Grandstream Networks, Inc.

GDS3710 Event Logs Configuration Guide

Table of Contents

Table of Tables

Table of Figures

SUPPORTED DEVICES

Following table shows Grandstream products supporting GDS37XX integration:

Model	Supported	Firmware
GDS3710	Yes	1.0.3.32 or higher

INTRODUCTION

GDS3710 HD is an IP video door system with a built-in hemispheric camera and some high-definition video capabilities. GDS3710 is ideal for monitoring from wall to wall without blind spots. Powered by an advanced Image Sensor Processor (ISP) and state of the art image algorithms, it delivers exceptional performance in all lighting conditions. It contains integrated PoE, LEDs, HD loudspeaker, RFID card reader, motion detector, lighting control switch, Alarm Input/output and more.

The GDS3710 IP video door system features industry-leading SIP/VoIP for 2-way audio and video streaming to smart phones and SIP phones, allowing to receive calls from GDS3710 on associated SIP phones when doorbell is pressed, opening door from the SIP phone, initiate calls from the phone to GDS3710 to get real time Video/Audio stream with GXP21xx IP Phones and only Audio stream with GXP17xx and GXP16xx IP Phones.

For monitoring purposes, GDS3710 does support Event logs notification via HTTP where the device will be sending via HTTP POST commands, log messages to HTTP server. Also, users could check the logs directly from the web UI of the device.

On the following parts we will go through on how to configure GDS3710 to receive event logs and the supported log messages on the unit.

CONFIGURE EVENT LOGS NOTIFICATION

For the purpose of demonstration, we will use simple HTTP server without authentication, but if the user wishes to use HTTP authentication to connect to server, then that is supported on the GDS software.

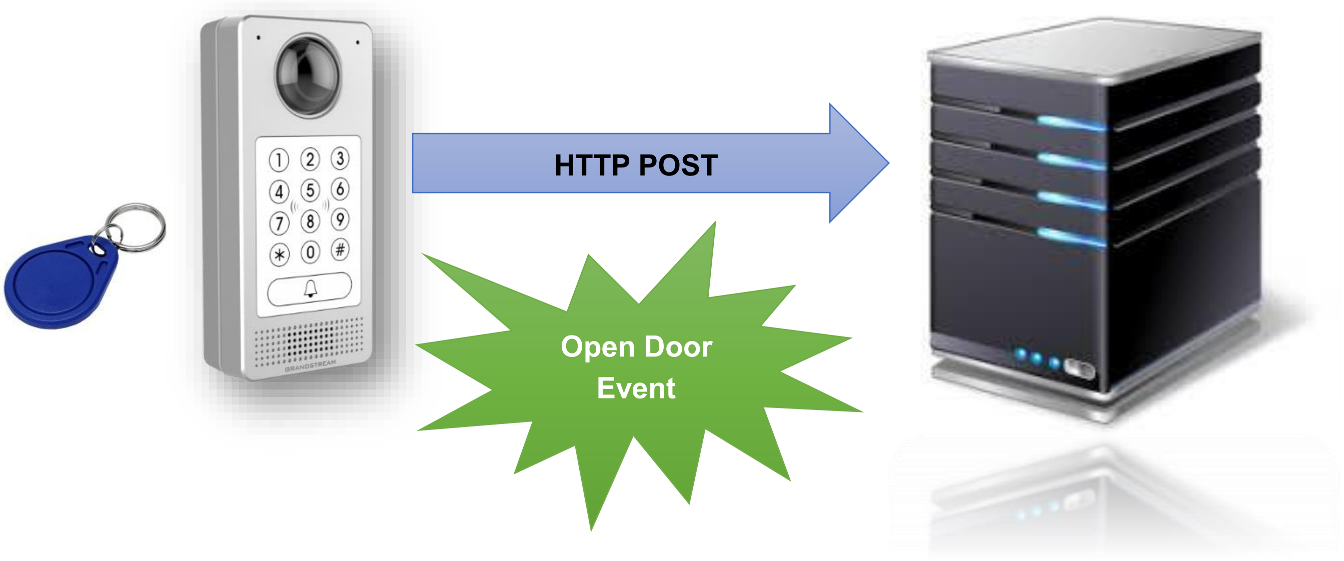


Figure 1: GDS HTTP Event Logs

GDS3710 Configuration Settings

The GDS3710 needs to be configured with the correct connection parameters to HTTP server in order to submit the log messages when events occur:

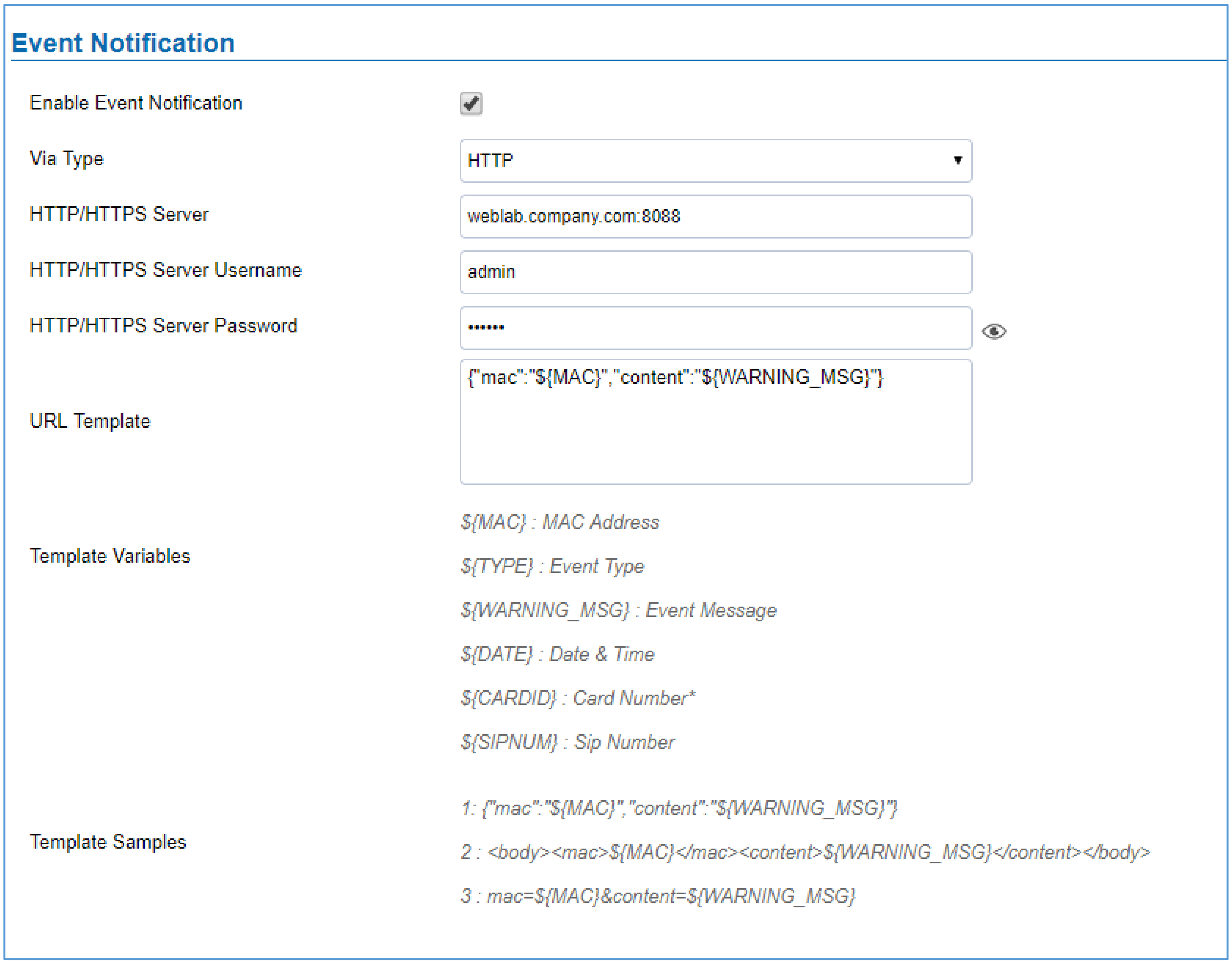
1. Access the GDS3710 Web GUI and navigate to "**Maintenance→Event Notification**".
2. Enable the event notification and choose the protocol to be used to send out the notification messages:
   - **HTTP or HTTPs are supported.**
3. Enter Server IP address or domain name (in case domain name is used then GDS should have a valid working DNS server).
4. If authentication is required, enter the username and password.
5. Enter the message template, otherwise leave to default:

   {"mac":"${MAC}","content":"${WARNING_MSG}"}

   This field can be used to customize the message content that will be sent to the HTTP server for event notification, following variables are supported for customization:

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

6. Click **Save** button to apply changes.
7. Press **Test** to test the connection.



Event Notification

Enable Event Notification	☑
Via Type	HTTP ▾
HTTP/HTTPS Server	weblab.company.com:8088
HTTP/HTTPS Server Username	admin
HTTP/HTTPS Server Password	••••••
URL Template	{"mac":"${MAC}","content":"${WARNING_MSG}"}
Template Variables	*${MAC} : MAC Address* *${TYPE} : Event Type* *${WARNING_MSG} : Event Message* *${DATE} : Date & Time* *${CARDID} : Card Number** *${SIPNUM} : Sip Number*

Template Samples	*1: {"mac":"${MAC}","content":"${WARNING_MSG}"}*
	2 : <body><mac>${MAC}</mac><content>${WARNING_MSG}</content></body>
	3 : mac=${MAC}&content=${WARNING_MSG}

Figure 2: GDS3710 Event Notification Configuration

Supported Event Logs

The GDS3710 supports the following Event log notification messages which indicates most of the events that can occur with the unit:

Table 1: Supported Event Logs

Event Type	Event Message	Use Case
100	Open Door via Card	Indicates that someone opens the door via card or key fob.
101	Open Door via Card (over Wiegand)	Indicates that someone opens the door via card or key fob using Wiegand interface connected to GDS.
200	Visiting Log	Indicates that door has been opened for visitor which pressed door bell button.
300	Open Door via Universal PIN	Indicates that door has been opened successfully using local PIN code via GDS keypad.
301	Open Door via Private PIN	Indicates that someone opened the door successfully using their private PIN code via GDS keypad.
302	Open Door via Guest PIN	Indicates that a guest used "Guest PIN" code to open the door using GDS keypad.
400	Open Door via DI	Indicates that door has been opened using DI (Digital Input) Signal, such as using a push button.
500	Call Out Log	Indicates the GDS unit initiated a call out, for example when someone uses the keypad to dial a number or press door bell button which preconfigured destination number.
501	Call In Log	Indicates that call has been received by the GDS unit.
504	Call Log (Door Bell Call)	Indicates that someone has initiated a call using door bell button.
600	Open Door via Card and PIN	Indicates that someone used his RFID card or key fob, plus his own private password to authenticate and open the door.
601	Keep Door Open (Immediately)	Key door Open (immediately) action has been performed from the web Interface.
602	Keep Door Open (Scheduled)	Key door Open (immediately) action has been set from the web Interface and the event is triggered.
700	Open Door via Remote PIN	Indicates that someone did send remote PIN code to open the door using GDS manager tool for example.
800	HTTP API Open Door	Indicates that someone did send remote PIN code to open the door HTTP API command.

900	Motion Detection	Indicates that motion detection is triggered.
1000	DI Alarm	Indicates that alarm IN is triggered.
1100	Dismantle by Force	Indicates that the unit has been dismantled by force.
1101	System up	Indicates that the system is UP
1102	Reboot	Indicates that the GDS unit has been rebooted.
1103	Reset (Clear All Data)	Factory reset (clear all data) has been performed.
1104	Reset (Retain Network Data Only)	Factory reset (Retain Network Data Only) has been performed.
1105	Reset (Retain Only Card Information)	Factory reset (Retain Only Card Information) has been performed.
1106	Reset (Retain Network Data and Card Information)	Factory reset (Retain Network Data and Card Information) has been performed.
1107	Reset (Wiegand)	Factory reset using Wiegand module has been performed on the unit.
1108	Config Update	Indicates that the system's configuration has been updated.
1109	Firmware Update (1.0.0.0)	Indicates that the system's firmware has been upgraded.
1200	Hostage Alarm	Indicates that someone has entered the hostage alarm PIN code to open the door.
1300	Invalid Password	Indicates that someone has entered wrong password PIN code to open the door for 5 attempts and corresponding alarm action has been triggered.
1400	Mainboard Temperature(32°C) Normal	Indicates that device's mainboard temperature is normal, (around 32°C).
1401	Mainboard Temperature(32°C) Too Low	Indicates that device's mainboard temperature is too low.
1402	Mainboard Temperature(32°C) Too High	Indicates that device's mainboard temperature is too high.
1403	Sensor Temperature(32°C) Normal	Indicates that device's sensor temperature is normal, (around 32°C).
1404	Sensor Temperature(32°C) Too Low	Indicates that device's sensor temperature is normal too low.
1405	Sensor Temperature(32°C) Too High	Indicates that device's sensor temperature is normal too high.