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P26261=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P26361=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P29061=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P29161=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P29261=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P29361=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=eventlog
- SET:[http|https]://<servername>/goform/config?cmd=set&P15553=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

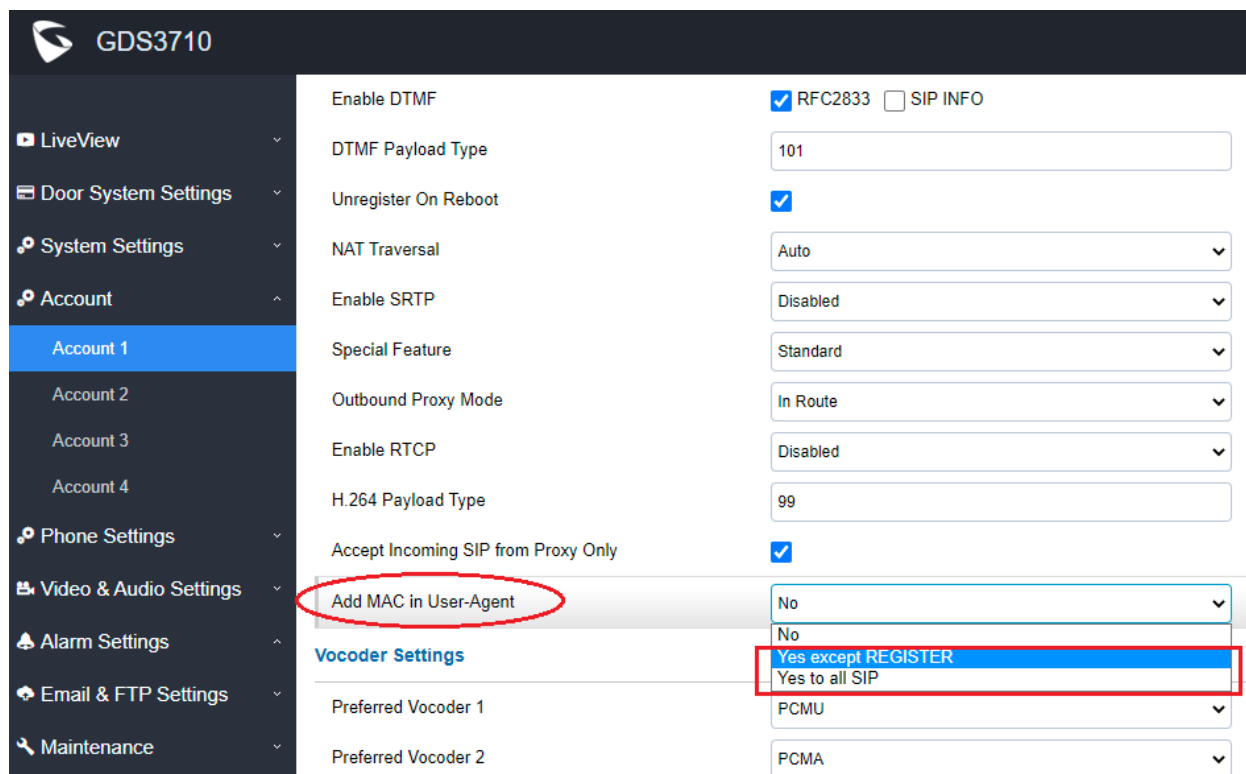
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

ADD MAC IN USER-AGENT

- **Web Configuration**

This option can be found under device web UI → Account → Account X → SIP Advanced Settings:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Account 1 (selected), Account 2, Account 3, Account 4, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, and Maintenance. The main content area displays settings for Account 1. Under the 'SIP Advanced Settings' section, the 'Add MAC in User-Agent' option is highlighted with a red circle. The dropdown menu for this option is open, showing three choices: 'No', 'Yes except REGISTER' (highlighted in blue), and 'Yes to all SIP' (highlighted with a red rectangle). Other settings visible include 'Enable DTMF' (checked), 'DTMF Payload Type' (101), 'Unregister On Reboot' (checked), 'NAT Traversal' (Auto), 'Enable SRTP' (Disabled), 'Special Feature' (Standard), 'Outbound Proxy Mode' (In Route), 'Enable RTCP' (Disabled), 'H.264 Payload Type' (99), 'Accept Incoming SIP from Proxy Only' (checked), 'Preferred Vocoder 1' (PCMU), and 'Preferred Vocoder 2' (PCMA).

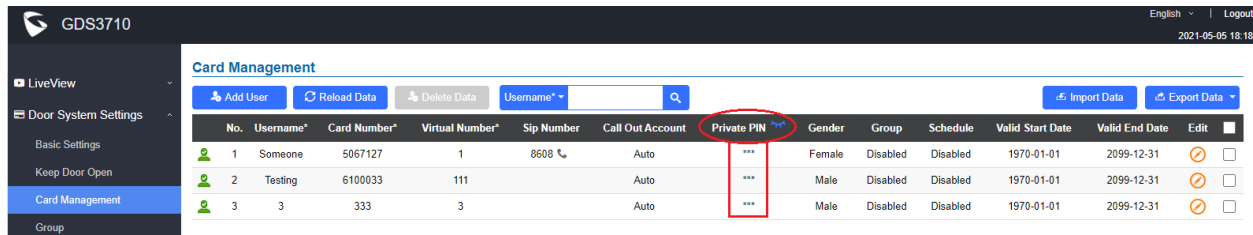
- **Functionality**

This feature enhancement is implemented during IoT with 3CX so that the GDS37xx can be compatible with 3CX auto provisioning, with option to add MAC address into User-Agent at SIP Header.

IMPROVED PIN MANAGEMENT AT CARD MANAGEMENT

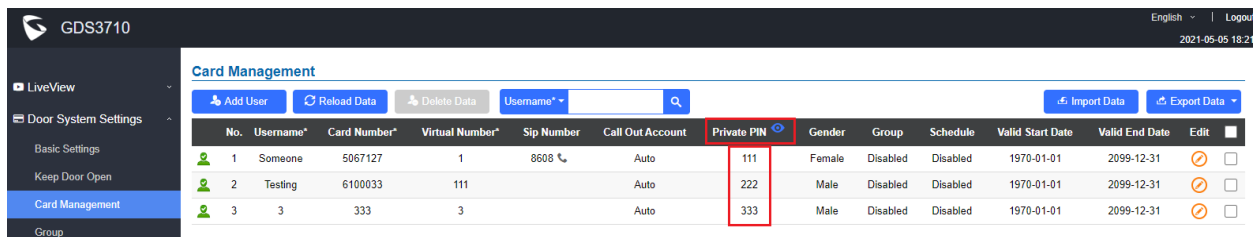
- Web Configuration**

This device web UI improvement can be found at: Door System Settings → Card Management:



The screenshot shows the 'Card Management' page in the GDS3710 web UI. The 'Private PIN' column is currently masked with asterisks (***). A red box highlights the 'Private PIN' header and the masked values in the data rows.

No.	Username*	Card Number*	Virtual Number*	Sip Number	Call Out Account	Private PIN	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	Someone	5067127	1	8608	Auto	***	Female	Disabled	Disabled	1970-01-01	2099-12-31	
2	Testing	6100033	111		Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	
3	3	333	3		Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	



The screenshot shows the 'Card Management' page in the GDS3710 web UI. The 'Private PIN' column is now revealed, showing the actual PIN values (111, 222, 333). A red box highlights the 'Private PIN' header and the revealed values in the data rows.

No.	Username*	Card Number*	Virtual Number*	Sip Number	Call Out Account	Private PIN	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	Someone	5067127	1	8608	Auto	111	Female	Disabled	Disabled	1970-01-01	2099-12-31	
2	Testing	6100033	111		Auto	222	Male	Disabled	Disabled	1970-01-01	2099-12-31	
3	3	333	3		Auto	333	Male	Disabled	Disabled	1970-01-01	2099-12-31	


- Functionality**

This feature enhancement is response to system administrators at field for convenient PIN management. Instead of clicking “Edit” to get into each card to check the private PIN, or export to .CSV file to edit and import, now system administrators can log in to the web UI and enable the displaying of all private PINs in one page for easy check.

By default this feature is disabled for security.

NOTES:

- This feature will not be available unless system administrator enabled “Enable PIN/Password Display (HTTPS)” at the “System Settings → Access Settings” page.
- This feature only works when HTTPS used as web UI access.
- When feature enabled, system click the “eyelid” icon will has all the PINs displayed from “dot” to related numbers, and the “eyelid” will become “eye” in the web UI.
- The related pre-requisite is listed as screenshot below.


GDS3710

▶ LiveView

☰ Door System Settings

⚙️ System Settings

Date & Time

Network Settings

OpenVPN® Settings

Access Settings

User Management

⚙️ Account

⚙️ Phone Settings

📺 Video & Audio Settings

🚨 Alarm Settings

✉️ Email & FTP Settings

🔧 Maintenance

📶 Status

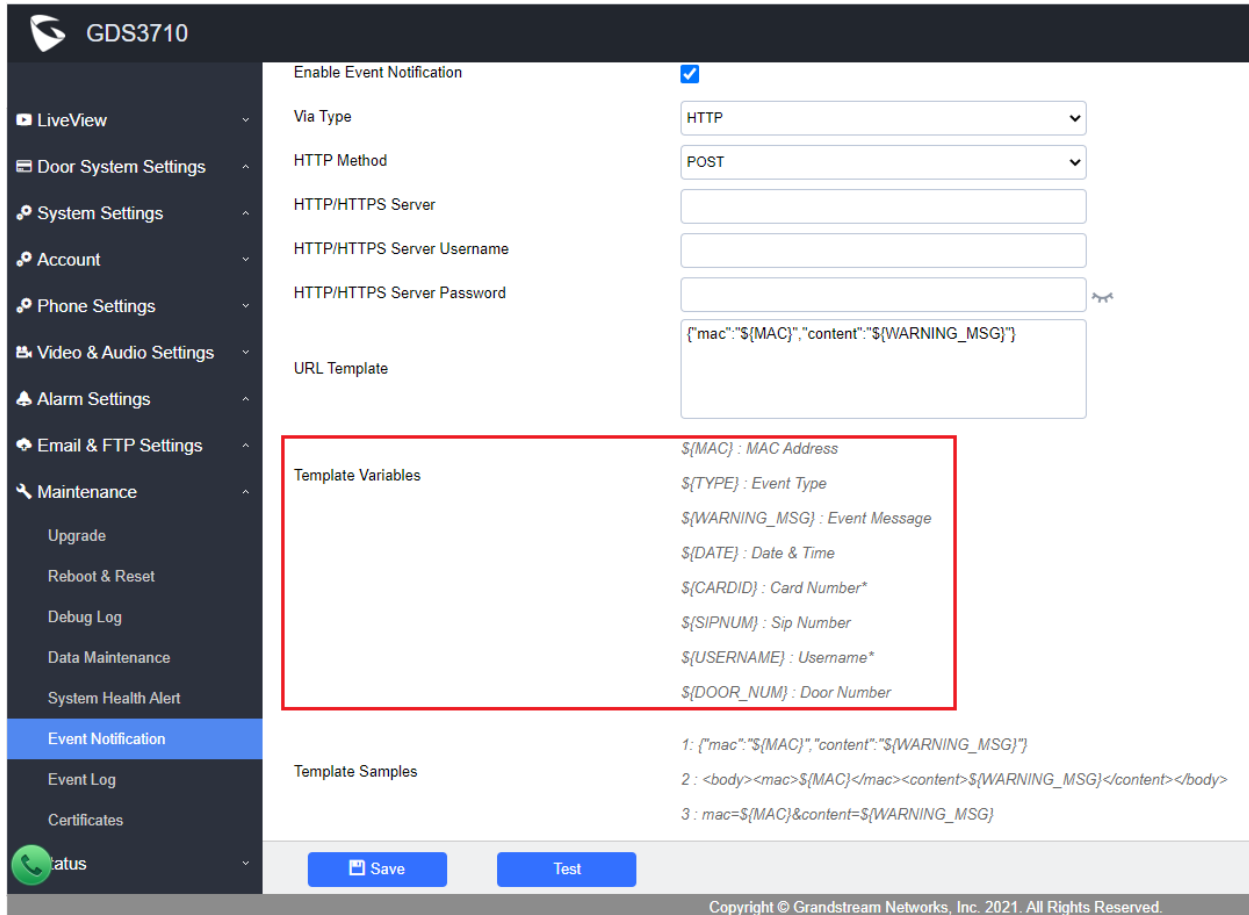
Access Settings

Web Access Mode	HTTPS	
Web Access Port	443	
MJPEG Authentication Mode	Challenge+Response	
RTSP Port	554	
User Login Timeout(min)	5	
Maximum Number of Login Attempts	5	
Locking Time of Login Error (m)	5	
Disable Web Access	<input type="checkbox"/>	
Enable UPnP Discovery	<input checked="" type="checkbox"/>	
Enable Anonymous LiveView	<input type="checkbox"/>	
Enable PIN/Password Display (HTTPS)	<input checked="" type="checkbox"/>	
Enable SSH	<input checked="" type="checkbox"/>	
SSH Port	22	
GDSManager Configuration Password	👁️
RTSP Password	6666	👁️

MORE TEMPLATE VARIABLES IN EVENT NOTIFICATION

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Notification:



The screenshot shows the GDS3710 web configuration interface. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Upgrade, Reboot & Reset, Debug Log, Data Maintenance, System Health Alert, Event Notification (highlighted), Event Log, and Certificates. The main content area is titled 'GDS3710' and shows the 'Event Notification' settings. The 'Enable Event Notification' checkbox is checked. Below it, there are fields for 'Via Type' (HTTP), 'HTTP Method' (POST), 'HTTP/HTTPS Server', 'HTTP/HTTPS Server Username', and 'HTTP/HTTPS Server Password'. The 'URL Template' field contains the text: `{ "mac": "${MAC}", "content": "${WARNING_MSG}" }`. A red box highlights the 'Template Variables' section, which lists the following variables: `${MAC}` : MAC Address, `${TYPE}` : Event Type, `${WARNING_MSG}` : Event Message, `${DATE}` : Date & Time, `${CARDID}` : Card Number*, `${SIPNUM}` : Sip Number, `${USERNAME}` : Username*, and `${DOOR_NUM}` : Door Number. Below this, the 'Template Samples' section shows three examples: 1: `{ "mac": "${MAC}", "content": "${WARNING_MSG}" }`, 2: `<body><mac>${MAC}</mac><content>${WARNING_MSG}</content></body>`, and 3: `mac=${MAC}&content=${WARNING_MSG}`. At the bottom, there are 'Save' and 'Test' buttons. The footer of the interface reads: 'Copyright © Grandstream Networks, Inc. 2021. All Rights Reserved.'

- **Functionality**

This feature enhancement is response to field request from system integrators for 2nd stage application development.

More template variables are added into the Event Notification so that system integrators can use them for related scripts, programs or applications.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.23

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

02/20/2021

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal or missed configuration settings in the web UI, factory reset is MANDATORY. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Added key sensitivity option.
- Added new feature “One-Way Interlocking Mode” to control two doors with one door only open when another door closed by installing additional 3rd party window/door sensors.
- Added pairing with GSC3570 open door without SIP call.
- Added configurable Scheduled Auto Reboot (to keep a healthy system running).
- Added support to allow IP addresses in whitelist to call the GDS37xx and bypass the setting of “Accept Incoming SIP from Proxy Only”
- Increased the amount of whitelist number.
- Added protection schema to prevent device reboot during a call.
- Improved web UI error login prompt message.
- Added Time Zone “GMT-03 (Argentina, Uruguay, Brasilia, San Paulo)”
- Modified tips at Card Management Page.
- Enhanced web UI password display with security and convenience.

BUG FIX

- Fixed wrong password input failed to lock up web UI.
- Fixed single whitelist number cannot be deleted
- Fixed in Data Maintenance Mode, import the exported file will fail with prompt “illegal certificate”.
- Fixed problem to import certificate of Zoom.
- Fixed error display issue when the certificate imported is valid for more than 2038.
- Fixed using Browser to view live video of Stream 1 will automatically switch to Stream 2.
- Fixed remote open door failure but phone’s UI showing successful during Alarm SIP Call.
- Fixed DTMF Open Door failure when Doorbell Call with Parallel Hunting Mode.
- Fixed sometimes device will automatically hang up the call when in SRTP mode.
- Fixed call won’t happen if turn off background light with long “no key input timeout” (e.g.: 7 seconds)
- Fixed failure to open door during preview.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out or unregistered, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P15543	Door_System_Settings.Basic_Settings.One-way_Interlocking_Doors_Mode (Value: 0:Disable 1:Enable)
P15544	Door_System_Settings.Basic_Settings.Key_Sensitivity_Level (Value: 0:Default 1:High)
P15540	Maintenance.Reboot_Reset.Auto_Reboot.Enable (Value: 0:Disable 1:Enable)
P15541	Maintenance.Reboot_Reset.Auto_Reboot.Week (Value: 0:Everyday 1:Sunday 2:Monday 3:Tuesday 4:Wednesday 5:Thursday 6:Friday 7:Saturday)
P15542	Maintenance.Reboot_Reset.Auto_Reboot.Hour_Min (Value: time string. Example: 14:20 ->1420)

UPDATED P-VALUE

P14320	Alarm_Settings.Alarm_Event_Config.Digit_Input_1 Update value range to 0-4
P14325	Alarm_Settings.Alarm_Event_Config.Digit_Input_2 Update value range to 0-4

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15543=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15544=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=reset_reboot
- SET:[http|https]://<servername>/goform/config?cmd=set&P15540=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15541=<value>
- SET:[http|https]://<servername>/goform/config?cmd=set&P15542=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

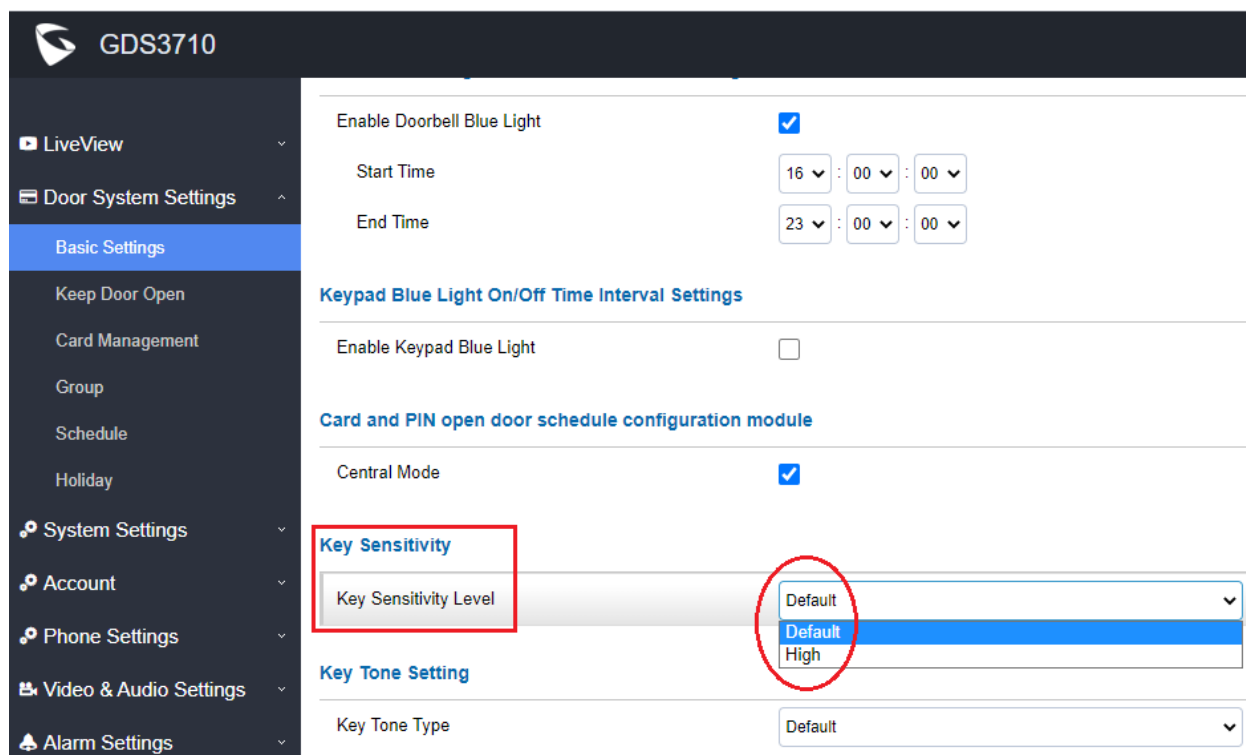
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

KEY SENSITIVITY OPTION

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



The screenshot shows the GDS3710 web configuration interface. On the left is a sidebar menu with options: LiveView, Door System Settings (expanded), Basic Settings (selected), Keep Door Open, Card Management, Group, Schedule, Holiday, System Settings, Account, Phone Settings, Video & Audio Settings, and Alarm Settings. The main content area is titled 'GDS3710' and contains several settings sections:

- Enable Doorbell Blue Light:** A checkbox that is checked.
- Start Time:** A time picker set to 16:00:00.
- End Time:** A time picker set to 23:00:00.
- Keypad Blue Light On/Off Time Interval Settings:** A section header.
- Enable Keypad Blue Light:** A checkbox that is unchecked.
- Card and PIN open door schedule configuration module:** A section header.
- Central Mode:** A checkbox that is checked.
- Key Sensitivity:** A section header with a red box around it.
- Key Sensitivity Level:** A dropdown menu with a red circle around it, showing 'Default' (selected), 'Default', and 'High' options.
- Key Tone Setting:** A section header.
- Key Tone Type:** A dropdown menu set to 'Default'.

- **Functionality**

This feature enhancement is implemented to resolve “ghost call” issue reported by customers located in warm or tropic weather area.

The GDS3710 keypad is capacitor touch panel. Previously only one set sensitivity parameter is used the drawback is when device installed in warm and high humidity area, due to the sensitivity is too high, the wind, rain drops, vibrations etc. will cause the keypad to make unexpected (doorbell) calls by itself (ghost call) and make the device in unstable usage condition.

Now two settings are included: Default and High.

The default setting is using less sensitivity keypad parameters which applied to most usage scenes, especially in warm and high humidity places like tropic regions or places near seaside or riverside where high humidity weather condition exists, especially in Summer.

The previous default in old firmware now is modified as “High” in key sensitivity lever. This set of parameters is designed for application scenes located in high latitude regions normally very cold and user might need to press the keypad with gloves. Due to the sensitivity is high, false positive might happen if such parameter used in different place like low latitude environment.

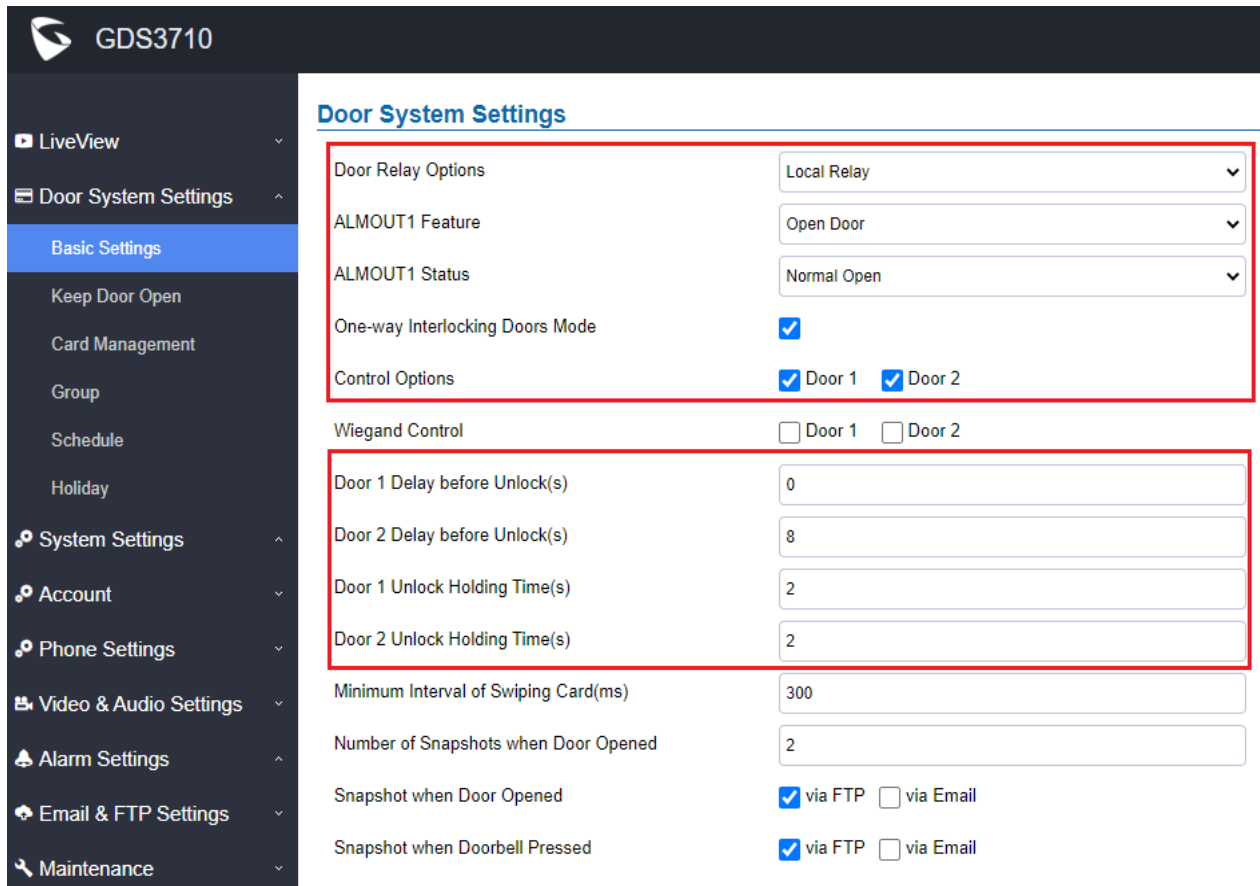
Most application scenes the Default setting of this firmware is good enough for application. Please use Default setting unless the usage scene really needs high keypad lever sensitivity.

If with default or low sensitivity keypad, the false positive ghost call issue still happens frequently, that might indicate an inappropriate wiring or installation, or maybe the hardware faulty. Please contact HELPDESK of Grandstream for assistance to resolve such problem.

ONE-WAY INTERLOCKING MODE

- **Web Configuration**

This option can be found under device web UI → Door System Settings. Below example configuration screenshots are for reference only, customers need to test and get own parameters in field:



GDS3710

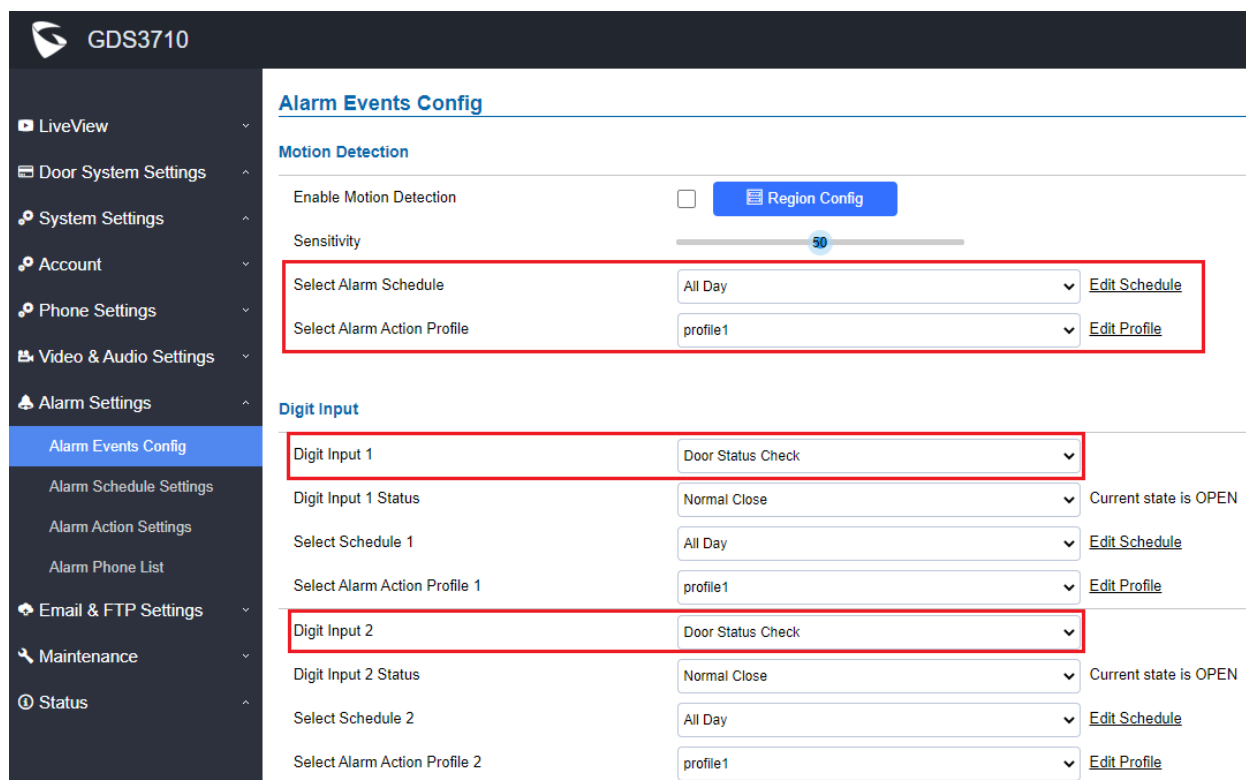
Door System Settings

Door Relay Options	Local Relay
ALMOUT1 Feature	Open Door
ALMOUT1 Status	Normal Open
One-way Interlocking Doors Mode	<input checked="" type="checkbox"/>
Control Options	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Wiegand Control	<input type="checkbox"/> Door 1 <input type="checkbox"/> Door 2
Door 1 Delay before Unlock(s)	0
Door 2 Delay before Unlock(s)	8
Door 1 Unlock Holding Time(s)	2
Door 2 Unlock Holding Time(s)	2
Minimum Interval of Swiping Card(ms)	300
Number of Snapshots when Door Opened	2
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input checked="" type="checkbox"/> via FTP <input type="checkbox"/> via Email

NOTES:

- Door 2 Delay before Unlock(s): Will be the total transit time from Door 1 to Door 2 right after the Door 1 is closed (this time will be "Door 1 unlock holding time"). In above example, the Door1 unlock holding time is 2 seconds, the transit time of hallway is 6 seconds, therefore the Door 2 Delay before Unlock is set to 8 seconds. The transit time and unlock holding time will be decided and adjusted based on actual application scene by the installer or system integrator.
- COM1 (ALMOUT1) only has two sockets for wiring, and NO ONLY. If the connected strike/lock is a NO strike, this means ALMOUT1 Status should be set to "Normal Open" then door will be closed when power is lost.

Digital Input to Check Door Status (Door 1 & Door 2):



GDS3710

Alarm Events Config

Motion Detection

Enable Motion Detection ☐ [Region Config](#)

Sensitivity

Select Alarm Schedule [Edit Schedule](#)

Select Alarm Action Profile [Edit Profile](#)

Digit Input

Digit Input 1

Digit Input 1 Status Current state is OPEN

Select Schedule 1 [Edit Schedule](#)

Select Alarm Action Profile 1 [Edit Profile](#)

Digit Input 2

Digit Input 2 Status Current state is OPEN

Select Schedule 2 [Edit Schedule](#)

Select Alarm Action Profile 2 [Edit Profile](#)

Go to **Alarm Settings** → **Alarm Events Config** → **Digit Input**, configured as follow:

Digit Input 1: Door Status Check. The DI will validate the current status of the Door, whether it is close or open, based on the sensor signal sending to the “Digit input 1”

Digit Input 1 Status: If set to **Normal Open:** Configured door status check will be triggered when Digital Input Status switch from Close to Open, If set to **Normal Close:** Configured door status check will be triggered when Digital Input Status switch from Open to Close. By default, Input Digit 1 Status is “Disabled”.

Digit Input 2: Door Status Check. The DI will validate the current status of the Door, whether it is close or open, based on the sensor signal sending to the “Digit input 2”

Digit Input 2 Status: If set to **Normal Open:** Configured door status check will be triggered when Digital Input Status switch from Close to Open, if set to **Normal Close:** Configured door status check will be triggered when Digital Input Status switch from Open to Close. By default, Input Digit 2 Status is “Disabled”.

NOTES:

- “Alarm Schedule” and “Alarm Action Profile” must be configured and selected otherwise the Digit Input channel will not be activated.
- There are two doors wired with window/door sensor separately, please make sure the door sensor is wired to correct Digit Input channel and refer to below sample wiring diagram for reference.

• Functionality

This feature is implemented based on request from customers in LATAM and EMEA region. It will allow GDS3710 to control two doors in one direction, **with additional 3rd party window/door sensor installed accordingly** (not provided by Grandstream).

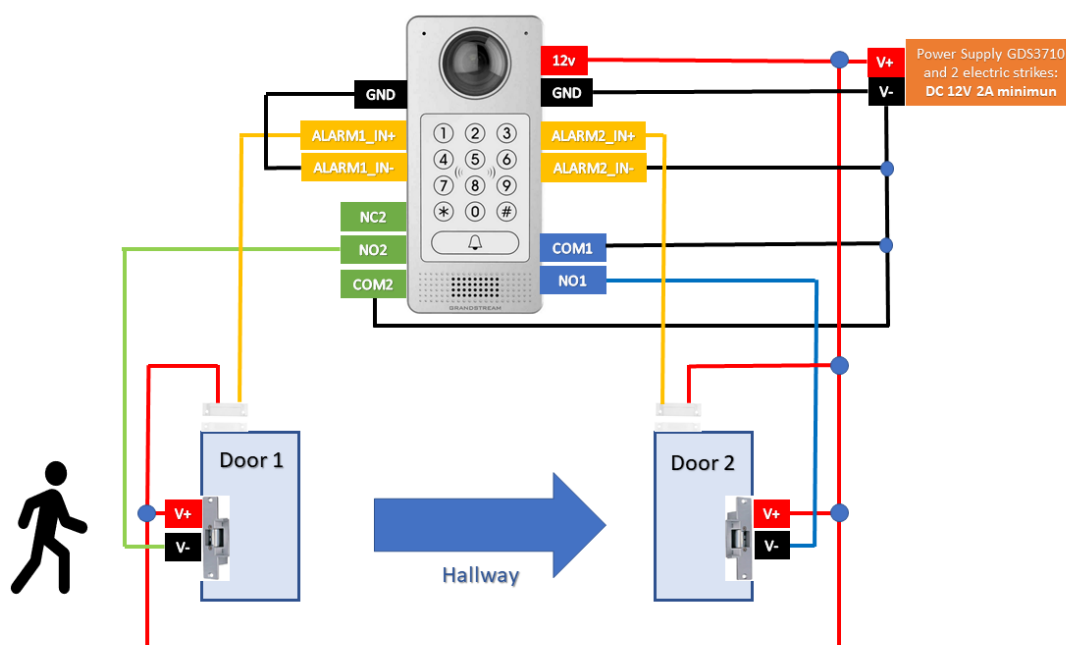
When configured and wired correctly, the two doors will operate under a controlling logic as below:

- 1) Only legal PIN or RFID card can open door when BOTH doors are detected closed.
- 2) When 1st door opened by valid user, the 2nd door is and will remain closed; the 2nd door will automatically open once detected the 1st door closed and programmed timer reached.
- 3) When 2nd door opening, the 1st door will NOT open even a valid PIN/RFID used.
- 4) If entering 1st door and after 1st door closed and 2nd door opened, the person failed to enter 2nd door promptly (after 2nd door opening time out) will be locked in between two doors until next transaction happens or ask help (e.g.: call posted number or press button if there is one) from security staff to open door remotely (via SIP call into GDS3710 or GDSManager, for example) .

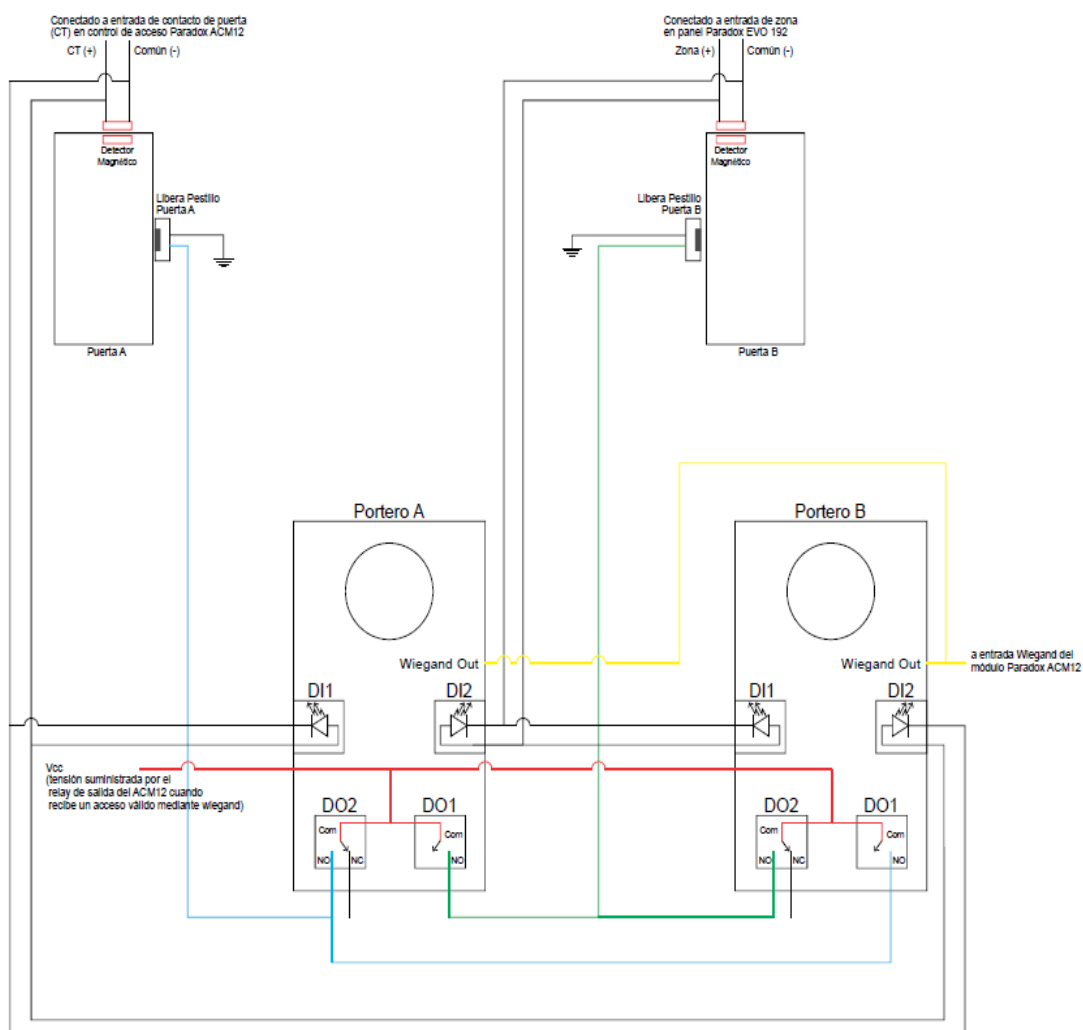
This open door logic will make sure two doors are open in “One-Way” direction, at any given time only one door can be opened, and only one legal open door request is allowed to execute. The hallway or scene between two doors could be monitored by installing Grandstream IP cameras.

This feature can be used in application scene like: College Dorm, Bank Branches, Government Offices, Medical Clinics, Private Clubs, etc., where there are two doors in place, high security and flow control is required (only one entry per time) but security guard may not be on site always.

Below is the illustrating drawing of the application scene:



Below is the wiring sample to implement this feature:



NOTES:

- If required to use the same two doors for “Exit” direction, another GDS3710 is required and it can be configured in Door 2 to control “Exit” direction. The wiring/connection will be mirrored.

Detailed document and example about how to configure this feature can be found at:

<http://www.grandstream.com/support/resources/?title=GDS3710>

PAIR WITH GSC3570 OPEN DOOR W/O SIP CALL

This new open door feature is a major enhancement to GDS37xx, but need to include GSC3570 paired to make it a whole solution. The GDS37xx/GSC3570 will be pairing together in LAN, and GDS37xx still controls the strike.

- **Functionality**

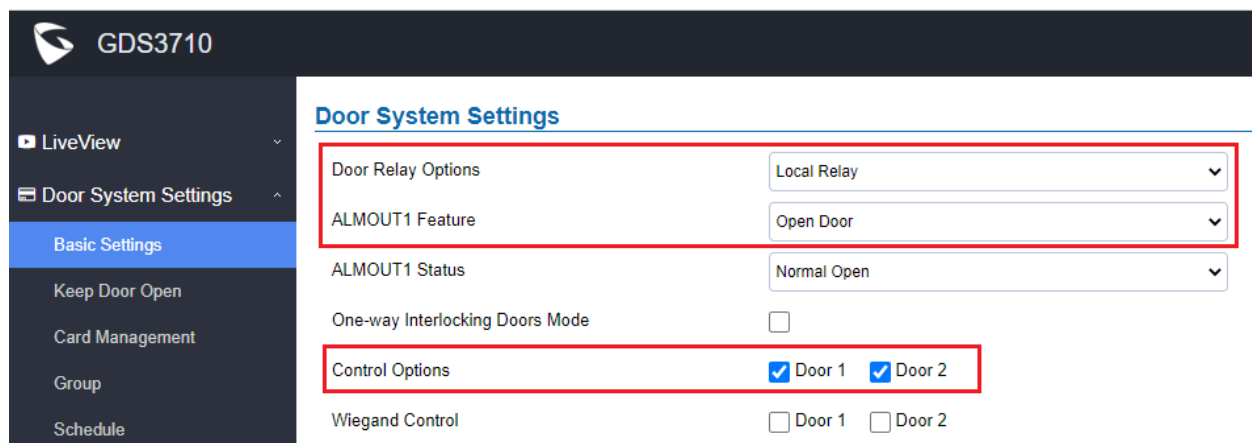
When enabled and configured this feature, the user will touch the GSC3570 and open the door directly via GDS37xx, without making SIP calls. This feature needs related matching GSC3570 firmware to work. The firmware required:

- **GSC3570: 1.0.5.9 or above**

- **Web Configuration**

GDS3710: (FW: 1.0.7.23 or above)

This setup can be found under device web UI → Door System Settings → Basic Settings:

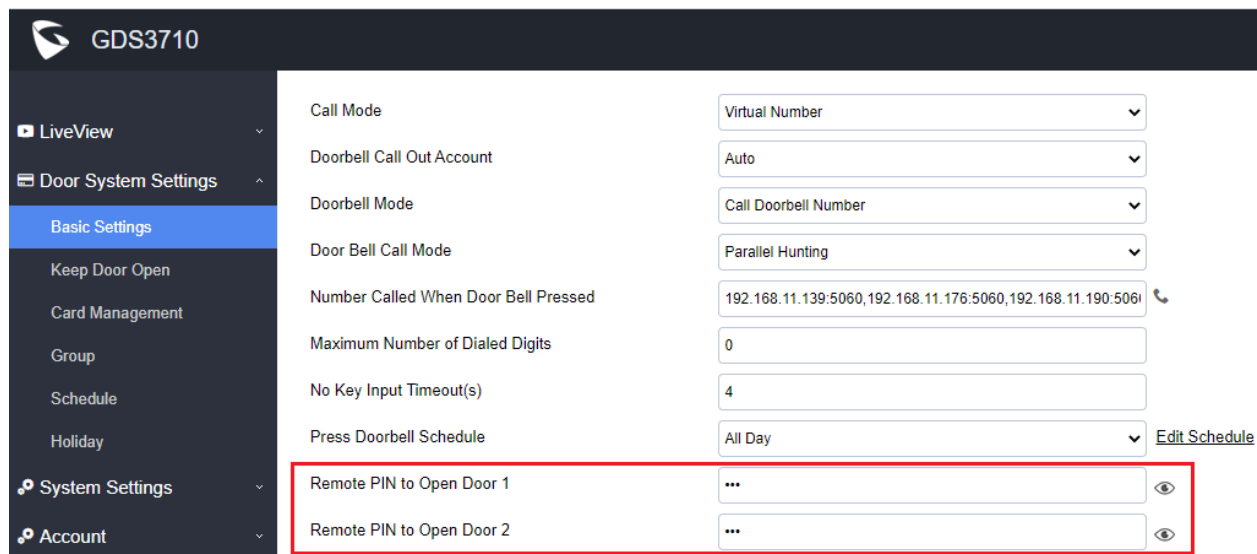


GDS3710

Door System Settings

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule

Door Relay Options	Local Relay
ALMOUT1 Feature	Open Door
ALMOUT1 Status	Normal Open
One-way Interlocking Doors Mode	<input type="checkbox"/>
Control Options	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Wiegand Control	<input type="checkbox"/> Door 1 <input type="checkbox"/> Door 2



GDS3710

Basic Settings

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
- System Settings
- Account

Call Mode	Virtual Number
Doorbell Call Out Account	Auto
Doorbell Mode	Call Doorbell Number
Door Bell Call Mode	Parallel Hunting
Number Called When Door Bell Pressed	192.168.11.139:5060,192.168.11.176:5060,192.168.11.190:5060
Maximum Number of Dialed Digits	0
No Key Input Timeout(s)	4
Press Doorbell Schedule	All Day Edit Schedule
Remote PIN to Open Door 1	...
Remote PIN to Open Door 2	...

The GDS37xx is configured to control the relay/strike with “Door Relay Option” selected as “Local Relay”, where 1 door or 2 door used, depending on user’s configuration and installation.

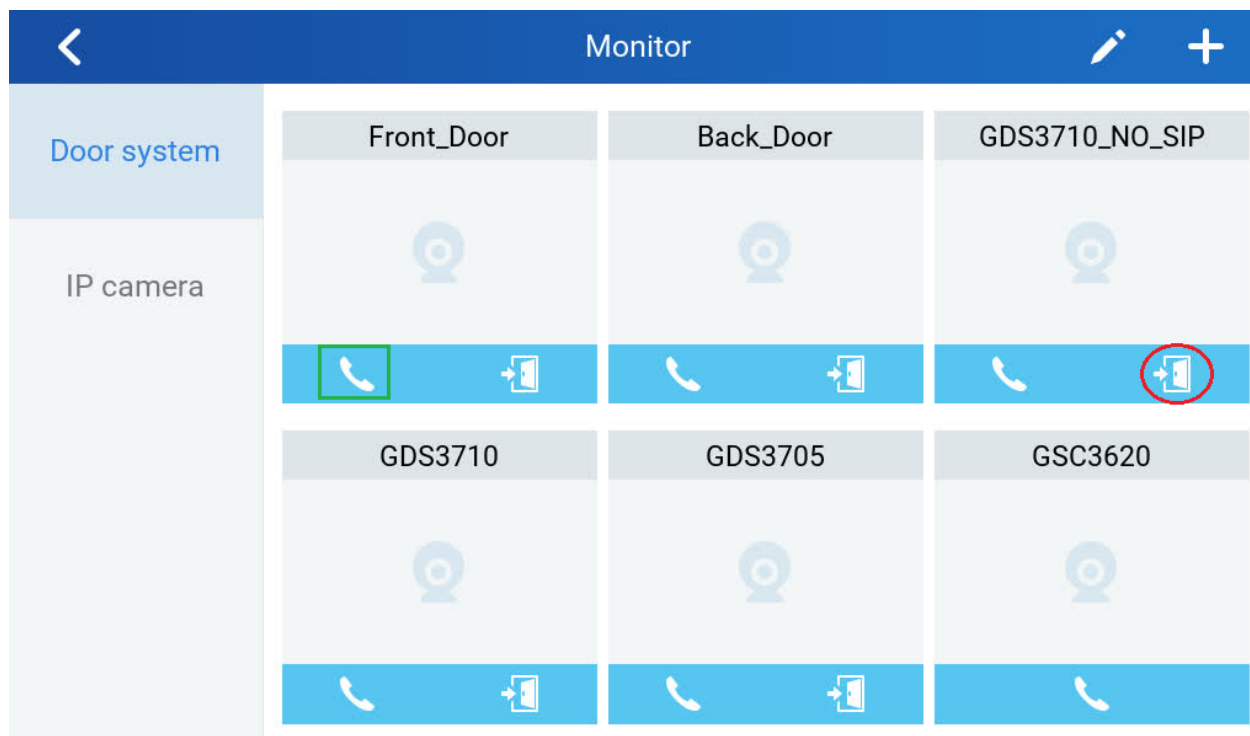
GSC3570: (FW: 1.0.5.9 or above)

The GSC3570 side also need to be configured according, like below:

Settings Grandstream Door System										
General Settings	Order	Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password
External Service	1	GDS	Account 1	Front_Door	873		Front_Door			
	2	GDS	Account 1	Back_Door	877		Back_Door			
Digital Output	3	GDS	Account 1	GDS3710_NO_SIP	192.168.11.126	192.168.11.126	Door1		Door2	
	4	GDS	Account 1	GDS3710	8606		SIP			

In the “SETTINGS → External Service”, input the IP address of GDS37xx where the GSC3570 paired with, and input the correct PIN for open related remote doors. The PIN should match with GDS37xx related remote PIN to open door.

Once configured successfully, in the touch screen UI of GSC3570, press “Monitor”, select “Door system”, will see UI like below:



Select the related door where the GSC3570 controlled, in this example, the “GDS3710_NO_SIP” located at right corner of top line is the one configured. Press the icon of open door (red circled one) will pop up another UI like below:



Press related “Door 1” or “Door 2” icon (two doors configured in this example), the GDS37xx will operate the strike and open the correspondent door accordingly.

If press the “Phone” icon (green square illustrated above), then the GSC3570 will make SIP phone call to the configured GDS37xx and open door remotely via SIP phone call like as before.

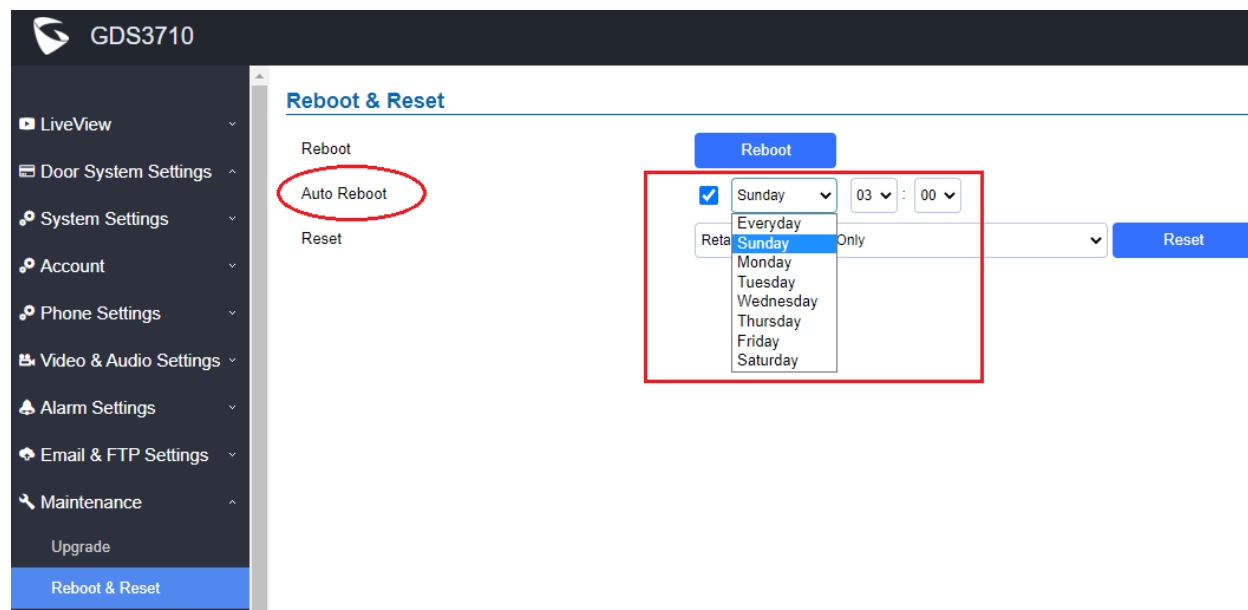
The application will help customers with installation scene where GSC3570 is located near Receptionist or related person, the user just use GSC3570 to operate GDS37xx to open door, without make a SIP phone call.

This application scene is good for hospital/clinic or senior house etc., environment where open door button or switch is NOT installed or wired, customer can just add a GSC3570 to open door from inside by related person (nurse or receptionist), to give convenience to their customers to come in or get out of the office or building.

SCHEDULED AUTO REBOOT

- **Web Configuration**

This option can be found under device web UI → Maintenance → Reboot & Reset:



- **Functionality**

This feature enhancement is response to field complains from system integrators using 3rd party NVR or open source RTSP live streaming solutions.

Due to chipset limitation as well as 2nd stage development or 3rd party integration, caused by accumulated broken RTSP threads due to all kinds of network reason (just like open tons of browser windows in PC), the unclosed threads will finally break down the video feeds. A reboot will clear all to make it work again.

Before implement this feature, customers need to write their own scripts to reboot the device, or using SIP NOTIFY from SIP Server to reboot the device, or manually reboot the device when found video stopped in the NVR or 3rd party RTSP server.

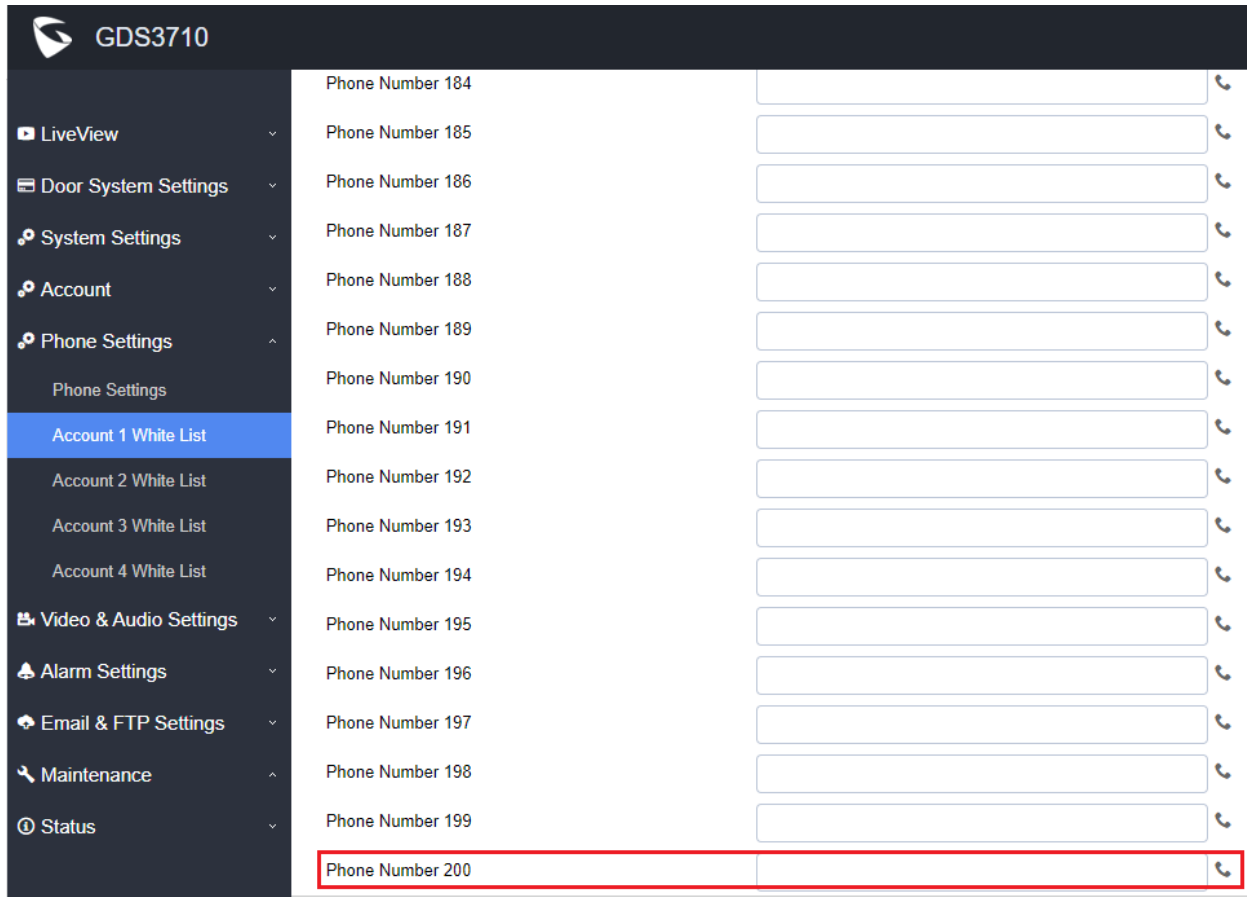
With this feature implemented, customer can configure convenient selected schedule to let the device reboot itself, per week or per day, to make a smooth and clean system, for the access control operation as well as reliable video feed.

Reliability is ensured by implement this new enhancement.

INCREASED WHITELIST

- Web Configuration**

This option can be found under device web UI → Phone Settings → Account X White List:



Phone Number	Input Field	Delete Icon
Phone Number 184	<input type="text"/>	🗑️
Phone Number 185	<input type="text"/>	🗑️
Phone Number 186	<input type="text"/>	🗑️
Phone Number 187	<input type="text"/>	🗑️
Phone Number 188	<input type="text"/>	🗑️
Phone Number 189	<input type="text"/>	🗑️
Phone Number 190	<input type="text"/>	🗑️
Phone Number 191	<input type="text"/>	🗑️
Phone Number 192	<input type="text"/>	🗑️
Phone Number 193	<input type="text"/>	🗑️
Phone Number 194	<input type="text"/>	🗑️
Phone Number 195	<input type="text"/>	🗑️
Phone Number 196	<input type="text"/>	🗑️
Phone Number 197	<input type="text"/>	🗑️
Phone Number 198	<input type="text"/>	🗑️
Phone Number 199	<input type="text"/>	🗑️
Phone Number 200	<input type="text"/>	🗑️

- Functionality**

This feature enhancement is response to field request from system integrators.

Now the Whitelist is increased to maximum 200 entries per Account. It can be IP address, SIP extension or Phone numbers, or hybrid/mixed.

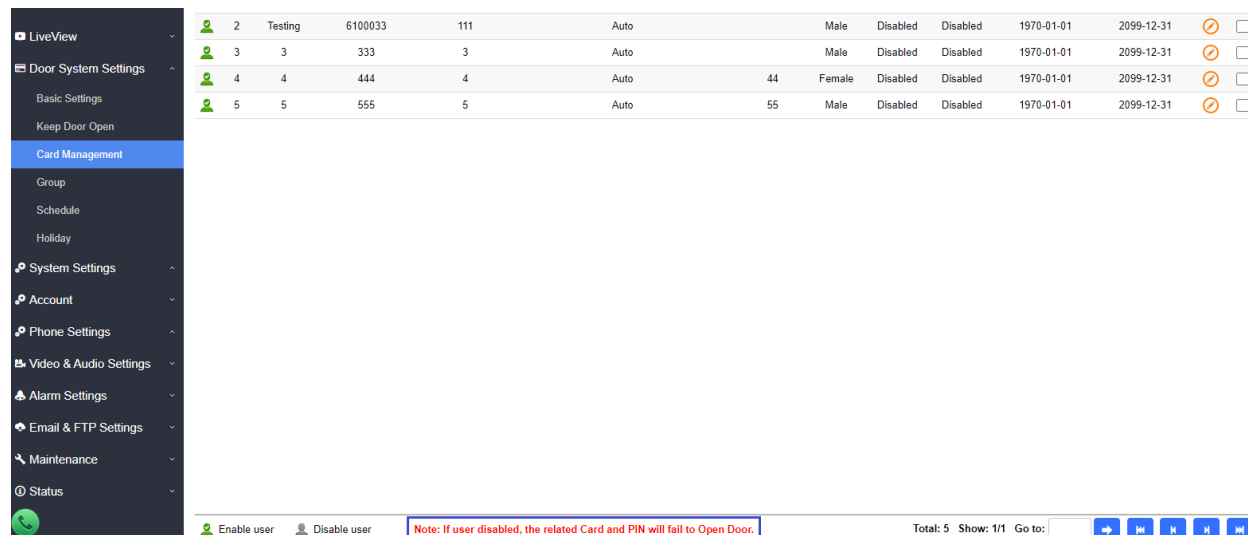
Also, when IP addresses in Whitelist, the “Accept Incoming SIP from Proxy Only” setting will be by passed even when it has been configured or enabled.

The “Accept Incoming SIP from Proxy Only” is configured to enhance SIP security to block goofing or hacking SIP calls from Internet. the IP address input to the Whitelist will allow the device with that IP to make calls to GDS37xx to open door.

MODIFIED TIPS AT CARD MANAGEMENT PAGE

- **Web Configuration**

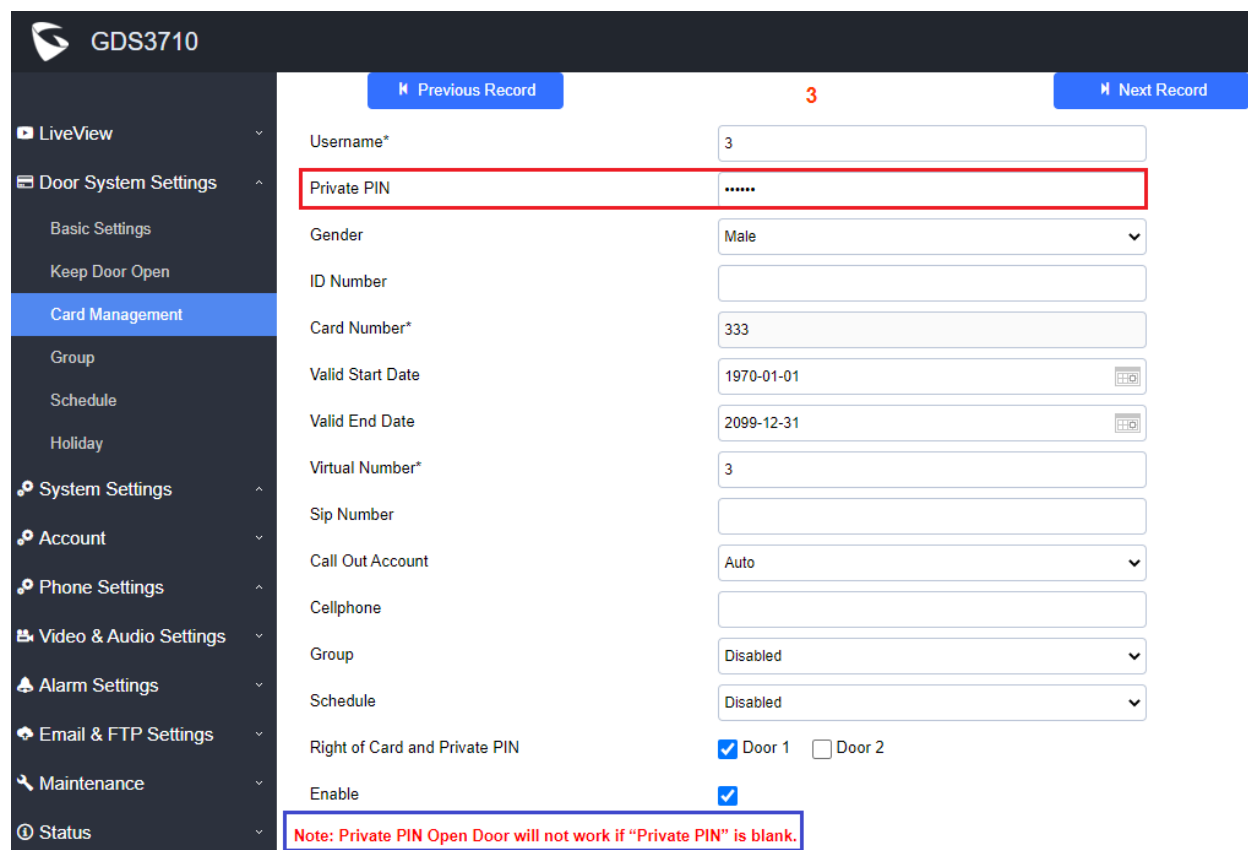
This option can be found under device web UI → Door System Settings → Card Management:



The screenshot shows the 'Card Management' page in the Grandstream web UI. On the left is a sidebar with navigation options: LiveView, Door System Settings (Basic Settings, Keep Door Open, Card Management), System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The 'Card Management' section is active, displaying a table with user information.

	2	Testing	6100033	111	Auto		Male	Disabled	Disabled	1970-01-01	2099-12-31		<input type="checkbox"/>
	3	3	333	3	Auto		Male	Disabled	Disabled	1970-01-01	2099-12-31		<input type="checkbox"/>
	4	4	444	4	Auto	44	Female	Disabled	Disabled	1970-01-01	2099-12-31		<input type="checkbox"/>
	5	5	555	5	Auto	55	Male	Disabled	Disabled	1970-01-01	2099-12-31		<input type="checkbox"/>

At the bottom of the table, there are controls: 'Enable user' (green icon), 'Disable user' (grey icon), a note box stating 'Note: If user disabled, the related Card and PIN will fail to Open Door.', and pagination information: 'Total: 5 Show: 1/1 Go to:'. Navigation buttons (Previous, Next, etc.) are also present.



The screenshot shows the 'Card Management' form for user 3. The sidebar is the same as in the previous screenshot. The form has fields for: Username* (3), Private PIN (masked with dots), Gender (Male), ID Number, Card Number* (333), Valid Start Date (1970-01-01), Valid End Date (2099-12-31), Virtual Number* (3), Sip Number, Call Out Account (Auto), Cellphone, Group (Disabled), Schedule (Disabled), Right of Card and Private PIN (Door 1 checked, Door 2 unchecked), and Enable (checked). A note at the bottom states: 'Note: Private PIN Open Door will not work if "Private PIN" is blank.'

- **Functionality**

This enhancement is based on customer's feedback to increase the usability with friendly UI.

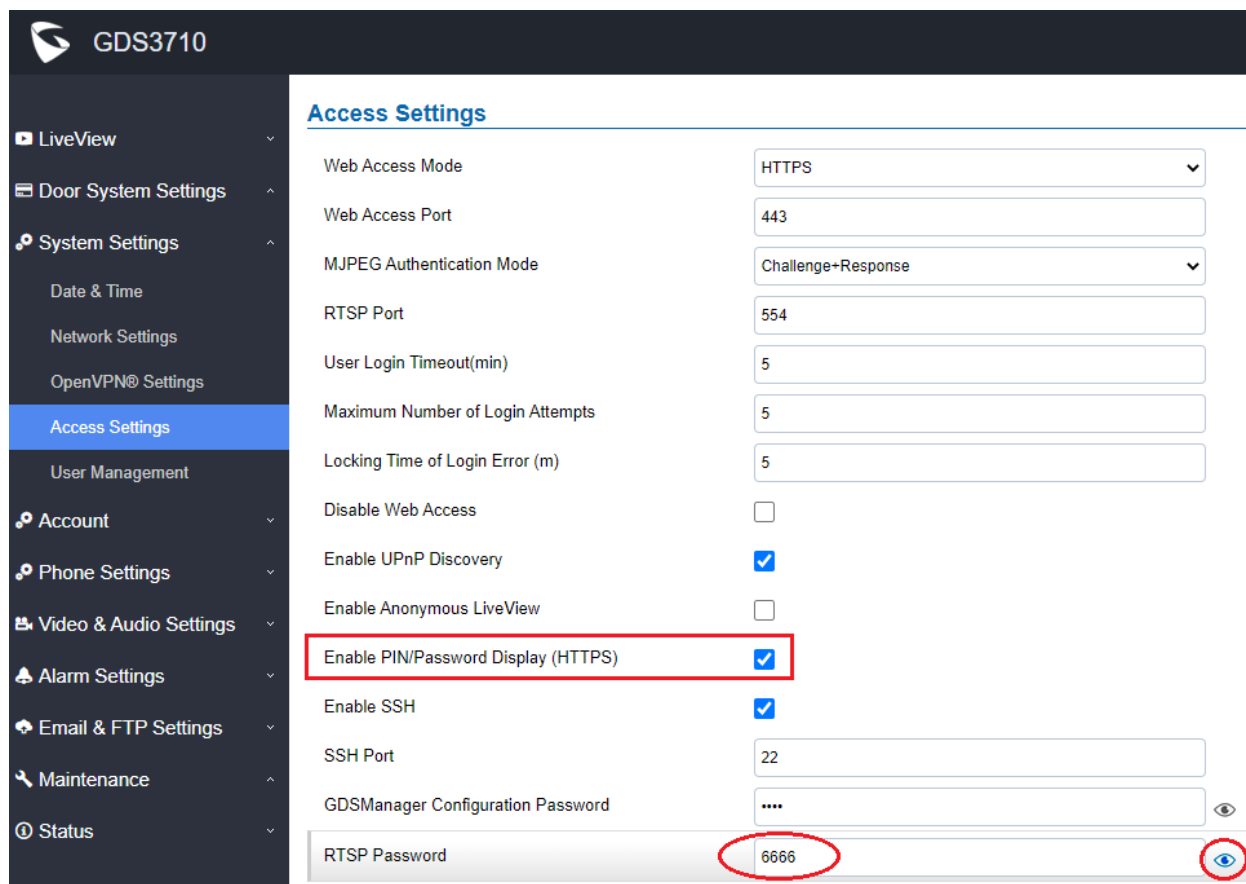
In the above screenshot, tips are added like:

- Note: If user disabled, the related Card or PIN will fail to Open Door.
- Note: Private PIN Open Door will not work if "Private PIN" is blank.

WEBUI PASSWORD DISPLAY WITH SECURITY AND CONVENIENCE

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



GDS3710

Access Settings

Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password
RTSP Password	6666

- **Functionality**

This feature enhancement is a compromised solution to response the feedback from system integrators as well as the request from ITSP customers.

ITSP customer provisioning device and do not want end user to mess around the device, therefore requesting NO password should be displayed in webUI.

System integrators have different application scenes, therefore requesting password to be displayed once logged in as admin, just for configuration and management convenience.

This feature is enhanced to meet both requirements.

By default, the “Enable PIN/Password Display (HTTPS)” is disabled for ITSP customer. Service provider customers are using Configuration Template to provision the device, they can change related P values to change the configuration of the provisioned device.

System integrators can check and enable the PIN/Password Display in the “Access Setting”. Once enabled, there will be an “eye” icon displayed in the webUI, putting mouse cursor to the “eye” icon, the related password or PIN will be displayed at the webUI. Once mouse cursor moved away, the PIN/Password will be displayed as dot “.” as usual.

This feature ONLY works in HTTPS mode. Due to the insecurity of HTTP, PIN/Password will NOT be displayed. PIN/Password can ONLY be displayed in HTTPS mode.

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.19

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

10/16/2020

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal or missed configuration settings in the webUI, factory reset is MANDATORY. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Added Alarm Action triggering when illegal card swiped.
- Added Newfoundland/Canada time zone.
- Added Card Number limitation with maximum number to be **2147483647**.
- Improved security vulnerability.
- Added Secure Open Door with GDS37xx/GSC3570 Peering and door lock/strike wired to GSC3570 Alarm_Out port and controlled by GSC3570 (located inside) instead of GDS37xx (located outside).
- Added Web Relay ON/OFF URL configuration field for some 3rd party Web Relay Door Controlling.
- Set “RTSP password” and “GDSManager Configuration Password” initial value to be GDS37xx default random password.
- Enhanced partition to prevent device failure with doorbell blue light solid on.

BUG FIX

- Fixed file import failure when using exported .csv file format.
- Fixed Stream 3 video used in SIP call even Stream 2 configured.
- Fixed [Telefonica] TCP_SRV reregistered address error during call.
- Fixed NAPTR/SRV not used in DNS Mode when resolving the proxy server.
- Fixed cannot dial using Virtual Number.
- Fixed Local PIN (public, private, guest) Open Door working only once at very first input in OpenVPN.
- Fixed Direct IP Call from IP phones in the same LAN also get rejected when enable “Accept Incoming SIP from Proxy Only” to block ghost calls.
- Fixed LLDP/VLAN setting disappeared from webUI when choosing static IP address.
- Fixed ringing back tone played in GDS37xx side before the alarm call triggered by silent alarm or hostage code be answered.
- Fixed upgrade/downgrade via SSH CLI commands not working.
- Fixed more than 6 motion detection alarm region configured at same time via Firefox browser, saving the configuration will not work and the MD region configured will be lost.
- Fixed failed to restore factory default random password via special key combination.
- Fixed when abnormal open door happened, the siren/alarm should not stop unless the alarm call answered or correct open door PIN entered.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P15440	Door_System_Settings.Basic_Settings.Door_Relay_Options Value: 0/1/2. 0: Loacl Relay 1: Webrelay 2: GSC3570 Relay
P15441	Door_System_Settings.Basic_Settings.Webrelay_ON_URL Type: String. Max.length = 1024
P15447	Door_System_Settings.Basic_Settings.Webrelay_OFF_URL Type: String. Max.length = 1024
P15442	Door_System_Settings.Basic_Settings. Webrelay_Username Type: String. Max.length = 128
P15443	Door_System_Settings.Basic_Settings. Webrelay_Password Type: String. Max.length = 128
P15444	Door_System_Settings.Basic_Settings.GSC3570_Account_to_Choose Value: 1/2/3/4 1: Account1 2: Account2 3: Account 4: Account4
P15445	Door_System_Settings.Basic_Settings.GSC3570_Phone_Number Type: String. Max.length = 128
P15446	Door_System_Settings.Basic_Settings.GSC3570_Password Type: String. Max.length = 128

UPDATED P-VALUE

P64	Added Option 39 -- GMT-03:30 (Newfoundland)
-----	---

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15440=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15441=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15447=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15442=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15443=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15444=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15445=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=door
- SET:[http|https]://<servername>/goform/config?cmd=set&P15446=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

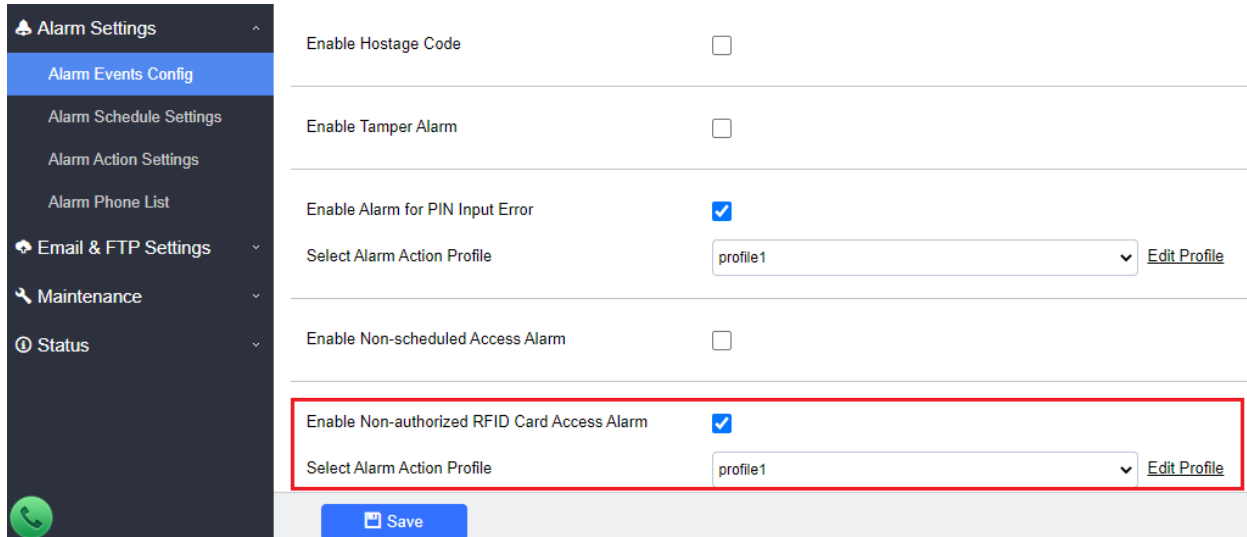
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

ALARM ACTION WHEN ILLEGAL CARD SWIPED

- Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Event Config:



Alarm Settings

- Alarm Events Config
- Alarm Schedule Settings
- Alarm Action Settings
- Alarm Phone List

Email & FTP Settings

Maintenance

Status

Enable Hostage Code ☐

Enable Tamper Alarm ☐

Enable Alarm for PIN Input Error ☒

Select Alarm Action Profile profile1 [Edit Profile](#)

Enable Non-scheduled Access Alarm ☐

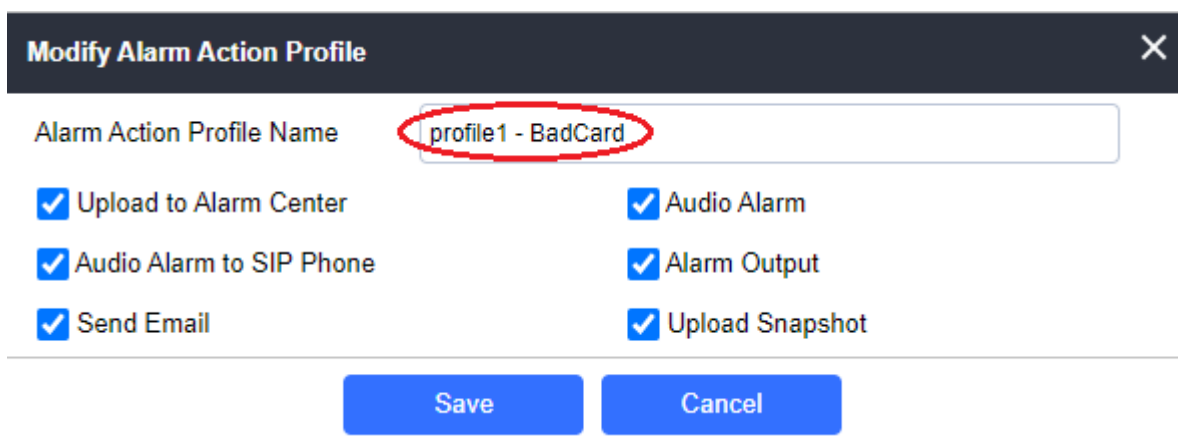
Enable Non-authorized RFID Card Access Alarm ☒

Select Alarm Action Profile profile1 [Edit Profile](#)

[Save](#)

- Functionality**

This feature enhancement is requested by customers from field. By enable this feature, any illegal card swiped trying to access the door will trigger alarm based on user's configuration, like below:



Modify Alarm Action Profile

Alarm Action Profile Name profile1 - BadCard

☒ Upload to Alarm Center ☒ Audio Alarm

☒ Audio Alarm to SIP Phone ☒ Alarm Output

☒ Send Email ☒ Upload Snapshot

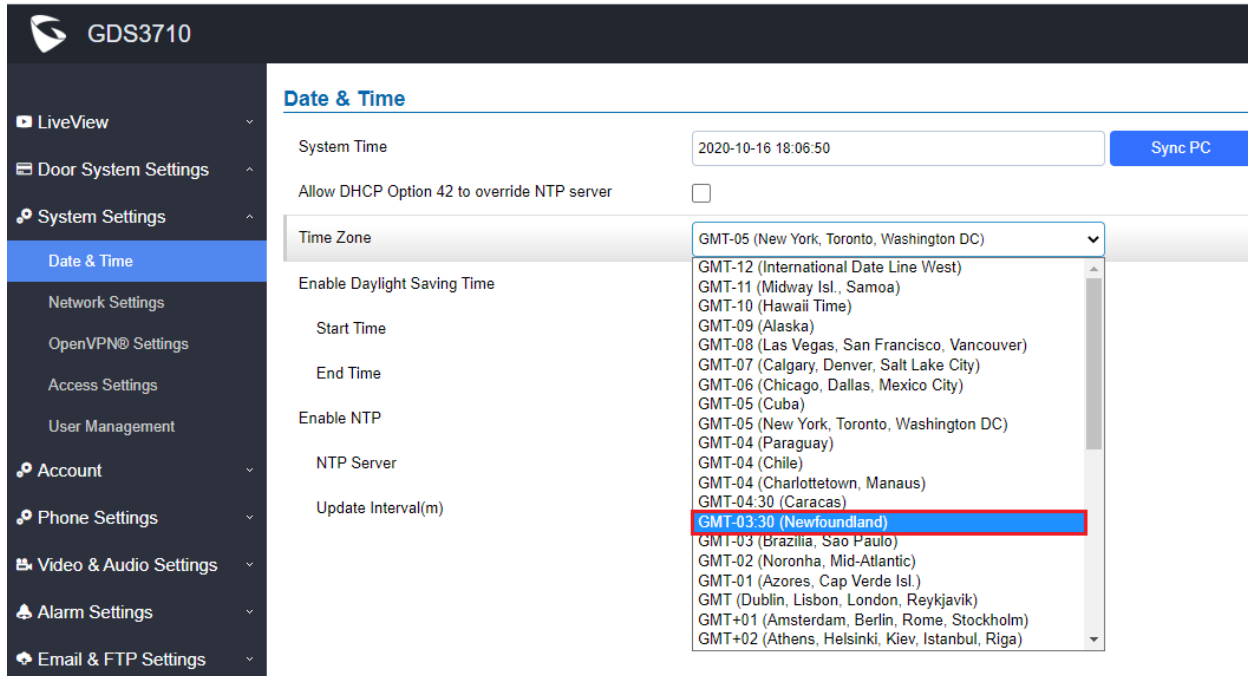
[Save](#) [Cancel](#)

User will get email, snapshot, etc., based on the Alarm Action Profile configured, to enhance the security of access control.

NEWFOUNDLAND/CANADA TIME ZONE

- **Web Configuration**

This option can be found under device web UI → System Settings → Date & Time → Time Zone:



GDS3710

Date & Time

System Time: 2020-10-16 18:06:50 Sync PC

Allow DHCP Option 42 to override NTP server: ☐

Time Zone: GMT-05 (New York, Toronto, Washington DC) ▼

Enable Daylight Saving Time: ☐

Start Time:

End Time:

Enable NTP: ☐

NTP Server:

Update Interval(m):

Time Zone List:

- GMT-12 (International Date Line West)
- GMT-11 (Midway Isl., Samoa)
- GMT-10 (Hawaii Time)
- GMT-09 (Alaska)
- GMT-08 (Las Vegas, San Francisco, Vancouver)
- GMT-07 (Calgary, Denver, Salt Lake City)
- GMT-06 (Chicago, Dallas, Mexico City)
- GMT-05 (Cuba)
- GMT-05 (New York, Toronto, Washington DC)
- GMT-04 (Paraguay)
- GMT-04 (Chile)
- GMT-04 (Charlottetown, Manaus)
- GMT-04:30 (Caracas)
- GMT-03:30 (Newfoundland)**
- GMT-03 (Brazilia, Sao Paulo)
- GMT-02 (Noronha, Mid-Atlantic)
- GMT-01 (Azores, Cap Verde Isl.)
- GMT (Dublin, Lisbon, London, Reykjavik)
- GMT+01 (Amsterdam, Berlin, Rome, Stockholm)
- GMT+02 (Athens, Helsinki, Kiev, Istanbul, Riga)

- **Functionality**

This feature is implemented based on request from Canadian customers located in this special time zone.

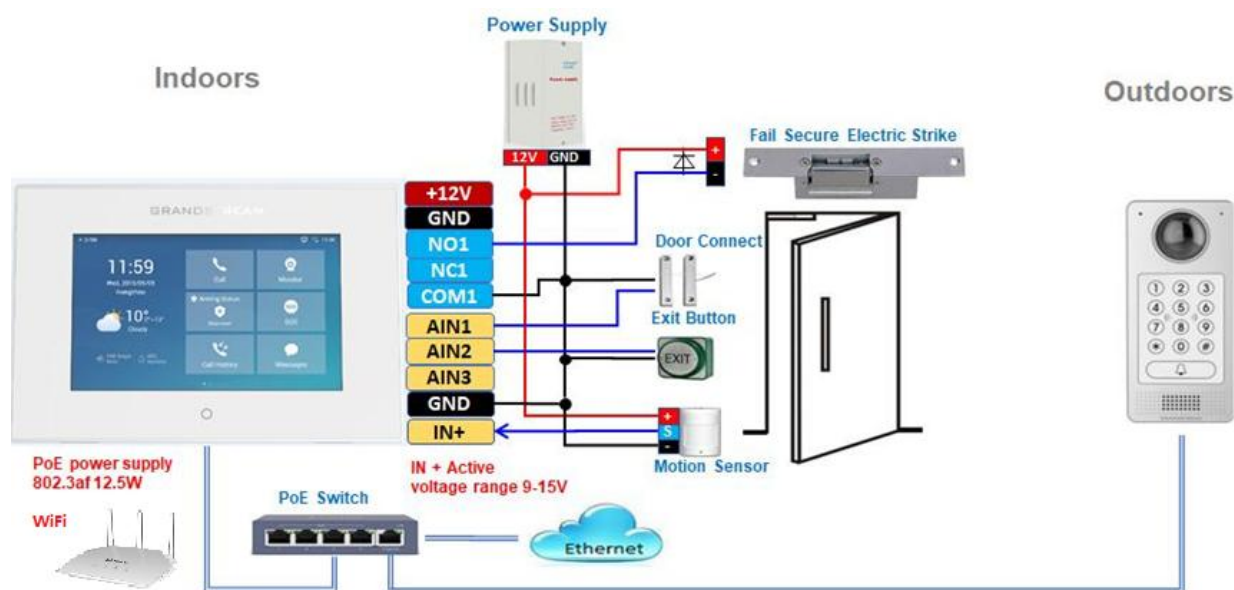
This feature can also be provisioned by ITSP service provider customers via using the P value and configuration template, as well as using UCM zero-configuration functionality.

GSC3570 SECURE OPEN DOOR VIA GDS37XX/GSC3570 PEERING

This secure open door new feature is a major enhancement to GDS37xx, but need to include GSC3570 to make it a whole solution. The GDS37xx/GSC3570 will be peering together in LAN/WAN via IP/SIP, the door lock/strike will be wired to GSC3570 Alarm_Out port and controlled by GSC3570 (located inside) instead of GDS37xx (located outside). This way the strike control is inside the building with enhanced security.

• Functionality

This application scene will be similar like below:



Minimum firmware required for this to work:

- Outdoor Device: GDS3710 (FW1.0.7.19) / GDS3705 (FW1.0.1.13)
- Indoor Device: GSC3570 (FW1.0.5.2)

The GDS37xx can be powered via PoE; the GSC3570 can connect to same network via PoE or Wi-Fi.

For open door combination with GSC3570 and GDS37xx, if GSC3570 needs to control multiple GDS37xx, it has to use SIP and the related GDS37xx will control the strike/lock. The different GDS37xx doorbell call will have "One Button Open Door" displayed when in "Preview" (early media support) or when call established. The GSC3570 user will press the virtual button on touch screen to remotely open the door controlled by the related GDS37xx. There is no door limitation for such usage but only ONE DOOR can be opened at one time. It is just a SIP call open door application, but strike/lock control circuit is located outdoor.

For "Secure Open Door", the GSC3570 is peering with GDS37xx. The GSC3570 controlling the relay/strike/lock from inside the building (Unlike GDS37xx installed outside), but only ONE door can be controlled because GSC3570 only has one Relay Control circuit build in.

This peering can be via LAN/WAN but LAN is recommended and actually most of the application scene are in LAN environment because most likely the GSC3570 and GDS37xx are in the same building.

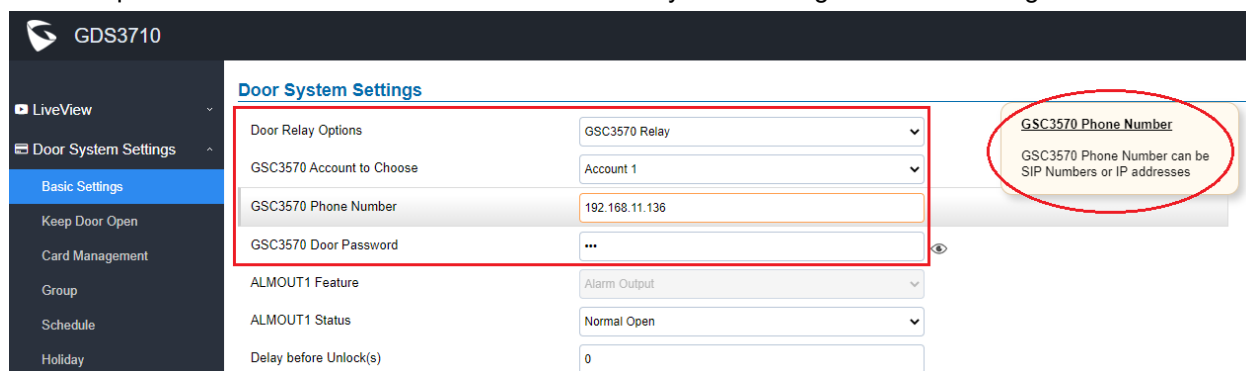
Although SIP/UCM over Internet/WAN also works, it is recommended to use static IP if the GSC3570 (inside) and GDS37xx (outside) are at same location in the same LAN. This setup is much simple and reliable in case there is network outage like Internet/UCM is down.

For the GSC3570 and GDS37xx peering, it can be used via SIP only (Cloud or UCM); IP only (No SIP proxy or UCM but static IP address) and Mixed (SIP and fallback to IP if Proxy failed).

• Web Configuration

GDS3710: (FW: 1.0.7.19 or above)

This setup can be found under device web UI → Door System Settings → Basic Settings:

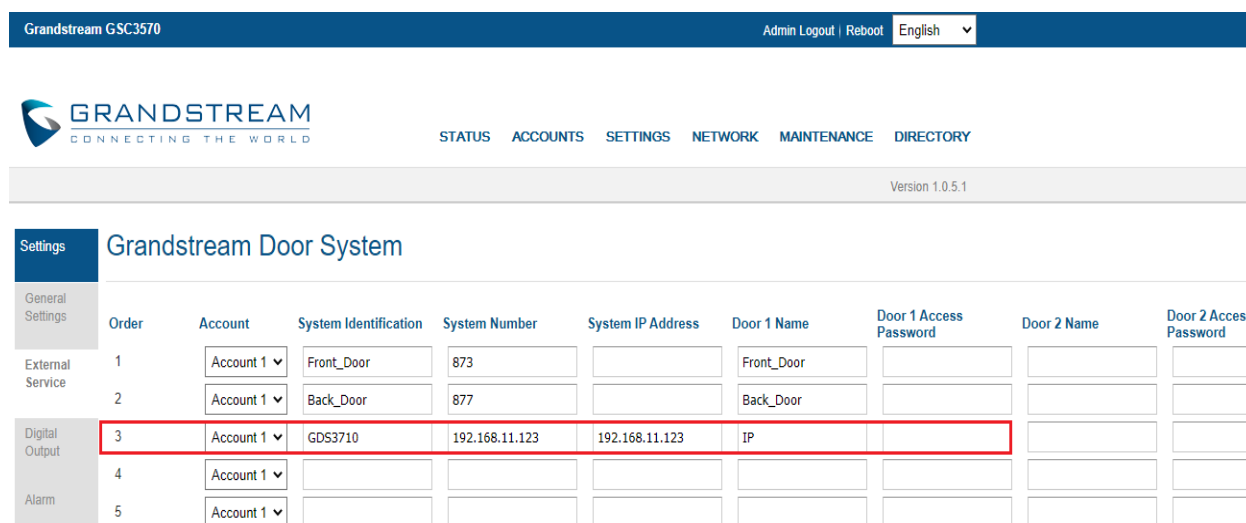


The screenshot shows the 'Door System Settings' page for a GDS3710 device. The 'Basic Settings' tab is selected. A red box highlights the 'GSC3570 Phone Number' field, which contains the value '192.168.11.136'. A callout bubble points to this field with the text: 'GSC3570 Phone Number can be SIP Numbers or IP addresses'.

Field	Value
Door Relay Options	GSC3570 Relay
GSC3570 Account to Choose	Account 1
GSC3570 Phone Number	192.168.11.136
GSC3570 Door Password	...
ALMOUT1 Feature	Alarm Output
ALMOUT1 Status	Normal Open
Delay before Unlock(s)	0

GSC3570: (FW: 1.0.5.2 or above)

The GSC3570 side also need to be configured according, like below:



The screenshot shows the 'Settings' page for a Grandstream GSC3570 device. The 'Grandstream Door System' section is expanded, showing a table with configuration details. A red box highlights the row for 'Digital Output' with Order 3.

Order	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password
1	Account 1	Front_Door	873		Front_Door			
2	Account 1	Back_Door	877		Back_Door			
3	Account 1	GDS3710	192.168.11.123	192.168.11.123	IP			
4	Account 1							
5	Account 1							

Settings

- General Settings
- External Service
- Digital Output
- Alarm
- SOS
- IPC
- Call Features
- Preferences

Digital Output

Digital Output	To door ▼
Account	Account 1 ▼
System Number	8606
System IP Address	192.168.11.123
Password	...
Unlock holding time	3

replace SIP extension with IP address
if no SIP proxy

Save Save and Apply Reset

If the solution/integration is using static IP address without SIP Proxy, all the devices involved (GDS/GSC/IP Phone) should choose “NAT Traversal” to “No” and should NOT “Use Random Port”, otherwise will have problem of ghost call (SIP signaling working but NO media).

Accounts

- Account 1
- Account 2
- General Settings
- Dialplan
- Network Settings**
- SIP Settings
- Codec Settings
- Call Settings
- Intercom Settings
- Account 3
- Account 4
- Account Swap

Network Settings

DNS Mode	A Record ▼
Primary IP	
Backup IP 1	
Backup IP 2	
NAT Traversal	No ▼
UPnP NAT Traversal	<input checked="" type="radio"/> No <input type="radio"/> Yes
Proxy-Require	

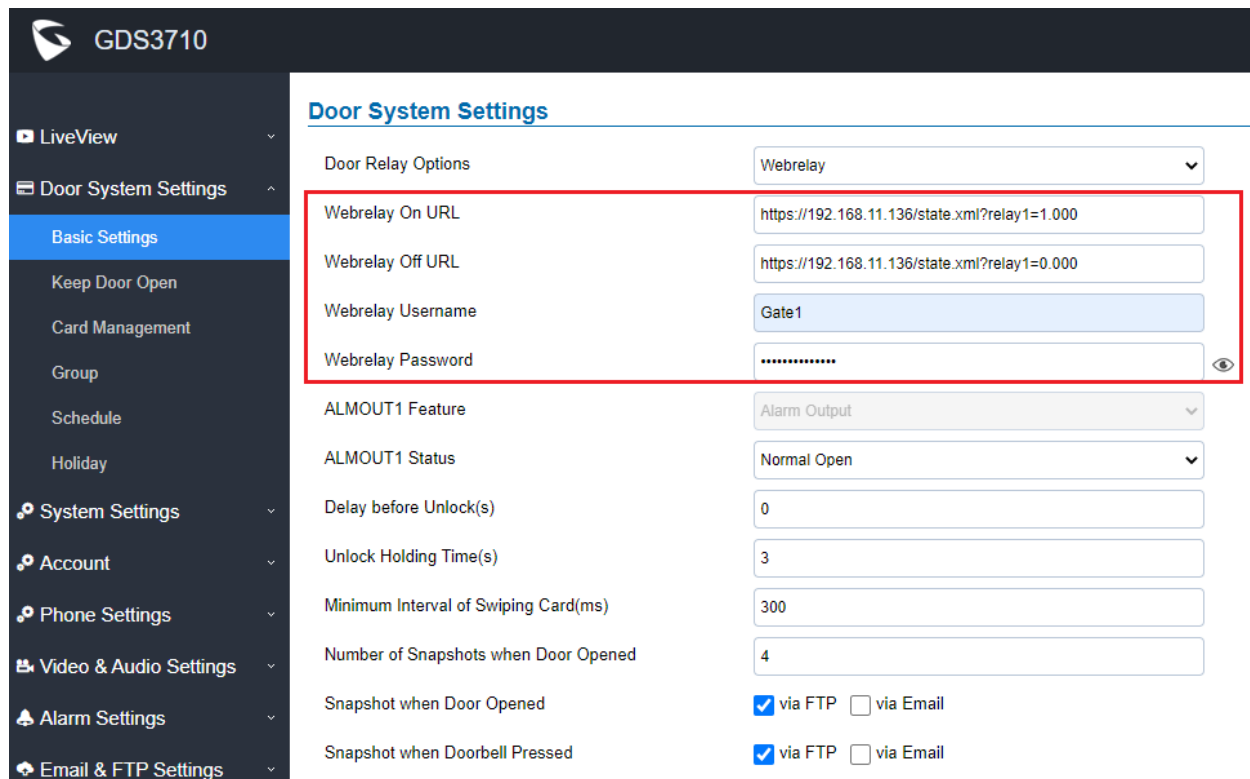
Save Save and Apply Reset

The IP phone or GSC3570 can use any empty SIP account, meaning it can be mixed if Account 1 registered to UCM/Proxy and Account 2 (blank) to use IP (but the account has to be configured as “Active”).

ENHANCED OPEN DOOR VIA 3RD PARTY WEBRELAY

- Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

Door Relay Options: Webrelay

Webrelay On URL: https://192.168.11.136/state.xml?relay1=1.000

Webrelay Off URL: https://192.168.11.136/state.xml?relay1=0.000

Webrelay Username: Gate1

Webrelay Password:

ALMOUT1 Feature: Alarm Output

ALMOUT1 Status: Normal Open

Delay before Unlock(s): 0

Unlock Holding Time(s): 3

Minimum Interval of Swiping Card(ms): 300

Number of Snapshots when Door Opened: 4

Snapshot when Door Opened: ☒ via FTP ☐ via Email

Snapshot when Doorbell Pressed: ☒ via FTP ☐ via Email

- Functionality**

This feature enhancement is response to field request to integration with 3rd party Webrelay controller, to install the relay controller inside the build to enhance the security or apply in some industry application solution.

Now there are two Webrelay URL fields available, with On or Off URL command allowed or other usage URL command allowed. Also allow Username and Password configured if the 3rd party Webrelay requiring this security feature.

If some 3rd party Webrelay only support one URL command, then just leave another Off URL blank, or put whatever there as long as it is NOT a URL command.

- 3rd Party Webrelay**

When Webrelay is selected, customers need to continue configure the Webrelay IP address or domain name, together with credentials like Username and Password, as well as the URL commands used by the 3rd party Webrelay.

When legal open door event happened, the configured web relay will get the communication from GDS3710, and will operate the strike to open door for the authenticated open door request. Or use that command to operate other industry application.

In web relay mode, the strike is wired to the web relay controller device.

The correct URL command, please refer to related 3rd party Webrelay User Manual or related documentation for details.

For more details about 3rd party Webrelay, please refer to below URL to get more information:

<https://www.controlbyweb.com/webrelay/> (Single/Dual/Quad, etc.)

<https://www.barix.com/barionet/> (Universal programable I/O device)

For detailed information about GDS3710, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.14

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

07/10/2020

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.7A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.5A	YES	
GDS3710 HW1.3A	YES	Only support HTTP upgrade
GDS3710 HW1.3B	YES	Only support HTTP upgrade
GDS3710 HW1.2A	YES	Only support HTTP upgrade

ENHANCEMENT

- Added OpenVPN support
- Added call termination button in the webUI
- Added ability to provision Card Management Users [Telefonica]
- Added displaying “Unauthorized door opening attempt” in the Event Log when illegal card used
- Added reboot/resync device via SIP Notify
- Added forcing password change after logging in via default password initially
- Added support “UserName” in HTTP Event Notification
- Added support for open door via Webrelay
- Added option to enable PIN/Password display

BUG FIX

- Fixed anonymous MJPEG stream viewing not function in “Basic” mode.
- Fixed IP peering call only use Account 1 to call.
- Fixed doorbell set parallel hunting door opened by one but other devices in the group still ringing.
- Fixed keypad blue light time interval not working when period is from night to morning.
- Fixed keypad white light will be off after call or PIN input when blue keypad light is set to on.
- Fixed not checking the full Whitelist numbers.
- Optimized and improved the delay of live preview in the supported browsers like Chrome and Firefox.
- Fixed as callee will not do stream negotiation.
- Fixed choosing “.gs” format to export data will get error “no data”.
- Fixed download CFG file in HTTPS mode may cause the device restart the web continuously.
- Fixed failed to upload custom ring tone.
- Fixed device failed sending request to secondary proxy if the primary proxy not responding.
- Fixed importing revised card information will not update in already existed cards.
- Fixed editing Motion Detection Region in some browser failed to save correctly.
- Fixed doorbell number is IP address the call cannot establish normally in Telefonica Mode.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P15514	System_Settings.Access_Settings.Enable_PIN_Password_Display_HTTPS Value: 0 / 1. 0: Disable; 1: Enable.
P15440	Door_System_Settings.Basic_Settings.Door_Relay_Options Value: 0 / 1. 0: Local Relay 1: WebRelay
P15441	Door_System_Settings.Basic_Settings.Webrelay_IP_Address Type: String. Max.length = 255
P15442	Door_System_Settings.Basic_Settings.Webrelay_Username Type: String. Max.length = 128
P15443	Door_System_Settings.Basic_Settings.Webrelay_Password Type: String. Max.length = 128
P7050	System_Settings.OpenVPN® Settings.Openvpn_Enable Value: 0 / 1. 0: Disable 1: Enable)
P7051	System_Settings.OpenVPN® Settings.Openvpn_Server_Address Type: String. Max.length = 256
P7052	System_Settings.OpenVPN® Settings.Openvpn_Port Value: 0 ~ 65535
P2912	System_Settings.OpenVPN® Settings.Openvpn_Transport Value: 0 / 1. 0: UDP 1: TCP
P9902	System_Settings.OpenVPN® Settings.Openvpn_CA Type: String. Max length = 8192
P9903	System_Settings.OpenVPN® Settings.Openvpn_Client_Certificate Type: String. Max.length = 8192
P9904	System_Settings.OpenVPN® Settings.Openvpn_Client_Key Type: String. Max.length = 8192
P8394	System_Settings.OpenVPN® Settings.Openvpn_Username Type: String. Max.length = 256
P8395	System_Settings.OpenVPN® Settings.Openvpn_Password Type: String. Max.length = 256
P8396	System_Settings.OpenVPN® Settings.Openvpn_Cipher_Method Value: 0/1/2/3 0: Blowfish; 1: AES-128; 2: AES-256; 3: Triple-DES
P8460	System_Settings.OpenVPN® Settings.Additional_Options Type: String. Max.length = 1024
P4428	Maintenance.Upgrade.Disable_SIP_NOTIFY_Authentication Value: 0 / 1. 0: Disable 1: Enable)

NEW HTTP API:

- **P15514**
GET:[http|https]://<servername>/goform/config?cmd=get&type=access
SET:[http|https]://<servername>/goform/config?cmd=set&P15514=<value>
- **P15440/ P15441/ P15442/ P15443**
GET:[http|https]://<servername>/goform/config?cmd=get&type=door
SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>
- **P7050/ P7051/ P7052/ P2912/ P8396/ P8394/ P8395/ P8460**
GET:[http|https]://<servername>/goform/config?cmd=get&type=openvpn
SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>
- **P9902/ P9903/ P9904**
GET:[http|https]://<servername>/goform/config?cmd=get&type=openvpn
UPLOAD:[http|https]://<servername>/goform/config?cmd=upload&type=4&index=x (x=0/1/2)
DEL:[http|https]://<servername>/goform/config?cmd=del&openvpn=x (x=0/1/2)
- **P4428**
GET:[http|https]://<servername>/goform/config?cmd=get&type=upgrade
SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

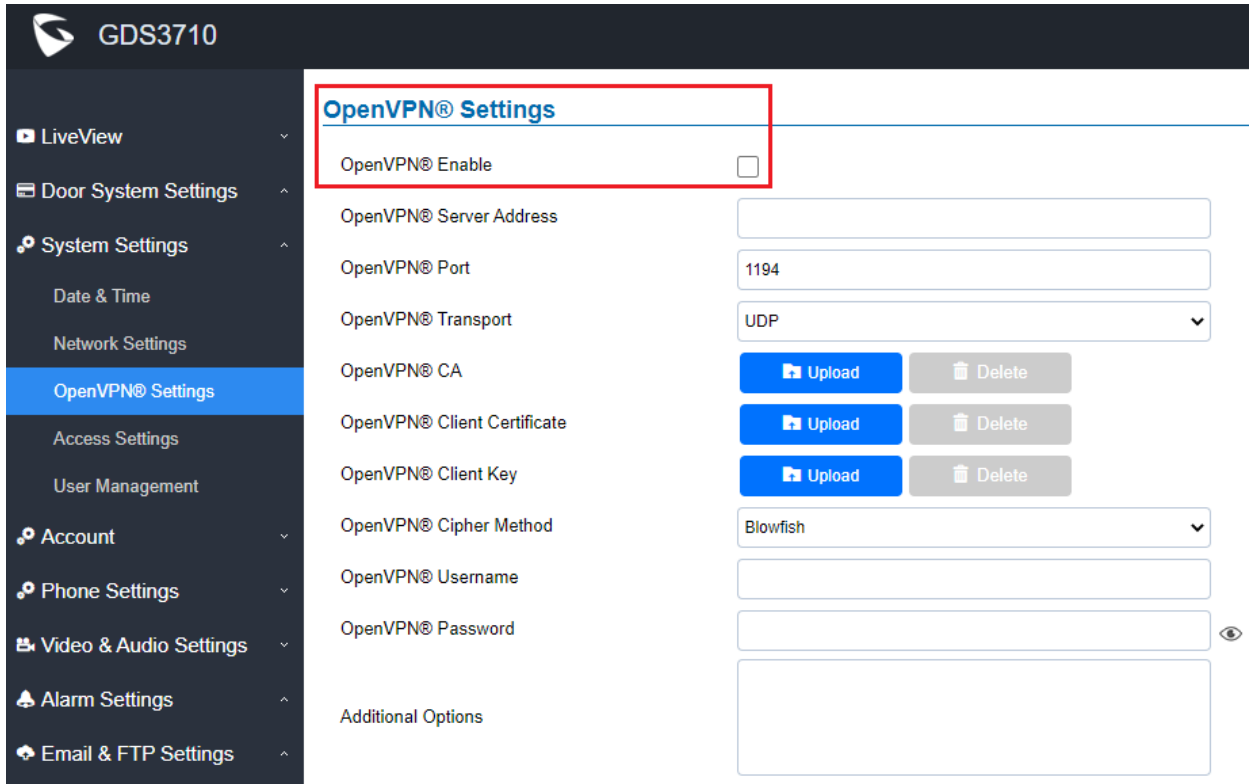
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

OPEN VPN SUPPORT

- **Web Configuration**

This option can be found under device web UI → System Settings → OpenVPN Settings:



The screenshot shows the web interface for a Grandstream GDS3710 device. On the left is a navigation menu with options like LiveView, Door System Settings, System Settings, and others. The 'System Settings' menu is expanded, and 'OpenVPN® Settings' is selected. The main content area shows the 'OpenVPN® Settings' page. At the top, the title 'OpenVPN® Settings' is highlighted with a red box. Below it is a checkbox labeled 'OpenVPN® Enable'. Further down are fields for 'OpenVPN® Server Address', 'OpenVPN® Port' (set to 1194), 'OpenVPN® Transport' (set to UDP), and 'OpenVPN® CA'. There are 'Upload' and 'Delete' buttons for the CA, Client Certificate, and Client Key. Below these are fields for 'OpenVPN® Cipher Method' (set to Blowfish), 'OpenVPN® Username', and 'OpenVPN® Password'. At the bottom is a section for 'Additional Options'.

- **Functionality**

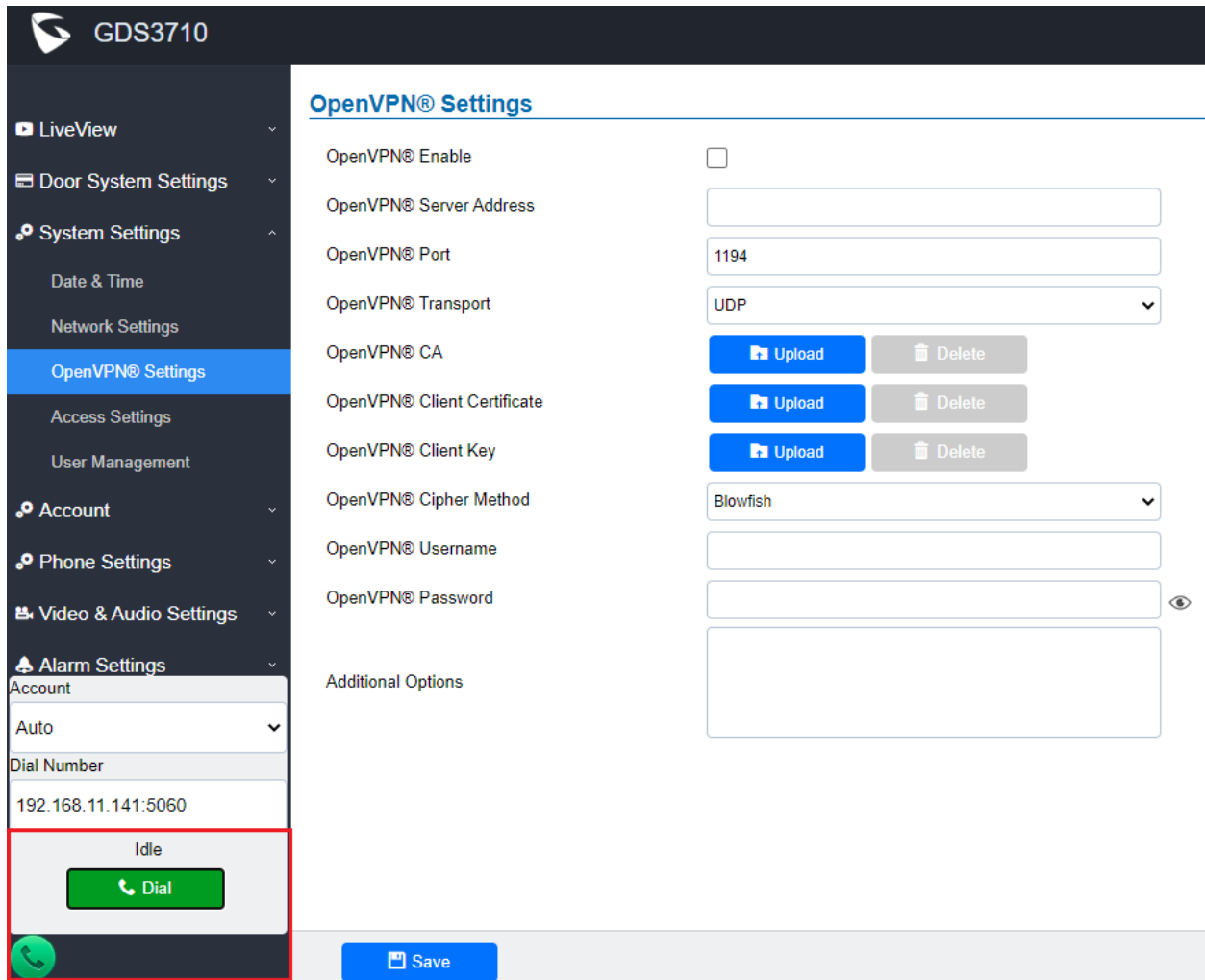
This feature enhancement will allow users to configure OpenVPN and connect the device to VPN network, so the device can be access and managed via VPN network.

This is very useful for enterprise customers. This feature is implemented based on request from business and service provider customers.

CALL TERMINATION BUTTON IN WEBUI

- **Web Configuration**

This option can be found at the lower left corner of the screen after logged into the device's webUI:



GDS3710

OpenVPN® Settings

OpenVPN® Enable ☐

OpenVPN® Server Address

OpenVPN® Port

OpenVPN® Transport

OpenVPN® CA

OpenVPN® Client Certificate

OpenVPN® Client Key

OpenVPN® Cipher Method

OpenVPN® Username

OpenVPN® Password


Additional Options


Account


Account: Auto

Dial Number: 192.168.11.141:5060

Idle


GDS3710

 LiveView

 Door System Settings

Basic Settings

Keep Door Open

Card Management

Group

Schedule

Holiday

System Settings


Account


Phone Settings

Account
 Auto

Dial Number
 192.168.11.141:5060

Connected

 End Call



Light Settings

Enable Key Blue Light ☒

Enable Background Light ☒

Doorbell Blue Light On/Off Time Interval Settings

Enable Doorbell Blue Light ☐

Keypad Blue Light On/Off Time Interval Settings

Enable Keypad Blue Light ☐

Card and PIN open door schedule configuration module

Central Mode ☒


Key Tone Setting

Key Tone Type Default

Wiegand Settings

Enable Wiegand Input ☐

Wiegand Output Disabled

 Save

Copyright © Grandstream Networks, Inc. 2020. All Rights Reserved.

- Functionality

This feature is implemented based on request from ITSP customers, as well as other customers in field.

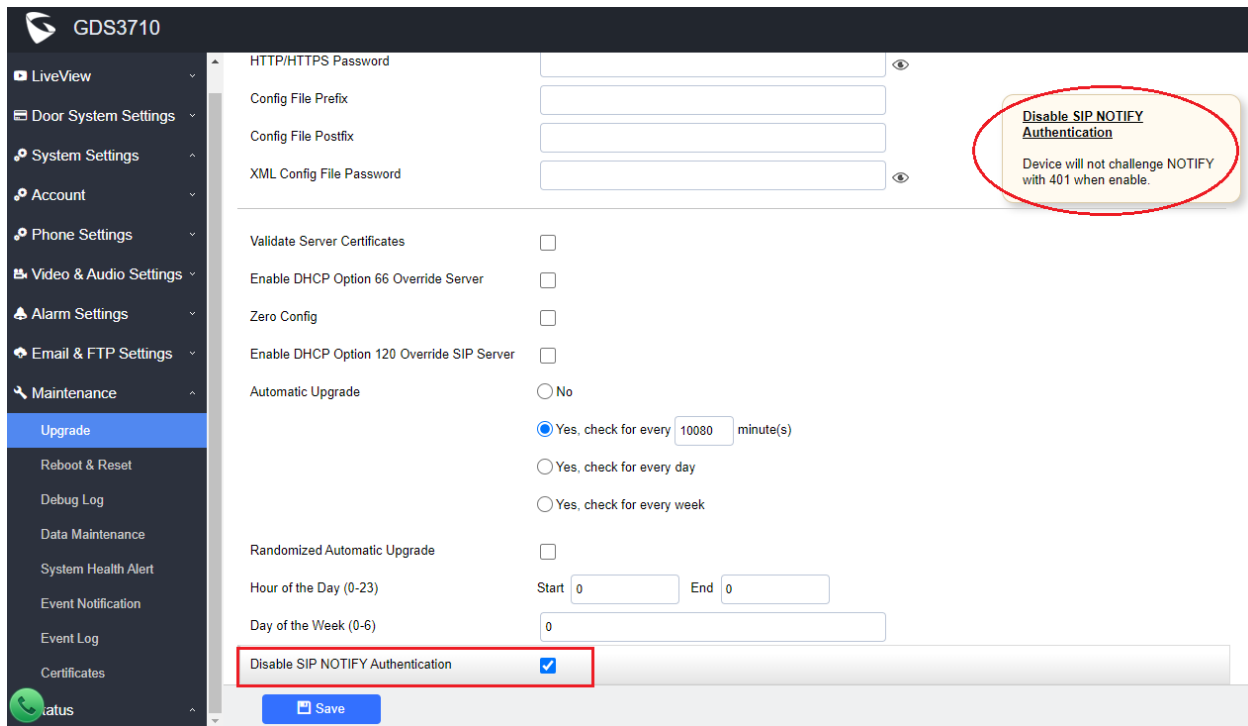
Previously there is a phone icon will allow user to make a call and hand up a call. The icon is “Green” when device is “idle” and “Red” when device is busy.

Adding this “End Call” icon will improve and make the call process UI more user friendly.

REBOOT/RESYNC VIA SIP NOTIFY

- Web Configuration**

This option can be found under device web UI → Maintenance → Upgrade:



GDS3710

- LiveView
- Door System Settings
- System Settings
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
 - Upgrade**
 - Reboot & Reset
 - Debug Log
 - Data Maintenance
 - System Health Alert
 - Event Notification
 - Event Log
 - Certificates
 - Status

HTTP/HTTPS Password

Config File Prefix

Config File Postfix

XML Config File Password

Validate Server Certificates ☐

Enable DHCP Option 66 Override Server ☐

Zero Config ☐

Enable DHCP Option 120 Override SIP Server ☐

Automatic Upgrade ☐ No

☒ Yes, check for every minute(s)

☐ Yes, check for every day

☐ Yes, check for every week

Randomized Automatic Upgrade ☐

Hour of the Day (0-23) Start End

Day of the Week (0-6)

Disable SIP NOTIFY Authentication ☒

Save

Disable SIP NOTIFY Authentication
 Device will not challenge NOTIFY with 401 when enable.

- Functionality**

For security concern, by default this feature is not enabled. If user check and disable this SIP NOTIFY feature, the device will reboot and resync with SIP proxy once get the SIP message.

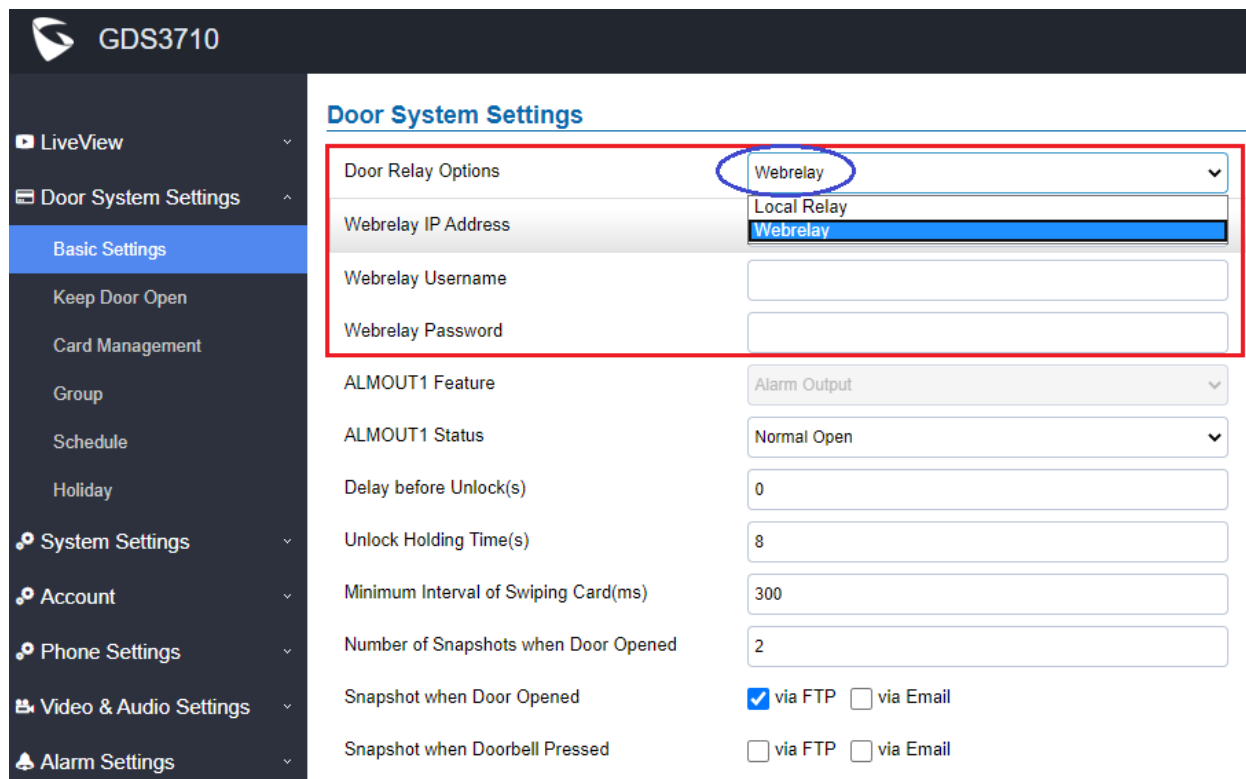
This feature is enabled by meeting the requirement from field. Lots of system administrators and integrators want this feature to upgrade firmware in controlled status, or reboot the device by specified time to improve the stability and reliability of the device.

This feature is very useful for enterprise customers. Users who use this feature need to understand the security risk involved to enable this feature.

OPEN DOOR VIA WEBRELAY

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

Basic Settings

Door Relay Options: **Webrelay** (selected)

Webrelay IP Address: **Local Relay** (selected)

Webrelay Username: **Webrelay**

Webrelay Password:

ALMOUT1 Feature: Alarm Output

ALMOUT1 Status: Normal Open

Delay before Unlock(s): 0

Unlock Holding Time(s): 8

Minimum Interval of Swiping Card(ms): 300

Number of Snapshots when Door Opened: 2

Snapshot when Door Opened: ☒ via FTP ☐ via Email

Snapshot when Doorbell Pressed: ☐ via FTP ☐ via Email

- **Functionality**

This feature enhancement is response to field request to integration with 3rd party web relay controller, to install the relay controller inside the build to enhance the security.

When log into the device, there is a new option called “Door Relay Options”. There are two choices in the pull-down selection: Local Relay, Webrelay.

- **Local Relay**

Local Relay is the GDS3710 controlling the relay. The strike is wired into the COM2 or COM1 port of the GDS3710 depending on 1 door or 2 door need to be controlled.

- **Webrelay**

When Webrelay is selected, customers need to continue configure the web relay IP address or domain name, together with credentials like Username and Password. When legal open door event happened, the configured web relay will get the communication from GDS3710, and will operate the strike to open door for the authenticated open door request.

In web relay mode, the strike is wired to the web relay controller device.

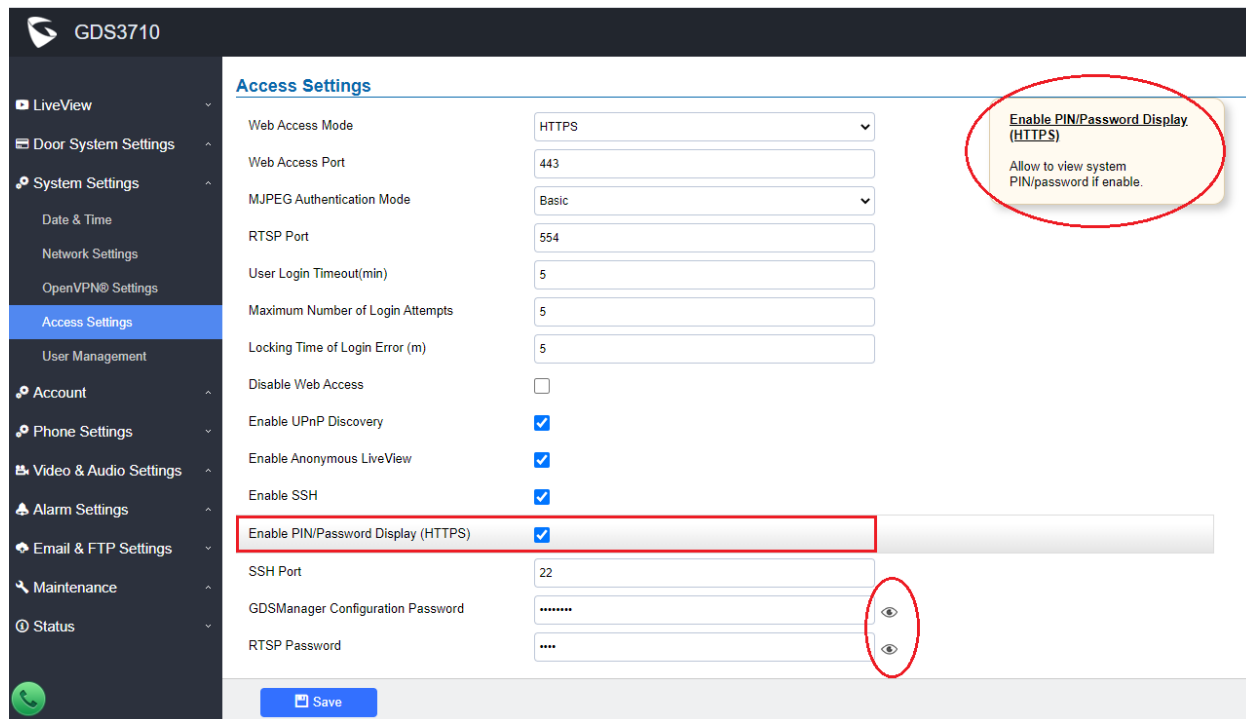
For more details about web relay, please refer to below URL to get more information:

<https://www.controlbyweb.com/webrelay/>

ENABLE PIN/PASSWORD DISPLAY

- Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



Enable PIN/Password Display (HTTPS)
 Allow to view system PIN/password if enable.

Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password	*****
RTSP Password	****

Save

- Functionality**

This feature is adding back upon request from field.

By default, this feature is disabled because ITSP or service provider do NOT want the PIN or password to be able to see by users.

But, some users, especially system administrators or system integrators want to see the password or PIN during the installation or device maintenance process. Now they can enable this feature, and “Click and Hole” the small “eye” icon on the right of the parameter field to see the previously hidden PIN or password, given them the convenience.

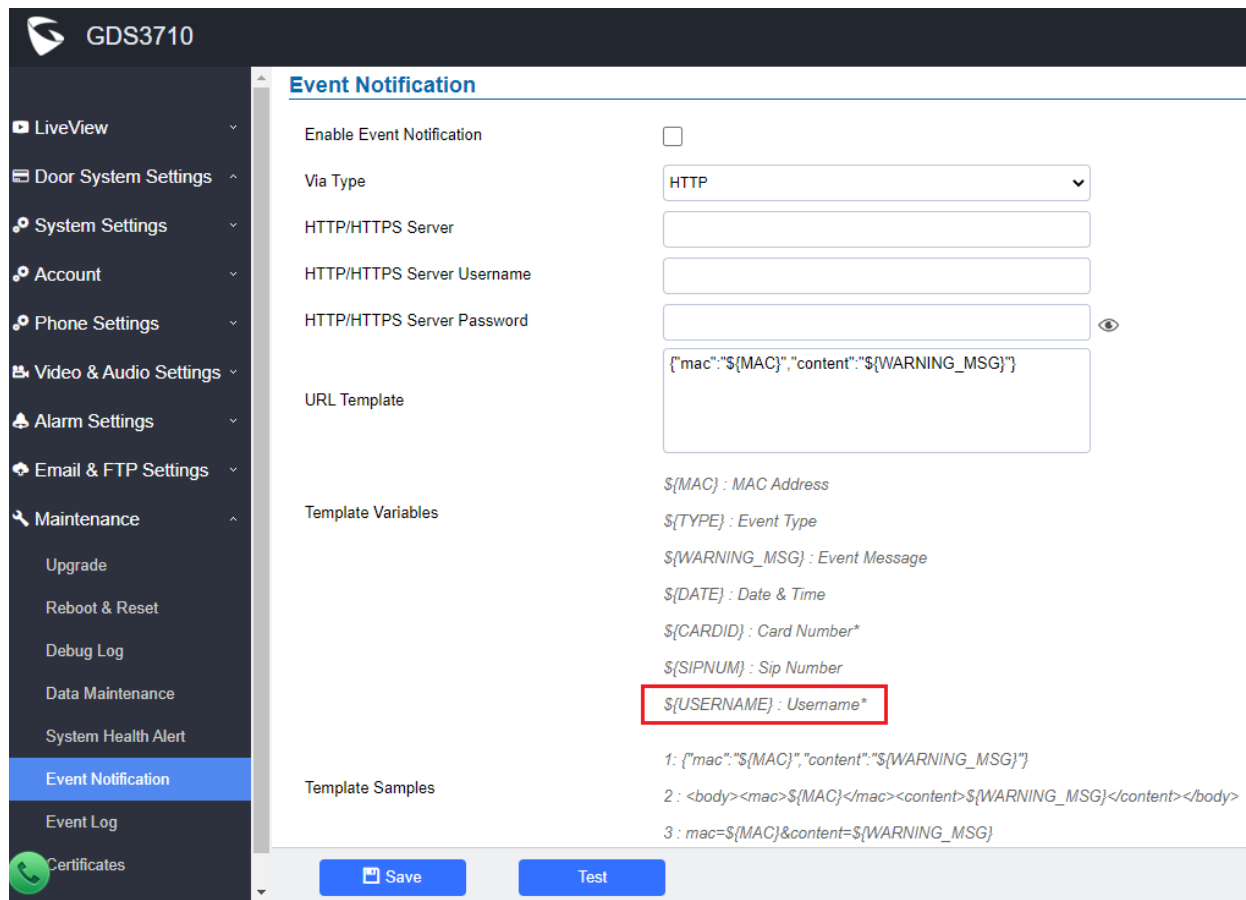
It is strongly recommended system administrator or system integrators to disable this feature once finished the installation and maintenance, for security purpose.

This is very useful for enterprise customers. This feature is implemented previously but removed due to ITSP customer’s request. But put back to meet the requirement of other customers like system administrator or system integrators, for their convenience.

SUPPORT “USERNAME” IN HTTP EVENT NOTIFICATION

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Notification:



The screenshot shows the GDS3710 web configuration interface. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Upgrade, Reboot & Reset, Debug Log, Data Maintenance, System Health Alert, Event Notification (highlighted), Event Log, and Certificates. The main content area is titled "Event Notification" and contains the following settings:

- Enable Event Notification:** A checkbox that is currently unchecked.
- Via Type:** A dropdown menu set to "HTTP".
- HTTP/HTTPS Server:** An empty text input field.
- HTTP/HTTPS Server Username:** An empty text input field.
- HTTP/HTTPS Server Password:** An empty text input field with a toggle icon on the right.
- URL Template:** A text area containing the template: `{"mac":"${MAC}","content":"${WARNING_MSG}"}`.
- Template Variables:** A list of variables:
 - `${MAC}` : MAC Address
 - `${TYPE}` : Event Type
 - `${WARNING_MSG}` : Event Message
 - `${DATE}` : Date & Time
 - `${CARDID}` : Card Number*
 - `${SIPNUM}` : Sip Number
 - `${USERNAME} : Username*` (highlighted with a red box)
- Template Samples:** Three examples of templates:
 - `1: {"mac":"${MAC}","content":"${WARNING_MSG}"}`
 - `2: <body><mac>${MAC}</mac><content>${WARNING_MSG}</content></body>`
 - `3: mac=${MAC}&content=${WARNING_MSG}`

At the bottom of the configuration area are two buttons: "Save" and "Test".

- **Functionality**

This feature is implemented based on request from customers in field.

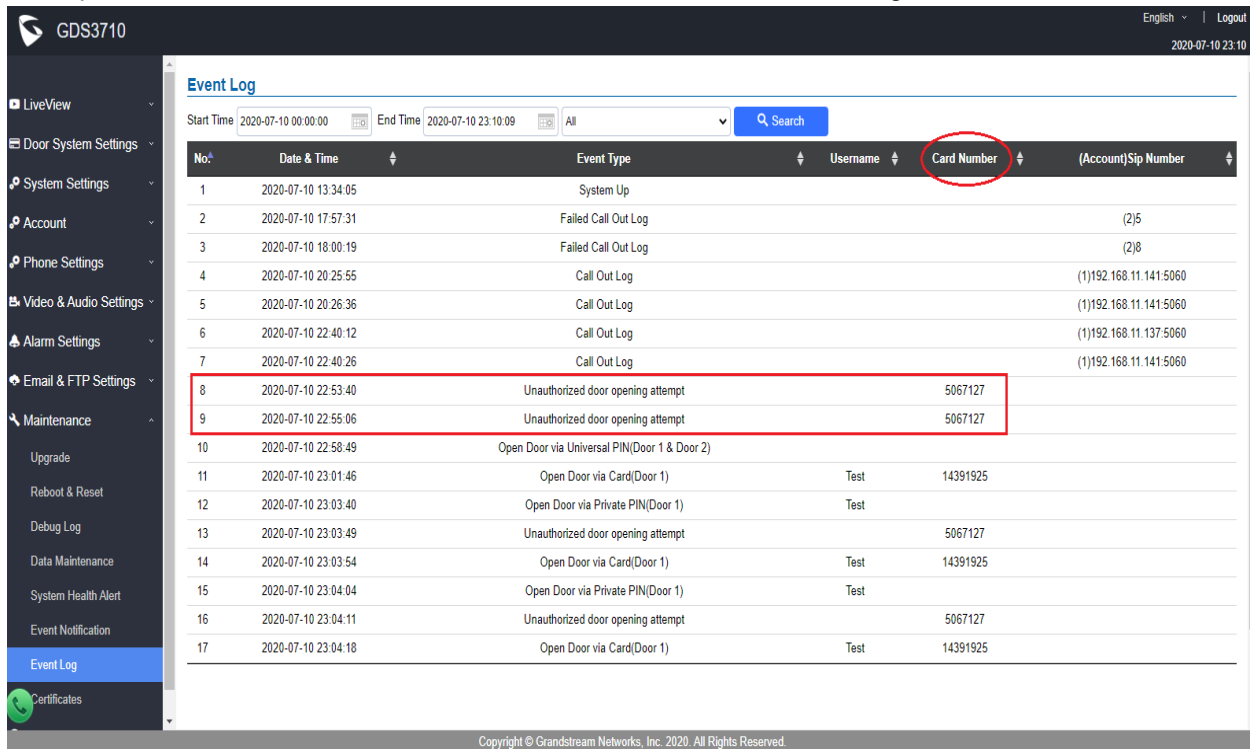
By adding “Username” in the Event Notification, system integrators can do 2nd stage development by using scripts to get report, understanding who and when and in which way to open the door.

This is very useful for enterprise customers who are doing 2nd stage development for daily HR or other tasks and get related report for the Access Control System.

LOG & DISPLAY “UNAUTHORIZED DOOR OPENING ATTEMPT” IN EVENT LOG

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Log:



No.	Date & Time	Event Type	Username	Card Number	(Account)Sip Number
1	2020-07-10 13:34:05	System Up			
2	2020-07-10 17:57:31	Failed Call Out Log			(2)5
3	2020-07-10 18:00:19	Failed Call Out Log			(2)8
4	2020-07-10 20:25:55	Call Out Log			(1)192.168.11.141:5060
5	2020-07-10 20:26:36	Call Out Log			(1)192.168.11.141:5060
6	2020-07-10 22:40:12	Call Out Log			(1)192.168.11.137:5060
7	2020-07-10 22:40:26	Call Out Log			(1)192.168.11.141:5060
8	2020-07-10 22:53:40	Unauthorized door opening attempt		5067127	
9	2020-07-10 22:55:06	Unauthorized door opening attempt		5067127	
10	2020-07-10 22:58:49	Open Door via Universal PIN(Door 1 & Door 2)			
11	2020-07-10 23:01:46	Open Door via Card(Door 1)	Test	14391925	
12	2020-07-10 23:03:40	Open Door via Private PIN(Door 1)	Test		
13	2020-07-10 23:03:49	Unauthorized door opening attempt		5067127	
14	2020-07-10 23:03:54	Open Door via Card(Door 1)	Test	14391925	
15	2020-07-10 23:04:04	Open Door via Private PIN(Door 1)	Test		
16	2020-07-10 23:04:11	Unauthorized door opening attempt		5067127	
17	2020-07-10 23:04:18	Open Door via Card(Door 1)	Test	14391925	

- **Functionality**

This feature is implemented to meet request of customers from field.

By logging the unauthorized card open door attempt, the system administrator can check the Event Log to see what illegal card number used trying to open door and take appropriate action.

This is enhancement to help system administrator or customers to get notification about the abnormal or illegal event from the log and enhance the administration, take appropriate action.

For detailed information, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.11

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

04/23/2020

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added configurable option to specify the cache time/refresh of DNS entries in Telefonica Mode.
- Added SIP Session Timer P Value for account 1/3/4 (only in Configuration File with P values)
- Revised SIP Account Name to Display Name
- Added support for Cisco QuoVadis/HydrantID CA

BUG FIX

- Fixed device received HTTP 302 then redirect to HTTPS failed to download the config file.
- Fixed device reboot due to keypad or RFID scanner mal-function error.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call sometimes.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- GDS3710 as Callee will not do stream negotiation.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P4208	Value: 1-1440. Phone_Settings.Phone_Settings.DNS_Cache_Expiration_Time
P28160	Value: 0-1440. Phone_Settings.Phone_Settings.DNS_Cache_Duration
P2395	Value: 0/1, 0:Disable 1:Enable. Account.Account_1.SessionTimer
P2595	Value: 0/1, 0:Disable 1:Enable. Account.Account_3.SessionTimer
P2695	Value: 0/1, 0:Disable 1:Enable. Account.Account_4.SessionTimer

NEW HTTP API:

- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P4208=<value>
- GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
- SET:[http|https]://<servername>/goform/config?cmd=set&P28160=<value>

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

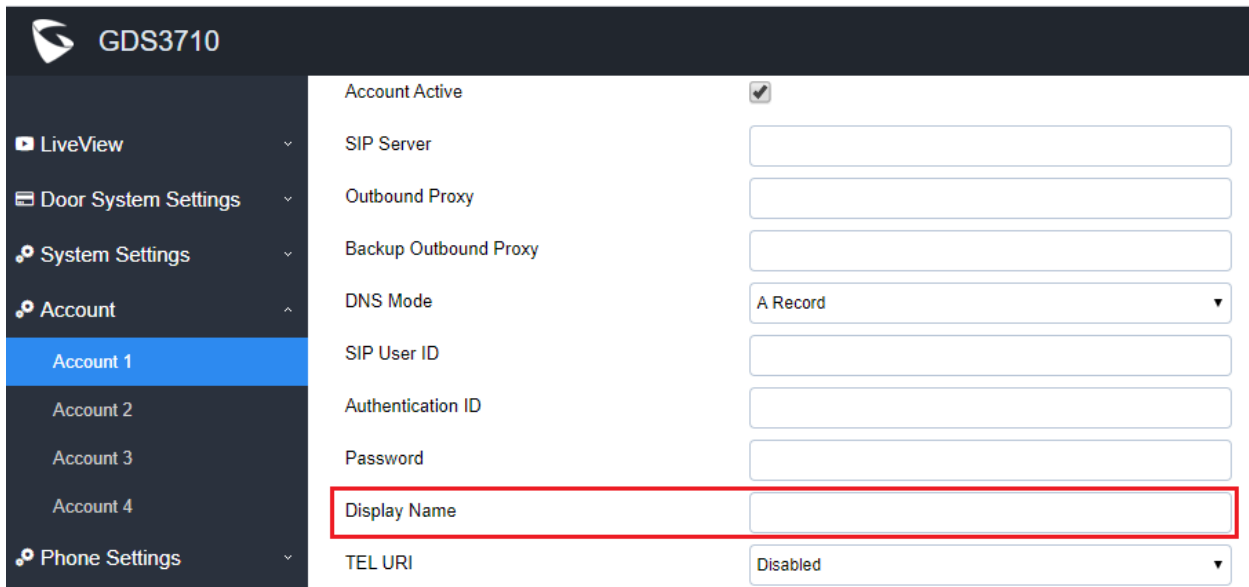
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

REVISED SIP ACCOUNT NAME TO DISPLAY NAME

- **Web Configuration**

This option can be found under device web UI → Account → Account X:



GDS3710	
Account Active	<input checked="" type="checkbox"/>
SIP Server	<input type="text"/>
Outbound Proxy	<input type="text"/>
Backup Outbound Proxy	<input type="text"/>
DNS Mode	A Record ▼
SIP User ID	<input type="text"/>
Authentication ID	<input type="text"/>
Password	<input type="text"/>
Display Name	<input type="text"/>
TEL URI	Disabled ▼

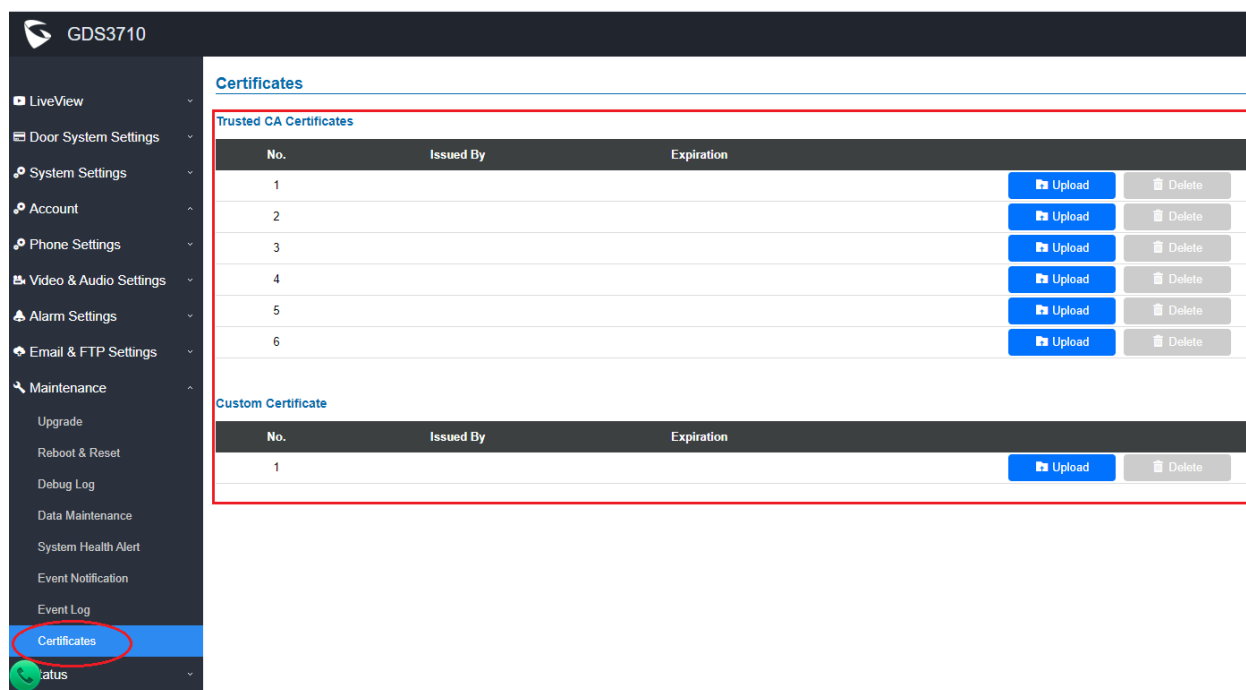
- **Functionality**

This feature enhancement is to allow user to input display name to be illustrated in far side SIP device (if having LCD display or similar hardware) so user will know what extension or device connected in SIP calling, to increase the usability.

SUPPORT FOR CISCO QUOVADIS/HYDRANTID CA

- Web Configuration**

This option can be found as seen below under device web UI → Maintenance → Certificates:



GDS3710

Certificates

Trusted CA Certificates

No.	Issued By	Expiration	Upload	Delete
1			Upload	Delete
2			Upload	Delete
3			Upload	Delete
4			Upload	Delete
5			Upload	Delete
6			Upload	Delete

Custom Certificate

No.	Issued By	Expiration	Upload	Delete
1			Upload	Delete

- Functionality**

This allows user to upload the Cisco QuoVadis/HydrantID CA.

For detailed information, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.10

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

03/23/2020

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Increased maximum unlock holding time to 1800 seconds (30 minutes).
- Added support for anonymous MJPEG stream viewing for each of the three streams.
- Added option to have dedicated password (username still admin) for RTSP stream and GDSManager.

BUG FIX

- Fixed not playing audio or IVR from server when calling a non-existent number.
- Fixed reboot loop when certain P values in the configuration file contains null value.
- Fixed call dropped at 2nd number in the doorbell list.
- Fixed busy tone played when calling 2nd number in the doorbell list.
- Fixed device connects when receiving 183 ringing from GXV33xx and GXV32xx.
- Fixed device not response to PIN input when account lost registration.
- Fixed event notification will be sent when disabled or non-exist card be swiped.
- Fixed unified password can still open door at non-scheduled time via Wiegand interface.
- Fixed GDSManager Configuration password and RTSP password cannot be set to null.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call sometimes.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- GDS3710 as Callee will not do stream negotiation.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P15512	RSTP Password, String & MIN length is 1, MAX length is 32
--------	---

MODIFIED P-VALUE

P14101	Updated "Unlock Holding Time(s)", new value range: 1 – 1800 (second, integer value)
--------	---

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

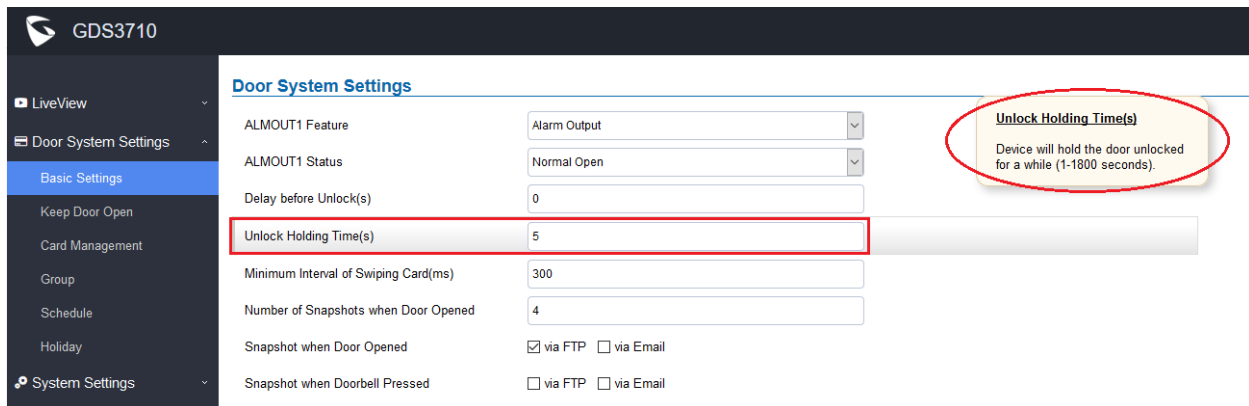
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

INCREASE UNLOCK HOLDING TIME

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

- ALMOUT1 Feature: Alarm Output
- ALMOUT1 Status: Normal Open
- Delay before Unlock(s): 0
- Unlock Holding Time(s): 5**
- Minimum Interval of Swiping Card(ms): 300
- Number of Snapshots when Door Opened: 4
- Snapshot when Door Opened: ☒ via FTP ☐ via Email
- Snapshot when Doorbell Pressed: ☐ via FTP ☐ via Email

Unlock Holding Time(s)
 Device will hold the door unlocked for a while (1-1800 seconds).

- **Functionality**

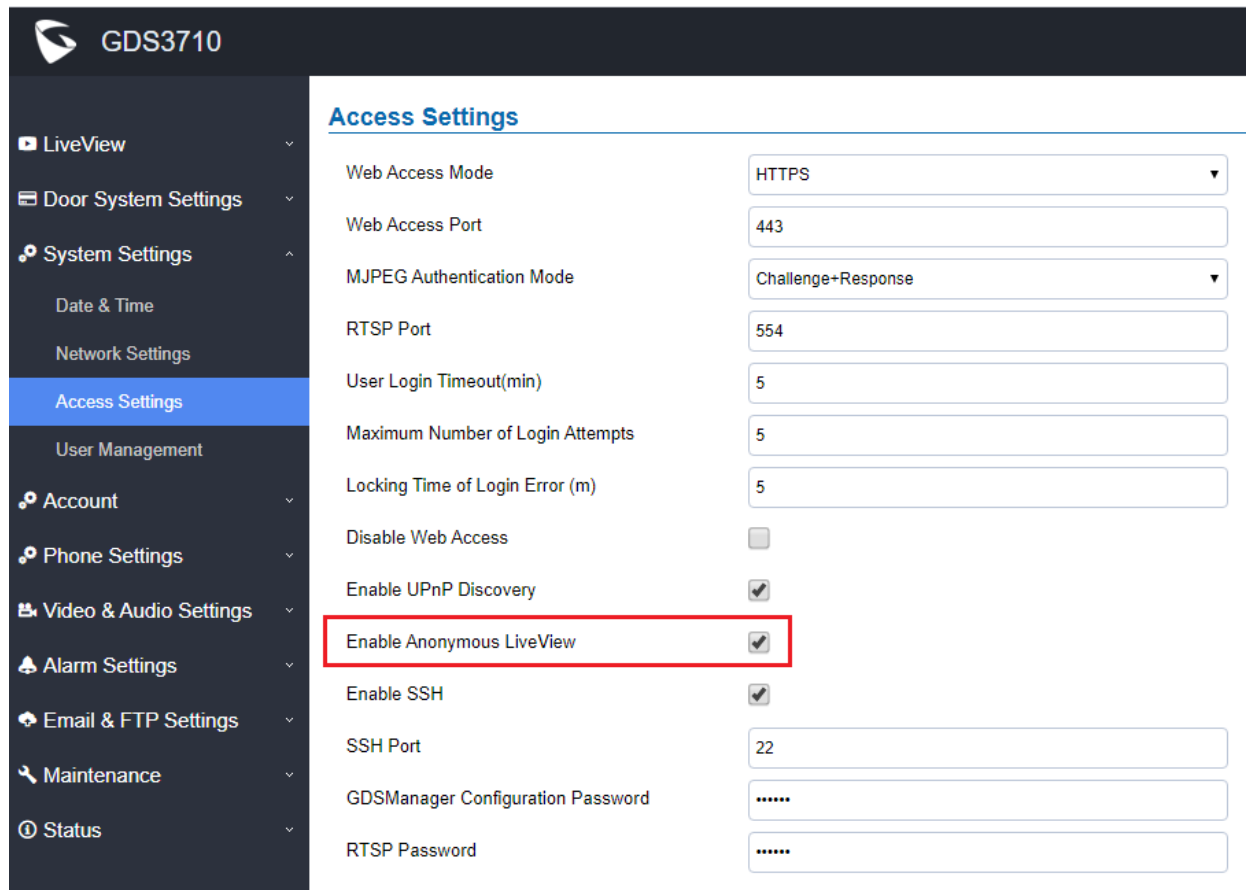
This feature enhancement is provided based on field feedback from customers. Some customer's application scene requires the door holding more time as open status, this enhancement is for them.

The increased unlock holding time is 1800 seconds, or 30 minutes.

ANONYMOUS MJPEG STREAM VIEWING FOR EACH STREAM

- Web Configuration**

This option can be found under device web UI → System Settings → Access Settings: click to check and “Enable Anonymous LiveView” as seen below:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, Access Settings (highlighted), User Management, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Access Settings' and contains the following configuration items:

Setting	Value
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password
RTSP Password

- Functionality**

This is a major enhancement for GDS3710 based on field feedback from customers. A lot of customers using MJPEG stream for in house re-development therefore do need the convenience more than the security. When above **Anonymous MJPEG LiveView** feature enabled, customer can use following URLs to retrieve the related MJPEG streams:

http(s)://IP:Port/anonymous/jpeg/stream=X (X= 0, 1, 2, or default 3)

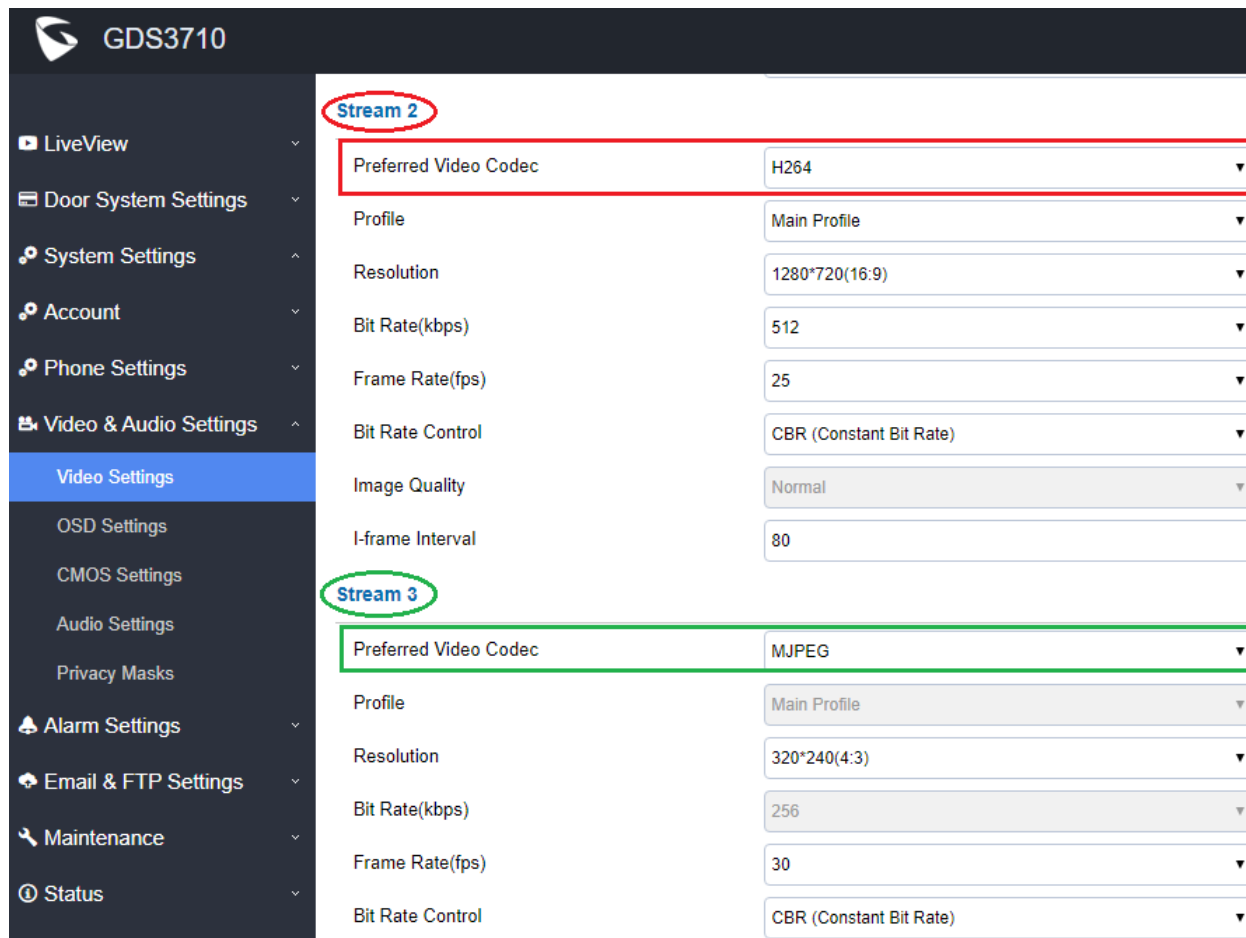
For example:

<https://192.168.1.128/anonymous/jpeg/stream=3>

NOTE:

- Except default value **3**, the stream 0, 1, 2 mapped to the stream 1, 2, 3 in the “Video Setting” page.
- Unless using default value 3, all other values require to choose “MJPEG” in the “Preferred Video Codec” in the “Preferred Video Codec”

For example, in this setting page:



Stream 2	
Preferred Video Codec	H264
Profile	Main Profile
Resolution	1280*720(16:9)
Bit Rate(kbps)	512
Frame Rate(fps)	25
Bit Rate Control	CBR (Constant Bit Rate)
Image Quality	Normal
I-frame Interval	80

Stream 3	
Preferred Video Codec	MJPEG
Profile	Main Profile
Resolution	320*240(4:3)
Bit Rate(kbps)	256
Frame Rate(fps)	30
Bit Rate Control	CBR (Constant Bit Rate)

Stream 2 (X=1) is H.264 and stream 3 (X=2) is MJPEG, therefore:

<https://192.168.1.128/anonymous/jpeg/stream=2>

would show the MJPEG live stream using stream3 resolution 320x240 (QVGA).

But if using:

<https://192.168.1.128/anonymous/jpeg/stream=1>

would get error message like below because stream 2 (X=1) is H.264, not MJPEG:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Configuration>
  <ResCode>-1</ResCode>
  <RetMsg>stream 1 is not MJPEG</RetMsg>
</Configuration>
```


- Because this feature is designed for in-house development, therefore the number of live MJPEG streams are limited. If below message shown, this means limitation reached.

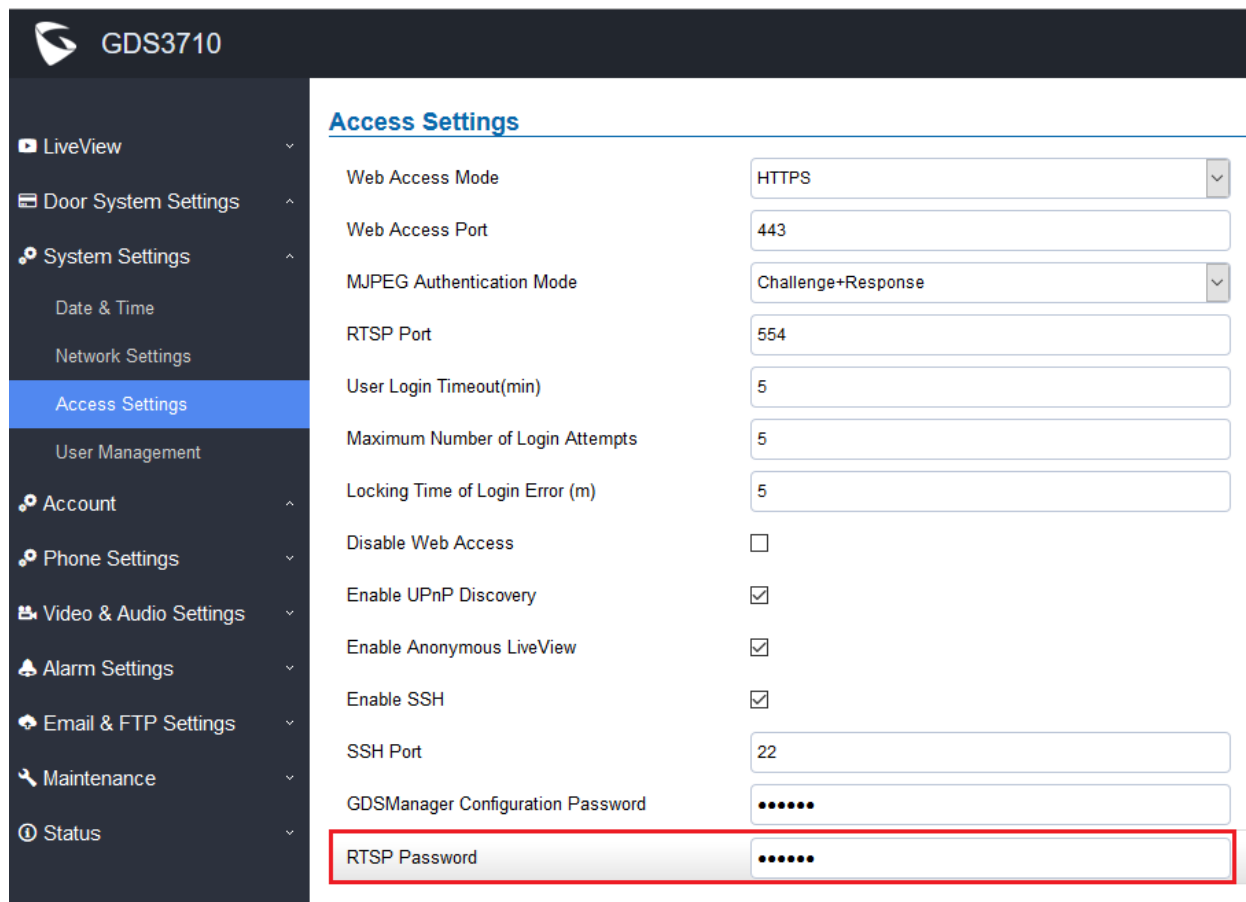
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<Configuration>  
  <ResCode>-1</ResCode>  
  <RetMsg>It is reached the maximum number</RetMsg>  
</Configuration>
```

DEDICATED PASSWORD FOR RTSP STREAM

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, Access Settings (selected), User Management, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Access Settings' and contains the following configuration items:

Setting	Value
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password
RTSP Password

The 'RTSP Password' field is highlighted with a red rectangular box.

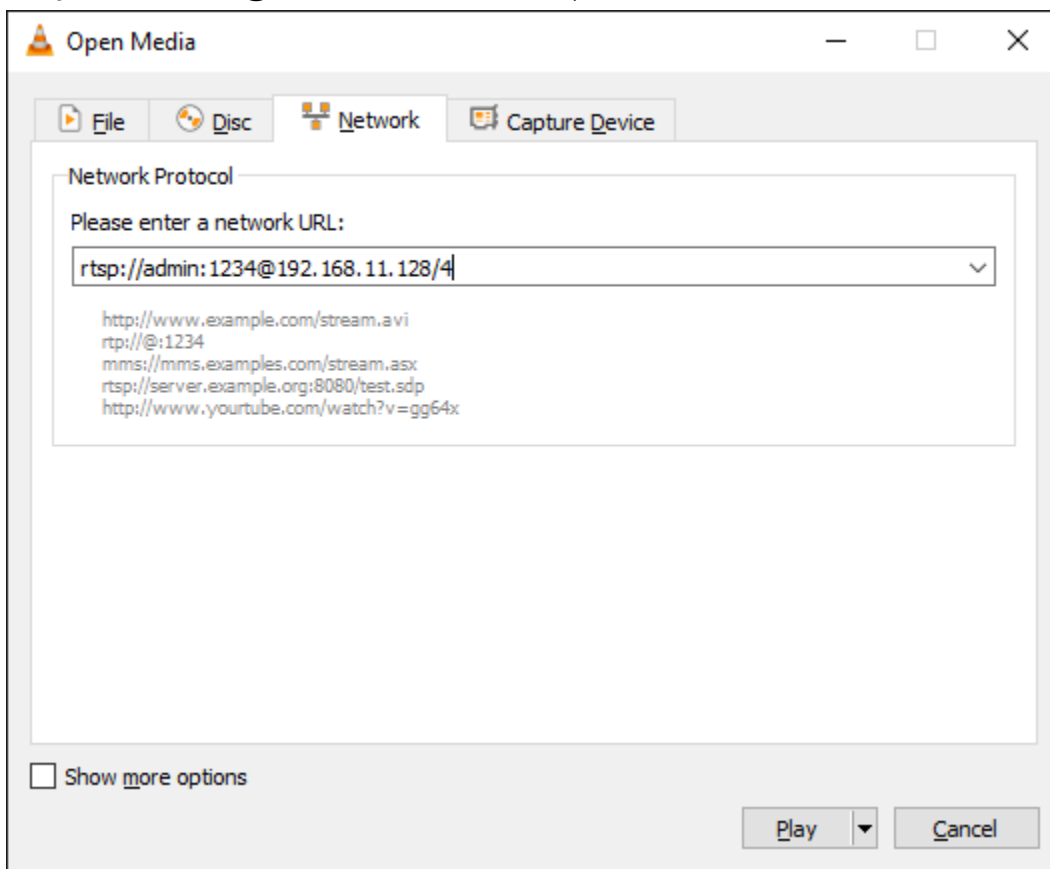
- **Functionality**

This feature enhancement is based on field feedback from customers. Customer request **NOT using admin password** to view the RTSP video stream via 3rd party applications like VLC Player or own development Scripts.

Now customer can still use amin as username, but NOT use amin password and configure another RTSP password to view the live stream via own scripts or 3rd paryt application like VLC Media Player.

For example, using VLC Media Player, if configure the RTSP password to be “1234” in GDS3710, then using following command can get the video stream:

rtsp://admin:1234@192.168.11.128/4 (here it shows the 2nd stream as “4” used)



FORMAT:

RTSP://admin:rtsp_password@IP_GDS3710:Port/X

(X = 0, 4, 8 correspondent to Stream 1, 2, 3)

The selected live video stream with audio will play out with some delay based on the computer processing power and network conditions.

NOTE:

- Please make sure the environment is secure before using this feature.
- Please reminder user the privacy when using this feature.

For detailed information, please refer to User Manual and Resource Center:

- **GDS3710 User Manual:**
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- **HOW-TO Guide**
<http://www.grandstream.com/support/resources/?title=GDS3710>
- **HTTP API** documentation can be downloaded from here:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.7.8

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

12/6/2019

SUMMARY OF UPDATE

The main purpose of this release is enhancement and minor fix found in previous build 1.0.7.7

Factory Reset is recommended once upgraded to this version due to major feature enhancement. If upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Enhanced the failover mechanism based on DNS SRV (mainly for ITSP customers)
- Include Holidays on Keep Door Open Schedule for Door 2

BUG FIX

- Fixed the input password error alarm too short and should be the same with other alarms.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call sometimes.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- GDS3710 as Callee will not do stream negotiation.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

FIRMWARE VERSION 1.0.7.7

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

10/31/2019

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement. Main security enhancement added to alarm the tampering of GDS37xx.

Factory Reset is recommended once upgraded to this version due to major feature enhancement. If upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added support for failover mechanism based on DNS SRV
- Added siren alarming function when door opened abnormally (special wiring required)
- Optimized debug output information
- Added option to only accept incoming SIP call from Proxy/Server
- Added including Holidays at Keep Door Open schedule
- Added reset/restore factory default password via special keypad combination operations

BUG FIX

- Fixed device sending out IPv6 packets.
- Fixed impossible to call virtual number at IP Peering (w/o SIP server) between GDS and IP phones.
- Fixed Speaker not playing audio message from server when calling a non-exist number
- Fixed device still send RTCP packets when RTCP is set to disable
- Fixed using G.729 device cannot communicate with DP7xx and GXP21xx SIP Phones
- Fixed device will not request to upgrade and download the configuration file if using TFTP mode with format like: IP_Address:Port/Path or IP_Address/Path

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call sometimes.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- GDS3710 as Callee will not do stream negotiation.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P15508	Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_1_Abnormal_Door_Control_Options (value: 0/1)
P15509	Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_2_Abnormal_Door_Control_Options (value: 0/1)

MODIFIED P-VALUE

P14320	Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_1 (value: 0/1/2/3)
P14325	Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_2 (value: 0/1/2/3)

NEW HTTP API

- P15508 -- Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_1_Abnormal_Door_Control_Options
(value: 0/1)

GET: *http://ip:port/goform/config?cmd=get&type=event*

SET: *http://ip:port/goform/config?cmd=set&P15508=<value> (value: 0/1)*

- P15509 -- Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_1_Abnormal_Door_Control_Options
(value: 0/1)

GET: *http://ip:port/goform/config?cmd=get&type=event*

SET: *http://ip:port/goform/config?cmd=set&P15509=<value> (value: 0/1)*

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

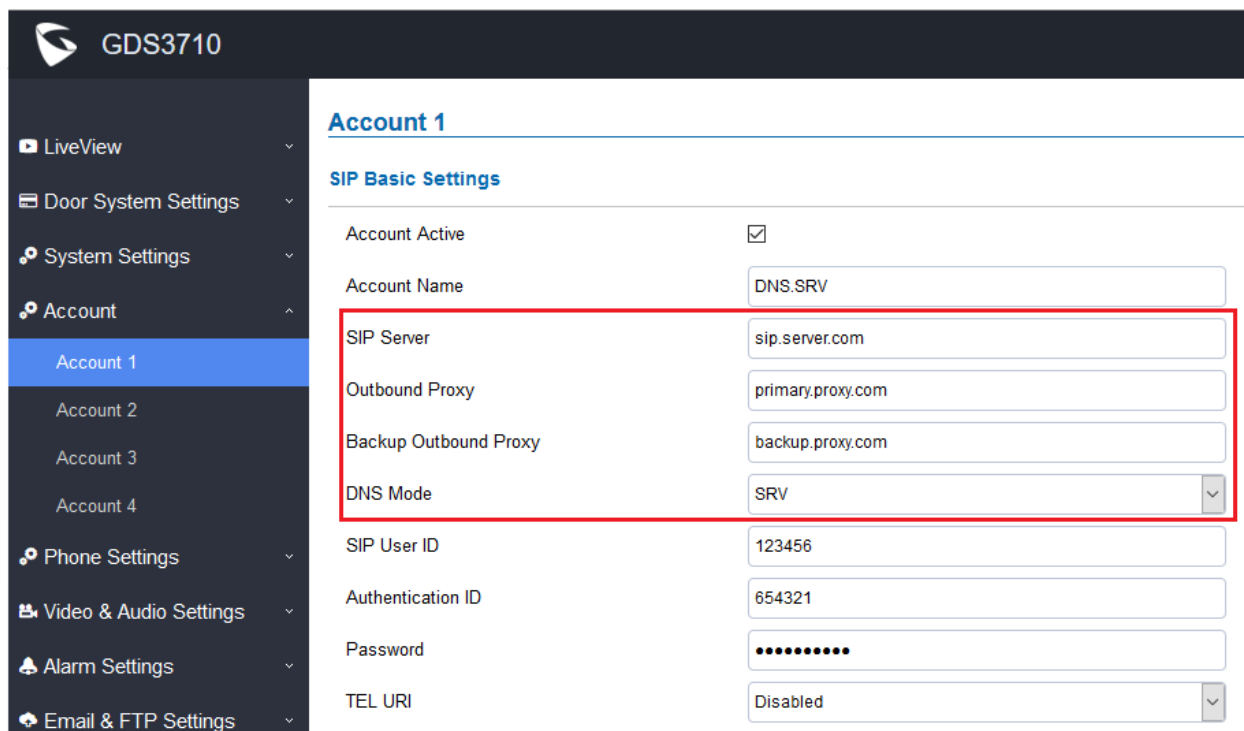
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

SUPPORT FAILOVER MECHANISM ON DNS SRV

- **Web Configuration**


This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



The screenshot shows the web configuration interface for a Grandstream GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Account 1 (selected), Account 2, Account 3, Account 4, Phone Settings, Video & Audio Settings, Alarm Settings, and Email & FTP Settings. The main content area is titled 'Account 1' and 'SIP Basic Settings'. It contains several configuration fields: Account Active (checked), Account Name (DNS.SRV), SIP Server (sip.server.com), Outbound Proxy (primary.proxy.com), Backup Outbound Proxy (backup.proxy.com), DNS Mode (SRV), SIP User ID (123456), Authentication ID (654321), Password (masked with dots), and TEL URI (Disabled). A red rectangular box highlights the SIP Server, Outbound Proxy, Backup Outbound Proxy, and DNS Mode fields.

- **Functionality**

This is a major feature enhancement for Service Provider, via DNS SRV (mainly for BroadSoft certified soft switch for major Internet Telephony service providers). Service providers can use this feature to provide smooth service transition backup in case service down.


GDS3710

- LiveView ▼
- Door System Settings ▼
- System Settings ▼
- Account ▲
 - Account 1
 - Account 2
 - Account 3
 - Account 4
- Phone Settings ▼
- Video & Audio Settings ▼
- Alarm Settings ▼
- Email & FTP Settings ▼
- Maintenance ▼
- Status ▼

SIP Advanced Settings

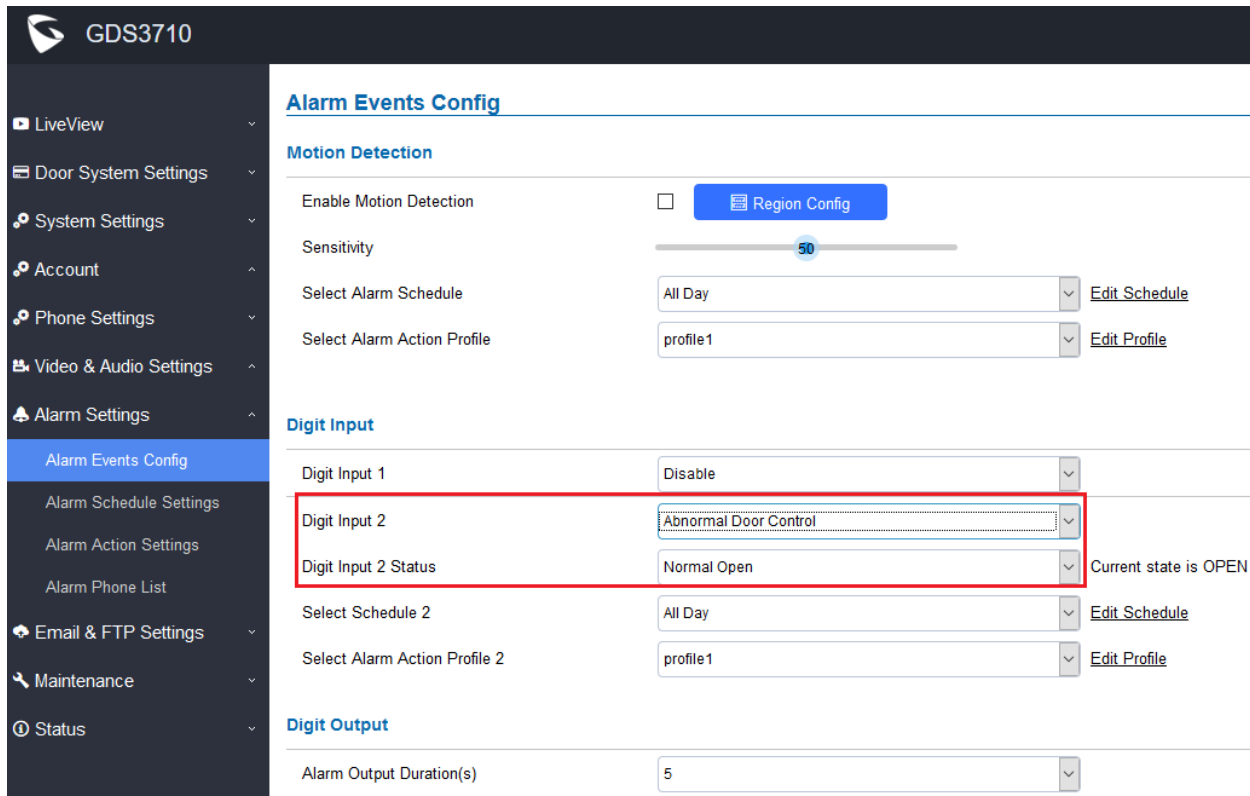
Registration Expiration(m)	<input type="text" value="60"/>
Re-register before Expiration(s)	<input type="text" value="0"/>
Local SIP Port	<input type="text" value="5060"/>
SIP Transport	<input type="text" value="UDP"/>
Stream	<input type="text" value="Stream 2"/>
Enable DTMF	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
DTMF Payload Type	<input type="text" value="101"/>
Unregister On Reboot	<input checked="" type="checkbox"/>
NAT Traversal	<input type="text" value="No"/>
Enable SRTP	<input type="text" value="Disabled"/>
Special Feature	<input type="text" value="Telefonica Spain"/> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Standard Broadsoft Telefonica Spain </div>
Outbound Proxy Mode	<input type="text" value="Standard"/>
Enable RTCP	<input type="text" value="Broadsoft"/>
H.264 Payload Type	<input type="text" value="99"/>

In the device web UI → Account X (X=1, 2, 3, and 4) → SIP Advanced Settings → Special Feature:
 There is a new feature specially designed for Telefonica Spain to match the service provided by Telefonica to their customers. Just need to enable this feature via either WebUI or Provisioning.

SIREN ALARMING WHEN DOOR OPENED ABNORMALLY (SPECIAL WIRING REQUIRED)

- **Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Events Config → Digit Input:



GDS3710

Alarm Events Config

Motion Detection

Enable Motion Detection ☐ [Region Config](#)

Sensitivity

Select Alarm Schedule [Edit Schedule](#)

Select Alarm Action Profile [Edit Profile](#)

Digit Input

Digit Input 1

Digit Input 2

Digit Input 2 Status Current state is OPEN

Select Schedule 2 [Edit Schedule](#)

Select Alarm Action Profile 2 [Edit Profile](#)

Digit Output

Alarm Output Duration(s)

- **Functionality**

This is a major security enhancement for GDS37xx when device be tampered to open the door abnormally.

When this feature enabled (special wiring required, see below wiring diagram), abnormal open door will be detected by DI port (Alarm_In2 or IN2 in below diagram showed) if wired correctly (connecting the COMx port to DIx port) therefore trigger siren alarm. Once abnormal open door alarm triggered, the siren will sound non-stop, until manually override by related person.

There are several ways to stop and disable the alarm:

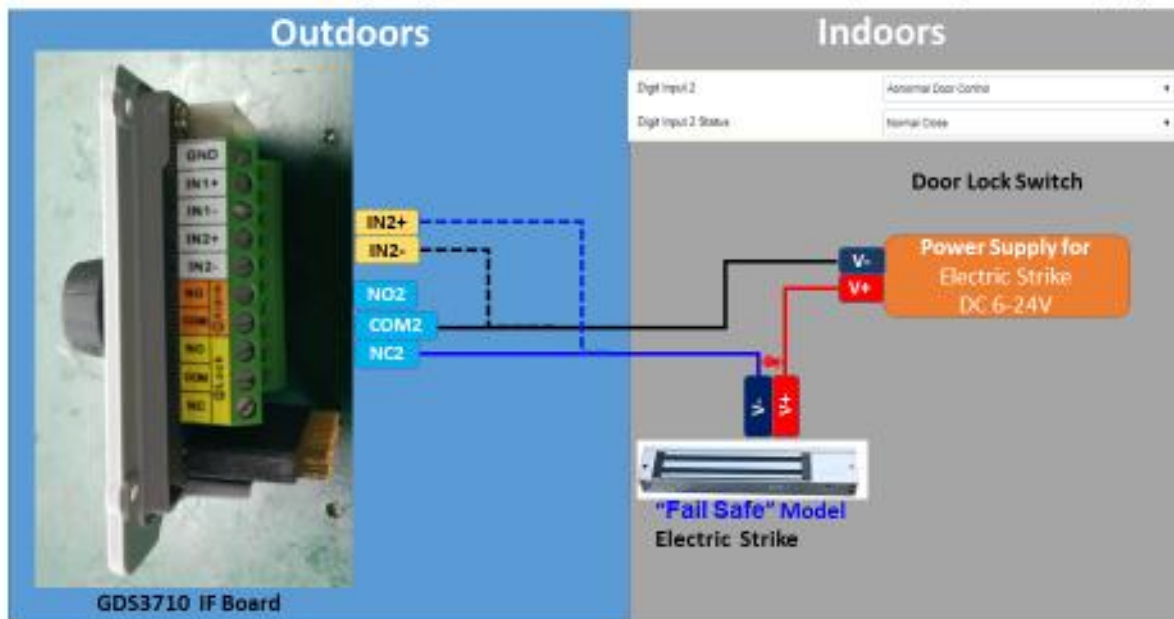
- 1) Power cycle the GDS37xx
- 2) Pick up the Alarm Phone Call (if configured)
- 3) Open Door using PIN (either public PIN or private PIN)

Once alarm triggered, the GDS3710 will **take snapshots** when the abnormal open door happened, email and upload the snapshots to FTP or Central Server (when configured); call the configured alarm SIP phone, send the alarm output (if connected). User will only be able to disable the siren using the 3 methods mentioned above.

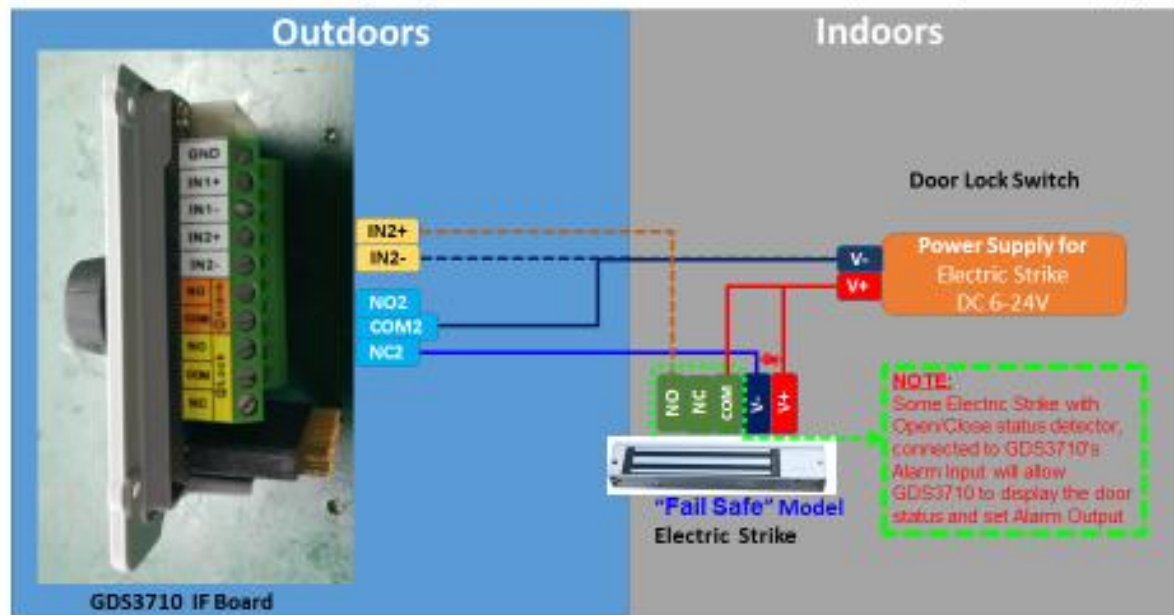
Detailed action information please refer to GDS37xx User Manual, "Alarm Action Settings" configuration.

Below are some diagrams showing the correct wiring to enable this new security enhancement feature:

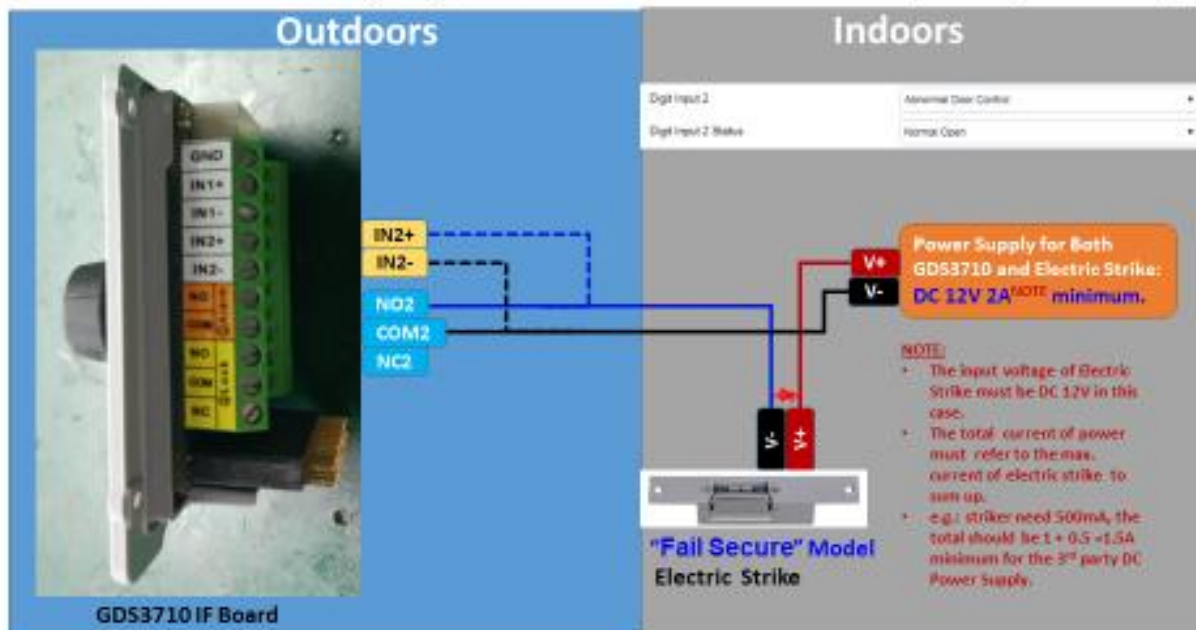
GDS3710 Connection & Wiring Diagrams ---- "Fail Safe" Electric Strike, 3rd Party Power Supply



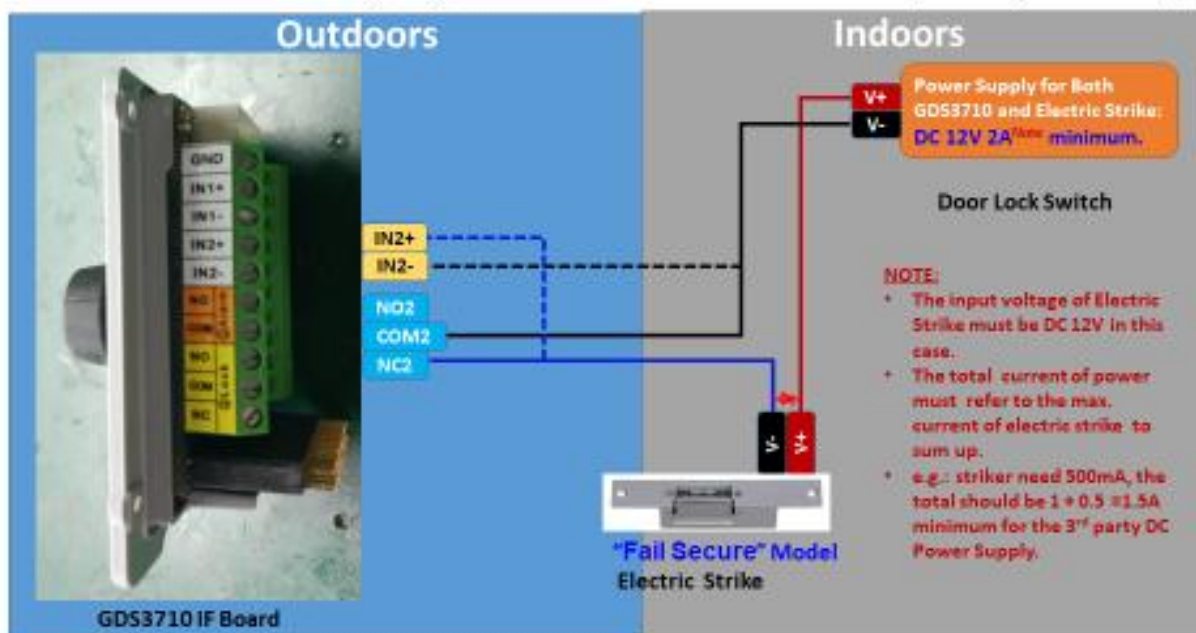
GDS3710 Connection & Wiring Diagrams ---- "Fail Safe" Electric Strike, 3rd Party Power Supply



GDS3710 Connection & Wiring Diagrams ---- "Fail Secure" Electric Strike, 3rd Party Power Supply

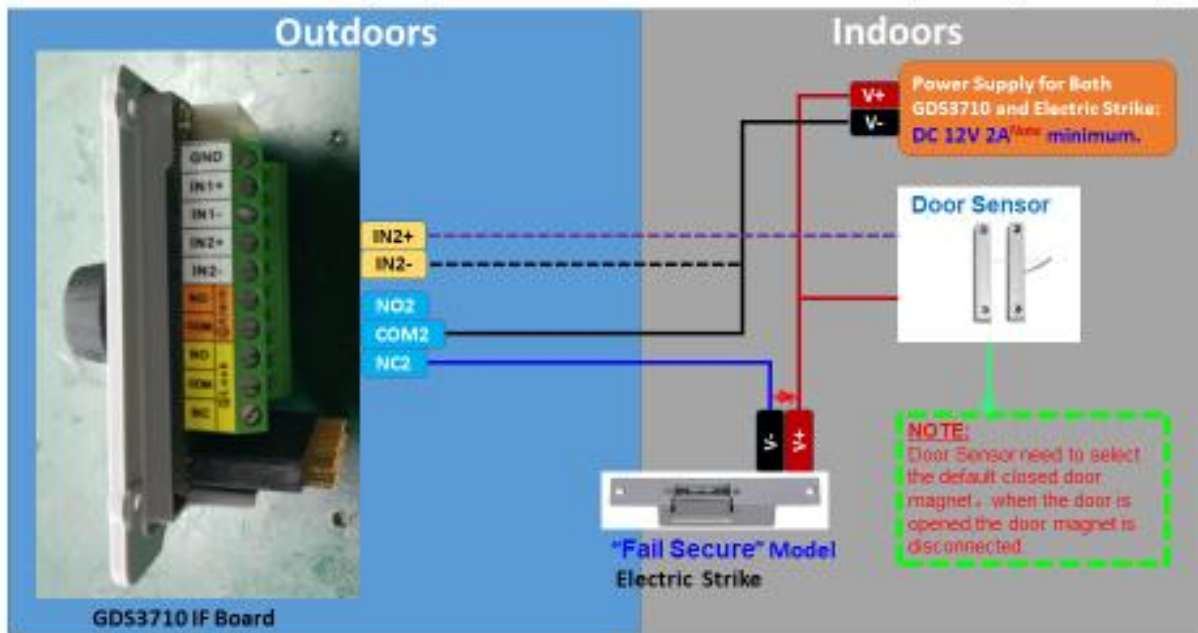


GDS3710 Connection & Wiring Diagrams ---- "Fail Secure" Electric Strike, 3rd Party Power Supply



If 3rd party door sensor installed, customer could wire the door sensor signal directly into the DI port (DI2 in below example) to trigger the alarm if the door opened abnormal. See below diagram:

GDS3710 Connection & Wiring Diagrams ---- "Fail Secure" Electric Strike, 3rd Party Power Supply



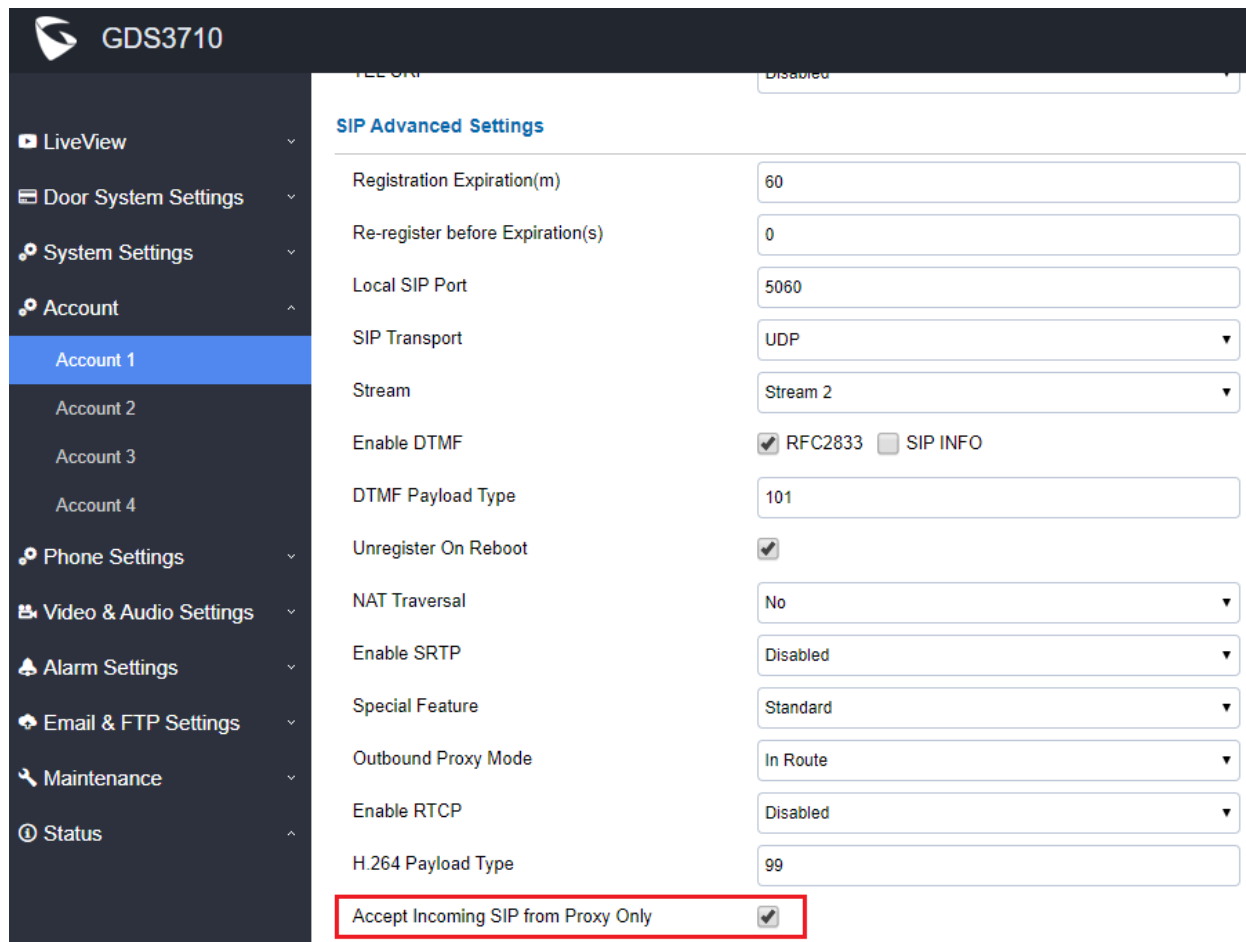
For detailed information, please refer to User Manual and Resource Center:

- GDS3710 User Manual:
http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf
- HOW-TO Guide
<http://www.grandstream.com/support/resources/?title=GDS3710>

ONLY ACCEPT INCOMING SIP CALL FROM PROXY/SERVER

- **Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



GDS3710

LiveView

Door System Settings

System Settings

Account

Account 1

Account 2

Account 3

Account 4

Phone Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status

SIP Advanced Settings

Registration Expiration(m) 60

Re-register before Expiration(s) 0

Local SIP Port 5060

SIP Transport UDP

Stream Stream 2

Enable DTMF ☒ RFC2833 ☐ SIP INFO

DTMF Payload Type 101

Unregister On Reboot ☒

NAT Traversal No

Enable SRTP Disabled

Special Feature Standard

Outbound Proxy Mode In Route

Enable RTCP Disabled

H.264 Payload Type 99

Accept Incoming SIP from Proxy Only ☒

- **Functionality**

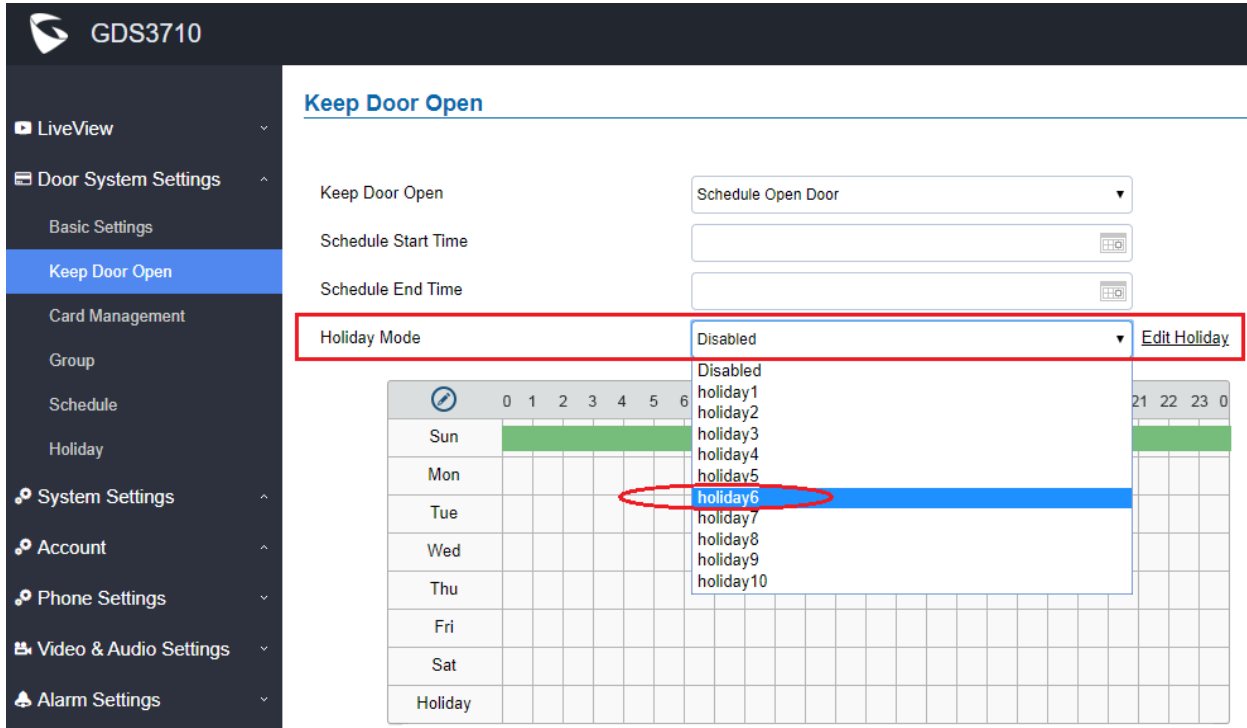
This feature is implemented based on field customer feedback.

This is also security enhancement for SIP phone calls. When this feature enabled, the GDS37xx will ONLY accept calls from authorized proxy/server. This will prevent SIP hacking or 'ghost' calls.

SUPPORT HOLIDAYS IN KEEP DOOR OPEN SCHEDULE

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Keep Door Open:



GDS3710

Keep Door Open

Keep Door Open: Schedule Open Door

Schedule Start Time:

Schedule End Time:

Holiday Mode: Disabled [Edit Holiday](#)

0 1 2 3 4 5 6 21 22 23 0

	0	1	2	3	4	5	6
Sun							
Mon							
Tue							
Wed							
Thu							
Fri							
Sat							
Holiday							

Disabled
 holiday1
 holiday2
 holiday3
 holiday4
 holiday5
holiday6
 holiday7
 holiday8
 holiday9
 holiday10

- **Functionality**

This feature is implemented based on field customer feedback either.

When configure Keep Door Open schedule, customers now can also specify which Holiday Schedule to be included into the Keep Door Open schedule, therefore make the GDS37xx more user friendly in such application scene configuration.

RESET FACTORY PASSWORD VIA SPECIAL KEY COMBINATION OPERATION

- **Functionality**

This is a new enhancement feature requested by ITSP service providers as well as lots of system integrators from Forum. This feature allows customers to reset the device administrator password to factory default via keypad operation through some special key combination.

When performing this operation, ONLY password will be reset back to factory default. All other setting or parameters will NOT be changed and will remain the same. This feature is specially designed for field engineers or technicians when dispatched in field but for some reason the administrator password is not available therefore not able to access the GDS37xx device to do the related maintenance.

Here are the steps to do such password reset operation via keypad:

Encoding Rules:

- Alphabet A – Z mapping to digit 1 – 26 respectively, no difference in lower or up case.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

NOTE:

- Suggest decoding the MAC and Password and write on paper before doing the reset operation.

Prerequisite condition:

- 1) MAC address of the GDS37xx (check the sticker at back of the device)
- 2) Default password of the GDS37xx (check the sticker at the back of the device)
- 3) Correct decoding the last 6 MAC address into digits (refer to encoding rule)
- 4) Correct decoding the default password into digits (refer to encoding rule)
- 5) Finish keypad input within 1 minute

Operation Steps:

- 1) When device is idle, input the special keypad combination with format: *****last_6_MAC**#**
- 2) Device will reach restore mode after correct digits in Step 1) entered. The backlight of keypad will flash quickly to tell operator the device is now in password reset/restore mode.
- 3) Operator will enter the correct decoded default password ending with # with format:
default_password_code# via the keypad within 60 seconds.
- 4) If wrong code combination entered, the GDS37xx will beep with error sound (three short beeps) then exit the password reset mode, and the backlight will stop flashing.
- 5) If the correct default password decode entered within 60 seconds, GDS37xx will play a long beep sound (advising correct operation), the device will reboot itself automatically.
- 6) If keypad entry time out (not finish the input within 60 seconds), the device will exit this password reset mode automatically and stop the backlight flashing.

After successful password reset, operator will then be able to log into the GDS37xx webUI with default password, all the configuration inside the device will be the same and will NOT be changed.

For example:

Decoding the string into digits and write to paper before doing the operation:

<i>Device with last 6 MAC address:</i>	33DDDD
<i>Decoding the last 6 MAC to digits would be:</i>	334444
<i>Default password is:</i>	xwpxz6AA
<i>Decoding the default password to digits would be:</i>	2423162426611

- 1) Enter *****334444**#** via keypad, get into the password reset mode, the keypad backlight will flash quickly.
- 2) Within 60 seconds, enter **2423162426611#**, the device will play one long beep then reboot itself.
- 3) Wait the device finishing boot up, log in the webUI using the default password, **xwpxz6AA**

FIRMWARE VERSION 1.0.7.4

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

07/23/2019

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and features enhancement. Main enhancement like added Service Provider (e.g.: Telefonica) feature support, etc.

Factory Reset is recommended once upgraded to this version due to major feature enhancement. If upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

This firmware would not be able to downgrade to version 1.0.3.X or below.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added support for failover mechanism based on DNS SRV.
- Added ability to separate webUI credentials from GDSManager credentials (via added P values).
- Added G.729 audio codec support.
- Optimized the DI alarm mechanism (reset required to enjoy this optimization feature).
- Added ability to enable multiple audio codecs simultaneously and specify priority of codecs.
- Added “Schedule” for firmware upgrade and provisioning.
- Added support for Voice Frame per TX in the audio settings.
- Added option to keep keypad blue light ON/OFF based on schedule.
- Added support for DHCP Option 120
- Added support for reregister before expiration option.
- Added support for anonymous RTSP Live View
- Adjusted system volume default value from 4 to 2.

BUG FIX

- Fixed noise audio issue when using GDSManager Intercom function.
- Fixed “[http\(s\)://IP_GDS3710:Port/snapshot/view0.jpg](http(s)://IP_GDS3710:Port/snapshot/view0.jpg)” does not return instant snapshot.
- Fixed and prevented two identical time durations could be configured.
- Fixed the device firmware cannot be downgraded after importing the P value file.
- Fixed device not contacting the NTP Server provided via DHCP Option 42.
- Fixed device not apply Config File when P value for Alarm Schedule/Profile are empty.
- Fixed modifying time zone or DST by configuration file the DST does not take effect.
- Fixed instant snapshot and live stream not retrievable when using MJPEG live snapshot and live stream URLs respectively:

Snapshot: [http\(s\)://admin:password@IP_Address_GDS:Port/jpeg/view.html](http(s)://admin:password@IP_Address_GDS:Port/jpeg/view.html)

MJPEG Stream: [http\(s\)://admin:password@IP_Address_GDS:Port/jpeg/mjpeg.html](http(s)://admin:password@IP_Address_GDS:Port/jpeg/mjpeg.html)

- Fixed GDS3710 calling out to any number can open door via DTMF (Security Enhancement: Only numbers inside RFID cards, White List and DoorBell will be able to remotely open door via DTMF).
- Fixed flooding registration packets cause webUI access stalled.
- Fixed error code 406 not acceptable for Door 2 and disabled the Events in GXV/GDS combination use.
- Fixed issue with decoding DNS (mDNS) answers from GDS3710.

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call sometimes.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- GDS3710 as Callee will not do stream negotiation.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P15505	Access_Settings.GDSManager_Configuration_Password (Value: String. Maximum length is 32)
P14560	Basic Settings.Enable Doorbell Blue Light.Start Time
P14561	Basic Settings.Enable Doorbell Blue Light.End Time
P14562	Basic Settings.Enable Doorbell Blue Light (Value 0: Disable 1: Enable)
P144	Date & Time.Allow DHCP Option 42 to override NTP server (Value 0: Disable 1: Enable)
P37	Account 1.Voice Frames Per TX (1 -- 64, default 2)
P486	Account 2.Voice Frames Per TX (1 -- 64, default 2)
P586	Account 3.Voice Frames Per TX (1 -- 64, default 2)
P686	Account 4.Voice Frames Per TX (1 -- 64, default 2)
P2330	Account 1.Re-register before Expiration(s) (0 -- 64800, default 0)
P2430	Account 2.Re-register before Expiration(s) (0 -- 64800, default 0)
P2530	Account 3.Re-register before Expiration(s) (0 -- 64800, default 0)
P2630	Account 4.Re-register before Expiration(s) (0 -- 64800, default 0)
P57	Account 1.Preferred Vocoder 1 (<0 8 9>, default 0)
P58	Account 1.Preferred Vocoder 2 (<0 8 9>, default 8)
P59	Account 1.Preferred Vocoder 3 (<0 8 9>, default 9)
P451	Account 2.Preferred Vocoder 1 (<0 8 9>, default 0)
P452	Account 2.Preferred Vocoder 2 (<0 8 9>, default 8)
P453	Account 2.Preferred Vocoder 3 (<0 8 9>, default 9)
P551	Account 3.Preferred Vocoder 1 (<0 8 9>, default 0)
P552	Account 3.Preferred Vocoder 2 (<0 8 9>, default 8)
P553	Account 3.Preferred Vocoder 3 (<0 8 9>, default 9)
P651	Account 4.Preferred Vocoder 1 (<0 8 9>, default 0)
P652	Account 4.Preferred Vocoder 2 (<0 8 9>, default 8)
P653	Account 4.Preferred Vocoder 3 (<0 8 9>, default 9)
P285	Maintenance.Upgrade.Randomized Automatic Upgrade (0 -- 23)
P8459	Maintenance.Upgrade.Hour of the Day (0 -- 23)
P286	Maintenance.Upgrade.Day of the Week (0 -- 6)

MODIFIED P-VALUE

P14000	Video_Audio_Settings, Audio_Settings, Preferred_Audio_Codec (Value:1, 2, 4)
P198	Account_1.Special Feature (Value 100: Standard 102: Broadsoft 129: Telefonica Spain)
P424	Account_2.Special Feature (value: 100: Standard 102: Broadsoft 129: Telefonica Spain)
P524	Account_3.Special Feature (value: 100: Standard 102: Broadsoft 129: Telefonica Spain)
P624	Account_4.Special Feature (value: 100: Standard 102: Broadsoft 129: Telefonica Spain)
P14003	System Volume. Default value: change from level 4 to lever 2.

NEW HTTP API

- P15505 -- Access_Settings.GDSManager_Configuration_Password (value: String, MAX Length is 32)
 GET: <http://ip:port/goform/config?cmd=get&type=access>
 SET: <http://ip:port/goform/config?cmd=set&P15505=<value>> (value: String, MAX Length is 32)
- P14562 -- Basic Settings -> Enable Doorbell Blue Light (0:Disable 1:Enable)
 GET: <http://ip:port/goform/config?cmd=get&type=door>
 SET: <http://ip:port/goform/config?cmd=set&P14562=<value>> (0:Disable 1:Enable)
- P14560 -- Basic Settings -> Enable Doorbell Blue Light -> Start Time
 GET: <http://ip:port/goform/config?cmd=get&type=door>
 SET: <http://ip:port/goform/config?cmd=set&P14560=<value>> (value: string)
- P14561 -- Basic Settings -> Enable Doorbell Blue Light -> End Time
 GET: <http://ip:port/goform/config?cmd=get&type=door>
 SET: <http://ip:port/goform/config?cmd=set&P14561=<value>> (value: string)
- P144 -- Date & Time -> Allow DHCP Option 42 to override NTP server (0:Disable 1:Enable)
 GET: <http://ip:port/goform/config?cmd=get&type=date>
 SET: <http://ip:port/goform/config?cmd=set&P144=<value>> (0:Disable 1:Enable)
- P37 -- Account 1 -> Voice Frames Per TX (1 -- 64)
 GET: <http://ip:port/goform/config?cmd=get&type=sip>
 SET: <http://ip:port/goform/config?cmd=set&P37=<value>> (1 -- 64)
- P486 -- Account 1 -> Voice Frames Per TX (1 -- 64)
 GET: <http://ip:port/goform/config?cmd=get&type=sip>
 SET: <http://ip:port/goform/config?cmd=set&P486=<value>> (1 -- 64)
- P586 -- Account 1 -> Voice Frames Per TX (1 -- 64)
 GET: <http://ip:port/goform/config?cmd=get&type=sip>
 SET: <http://ip:port/goform/config?cmd=set&P586=<value>> (1 -- 64)
- P686 -- Account 1 -> Voice Frames Per TX (1 -- 64)
 GET: <http://ip:port/goform/config?cmd=get&type=sip>
 SET: <http://ip:port/goform/config?cmd=set&P686=<value>> (1 -- 64)

- P2330 -- Account 1 -> Re-register before Expiration(s) (0 -- 64800, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P2330=<value>> (0 -- 64800)
- P2430 -- Account 2 -> Re-register before Expiration(s) (0 -- 64800, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P2430=<value>> (0 -- 64800)
- P2530 -- Account 3 -> Re-register before Expiration(s) (0 -- 64800, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P2530=<value>> (0 -- 64800)
- P2630 -- Account 4 -> Re-register before Expiration(s) (0 -- 64800, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P2630=<value>> (0 -- 64800)
- P57 -- Account 1 -> Preferred Vocoder 1 (<0|8|9>, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P57=<value>> (<0|8|9>)
- P58 -- Account 1 -> Preferred Vocoder 2 (<0|8|9>, default 8)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P58=<value>> (<0|8|9>)
- P59 -- Account 1 -> Preferred Vocoder 3 (<0|8|9>, default 9)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P59=<value>> (<0|8|9>)
- P451 -- Account 2 -> Preferred Vocoder 1 (<0|8|9>, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P451=<value>> (<0|8|9>)
- P452 -- Account 2 -> Preferred Vocoder 2 (<0|8|9>, default 8)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P452=<value>> (<0|8|9>)
- P453 -- Account 2 -> Preferred Vocoder 3 (<0|8|9>, default 9)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P453=<value>> (<0|8|9>)
- P551 -- Account 3 -> Preferred Vocoder 1 (<0|8|9>, default 0)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P551=<value>> (<0|8|9>)
- P552 -- Account 3 -> Preferred Vocoder 2 (<0|8|9>, default 8)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P552=<value>> (<0|8|9>)
- P553 -- Account 3 -> Preferred Vocoder 3 (<0|8|9>, default 9)
GET: <http://ip:port/goform/config?cmd=get&type=sip>
SET: <http://ip:port/goform/config?cmd=set&P553=<value>> (<0|8|9>)

- P651 -- Account 4 -> Preferred Vocoder 1 (<0|8|9>, default 0)
GET: http://ip:port/goform/config?cmd=get&type=sip
SET: http://ip:port/goform/config?cmd=set&P651=<value> (<0|8|9>)
- P652 -- Account 4 -> Preferred Vocoder 2 (<0|8|9>, default 8)
GET: http://ip:port/goform/config?cmd=get&type=sip
SET: http://ip:port/goform/config?cmd=set&P652=<value> (<0|8|9>)
- P653 -- Account 4 -> Preferred Vocoder 3 (<0|8|9>, default 9)
GET: http://ip:port/goform/config?cmd=get&type=sip
SET: http://ip:port/goform/config?cmd=set&P653=<value> (<0|8|9>)
- P285 -- Maintenance -> Upgrade -> Randomized Automatic Upgrade (0 -- 23)
GET: http://ip:port/goform/config?cmd=get&type=upgrade
SET: http://ip:port/goform/config?cmd=set&P285=<value> (0 -- 23)
- P8459 -- Maintenance -> Upgrade -> Hour of the Day (0-23)
GET: http://ip:port/goform/config?cmd=get&type=upgrade
SET: http://ip:port/goform/config?cmd=set&P8459=<value> (0 -- 23)
- P286 -- Maintenance -> Upgrade -> Day of the Week (0-6)
GET: http://ip:port/goform/config?cmd=get&type=upgrade
SET: http://ip:port/goform/config?cmd=set&P286=<value> (0 -- 6)

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

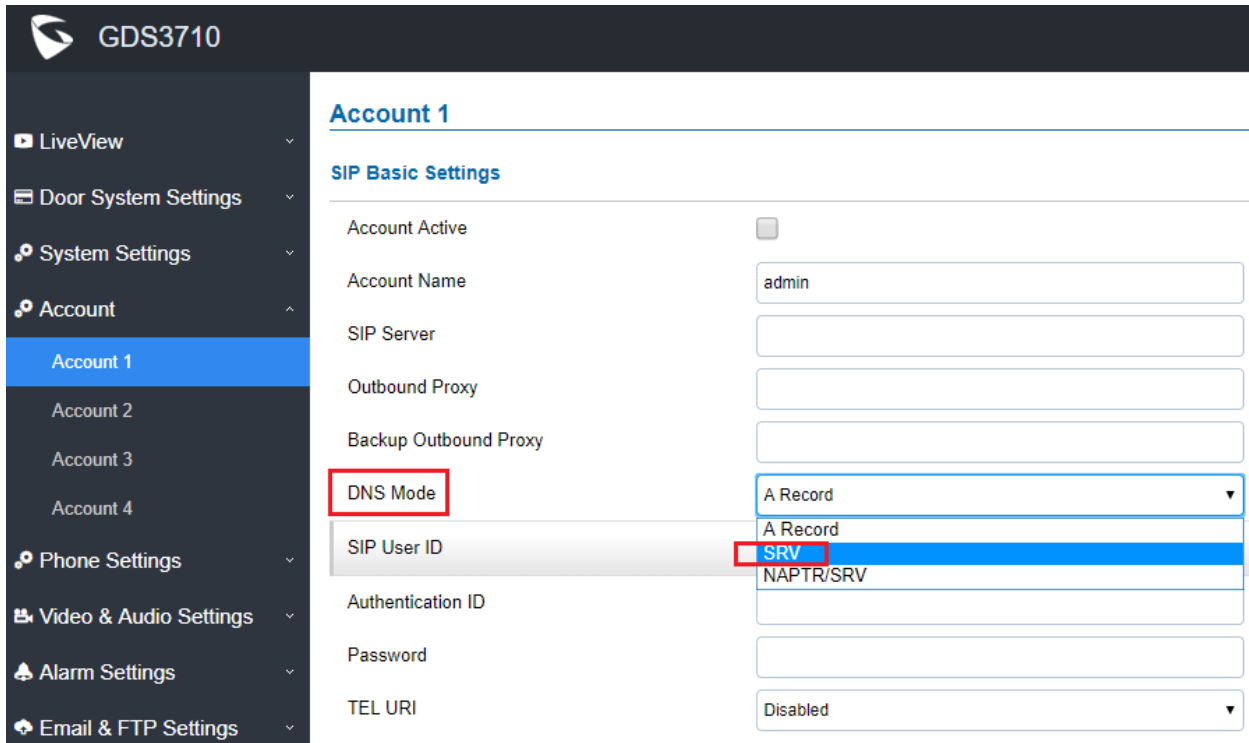
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

SUPPORT DNS SRV

- **Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



The screenshot shows the web configuration interface for a Grandstream GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account (expanded), Account 1 (selected), Account 2, Account 3, Account 4, Phone Settings, Video & Audio Settings, Alarm Settings, and Email & FTP Settings. The main content area is titled 'Account 1' and 'SIP Basic Settings'. It includes fields for Account Active (checkbox), Account Name (admin), SIP Server, Outbound Proxy, Backup Outbound Proxy, DNS Mode (dropdown menu), SIP User ID, Authentication ID, Password, and TEL URI (dropdown menu). The 'DNS Mode' dropdown is open, showing three options: 'A Record', 'SRV' (highlighted in blue), and 'NAPTR/SRV'. The 'SIP User ID' field is also highlighted with a red box.

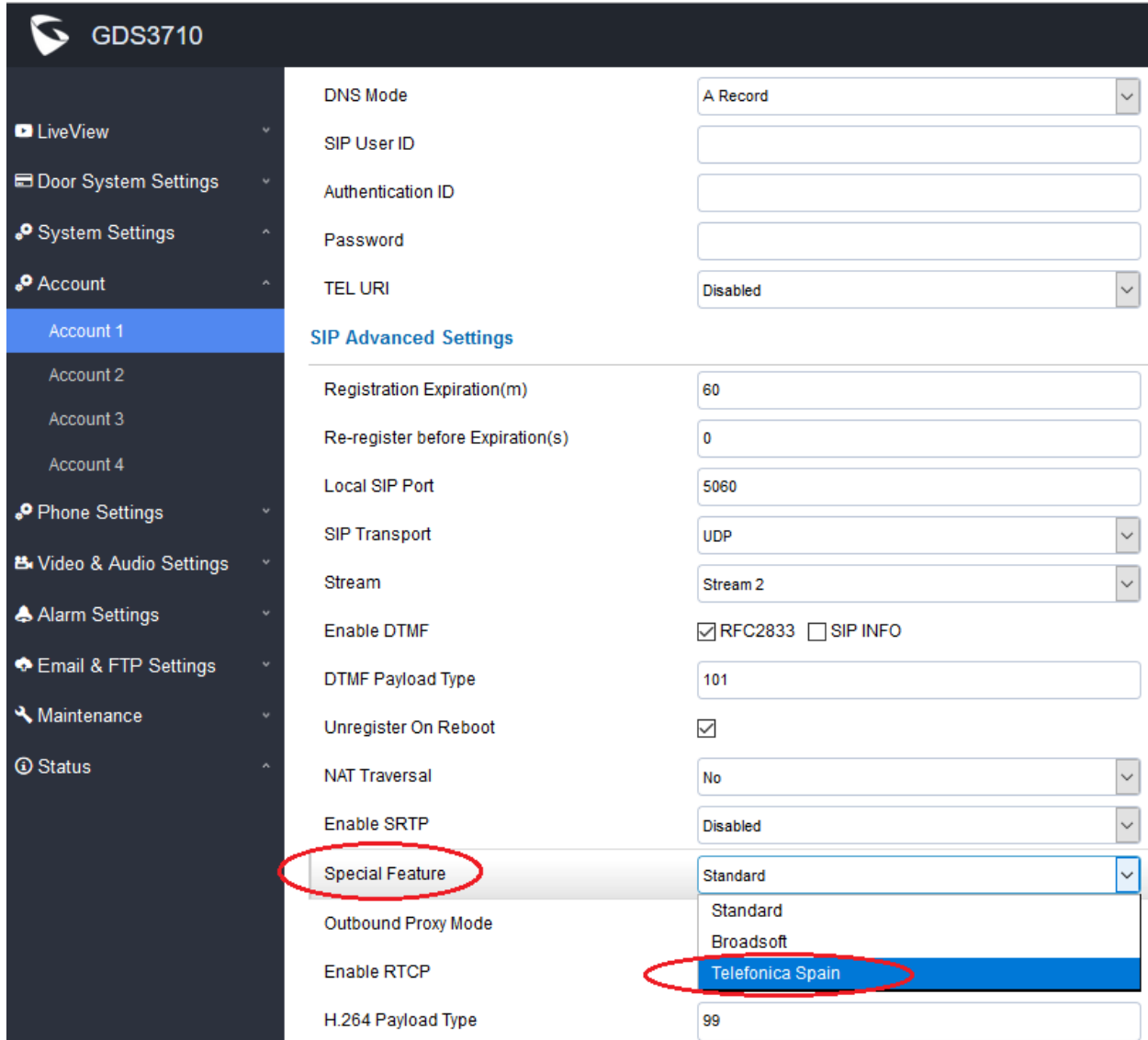
- **Functionality**

This is a major feature enhancement for Service Provider, via DNS SRV, service providers can provide smooth service transition backup in case service down.

SUPPORT SPECIAL FEATURE - TELEFONICA

- Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



GDS3710		
<ul style="list-style-type: none"> LiveView Door System Settings System Settings Account <ul style="list-style-type: none"> Account 1 Account 2 Account 3 Account 4 Phone Settings Video & Audio Settings Alarm Settings Email & FTP Settings Maintenance Status 	DNS Mode	A Record
	SIP User ID	
	Authentication ID	
	Password	
	TEL URI	Disabled
	SIP Advanced Settings	
	Registration Expiration(m)	60
	Re-register before Expiration(s)	0
	Local SIP Port	5060
	SIP Transport	UDP
	Stream	Stream 2
	Enable DTMF	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
	DTMF Payload Type	101
	Unregister On Reboot	<input checked="" type="checkbox"/>
	NAT Traversal	No
Enable SRTP	Disabled	
Special Feature	Standard	
Outbound Proxy Mode	Standard	
Enable RTCP	Broadsoft	
H.264 Payload Type	99	

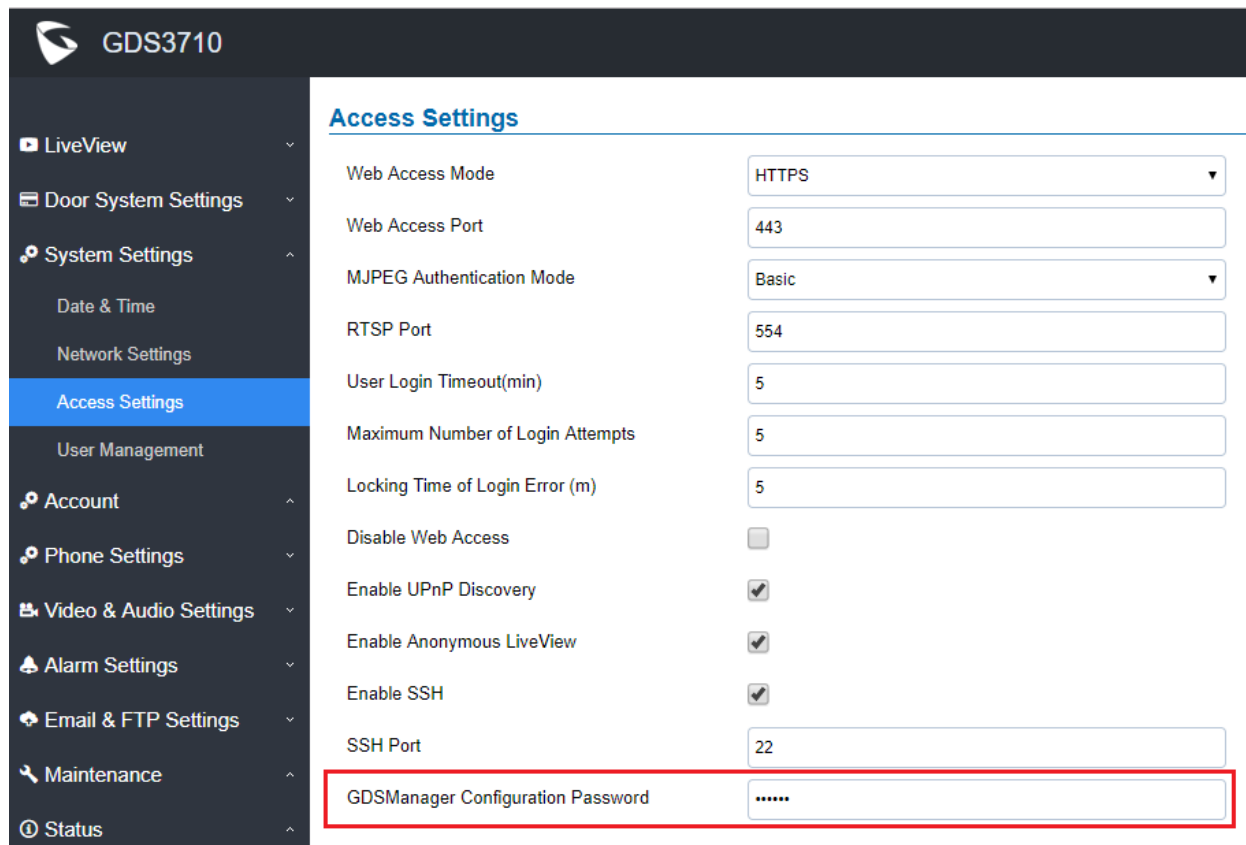
- Functionality**

This is a major feature enhancement for Service Provider. Special feature or Special Mode can be provisioned to match the Proxy of Service Provider like Telefonica, or Broadsoft. This is implemented for ITSP Service Provider. Normal customers just use “Standard” feature.

SEPARATE CREDENTIALS FOR GDSMANAGER

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



The screenshot shows the GDS3710 web UI. On the left is a sidebar menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, Access Settings (highlighted), User Management, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Access Settings' and contains the following configuration items:

Setting	Value
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password

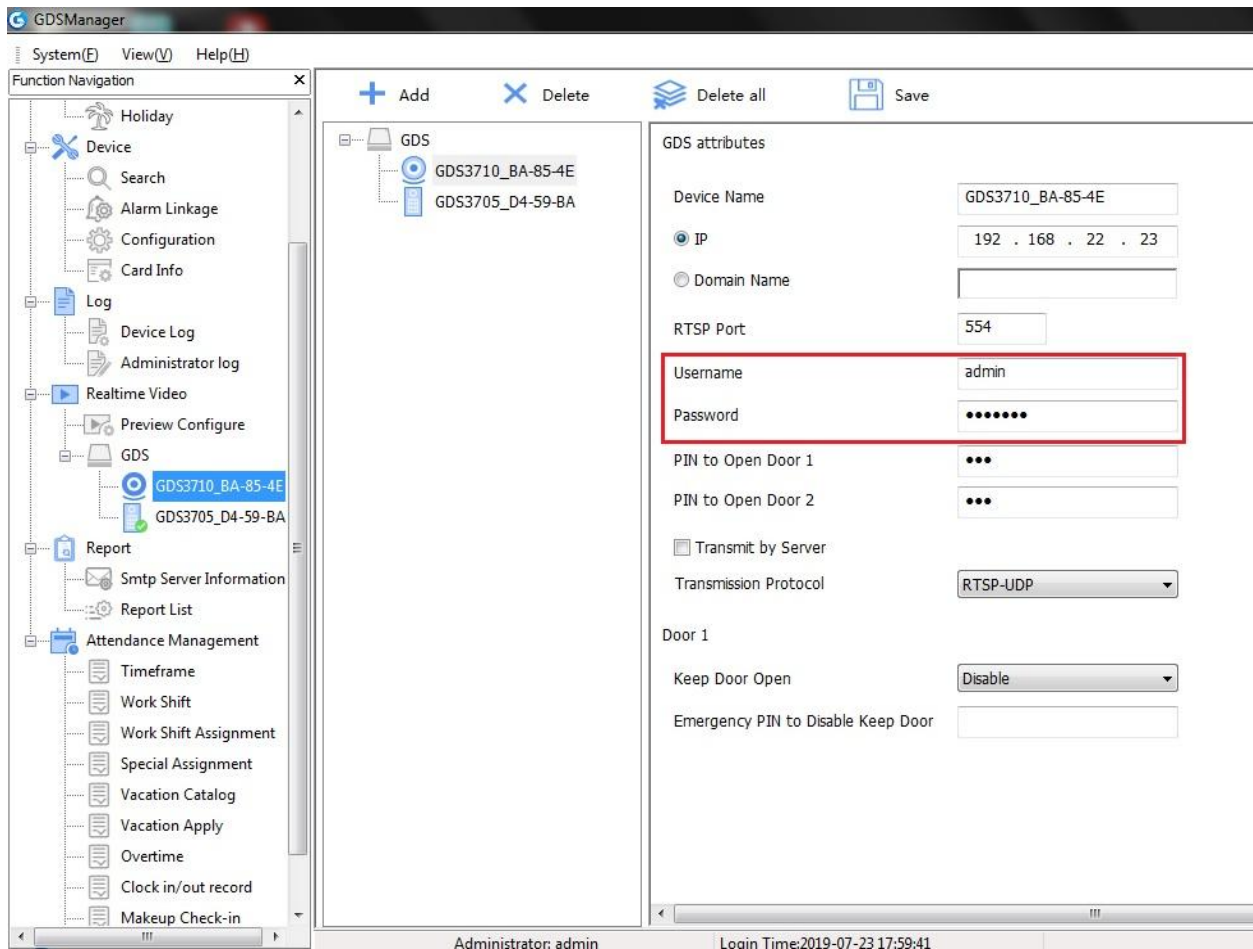
The 'GDSManager Configuration Password' field is highlighted with a red rectangular box.

- **Functionality**

This feature is implemented based on field customer feedback. Now separate credentials can be configured and used in GDSManager to communicate with GDS3710, instead of using GDS3710 webUI administrator's credentials. System administrators keep the admin password and use another password for GDSManager where usually operated by HR or other company staffs.

NOTE:

- *Make sure the correspondent password is configured in GDSManager like below:*

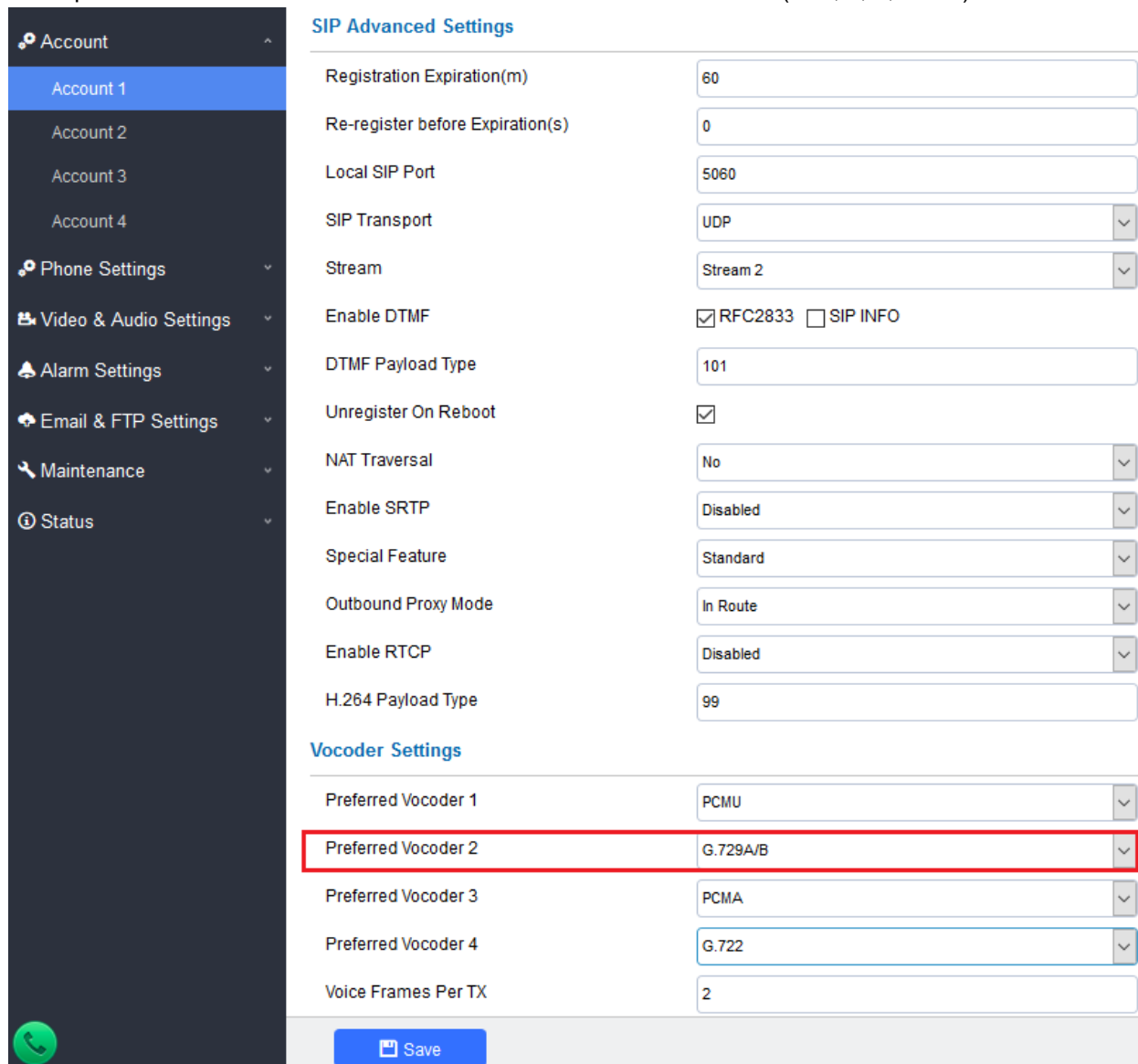


- *The password must match the password configured in the GDS3710 at above screenshot.*

G.729 AND MULTIPLE AUDIO CODECS SIMULTANEOUSLY WITH PRIORITY

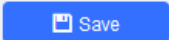
- Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



SIP Advanced Settings	
Registration Expiration(m)	60
Re-register before Expiration(s)	0
Local SIP Port	5060
SIP Transport	UDP
Stream	Stream 2
Enable DTMF	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
DTMF Payload Type	101
Unregister On Reboot	<input checked="" type="checkbox"/>
NAT Traversal	No
Enable SRTP	Disabled
Special Feature	Standard
Outbound Proxy Mode	In Route
Enable RTCP	Disabled
H.264 Payload Type	99

Vocoder Settings	
Preferred Vocoder 1	PCMU
Preferred Vocoder 2	G.729A/B
Preferred Vocoder 3	PCMA
Preferred Vocoder 4	G.722
Voice Frames Per TX	2



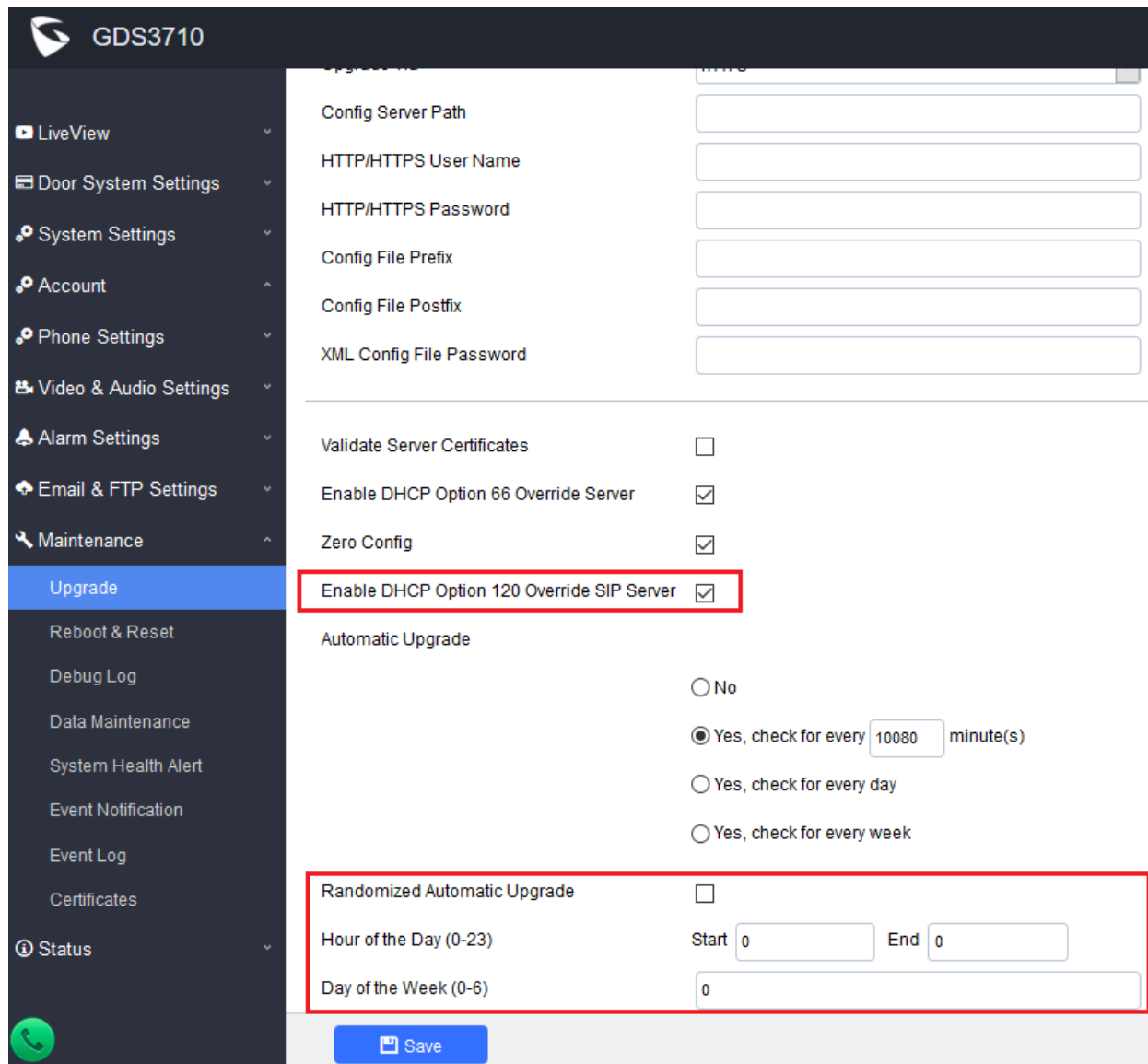
- Functionality**

This is an enhancement to allow ITSP Service Provider to use G.729 audio codec in their networks. Multiple audio codecs supported with specified priority be selected.

SCHEDULE FOR FIRMWARE UPGRADE AND PROVISIONING, DHCP OPTION 120

- Web Configuration**

This option can be found under device web UI → Maintenance → Upgrade:



GDS3710

- LiveView
- Door System Settings
- System Settings
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
 - Upgrade**
 - Reboot & Reset
 - Debug Log
 - Data Maintenance
 - System Health Alert
 - Event Notification
 - Event Log
 - Certificates
- Status

Upgrade

Config Server Path

HTTP/HTTPS User Name

HTTP/HTTPS Password

Config File Prefix

Config File Postfix

XML Config File Password

Validate Server Certificates ☐

Enable DHCP Option 66 Override Server ☒

Zero Config ☒

Enable DHCP Option 120 Override SIP Server ☒

Automatic Upgrade

☐ No

☒ Yes, check for every 10080 minute(s)

☐ Yes, check for every day

☐ Yes, check for every week

Randomized Automatic Upgrade ☐

Hour of the Day (0-23) Start 0 End 0

Day of the Week (0-6) 0

Save

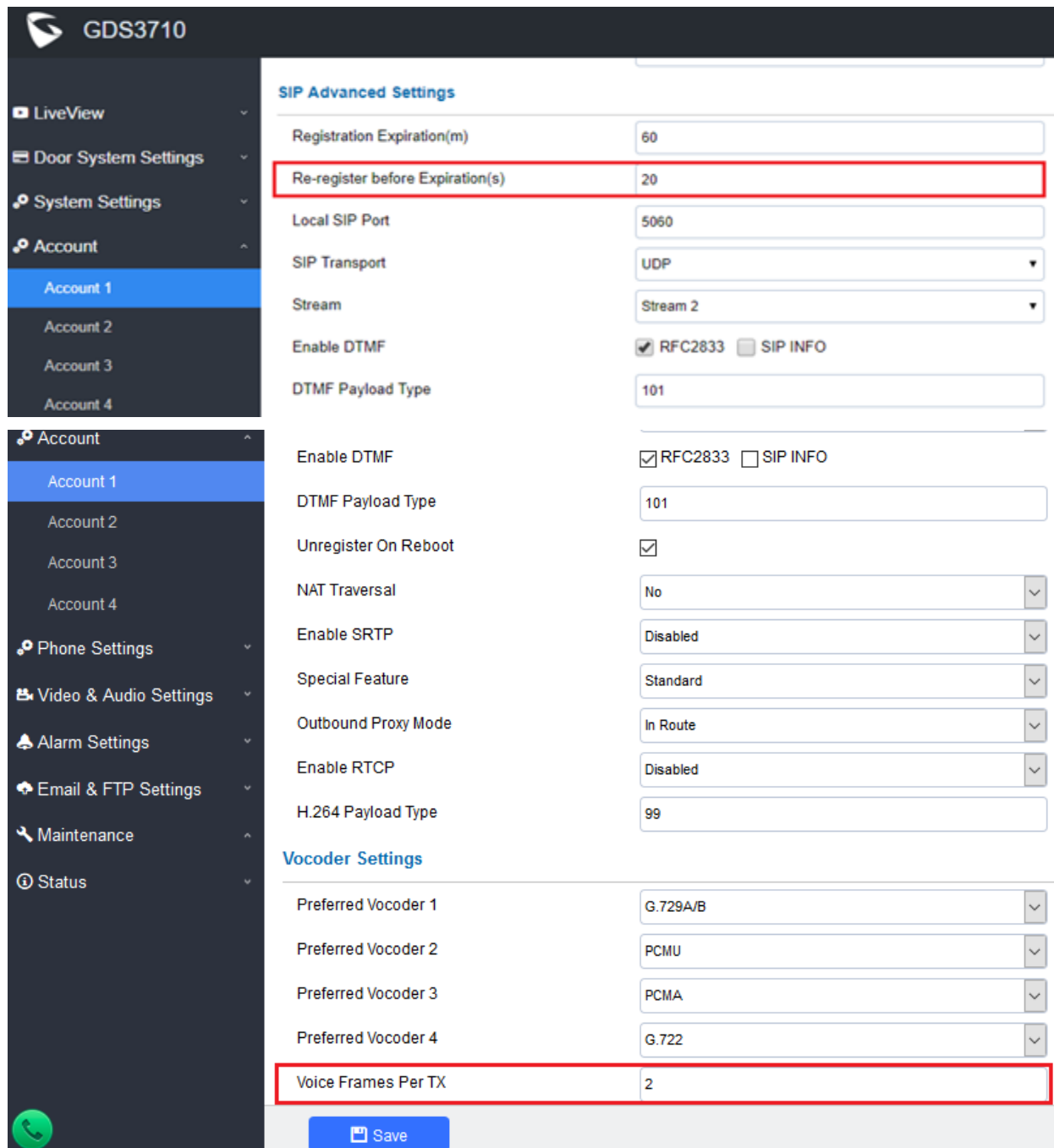
- Functionality**

This is an enhancement requested by ITSP service providers as well as lots of system integrators from Forum. This feature allows them to use DHCP Option 120 to override SIP Server; and let the GDS3710 either randomly check upgrade/provisioning server, or at configured schedule.

REREGISTER BEFORE EXPIRATION AND VOICE FRAME PER TX

- **Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



The screenshot shows the web configuration interface for a Grandstream GDS3710 device. The left sidebar contains a navigation menu with options: LiveView, Door System Settings, System Settings, Account (selected), Account 1 (selected), Account 2, Account 3, Account 4, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'SIP Advanced Settings' and contains the following fields:

- Registration Expiration(m): 60
- Re-register before Expiration(s): 20 (highlighted with a red box)
- Local SIP Port: 5060
- SIP Transport: UDP
- Stream: Stream 2
- Enable DTMF: ☒ RFC2833 ☐ SIP INFO
- DTMF Payload Type: 101
- Enable DTMF: ☒ RFC2833 ☐ SIP INFO
- DTMF Payload Type: 101
- Unregister On Reboot: ☒
- NAT Traversal: No
- Enable SRTP: Disabled
- Special Feature: Standard
- Outbound Proxy Mode: In Route
- Enable RTCP: Disabled
- H.264 Payload Type: 99

Below the SIP Advanced Settings is the 'Vocoder Settings' section, which contains the following fields:

- Preferred Vocoder 1: G.729A/B
- Preferred Vocoder 2: PCMU
- Preferred Vocoder 3: PCMA
- Preferred Vocoder 4: G.722
- Voice Frames Per TX: 2 (highlighted with a red box)

A 'Save' button is located at the bottom right of the configuration area.

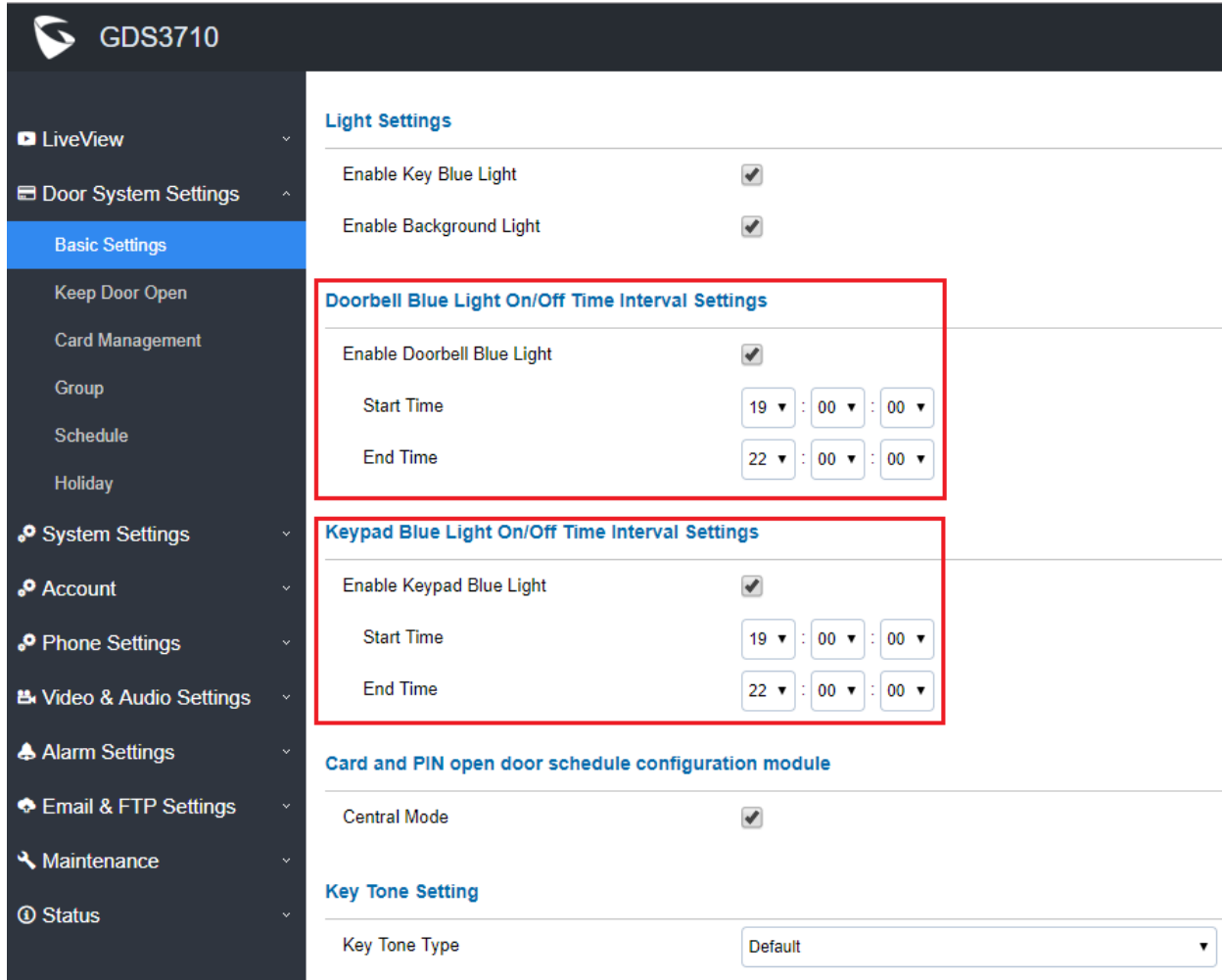
- **Functionality**

These parameters are mostly used by ITSP Service Provider. Normal users please do not touch those parameters because that could cause audio issue if parameters are incorrect.

KEYPAD BLUE LIGHT ON/OFF ON SCHEDULE

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
 - System Settings
 - Account
 - Phone Settings
 - Video & Audio Settings
 - Alarm Settings
 - Email & FTP Settings
 - Maintenance
 - Status

Light Settings

Enable Key Blue Light ☒

Enable Background Light ☒

Doorbell Blue Light On/Off Time Interval Settings

Enable Doorbell Blue Light ☒

Start Time 19 : 00 : 00

End Time 22 : 00 : 00

Keypad Blue Light On/Off Time Interval Settings

Enable Keypad Blue Light ☒

Start Time 19 : 00 : 00

End Time 22 : 00 : 00

Card and PIN open door schedule configuration module

Central Mode ☒

Key Tone Setting

Key Tone Type Default

- **Functionality**

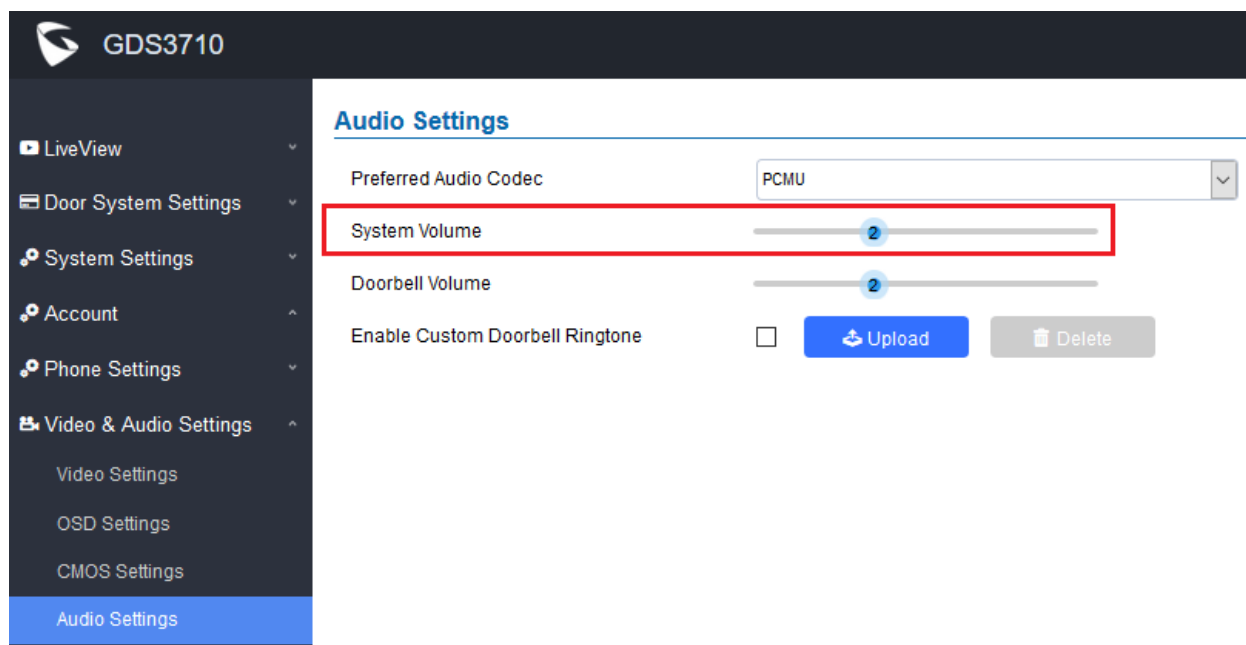
This is an enhancement for an existing features based on customer feedback from field.

By configure the keypad blue light and/or doorbell blue light ON/OFF based on schedule, GDS3710 will provide users easy access and operation to keypad during night time when ambient environment is dark.

ADJUST SYTEM DEFAULT VOLUME TO LEVER 2

- **Web Configuration**

This option can be found under device web UI → Video & Audio Settings → Audio Settings:



- **Functionality**

This is an enhancement based on customer feedback from field.

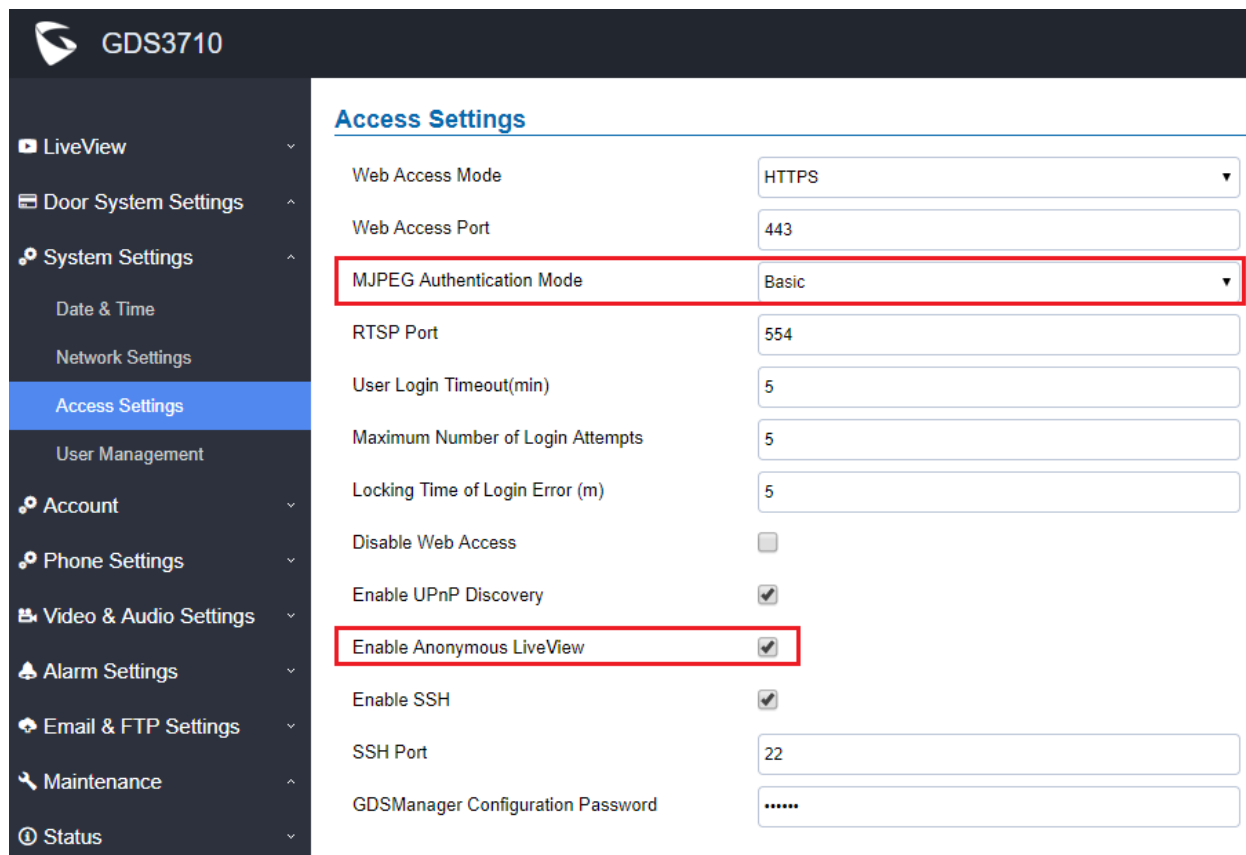
The previous default value is 4, the new default value is 2. Factory reset the new value 2 will take place.

Customer can adjust this value based on field or installation environment to meet the requirement.

SUPPORT ANONYMOUS RTSP LIVE VIEW

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



The screenshot shows the GDS3710 web UI. On the left is a sidebar menu with options: LiveView, Door System Settings, System Settings, Date & Time, Network Settings, Access Settings (highlighted), User Management, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main area is titled 'Access Settings' and contains the following configuration items:

Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password

- **Functionality**

This is a further enhancement for the already supported anonymous MJPEG LiveView streaming, request by customers like Service Provider and System Integrators or Installers. This feature allows system integrators to retrieve snapshots from GDS3710 directly without credentials, similar to fetch the live MJPEG streaming previously. This is good for system re-development.

When enabled this feature, **Special Access URL** required to retrieve the snapshot (frame by frame if refreshed) or live MJPEG video streaming:

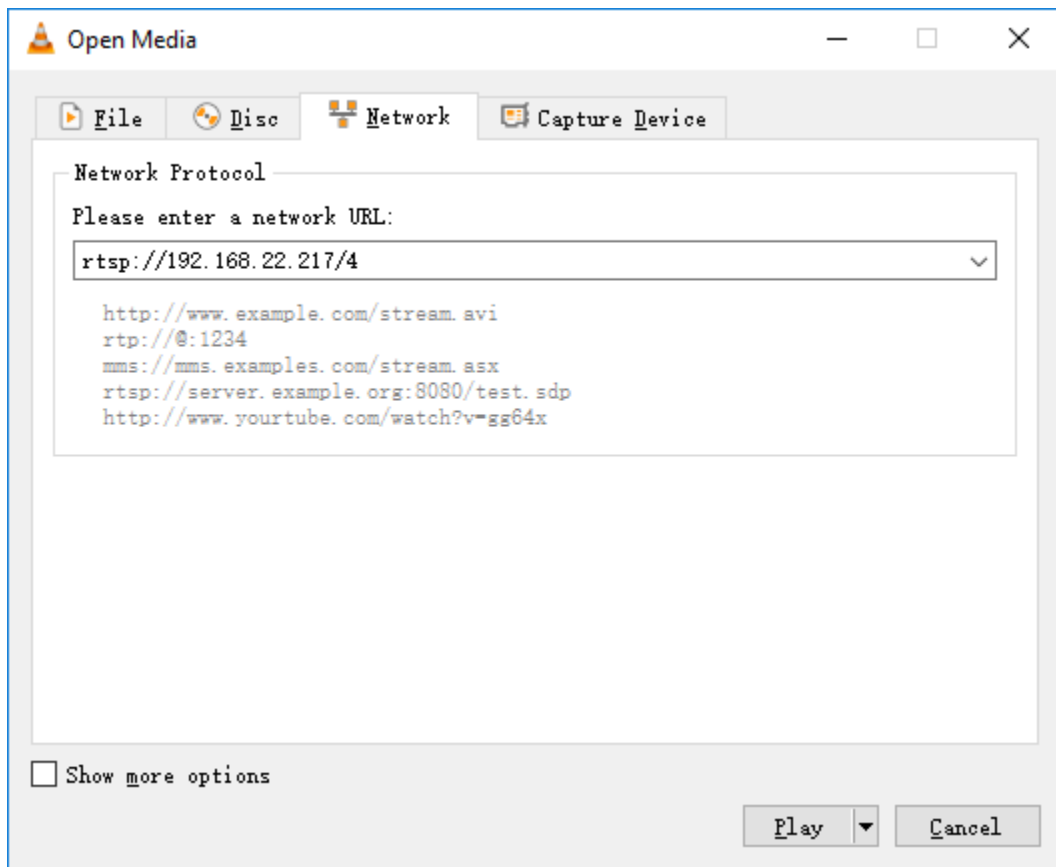
HTTP(S)://IP_GDS3710:Port/anonymous/snapshot/view.jpg (Snapshot)

OR: HTTP(S)://IP_GDS3710:Port/anonymous/snapshot/view.html (Snapshot)

HTTP(S)://IP_GDS3710:Port/videoview.html (Live MJPEG streaming)

For customers using VLC MediaPlayer or similar software program, previous firmware still requiring credentials. Now the issue is fixed and customers can view the live video using VLC or other 3rd party RTSP retriever to do re-development.

Using VLC Media Player for example:



FORMAT:

RTSP://IP_GDS3710:Port/X (*X = 0, 4, 8 correspondent to Stream 1, 2, 3*)

No credential is required in such implementation.

The live video and audio will play out with some delay based on the computer processing power and network conditions.

NOTE:

- Please make sure the environment is secure before enable this feature.
- Please reminder user the privacy when using this feature.

FIRMWARE VERSION 1.0.5.6

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

04/08/2019

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement since firmware 1.0.5.2. Main enhancement like added support for 4 SIP Accounts, DTMF payload, etc.

Factory Reset is recommended due to 4 SIP accounts added (to sort out all the internal registers and P value added). If upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI, factory reset is mandatory. Please backup the configuration and data before factory reset and import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added support for 4 SIP accounts.
- Added option to configure DTMF Payload value.
- Added and optimized number handling algorithm to work with GXV3370 open two doors.
- Added prompt reminder if H.264 payload type conflict with RTP payload type.
- Added feature support to upload customized doorbell so user can upload own voice prompt or music.
- Added clear button to delete unwanted uploaded audio file for doorbell ringtone. Optimized the uploading of customized ringtone.
- Added prevention mechanism to avoid unwanted alarm pulse spikes triggering alarm event.
- Added ITSP requested feature: Configure Keep Door Open actions from GDSManager.
- Added ITSP requested feature: GDSManager will synchronize with GDS3710 when changing the settings of Keep Door Open.
- Added management feature: Send out System Health Alerts via Email.
- Added feature to set “Schedule” for “Local PIN to Open Door”.
- Added support for Packetization Mode 0
- Added option to disable outbound proxy route header.
- Added feature support for CSV format when Import/Export data.
- Added feature support for Anonymous Snapshot.
- Enhanced security and limited the GDS3710 as Caller to open door via DTMF: Only numbers exist in Doorbell, Whitelist or RFID Card Management will be able to enter DTMF PIN to open door remotely.
- Added AlarmOut1 (COM1) to support “Normal Open” or “Normal Close” setting.
- Added Boot Version information into “Status” page.

BUG FIX

- Fixed pressing doorbell called SIP number using failed registration account.
- Fixed after factory reset if the first account is empty, parallel hunting in IP peering call would fail.
- Fixed alarm email failure when non-scheduled access alarm triggered.
- Fixed Emergency PIN to Disable Keep Door Open failed to be saved if Door1 and Door2 save together.
- Fixed “Allow Reset via SIP Notify” option showed “Disable” even configured “Enable”.
- Fixed “Emergency PIN to Disable Keep Door Open” in GDS3710 will not be synchronized with GDSManager.
- Fixed Wiegand Output mode when choosing “Relay and Local Authentication” the output signal is distorted and failed to work with 3rd party Door Controller.
- Fixed security issue where ALMOUT1 port with spike pulse could cause some model of strikes to open door during device reboot or restore lost power.
- Fixed Data imported might be partially failure sometimes.
- Fixed System Health Alert email will not send out if email title is empty.
- Fixed “Save” button will be unavailable if pressing “Test” button first in the “Event Notification” page.
- Fixed if HTTP port changed (not default port 80) Google Chrome will not play Live Video.
- Fixed uploading custom doorbell ringtone would uncheck the related choice box in UI automatically.
- Fixed device would reboot after receiving from UCM the zero configuration command to change the configuration file path.
- Fixed ALMOUT1 status would change from Normal Close to Normal Open after rebooting.
- Fixed device would not play default doorbell ringtone if enable “Custom Doorbell Ringtone Upload” without actually uploading any working audio file as ringtone.
- Fixed configure Door1 and Door2 remote PIN at the same time the Alarm_Out (COM1) port will not operate correctly.
- Fixed issue Wiegand Input to Open Door not consistent when using Guest PIN, Private PIN or Card and Private PIN.
- Fixed snapshots sending via email or uploaded to FTP not consistent with number configured.
- Fixed SIP account will off line after importing the P value.
- Fixed issue the keypad and card scanner will randomly stall and not response for a while (reported by ITSP customers).
- Fixed after Zero Config provisioning requires manually reboot to take effect.
- Fixed device will not start upgrading process when unchecked “Automatic Upgrade” option.
- Fixed the default value inconsistent between device and the imported file, as well as partial data failure for imported file.
- Fixed without conflict reminding prompt when configure local SIP port and local RTP port to be same value (which is not allowed).
- Fixed Zero Config not enabled by default in firmware 1.0.5.2
- Fixed “Automatic Upgrade” fail to happen at configured time window.
- Fixed DI as “Open Door” the “Digit Input 1 Status” and “Select Alarm Schedule” should be greyed out.
- Fixed Privacy Mask incorrectly editing operation would crash the browser.
- Fixed DI feature would fail or be blocked if without network connection.

- Fixed external alarm/doorbell device connected to COM1 only act once when configured Doorbell Mode as “Doorbell Output Control (Digital Output) 1” or “Both Above”. The duration now is the same as “Alarm Output Duration(s)” of “Digit Output” in “Alarm Settings”.
- Fixed only Account 1 can answer peered IP Call normally while this feature should work via port used.
- Fixed the “Reboot” event not reported in the “System Health Alert”.
- Fixed “LiveView” not working stably with latest Chrome (version 71.0.3578.98)
- Fixed Email Test returning Error but actual email working good due to the testing function not supporting special characters inside the email password.
- Fixed HTTP security issue in “Anonymous LiveView” (trace will show user information).

KNOWN ISSUES

- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call sometimes.
- Remote device can hear custom doorbell ringtone about 1~2 seconds when answering the call.
- GDS3710 as Callee will not do stream negotiation.
- When SIP account is logged out, pressing the keyboard is abnormal.
- When SIP transport mode is TLS/TCP, remote door opening might fail occasionally.

NEW P-VALUE

P78	Phone_Settings.User_Random_Port
P79	Account_1 DTMF Payload
P496	Account_2 DTMF Payload
P596	Account_3 DTMF Payload
P696	Account_4 DTMF Payload
P10470	Basic_Settings.Doorbell_Call_Out Account
P10471	Basic_Settings.Alarm_Call_Out_Account
P15498	Basic_Settings.Local_PIN_to_Open_Door_Schedule
P15490	System_Health_Alert.Enable_System_Health_Alert
P15491	System_Health_Alert.Delivery_Method
P15492	System_Health_Alert.Alert_Interval
P15493	System_Health_Alert.SIP_Registration_Status
P15494	System_Health_Alert.System_Reboot
P15495	System_Health_Alert.System_Temperature
P15496	System_Health_Alert.Email_Title
P957	Phone_Settings.SIP_Packetization_Compatible Mode
P271	Account.Account_1.Account_Active
P3	Account.Account_1.Account_Name
P32	Account.Account_1.Registration_Expiration(m)
P34	Account.Account_1.Password
P35	Account.Account_1.SIP_User_ID
P36	Account.Account_1.Authentication_ID
P40	Account.Account_1.Local_SIP_Port
P47	Account.Account_1.SIP_Server
P48	Account.Account_1.Outbound_Proxy
P52	Account.Account_1.NAT_Traversal
P63	Account.Account_1.TEL_URI
P81	Account.Account_1.Unregister_On_Reboot
P100	Account.Account_1.Special_Feature
P103	Account.Account_1.DNS_Mode
P130	Account.Account_1.SIP_Transport
P183	Account.Account_1.Enable_SRTP
P293	Account.Account_1.H.264_Payload_Type

P490	Account.Account_1.Enable_Keep_Alive
P2302	Account.Account_1.Enable_DTMF_RFC2833
P2303	Account.Account_1.Enable_DTMF_SIP-INFO
P2305	Account.Account_1.Outbound_Proxy_Mode
P2333	Account.Account_1.Backup_Outbound_Proxy
P2492	Account.Account_1.Enable_RTCP
P15480	Account.Account_1.Stream
P501	Account.Account_3.Account_Active
P502	Account.Account_3.SIP_Server
P503	Account.Account_3.Outbound_Proxy
P504	Account.Account_3.SIP_User_ID
P505	Account.Account_3.Authentication_ID
P506	Account.Account_3.Password
P507	Account.Account_3.Account_Name
P508	Account.Account_3.DNS_Mode
P509	Account.Account_3.TEL_URI
P511	Account.Account_3.Unregister_On_Reboot
P512	Account.Account_3.Registration_Expiration (m)
P513	Account.Account_3.Local_SIP_Port
P514	Account.Account_3.NAT_Traversal
P524	Account.Account_3.Special_Feature
P543	Account.Account_3.Enable_SRTP
P548	Account.Account_3.SIP_Transport
P562	Account.Account_3.H.264_Payload_Type
P590	Account.Account_3.Enable_Keep_Alive
P2502	Account.Account_3.Enable_DTMF_RFC2833
P2503	Account.Account_3.Enable_DTMF_SIP-INFO
P2505	Account.Account_3.Outbound_Proxy_Mode
P2533	Account.Account_3.Backup_Outbound_Proxy
P2592	Account.Account_3.Enable_RTCP
P15481	Account.Account_3.Stream
P601	Account.Account_4.Account_Active
P602	Account.Account_4.SIP_Server
P603	Account.Account_4.Outbound_Proxy

P604	Account.Account_4.SIP_User_ID
P605	Account.Account_4.Authentication_ID
P606	Account.Account_4.Password
P607	Account.Account_4.Account_Name
P608	Account.Account_4.DNS_Mode
P609	Account.Account_4.TEL_URI
P611	Account.Account_4.Unregister_On_Reboot
P612	Account.Account_4.Registration_Expiration (m)
P613	Account.Account_4.Local_SIP_Port
P614	Account.Account_4.NAT_Traversal
P624	Account.Account_4.Special_Feature
P643	Account.Account_4.Enable_SRTP
P648	Account.Account_4.SIP_Transport
P662	Account.Account_4.H.264_Payload_Type
P690	Account.Account_4.Enable_Keep_Alive
P2602	Account.Account_4.Enable_DTMF_RFC2833
P2603	Account.Account_4.Enable_DTMF_SIP-INFO
P2605	Account.Account_4.Outbound_Proxy_Mode
P2633	Account.Account_4.Backup_Outbound_Proxy
P2692	Account.Account_4.Enable_RTCP
P15482	Account.Account_4.Stream

MODIFIED P-VALUE

- Upgrade Zero_Config Default Value 0 → 1

NEW HTTP API

- N/A

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

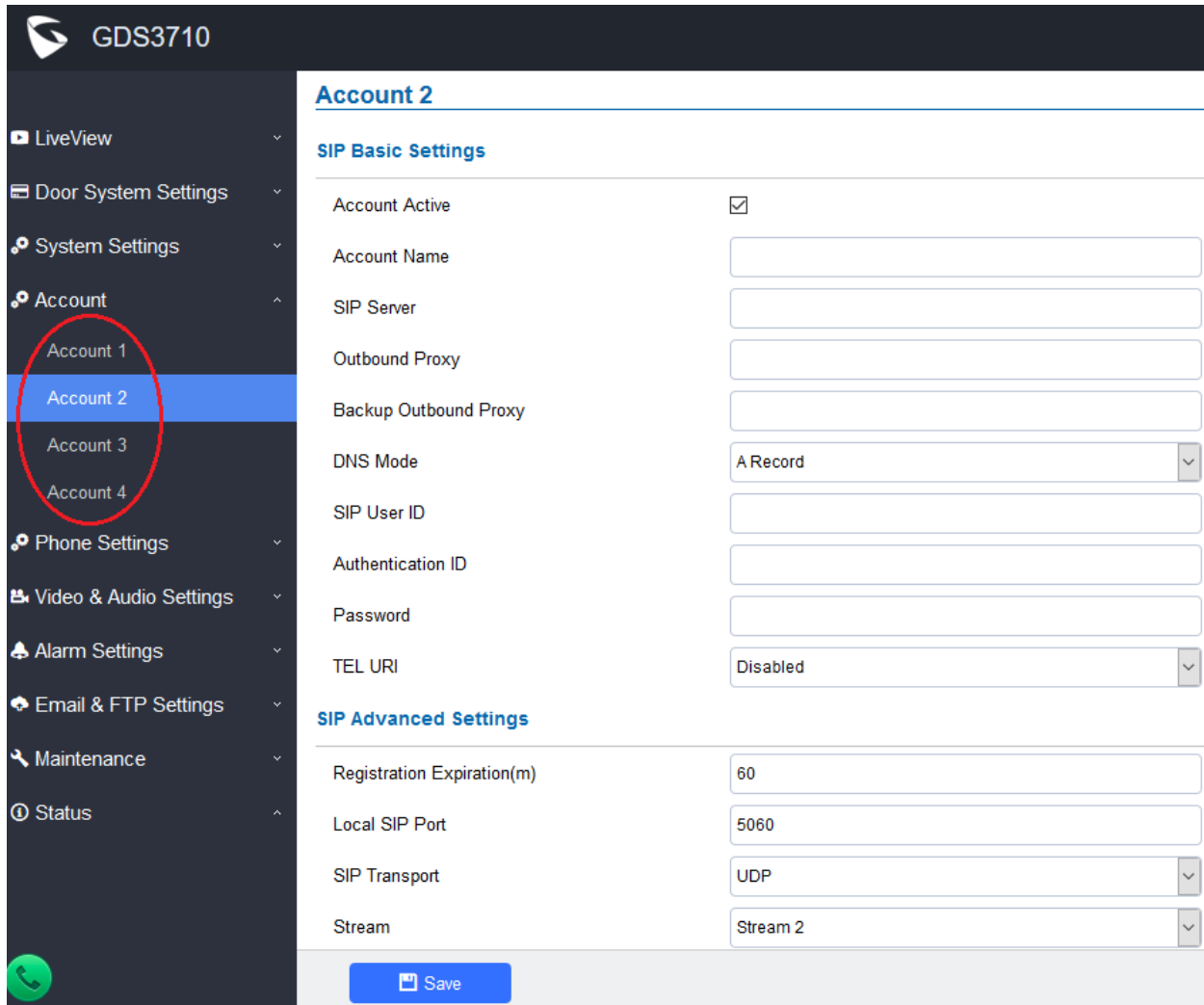
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

SUPPORT 4 SIP ACCOUNTS

- **Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



GDS3710

Account 2

SIP Basic Settings

Account Active	<input checked="" type="checkbox"/>
Account Name	<input type="text"/>
SIP Server	<input type="text"/>
Outbound Proxy	<input type="text"/>
Backup Outbound Proxy	<input type="text"/>
DNS Mode	A Record <input type="button" value="v"/>
SIP User ID	<input type="text"/>
Authentication ID	<input type="text"/>
Password	<input type="text"/>
TEL URI	Disabled <input type="button" value="v"/>

SIP Advanced Settings

Registration Expiration(m)	60
Local SIP Port	5060
SIP Transport	UDP <input type="button" value="v"/>
Stream	Stream 2 <input type="button" value="v"/>

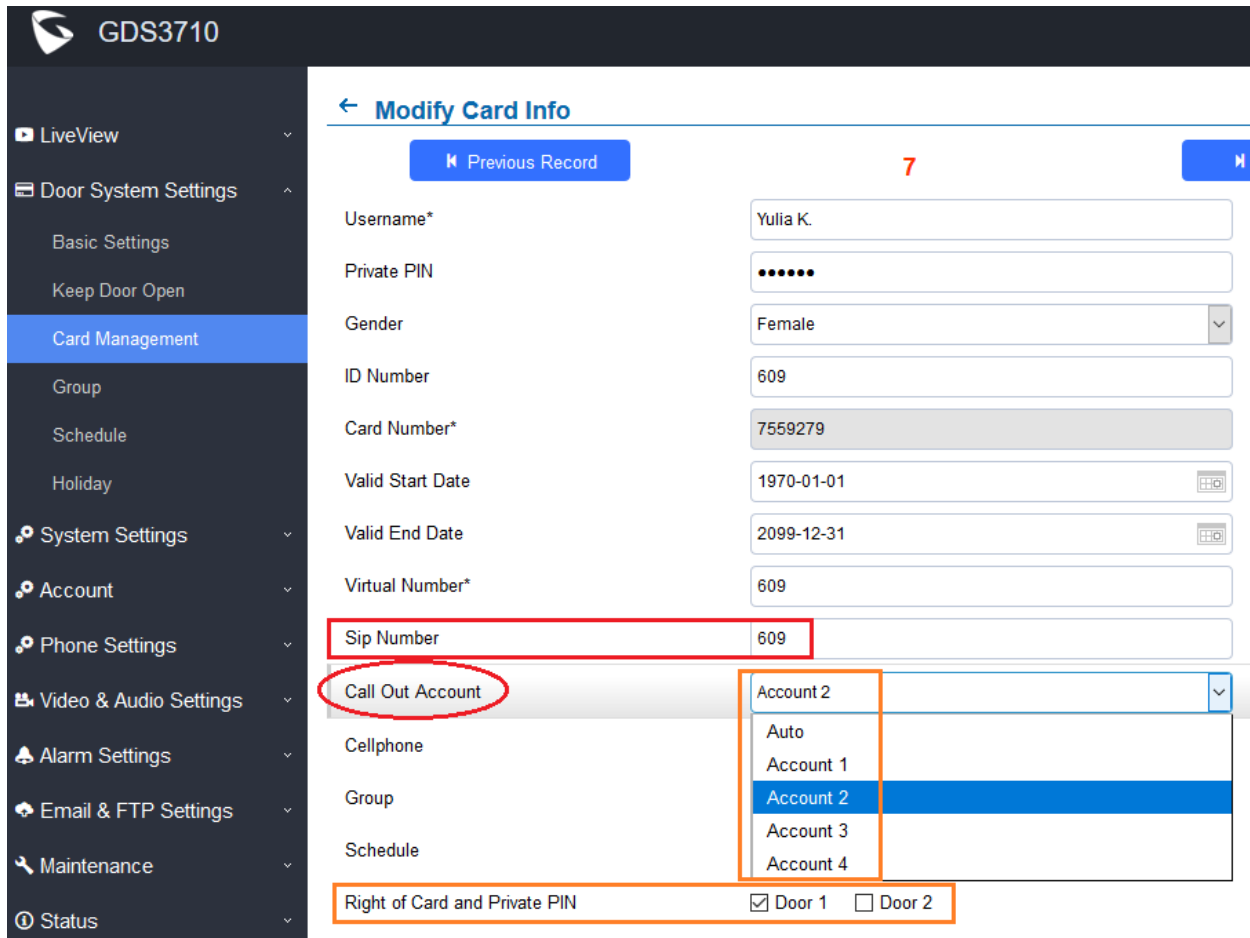
- **Functionality**

This is a major feature enhancement. Now GDS3710 can be registered to up to 4 different SIP Proxy or IPPBX to make calls and open doors.

Both “SIP Basic Settings” and “SIP Advanced Settings” are now located in the same UI page. See the above webUI screenshot for reference.

This feature is good for a building leased to different companies with own IPPBX but only one entrance or door. Now the doorbell can be programed to call different extensions of different IPPBX to allow guests or visitors to get into the building by different companies.

The number belongs to which SIP Proxy or IPPBX can be selected in the “Call Out Account” setting under “Card Management” page. Also which door the Card/PIN can be granted access also configured here. SIP number or the Virtual Number can be assigned here either. Please refer to below screenshot:



GDS3710

← Modify Card Info

[Previous Record](#) 7 [Next Record](#)

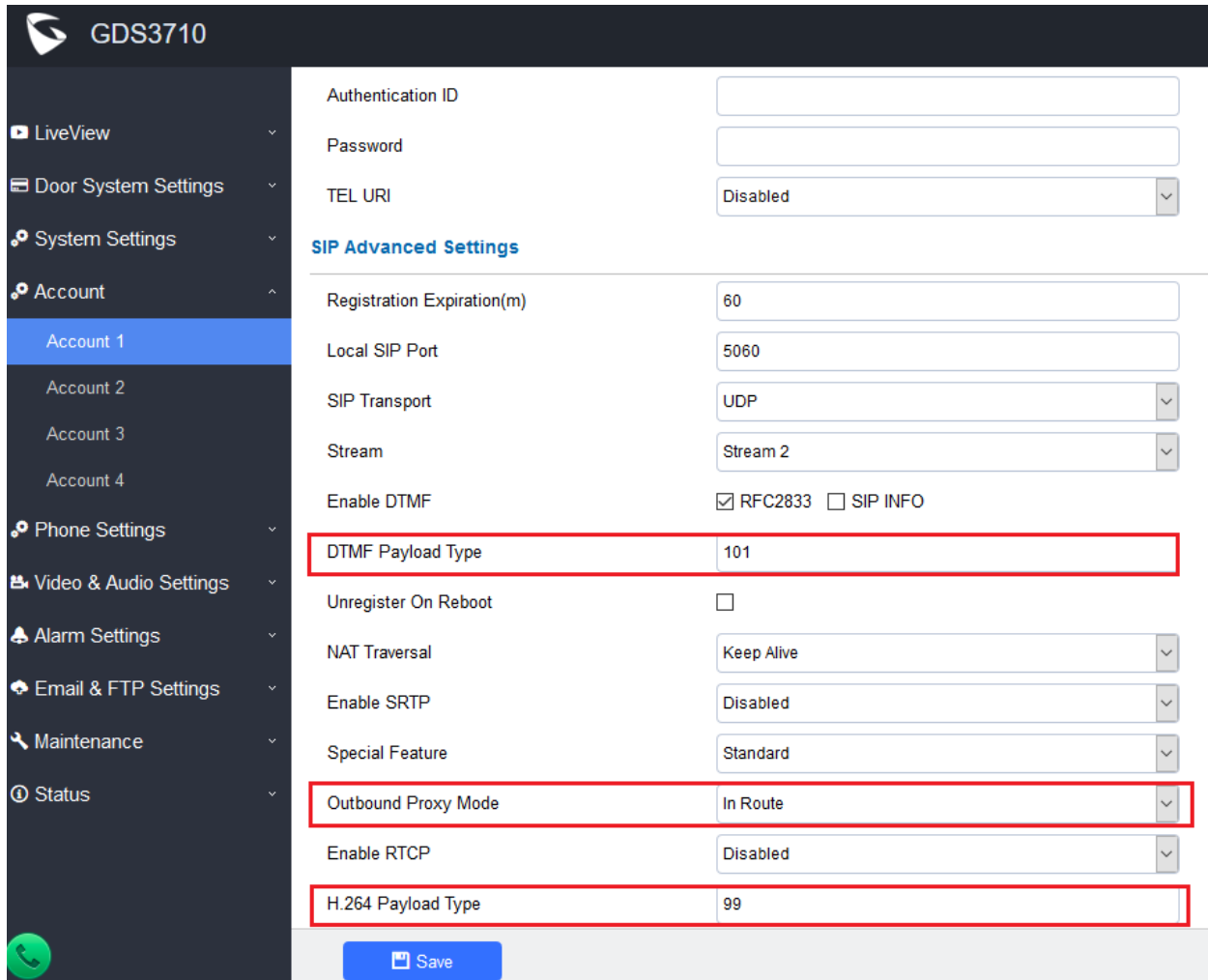
Username*	Yulia K.
Private PIN	•••••
Gender	Female
ID Number	609
Card Number*	7559279
Valid Start Date	1970-01-01
Valid End Date	2099-12-31
Virtual Number*	609
Sip Number	609
Call Out Account	Account 2
Cellphone	
Group	
Schedule	
Right of Card and Private PIN	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2

For special situation where no RFID card is assigned, system administrators can manually create a fake non-duplicable random number as “Card Number” (this is the database index, cannot be empty) but associate it with created PIN or SIP number or Virtual Number, as well as the Schedule or Group to control the door access privilege. Like for example, create these for guests, temporary or seasonal employees, cleaning ladies, contractors or UPS/FedEx person or postman.

CONFIGURE H.264, DTMF PAYLOAD AND PROXY ROUTE VALUE

- **Web Configuration**

This option can be found under device web UI → Account → Access X → SIP Advanced Settings:



GDS3710

LiveView

Door System Settings

System Settings

Account

Account 1

Account 2

Account 3

Account 4

Phone Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status

Authentication ID

Password

TEL URI

Disabled

SIP Advanced Settings

Registration Expiration(m)

60

Local SIP Port

5060

SIP Transport

UDP

Stream

Stream 2

Enable DTMF

☒ RFC2833 ☐ SIP INFO

DTMF Payload Type

101

Unregister On Reboot

☐

NAT Traversal

Keep Alive

Enable SRTP

Disabled

Special Feature

Standard

Outbound Proxy Mode

In Route

Enable RTCP

Disabled

H.264 Payload Type

99

Save

- **Functionality**

These parameters are designed for more compatibility with 3rd parties SIP Proxy or IPPBX and good for ITSP service providers as well as System Integrators. The parameters can be adjusted by just fill in the corrected value.

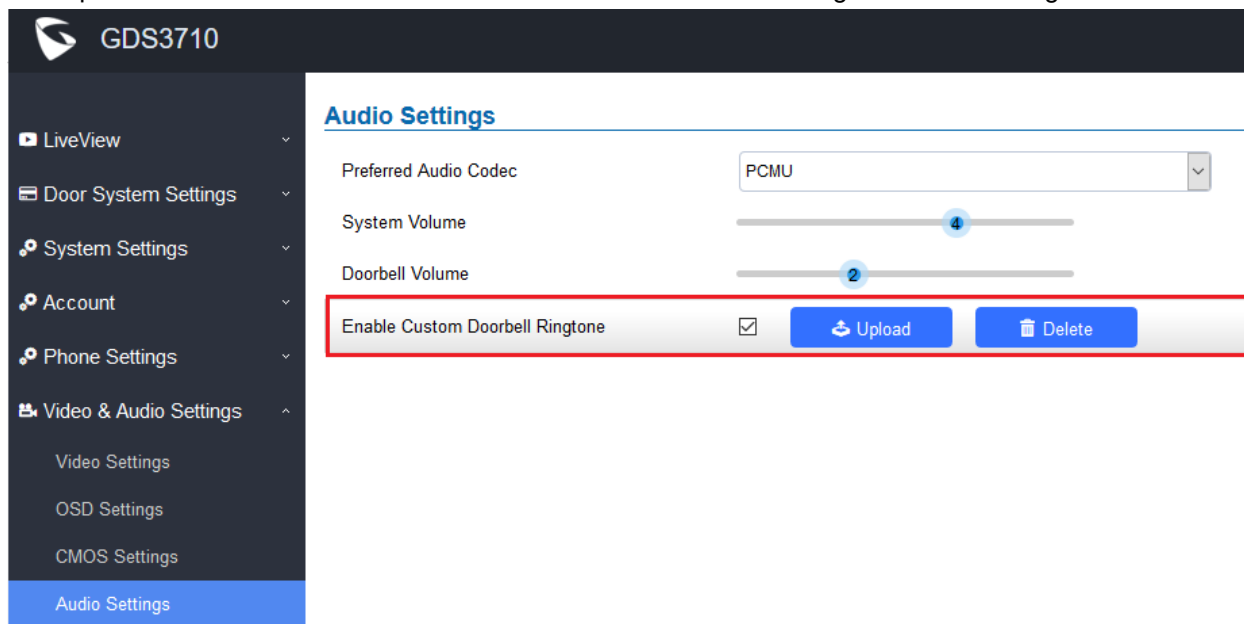
NOTE:

- *Make sure correct value are filled in. Otherwise DTMF open door will fail, there will be no video and sometimes the call will just fail to establish.*
- *If do not know the meaning of the value adjusted, please just use the default value.*

ADD OR DELETE CUSTOMIZED DOORBELL TONE

- **Web Configuration**

This option can be found under device web UI → Video & Audio Settings → Audio Settings:



- **Functionality**

This is an enhancement to allow user to upload own customized doorbell tones to meet the application scene requirement.

Please strictly follow below file requirement to upload working files:

Enable Custom Doorbell Ringtone

Support upload WAV, PCM audio file(size <= 600K). Format limit to:

WAV:

1. Sample Rate: 8k or 16k.
2. Channel: Mono-channel or Dual-channel.

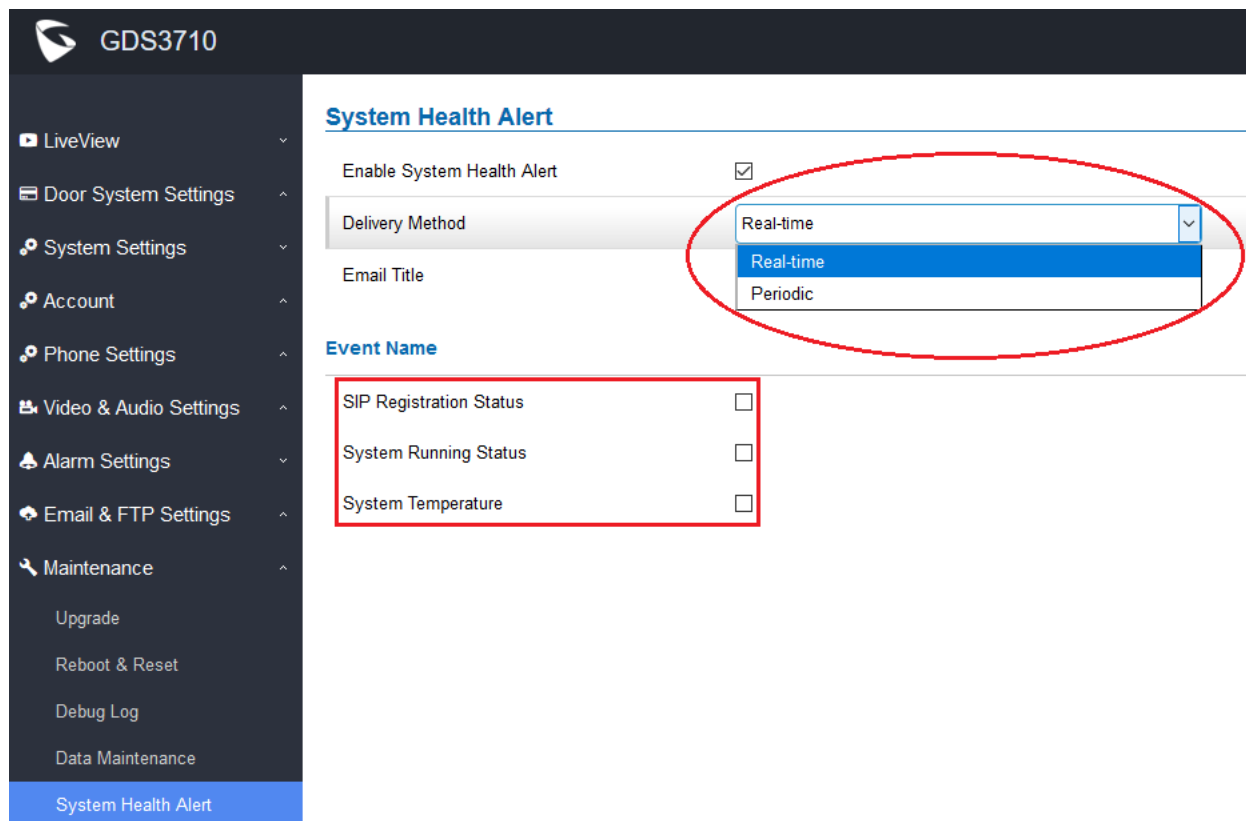
PCM:

1. Sample Rate: 8K.
2. Channel: Dual-channel.

SYSTEM HEALTH ALERTS VIA EMAIL

- **Web Configuration**

This option can be found under device web UI → Maintenance → System Health Alert:



The screenshot shows the 'System Health Alert' configuration page for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Upgrade, Reboot & Reset, Debug Log, Data Maintenance, and System Health Alert (highlighted in blue). The main content area is titled 'System Health Alert' and includes the following settings:

- Enable System Health Alert:** A checkbox that is checked.
- Delivery Method:** A dropdown menu with three options: 'Real-time' (selected and highlighted in blue), 'Real-time', and 'Periodic'. This dropdown is circled in red.
- Email Title:** A text input field.
- Event Name:** A section with three checkboxes:
 - SIP Registration Status
 - System Running Status
 - System Temperature
 This section is enclosed in a red rectangular box.

- **Functionality**

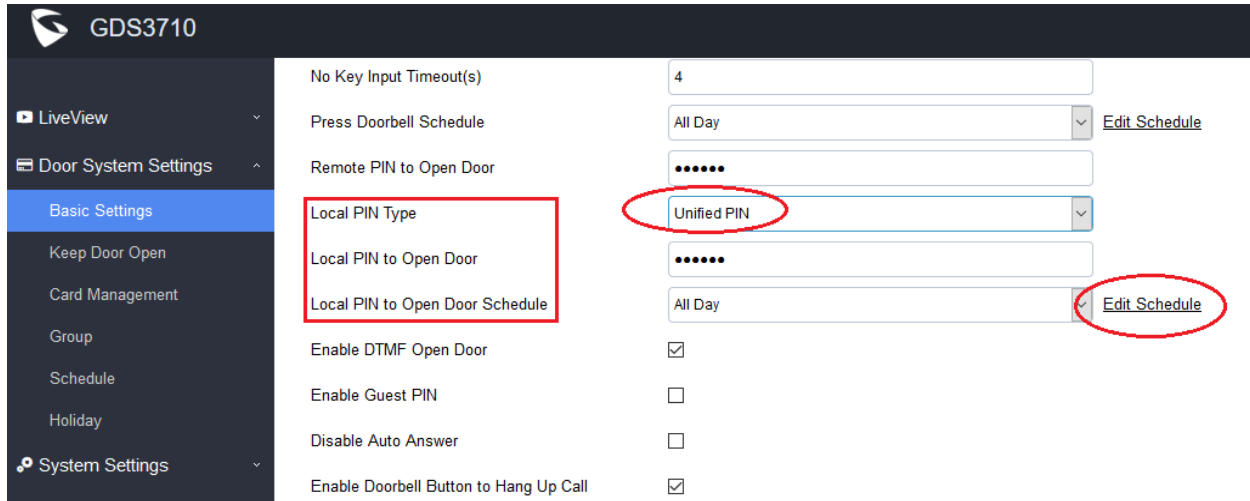
This is an enhancement requested by ITSP service providers as well as lots of system integrators from Forum. This feature allows them to get updated System Health Alert via email either in real time or in a period of time when configured.

The events name can be selected during the configuration. For all this to be working, the SMTP has to be configured and proof working otherwise email not working all in vain.

SET SCHEDULE FOR LOCAL PIN TO OPEN DOOR

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



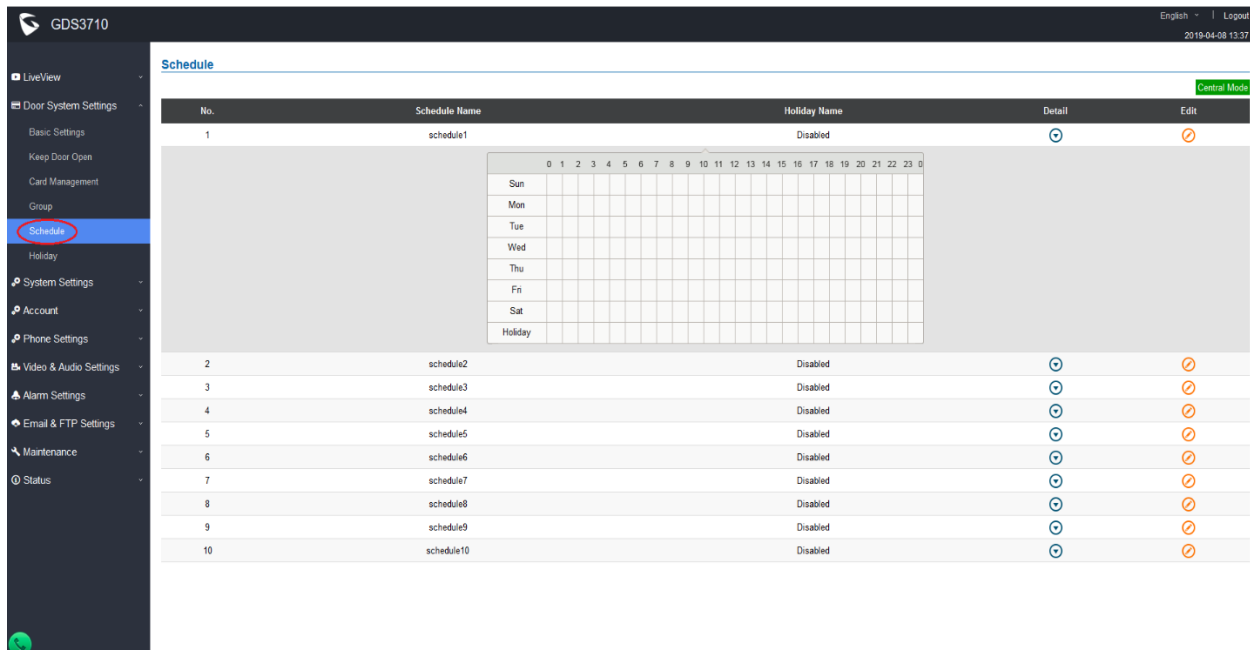
The screenshot shows the 'Basic Settings' page for the GDS3710 device. The left sidebar contains a menu with 'LiveView', 'Door System Settings', 'Basic Settings' (highlighted), 'Keep Door Open', 'Card Management', 'Group', 'Schedule', 'Holiday', and 'System Settings'. The main content area displays various settings:

- No Key Input Timeout(s): 4
- Press Doorbell Schedule: All Day (with an 'Edit Schedule' link)
- Remote PIN to Open Door: [Redacted]
- Local PIN Type: Unified PIN (circled in red)
- Local PIN to Open Door: [Redacted]
- Local PIN to Open Door Schedule: All Day (with an 'Edit Schedule' link circled in red)
- Enable DTMF Open Door: ☒
- Enable Guest PIN: ☐
- Disable Auto Answer: ☐
- Enable Doorbell Button to Hang Up Call: ☒

- **Functionality**

This is an enhancement for an existing features after feedbacks from customers. Currently, using Private PIN or RFID card, user can configure schedule in the “Card Management” database to control the time door can be accessed. But there is no schedule in the “Unified PIN”.

With this enhancement, users can now configure the “Schedule” to the “Unified PIN” so that the universal PIN also can be controlled by the Schedule therefore control the door access accordingly in the preconfigured time schedule.



The screenshot shows the 'Schedule' page in the GDS3710 web configuration. The left sidebar is the same as the previous screenshot, with 'Schedule' highlighted. The main content area displays a table of schedules:

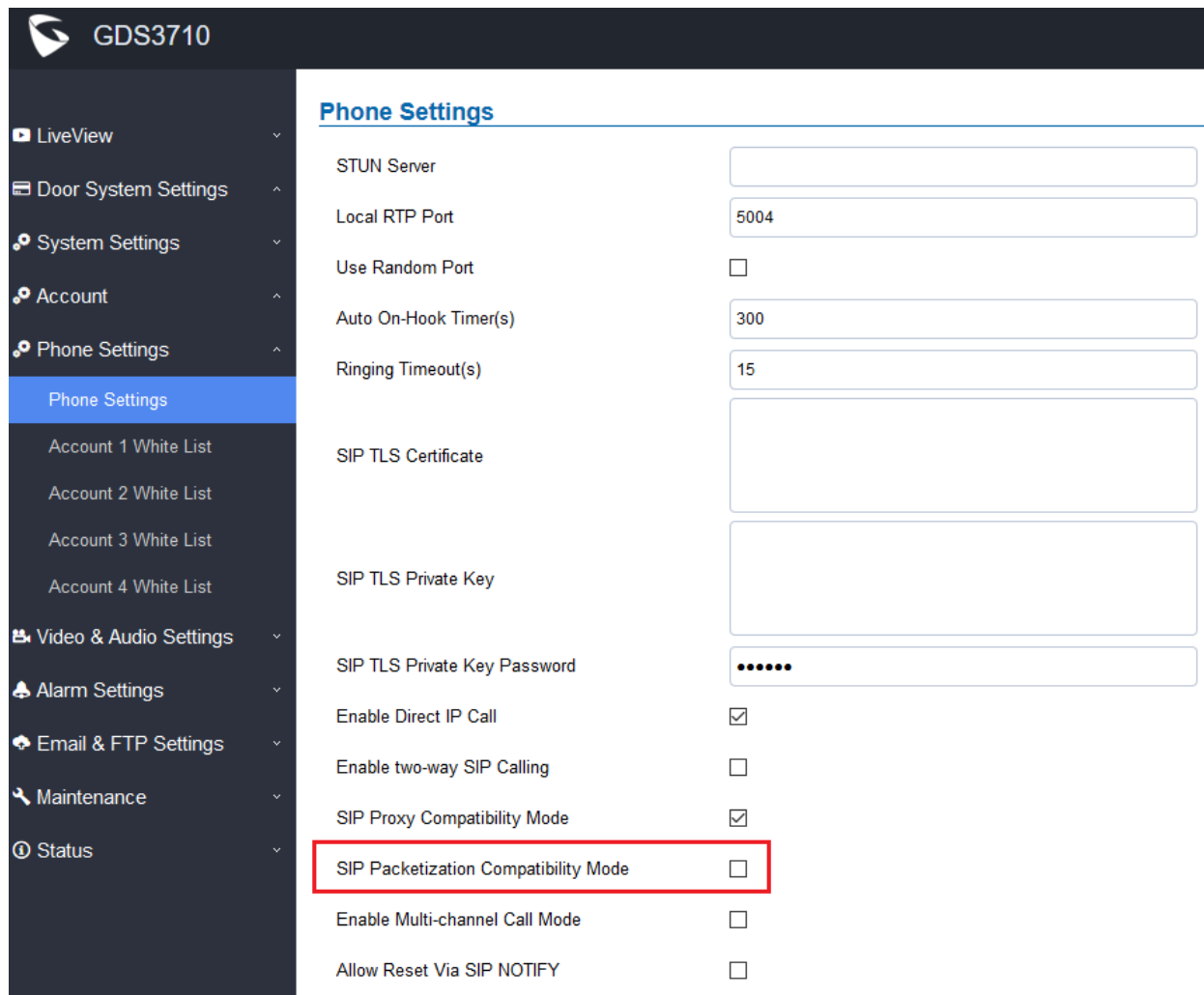
No.	Schedule Name	Holiday Name	Detail	Edit
1	schedule1	Disabled		
2	schedule2	Disabled		
3	schedule3	Disabled		
4	schedule4	Disabled		
5	schedule5	Disabled		
6	schedule6	Disabled		
7	schedule7	Disabled		
8	schedule8	Disabled		
9	schedule9	Disabled		
10	schedule10	Disabled		

Below the table, there is a calendar grid for the month of April 2019, showing days from Sunday to Saturday. The grid is currently empty, indicating no specific schedule events are configured.

SUPPORT PACKETIZATION MODE 0

- **Web Configuration**

This option can be found under device web UI → Phone Settings:



The screenshot shows the web configuration interface for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings, Account, Phone Settings, Phone Settings (highlighted), Account 1 White List, Account 2 White List, Account 3 White List, Account 4 White List, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Phone Settings' and contains various configuration options. The 'SIP Packetization Compatibility Mode' option is highlighted with a red box and is currently disabled (checkbox is unchecked).

Setting	Value
STUN Server	
Local RTP Port	5004
Use Random Port	<input type="checkbox"/>
Auto On-Hook Timer(s)	300
Ringing Timeout(s)	15
SIP TLS Certificate	
SIP TLS Private Key	
SIP TLS Private Key Password
Enable Direct IP Call	<input checked="" type="checkbox"/>
Enable two-way SIP Calling	<input type="checkbox"/>
SIP Proxy Compatibility Mode	<input checked="" type="checkbox"/>
SIP Packetization Compatibility Mode	<input type="checkbox"/>
Enable Multi-channel Call Mode	<input type="checkbox"/>
Allow Reset Via SIP NOTIFY	<input type="checkbox"/>

- **Functionality**

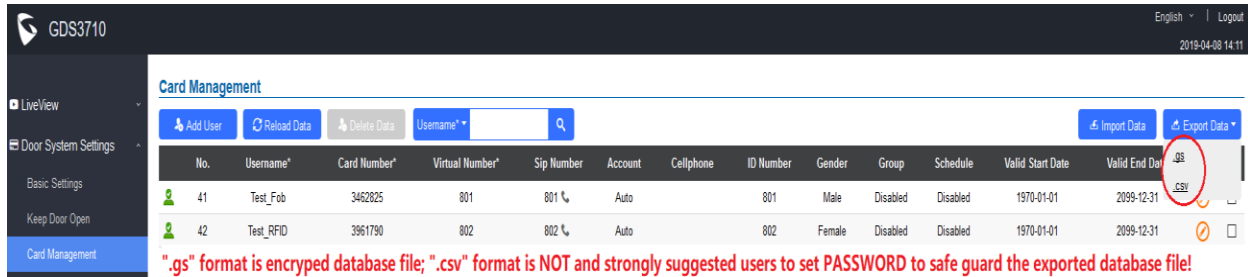
This is an enhancement for an existing features to be more compatible with 3rd party video phone devices like Cisco and Polycom.

This setting if enabled will allow GDS3710 using “Packetization Mode 0” to interact with legacy video products from Cisco or Polycom. The video from GDS3710 will be displayed in those 3rd party device.

SUPPORT CSV FORMAT WHEN IMPORT/EXPORT CARD DATA FILE

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Card Management:



Card Management

Add User | Reload Data | Delete Data | Username* | Search

Import Data | Export Data

No.	Username*	Card Number*	Virtual Number*	Sip Number	Account	Cellphone	ID Number	Gender	Group	Schedule	Valid Start Date	Valid End Date	
41	Test_Feb	3462825	801	801	Auto		801	Male	Disabled	Disabled	1970-01-01	2099-12-31	gs
42	Test_RFID	3961790	802	802	Auto		802	Female	Disabled	Disabled	1970-01-01	2099-12-31	csv

".gs" format is encrypted database file; ".csv" format is NOT and strongly suggested users to set PASSWORD to safe guard the exported database file!

- **Functionality**

This is an enhancement for an existing features after feedbacks from customers.

This setting allows user to import and export the Card Management Database using “.csv” format, in addition to the default encrypted “.gs” format. This will help system administrators using popular Excel to edit and revise the Card Information, then important back to the system in a batch mode.

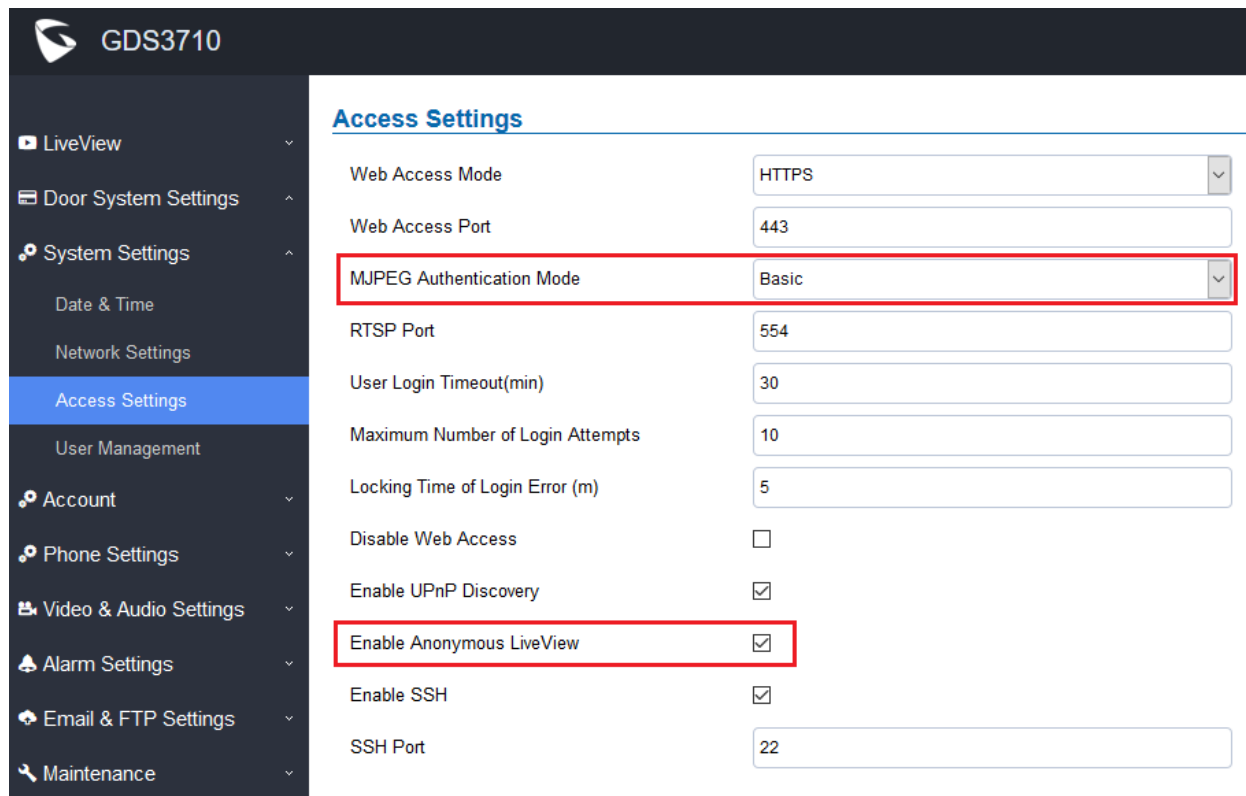
NOTE:

- “.gs” format is encrypted database file, it can NOT be edited and the password or PIN inside also can NOT be viewed.
- “.csv” format is **NOT encrypted** therefore all the content are viewable and editable. System Administrator should be VERY careful when export database in such file format, as convenience is provided in the cost of security.
- It is **STRONGLY** suggested system administrator to set PASSWORD to Safe Guard the exported CSV format database file when edit or revise the file using Excel.

SUPPORT ANONYMOUS SNAPSHOT

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



GDS3710

Access Settings

Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	554
User Login Timeout(min)	30
Maximum Number of Login Attempts	10
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22

- **Functionality**

This is a further enhancement for the already supported anonymous MJPEG LiveView streaming, request by customers like Service Provider and System Integrators or Installers. This feature allows system integrators to retrieve snapshots from GDS3710 directly without credentials, similar to fetch the live MJPEG streaming previously. This is good for system re-development.

When enabled this feature, **Special Access URL** required to retrieve the snapshot (frame by frame if refreshed) or live MJPEG video streaming:

HTTP(S)://IP_GDS3710:Port/anonymous/snapshot/view.jpg (Snapshot)
OR: HTTP(S)://IP_GDS3710:Port/anonymous/snapshot/view.html (Snapshot)

HTTP(S)://IP_GDS3710:Port/videoview.html (Live MJPEG streaming)

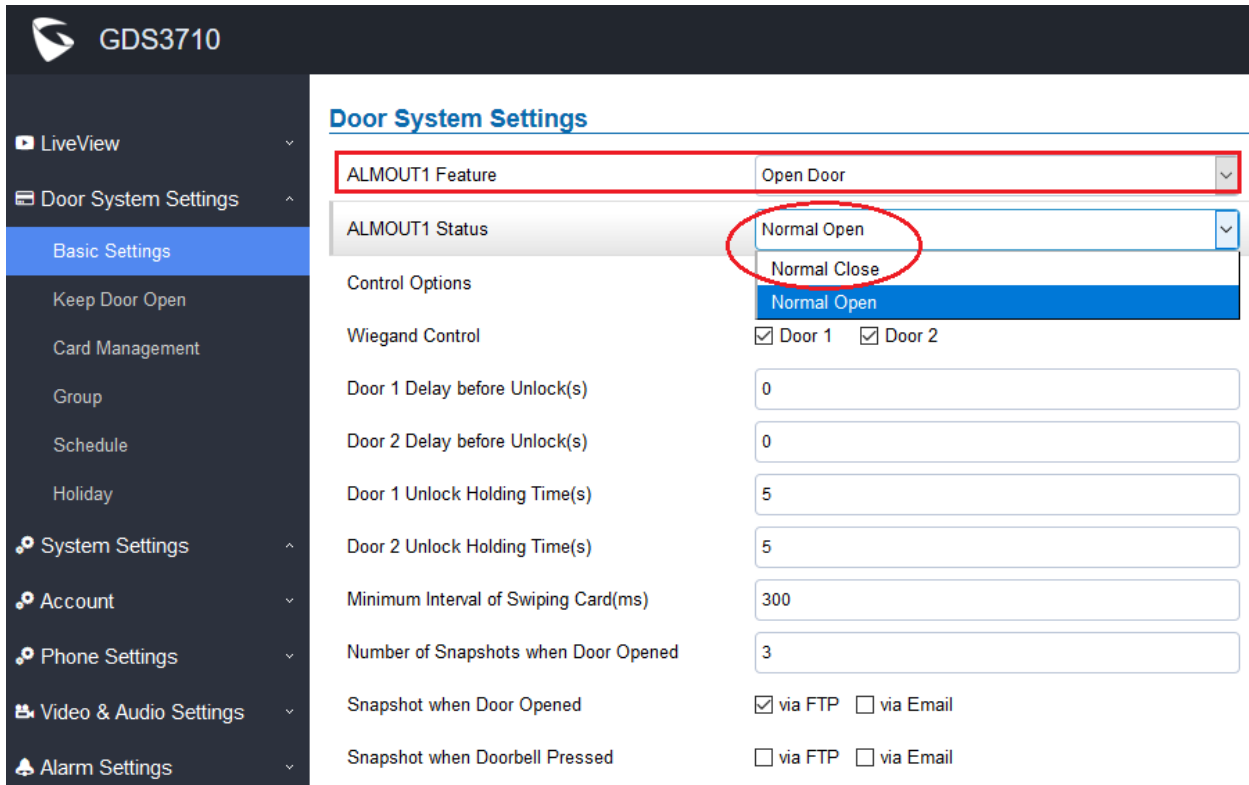
NOTE:

- Please make sure the environment is secure before enable this feature.
- Please reminder user the privacy when using this feature.

NORMAL OPEN/CLOSE IN ALARM_OUT1 (COM1) OPEN DOOR CONTROL

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

ALMOUT1 Feature: Open Door

ALMOUT1 Status: Normal Open

Control Options

Wiegand Control: ☒ Door 1 ☒ Door 2

Door 1 Delay before Unlock(s): 0

Door 2 Delay before Unlock(s): 0

Door 1 Unlock Holding Time(s): 5

Door 2 Unlock Holding Time(s): 5

Minimum Interval of Swiping Card(ms): 300

Number of Snapshots when Door Opened: 3

Snapshot when Door Opened: ☒ via FTP ☐ via Email

Snapshot when Doorbell Pressed: ☐ via FTP ☐ via Email

- **Functionality**

This is an enhancement for an existing features after feedbacks from customers.

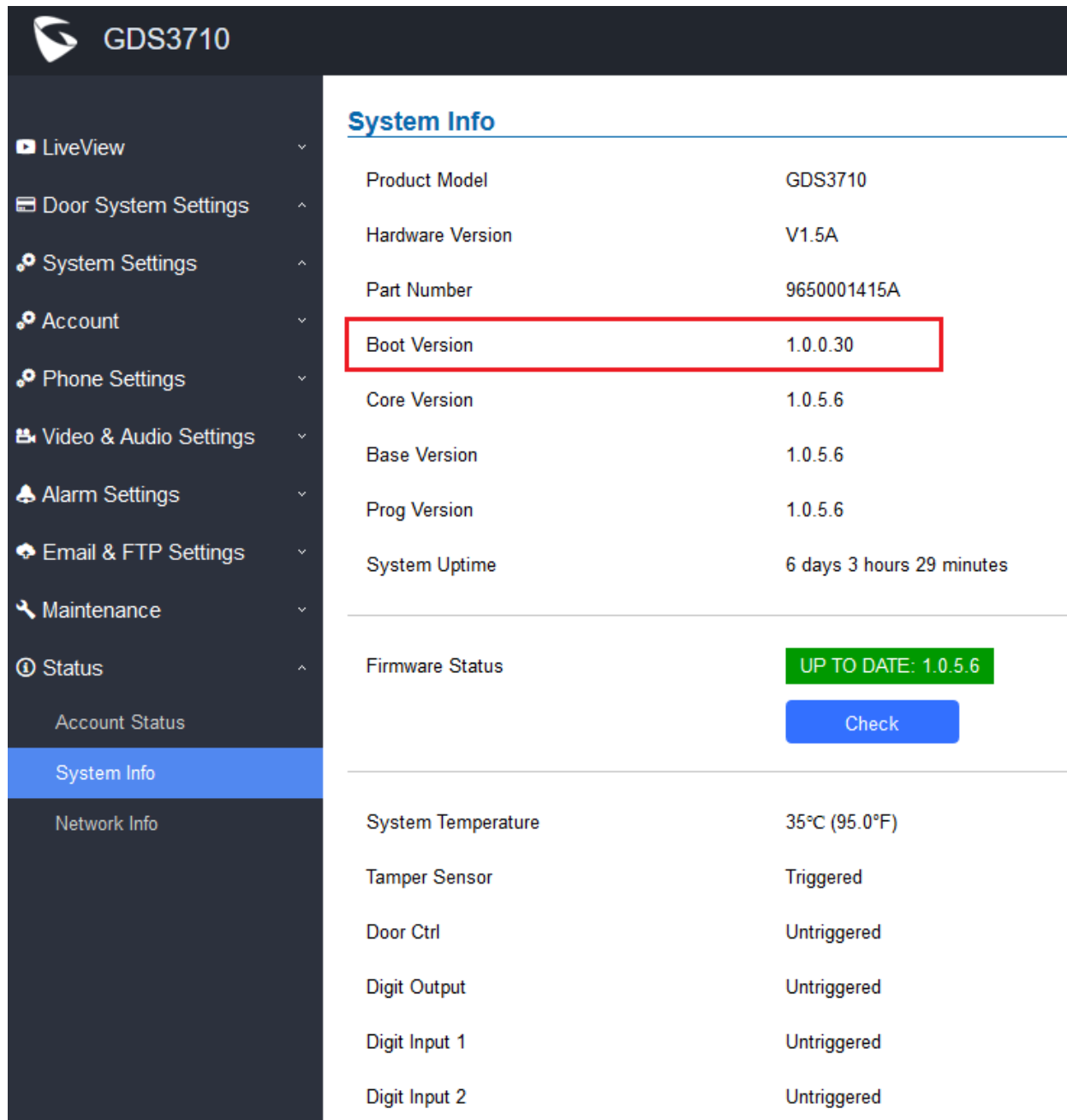
When re-using **ALMOUT1 (COM1)** interface to “Open Door” (controlling **DOOR2**) instead of “Alarm Output” (this is mutual exclusive, **ONLY** one choice will work), customers can choose “Normal Open” or “Normal Close” based on the electrical locker or striker used.

Please choose correctly based on the electrical locker or striker installed to avoid wrong operation.

ADDED BOOT VERSION IN “STATUS” PAGE

- **Web Configuration**

This option can be found under device web UI → Status → System Info:



The screenshot shows the GDS3710 web UI. On the left is a dark sidebar with a menu. The 'Status' option is selected and expanded, showing 'Account Status', 'System Info' (highlighted in blue), and 'Network Info'. The main content area is titled 'System Info' and contains a table of system details. The 'Boot Version' row is highlighted with a red border. Below the table, there is a 'Firmware Status' section with a green 'UP TO DATE: 1.0.5.6' status and a blue 'Check' button. At the bottom, another table lists hardware status items like System Temperature, Tamper Sensor, and various digital inputs/outputs.

System Info	
Product Model	GDS3710
Hardware Version	V1.5A
Part Number	9650001415A
Boot Version	1.0.0.30
Core Version	1.0.5.6
Base Version	1.0.5.6
Prog Version	1.0.5.6
System Uptime	6 days 3 hours 29 minutes

Firmware Status	
Firmware Status	UP TO DATE: 1.0.5.6
	Check

System Temperature	35°C (95.0°F)
Tamper Sensor	Triggered
Door Ctrl	Untriggered
Digit Output	Untriggered
Digit Input 1	Untriggered
Digit Input 2	Untriggered

- **Functionality**

This is an enhancement to display more technical information of GDS3710 in the “Status” page to help supporting users or customers when doing troubleshooting.

FIRMWARE VERSION 1.0.5.2

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

12/26/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement since firmware 1.0.4.9. Added lots of features and bug fixes. This firmware can NOT be downgraded to below 1.0.4.9.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI. Please backup the configuration and data before factory reset and import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added Alarm_Out port (COM1 interface) be used as Open Door 2. This mutual-exclusive function allows this port to be either as additional Open Door interface (together with COM2 interface now GDS3710 can control two doors) or normal Alarm_Out interface for 3rd party device. The two doors can be controlled by RFID, local and remote PINs respectively. This is a major enhancement, please refer User Manual for more details and how to use.
- Added option to Enable/Disable WebUI access.
- Added option to define number of snapshots to be uploaded when opening door
- Added option to specify digital input to be normal Open or normal Close
- Added ability to set schedule for Alarm In door opening
- Added support for using Digit Only as Private PIN
- Added option to configure “No Key Entry Timeout”
- Added ability to email snapshot when door opened
- Added option to allow anonymous viewing
- Added ability to display Motion Detection Region Configuration via popular browsers (Firefox, Chrome) without installing plugin, same as LiveView.
- Added option to configure payload type for H.264 (default value 99, adjusted to be more compatible)
- Extended VLAN tag ranges from 0 ~ 255 to 0 ~4094
- Added option to use Emergency PIN to overwrite “Keep Door Open” schedule and lockdown
- Enhanced debug logs and tagged with product model, MAC address
- Enhanced syslog messages by removing unnecessary details from the logs
- Added check and upgrade firmware feature in the “Status → System Info → Firmware Status” page
- Added ability to configure device with custom certificate signed by custom CA certificate
- Added device temperature to be displayed in Fahrenheit as well as Celsius
- Added support for special character “@” in the SIP User ID
- Added support of strong password including special characters for the GDS3710
- Added support of SIP NOTIFY to factory reset
- Added event log showing who opened the door using private PIN
- Added CONFIG for firmware and configure server path and type via SSH.
- Added PING function in the CLI interface SSH.

BUG FIX

- Fixed keypad no response issue.
- Fixed One Key Open Door feature failed in preview (early media) mode via parallel hunting
- Fixed IP peering call would fail if outbound proxy configured
- Fixed the open door delay when using DTMF method
- Fixed any key press will turn off the doorbell blue light when “enable doorbell blue light” configured
- Fixed randomly no audio issue on GDS3710 side
- Fixed video from GDS3710 frozen when hold/unhold twice by the video phone
- Fixed cannot set time zone ‘P64’ value via provisioning when DST ‘P10004’ enabled
- Fixed SIP password visible in the webUI
- Fixed incorrect warning message in event log
- Fixed STUN will not resolve when FQDN configured as STUN server
- Fixed pressing doorbell button would hang up the alarm call
- Fixed doorbell ‘Ding Dong’ sound non-stop if SIP account unregistered
- Fixed keypad no response issue
- Fixed security vulnerability to compromise root access via SSH
- Fixed GDS3710 ringback tone stops after 15 seconds when calling with GXV3370
- Fixed only the 1st extension or IP will be called if clicking the phone icon at webUI of “Basic Settings”
→ “Number Called When Door Bell Pressed” field
- Fixed GDS3710 falling into reboot cycle when provisioning with Broadsoft platform
- Fixed syslog with wrong timestamp issue
- Fixed failure to import/export setting of “Enable Anonymous LiveView”
- Fixed webUI access in some situation appearing close_wait issue
- Fixed error prompt when click retrieve lost/forgot password at logon home page
- Fixed GDS3710 always send H.264 RTP with lever 3.0 not adjust to 200OK SDP negotiation
- Fixed device during firmware upgrade keep on request for upgrade therefor into reboot loop
- Fixed alarm no sound when doorbell set volume level 0 and system set volume lever 6

KNOWN ISSUES

- LiveView page, the page may crash if click the “Local Configuration Function”
- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call.
- Doorbell pressed when multiple extensions configured in parallel hunting open door, if no answer and the call over time, the last call channel mapped LED indicator will not light off until manual intervene
- Open Door and Alarm snapshots, the file names are inconsistent when using Email, FTP, Central Storage, they should be synchronized.

NEW P-VALUE

P-Value	Values	Default Value	Comments
P8475	Type : string MAX length = 4096	NULL	Custom Certificate
P15476	0: Disable 1: Enable	0	Enable / Disable Reset via SIP NOTIFY

P15450	0: Alarm Output 1: Open Door
P15470	0: Normal Close 1: Normal Open
P15467	0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15468	0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15465	0 -- 20
P15466	1 -- 20
P15436	0 -- 60
P15474	0 – 20 and no more than 'Unlock Action Holding Time' value
P15475	0 – 20 and no more than 'Door 2 Unlock Action Holding Time' value
P14103	0: No 1: Yes
P15471	0: No 1: Yes
P15460	Max. length = 8
P15435	Max. length = 8
P15455	0: Disable 1: Immediate Open Door 2: Schedule Open Door
P15472	Max. length = 8
P15456	5 - 480
P15457	
P15458	
P15459	
P15473	0: Disable 1: Enable
P15469	0: Disable 1: Enable
P462	96-127
P15451	0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15431	0: Normal Open 1: Normal Close
P15452	0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15432	0: Normal Open 1: Normal Close

NEW HTTP API

P15476	GET:[http https]://<servername>/goform/config?cmd=get&type=sip SET:[http https]://<servername>/goform/config?cmd=set&P15476=<value>	0: Disable 1: Enable
P8475	GET: http://ip:port/goform/config?cmd=get&type=trustedca SET: http://ip:port/goform/config?cmd=set&P8475=<value>	Value=string, MAX length=4096
Check / Upgrade	SET: <a href="https://ip:port/goform/config?cmd=fw_upgrade&type=<value>">https://ip:port/goform/config?cmd=fw_upgrade&type=<value>	0: check available firmware version 1: firmware upgrade
P15450	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15450=<value>	0: Alarm Output 1: Open Door
P15470	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15470=<value>	0: Normal Close 1: Normal Open
P15467	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15467=<value>	0: Door1 Door2 2: Door1 & Door2 3: None
P15468	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15468=<value>	0: Door1 Door2 2: Door1 & Door2 3: None
P15465	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15465=<value>	0 ~ 20
P15466	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15466=<value>	1 ~ 20
P15436	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15436=<value>	0 ~ 60
P15474	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15474=<value>	0 ~ 20; No more than the value of "Unlock Action Holding Time"
P15475	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15475=<value>	0 ~ 20; No more than the value of "Door2 Unlock Action Holding Time"
P14103	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P14103=<value>	0: No 1: Yes
P15471	GET: http://<servername>/goform/config?cmd=get&type=door SET: http://<servername>/goform/config?cmd=set&P15471=<value>	0: No 1: Yes
P15460	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d	Max. length = 8

	oor SET: http://<servername>/goform/config?cmd=set&P15460=<value>	
P15435	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15435=<value>	Max. length = 8
P15455	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15455=<value>	0: Disable 1: Immediate Open Door 2: Schedule Open Door
P15472	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15472=<value>	Max. length = 8
P15456	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15456=<value>	5 ~ 480
P15457	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15457=<value>	
P15458	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15458=<value>	
P15459	GET: http://<servername>/goform/config?cmd=get&type=sch_open_d oor SET: http://<servername>/goform/config?cmd=set&P15459=<value>	
P15473	GET: http://<servername>/goform/config?cmd=get&type=access SET: http://<servername>/goform/config?cmd=set&P15473=<value>	0: Disable 1: Enable
P15469	GET: http://<servername>/goform/config?cmd=get&type=access SET: http://<servername>/goform/config?cmd=set&P15469=<value>	0: Disable 1: Enable
P462	GET: http://<servername>/goform/config?cmd=get&type=sip SET: http://<servername>/goform/config?cmd=set&P462=<value>	96-127
P15451	GET: http://<servername>/goform/config?cmd=get&type=event SET: http://<servername>/goform/config?cmd=set&P15451=<value>	0: Door1 Door2 2: Door1 & Door2 3: None
P15431	GET: http://<servername>/goform/config?cmd=get&type=event SET: http://<servername>/goform/config?cmd=set&P15431=<value>	0: Normal Open 1: Normal Close
P15452	GET: http://<servername>/goform/config?cmd=get&type=event SET: http://<servername>/goform/config?cmd=set&P15452=<value>	0: Door1 Door2 2: Door1 & Door2 3: None
P15432	GET: http://<servername>/goform/config?cmd=get&type=event	0: Normal Open

SET: http://<servername>/goform/config?cmd=set&P15432=<value>	1: Normal Close
---	-----------------

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

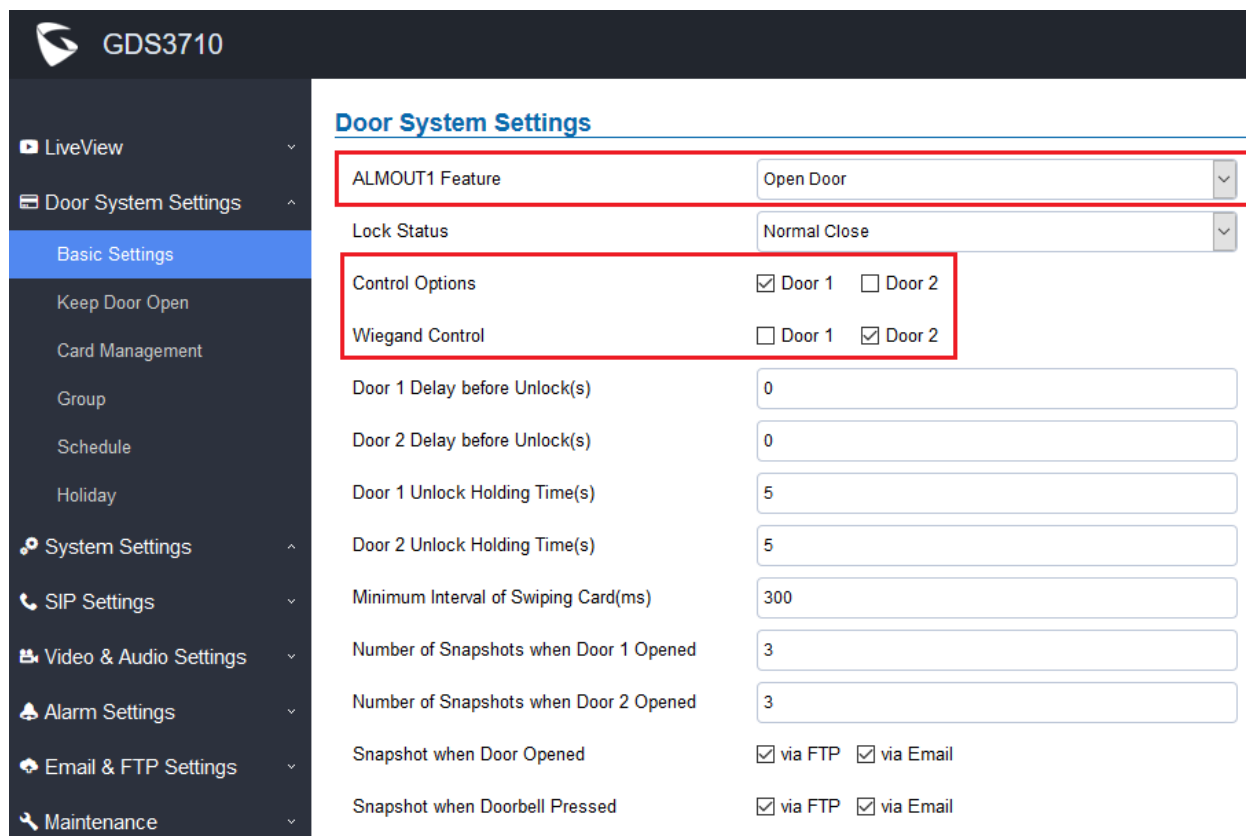
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

CONTROL DOOR2 VIA ALARM_OUT (COM1) INTERFACE

- Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

ALMOUT1 Feature: Open Door

Lock Status: Normal Close

Control Options: ☒ Door 1 ☐ Door 2

Wiegand Control: ☐ Door 1 ☒ Door 2

Door 1 Delay before Unlock(s): 0

Door 2 Delay before Unlock(s): 0

Door 1 Unlock Holding Time(s): 5

Door 2 Unlock Holding Time(s): 5

Minimum Interval of Swiping Card(ms): 300

Number of Snapshots when Door 1 Opened: 3

Number of Snapshots when Door 2 Opened: 3

Snapshot when Door Opened: ☒ via FTP ☒ via Email

Snapshot when Doorbell Pressed: ☒ via FTP ☒ via Email

- Functionality**

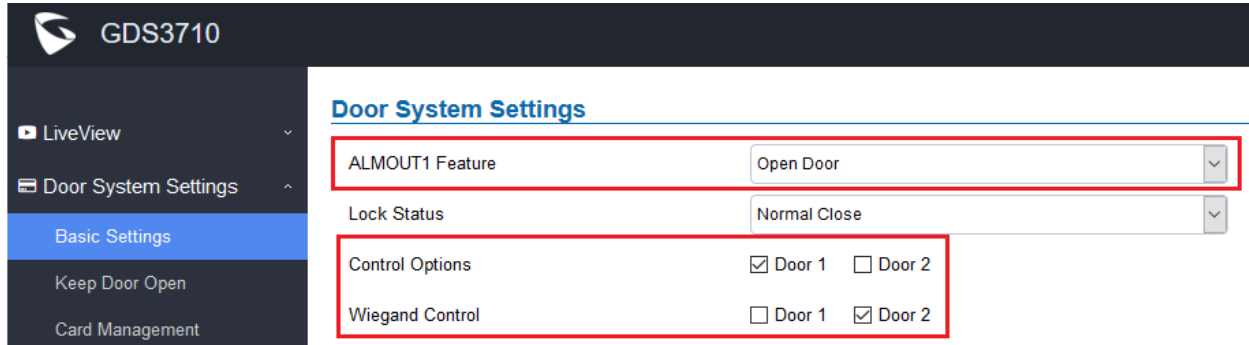
This is a major feature enhancement, by re-use Alarm_Out (COM1) interface to be either support per designed normal alarm out with 3rd party device, or control Door2 operation (the two functions are mutual-exclusive).

Customers can now use this Alarm_Out (COM1) interface to control Door2, in addition to the existing Locker/COM2 interface (controlling Door1). This feature when selected, will enable GDS3710 to control the operation of two doors via RFID, local and remote PINs.

For example, a 3rd party Wiegand Input device or GDS37xx can be installed at Door2 with related cable wired into the control GDS3710 installed at Door1. The Door1 and Door2 can be configured to be open by programmed RFID cards, PINs either separately or both.

NOTE:

- Interface for Door Control (Which Door can be OPEN):



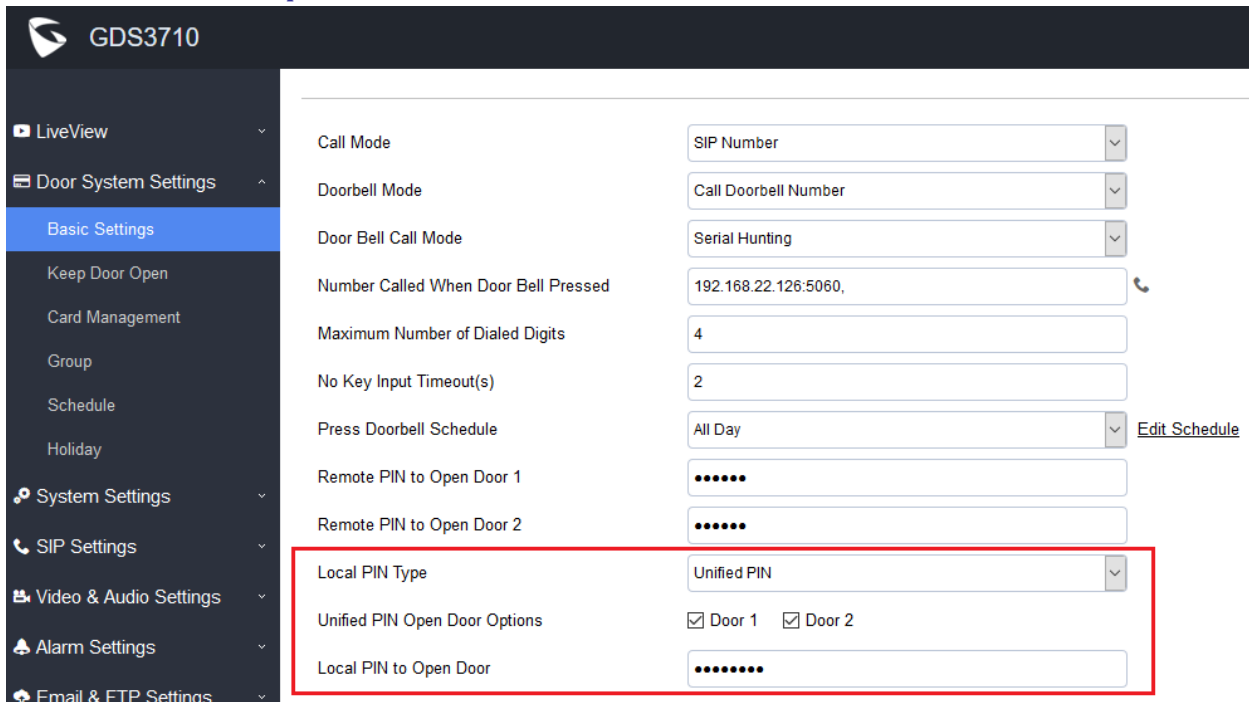
The screenshot shows the 'Door System Settings' page in the GDS3710 web interface. The left sidebar contains navigation options: LiveView, Door System Settings (selected), Basic Settings, Keep Door Open, and Card Management. The main content area is titled 'Door System Settings' and contains several configuration fields. A red box highlights the 'ALMOUT1 Feature' dropdown set to 'Open Door'. Another red box highlights the 'Lock Status' dropdown set to 'Normal Close'. A third red box highlights the 'Control Options' section, which includes checkboxes for 'Door 1' (checked) and 'Door 2' (unchecked). A fourth red box highlights the 'Wiegand Control' section, which includes checkboxes for 'Door 1' (unchecked) and 'Door 2' (checked).

If Alarm_Out (COM1) interface is set to control Door2 opening, “Lock Status” can be configured by choose “Normal Open” or “Normal Close” based on the strike used.

Unlike default COM2 which is designed for strike control and having three connecting sockets, the COM1 only has two connecting sockets. Therefore correct lock mode has to be configured to make the strike working as expected.

For above example, the GDS3710 is configured to control Door1 (wiring to COM2 interface); the 3rd party Wiegand Input is set to control Door2 (wiring to COM1 interface).

- Universal PIN for Operation of Doors:



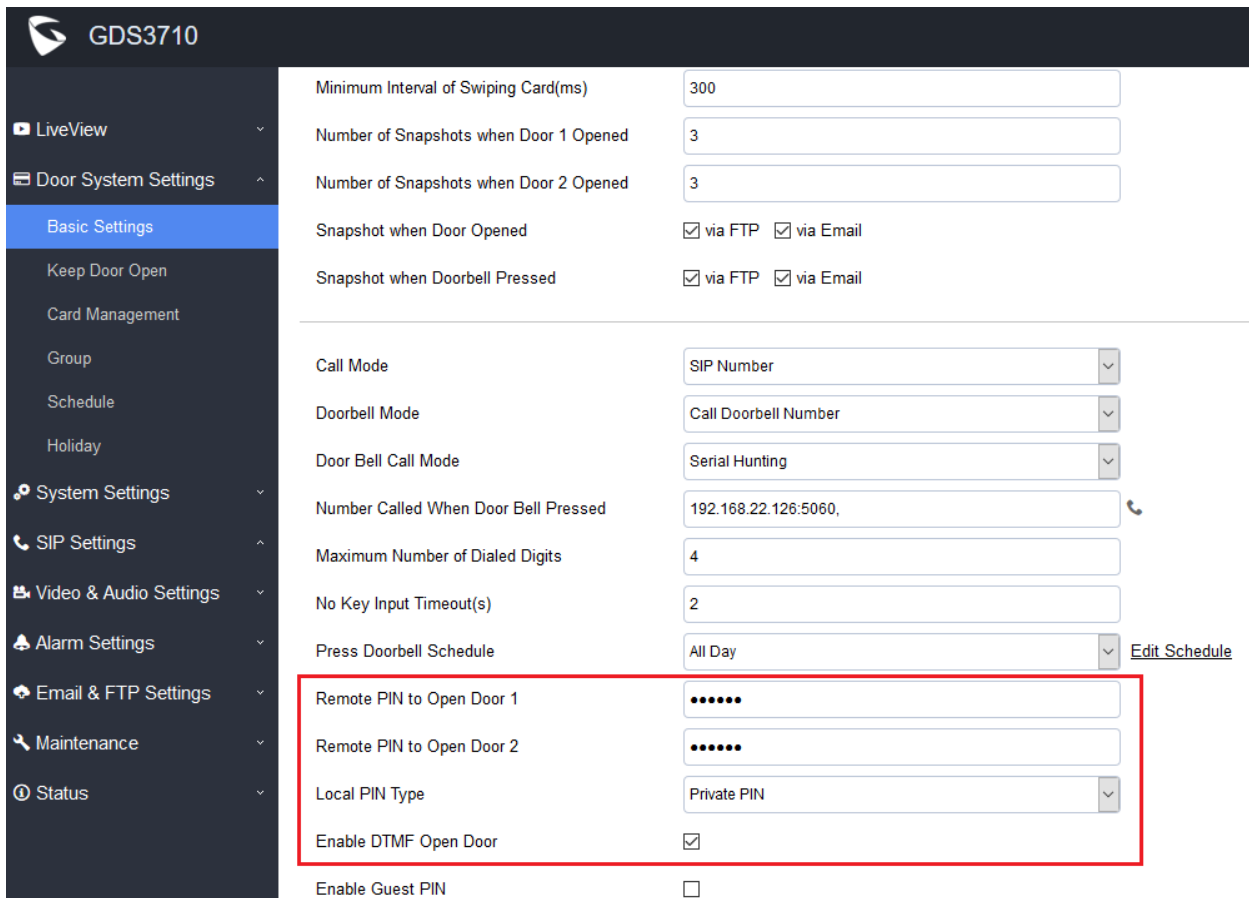
The screenshot shows the 'Universal PIN for Operation of Doors' settings page in the GDS3710 web interface. The left sidebar contains navigation options: LiveView, Door System Settings, Basic Settings, Keep Door Open, Card Management, Group, Schedule, Holiday, System Settings (selected), SIP Settings, Video & Audio Settings, Alarm Settings, and Email & FTP Settings. The main content area is titled 'Universal PIN for Operation of Doors' and contains several configuration fields. A red box highlights the 'Local PIN Type' dropdown set to 'Unified PIN'. Another red box highlights the 'Unified PIN Open Door Options' section, which includes checkboxes for 'Door 1' (checked) and 'Door 2' (checked). A third red box highlights the 'Local PIN to Open Door' field, which is currently empty.

If Unified PIN (Universal PIN) is configured to open door, then which door can be controlled by the PIN is configured in the UI once “Unified PIN” selected.

For example, like above screenshot, if this universal PIN is set to open both Door1 and Door2, but due to previous “Control Option” set to open Door1, and “Wiegand Control” set to open Door2, therefore the final result will be the **INTERSECT** result of both sets with condition qualified.


In above case, The PIN will only work at GDS3710 (Door1) and Wiegand Device (Door2) local input respectively. Meaning input PIN at GDS3710 will only open Door1 and will NOT open Door2.

- **Remote PIN to Operation of Doors:**



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
- System Settings
- SIP Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status

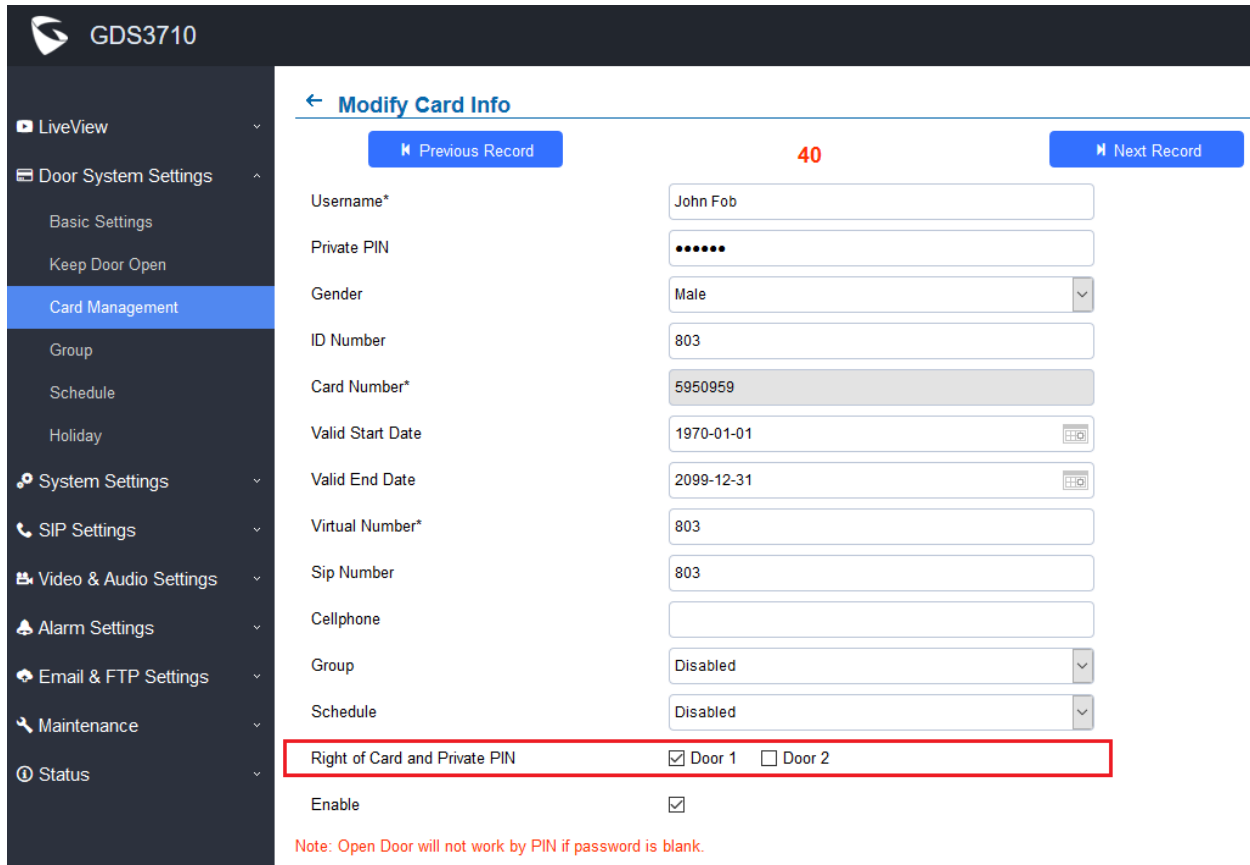
Minimum Interval of Swiping Card(ms)	300
Number of Snapshots when Door 1 Opened	3
Number of Snapshots when Door 2 Opened	3
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email
Call Mode	SIP Number
Doorbell Mode	Call Doorbell Number
Door Bell Call Mode	Serial Hunting
Number Called When Door Bell Pressed	192.168.22.126:5060, 
Maximum Number of Dialed Digits	4
No Key Input Timeout(s)	2
Press Doorbell Schedule	All Day Edit Schedule
Remote PIN to Open Door 1
Remote PIN to Open Door 2
Local PIN Type	Private PIN
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>

For remote PIN to open door, the PIN can be configured in above setting.

The PIN can be different for Door1 and Door2 and has to be configured correctly in related IP Phone which will be used to operate “One Key Open Door”.

If BOTH doors need to be opened at the same time, then both Door1 and Door2 has to be configured with exactly SAME password or PIN as DTMF open door.

- **Private PIN or Card & Private PIN:**



GDS3710

← **Modify Card Info**

Previous Record 40 Next Record

Username* John Fob

Private PIN ••••••

Gender Male

ID Number 803

Card Number* 5950959

Valid Start Date 1970-01-01

Valid End Date 2099-12-31

Virtual Number* 803

Sip Number 803

Cellphone

Group Disabled

Schedule Disabled

Right of Card and Private PIN ☒ Door 1 ☐ Door 2

Enable ☒

Note: Open Door will not work by PIN if password is blank.

If using RFID card or Private PIN to open door, then which door can be opened by the RFID card or Private PIN is configured via “Card Management”, see above screenshot.

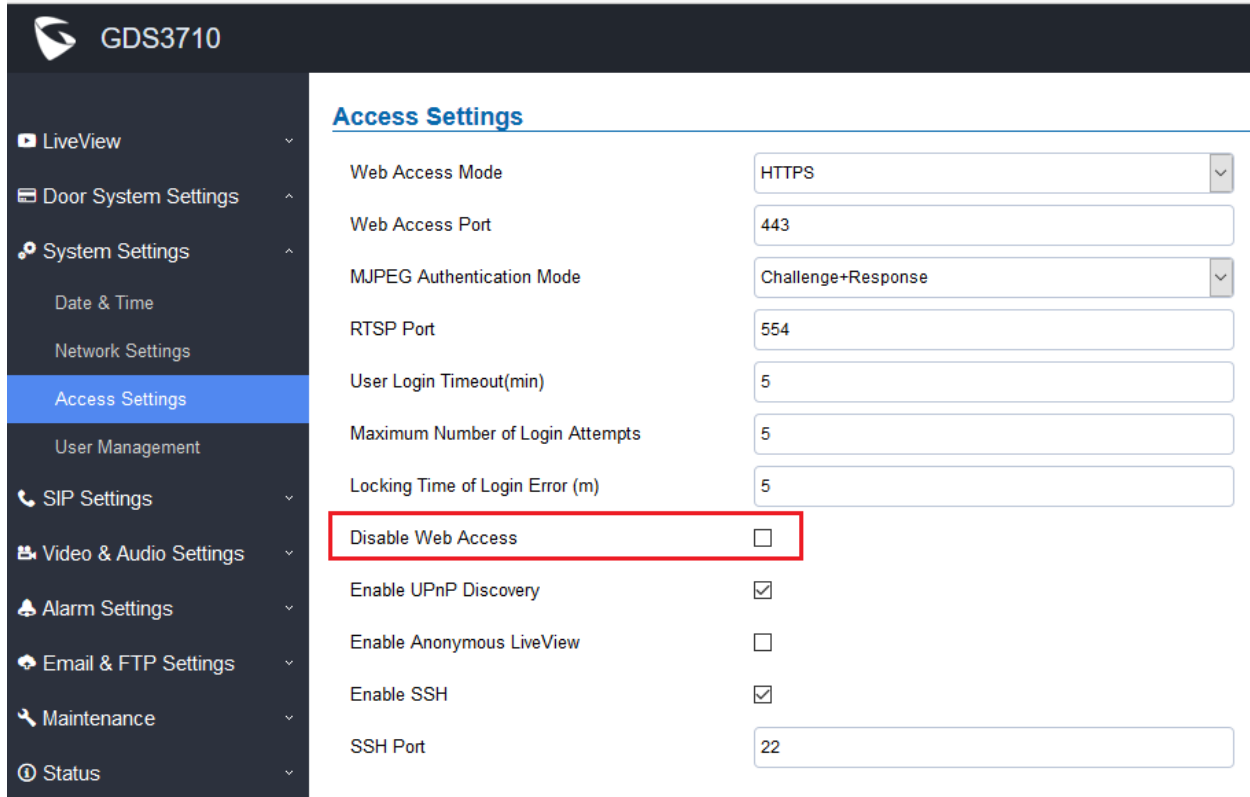
NOTE:

- For all the setting, the final result of which door can be opened is the **LOGIC INTERSECT OPERATION** of ALL the sets of condition qualified.
- Please refer to [GDS3710 User Manual](#) for details about how to configure and control the Door1 and Door2 operation respectively.

ENABLE / DISABLE WEB UI ACCESS

- Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



The screenshot shows the 'Access Settings' page for a GDS3710 device. The left sidebar contains a menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, Access Settings (highlighted), User Management, SIP Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Access Settings' and contains the following configuration items:

Setting	Value
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22

- Functionality**

This feature is designed for ITSP or service provider to “Disable” the webUI access for security or preventing end users mess up the configuration parameters. Not recommended for normal users. Please be very careful when using this feature.

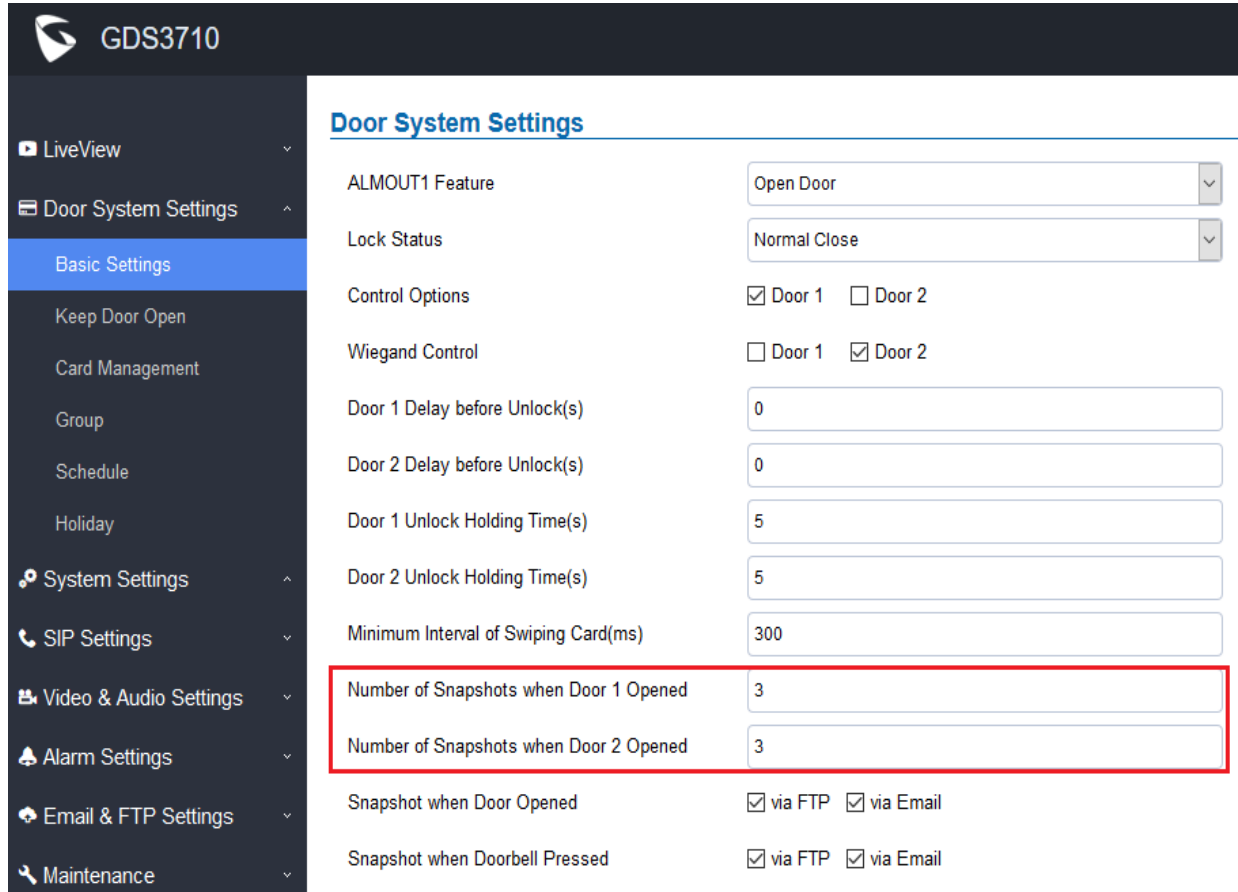
NOTE:

- If both WebUI and SSH are disabled, GDS3710 will get blocked and not be able to be accessed.*
- Only two ways to get it back:*
 - 1) Re-provisioned by ITSP or Service Provider (by adjusting the related parameters)*
 - 2) Hard Reset (GDS3710 has to be offline and uninstalled to perform this hard reset).*

DEFINE NUMBER OF SNAPSHOT UPLOADED WHEN OPEN DOOR

- Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

ALMOUT1 Feature	Open Door
Lock Status	Normal Close
Control Options	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2
Wiegand Control	<input type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Door 1 Delay before Unlock(s)	0
Door 2 Delay before Unlock(s)	0
Door 1 Unlock Holding Time(s)	5
Door 2 Unlock Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Number of Snapshots when Door 1 Opened	3
Number of Snapshots when Door 2 Opened	3
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email

- Functionality**

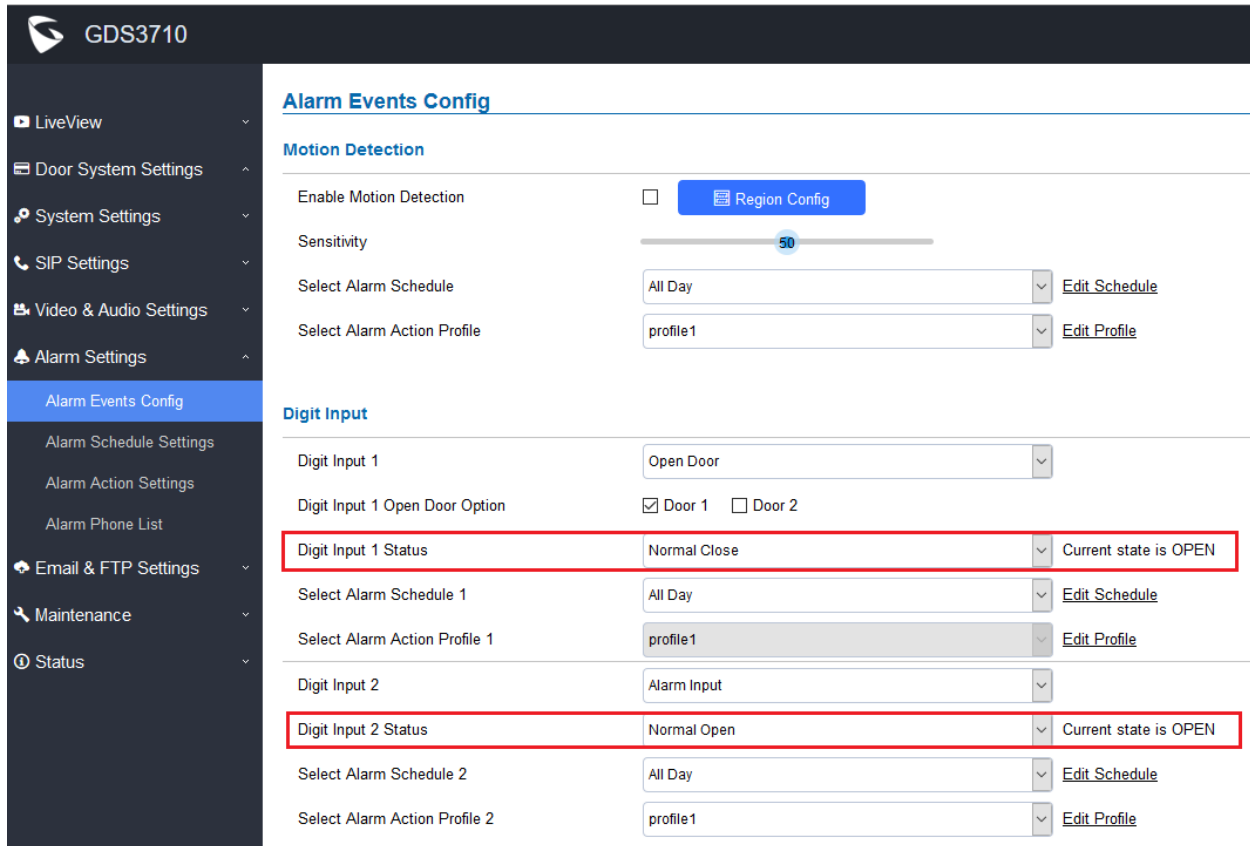
This is an enhancement for an existing feature after feedbacks from customers.

This setting allows user to get emails with snapshot attachments, or store the snapshots in the FTP server, when door is opened, or the Doorbell is pressed.

DEFINE DIGIT INPUT INTERFACE TO BE NORMAL OPEN OR CLOSE

- **Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Events Config:



GDS3710

Alarm Events Config

Motion Detection

Enable Motion Detection ☐ [Region Config](#)

Sensitivity

Select Alarm Schedule [Edit Schedule](#)

Select Alarm Action Profile [Edit Profile](#)

Digit Input

Digit Input 1

Digit Input 1 Open Door Option ☒ Door 1 ☐ Door 2

Digit Input 1 Status [Current state is OPEN](#)

Select Alarm Schedule 1 [Edit Schedule](#)

Select Alarm Action Profile 1 [Edit Profile](#)

Digit Input 2

Digit Input 2 Status [Current state is OPEN](#)

Select Alarm Schedule 2 [Edit Schedule](#)

Select Alarm Action Profile 2 [Edit Profile](#)

- **Functionality**

This is an enhancement for an existing feature after feedbacks from customers.

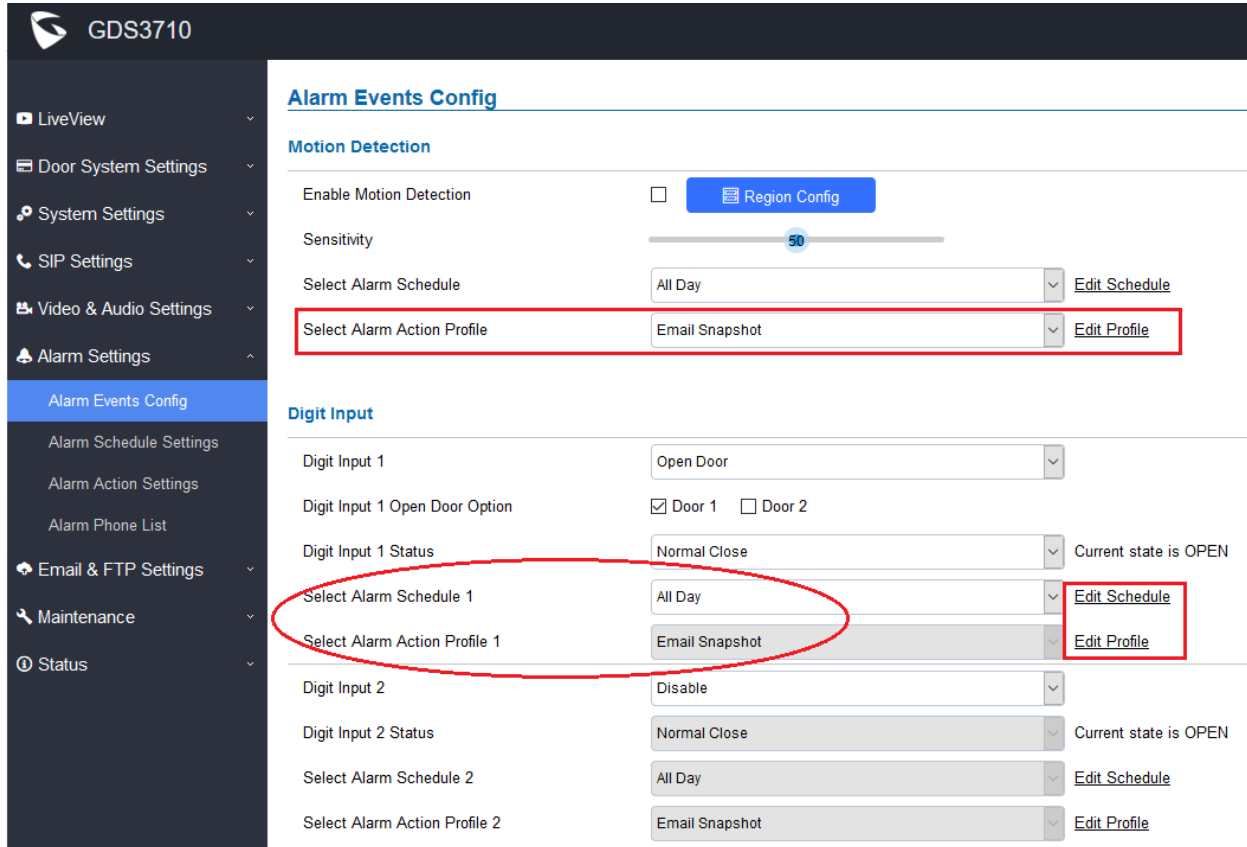
This setting allows user to select the interface to be normal Open or Close based on the 3rd party device or striker/locker used.

The Digit Input interface can be used for either Open Door or Alarm Input (by 3rd party sensors). Default is Disable therefore not used. Customers have to configure the ports before using them.

SET SCHEDULE FOR ALARM IN OPEN DOOR

- Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Events Config:



Alarm Events Config

Motion Detection

Enable Motion Detection ☐ [Region Config](#)

Sensitivity

Select Alarm Schedule [Edit Schedule](#)

Select Alarm Action Profile [Edit Profile](#)

Digit Input

Digit Input 1

Digit Input 1 Open Door Option ☒ Door 1 ☐ Door 2

Digit Input 1 Status Current state is OPEN

Select Alarm Schedule 1 [Edit Schedule](#)

Select Alarm Action Profile 1 [Edit Profile](#)

Digit Input 2

Digit Input 2 Status Current state is OPEN

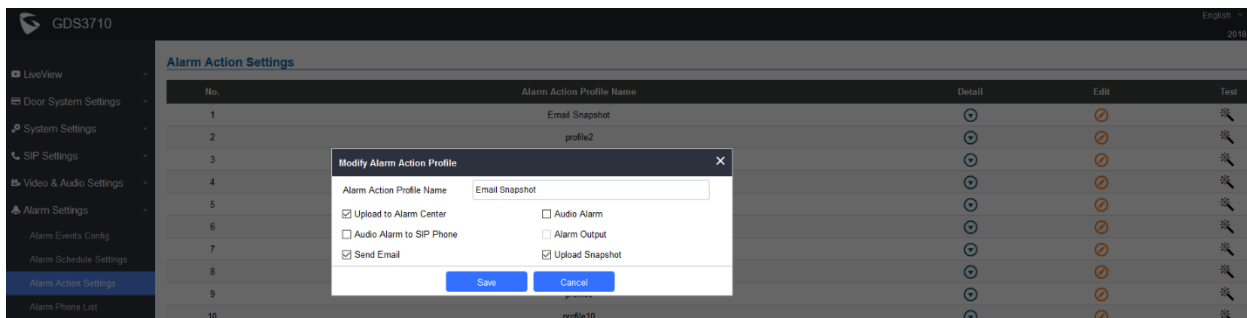
Select Alarm Schedule 2 [Edit Schedule](#)

Select Alarm Action Profile 2 [Edit Profile](#)

- Functionality**

This is an enhancement for an existing feature after feedbacks from customers. This setting allows user to set schedule and profile for Alarm In interface used as Open Door.

For example, above Alarm_In (COM1) interface configured and used as Open Door, with schedule set to “All Day” and Profile to be “Email Snapshot”, meaning this interface used as Open Door for all Days and will email snapshots when door opened.



Alarm Action Settings

No.	Alarm Action Profile Name	Detail	Edit	Test
1	Email Snapshot			
2	profile2			
3				
4				
5				
6				
7				
8				
9				
10	profile10			

Modify Alarm Action Profile

Alarm Action Profile Name

☒ Upload to Alarm Center ☐ Audio Alarm

☐ Audio Alarm to SIP Phone ☐ Alarm Output

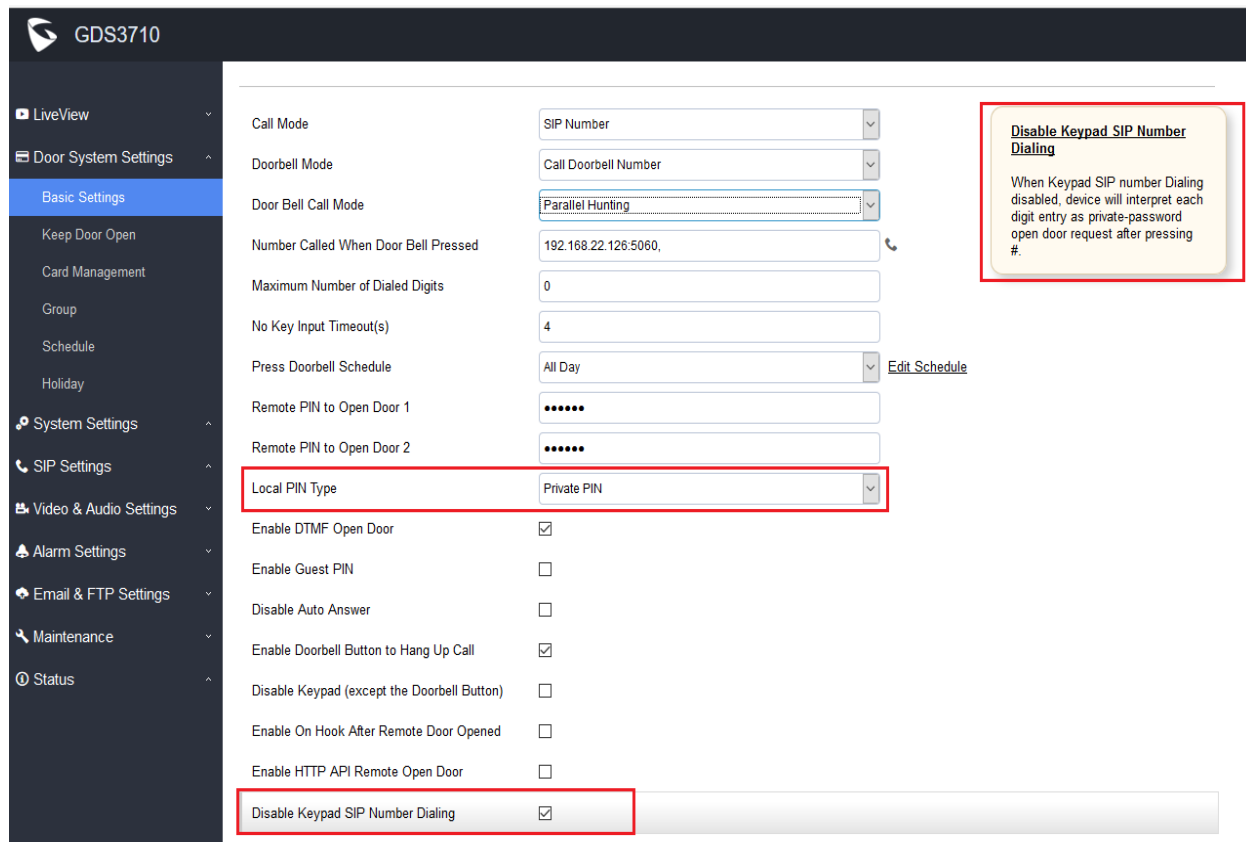
☒ Send Email ☒ Upload Snapshot

[Save](#) [Cancel](#)

OPEN DOOR VIA DIGIT ONLY PRIVATE PIN

• Web Configuration

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
- System Settings
- SIP Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status

Call Mode	SIP Number
Doorbell Mode	Call Doorbell Number
Door Bell Call Mode	Parallel Hunting
Number Called When Door Bell Pressed	192.168.22.126:5060,
Maximum Number of Dialed Digits	0
No Key Input Timeout(s)	4
Press Doorbell Schedule	All Day Edit Schedule
Remote PIN to Open Door 1	*****
Remote PIN to Open Door 2	*****
Local PIN Type	Private PIN
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>
Disable Auto Answer	<input type="checkbox"/>
Enable Doorbell Button to Hang Up Call	<input checked="" type="checkbox"/>
Disable Keypad (except the Doorbell Button)	<input type="checkbox"/>
Enable On Hook After Remote Door Opened	<input type="checkbox"/>
Enable HTTP API Remote Open Door	<input type="checkbox"/>
Disable Keypad SIP Number Dialing	<input checked="" type="checkbox"/>

Disable Keypad SIP Number Dialing

When Keypad SIP number Dialing disabled, device will interpret each digit entry as private-password open door request after pressing #.

• Functionality

This is an enhancement for an existing feature after feedbacks from customers and installers.

This setting allows user to use DIGIT ONLY private PIN to open door, with the cost of NOT be able to make any SIP calls (except for doorbell button call). User just input “**PrivatePIN#**” to open door, will NOT input PIN as SIP call enabled mode (with format “**VirtualNumber***PrivatePIN*#”. This makes the GDS3710 more like traditional access device.

NOTE:

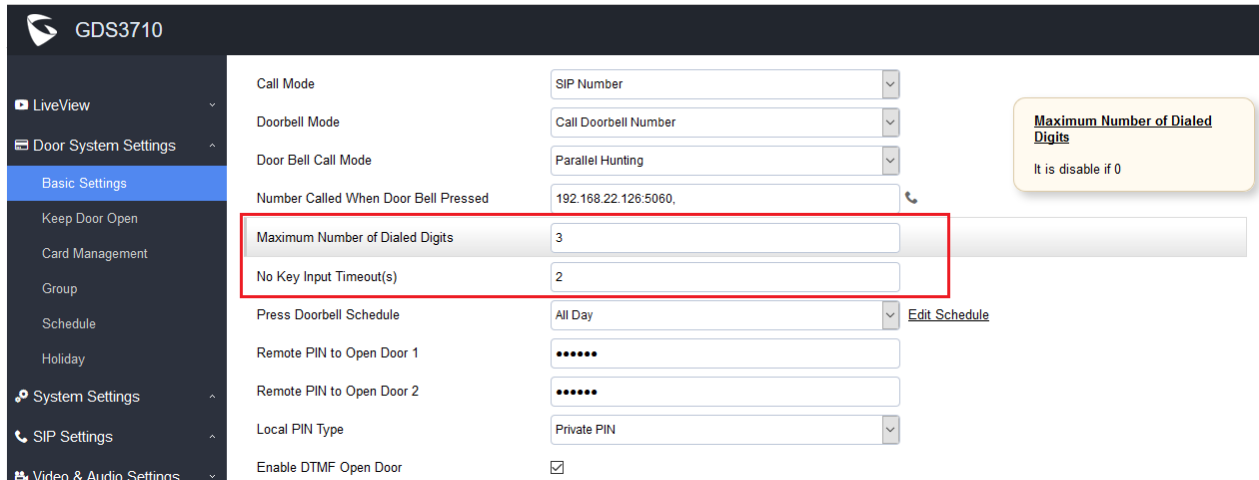
Following settings are required to make this feature working:

- “Disable Keypad SIP Number Calling” should be checked to enable this feature
- “Local PIN Type” should choose “Private PIN”
- Dial keypad to make SIP call will NOT work when above selected.
- PrivatePIN must be **UNIQUE** among users, otherwise the door will still open but log will NOT tell who opened the door due to duplicated PIN and whoever user last matched in the database with the PrivatePIN will be shown in the log.

SET “NO KEY ENTRY TIMEOUT”

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



The screenshot shows the GDS3710 web configuration interface. The left sidebar contains a menu with options: LiveView, Door System Settings (expanded), Basic Settings (selected), Keep Door Open, Card Management, Group, Schedule, Holiday, System Settings, SIP Settings, and Video & Audio Settings. The main content area displays various settings for the door system. A red box highlights the 'Maximum Number of Dialed Digits' (set to 3) and 'No Key Input Timeout(s)' (set to 2). A yellow callout box on the right states: 'Maximum Number of Dialed Digits' and 'It is disable if 0'.

- **Functionality**

This is an enhancement for an existing feature after feedbacks from customers.

This setting allows user to configure the timeout (in second) when no key input then sending out the SIP call automatically without press the “#” key. User can customize this parameter based on the environment this door phone installed.

For example in above screenshot:

“Maximum Number of Dialed Digits” is set to be “4”:

This is good for an installation allowing the door phone call ONLY the internal extensions to open door. The setting is 4, means user input 4 digit the GDS3710 will immediately dial out (saying the internal extension is using 4 digits)

“No Key Input Timeout(s)” is set to be “2” (second).

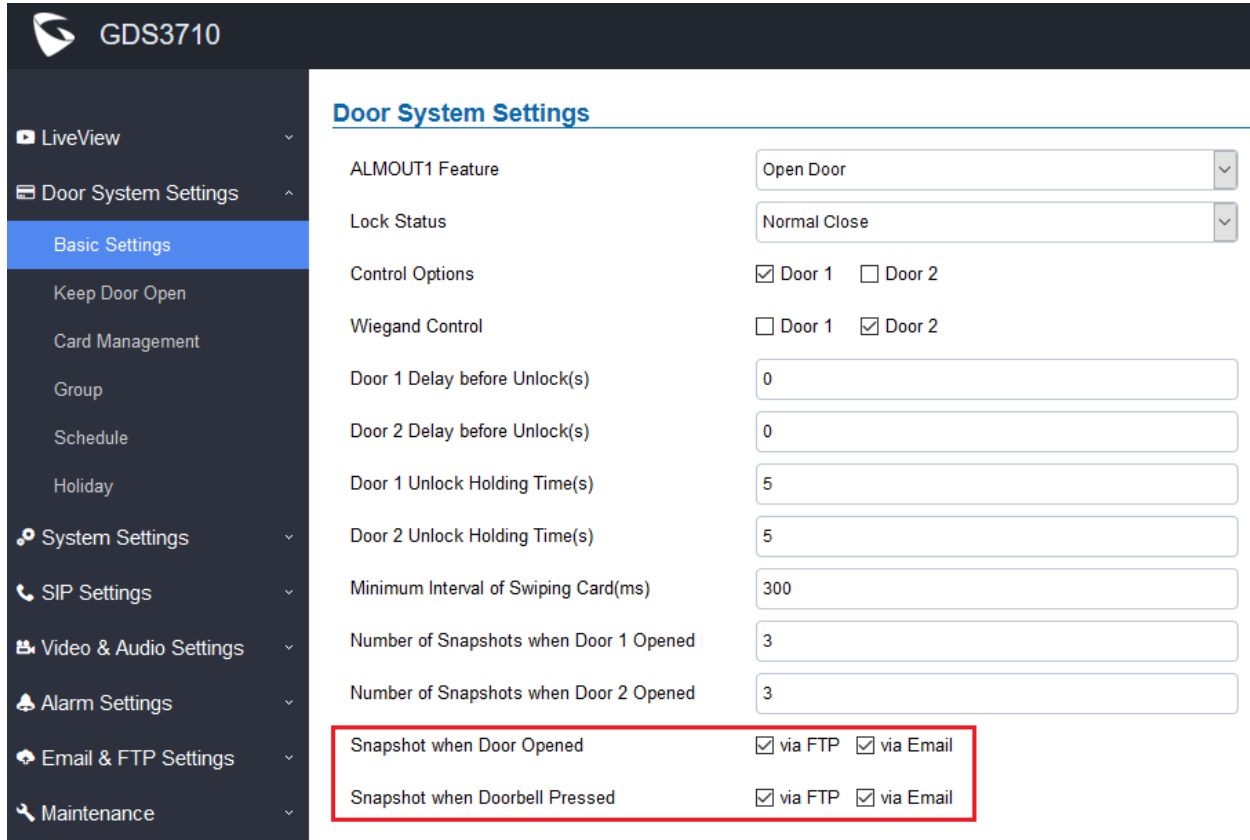
This means if user input the digits (less than 4 digit in above example), then wait and not more key strike, after 2 seconds (this can be customized by user or installer in the installation scene), the SIP call will automatically dial out without the “#” pressed.

Same as above screenshot example, if user input less than 4 digits, say input only 1 digit (“0” for example), then followed by the “#” key, then the GDS3710 door phone will immediately dial out “0” to establish the call. (“0” can be Operator or IVR depending on the IPPBX system configured)

EMAIL SNAPSHOTS WHEN DOOR OPENED

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



Door System Settings	
ALMOUT1 Feature	Open Door
Lock Status	Normal Close
Control Options	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2
Wiegand Control	<input type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Door 1 Delay before Unlock(s)	0
Door 2 Delay before Unlock(s)	0
Door 1 Unlock Holding Time(s)	5
Door 2 Unlock Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Number of Snapshots when Door 1 Opened	3
Number of Snapshots when Door 2 Opened	3
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input checked="" type="checkbox"/> via FTP <input checked="" type="checkbox"/> via Email

- **Functionality**

This is an enhancement for an existing feature after feedbacks from customers. This setting allows user to configure either email or FTP the snapshots when the door opened or the doorbell pressed or both.

For this feature to work, the correct Email (SMTP) settings, FTP settings or GDSManager (Central Storage) have to be configured.

Please refer to User Manual of GDS3710 and GDSManager for detailed configuration.

GDS3710 User Manual:

http://www.grandstream.com/sites/default/files/Resources/GDS3710_UserManual.pdf

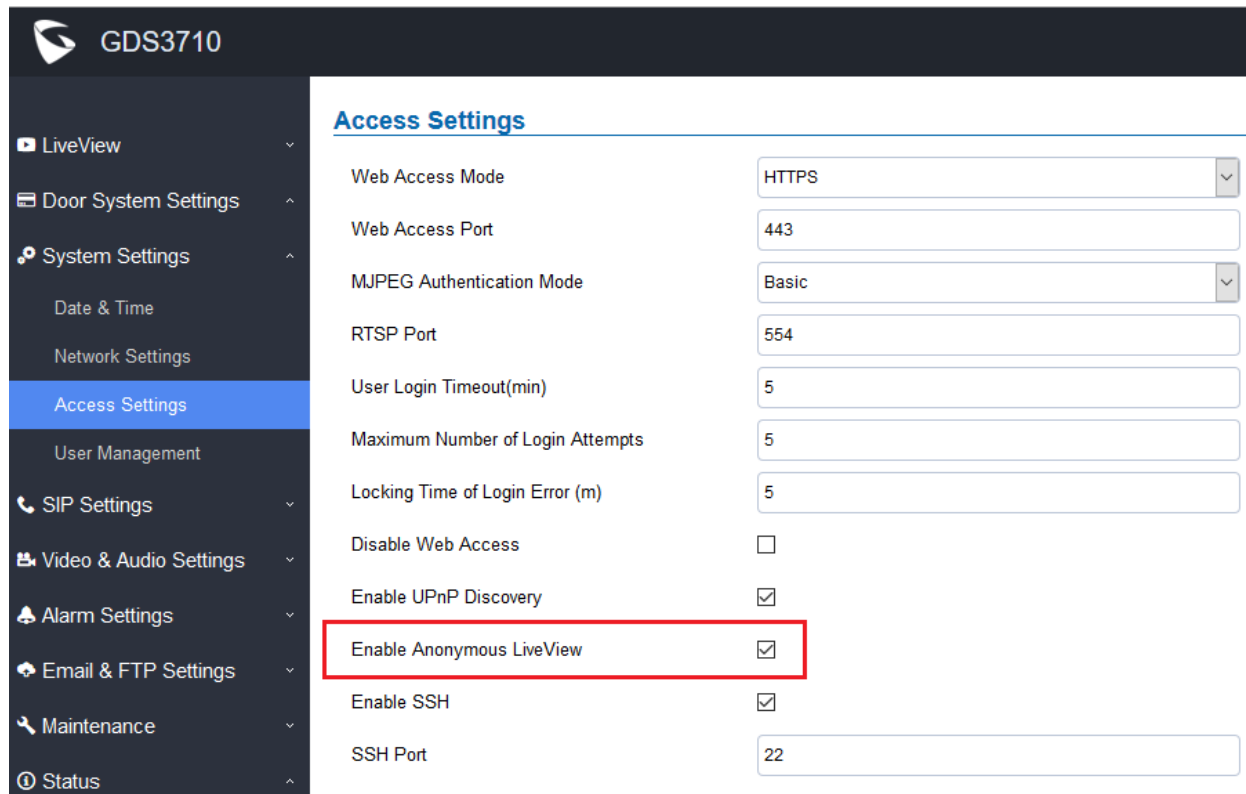
GDSManager User Manual:

http://www.grandstream.com/sites/default/files/Resources/GDSManager_User_Guide.pdf

ALLOW ANONYMOUS VIEWING

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



The screenshot shows the GDS3710 web UI. On the left is a sidebar menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, Access Settings (highlighted), User Management, SIP Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main area is titled 'Access Settings' and contains the following configuration items:

Setting	Value
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22

- **Functionality**

This is an enhancement request from customers like Service Provider and Installers. This feature allows system integrators to retrieve video from GDS3710 directly without credentials, good for system re-development or scripts running in LAN environment.

When enabled this feature, **a special access URL** is required to retrieve live video:

https://IP_GDS3710:Port/videoview.html

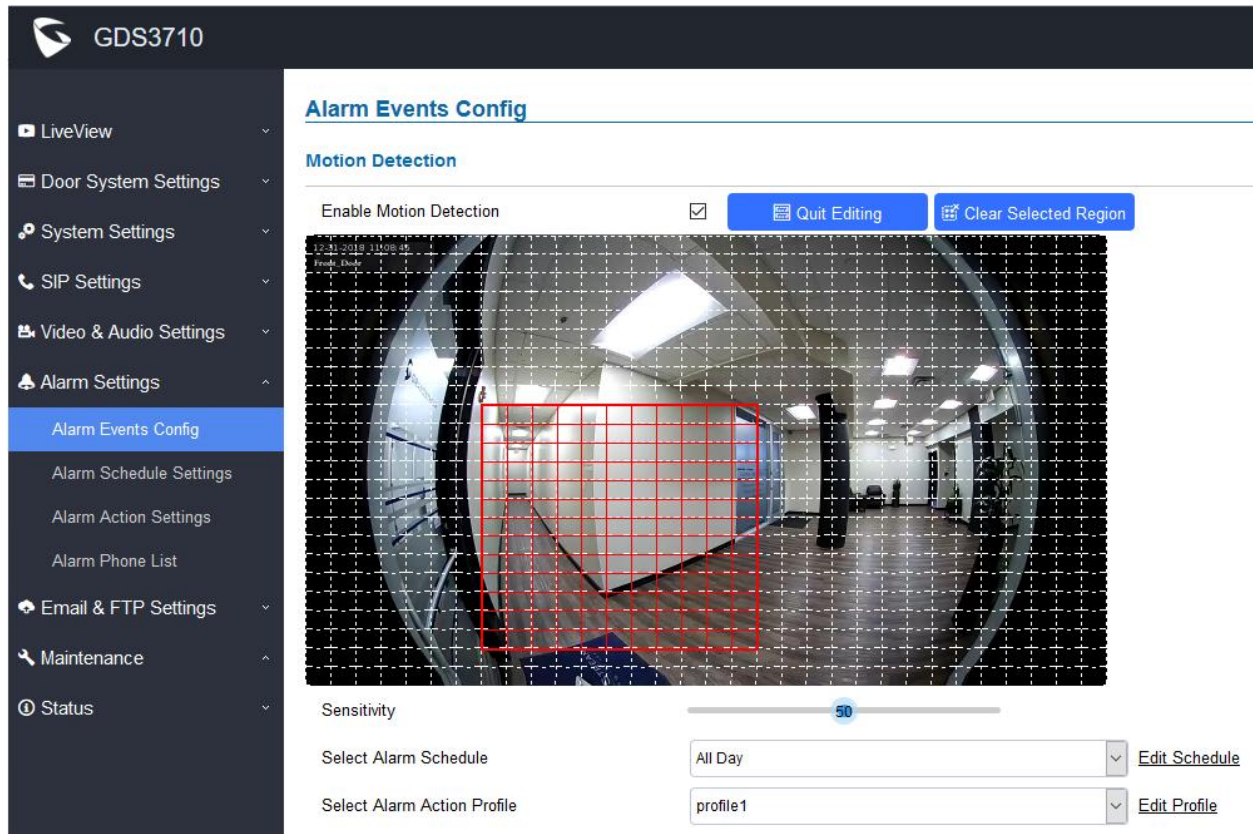
NOTE:

- Please make sure the environment is secure before enabling this feature.
- Please reminder user the privacy when using this feature.

DISPLAY MOTION DETECTION REGION CONFIGURATON WITHOUT PLUGIN

- **Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Events Config:



- **Functionality**

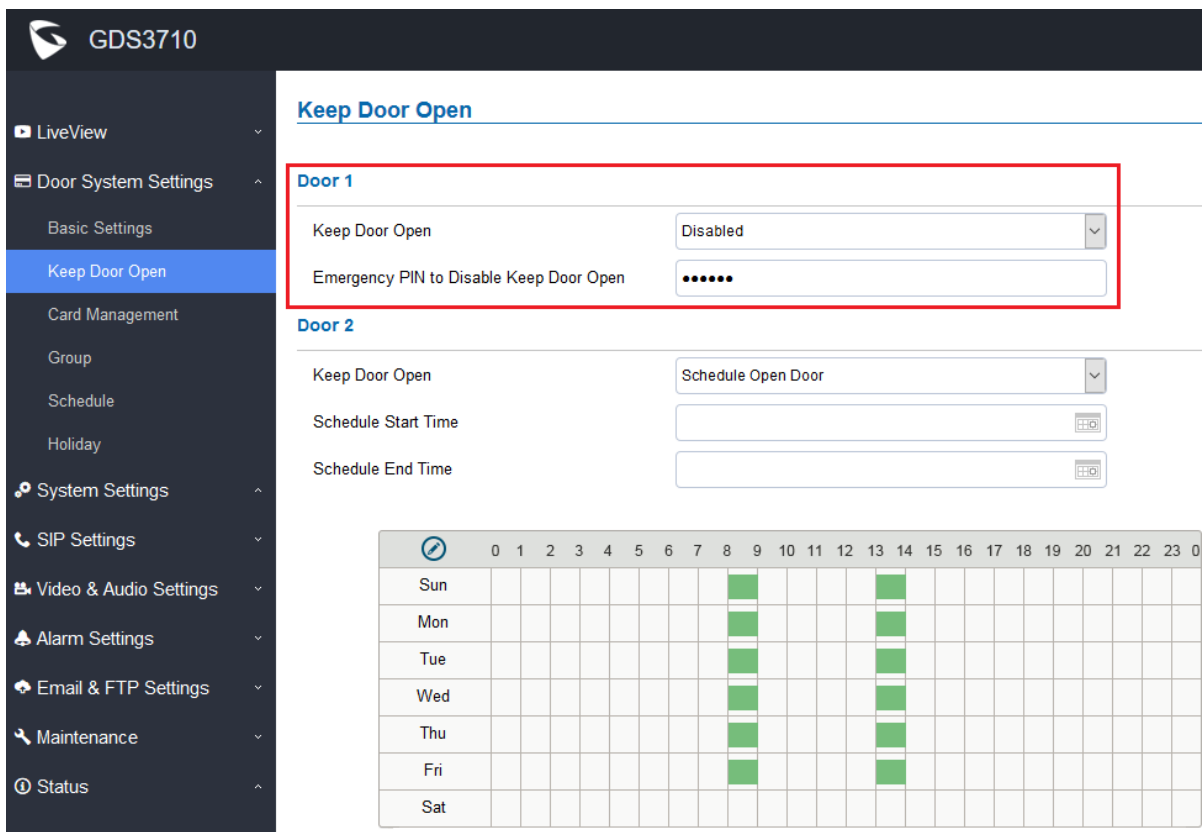
This is an enhancement for an existing feature, customer can now configure the Motion Detection Region without installing any plugins, same as LiveView.

This feature support most popular browsers like Firefox, Chrome, after NPAPI stopped support by those popular browsers for security reason.

EMERGENCY PIN TO OVERWRITE “KEEP DOOR OPEN” (LOCKDOWN)

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Keep Door Open:



GDS3710

Keep Door Open

Door 1

Keep Door Open: Disabled

Emergency PIN to Disable Keep Door Open:

Door 2

Keep Door Open: Schedule Open Door

Schedule Start Time: [Time Picker]

Schedule End Time: [Time Picker]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0
Sun																									
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									

- **Functionality**

This is an enhancement for existing feature from customers. This enhancement is especially good for application scenes or installations like public schools, libraries, city halls, clubs, etc., where at some scheduled time window the door should be opened to public access, but something emergency happened, the door can be lock down by staffs via either webUI or emergency PIN.

There are two ways to apply this emergency lock down:

1) WebUI:

During the emergency, staff can log in to above “Keep Door Open” page and select “Disabled” and click “Save” to immediately lock down the door.

2) Emergency PIN:

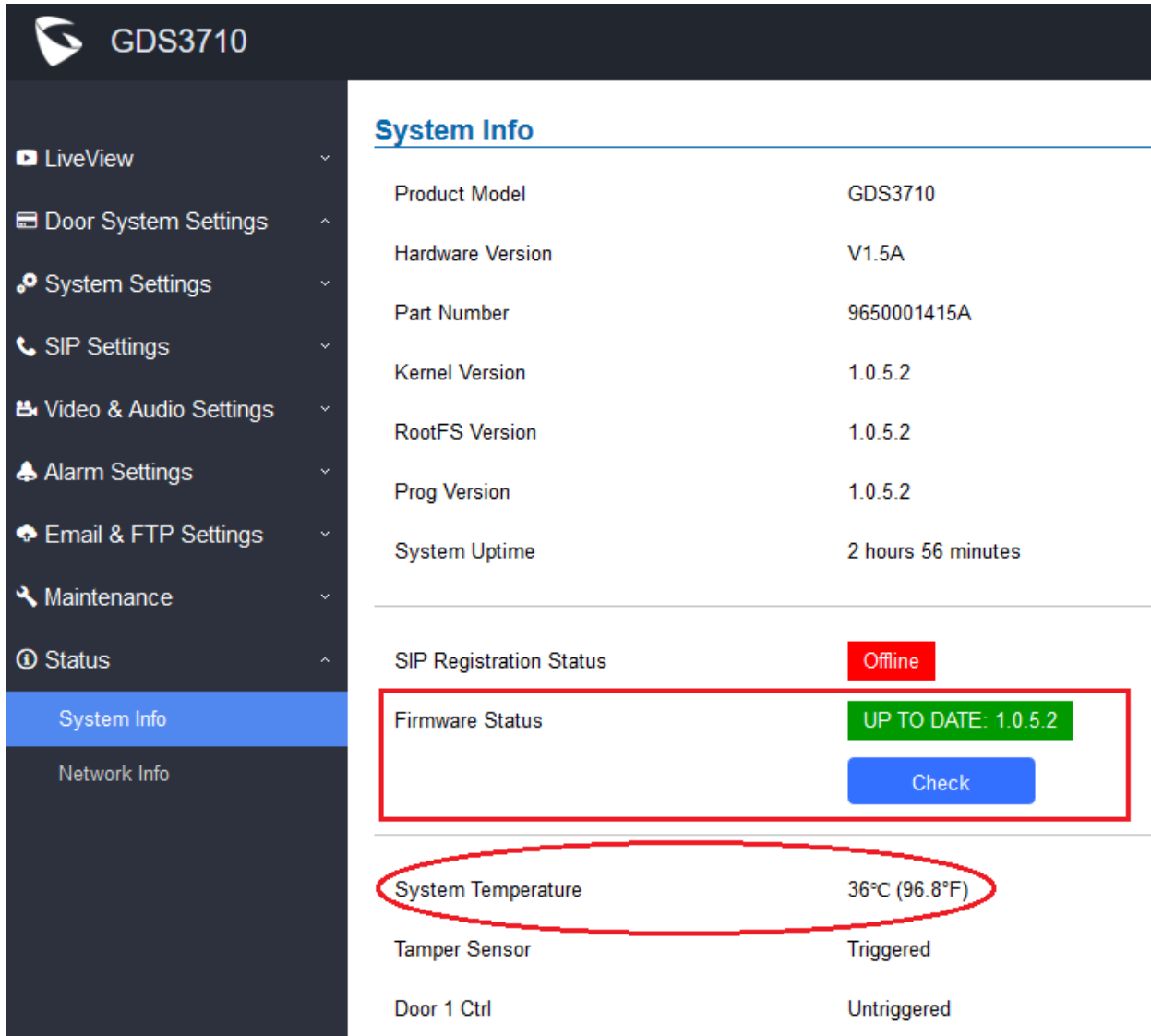
The emergency PIN can only be setup from webUI when “Keep Door Open” selected “Disabled”, to match that this is a PIN to lock down and “Disable” the open door. The PIN format to enter the PIN from the key pad of GDS3710 is like usual, add “*” and “#” before and after the PIN → “*PIN#”.

- When “Keep Door Open” in session and door opened, the white LED of GDS3710 will light up to show the door open status.

CHECK/UPGRADE FIRMWARE AND DISPLAY DEVICE TEMPERATURE

- Web Configuration**

This enhancement can be found under device web UI → Status → System Info:



The screenshot shows the GDS3710 web configuration interface. On the left is a sidebar with navigation options: LiveView, Door System Settings, System Settings, SIP Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Status, System Info (highlighted), and Network Info. The main content area is titled 'System Info' and contains a table of system details:

Product Model	GDS3710
Hardware Version	V1.5A
Part Number	9650001415A
Kernel Version	1.0.5.2
RootFS Version	1.0.5.2
Prog Version	1.0.5.2
System Uptime	2 hours 56 minutes

Below the table, there are three status indicators:

- SIP Registration Status: Offline (in a red box)
- Firmware Status: UP TO DATE: 1.0.5.2 (in a green box) with a blue 'Check' button below it. This entire section is enclosed in a red rectangular box.
- System Temperature: 36°C (96.8°F) (circled in red)

At the bottom, there are two more status indicators:

- Tamper Sensor: Triggered
- Door 1 Ctrl: Untriggered

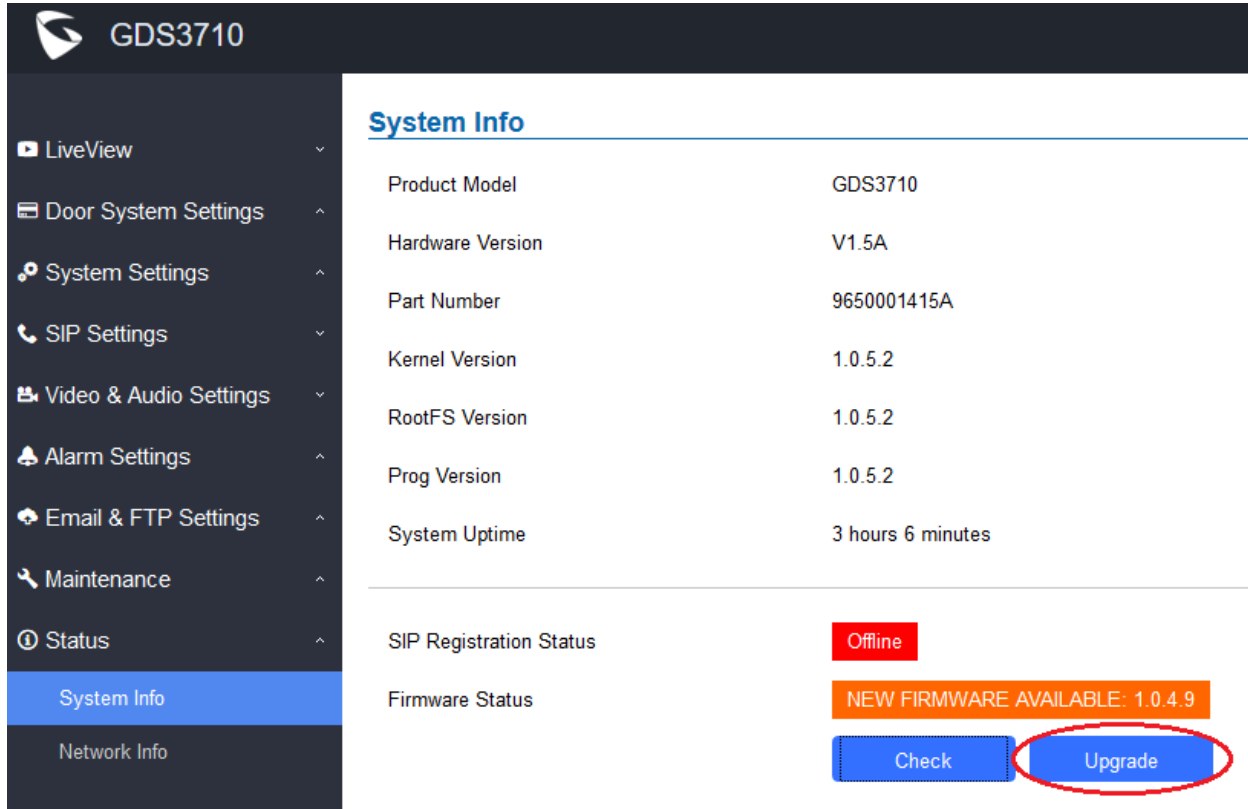
- Functionality**

This is an enhancement for an existing feature after feedbacks from customers.

This feature allows user to click “Check” button to see whether there is “NEW” firmware in the firmware server configured in the firmware server path under UI “Maintenance → Upgrade”:

- 1) If the firmware is the same, it will show “UP TO DATE: X.X.X.X”, where the “X.X.X.X” is the current up to date firmware version number.

- 2) If there are new firmware, the “Firmware Status” will show the available (different) firmware version number. If click “Upgrade” button, the GDS3710 will start download, flash and upgrade the firmware to the one in the server. The key pad blue LED will light up in pattern illustrating the download and burning progress status.


GDS3710

- ▶ LiveView
- ⚙ Door System Settings
- ⚙ System Settings
- ☎ SIP Settings
- 📺 Video & Audio Settings
- 🔔 Alarm Settings
- ✉ Email & FTP Settings
- 🔧 Maintenance
- 📶 Status
- System Info
- Network Info

System Info

Product Model	GDS3710
Hardware Version	V1.5A
Part Number	9650001415A
Kernel Version	1.0.5.2
RootFS Version	1.0.5.2
Prog Version	1.0.5.2
System Uptime	3 hours 6 minutes

SIP Registration Status

Firmware Status

Offline

NEW FIRMWARE AVAILABLE: 1.0.4.9

Check

Upgrade

- **Please do NOT power off the device when firmware burning/upgrade is in processing.**

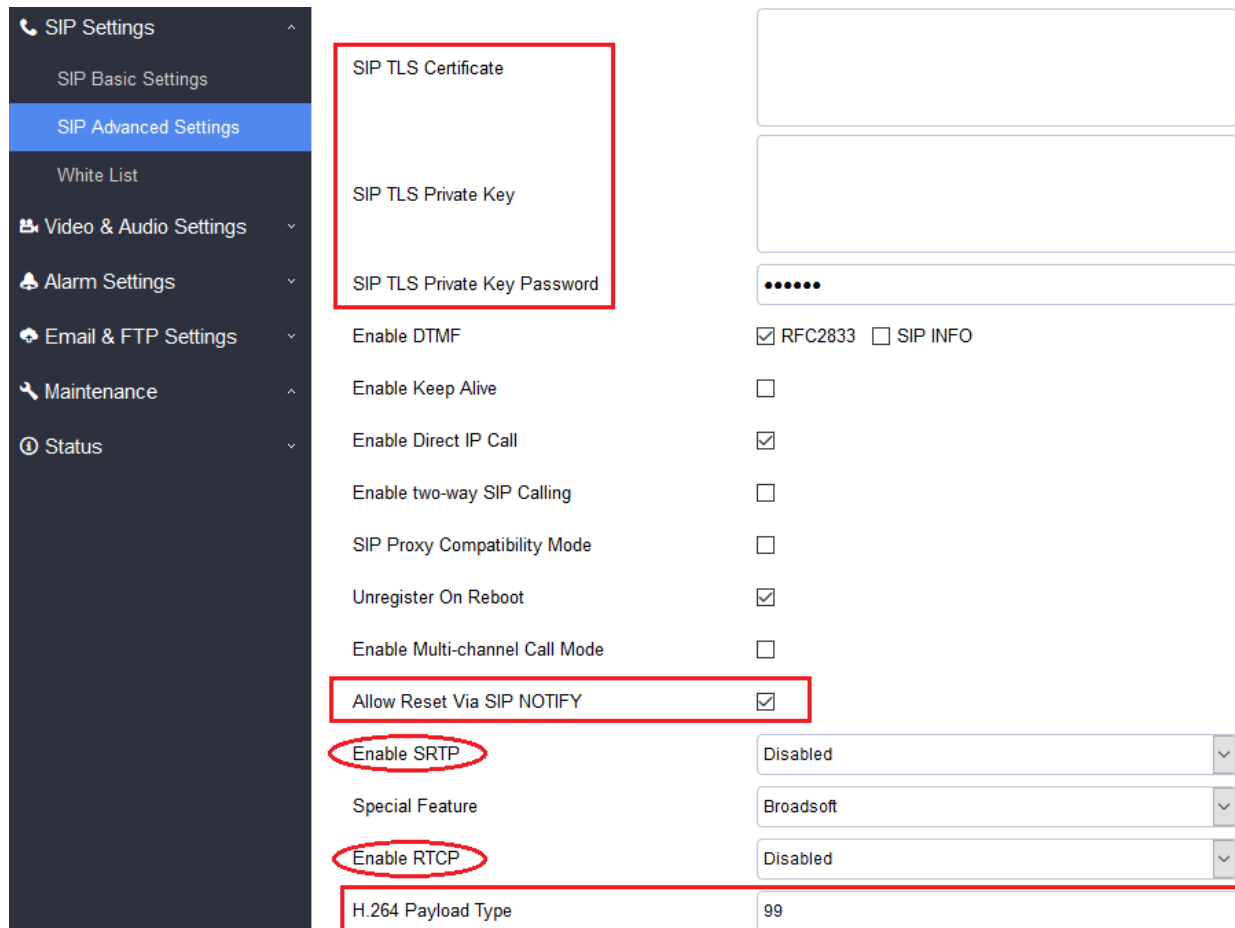
This version also adds the device temperature displayed in Fahrenheit to help users using imperial system, like below:

System Temperature		36°C (96.8°F)
Tamper Sensor		Triggered
Door 1 Ctrl		Untriggered
Door 2 Ctrl		Untriggered

SUPPORT SIP NOTIFY AND SET H.264 PAYLOAD TYPE

- **Web Configuration**

This option can be found under device web UI → SIP Settings → SIP Advanced Settings:



SIP Settings	SIP TLS Certificate	
SIP Basic Settings	SIP TLS Private Key	
SIP Advanced Settings	SIP TLS Private Key Password
White List	Enable DTMF	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
Video & Audio Settings	Enable Keep Alive	<input type="checkbox"/>
Alarm Settings	Enable Direct IP Call	<input checked="" type="checkbox"/>
Email & FTP Settings	Enable two-way SIP Calling	<input type="checkbox"/>
Maintenance	SIP Proxy Compatibility Mode	<input type="checkbox"/>
Status	Unregister On Reboot	<input checked="" type="checkbox"/>
	Enable Multi-channel Call Mode	<input type="checkbox"/>
	Allow Reset Via SIP NOTIFY	<input checked="" type="checkbox"/>
	Enable SRTP	Disabled
	Special Feature	Broadsoft
	Enable RTCP	Disabled
	H.264 Payload Type	99

- **Functionality**

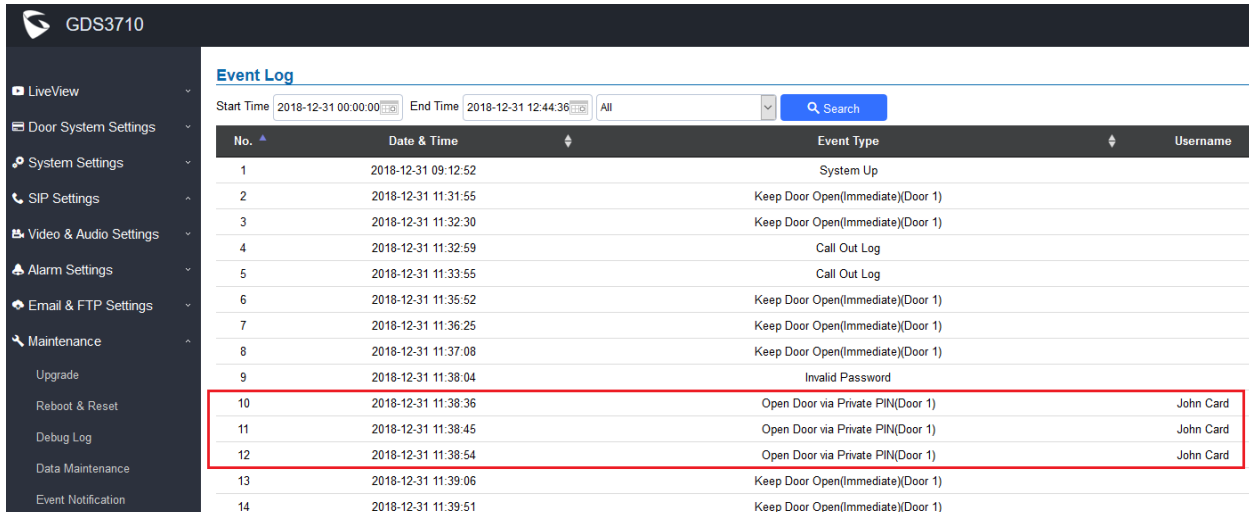
This is an enhancement for an existing features, to help ITSP or Service Provider customers to remotely provisioning and control the door phone (GDS3710) if something happened from customer side (e.g.: phone stolen, service fee due, etc.).

The H.264 payload type can now be configured to be compatible with 3rd party video phones, as well as other advanced SIP settings, to easy system integration process.

DISPLAY USER OPEN DOOR VIA PIN OVER EVENT LOG

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Log:



No.	Date & Time	Event Type	Username
1	2018-12-31 09:12:52	System Up	
2	2018-12-31 11:31:55	Keep Door Open(Immediate)(Door 1)	
3	2018-12-31 11:32:30	Keep Door Open(Immediate)(Door 1)	
4	2018-12-31 11:32:59	Call Out Log	
5	2018-12-31 11:33:55	Call Out Log	
6	2018-12-31 11:35:52	Keep Door Open(Immediate)(Door 1)	
7	2018-12-31 11:36:25	Keep Door Open(Immediate)(Door 1)	
8	2018-12-31 11:37:08	Keep Door Open(Immediate)(Door 1)	
9	2018-12-31 11:38:04	Invalid Password	
10	2018-12-31 11:38:36	Open Door via Private PIN(Door 1)	John Card
11	2018-12-31 11:38:45	Open Door via Private PIN(Door 1)	John Card
12	2018-12-31 11:38:54	Open Door via Private PIN(Door 1)	John Card
13	2018-12-31 11:39:06	Keep Door Open(Immediate)(Door 1)	
14	2018-12-31 11:39:51	Keep Door Open(Immediate)(Door 1)	

- **Functionality**

This is an enhancement for an existing feature, to help ITSP or Service Provider customers, as well as System Integrators or Administrators to understand who opened the door using PIN, which is not available in previous firmware.

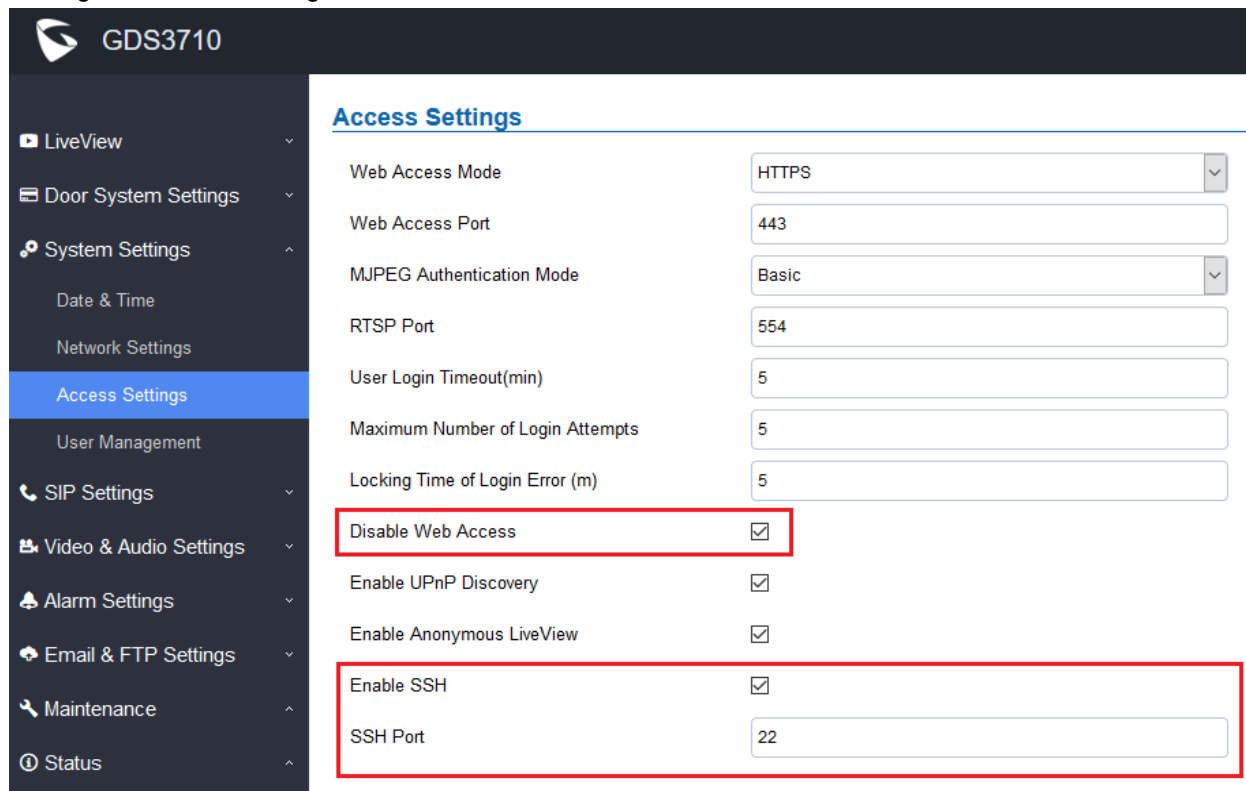
This feature enhances the local system administration and maintenance.

CONFIG FIRMWARE OR CONFIGURATION SERVER PATH AND PING TEST VIA SSH

- **Web Configuration**

This feature is added to allow user to change firmware server path or configuration server path via SSH. This is very useful for ITSP or service contractors or installer to maintenance the device, for example, the webUI is purposed blocked, ITSP or Service Technician can use scripts in SSH to perform necessary configuration or maintenance, or upgrade firmware.

The SSH has to be enabled to use this feature. The option can be found under device web UI → System Settings → Access Settings:



Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input checked="" type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22

- **Functionality**

This feature is added to allow users (service technician, installer, etc.) to configure or change the firmware server or configuration server path via SSH, enhance the security of SIP accounts configured in GDS37XX.

3rd party SSH application like **PuTTY** is required to use this feature.

For example, below is the screenshot of such CLI interface:

```

192.168.22.165 - PuTTY
login as: admin
admin@192.168.22.165's password:
Grandstream Command Shell Copyright 2006-2018
GDS3710> status

Product Model: GDS3710

Network:
  MAC Addr:          --00:0B:82:B3:1A:37
  LAN IP Address:    --192.168.22.165
  LAN Subnet Mask:   --255.255.255.0
  LAN Default Gateway: --192.168.22.1

System Statistics:
  Hardware Version:  --V1.5A
  Part Number:       --9650001415A
  Bootloader Version: --1.0.5.2
  Core Version:      --1.0.5.2
  Base Version:      --1.0.5.2
  Firmware Version:  --1.0.5.2
  System Up Time Since: --3 hours 53 minutes
GDS3710> help

Commands available:
  help      -- Show available commands
  exit      -- Exit this command shell
  status    -- Show the information of the system
  restart   -- Reboot the device
  reset     -- Factory reset
  upgrade   -- Upgrade the system
  config    -- Configure the device
  ping      -- Send ICMP ECHO_REQUEST packets to network hosts

GDS3710> config
CONFIG> help
Supported commands:
  set FWUpgradeType value      -- Set FW Upgrade Type 0-TFTP 1-HTTP, 2-HTTPS
  set FWServerPath value       -- Set FW Server Path
  set ConfigUpgradeType value  -- Set Config Upgrade Type 0-TFTP 1-HTTP, 2-HTTPS
  set ConfigServerPath value   -- Set Config Server Path
  get FWUpgradeType            -- Get FW Upgrade Type
  get FWServerPath             -- Get FW Server Path
  get ConfigUpgradeType        -- Get Config Upgrade Type
  get ConfigServerPath         -- Get Config Server Path
  commit                       -- Commit the changes to FLASH
  help                         -- Show this help text
  exit                         -- Exit this command shell
CONFIG> exit

GDS3710> ping www.grandstream.com
PING www.grandstream.com (45.55.195.232): 56 data bytes
64 bytes from 45.55.195.232: seq=0 ttl=53 time=10.591 ms
64 bytes from 45.55.195.232: seq=1 ttl=53 time=9.718 ms

```

NOTE:

- This feature is designed for ITSP Service Provider, or Service Technician or Installers.
- End users without necessary knowledge are strongly discouraged to access it, avoiding damage the device or making the device not working properly.

FIRMWARE VERSION 1.0.4.9

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

11/21/2018

SUMMARY OF UPDATE

This is **MAJOR UPDATE** with purpose of bug fixes and feature enhancement. Please read below WARNING carefully before upgrading.

It is strongly recommended for users to back up all the data (both configuration and application) before upgrade, also perform factory reset if the previous firmware is an old version in different FW level.

WARNING:

- **Self-reboot TWICE** is required to finish the whole upgrade process and it can take about **20 minutes**. Please be patient and DO NOT interrupt power. Incomplete upgrade can potentially brick the device.
- Please press keypad to verify the upgrade is finished. If BEEP sound heard and BLUE LED lighted up upon pressing, the means the device finished upgrading and booted up successfully. If other LED patterns are in progress or there is no BEEP sound/BLUE light, the device has not finished upgrade yet, DO NOT unplug power during this stage to prevent damaging the device.
- After upgrading, please download [GS Search](#) utility tool and perform a search within LAN using your PC. The device should show up in search result with the correct firmware version. Double clicking it will open device web UI successfully. That indicates upgrading has completed successfully.
- Once upgraded to 1.0.4.x firmware, **downgrade** to previous lower lever firmware (1.0.1.xx/1.0.2.xx/1.0.3.xx) is **NOT SUPPORTED**.
- Local firmware upgrade recommended. Please download and use the [GS Upgrade Tool](#) provided by Grandstream for local firmware upgrade, avoiding internet or power interruption to brick the device.
- For 1.0.1.xx and 1.0.2.xx firmware, single firmware file not supported and multiple unzipped binary files are required for successful upgrade. Please allow at least 20 minutes for local upgrade before log in back to check or power cycle the device.
- **Factory Reset** is recommended after upgrading from previous lower lever firmware. Please backup data before performing factory reset then restore back the data.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added support for TLSV1.2
- Optimized firmware upgrade process and reduced self-reboot from three time to twice.
- Support single firmware file upgrade with 6bit ECC.
- Single firmware file upgrade supported since 1.0.3.35. Previous lower lever firmware 1.0.1.xx/1.0.2.xx upgrade requires firmware with multiple binary files. Two firmware packages provided.

BUG FIX

- Fixed probability issue in 1.0.4.5 where upgrading from previous firmware if amboot not upgraded will stop the upgrade process therefore brick the device.
- Fixed device keeps on playing doorbell sound if account unregistered.
- Fixed issue that keypad not response sometimes.
- Fixed security vulnerability that root access may compromised via SSH.

KNOWN ISSUES

- LiveView page, the page may crash if click the “Local Configuration Function”
- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during the call.

NEW P-VALUE

- N/A

NEW HTTP API

- N/A

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.4.5 (REMOVED)

PRODUCT NAME

GDS3710 (HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A)

DATE

09/13/2018

SUMMARY OF UPDATE

This is **MAJOR UPDATE** with purpose of bug fixes and feature enhancement. Please read below WARNING carefully before upgrading.

It is strongly recommended for users to back up all the data (both configuration and application) before upgrade, also perform factory reset if the previous firmware is an old version in different FW level.

WARNING:

- **Three-times self-reboot** is required to finish the whole upgrade process and it can take **more than 30 minutes**. Please be patient and **DO NOT interrupt power** until 30 minutes later. Unplugging it before complete upgrade can potentially brick the device.
- After 30 minutes, please press any button on the device keypad to verify the symptom of complete upgrade. If it has a BEEP sound and BLUE light for the button light up upon pressing, the device has finished upgrading and rebooted successfully. If other patterns are in progress or there is no BEEP sound/BLUE light, the device has not finished upgrade yet, DO NOT unplug power during this stage to prevent damaging the device.
- After upgrading, please download [GS Search](#) app and perform a search within LAN using your PC. The device must show up in search result with the correct firmware. Double clicking it will open device web UI successfully. That indicates upgrading has successfully completed.
- Once upgraded to 1.0.4.x firmware, **downgrade** to previous lower lever firmware (1.0.1.xx/1.0.2.xx/1.0.3.xx) is **NOT SUPPORTED**.
- Local firmware upgrade recommended. Please download and use the [GS Upgrade Tool](#) provided by Grandstream for local firmware upgrade, avoiding internet or power interruption to brick the device.
- For 1.0.1.xx and 1.0.2.xx firmware, all the unzipped binary files are required for successful upgrade. Please allow at least **30 minutes** in local upgrade before log in back to check or power cycle the device.

- **Factory Reset** is recommended after upgrading from previous lower lever firmware.
Please backup data before performing factory reset then restore back the data.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Single firmware file upgrade supported with 6bit ECC.
- Support parallel hunting (simultaneously ringing configured extensions and/or IP addresses) when doorbell pressed.
- Added Card_ID, SIP extension, etc. details in the HTTP Event Notification.

BUG FIX

- Fixed DTMF open door issue with early media, SIN INFO.
- Fixed alarm not fired when enable silent alarm with schedule configured.
- Fixed initial audio chopped off issue with outgoing calls from GDS3710.
- Fixed Log Notification Type missing.
- Fixed call fails when dialing digit length less than the maximum number of digits.
- Fixed audio may be noisy after long time (in hours) of call (not feasible in real environment)
- Fixed No plugin preview not working when MJPEG video codec configured.
- Fixed “Card Issuing Mode Expired Timer” cannot be saved.
- Fixed key light not bright enough when using HTTP API to open the door.
- Fixed GDS3710 SSH access unauthorized with static IP address after reboot.
- Fixed the temperature alarm email cannot be sent normally.
- Fixed timer error when hanging up the call.
- Fixed spotted video image when switching call lines in GDS3710.

KNOWN ISSUES

- Video JPEG stream will fail in GXP audio phones when NAT involved.
- The SIP phone sending DTMF to GDS may sometimes hand up and clear the call
- Device will fail to send DNS resolution when Stun Server using FQDN (only IP Stun works)
- The 2nd outbound proxy will not use the DNS-SRV parsing domain name.

- The option may crash if click the “Local Configuration Function”
- INVITE to an ICMP address, the doorbell still rings as normal.
- The panel lights might off during a call

NEW P-VALUE

P-Value	Values	Default Value	Comments
P15434= <int> (Add)	0 -- 1	0	0. Serial Hunting 1. Parallel Hunting

NEW HTTP API

GET:

<http|https>://ip:port/goform/config?cmd=get&type=door

SET:

<http|https>://ip:port/goform/config?cmd=set&P15434=<0|1>

For details please refer to HTTP API Document and User Manual.

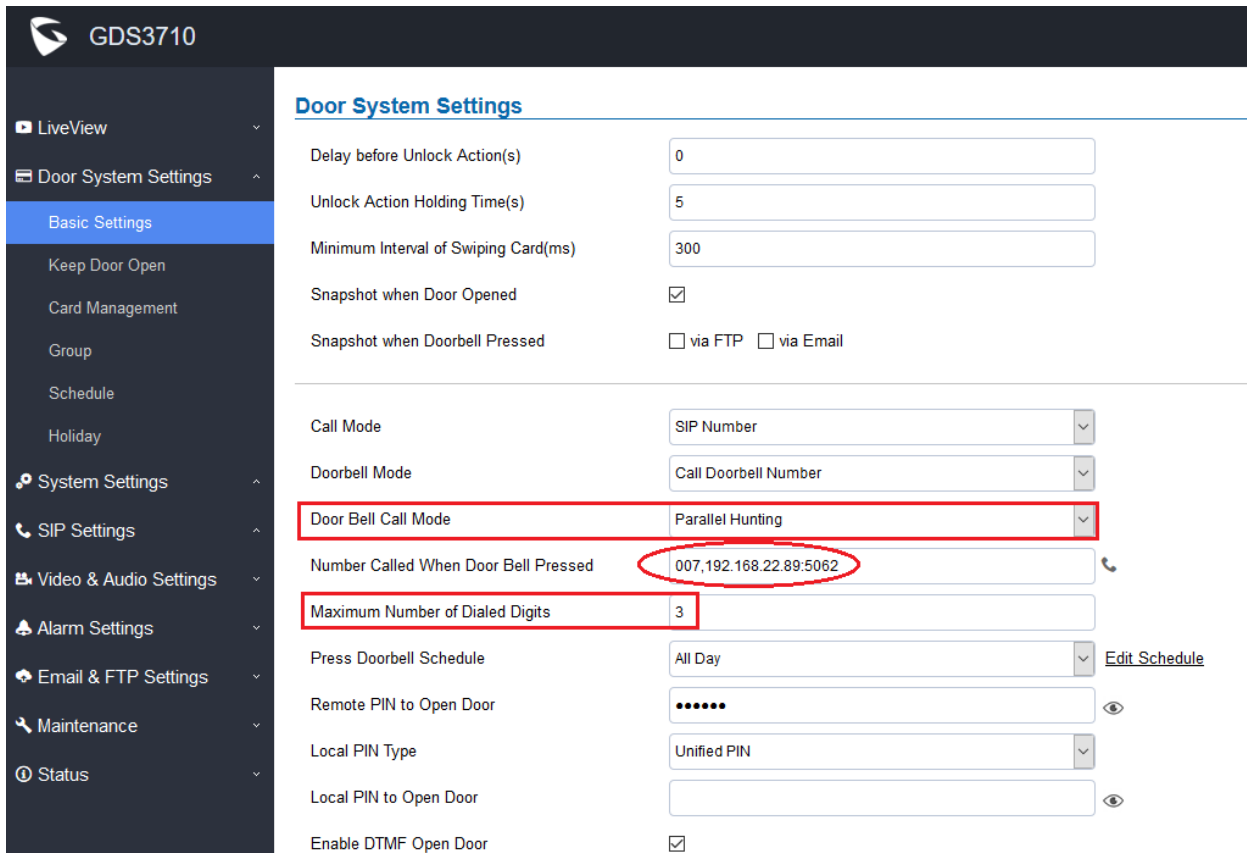
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

PARELLEL HUNTING/SIMUTANEOUS RINGING WHEN DOORBELL PRESSED

- **Web Configuration**

This option can be found under device web UI → Basic Settings →:



GDS3710

Door System Settings

Delay before Unlock Action(s)

Unlock Action Holding Time(s)

Minimum Interval of Swiping Card(ms)

Snapshot when Door Opened ☒

Snapshot when Doorbell Pressed ☐ via FTP ☐ via Email

Call Mode

Doorbell Mode

Door Bell Call Mode

Number Called When Door Bell Pressed

Maximum Number of Dialed Digits

Press Doorbell Schedule [Edit Schedule](#)

Remote PIN to Open Door

Local PIN Type

Local PIN to Open Door

Enable DTMF Open Door ☒

- **Functionality**

This feature allows user to configure SIP extensions (if having IPPBX) or IP addresses (if no IPPBX) or combined into the “Number Called When Door Bell Pressed” field, so the doorbell pressed, those IP phones will ring simultaneously (ringing at the same time). Anyone pick up the phone will be able to talk to the GDS3710 (or viewing the image at capable IP Phones), then press the digit PIN to open the door remotely, or use the “ONE KEY OPEN DOOR” feature if configured correctly with compatible IPPBX and IP Phones.

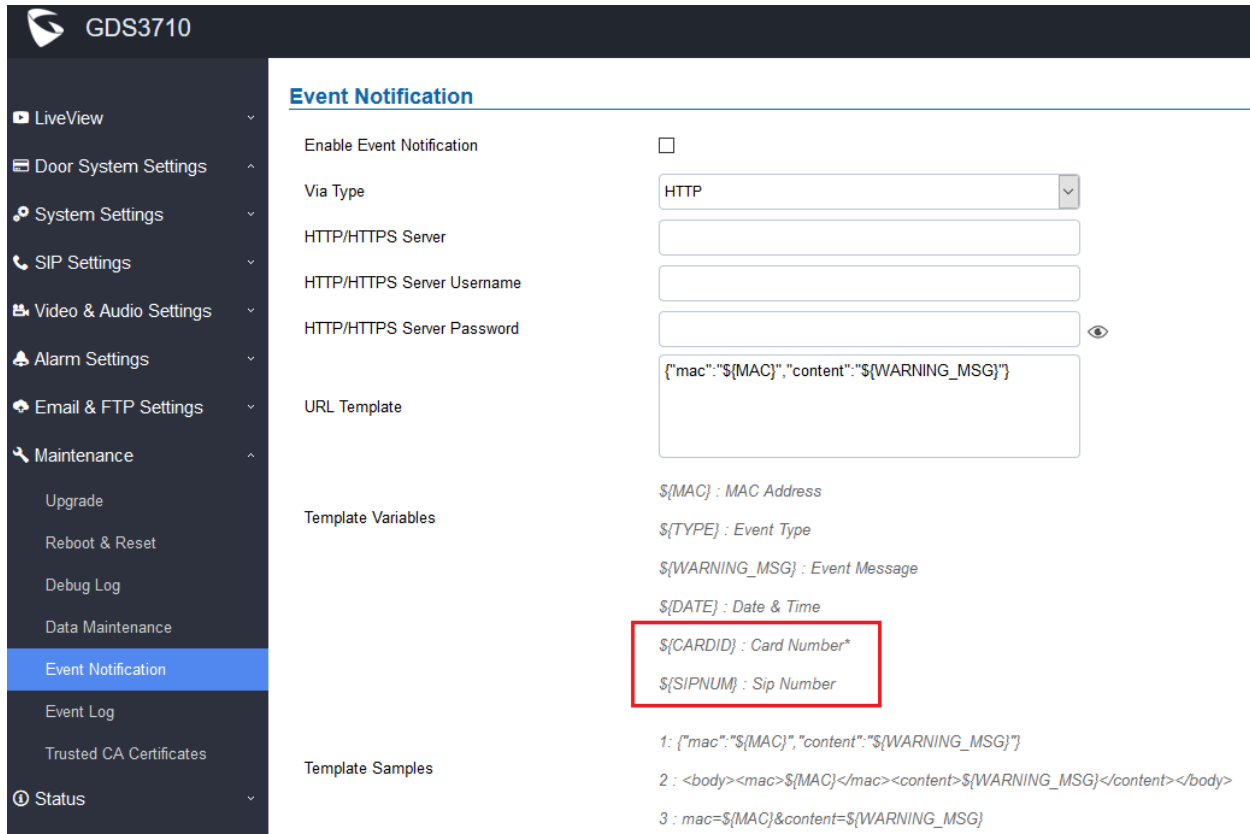
In “Door Bell Call Mode”, there are two options in the pull down menu: Serial Hunting, Parallel Hunting. “Serial Hunting” means extensions and/or/combined IP devices ring one after one by order (this feature has already been supported in previous firmware); “Parallel Hunting” means all the extensions and/or/combined IP devices ring simultaneously at the same time (new feature in this firmware).

User can select either one depending on the application scenarios.

EVENT NOTIFICATION

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Notification:



The screenshot shows the GDS3710 web configuration interface. On the left is a sidebar menu with options: LiveView, Door System Settings, System Settings, SIP Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance (highlighted), Upgrade, Reboot & Reset, Debug Log, Data Maintenance, Event Notification (highlighted), Event Log, Trusted CA Certificates, and Status. The main content area is titled 'Event Notification' and contains the following settings:

- Enable Event Notification:** A checkbox that is currently unchecked.
- Via Type:** A dropdown menu set to 'HTTP'.
- HTTP/HTTPS Server:** An empty text input field.
- HTTP/HTTPS Server Username:** An empty text input field.
- HTTP/HTTPS Server Password:** An empty text input field with an eye icon for toggling visibility.
- URL Template:** A text area containing the JSON template: `{"mac":"${MAC}","content":"${WARNING_MSG}"}`.
- Template Variables:** A list of variables:
 - `$(MAC)` : MAC Address
 - `$(TYPE)` : Event Type
 - `$(WARNING_MSG)` : Event Message
 - `$(DATE)` : Date & Time
 - `$(CARDID)` : Card Number*
 - `$(SIPNUM)` : Sip Number
- Template Samples:** Three examples of JSON templates:
 - `1: {"mac":"${MAC}","content":"${WARNING_MSG}"}`
 - `2: <body><mac>${MAC}</mac><content>${WARNING_MSG}</content></body>`
 - `3: mac=${MAC}&content=${WARNING_MSG}`

- **Functionality**

This is an enhancement for an existing feature after feedbacks from customers.

Added Card_ID, SIP extension, etc. details in the HTTP Event Notification which not supported in previous firmware. This will allow 3rd party system integrator or developers to implement related application for users. Details please refer to User Menu and HTTP API

If enabled, device can send HTTP events to related web server and allow 3rd party system integrators to implement dedicated usage applications for customers (e.g.: live monitor the door access status).

Released HTTP API documentation can be downloaded from here:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

- **New Pvalue**

P-Value	Values	Default Value	Comments
P15434= <int> (Add)	0 -- 1	0	2. Serial Hunting 3. Parallel Hunting

- **New HTTP API**

GET:

<http|https>://ip:port/goform/config?cmd=get&type=door

SET:

<http|https>://ip:port/goform/config?cmd=set&P15434=<0|1>

For details please refer to HTTP API Document and User Manual.

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

FIRMWARE VERSION 1.0.3.35

PRODUCT NAME

GDS3710 (HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A)

DATE

07/16/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement.

IMPORTANT UPGRADING NOTE

- **Local firmware upgrade recommended.**
- **Please download and use the “[Utility](#)” provided by Grandstream for local firmware upgrade, avoiding internet or power interruption to brick the device.**
- **[Factory Reset](#) is recommended after upgrading from old 1.0.1.xx or 1.0.2.xx firmware. Downgrade back to 1.0.1.xx or 1.0.2.xx is NOT supported once upgrade to 1.0.3.xx.**
- **Please backup data before performing factory reset then restore back the data.**

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added option to assign a schedule to the doorbell.
- Added option to set the maximum number of digits dialed.

BUG FIX

- Fixed FTP upload process incompatible issue.
- Fixed when Motion Detection enabled, alarming triggered but SIP call failed.
- Fixed fail to send DNS resolution when Stun Server using FQDN (only IP Stun works)
- Fixed pressing keypad during network interruption or outage, the key tone keeps buzzing.
- Fixed hostage code in use, “Enable on hook after remote door opened” should be invalid (setting overlapped) to know the hostage situation at door side.
- Fixed SRTP feature options should be: Disabled, Enable and Forced, Enable but not Forced.
- Fixed webUI misaligned in the Data Maintenance page.
- Fixed WebUI error heading under Network Infor submenu.
- Fixed the red prompted will pop up twice when wrong password inputted.
- Fixed the missing type of Log Notification (System Up).
- Fixed and specified the default initial start time of card is “1970-01-01” when adding.
- Fixed when MJPEG Authentication is different with the request the response message still return.

KNOWN ISSUES

- Video JPEG stream will fail in GXP audio phones when NAT involved.
- The SIP phone sending DTMF to GDS may sometimes hand up and clear the call
- Allowing to accept multiple calls at the same time
- The 2nd outbound proxy will not use the DNS-SRV parsing domain name.
- The HTTP web access device may appear close_wait
- The option may crash if click the “Local Configuration Function”
- INVITE to an ICMP address, the doorbell still rings as normal.

NEW FUNCTIONS

- Option to Assign Schedule to Door Bell.**
 This feature allow user to configure a schedule to the Doorbell Button. Once configured, the doorbell button will turn ON or OFF based on configured schedule. For example, some users do not want the doorbell to work during the night.
- Maximum Number of Dialed Digits**
 This feature will allow user to configure the maximum digits allowed to dial in the keypad. Once the configured condition satisfied, the device will send out the digit to call automatically without pressing #

NEW P-VALUE

P-Value	Values	Default Value	Comments
P15419=<int> (Add)	0 -- 20	0	Maximum Number of Dialed Digits
P15418=<int> (Add)	0 -- 10	0	Press Doorbell Schedule
P443=<int> (Update)	0 -- 2	0	Enable SRTP 0: Disable 1: Enable but No Forced 2: Enable and Forced

NEW HTTP API

P15419

GET:

<http|https>://<servername>/goform/config?cmd=get&type=door

SET:

<http|https>://<servername>/goform/config?cmd=set& P15419=<0-20>

P15418

GET:

<http|https>://<servername>/goform/config?cmd=get&type=door

SET:

<http|https>://<servername>/goform/config?cmd=set& P15418=<0-10>

P443

GET:

<http|https>://<servername>/goform/config?cmd=get&type=sip

SET:

<http|https>://<servername>/goform/config?cmd=set& P443=<0-20>

For details, please refer to the latest version of HTTP API Document and User Manual.

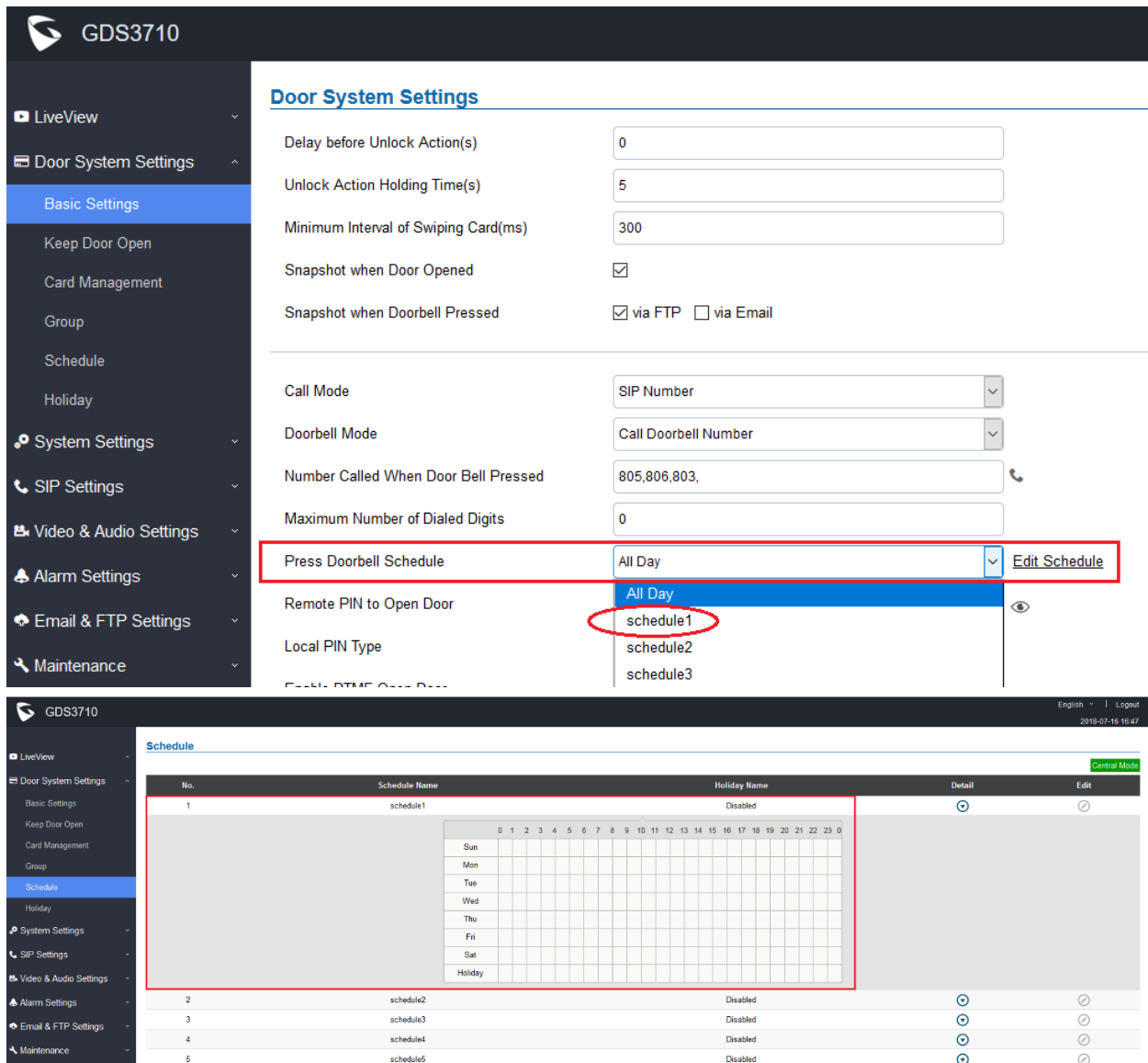
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

ASSIGN SCHEDULE TO DOORBELL

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



The screenshot displays the GDS3710 web configuration interface. The left sidebar shows the navigation menu with 'Door System Settings' expanded, and 'Basic Settings' selected. The main content area shows the 'Door System Settings' page. Under the 'Press Doorbell Schedule' section, a dropdown menu is open, showing 'All Day' selected and 'schedule1', 'schedule2', and 'schedule3' as options. The 'Edit Schedule' link is visible next to the dropdown. Below this, the 'Schedule' page is shown, featuring a table with columns for 'No.', 'Schedule Name', 'Holiday Name', 'Detail', and 'Edit'. The table lists five schedules, all currently set to 'Disabled'. A calendar grid is visible for 'schedule1', showing days of the week and months.

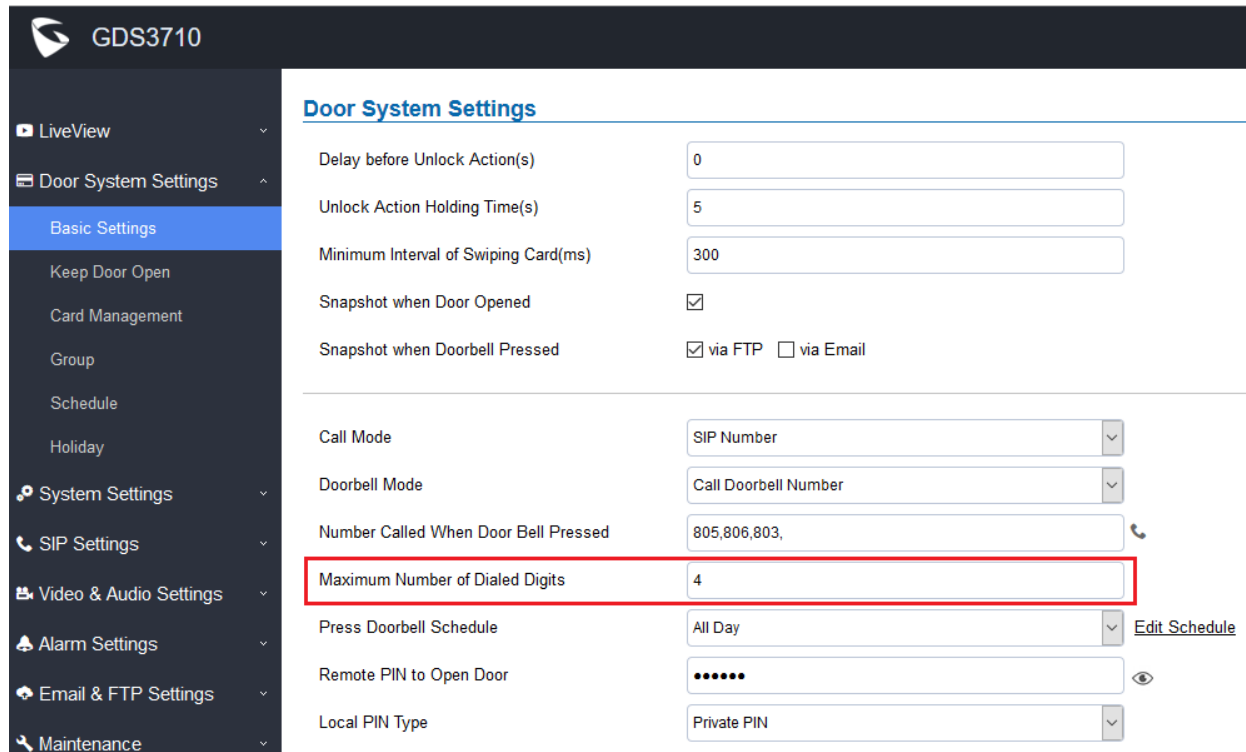
- **Functionality**

This feature allows user to configure a schedule to the Doorbell Button. Once configured, the doorbell button will turn ON or OFF based on configured schedule. For example, some users do not want the doorbell to work during the night.

MAXIMUM NUMBER OF DIGIT DIALED

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group
 - Schedule
 - Holiday
- System Settings
- SIP Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance

Door System Settings

Delay before Unlock Action(s)	0
Unlock Action Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Snapshot when Door Opened	<input checked="" type="checkbox"/>
Snapshot when Doorbell Pressed	<input checked="" type="checkbox"/> via FTP <input type="checkbox"/> via Email
Call Mode	SIP Number
Doorbell Mode	Call Doorbell Number
Number Called When Door Bell Pressed	805,806,803,
Maximum Number of Dialed Digits	4
Press Doorbell Schedule	All Day Edit Schedule
Remote PIN to Open Door
Local PIN Type	Private PIN

- **Functionality**

This feature will allow user to configure the maximum digits allowed to dial in the keypad. Once the configured condition satisfied, the device will send out the digits and call automatically without pressing #. This is similar to a very simple dial plan but just number of digits managed.

FIRMWARE VERSION 1.0.3.34

PRODUCT NAME

GDS3710 (HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A)

DATE

06/12/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement.

IMPORTANT UPGRADING NOTE

- **Local firmware upgrade recommended.**
- **Please download and use the “[Utility](#)” provided by Grandstream for local firmware upgrade, avoiding internet or power interruption to brick the device.**
- **[Factory Reset](#) is recommended after upgrading from old 1.0.1.xx or 1.0.2.xx firmware. Downgrade back to 1.0.1.xx or 1.0.2.xx is NOT supported once upgrade to 1.0.3.xx.**
- **Please backup data before performing factory reset then restore back the data.**

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Optimized ringing timeout and set to within 5 seconds.
- Optimized 4th MJPEG stream, added 1st, 2nd and 3rd MJPEG when encode type is MJPEG.
- Chrome and Firefox via websocket to get live video stream, NO Plugin required to install, but IE still requires the support of video plugin.
- Added support for basic authentication of MJPEG HTTP API (similar to GS IPC behavior).
- Added Open Door by configured schedule or time window.
- Added “Test” button for “Alarm Action” in the webUI.
- Added Alarm Notification for Access Attempts of users out of the configured schedule.
HTTP API Log Index Code: 1110, Non-scheduled Access (refer to related Log Type Document)
- Added option to send Snapshot via email when doorbell pressed.
- Added option to send “Call Completed Elsewhere” when doorbell pressed and door opened successfully by other GXP phones so no missing call logs will be displayed.
- Added RTCP/RTCP-XR for SIP Call.
- Improved Event Log UI layout.

BUG FIX

- Fixed GDS3710 doorbell call would fail if target is IP but with non-default port.
- Fixed GDS3710 RTCP feature not working as expected.
- Fixed Schedule Open Door time span configuration related issue.
- Fixed SMTP test failure when LLDP is disabled.
- Fixed NTP error occurred during RTCP/RTCP-XR transmission
- Fixed XML Config File not update the “Keep Door Open” settings if “Immediate Open Door” selected.
- Fixed the webpage display abnormal if there are special character “,” in the group name.
- Removed vague translation of “Open Door Valid Time” in WebUI and the HTTP API function module.
- Fixed the temperature sensor displayed abnormal in the WebUI.
- Fixed the doorbell tone distortion.
- Fixed HTTP API open door log message error.
- Fixed GDS3710 FTP uploading snapshots failure if FTP server using domain name.
- Fixed SIP call hangs up if DNS server is domain name

KNOWN ISSUES

- Video JPEG stream will fail in GXP audio phones when NAT involved.
- The SIP phone sending DTMF to GDS may sometimes hand up and clear the call
- Allowing to accept multiple calls at the same time
- Device will fail to send DNS resolution when Stun Server using FQDN (only IP Stun works)
- The 2nd outbound proxy will not use the DNS-SRV parsing domain name.
- The HTTP web access device may appear close_wait
- The option may crash if click the “Local Configuration Function”
- INVITE to an ICMP address, the doorbell still rings as normal.

NEW FUNCTIONS

- **Basic authentication of MJPEG video or Snapshot image via HTTP API to easy 3rd party System Integration, similar to GS IPC implementation.**

For easy system integration (with the cost of less secure), once the feature enabled (default is disabled), user can send HTTP API with correct credentials to retrieve MJPEG video or JPEG snapshot from GDS3710, similar to the behavior of Grandstream IP Cameras.

The HTTP API or CLI command listed as below:

MJPEG Video:

[http\(s\)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html](http(s)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html)

JPEG Snapshot:

[http\(s\)://admin:password@IP_GDS3710:Port/jpeg/view.html](http(s)://admin:password@IP_GDS3710:Port/jpeg/view.html)

NOTE:

- MJPEG stream may feel like animation due to the compromise of video quality and bandwidth.
- Similar command can be applied to open source application like **VLC MediaPlayer** to retrieve H.264 video stream with better quality:
rtsp://admin:password@IP_GDS3710:Port/X
where X= 0, 4, 8 corresponded to 1st, 2nd and 3rd video stream where 2nd **recommended**.

- **Open Door by configured schedule or time window.**

This feature is good for usage scene like schools or similar private or public places where the door needs to keep open at specific time window but closed otherwise. Also good for buildings or properties where a party or seminar need to be hosted for some period of time in a day (the door keeps open) then back to locked with authorized entry after that. Also good for lunch breaks in a factory or company where door open and no access log required.

- **Alarm Notification of Access Attempts by users out of the configured schedule**

This feature will allow related building or office managers aware the abnormal activities when legitimated users access the door out of the allowed configured schedule. For example, entry during weekend or night at not working hours.

- **Send Snapshot via email when doorbell pressed.**

This feature once enabled, the GDS3710 will email the snapshot when doorbell pressed, in addition to the existing feature that FTP the snapshots to the Server, if working SMTP configured.

- **Implemented “Call Completed Elsewhere” to omit “Missing Call Logs” in GXP phone**

This implementation will allow GXP phones NOT display “Missing Calls” in the log if the office having multiple GXP phones in the group to open door, can open door call is performed by other GXP.

- **Added RTCP/RTCP-XR for SIP Call to meet Cloud Solution Service Provider.**

This feature allows 3rd party Service Provider or Cloud Solution to monitor the operation status of the GDS3710 by using related SIP Calls.

NEW P-VALUE

P-Value	Values	Default Value	Comments
P15409	0: Disable 1: Enable	0	Email Snapshot when Doorbell Pressed
P15408	1~10	1	Non-scheduled Access Alarm Action Profile
P15407	0: Disable 1: Enable	0	Enable Non-scheduled Access Alarm
P2392	0: Disable 1: RTCP 2: RTCP-XR	0	Enable RTCP, RTCP-XR. Default disabled

NEW HTTP API

GET:

<http|https>://<servername>/goform/config?cmd=get&type=sip

SET:

<http|https>://<servername>/goform/config?cmd=set& P2392=<0|1|2>

For details please refer to HTTP API Document and User Manual.

NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

CHROME/FIREFOX NO PLUGIN REQUIRED FOR VIDEO LIVEVIEW

- **Web Configuration**

This option can be found under device web UI → LiveView →:



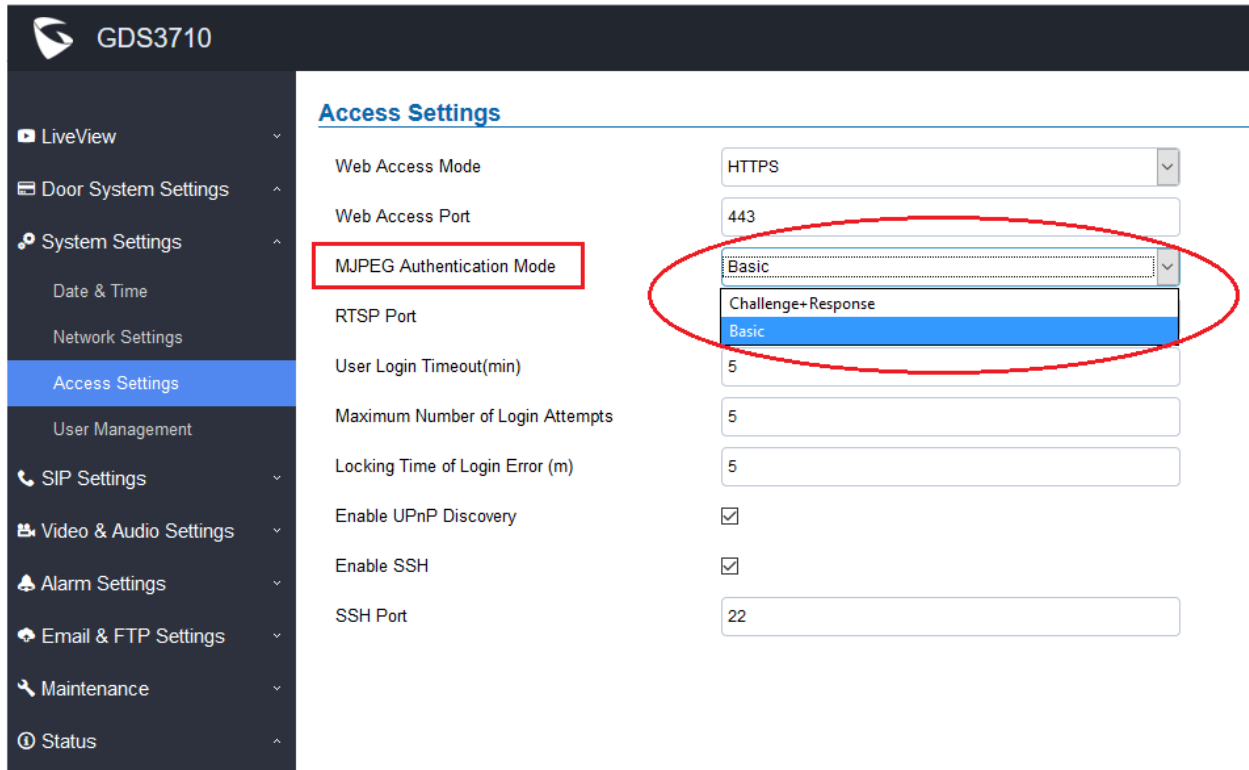
- **Functionality**

This feature allows user and installer to “Preview” the Live Video using popular browsers like Chrome or Firefox immediately without downloading and installing the plugins or NPAPIs like previously, due to most current browsers are not supporting the NPAPI anymore for security concern.

BASIC AUTHENTICATION of MJPEG VIDEO OR SNAPSHOT VIA HTTP API

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



The screenshot shows the GDS3710 web interface. On the left is a sidebar menu with options: LiveView, Door System Settings, System Settings (expanded), Date & Time, Network Settings, Access Settings (highlighted), User Management, SIP Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Access Settings' and contains the following configuration items:

- Web Access Mode: HTTPS
- Web Access Port: 443
- MJPEG Authentication Mode: Basic (highlighted with a red circle, showing a dropdown menu with 'Basic' and 'Challenge+Response' options)
- RTSP Port: (empty field)
- User Login Timeout(min): 5
- Maximum Number of Login Attempts: 5
- Locking Time of Login Error (m): 5
- Enable UPnP Discovery: ☒
- Enable SSH: ☒
- SSH Port: 22

- **Functionality**

Allow 3rd party system integrator or developers to implement related application for users. Details please refer to User Menu. By default this feature is disabled and use more secured “Challenge+Response” mode.

If enabled, user can send HTTP API with correct credentials to retrieve MJPEG video or JPEG snapshot from GDS3710, similar to the behavior of Grandstream IP Cameras.

The HTTP API or CLI command listed as below:

MJPEG Video:

[http\(s\)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html](http(s)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html)

JPEG Snapshot:

[http\(s\)://admin:password@IP_GDS3710:Port/jpeg/view.html](http(s)://admin:password@IP_GDS3710:Port/jpeg/view.html)

NOTE:

- MJPEG stream may feel like animation due to the compromise of video quality and bandwidth.
- Similar command can be applied to open source application like **VLC MediaPlayer** to retrieve H.264 video stream with better quality:
rtsp://admin:password@IP_GDS3710:Port/X
where X= 0, **4**, 8 corresponded to 1st, **2nd** and 3rd video stream where **2nd recommended**.
- Detailed information, please check out the updated *latest version* of **HTTP API**.

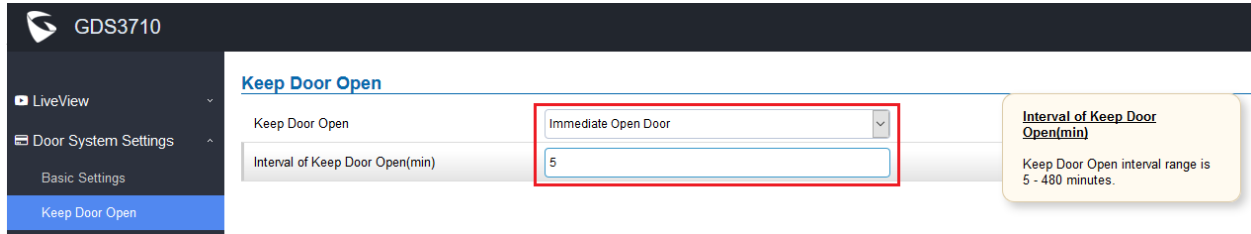
OPEN DOOR BY CONFIGURED SCHEDULE OR TIME WINDOW

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Keep Door Open:

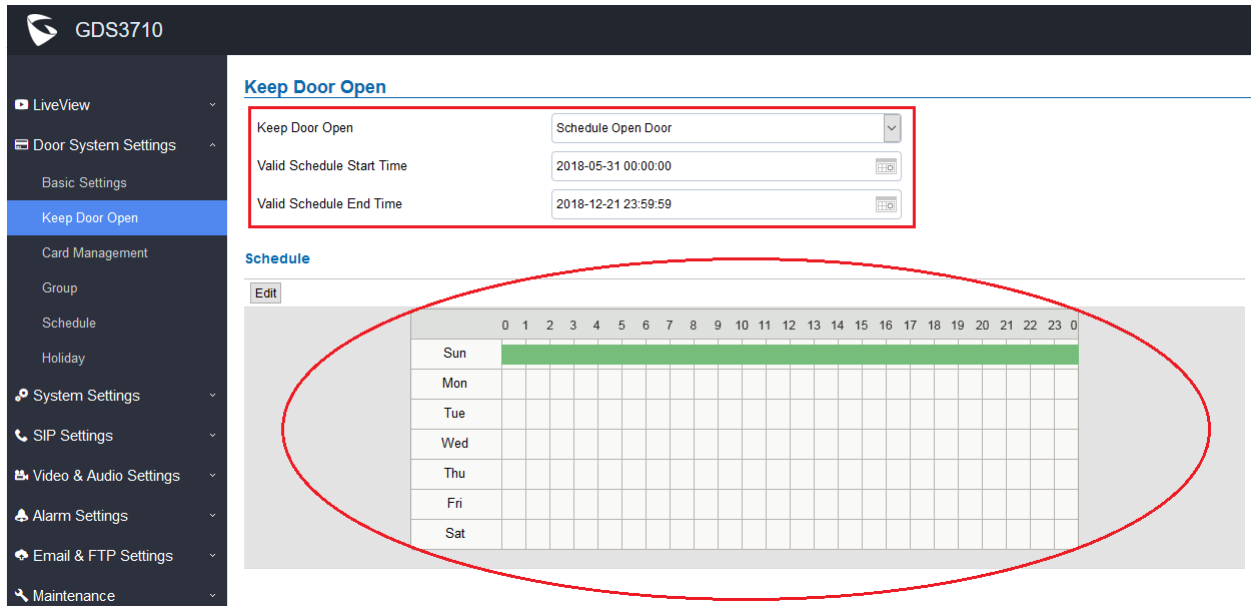
There are two mode:

1. Immediate Open Door (One Time Only Action)



The screenshot shows the 'Keep Door Open' configuration page for device GDS3710. The left sidebar contains a menu with 'LiveView', 'Door System Settings' (expanded), 'Basic Settings', and 'Keep Door Open' (selected). The main content area is titled 'Keep Door Open'. It features a dropdown menu for 'Keep Door Open' set to 'Immediate Open Door', a text input for 'Interval of Keep Door Open(min)' set to '5', and a yellow callout box stating 'Interval of Keep Door Open(min) Keep Door Open interval range is 5 - 480 minutes.'

2. Schedule Open Door (Repeated Action)



The screenshot shows the 'Keep Door Open' configuration page for device GDS3710, set to 'Schedule Open Door' mode. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Keep Door Open'. It features a dropdown menu for 'Keep Door Open' set to 'Schedule Open Door', a 'Valid Schedule Start Time' field set to '2018-05-31 00:00:00', and a 'Valid Schedule End Time' field set to '2018-12-21 23:59:59'. Below these fields is a 'Schedule' section with an 'Edit' button and a calendar grid. The calendar grid shows days of the week (Sun to Sat) and hours (0 to 23). The 'Sun' row is highlighted in green, indicating the door is open all day on Sunday. A red oval highlights the entire 'Schedule' section.

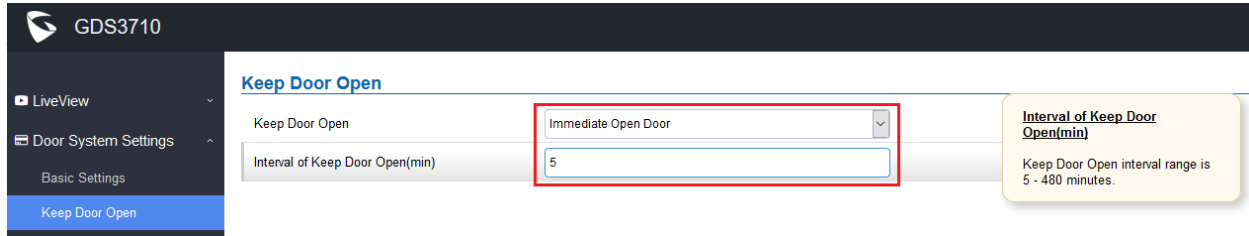
- **Functionality**

By default this feature is disabled. This feature when enabled will allow usage scene like schools or similar private or public places where the door needs to keep open at specific time window but closed otherwise. Also good for buildings or properties where a party or seminar need to be hosted for some period of time in a day (the door keeps open) then back to locked with authorized entry after that. Also good for lunch breaks in a factory or company where door open and no access log required.

ALARM NOTIFICATION OF ACCESS BY USERS OUT OF SCHEDULE

- Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Events Config:



- Functionality**

By default this feature is disabled. When configured and enabled, this feature will allow related building or office managers aware the abnormal activities when legitimated users access the door out of the allowed configured schedule. For example, entry during weekend or night at not working hours.

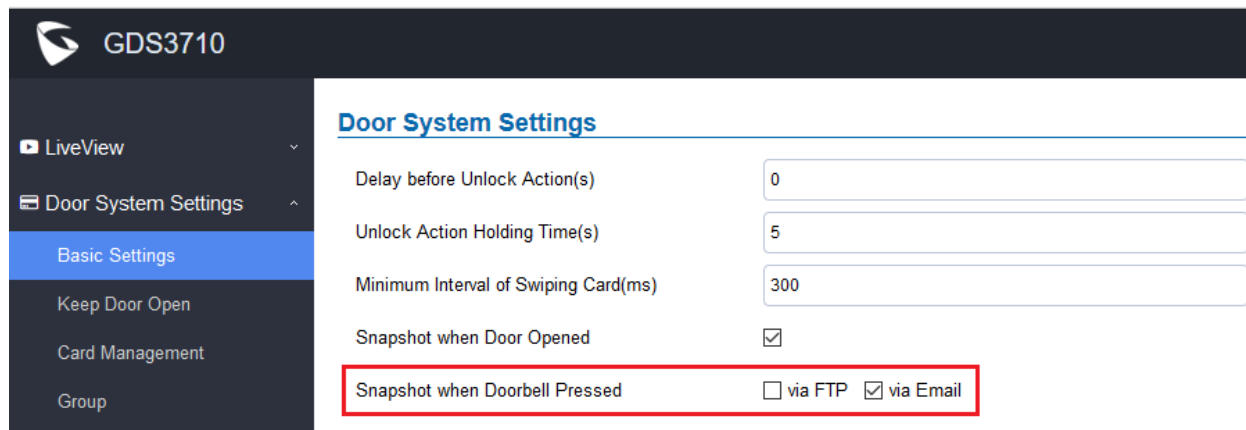
- New Pvalue**

P-Value	Values	Default Value	Comments
P15408	1~10	1	Non-scheduled Access Alarm Action Profile

SEND SNAPSHOT VIA EMAIL WHEN DOORBELL PRESSED

- Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

- LiveView
- Door System Settings
 - Basic Settings**
 - Keep Door Open
 - Card Management
 - Group

Door System Settings

Delay before Unlock Action(s): 0

Unlock Action Holding Time(s): 5

Minimum Interval of Swiping Card(ms): 300

Snapshot when Door Opened: ☒

Snapshot when Doorbell Pressed: ☐ via FTP ☒ via Email

- Functionality**

This feature once enabled, the GDS3710 will email the snapshot when doorbell pressed, in addition to the existing feature that FTP the snapshots to the Server, if working SMTP configured.

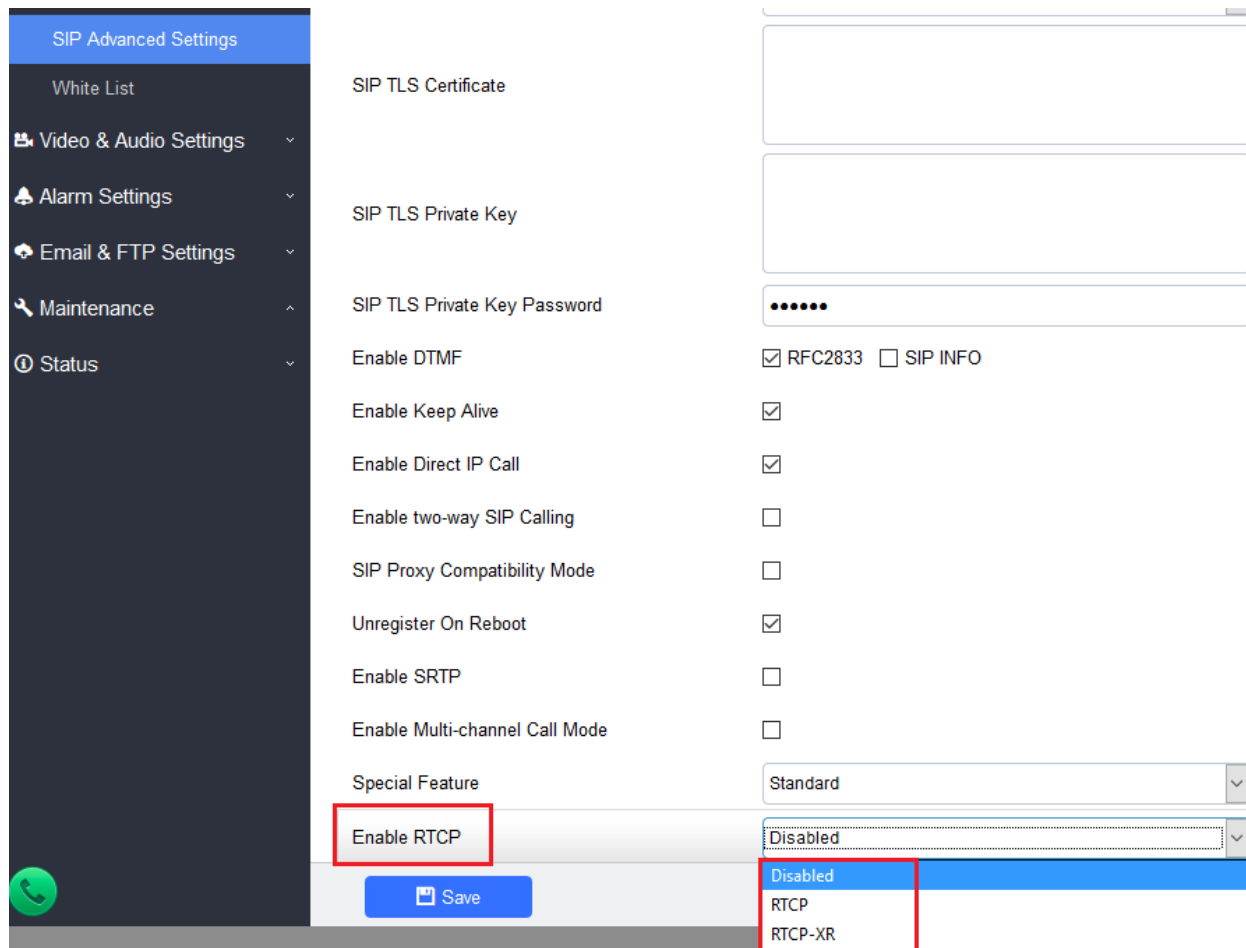
- New Pvalue**

P-Value	Values	Default Value	Comments
P15409	0: Disable 1: Enable	0	Email Snapshot when Doorbell Pressed

RTCP/RTCP-XR SIP CALL FOR ITSP/CLOUD SOLUTION

- Web Configuration**

This option can be found under device web UI → SIP Settings → SIP Advanced Settings:



The screenshot shows the 'SIP Advanced Settings' page. On the left is a dark sidebar with navigation links: 'SIP Advanced Settings' (selected), 'White List', 'Video & Audio Settings', 'Alarm Settings', 'Email & FTP Settings', 'Maintenance', and 'Status'. The main content area lists various settings: 'SIP TLS Certificate', 'SIP TLS Private Key', 'SIP TLS Private Key Password', 'Enable DTMF' (with checkboxes for RFC2833 and SIP INFO), 'Enable Keep Alive', 'Enable Direct IP Call', 'Enable two-way SIP Calling', 'SIP Proxy Compatibility Mode', 'Unregister On Reboot', 'Enable SRTP', 'Enable Multi-channel Call Mode', 'Special Feature' (set to Standard), and 'Enable RTCP'. The 'Enable RTCP' option is highlighted with a red box. Below it is a 'Save' button. To the right of 'Enable RTCP' is a dropdown menu that is open, showing three options: 'Disabled', 'RTCP', and 'RTCP-XR'. The 'RTCP' and 'RTCP-XR' options are highlighted with red boxes.

- Functionality**

This feature allows 3rd party Service Provider or Cloud Solution to monitor the operation status of the GDS3710 by using related SIP Calls.

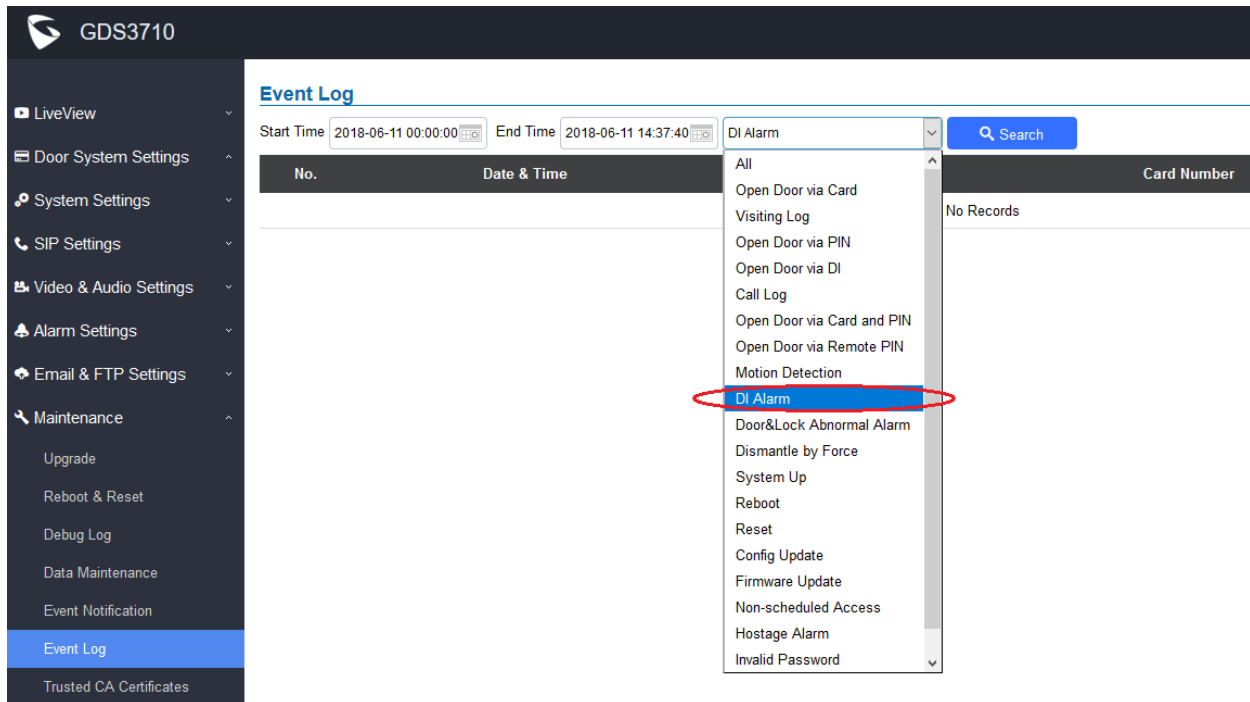
- New Pvalue**

P-Value	Values	Default Value	Comments
P2392	0, 1, 2	0: Disabled 1: RTCP 2: RTCP-XR	Enable RTCP, RTCP-XR. Default is Disabled.

IMPROVED EVENT LOG UI LAYOUT

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Log:



GDS3710

Event Log

Start Time: 2018-06-11 00:00:00 End Time: 2018-06-11 14:37:40

DI Alarm

Search

No.	Date & Time	Card Number
No Records		

Left Sidebar Menu:

- LiveView
- Door System Settings
- System Settings
- SIP Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
 - Upgrade
 - Reboot & Reset
 - Debug Log
 - Data Maintenance
 - Event Notification
 - Event Log**
 - Trusted CA Certificates

Event Log Dropdown Menu:

- All
- Open Door via Card
- Visiting Log
- Open Door via PIN
- Open Door via DI
- Call Log
- Open Door via Card and PIN
- Open Door via Remote PIN
- Motion Detection
- DI Alarm**
- Door&Lock Abnormal Alarm
- Dismantle by Force
- System Up
- Reboot
- Reset
- Config Update
- Firmware Update
- Non-scheduled Access
- Hostage Alarm
- Invalid Password

- **Functionality**

This UI layout improvement allows user to have a better choice and view about the Event Log.

FIRMWARE VERSION 1.0.3.32

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

05/08/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement.

IMPORTANT UPGRADING NOTE

- *Local firmware upgrade recommended.*
- *Please download and use the “[Utility](#)” provided by Grandstream for local firmware upgrade, avoiding internet or power interruption to brick the device.*
- *[Factory Reset](#) is recommended after upgrading from old 1.0.1.xx or 1.0.2.xx firmware. Downgrade back to 1.0.1.xx or 1.0.2.xx is NOT supported once upgrade to 1.0.3.xx.*
- *Please backup data before performing factory reset then restore back the data.*

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Added LED lighting indication pattern for firmware upgrade process. The sequence during upgrade is:
 - 1) Doorbell button blue LED will flash when firmware files are downloading.
 - 2) Digit 1,2,3 blue LED will flash during upgrading from 0 to 25%, then stays on;
 - 3) Digit 4,5,6 blue LED will flash during upgrading from 25 to 50%, then stays on;
 - 4) Digit 7,8,9 blue LED will flash during upgrading from 50 to 75%, then stays on;
 - 5) Digit *,0,# blue LED will flash during upgrading from 75 to 100%, then stays on;
 - 6) After all key's blue LEDs light on then flash twice then reboot itself to finish the upgrade process.
- Added White List Number to maximum 20 digits up to 30 records.
- Added support for HTTP command to Open Door.
- Added display device Logs at GDS webGUI.
- Added Start/End date for Card Management based on field feedback.
- Added "Test" Button for Alarm Action.
- Added "Alarm In/Out Status" display at GDS "Status" page GUI.
- Added Self-Define Event Notification Message.

BUG FIX

- Fixed Motion Detection and Tamper DI input, these two alarms cannot upload snapshots to the Central Storage and FTP server.
- Fixed Ringing timeout set to “0” unable to initiate the call.
- Fixed use call icon to call GXP/GXV phone and execute remote open door, the visiting log displayed error in GDSManager Utility Software.

KNOWN ISSUES

- Video JPEG stream will fail in GXP audio phones when NAT involved.
- The SIP phone sending DTMF to GDS may sometimes hand up and clear the call
- Allowing to accept multiple calls at the same time
- Device will fail to send DNS resolution when Stun Server using FQDN (only IP Stun works)
- The 2nd outbound proxy will not use the DNS-SRV parsing domain name.
- Device will not update to new IP after switching the network until after reboot.
- Device will not prompt error if IP address and Gateway configured incorrect.
- When unlocking latency is not zero, swiping card cannot clear unestablished SIP call.
- The HTTP web access device may appear close_wait
- The option may crash if click the “Local Configuration Function”
- IP address obtained by LLDP may be wrongly disabled.

NEW FUNCTIONS

- **LED Lighting Indication Pattern for Firmware Upgrade Process**

The sequence during upgrade is:

- 1) Doorbell button blue LED will flash when firmware files are downloading.
- 2) Digit 1,2,3 blue LED will flash during upgrading from 0 to 25%, then stays on;
- 3) Digit 4,5,6 blue LED will flash during upgrading from 25 to 50%, then stays on;
- 4) Digit 7,8,9 blue LED will flash during upgrading from 50 to 75%, then stays on;
- 5) Digit *,0,# blue LED will flash during upgrading from 75 to 100%, then stays on;
- 6) After all key's blue LEDs light on then flash twice then reboot itself to finish the upgrade process.

- **HTTP Open Door:**

3rd party system integrator can now "Enable" the HTTP API for Remote Open Door (Default is disabled, enable this feature customers will take the risk of security).

Grandstream provided a sample HTML utility to help customer to understand how to implement this feature. Details please refer to [HERE](#).

- **Self-Defined Event Message**

3rd party system integrator can now "Enable" the Event Notification and use Self-Defined Event Message. This allows system integrator to implement cloud service solution, like collecting real time event status from the GDS and centrally monitor the running status of the device.

NEW P-VALUE

P-Value	Values	Default Value	Comments
P15424	0- Disable 1- Enable	0	Enable HTTP API Remote Open Door
P15428	5~300	30	Open Door Valid Time
P15417	1: HTTP 2: HTTPS	1	Via Type
P15416	String	{"mac": "\${MAC} ", "content": " \${WARNING_MSG} "}	URL Template

NEW HTTP API

Enable HTTP API Remote Open Door



Open Door Valid Time

Enable Event Notification



Via Type

HTTP/HTTPS Server

HTTP/HTTPS Server Username

HTTP/HTTPS Server Password

URL Template

```
{"mac":"${MAC}","content":"${WARNING_MSG}"}
```

$\${MAC}$: MAC Address

For details please refer to User Menu.

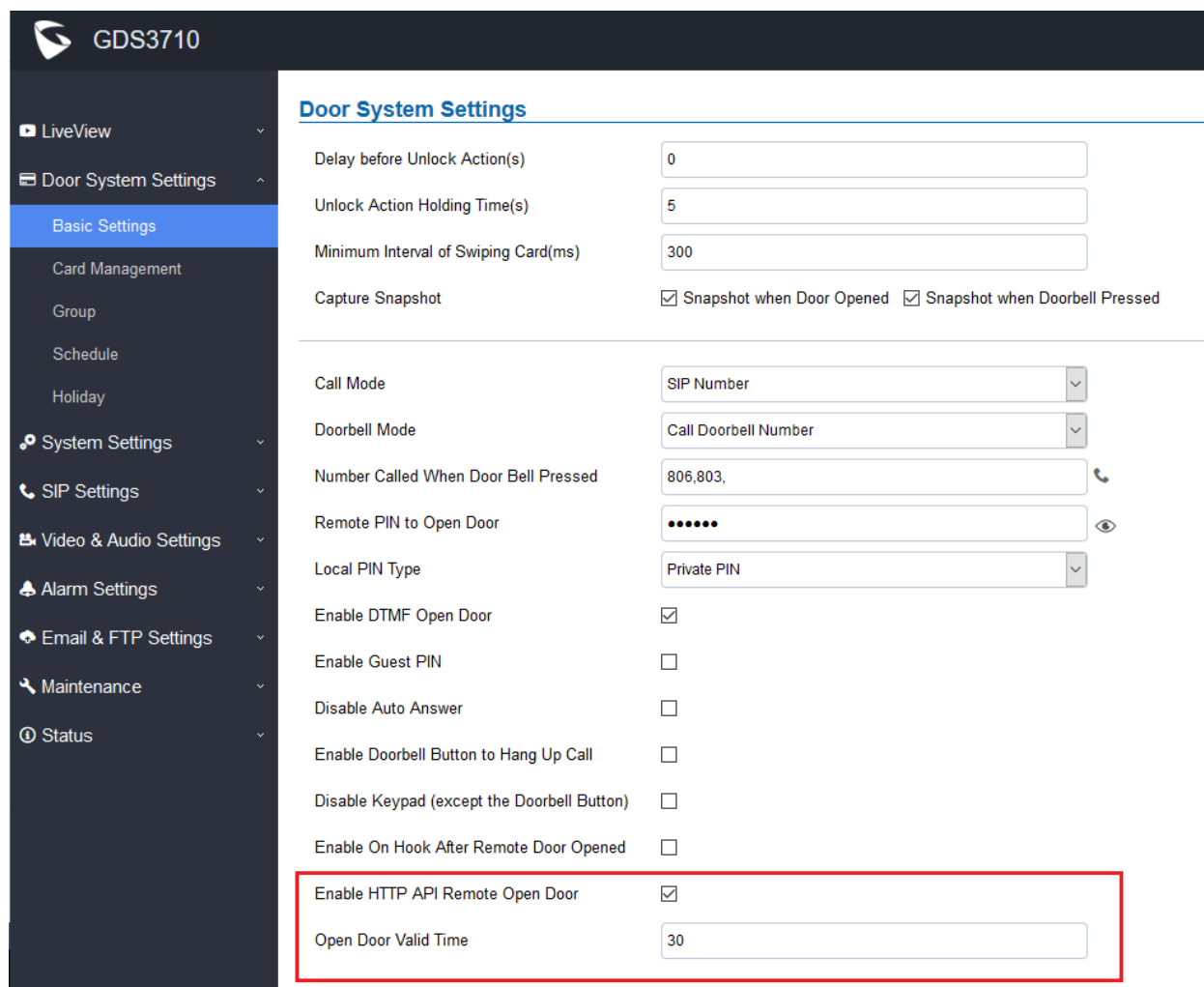
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.

HTTP OPEN DOOR

- Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



GDS3710

Door System Settings

Basic Settings

Card Management

Group

Schedule

Holiday

System Settings

SIP Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status

Delay before Unlock Action(s) 0

Unlock Action Holding Time(s) 5

Minimum Interval of Swiping Card(ms) 300

Capture Snapshot ☒ Snapshot when Door Opened ☒ Snapshot when Doorbell Pressed

Call Mode SIP Number

Doorbell Mode Call Doorbell Number

Number Called When Door Bell Pressed 806,803,

Remote PIN to Open Door

Local PIN Type Private PIN

Enable DTMF Open Door ☒

Enable Guest PIN ☐

Disable Auto Answer ☐

Enable Doorbell Button to Hang Up Call ☐

Disable Keypad (except the Doorbell Button) ☐

Enable On Hook After Remote Door Opened ☐

Enable HTTP API Remote Open Door ☒

Open Door Valid Time 30

- Functionality**

Allow 3rd party system integrator or developers to implement related application for users. Details please refer to User Menu or the sample HTML utility from Grandstream.

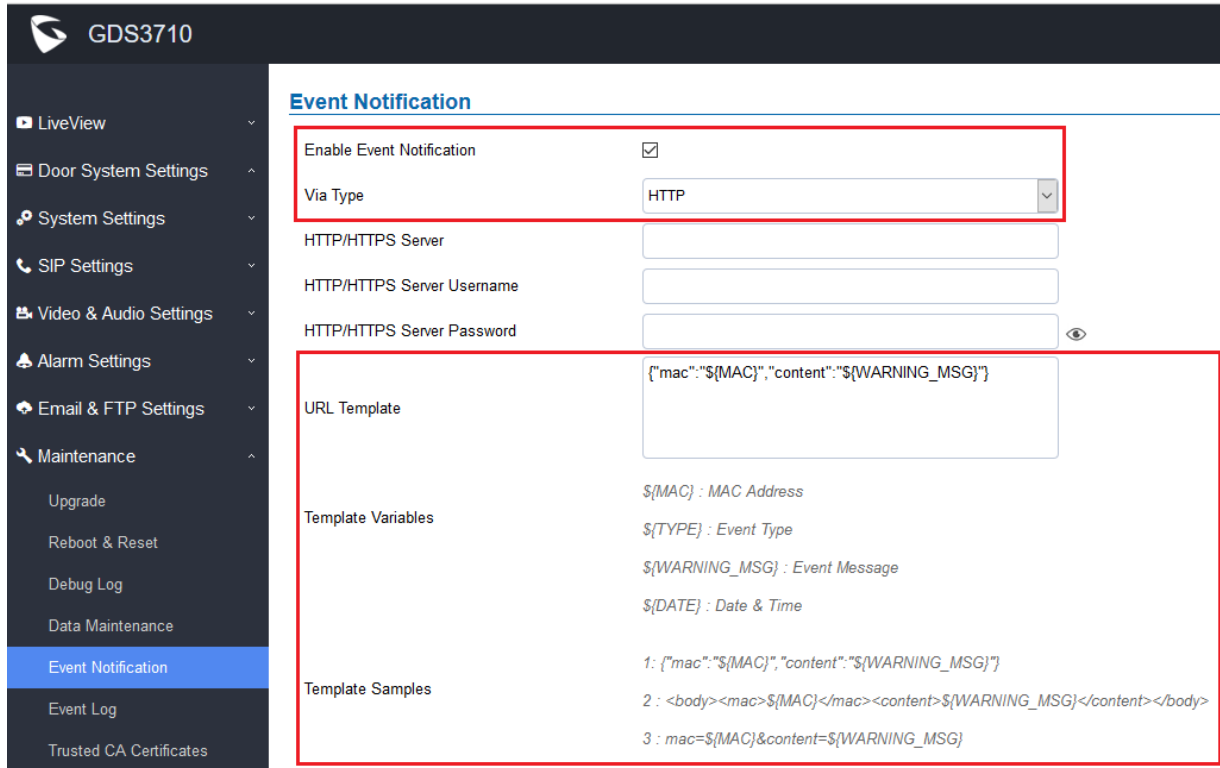
The Open Door Valid Time is a time window which allows the HTTP API to work when handing those HTTP API command, this is opened for user to configure based on the environment implemented.

For example, if the time is 30 seconds, then after initial HTTP API, within 30 seconds the valid command with correct authentication code should be received otherwise will time out and wait for new CLI.

SELF-DEFIND EVENT NOTIFICATION MESSAGE

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Notification:



Event Notification

Enable Event Notification ☒

Via Type HTTP

HTTP/HTTPS Server

HTTP/HTTPS Server Username

HTTP/HTTPS Server Password

URL Template

```
{ "mac": "${MAC}", "content": "${WARNING_MSG}" }
```

Template Variables

\${MAC} : MAC Address

\${TYPE} : Event Type

\${WARNING_MSG} : Event Message

\${DATE} : Date & Time

Template Samples

1: { "mac": "\${MAC}", "content": "\${WARNING_MSG}" }

2: <body><mac>\${MAC}</mac><content>\${WARNING_MSG}</content></body>

3: mac=\${MAC}&content=\${WARNING_MSG}

- **Functionality**

This feature allows the 3rd party system integrator or developer to implement Centralized Control or Monitor system (e.g.: the Cloud) to provide related service. Sample Event Notification Template illustrated in the webGUI. More details please refer to User Menu.

- **New Pvalue**

P-Value	Values	Default Value	Comments
P15424	2- Disable 3- Enable	0	Enable HTTP API Remote Open Door
P15428	5~300	30 (In Seconds)	Open Door Valid Time
P15417	1: HTTP; 2: HTTPS	1	Via Type
P15416	String	{ "mac": "\${MAC}", "content": "\${WARNING_MSG}" }	URL Template

FIRMWARE VERSION 1.0.3.31

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

04/23/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement.

IMPORTANT UPGRADING NOTE

- **Local firmware upgrade recommended.**
- **Please download and use the utility provided by Grandstream for local firmware upgrade, avoiding internet or power interruption to brick the device.**
- **Factory Reset is recommended after upgrading from old 1.0.1.x or 1.0.2.x firmware.**
- **Please backup data before performing factory reset then restore back the data.**

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- “Enable Doorbell Button to Hang Up Call” set as default value.
- Optimized ONVIF time zone settings and webGUI display.
- Added ability to disable certificate validation.
- Added event log and notification to System Up/Reboot/Reset/ConfigUpdate/FirmwareUpdate
- Added support for uploading Trusted CA Certificates
- Added “Unregister On Reboot” as default
- Added bad block handling schema in cache
- Added LED flash in pattern to indicate the provisioning process.

BUG FIX

- Fixed slow keypad response issue in some scenarios.
- Fixed Privacy Masks may fail sometimes if modifying audio codec or video resolution configuration.
- Fixed system no error prompt if configure IP address and Gateway incorrect.
- Fixed error when importing OSD text and alarm phone list in P value.
- Fixed the display format of time incorrect even the correct format chosen.
- Fixed at some noisy environment AEC broken causing echo at far side.
- Fixed backlight not off after RFID card swiped.
- Fixed sometimes device blocked, keypad dead without key tone and blue light, cannot make or accept SIP calls, no video and audio.
- Fixed not sending HTTP POST to the HTTP server.
- Fixed PIN Open Door stop working if DNS resolution failed
- Fixed incorrect password login issue and no password recovery email configured click “Save” showing the mailbox testing successful.
- Fixed the FTP configuration page the hint error and storage place error.
- Fixed SIP NOTIFY with resync event reboot the device issue.
- Fixed MD, Tamper Alarm, etc. snapshots storage location error.
- Fixed the device may reboot if enable HTTP server and Motion Detection.
- Fixed continuous MD events in long period of time could cause device no response to keypad and card swipe, and video continuously reconnecting.
- Fixed Group Adding Schedule Failure.
- Fixed Time Zone missing BagRep. Kiev (capital of Ukraine).

KNOWN ISSUES

- Video JPEG stream will fail in GXP audio phones when NAT involved.
- The SIP phone sending DTMF to GDS may sometimes hand up and clear the call
- Allowing to accept multiple calls at the same time
- Device will fail to send DNS resolution when Stun Server using FQDN (only IP Stun works)
- The 2nd outbound proxy will not use the DNS-SRV parsing domain name.
- Device will not update to new IP after switching the network until after reboot.
- Device will not prompt error if IP address and Gateway configured incorrect.
- When unlocking latency is not zero, swiping card cannot clear unestablished SIP call.
- The HTTP web access device may appear close_wait
- The option may crash if click the “Local Configuration Function”
- IP address obtained by LLDP may be wrongly disabled.

NEW FUNCTIONS

- **Key Function Modification:**

1. Depending on the first key input is "*" or numeric digit, the device will treat this as "password input" or "extension number input" separately, and Doorbell button will not function in this scene (not the first input) until the task finished or timeout.
2. If the first key input is Doorbell, device will treat this as calling the preconfigured numbers or IP addresses, then all other key input (like input local PIN to open door) will be disabled until the doorbell call finished or timeout.
3. When call in ringing stage before connected, all the keypad input will be disabled and no response, unless "Enable Doorbell Button to Hang Up Call" selected (default), then press the doorbell button can end the call. Otherwise if "Enable Doorbell Button to Hang Up Call" de-selected, call cannot be terminated from GDS keypad, the connected call will be terminated by far end and unconnected call will be ringing timeout.
4. When call established, all the keypad input will be treated as DTMF.

- **Alarm Modification**

1. When there are continuously alarm events in 30 minutes and every minute there is at least one new alarm event and alarm not be taken care, then the device will reduce the alarm frequency in next 10 minutes to save system resource. Instead of constantly sending out alarm, the device will send out one alarm in every 10 minutes, instead of sending lots of alarms, giving the above condition not changed.
2. If the next 10 minutes the condition not met, the device will restore back to normal alarm cycle to send out alarm.
3. If the above condition not satisfied, the device would use normal alarm cycle to send out alarm event report. That means if there is only one or less alarm event in every one minute, the device will just send out the alarm event when it happened.

NEW P-VALUE

P-Value	Values	Default Value	Comments
P8463	4- Disable 5- Enable	0	Validate Server Certificates
P8433-P8438	<string> Max.length=4096		Trusted CA Certificates Files

NEW HTTP API

<parameter>=<value>	Page	Values	Comments
P8463=<int>	Upgrade	0,1	Validate Server Certificates
type=<string>	Trusted CA Certificates	trustedca	Get Trusted CA Certificates info
P8433-P8438=< string >	Trusted CA Certificates	string	Trusted CA Certificates Files

NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use it from the user's point of view.



DOOR SYSTEM SETTINGS

- Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:

Door System Settings

Delay before Unlock Action(s)	<input type="text" value="0"/>
Unlock Action Holding Time(s)	<input type="text" value="5"/>
Min. Interval of Swiping Card(ms)	<input type="text" value="300"/>
Capture Image	<input checked="" type="checkbox"/> Unlock <input checked="" type="checkbox"/> Doorbell Pressed

Call Mode	<input type="text" value="SIP Number"/>
Doorbell Mode	<input type="text" value="Call Doorbell Number"/>
Number Called When Door Bell Pressed	<input type="text" value="803,806,"/> 
Remote PIN to Open the Door	<input type="text" value="....."/> 
Local PIN Type	<input type="text" value="Private Card PIN"/>
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>
Disable Auto Answer	<input type="checkbox"/>
Enable Doorbell Button to Hang Up Call	<input type="checkbox"/>
Disable Keypad (except Doorbell Button)	<input type="checkbox"/>
Enable On Hook After Remote Unlock	<input type="checkbox"/>

- **Functionality**

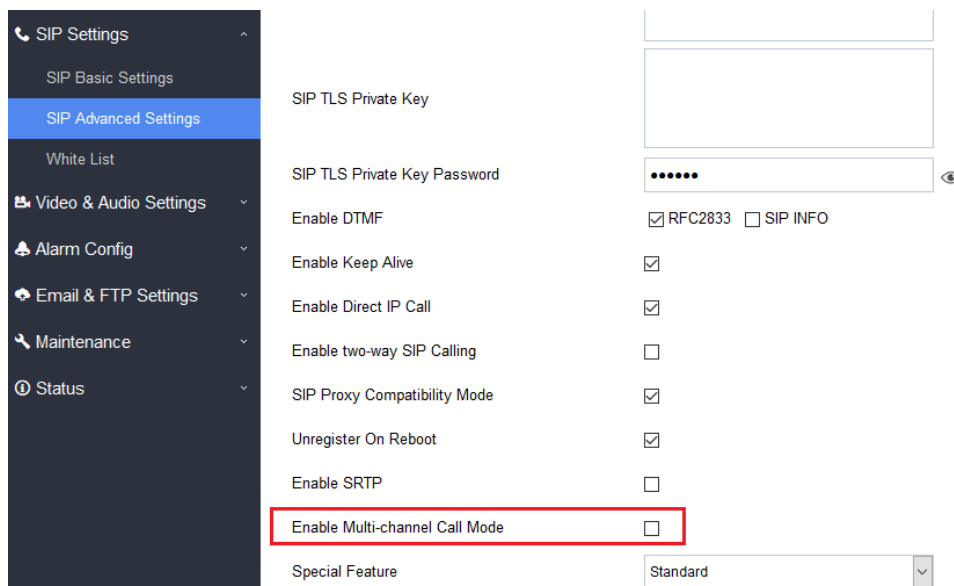
Several new functions have been revised for the wording:

1. Added taking snapshot when doorbell pressed.
2. Added lock keypad (only Doorbell working)
3. Added automatic clear the call when door opened.

MULTI-CHANNEL CALL MODE

- **Web Configuration**

This option can be found under device web UI → SIP Settings → SIP Advanced Settings:



The screenshot shows the 'SIP Settings' menu on the left, with 'SIP Advanced Settings' selected. The main panel displays various SIP configuration options. The 'Enable Multi-channel Call Mode' option is highlighted with a red box and is currently disabled (checkbox is unchecked). Other options include 'SIP TLS Private Key', 'SIP TLS Private Key Password', 'Enable DTMF', 'Enable Keep Alive', 'Enable Direct IP Call', 'Enable two-way SIP Calling', 'SIP Proxy Compatibility Mode', 'Unregister On Reboot', 'Enable SRTP', and 'Special Feature'.

- **Functionality**

This feature allows the device to receive multiple calls at the same time, with one active and others on hold (up to 4 calls maximum). The first call the blue LED light will light up keypad digit “1”, 2nd call will light up keypad digit “2”, and so on. On hold call will have related digit blinking while active call will have the digit blue LED solid light up. Call can be switched by pressing the blinking digits.

The default value is disabled, the device can only take ONE call at one time.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15427	Configure Multi-Channel Call Mode	Value = 0, Disable Value = 1, Enable	0, Disable

FIRMWARE VERSION 1.0.3.23

PRODUCT NAME

GDS3710 (*HW Supported: 1.3A, 1.3B, 1.5A, 1.6A, 1.7A*)

DATE

01/10/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement.

IMPORTANT UPGRADING NOTE

- *Once upgraded to 1.0.3.x firmware, **downgrading** to 1.0.2.x or previous lower firmware version is NOT SUPPORTED.*
- ***Factory Reset** is recommended after upgrading from old 1.0.1.x or 1.0.2.x firmware.*
- *Please backup data before performing factory reset then restore back the data.*

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	
GDS3710 HW1.7A	YES	

ENHANCEMENT

- Improved the tool tip content of “Central Mode”
- Improved the Doorbell Sound
- Added Standard Mode and Broadsoft Mode in SIP Settings, Broadsoft Supported.
- Improved some webGUI language and Tool Tip language.
- Added card ID number and phone number reported in event log message.
- Added “Click-to-Dial” feature support.

BUG FIX

- Fixed DHCP Option66 function invalid
- Fixed (Broadsoft) HTTP download fail when the URL contains double slash
- Fixed Session Timer on by default

- Fixed issues with Broadsoft Certificate
- Fixed audio collection failure when continuously pressing keys and swiping cards
- Fixed LLDP enabled SIP failed to register
- Fixed enabled silent alarm the Doorbell played.
- Fixed multiple RFID cards sharing same virtual number will cause private password invalid.
- Fixed GDSManager open door remotely the GDS3710 will not capture snapshot even configured.
- Fixed only calling first number in the alarm list
- Fixed confliction between Lock Keypad and Disable Auto Answer.
- Fixed mailbox configuration page cannot be closed.
- Fixed Wiegand keys output does not support private card PIN and private PIN.
- Fixed configuration file suffix displayed incorrectly.
- Fixed HTTPS failed to download the configuration file if file name with capital letters.
- Fixed alarm number deleted the device will still call the alarm phone when triggered.
- Fixed swipe card successfully will not cancel the unestablished SIP call.
- Fixed enable zero configuration will cause device reboot and download wrong data from UCM.
- Fixed text spelling error in Alarm Mail content.

KNOWN ISSUES

- Occasionally the keypad will slow or no response to the input but will recover in seconds
- The SIP phone sending DTMF to GDS may sometimes hang up and clear the call
- Allowing to accept multiple calls at the same time
- The 2nd outbound proxy will not use the DNS-SRV parsing domain name.
- GDS will not prompt when IP address and Gateway inconsistent.
- Device will not update to new IP after switching the network until after reboot.
- Modify audio codec and video resolution may cause privacy failure occasionally.
- When unlocking latency is not zero, swiping card cannot clear unestablished SIP call.

NEW P-VALUE

- P15425 Enable Wiegand Output Authentication
- P14121 Wiegand Output
- P6767 Firmware Upgrade Method
- P192 Firmware Server Path
- P6768 Firmware HTTP/HTTPS User Name
- P6769 Firmware HTTP/HTTPS Password
- P232 Firmware Upgrade File Prefix
- P233 Firmware Upgrade File Postfix
- P193 Automatic Upgrade Interval (Minutes)
- P212 Config Upgrade Method
- P237 Config Server Path
- P6776 Config HTTP/HTTPS User Name

- P6777 Config HTTP/HTTPS Password
- P234 Config Upgrade File Prefix
- P235 Config Upgrade File Postfix
- P2495 Enable Session Timer. 0: No. 1: Yes. Default is 0
- P424 Special Feature. 100: Standard. 102: Broadsoft. Default is 100
- P1360 HTTP/HTTPS User Name
- P1361 HTTP/HTTPS Password

NEW HTTP API

cmd=<string>	call	http sip call cmd
Call_type=<int>	<0 1>	0: end call 1: call
Call_num=<string>		Call num or IP
P15425=<int>	<0 1>	Enable Wiegand Output Authentication 0: Disable 1: Enable
P14121=<int>	<0 1 2>	Wiegand Output 0: Disable 1: Relay and Local authentication 2: Relay and Bypass local
P6767=<int>	<0 1 2>	Firmware Upgrade Method 0: TFTP 1: HTTP 2: HTTPS
P192=<string>		Firmware Server Path
P6768=<string>		Firmware HTTP/HTTPS User Name
P6769=<string>		Firmware HTTP/HTTPS Password
P232=<string>		Firmware Upgrade File Prefix
P233=<string>		Firmware Upgrade File Postfix
P193=<int>	60 - 525600	Automatic Upgrade Interval (Minutes)
P212=<int>	<0 1 2>	Config Upgrade Method 0: TFTP 1: HTTP 2: HTTPS
P237=<string>		Config Server Path
P6776=<string>		Config HTTP/HTTPS User Name
P6777=<string>		Config HTTP/HTTPS Password
P234=<string>		Config Upgrade File Prefix
P235=<string>		Config Upgrade File Postfix

NEW FEATURES OVERVIEW

This section lists major new features and describes how to use it from the user's point of view.

CENTRAL MODE

- Web Configuration**

This option can be found under device web UI → Dorr System Settings → Basic Settings → Card and Pin Schedule Configuration Mode.

Card and Pin schedule configuration Mode



- Functionality**

This feature only works with GDSManager. If enabled, Card Infor, Group, Schedule, Holiday can be synchronized with CentralServer (aka: GDSManager). No matter information revision on Central Side or on individual GDS side, this feature will make the information synchronized, from GDSManager to GDSs, or vice versa. Otherwise the revised information will only be updated locally. Default is Disabled.

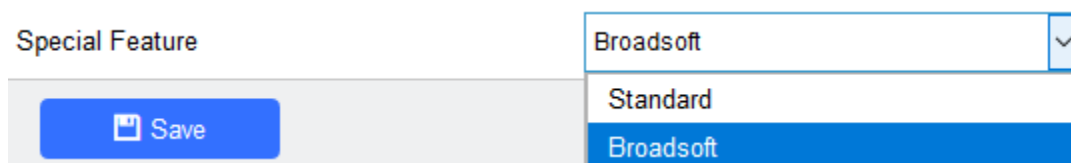
- New Pvalue**

Pvalue	Description	Value Range	Default
P15301	<New Pvalue> Central Mode	0 / 1 (0:Disable 1:Enable)	0

BROADSOFT MODE

- Web Configuration**

This option can be found under device web UI → SIP Settings → SIP Advanced Settings → Special Feature.



- Functionality**

This feature allows GDS to be compatible with Broadsoft softswitch. When enabled, the GDS will be able to be automatically mass provisioned and controlled by Broadsoft Server and provide features and services in that platform according.

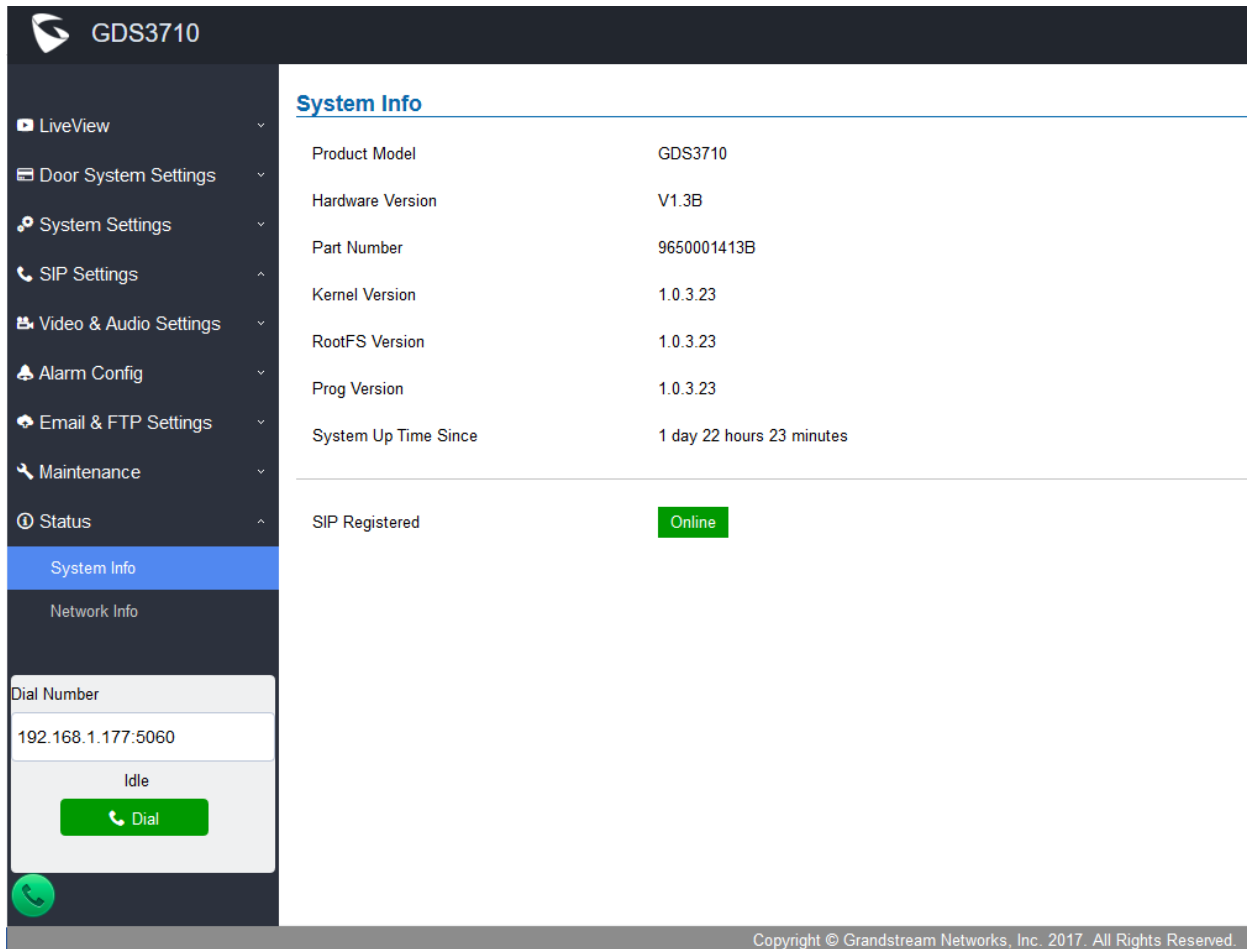
- **New Pvalue**

Pvalue	Description	Value Range	Default
P424	Configuration Special Features	Value = 100; Standard Value = 102; Broadsoft	100, Standard

CLICK TO DIAL

- **Web Configuration**

This feature allows user to log into the GDS webGUI and call out from GDS via browser. Administration privilege is required to use this function.



GDS3710

System Info

Product Model	GDS3710
Hardware Version	V1.3B
Part Number	9650001413B
Kernel Version	1.0.3.23
RootFS Version	1.0.3.23
Prog Version	1.0.3.23
System Up Time Since	1 day 22 hours 23 minutes

SIP Registered Online

Dial Number
192.168.1.177:5060

Idle

Dial

Copyright © Grandstream Networks, Inc. 2017. All Rights Reserved.

- **Functionality**

User can input and dial SIP extension number or phone number if the GDS registered to an operating SIP server/proxy. If no SIP server involved, user can still input the IP address and port number of a known IP video phone or audio phone in the same LAN.

FIRMWARE VERSION 1.0.3.13

PRODUCT NAME

GDS3710 (HW Supported: 1.3A, 1.3B, 1.5A, 1.6A)

DATE

12/3/2017

SUMMARY OF UPDATE

This is **MAJOR UPDATE** with new SDK.

Strongly recommend users to back up all the data (both configuration and application) before update, also perform factory reset if the previous firmware is old version in different lever.

IMPORTANT UPGRADING NOTE

- Once upgraded to 1.0.3.x firmware, **downgrading to 1.0.2.x or previous lower firmware version is NOT SUPPORTED.**
- **Factory Reset** is recommended after upgrading from old 1.0.1.x or 1.0.2.x firmware.
- Please backup data before performing factory reset then restore back the data

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW version	FW	Comments
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	

NEW P-VALUE

- | | |
|-------------------------------------|---|
| • Take snapshot when press keypad | P15420=0/1 0: Disable 1: Enable |
| • Enable Button to On Hook | P14582=0/1 0: Disable (Default) 1: Enable |
| • Disable Keypad | P15421=0/1 0: Disable (Default) 1: Enable |
| • Enable Unlock to On Hook | P15422=0/1 0: Disable (Default) 1: Enable |
| • Secondary Outbound Proxy | P2433=string Max.Length=255 |
| • Enable two-way SIP Calling | P8001=0/1 0: Disable 1: Enable |
| • Card Issuing State Expire Time(m) | P15423=1-1440 |
| • Enable Log Reporting | P15410=0/1 0: Disable 1: Enable |
| • HTTP Server Host | P15411=string Max. Length=128 |
| • HTTP Server Port | P15412=0-65535 |
| • HTTP Server URL | P15413=string Max.Length=256 |
| • HTTP Server Username | P15414=string Max.Length=128 |
| • HTTP Server Password | P15415=string Max.Length=128 |

ENHANCEMENT

- Improved the tool tip content of “Central Mode”
- Added option to disable alarm sound at phone side when event trigger SIP call to the phone.
- Increased maximum characters to 256 in “Number called when doorbell pressed” to allow serial hunting of SIP extensions or IP address with port or mixing of both, with each ring several seconds before going next.
- Added if schedule disabled, GDS3710 will bypass the option to open door.
- Enhanced the “Registration Expiration” timer settings.
- Adjusted some default values and its P values.
- Added feature to capture snapshot when doorbell pressed.
- Added feature to disable keypad input (lock keypad) and ONLY doorbell button can be pressed.
- Revised the tooltips of DI Open Door (alarm_in and alarm_out tooltips).
- Added option to disconnect call automatically after door open event.
- Added timer to expire Card Issuing Mode automatically.
- Added option to enable/disable call termination when OpenDoor Button (in the SIP phone side) pressed.
- Added ability for whitelist entries to open door using remote PIN.
- Implemented the HTTP Upload (RFID card) Log Event support for 3rd party Software Integration.
- Updated feature code input rule for *# or ** for doorbell and end operation in 2 seconds if pressed wrong.
- Added VLAN and Priority Parameters in the LLDP settings.

BUG FIX

- Fixed LLDP function not valid and IP will not automatically set to static if wrong VLAN Tag set.
- Fixed Wiegand lamp does not light up green when remote PIN entered to open door.
- Fixed Alarm Events Configuration displayed incorrectly.
- Fixed WDR mode very bright spot becoming pink issue and put back the WDR feature.
- Fixed swipe card still capture image even “capture image on unlock” unselected.
- Fixed unable to import the system configuration data.
- Fixed revising P value file with string like Holidays can still be imported
- Fixed using Hostage Code to open door if “capture image on unlock” un-checked, the device will not capture and upload the capture image.
- Fixed video cannot connect after motion detection alarm triggered.
- Fixed invalid P value in Holidays.
- Fixed SIP number is IP address and GDS as callee, DTMF unable to open door.
- Fixed GDS3710 cannot be searched and added by GVR355X NVR
- Fixed switch network the device restart
- Fixed network status page displayed error with default IP 192.168.1.168

- Fixed Group Information cannot be synchronized with GDSManager.
- Fixed initial delay in the audio call.
- Fixed * and ** not allowed in “Number called when doorbell pressed”.
- Fixed cannot handle IPPBX feature code “***”
- Fixed card information cannot be modified with IE9.
- Fixed DTMF set to SIP INFO or RFC2833, the open door function is invalid.
- Fixed device not reboot after receiving check-sync SIP message.
- Fixed STUN server filled the device will not send out Keep Alive packet.
- Fixed enable LLDP reboot the device will not do SIP registration.
- Fixed the PIN format is not consistent depending on In or Out call directions
- Fixed the schedule importing failed.
- Fixed DTMF cannot dial out from GDS3710 to interact with IVR.
- Fixed Guest PIN time duration unable to save.
- Fixed one-way audio issue in SIP call.
- Fixed in some network environment enable LLDP sometimes the device will not get IP address.
- Fixed using FQDN SIP domain name sometimes cause the key press no response.
- Fixed swipe card successfully the established unanswered SIP call by pressing doorbell not cancelled.
- Fixed keypad locked but the blue light still response to keypad pressing, should be no response.
- Fixed initial audio delay when audio call established.
- Fixed noise audio issue at the GDS output/speaker.
- Fixed invalid RFID card its mapped SIP extension can still remote open door by SIP call.
- Fixed if muted key tone, the wrong password input without prompt tone.
- Fixed UCM zero configuration the data pushed from UCM to GDS will not synchronized in GDS webGUI display.
- Fixed OSD time set for 12H the display in LiveView is not complete.
- Fixed card management page the information cannot be modified.
- Fixed when changing audio codec to G.722, the volume suddenly becomes louder.
- Fixed illegal format file imported to card management page without prompt warning.

KNOWN ISSUES

- The SIP phone sending DTMF to GDS may sometimes hand up and clear the call
- The alarm email text content may have error characters.
- When Doorbell On Hook uncheck but call established, press the button during the call in session will actually initial a new call and hold current call.
- GDS will accept new incoming call and automatically hold previous call but cannot get out of hold for previous call. GDS should reply 486 and reject all new incoming call when 1st call established.
- The 2nd outbound proxy will not use the DNS SRV parsing domain name.
- Occasionally the keypad will slow or no response to the input but will recover after seconds

NEW FEATURES OVERVIEW

This section lists major new features and describes how to use it from the user's point of view.

CENTRAL MODE

- **Web Configuration**

This option can be found under device web UI → Dorr System Settings → Basic Settings → Card and Pin Schedule Configuration Mode.

Card and Pin schedule configuration Mode

Central Mode
☒

- **Functionality**

This feature only works with GDSManager. If enabled, Card Infor, Group, Schedule, Holiday can be synchronized with CentralServer (aka: GDSManager). No matter information revision on Central Side or on individual GDS side, this feature will make the information synchronized, from GDSManager to GDSs, or vice versa. Otherwise the revised information will only be updated locally. Default is Disabled.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15301	<New Pvalue> Central Mode	0 / 1 (0:Disable 1:Enable)	0

DISABLE ALARM SOUND AT PHONE SIDE FOR TRIGERED SIP CALL

- **Web Configuration**

This option can be found under device web UI → SIP Settings → SIP Advanced Settings → Enable two-way SIP Calling.

Enable two-way SIP Calling
☒

- **Functionality**

This feature allows GDS to start two-way audio immediately at event triggered alarm calls. Default is checked, the alarm call triggered from GDS to phone will play pre-recorded Siren sound to the phone (user at phone side can press any key from the phone to stop Siren sound and start two-way communication).

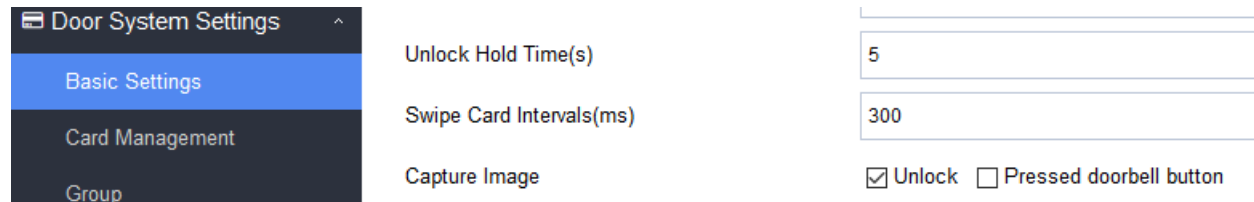
- **New Pvalue**

Pvalue	Description	Value Range	Default
P8001	Enable two-way SIP Calling	Value = 0; Disabled Value = 1; Enabled	1: Enabled

CAPTURE IMAGE WHEN DOOR BELL PRESSED

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings.



Door System Settings ^

- Basic Settings
- Card Management
- Group

Unlock Hold Time(s) 5

Swipe Card Intervals(ms) 300

Capture Image ☒ Unlock ☐ Pressed doorbell button

- **Functionality**

This feature allows GDS to take snapshot and upload to Central Server (GDSManager) or FTP server or send email attachment using preconfigured email account. Default is taking snapshot when door unlocked.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15420	Capture Image on Pressing Doorbell	Value = 0; Disabled Value = 1; Enabled	0: Disabled

DISABLE KEYPAD

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings.

Enable Doorbell Button to Hang Up Call ☐

Disable Keypad ☐

- **Functionality**

This feature allow user to lock and disable all keypad except the doorbell, so only press doorbell the GDS will be response. This meets some special usage scene where user only wants the doorbell.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15421	Disable Keypad	Value = 0; Disabled Value = 1; Enabled	1: Enabled

ENABLE REMOTE UNLOCK TO ON HOOK

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings.

Enable Remote Unlock to On Hook
☐

- **Functionality**

This feature will allow GDS to clear the call 5 seconds after the phone side successfully opened the door remotely. This will be convenient for IP phone users in case using hands free or speaker mode opening door remotely but forgetting hand up the phone to clear the call.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15422	Enable Remote Unlock to On Hook	Value = 0; Disabled Value = 1; Enabled	0: Disabled

DISABLE AUTO ANSWER

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings.

Enable Guest PIN ☐

Disable Auto Answer ☐

- **Functionality**

This feature allows to disable the default Auto Answer feature of the GDS door phone. The GDS will keep on ringing when called until someone press any button to pick up the call. This feature is for some special usage scenarios. Default is enabled and GDS is in Auto Answer mode.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P14580	Disable the Auto Answer of GDS	Value = 0; Disabled Value = 1; Enabled	1: Enabled

ENABLE DOORBELL BUTTON TO HANG UP CALL

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings.

Enable Doorbell Button to Hang Up Call ☐

Disable Keypad ☐

- **Functionality**

This feature allows doorbell button to be pressed to hand up the ongoing call, in case the number dialed is wrong or the callee is not available to answer the call made from the GDS door phone. Default is disabled.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P14582	Enable the Doorbell Button to Handup Call	Value = 0; Disabled Value = 1; Enabled	0: Disabled

CARD ISSUING STATE EXPIRED TIME

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings → Card Issuing State Setting → Enable Card Issuing Mode

Card Issuing State Setting

Enable Card Issuing Mode ☒

Card Issuing State Expire Time(m)

- **Functionality**

This feature will only available when “Enable Card Issuing Mode” select and enabled. The default value is 5 minutes. This feature will allow GDS to exist from the Card Issue Mode when the configured timer expired, This will help to prevent the human error in case the “Card Issuing Mode” is enabled and not restore back to the normal operation mode therefore the GDS is not operating as usual.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15423	Card Issuing Mode Effective Timer	Value Range (in Minutes): 1 ~ 1440	5 Minutes

LIGHT SETTINGS

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings → Light Settings

Light Settings

Enable Key Blue Light ☒

Enable Background Light ☒

- **Functionality**

This feature allow user to turn ON or OFF the Key Blue Light and the Background Light (White LED Light). Default both set of lights are On, so when key pressed the blue light will light up to show the key pressed, and the background white LED will light up to illuminate the user doing the operation.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P14800	Enable Key Blue Light	Value = 0; Disabled Value = 1; Enabled	1: Enabled
P14801	Enable Background Light	Value = 0; Disabled Value = 1; Enabled	1: Enabled

ENABLE DOORBELL BLUE LIGHT PER SETTINGS

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings.

Blue Doorbell Light Lighting Time Settings

Enable Blue Light	<input checked="" type="checkbox"/>
Start Time	17 : 00 : 00
End Time	23 : 00 : 00

- **Functionality**

This feature allows doorbell button blue light turn ON and OFF based on configured time schedule. For example user can configure the doorbell button light up in Blue Light in the evening when environment is dark without enough illumination. Default is disabled.

- **New Pvalue**

Pvalue	Description	Value Range (Pure Digital String)	Default
P14560	Doorbell Blue Light Start Time	MAX length is 6. Example: 125900 -> 12:59:00	000000
P14561	Doorbell Blue Light End Time	MAX length is 6. Example: 125900 -> 12:59:00	000000

ENABLE LOG REPORT

- **Web Configuration**

This option can be found under device web UI → Maintenance → Log Manager.

Log Manager

Enable Log Reporting	<input checked="" type="checkbox"/>
HTTP Server URL	<input type="text"/>
HTTP Server Username	<input type="text"/>
HTTP Server Password	<input type="password"/> 

- **Functionality**

This feature allow user to configure the Log Reporting feature via HTTP Server. The live log information will be sent to pre-configured HTTP Server for storage, diagnose and processing. The HTTP server can generate all kinds of related report based on the logs received. This is good for 3rd party redevelopment application usage.

- **New Pvalue**

Pvalue	Description	Value Range	Default
P15410	Enable Log Reporting	Value = 0; Disabled, 1; Enabled	0: Disabled
P15413	HTTP Server URL	Format: http://ip:port/path e.g.: http://192.100.10.10:80/	String. Max. Length=256
P15414	HTTP Server Username	String, Max. Length=128	String
P15415	HTTP Server Password	String, Max. Length=128	String.

FIRMWARE VERSION 1.0.2.25

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A*)

DATE

11/8/2017

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement

IMPORTANT UPGRADING NOTE

This version stopped HW1.2A/1.3A/1.3B fabrication support, still **support HTTP upgrade**.

Firmware applies to below HW versions:

HW version	FW	Comments
GDS3710 HW1.2A	YES	Only support HTTP upgrade image
GDS3710 HW1.3A	YES	Only support HTTP upgrade image
GDS3710 HW1.3B	YES	Only support HTTP upgrade image
GDS3710 HW1.5A	YES	
GDS3710 HW1.6A	YES	

NEW P-VALUE

- Enable Log Reporting P15410=0/1 (0: Disable 1: Enable)
- HTTP Server Host P15411=String (Max. Length=128)
- HTTP Server Port P15412=0-65535
- HTTP Server URL P15413=String (Max.Length=256)
- HTTP Server Username P15414=String (Max.Length=128)
- HTTP Server Password P15415=String (Max.Length=128)

ENHANCEMENT

- Added if schedule disabled, GDS3710 will bypass the option to open door.
- Implemented the HTTP Upload (RFID card) Log Event support for 3rd party Software Integration.

BUG FIX

- Fixed the initial delay in audio call
- Fixed the time will not be updated by NTP server after GDS reboot.
- Fixed the password field displayed with error.
- Fixed special character can be save and stored in Unlock Hold Time
- Fixed the system basic page display abnormal issue.
- Fixed GDS3710 cannot be searched and added by NVR GVR355x (via ONVIF)
- Fixed the P value is invalid for holiday
- Fixed Group information cannot be synchronized with GDSManager.
- Fixed reboot device after enable LLDP, SIP account may not be able to register.
- Fixed delete the RFID card operation the cancel icon not working
- Fixed enable LLDP might not be able to get IP address via DHCP in some (VLAN) environment

FIRMWARE VERSION 1.0.2.22

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A*)

DATE

09/18/2017

SUMMARY OF UPDATE

The main purpose of this release is bug fixes

IMPORTANT UPGRADING NOTE

- *Once upgraded to 1.0.2.x firmware, **downgrading** to 1.0.1.x or lower firmware version is NOT supported.*
- ***Factory Reset** is recommended after upgrading from 1.0.1.x to 1.0.2.x.*
- *Please backup data before performing factory reset then restore the data*

BUG FIX

- Fixed when uncheck "center mode", GDSManager group relationship etc. will fail.
- Fixed group deleted, group status and information disabled but card swiping fail.
- Fixed DTMF function is invalid at some cases.
- Fixed in Privacy Mask page the Show MD Region is invalid.
- Fixed set to 12-hour display format will not take effect and show wrong format.
- Fixed Silent Alarm option displaying errors.
- Fixed DTMF option format displayed wrong in IE browser.
- Fixed deleted 2nd alarm receiving email account the email still delivering.
- Fixed personnel, gender displaying error when card number is 0
- Fixed Wiegand Output feature issue.

FIRMWARE VERSION 1.0.2.21

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A)

DATE

08/31/2017

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement

IMPORTANT UPGRADING NOTE

- *Once upgraded to 1.0.2.x firmware, **downgrading** to 1.0.1.x or lower firmware version is NOT supported.*
- ***Factory Reset** is recommended after upgrading from 1.0.1.x to 1.0.2.x.*
- *Please backup data before performing factory reset then restore the data*

ENHANCEMENT

- Allow config and call IP address format on SIP field when dialing the Virtual Number
- Added "Silent Alarm" Mode
- Added option Backup/Restore including all passwords like SIP/FTP/RemoteAccess, etc.
- Added schedule support for Card and PIN
- Added LLDP support
- Added database automatic backup and synchronization
- Modified WebGUI style
- Added card information batch delete option in the WebGUI
- Added option to enable "Motion Detection", "Tamper Alarm" and backlight partially light
- Added card user limitation up to 2000 and group limit to 50.
- Added Card and PIN schedule configuration Central Mode. If enabled, the Group/Schedule/Holiday could only be synchronized from the Central of the GDS Manager
- Added LDC Ratio Control and Adjustment
- Expanded the range of Ring timeout
- Added option to disable Auto Answer
- Updated the "DingDong" tone when doorbell pressed
- Added function to check the default value
- Added Factory Reset via special procedures. Details please refer to updated User Manual
- Added file upload/download (card information, configuration etc.) can be executed after authentication
- Added enforcement when admin password is changed via WebGUI, user has to fill in a Valid Email

- Account to retrieve the email before the new admin password taking effect

BUG FIX

- Fixed Guest PIN invalid when modifying the guest pin conflicting with local PIN.
- Fixed the Blue Light turning off 1 minute late than configured time.
- Fixed SIP number is not displayed correctly at card management page.
- Fixed Holiday cannot display Chinese
- Fixed adjust resolution will make the Privacy Mask not working
- Fixed private door password displayed empty when PIN not configured
- Fixed error Email Format giving out confused prompt
- Fixed static IP with different subnet cannot be searched by GDSManager and GSuf_Pro
- Fixed Wiegand Output function is invalid sometimes.
- Fixed ONVIF device_service restart issue
- Fixed adjust and save the Door System setting page will restart the SIP client process
- Fixed Digital Input if in Open State, the Alarm State should also be in Open State
- Fixed revise the Group, Schedule and Holiday cannot be saved
- Fixed Wiegand Input can be directed to different protocol of the device
- Fixed Wiegand Input can be used as personal PIN to open the door
- Fixed one invalid P-value will fail the entire XML file import
- Fixed delete the group should automatically switch to disable card in that group
- Fixed group not available to displayed when carried schedule with holidays
- Fixed Wiegand Input can still open door even the “Wiegand Input” disabled
- Fixed exported configuration file missing P values of group, schedule and holidays
- Fixed issue when editing the region of Privacy Masks
- Fixed DHCP Option 66 invalid issue
- Fixed phone hand up but the doorbell still ringing
- Fixed Motion Detection sensibility is abnormal
- Fixed mute Key Tone will cause RFID card not response
- Fixed using Wiegand Input successfully open door via password but LED of Wiegand device is wrong

FIRMWARE VERSION 1.0.2.13

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A*)

DATE

06/26/2017

SUMMARY OF UPDATE

The main purpose of this release is bug fixes and feature enhancement

IMPORTANT UPGRADING NOTE

- *Once upgraded to 1.0.2.x firmware, **downgrading** to 1.0.1.x or lower firmware version is NOT supported.*
- ***Factory Reset** is recommended after upgrading from 1.0.1.x to 1.0.2.x.*
- *Please backup data before performing factory reset then restore the data*

ENHANCEMENT

- Supported **ONVIF Profile S**
- Added **"Privacy Mask"** support in Motion Detection Setting
- Updated OCX plugin engine to Version 3.1.0.74
- Added DTMF Open Door control option in WebGUI
- Supported HTTP API
- Optimized HTTP API for Card Management
- Added "enable blue doorbell light" option in the webGUI
- Added switch on the doorbell blue light by configured time period of the day.
- Implemented "Silent Alarm" mode
- Added HTTP API for getting snapshots and streams.
- Removed the size limit of load kernel

BUG FIX

- Fixed reload data is invalid.
- Fixed privacy mask may not work when adjusting CMOS video settings
- Fixed the initialization of DO causing short pulse when power up the device.
- Fixed webGUI may lose access when switching audio codecs.
- Fixed after getting IP address, the webGUI may not be accessible immediately.
- Fixed adjusting Mode, LED and Power Frequency settings may cause abnormal shutter speed.
- Fixed the display error of time zone.
- Fixed P value not working for enable DTMF Open Door.

FIRMWARE VERSION 1.0.2.9

PRODUCT NAME

GDS3710 (HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A)

DATE

06/1/2017

SUMMARY OF UPDATE

The main purpose of this release is bug fixes to response to market feedback.

IMPORTANT UPGRADING NOTE

- *Once upgraded to 1.0.2.x firmware, **downgrading** to 1.0.1.x or lower firmware version is NOT supported.*
- ***Factory Reset** is recommended after upgrading from 1.0.1.x to 1.0.2.x.*
- *Please backup data before performing factory reset then restore the data*

ENHANCEMENT

- Corrected errors in local PIN type tool tips.
- Add back DTMF Open Door as optional choice, with user acknowledging the security risk.
- Revised "Alarm Output Duration(s)" choice option as 5/10/15/20/25/30 seconds.

BUG FIX

- Fixed exporting file P value issue with Motion Detection data.
- Fixed changing the SSH port, it can be saved but cannot be accessed.
- Fixed device falling into reboot loop when failing to obtain IP address from network.
- Fixed ONVIF implementation causes automatic reboot due to memory leak.
- Fixed the initialization of DO causing short pulse when power up the device.
- Fixed back light and ring light issue when device rebooted.

FIRMWARE VERSION 1.0.2.5

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A, 1.6A*)

DATE

05/18/2017

SUMMARY OF UPDATE

This firmware version is a MAJOR update, with lots of bug fixes and feature enhancement

IMPORTANT UPGRADING NOTE

- *Once upgraded to 1.0.2.x firmware, **downgrading** to 1.0.1.x or lower firmware version is NOT supported.*
- ***Factory Reset** is recommended after upgrading from 1.0.1.x to 1.0.2.x.*
- *Please backup data before performing factory reset then restore the data*

ENHANCEMENT

- Added folder creation and file arrangement if multiple GDS3710s are uploading snapshots to FTP server.
- Improved the password prompt wording.
- Added DTMF audio playing when key be pressed.
- Separated volume control in webGUI.
- Added “Audio, Snapshot, Recording and File Path Saved” operation with icons at Live View webpage.
- Added “show password” feature when the eye icon be clicked in the webGUI.
- Added prompt popup message when capture button clicked.
- Use different email title to separate the Motion Detection and Temperature Out of the Range alarm.
- Set initial value of “0” for Virtual Number and SIP number if user leaving the field empty.
- Added support open door remotely via GDS Manager utility (after GDS Manager version 1.0.0.78)
- Supported GXP color phone JPEG_Over_HTTP support with encryption and authentication.
- Added SSH support with default TCP port 22, obsolete TELNET.
- Added GS_Wave (Android/iOS) Application support for Open Door.
- Added PING function in SSH CLI interface.
- Enhanced webGUI login process and added random default password.
- Enhance security by disable the DTMF to open door
- Disabled WDR Mode (temporarily, will enable once the pink color bug fixed)
- Added support of sending DTMF tone in SIP calling (RFC2833, SIP INFO)

BUG FIX

- Fixed web port and RTSP port not correct.
- Fixed exported system configuration data cannot be imported successfully.
- Fixed illegal or special characters can be saved into card number.
- Fixed non-digit characters can be saved into open door PIN field.
- Fixed abusively pressing keypad could make the key tone distorted and blue LED lighted abnormally.
- Fixed capture image not working when configured as “Card & Private PIN Mode”.
- Fixed exported configuration file without speaker volume, key tone volume and doorbell volume.
- Fixed Motion Detection selected region failed to be restored when exported.
- Fixed Option 66 feature not working.
- Fixed duplicated RFID card number can be added without prompt.
- Fixed the shutter speed not adjustable issue.
- Fixed failed test cases for ANATEL certification
- Fixed issue in peered IP Calling.
- Fixed P value cannot be written if the shutter speed is 1/5000.
- Fixed GDS3710 reboot cycle if P value is imported to the device incorrectly.
- Fixed firmware upgrade process could cause device to be automatically factory reset.
- Fixed Motion Detection sometimes abnormal issue.
- Fixed switching HTTPS to HTTP the port remains the same issue.
- Fixed cannot call GDS3710 via a number when peered with another device via IP.

FIRMWARE VERSION 1.0.1.19

PRODUCT NAME

GDS3710 (*HW Supported: 1.2A, 1.3A, 1.3B, 1.5A*)

DATE

03/06/2017

SUMMARY OF UPDATE

The main purpose of this release is bug fix and feature enhancement since \$1 Beta

ENHANCEMENT

- Added a button to view the password entered.
- Added "Guest Mode" for access control.
- Corrected some typo and wording reported.
- Added option to enable SIP extension call by dialing keypad directly.
- Removed the startup audio.
- Added OSD information into the alarm message title.
- Added RFIC card and Private PIN double authentication to improve the open door security.
- Added challenge-response algorithm to open door.
- Improved FTP snapshot filename by adding MAC address and event type.
- Update and improved G.722 AEC parameters.
- Reduced alarm email and attachment.
- Added function to allow all passwords been imported.
- Started one firmware file support from this version.
- Limited the remote PIN to open door to be pure digits only with maximum length of 8.
- Limited the maximum length of login password to be 32 characters.

BUG FIX

- Fixed device still has sound when volume set to 0
- Fixed AEC may fail sometimes at some special audio scenarios.
- Fixed HTTP Upgrade request the user-agent does not contain device name, hardware version and software version information for provisioning.
- Fixed press door bell will hand up alarming phone call.
- Fixed web port changing from 443 to 80, HTTPS cannot be accessed.
- Fixed no P value for shutter speed and interval of swiping card.
- Fixed click the UPnP cannot access the web interface.
- Fixed email setting page prompting error after clicking "Save".
- Fixed open door operation will clear all the pending calls, leave ongoing call untouched.
- Fixed configuration data cannot be imported normally.
- Fixed alarm email with abnormal name.
- Fixed no prompt tone when guest not input PIN in the required time window.
- Fixed input the wrong PIN, then correct PIN, the device will not open door.
- Fixed the RTSP value range, should be set to 554-65535.
- Fixed the snapshot filename different in FTP and Email.
- Fixed guest PIN and Private PIN confliction issue.
- Fixed DHCP OPTION66 not working problem.
- Fixed alarm snapshot cannot be uploaded to the central storage server.
- Fixed open door via PIN the equipment logs sometimes not match the record.
- Fixed the web port and RTSP port is not correct
- Fixed Guest PIN open door issue.