Grandstream Networks, Inc.

GDS372x - User Manual

GDS372x - User Manual

WELCOME

Thank you for purchasing Grandstream GDS3725/GDS3726/GDS3726Q/GDS3727.

The GDS3725/GDS3726/GDS3726Q/GDS3727 is an IP Video Smart Door Station that functions as a high-definition IP surveillance camera and intercom, delivering secure access control and monitoring for buildings of all sizes.

Key features include:

- A wide 152° video viewing angle for full wall-to-wall coverage
- AI ISP image processing for enhanced video clarity
- Built-in IC/ID card reader, NFC chip, two microphones, and one speaker for intercom functionality
- Alarm-in and alarm-out support for integration with external security devices

The GDS3725/GDS3726/GDS3726Q/GDS3727 can be managed using Grandstream's GDS Manager 2 software, which allows full control over device settings, card management, and live video feeds.

With an advanced AI Image Sensor Processor (ISP) and powerful image algorithms, the GDS3725/GDS3726/GDS3726Q/GDS3727 delivers 1080p Full HD video, providing clear visibility up to 3 meters even under extremely low-light conditions.

Additional capabilities include:

- PoE support for streamlined installation
- Intelligent white LED lighting for nighttime visibility
- Motion detection, intrusion detection, and loitering detection for enhanced security
- Expandable DI (Alarm Inout), DO (Alarm Output), RS-485 control interfaces for additional device integration

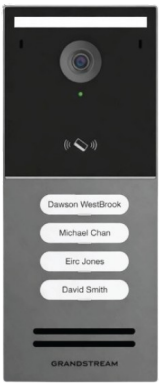
When used with Grandstream's GSC357X Control Station, GXV video phones, and GS-Wave mobile app, the GDS3725/GDS3726/GDS3726Q/GDS3727 offers a complete, end-to-end solution for access control, video intercom, and security recording.

PRODUCT OVERVIEW

Feature Highlights

The following table contains the major features of the GDS372x series.

GDS3725	2K ultra HD Camera, supports HDR and WDR, offers AI Intelligent Fill Light, and AI ISP. Strong security protection against external magnetic interference using Solid State Relay (SSR). Physical 15-key numeric keypad for PIN entry and local access control scenarios. Integrated bluetooth BLE 5.0. Supports multiple door opening methods, such as PIN, IC/ID cards, NFC, BLE, QR Code, SIP Call. Supports RFID cards, DTMF, remote PIN input, and Wiegand 26/34 input/output for integration with third-party systems. Compatible with SIP-based IPPBX systems and third-party NVRs (ONVIF Profile S & RTSP support). Supports AI-based behavior analsysis. Support Cloud and GDS Manager Application. IP66-rated for outdoor use and IK10-rated vandal resistance for both metal housing and lens area. Built-in dual microphone and speaker offers AI noise reduction.

GDS3726	2K ultra HD Camera, supports HDR and WDR, offers AI Intelligent Fill Light, and AI ISP. Strong security protection against external magnetic interference using Solid State Relay (SSR). Integrated bluetooth BLE 5.0. Supports multiple door opening methods, such as IC/ID cards, NFC, BLE, QR Code, SIP Call. Supports RFID cards, DTMF, remote PIN input, and Wiegand 26/34 input/output for integration with third-party systems. Compatible with SIP-based IPPBX systems and third-party NVRs (ONVIF Profile S & RTSP support). Supports AI-based behavior analsysis. Support Cloud and GDS Manager Application. IP66-rated for outdoor use and IK10-rated vandal resistance for both metal housing and lens area. Built-in dual microphone and speaker offers AI noise reduction.
 GDS3726Q	2K ultra HD Camera, supports HDR and WDR, offers AI Intelligent Fill Light, and AI ISP. Strong security protection against external magnetic interference using Solid State Relay (SSR). Integrated bluetooth BLE 5.0. Supports multiple door opening methods, such as IC/ID cards, NFC, BLE, QR Code, SIP Call. Compatible with SIP-based IPPBX systems and third-party NVRs (ONVIF Profile S & RTSP support). Supports AI-based behavior analsysis. Support Cloud and GDS Manager Application. IP66-rated for outdoor use and IK10-rated vandal resistance for both metal housing and lens area. Built-in dual microphone and speaker offers AI noise reduction. 4 customizable doorbell buttons
GDS3727	2K ultra HD Camera, supports HDR and WDR, offers AI Intelligent Fill Light, and AI ISP. Strong security protection against external magnetic interference using Solid State Relay (SSR). Integrated bluetooth BLE 5.0 and Dual-band Wi-Fi 6. Supports multiple door opening methods, such as IC/ID cards, NFC, BLE, QR Code, SIP Call. Compatible with SIP-based IPPBX systems and third-party NVRs (ONVIF Profile S & RTSP support). Supports AI-based behavior analsysis. Support Cloud and GDS Manager Application. IP66-rated for outdoor use with IK07-rated impact resistance. Built-in dual microphone and speaker offers AI noise reduction.

GDS372x Features at a Glance

Technical Specifications

The following table summarizes all the technical specifications, including the protocols/standards supported, voice codecs, telephony features, and upgrade/provisioning settings for GDS372x.

- GDS3725

Video Compression	H.264 High Profile / Main Profile / Base Profile, Motion JPEG
Image Sensor Resolution	1/3", 4MP, HDR
Lens Type	F2.2, FOV: 127°(H) x 70°(V) x 152°(D)
Day & Night	White light, 6x LED
Max Video Resolution	Video: up to 1920*1080, Snapshots: up to 1920*1080
Max Frame Rate	30 frames per second.

Wide Dynamic Range	Yes, up to 120dB.
PIR	Supported, 3-5 meters (10-16 feet)
AI ISP	Supported
Embedded Analytics	AI-based Motion detection
Microphone	Two mics
Speaker	3W
Application and GDS Manager	Support Cloud, SecureAccess Mobile App, and GDS Manager Application
Snapshots	Triggered upon events, sent to Email, FTP Server, GDS Manager, Cloud Server, SecureAccess App and/or Local.
Unlock Methods	SIP, HTTP API, Grandstream SecureAccess App, QR Code, RFID, NFC
Network Protocols	TCP/IP/UDP, HTTP/HTTPS, ARP/RARP, ICMP, DNS(A Record, SRV, NAPTR), DHCP, SSH, SMTP, TFTP, NTP, STUN, SIMPLE, TLS, SRTP, TR-069 mass provisioning, local upload firmware
Bluetooth	BLE 5.0
Telephony Features	SIP Paging, Multicast Paging, call-waiting with priority override, Account Sharing
Voice Codecs	G.711?/a, G.722 (wide-band), G.726-32, G.729 in-band and out-band DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Video Codecs	H.264
QoS	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, Ed25519 and X25519 based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control
Upgrade / Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file
Button	15-key numeric keypad 1 anti-tamper button (back) 1 reset button (inside)
RFID	13.56MHz&125kHz; MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Ultralight, MIFARE PLUS and MIFARE DESFire
RFID Number Supported	up to 5000
Access Control	2x Relay (SSR)
Alarm Input	3x Alarm in
Alarm Output	2x Alarm out
Network Interface	1x RJ45, One 10/100 Mbps port with integrated PoE
Expansion Interface	RS485, Wiegand 26/34 input and output, SD card slot
SD Card	Maximum capacity 256GB, requires Class 10 / V10 microSD (TF) card minimum, V30 or higher recommended.
Power & Green Energy Efficiency	DC power supply: DC 9-36V,12WPOE: 802.3af class 0
Ingress Protection	Weatherproof, vandal resistant, with support for wall bracket
Dimensions (H x W x D) and Weight	Unit: 204mm*87mm*35.5mmWeight: 1.56KGPackage Weight: 1.743KG
Interoperability	ONVIF (Profile S)
Package	GDS3725 Device, Quick Installation Guide, Wall Bracket, IC Card, Rain cover (optional)

Temperature and Humidity	Operating Temperature: - 30 - +60°C Operating Humidity: 10-90% (non condensing) Storage Temperature: -30 - +70°C Storage Humidity: 10-90% (non condensing)
Protection Class	IP66 (EN60529)IK10 (IEC62262) for both metal surface/buttons and lens area
Compliance	FCC, CE, RCM, IC, IP66, IK10

GDS3725 Technical Specifications

- GDS3726

Video Compression	H.264 High Profile / Main Profile / Base Profile, Motion JPEG
Image Sensor Resolution	1/3", 4MP, HDR
Lens Type	F2.2, FOV: 127°(H) x 70°(V) x 152°(D)
Day & Night	White light, 6x LED
Max Video Resolution	Video: up to 1920*1080, Snapshots: up to 1920*1080
Max Frame Rate	30 frames per second
Wide Dynamic Range	Yes, up to 120dB.
PIR	Supported, 3-5 meters (10-16 feet)
AI ISP	Supported
Embedded Analytics	AI-based Motion detection
Microphone	Two mics
Speaker	3W
Application and GDS Manager	Support Cloud, SecureAccess Mobile App, and GDS Manager Application
Snapshots	Triggered upon events, sent to Email, FTP Server, GDS Manager, Cloud Server, SecureAccess App and/or Local
Unlock Methods	SIP, HTTP API, Grandstream SecureAccess App, QR Code, RFID, NFC
Network Protocols	TCP/IP/UDP, HTTP/HTTPS, ARP/RARP, ICMP, DNS(A Record, SRV, NAPTR), DHCP, SSH, SMTP, TFTP, NTP, STUN, SIMPLE, TLS, SRTP, TR-069 mass provisioning, local upload firmware
Bluetooth	BLE 5.0
Telephony Features	SIP Paging, Multicast Paging, call-waiting with priority override, Account Sharing
Voice Codecs	G.711?/a, G.722 (wide-band), G.726-32, G.729 in-band and out-band DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Video Codecs	H.264
QoS	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, Ed25519 and X25519 based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control
Upgrade / Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file
Button	1 doorbell key 1 anti-tamper button (back) 1 reset button (inside)
RFID	13.56MHz&125kHz; MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Ultralight, MIFARE PLUS and MIFARE DESFire
RFID Number Supported	up to 5000

Access Control	2x Relay (SSR)
Alarm Input	3x Alarm in
Alarm Output	2x Alarm out
Network Interface	1x RJ45, One 10/100 Mbps port with integrated PoE
Expansion Interface	RS485, Wiegand 26/34 input and output, SD card slot
SD Card	Maximum capacity 256GB, requires Class 10 / V10 microSD (TF) card minimum, V30 or higher recommended.
Power & Green Energy Efficiency	DC power supply: DC 9-36V,12WPOE: 802.3af class 0
Ingress Protection	Weatherproof, vandal resistant, with support for wall bracket
Dimensions (H x W x D) and Weight	Unit: 204mm*87mm*35.5mmWeight: 1.55KGPackage Weight: 1.733KG
Interoperability	ONVIF (Profile S)
Package	GDS3726 Device, Quick Installation Guide, Wall Bracket, IC Card, Rain cover (optional)
Temperature and Humidity	Operating Temperature: - 30 - +60°C Operating Humidity: 10-90% (non condensing) Storage Temperature: -30 - +70°C Storage Humidity: 10-90% (non condensing)
Protection Class	IP66 (EN60529)IK10 (IEC62262) for both metal surface/buttons and lens area
Compliance	FCC, CE, RCM, IC, IP66, IK10

GDS3726 Technical Specifications

- GDS3726Q

Video Compression	H.264 High Profile / Main Profile / Base Profile, Motion JPEG
Image Sensor Resolution	1/3", 4MP, HDR
Lens Type	F2.2, FOV: 127°(H) x 70°(V) x 152°(D)
Day & Night	White light, 6x LED
Max Video Resolution	Video: up to 1920*1080, Snapshots: up to 1920*1080
Max Frame Rate	30 frames per second
Wide Dynamic Range	Yes, up to 120dB.
PIR	Supported, 3-5 meters (10-16 feet)
AI ISP	Supported
Embedded Analytics	AI-based Motion detection
Microphone	Two mics
Speaker	3W
Application and GDS Manager	Support Cloud, SecureAccess Mobile App, and GDS Manager Application
Snapshots	Triggered upon events, sent to Email, FTP Server, GDS Manager, Cloud Server, SecureAccess App and/or Local
Unlock Methods	SIP, HTTP API, Grandstream SecureAccess App, QR Code, RFID, NFC
Network Protocols	TCP/IP/UDP, HTTP/HTTPS, ARP/RARP, ICMP, DNS(A Record, SRV, NAPTR), DHCP, SSH, SMTP, TFTP, NTP, STUN, SIMPLE, TLS, SRTP, TR-069 mass provisioning, local upload firmware
Bluetooth	BLE 5.0

Telephony Features	SIP Paging, Multicast Paging, Call-waiting with priority override, Account Sharing
Voice Codecs	G.711?/a, G.722 (wide-band), G.726-32, G.729 in-band and out-band DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Video Codecs	H.264
QoS	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, Ed25519 and X25519 based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control
Upgrade / Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file
Button	4 Quick keys 1 Anti-tamper button (back) 1 Reset button (inside)
RFID	13.56 MHz & 125 kHz; MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Ultralight, MIFARE PLUS and MIFARE DESFire
RFID Number Supported	Up to 5000
Access Control	2x Relay (SSR)
Alarm Input	3x Alarm in
Alarm Output	2x Alarm out
Network Interface	1x RJ45, One 10/100 Mbps port with integrated PoE
Expansion Interface	RS485, Wiegand 26/34 input and output, SD card slot
SD Card	Maximum capacity 256GB, requires Class 10 / V10 microSD (TF) card minimum, V30 or higher recommended.
Power & Green Energy Efficiency	DC power supply: DC 9-36V,12WPOE: 802.3af class 3
Ingress Protection	Weatherproof, vandal resistant, with support for wall bracket
Dimensions (H x W x D) and Weight	Unit: 204mm*87mm*35.5mmWeight: 1.56 KG Package Weight: 1.743 KG
Interoperability	ONVIF (Profile S)
Package	GDS3726Q Device, Quick Installation Guide, Wall Bracket, IC Card, Rain cover (optional), Transparent Button Covers, Button Label Stickers.
Temperature and Humidity	Operating Temperature: - 30 - +60°C Operating Humidity: 10-90% (non condensing) Storage Temperature: -30 - +70°C Storage Humidity: 10-90% (non condensing)
Protection Class	IP66 (EN60529)IK10 (IEC62262) for both metal surface/buttons and lens area
Compliance	FCC, CE, RCM, IC, IP66, IK10

GDS3726Q Technical Specifications

- GDS3727

Video Compression	H.264 High Profile / Main Profile / Base Profile, Motion JPEG
Image Sensor Resolution	1/3", 4MP, HDR
Lens Type	F2.2, FOV: 127°(H) x 70°(V) x 152°(D)
Day & Night	White light, 6x LED
Max Video Resolution	Video: up to 1920*1080, Snapshots: up to 1920*1080
Max Frame Rate	30 frames per second.
Wide Dynamic Range	Yes, up to 120dB.

PIR	Supported, 3-5 meters (10-16 feet)
AI ISP	Supported
Embedded Analytics	AI-based Motion detection
Microphone	Two mics
Speaker	3W
Application and GDS Manager	Support Cloud, SecureAccess Mobile App, and GDS Manager Application
Snapshots	Triggered upon events, sent to Email, FTP Server, GDS Manager, Cloud Server, SecureAccess App and/or Local.
Unlock Methods	SIP, HTTP API, Grandstream SecureAccess App, QR Code, RFID, NFC
Network Protocols	TCP/IP/UDP, HTTP/HTTPS, ARP/RARP, ICMP, DNS(A Record, SRV, NAPTR), DHCP, SSH, SMTP, TFTP, NTP, STUN, SIMPLE, TLS, SRTP, TR-069 mass provisioning, local upload firmware
Bluetooth	BLE 5.0
Wi-Fi	Dual-band Wi-Fi 6, 802.11 a/b/g/n/ac/ax (2.4GHz & 5GHz)
Telephony Features	SIP Paging, Multicast Paging, call-waiting with priority override, Account Sharing
Voice Codecs	G.711?/a, G.722 (wide-band), G.726-32, G.729 in-band and out-band DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Video Codecs	H.264
QoS	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, Ed25519 and X25519 based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control
Upgrade / Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file
Button	1 doorbell key 1 anti-tamper button (back) 1 reset button (inside)
RFID	13.56MHz&125kHz; MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Ultralight, MIFARE PLUS and MIFARE DESFire
RFID Number Supported	up to 5000
Access Control	1x Relay (SSR)
Alarm Input	2x Alarm in
Alarm Output	1x Alarm out
Network Interface	1x RJ45, One 10/100 Mbps port with integrated PoE
Expansion Interface	RS485, SD card slot
SD Card	Maximum capacity 256GB, requires Class 10 / V10 microSD (TF) card minimum, V30 or higher recommended.
Power & Green Energy Efficiency	DC power supply: DC 12V,12WPOE: 802.3af class 0
Ingress Protection	Weatherproof, vandal resistant, with support for wall bracket
Dimensions (H x W x D) and Weight	Unit: 180.6mm*86.6mm*29mmWeight: 0.524KGPackage Weight: 0.721KG
Interoperability	ONVIF (Profile S)
Package	GDS3727 Device, Quick Installation Guide, Rain Cover, Wall Bracket, 13.56Mhz RFID Cards, Rain cover (optional)

Temperature and Humidity	Operating Temperature: - 30 - +60°C Operating Humidity: 10-90% (non condensing) Storage Temperature: -30 - +70°C Storage Humidity: 10-90% (non condensing)
Protection Class	IP66 (EN60529),IK07
Compliance	FCC, CE, RCM, IC, IP66, IK07

GDS3727 Technical Specifications

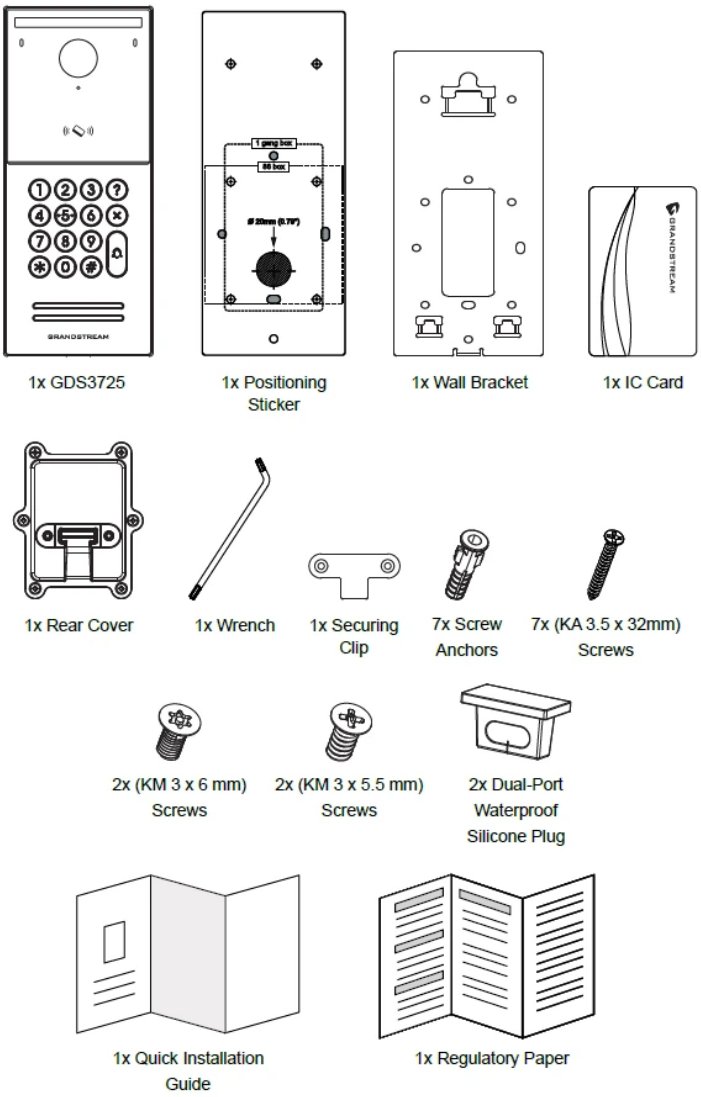
GETTING STARTED

This chapter provides basic installation instructions, including the list of the packaging contents and information for obtaining the best performance using the GDS372x series Video Smart Door Stations.

Equipment Packaging

- GDS3725

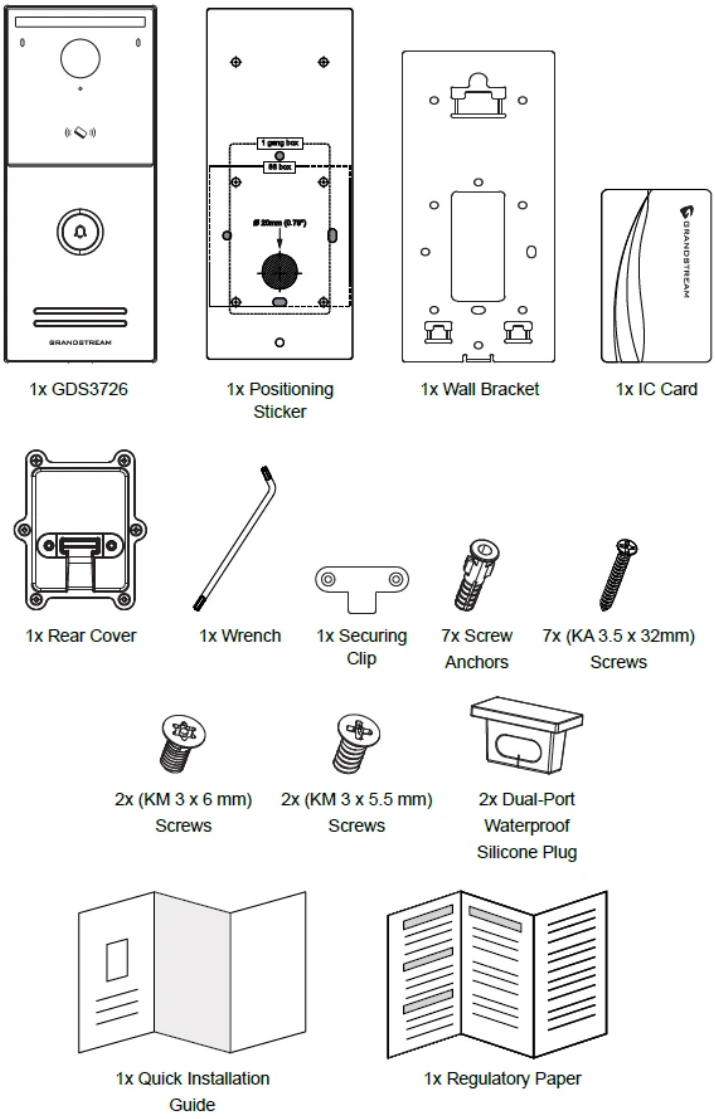
1 x GDS3725. 1 x Positioning Sticker. 1 x Wall Bracket. 1 x IC Card. 1 x Rear Cover. 1 x Wrench. 1 x Securing Clip.	7 x Screw Anchors. 7 x (ST 3.5 x 32mm) Screws. 2 x (M 3 x 6mm) Screws. 2 x (M 3 x 5.5mm) Screws. 2 x Dual-Port Waterproof Silicone Plug. 1 x Quick Installation Guide. 1 x Regulatory Paper.



GDS3725 Package Content

- GDS3726

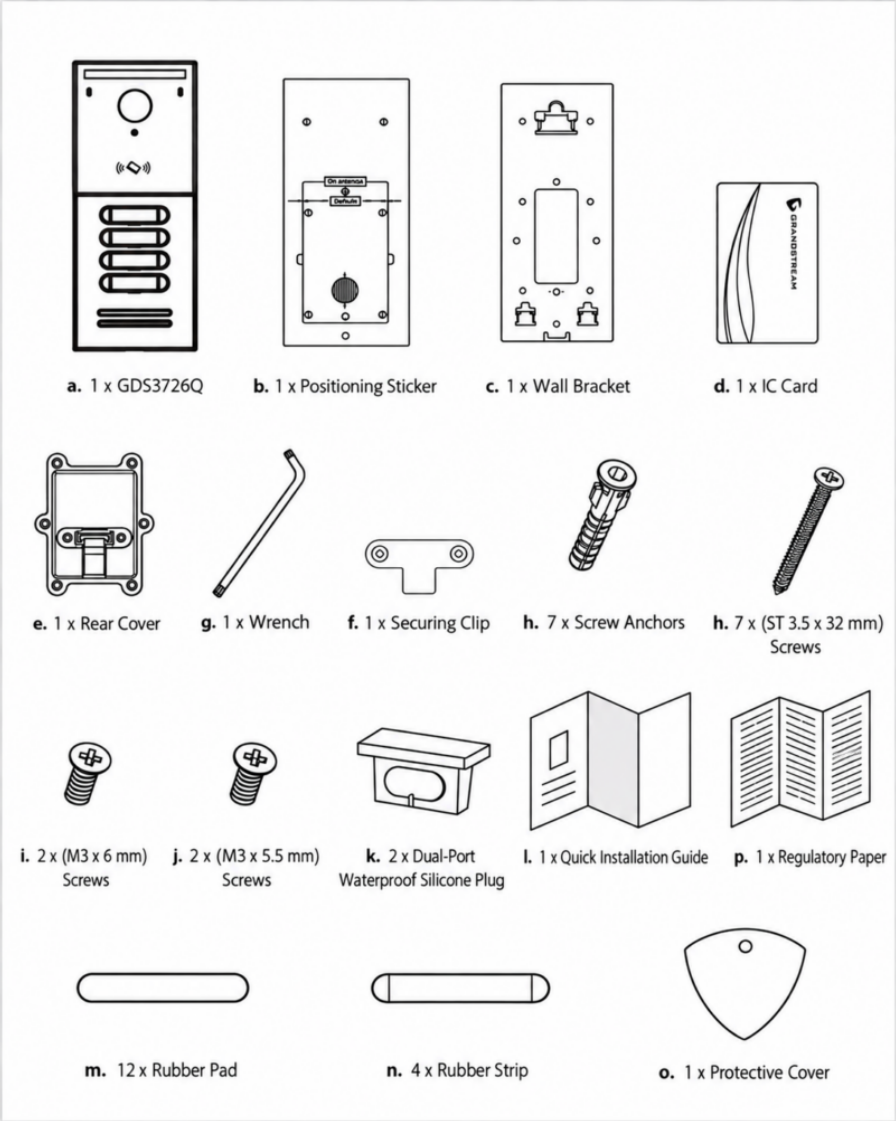
1 x GDS3726. 1 x Positioning Sticker. 1 x Wall Bracket. 1 x IC Card. 1 x Rear Cover. 1 x Wrench. 1 x Securing Clip.	7 x Screw Anchors. 7 x (ST 3.5 x 32mm) Screws. 2 x (M 3 x 6mm) Screws. 2 x (M 3 x 5.5mm) Screws. 2 x Dual-Port Waterproof Silicone Plug. 1 x Quick Installation Guide. 1 x Regulatory Paper.



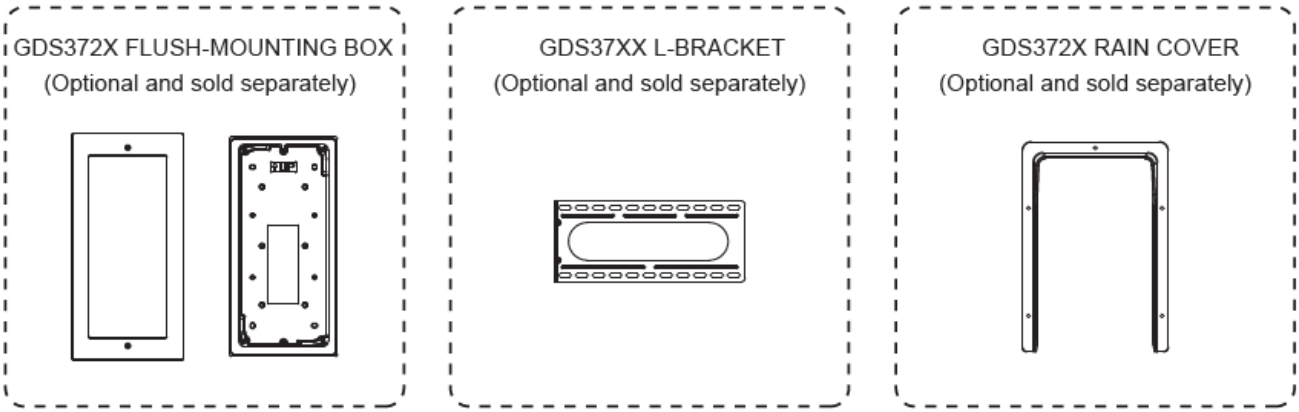
GDS3726 Package Content

- GDS3726Q

1 x GDS3726Q. 1 x Positioning Sticker. 1 x Wall Bracket. 1 x IC Card. 1 x Rear Cover. 1 x Wrench. 1 x Securing Clip. 12 x Rubber Pad	7 x Screw Anchors. 7 x (ST 3.5 x 32mm) Screws. 2 x (M 3 x 6mm) Screws. 2 x (M 3 x 5.5mm) Screws. 2 x Dual-Port Waterproof Silicone Plug. 1 x Quick Installation Guide. 1 x Regulatory Paper. 4 x Rubber Strip 1 x Protective Cover



In addition to the items included in the package, the following optional accessories are available separately and may be required for specific wall-mounting or in-wall installation configurations.

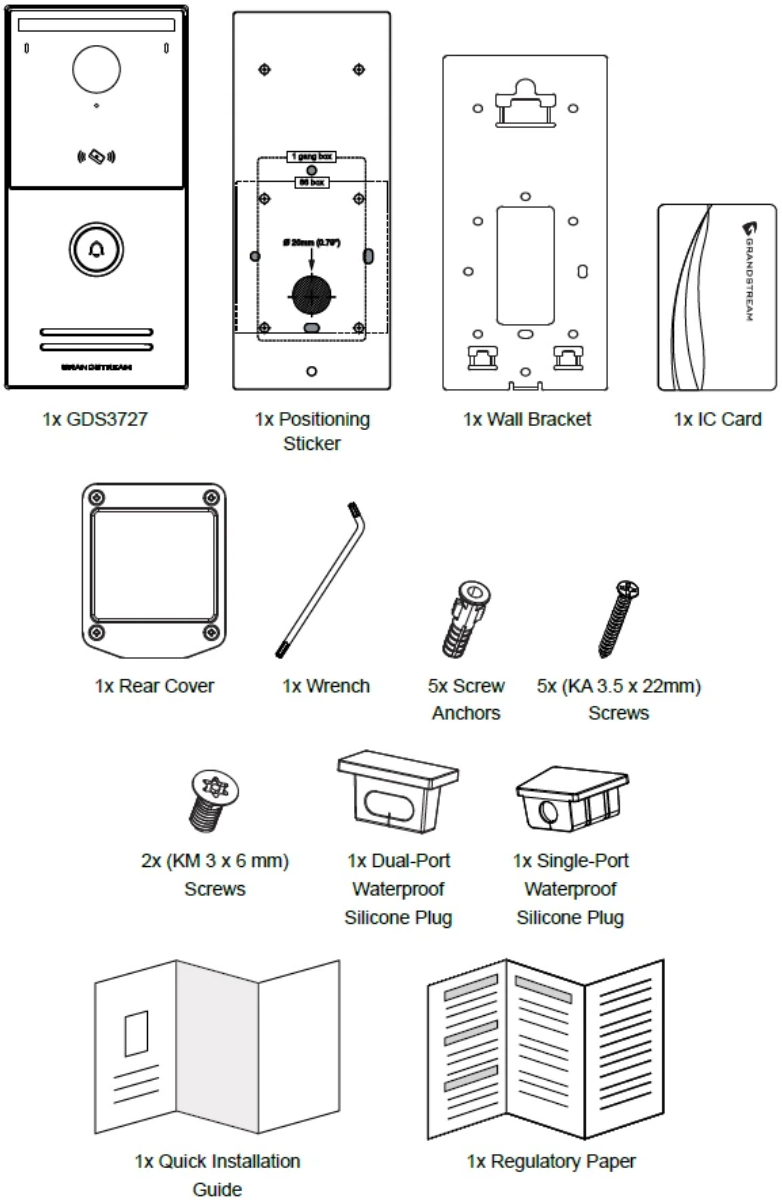


Accessory	Description	Availability
GDS372X Flush-Mounting Box	Flush-mounting box for in-wall installation of the GDS372X.	Optional; sold separately
GDS37XX L-Bracket	L-bracket for wall-mounting installation of the GDS37XX series.	Optional; sold separately
GDS372X Rain Cover	Protective rain cover for outdoor wall-mounted installation of the GDS372X.	Optional; sold separately

Check the package before installation. If you find anything missing, contact your system administrator.

- **GDS3727**

1 x GDS3727.1 x Positioning Sticker.1 x Wall Bracket.1 x IC Card.1 x Rear Cover.1 x Wrench.5 x Anchors.	5 x (KA 3.5 x 22mm) Screws.2 x (KM 3 x 6mm) Screws.1 x Dual-Port Waterproof Silicone Plug.1 x Single-Port Waterproof Silicone Plug.1 x Quick Installation Guide.1 x Regulatory Paper.



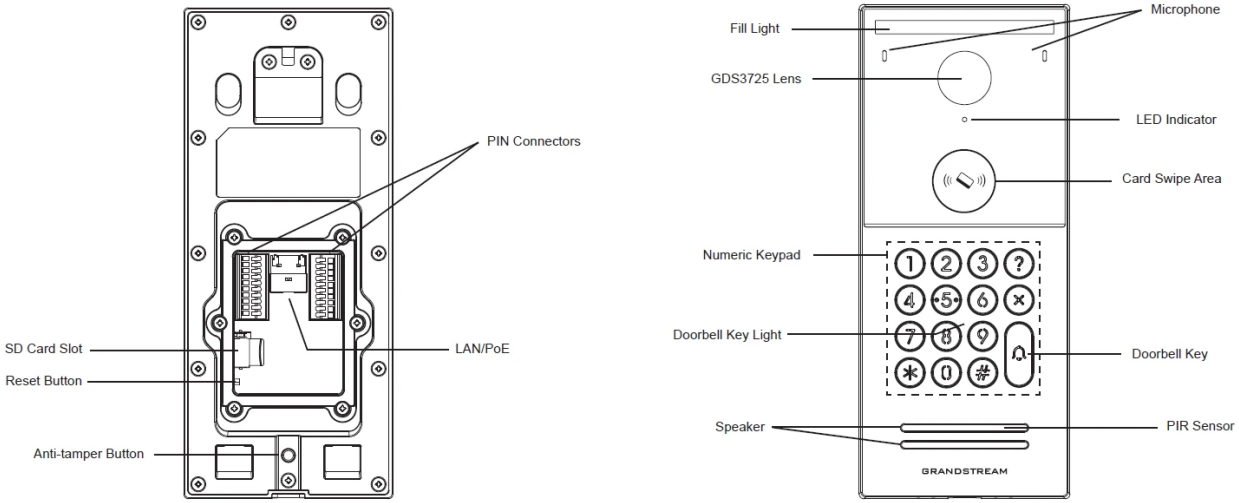
GDS3727 Package Content

Check the package before installation. If you find anything missing, contact your system administrator.

Description of the GDS372x

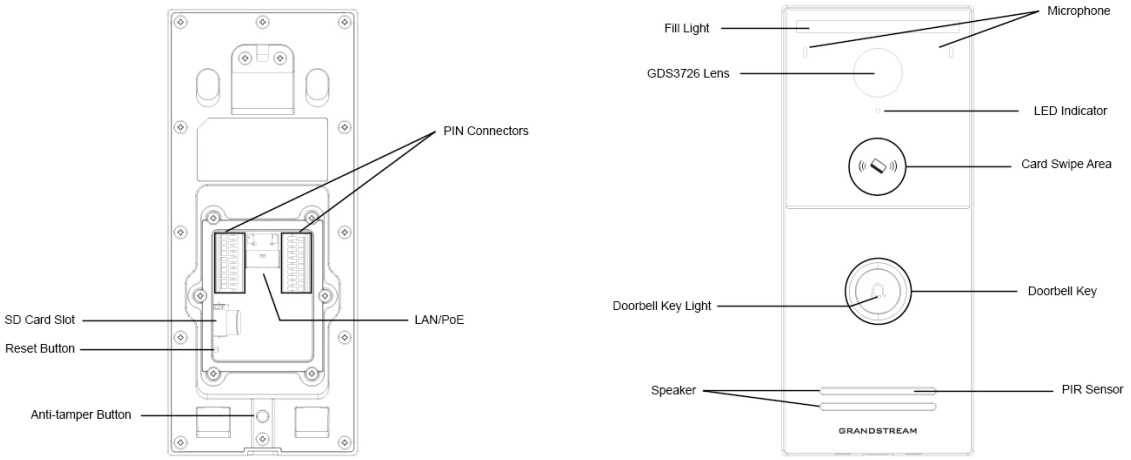
The figure below shows a description of the back and front views of the GDS372x series IP Video Smart Door Stations:

- **GDS3725**



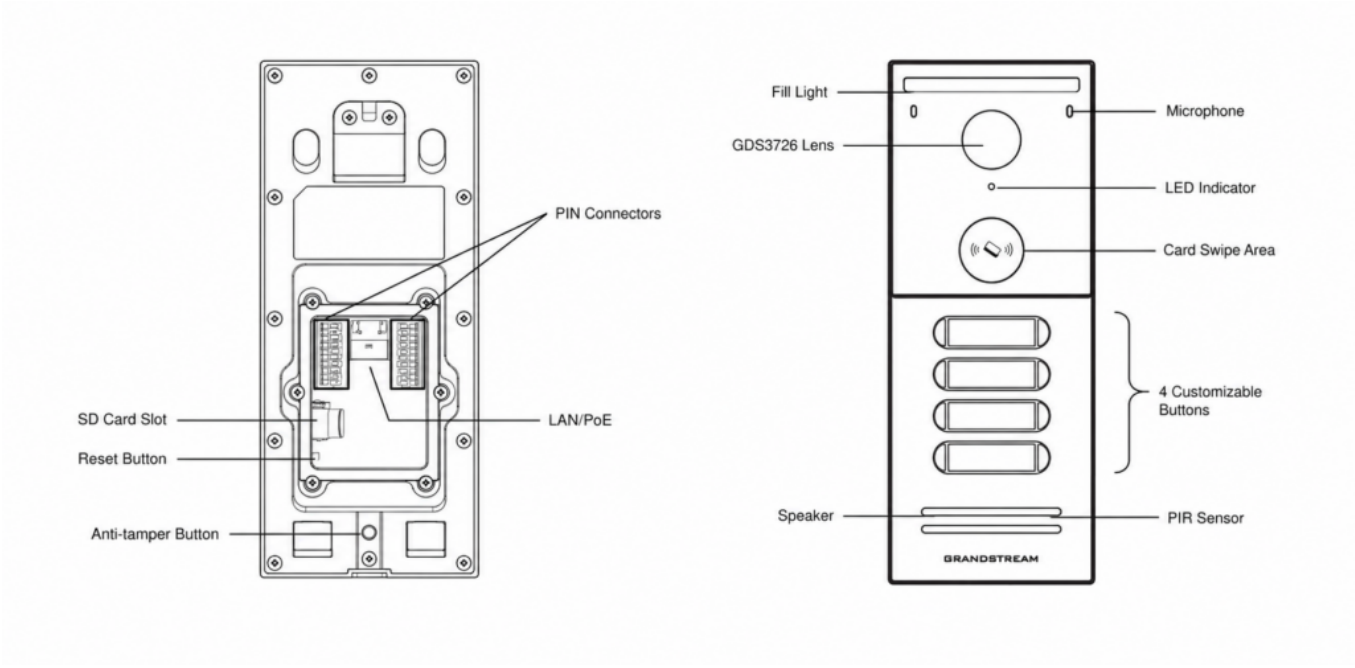
GDS3725 Front and Back View

- **GDS3726**



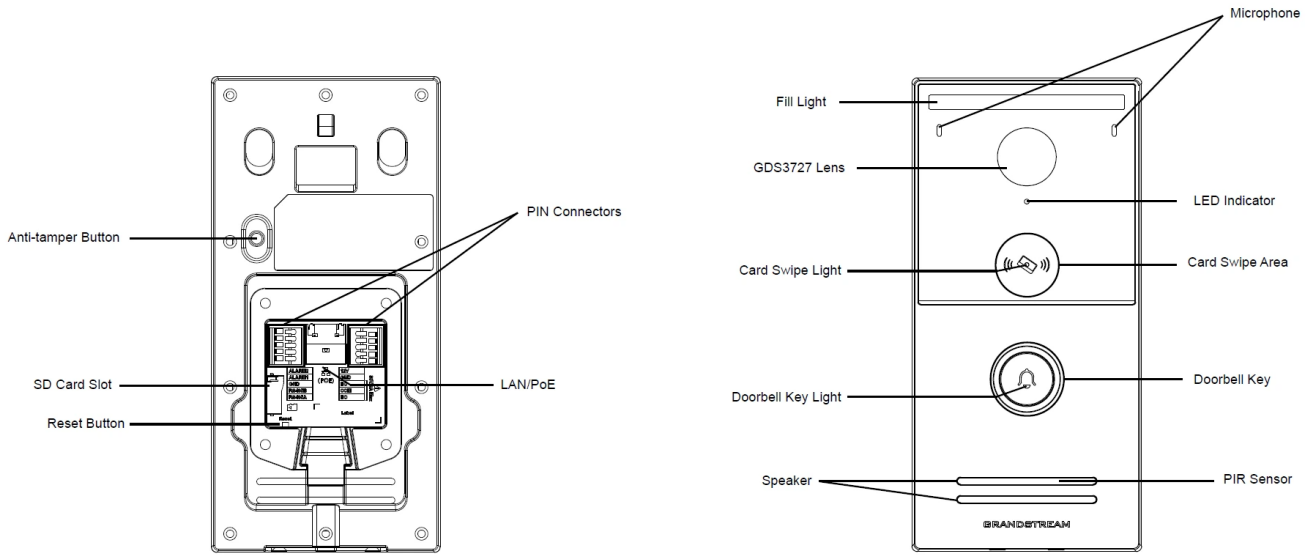
GDS3726 Front and Back View

- **GDS3726Q**



GDS3726Q Front and Back View

- **GDS3727**



GDS3727 Front and Back View

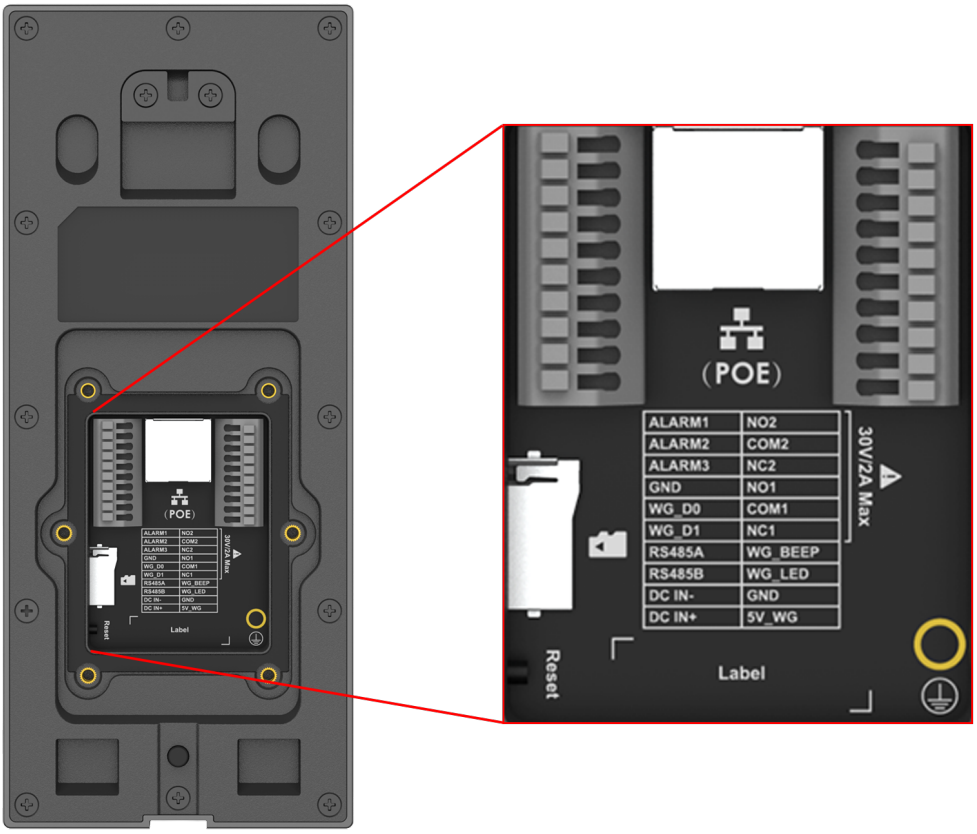
Front Keys Description

- **Fill Light** - Provides additional illumination in low-light environments, improving image quality for facial recognition, video calls, and surveillance. The fill light is automatically activated based on ambient lighting conditions when enabled in the device settings.
- **Microphone** - Captures audio during SIP calls, video intercom communication, and other voice-related functions. Multiple microphones provide enhanced voice pickup and improved noise reduction.
- **GDS372x Lens** - Captures live video for video calls, remote monitoring, facial recognition, and event recording. The wide-angle camera provides a clear view of visitors approaching the entrance.
- **LED Indicator** - Displays the current operating status of the device through different colors or flashing patterns, indicating events such as power status, call activity, registration status, or alarms.

- **Card Swipe Area** - Present a supported RFID or IC access card over the Card Swipe Area to authenticate and unlock the configured door. The device supports authorized cards configured locally or synchronized from the management platform.
- **Numeric Keypad (GDS3725 only)** - Use the Numeric Keypad to enter extension numbers, PIN codes, passwords, or other numeric information required for authentication or call placement.
- **Manager Key (GDS3725 only)** - Press the **Manager Key** to immediately place a call to the contact(s) configured under **Manager Key Setting** on the device's web interface. This key provides one-touch dialing for quick access to the designated manager or administrator.
- **Clear Key (X) (GDS3725 only)** - Press the **Clear Key (X)** to immediately delete all digits currently entered on the keypad and begin a new input. This allows users to quickly correct an incorrect entry without waiting for the configured **No Key Input Timeout (s)** to expire before entering new digits.
- **Doorbell Key Light** - Illuminates the Doorbell Key, making it easier to locate and operate in low-light conditions. The illumination may also indicate device status or user interaction depending on the system configuration.
- **Doorbell Key** - Press the **Doorbell Key** to immediately place a call to the contact(s) configured under **Doorbell Settings** on the device's web interface. This key provides one-touch dialing for quick access to the configured doorbell destination(s).
- **Speaker** - Outputs audio during SIP calls, doorbell communication, voice prompts, and system notifications, enabling two-way communication with visitors.
- **PIR Sensor** - Detects motion by sensing changes in infrared energy within its detection area. It can be used to trigger events such as visitor detection, video recording, or automatic wake-up of the device, depending on the configured settings.

GDS372x Wiring Connection

The GDS3725 provides a terminal block interface for power, relay control, alarm integration, RS-485 communication, and Wiegand input/output. Below is a detailed explanation of each pin and its function:



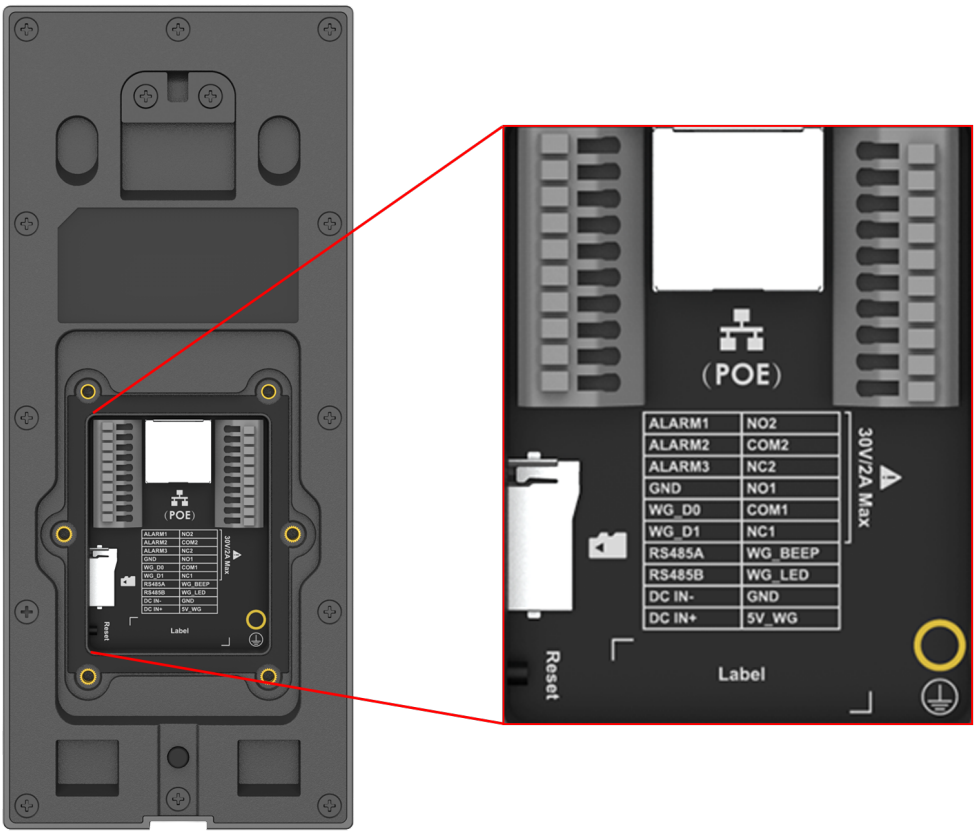
GDS3725 Wiring Connection

Connector	Function	Note
Network Port(PoE)	Ethernet and PoE Supply	Single 10/100Mbps network port, supports 802.3 af PoE power supply.
ALARM1	Alarm Input 1	Input for external devices (e.g., door contacts, sensors, or exit buttons).
ALARM2	Alarm Input 2	
ALARM3	Alarm Input 3	
GND	Alarm Ground	Common ground reference for alarm inputs.
RS485A	RS485 Communication (+)	Positive line for RS485 differential signal.
RS485B	RS485 Communication (-)	Negative line for RS485 differential signal.
DC IN-	Power Supply (-)	Negative terminal for DC power input.
DC IN+	Power Supply (+)	Positive terminal for DC power input. Supports a wide voltage range DC 9V-36V.
NO2	Relay Output2	For "Fail Secure" (Locked when Power Lost) Strike, connect COM2 & NO2. For "Fail Safe" (Open when No Power) Magnetic Lock, connect COM2 & NC2.Relay: 30VDC/2A.
COM2		
NC2		
NO1	Relay Output1	For "Fail Secure" (Locked when Power Lost) Strike, connect COM1 & NO1. For "Fail Safe" (Open when No Power) Magnetic Lock, connect COM1 & NC1.Relay: 30VDC/2A.
COM1		
NC1		
WG_BEEP	Wiegand Buzzer Control	Output to trigger the external Wiegand reader buzzer.

WG_LED	Wiegand LED Control	Output to control the LED status of the external Wiegand reader.
GND	Wiegand Ground	Ground for the Wiegand signal and power lines.
5V_WG	Wiegand Power Supply	Provides 5V power for an external Wiegand reader.
? (Chassis Ground)	Frame Ground	Screw/metal ring used to connect the device frame to the building's earth ground for surge protection and EMI shielding.
SD Card Slot	Data Storage	Maximum capacity 256GB.
Reset Button	System Reset	Press and hold to restore to factory defaults.
PIR	Motion Detection	Supported, detects motion 3-5 meters (10-16 feet) in front of the device.
Tamper Button	Tamper Detection	It prevents violent demolition.

GDS3725 Wiring Connection

The GDS3726 provides a terminal block interface for power, relay control, alarm integration, RS-485 communication, and Wiegand input/output. Below is a detailed explanation of each pin and its function:



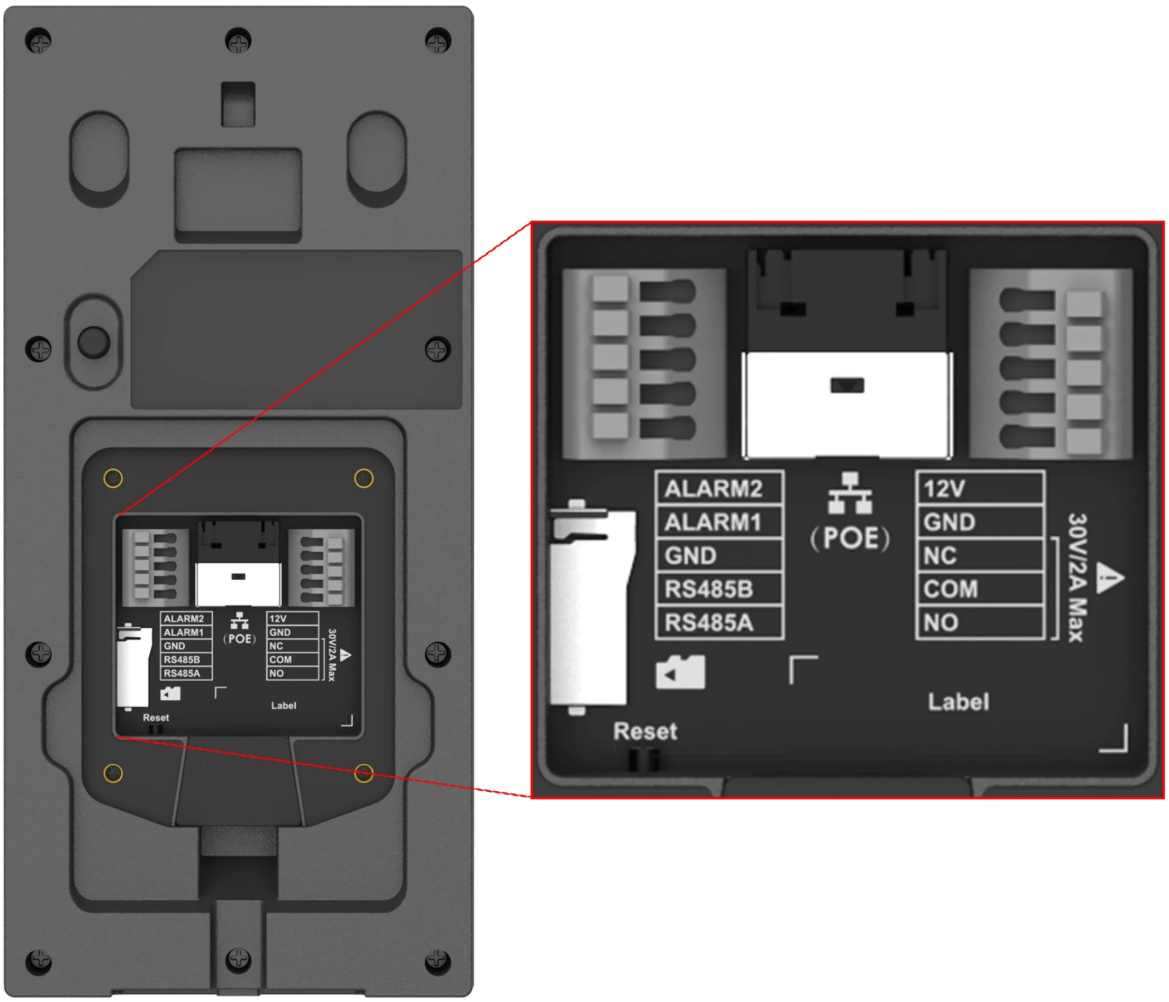
GDS3726 Wiring Connection

Connector	Function	Note
Network Port(PoE)	Ethernet and PoE Supply	Single 10/100Mbps network port, supports 802.3 af PoE power supply.
ALARM1	Alarm Input 1	Input for external devices (e.g., door contacts, sensors, or exit buttons).
ALARM2	Alarm Input 2	

ALARM3	Alarm Input 3	
GND	Alarm Ground	Common ground reference for alarm inputs.
RS485A	RS485 Communication (+)	Positive line for RS485 differential signal.
RS485B	RS485 Communication (-)	Negative line for RS485 differential signal.
DC IN-	Power Supply (-)	Negative terminal for DC power input.
DC IN+	Power Supply (+)	Positive terminal for DC power input. Supports a wide voltage range DC 9V-36V.
NO2	Relay Output2	For "Fail Secure" (Locked when Power Lost) Strike, connect COM2 & NO2. For "Fail Safe" (Open when No Power) Magnetic Lock, connect COM2 & NC2.Relay: 30VDC/2A.
COM2		
NC2		
NO1	Relay Output1	For "Fail Secure" (Locked when Power Lost) Strike, connect COM1 & NO1. For "Fail Safe" (Open when No Power) Magnetic Lock, connect COM1 & NC1.Relay: 30VDC/2A.
COM1		
NC1		
WG_BEEP	Wiegand Buzzer Control	Output to trigger the external Wiegand reader buzzer.
WG_LED	Wiegand LED Control	Output to control the LED status of the external Wiegand reader.
GND	Wiegand Ground	Ground for the Wiegand signal and power lines.
5V_WG	Wiegand Power Supply	Provides 5V power for an external Wiegand reader.
? (Chassis Ground)	Frame Ground	Screw/metal ring used to connect the device frame to the building's earth ground for surge protection and EMI shielding.
SD Card Slot	Data Storage	Maximum capacity 256GB.
Reset Button	System Reset	Press and hold to restore to factory defaults.
PIR	Motion Detection	Supported, detects motion 3-5 meters (10-16 feet) in front of the device.
Tamper Button	Tamper Detection	It prevents violent demolition.

GDS3726 Wiring Connection

The GDS3727 provides a terminal block interface for power, relay control, alarm integration, and RS-485 communication. Below is a detailed explanation of each pin and its function:



GDS3727 Wiring Connection

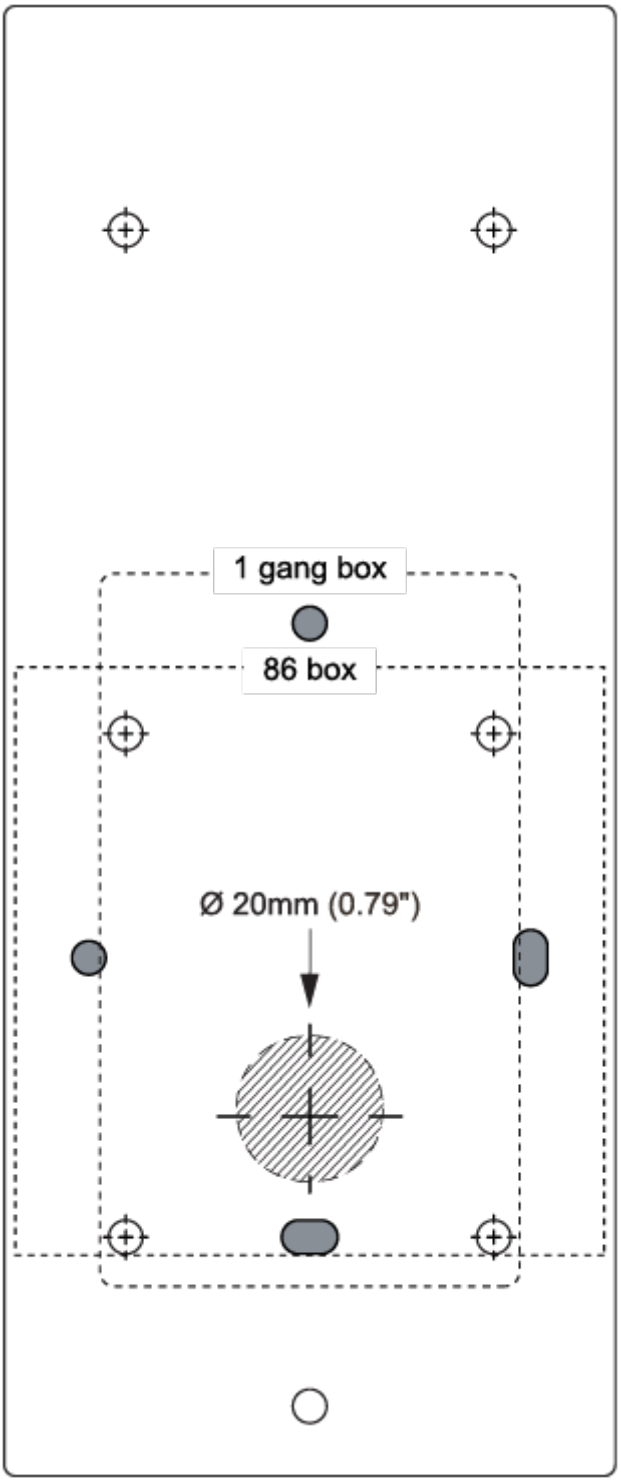
Connector	Function	Note
Network Port(PoE)	Ethernet and PoE Supply	Single 10/100Mbps network port, support 802.3 af PoE power supply.
GND	Power Supply	DC 12V, 1A Minimum.
12V		
NC	Relay Output	For "Fail Secure" (Locked when Power Lost) Strike, connect COM & NO. For "Fail Safe" (Open when No Power) Magnetic Lock, connect COM & NC.Relay: 30VDC/2A.
COM		
NO		
ALARM2	Alarm Input	Trigger input pins for external devices such as door sensors, exit buttons, or intrusion detectors.
ALARM1		
GND	Alarm GND	Ground reference specifically for Alarm1 and Alarm2.
RS485B	RS485 Communication	Differential signal pair for serial communication using the RS485 protocol.
RS485A		
SD Card Slot	Data Storage	Maximum capacity 256GB.
Reset Button	System Reset	Press and hold to restore to factory defaults.
PIR Sensor	Motion Detection	Detects motion 3-5 meters (10-16 feet) in front of the device.
Tamper Button	Tamper Detection	It prevents violent demolition.

GDS372x Wall Mount Installation

This section provides step-by-step instructions for mounting the GDS372x IP Video Door System, using the GDS3725 model as an example, on a wall using one of the available installation methods:

- With a 1-gang box
- With an 86 box
- Direct wall mount (no box)

A **positioning sticker** is included in the package to ensure accurate and aligned mounting across all installation types.

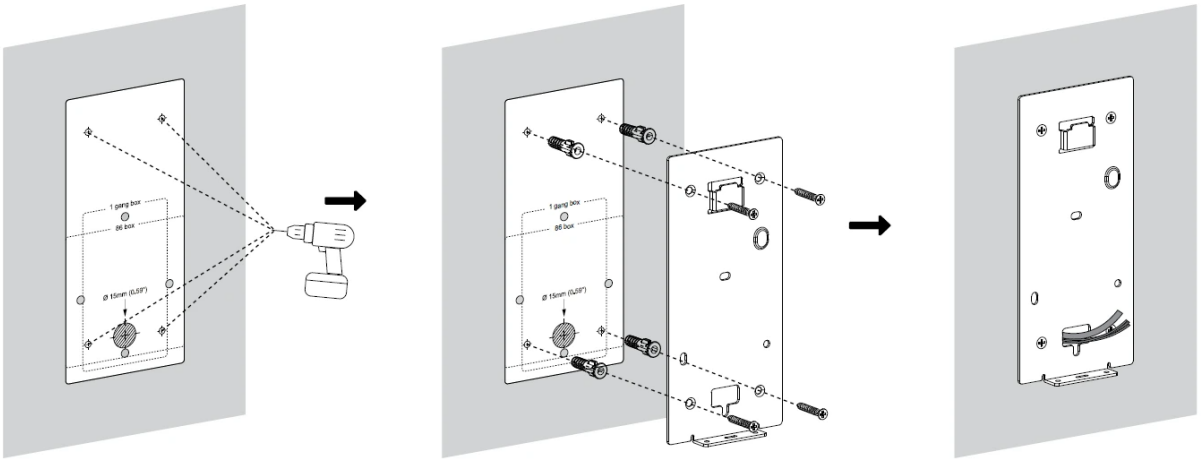


Please follow these steps carefully to ensure a weather-protected and tamper-resistant installation:

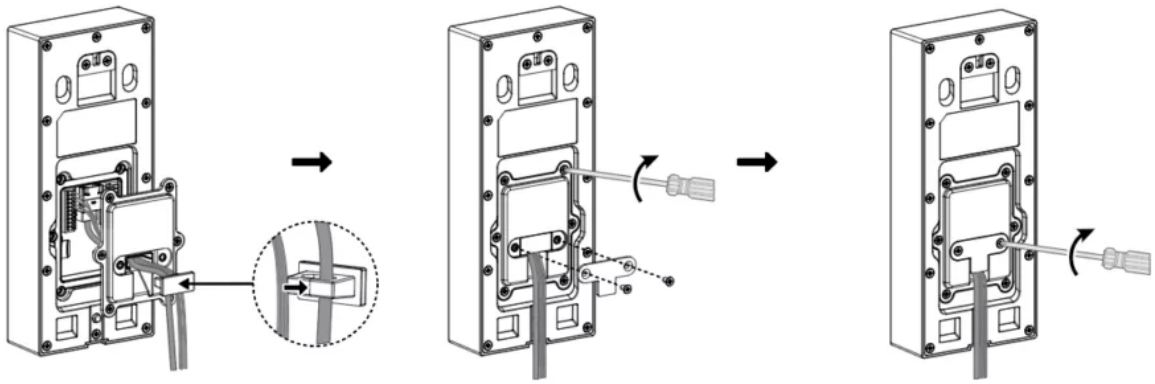
1. Place the provided **positioning sticker** on the wall at the desired mounting height.
2. Using the markings on the sticker as a guide, drill holes at the indicated positions.

Drill patterns may vary depending on the selected installation method (1-gang box, 86 box, or direct wall mount).

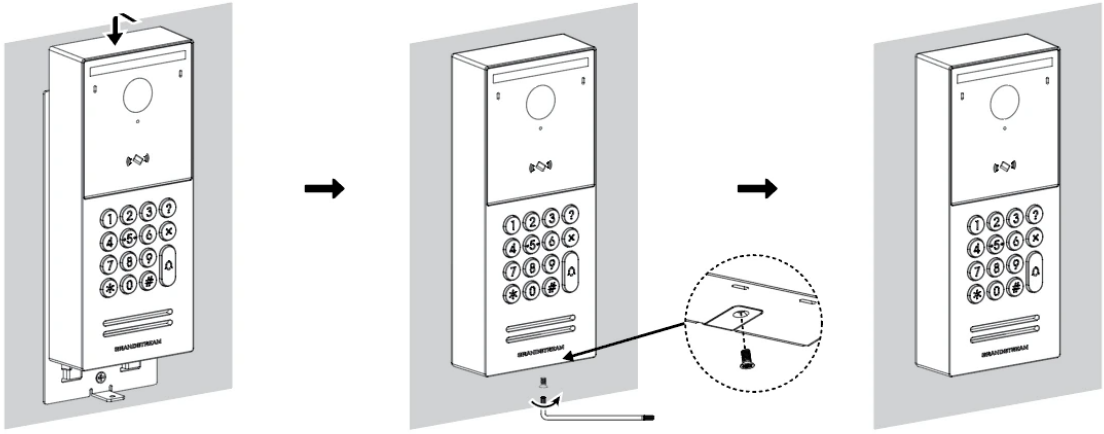
3. Insert the supplied **screw anchors** into the holes.
4. Secure the **wall-mounted bracket** using the included **KA 3.5 x 22mm self-tapping screws**.



5. Route the necessary cables (power, network, door strike, etc.) through the center opening of **the bracket**.
6. Insert the **waterproof silicone port plug** into the cable exit area at the bottom of the **rear cover** to protect and organize the cables.
7. Place the **rear cover** onto the bracket, aligning it with the screw holes.
8. Secure the rear cover by placing the **securing clip** on top of it.
9. Fix the securing clip included in the package.



10. Place the device onto the wall-mounted bracket.
11. Use a wrench to tighten the **KM 3 x 6mm screw**, securing the door station to the bracket.

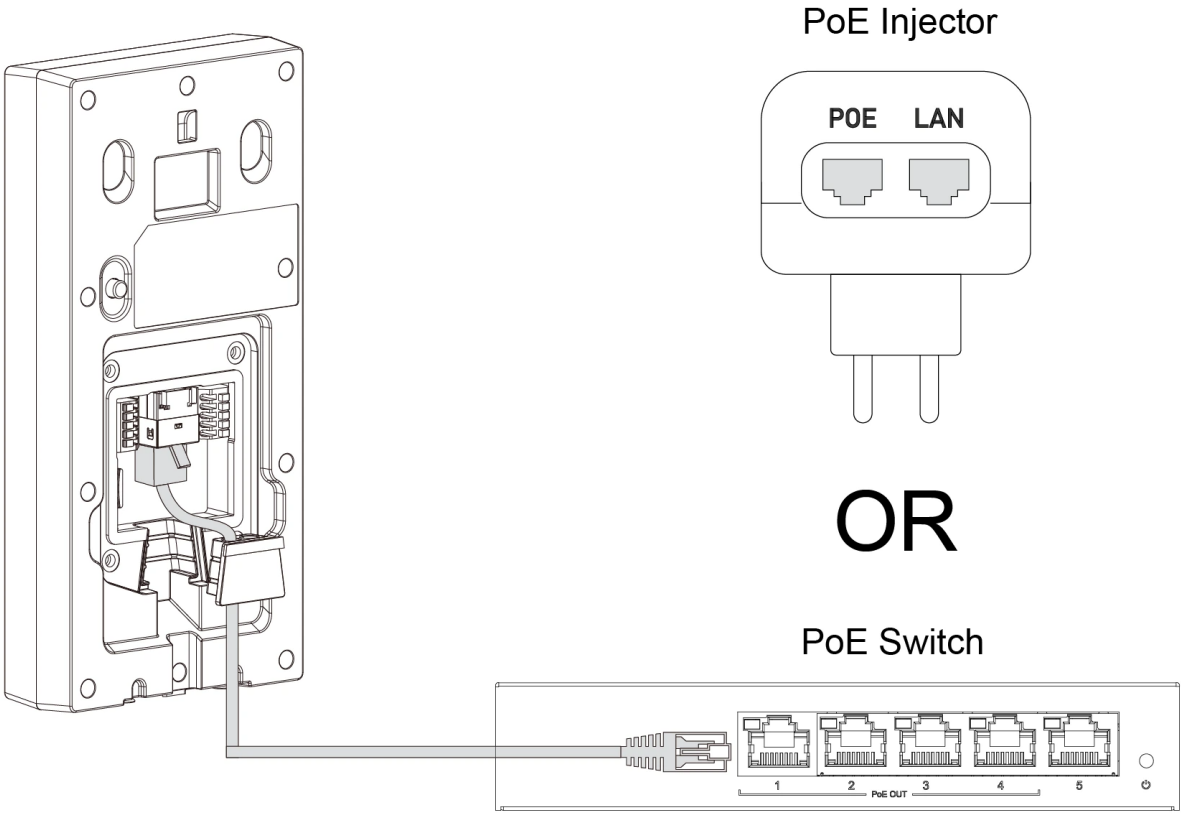


Powering the GDS372x

The GDS372x IP Video Smart Door Station can be powered using PoE or PSU:

Using PoE (Suggested)

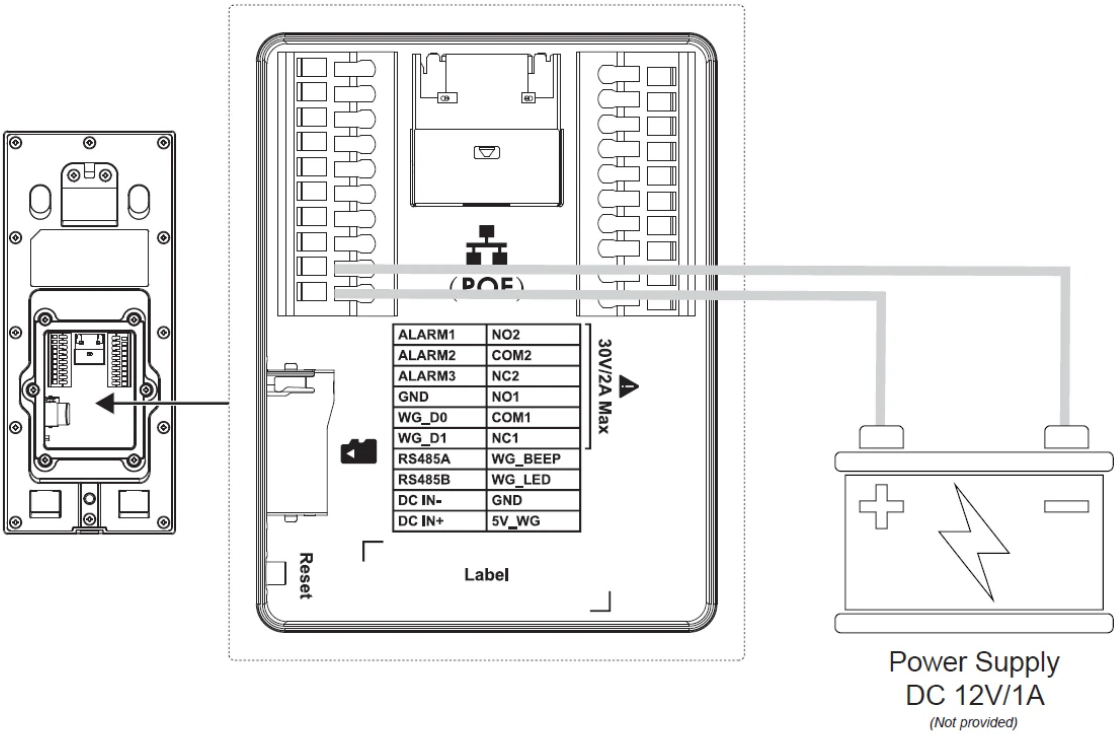
- Connect the other end of the RJ45 cable to the PoE switch.
- A PoE injector can be used if a PoE switch is not available.



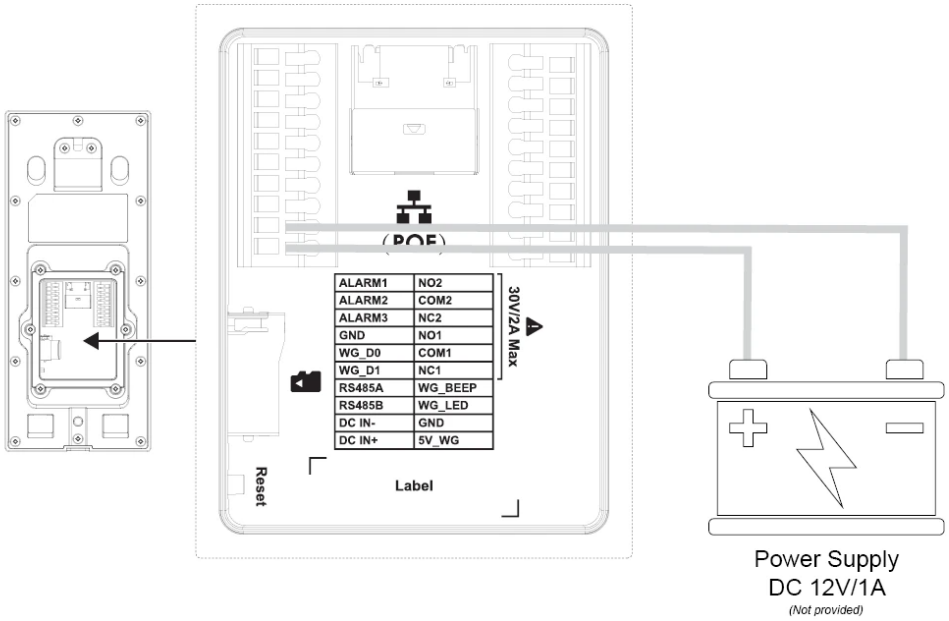
Powering the GDS372x Using PoE

Using Power Supply Unit (Not Provided)

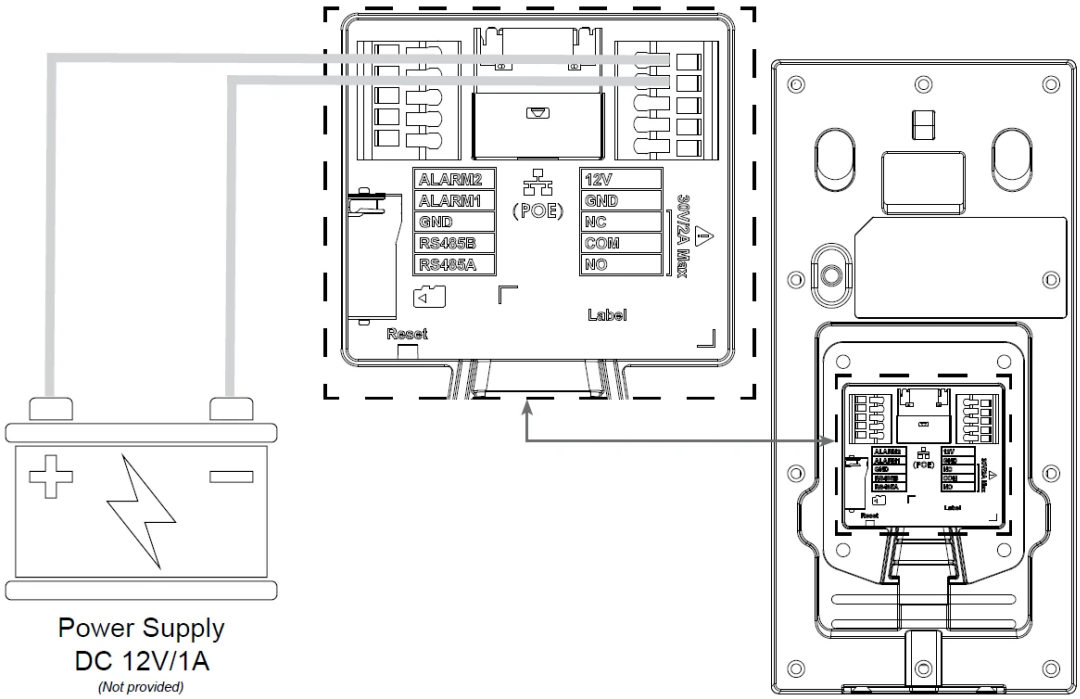
- Connect the other end of the RJ45 cable to a network switch or router.
- Connect a DC 12V power source via the related cable to the correct pins of the GDS372x.



Powering the GDS3725 using a Power Supply



Powering the GDS3726 using a Power Supply



Powering the GDS3727 using a Power Supply

GDS372x LED Lights and Backlights

The GDS372X features LED lights and key backlights to provide visual feedback for device status and operation. Their description and configuration options are outlined in this section.

LED Indicator

The following table lists the GDS372x LED indicator colors and flashing patterns.

LED Status	Description
LED off	Device in normal standby mode.
Solid Red	No network connection.
Slow Flashing Red	Pending events (such as missed calls or new SIP voicemails) or door access authentication failed.
Fast flashing Red	Alarm triggered.
Solid Green	Call in progress.
Slow Flashing Green	Outgoing call or incoming call ringing.
Fast flashing Green	Call on hold, or door access authentication succeeded.
Solid Blue	SD card formatting, or BLE/NFC mode active.
Slow Flashing Blue	IP announcement or card enrollment mode active.
Fast flashing Blue	Device rebooting, restoring factory settings, or powering on.
Fast Flashing White	Firmware upgrade in progress. The LED indicator, key backlight, and card reading light flash simultaneously.

- **Fast Flashing:** The LED remains on for 0.5 seconds, then off for 0.5 seconds.
- **Slow Flashing:** The LED remains on for 1 second, then off for 1 second.
- The GDS3726Q keypad LED indicator lights green during firmware upgrade.

Card Reader LED Light

The Card Reader LED provides visual feedback during card access operations and card enrollment. Its behavior can be configured on the Web UI under **System Settings -> Preferences -> Light Settings**.

Off: The Card Reader LED remains off at all times.

On: The Card Reader's white LED remains steadily lit in standby mode and flashes once slowly when a card is swiped.

- **Card verification successful:** The Card Reader LED flashes once slowly, while the Status LED turns green for 1 second.
- **Card verification failed:** The Card Reader LED flashes once slowly, while the Status LED turns red for 1 second.
- **Card enrollment mode:** The Card Reader LED is not affected by this setting. It continues to flash slowly until card enrollment is complete, while the Status LED flashes blue slowly.

Key Blacklight

The Key Light Mode setting can be configured on the Web UI under **System Settings -> Preferences -> Light Settings**. Three options are available, as described in the table below:

Model	Key LEDs	Options
GDS3725	12 x White Key LEDs1 x Green Key LED1 x Red Key LED1 x Blue Key LED	Always On: The key backlights remains on (Default).Keypress Always On: The keys backlights remains off and turns green when the key is pressed.Disable: The key backlights
GDS3726/GDS3727	1 x Green Key LED	

GDS372X ACCESS AND CONFIGURATION

The GDS372x includes an embedded web server that responds to HTTP/HTTPS GET and POST requests. This allows users to configure and manage the device through any standard web browser.

To begin configuration, please refer to the sections below.

- To access the GDS372x web interface, your computer must be connected to the same local network (subnet) as the GDS372x. (This is typically done by connecting your computer to the **same router, hub, or network switch** as the device.)
- If no hub or switch is available (or if all ports are in use), you can also connect the GDS372x **directly to your PC's Ethernet port** using a network cable and configure both devices with compatible static IP addresses.

Accessing the GDS372x via Dynamic IP (DHCP)

By default, the GDS372x is configured to automatically obtain an IP address from a DHCP server, such as your network router. This method is suitable for most typical office or home setups.

To connect the GDS372x to your network, please follow the instructions below:

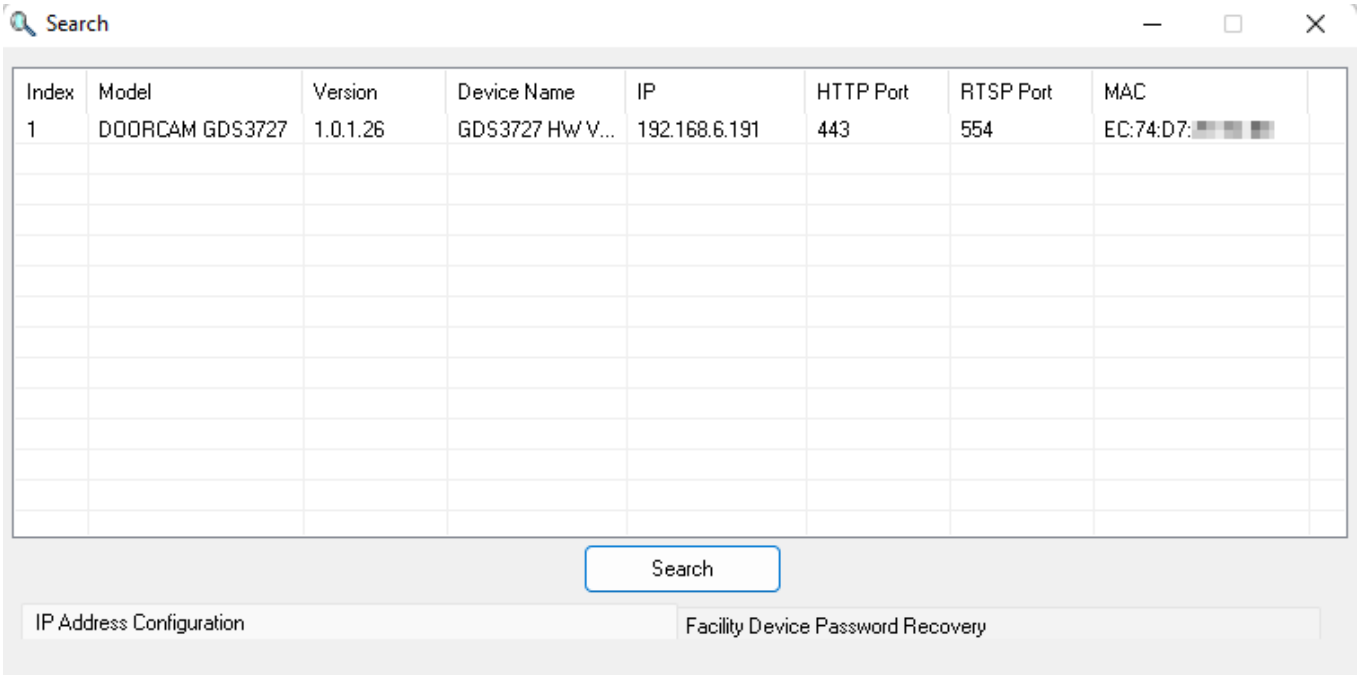
1. Use an Ethernet cable to connect the GDS372x to a router, network switch, or access point with DHCP enabled.
2. **Power the device** using **one** of the following methods:

   - **PoE (Power over Ethernet):** The GDS372x supports **IEEE 802.3af Class 3**, allowing it to receive power and data over a single Ethernet cable.
   - **Power Adapter:** Connect a DC 12V power source via the related cable to the correct pins of the GDS372x.
3. After the device powers on, it will receive an IP address from the DHCP server. You can locate this IP using the tools mentioned in the following sections.

Using GS Search to Retrieve the GDS372x IP Address

GS Search is a program that is used to detect and capture the IP address of the Grandstream facility management solution devices. Below are instructions for using the "GS Search" utility tool:

1. Download the GS Search utility tool from the Grandstream website using the following link: GS_Search
2. Double-click on the downloaded file, and the search window will appear.
3. Click on the "Search" button to start the discovery for Grandstream devices.
4. The detected devices will appear in the output field as shown below.



GS Search Discovery

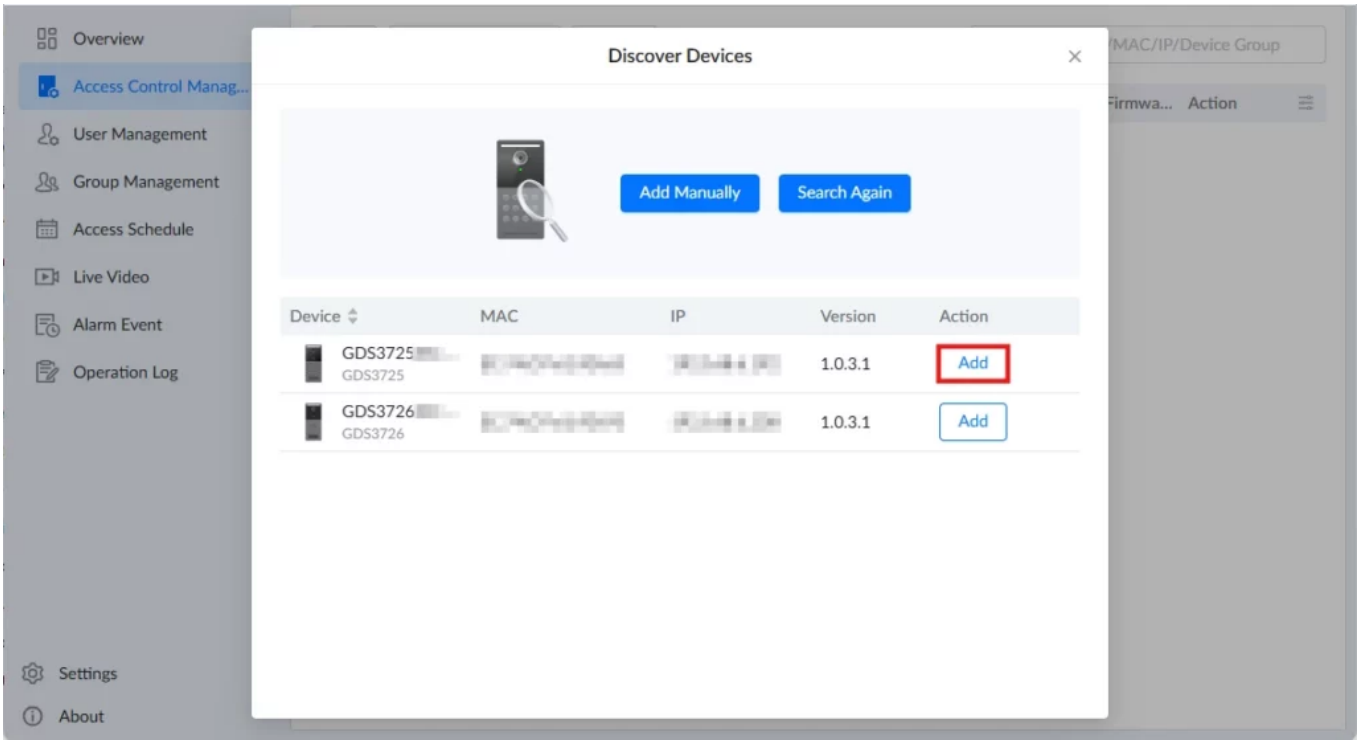
Using the GDS Manager 2 Utility Tool to Retrieve the GDS372x IP Address

Users can retrieve the IP address assigned to the GDS3725/GDS3726/GDS3726Q/GDS3727 from the DHCP server log or by using the Grandstream GDS Manager 2 application after installing the free utility provided by Grandstream.

Before discovering the device, ensure that **GDS Manager Mode** is enabled on the GDS3725/GDS3726/GDS3726Q//GDS3727. If GDS Manager Mode is disabled, the device will not be detected by GDS Manager 2.

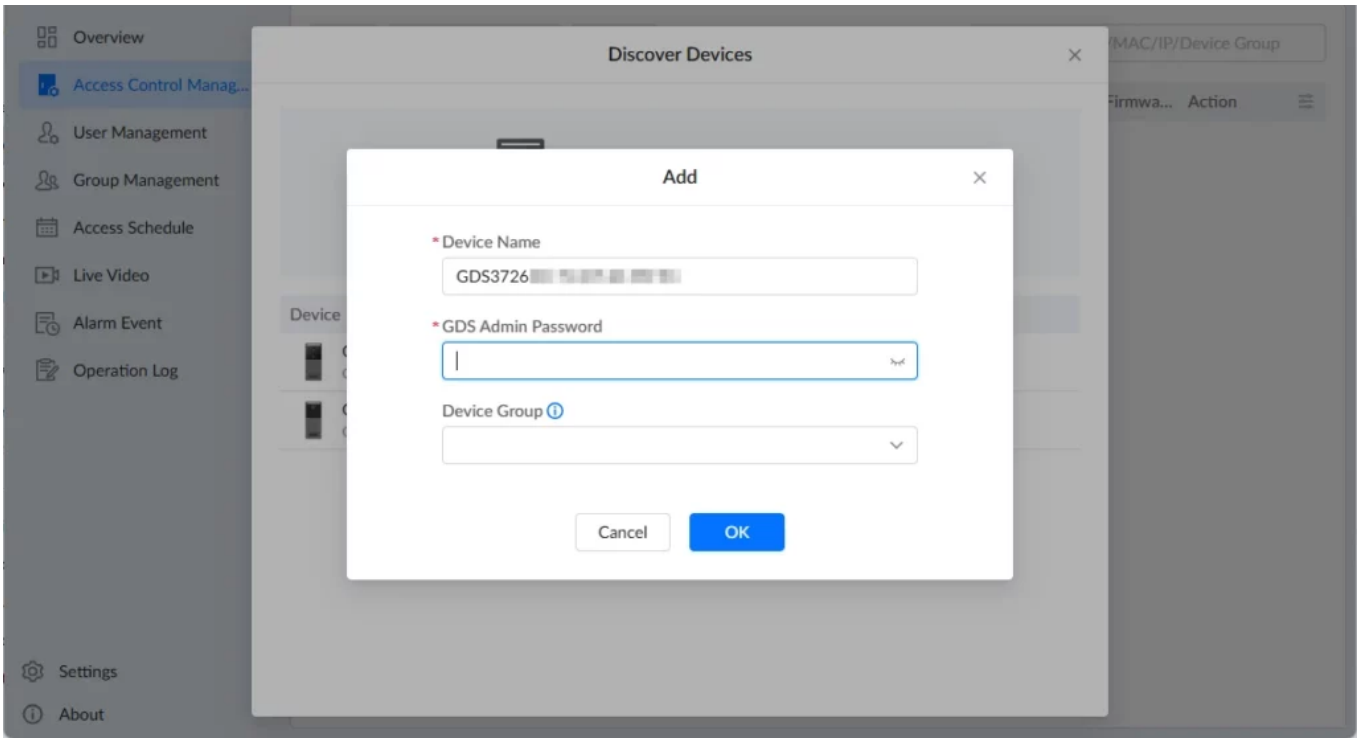
GDS372x Enable GDS Manager Mode

- Download and install the **GDS Manager 2** application on a Windows computer. GDS Manager 2 requires a 64-bit version of Windows 10 or later. You can download the software through the following link: https://www.grandstream.com/hubfs/Support%20Tools/GDSManager2_v1.1.16_for_windows.zip
- Launch **GDS Manager 2** and complete the initial setup by configuring an Access Password and specifying the application data storage path. Log in using the configured Access Password.
- On the GDS Manager 2 interface, access **Access Control Management** and click **Add** to open the **Discover Devices** window.



GDS Manager 2 -> Access Control Management -> Discovered Devices

- In the **Discover Devices** window, GDS Manager 2 will display the devices detected on the local network. If necessary, click **Search Again** to perform another device discovery.
- Locate the desired GDS3725/GDS3726/GDS3726Q in the discovered device list. The list displays information including the device name, MAC address, IP address, and firmware version.
- Click **Add** next to the desired device, enter the device's **Admin Password**, assign it to a **Device Group** if applicable, and click **OK**.



GDS Manager 2 -> Access Control Management -> Add Discovered Device

- The device will then be added to **Access Control Management**, where its assigned **IP address and port number** can be viewed in the **IP** field.

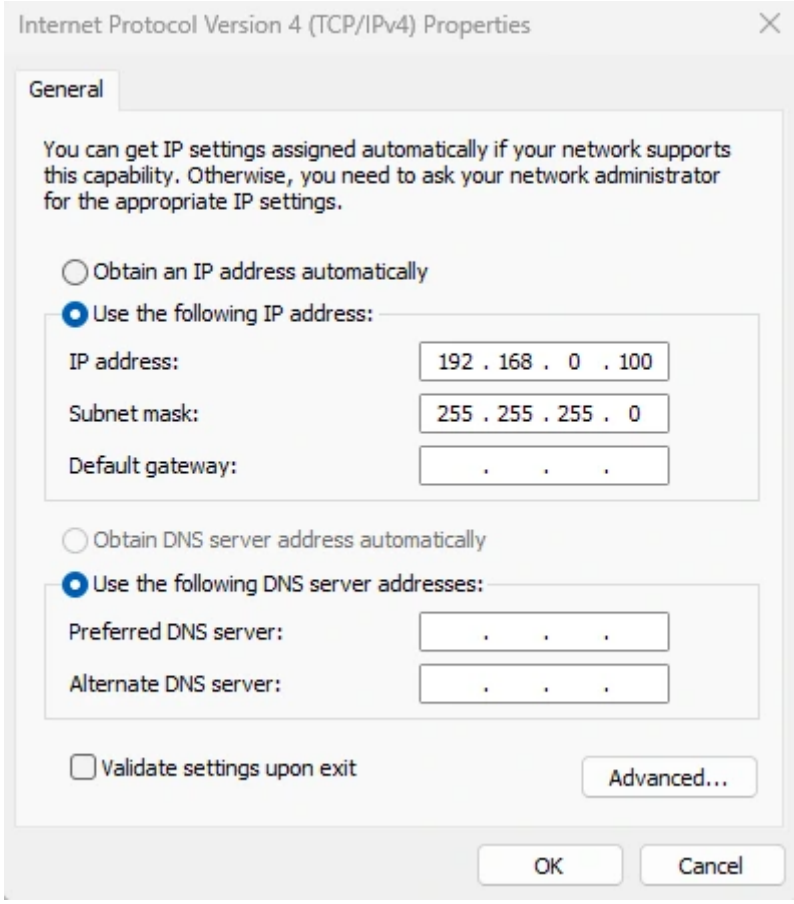
If the GDS3725/GDS3726/GDS3726Q does not appear during device discovery, verify that GDS Manager Mode is enabled on the device under Access Control Settings -> Basic Settings -> Access Control Settings -> GDS Manager.

Accessing the GDS372x via Static IP

If there is no DHCP server in the network, or the GDS372x does not get an IP from the DHCP server, users can connect the GDS372x to a computer directly, using a static IP to configure the GDS372x.

If no DHCP server is available or the DHCP request times out (after 3 minutes), the GDS372x will use its default static IP address: **192.168.0.160**

1. Connect the Ethernet cable from GDS372x to the computer network port directly.
2. Configure the computer using Static IP: **192.168.0.XXX** (1<XXX<255, **except for 160**) and configure the "Subnet mask" to "**255.255.255.0**". Leave the "Default Gateway" to "**Blank**" like below:



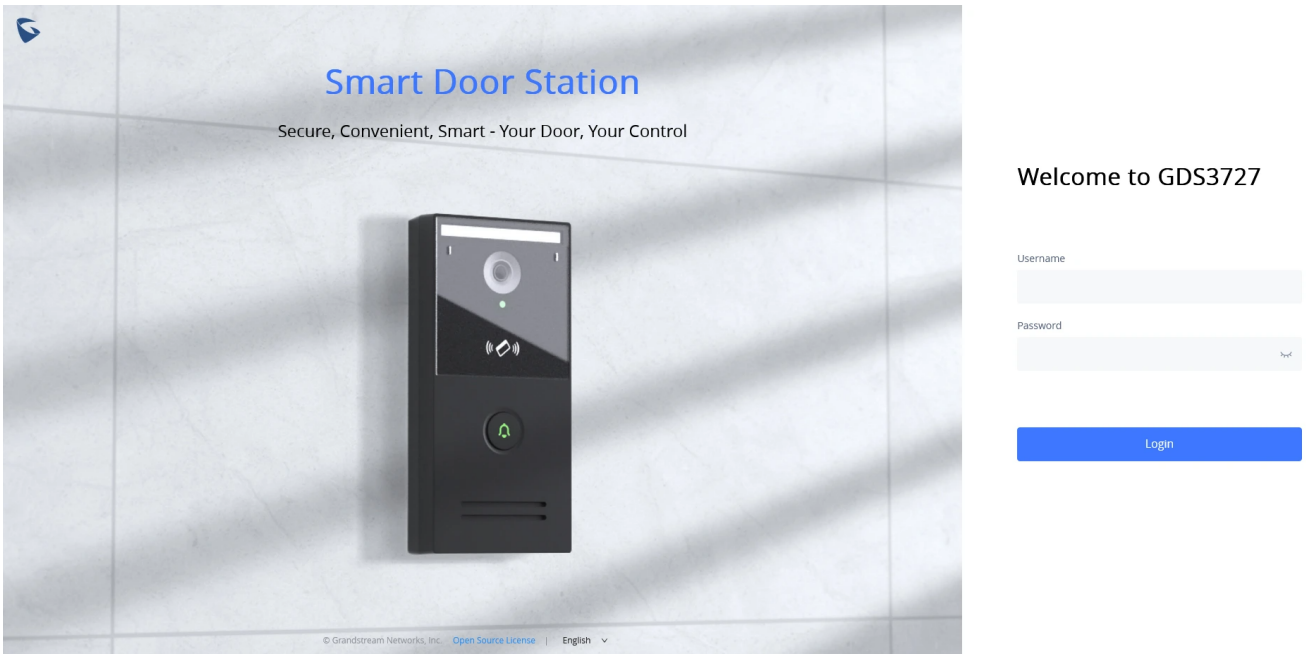
Static IP on Windows

4. Power on the GDS372x using a PoE injector or external DC power.
5. Enter **192.168.0.160** in the address bar of the browser to access the GDS372x Web UI.

GDS372x Web UI Login

Once the GDS372x is accessed through its IP address (whether static or dynamically assigned), the embedded Web User Interface (Web UI) will load in the browser. This interface allows administrators to configure and manage the device.

Upon accessing the Web UI, a **login screen** will appear, prompting for credentials:

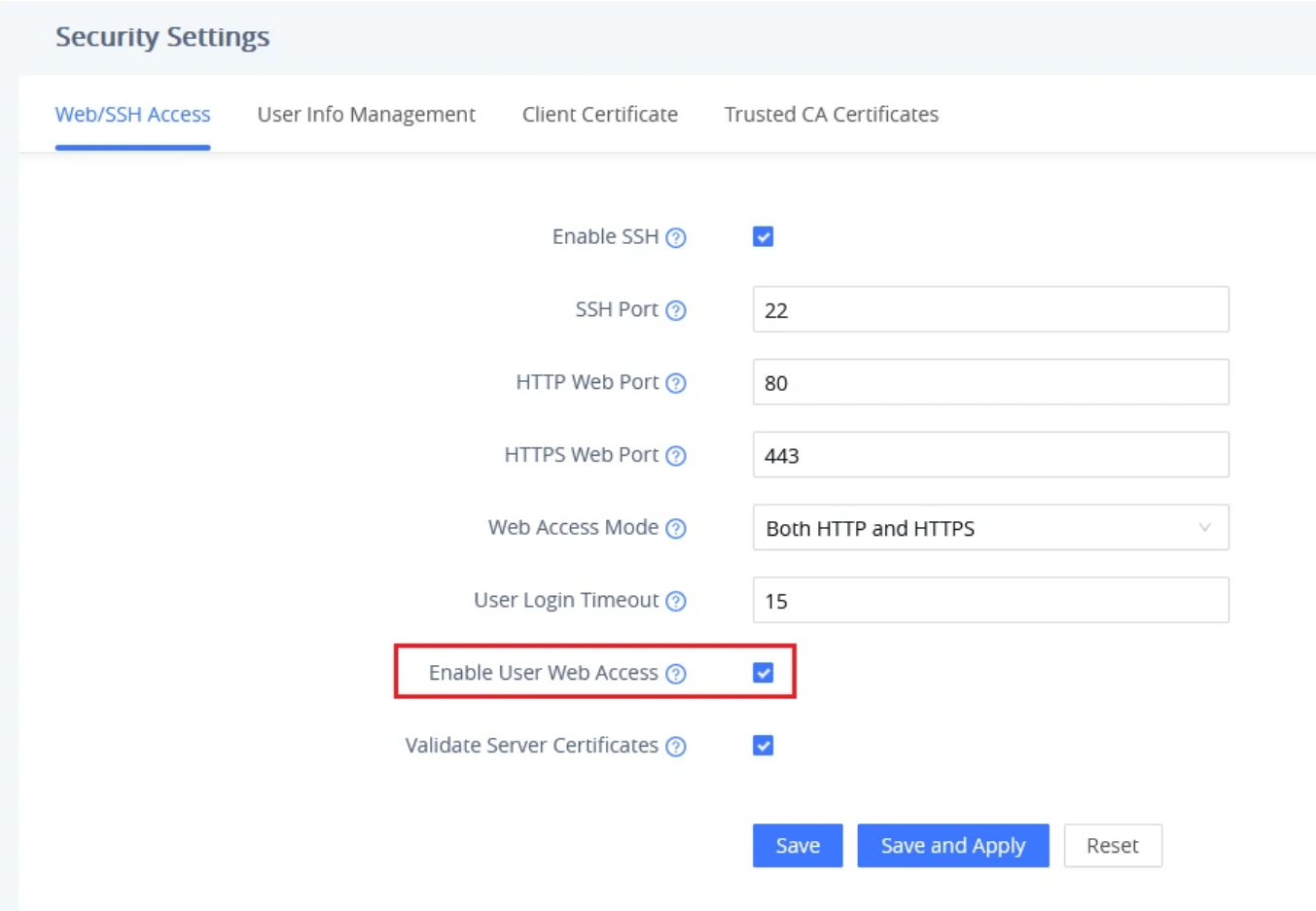


GDS372x Web UI Login

There are two default passwords for the login page:

User Level	User	Password	Web Pages Allowed
End User Level	user	123	Status Real-time Preview Calls Phone Settings Network Settings System Settings Maintenance Diagnostic
Administrator Level	admin	Random password available on the sticker at the back of the unit.	All pages

- Upon first logging into the Web UI, users will be prompted to **change the default administrator/user password**. This is a mandatory step for security purposes and must be completed before proceeding with any configuration.
- User-level access requires the option "Enable User Web Access" to be enabled in the security settings of the device (disabled by default).



Enable User Web Access

Saving and Applying Configuration Changes

After logging into the GDS372x Web UI and making any configuration changes, users must take action to ensure those changes are saved and applied correctly.

- Pressing the **"Save"** button will store the changes temporarily, but **they will not take effect** until the user clicks the **"Apply"** button at the top of the Web UI.
- Alternatively, users can simply click **"Save and Apply"** to save the settings and apply them immediately.

While most settings take effect after applying changes, it is recommended to reboot or power cycle the device to ensure all configurations are fully loaded and operational. This step is essential to finalize configurations that require a reboot, such as network settings.

To reboot the device remotely:

- Click the **"Reboot"** button located in the top-right corner of the Web UI.
- The browser will display a reboot message. Wait approximately **1 minute** before logging in again.

Pairing GDS372x with the SecureAccess App via Bluetooth

This section describes how to put your GDS372X device into BLE mode to pair it with the Grandstream mobile application SecureAccess for initial setup and management.

Before you begin, please note the following important points:

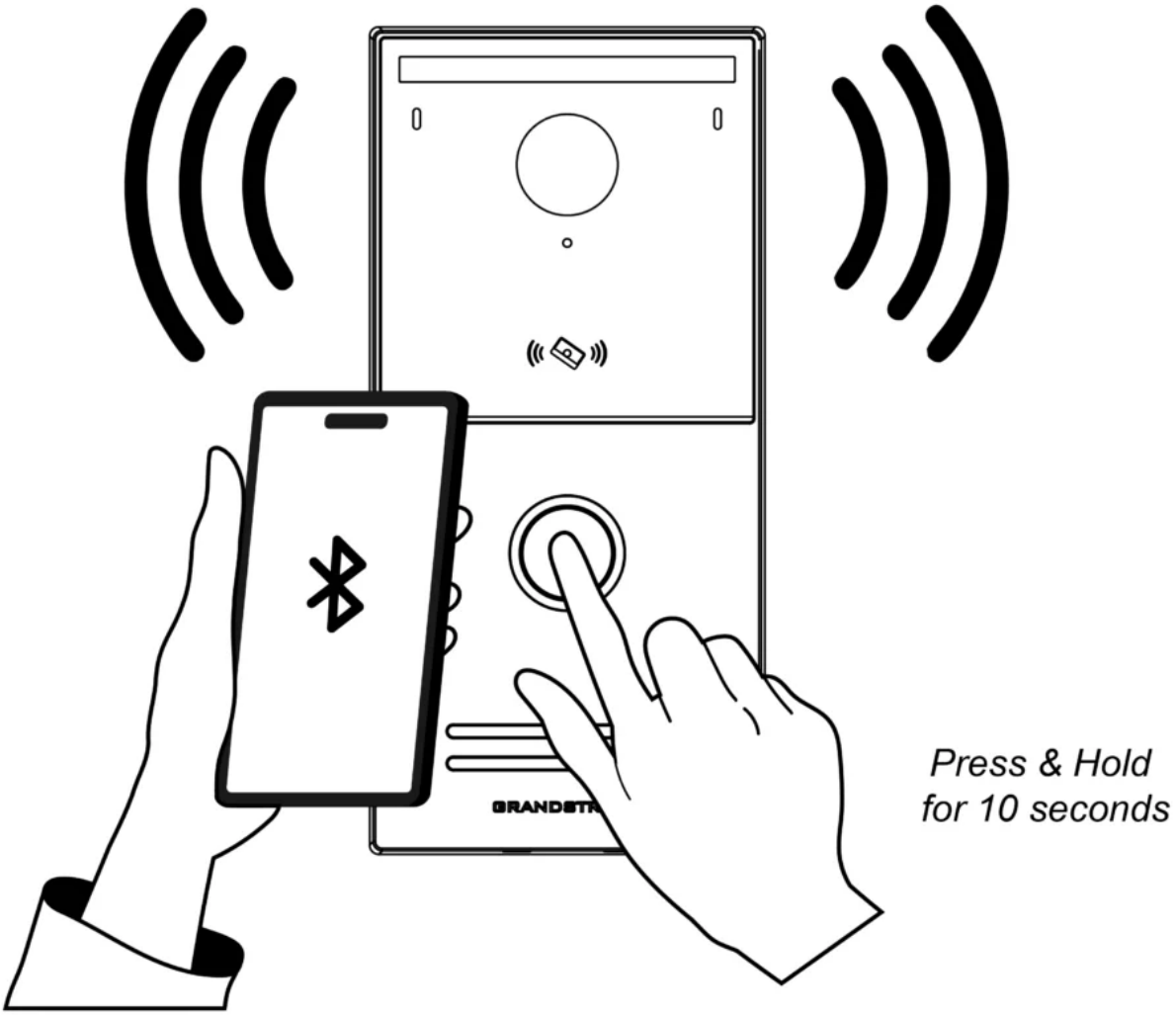
- Ensure the device is powered on.
- Have the mobile app installed on your smartphone. For detailed instructions on using the app, please refer to the **SecureAccess User Guide**.

To enter BLE pairing mode, please refer to the steps below:

1. Locate the doorbell button on the front of the GDS372x unit.
2. Press and hold the doorbell button for more than 10 seconds. Do not release the button during this time.

For the GDS3726Q, only **Key 1 (Top Key)** supports entering BLE mode. Press and hold this key for more than 10 seconds. Do not release the key during this time. The other three keys do not support this function.

3. You will hear a continuous beeping audio signal. This indicates the device has successfully entered BLE management mode and is discoverable by the app.
4. Open the mobile app and follow its instructions to complete the pairing and device discovery process.



GDS372x BLE Pairing Mode

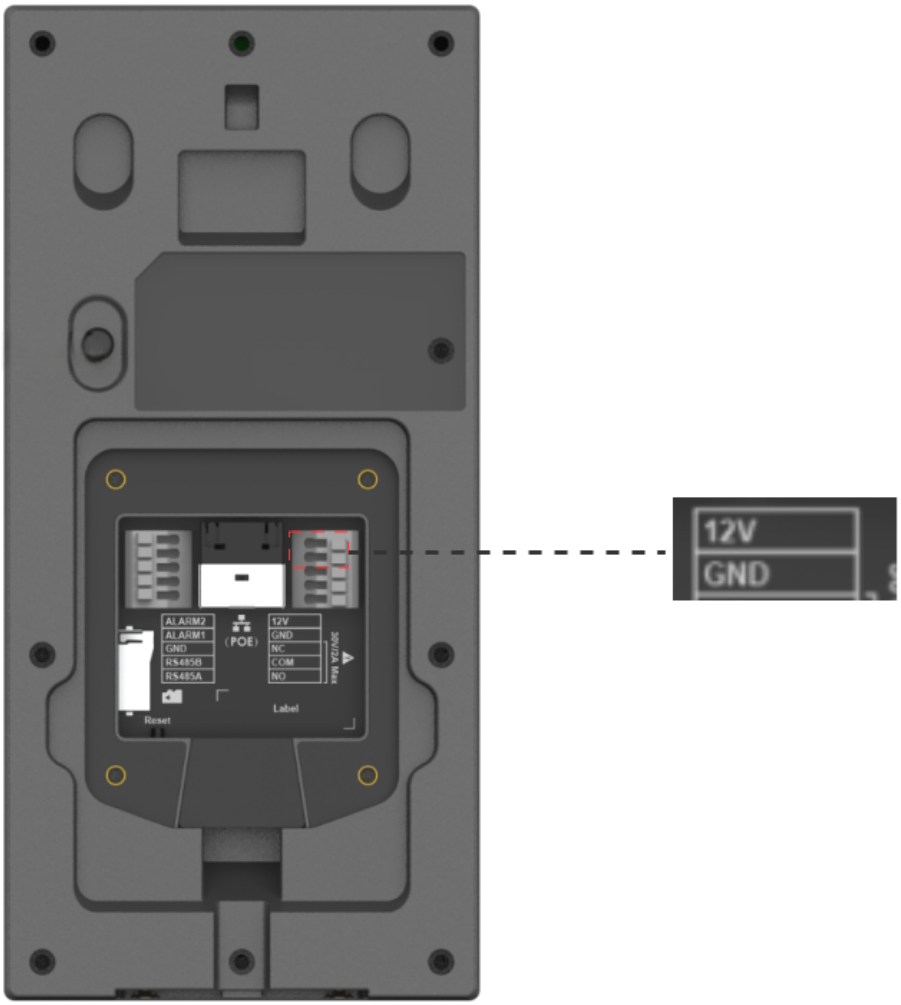
The GDS372X will automatically exit BLE management mode after 5 minutes, or you can press the doorbell button again to exit manually. The beeping sound will stop once the device exits management mode.

For comprehensive instructions on managing the GDS372x via the SecureAccess application, including initial

setup, configuration, and daily operation, please consult the Grandstream SecureAccess Administration Guide and User Guide.

Wi-Fi Deployment Setup (GDS3727 Only)

In cases where wiring the GDS3727 with an RJ45 cable to connect to the network is challenging or unavailable in certain deployments, the device offers an alternative way to integrate into the network through a Wi-Fi connection. This setup provides greater flexibility, reduces cabling requirements, and simplifies installation in indoor environments.

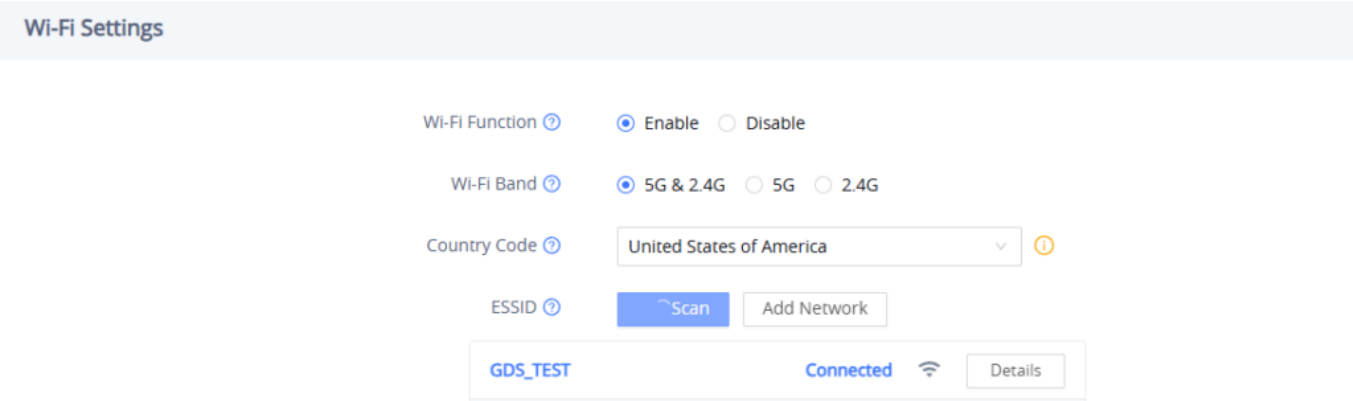


Wi-Fi connectivity is supported only on the Grandstream GDS3727 model, which is primarily designed for indoor use.

Basically, the device is first configured to connect to a Wi-Fi network using a predefined SSID. Once configured, when the device is powered via PSU only (12V and GND pins) and rebooted, it will automatically reconnect to the saved Wi-Fi network; this eliminates the need for a permanent Ethernet connection.

Please follow the steps below to achieve this:

- Connect the GDS3727 device to the network using an RJ45 cable.
- Access the Web UI, then navigate to **Network Settings -> Wi-Fi Settings**.
- Enable Wi-Fi function, scan for available networks, and connect the device to the desired Wi-Fi network.



- Once connected, disconnect the Ethernet cable and power the device using only the PSU (12V + GND). Upon reboot, the device will automatically reconnect to the configured SSID.

This allows the device to remain fully connected to the network via Wi-Fi while being powered solely through the PSU pins. This is ideal for installations where Ethernet cabling is not practical.

GDS372x APPLICATION SCENARIOS

The GDS372x IP Smart Video Door Station can be used in different scenarios.

Peering Mode without SIP Server

The GDS372x can operate in Peering Mode, enabling direct IP communication without relying on a SIP server. This setup is ideal for standalone deployments on local networks where centralized SIP infrastructure is not available or not needed.

This is the solution to upgrade the traditional analog Intercom and CCTV security system. All you need is a Power source, a Switch or a PoE Switch, and a compatible Grandstream device such as the GXV series video phones or WP8x6 Wi-Fi phones.

In this section, we will use the GSC3575 Control Station to demonstrate the peering process. However, the same principles apply when using other compatible Grandstream devices.

GDS3727 Peering Without SIP Server

Prerequisites

Before configuring peering mode, ensure the following:

1. **Power Supply Options**

- The GDS372x supports:
  - PoE (802.3af, Class 3) via Ethernet
  - 12V DC (1A) via rear pin connectors
- For the door strike or magnetic lock:
  - Can be powered using the **same PSU as the GDS372x** (if power rating allows)
  - Or separately, if **PoE is used for GDS372x**, and a **dedicated PSU** is used for the lock

2. **Networking**

- GDS372x and the receiving device must be on the **same local subnet**
- Static or dynamic IP addressing is supported

3. **Connected Hardware**

- For door unlock functionality, ensure the **relay pins (NO, NC, COM)** are wired to a functional lock device.

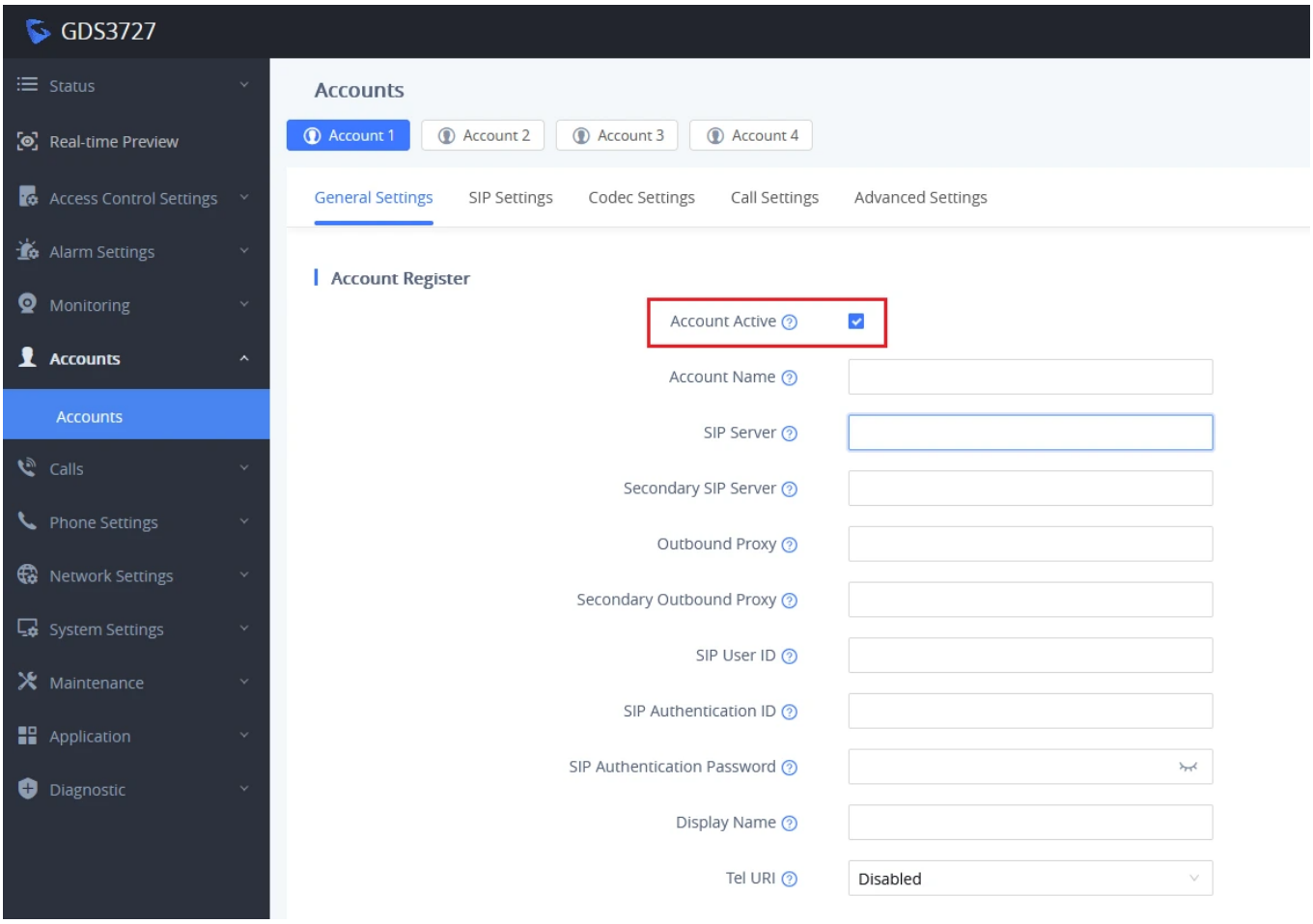
Ensure that Direct IP Call Mode is enabled on the GSC3574/GSC3575 (Web UI -> Phone Settings -> Call Settings -> Basic Settings) before configuring peering with the GDS372x, otherwise the peering process may fail.

Configuration Steps

- **On GDS372x**

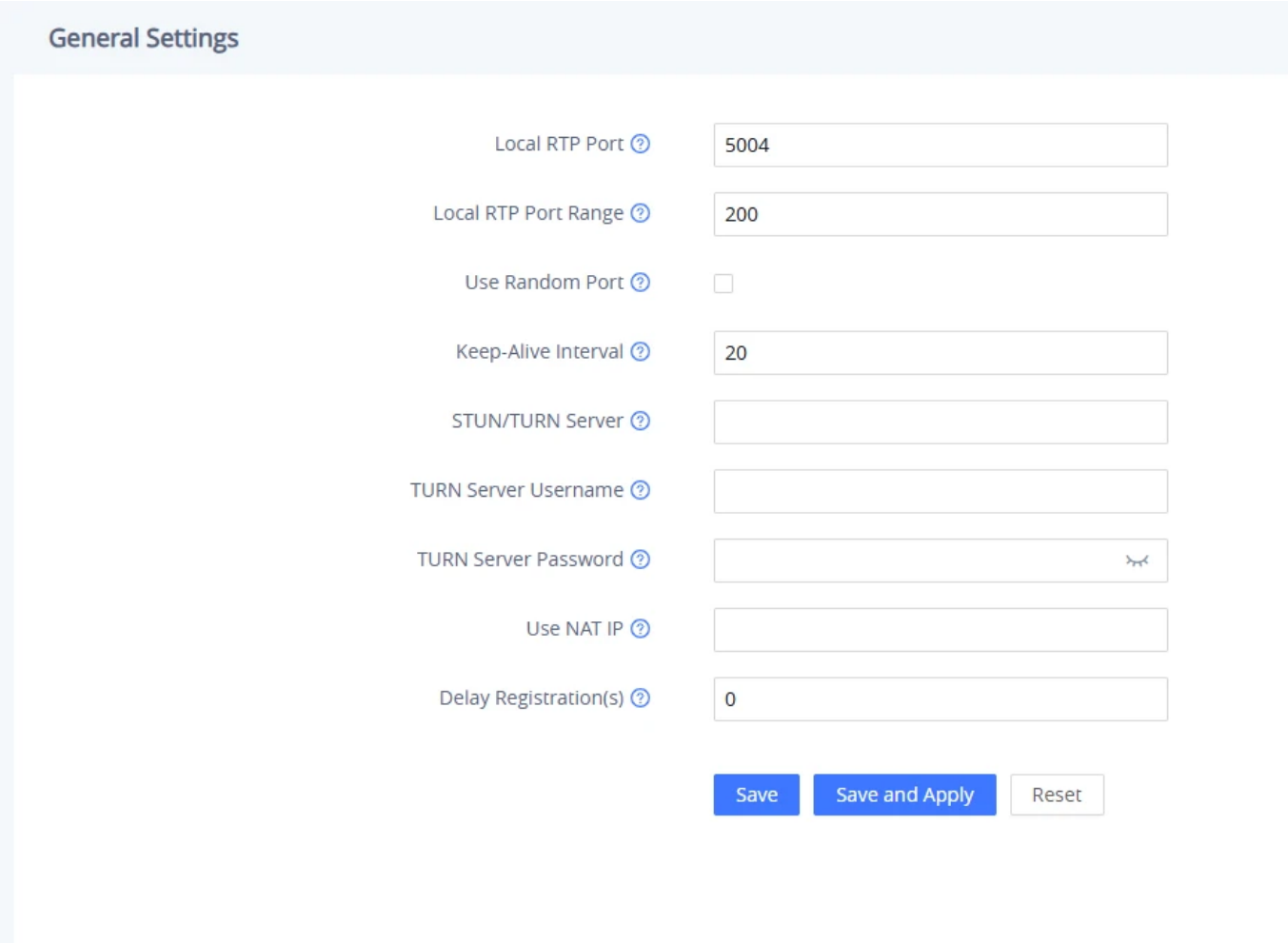
To enable direct IP communication with the GSC3575, configure the GDS372x using the steps below.

1. Enable the SIP account by navigating to **Account -> Basic Settings**.
2. Enable the account by setting "**Account Active**" to **Yes**, and leave all SIP credential fields empty. In peering mode, the device communicates directly via IP, so registration to a SIP server is unnecessary.



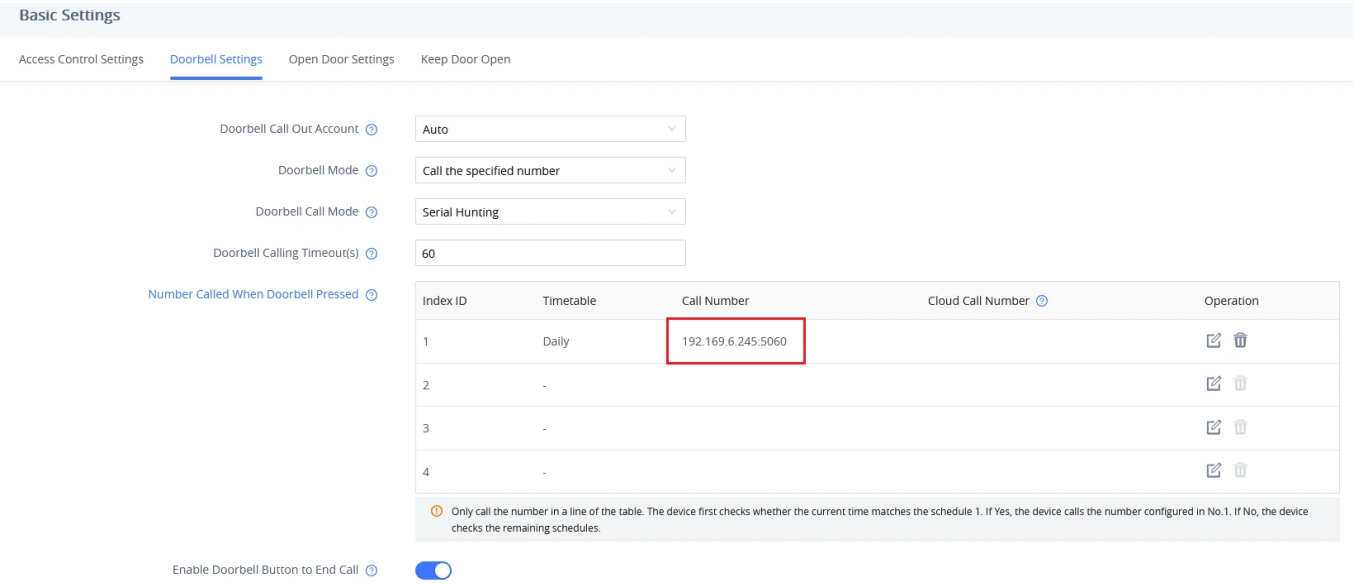
GDS372x General Account Settings Page

3. Navigate to **Phone Settings -> General Settings** and set **Use Random Port** to **No**. Fixed RTP ports ensure reliable audio and video transmission between static IP devices in direct IP mode.



GDS372x General Phone Settings Page

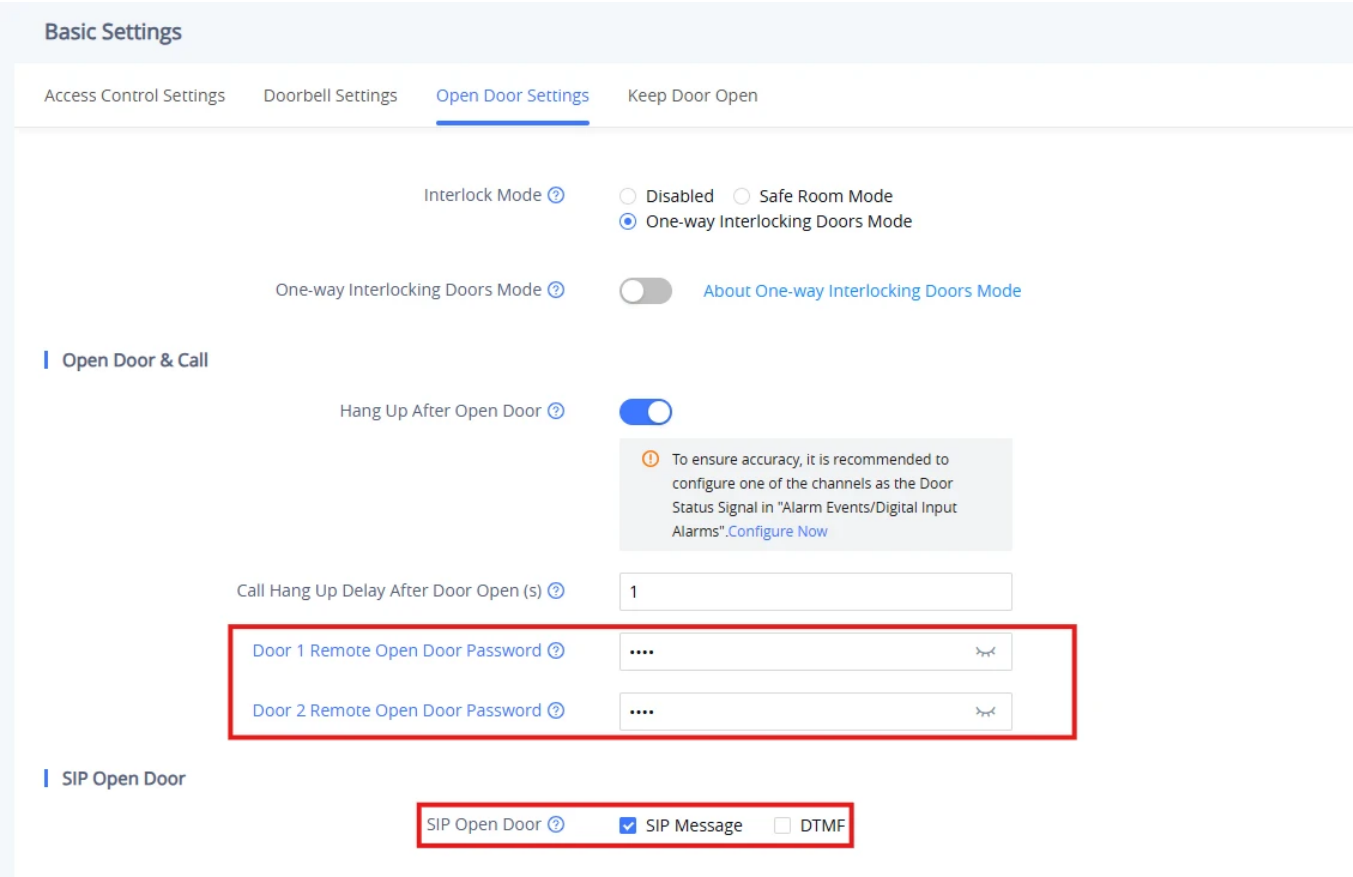
4. Go to **Access Control Settings -> Doorbell Settings** and enter the IP address or SIP URI of the target device (e.g., 192.168.1.88 or sip:192.168.1.88) in **Number Called When Doorbell Pressed**. This defines where the GDS372x should send calls when the doorbell is pressed.



GDS372x Doorbell Settings

5. Set the Remote Open Door Passwords under **Access Control Settings -> Open Door Settings**. This enables users to remotely unlock the door from the receiving device using either SIP signaling or DTMF input.

6. Click **Save and Apply** to ensure all settings are committed and activated.

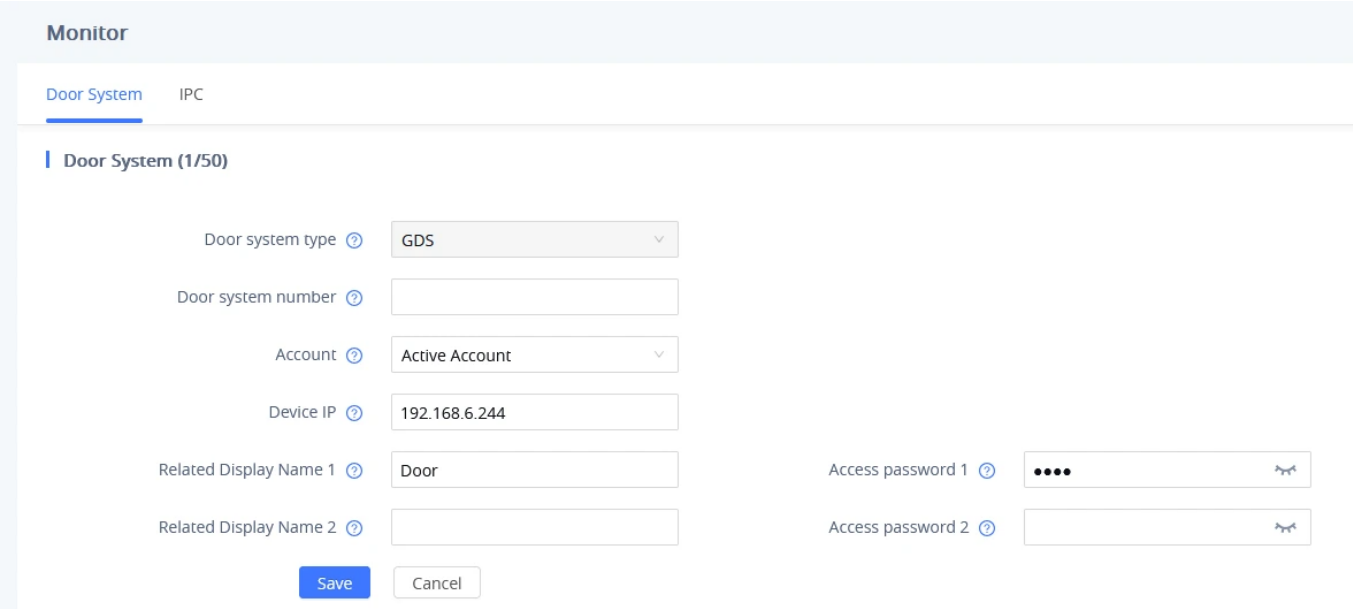


GDS372x Open Door Settings

- **On GSC3575 Control Station**

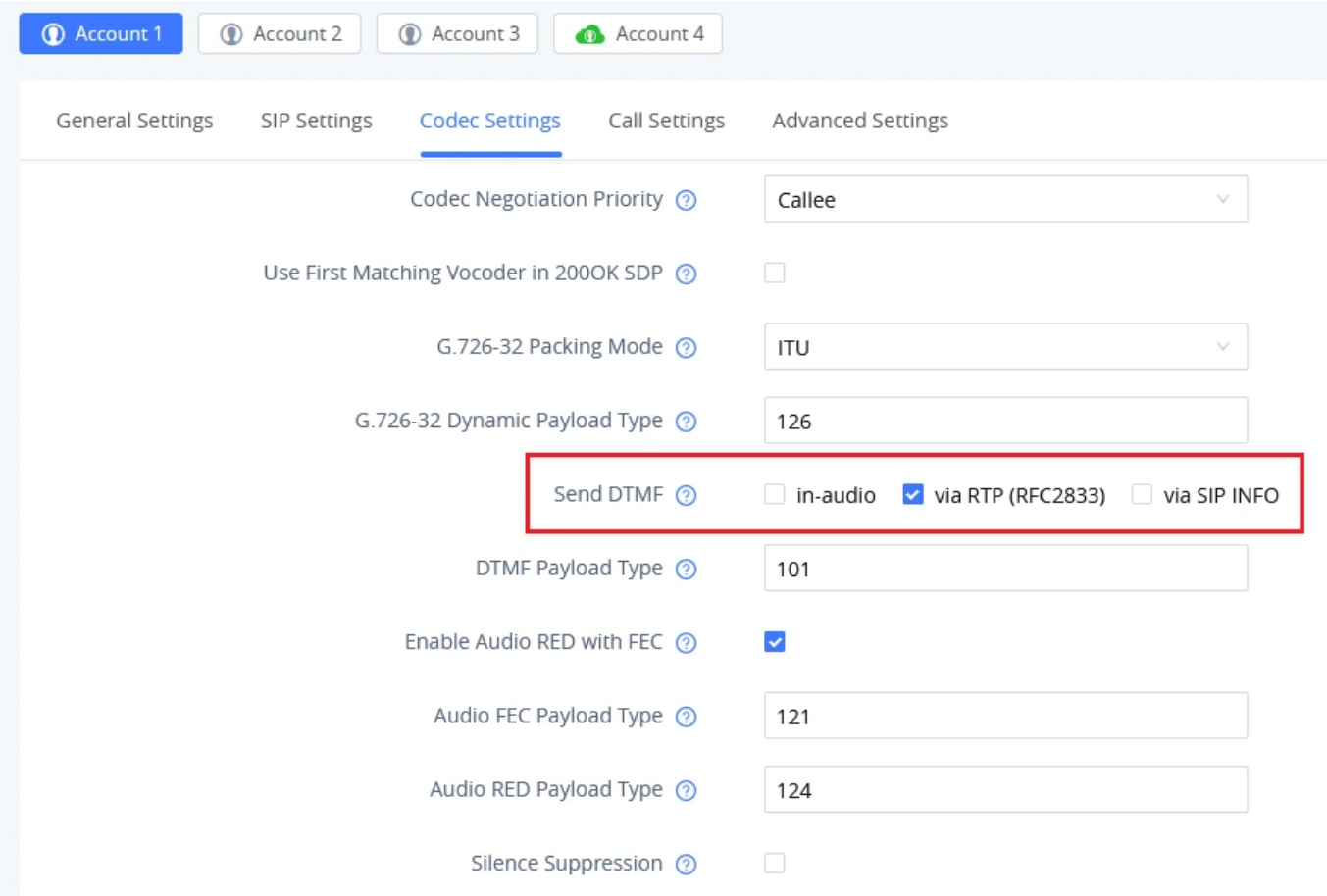
1. To enable two-way direct IP calling, repeat steps 1, 2, and 3 from the GDS372x configuration on the receiving device.
2. For the SIP-based relay trigger, users need to add the GDS372x door station to the list of monitored devices on the GSC3575 control station, as shown in the screenshot below.

   - Choose a door system number or leave the field blank.
   - Select the active account for monitoring.
   - Enter the GDS372x IP address under device IP.
   - Configure the Remote Open Door PIN as the access password.



GSC3575 Door System Monitor Settings

3. To enable door unlocking via **DTMF**, select the DTMF mode based on your GDS372x config in the codec settings configuration of the active account.



GSC3575 Account Codec Settings

Remotely Unlocking the Door

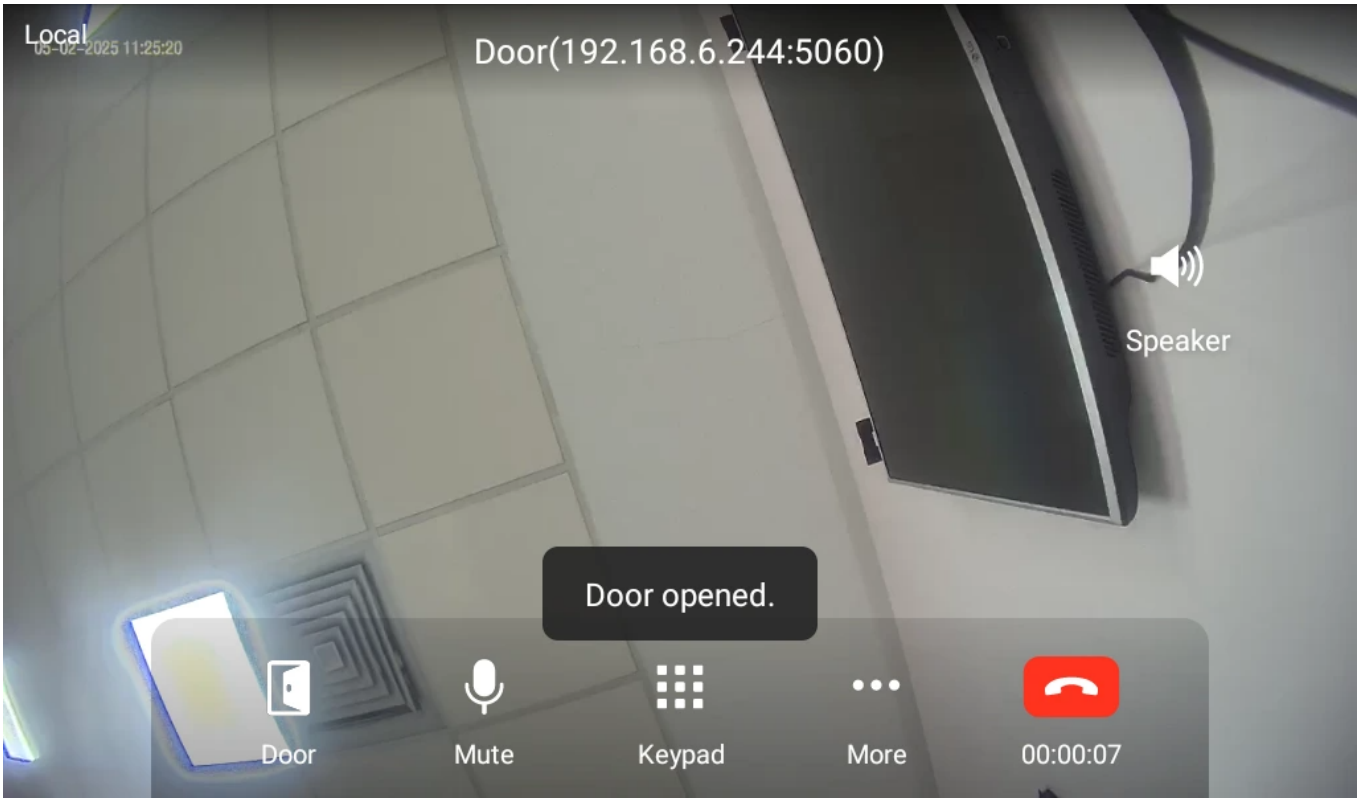
The diagram below shows the flow of the remote door unlocking using a direct IP call.

Direct IP Call for Remote Unlock

Once the doorbell is pressed:

1. The GSC3575 receives the call and shows a video stream from the GDS372x
2. The user can:

- Tap the unlock icon during the incoming call or active call screen to trigger the door relay via **SIP**.
- Enter the **Remote Open Door PIN** followed by the **pound key (#)** during the active call to unlock the door using DTMF.



Door Opened Prompt

Peering Mode with SIP Server

For medium to large-scale deployments, especially when multiple **GDS372x** units are deployed across a facility, **Direct IP peering is not recommended** due to limitations in maintaining simultaneous peer connections.

In such cases, using a **central SIP server,** like Grandstream's UCM6300, SoftwareUCM, or GCC IPPBX, or

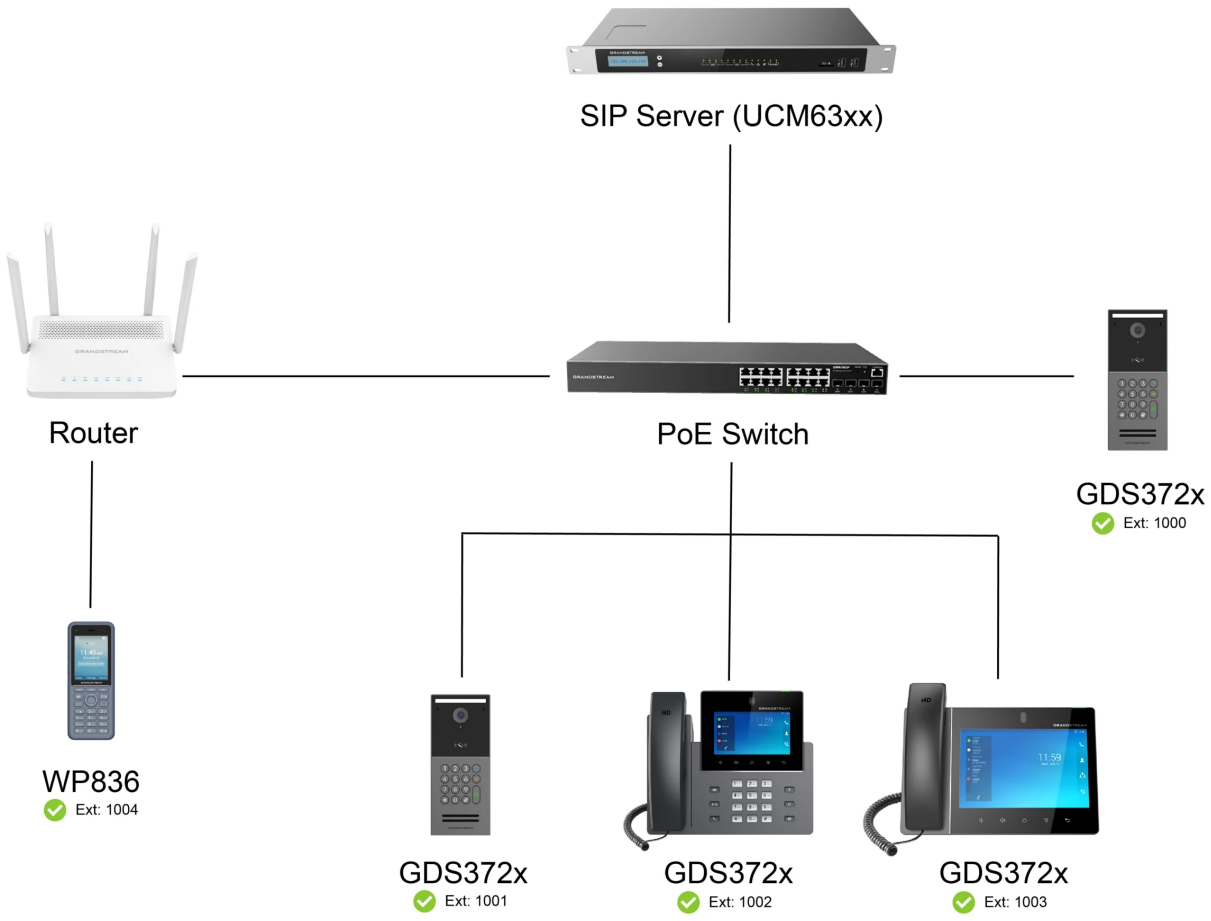
a compatible SIP proxy, is strongly advised to manage call routing, access control, and video intercom functionality efficiently. The SIP server acts as the core system to register all devices, allowing centralized management.

For a typical deployment, the following might be needed:

- Multiple **GDS372x** door systems (e.g., GDS3727)
- A **UCM6300 IPPBX** or other compatible SIP Server
- **GXV33xx/GXV34xx video phones**, **GSC357x intercom stations**, **WP8x6 Wi-Fi phones,** or any compatible devices.
- **PoE switch** with proper Cat5e/Cat6 cabling
- **Power supply unit (PSU)** if not using PoE.

If remote access is needed-for viewing live video feeds or unlocking doors remotely-a router with internet connectivity is essential. Additional requirements:

- **Router** with WAN access
- **Internet connection** (Fiber, DSL, 4G/5G, etc.)
- **Mobile device (Android/iPhone)** with SIP client or IP camera app (e.g., **GS Wave**)



Peering GDS372x with SIP Server

Peering Mode using NVR

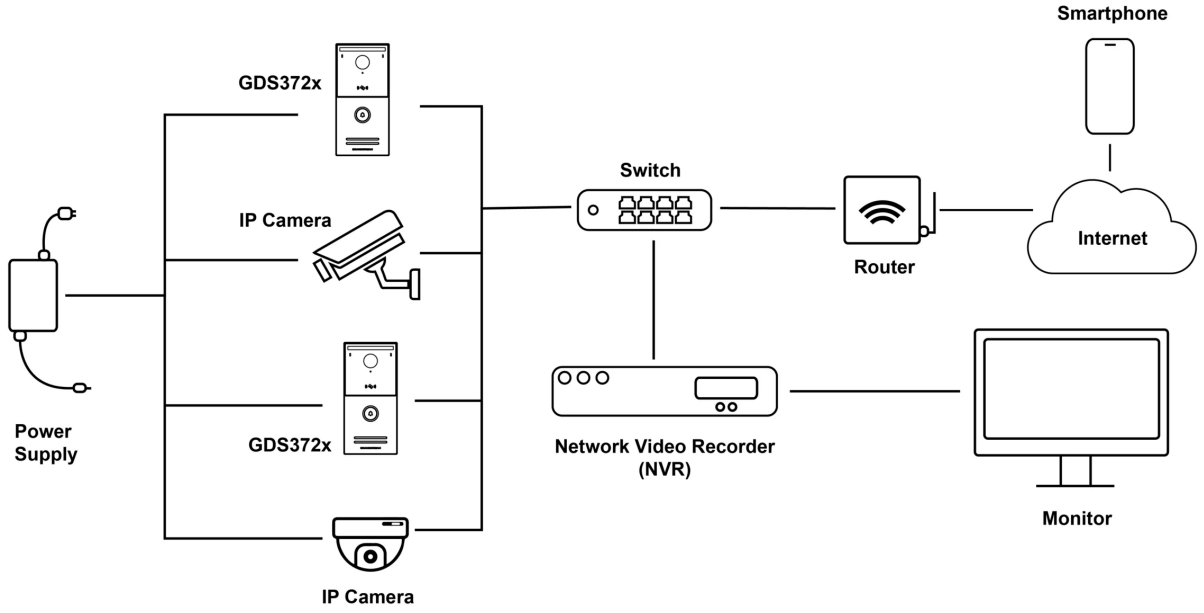
The GDS372x series supports seamless integration with third-party **Network Video Recorders (NVRs)** using the **ONVIF Profile S** standard. This enables centralized live monitoring, video recording, and event management for facility access and surveillance applications.

The key protocols used in this scenario are:

- **ONVIF Profile S**: Enables device discovery, stream configuration, and event handling.
- **RTSP (Real-Time Streaming Protocol)**: Used to stream live video to the NVR once authenticated and configured via ONVIF.

The recommended equipment list is:

- One or more **GDS372x** devices.
- **ONVIF-compliant NVR**.
- **PoE switch** or DC power supply.
- **Router** (for Internet access if remote viewing is needed)
- **Optional:** Android/iOS phone with compatible viewing app (e.g., IP Cam Viewer)



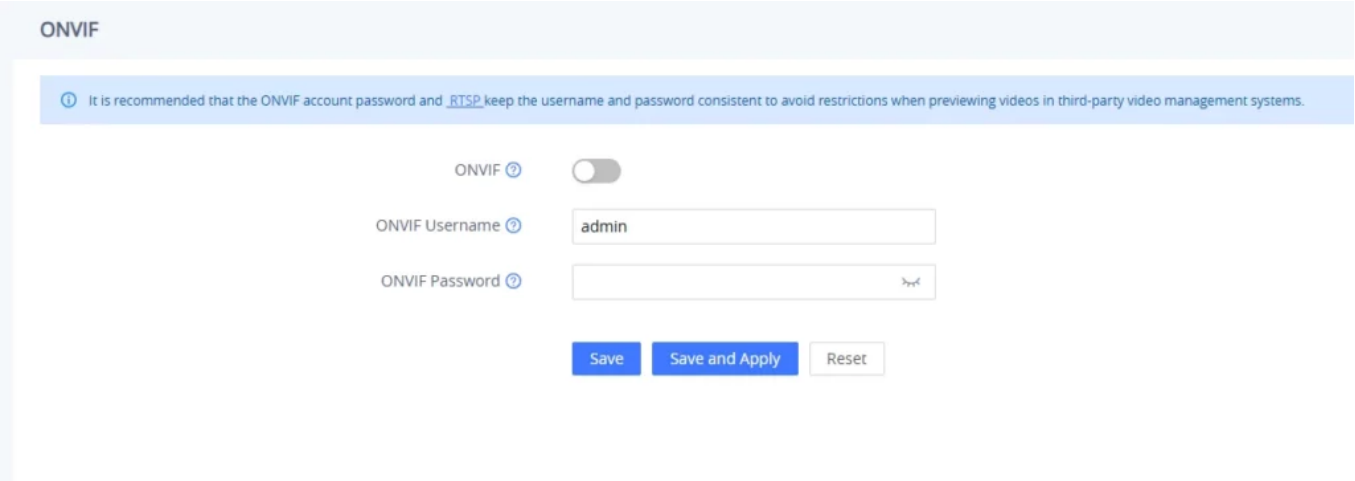
Peering GDS372x with an ONVIF Profile S NVR

The GDS372x Web UI provides options to configure **ONVIF access credentials**, which are essential for secure integration with NVRs or third-party ONVIF-compatible software. Under **Monitoring -> ONVIF**, you will find:

- **ONVIF Username**: This is the account the NVR or ONVIF client will use to authenticate with the GDS372x.
- **ONVIF Password**: The corresponding password for that username.

These credentials are used during the ONVIF device discovery, stream setup, and event service access phases.

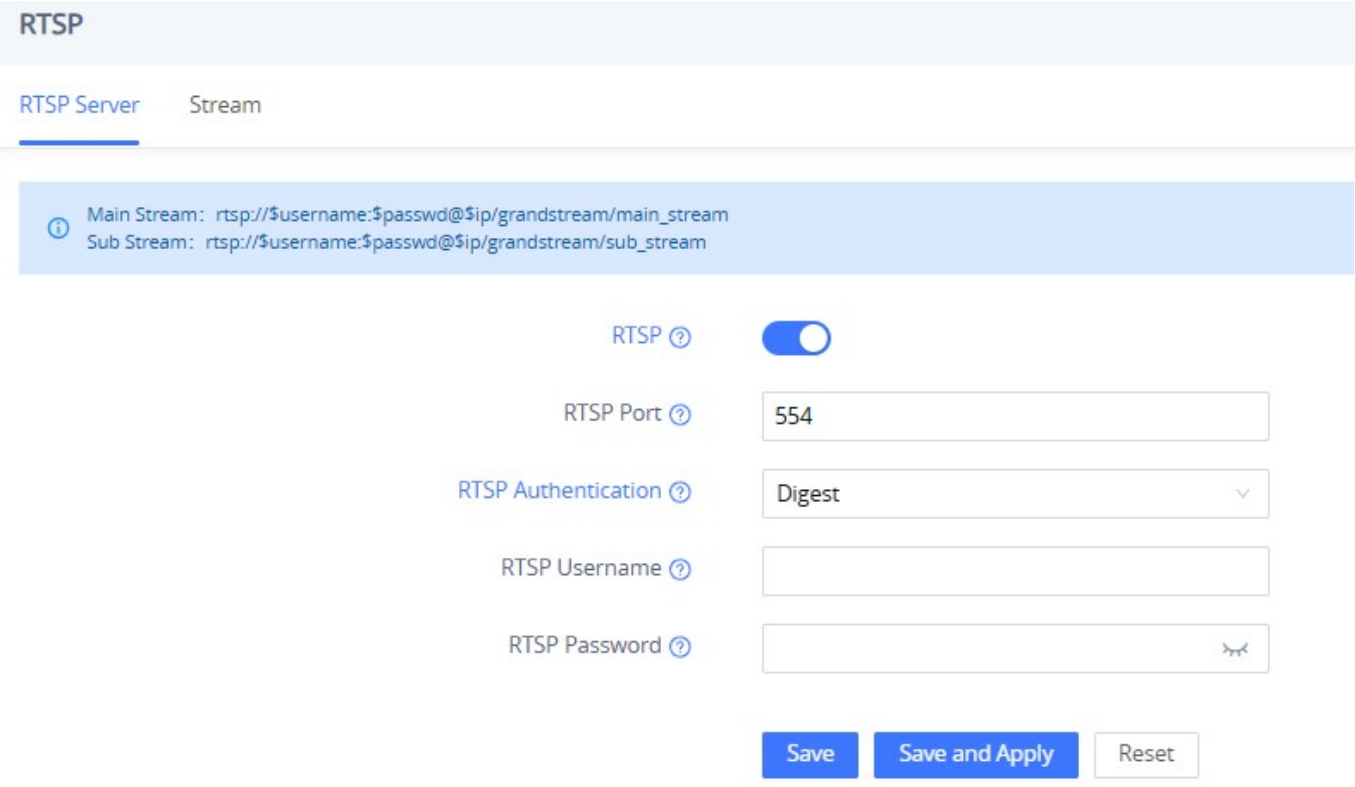
If the NVR or viewing client supports direct RTSP connections, the GDS372x acts as an RTSP server, streaming live video to the NVR. The NVR acts as an RTSP client, pulling the live video feed using the RTSP URL (which includes the username/password).



GDS372x ONVIF Settings

To configure RTSP settings, go to **Monitoring -> RTSP:**

- **RTSP Port** (default: 554)
- **RTSP Authentication**: define how credentials (username/password) are sent
- **RTSP Username**
- **RTSP Password**



GDS372x RTSP Settings

It is recommended that the ONVIF account and the RTSP account use the same username and password to avoid access issues when previewing video from third-party NVRs or VMS (Video Management Systems). Some systems will attempt RTSP authentication using the ONVIF credentials.

DTMF Door Open Permission

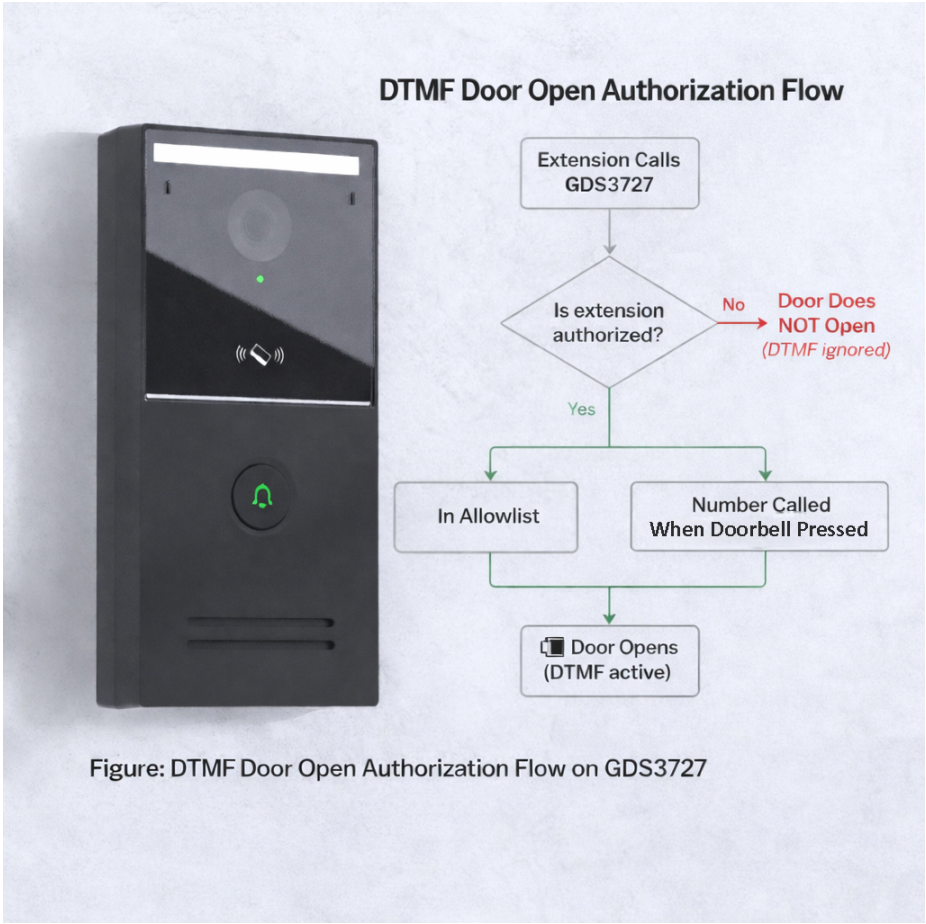
The GDS372x door phone supports unlocking the door via DTMF during an active call.

For security reasons, **only authorized extensions** are permitted to trigger door unlock using the configured DTMF password.

An extension is considered **authorized** if it meets **at least one** of the following conditions:

- It is added to the Allowlist under **Phone Settings -> General Settings -> Call Settings -> Allowlist Management**, if the Allowlist feature is enabled.
- It is configured as a SIP number in the **Number Called When Doorbell Pressed** field under **Access Control Settings -> Basic Settings -> Doorbell Settings -> Number Called When Doorbell Pressed**.

If an extension does **not** meet either condition, the door phone will **ignore the DTMF door open command**, even if the correct password is entered.



DTMF Door Open Permission

The authorization logic is as follows:

Extension Configuration	DTMF Door Open Result
Extension is in Allowlist	Door opens
Extension is configured on a Door Button (Number Called when Doorbell Pressed)	Door opens
Extension is NOT in Allowlist and NOT on any Door Button dial option	Door will NOT open

Example Scenarios

Scenario 1 - Authorized via Access Control List

- Extension **1001** is added to the **Access Control User List**
- Extension **1001** calls the door phone
- User enters the correct DTMF password

Result: The door unlocks successfully

Scenario 2 - Authorized via Door Button Configuration

- Door Button 1 is configured to call **Extension 1002**
- Extension **1002** calls the door phone manually
- User enters the correct DTMF password

Result: The door unlocks successfully (Because the extension is associated with a door button under **Number Called When Doorbell Pressed**)

Scenario 3 - Unauthorized Extension

- Extension **1003** is **not** in the Access Control User List
- Extension **1003** is **not** configured on any Door Button
- Extension **1003** calls the door phone
- User enters the correct DTMF password

Result: The door does **not** unlock. The DTMF command is ignored

Building Mode (GDS3725 Only)

The GDS3725 supports cloud-based building communication through GDMS SecureAccess Building Mode.

In Building Mode, users can place calls between building units by dialing [Building ID * Virtual Number #], Where:

[Virtual Number * PIN]

- **Building ID** identifies the target building.
- **Virtual Number** identifies the target building unit.

For more information about Building Mode, refer to the GDMS SecureAccess User Manual.

- When using PIN-based door access, users must enter [Virtual Number * PIN].
- Virtual Number must be unique for each building unit. Duplicate Virtual Numbers are not supported for PIN-based access authentication.

Home Assistant

The GDS372x series integrates with **Home Assistant** through the **Grandstream Home** integration available in HACS, enabling centralized monitoring and control within the Home Assistant ecosystem.

For further information about Home Assistant installation and configuration, please refer to the GDS372x Series Access Control with Home Assistant and HACS.

GDS372x PERIPHERAL CONNECTIONS

Below is the illustration of GDS372x peripheral connections for related applications. We will take the GDS3727 as our testing unit.

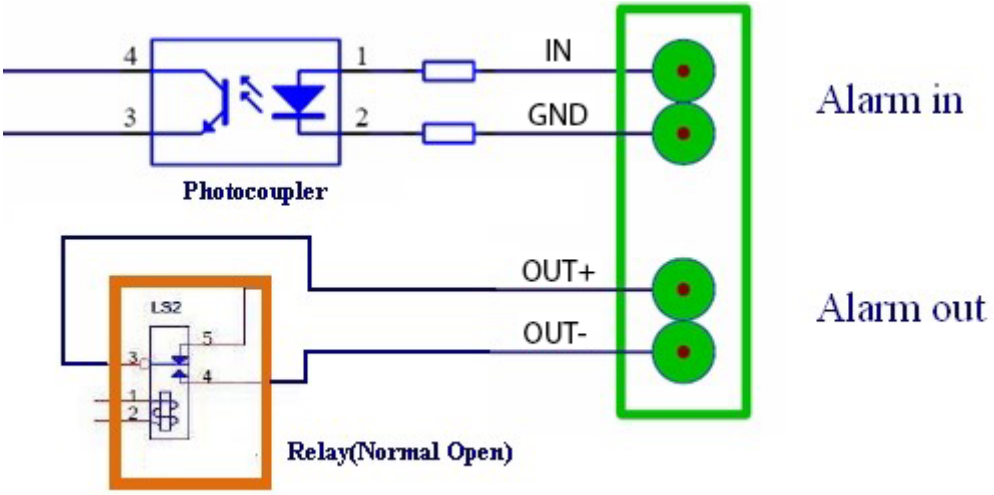
Peripheral Connections for GDS3727

Alarm IN/OUT

Alarm_In can be connected to 3rd-party sensors (such as an IR Motion Sensor, door contact switch, or panic button).

Alarm_Out can be connected to devices such as a 3rd-party siren, strobe light, or an electric door striker.

The figure below shows an illustration of the Circuit for Alarm_In and Alarm_Out.



Alarm InOut Circuit for GDS372x

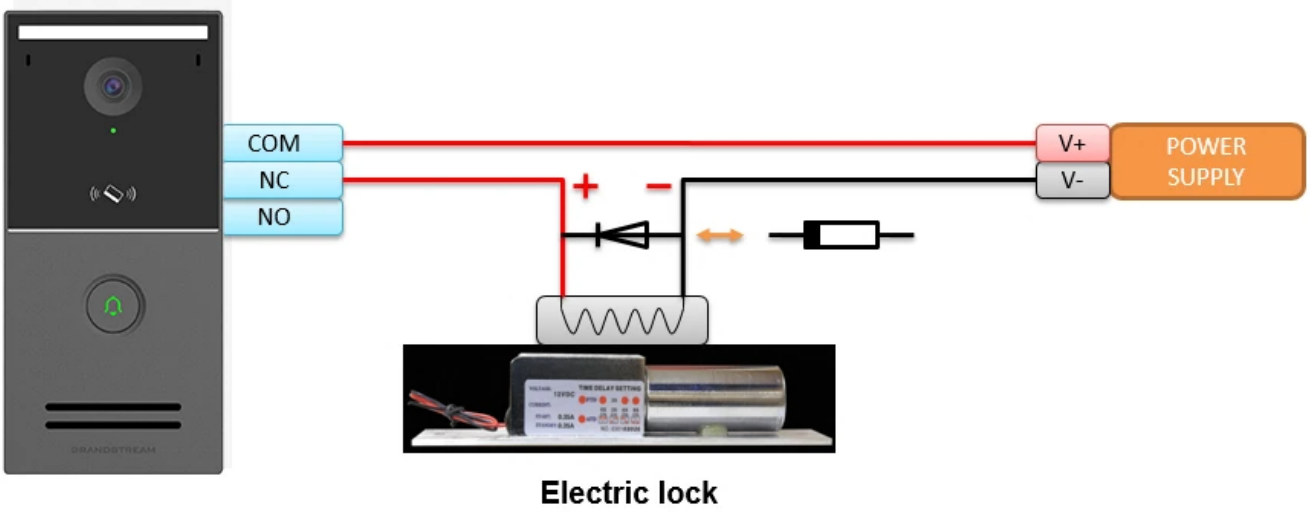
The Alarm_In and Alarm_Out circuit for the GDS372x should meet the following requirements:

Alarm Input	Dry contact (switch) input only.
Relay Output	125VAC/0.5A, 30VDC/2A, Normal Open, PINs

Higher voltage and wrong polarity connections are prohibited because this will damage the devices.

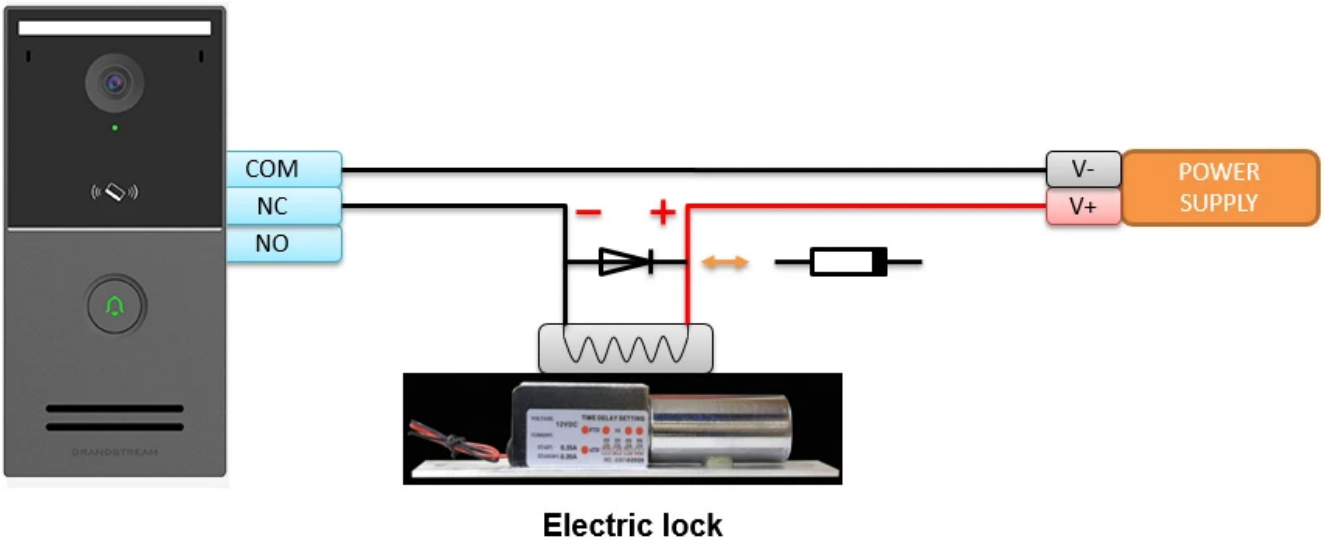
Protection Diode

When connecting the GDS372x to a door strike, it is recommended to set an EMF protection diode in reverse polarity for secure use. Below are examples of deploying the GDS372x for the protection diode.



Protection Diode Example 1

The reverse EMF protection diode must always be installed in reverse polarity across the door strike.



Protection Diode Example 2

Power polarity connection: Diode: SS24 or If>=2A, Vr>=40V.

Connection Examples

This section illustrates different connection scenarios for the GDS372x IP Video Door Station, with explanations and practical use cases for each wiring setup.

While the wiring principles apply across all models in the series, the GDS3727 is used in this section as the representative example in the diagrams for visual consistency.

- **PoE (802.3af Class 3)** can be used to power the GDS372x directly through the network cable, simplifying installation and cabling.
- **Shared Power Supply** (e.g., a 12V DC PSU) can be used to power both the GDS372x and connected devices like electric strikes or relays, provided the total current draw does not exceed the PSU's capacity.
- For fail-safe/fail-secure locks requiring **higher current**, it's often recommended to use a dedicated power supply for the lock, while using PoE or a separate PSU for the GDS372x to prevent voltage drops or instability.

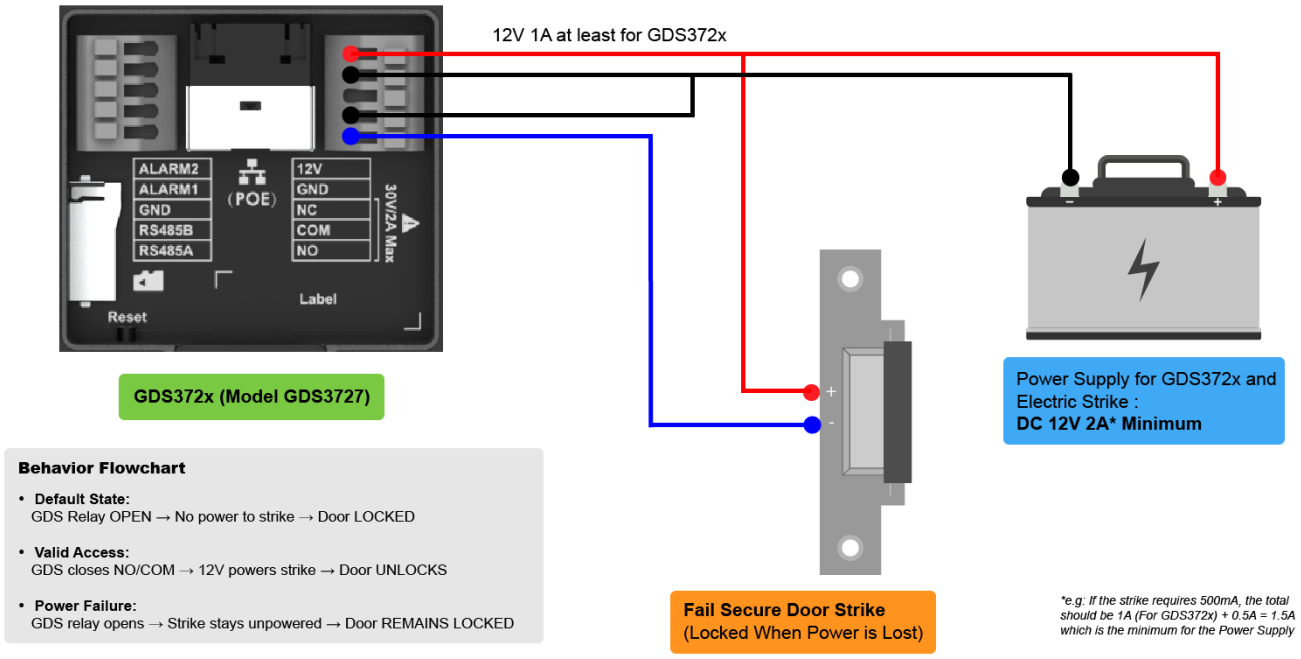
- **Do not reverse** 12V and GND pins when powering the GDS372x using an external power supply. This can permanently damage the GDS372x or any attached devices. Always verify polarity before powering the unit.
- If GDS and door strike/siren **share a PSU** that **doesn't provide enough amperage**, voltage drops or reboots may occur, especially during activation events. This can lead to **failed unlocking, corrupted config, or device damage over time**.
- **Exceeding the relay output limit** (above 30V or 2A) can push the internal relay beyond its safe operating range, potentially leading to **welded or burned contacts, complete relay failure, and, in extreme cases, a fire hazard**.
- Failing to **isolate high- and low-voltage** circuits can lead to unprotected mixing of power and control signals, increasing the risk of **electrical noise, system malfunctions, or even shock hazards.**

GDS372x with Fail-Secure Electric Strike

- **Pins used**: NO (Normally Open) and COM (Common)
- **Fail-secure strikes** require power to unlock.
- When the GDS372x sends an unlock signal, it closes the circuit between NO and COM, energizing the strike to unlock the door.

This setup is ideal for **high-security environments**, such as server rooms or storage areas, where doors stay locked in case of power failure to prevent unauthorized entry.

Avoid using **NC** (Normally Closed) for this setup. As a fail-secure lock needs power to unlock, using NC will supply power continuously, keeping the lock in an **open (unsecured) state** when idle.



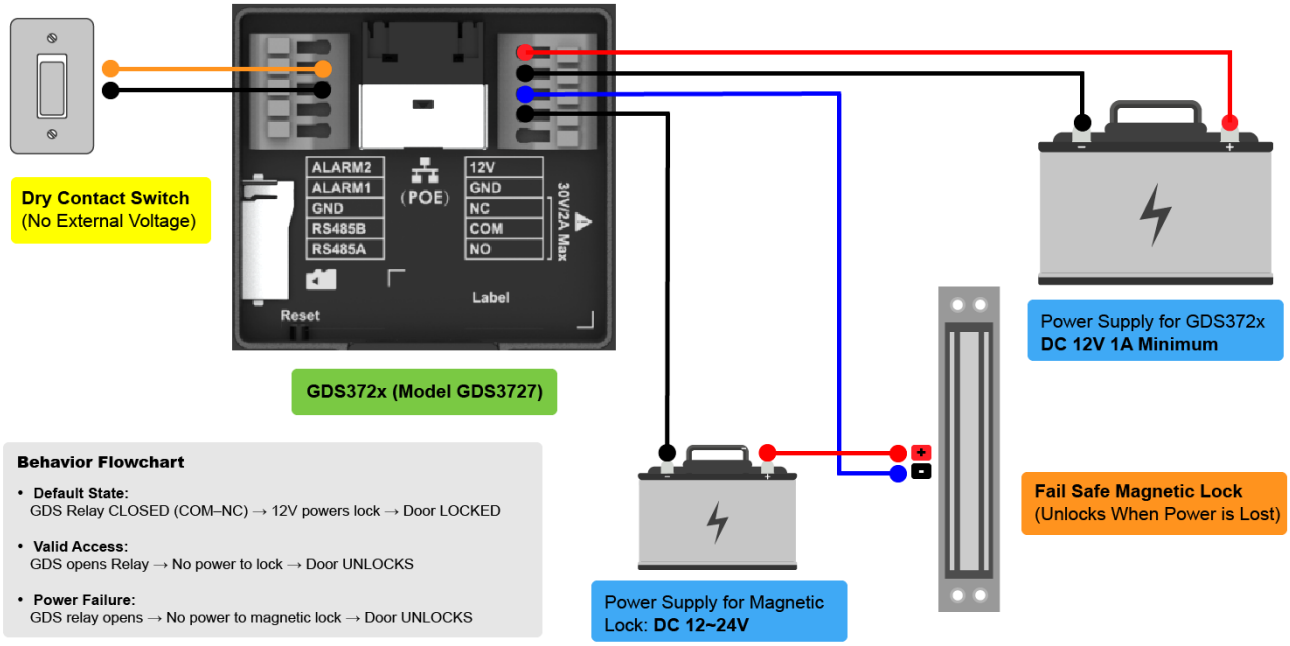
GDS3727 with Fail Secure Door Strike

GDS372x with Fail-Safe Magnetic Lock and Dry Contact Switch

- **Pins used**: For the magnetic lock -> **NC** (Normally Closed) and **COM** (Common), for the dry contact switch -> **ALARM1** (Alarm input 1) and **GND** (Ground).
- Fail-safe locks stay locked when powered, and unlock when power is cut.
- When the GDS372x triggers the relay (e.g., from button press or remote access), it opens the circuit, cutting power and unlocking the door.

This setup is especially effective in environments such as Emergency exits, where doors must remain locked by default and only unlock temporarily when access is granted.

Avoid wiring Fail-Safe Locks to **NO** (Normally Open) without a Timed Cutoff. If the relay stays closed (power applied continuously), the lock **may overheat or wear out**, especially electromagnetic locks designed for short bursts of power.

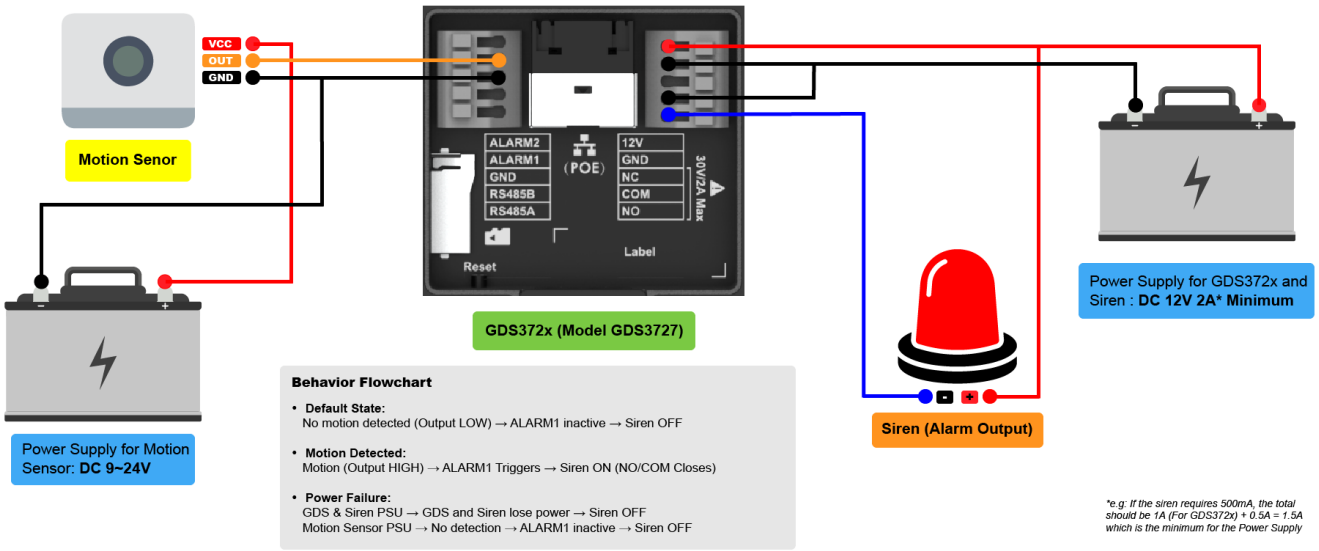


GDS372x with Fail Safe Magnetic Lock and Dry Contact Switch

GDS372x with Siren and Motion Sensor

- **Pins used**: For the siren -> **NO** (Normally Open) and **COM** (Common), for the motion sensor -> **ALARM1** (Alarm input 1) and **GND** (Ground).
- Most electronic sirens are active when powered.
- When the GDS372x triggers the relay (e.g., due to motion detection or alarm input), the NO contact closes with COM, powering the siren.

If you accidentally wire a siren to **NC** (Normally Closed), it will sound continuously unless the relay is activated to break the circuit; this is typically not desired for siren applications.



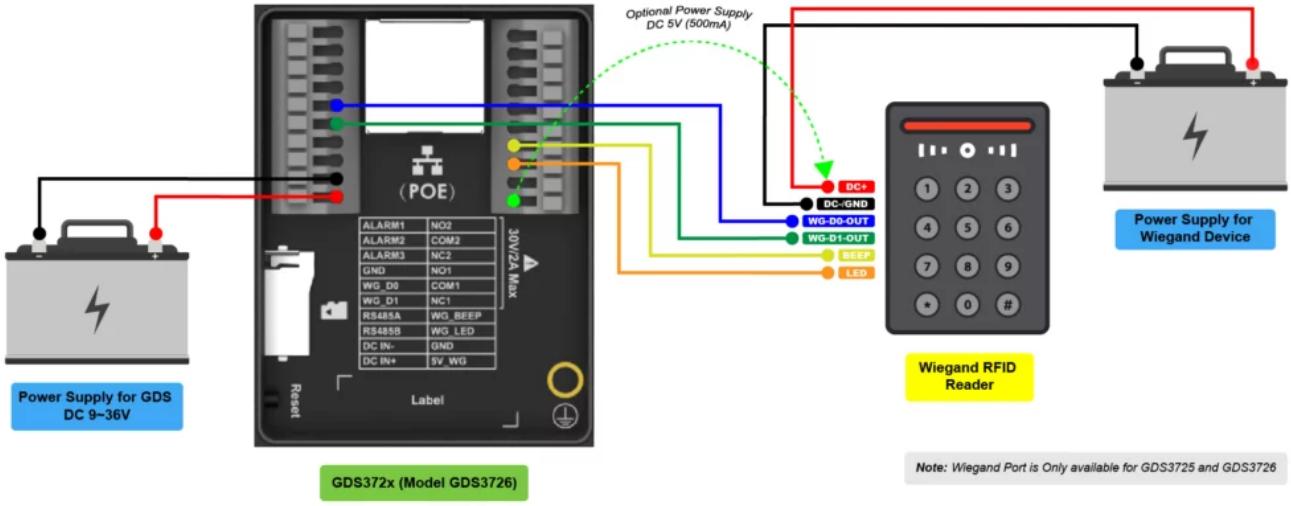
GDS372x with Siren and Motion Sensor

GDS372x with External RFID Card Reader

The GDS372x supports external **Wiegand RFID readers** to extend access control points. The Wiegand reader sends card/fob data to the GDS through the **WG_D0 and WG_D1 lines**, while the **WG_BEEP and WG_LED** pins allow the GDS to control reader feedback (such as LED indicators or buzzer beeps).

- **Pins used: WG_D0, WG_D1, WG_BEEP, WG_LED**, and optionally **5V_WG** (for powering the Wiegand reader if no external PSU is used).

Wiegand interface pins are available only on GDS3725 and GDS3726. The GDS3727 does not provide Wiegand input/output.



GDS372x with Wiegand RFID Reader

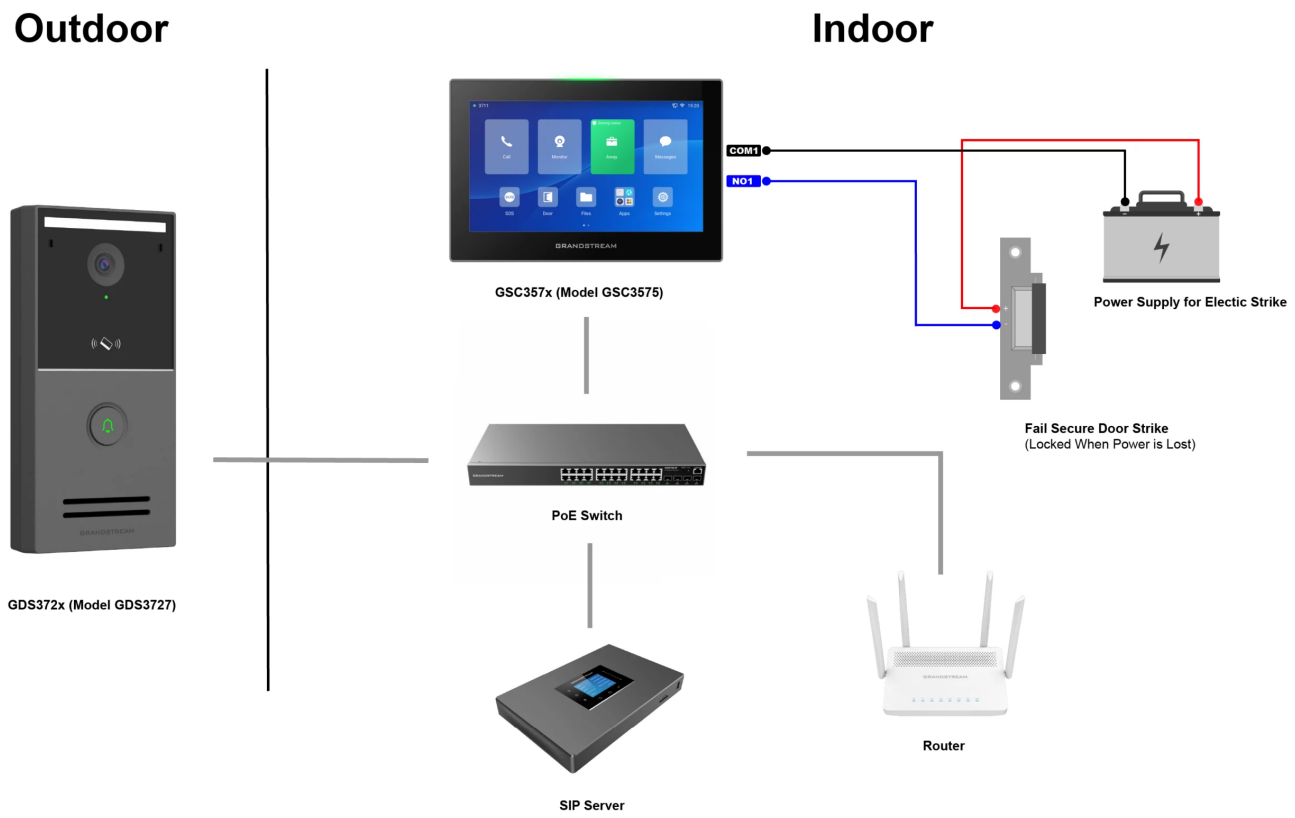
Secure Open Door Peering with GSC357x

In this enhanced access control setup, the **GSC357x Series** functions as the secure internal relay controller for unlocking doors, with the GDS372x door system installed outside. This configuration is ideal for increasing physical security by relocating the unlocking relay circuit indoors, where it is less vulnerable to tampering.

In this section, we will be using the GSC3575 control station with the GDS3727 door station for secure open door peering (SIP-Based Connection).

- **GDS372x** is installed **outside** the entry point (e.g., main gate or door).
- **GSC3575** is installed **indoors**, beyond the secured entry.
- The **electric lock or strike** is connected to the **GSC3575's Alarm_Out (relay) interface**, not the GDS.
- Communication between devices is established using **SIP accounts registered to a SIP server**.

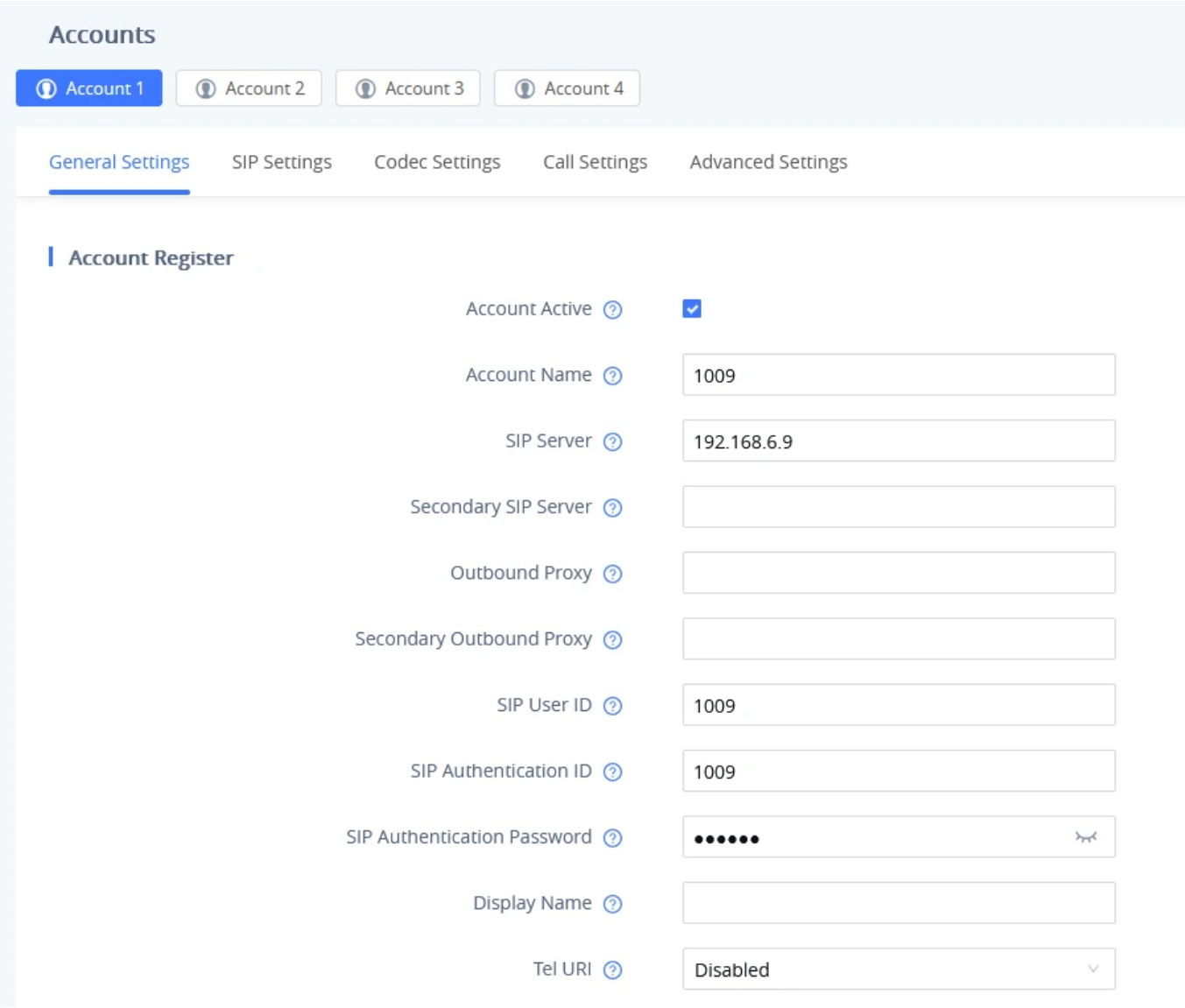
This configuration ensures secure access control by moving the unlocking relay indoors while utilizing centralized SIP server management.



GSC357x Secure Open Door with GDS372x

GDS372x Configuration Steps

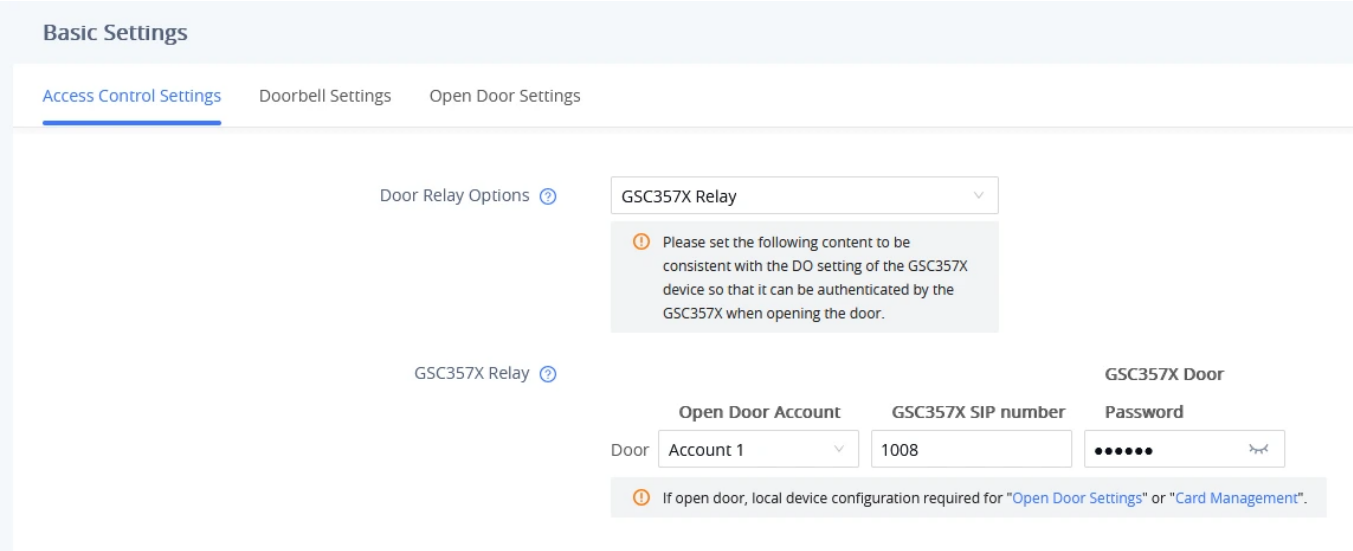
1. Log in to GDS372x Web UI
2. Under Account 1 Settings, register to the SIP server using the SIP credentials.



GDS372x Account Registration

3. Navigate to **Access Control Settings -> Basic Settings**:

- Set **Door Relay Options** to "GSC357X Relay"
- Set **Account** to Account 1.
- Set the **GSC357X SIP number** to its **SIP extension**.
- Set a **GSC357X Door Password** (shared with GSC3575)

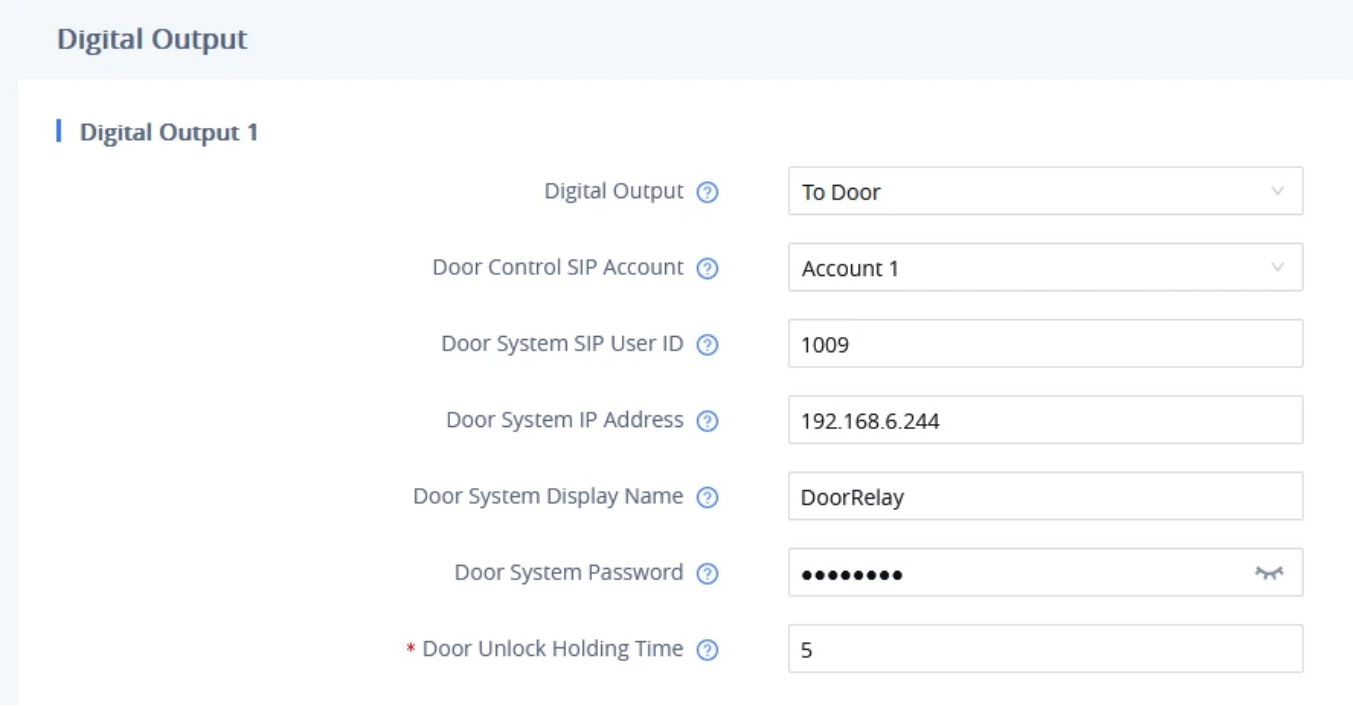


GDS372x GSC Relay Configuration

GSC357x Configuration Steps

1. Log in to the **GSC357x Web UI**.
2. Register the GSC357x account on the **same SIP server** as the GDS372x.
3. Navigate to **Settings -> Digital Output**:

- Set **Output Mode** to "To Door".
- Set **Door Control SIP Account** to Account 1.
- Set **Door System SIP User ID** to GDS372x SIP extension.
- Set the **Door System IP Address** to the GDS372x IP.
- Set **Door System Password** (same as on GDS372x).



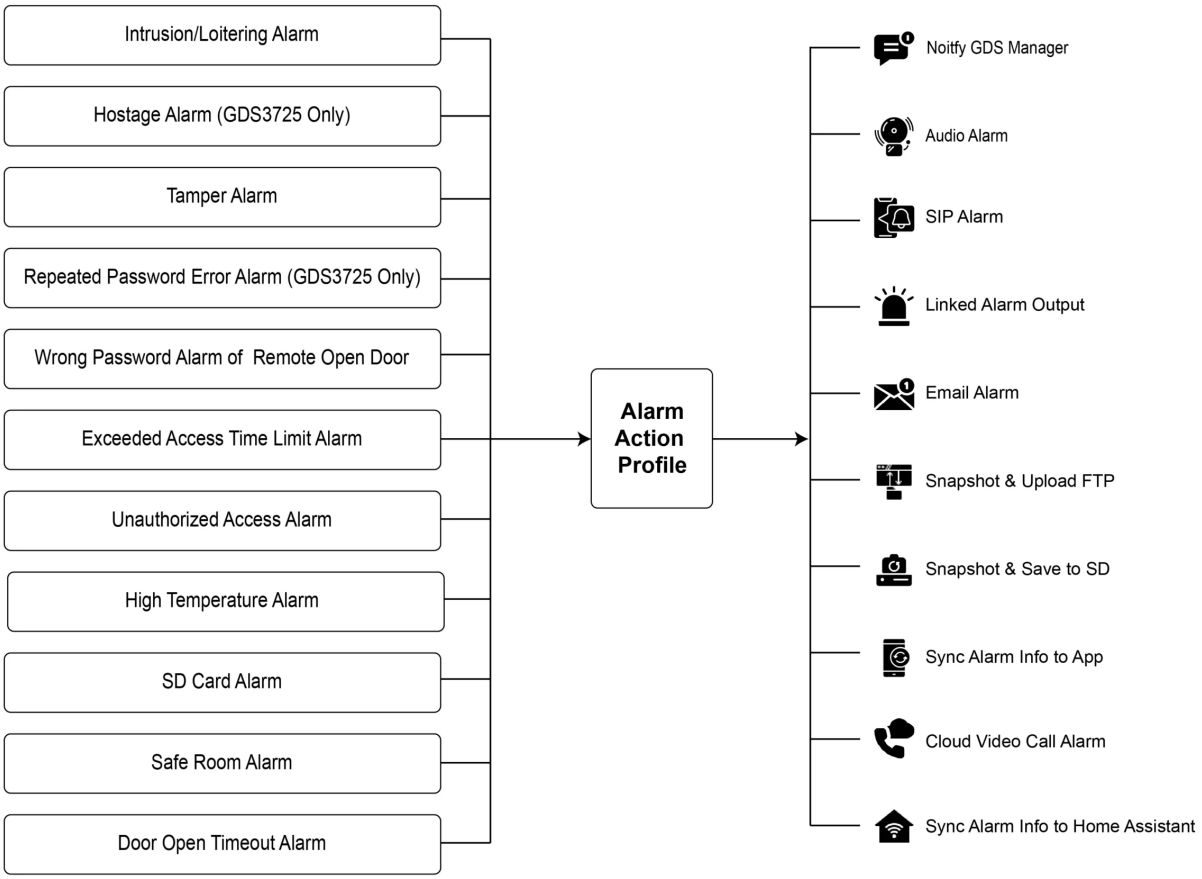
GSC357x Digital Output Settings

GDS372X BUILT-IN ALARM FUNCTIONS

The **GDS372x Series** includes a range of built-in alarms that can detect security events such as tampering, unauthorized access, or environmental conditions. These alarms trigger **user-defined response actions** through configurable **Alarm Profiles**.

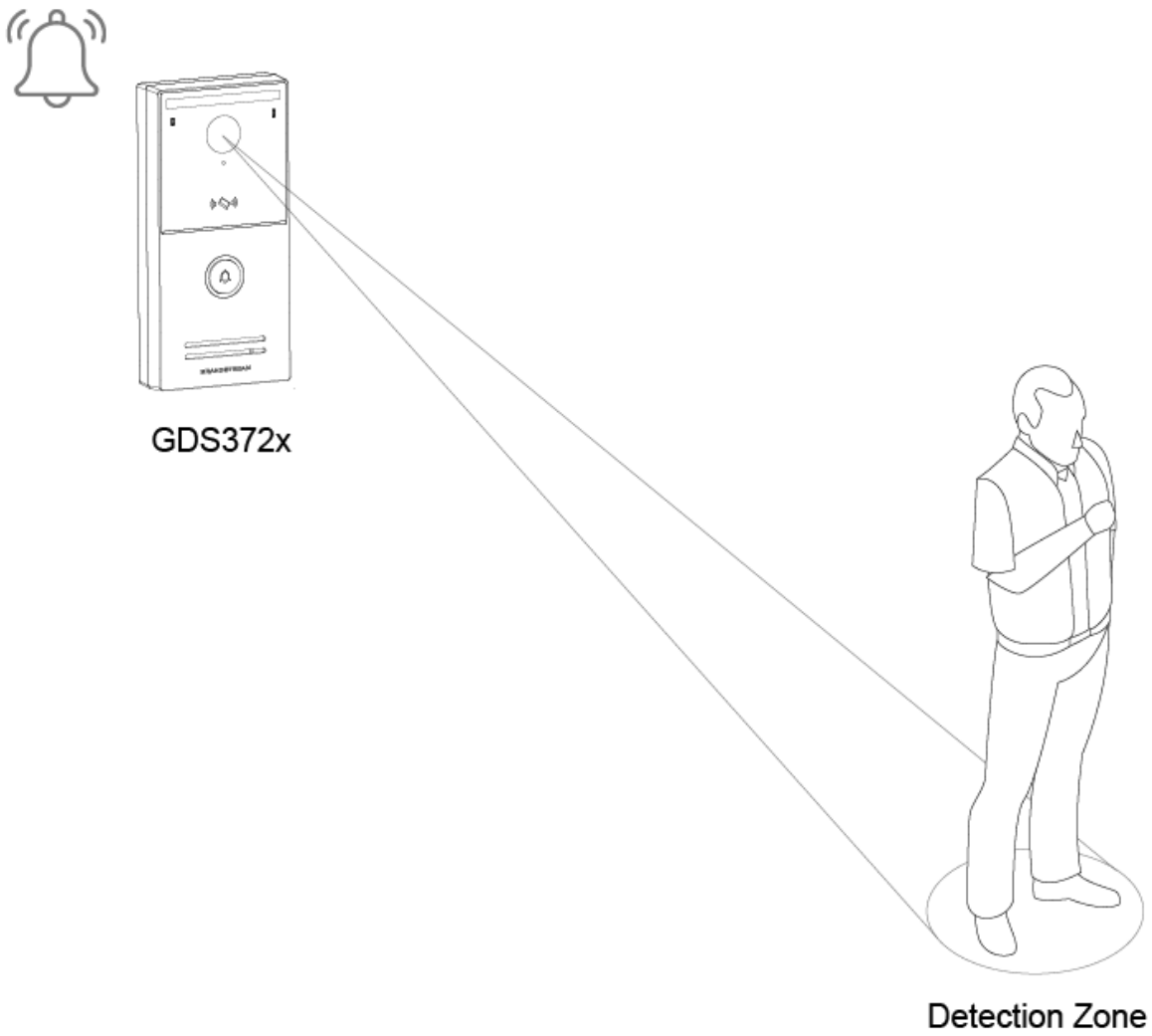
Each alarm event can be linked to one profile set under the **Alarm Action Profile** section in the GDS372x web UI. A profile defines which combination of responses should occur when an alarm is triggered.

For more information about the configuration options for each alarm, please refer to Alarm Event Settings.



GDS372x Built in Alarm Functions

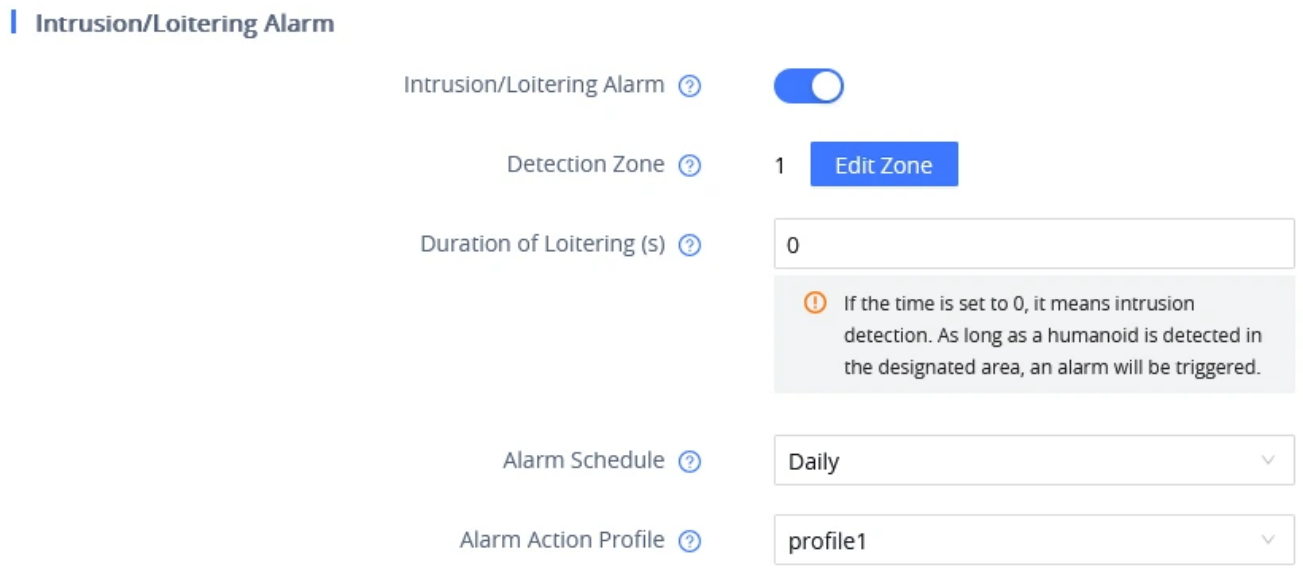
Intrusion/Loitering Alarm



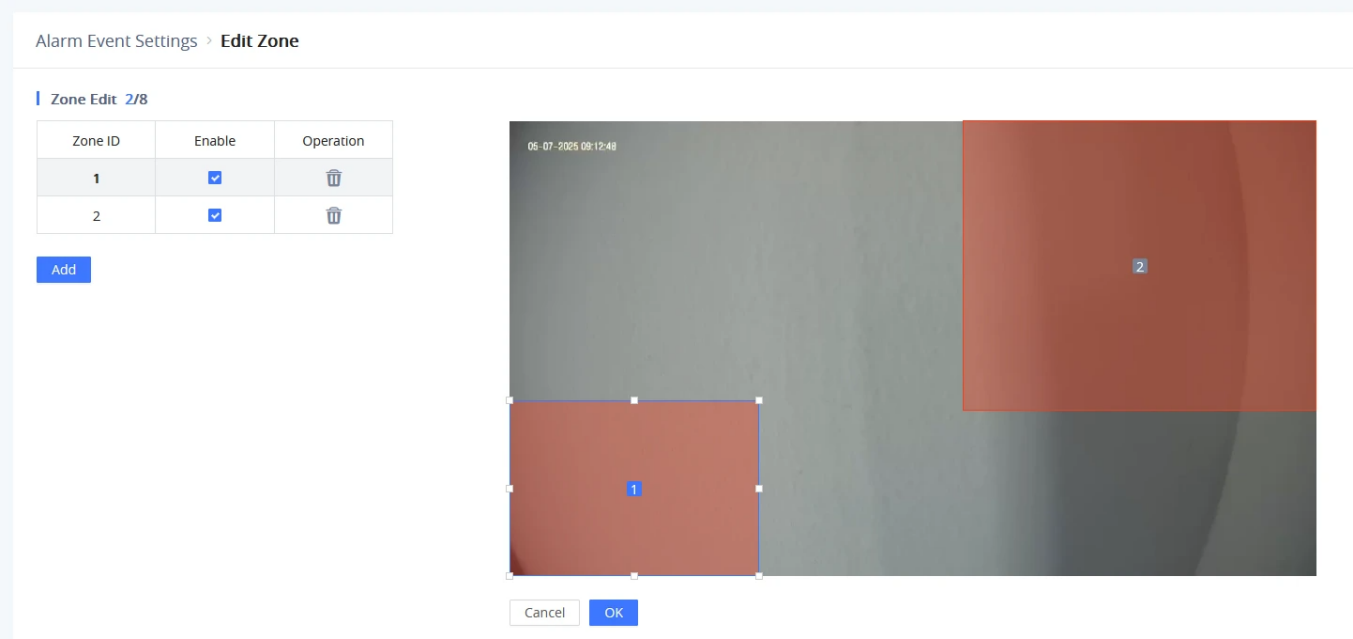
GDS372x IntrusionLoitering Alarm

This alarm monitors designated zones within the camera's field of view for unauthorized presence. Configure the detection zone by pressing **Edit Zone**, defining the desired area, and clicking Add.

When a humanoid figure is detected within the configured zones, the device generates an intrusion/loitering alarm and executes the configured alarm actions defined in the associated profile.

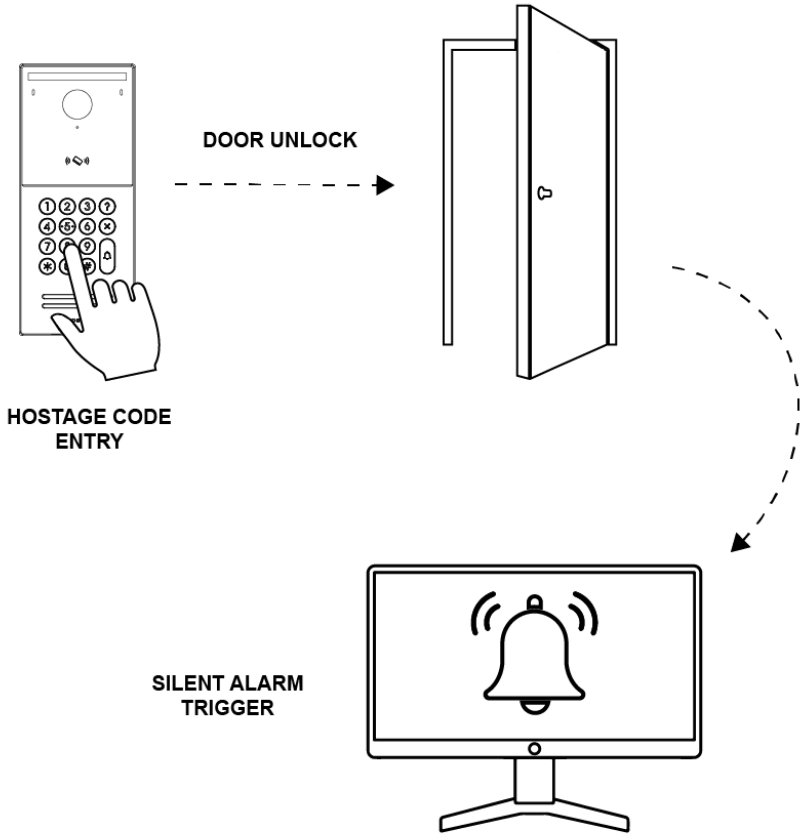


IntrusionLoitering Alarm Settings



IntrusionLoitering Alarm Settings Edit Zone

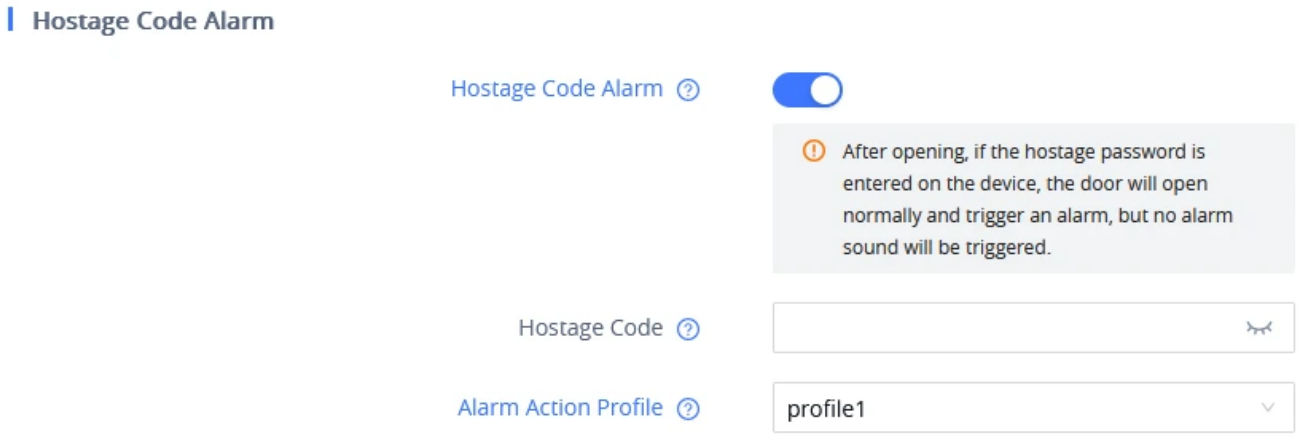
Hostage Code Alarm (GDS3725 Only)



GDS3725 Hostage Code Alarm

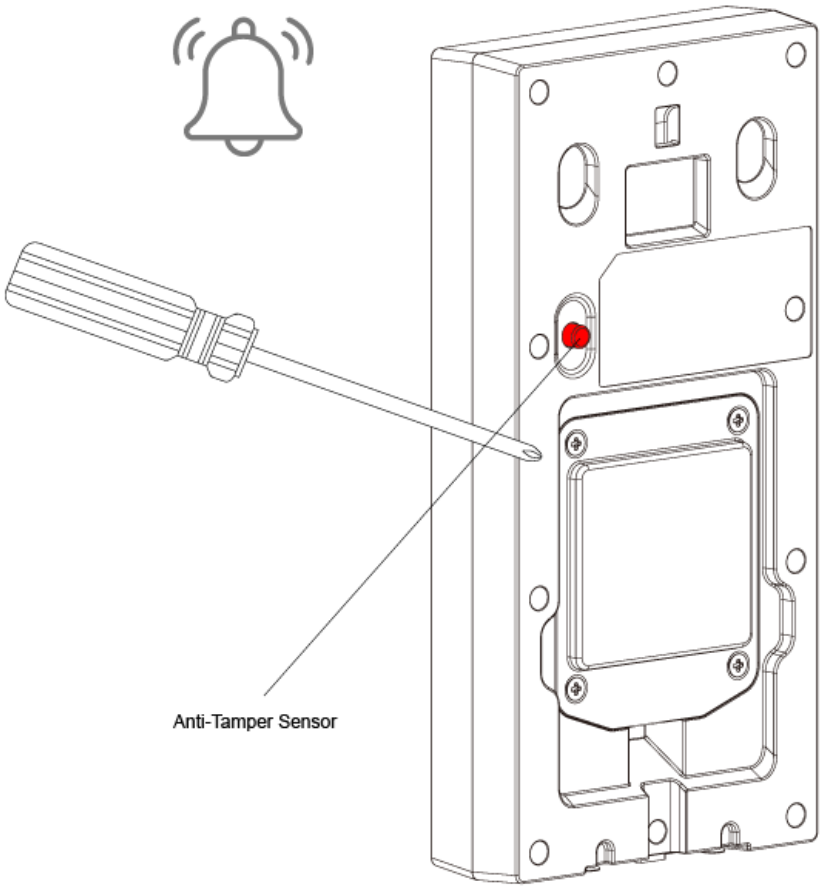
The GDS3725 Hostage Code Alarm helps improve safety by allowing a door to be opened normally while also triggering a silent alarm. This feature is particularly useful in environments where staff safety is critical, such as banks, retail stores, or secure offices.

When a user enters a predefined **hostage password** on the GDS3725 keypad, the door opens normally to avoid alerting the intruder. Simultaneously, the device generates a hostage code alarm and executes the configured alarm actions defined in the associated profile.



Hostage Code Alarm Settings

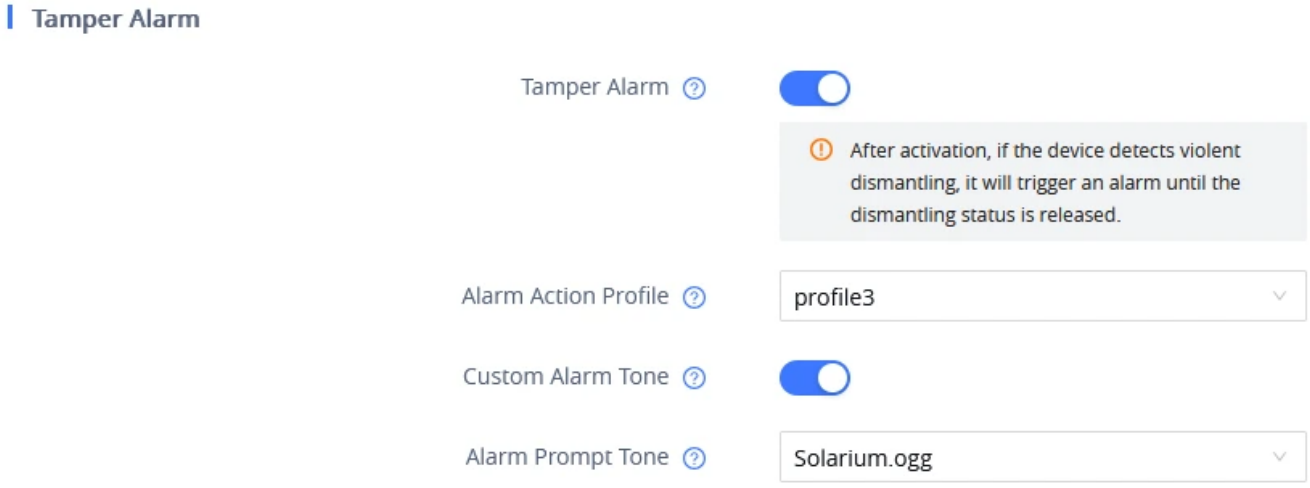
Tamper Alarm



GDS372x Tamper Alarm

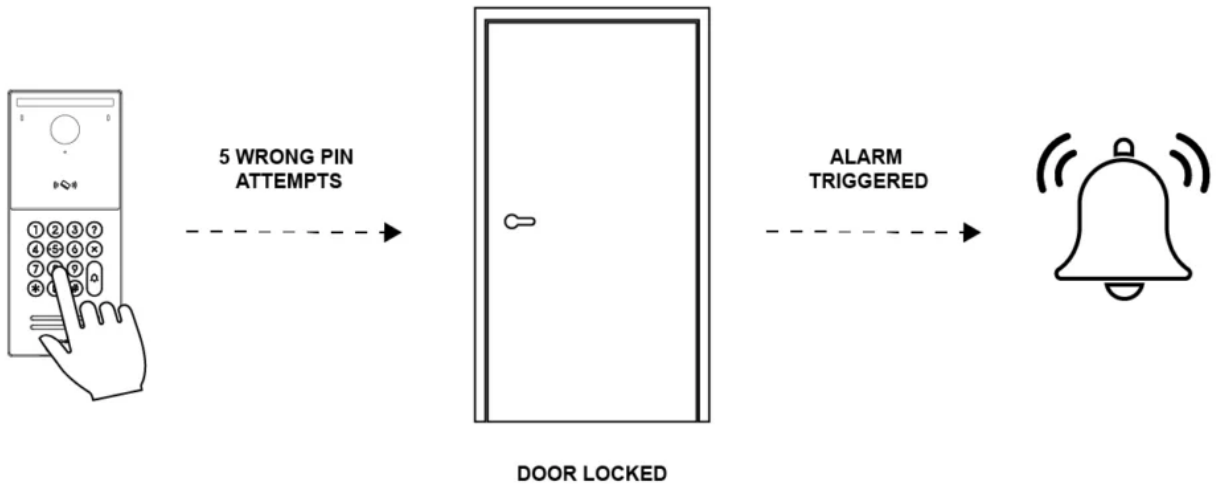
The GDS372x is equipped with a mechanical tamper detection button located on the back panel of the device. This feature is designed to enhance physical security by detecting unauthorized removal, forced detachment, or tampering attempts.

When the **tamper button** is triggered, the device generates a tamper alarm and executes the configured alarm actions defined in the associated profile.



Tamper Alarm Settings

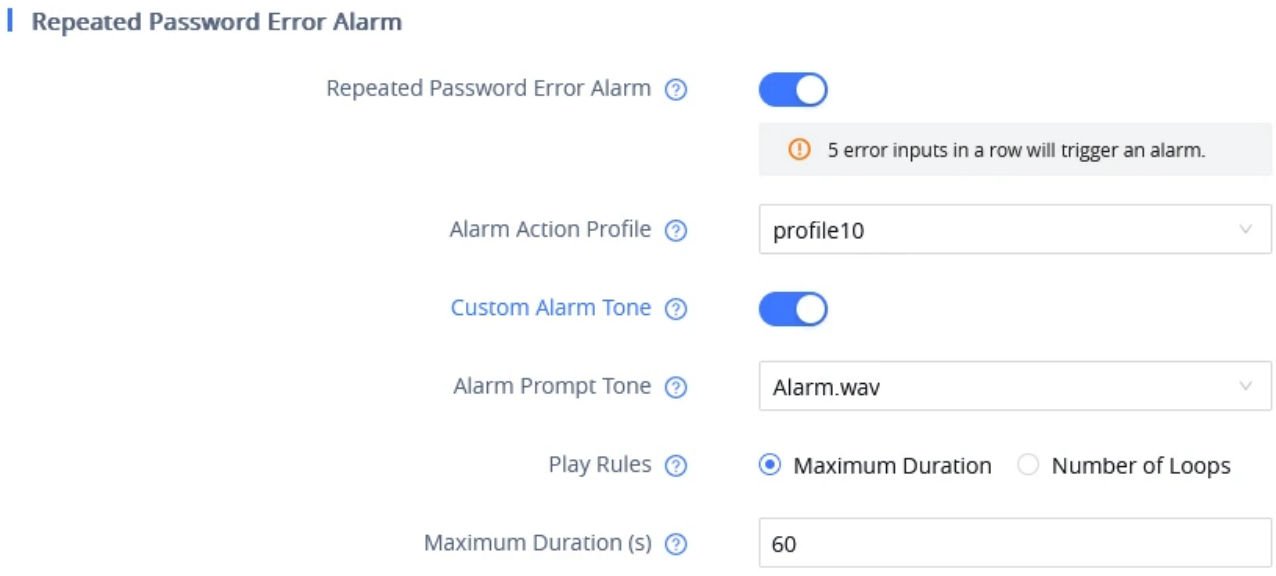
Repeated Password Error Alarm (GDS3725 Only)



GDS3725 Repeated Password Error Alarm

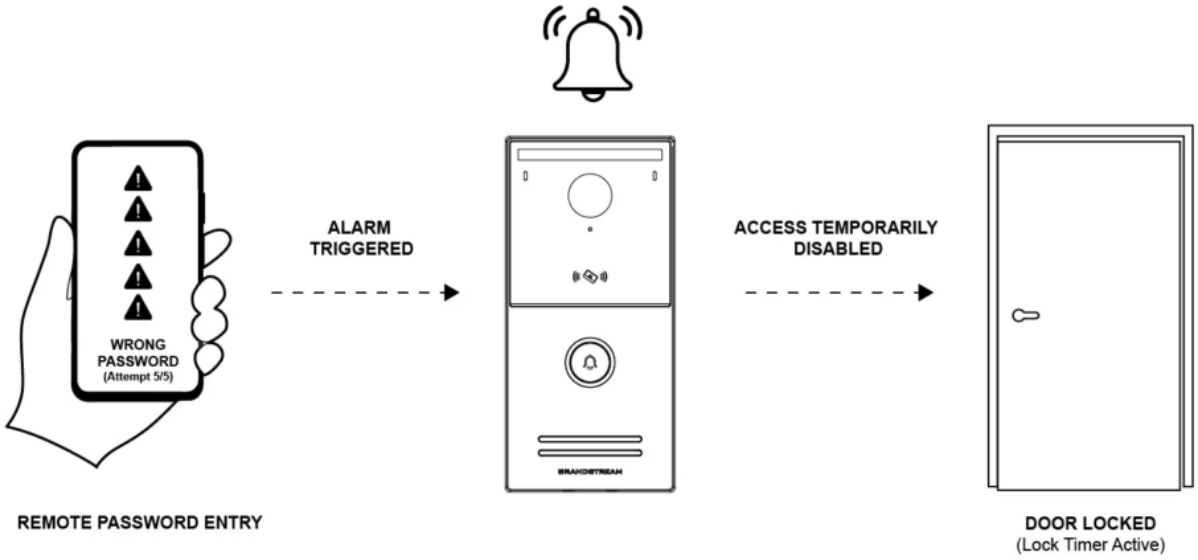
This alarm enhances security by monitoring consecutive failed GDS3725 keypad password attempts and notifying administrators of potential security breaches.

When a password is entered more than **five times incorrectly in a row**, the device generates a repeated password error alarm and executes the configured alarm actions defined in the associated profile.



Repeated Password Error Alarm Settings

Wrong Password Alarm of Remote Open Door

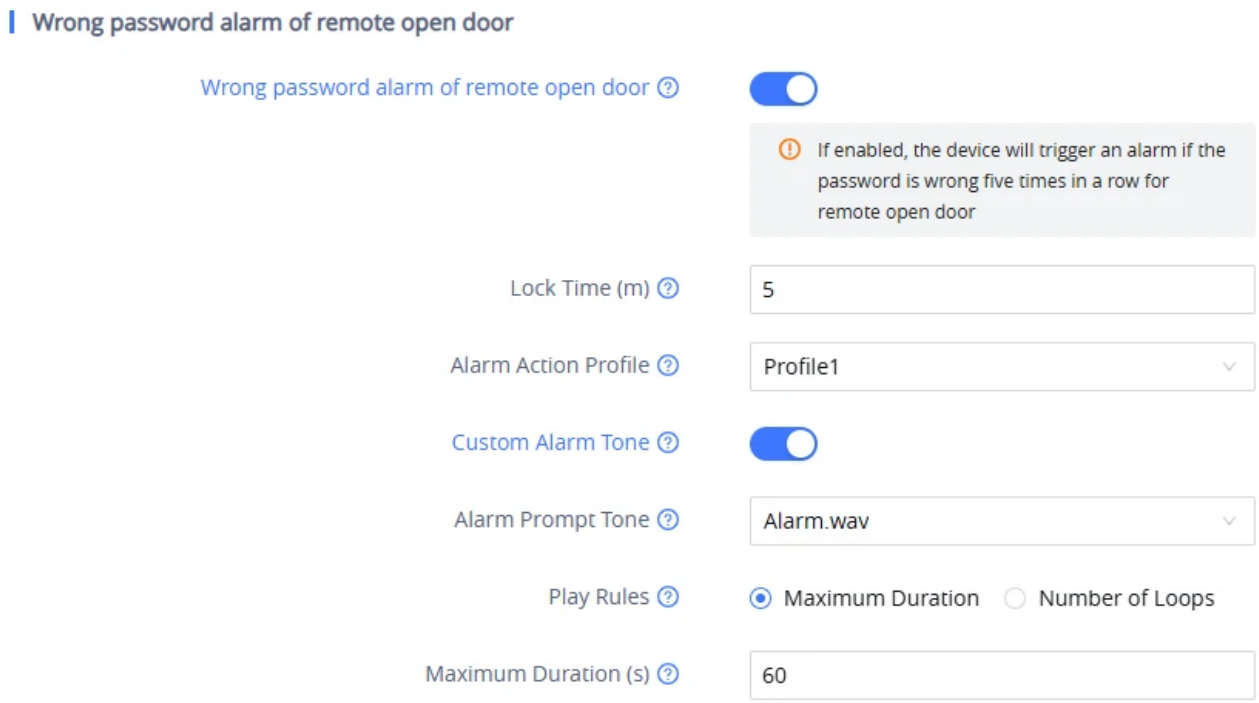


GDS372x Remote Unlock Wrong Password Alarm

This alarm improves security for remote access methods such as SIP calls, HTTP API, or mobile app unlock. This feature helps prevent brute-force attempts and repeated incorrect password entries during remote door unlocking.

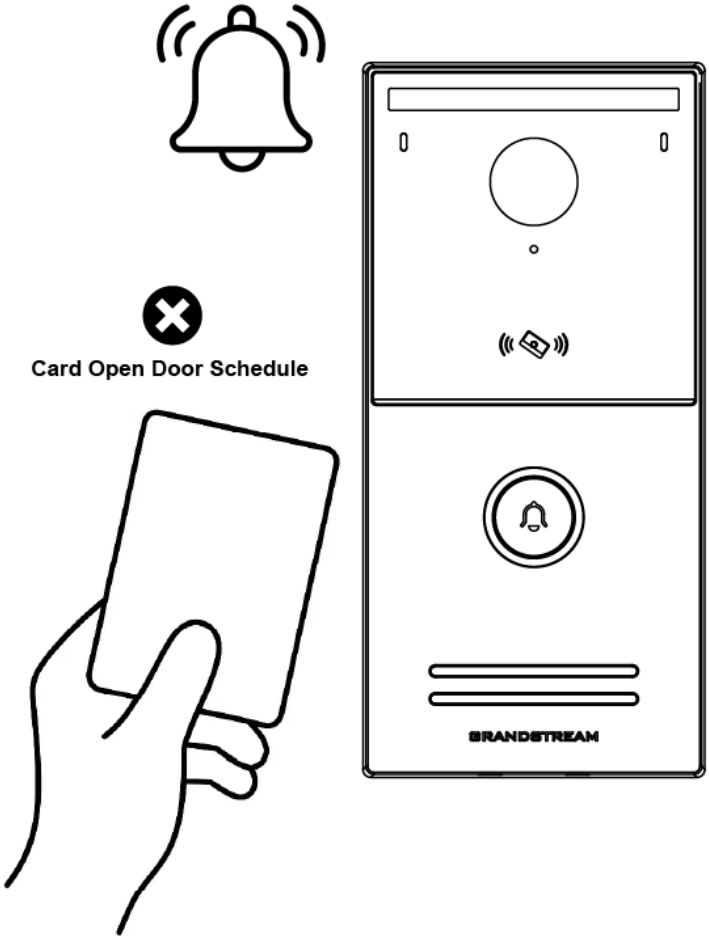
When a user enters an incorrect password **five consecutive times** during a remote unlock attempt, the device generates a wrong password alarm for remote open door and executes the configured alarm actions defined in the associated profile.

Additionally, the device temporarily disables remote door opening for a configured lockout period to prevent further unauthorized attempts.



Remote Unlock Wrong Password Alarm Settings

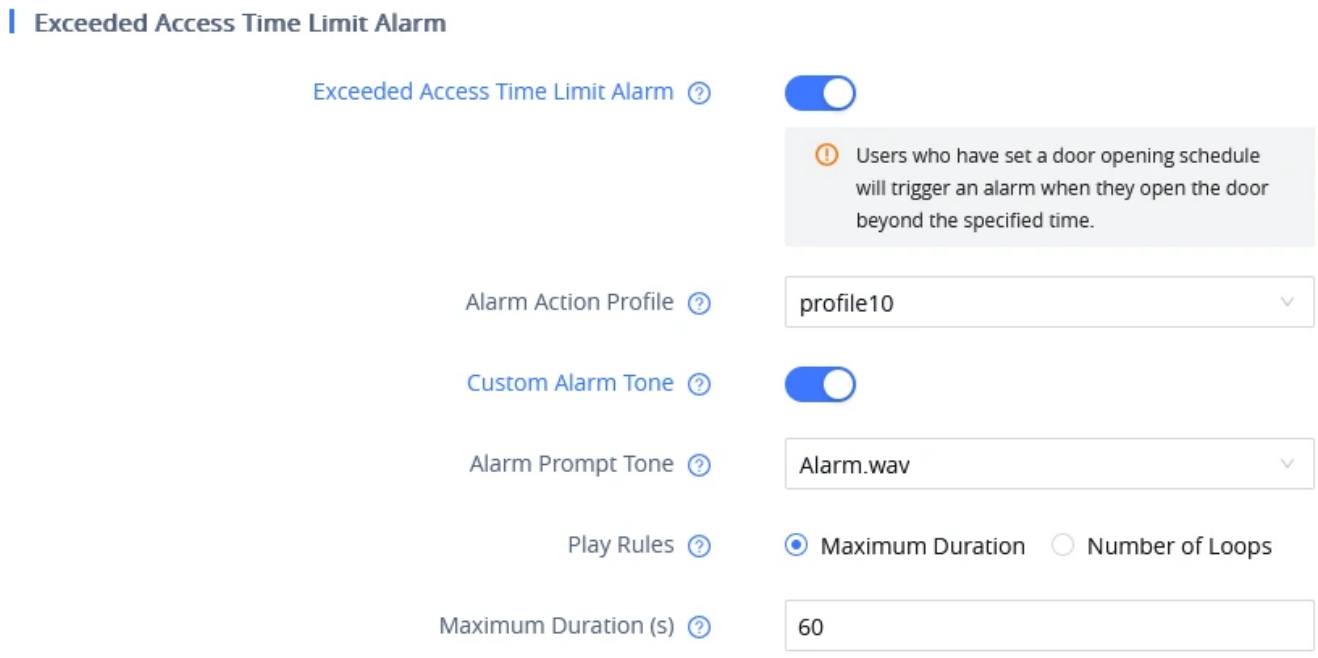
Exceeded Access Time Limit Alarm



GDS372x Exceeded Access Time Limit Alarm

This alarm enhances security by enforcing time-based access restrictions for registered users. It is particularly useful in environments where access is only permitted during specific hours, such as office spaces, restricted labs, or shared facilities.

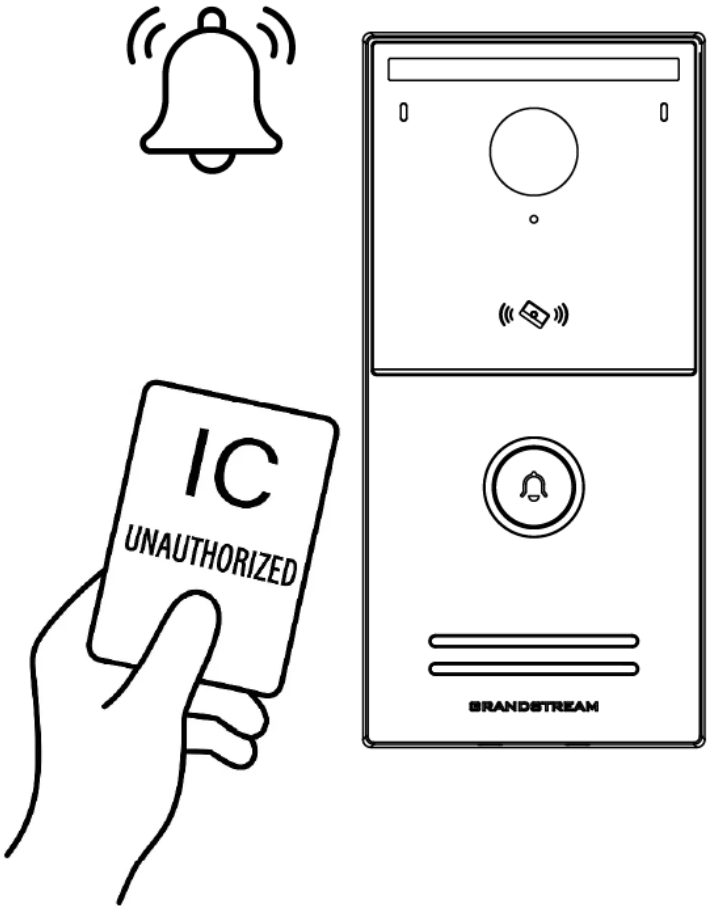
When a user presents a valid access card but attempts to open the door **outside of their predefined time schedule**, the device recognizes this as a time violation and generates an exceeded access time limit alarm and executes the configured alarm actions defined in the associated profile.



Exceeded Access Time Limit Alarm Settings

Administrators can configure the open door schedule for card users under **Access Control Settings -> Card Management.**

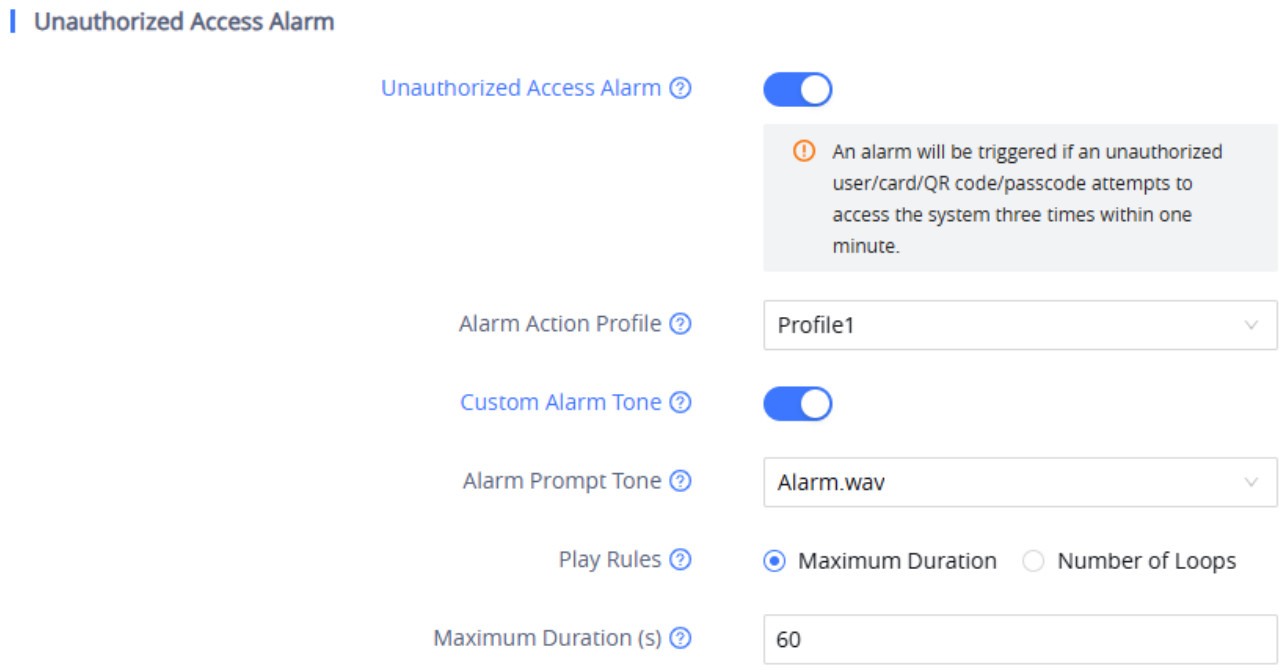
Unauthorized Access Alarm



GDS372x Unauthorized Access Alarm

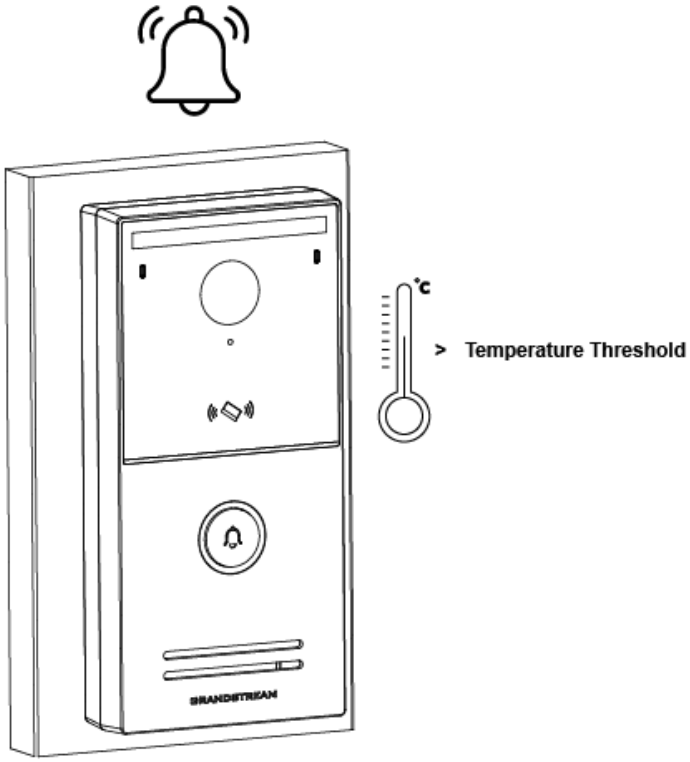
This alarm enhances access control by identifying and responding to the use of unregistered or unauthorized IC/ID cards at the GDS372x reader.

When an unrecognized or disabled IC card is scanned at the door reader, the device flags the attempt and generates an unauthorized access alarm, and executes the configured alarm actions defined in the associated profile.



Unauthorized Access Alarm Settings

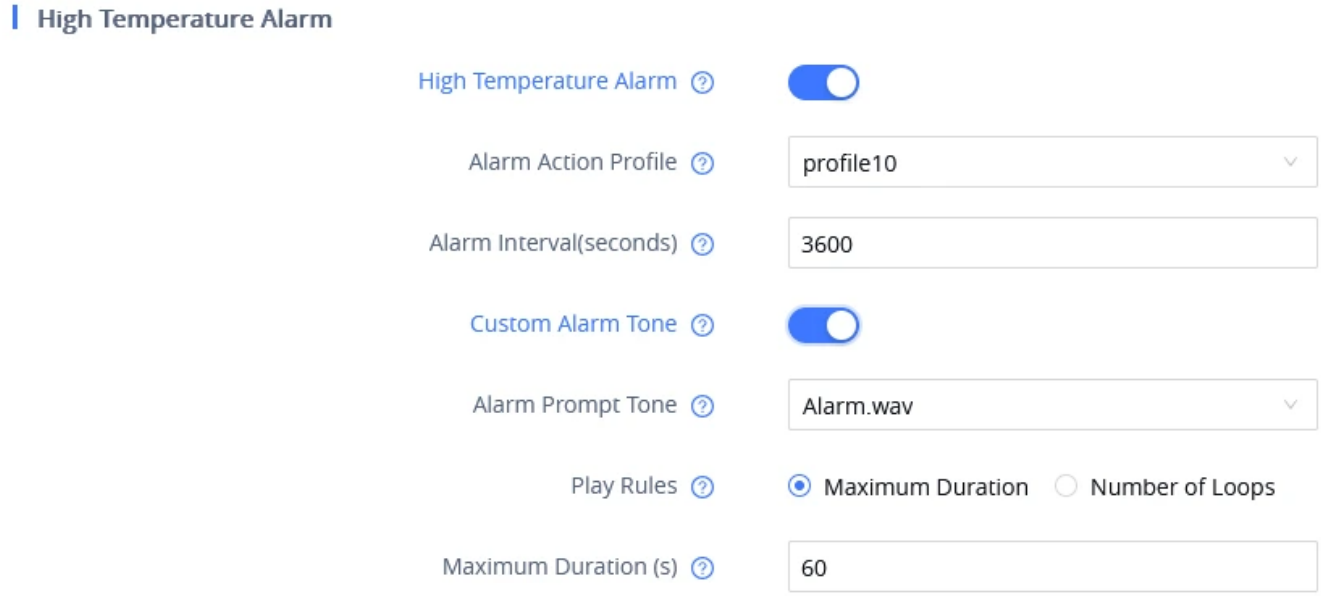
High Temperature Alarm



GDS372x High Temperature Alarm

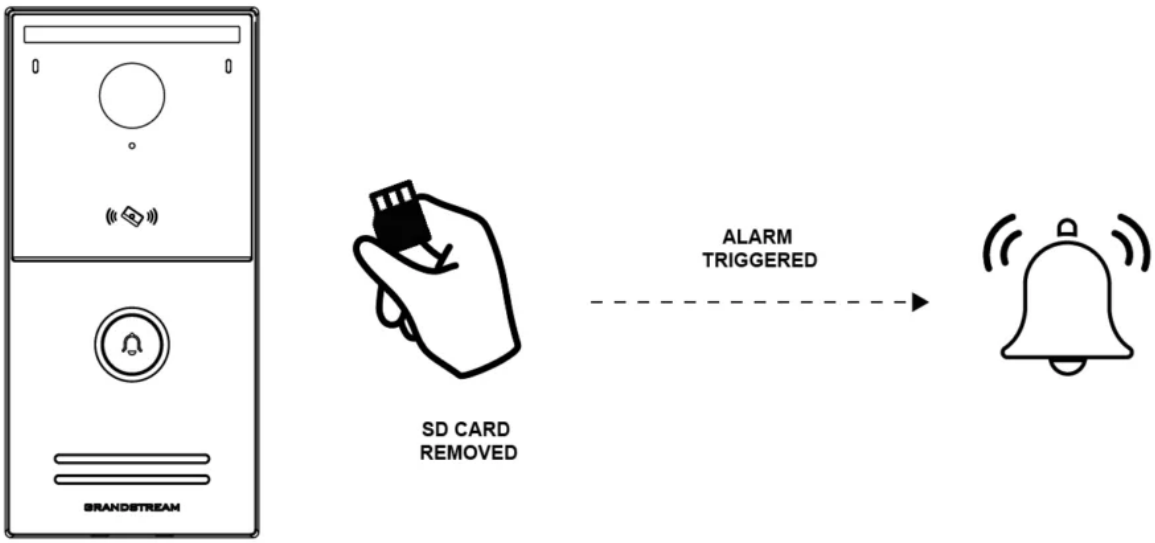
This alarm monitors the temperature of the device through an **internal sensor** that detects excessive temperature fluctuations.

When the device detects that the temperature exceeds the configured threshold, it generates a high temperature alarm at the **configured interval** and executes the configured alarm actions defined in the associated profile.



High Temperature Alarm Settings

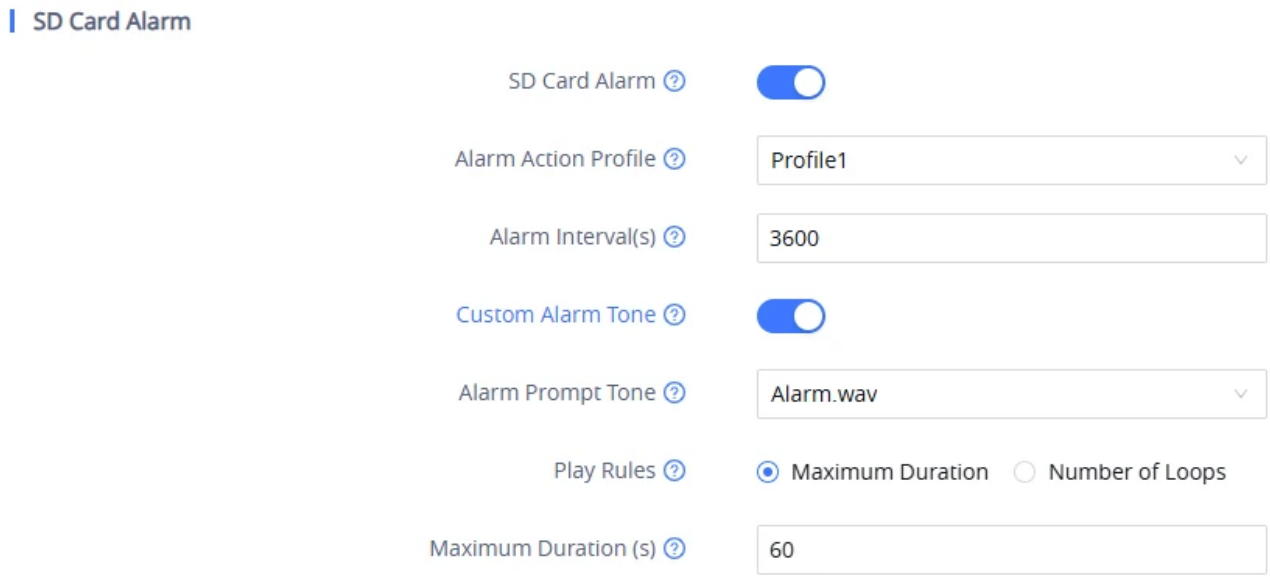
SD Card Alarm



GDS372x

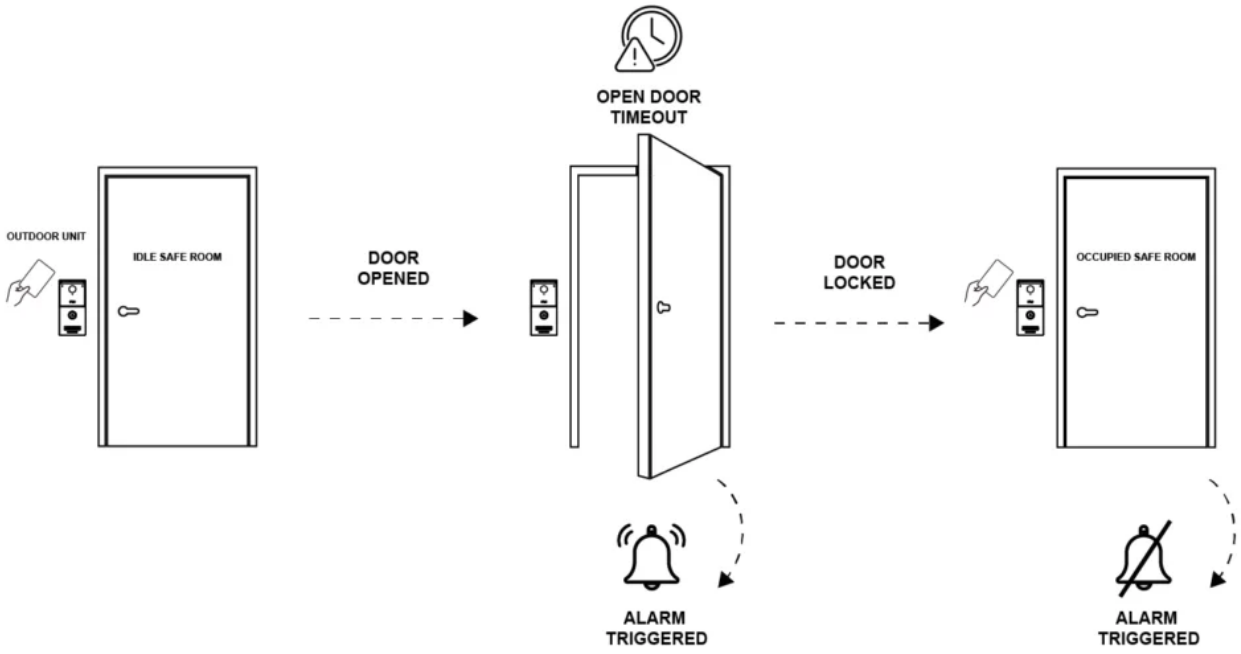
This alarm monitors the status of the **SD card** and detects conditions such as read/write operation failures, SD card removal, or other abnormalities by checking the SD card status at the configured interval.

When the device detects an abnormal condition, it generates an SD card alarm and executes the configured alarm actions defined in the associated profile.



SD Card Alarm Settings

Safe Room Alarm

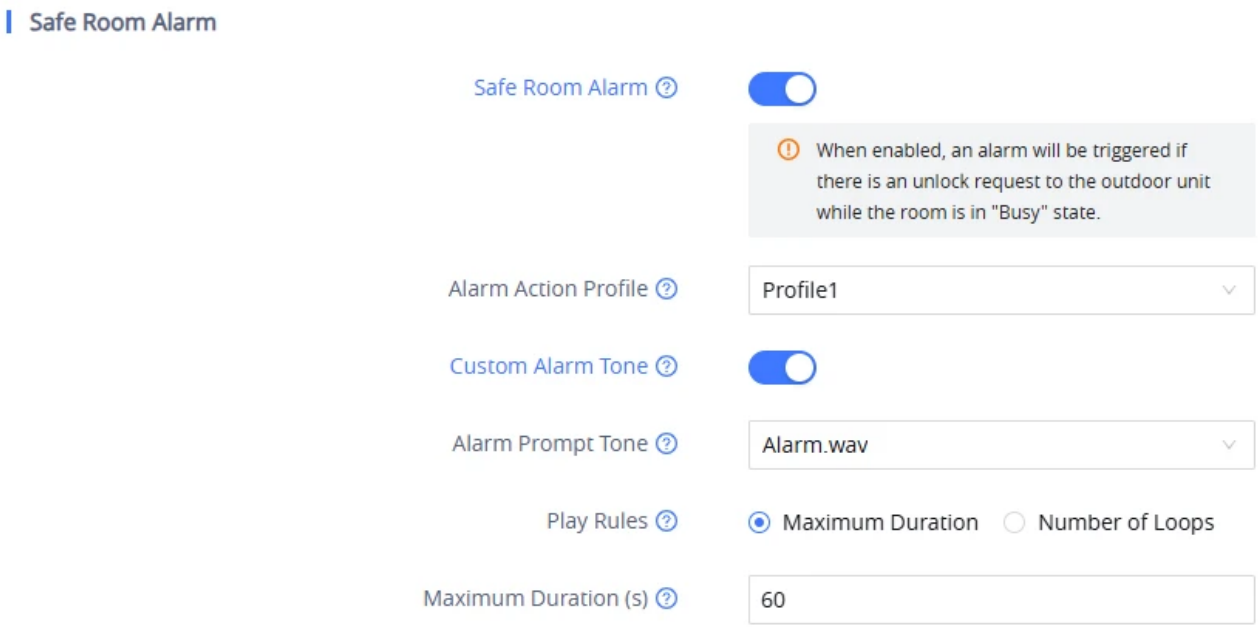


GDS372x Safe Room Alarm

This alarm is used in **Safe Room Mode**, a security feature that monitors whether the safe room is in an idle or occupied state and prevents entry attempts from the outdoor unit while the room is occupied. The alarm is triggered under the following conditions:

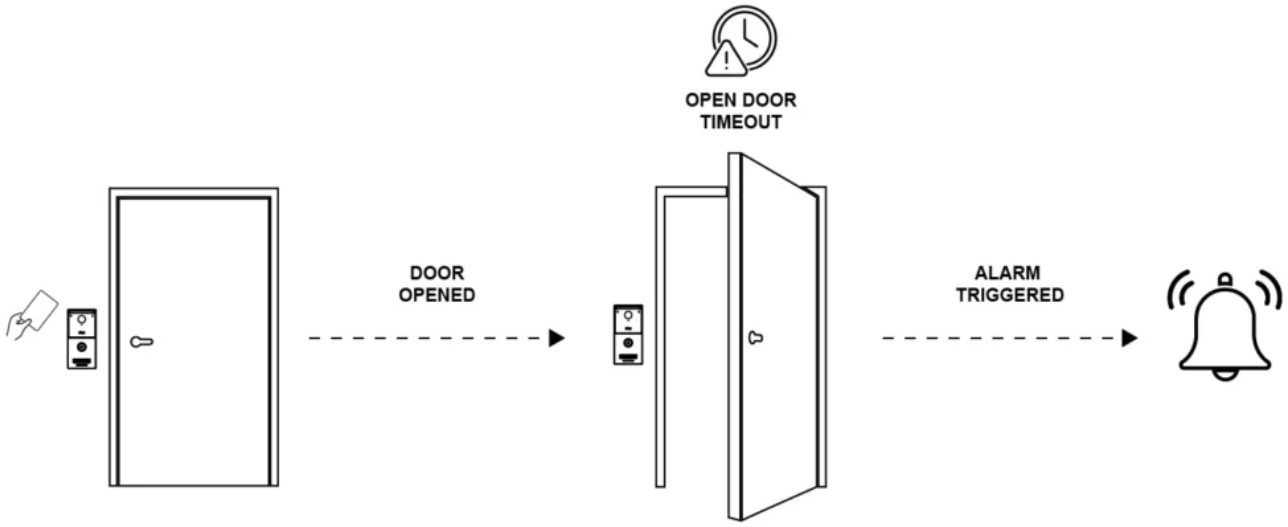
- When the safe room is **occupied** and an attempt is made to open the door from the outdoor unit, the device generates a 'Security Room Occupied' alarm record locally and/or through cloud services and executes the configured alarm actions defined in the associated profile..
- When the safe room is in **idle** state and the door is opened via card or password authentication from the outdoor or indoor unit, but is not closed within the duration configured in Open Door Timeout Alarm. In this case, the device generates an Open Door Timeout alarm and executes the configured alarm actions defined in the associated profile. Both Safe Room Alarm and Open Door Timeout Alarm must be enabled.

For further information about the Safe Room setup and configuration, please refer to the GDS372x Series Safe Room Guide.



Safe Room Alarm Setting

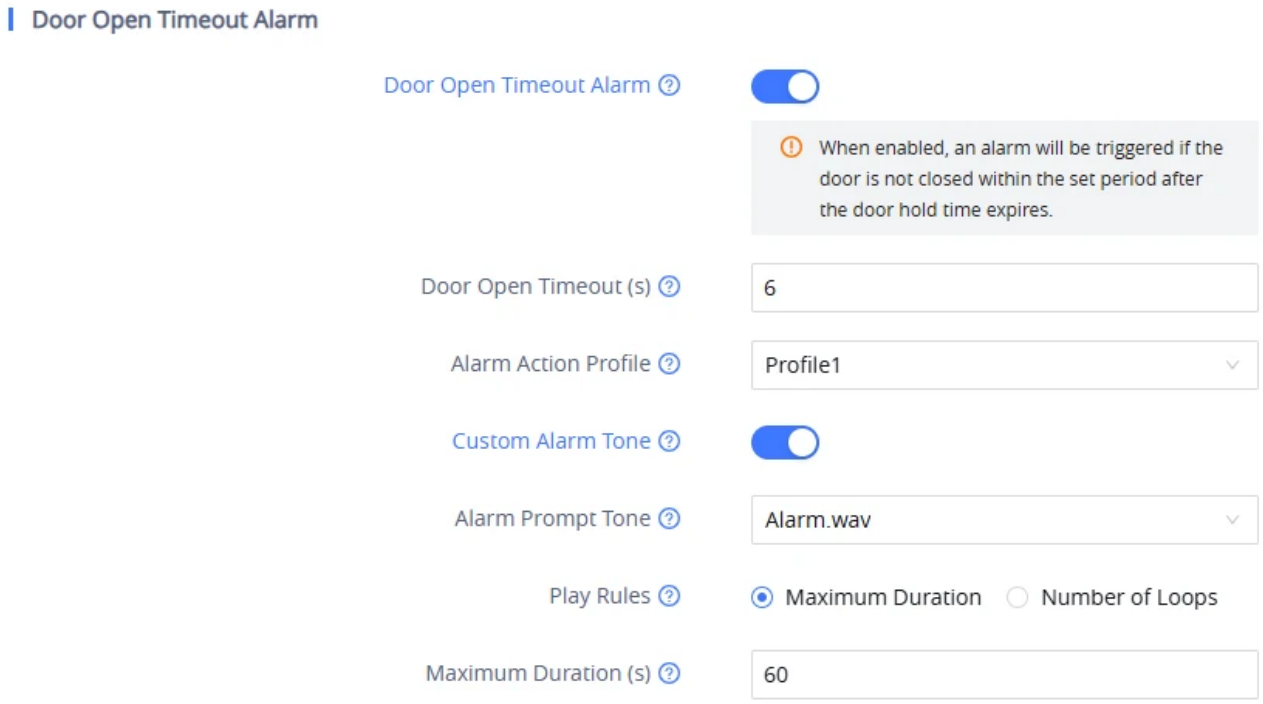
Door Open Timeout Alarm



GDS372x Door Open Timeout Alarm

This alarm enhances security when the door remains open beyond the **configured duration** and is used in Safe Room mode.

When the door remains open beyond the configured duration, the device generates an Open Door Timeout alarm and executes the configured alarm actions defined in the associated profile.



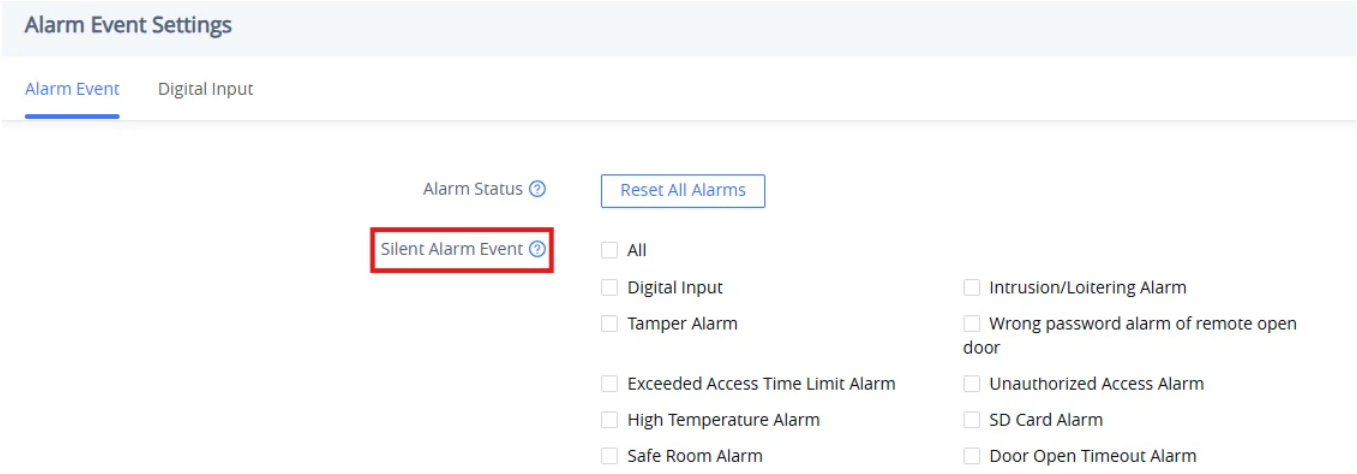
Door Open Timeout Alarm Settings

Silent Alarm

Users can specify which alarms should operate in silent mode, triggering the assigned actions without producing an audible sound. This is useful in scenarios where discreet alerts are required without disturbing the environment.

To set silent alarms, users can select the events that will trigger the silent alarm under **Alarm Event Settings** by checking the corresponding check boxes (multiple selections are allowed).

The Hostage Code Alarm is inherently a silent alarm by design. Therefore, it cannot be selected under the Silent Alarm Event settings.



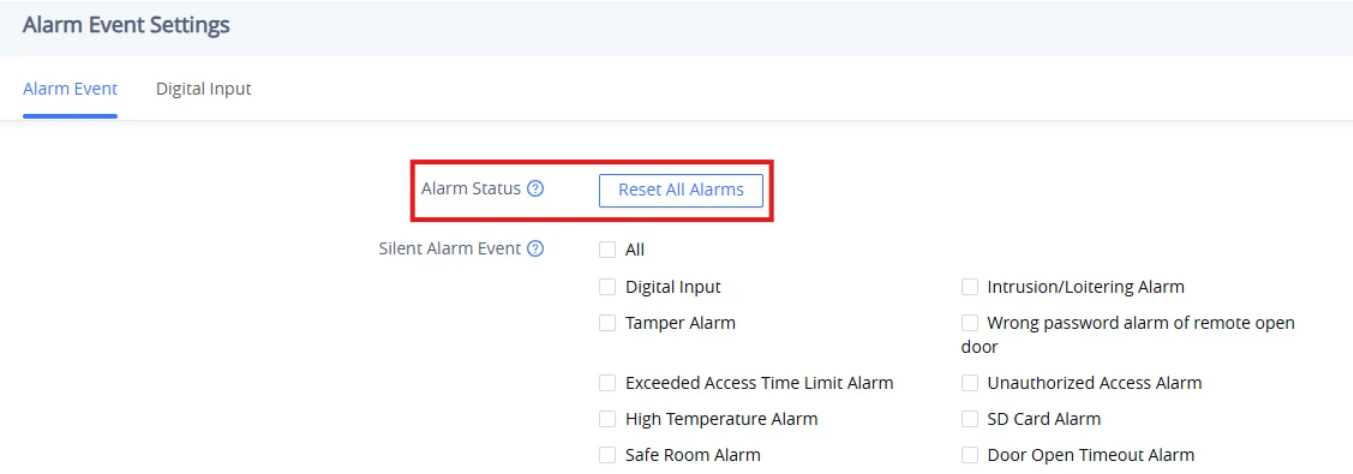
Silent Alarm Event

Reset All Alarms

This feature allows users to restore all alarm statuses on the GDS372x device and clear any active alarms

with a single click, returning the system to a neutral state and ensuring accurate monitoring.

To reset all alarms, navigate to the **Alarm Event Settings** page and click the "Reset All Alarms" button.



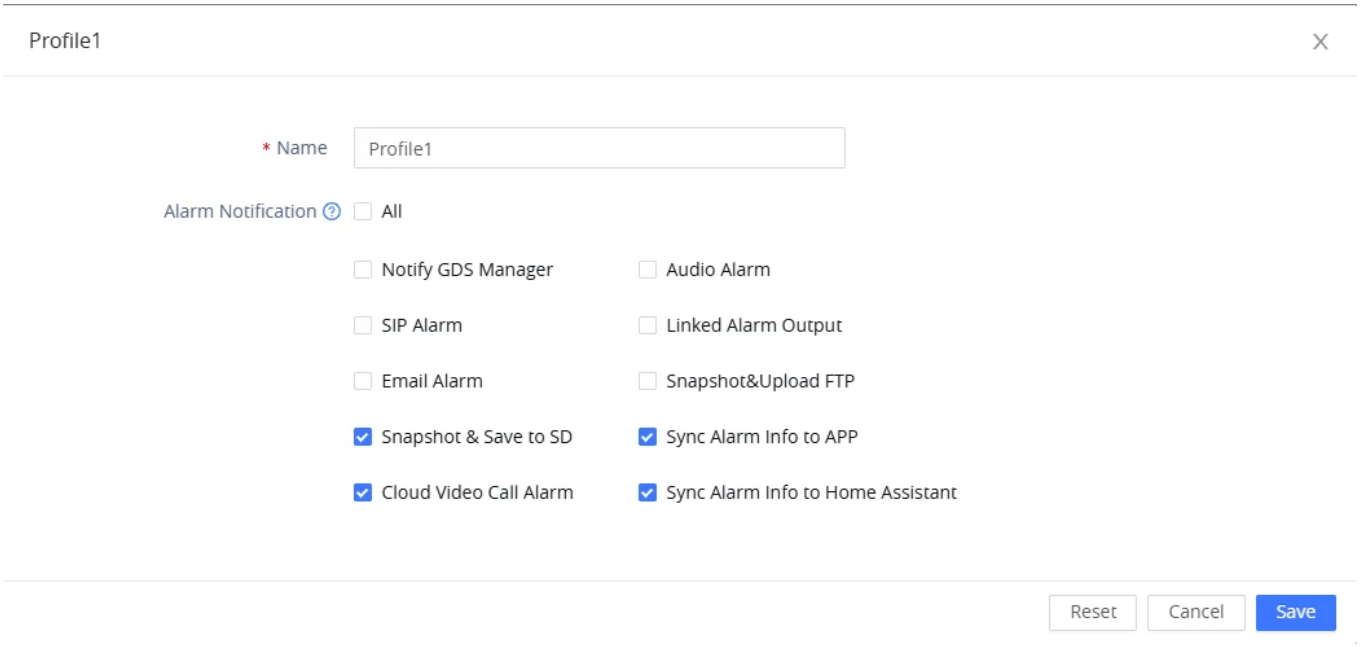
Reset All Alarms Button

Alarm Profile Association

Each alarm is mapped to a profile number (e.g., Profile 1, Profile 2, etc.) in the GDS372x settings. Each profile can define one or more alarm actions by selecting the corresponding checkboxes below or by enabling the All option:

- **Notify GDS Manager** 2: Sends a real-time notification to GDS Manager 2.
- **Audio Alarm**: Triggers built-in audio alarm.
- **SIP Alarm**: Calls a designated SIP endpoint (e.g., a video intercom).
- **Linked Alarm Output**: Activates relay/digital output (e.g., a siren).
- **Email Alarm**: Sends email notification.
- **Snapshot & Upload to FTP:** Captures a snapshot and uploads it to a configured FTP server.
- **Snapshot & Save to SD:** Captures a snapshot and saves it to the device's SD card.
- **Sync Alarm Info to App**: Sends the alarm information to the mobile app.
- **Cloud Video Call Alarm**: When the cloud service is enabled, Account 4 (Cloud Account) is automatically used as the callout account.
- **Syn Alarm Info to Home Assistant**: Sends alarm information to the Home Assistant platform.

- If Email Alarm is selected, configure Email Settings under **System Settings -> Email Settings**.
- If Snapshot & Upload FTP is selected, configure FTP Settings under **System Settings -> FTP Settings**.
- if Cloud Video Call Alarm is selected, configure the cloud call number under **Alarm Settings -> Alarm Action -> Alarm Notification Settings -> Cloud Video Call Alarm**.



GDS372x Alarm Action Profile Settings

GDS372X WEB UI SETTINGS

This section describes the options in the GDS372x Web GUI, summarized below:

- **Status:** Display the Account status, Network status, and System Info of the GDS372x.
- **Real-time Preview:** View the live video streams of the GDS372x using your browser.
- **Access Control Settings:** Configure door-related access and output settings, including door unlock methods, doorbell behavior, card management, door opening schedules, and access logs that record all door entry activities.
- **Alarm Settings:** Configure digital alarm input settings, built-in GDS372x alarm functions, action profiles, notification settings, alarm scheduling, and view logs of all triggered alarms.
- **Audio & Video Settings:** Configure audio settings and video-related functions such as OSD (On-Screen Display), CMOS parameters, and privacy masking.
- **Monitoring:** Configure ONVIF and RTSP settings for video streaming and integration with third-party systems.
- **Account Settings:** Configure the SIP account settings for the GDS372x.
- **Calls:** Place outgoing calls directly from the Web UI, review call history logs, and manage the call allowlist for enhanced control over incoming and outgoing call permissions.
- **Phone Settings:** Configure various call-related features such as ringtones, auto-answer, DND options, multicast paging, and other preferences.
- **Network Settings:** Configure network-related parameters, including IPv4 address mode (DHCP, Static, PPPoE), Wi-Fi settings, and advanced options such as OpenVPN(R) for secure remote access.
- **System Settings**: Manage system-level configurations such as time, Web/SSH access permissions, LED behavior, audio control, TR-069, backup and restore, email notifications, and FTP settings.
- **Maintenance**: Perform system maintenance tasks, including firmware upgrades, configuration provisioning, factory reset, event notification setup, and system diagnostics.
- **Application**: Configure account sharing on the GDS372x to synchronize SIP credentials with other supported Grandstream devices.
- **Diagnostic**: Provides built-in tools to test and verify device functionality, such as microphone test, relay out test, tamper test, etc.

Status Page Definitions

System Info

System Info -> Information	
Product Model	Product model of the GDS372x.
Part Number	Product part number.
Software Version	
Software Version	Boot: boot version number.Core: core version number.Prog: program version number. This is the main firmware release number, which is always used for identifying the software system of the GDS372x.Locale: locale version number.Res: Resolution version number.
IP Geographic Information	
Recommend Time Zone	Represent the time zone detected based on the IP address.
System Time	
System Up Time	System up time since the last reboot.
System Time	Current system time on the GDS372x system.
System Time-Zone	Displays the time zone that is configured by user.
SD Card Storage Status	
Total Space	Displays the total space of the connected SD card.
Used Space	Displays the used space of the connected SD card.
Available Storage	Displays the available space of the connected SD card.
PoE Detection	
PoE Status	Indicates that the device is powered using Power over Ethernet (PoE).
System Information	
Download System Information	Click to download system information.
Security Version	Displays the GDS372x security version.
System Info -> Status	
User Space	Shows the percentage of the user space used and the status of the Database.
Core Dump	Shows the status of the core dump and the core dump files generated if any. It also gives the ability to generate GUI/AVS/CPE/Phone core dump files manually.
Special Feature	OpenVPN(R) Support: displaying if the GDS372x supports OpenVPN(R).
System Info -> Cloud Service	
Overview	Displays the organization to which the device belongs.
Name of the package	Displays the name of the current package.
Expiration Date	Displays the expiration date of the package.
Status	Displays the current package status:ExpiredExpiring Soon TrialValidPermanent
A Description of the Package	Redirects to the SecureAccess License Fees page on Grandstream Cloud for information about the available licenses and fees.

Network Status

Network Status -> Ethernet	
LAN Port	Indicates the current status and speed (e.g., 100Mbps/Full) of the device's LAN connection.
MAC Address	Displays the unique hardware address assigned to the device's Ethernet interface.
PPPoE Link Up	Shows whether the PPPoE connection is established.
IPv4	
IPv4 Address Type	Indicates how the IPv4 address is obtained (e.g., DHCP, Static, PPPoE).
IPv4 Address	Displays the current IPv4 address assigned to the device.
Gateway	Shows the IPv4 default gateway used for routing external traffic.
IPv4 NAT Type	Displays the Network Address Translation type.
IPv6	
IPv6 Address Type	Indicates how the IPv6 address is assigned (e.g., Auto Config, Static).
Global Unicast Address	The device's public IPv6 address used for external communication.
Link-Local Address	An automatically assigned local IPv6 address valid only within the local network segment.
IPv6 Gateway	Shows the default IPv6 gateway address.
IPv6 DUID	DHCP Unique Identifier used for IPv6 DHCP communication.
IPv6 NAT Type	Indicates the IPv6 NAT behavior.
Network Status -> Wi-Fi	
WLAN MAC Address	The WLAN MAC Address is a unique identifier assigned to the Wi-Fi interface of the GDS372x, facilitating network communication and device recognition within the WLAN (Wireless Local Area Network).
SSID	The SSID (Service Set Identifier) is the name of the Wi-Fi network broadcasted by the access point, allowing devices like the GDS372x to identify and connect to the correct network.
Country Code	Displays the country where the GDS372x is deployed.
IPv4 Address Type	Indicates how the IPv4 address is assigned.
IPv4 Address	Displays the IPv4 address with its corresponding subnet mask.
Gateway	Displays the IP address of the gateway
IPv4 NAT Type	Displays the type of NAT used in the IPv4 network.
IPv6 Address Type	Displays how the GDS372x have had its IPv6 address assigned.
Global Unicast Address	Displays the IPv6 Global Unicast Address.
Link-Local Address	Displays the Link-Local Address.
IPv6 Gateway	Displays the IPv6 gateway address.
IPv6 DUID	Displays the DHCP Unique Identifier.
IPv6 NAT Type	Displays the IPv6 NAT Type used.
Network Status -> DNS & NAT	
DNS Server	Displays the Primary and secondary DNS servers used
DNS Mode	Displays the DNS mode used by each account
NAT Traversal	Displays the NAT traversal mode used

Account Status

Account	Account index, shows the list of supported accounts.
SIP User ID	Displays the configured SIP User ID for the account.
SIP Server	Displays the configured SIP Server address, URL or IP address, and port of the SIP server.
Operation	Displays the different types of operations that can be performed on each SIP account, including editing the account, accessing the voicemail....

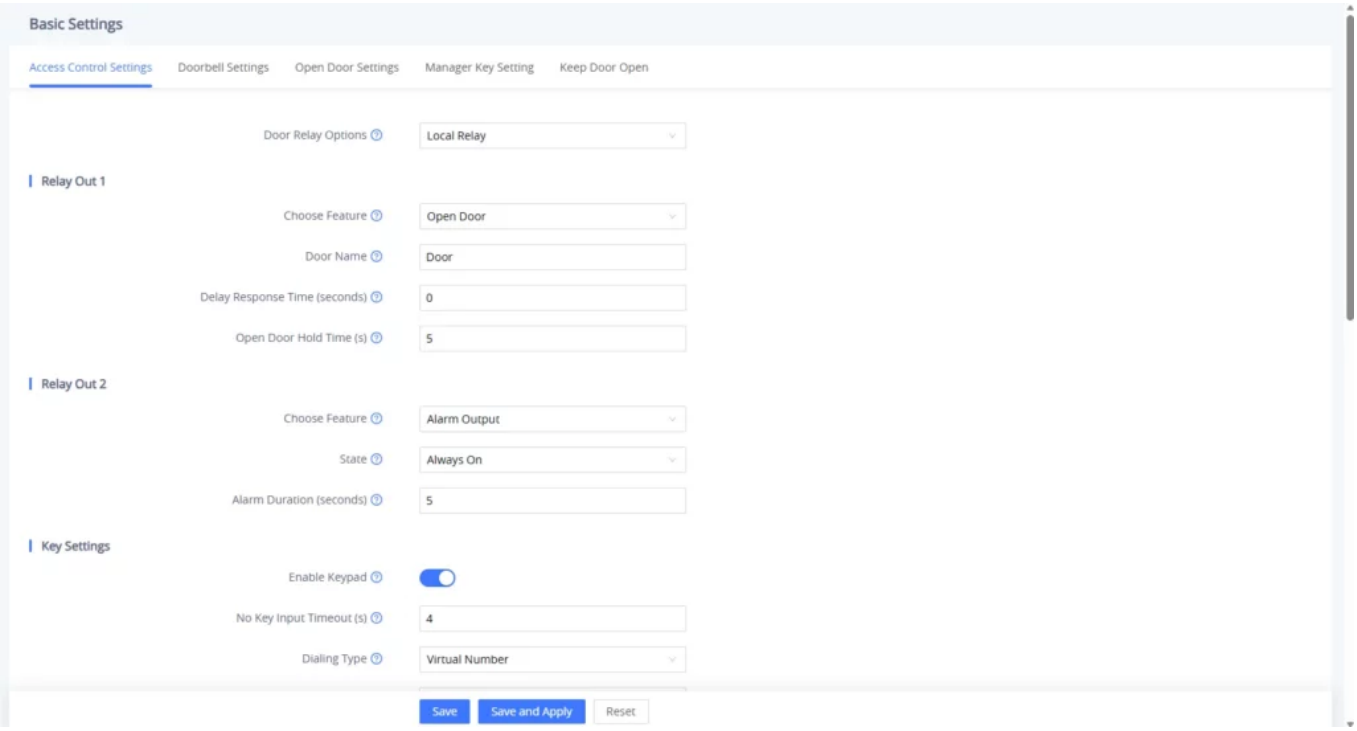
Real-time Preview Page Definitions

Stream 1	Displays the first video stream from the GDS372x real-time preview. The default set resolution is 1920*1080.
Stream 2	Displays the second video stream from the GDS372x real-time preview. The default set resolution is 1280*720.
	Redirects to the RTSP stream page to configure the prefrences for stream 1 and stream 2.
	Allows to refresh the video stream.
	Allows speed dialing by selecting both the calling account and the destination phone number or IP address.
	Adjusts the brightness for both streams.
	Adjusts the contrast for both streams.
	Adjusts the saturation for both streams.
	Opens the stream in full-screen mode.

Access Control Settings Page Definitions

Basic Settings

Access Control Settings



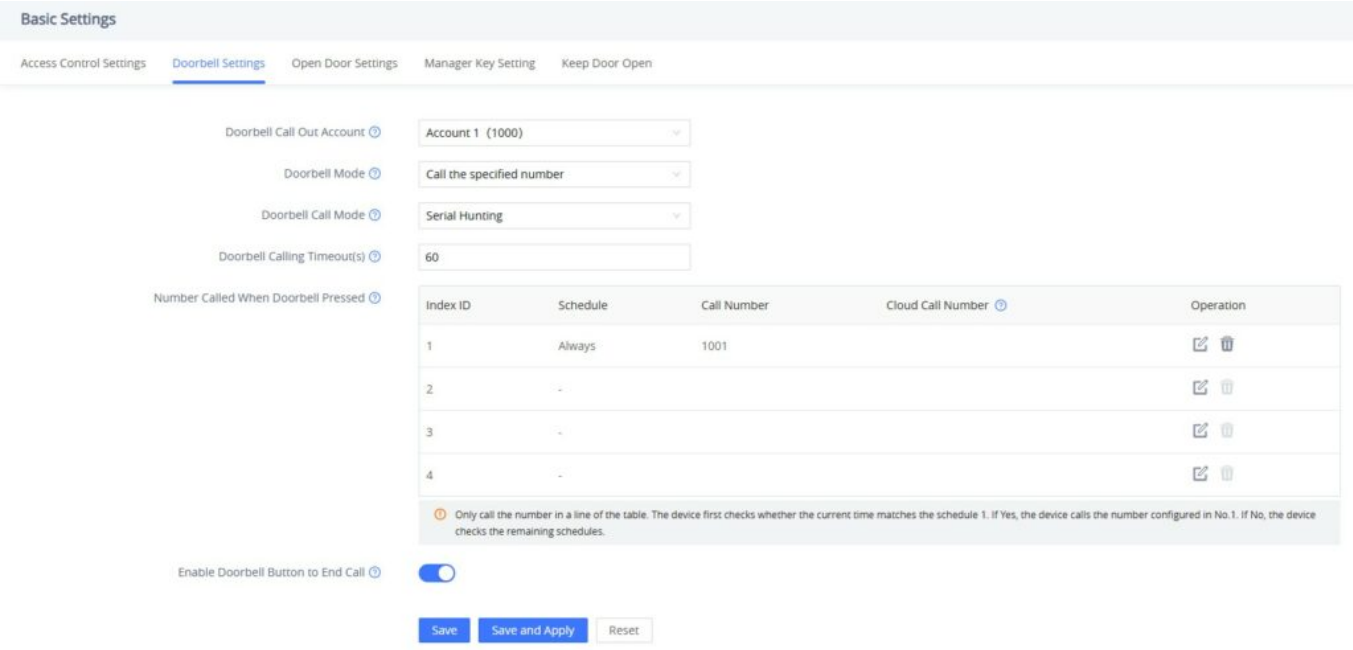
Access Control Settings Basic Settings Access Control Settings

Door Relay Options	Configure the door relay option:Local Relay: Local Relay refers to the GDS372x controlling the relay. The strike is connected to either the COM1 or COM2 port, depending on whether one or two doors need to be controlled.Web Relay: Triggers URLs for controlling the door relay. The configured web relay will get the communication from GDS372x, and will operate the strike to open door for the authenticated open door request GSC357X Relay: Allows connecting a GSC357X control station to ensure consistency with the DO digital output on the GSC357X. This requires entering the phone number and door password for proper integration and relay control. Send Wiegand Code on Remote Open Door Action: When this mode is selected, The device will send PIN1/PIN2 code via the Wiegand interface upon receiving a remote command to open door1 or door2.The default setting for the door relay option is "Local Relay".
WebRelay On URL	Enter the URL that is triggered to activate (turn on) the door relay through WebRelay.
WebRelay Off URL	Enter the URL that is triggered to deactivate (turn off) the door relay through WebRelay.
WebRelay Username	Enter the username required for authentication when accessing the WebRelay URLs for controlling the door relay.
WebRelay Password	Enter the password associated with the WebRelay Username, used for authentication to control the door relay via the WebRelay URLs.
GSC357X Relay	Configures the following GSC357x relay information:Open Door Account: The account from the GDS372x side used to control the door relay.GSC357X SIP number: The SIP number associated with the GSC357X control station GSC357X Door Password: A password set on both the GDS372x and the GSC357X control station that is required to open the door.
Open Door Hold Time (s)	The duration in which this relay remains active (i.e., how long the door stays unlocked) before automatically locking again.The valid range is 1 to 1800 seconds and default value is 5.
Relay Out 1 / Relay Out 2 (GDS3725/GDS3726 Only)	
Choose Feature	Selects the function of this relay output for the GDS372x. The Options include:Alarm Output: Configures the relay to trigger an external alarm device.Open Door: Configures the relay to control a door strike or lock for access control.The default setting is "Open Door".
Door Name	Enter the door name to be used with the Open Door feature.

Delay Response Time (seconds)	The time delay between receiving a door open command and activating this relay to unlock the door.The valid range is 0 to 20 seconds and default value is 0 which means instant.
Open Door Hold Time (s)	The duration in which this relay remains active (i.e., how long the door stays unlocked) before automatically locking again. The valid range is 1 to 1800 seconds and default value is 5.
State	Sets the default state of this alarm relay output. The options are:Always On: The relay is normally open and closes when triggered.Always Off: The relay is normally closed and opens when triggered.
?Alarm Duration (seconds)	The duration that this alarm output remains active when triggered. The valid range is 1 to 1800 seconds and default value is 5.
Key Settings (GDS3725 Only)	
Enable Keypad	Enables or disables the keypad buttons. The doorbell and management button are not affected by this setting. Enabled by default.
Enable Keypad	Configures the timeout between key presses. The valid range is 1-15 seconds, and the default setting is 4 seconds.
Dialing Type	Configures the dialing type used for keypad dialing. Available options are:Virtual NumberSIP NumberThe default setting is "Virtual Number".
Call Mode	Configures the call mode for Virtual Number dialing. Available options are:Parallel Hunting: Calls all configured numbers simultaneously.Serial Hunting: Calls the configured numbers sequentially.The default setting is "Serial Hunting".
Snapshot	
Snapshot Type	Specifies when the device captures an image. Options include:Open Door Snapshot: Takes a snapshot when the door is opened.Doorbell Pressed Snapshot: Takes a snapshot when the doorbell button is pressed.Both options are enabled by default.
Number of Snapshotd Photos	Specifies how many photos will be taken per snapshot event. The default number is 4.
Snapshot Storage Method	Determines where the snapshots are stored (FTP, SD Card).
Snapshot when Door Opened	Select the notification method of door opening snapshot. APP notification: Requires device management by the APP.Email Notification: Requires configuring email settings.Both options are enabled by default.
Snapshot Delay when Door Opened(s)	Sets a delay (in seconds) before taking a snapshot after the door has been opened. The valid range is 0 to 10 seconds and default value is 0.
Snapshot when Doorbell Pressed	Select the notification method of doorbell snapshot. APP notification: Requires device management by the APP.Email Notification: Requires configuring email settings.Both options are enabled by default.
Snapshot Delay when Doorbell Pressed(s)	Sets a delay (in seconds) before taking a snapshot after the doorbell is pressed. The valid range is 0 to 10 seconds and default value is 0.
Wiegand Settings (GDS3725/GDS3726 Only)	
Function Settings	Configures whether the device receives or sends Wiegand data. Available options are Wiegand Input and Wiegand Output.
Wiegand Output Function Mode	Defines how the GDS372x handles door relay actions when operating in Wiegand Output mode. The options are:Relay and Local Authentication: The device performs authentication locally and controls the relay directly while also outputting the Wiegand code.Relay and Bypass: The device bypasses local authentication and only sends the Wiegand code to the external controller. The external system is responsible for deciding whether to unlock the door.The default mode is Relay and Local Authentication.

Wiegand Card Reader Mode	Configures the data format used when reading or transmitting card credentials through the Wiegand interface.Wiegand-26: Uses the 26-bit Wiegand format, which is a widely supported protocol for basic access control cards.Wiegand-34: Uses the 34-bit Wiegand format, which supports larger card number ranges and is used in systems that require unique IDs.The default card reader mode is Wiegand-26.
Wiegand PIN Output Method	Configures how PIN data is transmitted through the Wiegand interface. Available options are:Disable: PIN data is not transmitted through Wiegand.4 Bit per Character: Sends each PIN character using 4-bit encoding.8 Bit per Character: Sends each PIN character using 8-bit encoding.Send All at Once: Sends the complete PIN as a single transmission.
Wiegand Control	Specifies which relay outputs (doors) are controlled by the Wiegand interface.Relay Out 1: The Wiegand interface controls Door 1.Relay Out 2: The Wiegand interface controls Door 2.
RS485	
Transmission Mode	Configures the OSDP communication role of the device. The peer device must be configured with the opposite role.
Encryption Method	Configures the encryption mode used for OSDP communication. Available options are:Mandatory Encryption: Data transmission and pairing will fail if the encryption keys do not match.Non-mandatory Encryption: If the encryption keys do not match, the system automatically switches to unencrypted transmission.No Encryption: Data is transmitted without encryption.
SCBK Value	Configures the SCBK (Secure Channel Base Key) used for OSDP secure communication. This value must match the SCBK configured on the peer device.
OSDP Address	Configures the OSDP device address. This address must match the address configured on the peer device. The valid range is 0-126.
Baud Rate	Configures the data transmission rate for OSDP communication. Both communicating devices must use the same baud rate for successful communication.
OSDP Open Door	Configures the door(s) allowed to be opened with OSDP communication.
GDS Manager	
GDS Manager Mode	If enabled, Group, Schedule, and Holiday settings are synchronized only from the Central GDS Manager server, while Card Info can be synchronized from both the Central system and the local device. If disabled, which is the default setting, all configurations are managed locally, and data from the Central system is ignored.
Home Assistant	
Home Assistant	When enabled, the device can be discovered, monitored, and managed through the Home Assistant platform via Grandstream Home integration.

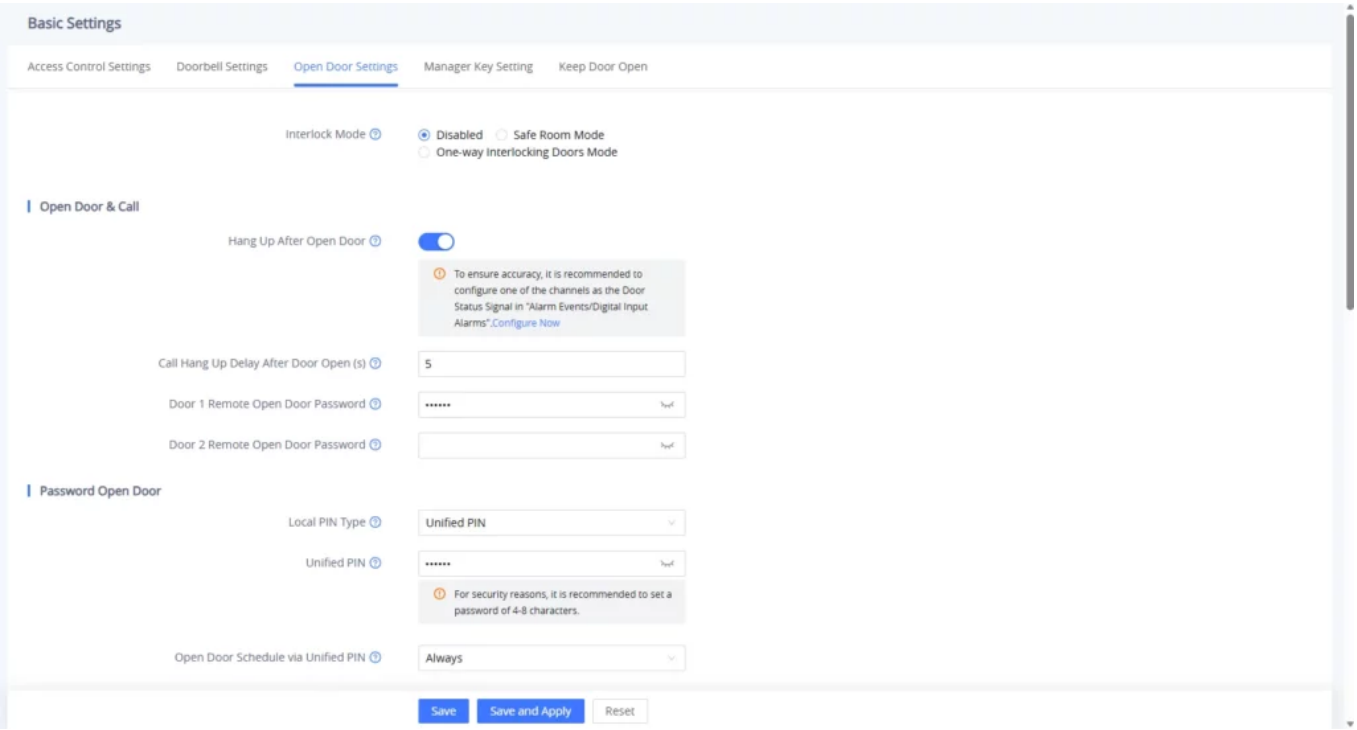
Doorbell Settings



Access Control Settings Basic Settings Doorbell Settings

Doorbell Call Out Account	Specifies the SIP account used to place the call when the doorbell is pressed. The default setting is "Auto".
Doorbell Mode	Defines the action triggered when the doorbell is pressed. Options include:Call the Specified Number: Initiates a call to the configured number, IP address, or SIP extension.Relay Out: Triggers the configured relay output.Both: Calls the specified number and triggers the relay output.The default option is "Call the Specified Number".
Doorbell Call Mode	Determines how calls are placed to multiple numbers when the doorbell is pressed. Options include:Serial Hunting: Calls the listed numbers one by one in sequence until one answers.Parallel Hunting: Calls all listed numbers simultaneously; the call is connected to the first one that answers.The default option is "Serial Hunting".
Doorbell Calling Timeout(s)	Specifies the timeout for calling a single number. If the remote party does not answer within this time, the call will automatically disconnect. The valid range is 10 to 90, and the default value is 60 seconds. Note: This setting takes precedence over the call timeout configured in the account settings.
Number Called When Doorbell Pressed	Defines the phone number, IP address, or SIP extension that the device will call when the doorbell is pressed, based on the table below:Index ID: A unique identifier for each call number configuration (up to 4 different index IDs can be set).Schedule: Specifies the schedule for when the call number is active (e.g., daily, schedule1, schedule2, etc).Call Number: The phone number, IP address, or SIP extension to be called when the doorbell is pressed (up to 15 numbers can be configured).Cloud Call Number (up to 5): Specifies cloud-based call numbers that can be used for remote access or communication (up to 5 numbers can be configured).Operation (Edit/Delete): Allows the user to modify (edit) or remove (delete) the call number entries from the configuration.
Enable Doorbell Button to End Call	When enabled, which is the default setting, pressing the doorbell button again will end the current active call.

Open Door Settings



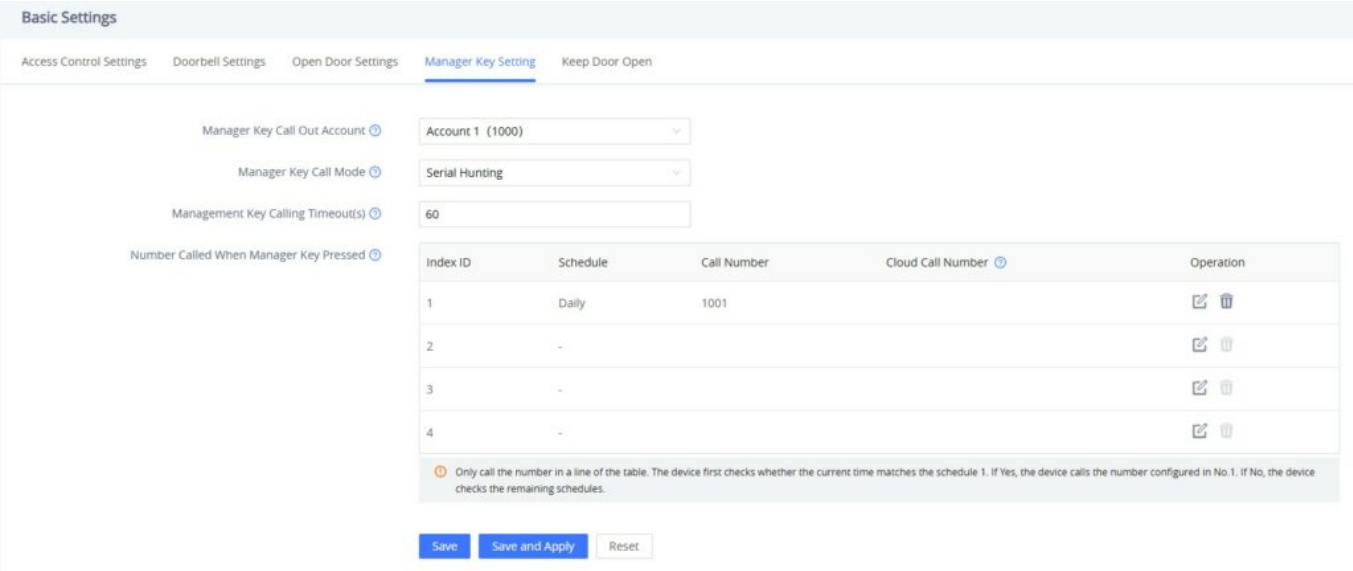
Access Control Settings Basic Settings Open Door Settings

Interlock Mode	Defines the interlock mode. Available options are:Disabled: Interlock mode is disabled.Safe Room Mode: Two devices control one door, ensuring that no one else can enter while the room is occupied.One-way Interlock Mode: One device controls two doors. After successful access authentication, the outer door opens first, and the inner door opens only after the outer door is closed.Disabled by default.
Usage Mode	Configures whether the device operates as the indoor or outdoor device in Safe Room Mode.
Relay Out	Configures the relay output interface used by the device in Safe Room Mode. Available options are Relay Out 1 and Relay Out 2.The default setting is Relay Out 1.
One-way Interlocking Doors Mode	Specifies whether the GDS372x controls two doors in a one-way interlocking mode. This option appears only when Relay Out 1 and Relay Out 2 are both set to "Open Door". For more information about configuring this feature, please refer to the GDS37xx documentation by clicking on this link.
Password Open Door (GDS3725 Only)	
Local PIN Type	Specifies the authentication method used to open the door via a PIN. Options include:PrivatePIN: Allows users to open the door using either their Private PIN or a valid card. The sequence for opening with the Private PIN is: "Enter the user's Virtual Number, then * (star), followed by the user's Private PIN".Unified PIN: Allows multiple users to share one unified PIN for opening doors. This is the default option.Card&Private PIN: Requires both a valid card and the user's Private PIN to unlock the door. The combination sequence is: "Swipe the user card, then enter * (star) followed by the user's Private PIN" Note: To open the door using a card when "PrivatePIN" or "Card&Private PIN" is selected, the RFID ID / IC Card feature must be enabled under Open Door Settings->RFID Open Door.
Unified PIN	Specifies the numeric unified PIN used to unlock the door.Note: This option is available when "Local PIN Type" is set to "Unified PIN".
Open Door Schedule via Unified PIN	Specifies the time periods during which the Unified PIN is valid. The schedule can always be set to be active, follow a daily pattern, or use custom time settings.The default setting is "Daily".Note: This option is available when "Local PIN Type" is set to "Unified PIN".

Open Door Selection via Unified PIN	Specifies which door(s) the Local PIN can unlock. Select one or both doors using the checkboxes.Note: This option is available when "Local PIN Type" is set to "Unified PIN".
Enable Guest PIN	When enabled, it allows a temporary PIN (Guest PIN) to open the door for a limited time period. Disabled by default.
Guest PIN	Specifies the numeric Guest PIN for temporary access.Note: This option is available when "Enable Guest PIN" is activated.
Guest PIN Start Time	Defines the start time when the Guest PIN becomes valid.Note: This option is available when "Enable Guest PIN" is activated.
Guest PIN End Time	Defines the end time when the Guest PIN expires.Note: This option is available when "Enable Guest PIN" is activated.
Guest PIN to Open Door Selection	Specifies which door(s) the Guest PIN can unlock. Select one or both doors using the checkboxes.
Open Door & Call	
Hang Up After Open Door	When enabled, this option automatically hangs up the call after the door is remotely opened.Disabled by default.
Call Hang Up Delay After Door Open (s)	Specifies the time in seconds before the system automatically disconnects the call after the door has been opened remotely. The valid range is 0 to 1800 and the default value is 5.
Door 1 Remote Open Door Password	Specifies the password required to remotely unlock Door 1 via SIP or HTTP API.
Door 2 Remote Open Door Password	Specifies the password required to remotely unlock Door 2 via SIP or HTTP API.
SIP Open Door	
Enable SIP Open Door	Enables the use of a PIN code, sent via SIP Message or DTMF tones, to remotely open the door. The default setting is "SIP Message" only.
HTTP API Open Door	
Enable HTTP API Remote Open Door	Configures the method for remotely opening the door via the HTTP API. Options include:Disable: Disables the HTTP API for remote door opening.Challenge+Response Authentication: Requires a challenge-response process for authentication before the door is opened.Basic Authentication: Requires a username and password for authentication before the door is opened. Disabled by default. Note: Grandstream Networks,Inc. is not responsible or liable for any security issues resulting from enabling the HTTP APl remote open door function.
HTTP API Open Door Compatibility Mode	Enables or disables HTTP API Compatibility in HTTPS. Disabled by default.
RFID Open Door	
IC Card Open Door	Enables or disables the ability to open the door using an IC (Integrated Circuit) card. Enabled by default.
Enable Compatible with Unencrypted IC Card	Allows compatibility with unencrypted IC cards. It is recommended to disable this feature for improved security, as unencrypted cards are more vulnerable to unauthorized access. Disabled by default.
Enable ID Card Open Door	Enables or disables the ability to open the door using an ID card. Enabled by default.
Minimum Interval for Swiping Card (ms)	Configures the interval time in milliseconds between consecutive card swipes for authentication. The valid range is 0 to 2000, and default value is 300.
APP Open Door	
APP Open Door Button	Enables or disables the use of the button within the mobile app to open the door. Enabled by default.
QR Code Open Door	Enables or disables the ability to open the door using a QR code generated by the app. Enabled by default.

Static QR Code Open Door	Enables or disables the ability to open the door using the static QR code generated by the app. Disabled by default.
Bluetooth BLE Open Door	If enabled, Bluetooth will be supported for opening the door. When using Bluetooth to open the door, the mobile app must be running. Enabled by default.
Sensitivity	Set the sensitivity of Bluetooth door opening. The higher the sensitivity, the greater the support for automatic door opening over longer distances.
Open Door Interval (s)	The interval between continuous Bluetooth door opening. The valid range is 5 to120. and the default value is 5 s.
NFC Open Door	Enables or disables NFC support to open the door. Enabled by default.
NFC Open Door Timeout (ms)	Specifies the time, in milliseconds, that the door remains unlocked after a successful NFC authentication. The valid range is 100 to 1000, and the default value is 500 ms.

Manager Key Setting (GDS3725 Only)

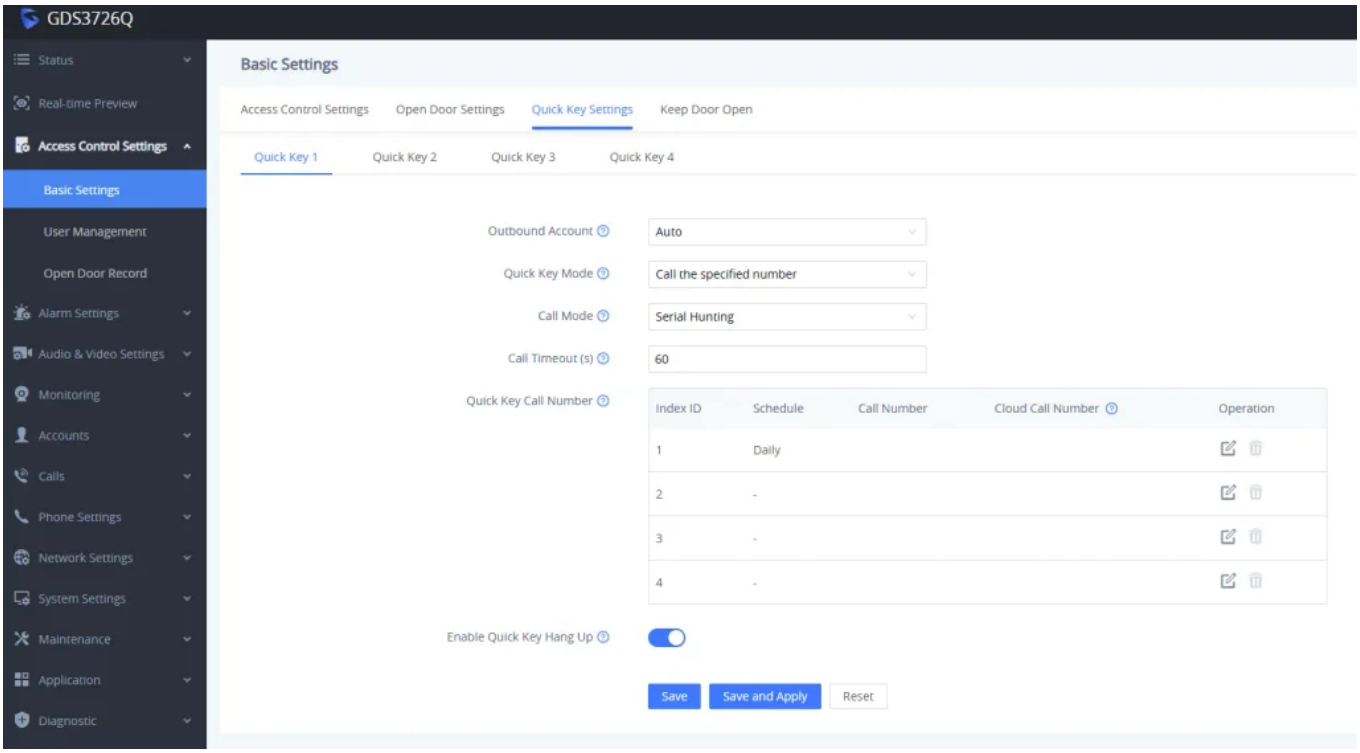


Access Control Settings Basic Settings Manager Key Setting

Basic Settings->Manager Key Setting (GDS3725 Only)	
Manager Key Call Out Account	Specifies the SIP account used to place the call when the manager key is pressed. The default setting is "Auto".
Manager Key Call Mode	Determines how calls are placed to multiple numbers when the manager key is pressed. Options include:Serial Hunting: Calls the listed numbers one by one in sequence until one answers.Parallel Hunting: Calls all listed numbers simultaneously; the call is connected to the first one that answers.The default option is "Serial Hunting".
Management Key Calling Timeout(s)	Specifies the timeout for calling a single number. If the remote party does not answer within this time, the call will automatically disconnect. The valid range is 10 to 90, and the default value is 60 seconds. Note: This setting takes precedence over the call timeout configured in the account settings.

Number Called When Manager Key Pressed	Defines the phone number, IP address, or SIP extension that the device will call when the manager key is pressed, based on the table below:Index ID: A unique identifier for each call number configuration (up to 4 different index IDs can be set).Schedule: Specifies the schedule for when the call number is active (e.g., daily, schedule1, schedule2, etc).Call Number: The phone number, IP address, or SIP extension to be called when the manager key is pressed (up to 15 numbers can be configured).Cloud Call Number (up to 5): Specifies cloud-based call numbers that can be used for remote access or communication (up to 5 numbers can be configured).Operation (Edit/Delete): Allows the user to modify (edit) or remove (delete) the call number entries from the configuration.

Quick Key Settings (GDS3726Q Only)

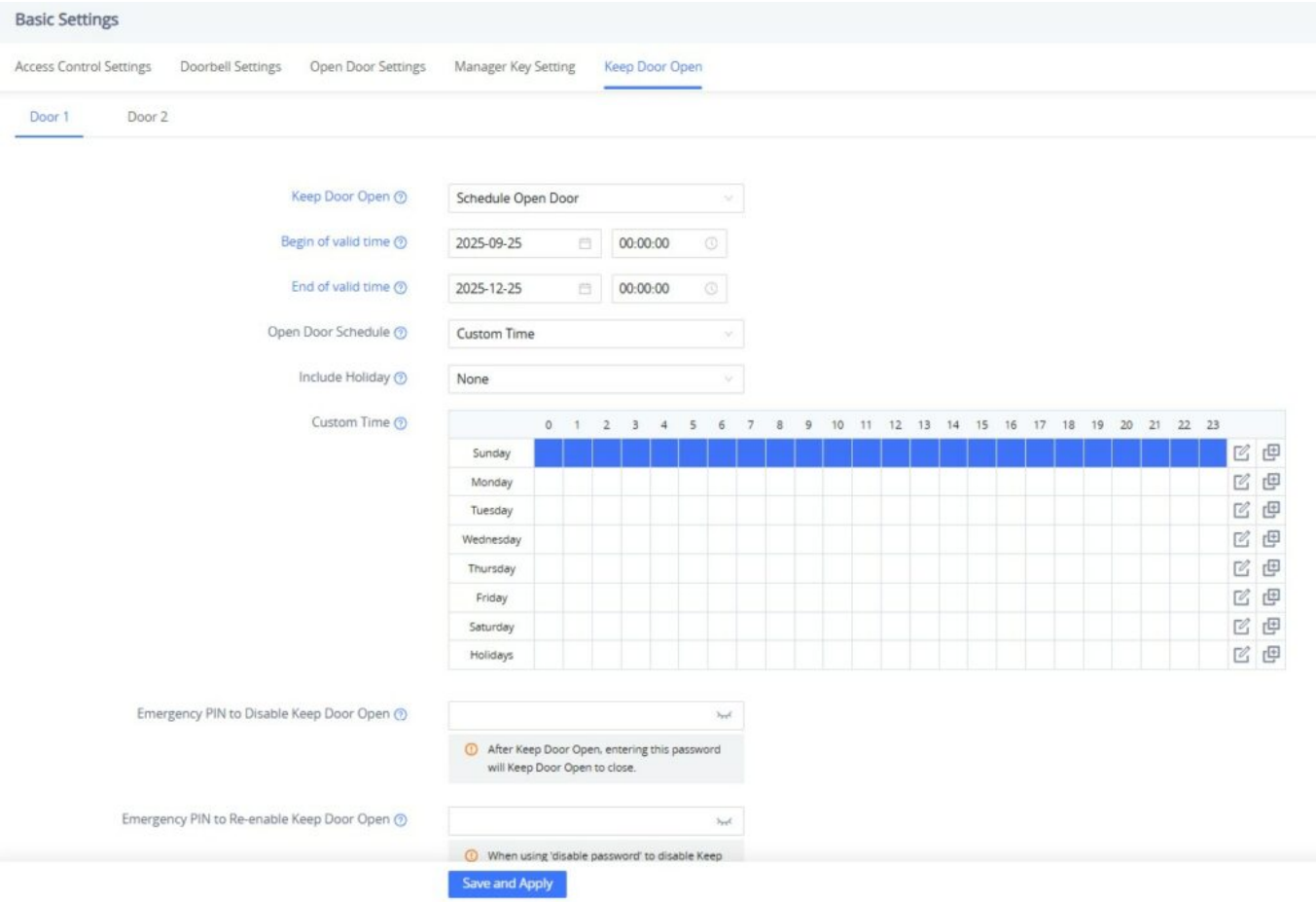


Basic Settings -> Quick Keys Settings (GDS3726Q Only)	
Outbound Account	Specifies the account used to place the call when the quick key is pressed. The default setting is "Auto".
Quick Key Mode	Defines the action triggered when the quick key is pressed. Options include: Call the Specified Number: Initiates a call to the configured number, IP address, or SIP extension. Relay Out: Triggers the configured relay output. Both: Calls the specified number and triggers the relay output. The default option is "Call the Specified Number".
Call Mode	Determines how calls are placed to multiple numbers when the quick key is pressed. Options include: Serial Hunting: Calls the listed numbers one by one in sequence until one answers. Parallel Hunting: Calls all listed numbers simultaneously; the call is connected to the first one that answers. The default option is "Serial Hunting".
Call Timeout(s)	Specifies the timeout for calling a single number. If the remote party does not answer within this time, the call will automatically disconnect. The valid range is 10 to 90, and the default value is 60 seconds. Note: This setting takes precedence over the call timeout configured in the account settings.

Quick Key Call Number	Defines the phone number, IP address, or SIP extension that the device will call when the quick key is pressed. If both a Cloud Call Number and a Call Number are configured, priority is given to the Cloud Call Number. If the Cloud Call Number fails or is unreachable, the device will use the configured Call Number. Available parameters include: Index ID: A unique identifier for each call number configuration (up to 4 different index IDs can be set). Schedule: Specifies the schedule for when the call number is active (e.g., daily, schedule1, schedule2, etc). Call Number: The phone number, IP address, or SIP extension to be called when the quick key is pressed (up to 15 numbers can be configured). Cloud Call Number (up to 5): Specifies cloud-based call numbers that can be used for remote access or communication (up to 5 numbers can be configured). Operation (Edit/Delete): Allows the user to modify (edit) or remove (delete) the call number entries from the configuration.
Enable Quick Key Hnag Up	When enabled, which is the default setting, pressing the quick key again will end the current active call.

When the GDS3726Q initiates a call via the configured Quick Keys, the remaining three keys become unresponsive.

Keep Door Open



Access Control Settings Basic Settings Keep Door Open

Door 1 / Door 2 (GDS3725/GDS3726 Only)

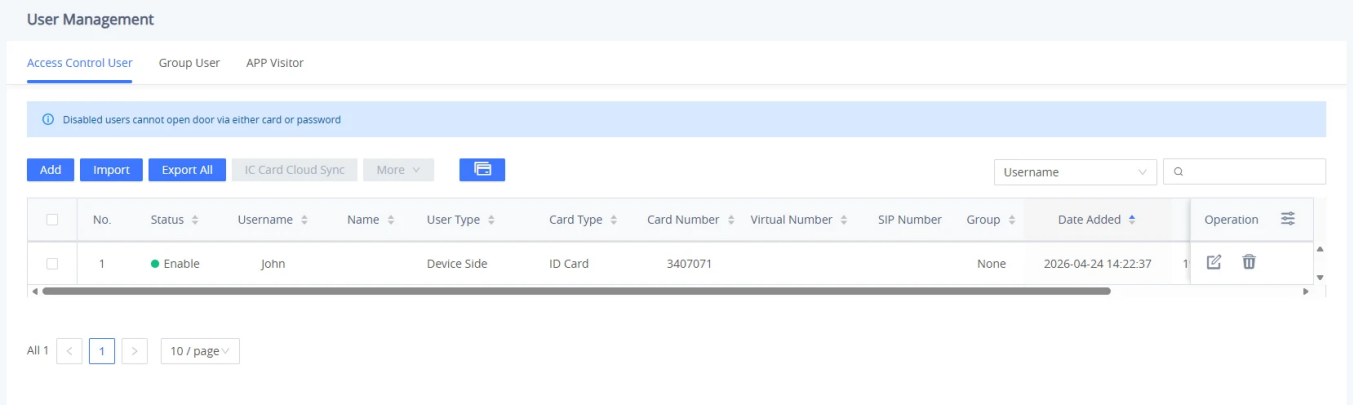
Keep Door Open	Configures the door to remain open. Options:Disable (default): Disable keeping the door open.Immediate Door Open: The door will open immediately without a schedule.Schedule Open Door: The door will open based on a pre-configured schedule.
Duration to Keep Door Open (m)	Specifies the time duration (in minutes) to keep the door open.
Keep Door Open Time	Logs the time for which the door will remain open after being triggered.
Begin of Valid Time	The start time of the scheduled period during which the door can remain open.
End of Valid Time	The end time of the scheduled period during which the door can remain open.
Open Door Schedule	Defines the schedule type for opening the door, with options like specific schedule slots (e.g., schedule1, schedule2).
Include Holiday	When enabled, the configured open door schedule also applies on the selected holiday.
Custom Time	A table that allows setting custom time rules when Open Door Schedule is set to "Custom Time", enabling the user to define specific intervals during which the door will remain open.
Emergency PIN to Disable Keep Door Open (GDS3725 Only)	Specifies the password that, when entered after the door is kept open, will immediately close the door.
Emergency PIN to Re-enable Keep Door Open (GDS3725 Only)	Specifies the password that, when entered after using the disable password, will reactivate the Keep Door Open function.

User Management

Access Control User

This page allows to manage all users who have access to the GDS372x device. Users can be added and managed either locally on this device or remotely via GDS Manager 2 or the Grandstream SecureAccess App.

Using unencrypted IC card compatibility mode presents a security risk. It is recommended to disable "Enable Compatible with Unencrypted IC Card" under **Access Control Settings->Basic Settings->Open Door Settings**, for enhanced access control security.

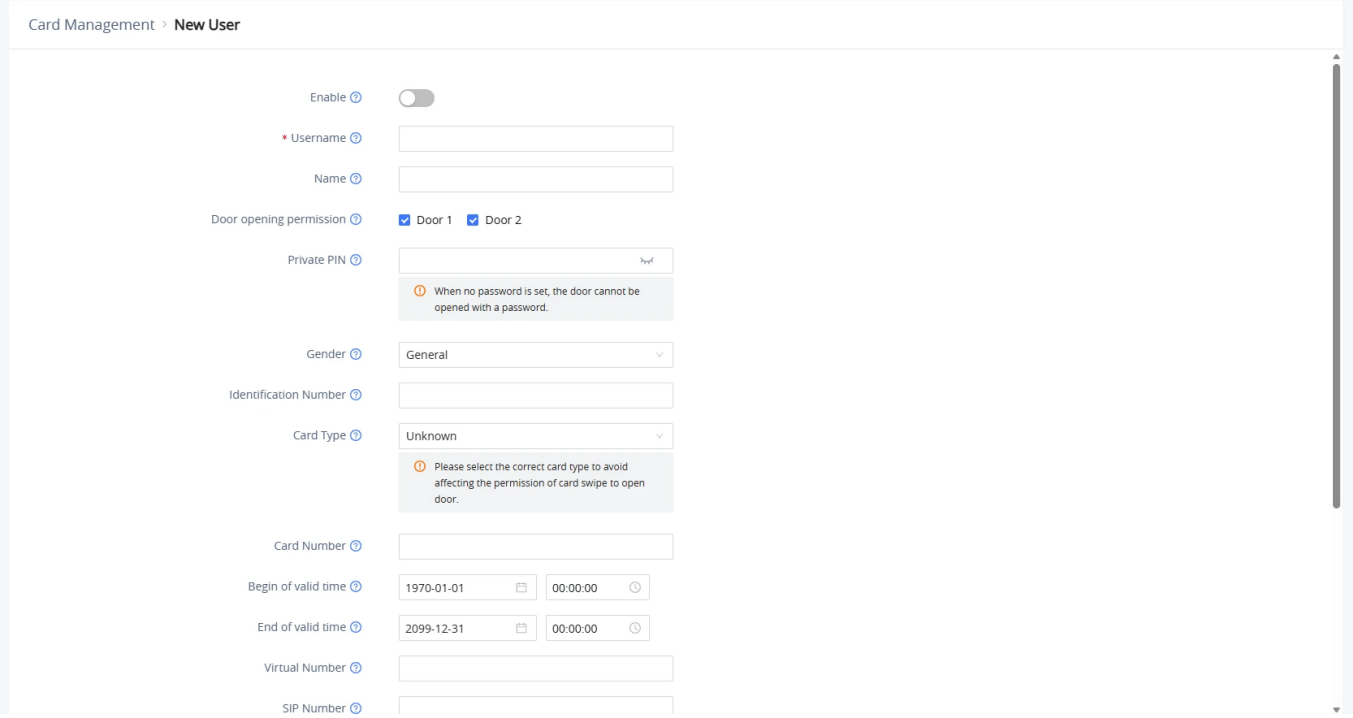


Access Control User Page

If the same card number is registered to multiple users across different systems, the following priority rule is applied:

- **Grandstream SecureAccess App:** A user registered via the Grandstream SecureAccess App will always take precedence over a user registered locally on the GDS372x.
- **Same System:** If a duplicate exists within the same system (e.g., two entries in the GDS372x local list, or two entries in the App), the user listed first (the entry with the higher sort order) will be given priority.

Add/Edit User

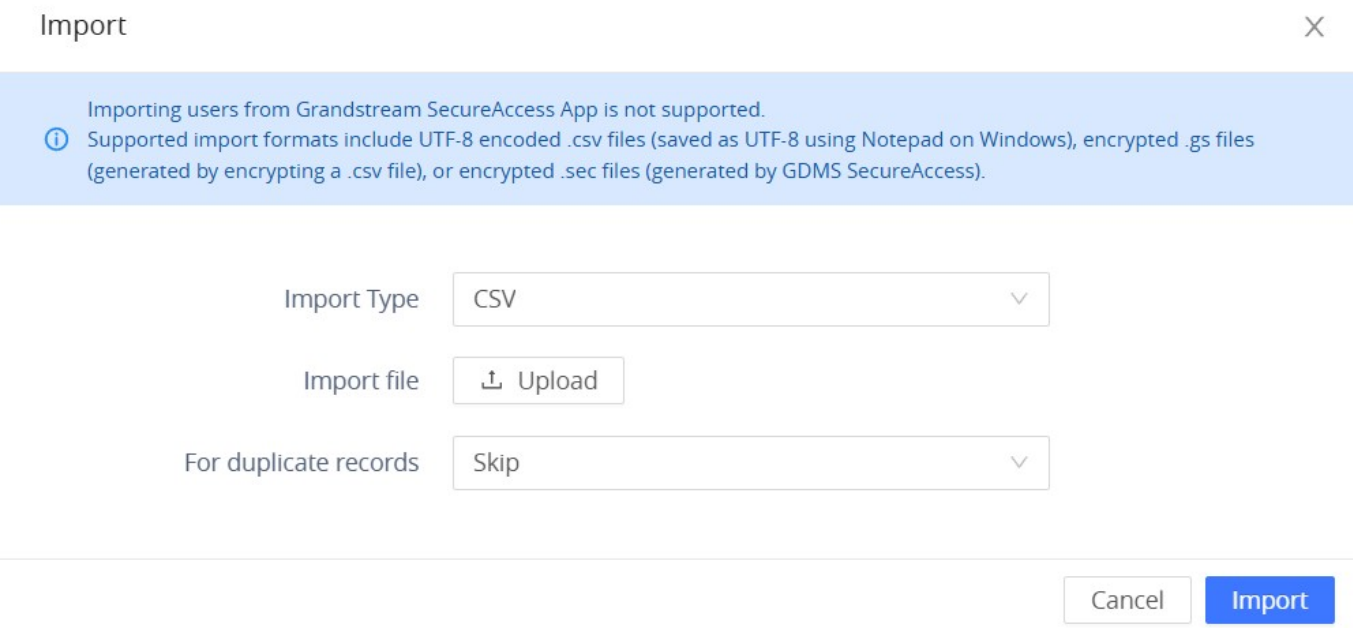


Access Control Settings User Management New User

Enable	Configure whether to enable the user.
Username	Enter the username of this user.
Name	Enter the name of the user to be displayed.
Door opening permission	Select the doors that the user can open.
Private PIN (GDS3725 Only)	Specifies the individual PIN assigned to the user for opening doors. Notes:* To open the door using a Private PIN, users need to enter their Virtual Number, followed by * (star), and then the assigned Private PIN.* If no Private PIN is set for the user, the door cannot be opened using a password.
Gender	Select the gender of the user.
Identification Number	Enter an identification number for this user.
Card Type	Choose the card type that the user will be using for door access. The options are:UnknownIC CardID Card
Card Number	Enter the IC/ID card number.
Begin of Valid Time	Specifies the start time from which the access control user's permissions become active.
End of Valid Time	Specifies the end time at which the access control user's permissions expire.
Virtual Number (GDS3725 / GDS3727 Only)	Enter the virtual number for this user.
SIP Number	Enter the SIP number for this user.
Call Out Account (GDS3725 / GDS3727 Only)	Select the GDS372x local call number.
Phone Number	Enter the phone number for this user.
Group	Choose a group to assign this user to. Each group may have different schedules.
Open Door Schedule	Specifies the time periods during which this user is allowed to open the door. Schedules can be set as daily, always, or follow predefined schedules (e.g., schedule1, schedule2, etc.).

Import

Allows the import of user data, typically from an external source or file, to add new users to the system.

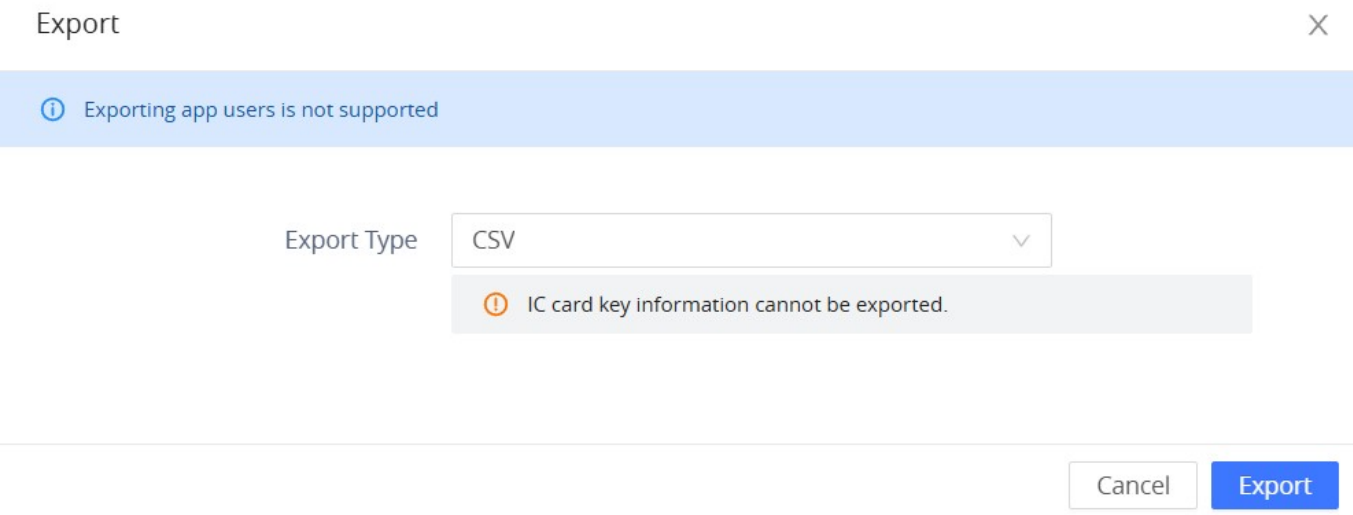


User Management Import

- Importing users from Grandstream SecureAccess App is not supported.
- Supported import formats include UTF-8 encoded .csv files (saved as UTF-8 using Notepad on Windows), encrypted .gs files (generated by encrypting a .csv file), or encrypted .sec files (generated by GDMS SecureAccess).

Export All

Exports all user data from the system to a file, allowing for backup or transfer to another system.



User Management Export All

- Exporting app users is not supported.

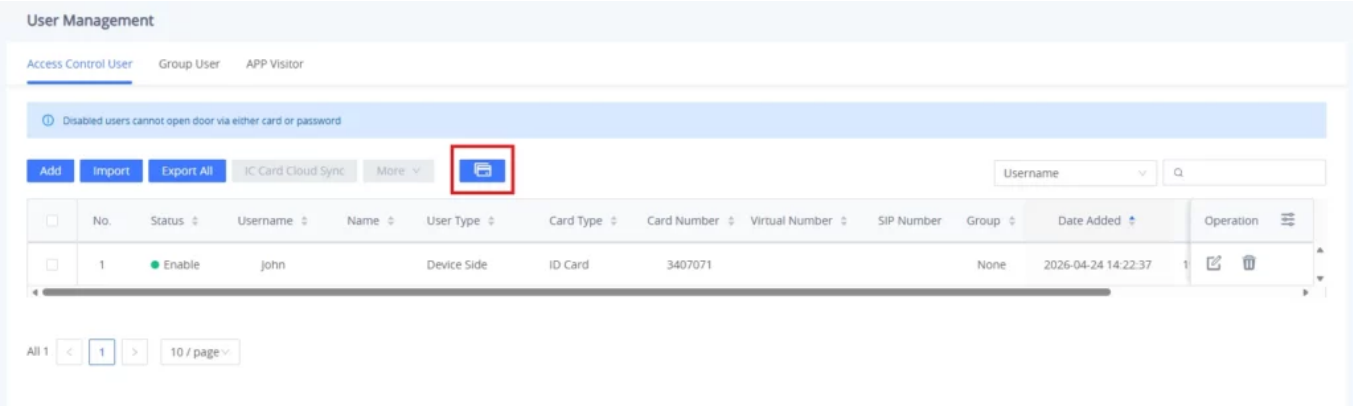
- IC card key information cannot be exported.
- Supported export types are CSV and GS. The .gs file is an encrypted .csv file. When exporting, a password must be set, and this password is only valid for the current exported file. Please keep it safe.

More

Provides additional options for managing selected users, including: Delete, Disable, Enable, Export.

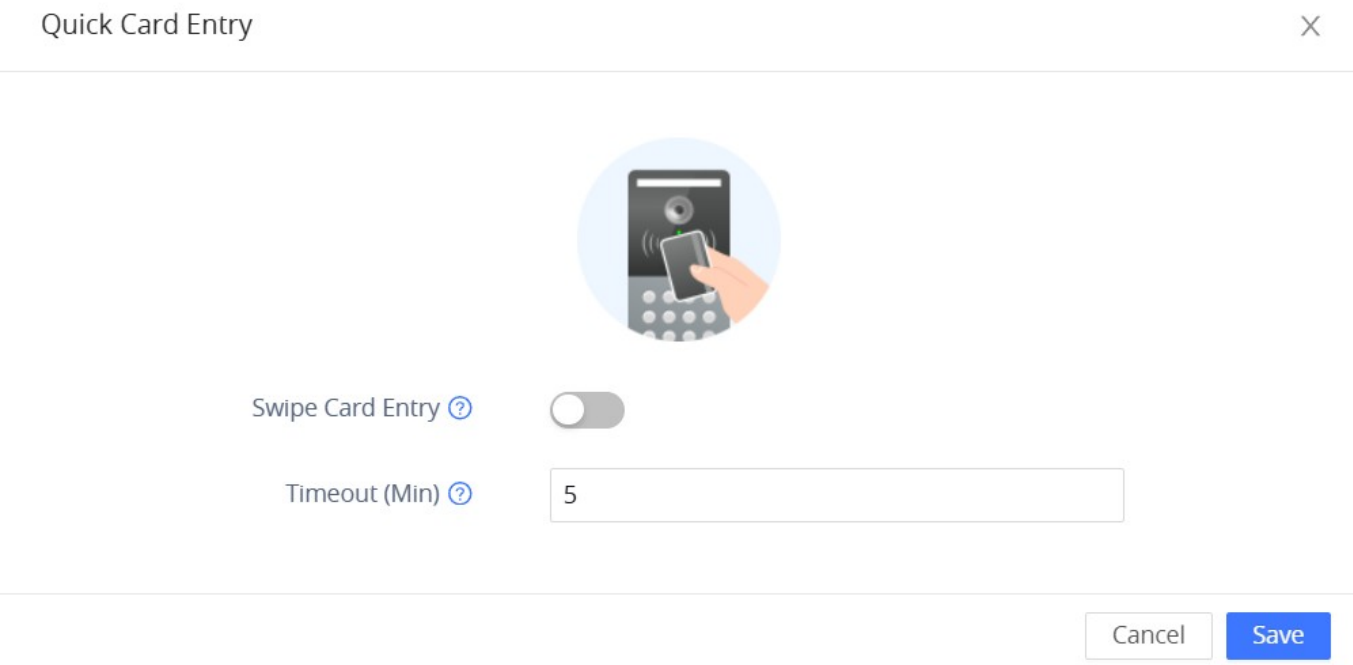
Quick Card Entry

Press to access the Quick Card Entry page. The button is located here:



Quick Card Entry Button

The following page will display.



Quick Card Entry

- **Swipe Card Entry:** If enabled, the LED light on the device will turn white and slowly flash, indicating that the device is in Quick Card Entry Mode. In this mode, when a card is swiped, the system will automatically add the swiped card number to the user list.

Note: Door opening via card swipe is disabled in this mode, meaning the card will only be registered, not used to unlock the door.

- **Timeout (Min):** Configures the duration for which Quick Card Entry Mode will remain active, with a range of

1 to 1440 minutes (1 minute to 24 hours). Once the set timer expires, Swipe Card Entry will be disabled, and the device will no longer automatically register swiped cards. The default setting is 5 min.

Group User

Add	
Group Name	Specifies the name for the new group, which will be used to identify and organize users within the system.
Schedule	Defines the schedule during which users in the group are allowed to open the door. This could be a daily, always, or specific schedule.
Operation	Edit: Allows modifying the name and schedule of the group.Delete: Deletes the group.

APP Visitor

APP Visitor	This tab is used to monitor access created via the GDS mobile app and it shows the following parameters:No: Entry number in the listVisitor ID: Unique ID assigned to the userStatus: Shows whether the access is "In Effect" or "Invalid"Name: Name assigned to the visitorCreator: The account that created the visitor recordMethod of Open Door: Method used to access (e.g., PIN code, QR Code)Door Opening Permission: Indicates which relays the visitor can activate (e.g., relay1, relay2)Times Limit of Open Door: Total allowed door openingsRemaining Time of Open Door: Remaining valid usesPeriodicity: Whether the visitor access is single-use or recurringAccess Time Period: Time-based access configurationBegin/End of Valid Time: Specific time window during which access is allowedNotes: Custom notes or comments about the user

Open Door Record

Export	Export open door record as .csv file.
No.	The record number or identifier for each door opening event in the system.
Open Door Type	Specifies the method used to open the door such as Keep Door Open, Card Open Door, SIP Open Door or 3rd Party Open Door.
Door information	Door being accessed (door1/door2).
Open DoorTrigger	Indicates the source that initiated the door opening event (e.g., when the door is opened with a card or PIN, this field displays the name of the corresponding user).
Keep Door Open Time	The date when the door remained open after being triggered.
End of Valid Time	The time when the scheduled door access or open period ends.
Operation	Displays the details of the Open Door record.

Alarm Settings Page Definitions

Alarm Event Settings

Alarm Event Settings -> Alarm Event	
Alarm Status	Click to restore all alarm statuses on this GDS372x device and clear active alarms.

Silent Alarm Event	Specifies which types of alarm events will trigger a silent alarm (multiple choices are supported):AllIntrusion/Loitering AlarmHostage Alarm (GDS3725 Only)Tamper AlarmRepeated Password Error Alarm (GDS3725 Only)Wrong Password Alarm of Remote Open DoorExceeded Access Time Limit AlarmUnauthorized Access AlarmHigh Temperature AlarmSD Card AlarmSafe Room AlarmDoor Open Timeout Alarm Digital Input
Intrusion/Loitering Alarm	
Intrusion/Loitering Alarm	Enables or disables the intrusion or loitering detection alarm.Disabled by default.
Detection Zone	Allows configuration of up to 8 zones in the camera view where intrusion or loitering is monitored.
Duration of Loitering (s)	Sets the time (in seconds) a person must stay in a zone to trigger the alarm. The valid range is 3-300 or 0, and the default vaue is 10 seconds. Note: If set to 0, an alarm is triggered as soon as as a humanoid is detected in the designated area.
Alarm Schedule	Defines when the alarm is active (e.g., daily, schedule1, schedule2, etc.).
Hostage Code Alarm (GDS3725 Only)	
Hostage Code Alarm	Enables or disables the hostage code alarm feature. When enabled, if the hostage password is entered on the device, the door will open normally and a silent alarm will be triggered (no local alarm sound). Disabled by default.
Hostage Code	Defines the specific password used as the hostage code. The PIN can be up to 8 characters long.
Tamper Alarm	
Tamper Alarm	Enables or disables the tamper alarm that detects physical tampering with the device.Disabled by default.
Repeated Password Error Alarm (GDS3725 Only)	
Repeated Password Error Alarm	Enables or disables an alarm that is triggered after 5 consecutive incorrect password attempts.Disabled by default.
Wrong Password Alarm of Remote Open Door	
Wrong Password Alarm of Remote Open Door	Enables or disables an alarm that is triggered if the remote door opening password is entered incorrectly multiple times.When enabled, the device will trigger an alarm if the password is entered incorrectly five times in a row for remote open door operations, including:SIP unlockHTTP API unlockApp unlockThis feature is disabled by default.
Lock Time (m)	Specifies the duration, in minutes, that remote door opening is disabled after multiple incorrect password attempts trigger an alarm. When the lock time expires, the incorrect password count is reset and remote door opening is re-enabled. Valid range is 1 to 1440, and the default value is 5 minutes.
Exceeded Access Time Limit Alarm	
Exceeded Access Time Limit Alarm	Enables or disables an alarm that is triggered if someone attempts to open the door outside of the allowed time.Disabled by default.
Unauthorized Access Alarm	
Unauthorized Access Alarm	Enables or disables an alarm that is triggered if the same unauthorized RFID card or QR code fails three times within one minute, an alarm will be triggered.Disabled by default.
High Temperature Alarm	
High Temperature Alarm	Enables or disables an alarm that is triggered when the device temperature exceeds the supported threshold.Disabled by default.
Alarm Interval (seconds)	Sets the minimum time interval (in seconds) between consecutive high-temperature alarm events.The valid range is 60 to 3600 and the default setting is 3600 seconds.
SD Card Alarm	

SD Card Alarm	Enables or disables an alarm that is triggered when SD card read/write operations fail.
Alarm Interval (seconds)	Sets the minimum time interval (in seconds) between SD card unavailability alerts.The valid range is 60 to 3600 and the default setting is 3600 seconds.
Safe Room Alarm	
Safe Room Alarm	Enables or disables the Safe Room Alarm. This alarm is triggered under the following conditions:When the safe room is in idle state and the door is opened via card or password authentication from the outdoor or indoor unit, but is not closed within the duration configured in Open Door Timeout Alarm. Both Safe Room Alarm and Open Door Timeout Alarm must be enabled.When the safe room is occupied and an attempt is made to open the door from the outdoor unit, the device silently generates a 'Security Room Occupied' alarm record.Note: If a user successfully authenticates but the door is not physically opened, the door will automatically lock after the timeout period, the safe room status will remain idle, and no alarm will be triggered.
Door Open Timeout Alarm	
Door Open Timeout Alarm	Enables or disables an alarm that is triggered in the two following scenarios: When the door remains open beyond the configured duration.In Safe Room Mode, when the safe room is in idle state and the door is opened via card or password from the outdoor or indoor unit, but is not closed within the configured duration.
Door Open Timeout (s)	Sets the delay, in seconds, before the Open Door Timeout alarm is triggered.
Alarm Event Settings -> Digital Input	
Digital Input 1 / Digital Input 2 / Digital Input 3 (GDS3725/GDS3726 Only)	
Digital Input	Selects the function of this digital input:Disabled: Input is inactive.Alarm Signal: Triggers an alarm when the input state changes.Open Door Signal: Triggers door opening when the input is activated.Door Status Signal: Monitors the door's open/closed state using the input.Default option is "Disabled".
Digital Input Type	Specifies the expected behavior of the digital input signal that will trigger an alarm or event.Always On: The digital input defaults to an open state. When the signal changes to closed, the preset event or alarm is triggered.Always Off: The digital input defaults to a closed state. When the signal changes to open, the preset event or alarm is triggered. Notes:When connecting a GDS digital input to a door lock using NO (Normally Open) and COM, set the digital input type to Always On.When connecting a GDS digital input to a door lock using NC (Normally Closed) and COM, set the digital input type to Always Off.
Alarm Schedule	For inputs set as Alarm Signal, this determines the time range when alarms can be triggered (e.g., daily, schedule1, etc).
Choose Door	For inputs configured as Open Door Signal, selects which door (Relay Out 1 or Relay Out 2) will be opened when the signal is triggered.
Common Configuration Options	
Alarm Action Profile	Defines the alarm action profile that triggers the alarm.
Custom Alarm Tone	Enables customization of the local audio alarm tone. This setting is disabled by default. Note: An audio alarm action profile must be assigned for this alarm event to hear this prompt.
Alarm Prompt Tone	Configures the alarm prompt tone that will play when this alarm is triggered. (Supported audio file formats: mp3, wav, ogg, wma, mid, m4a)
Play Rules	Specifies how the alarm will play when triggered by choosing one of the following methods:Maximum DurationNumber of LoopsThe default method is "Maximum Duration".
Maximum Duration (s)	Defines the maximum duration (in seconds) for this alarm event. The valid range is 1 to 3600 and the default value is 60 seconds.

Number of Loops	Sets how many times the alarm will repeat. The valid range is 1 to 10 and the default value is 1.

Alarm Action

Alarm Action -> Alarm Action Profile	
No.	The index number of the alarm action profile, with up to 10 profiles available.
Name	Custom name for identifying the profile (e.g., "Office Alarm," "Night Mode Alert").
Alarm Notification	Specifies the actions to be executed when the profile is triggered. Multiple options can be selected:All: Executes all available alarm notification methods.Notify GDS Manager: Sends a real-time notification to GDS Manager.Audio Alarm: Triggers the built-in audio alarm.SIP Alarm: Calls a designated SIP endpoint.Linked Alarm Output: Activates relay or digital output (e.g., a siren).Email Alarm: Sends an email notification.Snapshot & Upload to FTP: Captures a snapshot and uploads it to a configured FTP server.Snapshot & Save to SD: Captures a snapshot and saves it to the device's SD card.Sync Alarm Info to App: Sends alarm information to the mobile application.Cloud Video Call Alarm: When the cloud service is enabled, Account 4 (Cloud Account) is automatically used as the callout account. Sync Alarm Info to Home Assistant: Sends alarm information to the Home Assistant platform.Note: If Email Alarm is selected, configure Email Settings under System Settings -> Email Settings. If Snapshot & Upload FTP is selected, configure FTP Settings under System Settings -> FTP Settings. If Cloud Video Call Alarm is selected, configure the cloud call number under Alarm Settings -> Alarm Action -> Alarm Notification Settings -> Cloud Video Call Alarm.
Operation	The Available actions for the profiles are: Edit: Modify the configuration and actions of the profile.Simulation Alarm: Manually trigger the profile for testing or immediate response.
Alarm Action -> Alarm Notification Settings	
Call Mode	Specified the call mode for the SIP alarm:Serial Hunting: Calls targets one by one until one answers.Parallel Hunting: Calls all targets simultaneously.Default setting is "Serial Hunting".
Alarm Calling Timeout(s)	Sets the timeout period, in seconds, for alarm calls. If the remote party does not answer within this period, the call will automatically disconnect. The valid range is 10 to 90 and the default value is 60 seconds. Note: This setting takes precedence over the call timeout configured in the account settings.
Alarm Prompt Tone	Specifies the audio prompt played when a SIP alarm call is triggered. If set to silent prompt, no prompt is played and normal calls can be made immediately after connection. If a custom prompt is set, the recipient will first hear a 5-second prompt tone before normal communication begins. (Supported audio formats: MP3, WAV, OGG, WMA, MID, M4A)
SIP Alarm	
Call Number	Defines the number called when the SIP alarm is triggered, users can configure up to 4 numbers:Accounts: Select which SIP account to use for the outgoing alarm call.Call Number: Enter the SIP number or IP address to call.
Cloud Video Call Alarm	
Cloud Call Number	Enter the cloud-based number to be used for alarm calls, if applicable. When cloud service is enabled, Account 4 (Cloud Account) is fixed as the call-out account.
Audio Alarm	
Alarm Prompt Tone	Select a built-in audio file or upload a custom one to be played when the alarm is triggered. Supported formats: mp3, wav, ogg, wma, mid, m4a.

Play Rules	Define how the audio file will be played during the alarm. The options areMaximum Duration: Plays the sound based on a configured maximum duration.Number of Loops: Plays the selected alarm sound repeatedly for the specified number of timesThe default method is "Maximum Duration".
Maximum Duration (s)	Sets the maximum time (in seconds) the audio prompt will play. The valid range is 1-3600 seconds and the default setting is 60.
Number of Loops	Specifies how many times the audio will repeat. The valid range is 1-10 and the default setting is 1.

Alarm Record

Export	Export alarm record as .csv file.
Clear	Delete all alarm records from the list.
Refresh	Update the list to display the most recent alarm events.
No.	Sequential number of each alarm record.
Alarm Event	Triggered alarm type (e.g., Intrusion, Tamper Alarm).
Alarm triggered	Indicates the source that activated the alarm (e.g., if triggered by an unauthorized card or PIN, it shows the user's name).
Alarm Notification	The action(s) taken in response to the alarm (e.g., SIP Call, Audio Alarm).
Alarm Time	Timestamp when the alarm event occurred.
Operation	Specifies the action for the record, i.e., delete the selected entry.

Audio & Video Settings Page Definition

Audio Settings

Call Volume	Adjusts the speaker volume level during calls.
Doorbell Volume	Adjusts the speaker volume for the doorbell tone.
Open Door Tone Volume	Sets the volume for the confirmation tone played when the door is successfully opened.
Alarm Tone volume	Controls the loudness of general alarm notifications (e.g., intrusion, loitering).
Tamper Alarm Volume	Sets the volume level specifically for tamper alarm events.
System Volume	Adjusts the overall system sounds, including prompts and notifications.
Audio Settings	
Doorbell Tone	Configures the doorbell sound (Supports uploading audio files in MP3, WAV, OGG, WMA, MID, and M4A formats).
Internal Open Door Tone	Configures the tone played when the internal open door action is triggered (Supports uploading audio files in MP3, WAV, OGG, WMA, MID, and M4A formats).
External Open Door Tone	Configures the tone played when the external open door action is triggered (Supports uploading audio files in MP3, WAV, OGG, WMA, MID, and M4A formats).
Door Opening Failure Prompt Tone	The sound or prompt played when a door opening attempt fails, such as invalid card or access denied (Supports uploading audio files in MP3, WAV, OGG, WMA, MID, and M4A formats).
Key Tone	Specifies the sound feedback when pressing keypad buttons:Default: Standard system tone.DTMF: Dual-tone multi-frequency tones (like phone keypress sounds).Mute: Disables key press sounds.Default setting is "Default".

IP Announcement	
Announcement Time after Startup (s)	Configure the time when IP announcement can be triggered after booting up. Beyond this time, IP announcement cannot be triggered. Valid Range is 60-300 seconds. Default setting is 60.
Number of Loops	Configure the number of loop broadcasts for IP announcements. Valid Range is 1-3 times. Default setting is 1.

OSD Settings

Display time	Enables or disables the display of date and time on the video stream. Enabled by default.
OSD Date Format	Specifies the format in which the date is displayed:YYYY-MM-DDMM/DD/YYYYDD MM YYYYDefault setting is "MM/DD/YYYY".
OSD Time Format	Sets the format for displaying time:24H: 24-hour format (e.g., 14:00)12H: 12-hour format with AM/PMDefault setting is "24H".
OSD Date/Time Position	Selects the on-screen location where the date and time appear:Top LeftBottom LeftTop RightBottom RightDefault setting is "Top Left".
Display Text	Enables or disables the display of custom text on the video. Enabled by default.
OSD Text	Allows input of a custom label to display on the video stream. Maximum allowed byte length: 25.
OSD Text Position	Selects where the custom OSD text appears on the screen:Top LeftBottom LeftTop RightBottom RightDefault setting is "Top Right".

CMOS Settings

Wide Dynamic Range (WDR)	Enhances image visibility in scenes with both bright and dark areas by balancing exposure.WDR (Wide Dynamic Range): Enables wide dynamic range for better image clarity in challenging lighting.Normal: Disables WDR, using standard exposure settings.
WDR Schedule	Configures the Wide Dynamic Range (WDR) schedule. It can be set to Always, Daily, or a custom time period. To customize the schedule, navigate to System Settings -> Schedule.
Power Frequency	Sets the power line frequency to reduce flicker in the video caused by artificial lighting.60Hz.50Hz.Default setting is "60HZ".

Privacy Masks

Zone Edit 0/4	Configure up to 4 privacy mask zones to block specific areas in the video for privacy (e.g., windows, neighboring properties).Zone ID: Identifier for each mask zone (e.g., Zone 1, Zone 2).Enable: Check to activate the privacy mask for the selected zone.Operation: Remove the selected privacy mask zone.

Monitoring Page Definitions

Onvif

Onvif	Enable or disable ONVIF protocol support for integration with third-party video management systems. Disabled by default.
Onvif Username	Username used for ONVIF authentication when a third-party system connects to the device.
Onvif Password	Password used for ONVIF authentication. Note: It is recommended that the ONVIF account credentials match the RTSP stream credentials to avoid preview or connection issues in third-party software.

RTSP

RTSP->RTSP Server	
RTSP	Enable or disable the RTSP (Real-Time Streaming Protocol) server for video stream access. Disabled by default.
RTSP Port	Specifies the port used for RTSP streaming (default is 554).
RTSP Authentication	Select the method of user authentication for accessing the RTSP stream:Basic: Sends credentials in plain text (less secure).Digest: Sends hashed credentials (more secure and recommended).Default setting is "Digest".
RTSP Username	Username required to access the RTSP video stream.
RTSP Password	Password required to access the RTSP video stream. Note: For best compatibility with third-party software, use the same credentials as the ONVIF account.
RTSP->Stream	
Stream (1/2)	
Preferred Video Codec	Specifies the compression format used for streaming:H.264: Widely supported, good balance of quality and bandwidth.MJPEG: Uses more bandwidth, but offers high image quality per frame.Default setting is H.264.
Profile	Selects the H.264 profile for encoding:Baseline: Basic compatibility, low complexity.Main Profile: Better compression and quality, standard for most uses.High Profile: Best video quality and efficiency, requires more processing power.
Resolution	Specifies the output video resolution:1920x1080 (Full HD)1280x720 (HD)640x360 (Low resolution)480x272 (QVGA)Default resolution for Stream 1: 1920*1080.Default resolution for Stream 2: 1280*720.
Bit Rate(kbps)	Sets the target video bitrate in kilobits per second, affecting video quality and bandwidth usage. Options: 256, 512, 1024, 2048, 4096 kbps. Default setting for Stream 1: 2048.Default setting for Stream 2: 1024.
Frame Rate(fps)	Number of frames per second. A higher frame rate provides smoother video. Options: 5, 10, 15, 20, 25, 30 fps. Default setting is 30.
Bit Rate Control	Enables dynamic bitrate adjustment based on scene complexity and motion, optimizing bandwidth usage.
I-frame Interval	Specifies how many frames are sent between two consecutive I-frames (key frames). A lower interval improves seek performance and stream stability but increases bandwidth. Valid range is 5-150. Default setting is 30.

Accounts Page Definitions

Accounts

Account x->General Settings	
Account Register	
Account Active	Indicates whether the account is active.The default setting is "Yes".
Account Name	The name associated with each account.
SIP Server	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (e.g., sip.mycompany.com, or IP address)
Secondary SIP Server	The URL or IP address, and port of the SIP server. This will be used when the primary SIP server fails
Outbound Proxy	Defines IP address or Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller.

Secondary Outbound Proxy	Defines secondary outbound proxy that will be used when the primary proxy cannot be connected.
SIP User ID	User account information, provided by your VoIP service provider.
SIP Authentication ID	SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	The account password required for the GDS372x to authenticate with the SIP server before the account can be registered.After it is saved, this will appear as hidden for security purpose.
Display Name	The SIP server subscriber's name (optional) that will be used for Caller ID display (e.g., John Doe).
TEL URI	If the GDS372x has an assigned PSTN telephone number, this field should be set to "user=phone". A "user=phone" parameter will be attached to the Request-URI and "To" header in the SIP request to indicate the E.164 number. If set to "Enable", "tel:" will be used instead of "sip:" in the SIP request.
Network Settings	
DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. If "Use Configured IP" is selected, please fill in Primary IP, Backup IP 1 and Backup IP 2.A RecordSRVNAPTR/SRVUse Configured IP
Max Number Of Sip Request Retries	Sets the maximum number of retries for the device to send requests to the server. In DNS SRV configuration, if the destination address does not respond, all request messages are resent to the same address according to the configured retry times. Valid range: 1-10.
DNS SRV Failover Mode	Configures the preferred IP mode for DNS SRV. If set to "default", the first IP from the query result will be applied. If set to "Saved one until DNS TTL", previous IP will be applied before DNS timeout is reached. If set to "Saved one until no response", previous IP will be applied even after DNS timeout until it cannot respond.DefaultIf the option is set with "default", it will again try to send register messages to one IP at a time, and the process repeats.Saved one until DNS TTLIf the option is set with "Saved one until DNS TTL", it will send register messages to the previously registered IP first. If no response, it will try to send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up.Saved one until no responsesIf the option is set with "Saved one until no responses", it will send registered messages to the previously registered IP first, but this behavior will persist until the registered server does not respond.Failback follows failback expiration timer If "Failback follows failback expiration timer" is selected, the device will send all SIP messages to the current failover SIP server or Outbound Proxy until the failback timer expires.
Failback Expiration (m)	Specifies the duration (in minutes) since failover to the current SIP server or Outbound Proxy before making failback attempts to the primary SIP server or Outbound Proxy.
Register Before DNS SRV Failover	Configures whether to send REGISTER requests to the failover SIP server or Outbound Proxy before sending INVITE requests in the event of a DNS SRV failover.
Primary IP	Configures the primary IP address where the GDS372x sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 1	Configures the backup IP 1 address where the GDS372x sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 2	Configures the backup IP 2 address where the GDS372x sends DNS query to when "Use Configured IP" is selected for DNS mode.
Proxy-Require	A SIP Extension to notify the SIP server that the GDS372x is behind a NAT/Firewall.

NAT Traversal	Configures whether NAT traversal mechanism is activated. Please refer to user manual for more details.If set to "STUN" and STUN server is configured, the GDS372x will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the GDS372x will try to use public IP addresses and port number in all the SIP&SDP messages.The GDS372x will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be "Keep-alive". Configure this to be "No" if an outbound proxy is used. "STUN" cannot be used if the detected NAT is symmetric NAT. Set this to "VPN" if OpenVPN is used.
Media NAT Traversal	For configuring media NAT traversal strategies: If configured as "No," media NAT traversal will not be used. If configured as "Auto," it will follow the business logic of the "NAT traversal(STUN)" configuration. If configured as "STUN," it will obtain the public IP and port information after NAT through a shared STUN server. If configured as "TURN," it will forward the data stream through a TURN relay server. If configured as "ICE," it will collect local IP addresses, STUN-reflected addresses, and TURN relay addresses to dynamically select the optimal connection path.
Account x->SIP Settings	
Basic Settings	
SIP Registration	Selects whether the GDS372x will send SIP Register messages to the proxy/server. The default setting is "Enabled".
UNREGISTER on Reboot	If set to "No", the GDS372x will not unregister the SIP user's registration information before new registration.If set to "All", the SIP Contact header will use "*" to clear all SIP user's registration information. If set to "Instance", the GDS372x only needs to clear the current SIP user's info.
REGISTER Expiration	Specifies the frequency (in minutes) in which the GDS372x refreshes its registration with the specified registrar.The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
SUBSCRIBE Expiration	Specifies the frequency (in minutes) in which the GDS372x refreshes its subscription with the specified registrar.The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
Re-Register before Expiration	Specifies the time frequency (in seconds) that the GDS372x sends re-registration request before the Register Expiration. The default value is 0.
Registration Retry Wait Time	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
Add Auth Header on Initial REGISTER	If enabled, the GDS372x will add Authorization header in initial REGISTER request.Default is "Disabled".
Enable OPTIONS Keep-Alive	Configures whether to enable SIP OPTIONS to track account registration status. If enabled, the GDS372x will send periodic OPTIONS messages to server to track the connection status with the server.Default is "Disabled".
OPTIONS Keep-Alive Interval	Configures the time interval the GDS372x sends OPTIONS message to the server. If set to 30 seconds, it means the GDS372x will send an OPTIONS message to the server every 30 seconds.
OPTIONS Keep-Alive Max Tries	Configures the maximum number of times the GDS372x will try to send OPTIONS message consistently to server without receiving a response. If set to "3", the GDS372x will send OPTIONS message 3 times. If no response from the server, the GDS372x will re-register.
SUBSCRIBE for Registration	When set to "Yes", a SUBSCRIBE for Registration will be sent out periodically.The default setting is "No".
Use Privacy Header	Configures whether the "Privacy Header" is present in the SIP INVITE message.Default: the GDS372x will add "Privacy Header" when special feature is not "Huawei IMS".Yes: the GDS372x will always add "Privacy Header".No: the GDS372x will not add "Privacy Header".The default setting is "default".

Use P-Preferred- Identity Header	Configures whether the "P-Preferred-Identity Header" is present in the SIP INVITE message.Default: the GDS372x will add "P-Preferred-Identity header" when special feature is not "Huawei IMS".Yes: the GDS372xwill always add "P-Preferred-Identity header".No: the GDS372x will not add "P-Preferred-Identity header".
Add MAC in User-Agent	If Yes except REGISTER, all outgoing SIP messages will include the GDS372x's MAC address in the User-Agent header, except for REGISTER and UNREGISTER.If Yes to All SIP, all outgoing SIP messages will include the GDS372x's MAC address in the User-Agent header.If No, the GDS372x's MAC address will not be included in the User-Agent header in any outgoing SIP messages.The default setting is "No".
SIP Transport	Selects the network protocol used for the SIP transport.The default setting is "UDP".
Enable TCP Keep-alive	Configures whether to enable TCP Keep-alive for the TCP connection between the terminal and the SIP server.
Local SIP Port	Configures the local SIP port used to listen and transmit.
SIP URI Scheme when using TLS	Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport. The default setting is "sips".
Use Actual Ephemeral Port in Contact with TCP/TLS	Configures whether the actual ephemeral port in contact with TCP/TLS will be used when TLS/TCP is selected for SIP Transport.The default setting is "No".
Support SIP Instance ID	Configures whether SIP Instance ID is supported or not.The default setting is "Yes".
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
SIP Timer D Interval	Sets the wait time for response retransmissions when the INVITE receives a 3xx ~ 6xx response. Valid range is 32-64 seconds. Default is 32.
Outbound Proxy Mode	Configures whether to put the Outbound Proxy in the Route header, or if SIP messages should always be sent to Outbound Proxy.In routeNot in routeAlways send toDefault is "in route".
Enable 100rel	When enabled, the 100rel tag is appended to the value of the Supported header of the initial signaling messages.The default setting is "No".
Session Timer	
Enable Session Timer	Configures whether to enable session timer function. It enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. If set to "Yes", the GDS372x will use the related parameters when sending session timer according to "Session Expiration". If set to "No", session timer will be disabled.The default setting is "No".
Session Expiration	Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand.The default setting is 180. The valid range is from 90 to 64800.
Min-SE	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
Caller Request Timer	If set to "Yes" and the remote party supports session timers, the GDS372x will use a session timer when it makes outbound calls.The default setting is "No".

Callee Request Timer	If set to "Yes" and the remote party supports session timers, the GDS372x will use a session timer when it receives inbound calls.The default setting is "No".
Force Timer	If set to "Yes", the GDS372x will use the Session Timer even if the remote party does not support this feature. Otherwise, Session Timer is enabled only when the remote party supports it.The default setting is "No".
UAC Specify Refresher	As a caller, select UAC to use the GDS372x as the refresher, or select UAS to use the callee or proxy server as the refresher. When set to "Omit", the refresh object is not specified.The default setting is "UAC".
UAS Specify Refresher	As a callee, select UAC to use caller or proxy server as the refresher, or select UAS to use the GDS372x as the refresher.The default setting is "UAC".
Force INVITE	Select "Yes" to force using the INVITE method to refresh the session timer.The default setting is "No".
Account x->Codec Settings	
Audio	
Preferred Vocoder(Choice 1 - 5)	Multiple vocoder types are supported on the GDS372x, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message. The vocoders supported are: PCMUPCMAG.722 (wide band)G.729A/BG.726-32
Codec Negotiation Priority	Configures the GDS372x to use which codec sequence to negotiate as the callee. When set to "Caller", the GDS372x negotiates by SDP codec sequence from received SIP Invite. When set to "Callee", the GDS372x negotiates by audio codec sequence on the GDS372x. The default setting is "Callee".
Use First Matching Vocoder in 200OK SDP	When set to "Yes", the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is "No".
G.726-32 Packing Mode	Selects "ITU" or "IETF" for G.726-32 packing mode.The default setting is "ITU".
G.726-32 Dynamic Payload Type	Specifies G.726-32 payload type. Valid range is 96 to 126. Default is 126.
Send DTMF	Specifies the mechanism to transmit DTMF digits. There are 3 supported modes:In audio: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs).RFC2833 sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.SIP INFO uses SIP INFO to carry DTMF.Default setting is "RFC2833".
DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Enable Audio RED with FEC	If set to "Yes", FEC will be enabled for audio call.
Audio FEC Payload Type	Configures audio FEC payload type. The valid range is from 96 to 126.The default value is 121.
Audio RED Payload Type	Configures audio RED payload type. The valid range is from 96 to 126.The default value is 124.
Silence Suppression	Configures G.729 silence suppression, also known as dynamic voice detection (VAD). When set to "Yes", the device detects periods of no voice activity during a call and sends a minimal number of VAD packets instead of continuous voice packets. Default setting is "No".

Voice Frames Per TX	Configures the number of voice frames transmitted per packet. It is recommended that the IS limit value of Ethernet packet is 1500 bytes or 120 kbps. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used in the codec table or negotiate the payload type during the actual call. For example, if set to 2 and the first code is G.729, G.711 or G.726, the "ptime" value in the SDP datagram of the INVITE request is 20 ms. If the "Voice Frame/TX" setting exceeds the maximum allowed value, GDS372x will use and save the maximum allowed value for the selected first codec. It is recommended to use the default setting provided, and incorrect setting may affect voice quality.The default setting is 2.
Preferred Video Codec	
Preferred Video Codec	Specifies the prefered video codec used for GDS372x. The supported codec for this device is H.264.
Enable Video FEC	When enabled, the video sender will temporarily allocate part of the bandwidth to one data channel to send FEC data to system, thus, to improve the video quality the receiver gets. Enabling this function will take up part of bandwidth and reduce call rate. The default setting is "Yes".
FEC Payload Type	Configures FEC payload type. The range is 96-126. Default setting is 120.
Packetization Mode	Configures video packetization mode. If set to "Single NAL Unit Mode", the packetization mode will be negotiated as single NAL unit mode when dial video calls, if the other party does not support the negotiation, then single NAL unit mode will be used for video encoding by default. If set to "Non-Interleaved Mode", the packetization mode will be negotiated as Non-interleaved mode when dial video calls, If the other party does not support negotiation, then the Non-interleaved mode will be used for video encoding by default. The default setting is "Non-Interleaved Mode".
Image Size	Sets the image size. It can be selected from the dropdown list.1080P720P4CIFVGAThe default setting is 1080P.
Use H.264 Constrained Profiles	Configures that whether to set H.264 constrained profiles.The default setting is "Yes".
H.264 Profile Type	Selects the H.264 profile type from the dropdown list.Baseline ProfileMain ProfileHigh ProfileBP/MP/HP (Default Setting)Note: Lower levels are easier to decode, but higher levels offer better compression. Usually, for the best compression quality, choose "High Profile"; for playback on low-CPU machines or mobile devices, choose "Baseline Profile". If "BP/MP/HP" is selected, all three profiles "Baseline Profile" "Main Profile" and "High Profile" will be used for negotiation during video decoding to achieve the best result. This is usually used in video conference when there is higher requirement on the video.
Video Bit Rate	Configures the bit rate for video call. It can be selected from the dropdown list. The default setting is 2048 kbps. Note: The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. For some network environment, the default setting "1080P" might be too high that causes no video or video quality issue during video call. In this case, please change "H.264 Image Size" to "VGA" or "CIF" and change "Video Bit Rate" to "384kbps" or lower.
SDP Bandwidth Attribute	Specifies the SDP (Session Description Protocol) bandwidth attribute used for video streaming.Standard: Uses AS format at the session level and TIAS format at the media level.Media Stream Level: Uses AS format at the media level only.Session Level: Uses AS format at the session level only.None: No changes are made to the session format.The default Setting is "Media Stream Level". Note: Please do not modify this setting without knowing the session format supported by the server. Otherwise, it might cause video decoding failure.
H.264 Payload Type	Enter H.264 codec payload type. The valid range is from 96 to 126. Default is 99.

Packet Retransmission	If set to "NACK", the signaling will carry NACK info. After negotiation, the media will use NACK to retransmit lost packets. If set to "NACK+RTX (SSRC-GROUP) ", the signaling will carry both NACK and RTX info. After negotiation, the media will use NACK+RTX (SSRC-GROUP), which is the default setting, to achieve packet loss retransmission. If set to "Disabled", packet loss retransmission cannot be used.
RTP Settings	
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu.NoEnabled but Not ForcedEnabled and ForcedOptionalThe default setting is "No".
SRTP Key Length	Allows users to specify the length of the SRTP calls. Available options are:AES 128&256 bitAES 128 bitAES 256 bitDefault setting is AES 128&256 bit
Crypto Life Time	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, GDS372x does not add the crypto lifetime to SRTP header. The default setting is "No".
RTCP Destination	Configures the server address. When there is a call, the RTCP package sent from the GDS372x will also be sent to this address. Note: The address should contain port number.
RTCP Keep-Alive Method	Configures the RTCP channel keep-alive packet type.Receiver Report: The RTCP channel will sends "receiver report+source description+RTCP extension" as keep-alive data.Sender Report: The RTCP channel will sends "Sender report+source description+ RTCP extension" as keep-alive data.Default setting is "Receiver Port".
RTP Keep-Alive Method	Configures the RTP channel keep-alive packet type.No: No data will be sentRTP Version 1: The wrong version infor "1" will be carried when sending RTP data packets.Default setting is "RTP Version 1".
Symmetric RTP	Configures whether Symmetric RTP is used or not. Symmetric RTP means that the UA uses the same socket/port for sending and receiving the RTP stream. The default setting is "No".
RTP IP Filter	Configures whether to filter the received RTP. If set to "Disable", the device will receive RTP from any address; If set to "IP Only", the device will receive RTP from certain IP address in SDP with no port limited; If set to "IP and Port", the device will only receive RTP from IP address & port in SDP. Disabled by Default
RTP Timeout (s)	Configures the RTP timeout of the GDS372x. If the GDS372x does not receive the RTP packet within the specified RTP time, the call will be automatically disconnected. The default range is 0 and 6-600. If set to 0, the GDS372x will not hang up the call automatically.
Account x->Call Settings	
General	
Add Video Capability	Configures the video sending and receiving capability for the account to ensure SIP proxy compatibility.The default setting is "sendonly".sendonly: Send video only.sendrecv: Send and receive video.
Auto Answer	Specifies whether the GDS372x automatically answers incoming calls. Options:Yes: The device automatically answers incoming calls after a short reminder beep (Default setting).No: The device does not automatically answer incoming calls.Intercom/Paging Only: The device automatically answers only intercom or paging calls.
Custom Alert-Info for Auto Answer	Specifies the Alert-Info content used to trigger automatic answering for paging/intercom calls (Maximum allowed length is 20 characters). Notes:Only when the Alert-Info header of an incoming call matches the configured content will the device automatically answer the call.If left blank, paging calls will ring according to the Incoming Call Rules instead of being auto-answered.
Play warning tone for Auto Answer Intercom	If enabled, GDS372x will play warning tone when auto answering Intercom.
Send Anonymous	If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous. Default is "No".

Anonymous Call Rejection	If set to "Yes", anonymous calls will be rejected.The default setting is "No".
Call Log	Configures Call Log setting on the GDS372x.Log All CallsLog incoming/outgoing only (missed calls will NOT be logged)Disable Call LogThe default setting is "Log All Calls".
Mute on Intercom Answer	If enabled, the GDS372x will mute the mirophone after answer an intercom call via Call-Info/Alert-Info.
Ring Timeout	Configures the timeout (in seconds) for the GDS372x to ring when an incoming call is not answered. Valid range is 30 to 3600. The default setting is 60.
Call Timeout	Set the SIP call timeout(in seconds). When the SIP call exceeds the set time, the call will be automatically hung up. When set to 0, the call will not be automatically hung up. Valid range is 0 to 65535. Default setting is 0.
Calling Timeout (s)	Specifies the maximum duration, in seconds, the system will wait for the call to be answered. If the call is not answered within this period, it will automatically disconnect. The valid range is 10 to 300 seconds, and the default is 90 seconds.
Ringtone	
Account RingTone	Allows users to configure the ringtone for the account. Users can choose from different ringtones from the dropdown menu.Note: User can also choose silent ring tone or doorbell.
Ignore Alert-Info header	Configures to play default ringtone by ignoring Alert-Info header.The default setting is "No".
Account x->Advanced Settings	
Security Settings	
Check Domain Certificates	Configures whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. The default setting is "No".
Validate Certificate Chain	Validate certification chain when TCP/TLS is configured.The default setting is "No".
Validate Incoming SIP Messages	Specifies if the GDS372x will check the incoming SIP messages Caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
Allow Unsolicited REFER	Configures whether to dial the number carried by Refer-to header after receiving out-of-dialog SIP REFER request actively.If set to "Disabled", the GDS372x will send error warning and stop dialing.If set to "Enabled/Force Auth", the GDS372x will dial the number after sending authentication. If the authentication fails, it will stop dialing.If set to "Enabled", the GDS372x will dial all numbers carried by SIP REFER.
Accept Incoming SIP from Proxy Only	When set to "Yes", the SIP address of the Request URL in the incoming SIP message will be checked. If it does not match the SIP server address of the account, the call will be rejected. The default setting is "No".
Check SIP User ID for Incoming INVITE	If set to "Yes", SIP User ID will be checked in the Request URI of the incoming INVITE. If it does not match the GDS372x's SIP User ID, the call will be rejected. The default setting is "No".
Allow SIP Reset	Allow SIP Notification message to perform factory reset.The default setting is "No".
Authenticate Incoming INVITE	If set to "Yes", the GDS372x will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response.The default setting is "No".
SIP Realm Used For Challenge INVITE & NOTIFY	Configures this option to verify incoming INVITE, only take effect when enabled incoming INVITE first. It is used to verify provision NOTIFY information, including check-sync, resync and reboot, but only effective when enabled SIP authentication.
MOH	

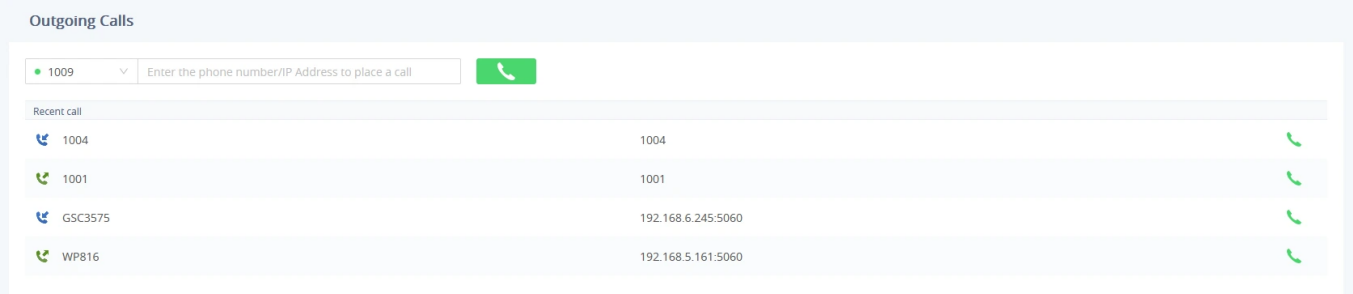
MOH Mode	Configures MOH mode:If set to "Local MOH", a local MOH audio file needs to be uploaded for this mode to work. If set to "Disable" the MOH will be disabled.Default setting is "Disable".
Upload Local MOH Audio File	Click to upload audio file from PC. The MOH audio file should be ".ogg" format.
Advanced Features	
Special Feature	Different soft switch vendors have special requirements. Therefore, users may need select special features to meet these requirements. Users can choose from the drop down list:Standard ModeNortel MCSBroadsoftCBCOMRNKSylantroHuawei IMSPhonePowerUCM Call centerZoom
Reboot on check-sync event without "reboot="	When enabled, the device reboots upon receiving a SIP NOTIFY check-sync event without the 'reboot=' header. When disabled, the device performs provisioning only without rebooting.

Calls Page Definitions

Outgoing Calls

This page allows users to place outgoing calls from the GDS372x device using the Web UI.

- **Account Selection:**
  Choose the SIP account to use when making a call from the available configured accounts. Please note that only active accounts with a populated User ID field will appear in the account selection list, In case of a direct IP Calling method, you can populate the User ID field with any information to highlight that the selected account is using direct IP calling.
- **Dial Number/IP:**
  Enter the **phone number** or **IP address** of the destination you want to call.
- **Call Button:**
  Initiates the call using the selected account and the entered number/IP.
- **Recent Calls List:**
  Displays a history of recently dialed numbers for quick redial. You can click on an entry to automatically populate the dial field.



GDS372x Outgoing Calls Page

Call History

Call History->Call History	
Delete	Removes selected call records from the list.
Delete All	Clears all call history records.
Add to Allowlist	Adds selected numbers to the allowlist to permit future calls.
Call Status	Indicates the direction of the call: Outgoing, Incoming.
Name	Displays the contact name if available.
Number	The phone number or IP address involved in the call.

Time	Timestamp of when the call occurred.
Operation	Available actions for each record:Dial: Dial the number.Details: View full call information.Add to Allowlist: Permit future calls from this number/IP.Add Users of the Access Control: Create an access control user entry with this number.Delete: Remove the individual call record.
Call History->Intercept record	
Delete	Removes selected intercepted call records from the list.
Add to Allowlist	Adds selected numbers to the allowlist, allowing future calls from them.
Name	Displays the caller's name if available.
Number	The intercepted phone number or IP address.
Time	Timestamp of when the call was intercepted.
Operation	Available actions for each record:Dial: Call the intercepted number.Details: View more information about the intercepted call.

Call Settings

Video Call	Enables the video call feature on the GDS372x. The default setting is "Yes".
Video Frame Rate	The video frame rate is adjustable based on network condition. Increasing the frame rate will significantly increase the amount of data transmitted, therefore consuming more bandwidth. The video quality will deteriorate due to packet loss if extra bandwidth is not allocated.
Call Waiting	Enables the call waiting feature. If it is not checked, the GDS system will reject the second incoming call during an active session without user's knowledge. But this missed call record will be saved to remind users. The default setting is "Yes".
Call Waiting Tone	Specifies whether the GDS372x plays a call waiting tone when another incoming call is received while a current call is in progress. The default setting is "Yes".
DND	Enable/disable the DND (Do not disturb) feature. If enabled, this device will block all incoming calls. Disabled by default.
DND Prompt Sound	Enable/disabed the sound or tone played when a call is received while the device is in Do Not Disturb (DND) mode. Enabled by default.
Multicast Tone	Enables/disables multicast tone.If enabled, there will be a prompt tone at the beginning and end of the multicast. Disabled by default.
Automatic Answer Ringing Time (s)	Configures a ringing timer after which the GDS372x will answer an incoming call automatically. Valid range is 0 to 10 seconds and the default setting is 0.
Filter Characters	Specifies characters to be automatically removed when dialing numbers. These characters are not part of the actual phone number and will be filtered out during dialing (Multiple characters can be set for filtering). For example: if set to "[()-]", when dialing (0571)-8800-8888, the character "()-" will be automatically filtered and dial 057188008888 directly. Notes:Filtering applies to calls initiated from call history or Click2Dial.Dialing directly from the keypad will not filter any characters.
Return Code When Enable DND	When DND is enabled, the GDS372x will send the selected type of SIP message.
Call Settings -> Allowlist Management	
Allowlist	Enable or disable allowlist functionality. If enabled, only the allowlist numbers are be able to call in, other numbers will be blocked. (Disabled by default)
Add	Manually add a new entry to the allowlist (name and number/IP).
Delete	Remove selected entries from the allowlist.
Delete All	Clear all entries from the allowlist.

Name	The label or identifier for the allowed contact.
Number	The phone number or IP address to allow.
Operation	Available actions for each entry:Edit: Modify the name or number/IP.Delete: Remove the specific allowlist entry.

Phone Settings Page Definitions

General Settings

Local RTP Port	This parameter defines the local RTP port used to listen and transmit. It is the base RTP port for channel 0. When configured, channel 0 will use this port _value for RTP; channel 1 will use port_value+2 for RTP. Local RTP port ranges from 1024 to 65400 and must be even. Default value is 5004.
Local RTP Port Range	Gives users the ability to define the parameter of the local RTP port used to listen and transmit. This parameter defines the local RTP port from 24 to 10000. This range will be adjusted if local RTP port + local RTP port range is greater than 65486. Default setting is 200.
Use Random Port	When set to "Yes", this parameter will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is "No" Note: This parameter must be set to "No" for Direct IP Calling to work.
Keep-alive Interval	Specifies how often the GDS372x sends a blank UDP packet to the SIP server to keep the "ping hole" on the NAT router to open. The default setting is 20 seconds. The valid range is from 10 to 160.
STUN/TURN Server	The IP address or Domain name of the STUN server. STUN resolution results are displayed in the STATUS page of the Web GUI.Only non-symmetric NAT routers work with STUN.
TURN Server Username	The username to validate the STUN server.
TURN Server Password	The password to validate the STUN server.
Use NAT IP	The NAT IP address used in SIP/SDP messages. This field is blank at the default settings. It should ONLY be used if it is required by your ITSP.
Delay Registration(s)	Conifgures the delay time for account registeration after device booted up.

Ringtone

Auto Config CPT by Region	Configures whether to choose Call Progress Tone automatically by region. If set to "Yes", the phone will configure CPT (Call Progress Tone) according to different regions automatically. If set to "No", you can manually configure CPT parameters.The default setting is "No".
Call Progress Tones: Ring Back Tone Busy Tone Reorder Tone Call-Waiting Tone	Configures tone frequencies according to user preference. By default, the tones are set to North American frequencies. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds.Syntax: f1=val,f2=val [,c=on1/off1[-on2/off2[-on3/off3]]]. (Frequencies are in Hz and cadence on and off are in 10ms)ON is the period of ringing ("On time" in "ms") while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeats the pattern.Please refer to the document below to determine your local call progress tones: https://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf
Call-Waiting Tone Gain	Adjusts the call waiting tone volume. Users can select "Low", "Medium" or "High". The default setting is "Low".
Default Ring Cadence	Defines the ring cadence for the phone. The default setting is: c=2000/4000.

Multicast Paging

Multicast Paging->Multicast Paging	
Paging Barge	During an active call, if an incoming multicast paging has higher priority (Disable being the highest and 1 being the second), then the device will be hung up and multicast paging will be played. The default setting is "Disabled".
Paging Priority Active	If enabled, during a multicast page if another multicast is received with higher priority (1 being the highest) that one will be played instead. Enabled by default.
Multicast Paging->Multicast Listening	
Priority	Indicates the priority level for the multicast listening. A lower number (1) indicates higher priority, while a higher number (10) indicates lower priority.
Listening Address	Specifies the multicast IP address that the device listens to for paging or announcements. This address allows the device to receive audio from a multicast stream.
Label	A user-defined label or name to identify the multicast listening configuration. This can be helpful for organizing multiple multicast streams.

Network Settings Page Definitions

Ethernet Settings

Internet Protocol	Selects whether to prefer IPv4 or IPv6. Default is IPv4 Only.
IPv4	
IPv4 Address Type	Users could select "DHCP", "Static IP" or "PPPoE".DHCP: Obtain IP address via a DHCP server in the LAN. All domain values for static IP/PPPoE are unavailable, even though the values have been saved in the flash.PPPoE: Configures PPPoE account/password. Obtain the IP address from the PPPoE server via dialing.Static IP: Manually configures IP Address, Subnet Mask, Default Router's IP Address, DNS Server 1, and DNS Server 2.By default, it is set to "DHCP".
DHCP VLAN Override	Selects the DHCP Option VLAN mode. When set to "DHCP Option 132 and DHCP option 133", the GDS372x will get DHCP option 132 and 133 as VLAN ID and VLAN priority. When set to "Encapsulated in DHCP Option 43", the GDS372x will get values from Option 43 which encapsulate VLAN ID and VLAN priority. Note: Please make sure the "Allow DHCP Option 43 and Option 66 to Override Server" setting under maintenance->upgrade is checked. The default setting is "Disable".
Hostname (Option 12)	Sets the name of the client in the DHCP request. It is optional but may be required by some Internet Service Providers. The field is empty by default.
Vendor Class ID(Option 60)	Configures the vendor class ID header in the DHCP request.The default setting is "Grandstream GDS3725/GDS3726/GDS3727".
IP Address	Defines the GDS372x's static IP address if the static IP is used.
Subnet Mask	Determines the network's subnet mask if the static IP is used.
Default Gateway	Defines the network's gateway address if the static IP is used.
DNS Server 1	Configures the primary DNS IP address if the static IP is used.
DNS Server 2	Configures the secondary DNS IP address if the static IP is used.
Preferred DNS Server	Enter the Preferred DNS server.
PPPoE Account ID	Configures the PPPoE account ID if the PPPoE is used.
PPPoE Password	Sets the PPPoE password if the PPPoE is used.

Layer 2 QoS 802.1Q/VLAN Tag	Assigns the VLAN Tag of the Layer 2 QoS packets for Ethernet. The Default value is 0.
Layer 2 QoS 802.1p Priority Value	Assigns the priority value of the Layer 2 QoS packets for Ethernet. The Default value is 0.
IPv6	
IPv6 Address	Configures the appropriate network settings on the GDS372x. Users could select from "Auto-configured" or "Statically configured".
Static IPv6 Address	Enter the static IPv6 address in "Statically configured" IPv6 address type.
IPv6 Prefix Length	Enter the IPv6 prefix length in "Statically configured" IPv6 address type. This field is empty by default.
IPv6 Prefix (64 bits)	Enter the IPv6 Prefix (64 bits) when Prefix Static is used in "Statically configured" IPv6 address type. This field is empty by default.
IPv6 Gateway	The gateway when static IPv6 is used.
DNS Server 1	Enter DNS Server 1 when static IP is used.
DNS Server 2	Enter DNS Server 2 when static IP is used.
Preferred DNS Server	Enter the Preferred DNS server.
802.1X	
802.1x Mode	Enables and selects the 802.1x mode for the GDS372x system. The supported 802.1x modes are:EAP-MD5EAP-TLSEAP-PEAPv0/MSCHAPv2 The default setting is "Disable".
802.1x Identity	Enters the identity information for the selected 802.1x mode. (This setting will be displayed only if 802.1 X mode is enabled).
MD5 Password	Enters the MD5 password for this 802.1x mode
802.1X CA Certificate	Uploads the CA Certificate file to the GDS372x. This certificate is used only when the 802.1X authentication mode is set to TLS or PEAP. It is not required for MD5 mode.
802.1X Client Certificate	Loads the Client Certificate file to the GDS372x. (This setting will be displayed only if the 802.1 X TLS mode is enabled)

Wi-Fi Settings

Wi-Fi Function	Enables / Disables the Wi-Fi on the GDS372x. Enabled by default.
Wi-Fi Band	Set the type of Wi-Fi Band whether its 2.4G or 5G or 5G & 2.4G (default).
Country Code	Configures Wi-Fi country code.
ESSID	This parameter sets the ESSID for the Wireless network. Press "Scan" to scan for the available wireless network. Click on "Connect" and enter the authentication credentials of the Wi-Fi network to connect to. Users can connect to hidden networks by pressing on "Add Network" and configure: ESSID: Configure the hidden ESSID name. Security Mode: Defines the security mode used for the wireless network when the SSID is hidden. Default is "WPA". Password: Determines the password for the selected Wi-Fi network. Advanced: Configures IPv4 and IPv6 modes.

OpenVPN(R) Settings

OpenVPN(R) Enable	Enables/Disables OpenVPN(R) feature. Default is "No".
Manual Import	
Import OpenVPN(R) Configuration	Imports the configuration file from the current computer. After importing, the local configuration will be overwritten and OpenVPN(R) function is automatically enabled.

Local Configuration	
OpenVPN(R) Server Address	Specify the IP address or FQDN for the OpenVPN(R) Server.
OpenVPN(R) Port	Specify the listening port of the OpenVPN(R) server. The valid range is 1 - 65535. The default value is "1194".
OpenVPN(R) Transport	Specifies whether OpenVPN(R) connections use TCP or UDP as the transport protocol. The default value is "UDP".
OpenVPN(R) CA	Click on "Upload" to upload the Certification Authority of OpenVPN(R). For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN(R) Certificate	Click on "Upload" to upload OpenVPN(R) certificate. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN(R) Client Key	Click on "Upload" to upload OpenVPN(R) Key. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN(R) Client Key Password	Allows user to set password for client.key file
OpenVPN(R) TLS Key	Uploads the OpenVPN(R) TLS .key file
OpenVPN(R) TLS Key Type	Selects the encryption type of the OpenVPN(R) TLS key. it can be set to : TLS-Auth, TLS-Crypt, TLS-Crypt V2
OpenVPN(R) Cipher Method	Specifies the Cipher method used by the OpenVPN(R) server. The available options are:BlowfishAES-128AES-256Triple-DESThe default setting is "Blowfish".
OpenVPN(R) Username	Configures the optional username for authentication if the OpenVPN server supports it.
OpenVPN(R) Password	Configures the optional password for authentication if the OpenVPN server supports it.
OpenVPN(R) Comp-lzo	Configures enable/disable the LZO compression. When the LZO Compression is enabled on the OpenVPN server, you must turn on it at the same time. Otherwise, the network will be abnormal. Default value is YES.
Additional Options	Additional options to be appended to the OpenVPN(R) config file, separated by semicolons. For example, comp-lzo no;auth SHA256Note: Please use this option with caution. Make sure that the options are recognizable by OpenVPN(R) and do not unnecessarily override the other configurations above.

Advanced Settings

Advanced Network Settings	
DNS Refresh Timer (m)	Configures the refresh time (in minutes) for DNS query. If set to "0", the GDS372x will use the DNS query TTL from DNS server response. the Default value is "0"
DNS Failure Cache Duration (m)	Configures the duration (in minutes) of the previous DNS cache when the DNS query fails. If set to "0", the feature will be disabled. Note: Only valid for SIP registration. The Default value is "0"
Enable LLDP	Enables/Disables the LLDP (Link Layer Discovery Protocol) service. Enabled by default.
LLDP TX Interval	Configures LLDP TX Interval (in seconds). Valid range is 1 to 3600. Default is 60.
Enable CDP	Enables/Disables the Cisco Discovery Protocol feature. Enabled by default.
Layer 3 QoS for SIP	Configures the Layer 3 QoS parameter for SIP. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0 to 63, and default value is 26.

Layer 3 QoS for Audio	Configures the Layer 3 QoS parameter for audio. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0 to 63, and default value is 46.
Layer 3 QoS For Video	Configures the Layer 3 QoS parameter for video packets. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0 to 63, and default value is 34.
HTTP/HTTPS User-Agent	Configures the user-agent for HTTP/HTTPS request.
SIP User-Agent	This sets the user-agent for SIP. If the value includes word "$version", will replace it with the real system version.
Proxy	
HTTP Proxy	Specifies the HTTP proxy URL for the GDS372x to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
HTTPS Proxy	Specifies the HTTPS proxy URL for the GDS372x to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
Bypass Proxy for	Configures the destination IP address where no proxy server is needed. The GDS372x will not use a proxy server when sending packets to the specified destination IP address.
Remote Control	
Action URI Support	Configures whether to enable GDS372x to handle Action URI request.Default is "Enabled".
Action URI Allowed IP List	List of allowed IP addresses from which the GDS372x receives the Action URI. Maximum allowed length is 512, and default setting is "any".

System Settings Page Definitions

Time Settings

NTP Server	Configures the URL or IP address of the NTP server. The GDS372x may obtain the date and time from the server. The default server is "pool.ntp.org".
Enable Authenticated NTP	Configures whether to enable NTP authentication. If enabled, a cryptographic signature appended to each network packet. If the key is incorrectly configured, the GDS372x will refuse to use the time provided by the NTP server. This setting is disabled by default.
Authenticated NTP Key ID	Configures the key ID for authenticated NTP. The default value is "1".
Authenticated NTP Key	Upload the key file for authenticated NTP. Note: Only supports MD5 key type.
Allow DHCP Option 42 to Override NTP Server	Obtains NTP server address from a DHCP server using DHCP Option 42; it will override configured NTP Server. If set to "No", the GDS372x will use configured NTP server to synchronize time and date even if an NTP server is provided by DHCP server. The default setting is "Yes".
DHCP Option 2 to Override Time Zone Setting	Obtains time zone setting (offset) from a DHCP server using DHCP Option 2; it will override the selected time zone. If set to "No", the GDS372x will use the selected time zone even if provided by the DHCP server. The default setting is Yes.
Time Zone	Configures the date/time display according to the specified time zone. The default setting is "Auto".

Self-defined Time Zone	When the Time Zone option is set to "Self-Defined", this parameter allows users to specify their own custom time zone using the following syntax: std offset dst [offset], start [/time], end [/time]std: Abbreviation for standard time (e.g., MTZ).offset: The difference (in hours) from UTC for standard time.dst: Abbreviation for daylight saving time (e.g., MDT).[offset]: The difference (in hours) from UTC for daylight saving time (usually 1 hour ahead of standard time).start [/time]: The rule that defines when daylight saving time begins.end [/time]: The rule that defines when daylight saving time ends. The default self-defined time zone is "MTZ+6MDT+5,M4.1.0,M11.1.0". Note:A positive (+) offset value means the local time zone is west of the Prime Meridian (Greenwich Meridian).A negative (-) offset value means the local time zone is east of the Prime Meridian.
Date Display Format	Determines which format will be used to display the date.It can be selected from the drop-down list. YYYY-MM-DD: 2012-01-31MM-DD-YYYY: 01-31-2012DD-MM-YYYY: 31-01-2012ddd, mmm DD: Tue, Jan 31The default setting is "YYYY-MM-DD".
Time Display Format	Specifies which format will be used to display the time. It can be selected from a 12-hour or 24-hour format. The default setting is 24 Hour format.

Schedule

Schedule -> Schedule	
Name	The name given to the schedule (e.g., "Work Hours," "Weekend Access").
Holiday	Associates the schedule with specific holidays. The options include no holiday or a selected holiday (up to 10 holidays can be created).
Custom Time	Defines the specific times during which the door will be accessible according to the schedule (e.g., 9:00 AM to 5:00 PM). Users can configure up to 8 time intervals for each day of the week.
Schedule -> Holidays	
Name	The name given to the holiday (e.g., "New Year's Day," "Company Holiday").
Date	Specifies the holiday dates, with up to 5 dates allowed per holiday.

Security Settings

Security Settings -> Web/SSH Access	
Enable SSH	Enables SSH access to the GDS372x. Default setting is "Yes".
SSH Port	Customizes SSH port. Valid range: 1 - 65535. Default port is 22.
HTTP Web Port	Configures the HTTP port under the HTTP web access mode. Valid range: 80-65500 Default port is 80.
HTTPS Web Port	Configures the HTTPS port under the HTTP web access mode.Valid range: 80-65500 Default port is 443.
Web Access Mode	Determines which protocol will be used to access the GDS372x' s Web GUI. It can be selected from HTTP and HTTPS or Both. The default setting is HTTPS.
User Login Timeout	Set login timeout (in minutes) for user. If there is no activity within the specified amount of time, the user will be logged out, and the system will jump to the login page automatically. Default is 15 minutes.
Enable User Web Access	Toggle to enable or disable user web UI access. Default Settings is "Disabled".
Validate Server Certificates	Verify the server certificate using the trusted certificates for TLS. If disabled, the device will bypass certificate verification. Enabled by default.
Security Settings -> User Info Management	

Current Password	Enter the current password.
User	
User Account	Displays the name of the user account.
New Password	Allows the administrator to set the password for user-level web GUI access. This field is case sensitive with a maximum length of 512 characters. The default password is "123".
Confirm Password	Enter the new User password again to confirm.
Administrator	
Admin Account	Displays the name of the admin account.
New Password	Allows the user to change the admin password. The password field is purposely blank after clicking the "Save" button for security purpose. This field is case sensitive with a maximum length of 512 characters.
Confirm Password	Enter the new Admin password again to confirm.
Security Settings -> Client Certificate	
Minimum TLS Version	Configures the minimum TLS version supported by the GDS372x. The default setting is "TLS 1.2".
Maximum TLS Version	Configures the maximum TLS version supported by the GDS372x. The default setting is "Unlimited".
Enable Weak TLS Cipher Suite	This setting controls how the GDS372x handles weak TLS cipher suites for encryption. The options are:Enable Weak TLS Cipher Suites: Allows the device to use weak TLS cipher suites for encrypting data.Disable Symmetric Encryption RC4/DES/3DES: Disables weak symmetric ciphers RC4, DES, and 3DES.Disable Symmetric Encryption SEED: Disables the SEED symmetric cipher.Disable All Weak Symmetric Encryption: Disables all weak symmetric ciphers.Disable Symmetric Authentication MD5: Disables the weak MD5 authentication method.Disable All Weak TLS Cipher Suites: Disables all weak TLS cipher suites (default setting).
SIP TLS Certificate	Defines the SSL certificate used for SIP over TLS.
SIP TLS Private Key	Defines the SSL Private key used for SIP over TLS.
SIP TLS Private Key Password	Defines the SSL Private key password used for SIP over TLS.
Custom Certificate	Allows to upload a Custom Certificate file to GDS372x.
Security Settings -> Trusted CA Certificates	
Load CA Certificates	Loads certificate authority (CA) certificates. Options include default certificates, custom certificates, or all certificates.
Index ID	A unique identifier for each CA (Certificate Authority) certificate entry in the list.
Issued By	Displays the name of the Certificate Authority that issued the trusted certificate.
Expiration	Shows the expiration date of the CA certificate, indicating until when it is valid for secure communications.

Preferences

Preferences->Light Settings	
Keypad Light Mode	Controls the backlight behavior of the keypad:Disable: Turns off the keypad backlight.Always On: Keeps the keypad backlight on at all times.Keypress Always On: Keeps only the key symbols illuminated.Default setting is "Always On".
Start Time	Sets the time range during which the keypad backlight will be active (if not disabled).
End Time	Sets the time range during which the keypad backlight will be active (if not disabled).

Doorbell Button Light Brightness	Set the brightness level of the LED light surrounding the doorbell button on the device. This feature allows users to adjust visibility according to ambient lighting conditions. The available options are:Dim: Lowest brightness, suitable for low-power environments.Moderate: Balanced brightness for typical indoor or shaded outdoor conditions.Bright: Enhanced visibility for most outdoor settings.High Bright: Maximum brightness for very bright or low-visibility environments.The default setting is "Moderate".
LED in The Card Reader Area	Enables or disables the LED light around the card reader area to indicate status or enhance visibility. Enabled by default.
LED Fill Light Mode	Controls the fill light near the camera:Disabled: Turns off the fill light.Auto: Automatically turns on the fill light based on lighting conditions.Manual: The fill light will remain on continuously for a configured duration.Default setting is "Auto".
LED Fill Light Time	Defines the time range during which the LED fill light remains continuously active when LED Fill Light Mode is set to "Manual". Users can configure up to 3 non-conflicting time periods.

TR-069

Enable TR-069	Sets the GDS372x system to enable the "CPE WAN Management Protocol" (TR-069). Enabled by default.
ACS URL	Specifies URL of TR-069 ACS (e.g., http://acs.mycompany.com), or IP address. Default URL is "https://acs.gdms.cloud".
TR-069 Username	Enters username to authenticate to ACS.
TR-069 Password	Enters password to authenticate to ACS.
Periodic Inform Enable	Sends periodic inform packets to ACS. This setting is enabled by default.
Periodic Inform Interval	Configures how often the GDS372x sends "Inform" packets to the ACS. The interval determines the frequency of these periodic status updates. The valid range is 1 to 4294967295, and the default value is 86400 seconds.
Connection Request Username	Enters username for the ACS to connect to the GDS372x.
Connection Request Password	Enters password for the ACS to connect to the GDS372x.
Connection Request Port	Enters the port for the ACS to connect to the GDS372x. Valid range: 1-65535 Default port is 7547.
CPE SSL Certificate	Uploads Cert File for the GDS372x to connect to the ACS via SSL.
CPE SSL Private Key	Uploads Cert Key for the GDS372x to connect to the ACS via SSL.
Start TR-069 at Random Time	If enabled, TR-069 will send out the first INFORM message to the server on randomized timing between 1 to 3600 seconds after the GDS372x boots up. Disabled by default.

Email Settings

SMTP Server	The address of the outgoing mail server used to send email notifications (e.g., smtp.gmail.com).
SMTP Server Port	The port number used by the SMTP server (commonly 465 for SSL, 587 for TLS).
From Email Address	The email address shown as the sender in outgoing email notifications.
Sender Email Username	The username used to authenticate with the SMTP server.
Sender Email Password	The password or app-specific password used for SMTP authentication.
SSL	Enables/Disables SSL/TLS encryption for secure email transmission. (Enabled by default)

Test Email	A button to send a test email using the configured settings to verify that email notifications are working.
Email Notification Address	
Recipient Address 1	The email addresses of the recipient 1 that will receive notifications (e.g., snapshots, alarms).
Recipient Address 2	The email addresses of the recipient 2 that will receive notifications (e.g., snapshots, alarms).
Email Notification Address	
Email Subject	Allows configuration of the subject line used in alarm notification emails. This field supports dynamic variables that will be automatically replaced with actual values when the email is generated:${MAC}: Device MAC address${WARNING_MSG}: Event message details${IP_ADDR}: Device IP address${DATE}: Date and time of the event${CARDID}: Card number used (if applicable)${USERNAME}: Username associated with the event${MODEL}: Device model information${OSD}: On-Screen Display textThe default email subject is "${MODEL}_${MAC}_${WARNING_MSG}_${OSD}"
Email Content	Allows configuration of the body text used in alarm notification emails. This field supports dynamic variables that will be automatically replaced with actual values when the email is generated:${MAC}: Device MAC address${WARNING_MSG}: Event message details${IP_ADDR}: Device IP address${DATE}: Date and time of the event${CARDID}: Card number used (if applicable)${USERNAME}: Username associated with the event${MODEL}: Device model information${OSD}: On-Screen Display textThe default email content template is:"Detected: ${WARNING_MSG}Model: ${MODEL}MAC Address: ${MAC}Alarm Time: ${DATE}"

FTP Settings

FTP Server	The domain name or IP address of the FTP server used to store snapshots or recorded data.
FTP Server Port	The communication port used to connect to the FTP server (default is port 21).
FTP Server Username	The username required to authenticate and access the FTP server.
FTP Server Password	The password associated with the FTP server username for login authentication.
Storage Path	The directory or folder path on the FTP server where the files will be stored (e.g., /snapshots).
Test FTP Server	A button to verify the FTP connection and ensure that the credentials and path are correct.

Maintenance Page Definitions

Upgrade and Provisioning

Upgrade and Provisioning -> Firmware	
Current Version	Displays the current firmware version of the GDS372x.
Upgrade via Manual Upload	
Upload Firmware File to Update	Allows users to load the local firmware to the GDS372x to update the firmware.
Upgrade via Network	
Firmware Upgrade Mode	Allows users to choose one of the following the firmware upgrade methods: TFTP, HTTP, HTTPS, FTP, or FTPS. The default setting is "HTTPS".

Firmware Server Path	Set the IP address or domain name of the firmware server. The URL of the server that hosts the firmware release. This field is empty by default. Administrators can also configure variables in the URL. The following variables are supported:* $PN: is replaced with the GDS372x model.* $MAC: is replaced with the MAC address of the GDS372x.
Firmware Server Username	Enters the username for the firmware server.
Firmware Server Password	Enters the password for the firmware server.
Firmware File Prefix	Checks if the firmware file is with matching prefix before downloading it. This field enables users to store different versions of firmware files in one directory on the firmware server.
Firmware File Postfix	Checks if the firmware file is with matching postfix before downloading it. This field enables users to store different versions of firmware files in one directory on the firmware server.
Upgrade Detection	
Upgrade	Click the "Start" button to check whether the firmware in the firmware server has an updated version, if so, update immediately.
Upgrade and Provisioning -> Config File	
Configure Manually	
Download Device Configuration	Click to download the device configuration file in .txt format.
Upload Device Configuration	Upload the configuration file to the GDS372x.
Configure via Network	
Config Upgrade Via	Selects the provisioning method: TFTP, HTTP or HTTPS, FTP, FTPS. The default setting is "HTTPS".
Config Server Path	Sets IP address or domain name of the configuration server. The server hosts a copy of the configuration file to be installed on the GD372x. This field is empty by default. Administrators can also configure variables in the URL. The following variables are supported:* $PN: is replaced with the GDS372x model.* $MAC: is replaced with the MAC address of the GDS372x.
Config Server Username	Configures the username for the config server.
Config Server Password	Configures the password for the config server.
Config File Prefix	Checks if configuration files are with matching prefix before downloading them. This field enables users to store different configuration files in one directory on the provisioning server.
Config File Postfix	Checks if configuration files are with matching postfix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
Authenticate Config File	Sets the GD372x system to authenticate configuration file before applying it. When set to "Yes", the configuration file must include value P1 with GD372x system's administration password. If it is missed or does not match the password, the GD372x system will not apply it. The default setting is "No".
XML Config File Password	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file is using OpenSSL.
Upgrade and Provisioning -> Provision	
Auto Upgrade	
Automatic Upgrade	Specifies when the firmware upgrade process will be initiated; there are 4 options:No: The GD372x will only do upgrade once at boot up.Yes, check for upgrade periodically: User needs to set an automatic check interval in minutes.Yes, check for upgrade every day: User needs to specify "Hour of the day (0-23)".Yes, check for upgrade every week: User needs to specify "Hour of the day (0-23)" and "Day of the week (0-6)".Notes:Day of week setting starts from Sunday.The default setting is "No".
Start Upgrade at Random Time	Configures whether the GD372x will upgrade automatically at random time point within the configured period.

Automatic Upgrade Check Interval (m)	Configures how often the GDS372x checks for firmware upgrade (in minutes). This setting is only valid if the user selects "Yes, check for upgrade periodically" in the "Automatic Upgrade". The valid range is 60-86400, and the default setting is 10080 (namely 7 days).
Hour of the Day (0-23)	Defines at which hour of the day the GD372x system will check the HTTP/HTTPS/TFTP/FTP/FTPS server for firmware upgrades or configuration files changes.
Day of the Week (0-6)	Defines which day of the week the GD372x system will check the HTTP/HTTPS/TFTP/FTP/FTPS server for firmware upgrades or configuration files changes.
Firmware Upgrade and Provisioning	Defines the GD372x system's rules for automatic upgrade. It can be selected from:Always check for new firmware.Check new firmware only when F/W pre/suffix changes.Always skip the firmware Check.The default setting is "Always check for new firmware".
DHCP Option	
Allow DHCP Option 43 and Option 66 to Override Server	If DHCP option 43, and 66 is enabled on the LAN side, the device will reset the CPE, upgrade, network VLAN tag, and priority configuration according to option 43 sent by the server. At the same time, the update mode and server path of the configuration upgrade mode will be reset according to the option 66 sent by the server. Default is "Yes".
DHCP Option 120 Override SIP Server	Configures the GD372x system to allow the DHCP offer message to override the SIP Server Path via the Option 120 header. The default setting is "No".
Additional Override DHCP Option	Configures additional DHCP Options (150 or 160) to be used for firmware server instead of the configured firmware server or the server from DHCP Option 43 and 66. This option will be effective only when "Allow DHCP Option 43 and Option 66 to Override Server" is enabled.The default setting is "Option 150".
Allow DHCP Option 242 (Avaya IP Phones)	Enables DHCP Option 242. Once enabled, the GD372x will use the configuration info issued by the local DHCP in Option 242 to configure the proxy, transport protocol, and server path.The default setting is "No".
Config Provision	
Config Provision	Device will download the configuration files and provision by the configured order.
Download and Process All Available Config Files	By default, the device will provision the first available config in the order of cfgMAC.xml, cfgMODEL.xml, and cfg.xml (corresponding to device specific, model specific, and global configs). If set to "Yes", the device will download and apply (override) all available configs in the order of cfg.xml, cfgMODEL.xml, cfgMAC.xml. The default setting is "No".
3CX Auto Provision	If enabled, the GD372x will send SUBSCRIBE requests to the multicast address in LAN during bootup for automatic provisioning. This feature requires 3CX server support.
Upgrade and Provisioning -> Advanced Settings	
Send HTTP Basic Authentication By Default	Specifies whether the device should always include HTTP/HTTPS authentication credentials when using wget to download firmware or configuration files.Yes: Always send the username and password, regardless of whether the server requests authentication.No: Only send the username and password when the server requires authentication.The default setting is "No".
Enable SIP NOTIFY Authentication	Enables the GD372x to challenge SIP NOTIFY with 401. The default setting is "Yes".
Validate Certification Chain	Configures whether to validate the server certificate when download the firmware/config file. If it is set to "Yes", the GD372x will download the firmware/config file only from the legitimate server. Default setting is "No".
Use Auto Location Service	Configures whether to allow access to the AutoConfig service. If not checked, access to service.ipvideotalk.com will be disabled. Default value is "Enabled".

Factory Reset	Resets the GDS372x system to the default factory setting mode.

System Diagnostics

System Diagnostics->Syslog	
Syslog Protocol	Select the transport protocol over which log messages will be carried. The options are:UDP: Syslog messages will be sent over UDP.SSL/TLS: Syslog messages will be sent securely over TLS connection.The default setting is "UDP".
Syslog Server	Configures the URI which the GDS372x system will send the syslog messages to.
Syslog Level	Selects the level of logging for syslog. The default setting is "None". There are 4 levels from the dropdown list: DEBUG, INFO, WARNING and ERROR. The following information will be included in the syslog packet:DEBUG (Sent or received SIP messages).INFO (Product model/version on boot up, NAT related info, SIP message summary, Inbound and outbound calls, Registration status change, negotiated codec, Ethernet link up).WARNING (SLIC chip exception).ERROR (SLIC chip exception, Memory exception).Note: Changing syslog level does not require a reboot to take effect.
Syslog Keyword Filter	Only send the syslog with keyword, multiple keywords are separated by comma.Example: set the filter keyword to "SIP" to filter SIP log.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages. The default setting is "No".
System Diagnostics->Packet Capture	
With RTP Packets	Includes Real-time Transport Protocol (RTP) packets used for audio/video streams in the packet capture file.
With Secret Key Information	If enabled, includes encrypted key information in the capture (useful for debugging but should be used with caution due to security concerns).
Start	Begins the packet capture process.
Stop	Stops the ongoing packet capture.
Download	Downloads the captured packet file in a .tar archive. After extraction, the capture file will be available in .pcapng format for offline analysis.
Delete	Deletes the saved packet capture file from the device.
System Diagnostics->Ping	
Input	Enter a domain name or IP address to test network connectivity (e.g., 8.8.8.8 or example.com).
Start	Initiates the ping test to check if the device can reach the specified address and measure the packet loss.
System Diagnostics->Traceroute	
Input	Enter a domain name or IP address to trace the network path (e.g., 8.8.8.8 or example.com).
Start	Begins the traceroute process to identify the route and intermediate hops taken to reach the destination from the device.
System Diagnostics->Remote Diagnostics	
Start	Enables remote diagnostics, allowing remote access the device and collection of diagnostic logs. Access will automatically expire after a set period for security purposes.
System Diagnostics->Audio Diagnosis	
Audio Diagnostic Server	Specifies the server address used for audio diagnosis, typically provided by the system administrator or support team.
Audio Diagnosis	Enables or disables the audio diagnostic feature. When enabled, the device connects to the specified server for troubleshooting purposes.

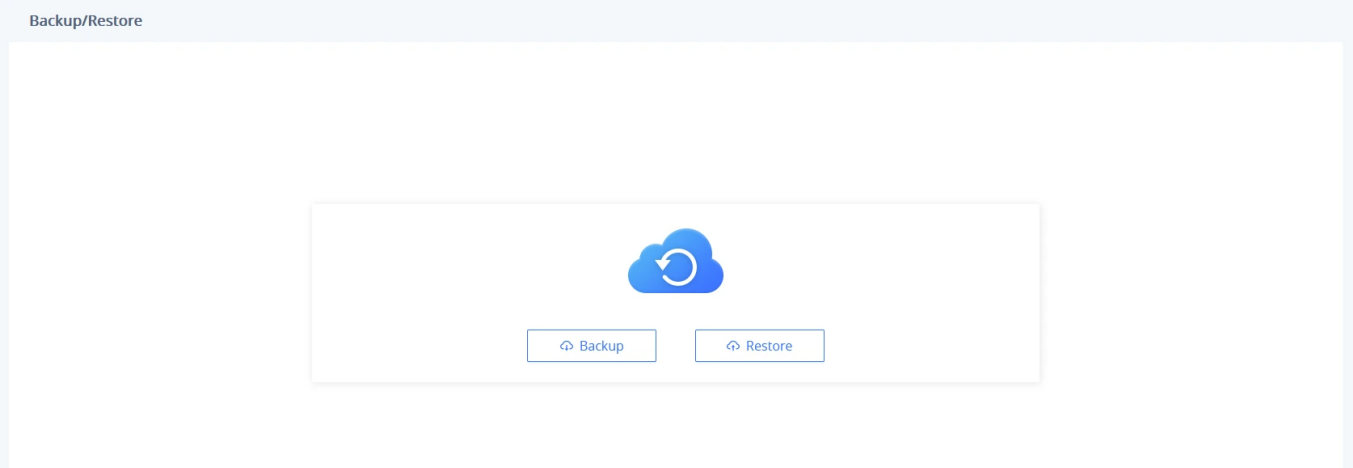
Event Notification

Device Status	
Bootup Completed	Configures the event URL when GDS372x boots up.
Registered	Configures the event URL when an account in the GDS372x is registered successfully.
Unregistered	Configures the event URL when an account in the GDS372x is unregistered.
Log On	Configures the event URL when users log on the GDS372x successfully.
Log Off	Configures the event URL when users log off the GDS372x.
Access control operation	
Relay Trigger	Configures the Action URL to send when the relay is triggered.
Relay Off	Configures the Action URL to send when the relay is turned off.
Valid Card Swipe in	Configures the Action URL to send when the valid card is swiped in.
Invalid Card Swipe in	Configures the Action URL to send when the invalid card is swiped in.
Input Trigger	Configures the Action URL to send when digital input is triggered.
Input Off	Configures the Action URL to send when digital input is turned off.
Call Operation	
Incoming Call	Configures the event URL when GDS372x has an incoming call.
Outgoing Call	Configures the event URL when GDS372x has an outgoing call.
Missed Call	Configures the event URL when the GDS372x has new a missed call.
Established Call	Configures the event URL when a call is established.
Terminated Call	Configures the event URL when a call is disconnected.

Backup/Restore

This page allows users to back up or restore the device configuration.

- **Backup:**
  Click this button to download and save the current configuration settings of the GDS372x. The file will be saved in **.uf format**, which can later be used to restore the same settings.
- **Restore:**
  Click this button to upload a previously saved **.uf** configuration file and apply it to the device. This will overwrite the current settings.



Application Page Definitions

Account Sharing

Account Sharing->Account Sharing	
General Settings	
Enable Account Sharing	Select whether to enable Account Sharing. This feature is disabled by default.
Role in Account Sharing	Specifies the role of the device in an account sharing setup.Host Device: Registers an account on the IP PBX and allows guest devices to make calls through its account.Guest Device: Does not register an account on the IP PBX and relies on the host device to place and receive calls within the network.The default option is "Guest Device".
SIP Server Port	Specifies the SIP service port used for account sharing. A value of 0 means a random port will be assigned. Valid range is 0-65535. Default port is 15060.
Group Name	Set the group name, in the host-guest mode, devices with the same group name can discover each other. Note: This item is mandatory if using Account Sharing. The verification format is domain type
Group Password	In the host-guest mode, after setting the group password, the guest device with the same group password as the host device can successfully register an account on the host device. Note:This item is mandatory if using Account Sharing.
Account Settings	
Associated account	Specifies the account behavior in Account Sharing:Host Device Role: Specifies which host account will be used as the outgoing and incoming account for calls outside of the Account Sharing network.Guest Device Role: Specifies which host account the guest device will register to for making and receiving calls.
Guest Account Name	This setting specifies the account name corresponding to the account used by the guest device.
Ringing tone Settings	
Sync Ringing In Group	Specifies whether the ringtones of all successfully registered guest devices in the group will play in synchronization when a call is received. The default setting is "No".
Ringtone	Select an existing ringtone or upload a custom audio file. (Supported formats include MP3, WAV, OGG, WMA, MID, and M4A)
Account Sharing->Account Sharing List	
Discover Device list	
Refresh	Click to refresh the list of discovered devices.

Diagnostic Page Definitions

Microphone Test	Tests the microphone's functionality by capturing and playing back audio input.
Speaker Test	Tests the speaker by playing a sample sound to confirm output functionality.
Reset Key Test	Checks if the hardware reset button is responsive and functioning correctly.
Light Test	Activates the LED lights to verify their operation (e.g., indicator or fill light).
Certificate Test	Verifies the integrity and validity of installed security certificates.

SD Card Test	Checks if an inserted SD card is recognized and functioning properly.
Relay Out Test	Tests the relay output by triggering it manually to ensure proper response (e.g., unlocking a door).
Alarm Input Test	Verifies the functionality of alarm input interfaces by detecting signal changes.
Card Swipe Test	Tests RFID or IC card reading capability.
Key Test	Tests the physical keypad buttons to ensure each key press is detected.
Wiegand Test (GDS3725/GDS3726 Only)	Tests Wiegand communication by detecting Wiegand input and verifying Wiegand output transmission.
Tamper Test	Simulates or detects a tamper event to confirm the tamper switch is operational.
PIR Test	Tests the Passive Infrared (PIR) sensor for motion or presence detection.

GDS372x HTTP API

Grandstream Door Systems supports HTTP API (Application Programming Interface).

For more details, please refer to the following guide:

> GDS372x - HTTP API Guide

The document explains in detail the external HTTP-based application programming interface and parameters of functions via the supported method. The HTTP API is firmware-dependent. Please refer to the related firmware Release Note for the supported functions.

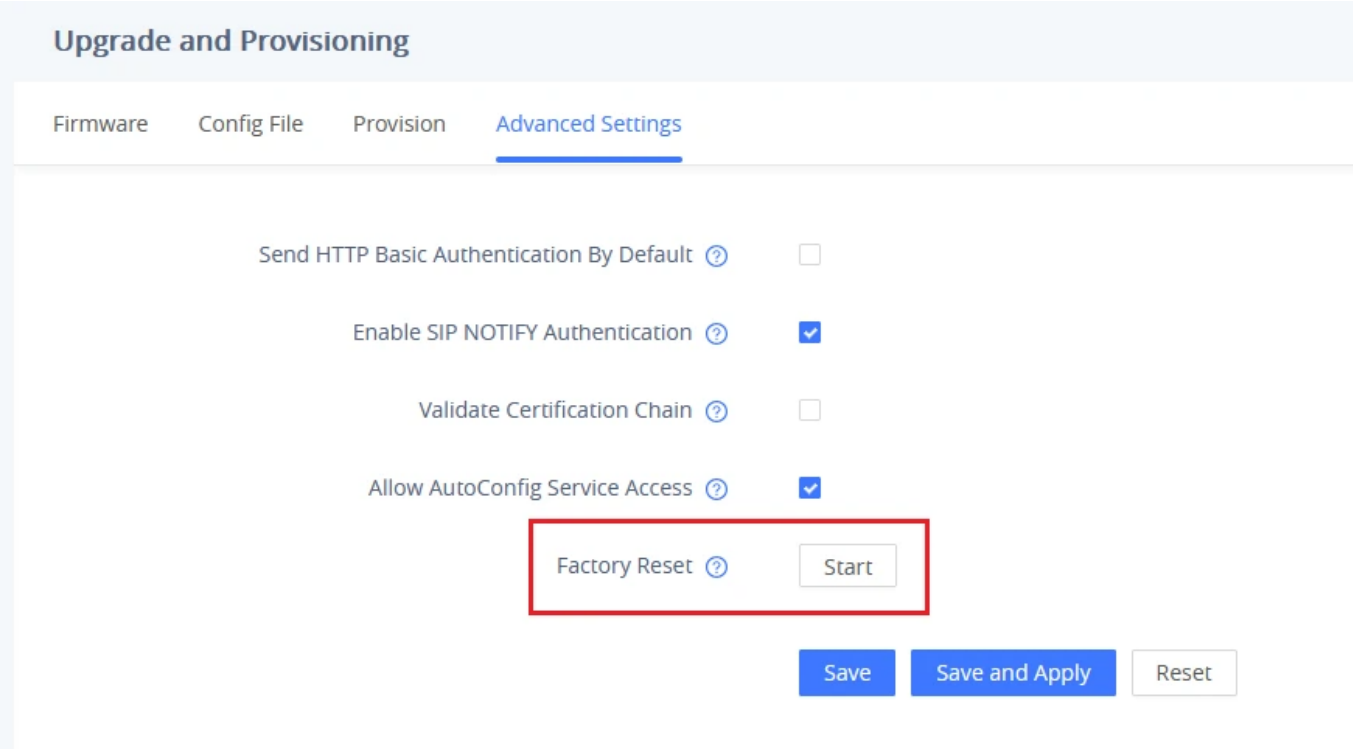
Administrator Privilege is required, and administrator authentication verification has to be executed before any operation on the related parameter configuration.

FACTORY RESET

Restore to Factory Default via Web GUI

To perform a factory reset to the GDS372x via the Web GUI, please refer to the following steps:

1. Access the GDS372x Web GUI using the admin username and password.
2. Navigate to **Maintenance →Advanced Settings.**
3. Press the Factory Reset button as displayed in the following screenshot.

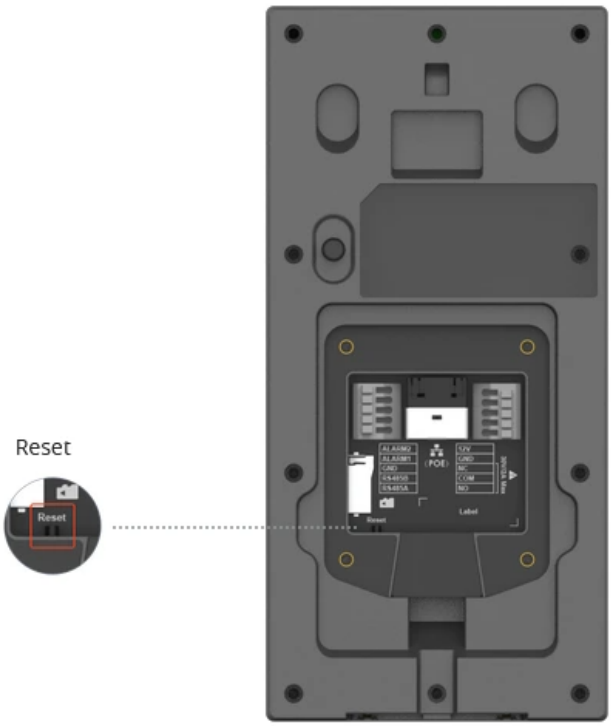


GDS372x Web UI Factory Reset

Factory Reset via the Reset Button

To perform a hard factory reset on the GDS372x device:

1. Power on the device.
2. Press and hold the RESET button (located inside the device or on the back panel) for about 10 seconds until the LED indicators flash.



3. Release the button. The device will reboot and restore to factory default settings.

- Power must **NOT** be lost while performing a hard factory reset.
- This process erases all settings and configurations. Ensure you back up any important data before proceeding.

CHANGE LOG

This section documents significant changes from previous versions of the user manual for GDS372x. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.3.9

- No major changes.

Firmware Version 1.0.3.5

- Added support for Home Assistant. [Access Control Settings] [Home Assistant] [Syn Alarm Info to Home Assistant]
- Added support for RS485. [Access Control Settings]
- Added support for Wiegand Function Settings (GDS3725/GDS3726 Only). [Access Control Settings]
- Added support for Wiegand Test (GDS3725/GDS3726 Only). [Diagnostic]
- Added support for Open Door Timeout Alarm. [Alarm Event Settings] [Door Open Timeout Alarm]
- Added support for SD Card Alarm. [Alarm Event Settings] [SD Card Alarm]
- Added support for Safe Room Alarm. [Alarm Event Settings] [Safe Room Alarm]
- Added support for Interlock Mode. [Open Door Settings]
- Added support for WDR Schedule. [CMOS Settings]
- Added support for Reboot on check-sync event without "reboot=" [Accounts]
- Added the configuration option "Hang up After Open Door". [Hang up After Open Door]
- Merged the Schedules. [Schedule]
- Added Cloud Service Page. [Cloud Service]
- Added support for Building Mode (GDS3725 Only). [Building Mode]

Firmware Version 1.0.1.35

- Added support for video capability configuration For SIP accounts. [Add Video Capability]
- Updated the Alarm Notification Settings page to support configuring the Cloud Call Number and SIP alarms independently. [Alarm Notification Settings]

Firmware Version 1.0.1.30

- No major changes.

Firmware Version 1.0.1.26

- This is the initial version for GDS372x.