

深圳市潮流网络技术有限公司

GDS371X 系列 可视门禁

用户手册



GDS3712



GDS3710

技术支持

深圳市潮流网络技术有限公司为客户提供全方位的技术支持。您可以与本地代理商或服务提供商联系，也可以与公司总部直接联系。

地址：深圳市南山区科技园高新北区酷派大厦 C 座 14 层

邮编：518057

网址：<http://www.grandstream.cn>

客服电话：0755-26014600

客服传真：0755-26014601

技术支持热线：4008755751

技术支持论坛：<http://forums.grandstream.com/forums>

网上问题提交系统：<http://www.grandstream.com/support/submit-a-ticket>

商标注明



和其他潮流网络商标均为深圳市潮流网络技术有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

欢迎使用	17
产品概述	18
功能亮点	18
技术参数	18
入门	23
包装清单	23
GDS371x 描述	25
GDS371x 安装连线	26
GDS371x 接线引脚	27
GDS371x 背板连接	29
连接示例	30
使用 PoE 为设备供电	30
使用 PSU 为设备供电	31
了解 GDS371x	32
将 GDS371x 通过 DHCP 服务器连接到网络（推荐）	32
Windows 平台	32
GS Search	34
GDS Manager 管理工具	34
Apple 平台	35

使用静态 IP 连接 GDS371x	37
GDS371x 应用场景	39
无 SIP 服务器或 Internet 的对等模式	39
使用 SIP 服务器(UCM6XXX)	39
使用网络视频录像机 (NVR)	40
GDS371x 外设连接	41
报警输入/输出	42
保护二极管	43
连接示例	44
使用第三方电源接线示例	44
使用 GDS3710 和电锁两种电源的接线示例	45
使用 PoE 为 GDS3710 供电和第三方电源为电锁供电	45
良好的电击和大功率设备接线示例	46
Wiegand 模块接线示例	47
Wiegand 设备的第三方电源输入示例	47
GDS371x 和 Wiegand Device 的电源输入示例	48
输出示例, 配有 Wiegand 设备的第三方电源	48
Wiegand RFID 读卡器示例	49
当门异常打开时报警	49
GDS371X 连接: IN2 设置为常闭和使用第三方电锁的“失败安全”情景	50
GDS371X 连接: IN2 设置为常开和使用第三方电锁的“安全失败”情景	51
GDS371X 连接: IN2 设置为常开和使用带有门传感器的第三方电锁的“安全失败”场景	

.....	52
与 GSC3570 对接安全开门	52
单向互锁模式	55
通过 GDS37XX 带或不带 SIP 通话的开门	59
GDS371x WEB 主页	62
GDS371x 配置 & 语言页面	63
GDS371x 设置	64
实时预览	64
现场快速查看实时图像	65
MJPEG 流	68
门禁系统设置	70
基本设置	71
使用 Alarm Out (COM 1) 控制第二扇门	79
强制开门	82
紧急密码	85
卡片管理	86
手动添加卡片用户	87
自动添加用户卡片	89
分组	90
日程表	91
节假日	92
系统设置	92
时间日期设置	92

网络设置	93
OpenVPN® 设置	95
SNMP 设置	96
TR-069	98
访问设置	99
用户管理	102
账号	103
Account 1 - 4	103
电话设置	107
电话设置	107
账号[1-4] 白名单	109
点击拨打	110
音视频设置	111
视频设置	111
OSD 设置	113
CMOS 设置	114
音频设置	115
隐私遮挡	116
报警设置	116
A 报警事件配置	117
移动侦测	117
非授权 RFID 卡访问报警	122

报警动作设置	122
报警电话列表	124
邮件 & FTP 设置	124
邮件设置	125
FTP 和中心存储	125
维护设置	127
升级	128
重启 & 重置	129
系统日志	130
数据维护	131
系统健康通知	132
事件通知	133
事件日志	134
证书	136
状态	137
账号状态	137
系统信息	138
网络信息	140
连接 GDS371x 和 GXV33XX	141
连接 GS Wave 与 GDS371x 门系统	141
GDS371x HTTP API	141
恢复出厂	142

通过 Web GUI 恢复出厂	142
硬恢复出厂	142
使用 GS Search 硬恢复出厂	145
通过 SIP NOTIFY 恢复出厂设置	147
通过特殊组合键恢复出厂密码	147

表目录

表 1 : GDS3710/GDS3712 特性一览	18
表 2 : GDS3710 技术规格	21
表 3 : GDS3712 技术规格	23
表 4 : GDS371x 接线引脚	29
表 5 : 主界面描述	63
表 6 : 门禁系统设置	78
表 7 : 强制开门列表	83
表 8 : 强制开门时间设置	84
表 9 : 卡片信息	89
表 10 : 添加组	91
表 11 : 白名单	110
表 12 : CMOS 设置	115
表 13 : 音频设置	115
表 14 : 移动侦测	118
表 15 : 静默报警	120
表 16 : 挟持密码报警	120
表 17 : 防拆报警	120
表 18 : 键盘多次输入错误报警	121

表 19 : 启用超出日程表访问报警	121
表 20 : 报警电话列表	124
表 21 : 升级	129

图目录

图 1 : GDS3710 包装清单	24
图 2 : GDS3712 包装清单	25
图 3 : GDS3710 前视图和后视图	26
图 4 : GDS3712 前视图和后视图	26
图 5 : DS371x 背板连接	29
图 6 : GDS371x 后盖	30
图 7 : 连接示例	30
图 8 : 为 GDS371x 上电	31
图 9 : 通过 UPnP 检测 GDS3710	33
图 10 : GDS3710 登录界面	33
图 11 : GS Search Discovery	34
图 12 : GDS3710x 搜索	35
图 13 : Bonjour 设置界面	36
图 14 : Windows 静态 IP 地址配置	38
图 15 : GDS3710 配合 UCM6XXX 使用	40
图 16 : GDS3710 配合 S NVR 使用	41
图 17 : GDS3710 外设连接	42
图 18 : GDS371x 的报警输入/输出电路图	43
图 19 : 实施案例 1	44
图 20 : 实施案例 2	44
图 21 : 使用第三方电源接线示例	45

图 22 : 使用 GDS3710 和电锁两种电源的接线示例	45
图 23 : 使用 PoE 为 GDS3710 供电和第三方电源为电锁供电接线示例	46
图 24 : 需要避免的电锁连接示例	46
图 25 : 良好的电击和大功率设备接线示例	47
图 26 : Wiegand 设备的第三方电源输入示例	47
图 27 : GDS371x 和 Wiegand Device 的电源输入示例	48
图 28 : 输出示例, 配有 Wiegand 设备的第三方电源	49
图 29 : Wiegand RFID 读卡器示例	49
图 30 : 数字输入设置为常闭	50
图 31 : IN2 设置为常闭和使用第三方电锁的“失败安全”	51
图 32 : 数字输入设置为常开	51
图 33 : IN2 设置为正常开放和使用第三方电锁的“安全失败”情景	51
图 34 : IN2 设置为常开和使用带有门传感器的第三方电锁的“安全失败”场景	52
图 35 : GSC3570 通过 GDS3710 开门	52
图 36 : GSC3570 安全开门通过 GDS3710-GDS3710 配置	54
图 37 : GSC3570 通过 GDS3710-GSC3570 门系统配置安全开门	54
图 38 : GSC3570 通过 GDS3710-GSC3570 数字输入配置安全开门	55
图 39 : 单向连锁模式	56
图 40 : 单向连锁模式_GDS3710_CONFIGURATION_1	57
图 41 : 单向连锁模式_GDS3710_CONFIGURATION_2	58
图 42 : GDS37XX 配置示例	60
图 43 : GSC3570 配置示例	60

图 44 : 使用 SIP 通话开门.....	61
图 45 : 不使用 sip 通话开门.....	62
图 46 : 主界面.....	63
图 47 : GDS3712 登录界面.....	64
图 48 : 实时预览: 谷歌浏览器.....	65
图 49 : MJPEG 认证模式.....	66
图 50 : GDS3712 Admin 登录界面.....	66
图 51 : 使用安全 MJPEG 认证模式的实时图片.....	67
图 52 : 使用基本 MJPEG 身份验证模式的 MJPEG 视图.....	68
图 53 : MJPEG 认证模式.....	68
图 54 : MJPEG 查看 web 登录界面.....	69
图 55 : MJPEG 实时视图使用安全的 MJPEG 认证模式.....	69
图 56 : MJPEG 使用 Basic MJPEG 认证模式实时预览.....	70
图 57 : 门禁系统设置界面.....	71
图 58 : Alarm_Out1 功能.....	79
图 59 : Alarm_Out1 功能.....	80
图 60 : 通用本地密码.....	81
图 61 : 卡的权利和私人密码.....	82
图 62 : 强制开门开门.....	83
图 63 : 时间表开门.....	84
图 64 : 编辑时间表.....	85
图 65 : 强制开门 - 紧急密码.....	86

图 66 : 卡片管理	87
图 67 : 卡片信息	88
图 68 : 隐藏个人密码	89
图 69 : 查看个人密码	90
图 70 : 启用密码显示 (HTTPS)	90
图 71 : 添加组	91
图 72 : 组的列表	91
图 73 : 编辑日程表	92
图 74 : 编辑节假日	92
图 75 : 时间日期界面	93
图 76 : 网络设置页面	94
图 77 : OpenVPN 设置界面	95
图 78 : TR-069 设置界面	98
图 79 : 网页访问界面	100
图 80 : 用户管理界面	102
图 81 : 密码找回邮箱	103
图 82 : SIP 账号设置界面	104
图 83 : 电话设置界面	108
图 84 : 白名单页面	110
图 85 : 点击拨打	110
图 86 : 视频设置界面	111
图 87 : OSD 设置界面	114

图 88 : CMOS 设置界面	114
图 89 : 音频设置界面	115
图 90 : 隐私遮挡配置界面	116
图 91 : 事件配置界面	117
图 92 : 配置界面	118
图 93 : 数字输入	118
图 94 : 报警时间表	121
图 95 : 编辑时间表	122
图 96 : 非法刷卡时的报警动作	122
图 97 : 报警动作	123
图 98 : 编辑报警动作	123
图 99 : 报警电话列表	124
图 100 : 邮件设置 - SMTP 页面	125
图 101 : 图片存储设置界面	126
图 102 : FTP 文件名	127
图 103 : 重启和重置配置界面	130
图 104 : 系统日志界面	131
图 105 : 数据维护界面	131
图 106 : 系统健康通知	132
图 107 : 日志管理页面	134
图 108 : 事件日志	136
图 109 : 上传认证证书	137

图 110 : 系统状态界面	138
图 111 : 系统信息界面	139
图 112 : 网络信息页面	140
图 113 : 通过 Web GUI 恢复出厂	142
图 114 : 韦根连接图	143
图 115 : 韦根连接图	144
图 116 : GS Search 界面	145
图 117 : GS Search - 选中设备去 reset	146
图 118 : GS Search - reset	147

欢迎使用

GDS3710 是一款全景高清 IP 可视门禁系统，也可作为高清 IP 监控摄像机和 IP 对讲机为各种规模的建筑设施提供门禁控制和视频监控。这款强大的 IP 可视门禁系统提供 180 度的广角视频，内置 RFID 芯片读取器，实现安全无钥进入，内置麦克风和扬声器，支持视频对讲功能，并可与现有安全设备集成。GDS3710 与潮流网络的免费门禁管理软件 GDS Manager 配合部署，支持批量 RFID 卡信息多点推送，支持实时多点视频监控送并对 GDS 进行统一管理。通过符合 ONVIF 配置文件，可以将 GDS3710 与任何第三方 ONVIF 兼容监视或记录解决方案集成。GDS3710 采用先进的图像传感器处理器（ISP）和先进的图像算法，提供 1080P 高清视频分辨率，凭借卓越的性能，并在所有照明条件下提供出色的性能。采用 SIP/VoIP 技术，支持对智能手机、SIP 终端以及 GDS 管理软件进行双向音视频流发送。GDS3710 集成 PoE，白色 LED 智能补光，用于安全保护的移动侦测，以及照明控制开关等。GDS3710 配合潮流网络 IP 话机，多媒体可视电话、GS Wave 软电话提供了整套智能楼宇安防解决方案。

GDS3712 是一个半球 IP 视频对讲系统，也可作为高清 IP 监视摄像头，为各种尺寸的建筑提供设施访问控制和安全监控。GDS3712 采用高级图像传感器处理器图（ISP）和先进的图像算法，提供凭借卓越的性能。采用 SIP/VoIP 技术，支持对智能手机、SIP 终端以及 GDS 管理软件进行双向音视频流发送。GDS3712 集成 PoE，用于安全保护的移动侦测，照明控制开关、以及警报输入/输出等。GDS3712 也可以使用 GSURF PRO 或任何符合 ONVIF 的视频管理系统来管理。它还提供了灵活的 HTTP API，可轻松与第三方应用程序和其他监视系统集成。GDS3712 配合潮流网络 IP 话机，多媒体可视电话、GS Wave 软电话提供了整套智能楼宇安防解决方案。

产品概述

功能亮点

下表包含 GDS3710 和 GDS3712 的主要特性。

表 1: GDS3710/GDS3712 特性一览

技术参数

下表是 GDS3710 的所有技术规范，包括支持的协议/标准，语音编解码器，电话功能和升级/配置设置。

 <p>GDS3710</p>	<ul style="list-style-type: none"> ● 高性能流服务器，允许多个同时流传输会话访问。 ● 200 万像素 CMOS, 1920H x 1080V。 ● 与大多数第三方 SIP / VoIP 设备和领先的 SIP / NGN / IMS 平台具备良好的兼容性。 ● 2 报警输入/输出通道。 ● RS485, Wiegand 输入/输出。 ● RFID 卡读取器 ● 防风雨，防破坏
 <p>GDS3712</p>	<ul style="list-style-type: none"> ● 高性能流服务器，允许多个同时流传输会话访问。 ● 200 万像素 CMOS, 1920H x 1080V。 ● 与大多数第三方 SIP / VoIP 设备和领先的 SIP / NGN / IMS 平台具备良好的兼容性。 ● 2 报警输入/输出通道。 ● Wiegand 输入/输出。 ● 支持移动侦测 ● 内置麦克风和扬声器提供语音选项和对讲功能。 ● 防风雨，防破坏

视频压缩	H.264 High Profile / Main Profile / Base Profile, Motion JPEG.
图像传感器	1/2.7" , 2 200 万像素 1920H x 1080V.
镜头类型	1/2" , F2.5, FOV: 180° (W) x 150° (H).
日间&夜间	白色 LED 智能补光
最大分辨率	1920 x 1080.
最大分帧率	30fps
最小光圈	0.5Lux.
宽动态范围	支持, 高达 120dB.
嵌入式分析	动态检测
快照	通过电子邮件和/或 FTP 发送的事件触发
多流解决方案	高性能流服务器允许多用户同时访问: 主视频流: 1920 x 1080 分辨率, 用于连续全高清录制 辅助视频流: 640 x 480 分辨率, 用于 SIP / VoIP 视频通话 第三视频流: 320 x 240 分辨率的智能手机 APP 应用程序
网络协议	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, TR-069, ARP/RARP, ICMP, DNS, DHCP, SSH, SMTP, TFTP, NTP, STUN, TLS, SRTP.
SIP/VoIP	与大多数第三方 SIP / VoIP 设备和领先的 SIP / NGN / IMS 平台兼容
语音编码	G.711μ/a-law, G.722, G.729A/B, DTMF (RFC2833, SIP INFO), AEC.
QoS	第 2 层 QoS (802.1Q, 802.1P) 和第 3 层 QoS (ToS, DiffServ,

	MPLS)
安全性	用户和管理员级别访问控制，基于 MD5 和 MD5 的身份验证，256 位 AES 加密配置文件，TLS，SRTP，HTTPS，802.1Q
升级/配置	通过 TFTP / HTTP / HTTPS 进行固件升级，使用 TR-069 或 AES 的加密 XML 配置文件进行大规模部署。
音频输入	内置麦克风，高达 1.5m 带 AEC
音频输出	内置高清扬声器，放音范围高达 3 米
按键	12 键触摸板和一个电容式门铃按钮，每个都有单独的 LED 指示灯
RFID	RFID 125KHz: EM4100 (包括 1 张 RFID 卡和 1 个 RFID 钥匙扣)
报警输入	支持，2 通道，Vin <15V，用于门传感器或其他设备
报警输出	支持，是，2 通道，125VAC / 0.5A，30VDC / 2A，常开或常闭，用于电锁，灯开关或其他设备
网络接口	10M/100M 自适应
扩展接口	Wiegand (26 bits)输入输出接口
尺寸及重量	173mm(H) x 80mm(W) x 36mm(D). 0.6 Kg.
电源	PoE IEEE 802.3af 3 类或 12VDC / 1A 连接 (不包括交流电源适配器)
互操作性	ONVIF (Profile S).
侵入保护	防风雨，防破坏，支持额外的后加强金属板
湿度/温度	操作：-30° C 至 60° C (-22° F 至 140° F)

	储存: -35° C 至 60° C (-31° F 至 140° F) 湿度: 10%至 90%无冷凝
防护等级	IP66 (EN60529), IK09 (IEC62262).
认证	FCC: Part 15 subpart B Class B; Part 15 C; MPE CE: EN 55032 Class B; EN 61000-3-2; EN 61000-3-3; EN 50130; EN 60950-1; EN 300330; EN 301489; EN 62311 RCM: AS/NZS CISPR 22; AS/NZS 4268; AS/NZS 60950.1 IC: ICES-003; RSS310

表 2: GDS3710 技术规格

视频压缩	H.264 High Profile / Main Profile / Baseline Profile, Motion JPEG.
图像传感器	1/2.7" , 两百万像素 1920H x 1080V.
镜头类型	1/2" , F2.5, FOV:180° (W) x 150° (H).
最大分辨率	1920 x 1080.
最大帧率	30fps
最小光圈	0.5Lux.
宽动态范围	支持高达 120dB
视频比特率	128 kbps 至 4 Mbps, 用于预览和录音的多种类比特率。
PoE	IEEE 802.3af Class 3.
嵌入式分析	动态检测
快照	通过电子邮件和/或 FTP 发送的事件触发
多流解决方案	高性能流服务器允许多用户同时访问:

	<p>主视频流：1920 x 1080 分辨率，用于连续全高清录制</p> <p>辅助视频流：640 x 480 分辨率，用于 SIP / VoIP 视频通话</p> <p>第三视频流：320 x 240 分辨率的智能手机 APP 应用程序</p>
网络协议	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, TR-069, ARP/RARP, ICMP, LLDP-MED, DNS, DHCP, SSH, SMTP, TFTP, NTP, STUN, TLS, SRTP
SIP/VoIP	与大多数第三方 SIP / VoIP 设备和领先的 SIP / NGN / IMS 平台兼容
视频编码	G.711 μ /a-law, G.722, G.729A/B, DTMF (RFC2833, SIP INFO), AEC.
QoS	第二层 QoS (802.1Q, 802.1P)和第三层 QoS (ToS, DiffServ, MPLS).
安全性	用户和管理员级别访问控制，基于 MD5 和 MD5 的身份验证，256 位 AES 加密配置文件，TLS，SRTP，HTTPS，802.1Q
升级/ 配置	通过 TFTP / HTTP / HTTPS 进行固件升级，使用 TR-069 或 AES 的加密 XML 配置文件进行大规模部署。
音频输入	内置麦克风，高达 1.5m 带 AEC
音频输出	内置高清扬声器（2 瓦），放音范围高达 3 米
按钮	1 带有蓝色背光灯的呼叫按钮
报警输入	2 通道，Vin <15V，用于门传感器或其他设备
报警输出	2 通道，125VAC / 0.5A，30VDC / 2A，常开或常闭，用于电锁，灯开关或其他设备
网络接口	10M/100M 自适应
扩展接口	Wiegand (26 bits) 输入输出

尺寸及重量	明装: 173mm(H) x 80mm(W) x 36mm(D); 暗装: 217mm(H) x 120mm(W) x 11.6mm(D) 重量: 0.625 kg
电源	PoE IEEE 802.3af 3 类或 12VDC / 1A 连接 (不包括交流电源适配器)
侵入保护	防风雨, 防破坏, 支持额外的后加强金属板
温度/湿度	操作: -30° C to 60° C (-22° F to 140° F) 存储: -35° C to 60° C (-31° F to 140° F) 湿度: 10% to 90% 无冷凝
防护等级	IP66 (EN60529), IK09 (IEC62262).
认证	FCC: Part 15 subpart B Class B; Part 15 C; MPE CE: EN 55032 Class B; EN 61000-3-2; EN 61000-3-3; EN 50130; EN 60950-1; EN 300330; EN 301489; EN 62311 RCM: AS/NZS CISPR 22; AS/NZS 4268; AS/NZS 60950.1 IC: ICES-003; RSS310 UKCA

表 3: GDS3712 技术规格

入门

本章提供基本的安装说明, 包括包装内容的列表和信息, 以使用 GDS371X 视频门系统获得最佳性能。

包装清单

GDS3710

- | | |
|---|--|
| <ul style="list-style-type: none"> • 1 x GDS3710 • 1 x 安装支架 • 1 x 钻孔模板 | <ul style="list-style-type: none"> • 1 x 韦根线缆 • • 1 x 镜头清洁布 |
|---|--|

- 1 x 保护套
 - 4 x 橡胶垫圈
(用于密封背面
电缆)
 - 6 x 背板螺丝
 - 6 x 支架螺钉和
锚
 - 4 x 防撬螺丝
 - 1 x 防篡改六角
扳手
- - 1 x RFID Card (更多可从合作伙伴/经销商处购买)
 - 1 x Key Fob (更多可从合作伙伴/经销商处购买)
 -
 - 1 x 框架后盖
 -
 - 1 x 快速安装手册
 - 1 x GPL 证书.



图 1: GDS3710 包装清单

GDS3712

1 x GDS3712. 1 x 安装支架 1 x 钻孔模板 4 x 橡胶垫圈（用于密封背面电缆） 6 x 背板螺丝	6 x 支架螺钉和锚 1 x 防篡改六角扳手。 4 x 防撬螺丝 1 x 韦根线缆。 1 x 框架后盖 1 x 快速安装手册
--	---



图 2: GDS3712 包装清单

注意

安装前检查包装。如果您发现任何缺失，请与您的经销商联系。

GDS371x 描述

下图包含 GDS371x IP 可视门禁系统的后视图和前视图的组件:

GDS3710



图 3: GDS3710 前视图和后视图

GDS3712

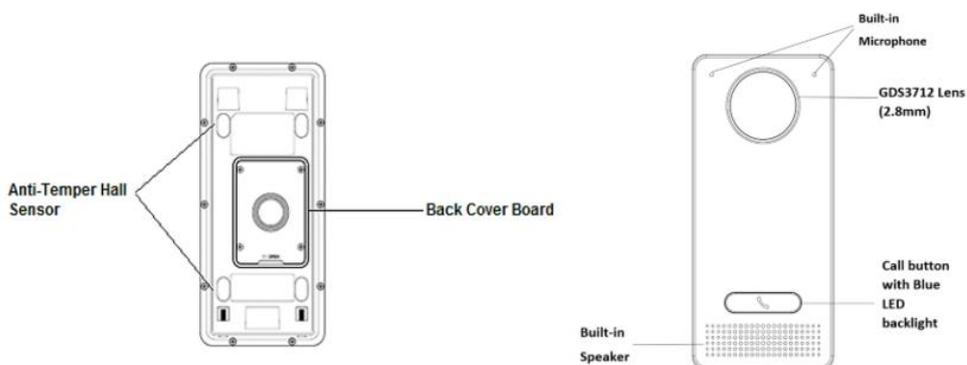


图 4: GDS3712 前视图和后视图

GDS371x 安装连线

GDS371x PoE 或 PSU 供电。

使用 PoE 供电 (建议)

- 将 RJ45 电缆的另一端连接到 PoE 交换机。
- 如果 PoE 开关不可用，可以使用 PoE 进样器。

使用电源适配器作为电源 (未提供 PSU)

- 将 RJ45 电缆的另一端连接到网络交换机或路由器。

- 通过相关电缆将 DC 12V 电源连接到 GDS371x 对应的引脚。

GDS371x 接线引脚

Jack	Signal	Function	Note	
J2 (Basic) 3.81mm	TX+	Ethernet PoE 802.3af Class 3, 12.95W	橙/白	数据
	TX-		橙	
	RX+		绿/白	
	RX-		绿	
	PoE_SP2		蓝 + 蓝/白	请将这两根导线短接在一起，分别连接到 SP1, SP2, 即使 PoE 未使用。
	PoE_SP1		棕 + 棕/白	
	GND	电源供电	最小 DC 12V, 1A	
12V				
J3 (Advanced) 3.81mm	GND	报警 GND		
	ALARM1_I N+	报警输入	Vin<15V	
	ALARM1_I N-			
ALARM2_I				

	N+			
	ALARM2_I N-			
	NO1	报警输出	继电器: 30VDC/2A; 125VAC/0.5A	
	COM1			
	NO2	电锁	对于“失败安全”(在失电时锁定)打击, 连接 COM2 和 NO2; 对于“故障安全”(无电源时打开)磁性锁定, 连接 COM2 和 NC2。 继电器: 30VDC / 2A; 125VAC / 0.5A	
	COM2			
NC2				
J4 (Special) 2.0mm	GND	韦根电源 GND	黑色	输入输出都要接线
	WG_D1_O UT	韦根输出信号	橙	GDS3710 作为读卡器的输出, 连接引脚 1, 2, 3
	WG_D0_O UT		棕	
	LED	Wiegand 输出 LED 信号	蓝	外部读卡器; 或 GDS3710 仅作为接收器
	WG_D1_IN	韦根输入信号	白	外部卡读卡器
	WG_D0_IN		绿	连接引脚 1,4,5,6,7,8
	BEEP	韦根输出 BEEP 信号	黄	仅适用于外部读卡器

	5V	韦根电源输出	红	<p>仅适用于外部卡读卡器。</p> <p>12VDC 供电外部读卡器必须使用自己的电源，不能使用此引脚。</p>
--	----	--------	---	---

表 4: GDS371x 接线引脚

GDS371x 背板连接

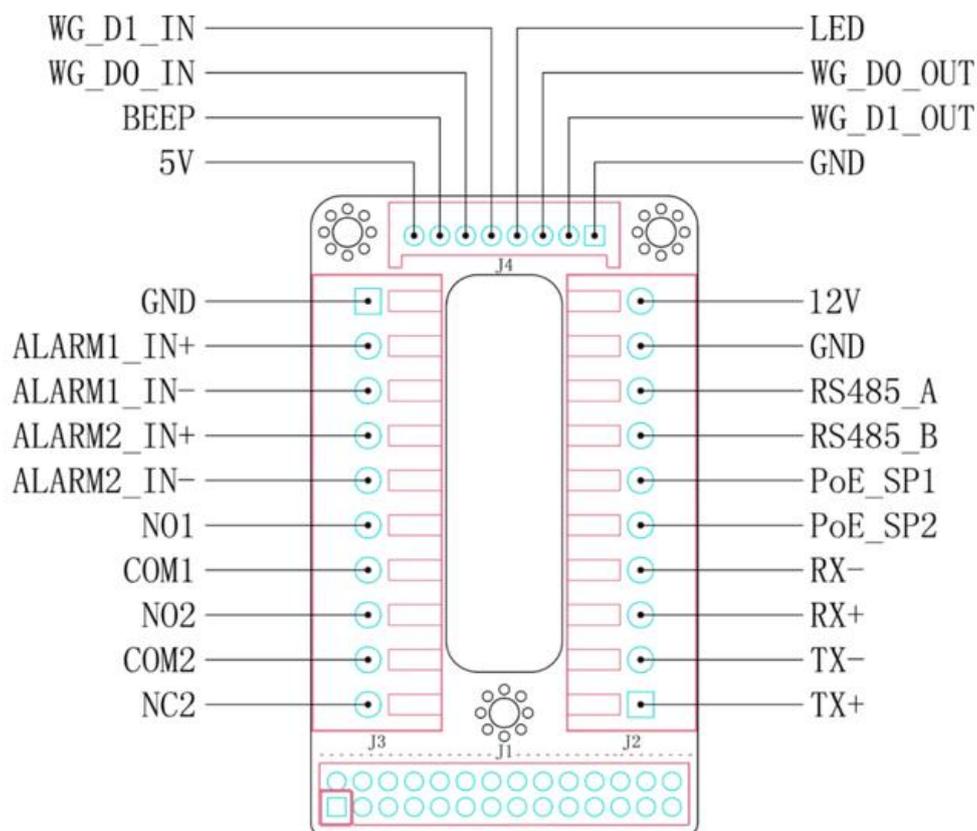


图 5: DS371x 背板连接

连接示例

通过使用 PoE 或 PSU 连接 GDS，请按照以下步骤操作：

打开 GDS3710 的后盖板，如下图所示：

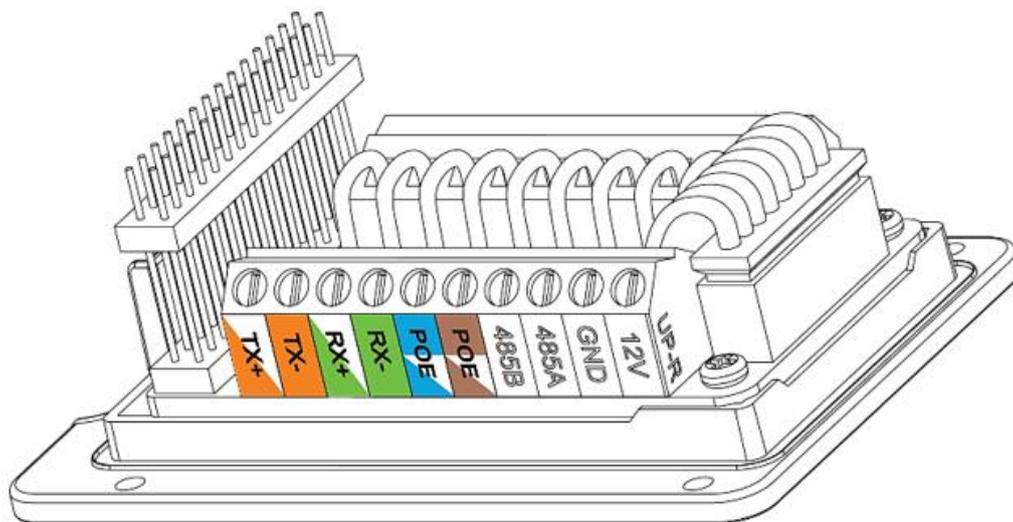


图 6: GDS371x 后盖

使用 PoE 为设备供电

切入 RJ45 电缆的塑料护套，然后解开并配对颜色，如下所示：

将 RJ45 的每种颜色连接到 GDS3710 对应的引脚，这样用户可以使用 PoE 为设备供电。

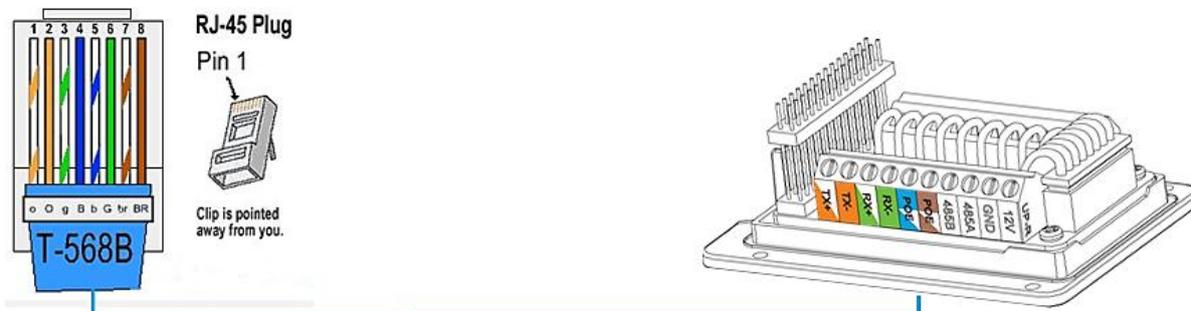


图 7: 连接示例

将 RJ45 的每种颜色连接到 GDS371x 对应的引脚，这样用户可以使用 PoE 为设备供电。

使用 PSU 为设备供电

使用 PSU 为设备供电，请使用万用表检测电源的极性，然后将 GND 连接到 PSU 的负极，将 12V 电源连接到 PSU 的正极。

注意：如果用户没有 PoE 交换机，则无需将蓝线和棕线连接到 GDS3710，因为它用于通过以太网为设备供电。

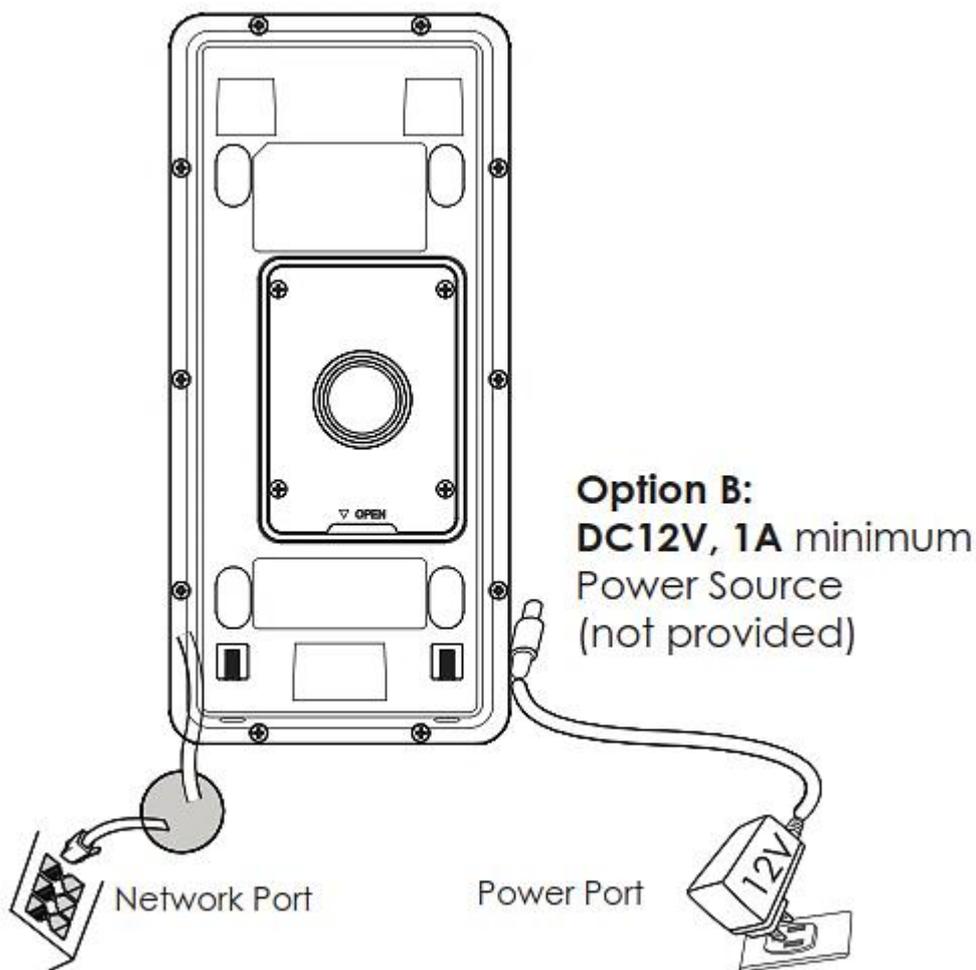


图 8: 为 GDS371x 上电

了解 GDS371x

GDS371x 有一个嵌入式 Web 服务器来响应 HTTP GET / POST 请求。嵌入式 HTML 页面允许用户通过 Microsoft Internet Explorer 或 Firefox 和 Chrome（需要来自潮流的插件）配置 GDS371x。

1. 从 GDS371X WebGUI 下载 WebControl 插件，对于苹果平台 OS-X，目前只支持 MJPEG 视频编解码器。

注意：

请在下载或安装用于 Firefox / Chrome 的潮流 WebControl 插件或用 IE 浏览器的“GSViewerX.cab”时，暂时禁用防病毒或 Internet 安全软件。请关闭浏览器以安装下载的插件或 Active-X。

如果杀毒或安全软件提示，请信任并安装下载的文件。

将 GDS371x 通过 DHCP 服务器连接到网络（推荐）

默认情况下，GDS371x 启用时作为 DHCP 客户端，它将从运行 DHCP 服务器的网络自动获取 IP 地址。

Windows 平台

Windows 用户有两种方法访问 GDS371x：

1. 即插即用

默认情况下，GDS371x 的 UPnP 功能打开。对于使用启用 UPnP 的 Windows 网络（大多数 SOHO 路由器支持 UPnP）的客户，访问 GDS371x 非常容易：在此示例中，我们将 GDS3710 作为示例：

1. 在 windows 桌面上找到网络图标  Network 。
2. 单击图标进入“网络”，GDS3710 将列为“其他设备”，如下所示。如果没有显示，请刷新页面。
否则，UPnP 可能不在网络中活动。

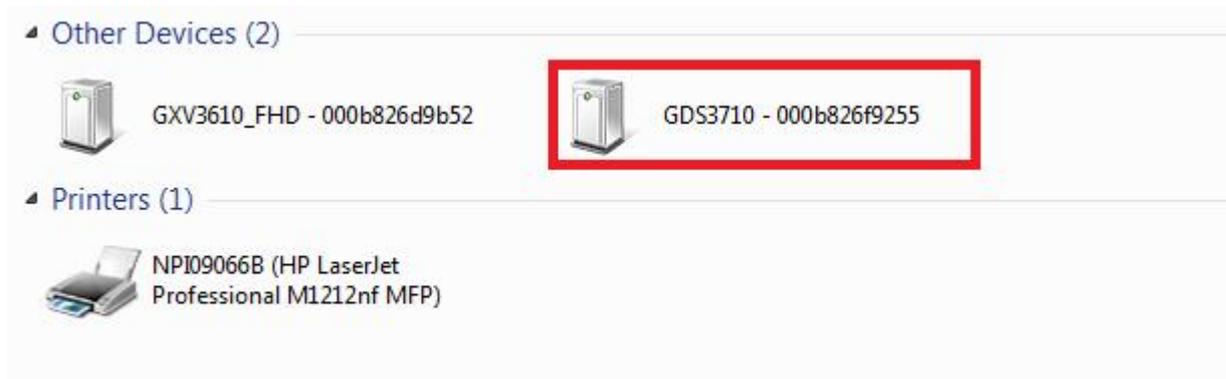


图 9: 通过 UPnP 检测 GDS3710

单击相关 GDS3710 的显示图标，默认浏览器（例如：Firefox 或 Chrome）将打开并直接连接到登录页面。

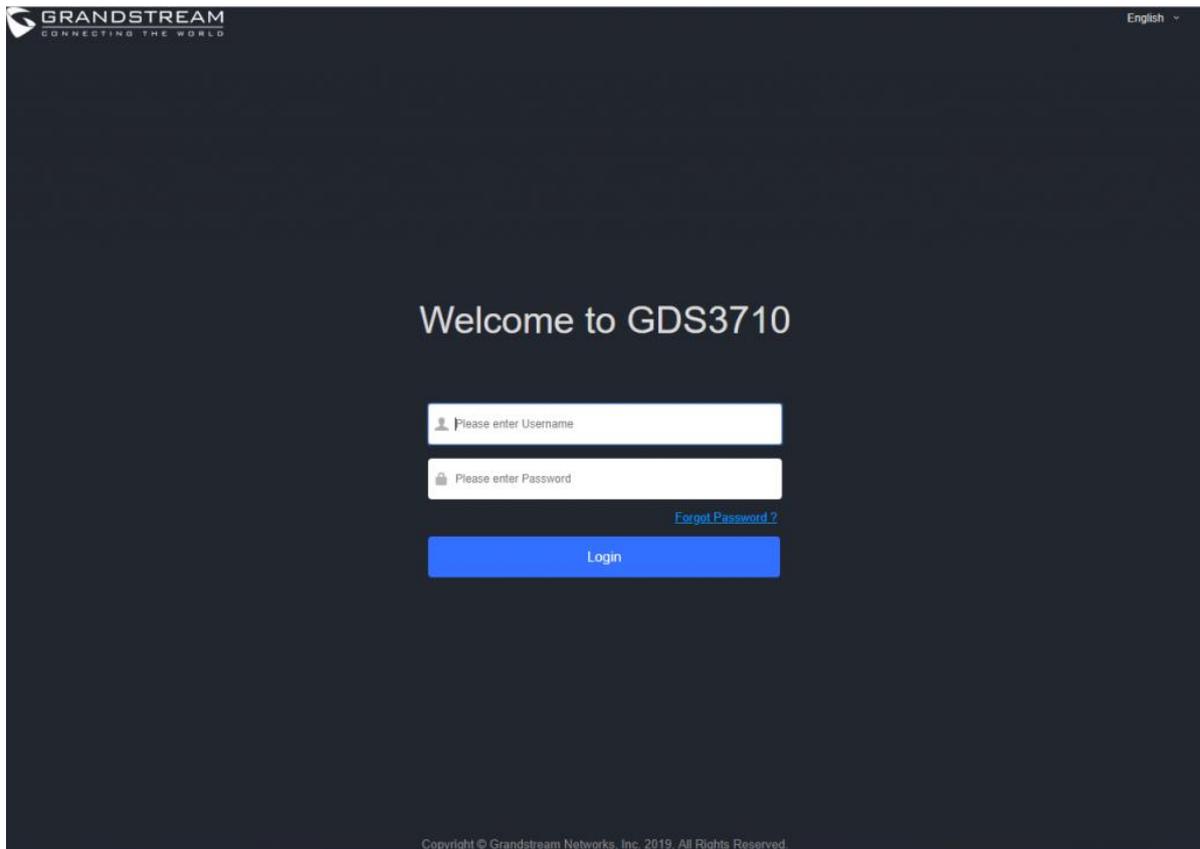


图 10: GDS3710 登录界面

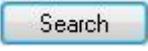
登录后，将显示提示消息，要求插件安装。

- 禁用安全或防病毒软件，下载并安装插件，关闭并再次打开浏览器，若单击“LiveView”，将显示嵌入的视频，然后单击流号码。

GS Search

GS 搜索是一种用于检测和捕获 Grandstream 设备的 IP 地址的程序，以下是使用“GS Search”

实用程序工具的说明：

- 使用连接下载 GS 搜索实用工具：[GS_Search](#)
- 双击下载的文件，将出现搜索窗口。
- 点击  按钮，开始搜索潮流设备。
- 检测到的设备将出现在下面的输出字段中。

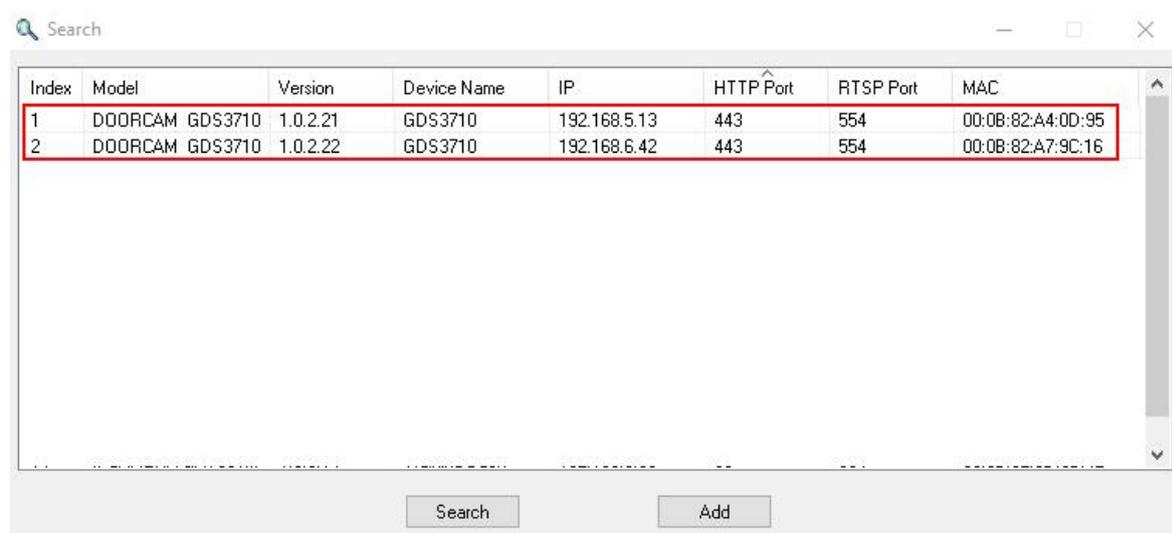


图 11: GS Search Discovery

- 双击对应的设备，直接可以访问它的 web

GDS Manager 管理工具

用户可以知道从 DHCP 服务器日志分配给 GDS371x 的 IP 地址，或者在安装了潮流提供的免费实

用工具后使用 GDS Manager。下面是用户可以找到使用“GDS Manager”实用工具的说明：

- 使用链接下载 GDS Manager 工具: [GDSManager Download](#)
- 安装并运行 GDS Manager, 应该先运行服务器, 然后在运行 GDSMANAGER (客户端)



- 在 GDS Manager 上, 点击  Search 按钮去搜索设备
- 检测到的设备将显示在输出字段中, 如下所示:



<input type="checkbox"/> Index	Model	Version	Device Name	IP	HTTP Port	RTSP Port	Mac
<input type="checkbox"/> 1	GDS3710	1.0.2.21	GDS3710	192.168.5.13	443	554	00:08:82:A4:0D:95
<input type="checkbox"/> 2	GDS3710	1.0.2.22	GDS3710	192.168.6.42	443	554	00:08:82:A7:9C:16

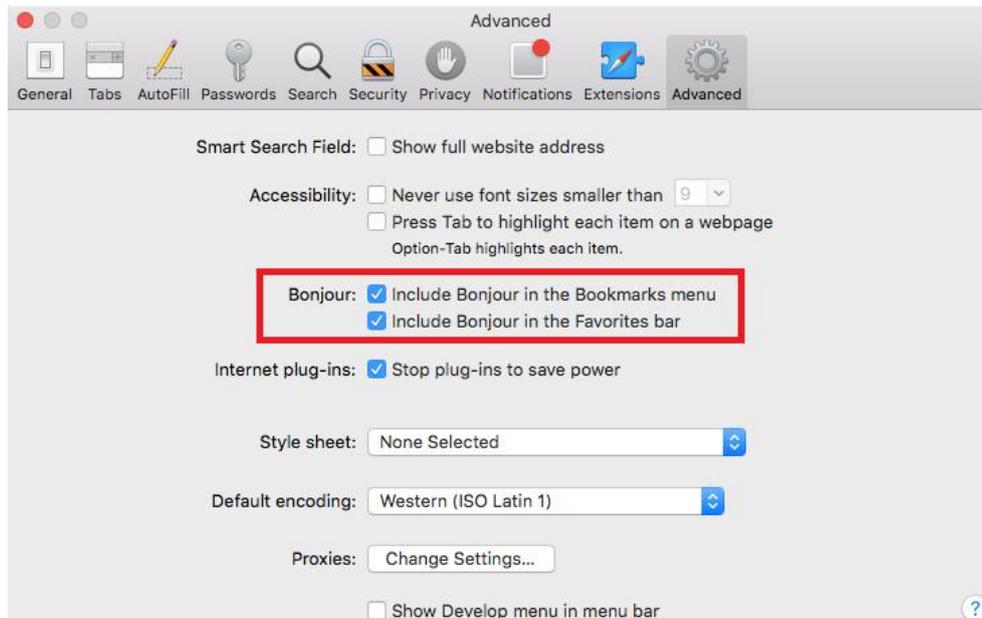
图 12: GDS3710x 搜索

- 双击检测到的 GDS3710, 浏览器将自动打开并显示设备的 Web 配置页面。
- 如果没有安装, 浏览器将询问插件, 请授权安装插件。
- 输入管理员用户名和密码以访问 Web 配置界面, 当前出厂都是随机密码, 每台设备密码都不一样, 设备密码用标签纸贴在设备的后盖上。

Apple 平台

对于苹果用户, 请打开 Safari 的 Bonjour 以查找和访问 GDS371x。

1. 打开 Safari, 选择“高级”打开高级设置。
2. 单击“在书签菜单中包括 Bonjour”和“在收藏夹栏中包含 Bonjour”, 然后关闭设置页面并返回 Safari。



3. Bonjour 现在将嵌入 Safari 中显示。选择“Bonjour”下拉菜单并选择“网页”，相关设备如 GDS371x 将在显示那里。



图 13: Bonjour 设置界面

4. 单击显示出来的 GDS371x，进入 GDS371x 的配置界面。

5. 要查看 MJPEG 视频流，用户应在指定正确的协议（HTTP 或 HTTPS 和正确的端口号）时在浏览器中输入以下 URL：`http (s) : // IP_address_GDS:Port/jpeg/mjpeg.html`

注意:

- 上面提供的说明基于 Safari / OS-X，其他 Apple 平台（如 iOS（iPhone / iPad））可以使用类似的方法。



- 推荐使用 iPhone / iPad (iOS) 用户在 Apple Store 中使用应用程序。
- 推荐和验证来自 Apple Store 的免费或付费应用程序 (如 “IP Cam Viewer”) 配合潮流的 GDS371x 一起使用。
- Apple Store 应用程序, 如 “IP Cam Viewer” 将支持 H.264 视频编解码器。

使用静态 IP 连接 GDS371x

如果网络中没有 DHCP 服务器, 或者 GDS371x 没有从 DHCP 服务器获取到 IP, 用户可以直接将 GDS371x 连接到计算机, 为 GDS371x 配置静态 IP。

1. 如果没有 DHCP 服务器或 DHCP 提供超时 (3 分钟后), 默认静态 IP 为 192.168.1.168

2. 将 GDS371x 使用 RJ45 电缆直接连接到计算机的网络端口。
3. 使用静态 IP: 192.168.1.XXX (1 < XXX < 255, 168 除外) 配置计算机, 并将“子网掩码”配置为“255.255.255.0”。将“默认网关”保留为“空白”, 如下所示:

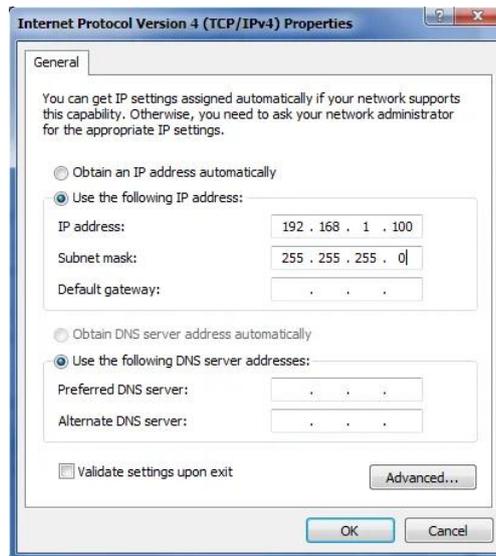


图 14: Windows 静态 IP 地址配置

4. 使用 PoE 进样器或外部直流电源为 GDS371x 上电。
 5. 网络连接完成后启动浏览器。
 6. 在浏览器的地址栏中输入 192.168.1.168, 使用管理员凭据登录设备。默认用户名和密码都设置为 admin。
 7. 浏览器将询问是否安装插件或 ActiveX, 若已安装插件将进入主页并显示 GDS371x 的 Web 界面。
 8. 访问 Web 配置界面。IE 将指示“此网站要安装以下加载项: GSViewerX.cab”, 请允许安装。
 9. Firefox, Chrome 用户需要下载并安装以下插件才能看到视频, 插件可以使用以下链接下载:
- 注意:** 在下载并安装潮流插件时, 请暂时禁用杀毒或安全软件并关闭所有浏览器。

GDS371x 应用场景

GDS371x 门禁系统可以用于不同的场景。

无 SIP 服务器或 Internet 的对等模式

对于像远程仓库/存储，杂货店，小型（外卖）餐馆的环境，只需使用静态 IP 与 PoE 交换机形成

LAN，使用潮流的视频电话 GXV3x50，GXV3x70 将满足您基本的对讲，开门和监控要求。

这是升级版传统模拟对讲和 CCTV 安全系统的解决方案，所有你需要的是一个电源，交换机或 PoE

交换机和潮流 GXV3x50 或 GXV3x70 视频电话。

设备列表可以在下面找到：

GDS371x

GXV33xx or GXV34xx

带有相关 Cat5e / Cat6 接线的 PoE 交换机

使用 SIP 服务器(UCM6XXX)

对于更大的架构，可能需要多个 GDS3710，由于多个连接的存在，对等连接在这种情况下将不工

作。这种情况需要 IPPBX 或 SIP 代理来完成。

如果需要远程访问，必须要添加具有互联网访问功能的路由器如以下列表所示：

- 若干 GDS371x
- UCM6XXX 或其他 SIP 服务器
- GXV33xx 或 GXV34xx 视频话机
- 带有相关 Cat5e / Cat6 接线的 PoE 交换机
- 电锁

如果需要远程访问 GDS371x 以观看实况视频流，则需要访问 Internet，并且需要更多设备，如

- 路由器
- 互联网接入（光纤，3G，4G，电缆或 DSL）
- 带第三方应用程序（如 IP Cam Viewer）的 iPhone 或 Android 手机

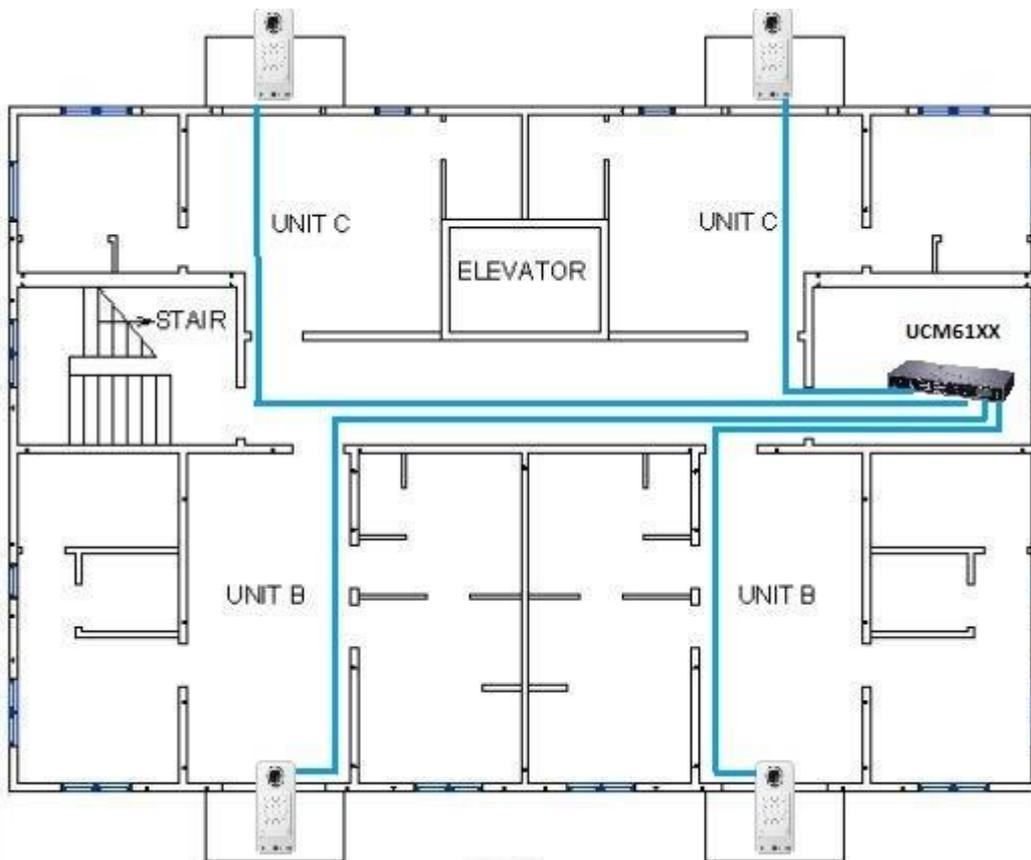


图 15: GDS3710 配合 UCM6XXX 使用

使用网络视频录像机 (NVR)

对于两个以上 GDS371x 的使用，如果需要本地视频录像，则需要添加 NVR，以保存人们进门时所有的视频流。设备列表：

- 若干 GDS371x
- 支持 Onvif Profile S 的 NVR
- 带有相关 Cat5e / Cat6 接线的 PoE 交换机

- 路由器
- 互联网接入（光纤，3G，4G，电缆或 DSL）
- 带第三方应用程序的 iPhone 或 Android 手机

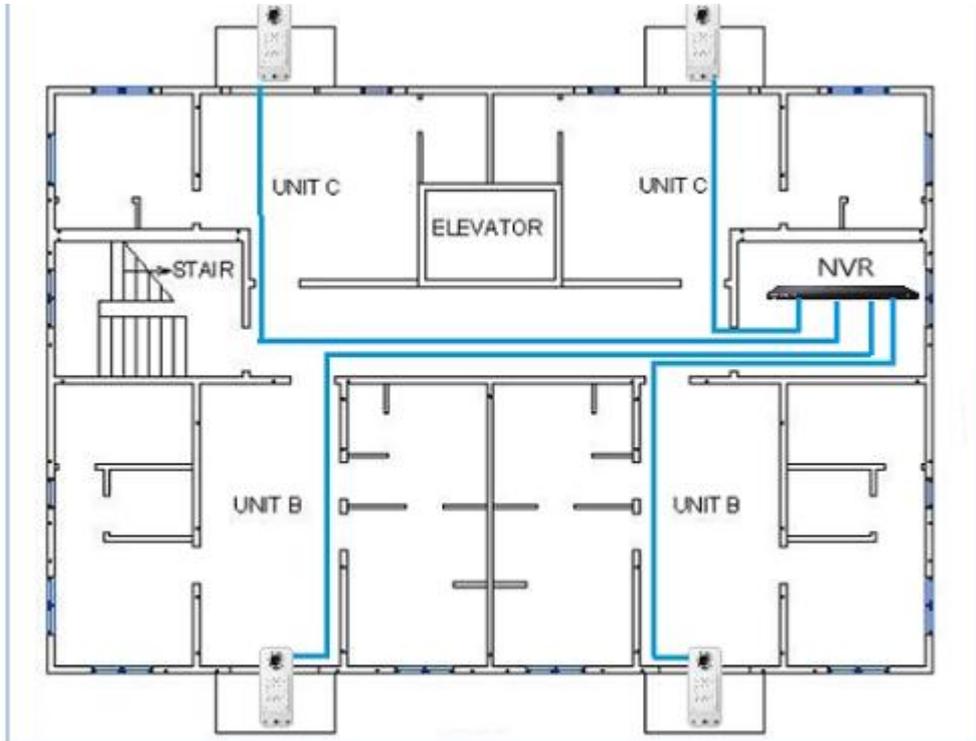


图 16: GDS3710 配合 S NVR 使用

GDS371x 外设连接

下面是相关应用的 GDS371x 外设连接说明。以 GDS3710 为例。



图 17: GDS3710 外设连接

报警输入/输出

报警输入可以选择任何第三方传感器（如 IR 运动传感器）。

报警输出设备可以选择第三方警笛和频闪灯或电动门锁等。

下图是连接报警输入和报警输出的电路图。

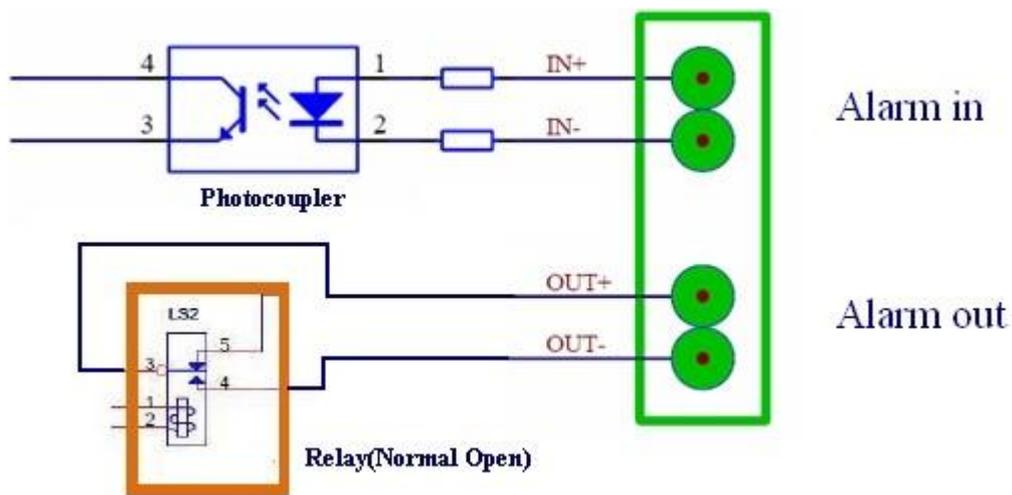


图 18: GDS371x 的报警输入/输出电路图

注意:

- GDS3710 的报警输入/输出电路必须满足以下需求

报警输入	$3V < V_{in} < 15V$, PINs (1.02K Ω)
报警输出	125VAC/0.5A, 30VDC/2A, Normal Open, PINs

- 报警输入电路，如果在上表中指定的 3V 和 15V 之间存在任何电压变化，GDS3710 报警输入端口将检测它并触发动作和事件。
- 禁止高电压和极性错误连接，这会损坏设备。

保护二极管

当将 GDS371x 连接到门极时，建议将 EMF 保护二极管设置为反极性，以确保安全使用，以下是 GDS3710 的保护二极管的部署示例。

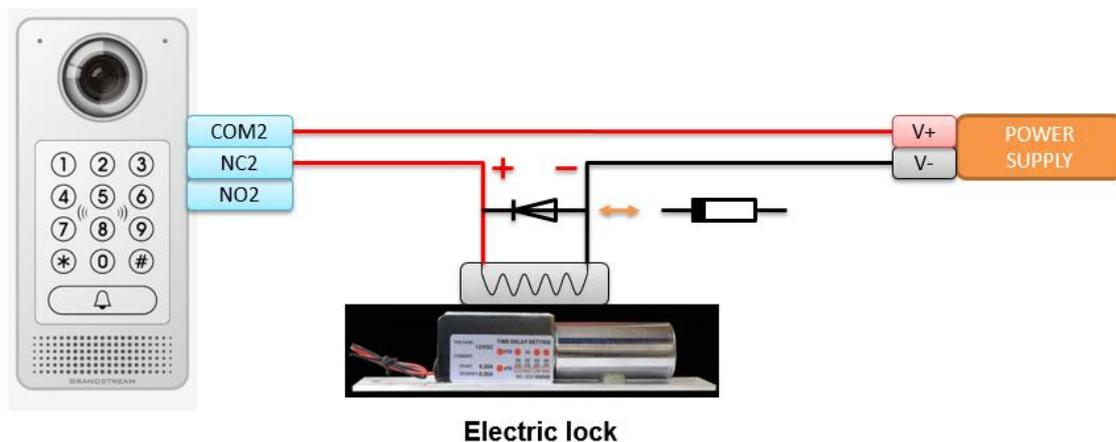


图 19: 实施案例 1

反电动势保护二极管必须始终以反向极性安装在门的敲击之间。

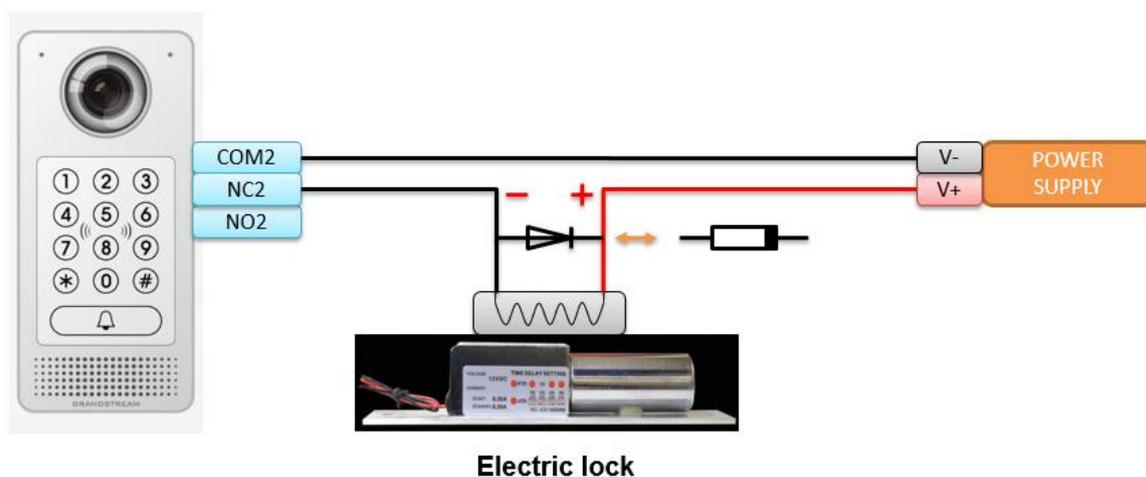


图 20: 实施案例 2

注意:

电力极性连接: 二极管: SS24 or $I_f \geq 2A, V_r \geq 40V$ 。

连接示例

下面的示例显示如何使用 GDS3710 背盖上的接线, 以便与外部设备连接。使用“NO”(常开)型号电锁作为示例, “NC”(常闭)应该类似, 并且用户需要决定在门上使用哪个型号(NO 或 NC)。

使用第三方电源接线示例

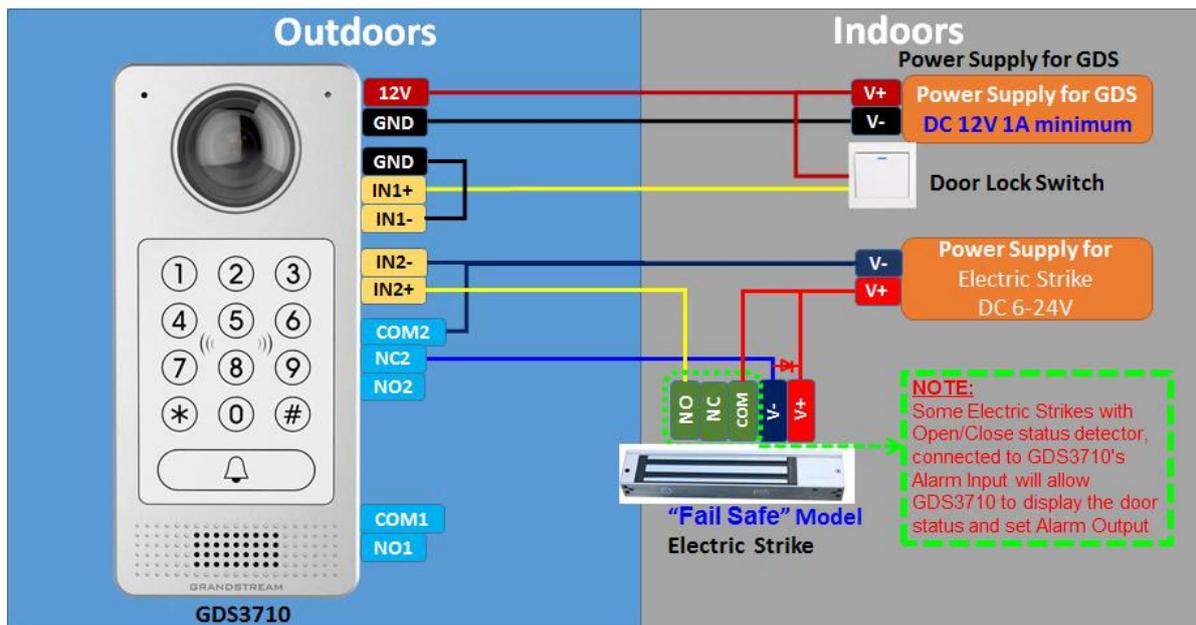


图 21: 使用第三方电源接线示例

使用 GDS3710 和电锁两种电源的接线示例

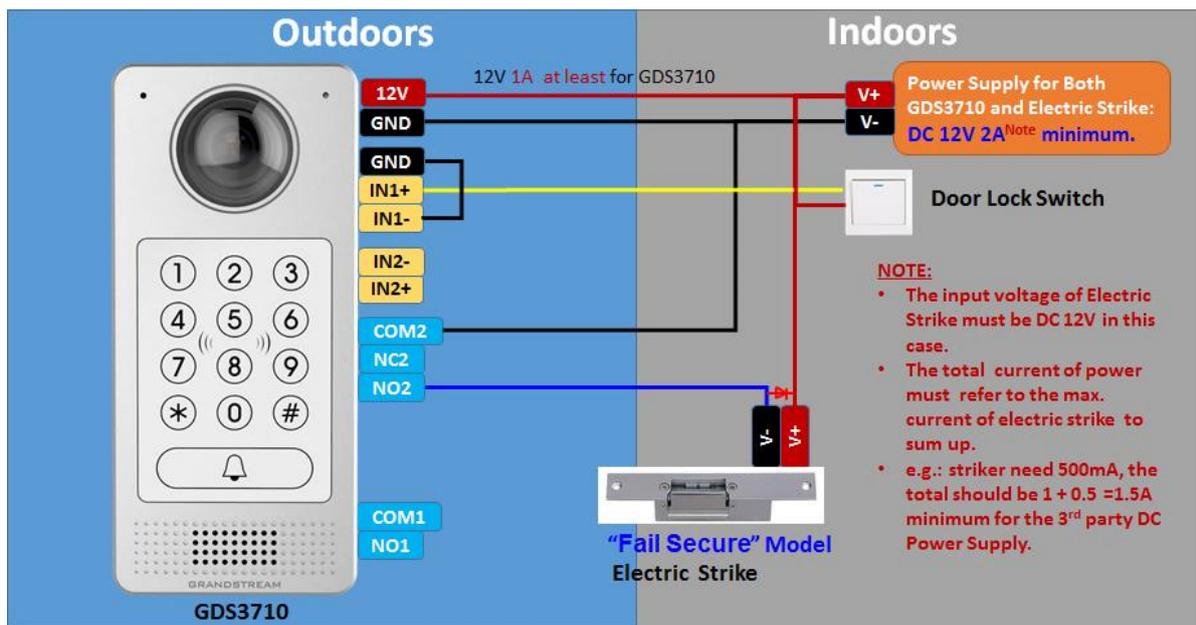


图 22: 使用 GDS3710 和电锁两种电源的接线示例

使用 PoE 为 GDS3710 供电和第三方电源为电锁供电

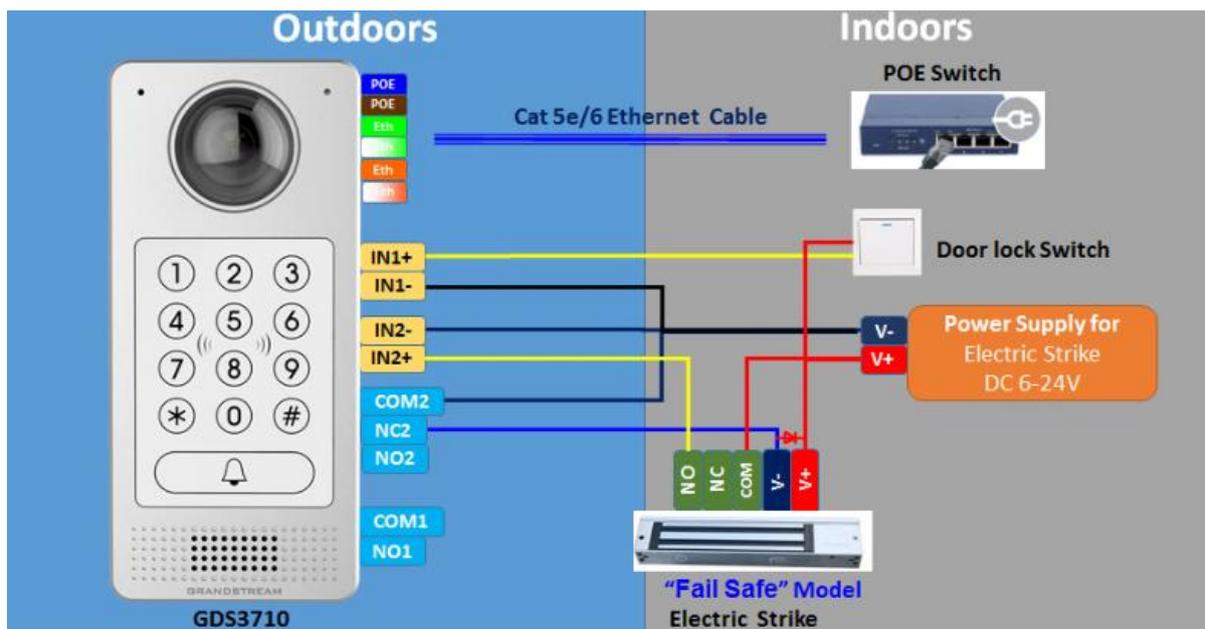


图 23: 使用 PoE 为 GDS3710 供电和第三方电源为电锁供电接线示例

警告:

在为电锁提供电源时应避免以下示例

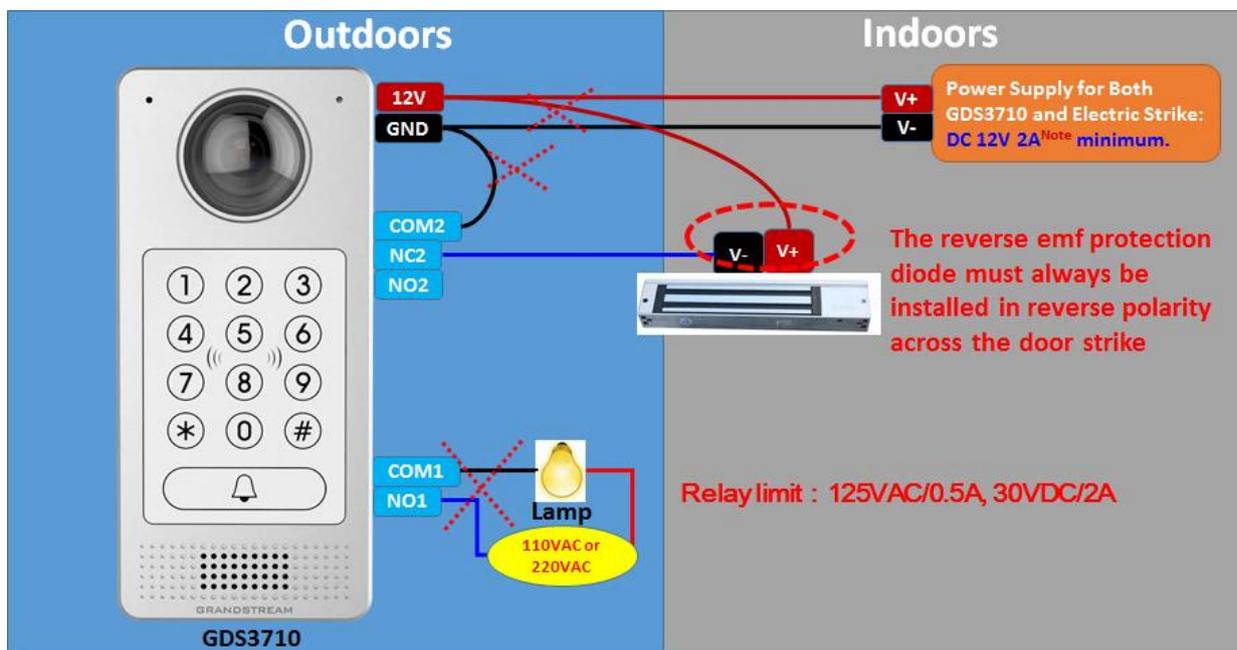


图 24: 需要避免的电锁连接示例

良好的电击和大功率设备接线示例

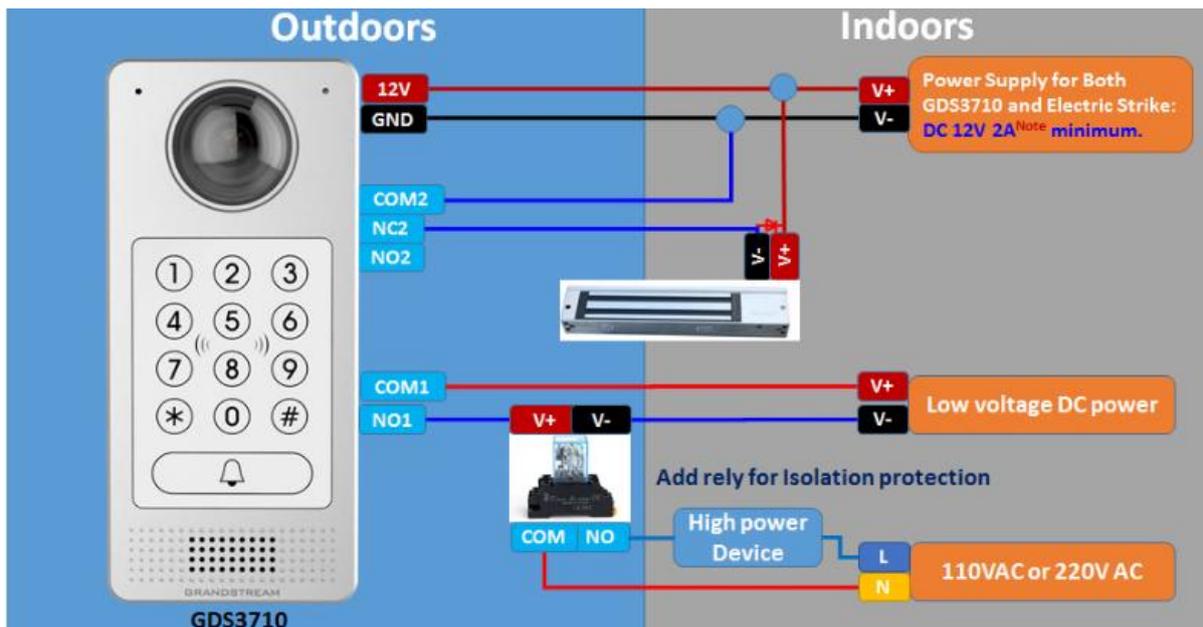


图 25: 良好的电击和大功率设备接线示例

Wiegand 模块接线示例

GDS371X 软件包配备了一条 Wiegand 电缆，用于输入/输出 Wiegand 连接。以下示例显示了如何将 Wiegand 输入/输出设备连接到 GDS371X。

Wiegand 设备的第三方电源输入示例

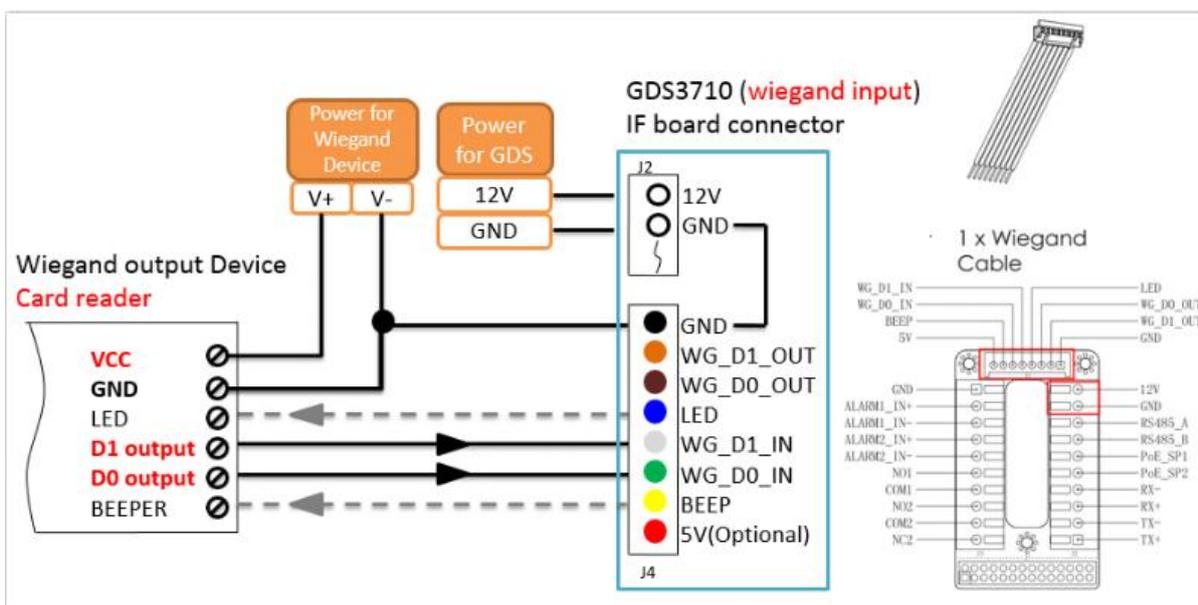


图 26: Wiegand 设备的第三方电源输入示例

确保连接 Wiegand 设备的 GND 和 GDS371X Wiegand 端口。

对于 Wiegand 输入模式，LED 和 Beep 引脚要求 Wiegand 设备支持这些接口。当不连接时，这两个引脚不会影响 Wiegand 总线。

GDS371x 和 Wiegand Device 的电源输入示例

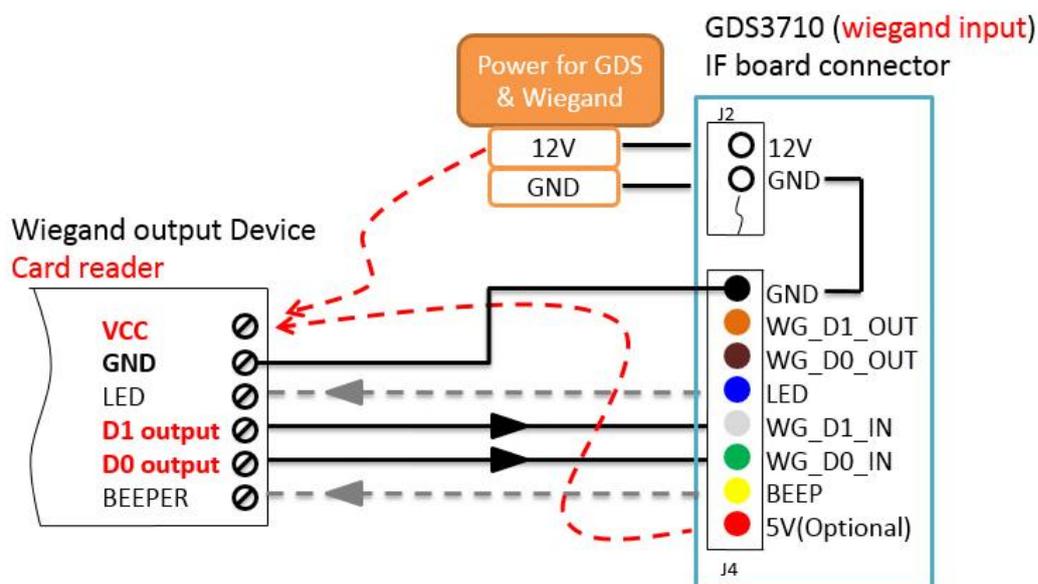


图 27: GDS371x 和 Wiegand Device 的电源输入示例

如果电源为 12VDC，Wiegand 设备可以共享 GDS371x 的相同电源。但是用户需要检查电源的最大功耗和最大容量。

如果 Wiegand 设备使用 5VDC，GDS371X Wiegand 端口可以提供最大 500mA 的 5VDC 来加电 Wiegand 设备。

输出示例，配有 Wiegand 设备的第三方电源

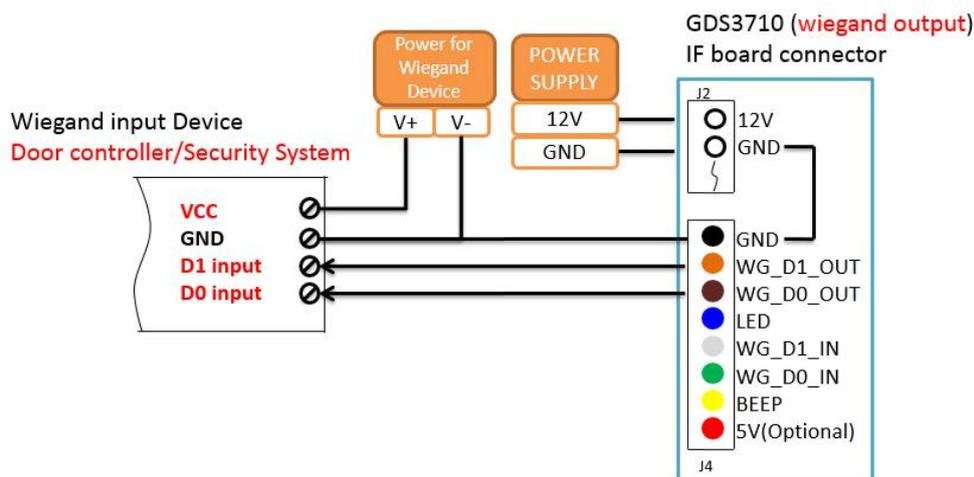


图 28: 输出示例, 配有 Wiegand 设备的第三方电源

当 GDS3710 的 Wiegand 输出连接时, 它作为第三方 Wiegand 设备的信号接收器, 连接到门控制器。主要接线为 GND, D0 和 D1。因为通常是门控制器将消耗大电流和电力, 电源应分开。

Wiegand RFID 读卡器示例

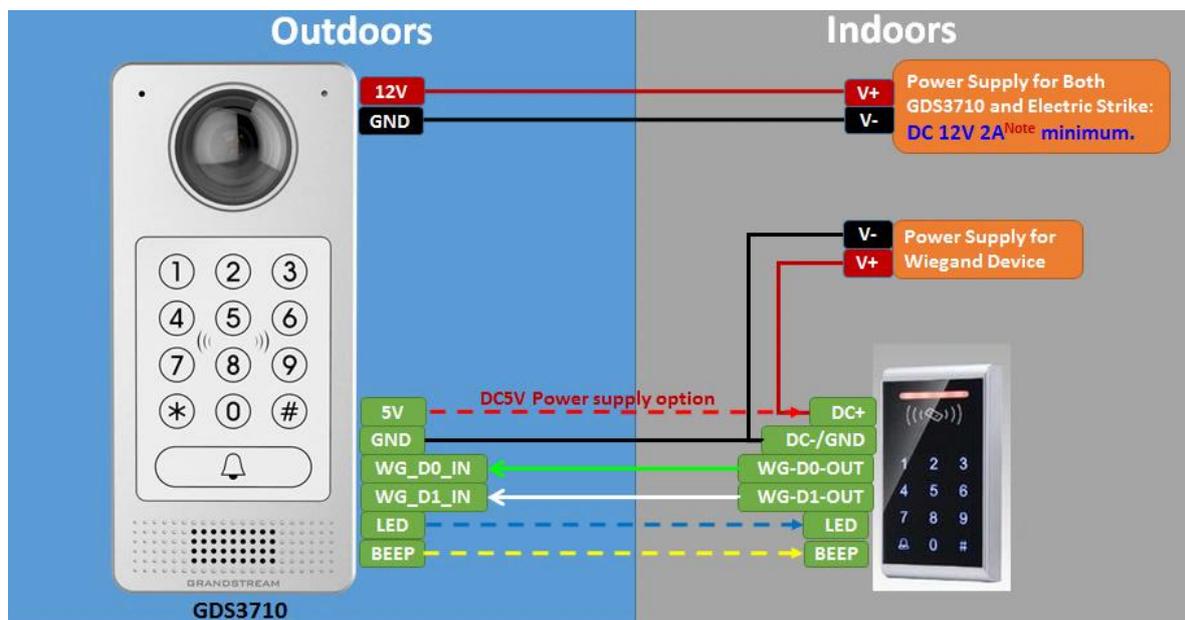


图 29: Wiegand RFID 读卡器示例

当门异常打开时报警

当启用此功能 (需要特殊接线, 请参见下面的接线图) 时, 如果正确连接 (将 COMX 端口连接到 DIX 端口), 则 DI 端口 (alarm_in2 或 in 2 中显示) 将检测到异常的开门。一旦触发了异常的敞开

的门警报，警笛声将不停地听起来，直到被相关人员手动覆盖。

有几种停止和禁用警报的方法：

- 1) GDS37xx 上电
- 2) 接听警报电话（如果配置）
- 3) 使用 PIN（公共 PIN 或私人 PIN，仅适用于 GDS3710 型号的选项）打开门）

触发警报后，当异常的开门死机发生时，GDS371X 将拍摄快照，使用电子邮件并将快照上传到 FTP 或 Central Server（配置后）；调用配置的警报 SIP 电话，发送警报输出（如果连接）。用户只能使用上述 3 种方法禁用警报器。

详细的操作信息请参阅 GDS37XX 用户手册，“警报操作设置”配置。

以下的一些图表是启用此功能的正确接线：

GDS371X 连接：IN2 设置为常闭和使用第三方电锁的“失败安全”情景

数字输入

数字输入 1	电锁控制异常	▼
数字输入1状态	常闭	▼ 检测到当前状态为 打开
选择日程 1	全天	▼ 编辑日程表
选择报警联动方案 1	profile1	▼ 编辑方案

图 30：数字输入设置为常闭

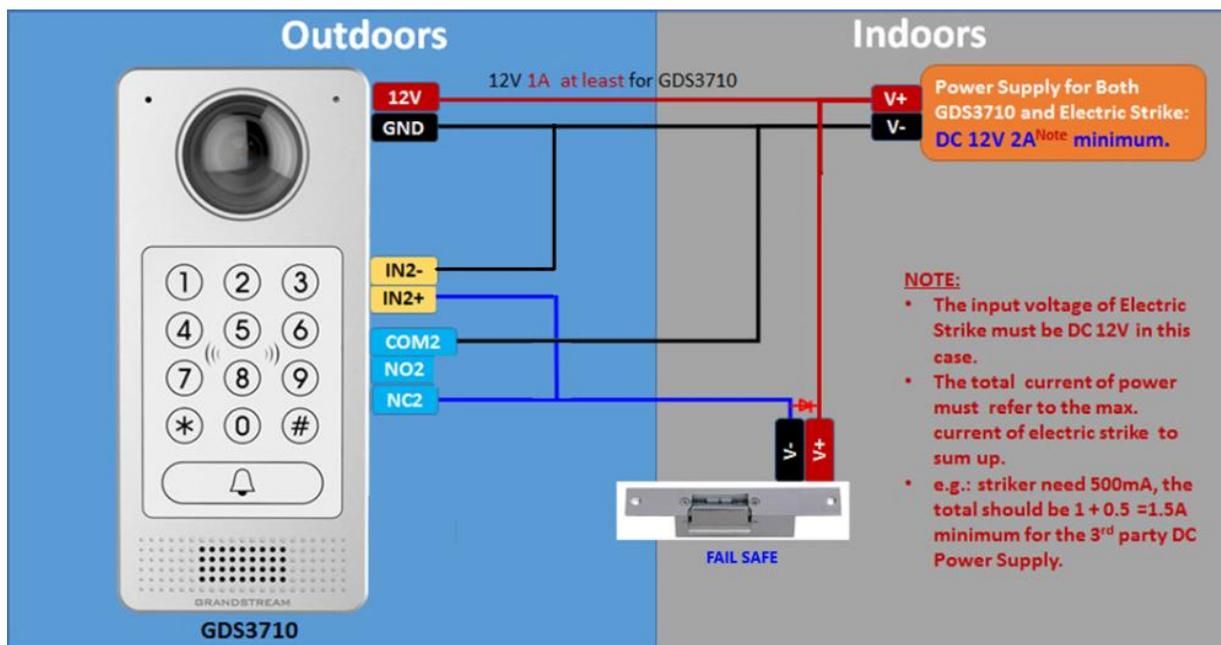


图 31: IN2 设置为常闭和使用第三方电锁的“失败安全”

GDS371X 连接: IN2 设置为常开和使用第三方电锁的“安全失败”情景

Digit Input

Digit Input 1 Abnormal Door Control ▼

Digit Input 1 Abnormal Door Control Options Door 1 Door 2

Digit Input 1 Status Normal Open ▼

图 32: 数字输入设置为常开

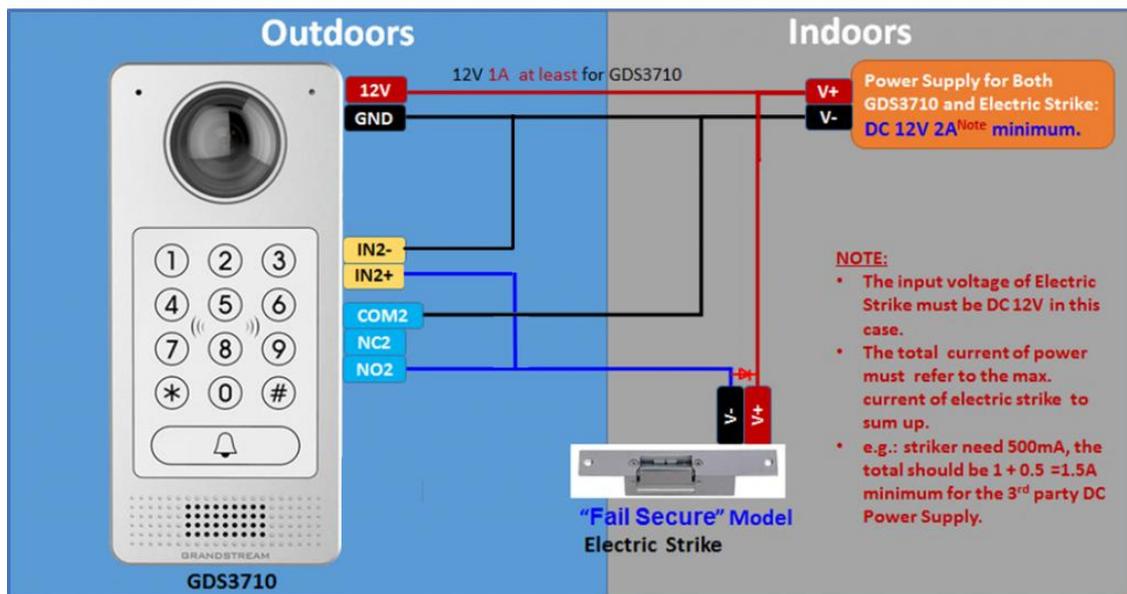


图 33: IN2 设置为正常开放和使用第三方电锁的“安全失败”情景

GDS371X 连接：IN2 设置为常开和使用带有门传感器的第三方电锁的“安全失败”场景

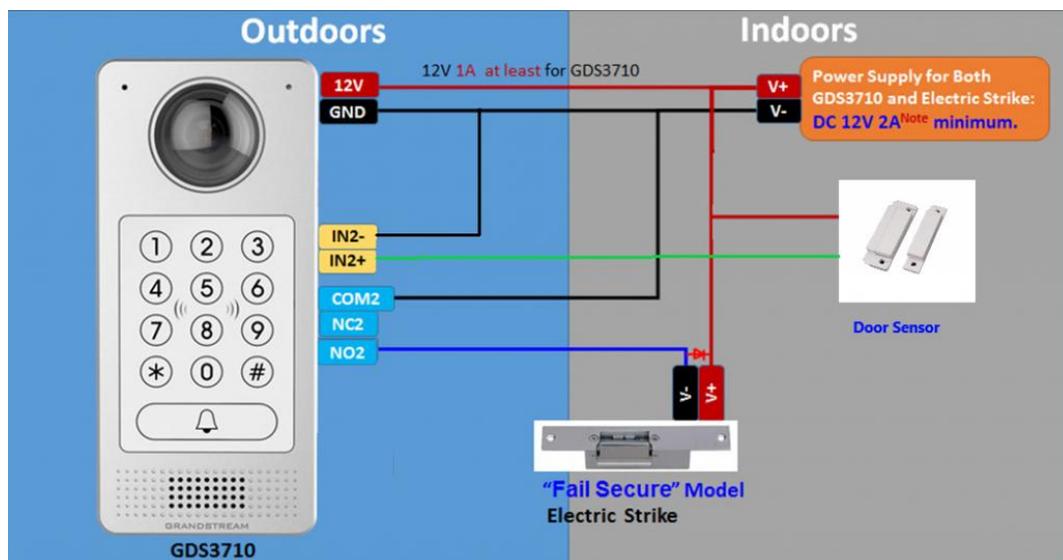


图 34：IN2 设置为常开和使用带有门传感器的第三方电锁的“安全失败”场景

与 GSC3570 对接安全开门

这个功能是 GDS37XX 的新增功能，需要搭配 GSC3570 一起来组成整体解决方案。GDS37XX/和 C3570 在 LAN/WAN 中将通过 IP/SIP 对接，门锁/开关连接到 GSC3570 Alarm_out 端口，并由 GSC3570 控制。这样，控制开关在室内，更具有较强的安全性。以下是一个设置示例：

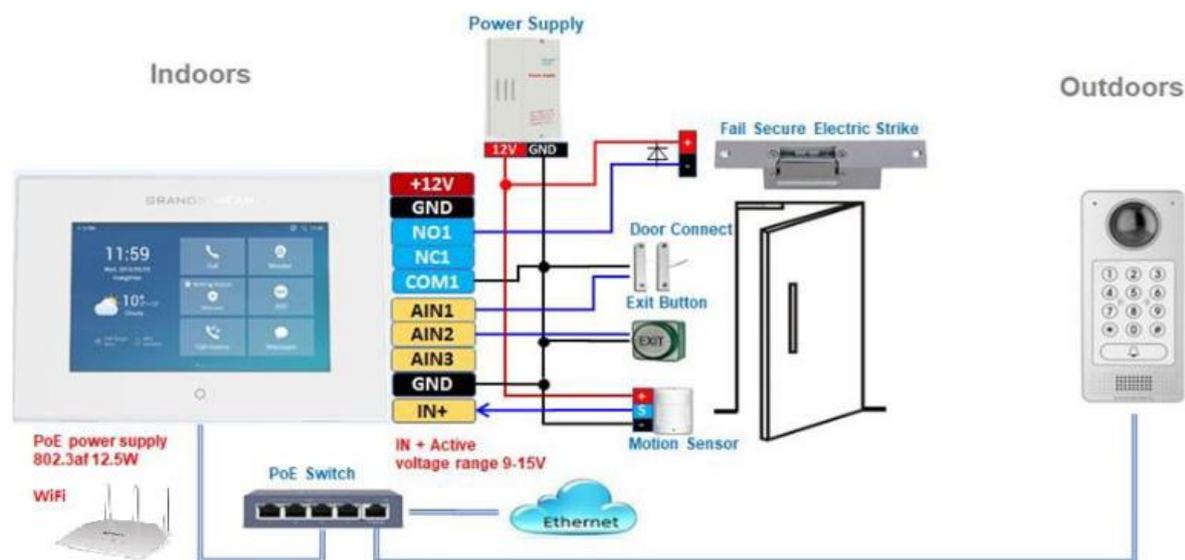


图 35：GSC3570 通过 GDS3710 开门

注意:

最低要求固件版本:

- 室外设备: GDS371X (FW1.0.11.23) 和 GDS370X (FW1.0.3.11)
- 室内设备: GSC3570 (FW1.0.5.2)

GDS37XX 可以通过 POE 供电, GSC3570 可以通过 POE 或 WiFi 连接到同一网络。对于与 GSC3570 和 GDS37XX 的开门组合, 如果 GSC3570 需要控制多个 GDS37XX, 则必须使用 SIP, 并且相关的 GDS37XX 将控制电锁。不同的 GDS37XX 门铃呼叫将在“预览”(早期媒体支持) 中或建立呼叫时显示“一个按钮打开门”。

对于“安全开门”, GSC3570 与 GDS37XX peer 对接, GSC3570 在室内控制继电器

//strike/锁

(与外部安装的 GDS37XX 不同), 但是只能控制一扇门, 因为 GSC3570 只有一个继电器控制电路通道。

这种对接可以通过 LAN/WAN, 但建议使用 LAN, 实际上大多数应用程序场景都在 LAN 环境中, 因为 GSC3570 和 GDS37XX 很可能在同一建筑物中。尽管 Internet/WAN 上的 SIP/UCM 也可以工作, 但如果 GSC3570 (内部) 和 GDS37XX (外部) 在同一 LAN 中, 还是建议使用静态 IP。

此设置非常简单且可靠, 以防出现网络中断, 如 Internet/UCM 宕机。

对于 GSC3570 和 GDS37xx peer 对 jiSIP(云或 UCM)使用;只有 IP(没有 SIP 代理或 UCM),

只有静态 IP 地址)和混合(SIP 和代理失败时回退到 IP)。

GDS3710 Web 配置

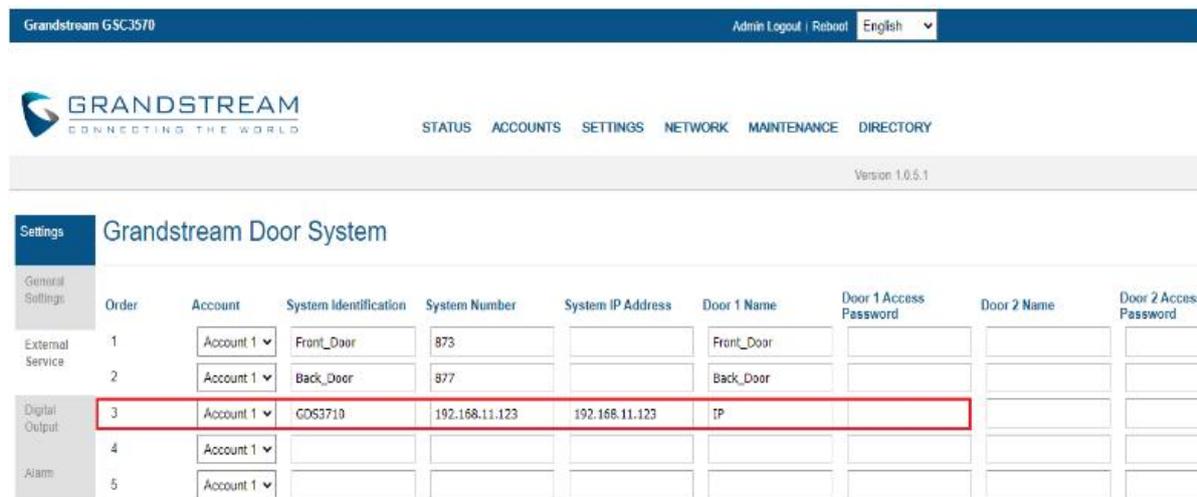
由路径: web UI→门禁设置 →基础设置, 可以找到如下界面:



图 36:GSC3570 安全开门通过 GDS3710-GDS3710 配置

GSC3570 Web 配置

GSC3570 也需要进行配置, 请参考如下图:



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							

图 37:GSC3570 通过 GDS3710-GSC3570 门系统配置安全开门

然后, 我们在 GSC3570 上配置数字输入, 如下图:



图 38:GSC3570 通过 GDS3710-GSC3570 数字输入配置安全开门

注意:

- 如果解决方案/集成使用没有 SIP 代理的静态 IP 地址方式，则所有涉及的设备（GDS/GSC/IP 电话）都应“NAT Traversal”设置为“否”，并且不应“使用随机端口”，否则会有问题。
- IP 电话或 GSC3570 可以使用任何空的 SIP 帐户，这意味着如果帐户 1 注册到 UCM/代理和 Account2（空白）以使用 IP（但必须将帐户配置为“活动”）。

单向互锁模式

注意:

此配置是 GDS3710 型号独有的。

此功能将允许 GDS3710 在一个方向上控制两个门，并相应地安装了附加的第三方窗口/门传感器（Grandstream 不提供）。配置步骤，如下所示：

- 1) 当检测到两个门关闭时，只有合法的 PIN 或 RFID 卡才能打开门。（仅适用于 GDS3710 型号）。
- 2) 当用户打开第一扇门时，第二扇门将保持关闭；一旦检测到第一扇门关闭并到达编程计时器后，

第二扇门将自动打开。

3) 当第二扇门打开时，即使使用有效的 PIN/RFID，第一扇门也不会打开。（仅适用于 GDS3710 型号）

4) 如果进入第一扇门并且在第一扇门关闭并打开第二扇门后，该人未能及时进入第二扇门（第二扇门打开时间超时）将锁定在两扇门之间，直到有其他人进入或向安全人员寻求帮助（例如：呼叫发布号码等）才能打开门（例如，通过 SIP 调用 GDS3710 或 GDSMANAGER）。

此开门的逻辑是确保朝着“单向”方向打开两扇门，在任何给定时间只能打开一扇门，并且只允许一个合法的开门请求执行。

可以通过安装 Grandstream IP 摄像机来监视两个门之间的走廊或场景。

此功能可以在应用程序场景中使用：大学宿舍，银行分支机构，政府办公室，医疗诊所，私人俱乐部等有两扇门且需要高安全性和流量控制（每次仅一个条目），但保安人员可能不在现场的场景。以下是该场景场景的接线示例：

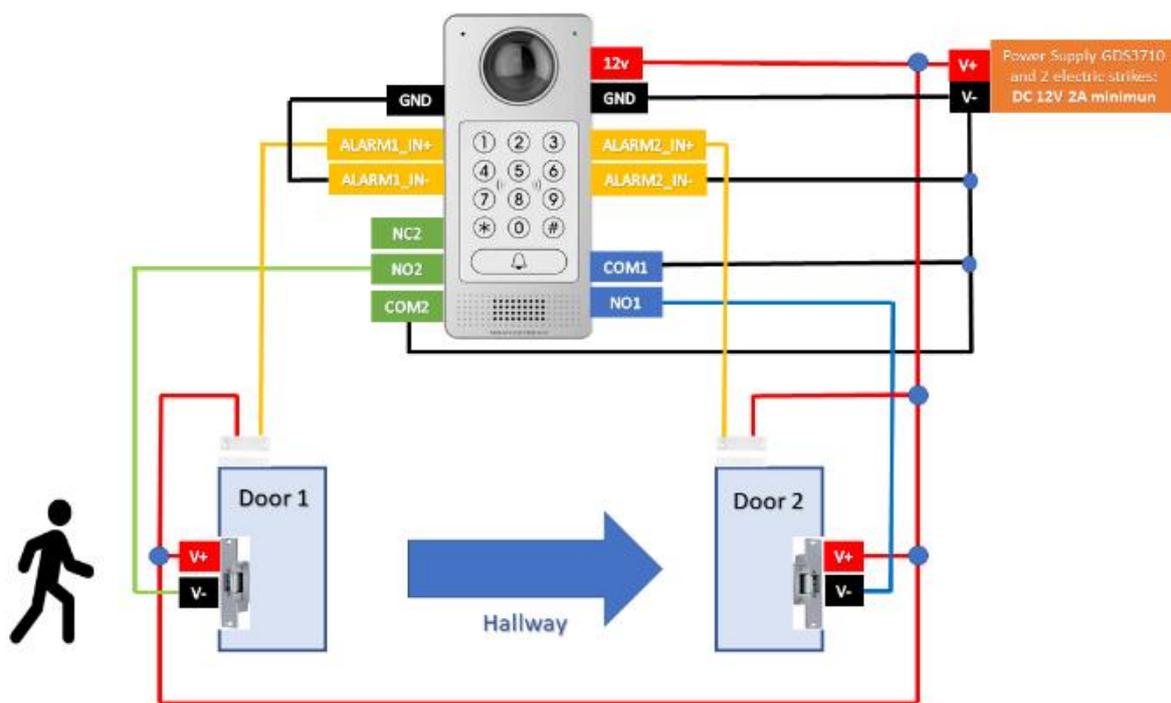


图 39:单向连锁模式

注意:

如果需要使用相同的两个门来进行“离开”方向，则需要另一个 GDS3710，并且可以在门 2 中配置以控制“离开”方向。接线/连接将使用镜像。

Web 配置

可以在设备 Web UI→门禁系统设置下找到此选项。以下示例配置屏幕截图仅供参考。

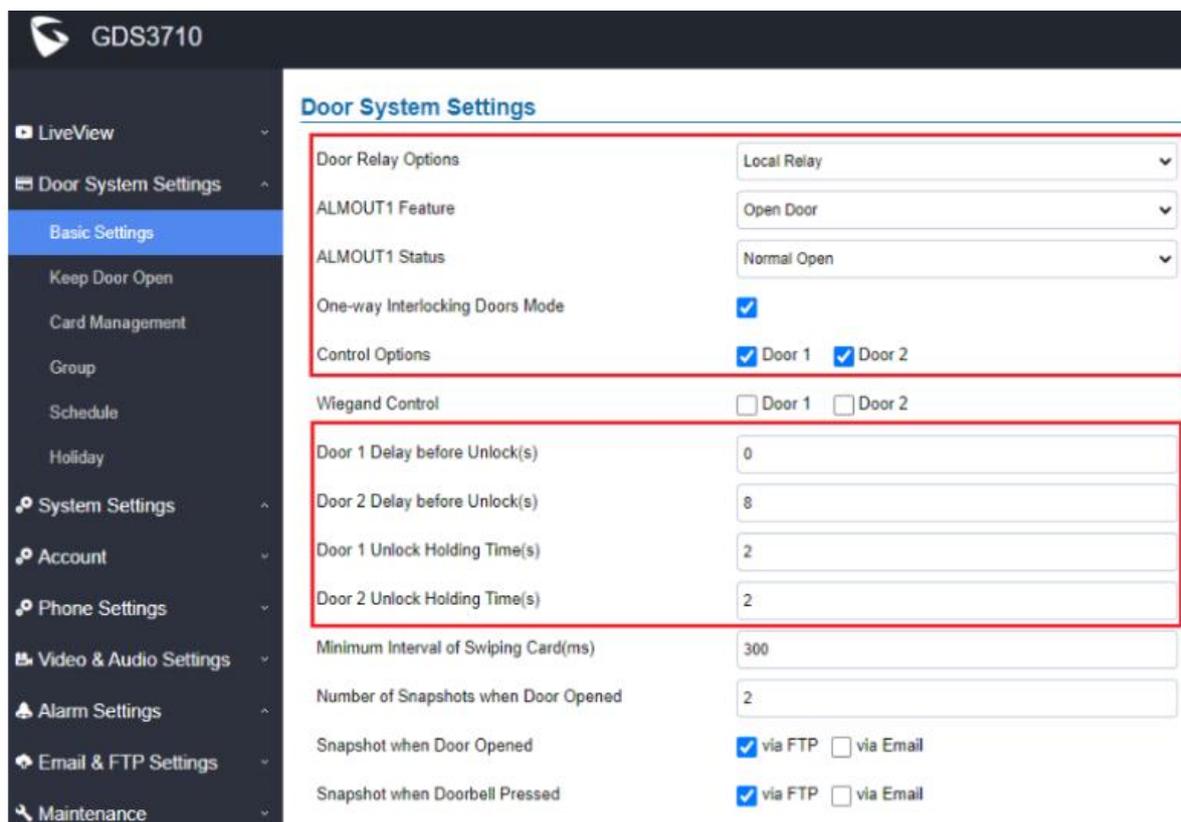


图 40: 单向连锁模式_GDS3710_CONFIGURATION_1

注意:

- 门 2 延迟解锁前: 是门 1 关闭后从门 1 到门 2 的总运输时间 (这段时间是“门 1 解锁固定时间”)。
- 在上面的示例中, 门 1 解锁固定时间为 2 秒, 走廊的运输时间为 6 秒, 因此, 在解锁设置为 8 秒之前, 门 2 延迟。
- 安装程序或系统集成器将在实际的应用程序场景上确定和调整 d 的运输时间和解锁时间。
- com1 (almout1) 只有两个用于接线的插座。如果连接的 strike/lock 是打开的, 这意味着应将 Almout1 状态设置为“正常打开”, 那么当没接电源时, 门将关闭。

数字输入以检查门状态（门1和门2）

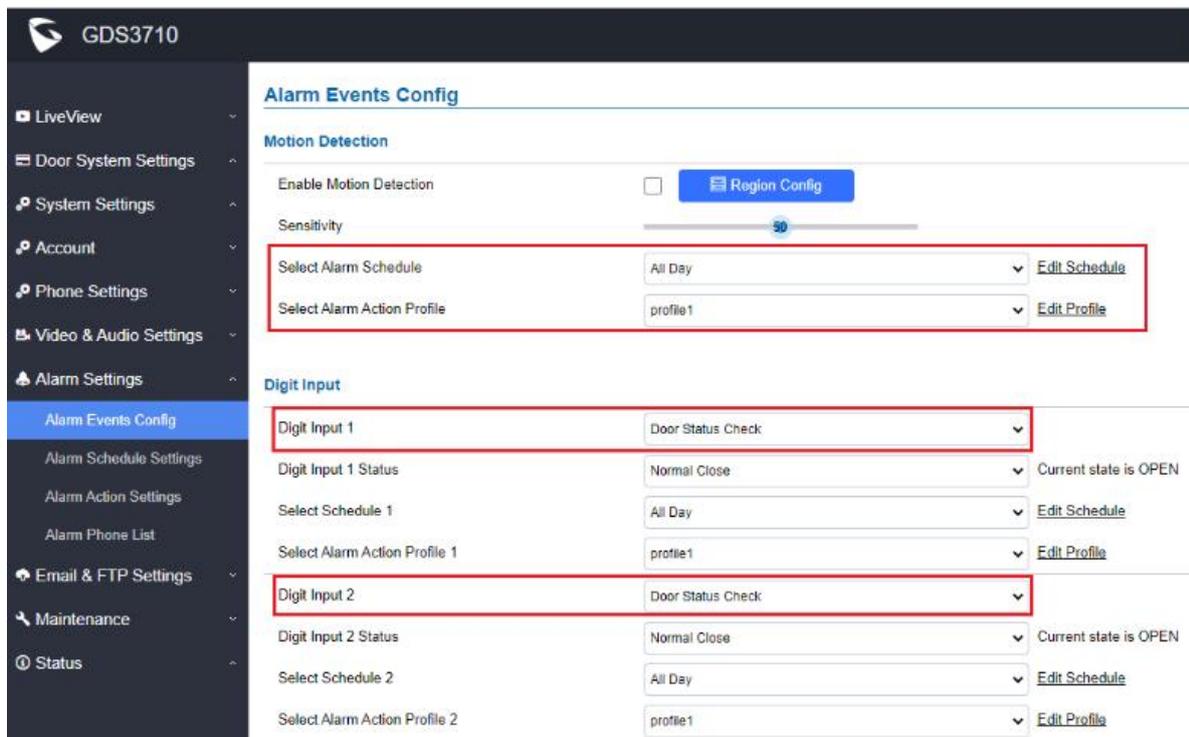


图 41: 单向连锁模式_GDS3710_CONFIGURATION_2

继续进行警报设置→警报事件配置→数字输入，配置如下：

- 数字输入 1：门状态检查。DI 将在传感器信号上验证门的当前状态，无论是关闭还是打开，d 都发送到“数字输入 1”。
- 数字输入 1 状态：如果设置为常开：当数字输入状态从关切到开时，将触发门的状态检查；如果设置为常闭：当数字输入状态从开切到关时，将触发配置的门状态检查。默认情况下，输入数字 1 状态“禁用”。
- 数字输入 2：门状态检查。DI 将在传感器信号上验证门的当前状态，无论是关闭还是打开，d

都发送到“数字输入 2”。

- 数字输入 2 状态：如果设置为常开：当数字输入状态从关切到开时，将触发门的状态检查；如果设置为常闭：当数字输入状态从开切到关时，将触发门的状态检查。默认情况下，输入数字 2 状态是“禁用的”。

注意：

- 必须配置“警报时间表”和“警报操作模板”，否则数字输入通道将不会被激活。
- 有两扇门分别装有门窗传感器，，请确保门传感器连接到正确的数字输入通道，可请参阅单向连锁模式的图示。

通过 GDS37XX 带或不带 SIP 通话的开门

此功能需要固定的 GDS37XX 固件来实现。最低固件版本：

- GDS3710: 1.0.7.19 或 跟高
- GDS3705: 1.0.1.13 或 更高

从 GDS37XX 方面来看，配置是相同的。唯一不同的是被控制的门的数量:如果使用 GDS37XX 控制的本地继电器，可以控制两个门。

如果使用 GSC3570 继电器，只能控制一个门。PIN 和其他设置与 GDS3710 的 SIP 远程开门或 GSC3570 安全开门相同。

区别主要体现在 GSC3570 的触摸屏 UI 操作上。

Door System Settings

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

Door Relay Options Local Relay ▼

ALMOUT1 Feature Local Relay ▼

ALMOUT1 Status Normal Open ▼

Control Options Door 1 Door 2

Wiegand Control Door 1 Door 2

Door 1 Delay before Unlock(s)

Door 2 Delay before Unlock(s)

Door 1 Unlock Holding Time(s)

Door 2 Unlock Holding Time(s)

Minimum Interval of Swiping Card(ms)

Call Mode SIP Number ▼

Doorbell Mode Call Doorbell Number ▼

Doorbell Call Out Account Auto ▼

Door Bell Call Mode Serial Hunting ▼

Number Called When Door Bell Pressed

Remote PIN to Open Door 1

Remote PIN to Open Door 2

图 42: GDS37XX 配置示例

Grandstream Door System										
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	
1	GDS	Account 1	Front_Door	873		Front_Door				
2	GDS	Account 1	Back_Door	877		Back_Door				
3	GDS	Account 1	GDS3710	192.168.11.125	192.168.11.125	IP				
4	GDS	Account 1	GDS3710	8606		SIP				
5	GDS	Account 1	GDS3705	192.168.11.116	192.168.11.116	IP1		IP2	***	
6	GDS	Account 1								

图 43: GSC3570 配置示例

使用 SIP 通话开门:

当 GSC3570 与 GDS37XX 建立通话后, 屏幕显示虚拟开门按钮, 用户按下按钮开门:

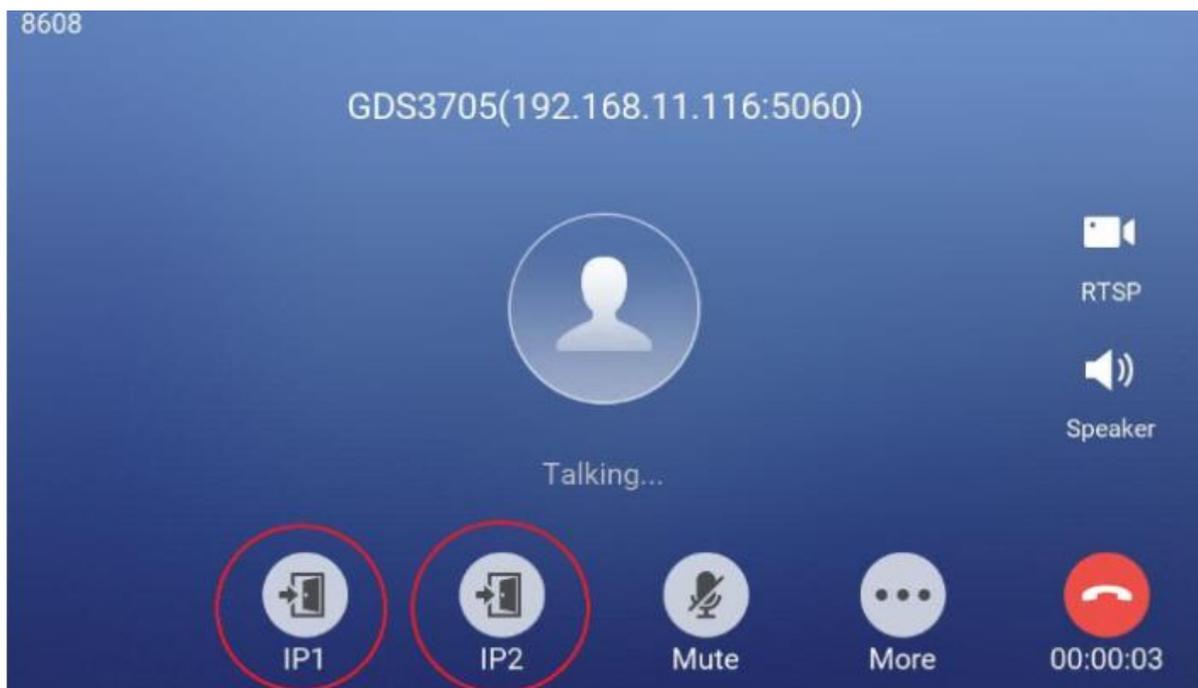


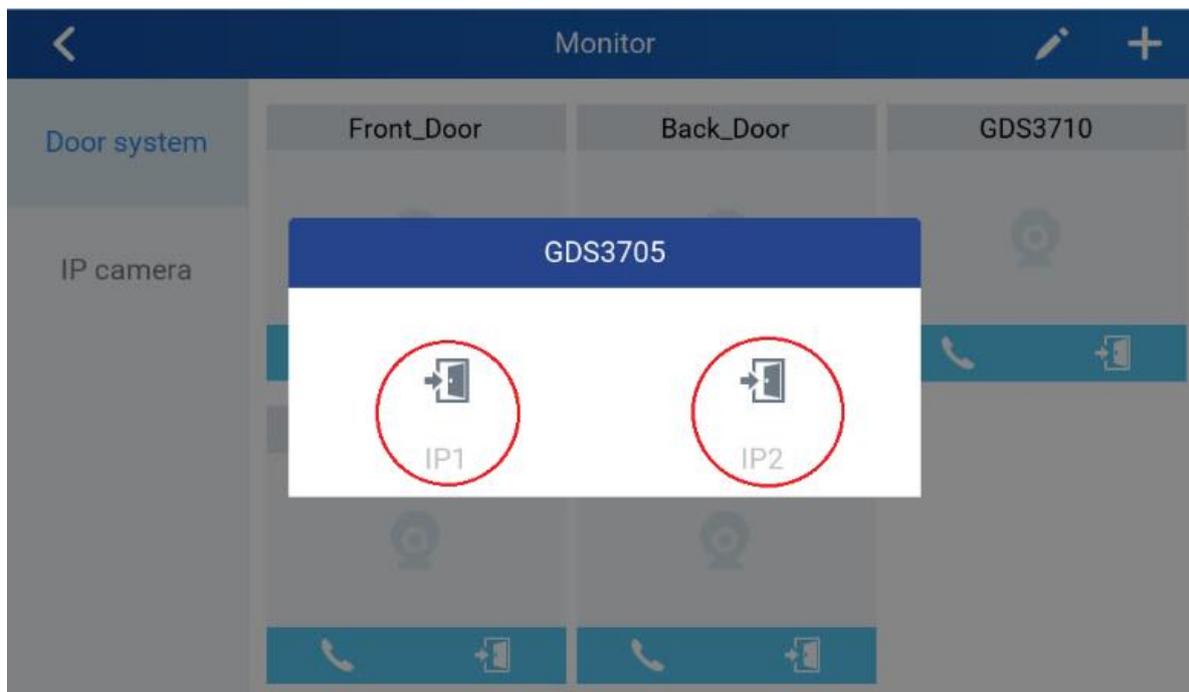
图 44: 使用 SIP 通话开门

不使用 SIP 通话开门:

在 GSC3570 空闲屏, 按“监控→门禁系统”, 会显示相应的 GDS37XX。在蓝色栏中, 左边是“电话”图标, 右边是“开门”图标。“电话”图标将建立 SIP 呼叫。

按“开门”图标, GSC3570 将直接开门, 并且没有 SIP 通话。根据控制的门数, 如果配置了一扇门, 门将直接打开;如果设置了两扇门, 则会弹出另一个屏幕, 让用户选择打开哪一扇门, 如下图所示:





当门被成功打开时，将出现以下消息：



图 45：不使用 sip 通话开门

GDS371x WEB 主页

一旦成功登录到 GDS3710，用户将看到以下页面。

注意：显示的选项可能因浏览器而异，也可能因 GDS 型号而异(GDS3710/GDS3712)

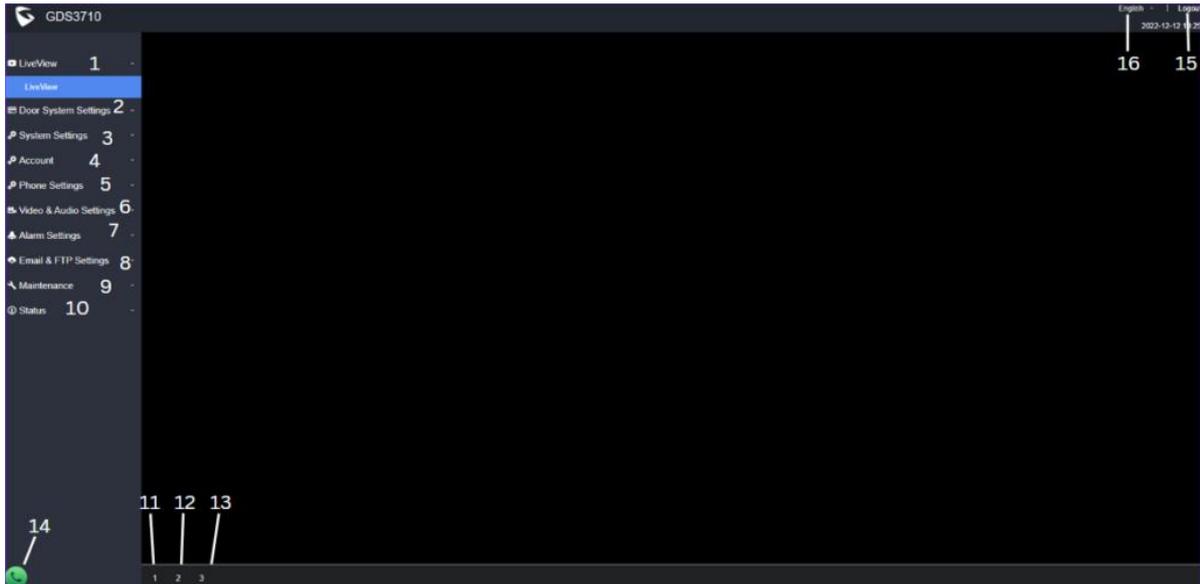


图 46: 主界面

序号	选项	描述
1	实时预览	访问进入实时预览界面
2	门禁设置	访问进入门禁设置界面.
3	系统设置	访问进入系统设置界面
4	账号	访问进入账号配置界面
5	电话设置	访问进入电话设置界面
6	音视频设置	访问进入音视频配置界面
7	报警配置	访问进入报警配置界面
8	邮箱 & FTP 设置	访问进入邮箱&FTP 界面
9	维护	访问进入维护页面
10	状态	点击, 进入状态界面
11	视频流 1	播放码流 1.
12	视频流 2	播放码流 2
13	视频流 3	播放码流 3
14	呼叫接口	允许从 web 界面呼叫接口, 拨打呼出
15	登出	登出 web 页面
16	语言	选择 web 显示的语言

表 5: 主界面描述

GDS371x 配置 & 语言页面

- 在浏览器上输入 GDS371x 的 IP 地址后，将弹出登录网页，允许用户配置 GDS371x 的相关参数。
- 单击“语言”下拉菜单时，将显示支持的语言，如下图所示。单击选择需要显示的语言。

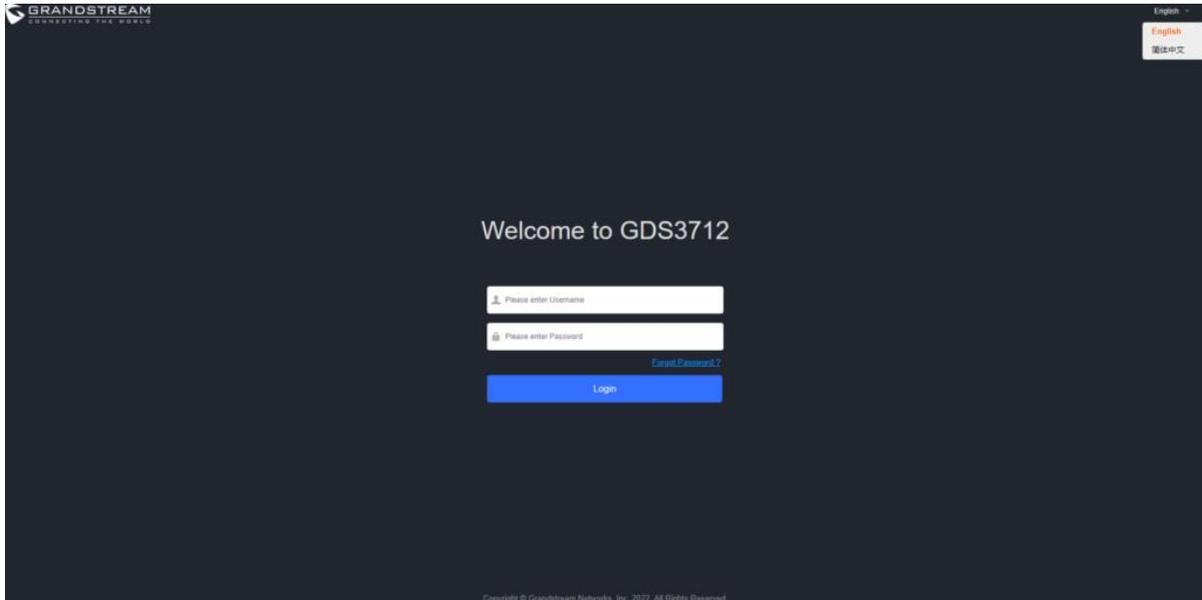


图 47: GDS3712 登录界面

注意:

目前固件，仅支持英文和简体中文

GDS371x 设置

实时预览

此页面允许用户在安装运行相关插件后从浏览器查看 GDS371x 的实时视频。

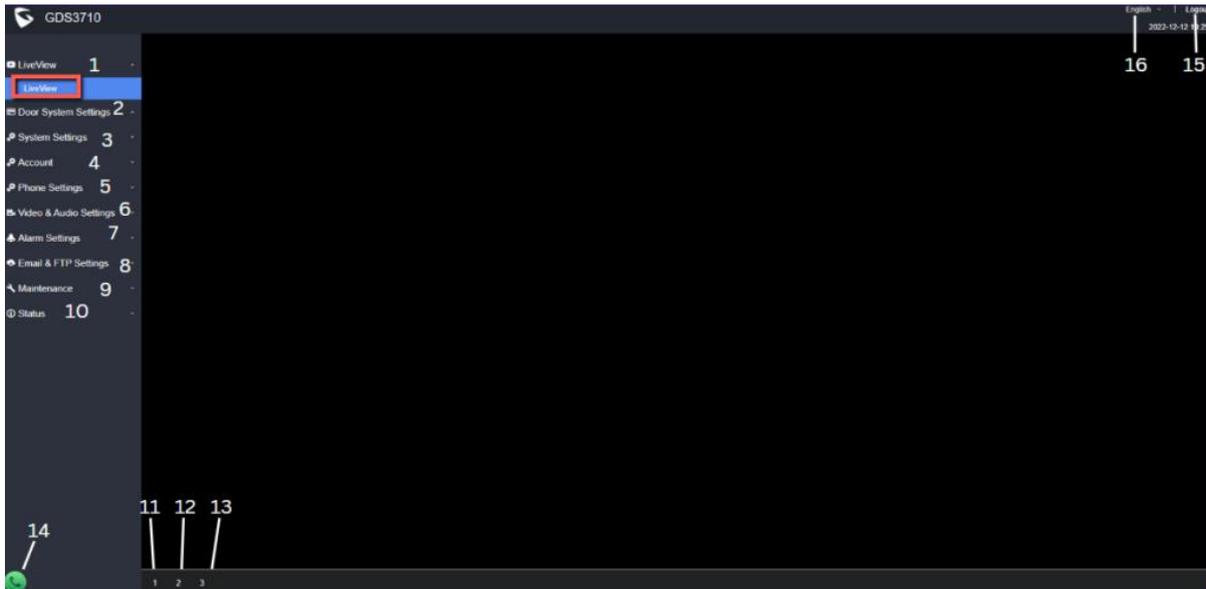


图 48: 实时预览: 谷歌浏览器

3 路视频流可选:

- 主视频流: 1920 * 1080 分辨率, 建议连续全高清录制。
- 辅助视频流: 640 * 480 分辨率 (GDS3712 是 1280 x 720 分辨率), 推荐用于 SIP / VoIP 视频通话 (如果与 GXV3470 / GXV3480 一起使用)。
- 第三视频流: 320 * 240 分辨率, 推荐用于智能手机或平板电脑应用程序 (例如(IP Cam Viewer))。

现场快速查看实时图像

用户可以通过 HTTP API 从 GDS371x 实时获取视图快照, 这可以在不安装任何浏览器插件的情况下使用。从固件 1.0.3.34 开始, 用户可以根据 JPEG 认证模式部署两种方式查看实时图像, 可在以下路径下设置:

Web UI

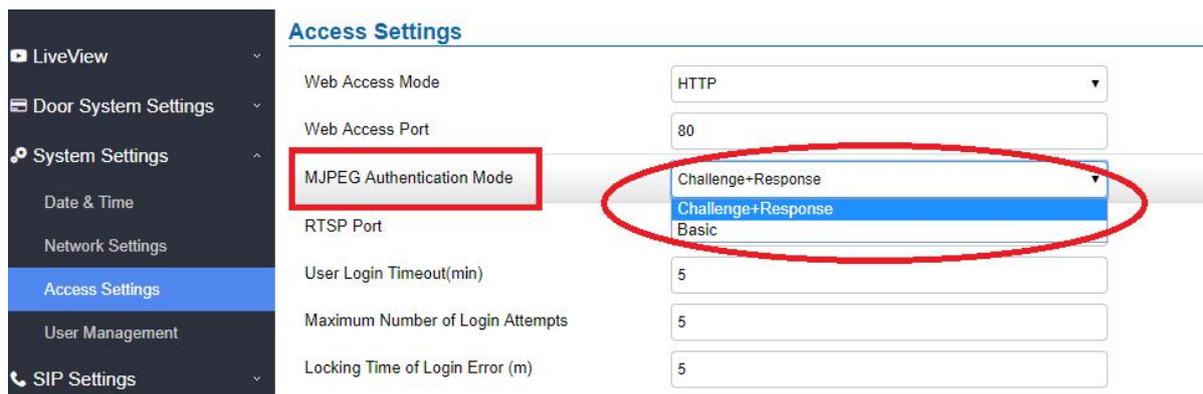


图 49: MJPEG 认证模式

1). Challenge+Response MJPEG 认证模式:

请按照以下步骤在此模式下通过 HTTP 命令进行快照:

1. 在浏览器中输入:`http(s)://IP_Address_GDS:Port/jpeg/view.html`
2. 浏览器将弹出下面的窗口, 用户需要输入登录用户名和密码。

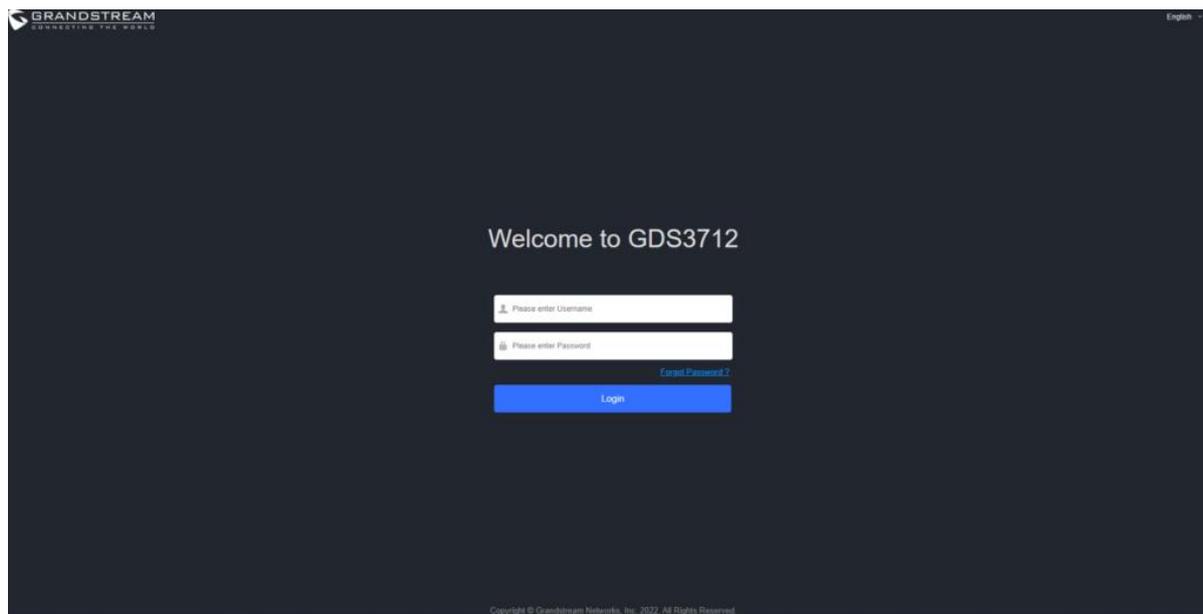


图 50: GDS3712 Admin 登录界面

2. 浏览器将显示视频的一帧(720p)作为实时图片。

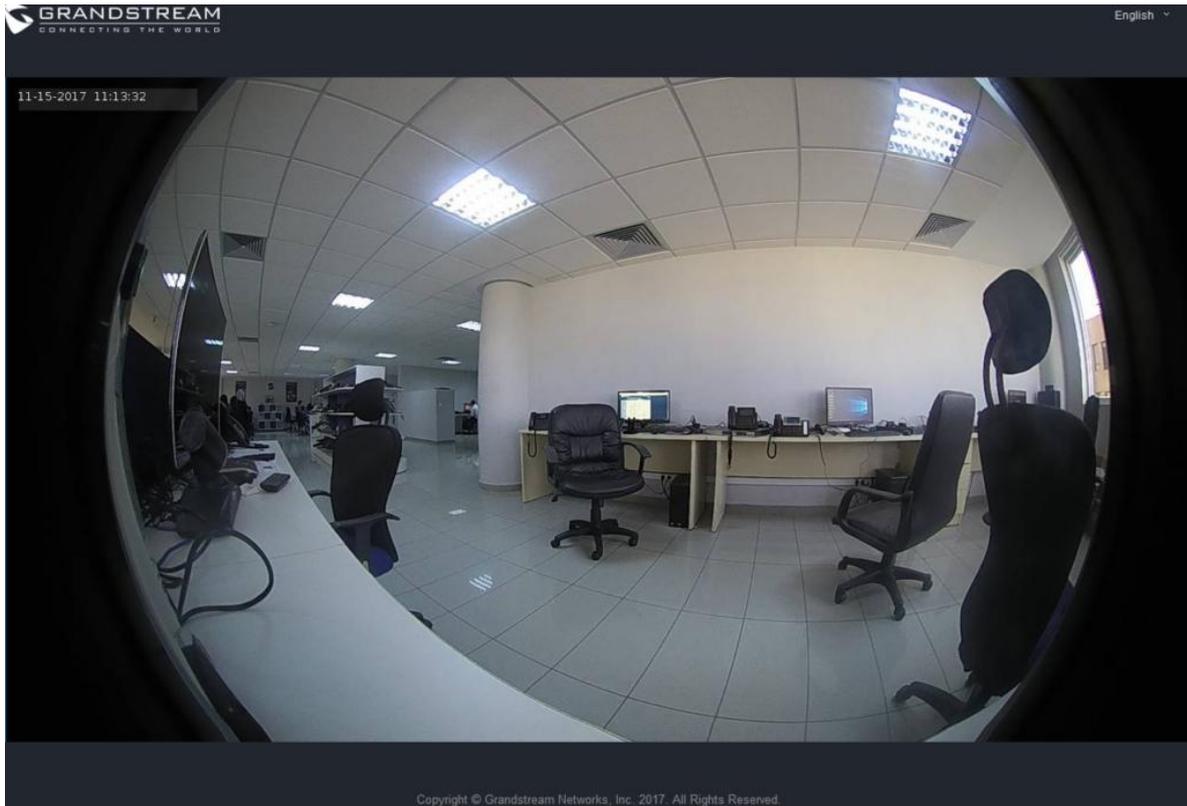


图 51: 使用安全 MJPEG 认证模式的实时图片

注意:

这在所有浏览器上都是支持的，无需安装任何插件，但需要管理用户身份验证以提高安全性。

2). Basic MJPEG 认证:

请按照以下步骤在此模式下通过 HTTP 命令进行快照:

1. 在浏览器中输入: `http(s)://admin:password@IP_Address_GDS:Port/jpeg/view.html`
2. 浏览器将显示视频的一帧(720p)作为快照。

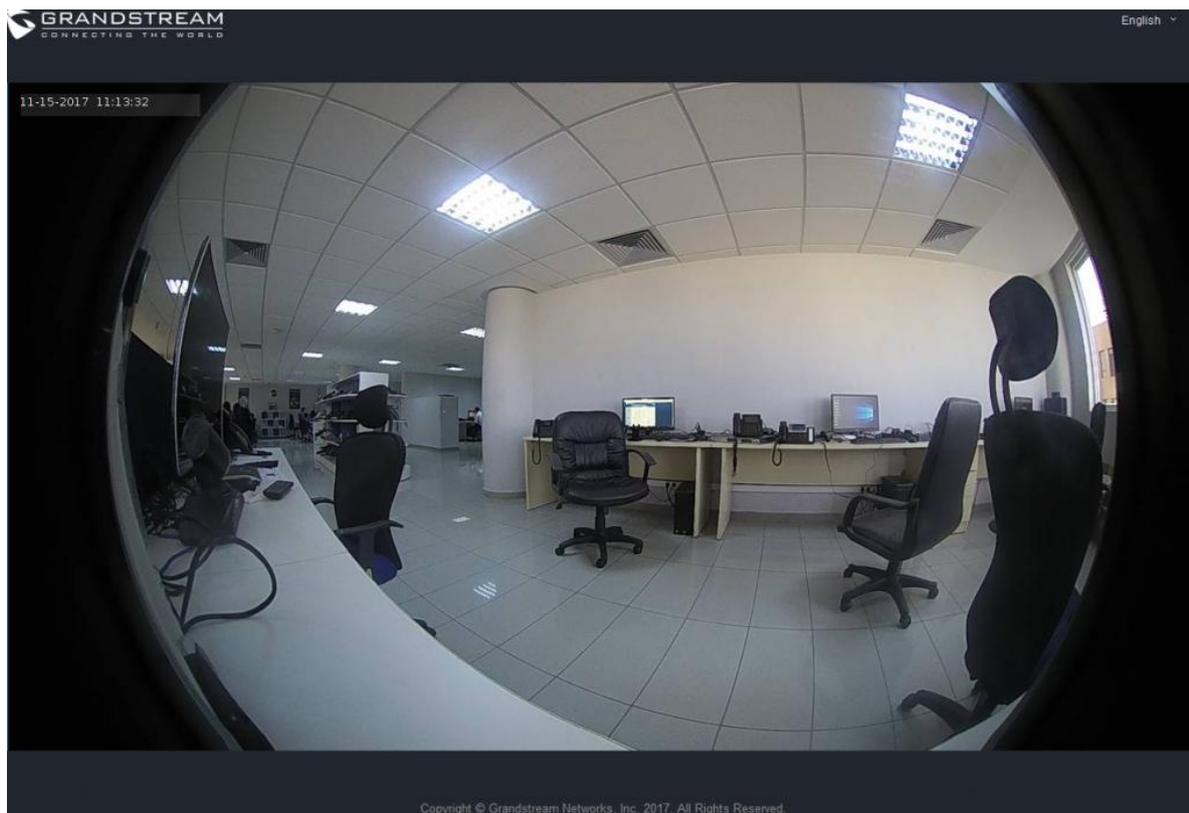


图 52: 使用基本 MJPEG 身份验证模式的 MJPEG 视图

MJPEG 流

GDS371x 通过 HTTP API 命令支持 MJPEG 流实时查看，这可以在不安装实时查看浏览器插件的情况下使用。从固件 1.0.3.34 开始，用户可以根据 JPEG 认证模式的两种方法来检索 MJPEG 流，可在以下路径下设置。

Web UI

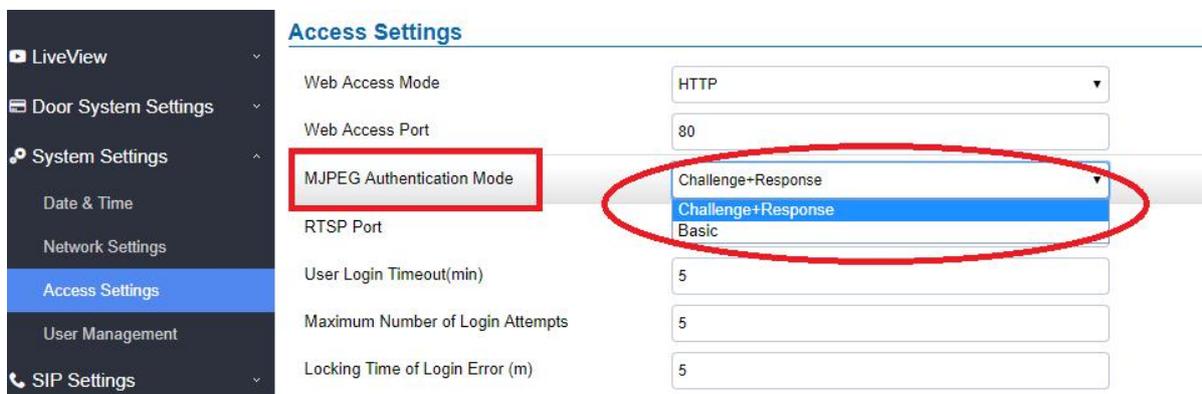


图 53: MJPEG 认证模式

1). Challenge+Response MJPEG 认证模式:

为了在此模式下使用 MJPEG stream over HTTP 命令获得实时视图流, 请遵循以下步骤:

浏览器输入: `http(s)://IP_Address_GDS:Port/jpeg/mjpeg.html`

1. 浏览器将弹出下面的窗口, 用户需要输入登录用户名和密码

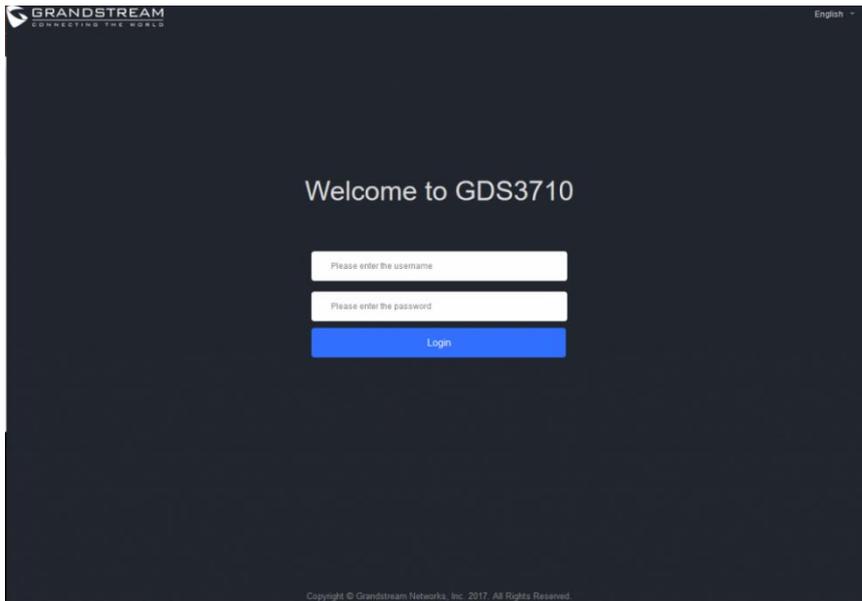


图 54: MJPEG 查看 web 登录界面

3. 浏览器将显示 MJPEG 流 (720p).

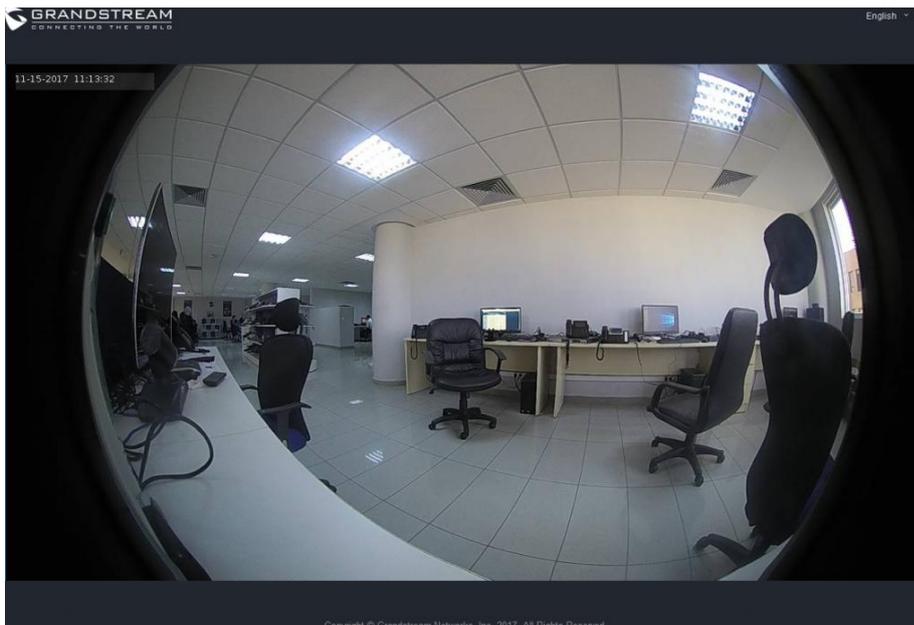


图 55: MJPEG 实时视图使用安全的 MJPEG 认证模式

注意

这在所有浏览器上都是支持的，无需安装任何插件，但需要管理用户身份验证以提高安全性。

2). Basic MJPEG 认证模式:

请按照以下步骤在此模式下通过 HTTP 命令进行快照:

1. 在浏览器中输入: `http(s)://admin:password@IP_Address_GDS:Port/jpeg/view.html`
2. 浏览器将显示视频的一帧(720p)作为快照。

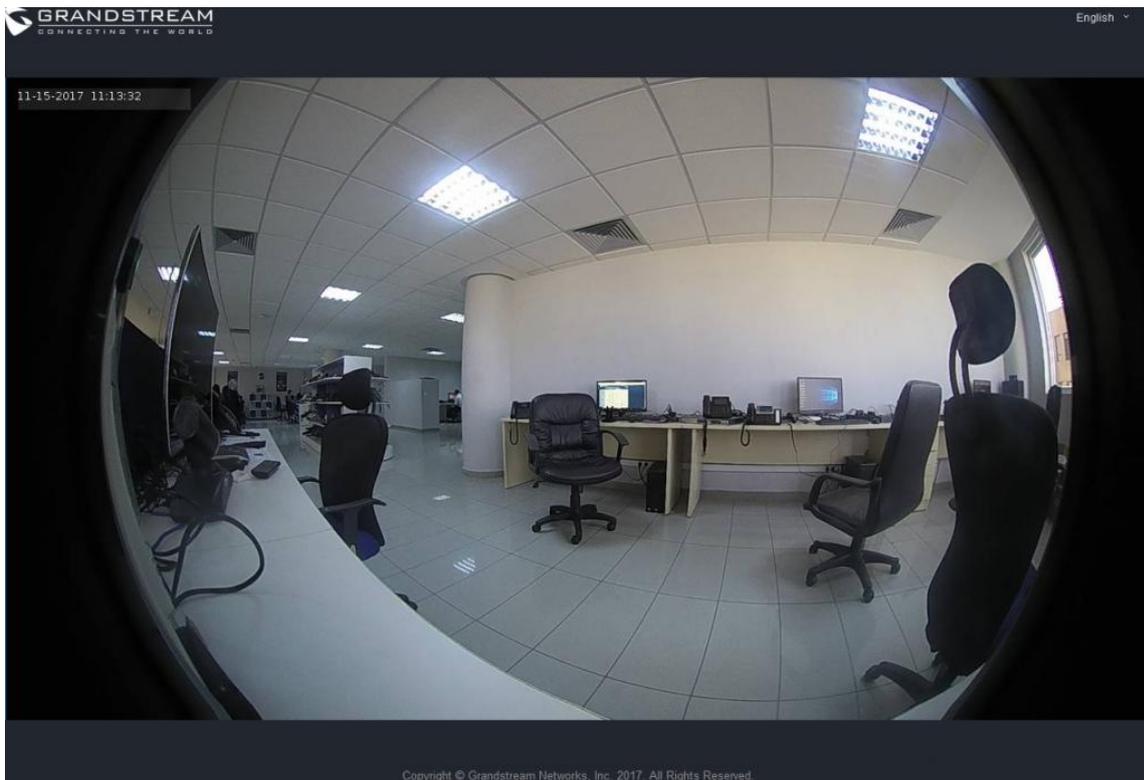


图 56: MJPEG 使用 Basic MJPEG 认证模式实时预览

注意

类似的命令可以应用到 VLC MediaPlayer 等开源应用中，以更好的质量检索 H.264 视频流:

`rtsp://admin:password@IP_GDS3710:端口/X`

其中 X=0,4,8 分别对应第 1、2、3 个视频流(推荐第 2 个)。

门禁系统设置

此页面允许用户配置关于系统操作的参数，例如门的输入 PIN 和管理用户的设置。

基本设置

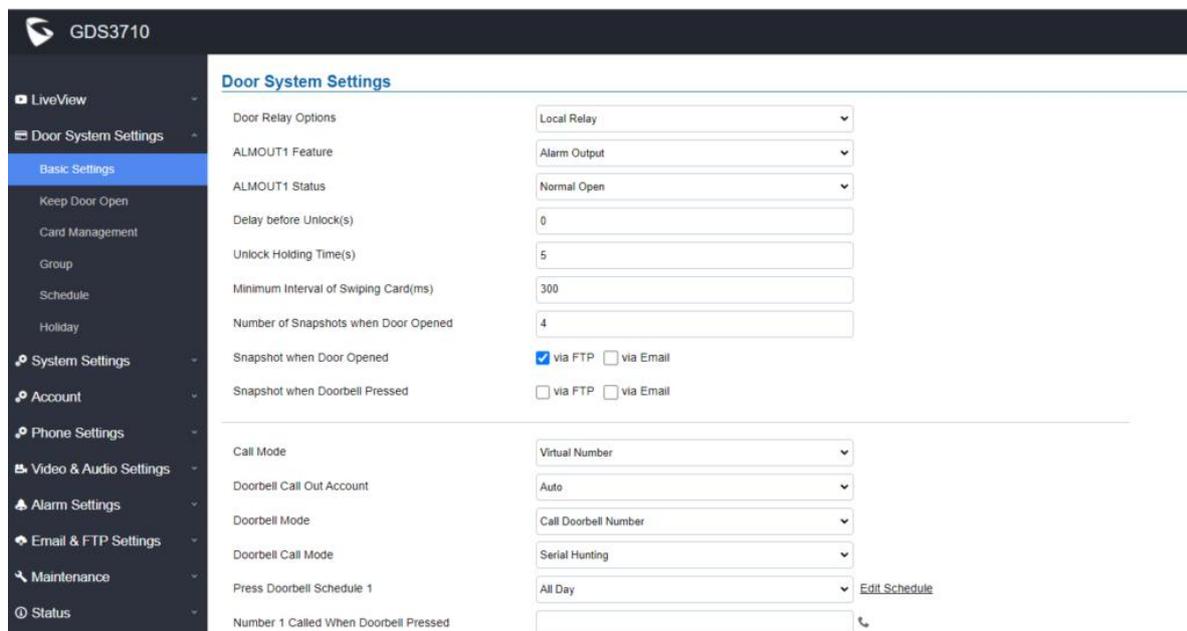


图 57: 门禁系统设置界面

门锁 Relay 选 项

该特性允许客户将 GDS37XX 与第三方 web 中继集成，通过脚本或其他应用程序在网络上控制开门，满足真实应用场景，增强安全性。用户需要输入 web 中继的 IP 地址或域名，以及认证信息，才能使其工作。There are four choices in the pull-down selection:

本地 Relay: 本地 Relay 是 GDS371X 控制的。根据需要控制 1 门或 2 门，门锁被连接到 GDS371X 的 COM2 或 COM1 端口

Webrelay: 当选择 Webrelay 时，客户需要继续配置 Webrelay 的 IP 地址或域名，以及用户名和密码等信息。当合法开门事件发生时，所配置的 web Relay 将获得来自 GDS371x 的通信，并对经过认证的开门请求进行开门操作

GSC3570 Relay: 当门 Relay 设置为 GSC3570 时，它提供了通过输入电话号码和门密码将其连接到 GSC3570 设备的选项。

远程开门发送 Wiegand 代码动作:当执行远程 HTTP API 开门 door1/door2 时，设备将通过 Wiegand 接口发送 PIN1/PIN2 代码。

	<p>注意: webrelay 模式下,被连接到 web 中继控制器设备。</p>
Webrela y URL ON	<p>当“门锁 Relay 选项”设置为“Webrelay”时,请输入第三方控制器使用的正确 URL,以便 GDS3710 发送激活中继的命令。 这增加了额外的安全层,因此当合法的开门事件发生时,配置的 web 中继将从 GDS371x 获得通信,并将为经过身份验证的开门请求操作敲门,或使用该命令操作其他行业应用程序。 注意:</p> <p>有两个 Webrelay URL 字段可用,允许打开或关闭 URL 命令或其他使用 URL 命令。如果第三方网络中继需要此安全特性,也允许配置用户名和密码。</p> <p>如果一些第三方网络中继只支持一个 URL 命令,那么就把另一个 off URL 空着。</p>
Webrela y URL OFF	<p>当门锁 relay 选项设置 Webrelay,然后输入由第三方控制器使用的正确 URL,以便 GDS3710 发送禁用中继的命令</p>
Webrela y Usernam e	<p>输入 webrelay 用户名</p>
Webrela y Passwor d	<p>输入 webrelay 密码</p>
ALMOU T1 功能	<p>该选项允许选择使用 Alarm_Out (COM1)接口作为第三方设备的报警输出,或控制第二个门“门 2”(两个功能互斥)。 当选择“开门”选项时,将使 GDS3710 能够通过 RFID、本地和远程 pin 码控制两扇门的操作。</p>
ALMOU T1 状态	<p>取决于锁的状态,设置常开或常闭</p>
开锁延迟 响应时间	<p>当用户发出授权时,设备将在指定的延迟(秒)后开门。</p>

(秒))	
开锁保持时间(秒)	配置锁保持时间，单位为秒(缺省值为 5 秒)。设备将在指定的时间内保持门不锁。范围:1-1800 秒。
刷卡间隔时间(毫秒)	定义连续刷卡的时间间隔(毫秒)。范围应该在 0ms 和 2000ms 之间。
开门抓拍照片数量	定义 GDS 发送的快照数量(通过 FTP 或 Email)，最多 4 个截图。
开门抓拍	用户可以选择在门打开时将快照通过电子邮件发送，而不通过 FTP 将快照发送到 FTP 服务器。
按门铃键抓拍	用户可以选择在按门铃时将快照通过电子邮件发送，而不通过 FTP 将快照发送到 FTP 服务器。
拨号类型	从 GDS3710 键盘拨号时选择呼叫 SIP 号码还是虚拟号码。
门铃呼出账号	此选项设置用于在门铃触发时拨打电话的帐户。如果设置为自动，GDS 将使用第一个可用帐户。
门铃模式	<p>配置按下门铃时要执行的操作，有三个选项可用：</p> <p>呼叫门铃号码：按下门铃时，将呼叫“按下门铃时呼叫的号码”</p> <p>控制门铃输出（数字输出 1）：当按下门铃时，输出 1 的电子锁打开，持续时间为（1s 至 4s），选项仅适用于 GDS3710 型号</p> <p>以上两项：选中后，“呼叫门铃号码”和“控制门铃输出”选项均已启用，选项仅适用于 GDS3710 型号</p>
门铃呼叫模式	<p>当按下门铃按钮时，选择所呼叫号码的响铃策略，使其为顺振或同振：</p> <p>顺振模式：配置的扩展名和/或 IP 地址将按顺序逐个响起。</p>

	<p>同振模式：配置的扩展和/或 IP 地址将同时响铃（最多 4 个同时进行的 SIP 呼叫）。</p>
<p>按门铃时间表 1-4</p>	<p>选择时间安排时，按下门铃将呼叫所配置的目的地。</p> <p>注： 最多可配置 4 个不同的“时间表”。</p> <p>“门铃”呼叫号码或 IP 地址必须在相关的“时间表”中配置</p> <p>表的优先级顺序为“日程 1、2、3、4”。设备将首先检查并验证当前时间是否符合“时间表 1”，如果符合则使用“表 1”中配置的号码拨出；如果不匹配，则检查“表 2”，如果匹配，则使用号码 2 中配置的号码拨出，并循环检查验证，直到结束。</p>
<p>按门铃呼叫号码 1-4</p>	<p>配置门铃按下时被叫 SIP 分机号(SIP Server 模式)或带端口号的 IP 地址(IP 模式):</p> <p>SIP Server 模式:</p> <p>该字段可以配置为存储多个 SIP 号码，如果配置了多个号码(例如:1001,1002,1003)，用“,”分隔，GDS3710 将顺序呼叫每个号码(GDS 将默认为每个号码振铃 15 秒，这可以在 ring Timeout 上更改)或在 Parallel Hunting 模式下同时振铃。</p> <p>当使用 UCM 时，用户还可以在那里配置一个 Ring Group 分机(例如 6400)，它将同时振铃多个分机，或者根据 Ring Group 振铃策略一个接一个地振铃</p> <p>如果所有话机都是 GXP21XX，手机将逐帧播放视频，用户可以通过按远端 _PIN#或按开门按钮(如果已配置)开门。</p> <p>如果手机侧开启了早期媒体，用户可以在接听电话前通过开门键发送 PIN 码(当然用户也可以在接听电话后开门)。</p> <p>IP 模式:</p> <p>用户需要为话机配置多个 IP 地址而不是 SIP 分机，当门铃按下 GDS3710 时，将根据门铃呼叫模式策略以串行或并行模式对所配置的 IP 地址进行振铃。</p> <p>如果开启了早媒体，则 GXV33XX 将在振铃时接收视频流，如果用户已经配置了开门键，则可以按开门键开门(当然用户也可以接听电话后开门)。</p>

	GXP21XX 话机使用 JPEG 流接收 GDS3710 视频，这意味着如果启用或禁用早期媒体，它将接收视频。备注:最大支持 256 个字符。
最长拨号长度	配置键盘上允许拨号的最大数字数。一旦满足配置条件，设备将不按#自动发送号码呼叫。如果设置为 0 则禁用。
无按键输入超时(秒)	定义无键时的超时时间(以秒为单位)。如果超时后未按下任何键，则不按“#”，数字将被发送出去。缺省值是 4 秒。有效范围为 1~15。
按门铃时间表	为门铃按钮配置一个时间表，一旦配置，门铃将根据配置的时间表开启/关闭。默认设置为“全天”。
远程开门密码	配置存储在 GDS3710 中的 PIN 码，远程 SIP 电话需要输入并匹配此 PIN 码(通话时通过 DTMF 发送)，GDS3710 才能开门。 注意:为了增强安全性，当从 GDS 发起呼叫时，只有“白名单”中存在的号码才能使用 DTMF PIN 远程开门。
本地开门密码类型	<p>有三种选择:个人密码，统一密码或卡和个人密码。</p> <p>个人密码:意味着每个用户都有个人密码，GDS 会记录每次是谁开的门。用户需要在 GDS3710 上输入如下顺序开门[*虚拟号码*个人密码#]。</p> <p>注意:</p> <p>当设备了个人密码，用户也可以使用他们的卡，来开门。</p> <p>更多详细信息和条件请参见[关闭 SIP 号码拨号]。</p> <p>统一:意味着所有会员都用同一个密码解锁。用户需要在 GDS3710 键盘上输入以下顺序开门[*统一密码#]。</p> <p>卡和私人密码:意味着每个会员都需要刷卡并输入个人密码才能按以下顺序开门[刷卡+ *个人密码#]</p> <p>注意:此特性只能在 GDS3710 上配置。</p>
本地开门密码	密码存储在 GDS3710 中，本地输入此密码在 GDS3710 键盘上将开门。(此功能需要激活统一密码。

本地开门 密码时间 表	为本地 PIN 开门配置一个时间表。一旦配置，门打开能力使用本地 PIN 与打开/关闭基于配置的时间表。默认设置为“ All Day ”。
启用 DTMF 开 门	启用后，远程 SIP 话机可以在通话时通过输入配置的远程 PIN 码(PIN 码通过 DTMF 发送)开门。禁用“ 默认设置 ”。
启用临时 密码	启用临时密码
临时密码	配置临时密码用于开门
临时密码 有效期开 始时间	选择临时密码生效的开始时间
临时密码 有效期结 束时间	选择临时密码生效的结束时间
禁用自动 接听	选中后，GDS3710 将不自动接听来电，用户可按任意键接听来电。默认设置为未勾选。
启用门铃 键挂机	如果选中，则用户按下门铃按钮即可挂断正在进行的通话。默认启用。
禁用键盘 (不含门铃 键)	选中时，键盘将被禁用，只有门铃按钮可以按下。
启用远程 开门挂断 通话	当被检查时，呼叫将在远程开门事件发生 5 秒后自动断开。
启用 HTTP API 远程	启用此选项允许使用 HTTP API 命令远程打开门。 禁用:关闭该选项。 Challenge + Response 认证:此选项允许使用多步骤方法进行身份验证

开门	<p>Basic 认证 t 该选项使用一个简单的请求进行身份验证::</p> <p>开门命令示例: https://admin:password@192.168.23.123/goform/apicmd?remotepin=12345&type=1</p> <p>关门命令示例: https://admin:password@192.168.23.123/goform/apicmd?remotepin=12345&type=2</p> <p>重要提示:我们不会对任何由于打开 HTTP API 远程功能而导致的安全问题负责, 默认情况下该选项是禁用的, 用户应该在知道如何降低风险的情况下启用它。 注意:当 HTTP API 打开门执行时, 通过 Wiegand 发送 PIN 码的选项添加在 GDS3710 模型的新固件升级上。</p>
禁止按键 拨打 SIP 号码	<p>当 SIP 号码拨号禁用时, 按#后, 设备将把每个数字输入定义为私人密码开门请求。</p> <p>注: “本地开门密码类型” 应该选择私人密码。 . 私人密码在用户之间必须是唯一的, 否则门仍然会打开 私密码在用户中必须是唯一的, 否则门打开, 但日志查不到谁打开了门, 因为重复的密码和数据库中最后匹配的用户与私人密码将显示在日志中。</p>
启用发卡 状态	<p>选中启用 RFID 卡发卡程序。当 RFID 卡扫入 GDS3710 时, 会将卡信息添加到 [卡片管理]中。</p>
发卡状态 超时时间 (分)	<p>当定时器到达时, 自动关闭发卡模式(取值范围为 1 ~ 1440, 单位为分钟)。</p>
启用按键 蓝色灯光	<p>选中后, 当按下 GDS3710 的按键时, 将激活蓝色指示灯。</p>
启用背光 灯	<p>选中时, 点击 GDS3710 的按键背景灯将打开</p>
启用蓝色 门铃灯	<p>开启后, 门铃 LED 会根据设置的开始/结束时间亮起。例如, 当 GDS 部署在黑暗环境时, 可以使用此选项, 使用门铃 LED 可以轻松定位 GDS。</p>

启用蓝色键盘灯	开启后，键盘 LED(门铃 LED 除外)将根据设置的开始/结束时间亮起。例如，当 GDS 部署在黑暗环境时，可以使用此选项，使用键盘 LED 可以轻松定位 GDS。
中心模式	如果启用，组/时间表/假日只能从中央(GDS 管理器)同步，本地配置将不允许。如果禁用，则只允许从 GDS3710 进行本地配置。
按键灵敏度级别	<p>设置灵敏度级别:</p> <p>默认:在此模式下，GDS3710 使用了灵敏度较低的键盘参数，适用于大多数使用场景，特别是在温暖和高湿的地方，如热带地区或海边或河边，存在高湿度的天气条件，特别是在夏季。</p> <p>高:此选项适用于位于高纬度地区的应用场景，通常非常寒冷，用户可能需要戴着手套按键盘。由于该参数灵敏度较高，在低纬度等不同环境下使用可能会出现误报。</p> <p>注意:大多数应用场景，该固件的默认设置已经足够应用。请使用默认设置，除非使用场景确实需要高键盘杠杆灵敏度。</p> <p>如果使用默认或低灵敏度键盘，幽灵呼叫问题仍然经常发生，这可能表明有不适当的布线或安装，或者可能是硬件故障。请与我们的 Grandstream 支持联系，以帮助解决此类问题。</p>
按键声	<p>配置 GDS3710 的按键音</p> <p>默认: 按下 GDS3710 键会发出 Beeps</p> <p>DTMF: 按下 GDS3710 键会发出 DTMF 音</p> <p>静音: 按下 GDS3710 键会没有按键音。</p>
启用韦根输入功能	当 GDS 连接到维根时，需要启用该选项。输出设备(如 RFID 读卡器)
韦根输出功能	当 GDS 为韦根输出设备时，该选项将被启用。(例如:输入设备为门控制器)

表 6: 门禁系统设置

注意:远程 SIP 话机需要与 web 页面配置匹配的密码(0-9，以# key 结尾)才能开门(通过 DTMF)。

GDS3710 支持多用户 RFID 开门，每个用户都有自己的 PIN 码。对于用户数较大的环境(限制为 2000)，GDS3710 很难管理所有这些用户，因此需要使用单独的 PC 或 Server 进行这种管理和监

控。

在有大量用户(限制为 2000)的环境中，另一种可能性是 GDS3710 设置一个统一的本地密码为所有用户开门。

使用 Alarm Out (COM 1) 控制第二扇门

从固件 1.0.5.2 开始，用户可以设置 Alarm_Out (COM1)接口来控制第二个门，除了现有的 Locker/COM2 接口(控制 Door1)。该功还允许 GDS3710 通过 RFID、本地和远程开门码来控制两扇门的操作。

例如，第三方韦根输入设备或 GDS3710 上可以安装在 Door2，并将相关电缆连接到安装在 Door1 上去控制 GDS3710。Door1 和 Door2 可以通过编程的 RFID 卡和 PIN 分别或同时设置为打开。

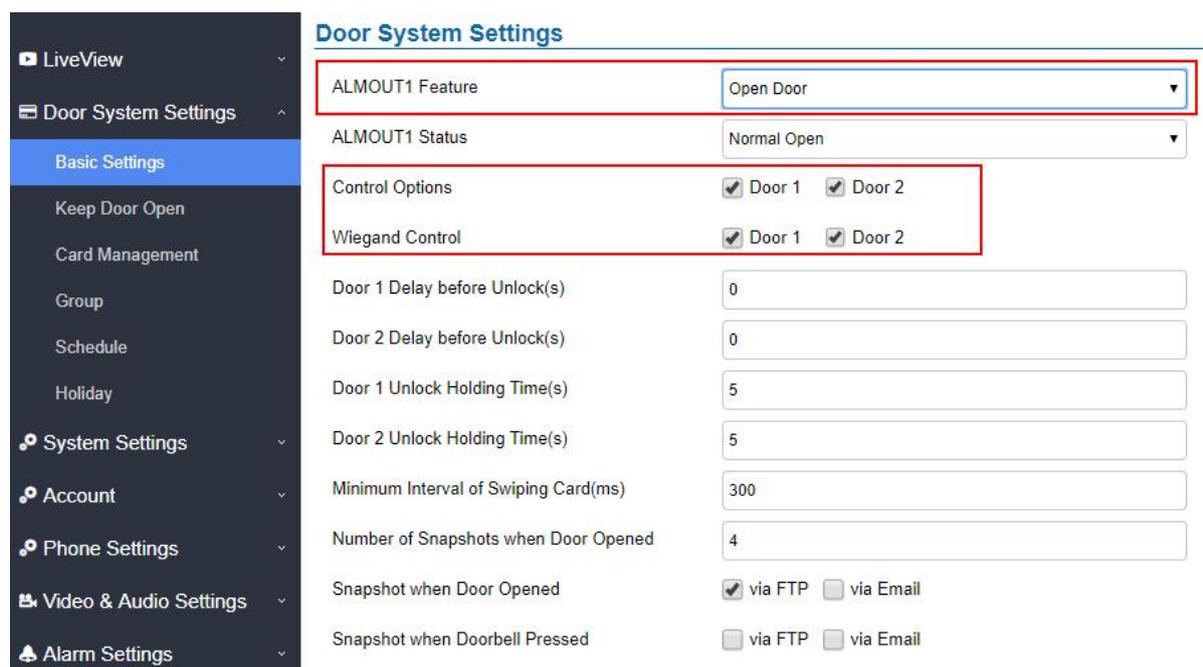


图 58: Alarm_Out1 功能

门控制界面(哪扇门可以打开)

如果设置 “Alarm_Out (COM1)” 接口控制门 2 的开启，“ALMOUT1 状态” 可根据不同的门锁方式选择 “常开” 或 “常关”。

与默认的 COM2 不同，COM2 是为控制开门而设计的，有三个连接口，COM1 只有两个连接口。

因此，必须配置正确的锁定模式，以确保锁按预期工作。对于上面的例子，GDS3710 配置为控制 Door1(接线到 COM2 接口);第三方 Wiegand Input 设置为控制 Door2(连接到 COM1 接口)。

对于上面的例子，GDS3710 配置为控制 Door1(接线到 COM2 接口);第三方 Wiegand Input 设置为控制 Door2(连接到 COM1 接口)。

在断电的情况下，关闭电源时的 DOOR STATUS 将取决于以下情况:

- com2 有三个引脚，分别对应 NO 或 NC。因此，当连接 NC2 和 COM2(故障安全)时，当断电时，锁将打开，当连接 COM2 和 NO2 时，当断电时门将“锁定”(故障安全)。
- com1 (ALMOUT1)只有两个 PIN，并且只有 NO。如果所连接的锁是 NO 罢工，这意味着 ALMOUT1 状态设置为“常开”，则断电时门将关闭;如果所连接的锁是 NC 罢工，且 ALMOUT1 状态设置为“常闭”，则断电时门将打开。

○ 使用统一密码:开门

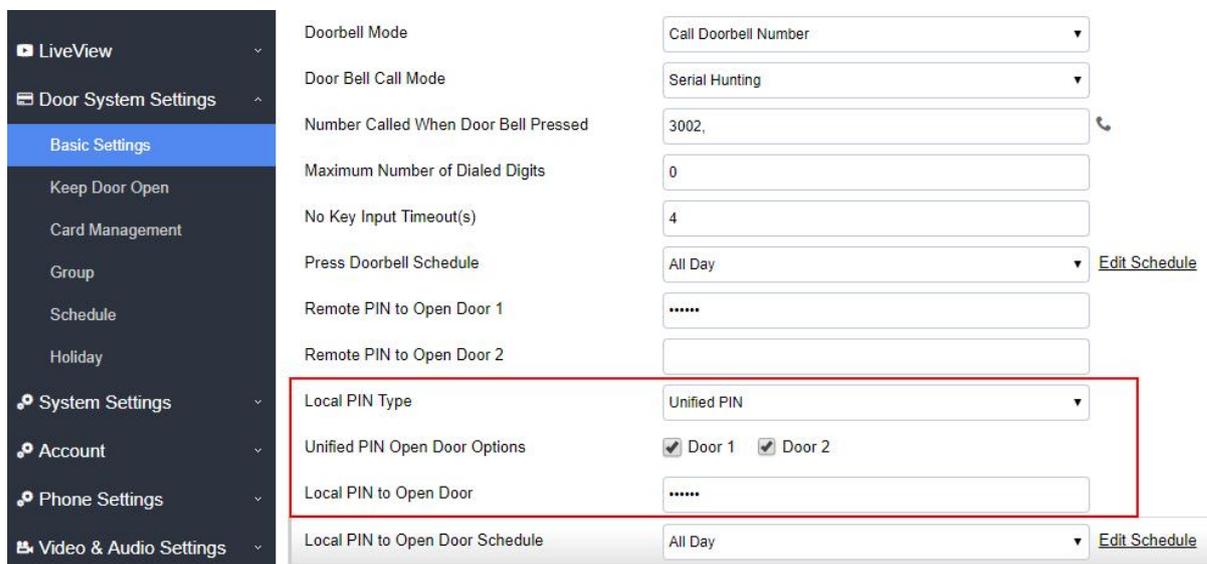


图 59: Alarm_Out1 功能

如果配置了统一密码 (Universal PIN)开门，那么一旦选择了“统一密码”，则在 UI 中可以配置该密码可以控制哪扇门

例如，如上图，如果这个通用密码设置为同时打开 Door1 和 Door2，但由于之前的“控制选项”设置为打开 Door1，“韦根控制”设置为打开 Door2，因此最终结果将是两组条件合格的综合结果。

○ 使用远程密码开门:

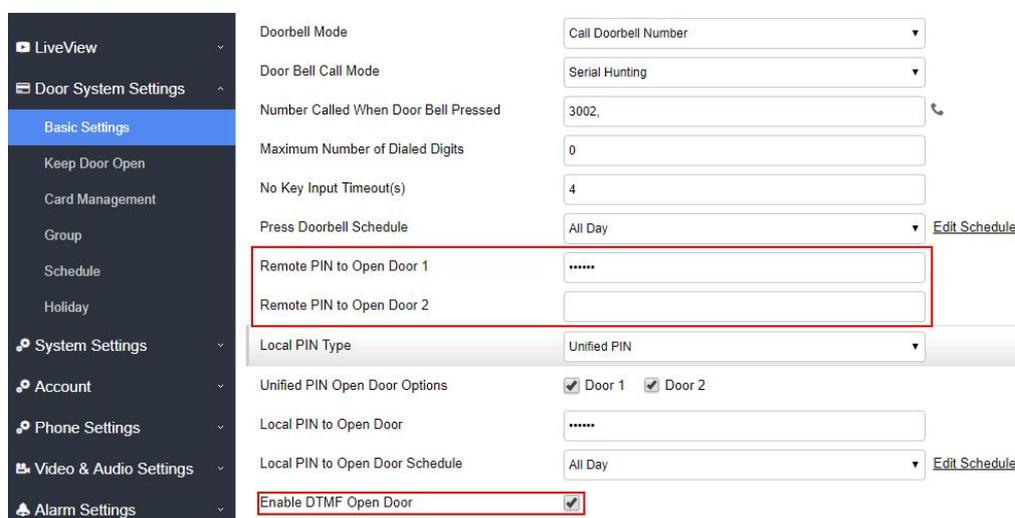
对于远程密码开门，密码配置可以参考在下面的例子。

Door1 和 Door2 密码可以不同，必须在相应的 IP 话机上正确配置，用于操作“一键开门”。

如果两扇门需要同时打开，那么 Door1 和 Door2 都必须配置相同的密码或 DTMF。

注意

为了增强安全性，当从 GDS 发起呼叫时，只有“门铃按下时呼叫的号码”、“账号白名单”或“卡管理”（仅 GDS3710 有该功能）存在的号码，才能使用 DTMF 密码远程开门。



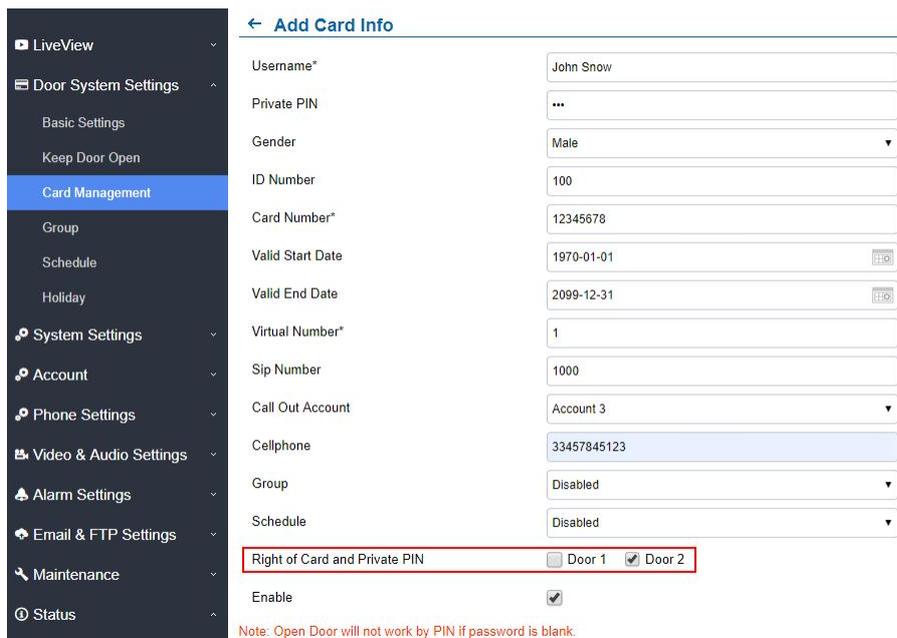
Doorbell Mode	Call Doorbell Number
Door Bell Call Mode	Serial Hunting
Number Called When Door Bell Pressed	3002,
Maximum Number of Dialed Digits	0
No Key Input Timeout(s)	4
Press Doorbell Schedule	All Day Edit Schedule
Remote PIN to Open Door 1
Remote PIN to Open Door 2	
Local PIN Type	Unified PIN
Unified PIN Open Door Options	<input checked="" type="checkbox"/> Door 1 <input checked="" 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"/>

图 60: 通用本地密码

○ 个人密码或卡片 & 个人密码:

注意

此配置仅适用于 GDS3710 型号。



← Add Card Info

Username*	John Snow
Private PIN	...
Gender	Male
ID Number	100
Card Number*	12345678
Valid Start Date	1970-01-01
Valid End Date	2099-12-31
Virtual Number*	1
Sip Number	1000
Call Out Account	Account 3
Cellphone	33457845123
Group	Disabled
Schedule	Disabled
Right of Card and Private PIN	<input type="radio"/> Door 1 <input checked="" type="radio"/> Door 2
Enable	<input checked="" type="checkbox"/>

Note: Open Door will not work by PIN if password is blank.

图 61: 卡的权利和私人密码

如果使用 RFID 卡或私人 PIN 开门，那么通过“卡管理”配置 RFID 卡或私人 PIN 可以打开哪扇门，见上图截图。

注意

对于所有的设置，哪扇门可以打开的最终结果是所有符合条件的集合的逻辑相交运算。

请参阅我们的打开门流程图，以便更好地了解如何配置和控制两个门操

作：http://firmware.grandstream.com/GDS3710_opendoors_logic.pdf

强制开门

该功能允许用户设置立即或计划开门，适合的使用场景，如学校或类似的私人或公共场所，门需要在特定的时间窗口保持打开，其余时间关闭。对于需要举办一段时间研讨会的场景或物业，或者工厂或公司的午餐休息时间，门保持打开，不需要访问记录，然后在授权进入后重新锁定，默认情况下是禁用的。

GDS3712 提供了单独配置 Door1 和 Door2 的选项，直接门打开或计划门打开；GDS3710，两个门只有有一个配置选项。

有两种模式:

1. 强制开门 (一次性的动作)

Keep Door Open

Keep Door Open	Immediate Open Door ▼
Interval of Keep Door Open(min)	5

图 62: 强制开门开门

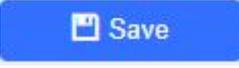
表 7: 强制开门列表

强制开门

选择开门模式

强制开门保持时间(分)

设置以分钟为单位的开门时间。点

击  立即开门。

注意

当警报 OUT 1 设置为打开门, 则此选项将分别用于每扇门。

2. 时间表开门 (重复性动作)

Keep Door Open

Door 1

Keep Door Open	Schedule Open Door	▼
Schedule Start Time	2019-11-05 12:31:32	
Schedule End Time	2019-11-27 00:00:00	
Holiday Mode	holiday1	▼ 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																										

Door 2

Keep Door Open	Disabled	▼
Emergency PIN to Disable Keep Door Open	<input type="text"/>	

图 63: 时间表开门

强制开门

选择强制开门模式(在这种情况下安排开门)。

有效期开始时间

设置门锁开启开始的时间

有效期结束时间

设置门锁开启结束的束时间

时间表

从计划列表中选择预配置的计划。

假日模式

选择要包含在“保持门打开”计划中的假日时间表(支持门1和门2)。

表 8: 强制开门时间设置

点击编辑日程，选择每天门将保持开放的时间段，如下面的截图所示。

Modify Schedule
✕

Sun	Period1	12 ▾	: 00 ▾	-	14 ▾	: 00 ▾
Mon	Period2	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Tue	Period3	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Wed	Period4	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Thu	Period5	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Fri	Period6	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Sat	Period7	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
	Period8	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾

Copy
 Sun
 Mon
 Tue
 Wed
 Thu
 Fri
 Sat
 Select All

Save

Cancel

图 64: 编辑时间表

注意

在“强制开门”设置中可以配置各种时间表，用户可以选择他们喜欢使用的时间表。

紧急密码

ote

注意

此配置仅适用于 GDS3710

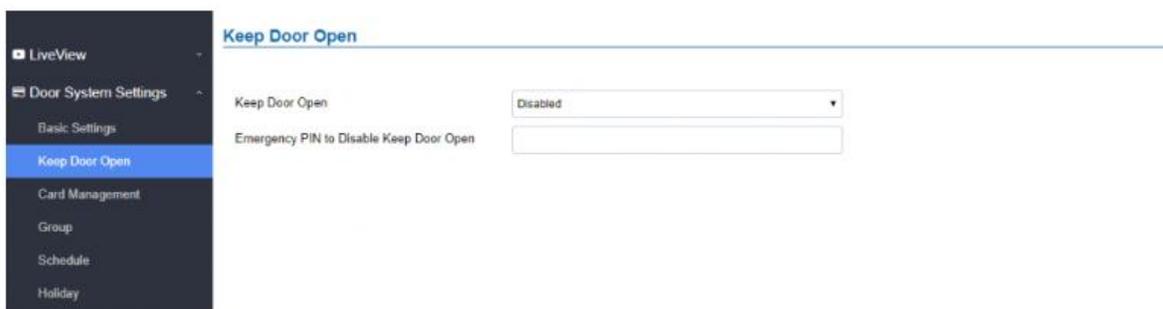


图 65: 强制开门 - 紧急密码

当“强制开门”选项设置为“禁用”时，用户可以通过拨打要使用的紧急 PIN 设置，从设备键盘强制关闭门。

示例:

填写紧急密码，去禁用“强制开门”。

使用立即/时间表强制开门的方法开门

输入“紧急密码，如，:*2018#

输入*紧急 PIN#后，GDS 将关闭门，进入 web GUI 时，“强制开门”部分自动切换到“禁用”选项。

注意

当 ALMOUT1 功能设置为打开门，那么单独的强制开门功能将可用于每个门在此页面上。

卡片管理

注意

此配置仅适用于 GDS3710 型号

本页面允许用户添加 RFID 卡的信息，有两种方式：手动添加和自动添加。

Card Management													
Add User Reload Data Delete Data Username* <input type="text"/> 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	Edit
1	John	33656478	1	1000	Auto	33457845123	412	Male	Disabled	Disabled	1970-01-01	2099-12-31	
2	Robert	124578	2	2000	Account 1	212682522210	413	Male	Disabled	Disabled	1970-01-01	2099-12-31	

图 66: 卡片管理

注意

- GDS3710 最多支持 2000 个卡片。
- 点击  或  导入/导出存储在 GDS3710 上的用户配置文件、信息和数据。
- 用户可以导出和上传 csv 和 gs 文件:
- “.gs”格式是加密的数据库文件，不能编辑，密码或 PIN 码也不能查看。
- “.csv”格式未加密，因此所有内容都是可查看和编辑的。
- 系统管理员在以这种文件格式导出数据库时应该非常小心，因为以安全为代价提供了方便。强烈建议系统管理员在使用 Excel 编辑或修改导出的 CSV 格式数据库文件时，将“密码”设置为“安全保护”。

手动添加卡片用户

点击  ，可以新建一个用户卡片，如下图：

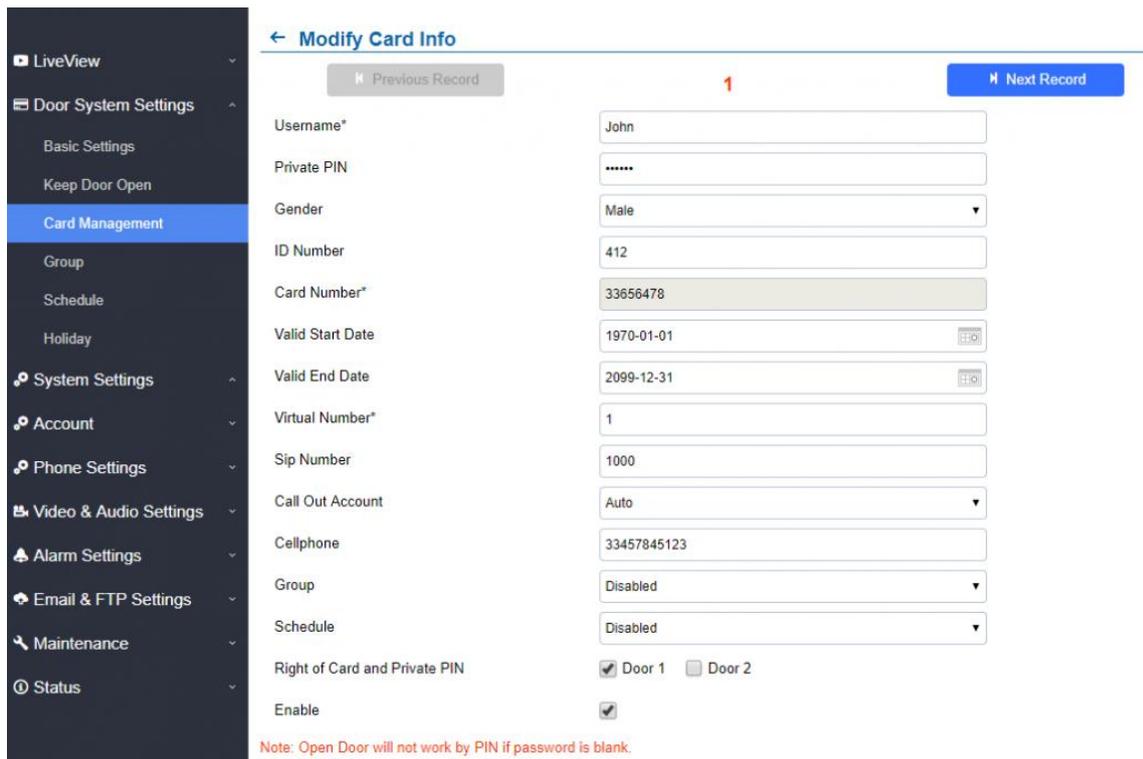


图 67: 卡片信息

用户名	配置用户名以识别用户。
个人开门密码	设置指定的密码用于开门
性别	设置性别, 男或女
证件号	输入一个 ID 号码(该号码由管理员设置, 以唯一地标识每个用户)。
卡号	输入 RFID 卡号 (这是写在 RFID 卡上的号码。启用卡发状态时, 将自动添加此字段)。可以设置的最大字段: 2147483647.
有效期起始	配置 RFID 卡的有效起始日期。
有效期结束	配置 RFID 卡的有效结束日期。
虚拟号	当直接从键盘拨号时, GDS 仅接受用于识别用户的虚拟号码, 一旦输入虚拟号码, 然后按 # 键, 将拨打 SIP 号码。
SIP 号	Sip 号码与虚拟号码映射, 一旦拨打虚拟号码, GDS3710 将向 SIP 号码发送 INVITE。 注意: 该选项可以设置分机号也可以设置 IP 地址, 例如 192.168.5.124
呼出账号	选择 GDS3710 在键盘拨号时调用用户 SIP 号码的帐号。默认为自动。
手机	用户手机号
分组	指定将用户添加到哪个组。
日程表	指定日程表给用户。
片权及私人密码	选择用户可以开锁的门。

启用 如果勾选，用户的 RFID 和私人 PIN 将被激活用于开门。如果不勾选，私人 PIN 或 RFID 卡刷卡将不会生效。

表 9: 卡片信息

注意

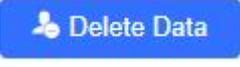
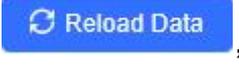
- 分组里的日程表权限优先级高于日程表
- 如果时间表被设置为“禁用”，RFID 卡将在全天刷卡都可用。
- 如果用户禁用，相关卡或密码将无法打开门。

如果“私人密码”是空白，该用户将无法“开门”。

自动添加用户卡片

如果选中[启用发卡模式]，则 GDS3710 键盘开始闪烁，一旦刷卡，存储在卡片上的数据将被添加到 GDS3710 卡片管理页面，用户仍然可以通过手动编辑修自动添加的条目。

用户操作

- 点击  去编辑条目或显示条目的详细信息。
- 选择条目并单击 ，去删除已选中的条目。
- 点击 ，更新输入到 GDS3710 的数据。
- 用户可以使用      ，来浏览用户管理页面。

显示个人密码

个人密码可以从卡片管理页面查看，默认会隐藏掉。

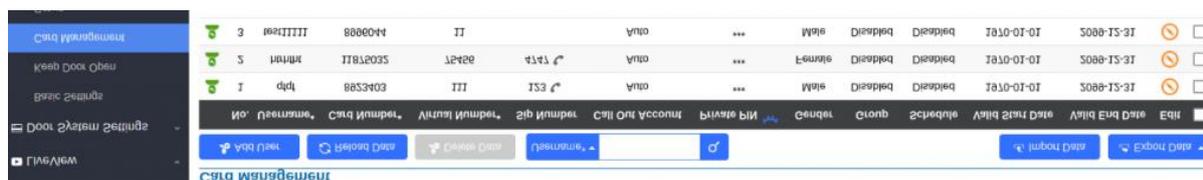
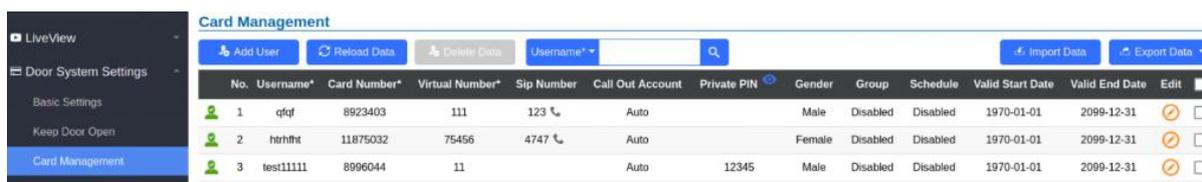


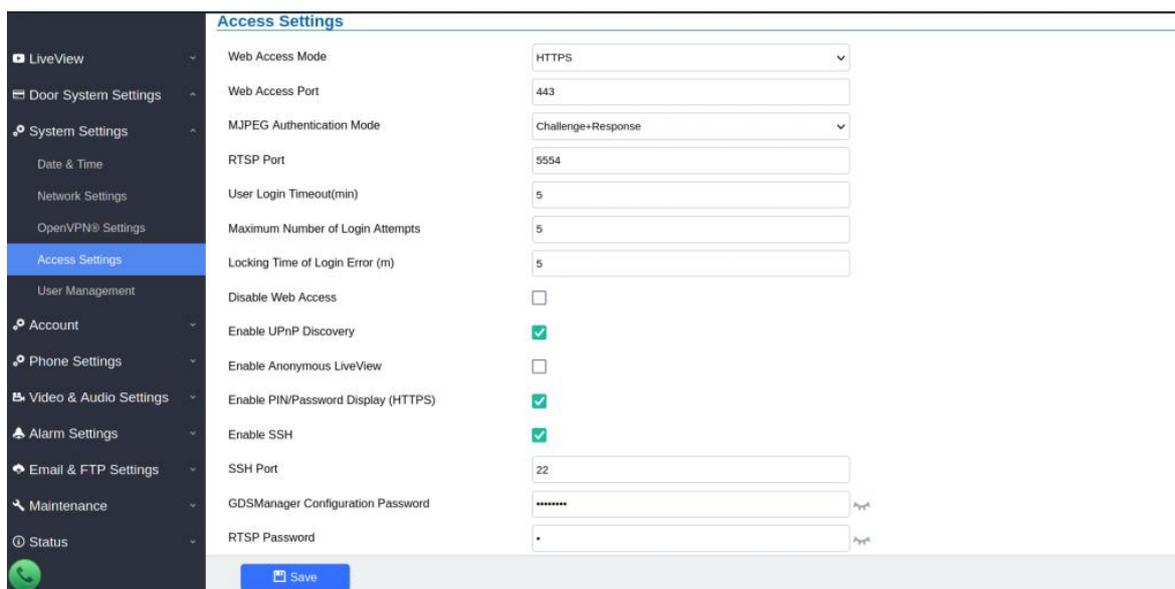
图 68: 隐藏个人密码



No.	Username*	Card Number*	Virtual Number*	Sip Number	Call Out Account	Private PIN	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	qtrf	8923403	111	123	Auto		Male	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>
2	hrhth	11875032	75456	4747	Auto		Female	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>
3	test11111	8996044	11		Auto	12345	Male	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>

图 69: 查看个人密码

要启用该功能，请在 web 界面上进入系统设置>访问设置，将 web 访问模式切换为 HTTPS，并启用 PIN/密码显示(HTTPS)。



Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	5554
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	*

图 70: 启用密码显示 (HTTPS)

注意

默认该功能不启用。

该功能仅仅适用于使用 HTTPS 访问 web 的情况。

分组

注意

该配置仅适合 GDS3710。

组页面允许管理包含多个用户的组，点击  去创建新的租，点击  去编辑已存在的租，点击  去删掉选中的组。

注意

用户最多可以创建 50 个组。

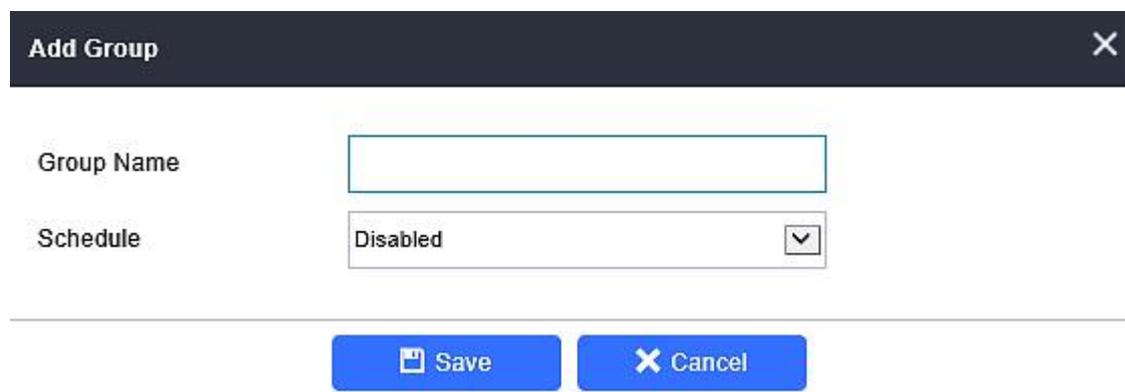


图 71: 添加组

组名

配置名称以标识组

日程表

指定组将使用的日程表

表 10: 添加组

下图显示了创建的组的列表

Group				
+ Add				
No.	Group Name	Schedule	Edit	Delete
1	Support	schedule1		
2	Sales	schedule2		
3	Documentation	schedule3		

图 72: 组的列表

日程表

日程表界面允许管理计划并分配给用户的开门的时间有效期。超出配置的时间间隔，GDS3710 将不允许用户开门。

点击  去编辑日程表 或点击  查看日程细节。

注意

GDS3710 支持 10 个日程表。

Schedule

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		

图 73: 编辑日程表

节假日

节假日配置页面允许管理配置假日，且将分配给用户的门系统使用。

点击  可以编辑节假日配置，点击  可以查看节假日细节。

Holiday

No.	Holiday Name	Detail	Edit
1	holiday1		
2	holiday2		
3	holiday3		
4	holiday4		
5	holiday5		
6	holiday6		
7	holiday7		
8	holiday8		
9	holiday9		
10	holiday10		

图 74: 编辑节假日

系统设置

通过该界面，用户可以配置 GDS3710 的日期时间、网络设置、访问 GDS3710 的方式和访问 Web 界面的密码。

时间日期设置

此页面允许用户调整 GDS3710 的系统日期和时间。

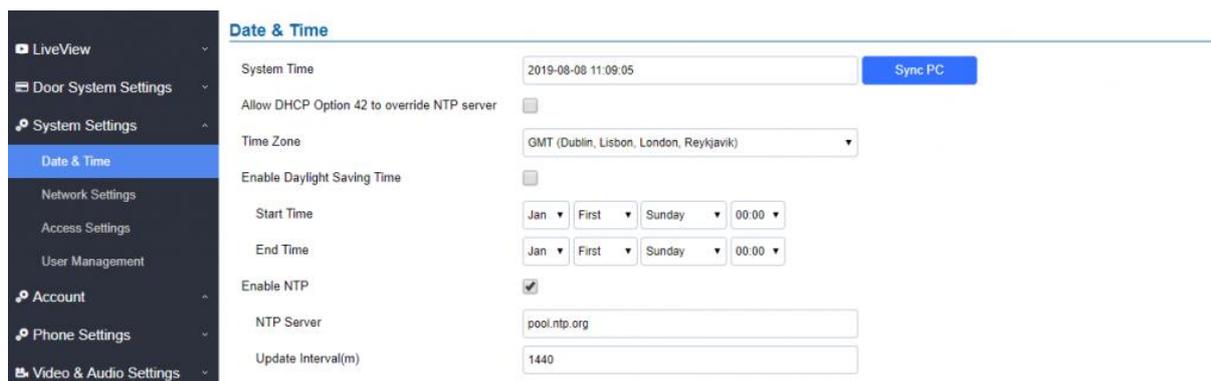


图 75: 时间日期界面

系统当前时间	显示系统的当前时间
启动 DHCP option 42 设定 NTP 服务器	Defines whether DHCP Option 42 should override NTP server or not. When 启用 DHCP Option 42 将覆盖从 NTP 服务器获取的时间，如果它设置在局域网。默认设置为“是”。
同步 PC	点击同步电脑的时间.
时区	Selects from drop down menu the preferred time zone.
启用夏令时	启用夏令时
开始时间	设置开始时间
开始时间	设置结束时间
启用 NTP	通过 NTP 同步设备时间
NTP 服务器	配置 NTP 服务器的地址
更新时间间隔	配置从 NTP 服务器检索更新的间隔（分钟）

网络设置

此页面允许用户为 GDS3710 设置静态 IP 地址或是获取 DHCP 地址。

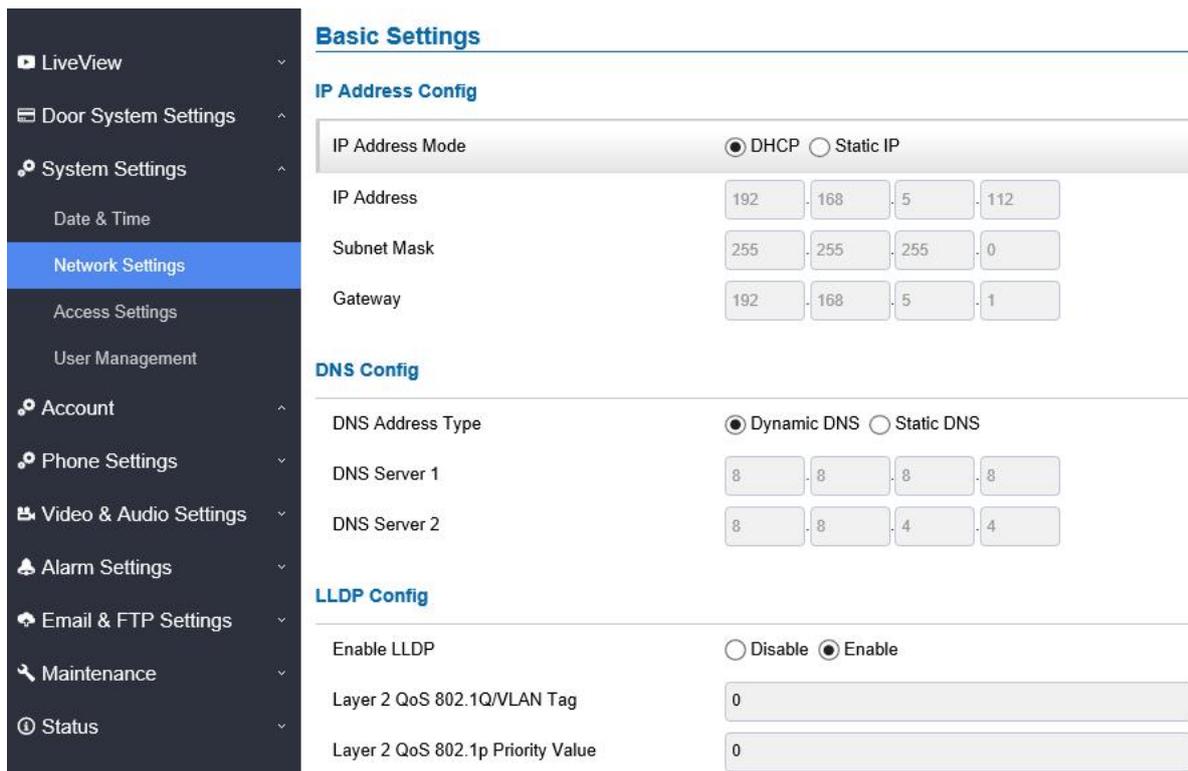


图 76: 网络设置页面

IP 地址类型	可以设置 DHCP 或静态 IP. 默认是 DHCP. (建议使用静态 IP)
IP 地址	配置静态 IP 地址.
子网掩码	配置子网掩码
网关	配置网关
DNS 类型	选择 DNS 类型: 动态 DNS 或静态 DNS。
DNS 服务器 1	输入 DNS 服务器 1 的 IP 地址
DNS 服务器 2	输入 DNS 服务器 2 的 IP 地址
启用 LLDP	控制 LLDP (Link Layer Discovery Protocol)服务。默认设置为“启用”
Layer 2 QoS 802.1Q/VLAN Tag	设置二层 QoS802.1Q VLAN Tag。默认值是 0.
Layer 2 QoS 802.1p 优先级	设置第二层 QoS802.1p 的优先级。默认值是 0.

注意

- 如果 GDS371x 位于 SOHO (Small Office Home Office)路由器的后面, 并为远程访问配置了端口转发, 则应使用静态 IP, 以避免路由器重启后 IP 地址更改。
- 对于远程访问, tcp 端口大于 5000 建议使用端口转发 HTTP。因为有些 ISP 会阻塞入站流量

的 80 端口。例如，将默认 HTTP 端口从 80 更改为 8088，以确保 TCP 端口不会被阻塞。

- 除 HTTP 端口外，还需要通过端口转发配置 RTSP 端口，使远端可以查看视频流。
- 如果默认的 TCP 端口 80 更改为“A”，则 RTSP 端口应为“2000+A”（由默认的 TCP 554 更改）。路由器的 TCP 端口“A”和“2000+A”都应该配置为端口转发。例如，HTTP 端口更改为 8088 时，RTSP 端口应设置为 10088，TCP 端口 8088 和 10088 都应配置为端口转发，以实现远程 GDS3710 访问：web 门户端口为 8088，视频流端口为 10088。

OpenVPN® 设置

此界面允许 GDS 配置 OpenVPN。

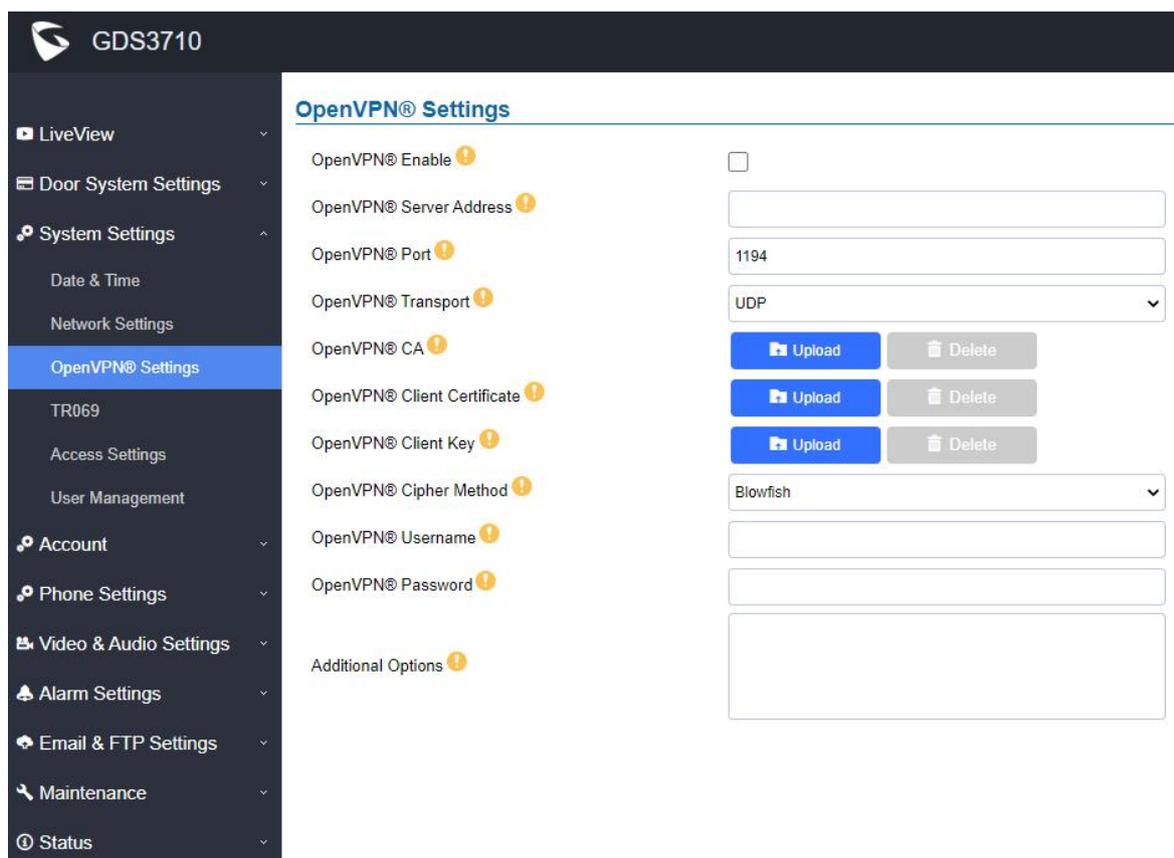


图 77: OpenVPN 设置界面

启用 OpenVPN®

启用/禁用 OpenVPN®功能，并需要用户去访问 OpenVPN®服务器。
 注意:要使用 OpenVPN®功能，用户必须启用 OpenVPN®并配置与 OpenVPN®相关的所有设置，包括服务器地址、端口、OpenVPN®CA、证书和密钥。此外，用户还必须将 SIP 帐户设置为使

	用“VPN”进行“NAT Traversal”(在帐户下)
OpenVPN® 服务器地址	配置访问 OpenVPN® server 的 URL/IP。
OpenVPN® 端口	设置 OpenVPN® server 的端口，默认为 1194。
OpenVPN® 传输方式	设置 OpenVPN®的传输方式为 UDP 或 TCP 默认是 TCP。
OpenVPN® CA	OpenVPN®服务器出于身份验证目的所需的 OpenVPN®CA 文件 (CA.crt)。按“上传”将相应的文件上传到设备。
OpenVPN® 客户端证书	OpenVPN®CA 文件(CA .crt)，用于 OpenVPN®服务器进行身份验证。点击“上传”，将相应的文件上传到设备上。
OpenVPN® 客户端密钥	OpenVPN®CA 文件(CA .crt)，用于 OpenVPN®服务器进行身份验证。点击“上传”，将相应的文件上传到设备上。
OpenVPN® 加密方式	OpenVPN®的密码方法必须与 OpenVPN®服务器使用的密码方法相同。支持的方法有:Blowfish、AES-128、AES-256 和 Triple-DES。
OpenVPN® 用户名	配置 OpenVPN®认证用户名(可选)。
OpenVPN® 密码	配置 OpenVPN®认证密码(可选)。
附加参数	附加到 OpenVPN®配置文件中的其他选项，用分号分隔。例如， <code>comp -lzo no;auth SHA256</code> 注意:请谨慎使用此选项。确保这些选项可以被 OpenVPN®识别，不要不必要地覆盖上面的其他配置。

SNMP 设置

此页面可配置 GDS371x SNMP 参数

选项	描述
启用 SNMP	启用/禁用 SNMP 功能 默认是 "禁用".
版本	选择 SNMP 版本: Version 1、Version 2c、Version 3 默认是 "Version 3"

SNMP 端口	设置 SNMP 端口 默认是 "161".
SNMPv1/v2c Community	填写 SNMPv1/v2c Community.
SNMP Trap 版本	选择 SNMP Trap 版本: Version 1、Version 2c、Version 3 默认是 "Version 3"
SNMP Trap IP 地址	填写 SNMP Trap IP 地址
SNMP Trap 端口	设置 SNMP Trap 端口 默认是 "162".
SNMP Trap 间隔	设置 SNMP Trap 间隔 默认是 "5".
SNMPv1/v2c Trap Community	填写 SNMPv1/v2c Trap Community。
SNMPv3 用户名	填写 SNMPv3 用户名
SNMPv3 S 安全级别	设置 SNMPv3 安全级别: noAuthUser、authUser、privUser 默认是 "noAuthUser".
SNMPv3 认证协议	选择 SNMPv3 认证协议: None、MD5、SHA 默认是 "无".
SNMPv3 私钥协议	填写 SNMPv3 私钥协议。 None、DES、AES AES128
SNMPv3 认证密钥	填写 SNMPv3 认证密钥。
SNMPv3 私钥	填写 SNMPv3 私钥。

SNMPv3 Trap 用户名	填写 SNMPv3 Trap 用户名
SNMPv3 Trap 安全级别	选择 SNMPv3 Trap 安全级别： noAuthUser、authUser、privUser 默认是 "noAuthUser"
SNMPv3 Trap 认证协议	选择 SNMPv3 Trap 认证协议： None、MD5、SHA 默认是 "无"
SNMPv3 Trap 私钥协议	选择 SNMPv3 Trap P 私钥协议： None、DES、AES AES128 默认是 "无".
SNMPv3 Trap 认证密钥	填写 SNMPv3 Trap 认证密钥
SNMPv3 Trap 私钥	填写 SNMPv3 Trap 私钥

TR-069

此页面可以配置 GDS 的 TR-069 参数。

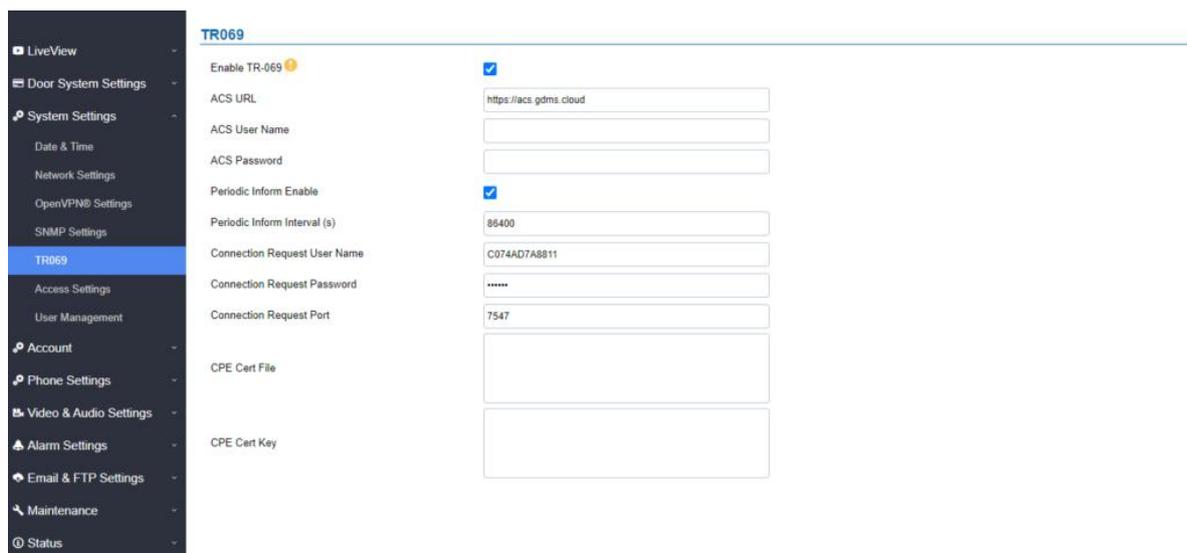


图 78: TR-069 设置界面

启用 TR-069	设置设备启用“CPE 广域网管理协议” (TR-069)。默
-----------	--------------------------------

	认设置为“否”。 注意:修改后需要重启设备才能生效。
ACS URL	TR-069 ACS 的 URL(例如 http://acs.test.com)或 IP 地址。
ACS 用户名	输入用户名进行 ACS 认证。
ACS 密码	输入密码进行 ACS 认证。
开启定时连接	定期向 ACS 发送通知报文。默认为“No”。
定时连接间隔(秒)	配置以指定的时间间隔向 ACS 发送周期性的 Inform 报文。默认设置为 86400
ACS 连接请求用户名	输入 ACS 连接设备的用户名。
ACS 连接请求密码	输入 ACS 连接设备的密码。
ACS 连接请求端口	输入 ACS 连接设备的端口。
CPE 证书	输入证书文件，用于设备通过 SSL 连接到 ACS。 注:CPE 版本已更新至 1.0.5.5
CPE 证书密钥	上传 Cert Key，用于设备通过 SSL 连接 ACS。

访问设置

此页用于配置 GDS3710 网页访问参数。

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 

图 79: 网页访问界面

Web 访问模式	设置访问 webGUI 的方式为 HTTP 或 HTTPS。
Web 访问端口	指定 Web 访问的 TCP 端口，默认为 443。 允许第三方系统集成商或开发者为用户实现相关应用。默认情况下，该功能是禁用的，并使用更安全的“Challenge+Response”模式。如果启用，用户可以发送带有正确凭证的 HTTP API 从 GDS3710 检索 MJPEG 视讯流或 JPEG 快照。
JPEG 认证模式	注： 可以通过以下 URL 检索 MJPEG 流 基于 HTML 的 http://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html 流 http(s):// admin: password@ip:端口/ jpeg /流。 通过上述方法检索的 MJPEG 流在后台运行，无法进行调优。如果用户需要更大的灵活性，他们可以使用三个可配置的视频流。
RTSP 端口	指定媒体流的 RTSP 端口，默认 TCP 端口 554。
用户登录超时时间 (分钟)	如果在这段时间内没有任何操作，GDS371x 将从 Web GUI 注销，范围在 3 到 60 之间。
用户登录最大尝试次	允许登录错误次数限制，如果登录失败次数超过该值，GDS371x

数	webGUI 将被锁定，锁定时间为“登录错误锁定时间”。
登录错误锁定时间(分钟)	指定在允许新的登录尝试之前 GDS371x 被锁定的时间。
禁止网页访问	<p>允许或拒绝对 GDS371x 的 web 访问。(启用该选项时 HTTP API 不生效)。</p> <p>注意:如果 web 和 SSH 都被禁用，GDS371x 将被阻塞，无法访问。由 ITSP 或服务提供商重新提供(通过调整相关参数)硬复位(GDS371x 必须离线并卸载才能执行此硬复位)。</p>
启用 UPnP 搜索	UPnP(或 mDNS)功能，用于本地发现。启用默认设置。
启用匿名预览视频	<p>启用后，用户可以显示来自 GDS 的摄像机流，不需要管理员用户名和密码登录，使用以下 URL:</p> <p>http(s)://GDS371x_IP:端口/ videoview.html</p> <p>用户也可以在没管理员权限的情况下使用以下 URL 检索实时快照: http(s)://IP:port/anonymous/snapshot/view.html 或 https://IP_GDS371x:Port/anonymous/snapshot/view.jpg</p> <p>通过 RTSP 检索视频流，用户可以使用以下格式:RTSP://IP_GDS371x:Port/X，其中 X=0,4,8 分别用于第 1、2、3 个流。 要检索匿名 MJPEG，用户可以使用以下 url 检索相关的 MJPEG 流: http(s)://IP:Port/anonymous/jpeg/stream=X (X=0, 1, 2, or default 3)</p> <p>例如：https://192.168.1.128/anonymous/jpeg/stream=3</p> <p>注意： 除默认值 3 外，流 0,1,2 映射到“视频设置”页面中的流 1,2,3。 除非使用默认值 3，否则所有其他值都需要在“优先视频编码”中选择“MJPEG”。</p>
启用 SSH	允许 SSH 访问远程安全配置目的(重新启动，升级…)
启用密码显示(HTTPS)	如果启用，该选项允许查看系统 PIN/密码。默认为“禁用”。
SSH 端口	SSH 端口。默认是 22。
GDSManager 配置密码	<p>用户可以在该字段设置自定义管理员密码，而不是使用 GDS371x web 管理员密码，该自定义管理员密码将是登录 GDSManager server 时使用的密码。</p> <p>默认密码为 GDS371x 的 Admin 默认随机密码。</p>
RTSP 密码	<p>此功能增强基于来自客户的现场反馈。客户要求不使用管理员密码通过第三方应用程序(如 VLC 播放器或自己的开发脚本)查看 RTSP 视频流。</p> <p>现在客户仍然可以使用管理员作为用户名，但不使用管理员密码，并配置另一个 RTSP 密码，通过自己的脚本或第三方应用程序如 VLC 媒体播放器查看直播流。</p> <p>例如，使用 VLC Media Player，如果在 GDS371x 中配置 RTSP 密</p>

码为“1234”，则使用以下命令可以获得视流:RTSP://admin:1234@192.168.11.128/4(这里显示 2ndstream 为“4”使用)

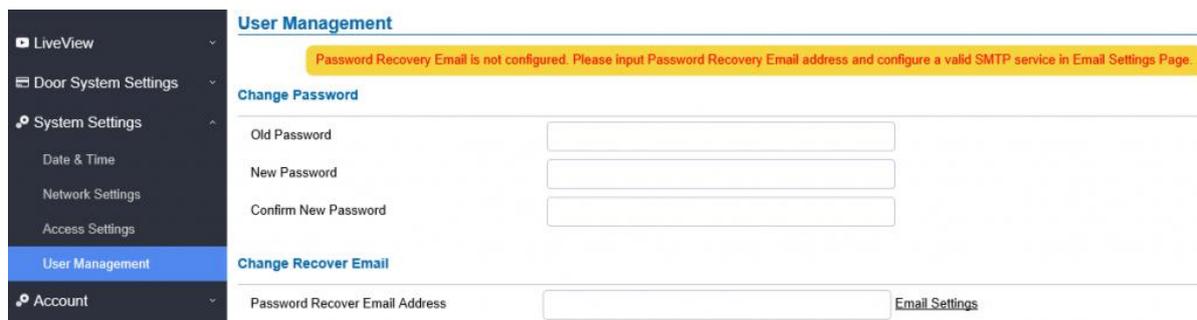
格式: RTSP://admin:rtsp_password@IP_GDS371x:Port/X (X = 0, 4, 8 对应码流 1, 2, 3)

Th 根据计算机处理能力和网络条件, 所选的带音频的实时视频流将会有有一定的延迟。

注意:
使用此功能前, 请确保环境安全。使用本功能时, 请提醒用户注意隐私。

用户管理

此页面允许用户为管理员配置密码。由于这是一款安全产品, 所以使用仅限于管理员。



The screenshot shows the 'User Management' section of a web interface. It includes a sidebar with navigation options like 'LiveView', 'Door System Settings', 'System Settings', 'Date & Time', 'Network Settings', 'Access Settings', 'User Management', and 'Account'. The main content area has a yellow warning banner: 'Password Recovery Email is not configured. Please input Password Recovery Email address and configure a valid SMTP service in Email Settings Page.' Below this, there are two sections: 'Change Password' with three input fields for 'Old Password', 'New Password', and 'Confirm New Password'; and 'Change Recover Email' with one input field for 'Password Recover Email Address' and a link to 'Email Settings'.

图 80: 用户管理界面

旧密码

修改新密码必须填写旧密码

新密码

填写新的密码

确认新密码

重新输入新密码进行验证, 必须匹配。

密码找回邮箱

强烈推荐使用此选项, 因为如果密码丢失, 您可以在配置的电子地址上恢复。
注意:请确保在“电子邮件设置”下配置 SMTP 电子邮件设置

注意

修改密码时, 用户需要设置“密码恢复邮箱”, 该邮箱必须是在“Email & FTP 设置邮箱设置”下可配置的有效邮箱账户, 以便在新 admin 密码生效前找回邮箱, 如下图所示。

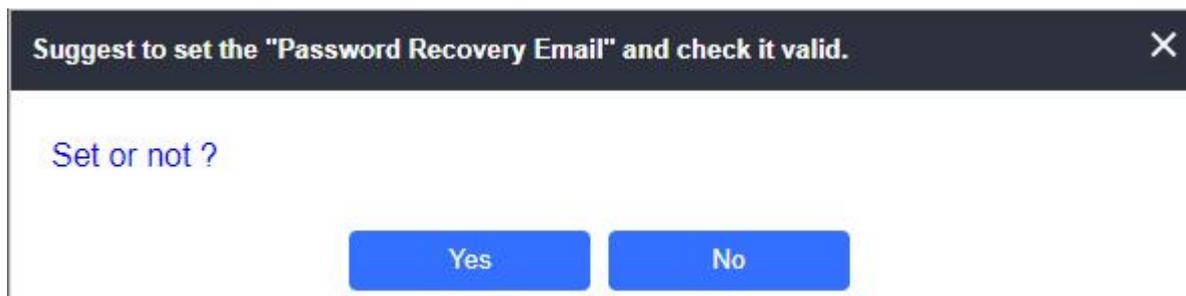


图 81: 密码找回邮箱

账号

从 1.0.5.6 版本开始，GDS371x 支持 4 个 SIP 帐号和 4 条线路，本节涵盖每个帐号的基本和高级 SIP 设置的配置。

Account 1 - 4

通过该界面，管理员可以对每个 SIP 帐号进行基本配置和高级配置。

账号 1	
SIP 基本设置	
激活账号	<input checked="" type="checkbox"/>
SIP 服务器	192.168.160.139
次要SIP服务器	
出局代理服务器	
备用出局代理服务器	
DNS模式	A Record
SIP用户ID	1010
确认用户ID	1010
密码
显示名	
TEL URI	禁用
SIP 高级设置	
注册有效期(分)	60
注册期限内重新注册等待时间(秒)	0
本地 SIP 端口	5060
SIP 传输方式	UDP
DTMF 使能	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
DTMF有效荷载类型	101

图 82: SIP 账号设置界面

SIP 基础设置	
激活账号	该帐号是否激活。默认为“是”。
SIP 服务器	从 VoIP 服务提供商或本地 IPPBX 配置 SIP 服务器的 FQDN 或 IP。
次要 SIP 服务器	从 VoIP 服务提供商或本地 IPPBX 配置备用 SIP 服务器的 FQDN 或 IP。 备用 SIP 服务器允许用户在主 SIP 服务器出现问题时使用备用 SIP 服务器确保业务可用。
出局代理服务	配置出站代理、媒体网关或会话边界控制器的 IP 地址或域名。它被 GDS 用于不同网络环境中的防火墙或 NAT 穿透。 如果检测到对称 NAT, STUN 将不起作用, 只有出站代理可以提供解决方案。
备用出局代理服务器	配置当“出局代理”注册失败时使用备用出局代理。默认情况下, 该字段为空。
DNS 模式	配置转换 SIP Server FQDN 的 DNS 模式(默认为 A Record): A 记录, SRV, NAPTR/SRV。
SIP 用户 ID	从 ITSP 配置 SIP 用户名或电话号码。 备注:支持字母、数字和特殊字符@。
认证 ID	配置 SIP 代理使用的认证 ID。
密码	S 设置 SIP 代理使用的认证密码。 注意:出于安全考虑, SIP 密码在 web 界面上会隐藏。
显示名称	允许用户在远端 SIP 设备(如果有 LCD 显示器或类似硬件)上输入显示名称, 以使用户知道在 SIP 呼叫中连接的分机或设备, 以提高可用性。
TEL URI	在下拉列表中选择“User=Phone”或“Enabled”。 如果 SIP 帐号已经分配了 PSTN 电话号码, 该字段需要设置为“User=Phone”。然后, “User=Phone”参数将附加到 SIP 请求中的 request-line 和“to”报头, 以指示 E.164 号码。如果设置为“Enable”, 在 SIP 请求中将使用“Tel:”而不是“SIP:”。默认设置为“禁用”。

SIP 高级设置	
注册有效期 (分)	设置注册过期时间。 默认为 60 分钟。有效范围为 1 ~ 64800 分钟。
注册期限内 重新注册等 待时间(秒)	指定在注册过期之前 GDS371x 发送重新注册请求的时间频率(秒)。缺省值为 0。取值范围是 0 ~ 64800 秒。
本地 SIP 端 口	设置本地 SIP 端口。帐号 1 默认为 5060，帐号 2 默认为 5062，帐号 3 默认为 5064，帐号 4 默认为 5066。
SIP 传输方 式	选择 SIP 传输协议。UDP, TCP 或 TCP/TLS。默认设置为 UDP。
码流	选择从该 SIP 帐号发起呼叫时 GDS371x 使用的视频流。默认为流 2
DTMF	指定传输 DTMF 数字的机制。支持 2 种模式:RFC2833 用 RTP 报文发送 DTMF。用户可以通过 RTP 包查看发送的 dtmf 和按下的数字。SIP INFO 使用 SIP INFO 承载 DTMF。默认设置为“RFC2833”
DTMF 有效 荷载类型	使用 RFC2833 为 DTMF 配置有效负载类型。缺省值为 101。范围:96 ~ 127。
重启时注销 注册	允许 GDS 重启时清除 SIP 用户注册信息。SIP REGISTER 消息将包含“Expires: 0”以解除连接绑定。
NAT 检测	<p>该参数用于配置是否激活 NAT 穿透机制。用户可以从 No、STUN、Keep-alive、UPnP、Auto 中选择机制。默认设置为“否”。</p> <p>如果设置为“STUN”，并且配置了 STUN 服务器，则 GDS 会按照 STUN 服务器进行路由。如果 NAT 类型为 Full Cone、Restricted Cone 或 port - Restricted Cone，则单元将尝试在所有 SIP&SDP 消息中使用公共 IP 地址和端口号。</p> <p>如果配置为 keep -alive, GDS 会定期向 SIP 服务器发送空 SDP 报文以保持 NAT 端口开放。如果使用出站代理，则配置为“No”。如果检测到的 NAT 是对称 NAT，则“STUN”不能使用。如果防火墙和防火墙后的 SIP 设备都能使用 UPNP，则可以设置为“UPNP”。双方将协商使用哪个端口允许 SIP 通过。</p>

启用 SRTP	请根据下拉菜单选择是否启用 SRTP 模式。默认设置为“禁用”，其他两种模式为“启用但不强制”和“启用并强制”。
特殊模式	配置 GDS 设置，以满足不同厂商的服务器需求。用户可以选择 Standard, Broadsoft 或 Telefonica Spain。系统默认设置为“Standard”。
出局代理模式	In route:出局代理 FQDN 位于路由报头中。用于 SIP 分机通知 SIP 服务器该设备位于 NAT/防火墙之后，始终发送到 SIP 消息将始终发送到出站代理。不在路由中:从 SIP 请求中删除 route 头。
启用 RTCP	此选项允许第三方服务提供商或云解决方案通过使用相关的 SIP 呼叫来监控 GDS371x 的运行状态。默认情况下，它是禁用的。用户可以选择 RTCP 或 RTCP-xr。
H.264 有效载荷类型	H.264 有效载荷类型现在可以配置为与第三方视频电话兼容，以及其他高级 SIP 设置，以简化系统集成过程。默认值是 99。
仅允许来自 SIP 服务器的 SIP 请求	当设置为“Yes”时，将检查传入 SIP 消息中请求 URL 的 SIP 地址。如果与该帐号的 SIP 服务器地址不匹配，则呼叫将被拒绝。默认设置是禁用的。
在 User-Agent 添加 MAC	此选项与 3CX 一起使用，因此 GDS37xx 可以与 3CX 自动配置兼容。该选项将 MAC 地址添加到 SIP 报头中的 User-Agent 中。No:关闭该选项，对所有 SIP 是:SIP 消息将始终表现为 User-Agent，除 REGISTER 消息外，SIP 消息将始终表现为 User-Agent
TLS 使用的 SIP URI 格式	此选项允许 GDS371x 作为 SIP 客户端与 Cisco WebEX 服务器一起工作。SIP 和 SIPS 两种模式。
支持 SIP 实例 ID	启用后，GDS371x 将作为 SIP 客户端与 Cisco WebEx 服务器一起工作。
语音编码配置	
选择 1	按优先级顺序选择第一个音频编解码器(最低优先级为最高优先级)。支持的编解码器有 PCMU、PCMA、G.722 和 G.729A/B。

选择 2	按优先级顺序选择第二个音频编解码器(最低优先级为最高优先级)。支持的编解码器有 PCMU、PCMA、G.722 和 G.729A/B。
选择 3	按优先级顺序选择第三个音频编解码器(最低优先级为最高优先级)。支持的编解码器有 PCMU、PCMA、G.722 和 G.729A/B。 .
选择 4	按优先级顺序选择第四个音频编解码器(最低优先级为最高优先级)。支持的编解码器有 PCMU、PCMA、G.722 和 G.729A/B。
编解码协商 优先级	选择协商优先级，无论是呼叫方还是被呼叫方，默认设置为 Callee。
语音帧/TX	配置每个报文传输的语音帧数。在配置时，应该注意 SDP 的“ptime”值将随着这里的不同配置而改变。这个值与使用的编解码器和有效负载调用期间传输的实际帧有关。对于最终用户，建议使用默认设置，不正确的设置可能会影响音频质量。缺省值为 2。取值范围为 1~64。

电话设置

话机设置允许用户配置 GDS371x 话机设置和所有 SIP 帐号的白名单。

电话设置

通过此界面，您可以对 GDS371x 话机进行配置。

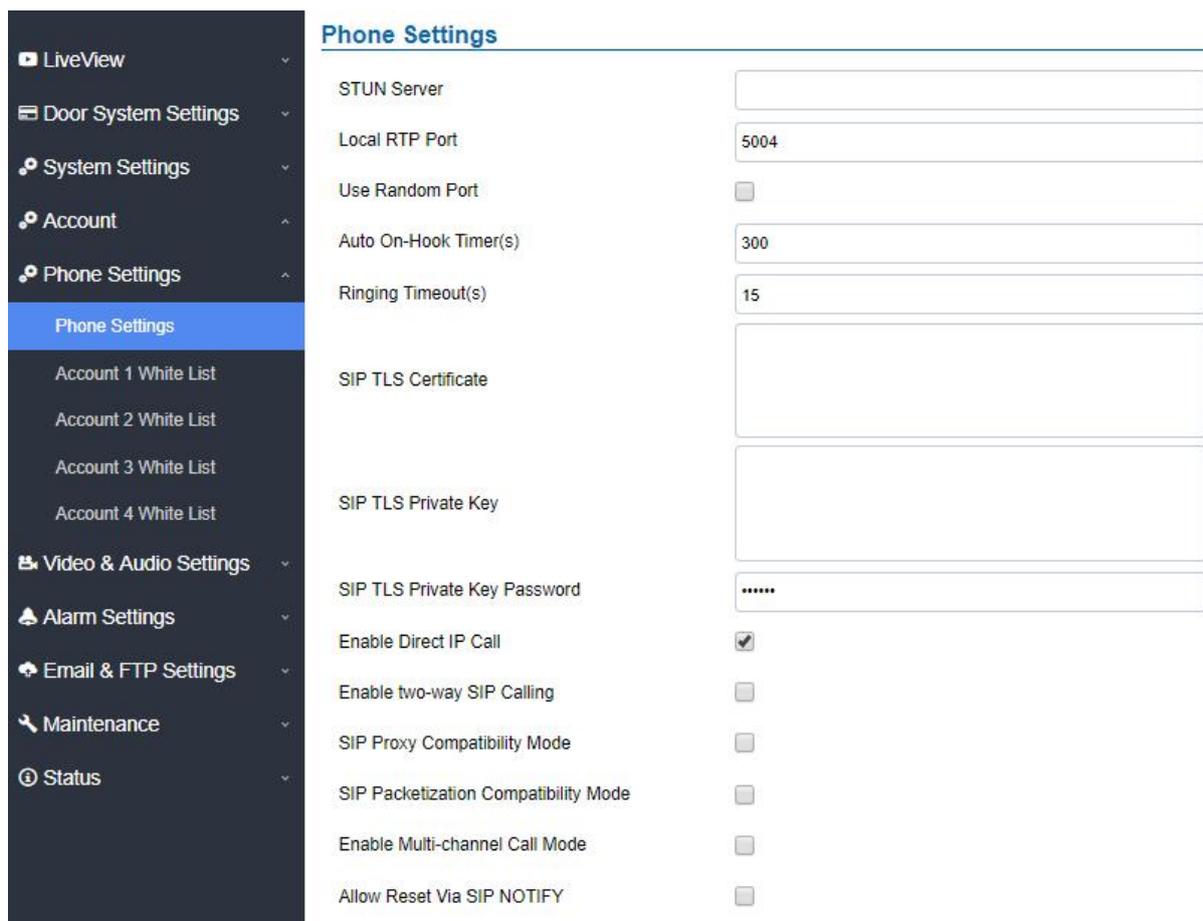


图 83: 电话设置界面

STUN 服务器	配置 STUN 服务器的 FQDN 或 IP。如果设备位于非对称路由器的后面，STUN 服务器可以帮助穿透和解决 NAT 问题。
本地 RTP 端口	为媒体设置本地 RTP 端口。默认值为 5004。范围 1024~65400
使用随机端口	强制 GDS 对 SIP 和 RTP 消息使用随机端口。当多个单元处于相同的全锥 NAT 后时，这通常是必要的。默认设置为“禁用”。 备注:该参数必须设置为“禁用”，IP 直呼才能正常工作。
主动挂断计时(秒)	配置 SIP 通话自动断开定时器(单位:秒)。默认值为 300。范围 0~65535。
振铃超时时间(秒)	指定振铃超时时间，当超过此时间后被叫没有应答时，GDS 将挂断本次呼叫。取值范围为 0s ~ 90s。默认情况下;它是“30”秒。
DNS 缓存刷新时间(分)	配置 DNS 缓存过期时间，默认值为 30，范围为 1 ~ 1440
DNS 缓存保存时间(分)	配置 DNS 缓存过期时间，默认值为 30，范围为 1 ~ 1440
SIP TLS 认证	在这里输入 TLS 证书进行加密。
SIP TLS 私钥	此处输入私钥用于 TLS 安全保护。

SIP TLS 私钥密码	SIP TLS 私钥密码。
启用 IP 直接呼叫	接受点对点 IP 呼叫(仅在 UDP 上)没有 SIP 服务器。默认为“启用”。
启用语音报警模式	允许用户开启/关闭 SIP 通话中按门铃触发的报警声音
SIP 服务器兼容模式	支持更多的代理兼容带宽成本，SIP 呼叫将发送音频无论什么。
SIP 打包兼容模式	启用后，GDS 在 SDP 中将有“packeization -mode = 0”。当 GDS 与仅接受此值来解码 RTP 的传统视频电话交互时，这是必需的。
启用多路呼叫模式	<p>该功能允许设备同时接收多个呼叫，其中一个呼叫处于活动状态，其他呼叫处于保持状态(最多 4 个呼叫)。第一次呼叫蓝色 LED 灯将点亮键盘数字“1”，第二次呼叫将点亮键盘数字“2”，依此类推。</p> <p>保持呼叫将有相关数字闪烁，而主动呼叫将有数字蓝色 LED 固态亮起。按闪烁的数字切换通话。</p>
允许通过 SIP 通知重置	<p>允许通过 SIP 通知直接对设备进行出厂复位。如果“允许通过 SIP 通知重置”勾选，那么一旦 GDS3710 接收到 SIP 服务器发送的带有 Event: Reset 的 SIP NOTIFY, GDS3710 将在认证后进行出厂重置。</p> <p>此身份验证可以使用： 如果 GDS3710 上没有配置 SIP 帐号，则为 admin 密码。 如果在 GDS371x 上配置了 SIP 帐号，则为“SIP User ID”和“Password”。默认为未选中(已禁用)。</p>

账号[1-4] 白名单

此页面允许用户配置每个帐号的白名单，白名单是可以呼叫 GDS371x 的电话号码或分机号列表。

(从白名单中的话机呼出，自动接听，其他所有呼入话机将被拦截)，每个 SIP 帐号最多可配置 200 个白号码。

此外，除了与活动卡相关联的号码，以及“门铃按下时被叫号码”设置上的号码外，所有白名单号码都可以使用相应的 PIN 码远程开门。

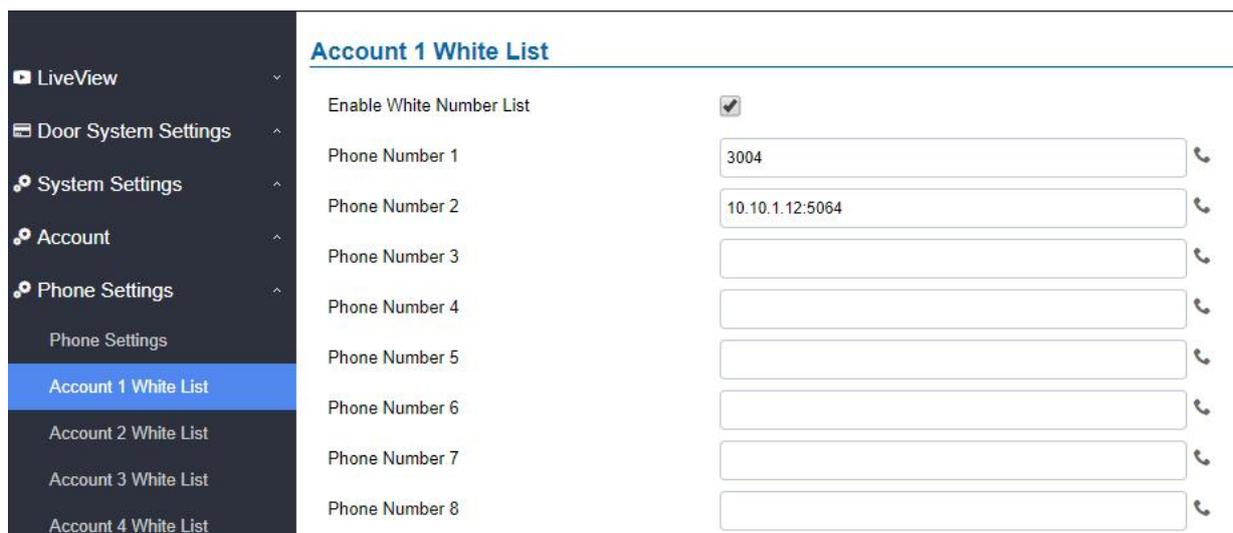


图 84: 白名单页面

下表给出了选项的简要概述:

启用白名单列表	启用白名单功能
电话号码 1 -200	添加一个新的号码到白名单

表 11: 白名单

点击拨打

GDS371x 允许用户使用“点击拨号”功能来管理他们的呼叫，该功能允许用户使用 Web GUI 通过按“点击拨号”按钮来发起呼叫，以访问如下截图所示的呼叫菜单。

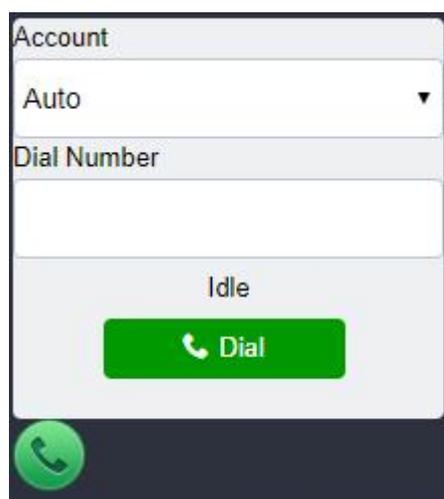


图 85: 点击拨打

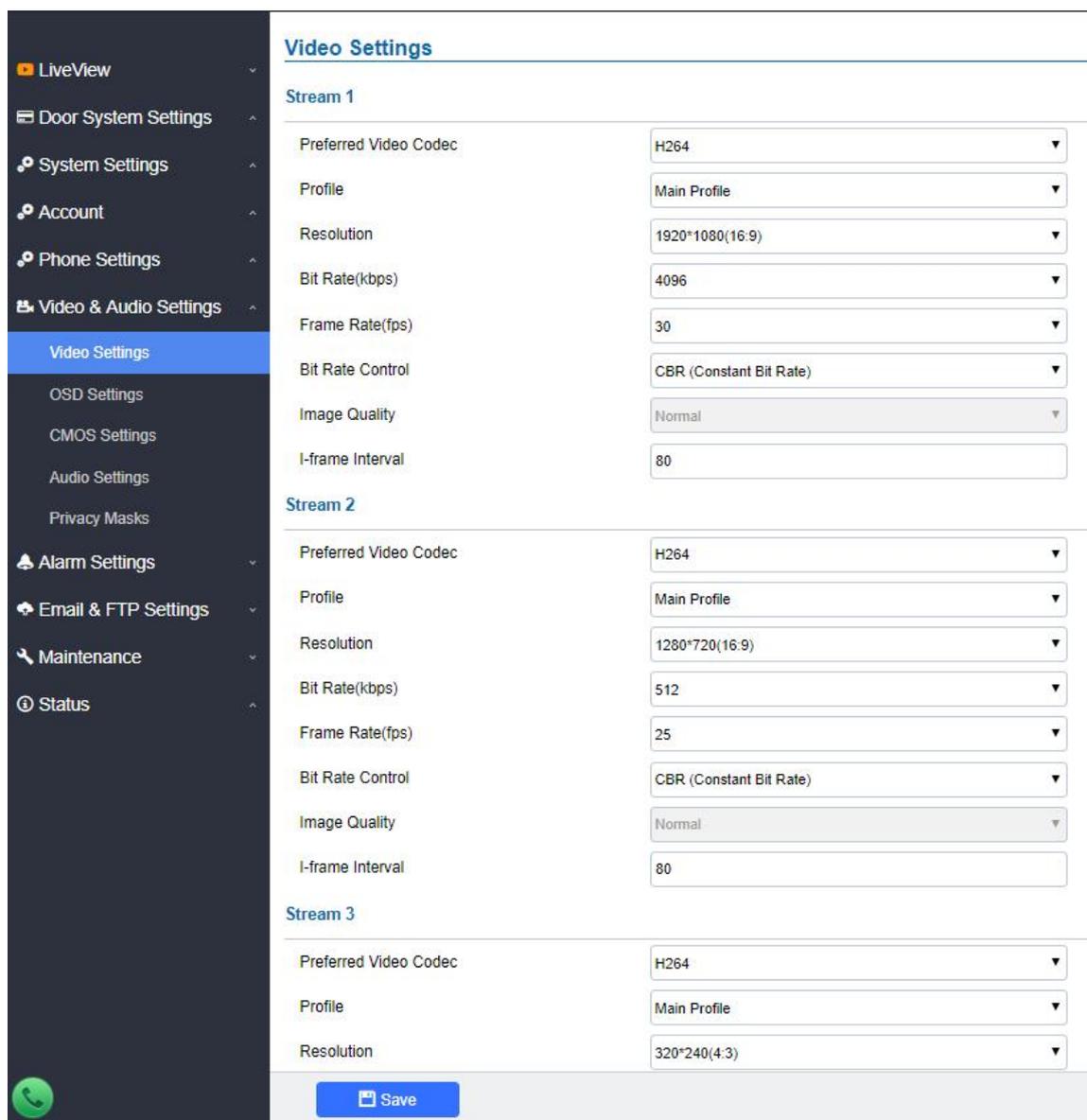
注意

只有白名单号码才能在呼叫 GDS3710 时使用 PIN 码远程开门

音视频设置

音频和视频设置允许用户配置视频/音频编解码器、视频分辨率、CMOS 设置和音频相关设置。

视频设置



Video Settings	
Stream 1	
Preferred Video Codec	H264
Profile	Main Profile
Resolution	1920*1080(16:9)
Bit Rate(kbps)	4096
Frame Rate(fps)	30
Bit Rate Control	CBR (Constant Bit Rate)
Image Quality	Normal
I-frame Interval	80
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	H264
Profile	Main Profile
Resolution	320*240(4:3)

图 86: 视频设置界面

视频编码 (码流 1)

选择视频编解码器, 支持的编解码器为 H.264 和 MJPEG。默认设置为 H.264。

Profile	选择 H.264 配置文件。有三个配置文件:基线、主配置文件和高配置文件。默认设置为“Main Profile”。
分辨率	指定视频图像使用的分辨率(以像素为单位), 1080p 或 720p。
码率 (kbps)	选择使用的视频比特率或带宽。
最高帧速率(fps)	选择使用的最大帧速率(如果使用大帧, 则使用更多数据)。
码率控制	选择固定比特率或可变比特率。
图像质量	选择使用可变比特率时使用的图像质量。
I 帧间隔	配置 i 帧间隔(建议为帧速率的 2~3 倍)。
视频编码 (码流 2)	选择视频编解码器, 支持的编解码器为 H.264 和 MJPEG。默认设置为 H.264。
Profile	选择 H.264 配置文件。有三个配置文件:基线、主配置文件和高配置文件。默认设置为“Main Profile”。
分辨率	指定视频图像使用的分辨率(以像素为单位), 1080p 或 720p。
码率 (kbps)	选择使用的视频比特率或带宽。
最高帧速率(fps)	选择使用的最大帧速率(如果使用大帧, 则使用更多数据)。
码率控制	选择固定比特率或可变比特率。
图像质量	选择使用可变比特率时使用的图像质量。
I 帧间隔	配置 i 帧间隔(建议为帧速率的 2~3 倍)。
视频编码(码流 3)	选择视频编解码器, 支持的编解码器为 H.264 和 MJPEG。默认设置为 H.264。
Profile	选择 H.264 配置文件。有三个配置文件:基线、主配置文件和高配置文件。默认设置为“Main Profile”。
分辨率	指定视频图像使用的分辨率(以像素为单位), 1080p 或 720p。
码率 (kbps)	选择使用的视频比特率或带宽。
最高帧速率(fps)	选择使用的最大帧速率(如果使用大帧, 则使用更多数据)。
码率控制	选择固定比特率或可变比特率。
图像质量	选择使用可变比特率时使用的图像质量。
I 帧间隔	配置 i 帧间隔(建议为帧速率的 2~3 倍)。

注意

- 如需透过互联网浏览 GDS371x, 建议使用 h.264。

- 有关 H.264 的 BP、MP 和 HP 的定义，请参阅: H.264 Profile
- 如果选择 MJPEG，将帧率降低到最小值以节省带宽并获得更好的图像。
- GS GDS371x 提供三种视频流，用户可以灵活使用。例如，高分辨率流用于本地录制，另一种低分辨率或高分辨率用于 SIP 视频电话呼叫或远程智能手机监控应用，或反之亦然，取决于应用场景。
- 在安装前使用下面的链接计算带宽和存储：

<http://www.grandstream.com/support/tools/bandwidth-storage-calc>

检索视频流

- 用户可使用以下格式以 RTSP 方式检索视频流：

rtsp://admin:password@IP_GDS3710:Port/X，其中 X=0,4,8 分别用于第 1，第 2，第 3 个流

- 要通过 http 检索 MJPEG 视频流，用户可以使用以下格式：[http\(s\)://admin:password@IP:端口/jpeg/流=X](http(s)://admin:password@IP:端口/jpeg/流=X) (X=流通道 0,1,2)

重要提示

- MJPEG 是未压缩的视频，它会消耗大量的带宽和硬件资源，建议在使用它的同时考虑到它可能会降低网络和设备的速度。

OSD 设置

“OSD 设置(屏幕显示)”可在视频屏幕上显示时间和文本。

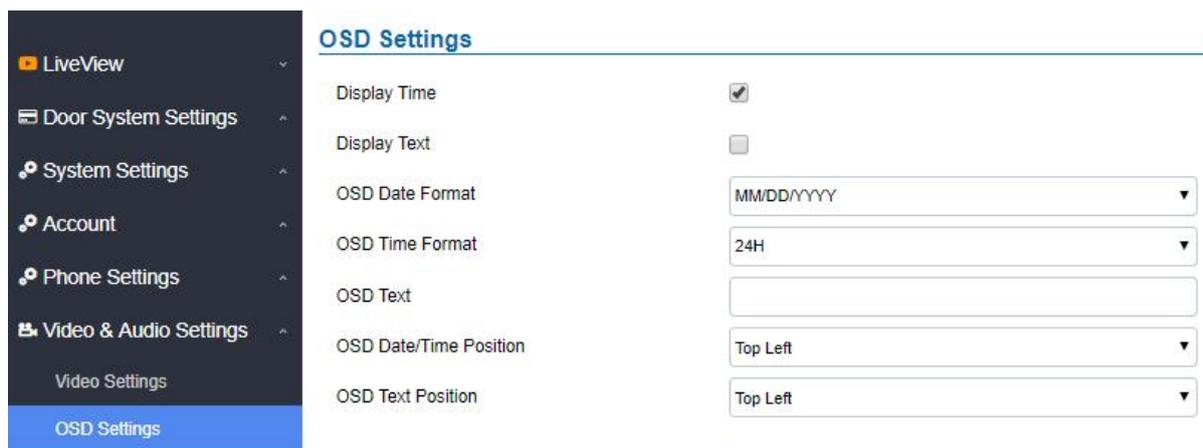


图 87: OSD 设置界面

显示时间	选中后，视频图像内将显示时间。
显示文本	选中后，在“OSD 文本”上输入的文本将显示在视频图像上。
OSD 日期格式	OSD 日期格式，根据用户喜好选择。
OSD 时间格式	OSD 时间格式，根据用户喜好选择。
OSD 文本	输入文本(以识别 GDS3710)，它将显示在屏幕上。最大长度为 32。
OSD 日期/时间位置	在屏幕上显示日期/时间位置
OSD 文本位置	显示文本在屏幕上的位置。

CMOS 设置

本页面针对不同场景配置 CMOS 参数。

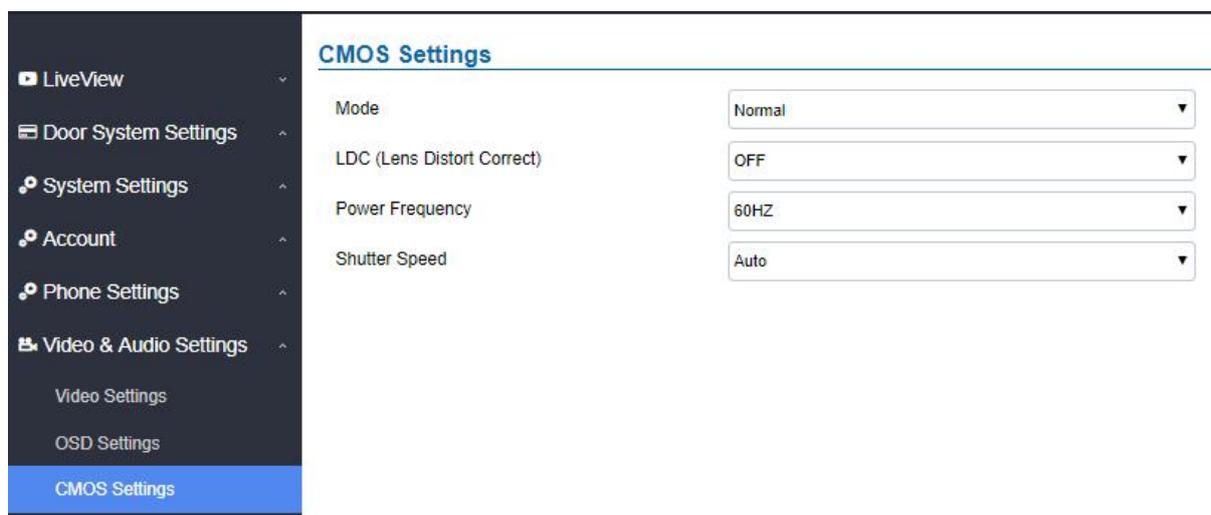


图 88: CMOS 设置界面

模式	根据不同的光照情况，下拉选择“正常、低光、WDR”。默认的“正常”。
LDC	默认的“关闭”。当“ON”时，显示将采取正常形状，但将失去位于原始视图角落的一些细节。
LDC 比率	选择“LDC Ratio”。可用选项:0.7;0.8;0.9;1.0;1.1;1.2;1.3。缺省值为1.0
电源频率	选择频率功率。50Hz 或 60Hz。
快门速度	定义在截屏时，相机快门或暴露在光线下的时间。

表 12: CMOS 设置

音频设置

通过此界面，用户可以配置音频设置。

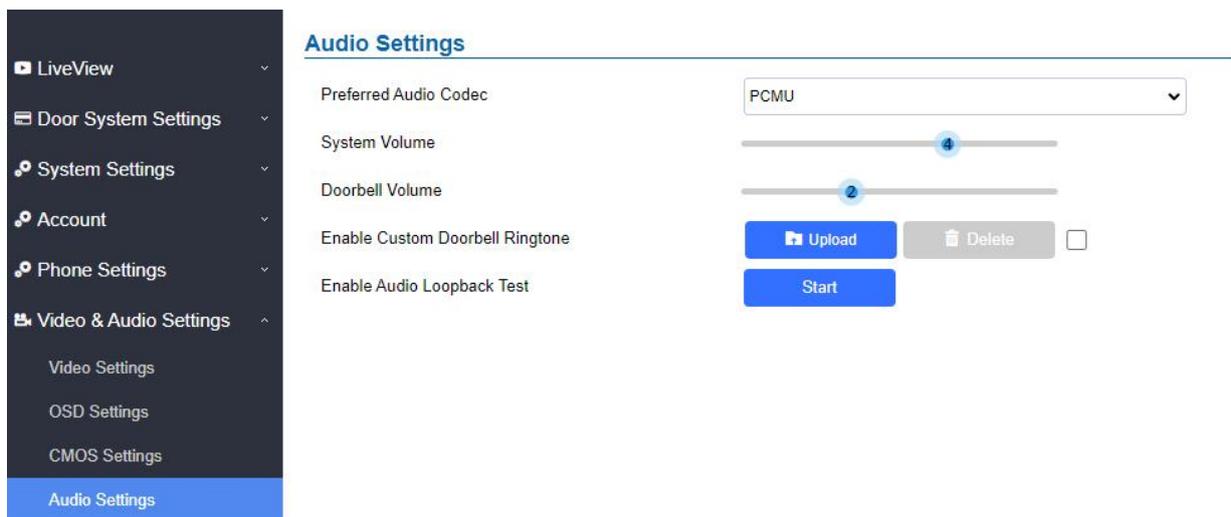


图 89: 音频设置界面

音频编码	配置音频编解码。三种编解码器可用:支持 PCMU、PCMA 和 G.722。
系统音量	调整连接的扬声器音量
门铃音量	调节门铃音量。
启用自定义门铃音	用户可以勾选此选项，以便使用自定义门铃铃声。关闭该选项时，使用“默认铃声”。
启用音频回环测试	启用时，表示设备已准备好进行音频环回测试。请记得在测试后禁用此模式。 注意:OQA Speaker 测试已经从固件版本 1.0.11.23 开始优化

表 13: 音频设置

- 点击  去更新铃音文件，然后点击  。
- 点击  删除已存在的自定义铃声。
- 支持上传 WAV、PCM 音频文件(大小<= 600K)。格式限制如下:

WAV:

1. 采样率:8k 或 16k。
2. 通道:单通道或双通道。

PCM:

1. 采样率: 8K.
- 2.通道: 双通道

注:不接受空音频文件。

隐私遮挡

在本界面中，用户最多可以配置 4 个不同区域的隐私遮挡，通过选择需要设置隐私遮挡的区域，如下图所示。

启用隐私遮挡后，相关区域的视频将被黑色屏蔽，该掩码内不显示任何视频。

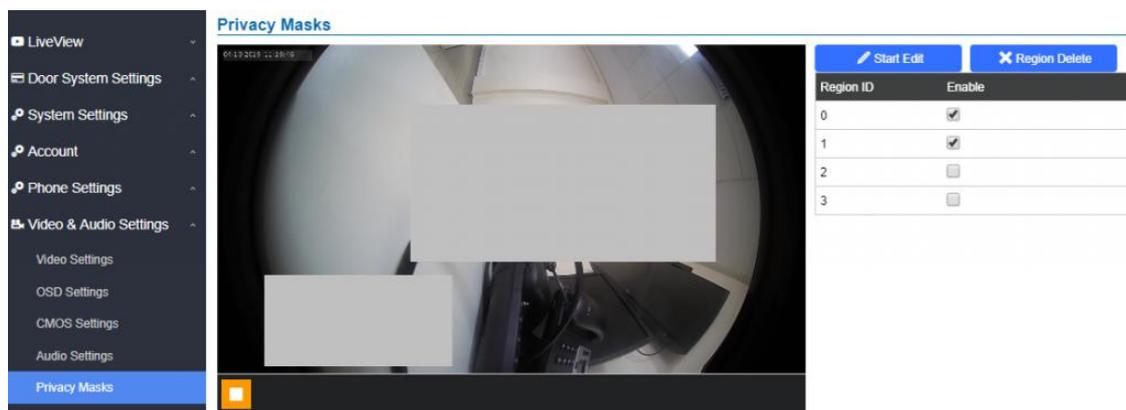


图 90：隐私遮挡配置界面

报警设置

通过此界面，您可以配置告警计划和告警动作。

A 报警事件配置

该页允许用户配置 GDS371x 事件，以在预定义的时间表内触发程序化的操作。

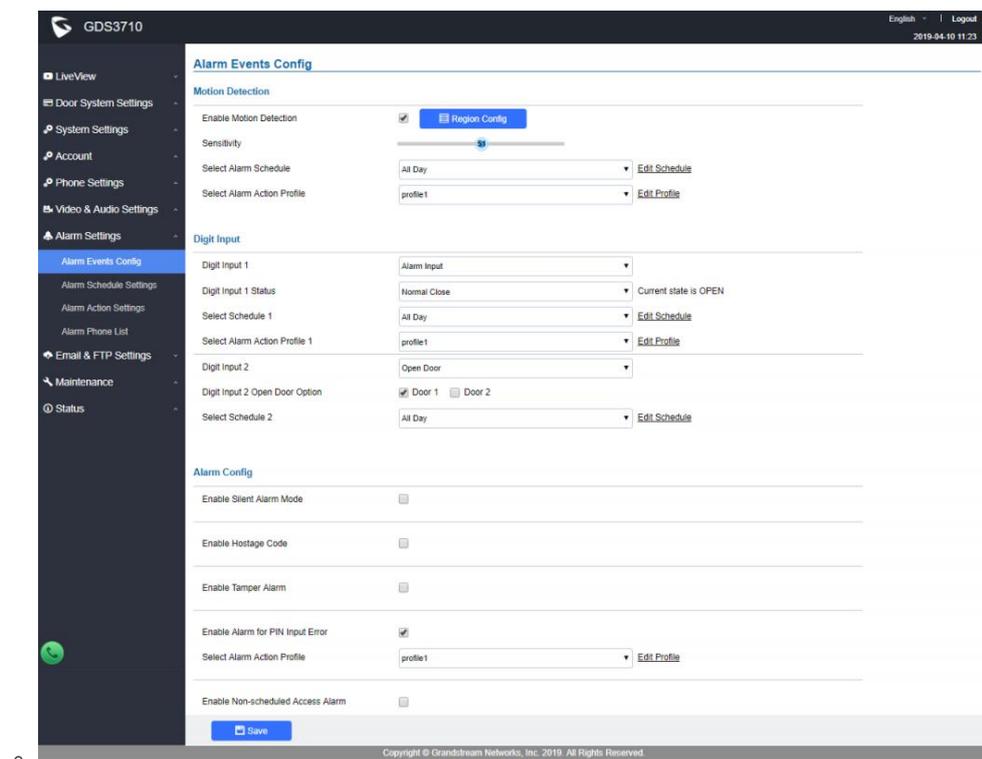


图 91: 事件配置界面

报警可由运动检测或 GDS371x 输入触发。

移动侦测

用户可以通过运动检测选择特定区域触发警报。

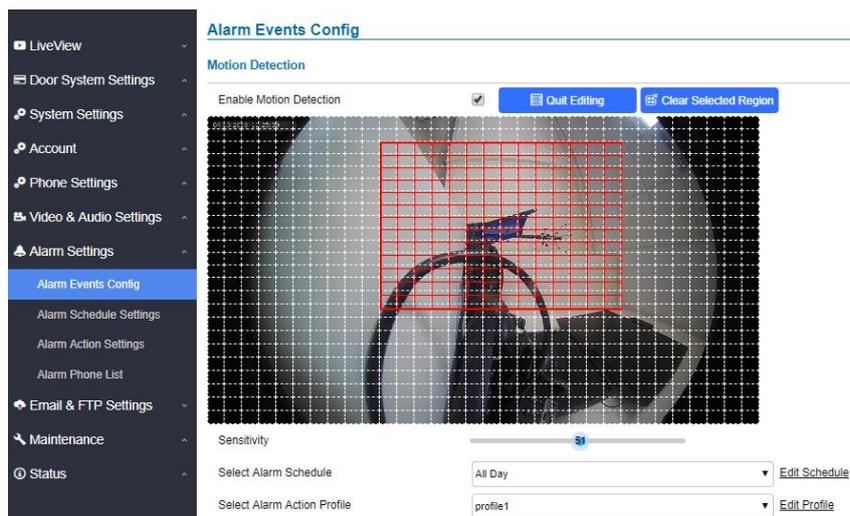


图 92: 配置界面

启用移动侦测报警

开启移动侦测功能

区域配置

配置移动侦测区域。

退出编辑

退出移动侦测区域配置菜单。

清除已选择的编辑区域

在屏幕上选择一个区域，然后点击“清除”删除该区域。

灵敏度

指定区域灵敏度(0-100%之间的值)。

选择报警日程

设置告警时间计划。

选择报警联动方案

选择已编程的告警动作配置文件。

表 14: 移动侦测

数字输入

Digit Input

Digit Input 1	Alarm Input	
Digit Input 1 Status	Normal Close	Current state is OPEN
Select Schedule 1	All Day	Edit Schedule
Select Alarm Action Profile 1	profile1	Edit Profile
Digit Input 2	Open Door	
Digit Input 2 Open Door Option	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2	
Select Schedule 2	All Day	Edit Schedule

图 93: 数字输入

选择“输入法”(告警输入或“门开”)。默认禁用。

数字输入端口有 3 种工作模式:

1. 报警输入:连接传感器触发报警。
2. 开门:连接开关从里面开门。
3. 异常门控制:当设备被篡改以异常打开门时,这是 GDS37xx 的主要安全增强。请检查门开启异常区段的警报器警报。

数字输入 1

	如果数字输入口连接交换机，在断电、设备开机或固件升级期间，数字输入口不能工作。
数字输入 1 开门选项	当“数字输入”设置为“开门”时，当告警 IN 1 触发时，用户可以选择受影响的门。
数字输入 1 状态	若设置为“常开”：当“数字输入状态”由“关闭”切换为“打开”时，将触发已配置的告警。 若设置为“正常关闭”：当“数字输入状态”由“打开”切换到“关闭”时，将触发已配置的告警。 默认情况下，“输入数字 1 状态”为“禁用”。
选择日程 1	选择预定义的告警时间段。选择“Profile 1”的预定义告警动作。
选择“告警动作配置文件 1”	选择“Profile 1”的预定义告警动作。
数字输入 2	选择“输入法”（告警输入或“门开”）。默认禁用。 数字输入端口有 2 种工作模式： 1. 报警输入：连接各种传感器触发报警。 2. 开门：连接开关从里面开门。 如果数字输入口连接交换机，在断电、设备开机或固件升级期间，数字输入口不能工作。
数字输入 2 开门选项	当“数字输入”设置为“开门”时，当告警 IN 2 触发时，用户可以选择受影响的门。
数字输入 2 状态	若设置为“常开”：当“数字输入状态”由“关闭”切换为“打开”时触发该告警。 若设置为“常闭”：当“数字输入状态”由“打开”切换到“关闭”时，将触发已配置的告警。 默认情况下，“输入数字 2 状态”为“禁用”。
选择日程 2	选择预定义的告警时间段。
选择“告警动作配置文件 2”	选择 Profile 2 的预定义告警动作。
报警输出持续时间(秒)	选择告警输出时间：1/2/3/4/5/10/15/20/25/30 秒。当 ALMOUT1 功能设置为“开门”时，该选项将被隐藏。 注意：此配置仅适用于 GDS3710 型号。

数字输入

启用静默报警模式

如果静音报警模式启用，GDS371x 将禁用告警声音和背景光为指定的报警类型(数字输入，运动检测…)当他们被触发。

注意

此选项仅影响警报声光，其他操作仍将应用。

注意

在已触发的报警呼叫中，可以通过配置静音报警模式关闭警报器的声音。

启用静音报警模式	启用/禁用报警模式
静音报警选项	当启用静音报警模式时，用户可以指定将静音模式应用于哪些报警选项。 可用的选项有:数字输入，移动侦测，防拆报警和密码错误。

表 15: 静音报警

挟持密码

注意

该配置项仅 GDS3710 支持

挟持密码可在危急情况下使用，例如绑架或紧急情况，用户需要输入以下顺序来触发挟持密码模式设置的动作：“*挟持密码#”。

启用挟持密码	启用/关闭挟持密码
挟持密码	配置密码
选择报警联动方案	选择在 GDS3710 键盘上输入挟持密码时要采取的报警动作。注意：在此模式下不会触发声音警报。

表 16: 挟持密码报警

防拆报警

防拆报警是防黑客从硬件水平攻击。选中此选项时，如果 GDS371x 从安装板上移除，将触发配置的报警操作。在 GDS371x 上有一个嵌入式机制，允许它检测何时被移除。

启用防拆报警	当激活此模式时，GDS371x 将保持报警，直到报警解除。
选择报警联动方案	为篡改告警模式选择要触发的告警动作类型。

表 17: 防拆报警

启用键盘多次输入错误报警

注意

此配置仅适用于 GDS3710 型号。

启用键盘多次输入错误报警

启用键盘多次输入错误报警, GDS3710 将在每 5 次错误尝试时触发报警动作。

选择报警联动方案

选择错误 5 次触发的告警动作类型。

表 18: 键盘多次输入错误报警

超出日程表访问报警

注意

此配置仅适用于 GDS3710 型号。

启用超出日程表访问报警

当启用此功能时, 当超出允许配置的时间表进入门时, GDS3710 将触发警报给相关管理员。

选择报警联动方案

选择需要触发的告警动作类型

表 19: 启用超出日程表访问报警

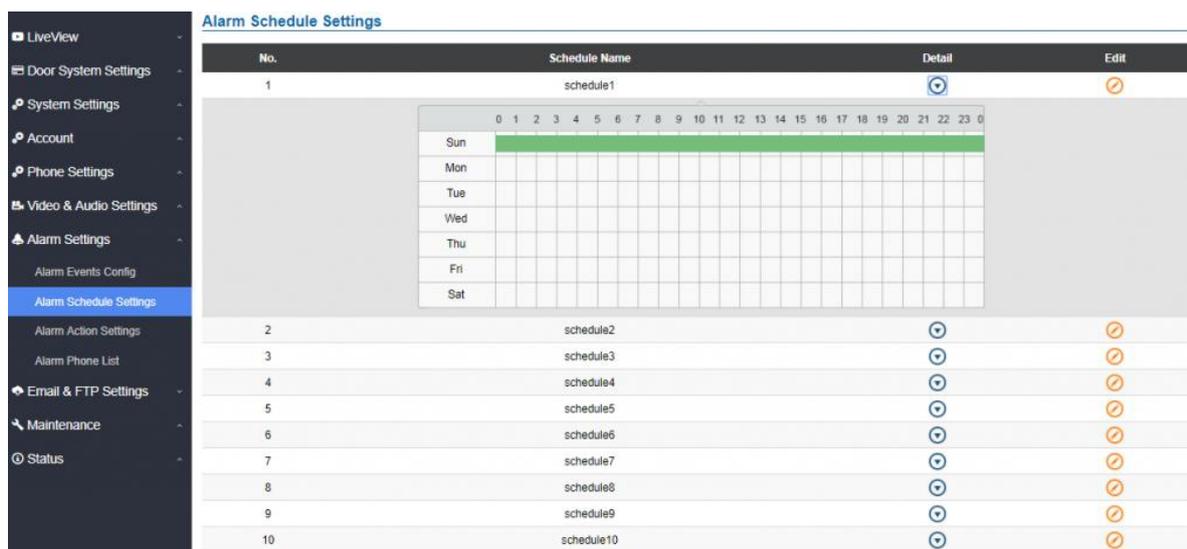


图 94: 报警时间表

GDS3710 最多支持 10 个可配置的告警计划表, 时间跨度由用户指定。

用户可以通过点击  按钮, 编辑闹钟时间表。通常 24 小时的跨度为 00:00 ~ 23:59, 是 24 小时的格式。

在调度编程过程中, 用户可以将配置复制到不同的日期。

Modify Schedule
✕

Schedule Name

Sun	Period1	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="23"/>	:	<input type="text" value="59"/>
Mon	Period2	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>
Tue	Period3	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>
Wed	Period4	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>
Thu	Period5	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>
Fri	Period6	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>
Sat	Period7	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>
	Period8	<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="00"/>	:	<input type="text" value="00"/>

Copy Sun Mon Tue Wed Thu Fri Sat Select All

Save
Cancel

图 95: 编辑时间表

非授权 RFID 卡访问报警

注意

此配置仅适用于 GDS3710 型号。

开启该功能后，任何非法刷卡试图进入大门的行为都会根据用户配置触发报警。

启用非授权 RFID 卡访问报警	启用/禁用在未经授权的刷卡时激活概要文件执行的选项。
选择报警联动方案	选择在未授权的卡刷卡后触发的告警操作类型。

图 96: 非法刷卡时的报警动作

报警动作设置

此页面指定“告警操作”使用的“概要”配置。告警动作生效前，需要先创建配置文件。

Alarm Action Settings

No.	Alarm Action Profile Name	Detail	Edit	Test
1	profile1			
<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Upload to Alarm Center <input checked="" type="checkbox"/> Audio Alarm to SIP Phone <input checked="" type="checkbox"/> Send Email <input checked="" type="checkbox"/> Audio Alarm <input checked="" type="checkbox"/> Alarm Output <input checked="" type="checkbox"/> Upload Snapshot </div>				
2	profile2			
3	profile3			
4	profile4			
5	profile5			
6	profile6			
7	profile7			
8	profile8			
9	profile9			
10	profile10			

图 97: 报警动作

用户点击  按钮，配置报警动作选项，如下图：

Modify Alarm Action Profile ✕

Alarm Action Profile Name

Upload to Alarm Center

Audio Alarm to SIP Phone

Send Email

Audio Alarm

Alarm Output

Upload Snapshot

Save
Cancel

图 98: 编辑报警动作

当用户需要测试告警动作配置文件时，单击  按钮，GDS 会自动启动所选告警动作配置文件上的所有动作。

上传中心

如果选择，GDS Manager 将弹出报警窗口并发出报警声。

SIP 电话提醒

如果选择，GDS371x 将拨打预配置(视频或音频)电话，并播放声音报警。

邮件联动

选中后，带有快照的电子邮件将被发送到预先配置的电子邮件目的地。

声音报警

如果选择，GDS371x 将使用内置扬声器播放报警音频

联动报警输出

如果选择，则告警将被发送到连接在“告警输出”接口上的设备(例如:警报器)。

上传图片

如果勾选，则事件触发时刻的快照将被发送到预先配置的目的地(如:FTP 或电子邮件)。

报警电话列表

该页面允许用户配置报警电话列表，当事件触发时 GDS371x 将呼叫(例如:按门铃)。

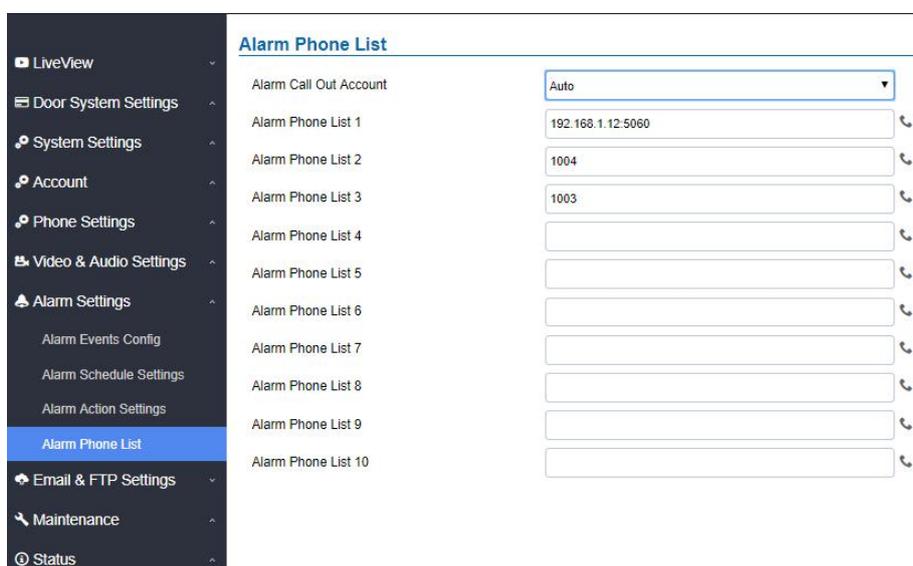


图 99: 报警电话列表

报警呼出账号

配置当触发告警时，GDS 使用的 SIP Account。

报警电话列表 t1-10

在电话告警列表中添加或删除号码。(当使用 IP 地址时，需要追加端口，例如:192.168.1.12:5060)。

表 20: 报警电话列表

一旦事件被触发(移动检测，门铃按下…)，GDS3710 将呼叫第一个号码，一旦呼叫超时且第一个号码没有返回应答，GDS3710 将尝试列表上的下一个号码，以此类推。远程话机接通后，会播放事件提示音，提示有事件触发。

邮件 & FTP 设置

此目录包含“电子邮件”和“FTP 设置”。

邮件设置

通过该界面，用户可以配置电子邮件客户端，在告警触发时发送电子邮件。

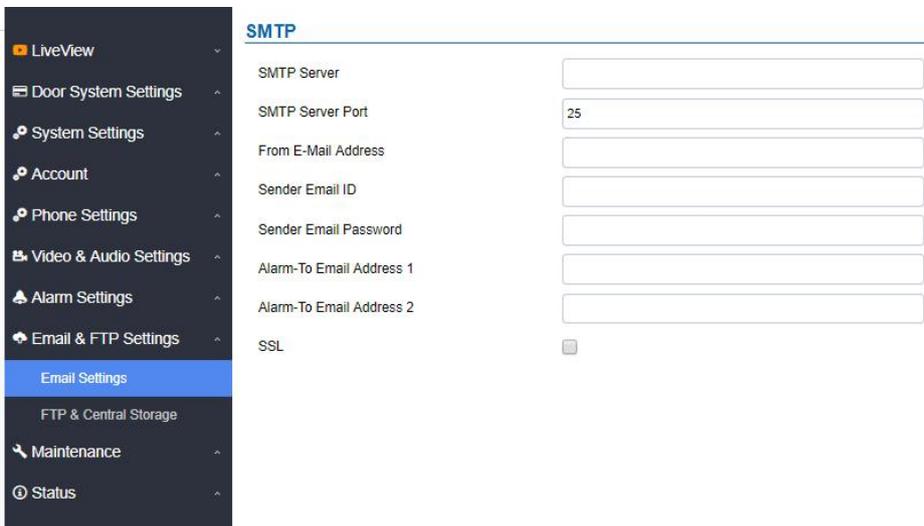


图 100: 邮件设置 - SMTP 页面

SMTP 服务器	配置 SMTP 邮件服务器 IP 或域名。
SMTP 服务器端口	SMTP 服务器端口。
发件地址	发送告警邮件的邮箱地址，一般为客户端邮箱 ID。
发件邮箱用户名	指定发件人使用的电子邮件系统中的用户 ID 或帐户 ID。
发件邮箱密码	指定发件人使用的电子邮件系统中的密码。
报警收件箱 1	接收告警邮件的第一个邮箱地址。
报警收件箱 2	接收告警邮件的第二个邮箱地址。
SSL	检查 SMTP 电子邮件服务器是否需要 SSL。

邮件设置 - SMTP

注意

- 单击“保存”，保存邮件配置信息。
- 设置完成后，点击“电子邮件测试”，如果设置正确，将发送测试电子邮件，并在首页显示“电子邮件测试成功” E-Mail test successfully 的信息。

FTP 和中心存储

此页面允许用户配置 FTP 设置以上传捕获图像。

存储服务器类型	选择上传图片到 GDS Manager 还是上传图片到 FTP 服务器。
FTP 服务器	配置 FTP 的服务器的 IP 地址或域名
FTP 服务器端口	设置 FTP 的端口
FTP 用户名	设置 FTP 服务器的用户名
FTP 密码	设置 FTP 服务器的密码
FTP 路径	设置具体的 FTP 路径
FTP 测试	点击去测试 FTP

注意

当使用存储服务器类型作为中央存储时，空白字段可能意味着在 GDSManager 中没有配置。

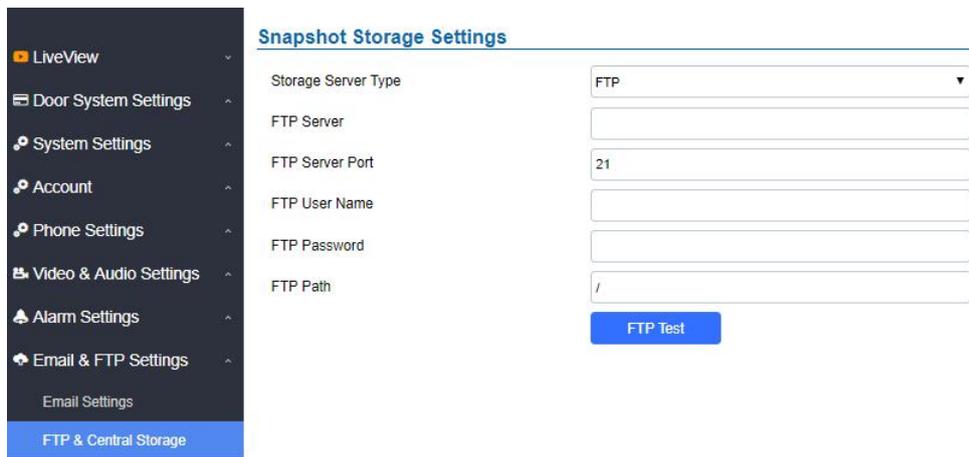


图 101: 图片存储设置界面

注意

- 如果 FTP 服务器连接成功，FTP 服务器会上传一个包含成功连接信息的 txt 文件。在 WEB GUI 上将会弹出下面的消息将会弹出 **FTP test successfully**。
- 中央存储将使用 GDS 管理器内置的 FTP 服务器存储屏幕截图。

FTP 文件名

设置 FTP 服务器存储快照时(按门铃或门未锁时)，GDS 会创建以设备 MAC 地址为单位的文件夹

(如果多个 GDS3710/ gds3712 向同一个 FTP 服务器发送快照)。

在每个文件夹中，根据 MAC 地址或设备，根据日期创建文件夹，将不同日期收到的快照进行组织和分类，便于分析。

在 DATE 分类的每个文件夹中，快照文件的命名模式如下：

FTP 文件名	描述
CARD	意味着开门操作是使用 RFID 卡
LPIN (本地 PIN)	这意味着开门操作是通过本地 PIN(私有 PIN, 或统一 PIN, 或客户 PIN)。
RPIN 远端的 PIN)	意思是开门操作是通过远程 PIN 或 DTMF PIN。(通过本地或远程 SIP 扩展, 或 GS_Wave/手机, 或 GDSManager(如果安装在运行中))。
RING	意味着有人按门铃时拍下的照片。

执行上述操作后，发送给 FTP 服务器的 FTP 文件名如下图所示：

```
[To Parent Directory]
Friday, March 02, 2018 9:39 AM 76504 BA854E CARD 2018-03-02 100355 7558019 0.jpg
Friday, March 02, 2018 9:39 AM 82105 BA854E CARD 2018-03-02 100356 0.jpg
Friday, March 02, 2018 9:39 AM 83406 BA854E CARD 2018-03-02 100356 7558019 1.jpg
Friday, March 02, 2018 9:39 AM 82427 BA854E CARD 2018-03-02 100357 0.jpg
Friday, March 02, 2018 9:39 AM 83266 BA854E CARD 2018-03-02 100358 0.jpg
Friday, March 02, 2018 9:39 AM 85094 BA854E CARD 2018-03-02 100359 0.jpg
Friday, March 02, 2018 9:39 AM 87633 BA854E CARD 2018-03-02 100400 0.jpg
Friday, March 02, 2018 9:39 AM 86810 BA854E CARD 2018-03-02 100401 0.jpg
Friday, March 02, 2018 7:46 AM 76148 BA854E LPIN 2018-03-02 080942 0.jpg
Friday, March 02, 2018 7:46 AM 75696 BA854E LPIN 2018-03-02 080943 0.jpg
Friday, March 02, 2018 7:46 AM 79922 BA854E LPIN 2018-03-02 080944 0.jpg
Friday, March 02, 2018 7:46 AM 81914 BA854E LPIN 2018-03-02 080945 0.jpg
Friday, March 02, 2018 7:46 AM 79908 BA854E LPIN 2018-03-02 080946 0.jpg
Friday, March 02, 2018 7:46 AM 79514 BA854E LPIN 2018-03-02 080947 0.jpg
Friday, March 02, 2018 7:46 AM 80353 BA854E LPIN 2018-03-02 080948 0.jpg
Friday, March 02, 2018 8:36 AM 81201 BA854E LPIN 2018-03-02 090050 0.jpg
Friday, March 02, 2018 8:36 AM 82609 BA854E LPIN 2018-03-02 090051 0.jpg
Friday, March 02, 2018 8:36 AM 79362 BA854E LPIN 2018-03-02 090052 0.jpg
Friday, March 02, 2018 8:36 AM 86139 BA854E LPIN 2018-03-02 090053 0.jpg
Friday, March 02, 2018 8:36 AM 85269 BA854E LPIN 2018-03-02 090054 0.jpg
Friday, March 02, 2018 8:36 AM 84463 BA854E LPIN 2018-03-02 090055 0.jpg
Friday, March 02, 2018 8:36 AM 86007 BA854E LPIN 2018-03-02 090056 0.jpg
Friday, March 02, 2018 8:50 AM 82610 BA854E LPIN 2018-03-02 091348 0.jpg
Friday, March 02, 2018 8:50 AM 81378 BA854E LPIN 2018-03-02 091349 0.jpg
Friday, March 02, 2018 8:50 AM 83379 BA854E LPIN 2018-03-02 091350 0.jpg
Friday, March 02, 2018 8:50 AM 83745 BA854E LPIN 2018-03-02 091351 0.jpg
Friday, March 02, 2018 8:50 AM 87227 BA854E LPIN 2018-03-02 091352 0.jpg
Friday, March 02, 2018 8:50 AM 87199 BA854E LPIN 2018-03-02 091353 0.jpg
Friday, March 02, 2018 8:50 AM 84078 BA854E LPIN 2018-03-02 091354 0.jpg
Friday, March 02, 2018 9:44 AM 77783 BA854E LPIN 2018-03-02 100955 0.jpg
```

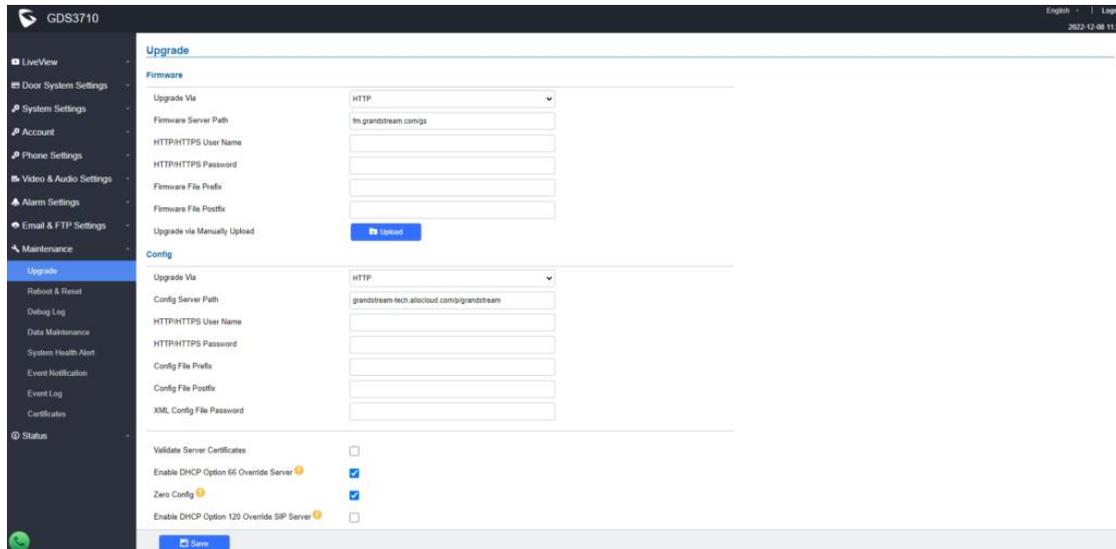
图 102: FTP 文件名

维护设置

本页面主要显示 GDS371x 维护参数。

升级

本页面主要包含了 GDS371x 升级的相关参数



升级方式

选择升级固件的方式支持 TFTP, HTTP 和 HTTPS。

固件服务器路径

设置 IP 地址或域名

HTTP/HTTPS 用户名

HTTP/HTTPS 服务器的用户名

HTTP/HTTPS 密码

HTTP/HTTPS 服务器的密码

固件文件前缀

如果配置了，只有匹配加密前缀的固件文件将被下载并写入设备。

固件文件后缀

如果配置了，只有带有匹配的加密后缀的固件将被下载并存入设备。

手动上传升级

支持手动上传固件升级文件。

升级方式

选择升级固件的方式支持 TFTP, HTTP 和 HTTPS。

配置文件服务器路径

设置 IP 地址或域名。

HTTP/HTTPS 用户名

HTTP/HTTPS 服务器的用户名

HTTP/HTTPS 密码

HTTP/HTTPS 服务器的密码

配置文件前缀

如果配置了，只有匹配加密前缀的固件文件将被下载并写入设备。

配置文件后缀

如果配置了，只有带有匹配的加密后缀的固件将被下载并存入设备。

XML 配置文件密码

设置配置文件的密码。

验证服务器证书

启用此选项，以便在 TLS 连接期间使用受信任的证书

	验证证书。
自动升级周期	升级周期(单位:分钟)。
启用 DHCP Option 66 服务器设置	激活 DHCP 选项 66 覆盖升级/配置服务器。
零配置	启用零配置, 用于设备自动升级
启用 DHCP 选项 120 服务器设置	启用本地服务器的 DHCP Option 120 覆盖话机上的 SIP server。默认设置为启用
自动升级	启用自动升级和配置。设置每 X 分钟、每天或每周的供应计划。默认为“否”。
随机自动升级	启用并定义 GDS 随机检查更新的开始/结束时间和星期几。
禁用 SIP NOTIFY 鉴权	如果选中此选项, 设备将不会用 401 挑战 NOTIFY。默认设置为“启用”。

表 21: 升级

LED 模式

在升级过程中, 从固件 1.0.3.32 开始, GDS 将使用 LED 照明显示升级过程的进度, 如下所示:

1. 下载固件文件时, 门铃按钮蓝色 LED 会闪烁。(GDS3712 呼叫按钮闪烁)
2. 数字 1、2、3 蓝色 LED 在从 0 升级到 25%时闪烁, 然后保持常亮。(适用于 GDS3710)
3. 数字 4、5、6 蓝色 LED 在从 25%升级到 50%时闪烁, 然后保持常亮。(适用于 GDS3710)
 1. 数字 7、8、9 蓝色 LED 在从 50%升级到 75%时闪烁, 然后保持常亮。(适用于 GDS3710)
 2. 数字*, 0, #蓝色 LED 在从 75 升级到 100%时闪烁, 然后保持常亮。(适用于 GDS3710)
 3. 所有钥匙的蓝色 led 灯亮起, 然后闪两次, 然后重新启动自己完成升级过程。(适用于 GDS3710)。

重启 & 重置

此页面允许用户重新启动和重置 GDS371x。

Reboot & Reset

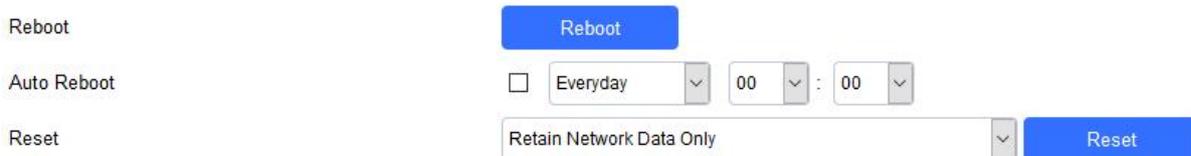


图 103: 重启和重置配置界面

重启	点击，GDS 将会重启。
自动重启	有了这个功能，用户可以方便地自行设置设备重启的时间表，每周或每天，以使性能平稳
重置	重置有两个功能。
清除所有数据	GDS 将被恢复出厂，所有数据都会被清除
清除除网络外所有数据	所有数据将被擦除，除了网络数据，如 IP 地址…
清除卡片信息以外的所有数据	除卡片信息外，所有数据将被擦除。 (配置仅适用于 GDS3710)
清除除网络和卡片信息以外所有数据	除卡片信息外，所有数据将被擦除。 (配置仅适用于 GDS3710)

系统日志

本页面允许用户配置 SYSLOG 收集信息，以帮助解决 GDS371x 的问题。

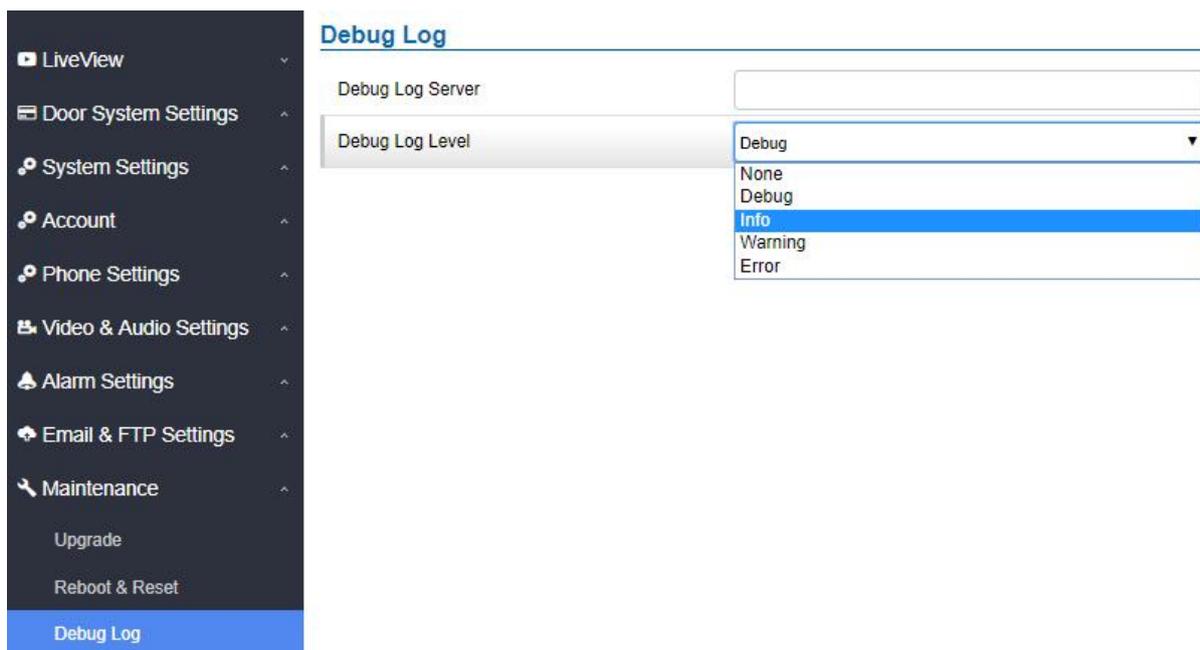


图 104: 系统日志界面

- 有五个级别的调试，无，调试，信息，警告，错误。
- 输入 Syslog 服务器和级别后，按“保存”键，然后重启 GDS3710 以应用设置。

数据维护

通过此界面可以导入导出配置文件，管理 GDS371x 的配置文件。

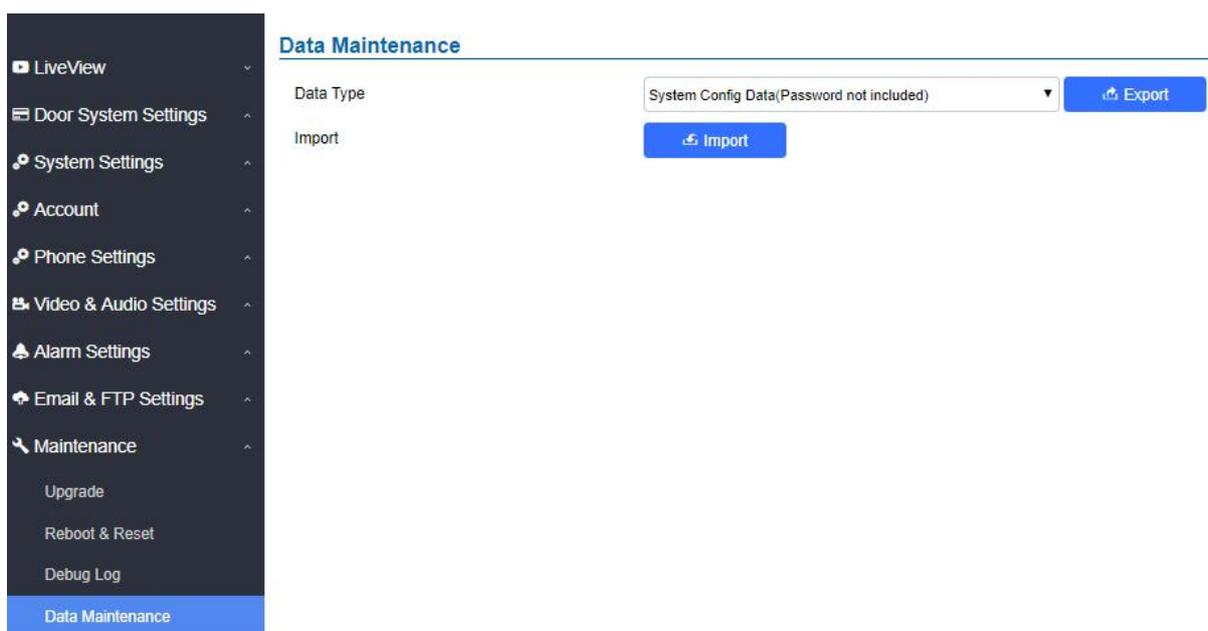


图 105: 数据维护界面

注意

用户可以选择在导出的配置文件中包含所有密码(SIP、FTP、Remotes access...), 也可以选择
不包含。

系统健康通知

通过此选项, 用户可以实时或定期收到帐号的 SIP 注册状态、系统运行状态或系统温度的告警邮件。

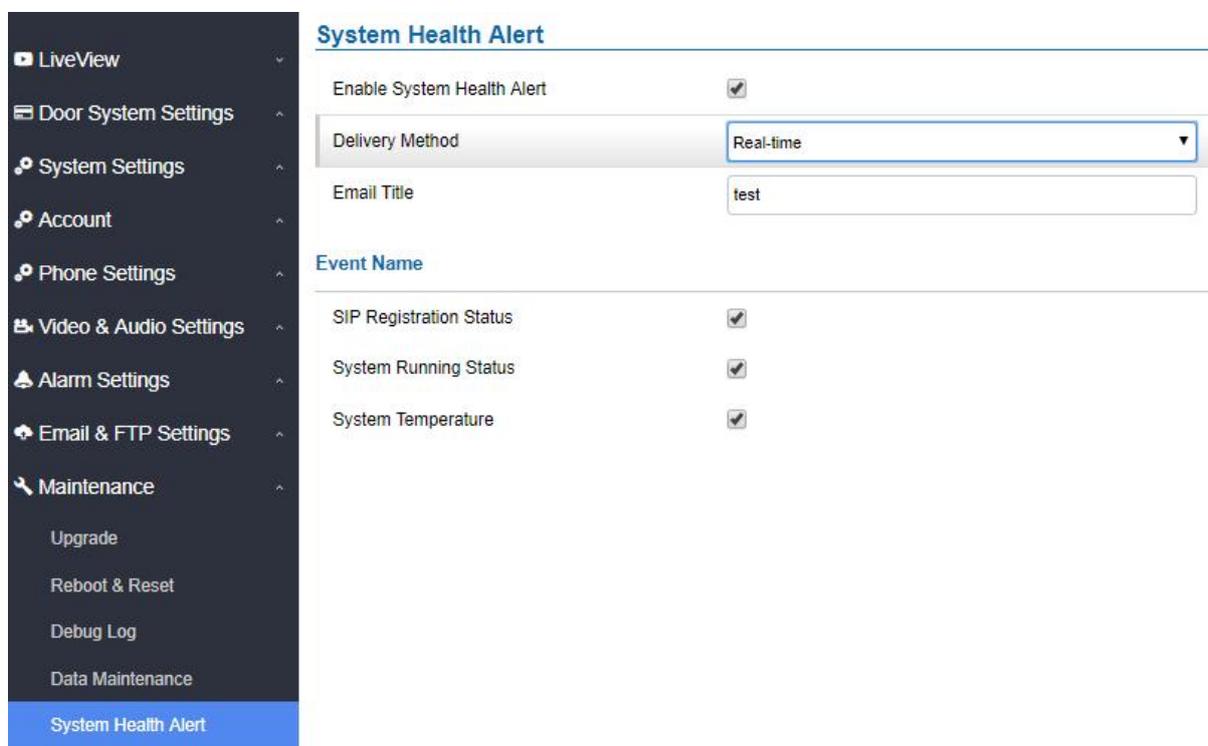


图 106: 系统健康通知

启用系统健康通知

选中此选项后, GDS 将使用已配置的[电子邮件设置]就在“事件名称”部分中选择的事件发送警报电子邮件。

发送方式

设置为“实时”时, GDS 每秒会连续发送提醒邮件。
当设置为“定时”时, 用户可以自定义告警邮件的时间间隔。

邮件主题

自定义邮件标题。最大长度为 256 个字符。

SIP 注册状态

勾选后, 电子邮件将包含所有 4 个帐户的离线/在线指示。

系统运行状态

勾选时, 电子邮件将包含系统正常运行时间。

系统温度

当勾选时, Email 将包含系统的温度值在 °C 和 °F, 以及温度是否
正常。

事件通知

此页面允许用户配置事件通知细节，GDS3710 将使用这些细节与 HTTP 服务器通信以记录事件。

启用并配置该功能后，所有事件日志将被上传到服务器:RFID 开门、PIN 开门、SIP 呼叫、报警等。

例子:

此页面允许用户配置事件通知细节，GDS3710 将使用这些细节与 HTTP 服务器通信以记录事件。

启用并配置该功能后，所有事件日志将被上传到服务器:RFID 开门、PIN 开门、SIP 呼叫、报警等。

例子:POST / HTTP/1.1

Host: 192.168.6.107

Authorization: Basic Og==

Connection: keep-alive

Content-Length: 90

Date: 2017-11-09; Time: 14:07:27; Event describe: Use card open door. Card ID:
378690700.

拨打电话后，当门铃按下时，GDS3710 将向配置的 HTTP 服务器发送以下包含“电话呼叫”事件的 HTTP POST:

POST/HTTP/1.1

Host:192.168.6.107

Authorization:BasicOg==

Connection:keep-alive

Content-Length:62

Date: 2017-11-09; Time: 14:13:12; Event describe: Phone call.

第三方软件可以使用这些 HTTP POST 消息来集成 GDS371x。

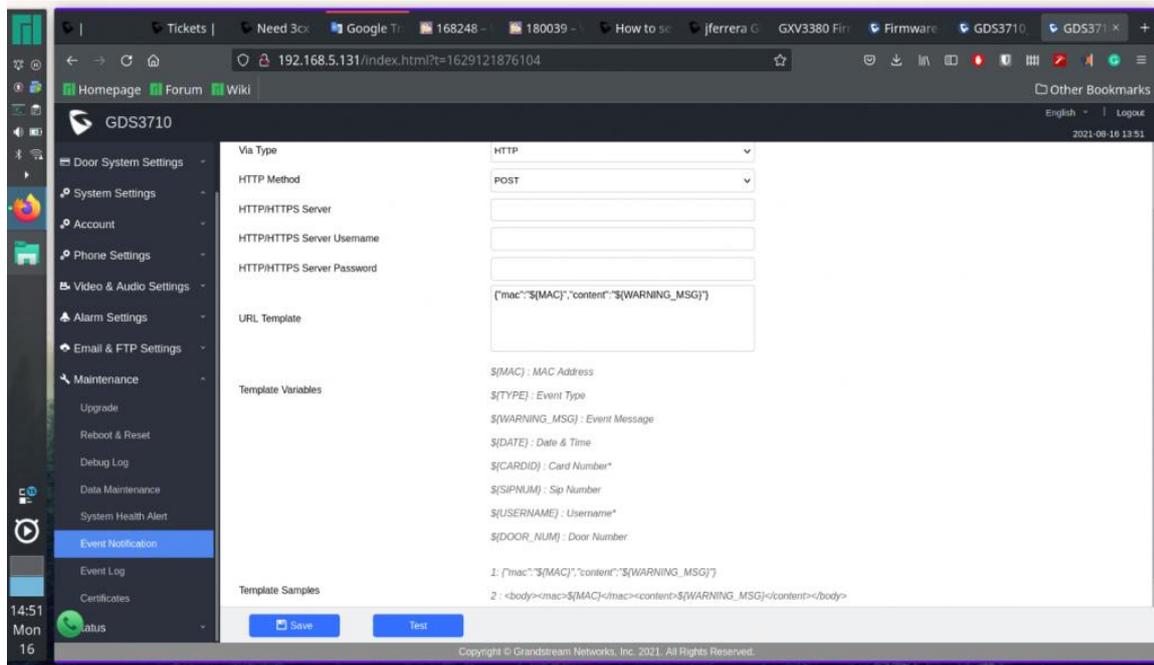


图 107: 日志管理页面

启用事件通知

启用事件通知功能

方式

选择将使用哪种协议连接到日志服务器(HTTP 或 HTTPS)。

HTTP Method

选择将使用哪种 HTTP 方法将日志发送到服务器(POST 或 GET)。

HTTP/HTTPS 服务器

输入日志服务器的 IP 地址或域名。

HTTP 服务器用户名

配置 HTTP(s) 服务器的用户名。

HTTP 服务器密码

配置 HTTP(s) 服务器的密码

模板变量

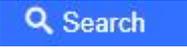
指定将发送到服务器的事件日志消息的模板，用户可以使用以下变量自定义消息：

\${MAC} : MAC Address
 \${TYPE} : Event Type
 \${WARNING_MSG} : Event Message
 \${DATE} : Date & Time
 \${CARDID} : Card Number
 \${SIPNUM} : SIP Number

事件日志

用户可以直接在 GDS web 界面的“维护事件日志”菜单下查看所有设备日志。

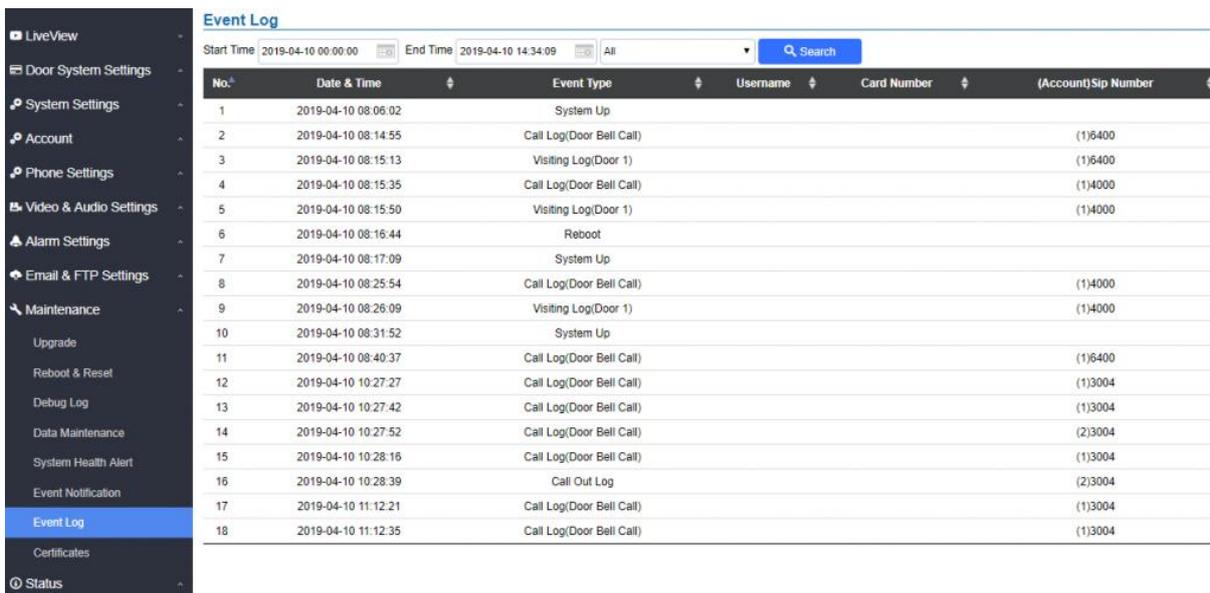
为了获得特定日期间隔的日志，请选择开始时间和结束时间，然后使用下拉列表选择要检查的事件类

型，然后单击  以显示记录。

过滤包括以下事件类型：

- 刷卡开门
- 未经授权的开门方式
- 来访记录
- D1 开门
- 密码开门
- 呼叫记录
- 刷卡+密码开门
- 远程密码开门
- 移动侦测
- 探头报警
- 门锁异常
- 暴力拆除
- 宕机
- 重启
- 重置
- 配置更新
- 固件更新
- 超出日程表访问
- 挟持报警
- 密码输入错误

- 温度报警



No.	Date & Time	Event Type	Username	Card Number	(Account)Sip Number
1	2019-04-10 08:06:02	System Up			
2	2019-04-10 08:14:55	Call Log(Door Bell Call)			(1)6400
3	2019-04-10 08:15:13	Visiting Log(Door 1)			(1)6400
4	2019-04-10 08:15:35	Call Log(Door Bell Call)			(1)4000
5	2019-04-10 08:15:50	Visiting Log(Door 1)			(1)4000
6	2019-04-10 08:16:44	Reboot			
7	2019-04-10 08:17:09	System Up			
8	2019-04-10 08:25:54	Call Log(Door Bell Call)			(1)4000
9	2019-04-10 08:26:09	Visiting Log(Door 1)			(1)4000
10	2019-04-10 08:31:52	System Up			
11	2019-04-10 08:40:37	Call Log(Door Bell Call)			(1)6400
12	2019-04-10 10:27:27	Call Log(Door Bell Call)			(1)3004
13	2019-04-10 10:27:42	Call Log(Door Bell Call)			(1)3004
14	2019-04-10 10:27:52	Call Log(Door Bell Call)			(2)3004
15	2019-04-10 10:28:16	Call Log(Door Bell Call)			(1)3004
16	2019-04-10 10:28:39	Call Out Log			(2)3004
17	2019-04-10 11:12:21	Call Log(Door Bell Call)			(1)3004
18	2019-04-10 11:12:35	Call Log(Door Bell Call)			(1)3004

图 108: 事件日志

有关事件日志的更多信息，请访问本指南。

注意

- GDS3710 日志存储空间的最大大小约为 64M。
- 每个事件日志的大小为 48 字节。
- 如果日志数据超过最大存储空间，则会自动释放最旧的日志，即 128K 的旧数据。

证书

该页面最多支持上传 6 个受信任的 CA 证书文件，在 SSL 交换过程中受 GDS 信任。

此外，用户还可以在自定义证书部分中使用自定义 CA 证书签名的自定义证书配置设备。

Certificates

Trusted CA Certificates

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

Custom Certificate

No.	Issued By	Expiration		
1			 Upload	 Delete

图 109: 上传认证证书

上传您的受信任 CA 证书:

点击  Upload 按钮上传文件, 会显示上传文件的相关信息, 如“发布日期”和“过期日期”。

Trusted CA Certificates

No.	Issued By	Expiration		
1	-	2018-07-17 15:46:03	 Upload	 Delete
2			 Upload	 Delete

点击  Delete, 用户可按删除其中一个文件。

点击  Upload 按钮, 上传文件, 会显示上传文件的相关信息, 如“发布日期”和“过期日期”。

Custom Certificate

No.	Issued By	Expiration		
1			 Upload	 Delete

状态

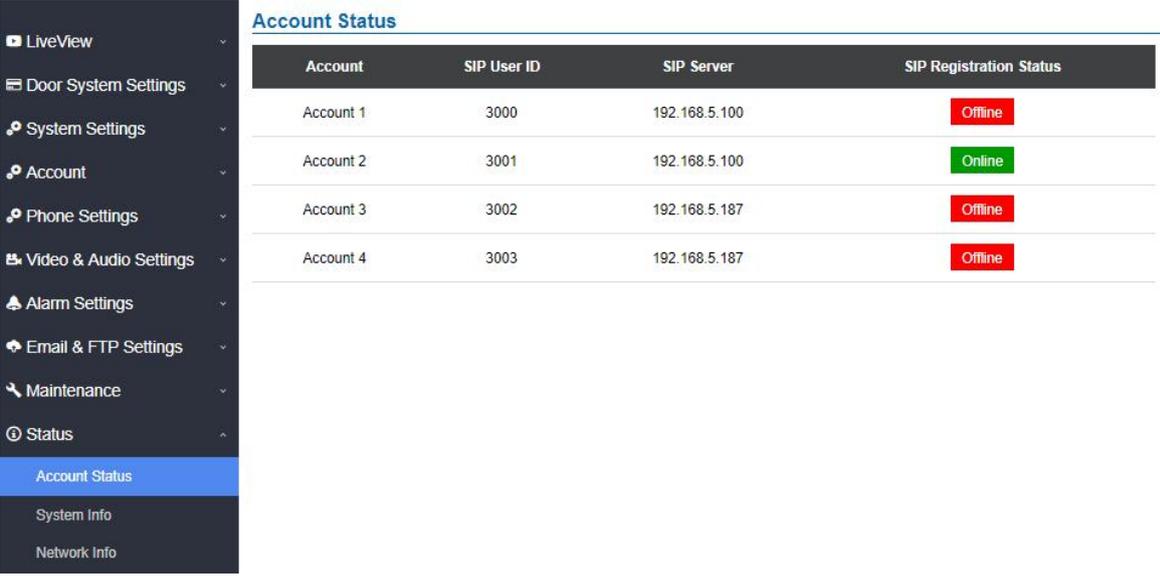
该页面可以显示 GDS371x 的系统状态和网络状态。

账号状态

显示帐号 1~帐号 4 的 SIP 用户 ID、SIP 服务器、SIP 注册状态。

注意

- 注册成功后，“SIP 注册状态”显示为“在线”
- 当 SIP 帐号未注册时，“SIP 注册状态”显示为“离线”



Account	SIP User ID	SIP Server	SIP Registration Status
Account 1	3000	192.168.5.100	Offline
Account 2	3001	192.168.5.100	Online
Account 3	3002	192.168.5.187	Offline
Account 4	3003	192.168.5.187	Offline

图 110: 系统状态界面

系统信息

该页面主要显示系统信息，如产品型号，硬件版本，软件版本等。

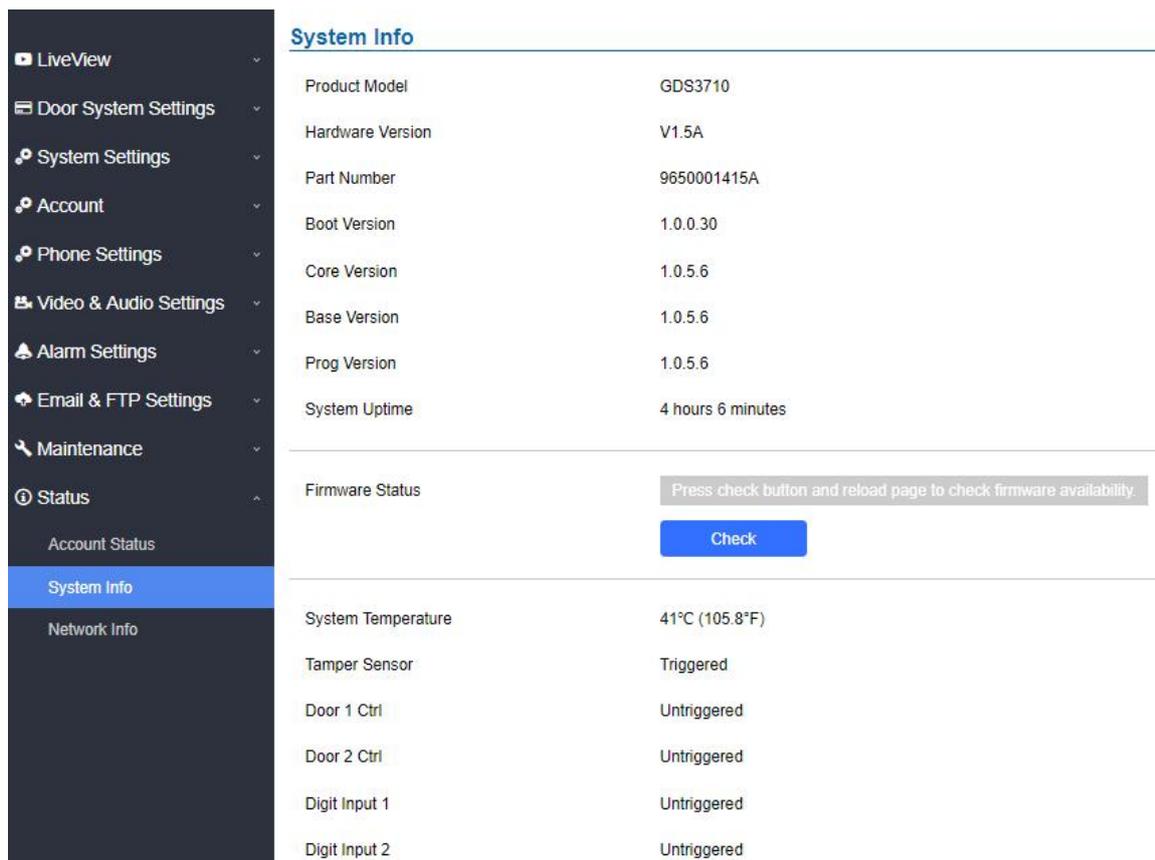


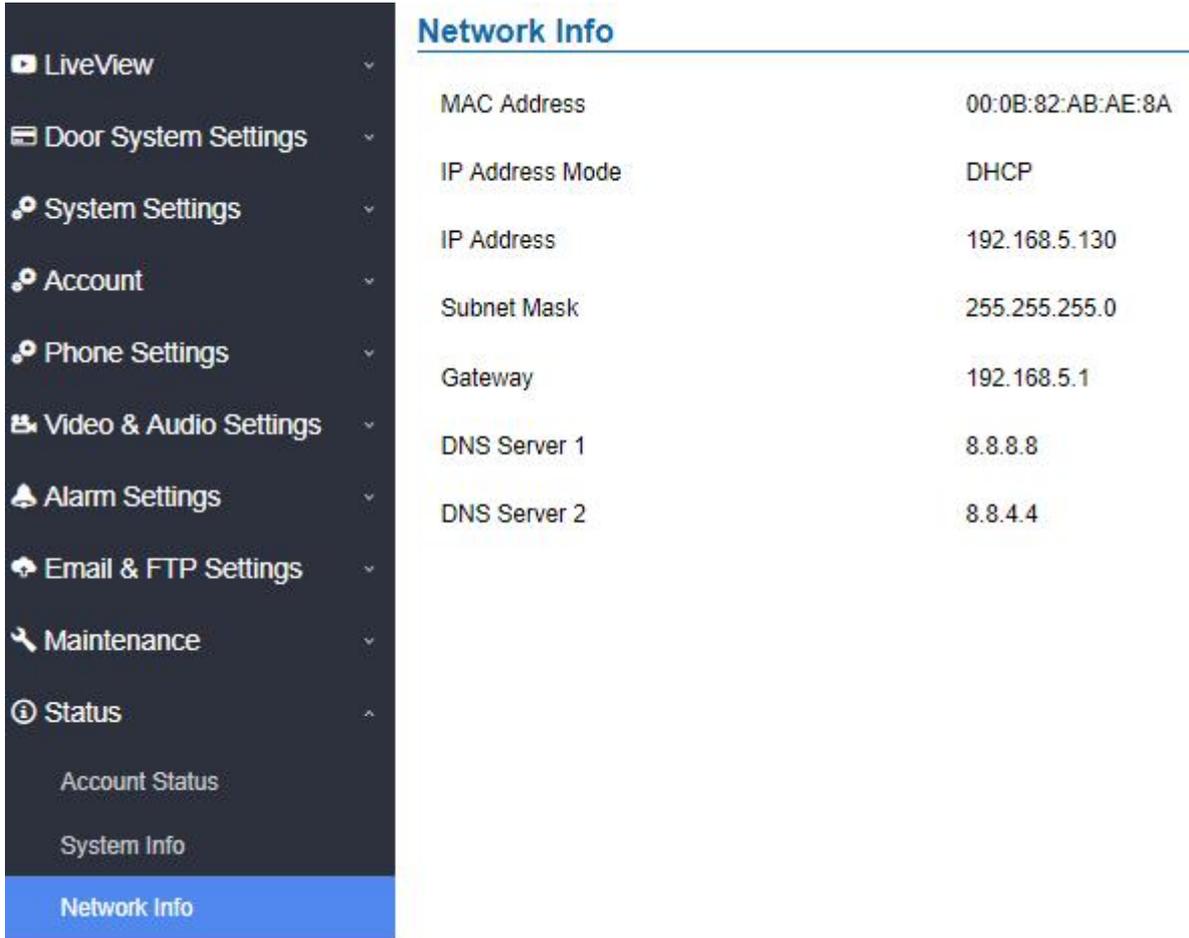
图 111: 系统信息界面

产品型号	显示设备的型号
硬件版本	显示设备的硬件版本号
P/N 编号	显示设备的 PN 号
Boot 版本	显示设备的 BOOT 版本
Core 版本	显示设备的 core 版本
Base 版本	显示设备的 base 版本
Prog 版本	显示设备的主程序版本
运行时长	显示系统自从启动后，运行的时间
SIP 注册状态	展示 SIP 账号注册状态
固件状态	点击  按键，检查检测软件是否是最新版本，如果不是请立刻升级。
系统温度	显示当下系统的温度 (in ° C and ° F).
防拆传感器	显示是否触发防拆传感器。
数字输出	显示是否触发 Alarm Out。 如果 ALMOUT1 功能设置为开门，则会显示两个字段，分别表示门 1 和门 2 的状态。

数字输入 1	显示告警 IN 1 是否被触发。
数字输入 2	显示告警 IN 2 是否被触发。

网络信息

此页面显示 GDS3710 的网络信息。



MAC Address	00:0B:82:AB:AE:8A
IP Address Mode	DHCP
IP Address	192.168.5.130
Subnet Mask	255.255.255.0
Gateway	192.168.5.1
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4

图 112: 网络信息页面

MAC 地址	显示 GDS371x 的 MAC 地址
IP 地址类型	显示 IP 地址类型
IP 地址	显示 GDS 的 IP 地址。
Subnet Mask	显示子网掩码地址
Gateway	显示网关地址
DNS Server 1	显示 DNS1 地址
DNS Server 2	显示 DNS2 地址

连接 GDS371x 和 GXV33XX

GDS371x 门系统提供了与 GXV33xx 的强大集成，允许用户打开门，向 GDS371x 发起呼叫，并获得实时音频/视频流。

GXV33xx 与 GDS371x 有两种不同的连接方式，一种是通过点对等模式(没有 SIP 服务器)连接，另一种是通过 SIP 服务器连接。详情请参阅以下指引:

<https://documentation.grandstream.com/knowledge-base/connecting-gds37xx-with-gxv33x/>

连接 GS Wave 与 GDS371x 门系统

GDS371x 门系统可以与 GS Wave 软电话应用程序交互，允许用户打开门，向 GDS371x 发起呼叫，在安全监控期间提供更多的移动性，并增加与基本通信和实时音频/视频流的连接。

gs Wave Android:有关配置 GDS371x 连接 Grandstream Wave Android™ 版本所需步骤的详细信息，请参阅以下指南:

<https://documentation.grandstream.com/knowledge-base/connecting-gds3710-with-wave-lite-android-guide/>

- GS Wave IOS: 有关配置 GDS371x 连接 Grandstream Wave iOS™ 版本所需步骤的详细信息，请参阅以下指南:

- <https://documentation.grandstream.com/knowledge-base/connecting-gds3710-with-wave-lite-ios-guide/>

GDS371x HTTP API

Grandstream Door 系统支持 HTTP API(应用程序编程接口)。详情请参阅以下指引:

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

本文档通过所支持的方法详细介绍了基于 http 的外部应用程序编程接口和函数的参数。HTTP API 依赖于固件。支持的功能请参见相关固件版本说明书。

说明需要具有“管理员权限”，在进行相关参数配置前，需要先进行管理员身份验证。

恢复出厂

通过 Web GUI 恢复出厂

通过 Web GUI 对 GDS371x 进行出厂复位，请参考以下步骤：

1. 使用自带的默认密码访问 GDS371x Web GUI。
2. 维护—重启和重置，选择复位类型，按下复位按钮，如下图所示。



图 113：通过 Web GUI 恢复出厂

注意

保留网络数据和卡信息或仅 Crad 信息选项仅在 GDS3710 模式上可用

硬恢复出厂

注意

仅 GDS3710 型号支持通过韦根线缆复位设备。

部分用户没有妥善保存修改后的密码，忘记了修改后的密码。由于 GDS3710 没有内置的重置按钮（潮流网络故意设计这种方式来增强安全性），这将使 GDS3710 无法访问。

从固件 1.0.2.21 开始，潮流网络引入了一种特殊的方法，使用 GDS3710 附带的韦根接口电缆进行硬工厂重置。下面是所提供的韦根电缆正常连接的照片。

重要提示

执行硬出厂复位时，电源一定不能丢失。



图 114: 韦根连接图

对 GDS371x 进行硬出厂复位，请参考以下步骤：

1. GDS3710 断电。
2. 取所提供的韦根电缆，按下图所示连接(或短路)相关的彩色电线。请确保连接正确牢固：

将白色和棕色电缆连接在一起。

连接绿色和橙色电缆。

对 GDS371x 进行硬出厂复位，请参考以下步骤：

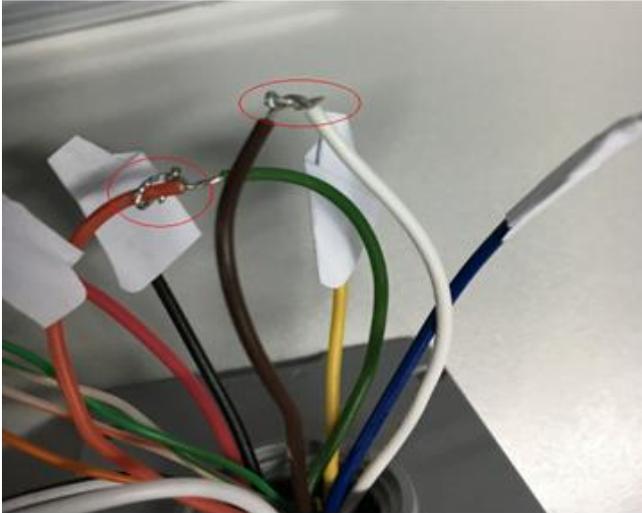


图 115: 韦根连接图

3. GDS3710 上电。在 10 秒左右的时间内，键垫 LED 照明将由固态照明变为闪烁，闪烁时间窗口约为 30 秒。指示灯闪烁时，用户需要输入以下组合键*0#。

注意

- 如果输入正确的组合键，最后一个输入键将播放长音，说明输入的正确组合键，然后 GDS3710 将进入出厂复位模式。
- 在闪烁期间内，如果用户未完成组合键操作，或按错组合键，GDS3710 将快速播放三次短哔声说明错误。然后，GDS3710 将进入正常启动过程。如果用户想要进行硬出厂重置，则必须从头再执行一次操作。

4. 3~5 分钟后，GDS3710 将完成复位，此时用户可以使用出厂默认密码登录 GDS3710 web 界面。

5. 用户必须关闭 GDS3710 电源，拔下韦根电缆，再次上电 GDS3710，并确保 GDS3710 正常运行

使用 GS Search 硬恢复出厂

GDS371x 可以通过以下步骤使用 GS 搜索工具重置:

1. 打开 GS 搜索工具，可以从 Grandstream 工具页面下载。如 [Grandstream tools page](#)。

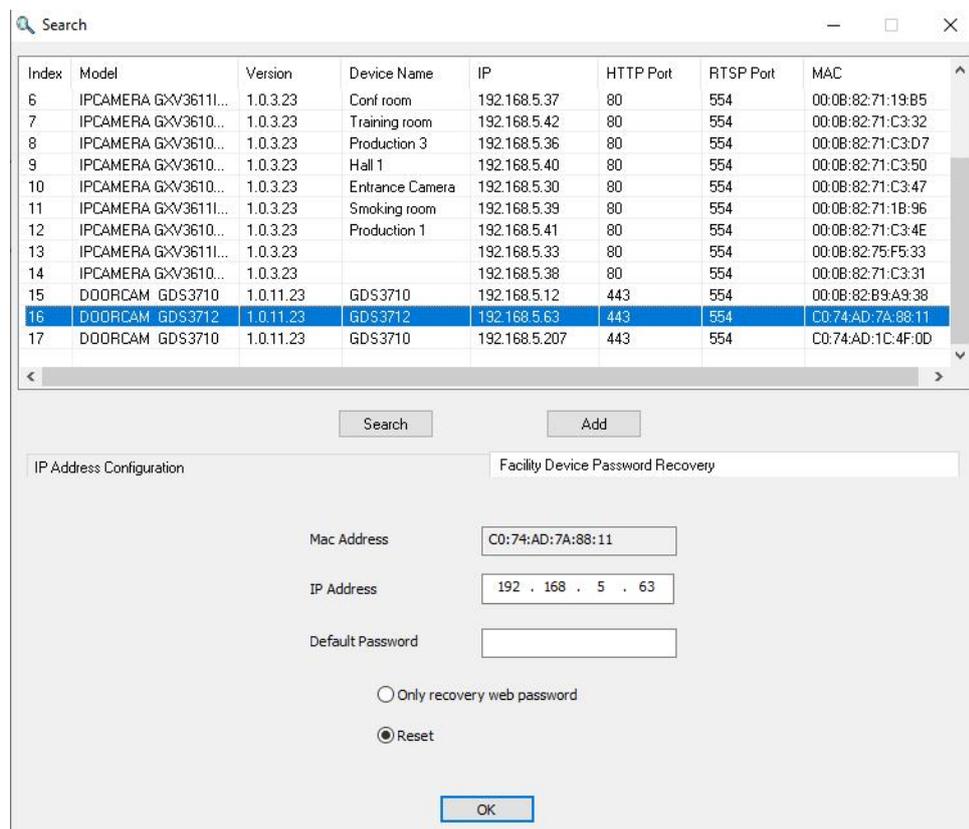


图 116: GS Search 界面

2. 选择有问题的设备，如图中 GDS3712，然后选择设施设备密码恢复。

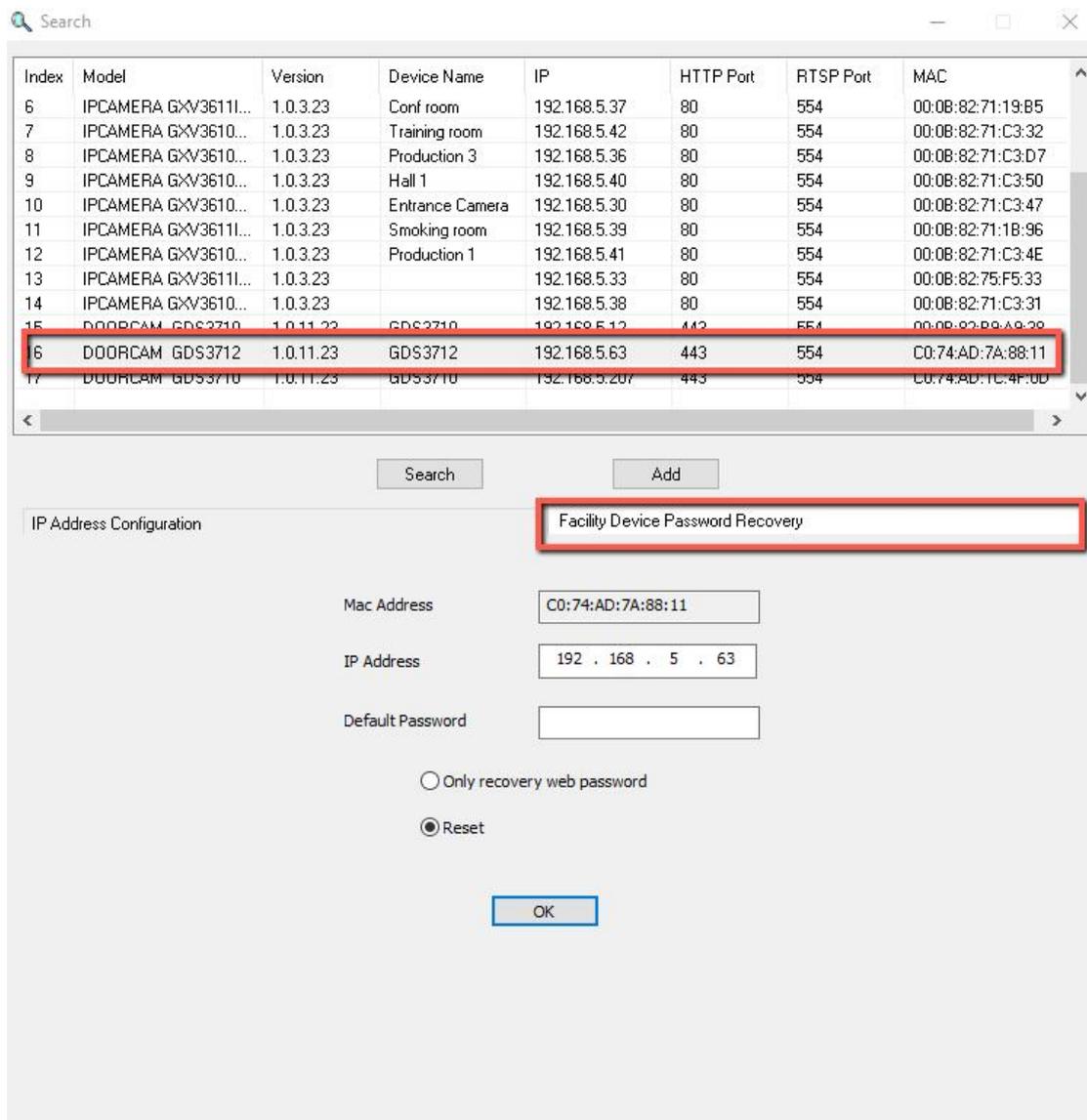


图 117: GS Search - 选中设备去 reset

3. 单击“重置”按钮，执行设备复位操作。

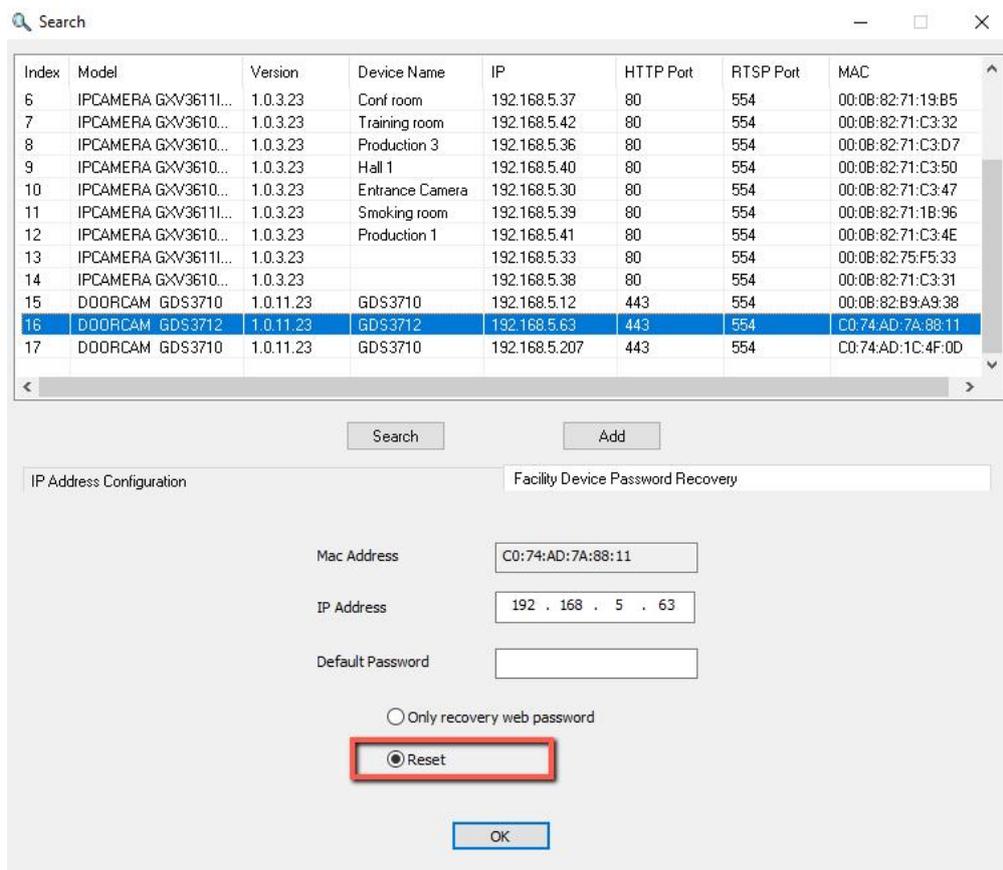


图 118: GS Search - reset

通过 SIP NOTIFY 恢复出厂设置

1. 通过在浏览器中输入其 IP 地址访问您的 GDS371x UI。
2. 进入“电话设置”页面。
3. 通过勾选该选项启用“允许通过 SIP NOTIFY 重置”。(默认禁用)
4. 一旦收到带有“event: reset”的 SIP NOTIFY, GDS371x 将在认证阶段后执行出厂重置。

注意

- 在采取出厂重置操作之前, 将首先对接收到的 SIP NOTIFY 进行验证。
- 认证可以使用管理员密码(如果没有配置 SIP 帐号)或通过 SIP 帐号凭据(SIP 用户 ID 和密码)进行。

通过特殊组合键恢复出厂密码

注意

以下配置仅适用于 GDS3710 型号。

该功能允许客户通过一些特殊的组合键通过键盘操作将设备管理员密码重置为出厂默认值。

执行该操作时，所有密码将被重置为出厂设置。所有其他设置或参数将保持不变。

以下是通过键盘进行密码重置操作的步骤：

编码规则如下：

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

注意

1. GDS37xx 的 MAC 地址(查看设备背面的贴纸)
2. GDS37xx 默认密码(查看设备背面贴纸)
3. 正确解码后 6 个 MAC 地址为数字(参考编码规则)
4. 将默认密码正确解码为数字(参考编码规则)
5. 在 1 分钟内完成键盘输入

操作步骤如下：

- 1)当设备空闲时，输入特殊键盘组合，格式为:***last_6_MAC**#
- 2)在步骤 1 中输入正确数字后，设备将进入恢复模式。键盘背光将快速闪烁，告诉操作员设备现在处于密码重置/恢复模式。
- 3)操作员将在 60 秒内通过键盘输入正确的解码后的默认密码，以#结尾，格式

为:default_password_code#。

4)如果输入错误的密码组合，GDS37xx 会发出错误提示音(三声短提示音)，然后退出密码重置模式，背光灯停止闪烁。

5)如果在 60 秒内输入正确的默认密码解码，GDS37xx 会发出很长的哔哔声(提示正确操作)，设备会自动重启。

6) 如果键盘输入超时(60 秒内未完成输入)，设备将自动退出密码重置模式，并停止背光闪烁。密码重置成功后，操作员可以使用默认密码登录 GDS37xx 的 web 界面，设备内部的所有配置将保持不变，不会被更改。

示例:

将字符串解码为数字，并在执行操作之前写入纸张:

后 6 个 MAC 地址的设备:33DDDD

将最后 6 个 MAC 解码为数字:334444

默认密码:xwpxz6AA

将默认密码解码为数字:2423162426611

1)通过键盘输入***334444**#，进入密码重置模式，键盘背光快速闪烁。2)在 60 秒内，输入 2423162426611#，设备会发出一声很长的哔哔声，然后自动重启。

2)等待设备启动完成后，使用默认密码 xwpxz6AA 登录 web 界面