

Grandstream Networks, Inc.

GDS37xx Door System

HTTP API



Table of Contents

CHANGE LOG	4
HTTP API Version 1.0.0.37	4
HTTP API Version 1.0.0.36	4
HTTP API Version 1.0.0.32	4
HTTP API Version 1.0.0.28	4
HTTP API Version 1.0.0.25	5
HTTP API Version 1.0.0.23	5
HTTP API Version 1.0.0.18	5
HTTP API Version 1.0.0.13	5
SUPPORTED DEVICES.....	6
OVERVIEW	7
1. Authentication.....	8
2. URL Parameter Definitions.....	10
3. XML Returned by Device	10
PARAMETERS	12
1. Card Management	12
2. Door System Basic Settings.....	16
3. Keep Door Open.....	23
4. Group	25
5. Schedule	26
6. Holiday	28
7. Date and Time	30
8. Network Settings.....	33
9. Access Settings	35
10. User Management	37
11. SIP Settings.....	38
12. White List.....	44
13. Video Settings	46
14. On Screen Display (OSD) Settings.....	50
15. CMOS Settings.....	52
16. Audio Settings	54
17. Privacy Masks	55
18. Alarm Config.....	57



19.	Alarm Schedule Configuration.....	68
20.	Alarm Action Configuration	70
21.	Alarm Phone List	72
22.	Email Settings.....	73
23.	FTP Settings.....	75
24.	Upgrade Configuration.....	77
25.	Reboot & Reset	79
26.	Syslog or Debug	82
27.	Data Maintenance.....	83
28.	System Health Alert	83
29.	Event Notification.....	84
30.	Certificates	87
31.	System Status	88
32.	Network Status	90
33.	Firmware Available Version Check.....	92
34.	Card Data Import/Export	93
35.	OpenVPN Settings.....	93
36.	TR069 Settings.....	95
HTTP API APPLICATION EXAMPLES		98
1.	General Parameter Revision	98
2.	JPEG (Snapshot).....	105
3.	MJPEG Stream (Challenge Mode or Basic Mode).....	109
4.	HTTP API to Open Door	119

Table of Figures

Figure 1: MJPEG Authentication Mode.....	109
Figure 2: Video Settings.....	112
Figure 3: Basic MJPEG Authentication.....	115
Figure 4: Video settings	116



CHANGE LOG

This section documents significant changes from previous versions of the GDS37xx_HTTP_API. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

HTTP API Version 1.0.0.37

Product Name: GDS3710 Firmware 1.0.7.24 / GDS3705 Firmware 1.0.1.16

- Added Pvalue P15553 for Event Notification HTTP Method [Event Notification]
- Added Pvalues P26061/P26161/P26261/P26361 for MAC in User-Agent [GDS37XX Account Settings]
- Added Pvalues P29061/P29161/P29261/P29361 for Codec Negotiation Priority [GDS37XX Account Settings]

HTTP API Version 1.0.0.36

Product Name: GDS3710 Firmware 1.0.7.23 / GDS3705 Firmware 1.0.1.16

- Added PValues for TR069 [TR069 Settings]
- Added Pvalue P15543 for One-way Interlocking Doors Mode [Door System Basic Settings]
- Added Pvalue P15544 for Key Sensitivity Level [Door System Basic Settings]
- Added Pvalues for Configurable Auto Reboot. [Reboot & Reset]
- Added Pvalues for Unauthorized Door Opening Attempt Alarm [Alarm Config]
- Added Pvalues for Time zone GMT-3:30 (Newfoundland) [Date and Time]
- Added One-way Interlocking Doors Mode [Alarm Config]
- Added Pvalue for Use P-Access-Network-Info Header [GDS37XX Account Settings]
- Updated range of P15440 [Door System Basic Settings]
- Added Pvalue to set Key Sensitivity Level for GDS3710 [Door System Basic Settings]

HTTP API Version 1.0.0.32

Product Name: GDS3710 Firmware 1.0.7.14 / GDS3705 Firmware 1.0.1.11

- Added PValues P15440 to P15443 for Door Relay Options [Door System Basic Settings]
- Added Pvalue P15514 for PIN Password Display in HTTPS [Door System Basic Settings]
- Added Pvalue P4428 to Disable SIP Notify Authentication [Upgrade Configuration]
- Added Pvalues for OpenVPN Settings [OpenVPN Settings]

HTTP API Version 1.0.0.28

Product Name: GDS3710 Firmware 1.0.7.7 / GDS3705 Firmware 1.0.1.3

- Add RTSP Password. [Access Settings]
- Update Unlock holding time, MAX to 1800. [Door System Basic Settings]
- Add P2395/P2595/P2695. [GDS37XX Account Settings]



HTTP API Version 1.0.0.25

Product Name: GDS3710 Firmware 1.0.7.7 / GDS3705 Firmware 1.0.1.3

- Added Pvalues P15508 and P15509 for Abnormal Door Control. [Alarm Config]
- Added new HTTP API for abnormal door control. [Alarm Config]
- Added Pvalues P15506 and P15507 for Holiday Mode [Keep Door Open]

HTTP API Version 1.0.0.23

Product Name: GDS3710 Firmware 1.0.7.4 / GDS3705 Firmware 1.0.1.3

- Added Pvalue P1411 for “DHCP Option 120 Override SIP Server”. [Upgrade Configuration]
- Updated ChallengeString. [JPEG (Snapshot)]
- Added Pvalues P2347/P2447/P2547/P2647 for Accept Incoming SIP from Proxy Only. [GDS37XX Account Settings]
- Added Pvalues P57/P58/P59/P60 for Special Feature Telefonica Spain. [GDS37XX Account Settings]
- Added Pvalues P37/P486/P586/P686 for Voice Frames per TX. [GDS37XX Account Settings]
- Update P100 to P198 for Special Feature. [GDS37XX Account Settings]
- Added Pvalue P2330 for Re-register before Expiration. [GDS37XX Account Settings]
- Added Pvalues P57/P58/P59/P60 for preferred Vocoder. [GDS37XX Account Settings]
- Added Pvalue P8458/P8459/P286 for Randomized Automatic Upgrade options. [Upgrade Configuration]

HTTP API Version 1.0.0.18

Product Name: GDS3710 Firmware 1.0.5.6 / GDS3705 Firmware 1.0.0.41

- Added second door opening support on GDS3705 via command. [HTTP API to Open Door]
- Added P-value 15473 on GDS3705 for option [Disable Web Access]
- Added P-Values P79/P496/P596/P696 for option [DTMF Payload Type]
- Added P-Values P293/P462/P562/P662 for option [H.264 Payload Type]
- Added Multi-SIP account on GDS3710. [GDS37XX Account Settings]
- Added White List for each of the 4 SIP accounts on GDS3710. [GDS37XX White List]
- Added System Health Alert command. [System Health Alert]

HTTP API Version 1.0.0.13

Product Name: GDS3710 Firmware 1.0.5.2 / GDS3705 Firmware 1.0.0.37

- Added P-value 15476 for option [Allow Reset Via SIP NOTIFY]
- Added P-value 15473 for option [Disable Web Access]
- Added P-value 15469 for option [Enable Anonymous LiveView]
- Extended VLAN tag range from 0 to 4094 for option [Layer 2 QoS 802.1Q/VLAN Tag]
- Added Firmware Available Version Check command [Firmware Available Version Check]
- Added Card Data Import/Export commands [Card Data Import/Export]
- Added P-value 462 for H.264 Payload Type. [GDS37XX Account Settings]

SUPPORTED DEVICES

The following table shows GDS37XX Grandstream products supporting HTTP API covered in this guide:

Model	Firmware
GDS3710	1.0.7.24
GDS3705	1.0.1.16



OVERVIEW

Grandstream Door System Interface HTTP API (Application Programming Interface) supports RFC3550 (RTP).

This 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 must be executed before any operation to the related parameter configuration.

Syntax: Client → Server

```
https://<servername>/goform/config?cmd=get&type=<module>
```

```
https://<servername>/goform/config?cmd=set&<param>=<value>&<param1>=<value>...
```

Notes:

- **<param>** is used to identify the different parameter of functions.
- **<module>** is used to identify the different module of functions.

1. Authentication

Authentication is using encrypted Challenge / Response mode. After successful authentication, the user with administration privilege needs to include the authentication information in each request header of the operation before the operation can be executed.

The authentication process is shown as following:

Step 1:

Client → Server

```
https://<servername>/goform/login?cmd=login&user=admin&type=0
```

Server → Client

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <ChallengeCode>ChallengeString</ChallengeCode>
  <LoginType>0</LoginType>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step 2:

Client → Server

```
https://<servername>/goform/login?cmd=login&user=admin&authcode=<authcodestring>&type=0
```

Server → Client

```
HTTP/1.0 200 OK Content-Type: text/xml;charset=UTF-8
Set-Cookie: session=ac81cade4c9d9264f50c45018fb02c12;path=/;
Set-Cookie: uname=admin;path=/;
Set-Cookie: level=1;path=/;

<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <LoginType>0</LoginType>
  <RetMsg>OK</RetMsg>
</Configuration>
```



Notes:

The rule of authentication code string is generated via following rules:

- *authcodestring* = md5(ChallengeString:GDS3710IZpRsFzCbM:password);
 - ChallengeString is the reply strings from *Server* by **Step 1**
 - Password is the login password of the GDS37xx device.
- The **RED** part of the string is the replied authentication information from *Sever* after successful authentication. Such information needs to exist in the operation message header of all the following operations, otherwise the operation is abnormal and will fail.

Example: Delete the card with ID number: 7465995

Client ➔ *Server*

```
POST /goform/config
HTTP/1.1
Host: 192.168.86.8
Connection: keep-alive
Content-Length: 26
Cache-Control: max-age=0
Origin: https://192.168.86.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.98 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
If-Modified-Since: 0
Referer: https://192.168.86.8/Pages/user_list.html?t=1496385815560
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8
Cookie: gdsauthkey4433=150e080c781be0deb8d5a8a2c6ed95d2; gdslanguage=zh;
session=643e985e113a50979fd245762be01a57; uname=admin; level=1;
gdsauthkey443=643e985e113a50979fd245762be01a57; curpage=user_list.html
cmd=del&user_list=7465995,
```

Note:

The **RED** part of the string is the Authentication String **MUST** be carried in the header message by the cookie during operation



Tips of HTTP API Usage:

- In most situation, parameters fetched by using “GET” can be revised by using “SET”, except Status or Display parameter information.
- When using “SET”, sometimes there are inter-action or restrictions among those related parameters, all parameters must “SET” or configure correctly together before the device taking effect.
- Please refer to related WebGUI page for reference if not sure about the HTTP API.

2. URL Parameter Definitions

<parameter>=<value>	Values	Description
cmd=<string>	add/del/set/get /reboot/reset/fw_upgrade /export/upload	Operation command type (Required): add: add parameter or data del: delete parameter or data set: set device parameter get: get command or parameter reboot: reboot device reset: factory reset device fw_upgrade: check FW version or upgrade FW export: export data upload: import data

3. XML Returned by Device

Response Code	Response Text	Description
0	OK	Success
1		User does not exist
2		Password error
3		Max login or max white list number
4		Phone number exist
5		Parameter should not be empty
6		Parameter contain illegal characters
7		Message sending error
8		New password not match
9		FTP test error



10		Hostage passwd
11		Remote /Local PIN not same with hostage password
12		SMTP timeout
13		Retrieve Password (Account is no exist)
14		SMTP authentication failed
15		SMTP test failed
16		Invalid SMTP server
17		Email address is empty
18		Email test timeout
19		SIP is calling
401		Authentication failed
408		Session time out

Example:

Returned XML by device:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
</Configuration>
```



PARAMETERS

1. Card Management

Supported Devices: **GDS3710/GDS3705**

Method Supported: **cmd = get/add/set/del**

Get:

http://<servername>/goform/config?cmd=get&type=user_list

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <total>1</total>
  <item>
    <idx>0</idx> <!-- index, assigned by system -->
    <ID>1</ID> <!-- card number -->
    <room_num>1</room_num> <!-- virtual number -->
    <sip_num>1</sip_num> <!-- sip number -->
    <username>1</username> <!-- user name -->
    <passwd>1</passwd> <!-- open door password -->
    <gender>0</gender> <!-- gender -->
    <identify_num>1</identify_num> <!-- ID number -->
    <cellphone_num>1</cellphone_num> <!-- cellphone number -->
    <EOD>20991231</EOD> <!-- card valid date -->
    <enable_card>1</enable_card> <!-- enable or disable -->
  </item>
  <item>
    <idx>2</idx>
    <ID>2</ID>
    <room_num>2</room_num>
    <sip_num>2</sip_num>
    <username>2</username>
    <passwd>1</passwd>
```



```

<gender>0</gender>
<identify_num>2</identify_num>
<cellphone_num>2</cellphone_num>
<EOD>20991231</EOD>
<enable_card>1</enable_card>
</item>
<item>
  <idx>2</idx>
  <ID>1</ID>
  <room_num>1</room_num>
  <sip_num>1</sip_num>
  <username>1</username>
  <passwd>1</passwd>
  <gender>0</gender>
  <identify_num>1</identify_num>
  <cellphone_num>1</cellphone_num>
  <EOD>20991231</EOD>
  <enable_card>1</enable_card>
</item>
</Configuration>

```

Add / Set:

http://<servername>/goform/config?cmd=<add/set>&<parameter>=<value>...

Notes:

To add a new card to your card management database or edit an already created one; you will need to make sure to mention the 3 important fields in your request:

- *username; Card Number (ID); virtual number (room_number)*

For example:

+ Add new Card:

https://192.168.1.162/goform/config?cmd=add&ID=258974&room_num=12&sip_num=12&username=Someone&passwd=236987&gender=1&identify_num=12&EOD=20991231



+ Set the "enable_card" flag for that created card:

https://192.168.5.147/goform/config?cmd=set&ID=258974&room_num=12&username=Someone&sip_num=12&passwd=236987&gender=1&identify_num=12&EOD=20991231&enable_card=1

<parameter>=<value>	Values	Description
ID=<int>	Numeric Digits	RFID card number. Unique and cannot be empty
room_num =<int>	Numeric Digits	Virtual Number (Room Number) Cannot be empty
sip_num =<string>	Numeric Digits	SIP extension number (max. length: 20) Binding via SIP
username =<string>	Character Strings	Name (max. 32 characters). Cannot be empty
passwd =<string>	Numeric Digits	PIN to open door (max. length: 12)
gender =<int>	<0 1>	Gender 0 - Male (Default) 1 - Female
identify_num =<string>		ID Number (max. length: 20)
cellphone_num =<int>		Cell Number (max. length: 16)
SOD=<int>		Valid Start Date Format: 20171001 (YYYYMMDD) Default: 19700101
EOD =<int>		Valid End Date Format: 20171001 (YYYYMMDD) Default: 20991231
enable_card =<int>	<0 1>	Enable the RFID card 0: Disable 1: Enable
account	<0 1 2 3 4>	Call Out Account 0: Auto 1: Account 1 2: Account 2 3: Account 3 4: Account 4



group_id	<0-50>	Group: The group id must exist, or group_id=0
sch_id	<0-10>	Schedule 0: Disable 1: Schedule 1 2: Schedule 2 3: Schedule 3 4: Schedule 4 5: Schedule 5 6: Schedule 6 7: Schedule 7 8: Schedule 8 9: Schedule 9 10: Schedule 10

Del:

http://<servername>/goform/config?cmd=del&ID=ID1,ID2,ID3,ID4,...

Notes:

- To delete a card, you need only to mention the ID number which is the Card Number.
- Max 20 cards can be deleted at the same time.

Example:

https://192.168.1.162/goform/config?cmd=del&ID=258974

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
</Configuration>
```



2. Door System Basic Settings

Support method: **cmd = get / set**

Get:

```
http://<servername>/goform/config?cmd=get&type=door
```

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P14100>0</P14100>
  <P14101>5</P14101>
  <P14829>300</P14829>
  <P14830>1000</P14830>
  <P14846>2</P14846>
  <P14102>5</P14102>
  <P14103>1</P14103>
  <P15420>1</P15420>
  <P15421>1</P15421>
  <P14105>0</P14105>
  <P10464>1</P10464>
  <P10465>0</P10465>
  <P15423>5</P15423>
  <P14340>0</P14340>
  <P14120>0</P14120>
  <P14121>0</P14121>
  <P14800>1</P14800>
  <P14801>1</P14801>
  <P14856>0</P14856>
  <P14827>0</P14827>
  <P15434>1</P15434>
```



```

<P10457>88</P10457>
<P10463/>
<P14850>0</P14850>
<P14851/>
<P14852/>
<P14853/>
<P14858>0</P14858>
<P14560>142000</P14560>
<P14561>200059</P14561>
<P14562>1</P14562>
<P14580>0</P14580>
<P15301>0</P15301>
</Configuration>

```

Set:

<http://<servername>/goform/config?cmd=set&<parameter>=<value>...>

<parameter>=<value>	Model Supported	Values	Description
P15440=<int>	GDS3710/GDS3705	<0 1 2>	Door Relay Options 0: Local Relay 1: Webrelay 2: GSC3570 Relay
P15441=<string>	GDS3710/GDS3705		Webrelay IP Address (Max. Length=255)
P15442=<string>	GDS3710/GDS3705		Webrelay Username (Max. Length=128)
P15443=<string>	GDS3710/GDS3705		Webrelay Password (Max. Length=128)
P15444=<int>	GDS3710/GDS3705	<1 2 3 4>	Open Door Account to Choose N-Account N
P15445=<string>	GDS3710/GDS3705		GSC3570 Username (Max. Length=128)
P15446=<string>	GDS3710/GDS3705		GSC3570 Password (Max. Length=128)



P15450=<int>	GDS3710/GDS3705	<0 1>	ALMOUT1 Feature 0: Alarm Output 1: Open Door
P15470=<int>	GDS3710/GDS3705	<0 1>	Lock Status 0: Normal Close 1: Normal Open
P15467=<int>	GDS3710/GDS3705	<0 1 2 3>	Control Options 0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15468=<int>	GDS3710/GDS3705	<0 1 2 3>	Wiegand Control Options 0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P14100=<int>	GDS3710/GDS3705	0 - 20	Delay before Unlock Action(s)
P15465=<int>	GDS3710/GDS3705	0 - 20	Door 2 Delay before Unlock(s)
P14101=<int>	GDS3710/GDS3705	1 - 1800	Unlock Action Holding Time(s)
P15466=<int>	GDS3710/GDS3705	1 - 1800	Door 2 Unlock Holding Time(s)
P14829=<int>	GDS3710/GDS3705	0 - 2000	Minimum Interval of Swiping Card (in millisecond)
P15474=<int>	GDS3710	0 – 4 and no more than 'Unlock Action Holding Time' value.	Number of Snapshots when Door Opened
P15475=<int>	GDS3710	0 – 4 and no more than second 'Door 2 Unlock Action Holding Time' value.	Number of Snapshots when Door 2 Opened
P14103=<int>	GDS3710	<0 1>	Snapshot when Door Opened 0: No 1: Yes



P15471=<int>	GDS3710	<0 1>	Snapshot when Door Opened -- via Email: 0: No; 1: Yes
P15420=<int>	GDS3710	<0 1>	Snapshot when doorbell pressed – via FTP 0: No 1: Yes
P15409=<int>	GDS3710	<0 1>	Snapshot when doorbell pressed – via Email 0: No 1: Yes
P14856=<int>	GDS3710/GDS3705	<0 1>	Call Mode: 0: Virtual Number (or Room Number) 1: SIP Number
P14827=<int>	GDS3710/GDS3705	<0 1 2>	DoorBell Mode: 0: Call Doorbell Number 1: Doorbell Output Control (DO1) 2: Both above
P10470=<int>	GDS3710/GDS3705	<0 1 2 3 4>	Doorbell Call Out Account: 0: Auto 1: Account 1 2: Account 2 3: Account 3 4: Account 4
P15434=<int>	GDS3710/GDS3705	<0 1>	Door Bell Call Mode: 0: Serial Hunting 1: Parallel Hunting
P10462=<string>	GDS3710/GDS3705		Number Called When Door Bell Pressed (Max. Length=255)
P15418=<int>	GDS3710/GDS3705	0--10	Press Doorbell Schedule
P15419=<int>	GDS3710/GDS3705	0--20	Maximum Number of Dialed Digits
P15436=<int>	GDS3710/GDS3705	1 - 15	No Key Input Timeout(s)
P10457=<string>	GDS3710/GDS3705		Remote PIN to Open Door Max. length = 8



P15460=<string>	GDS3710/GDS3705		Remote PIN to Open Door 2. Max. length = 8
P10464=<int>	GDS3710/GDS3705	<0 1 2>	PIN type for Open Door locally: 0: Private PIN 1: Unified PIN 2: Card & private PIN
P10463=<string>	GDS3710/GDS3705		Local PIN to Open Door (all digit value)
P14858=<int>	GDS3710/GDS3705	<0 1>	Enable DTMF Open Door 0: Enable 1: Disable (Default)
P14825=<int>	GDS3710/GDS3705	<0 1>	Enable Guest PIN Open Door: 0: Disable 1: Enable
P14851=<string>	GDS3710/GDS3705		Guest PIN: Numerical Digits Max. Length = 8
P14852=<string>	GDS3710/GDS3705	e.g.: 2017/06/14 00:00:00	Guest PIN starting time
P14853=<string>	GDS3710/GDS3705	e.g.: 2017/06/14 02:02:10	Guest PIN ending time
P14580=<int>	GDS3710/GDS3705	<0 1>	Disable Auto-Answer 0: Disable (Default) 1: Enable
P14582=<int>	GDS3710/GDS3705	<0 1>	Enable Doorbell Button to Hang Up Call 0: Disable (Default) 1: Enable
P15421=<int>	GDS3710/GDS3705	<0 1>	Disable Keypad (except Doorbell Button) 0: Disable (Default) 1: Enable
P15422=<int>	GDS3710/GDS3705	<0 1>	Enable On Hook After Remote Door Opened 0: Disable (Default) 1: Enable



P15424=<int>	GDS3710/GDS3705	<0 1>	Enable HTTP API Remote Open Door 0: Disable (Default) 1: Enable
P15433=<int>	GDS3710/GDS3705	<0 1>	Disable Keypad SIP Number Dialing 0: Disable (Default); 1: Enable
P15543=<int>	GDS3710/GDS3705	<0 1>	One-way Interlocking Doors Mode 0: Disable (Default) 1: Enable
P15428=<int>	GDS3710/GDS3705	5 -- 300	Open Door Valid Time
P15543=<int>	GDS3710/GDS3705	<0 1>	One-way Interlocking Doors Mode 0: Disable (Default); 1: Enable
P10465=<int>	GDS3710/GDS3705	<0 1>	Enable Card Issuing Mode 0: Disable (Default) 1: Enable
P15423=<int>	GDS3710/GDS3705	1-1440	Card Issuing State Expire Time(m)
P14800=<int>	GDS3710/GDS3705	<0 1>	Enable Key Blue Light 0: Disable 1: Enable
P14801=<int>	GDS3710	<0 1>	Enable White LED Back Light 0: Disable 1: Enable
P15301=<int>	GDS3710/GDS3705	<0 1>	Central Mode 0: Disable (Default) 1: Enable
P15544=<int>	GDS3710/GDS3705	<0 1>	Key Sensitivity Level 0: Default 1: High
P14340=<int>	GDS3710/GDS3705	<0 1 2>	Key Pressing Tone 0: Default 1: DTMF 2: Mute



P14120=<int>	GDS3710/GDS3705	<0 1>	Enable Weigand Input 0: Disable 1: Enable
P14121=<int>	GDS3710/GDS3705	<0 1 2>	Weigand Output 0: Disable 1: Relay and Local Authentication 2: Relay and Bypass Local
P14560=<string>	GDS3710/GDS3705		Start time turning on the Blue Door Bell Light Digit string like "1459". The first two digit is 24-hour format, last two is minutes 00 <= hour <=23; 00 <= minute <= 59
P14561=<string>	GDS3710/GDS3705		End time turning on the Blue Door Bell Light Digit string like "1459". The first two digit is 24-hour format, last two is minutes 00 <= hour <=23 00 <= minute <= 59
P14562=<int>	GDS3710/GDS3705	<0 1>	Enable Door Bell Blue Light 0: Disable 1: Enable
P15514	GDS3710/GDS3705	<0 1>	System_Settings.Access_Settings.Enable_PIN_Password_Display_HTTPS 0: Disable; 1: Enable.
P15544=<int>	GDS3710	<0 1>	Set Key Sensitivity level: 0: Default 1: High.

- **P15514**

GET:[\[http/https\]://<servername>/goform/config?cmd=get&type=access](http/https://<servername>/goform/config?cmd=get&type=access)
SET:[\[http/https\]://<servername>/goform/config?cmd=set&P15514=<value>](http/https://<servername>/goform/config?cmd=set&P15514=<value>)



- P15440/ P15441/ P15442/ P15443

GET:`[http/https]://<servername>/goform/config?cmd=get&type=door`
SET:`[http/https]://<servername>/goform/config?cmd=set&Pxxx=<value>`

3. Keep Door Open

Supported Devices: **GDS3710/GDS3705**

Support method: **cmd = get / set**

Get:

`http://<servername>/goform/config?cmd=get&type=sch_open_door`

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P14042>14</P14042>
  <P14043>4</P14043>
  <P14044>7</P14044>
  <P15429>2</P15429>
  <P15430>5</P15430>
  <P15211>20180514000000</P15211>
  <P15212>20180522000000</P15212>
  <P15213>door sch,0@0000@2359</P15213>
</Configuration>
```

Set:

`http://<servername>/goform/config?cmd=set&<parameter>=<value>...`

<parameter>=<value>	Model Supported	Values	Description
P15429=<int>	GDS3710/GDS3705	0 - 2	Keep Door Open 0: Disable 1: Immediate Open Door



			2: Schedule Open Door
P15435=<digital string>	GDS3710/GDS3705		Emergency PIN to Disable Keep Door Open
P15430=<int>	GDS3710/GDS3705	5 - 480	Length(m) to Keep Door Open
P15211=<digital string>	GDS3710/GDS3705		Schedule Start Time
P15212=<digital string>	GDS3710/GDS3705		Schedule End Time
P15506=<int>	GDS3710		Holiday Mode 0: Disabled 1-10: Holiday1-10
P15213=<string>	GDS3710/GDS3705		Schedule Table Format: door_sch,index@start_time@end_time Example: P15213=door_sch,0@0000@2359
P15455=<int>	GDS3710/GDS3705	0 - 2	Keep Door Open 0: Disable 1: Immediate Open Door 2: Schedule Open Door
P15435=<digital string>	GDS3710/GDS3705		Emergency PIN to Disable Keep Door Open (Door 2)
P15456=<int>	GDS3710/GDS3705	5 - 480	Length(m) to Keep Door Open (Door 2)
P15457=<digital string>	GDS3710/GDS3705		Schedule Start Time (Door 2)
P15458=<digital string>	GDS3710/GDS3705		Schedule End Time (Door 2)
P15507=<int>	GDS3710		Holiday Mode (Door 2) 0: Disabled 1-10: Holiday1-10
P15459=<string>	GDS3710/GDS3705		Schedule Table (Door 2) Format: door_sch,index@start_time@end_time Example: P15459=door_sch,0@0000@2359



4. Group

Supported Devices: **GDS3710/GDS3705**

Support Methods: **cmd = get/add/set/del**

Get:

```
http://<servername>/goform/config?cmd=get&type=group
```

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <group>
    <groupid>1</groupid>
    <schid>0</schid>
    <groupName>Qua</groupName>
  </group>
  <group>
    <groupid>2</groupid>
    <schid>1</schid>
    <groupName>Tech</groupName>
  </group>
  <P15301>0</P15301>
  <schdeulelist>
    <schdeuleitem>AAA@0,</schdeuleitem>
    <schdeuleitem>BBB@0,</schdeuleitem>
    <schdeuleitem>schedule3@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule4@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule5@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule6@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule7@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule8@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule9@0,0@0000@0000,</schdeuleitem>
    <schdeuleitem>schedule10@0,0@0000@0000,</schdeuleitem>
  </schdeulelist>
</Configuration>
```



Add:

http://<servername>/goform/config?cmd=add<para1>=<value1>&<para2>=<value2>

<para>=<value>	Values	Description
groupname=<string>&schid=<int>	groupname: string	groupname Max. Length=64
	schid: 1 -- 10	Time Schedule Index

Set:

http://<servername>/goform/config?cmd=set<para1>=<value1>&<para2>=<value2>&<para3>=<value3>

<parameter>=<value>	Values	Description
<para1>=<value1>&<para2>=<value2>&<para3>=<value3>	groupid: 1-10	groupname Max. Length=64
groupid=<int>&groupname=<string>&schid=<int>	schid: 1-10	schid: Time Schedule Index groupid: group index.

Del:

http://<servername>/goform/config?cmd=del<para1>=<value1>

<parameter>=<value>	Values	Description
groupid=<int>	1 - 10	groupid: group index.

5. Schedule

Supported Devices: **GDS3710/GDS3705**

Support Methods: **cmd = get / set**

Get:



http://<servername>/goform/config?cmd=get&type=door_schedule

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P15301>0</P15301>
  <P15200>AAA@0,</P15200>
  <P15201>BBB@0,</P15201>
  <P15202>schedule3@0,0@0000@0000,</P15202>
  <P15203>schedule4@0,0@0000@0000,</P15203>
  <P15204>schedule5@0,0@0000@0000,</P15204>
  <P15205>schedule6@0,0@0000@0000,</P15205>
  <P15206>schedule7@0,0@0000@0000,</P15206>
  <P15207>schedule8@0,0@0000@0000,</P15207>
  <P15208>schedule9@0,0@0000@0000,</P15208>
  <P15209>schedule10@0,0@0000@0000,</P15209>
  <holidayitem>holiday1,</holidayitem>
  <holidayitem>holiday2,</holidayitem>
  <holidayitem>holiday3,</holidayitem>
  <holidayitem>holiday4,</holidayitem>
  <holidayitem>holiday5,</holidayitem>
  <holidayitem>holiday6,</holidayitem>
  <holidayitem>holiday7,</holidayitem>
  <holidayitem>holiday8,</holidayitem>
  <holidayitem>holiday9,</holidayitem>
  <holidayitem>holiday10,</holidayitem>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value>	Model Supported	Value	Description
---------------------	-----------------	-------	-------------



P15200=<string>	GDS3710/GDS3705	Value format: name@holiday_mode,weekday0@start_time0@end_time0,weekday1@start_time1@end_time1,... Use (,) as separator when set multiple numbers. e.g.: AAA@0,0@0830 @1459 ,0@1600@1800, AAA is a revisable name for a schedule, Max. Length = 64 1 st @ represent holiday mode, 0-10. 2 st @ represent date of the week, 0-6, Sunday to Saturday 3 rd @ the pre-four digits represent start time of that period, 0830 represent 08:30 in 24 hour format; 2 nd @ the post-four digits represent end time of that period, 1459 represent 14:59 in 24 hour format.
P15201=<string>		
P15202=<string>		
P15203=<string>		
P15204=<string>		
P15205=<string>		
P15206=<string>		
P15207=<string>		
P15208=<string>		
P15209=<string>		

Notes:

- There should be **NO** overlap in any time period configured in the same day.
- (,) should be used to separate the different time period configured.

6. Holiday

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=holiday

Example:



```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P15301>0</P15301>
  <P15250>schedule_1,</P15250>
  <P15251>schedule_2,</P15251>
  <P15252>schedule_3,</P15252>
  <P15253>schedule_4,</P15253>
  <P15254>schedule_5,</P15254>
  <P15255>schedule_6,</P15255>
  <P15256>schedule_7,</P15256>
  <P15257>schedule_8,</P15257>
  <P15258>schedule_9,</P15258>
  <P15259>schedule_10,</P15259>
</Configuration>
```

Set:

<http://<servername>/goform/config?cmd=set&<parameter>=<value>...>

<parameter>=<value>	Model Supported	Value	Description
P15250=<string>	GDS3710/ GDS3705		Value format: name,start_date0@end_date0, start_date1@end_date1, Use (,) as separator when set multiple dates. e.g.: schedule_1,20180405@20180420, 20180421@20180425, schedule_1 is a revisable name for a schedule, Max. Length = 64
P15251=<string>			
P15252=<string>			
P15253=<string>			
P15254=<string>			
P15255=<string>			
P15256=<string>			
P15257=<string>			
P15258=<string>			
P15259=<string>			

- There should be **NO** overlap in any time period configured in the same day.
- (,) should be used to separate the different time period configured.



7. Date and Time

Supported Devices: **GDS3710/GDS3705**

Support Methods: **cmd = get/set**

Get:

```
http://<servername>/goform/config?cmd=get&type=date
```

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P64>16</P64>
  <P246></P246>
  <P5006>1</P5006>
  <P30>pool.ntp.org</P30>
  <P10006>1440</P10006>
  <P10004>0</P10004>
  <P10005/>
  <P10008>0</P10008>
  <P14040>2018</P14040>
  <P14041>4</P14041>
  <P14042>24</P14042>
  <P14043>15</P14043>
  <P14044>49</P14044>
  <P14045>16</P14045>
</Configuration>
```

Set:

```
http://<servername>/goform/config?cmd=set<parameter>=<value>...
```



<parameter>=<value>	Model Supported	Values	Description
P144=<int>	GDS3710/ GDS3705	<0 1>	Allow DHCP Option 42 to override NTP server
P64=<int>	GDS3710/ GDS3705	0 - 38 and 55,56	Time Zone: 1: GMT-12 (Eniwetok, Kwajalein) 2: GMT-11 (Midway Isl., Samoa) 3: GMT-10 (Hawaii, Aleutian Isl.) 4: GMT-09 (Alaska) 5: GMT-08 (Las Vegas, San Francisco, Vancouver) 6: GMT-07 (Calgary, Denver, Salt Lake City) 7: GMT-06 (Chicago, Dallas, Mexico City) 8: GMT-05 (Cuba) 9: GMT-05 (New York, Toronto, Washington DC) 10: GMT-04 (Paraguay) 11: GMT-04 (Chile) 12: GMT-04 (Charlottetown, Manaus) 55: GMT-04:30 (Caracas) 39: GMT-03:30 (Newfoundland) 13: GMT-03 (Argentina, Uruguay, Brasilia, Sao Paulo) 14: GMT-02 (Noronha, Mid-Atlantic) 15: GMT-01 (Azores, Cap Verde Isl.) 16: GMT (Dublin, Lisbon, London, Reykjavik) 17: GMT+01 (Amsterdam, Berlin, Rome, Stockholm) 18: GMT+02 (Athens, Helsinki, Istanbul, Riga) 19: GMT+02 (Egypt) 20: GMT+02 (Israel) 21: GMT+02 (Lebanon) 22: GMT+02 (Syria) 23: GMT+03 (Moscow, Riyadh) 24: GMT+03 (Iraq) 25: GMT+03:30 (Iran) 26: GMT+04 (Abu Dubai, Baku)



			27: GMT+04:30 (Kabul) 28: GMT+05 (Islamabad, Karachi, Tashkent) 29: GMT+05:30 (Bombay, Calcutta, New Delhi) 30: GMT+06 (Novosibirsk, Omsk) 31: GMT+07 (Bangkok, Hanoi, Jakarta) 32: GMT+08 (Beijing, Hong Kong, Shanghai, Taipei) 33: GMT+09 (Osaka, Sapporo, Tokyo) 34: GMT+09:30 (Adelaide, Darwin) 35: GMT+10 (Hobart) 36: GMT+10 (Canberra, Melbourne, Sydney) 37: GMT+11 (Solomon Isl.) 38: GMT+12 (Auckland, Wellington) 56: GMT+13 (Auckland, Wellington)
P10004=<int>	GDS3710/ GDS3705	<0 1>	Enable Daylight Saving Time 0: Disable 1: Enable
P14829=<string>	GDS3710/ GDS3705		Start time for Daylight Saving Time
P14103=<string>	GDS3710/ GDS3705		End time for Daylight Saving Time
P5006=<int>	GDS3710/ GDS3705	<0 1>	Enable NTP 0: Disable 1: Enable
P30=<string>	GDS3710/ GDS3705		NTP Server
P10006=<int>	GDS3710/ GDS3705	60 - 1440	Interval of time update (minute)



8. Network Settings

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

```
http://<servername>/goform/config?cmd=get&type=net
```

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P67>00:0B:82:B9:A9:1C</P67>
  <P8>0</P8>
  <P9>192</P9>
  <P10>168</P10>
  <P11>5</P11>
  <P12>202</P12>
  <P13>255</P13>
  <P14>255</P14>
  <P15>255</P15>
  <P16>0</P16>
  <P17>192</P17>
  <P18>168</P18>
  <P19>5</P19>
  <P20>1</P20>
  <P10107>0</P10107>
  <P21>192</P21>
  <P22>168</P22>
  <P23>5</P23>
  <P24>1</P24>
  <P25>192</P25>
  <P26>168</P26>
  <P27>5</P27>
```



```

<P28>1</P28>
<P1684>1</P1684>
<P51>0</P51>
<P87>0</P87>
</Configuration>

```

Set:

<http://<servername>/goform/config?cmd=set&<parameter>=<value>...>

<parameter>=<value>	Model Supported	Values	Description
P8=<int>	GDS3710/GDS3705	<0 1>	IP Address Mode 0: DHCP 1: Static IP
P9=<int>	GDS3710/GDS3705	0 - 255	IP Address P9.P10.P11.P12
P10=<int>	GDS3710/GDS3705	0 - 255	
P11=<int>	GDS3710/GDS3705	0 - 255	
P12=<int>	GDS3710/GDS3705	0 - 255	
P13=<int>	GDS3710/GDS3705	0 - 255	Subnet Mask P13.P14.P15.P16
P14=<int>	GDS3710/GDS3705	0 - 255	
P15=<int>	GDS3710/GDS3705	0 - 255	
P16=<int>	GDS3710/GDS3705	0 - 255	
P17=<int>	GDS3710/GDS3705	0 - 255	Gateway P17.P18.P19.P20
P18=<int>	GDS3710/GDS3705	0 - 255	
P19=<int>	GDS3710/GDS3705	0 - 255	
P20=<int>	GDS3710/GDS3705	0 - 255	
P10107=<int>	GDS3710/GDS3705	<0 1>	DNS
P21=<int>	GDS3710/GDS3705	0 - 255	DNS Server 1 P21.P22.P23.P24
P22=<int>	GDS3710/GDS3705	0 - 255	
P23=<int>	GDS3710/GDS3705	0 - 255	
P24=<int>	GDS3710/GDS3705	0 - 255	
P25=<int>	GDS3710/GDS3705	0 - 255	DNS Server 2
P26=<int>	GDS3710/GDS3705	0 - 255	



P27=<int>	GDS3710/GDS3705	0 - 255	P25.P26.P27.P28
P28=<int>	GDS3710/GDS3705	0 - 255	
P1684=<int>	GDS3710/GDS3705	<0 1>	Enable LLDP 0: Disable 1: Enable
P27004=<int>	GDS3705	<0 1>	Enable VLAN 0: Disable 1: Enable
P51=<int>	GDS3710/GDS3705	0-4094	Layer 2 QoS 802.1Q/VLAN Tag
P87=<int>	GDS3710/GDS3705	0-7	Layer 2 QoS 802.1p Priority Value

9. Access Settings

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=access

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P12054>1</P12054>
  <P901>443</P901>
  <P903>554</P903>
  <P12056>5</P12056>
  <P14832>5</P14832>
  <P14834>5</P14834>
  <P12052>1</P12052>
  <P12053>1</P12053>
```



```
<P276>1</P276>
<P27006>22</P27006>
</Configuration>
```

Set:

```
http://<servername>/goform/config?cmd=set<parameter>=<value>...
```

<parameter>=<value>	Model Supported	Values	Description
P12054=<int>	GDS3710/GDS3705	<0 1>	Web Access Mode 0: HTTP 1: HTTPS
P901=<int>	GDS3710/GDS3705	HTTP: 80 - 65535 HTTPS: 443 - 65535	Web Port
P15406=<int>	GDS3710	<0 1>	MJPEG Authentication Mode 0: Challenge+Response 1: Basic
P903=<int>	GDS3710	554 - 65535	RTSP Port
P12056=<int>	GDS3710/GDS3705	3 - 60	User Login Timeout (minute)
P14832=<int>	GDS3710/GDS3705	3 - 10	Max. Number of Login Attempts
P14834=<int>	GDS3710/GDS3705	5 - 60	Login error lockout time (minute)
P15473=<int>	GDS3710/GDS3705	<0 1>	Disable Web Access 0: Disable 1: Enable
P12053=<int>	GDS3710/GDS3705	<0 1>	Enable UPnP Discovery 0: Disable 1: Enable



P15469=<int>	GDS3710	<0 1>	Enable Anonymous LiveView 0:Disable 1:Enable
P276=<int>	GDS3710/GDS3705	<0 1>	Enable SSH 0: Disable 1: Enable
P27006=<int>	GDS3710/GDS3705	22 - 65535	SSH Port
P15505=<string>	GDS3710/GD3705		GDSManager Configuration Password MIN length is 1 MAX length is 32
P15512=<string>	GDS3710		RTSP Password MIN length is 1 MAX length is 32

10. User Management

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = set**

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value> >	Model Supported	Values	Description
oldpwd=<string>			Oldpwd: Old Password, Max. Length = 32
Newpwd=<string>			Newpwd: New Password Max. Length = 32
cfmnewpwd=<string>			cfmnewpwd: Confirmed New Password; Max. Length = 32



	GDS3710/ GDS3705		e.g.: cmd=set&oldpwd=123&newpwd=admin&cfmnewpwd=admin Oldpwd、Newpwd、cfmnewpwd , three must be set at the same time, and Newpwd must be the same as cfmnewpwd. Otherwise invalid.
P10124=<string>			Password Recover Email Address

11.SIP Settings

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=sip

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P12054>1</P12054>
  <P499>0</P499>
  <P407/>
  <P402/>
  <P2412/>
  <P403/>
  <P2433/>
  <P408>0</P408>
  <P404/>
  <P405/>
  <P409>0</P409>
  <P76/>
  <P412>60</P412>
```



```

<P413>5060</P413>
<P39>5004</P39>
<P10451>300</P10451>
<P14847>15</P14847>
<P448>0</P448>
<P8000>1</P8000>
<P8004>0</P8004>
<P2402>1</P2402>
<P2403>0</P2403>
<P1309>0</P1309>
<P10453>1</P10453>
<PlpCallSave>1</PlpCallSave>
<P10454>0</P10454>
<P8001>0</P8001>
<P8003>0</P8003>
<P411>1</P411>
<P443>0</P443>
<P15427>0</P15427>
<P424>100</P424>
<P406/>
<P281>s1pphone</P281>
</Configuration>

```

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

- GDS37XX Account Settings**

<parameter>=<value>				Values	Model Supported	Description
Account 1	Account 2	Account 3	Account 4			
P271=<int>	P401=<int>	P501=<int>	P601=<int>	<0 1>	GDS3710/ GDS3705	Account Active (In Use). 0: No 1: Yes
P210=<int>	P499=<int>	P599=<int>	P699=<int>	<0 1>	GDS3710/ GDS3705	SIP Registration Status(Read Only)
P3=<string>	P407=<string>	P507=<string>	P607=<string>		GDS3710/ GDS3705	Account Name Max. Length = 64



P47=<string>	P402=<string>	P502=<string>	P602=<string>		GDS3710/ GDS3705	SIP Server Max. Length = 255
P2312=<string> >	P2412=<string>	P2512=<string>	P2612=<string> >		GDS3710/ GDS3705	Secondary SIP Server Max. Length = 255
P48=<string>	P403=<string>	P503=<string>	P603=<string>		GDS3710/ GDS3705	Outbound Proxy Max. Length = 255
P2333=<string> >	P2433=<string>	P2533=<string>	P2633=<string> >		GDS3710/ GDS3705	Backup Outbound Proxy Max. Length = 255
P103=<int>	P408=<int>	P508=<int>	P608=<int>	<0 1 2>	GDS3710/ GDS3705	DNS Mode 0: A Record 1: SRV 2: NAPTR/SRV
P35=<string>	P404=<string>	P504=<string>	P604=<string>		GDS3710/ GDS3705	SIP User ID Max. Length = 255
P36=<string>	P405=<string>	P505=<string>	P605=<string>		GDS3710/ GDS3705	Authenticate ID Max. Length = 255
P34=<string>	P406=<string>	P506=<string>	P606=<string>		GDS3710/ GDS3705	Authenticate password Max. Length = 255
P63=<int>	P409=<int>	P509=<int>	P609=<int>	<0 1 2>	GDS3710/ GDS3705	TEL URI 0: Disabled 1: User = Phone 2: Enable
P32=<int>	P412=<int>	P512=<int>	P612=<int>	60 - 64800	GDS3710/ GDS3705	Registration Expiration(m)
P2330=<int>	P2430=<int>	P2530=<int>	P2630=<int>	P2630= <int>	GDS3710/ GDS3705	Re-register before Expiration(s)
P40=<int>	P413=<int>	P513=<int>	P613=<int>	1 - 65535	GDS3710/ GDS3705	Local SIP Port
P130=<int>	P448=<int>	P548=<int>	P648=<int>	<0 1 2>	GDS3710/ GDS3705	SIP Transport 0: UDP 1: TCP 2: TLS/TCP
P2302=<int>	P2402=<int>	P2502=<int>	P2602=<int>	<0 1>	GDS3710/ GDS3705	Enable DTMF RFC2833



						0: Disable 1: Enable
P2303=<int>	P2403=<int>	P2503=<int>	P2603=<int>	<0 1>	GDS3710/ GDS3705	Enable DTMF SIP INFO 0: Disable 1: Enable
P79=<int>	P496=<int>	P596=<int>	P696=<int>		GDS3710/ GDS3705	DTMF Payload Type
P490=<int>	P1309=<int>	P590=<int>	P690=<int>	<0 1>	GDS3710/ GDS3705	Enable Keep Alive 0: Disable 1: Enable
P52=<int>	P414=<int>	P514=<int>	P614=<int>	<0 1 2 3 4>	GDS3710/ GDS3705	NAT Traversal 0: No 1: STUN 2: Keep Alive 3: UPnP 4: Auto 5: VPN
P81=<int>	P411=<int>	P511=<int>	P611=<int>	<0 1>	GDS3710/ GDS3705	Unregister On Reboot 0: Disable 1: Enable
P183=<int>	P443=<int>	P543=<int>	P643=<int>	<0 1 2>	GDS3710/ GDS3705	Enable SRTP 0: Disable 1: Enable but not Forced 2: Enable and Forced
P198=<int>	P424=<int>	P524=<int>	P624=<int>	<100 1 02>	GDS3710/ GDS3705	Special Feature 100: Standard 102: Broadsoft 129: Telefonica Spain
P2305=<int>	P2405=<int>	P2505=<int>	P2605=<int>	<0 1 2>	GDS3710/ GDS3705	Outbound Proxy Mode 0:in route 1:not in route 2:always send to



P2306=<int>	P2406=<int>	P2506=<int>	P2606=<int>	<0 1>	GDS3705	Validate Incoming Messages 0:No 1:Yes
P2492=<int>	P2392=<int>	P2592=<int>	P2692=<int>	<0 1 2>	GDS3710/ GDS3705	Enable RTCP 0: Disable 1: RTCP 2: RTCP-XR
P293=<int>	P462=<int>	P562=<int>	P662=<int>	<96-127 & !=101>	GDS3710	H.264 Payload Type
P2347<int>	P2447<int>	P2547<int>	P2647<int>	<0 1>	GDS3710/ GDS3705	Accept Incoming SIP from Proxy Only 0:No 1:Yes
P26061=<int>	P26161=<int>	P26261=<int>	P26361=<int>	<0 1 2>	GDS3710/ GDS3705	Add MAC in User-Agent 0: No 1: Yes, except REGISTER 2: Yes to all SIP
P37=<int>	P486=<int>	P586=<int>	P686=<int>	1 - 64	GDS3710/ GDS3705	Voice Frames Per TX
P57=<int>	P451=<int>	P551=<int>	P651=<int>	<0 8 9 18>	GDS3710/ GDS3705	Preferred Vocoder 1 0: PCMU 8: PCMA 9: G.722 18: G729A/B
P58=<int>	P452=<int>	P552=<int>	P652=<int>	<0 8 9 18>	GDS3710/ GDS3705	Preferred Vocoder 2 0: PCMU 8: PCMA 9: G.722 18: G729A/B
P59=<int>	P453=<int>	P553=<int>	P653=<int>	<0 8 9 18>	GDS3710/ GDS3705	Preferred Vocoder 3 0: PCMU 8: PCMA



						9: G.722 18: G729A/B
P60=<int>	P454=<int>	P554=<int>	P654=<int>	<0 8 9 18>	GDS3710/ GDS3705	Preferred Vocoder 4 0: PCMU 8: PCMA 9: G.722 18: G729A/B
P26058=<int>	P26158=<int>	P26258=<int>	P26358=<int>	<0 1>	GDS3710/ GDS3705	Use P-Access- Network-Info Header 0: Disable 1: Enable
P29061=<int>	P29161=<int>	P29261=<int>	P29361=<int>	<0 1>	GDS3710/ GDS3705	Codec Negotiation Priority 0: Caller 1: Callee

Phone Settings

<parameter>=<value>	Values	Supported Model	Description
P76=<string>		GDS3710/ GDS3705	STUN Server
P39=<int>	1 - 65535	GDS3710/ GDS3705	Local SIP Port
P10451=<int>	0 - 65535	GDS3710/ GDS3705	Auto On-Hook Timer (Seconds)
P29610=<int>	48- 10000	GDS3710/ GDS3705	Use Random Port
P14847=<int>	0 - 90	GDS3710/ GDS3705	Ring Timeout
P280=<string>		GDS3710/ GDS3705	SIP TLS Certificate
P279=<string>		GDS3710/ GDS3705	SIP TLS Private Key
P281=<string>		GDS3710/ GDS3705	SIP TLS Private Key Password
P10453=<int>	<0 1>	GDS3710/ GDS3705	Enable Direct IP Call



			0: Disable 1: Enable
P8001=<int>	<0 1>	GDS3710/ GDS3705	Enable two-way SIP Calling 0: Disable 1: Enable
P8003=<int>	<0 1>	GDS3710	SIP Proxy Compatibility Mode 0: Disable 1: Enable
P15476=<int>	<0 1>	GDS3710/ GDS3705	Allow Reset Via SIP NOTIFY 0: Disable (default) 1 : Enable
P957=<int>	<0 1>	GDS3710	SIP Packetization Compatibility Mode 0: Disable 1: Enable
P2495=<int>	<0 1>	GDS3710 (for BroadSoft)	Enable Session Timer 0: Disable 1: Enable

12. White List

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/add/set/del**

Get:

http://<servername>/goform/config?cmd=get&type=sip

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
```



```
<P10460>1111</P10460>
<P10460>2222</P10460>
<P10460>3333</P10460>
</Configuration>
```

Set:

```
http://<servername>/goform/config?cmd=set&P10460=num
```

Add:

```
http://<servername>/goform/config?cmd=add&P10460=num
```

Del:

```
http://<servername>/goform/config?cmd=del&P10460=num1,num2,num3, ...
```

- **GDS37XX White List**

<parameter>=<value>				Values	Description
Account 1	Account 2	Account 3	Account 4		
P10410=<int>	P10454=<int>	P10420=<int>	P10430=<int>	<0 1>	Enable White List 0: Disable 1: Enable
P10411=<string>	P10460=<string>	P10421=<string>	P10431=<string>		Use (,) as separator when deleting multiple numbers.



13. Video Settings

Supported Devices: **GDS3710 only**

Supported Methods: **cmd = get/set**

Get:

```
http://<servername>/goform/config?cmd=get&type=video
```

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<Configuration>
```

```
<ResCode>0</ResCode>
```

```
<RetMsg>OK</RetMsg>
```

```
<P10572>1</P10572>
```

```
<P12306>96</P12306>
```

```
<P12313>1</P12313>
```

```
<P12307>1025</P12307>
```

```
<P12315>4096</P12315>
```

```
<P12904>30</P12904>
```

```
<P12924>0</P12924>
```

```
<P12311>2</P12311>
```

```
<P12312>80</P12312>
```

```
<P12706>96</P12706>
```

```
<P12713>1</P12713>
```

```
<P12707>1022</P12707>
```

```
<P12708>512</P12708>
```

```
<P12709>25</P12709>
```

```
<P12710>0</P12710>
```

```
<P12711>2</P12711>
```

```
<P12712>80</P12712>
```

```
<P13106>96</P13106>
```

```
<P13113>1</P13113>
```

```
<P13107>0</P13107>
```

```
<P13108>256</P13108>
```

```
<P13109>30</P13109>
```

```
<P13110>0</P13110>
```

```
<P13111>2</P13111>
```

```
<P13112>80</P13112>
```



</Configuration>

Set:

<http://<servername>/goform/config?cmd=set&<parameter>=<value>...>

<parameter>=<value>	Values	Description
Stream 1		
P12306=<int>	<26 96>	Video Codec: 26: H.264 96: MJPEG
P12313	<0 1 2>	Profile: 0: Baseline 1: Main Profile 2: High Profile
P12307=<int>	<1022 1025>	Resolution: 1025: 1920*1080 (16:9) 1022: 1280*720 (16:9)
P12315=<int>	<1024 2048 4096>	Video Bit Rate (kbps) 1024: 1024kb 2048: 2048kb 4096: 4096kb
P12904=<int>	<5 10 15 20 25 30>	Max. Frame Rate (fps) 5: 5fps 10: 10fps 15: 15fps 20: 20fps 25: 25fps 30: 30fps
P12924=<int>	<0 1>	Video Bit Rate Control 0: Constant Bit Rate (CBR) 1: Variable Bit Rate (VBR)
P12311=<int>	<0 1 2 3 4>	Image Quality (Valid only when VBR selected) 0: Very High 1: High 2: Normal 3: Low 4: Very Low



P12312=<int>	1 - 100	I-Frame Interval
Stream 2		
P12706=<int>	<26 96>	Video Codec: 26: H.264 96: MJPEG
P12713	<0 1 2>	Profile: 0: Baseline 1: Main Profile 2: High Profile
P12707=<int>	<1022 1 1010>	Resolution: 1022: 1280*720 (16:9) 1: 640*480 (4:3) 1010: 480*272 (16:9)
P12708=<int>	<256 512 1024>	Video Bit Rate (kbps) 256: 256kb 512: 512kb 1024: 1024kb
P12709=<int>	<5 10 15 20 25>	Max. Frame Rate (fps) 5: 5fps 10: 10fps 15: 15fps 20: 20fps 25: 25fps
P12710=<int>	<0 1>	Video Bit Rate Control 0: Constant Bit Rate (CBR) 1: Variable Bit Rate (VBR)
P12711=<int>	<0 1 2 3 4>	Image Quality (Valid only when VBR selected) 0: Very High 1: High 2: Normal 3: Low 4: Very Low
P12712=<int>	1 - 100	I-Frame Interval
Stream 3		
P13106=<int>	<26 96>	Video Codec: 26: H.264 96: MJPEG



P13113=<int>	<0 1 2>	Profile: 0: Baseline 1: Main Profile 2: High Profile
P13107=<int>	<0 1008>	Resolution: 1008: 352*240 (CIF) 0: 320*240 (4:3)
P13108=<int>	<128 256 512>	Video Bit Rate (kbps) 128: 128kb 256: 256kb 512: 512kb
P13109=<int>	<5 10 15 20 25 30>	Max. Frame Rate (fps) 5: 5fps 10: 10fps 15: 15fps 20: 20fps 25: 25fps 30: 30fps
P13110=<int>	<0 1>	Video Bit Rate Control 0: Constant Bit Rate (CBR) 1: Variable Bit Rate (VBR)
P13111=<int>	<0 1 2 3 4>	Image Quality (Valid only when VBR selected) 0: Very High 1: High 2: Normal 3: Low 4: Very Low
P13112=<int>	1 - 100	I-Frame Interval



14. On Screen Display (OSD) Settings

Supported Devices: **GDS3710 only**

Support **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=osd

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P10044>1</P10044>
  <P10045>0</P10045>
  <P10001>1</P10001>
  <P10007>0</P10007>
  <P10040/>
  <P10041>0</P10041>
  <P10046>0</P10046>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value>	Values	Description
P10044=<int>	<0 1>	Display Time 0: Disable 1: Enable
P10045=<int>	<0 1>	Display Text 0: Disable



		1: Enable
P10001=<int>	<0 1 2>	OSD Date Format 0: Year – Month - Date 1: Month – Date - Year 2: Date – Month - Year
P10007=<int>	<0 1>	OSD Time Format 0: 24 hours 1: 12 hours
P10040=<string>		OSD Text Length Max. Length = 32
P10041=<int>	<0 1 2 3>	OSD Position for Date/Time 0: Top Left 1: Bottom Left 2: Top Right 3: Bottom Right
P10046=<int>	<0 1 2 3>	OSD Position for Text 0: Top Left 1: Bottom Left 2: Top Right 3: Bottom Right



15. CMOS Settings

Supported Devices: **GDS3710 only**

Supported Methods: **cmd = get/set**

Get:

`http://<servername>/goform/config?cmd=get&type=cmos`

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P10572>1</P10572>
  <P10573>0</P10573>
  <P14565>10</P14565>
  <P12314>1</P12314>
  <P10503>0</P10503>
</Configuration>
```

Set:

`http://<servername>/goform/config?cmd=set&<parameter>=<value>...`

<parameter>=<value>	Values	Description
P10572=<int>	<1 2 3>	Mode: 1: Normal 2: Low Light 3: WDR (Wide Dynamic Range)
P10573=<int>	<0 1>	LDC (Lens Distortion Correction) 0: Disable / OFF 1: Enable / ON



P12314=<int>	<0 1>	Power Frequency (For Avoiding Video Flicker) 0: 50HZ 1: 60HZ
P10503=<int>	<0 30 60 125 250 500 1000 2000 5000 1000 0>	Shutter Speed: 0: Auto 30: (1/30)s 60: (1/60)s 125: (1/125)s 250: (1/250)s 500: (1/500)s 1000: (1/1000)s 2000: (1/2000)s 5000: (1/5000)s 10000: (1/10000)s



16.Audio Settings

Supported Devices: **GDS3710/GDS3705**

Support Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=audio

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>

<Configuration>

  <ResCode>0</ResCode>

  <RetMsg>OK</RetMsg>

  <P14000>1</P14000>

  <P14002>13</P14002>

  <P14003>4</P14003>

  <P14836>4</P14836>

  <P14835>4</P14835>

</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value>	Model Supported	Values	Description
P14000=<int>	GDS3710/GDS3705	<1 2 4>	Audio Codec: 1: PCMU 2: PCMA 4: G722
P14003=<int>	GDS3710/GDS3705	GDS3710: 0 – 6 GDS3705: 0 - 7	System Volume
P14835=<int>	GDS3710/GDS3705	GDS3710: 0 – 6 GDS3705: 0 - 7	Door Bell Volume



17. Privacy Masks

Supported Devices: **GDS3710 only**

Supported Methods: **cmd = get/set**

Get:

`http://<servername>/goform/config?cmd=get&type=privacy`

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>

  <ResCode>0</ResCode>

  <RetMsg>OK</RetMsg>

  <P14225>0@0,0,0,0;0@0,0,0,0;0@0,0,0,0;0@0,0,0,0;</P14225>

</Configuration>
```

Set:

`http://<servername>/goform/config?cmd=set&<parameter>=<value>...`

<parameter>=<value>	Values	Description
P14225=<string>		Region for Privacy Masks <u>Format:</u> Enable @Top Left x1 coordinates, Top Left y1 coordinates; Bottom Right x2 coordinates, Bottom Right y2 coordinates. e.g.: 0@0,0,0,0; 0@0,0,0,0; 0@0,0,0,0; 0@0,0,0,0; Digit before @ represents function, 0: Disable/Hide 1: Enable/Display Coordinates are separated by (,)



Region is separated by (;)

Please Do remember the last; and configure the 4 regions at the same time all at once.

Rules:

0 <= x1, x2 <= 704; 0 <= y1, y2 <= 576; x1 <= x2; y1 <= y2

18.Alarm Config

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

```
http://<servername>/goform/config?cmd=get&type=event
```

Example: For GDS3710

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P15450>0</P15450>
  <P15451>0</P15451>
  <P15452>0</P15452>
  <P15508>1</P15508>
  <P15509>0</P15509>
  <P12054>1</P12054>
  <P10250>0</P10250>
  <P14221>0</P14221>
  <P14222>1</P14222>
  <P14223>50</P14223>
  <P14224>[0,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,0]</P14224>
  <P14320>0</P14320>
  <P14321>0</P14321>
  <P14322>1</P14322>
  <P14325>0</P14325>
  <P14326>0</P14326>
```



<P14327>1</P14327>
<P903>554</P903>
<P3>admin</P3>
<P2>PzBmH4qQ</P2>
<P14200>schedule1,0@0000@2359,</P14200>
<P14201>schedule2,0@0000@2359,</P14201>
<P14202>schedule3,0@0000@2359,</P14202>
<P14203>schedule4,0@0000@2359,</P14203>
<P14204>schedule5,0@0000@2359,</P14204>
<P14205>schedule6,0@0000@2359,</P14205>
<P14206>schedule7,0@0000@2359,</P14206>
<P14207>schedule8,0@0000@2359,</P14207>
<P14208>schedule9,0@0000@2359,</P14208>
<P14209>schedule10,0@0000@2359,</P14209>
<P14300>profile1@0,0,0,0,0,0,</P14300>
<P14301>profile2@0,0,0,0,0,0,</P14301>
<P14302>profile3@0,0,0,0,0,0,</P14302>
<P14303>profile4@0,0,0,0,0,0,</P14303>
<P14304>profile5@0,0,0,0,0,0,</P14304>
<P14305>profile6@0,0,0,0,0,0,</P14305>
<P14306>profile7@0,0,0,0,0,0,</P14306>
<P14307>profile8@0,0,0,0,0,0,</P14307>
<P14308>profile9@0,0,0,0,0,0,</P14308>
<P14309>profile10@0,0,0,0,0,0,</P14309>
<P10467>0</P10467>
<P10466/>
<P14341>5</P14341>
<P10468>1</P10468>



```

<P10469/>

<P14350>0</P14350>

<P14355>1</P14355>

<P14354/>

<P14825>1</P14825>

<P14826>1</P14826>

<P14568>0@0@0@0@0</P14568>

</Configuration>

```

Example: For GDS3705

```

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>

  <ResCode>0</ResCode>

  <RetMsg>OK</RetMsg>

  <P12054>1</P12054>

  <P14320>0</P14320>

  <P15431>0</P15431>

  <P14321>0</P14321>

  <P14322>1</P14322>

  <P14325>0</P14325>

  <P14326>0</P14326>

  <P14327>1</P14327>

  <P903>554</P903>

  <P2>admin</P2>

  <ALMIN1_STATUS>1</ALMIN1_STATUS>

  <ALMIN2_STATUS>1</ALMIN2_STATUS>

  <P14200>schedule1,0@0000@2359,</P14200>

  <P14201>schedule2,0@0000@2359,</P14201>

  <P14202>schedule3,0@0000@2359,</P14202>

  <P14203>schedule4,0@0000@2359,</P14203>

```



<P14204>schedule5,0@0000@2359,</P14204>
<P14205>schedule6,0@0000@2359,</P14205>
<P14206>schedule7,0@0000@2359,</P14206>
<P14207>schedule8,0@0000@2359,</P14207>
<P14208>schedule9,0@0000@2359,</P14208>
<P14209>schedule10,0@0000@2359,</P14209>
<P14300>profile1@0,0,0,0,0,0,</P14300>
<P14301>profile2@0,0,0,0,0,0,</P14301>
<P14302>profile3@0,0,0,0,0,0,</P14302>
<P14303>profile4@0,0,0,0,0,0,</P14303>
<P14304>profile5@0,0,0,0,0,0,</P14304>
<P14305>profile6@0,0,0,0,0,0,</P14305>
<P14306>profile7@0,0,0,0,0,0,</P14306>
<P14307>profile8@0,0,0,0,0,0,</P14307>
<P14308>profile9@0,0,0,0,0,0,</P14308>
<P14309>profile10@0,0,0,0,0,0,</P14309>
<P10467>0</P10467>
<P14341>5</P14341>
<P10468>1</P10468>
<P10469>(null)</P10469>
<P14350>0</P14350>
<P14355>1</P14355>
<P14354>(null)</P14354>
<P14825>1</P14825>
<P14826>1</P14826>
<P15406>1</P15406>
<P15409>1</P15409>
<P15407>0</P15407>
<P15408>1</P15408>



<P14568>0@0@0@0@0</P14568>

</Configuration>

Set:

http://ip:port/goform/config?cmd=set&PXXXXX=<value>

<parameter>=<value>	Model Supported	Values	Description
P10250=<int>	GDS3710	<0 1>	Enable Motion Detection Alarm 0: Disable 1: Enable
P14223=<int>	GDS3710	0 – 100	Sensitivity of Motion Detection
P14224=<string>	GDS3710		Region of Motion Detection <u>Format:</u> [Top Left x1 coordinates, Top Left y1 coordinates, Bottom Right x2 coordinates, Bottom Right y2 coordinates] e.g.: [1,5,7,15],[11,8,16,17],[19,9,26,19],[0,0, 0,0], [0,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,0] Coordinates are separated by (,) Region is separated by (;) The 8 regions must be configured at the same time all at once. Rules: 0 <= x1, x2 <= 704; 0 <= y1, y2 <= 576; x1 <= x2; y1 <= y2
P14221=<int>	GDS3710	<0 1 2 3 4 5 6 7 8 9 10>	Select Alarm Schedule 0: All Day 1: Schedule1 2: Schedule2



			3: Schedule3 4: Schedule4 5: Schedule5 6: Schedule6 7: Schedule7 8: Schedule8 9: Schedule9 10: Schedule10
P14222=<int>	GDS3710	<1 2 3 4 5 6 7 8 9 10>	Alarm Action Profile 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P14320=<int>	GDS3710/GDS3705	<0 1 2>	Action of Alarm Input Channel 1 0: Disable 1: Alarm Input 2: Open Door 3: Abnormal Door Control 4: Door Status Check
P15451=<int>	GDS3710/GDS3705	<0 1 2 3>	Digit Input 1 Open Door Options 0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15508=<int>	GDS3710/GDS3705	<0 1>	Digit Input 1 Abnormal Door Control Options 0: Door 1 1: Door 2
P15431=<int>	GDS3705	<0 1>	Input Digit 1 State 0: Normal Open 1: Normal Close



P14321=<int>	GDS3710/GDS370 5	<0 1 2 3 4 5 6 7 8 9>	Select Alarm Schedule 1 0: All Day 1: Schedule1 2: Schedule2 3: Schedule3 4: Schedule4 5: Schedule5 6: Schedule6 7: Schedule7 8: Schedule8 9: Schedule9 10: Schedule10
P14322=<int>	GDS3710/GDS370 5	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 1 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P14325=<int>	GDS3710/GDS370 5	<0 1 2 3>	Action of Alarm Input Channel 1 0: Disable 1: Alarm Input 2: Open Door 3: Abnormal Door Control 4: Door Status Check
P15452=<int>	GDS3710/GDS370 5	<0 1 2 3>	Digit Input 2 Open Door Options 0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None



P15509=<int>	GDS3710/GDS3705	<0 1>	Digit Input 1 Abnormal Door Control Options 0: Door 1 1: Door 2
P15432=<int>	GDS3705	<0 1>	Input Digit 2 State 0: Normal Open 1: Normal Close
P14326=<int>	GDS3710/GDS3705	<0 1 2 3 4 5 6 7 8 9>	Select Alarm Schedule 2 0: All Day 1: Schedule1 2: Schedule2 3: Schedule3 4: Schedule4 5: Schedule5 6: Schedule6 7: Schedule7 8: Schedule8 9: Schedule9 10: Schedule10
P14327=<int>	GDS3710/GDS3705	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 2 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P14341=<int>	GDS3710/GDS3705	<5 10 15 20 25 30>	Alarm Output Duration (Seconds) 5: 5s (Default) 10: 10s 15: 15s 20: 20s



			25: 25s 30: 30s
P10467=<int>	GDS3710/GDS370 5	<0 1>	Enable Hostage Code 0: Disable 1: Enable
P10466=<string>	GDS3710/GDS370 5		Hostage Code: All digits string Max. Length = 10
P10468=<int>	GDS3710/GDS370 5	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P14350=<int>	GDS3710/GDS370 5	<0 1>	Enable Tamper Alarm 0: Disable 1: Enable
P14355=<int>	GDS3710/GDS370 5	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P14825=<int>	GDS3710/GDS370 5	<0 1>	Enable Keypad Input Error Alarm 0: Disable



			1: Enable
P14826=<int>	GDS3710/GDS3705	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P15407=<int>	GDS3710/GDS3705	<0 1>	Enable Non-scheduled Access Alarm 0: Disable 1: Enable
P15408=<int>	GDS3710/GDS3705	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5 6: profile6 7: profile7 8: profile8 9: profile9 10: profile10
P15515=<int>	GDS3710/GDS3705	<0 1>	Enable Unauthorized Door Opening Attempt Alarm
P15516=<int>	GDS3710/GDS3705	<1 2 3 4 5 6 7 8 9 10>	Select Alarm Action Profile 1: profile1 2: profile2 3: profile3 4: profile4 5: profile5



			6: profile6
			7: profile7
			8: profile8
			9: profile9
			10: profile10



19. Alarm Schedule Configuration

Supported Devices: **GDS3710/GDS3705**

Support **cmd = get/set**

Get:

`http://<servername>/goform/config?cmd=get&type=alarm_schedule`

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P14200>schedule1,0@0000@2359,</P14200>
  <P14201>schedule2,0@0830@1459,0@1500@1820,</P14201>
  <P14202>schedule3,0@0000@2359,</P14202>
  <P14203>schedule4,0@0000@2359,</P14203>
  <P14204>schedule5,0@0000@2359,</P14204>
  <P14205>schedule6,0@0000@2359,</P14205>
  <P14206>schedule7,0@0000@2359,</P14206>
  <P14207>schedule8,0@0000@2359,</P14207>
  <P14208>schedule9,0@0000@2359,</P14208>
  <P14209>schedule10,0@0000@2359,</P14209>
</Configuration>
```

Set:

`http://<servername>/goform/config?cmd=set&<parameter>=<value>...`

<parameter>=<value>	Values	Description
P14200=<string>		e.g.: <P14201>schedule2,0@0830@1459,0@1500@18
P14201=<string>		20,</P14201>



P14202=<string>		schedule2 is a revisable name for a time period, Max. Length = 20
P14203=<string>		
P14204=<string>		1 st @ represent date of the week, 0-6, Sunday to Saturday
P14205=<string>		2 nd @ the pre-four digits represent start time of that period, 0830 represent 08:30 in 24 hour format;
P14206=<string>		2 nd @ the post-four digits represent end time of that period, 1459 represent 14:59 in 24 hour format.
P14207=<string>		<u>NOTE:</u>
P14208=<string>		There should be NO overlap in any time period configured in the same day.
P14209=<string>		(,) should be used to separate the different time period configured.



20. Alarm Action Configuration

Supported Devices: **GDS3710/GDS3705**

Support **cmd = get/set**

Get:

`http://<servername>/goform/config?cmd=get&type=alarm_profile`

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P14827>0</P14827>
  <P14300>profile1@0,0,0,0,0,0</P14300>
  <P14301>profile2@0,0,0,0,0,0</P14301>
  <P14302>profile3@0,0,0,0,0,0</P14302>
  <P14303>profile4@0,0,0,0,0,0</P14303>
  <P14304>profile5@0,0,0,0,0,0</P14304>
  <P14305>profile6@0,0,0,0,0,0</P14305>
  <P14306>profile7@0,0,0,0,0,0</P14306>
  <P14307>profile8@0,0,0,0,0,0</P14307>
  <P14308>profile9@0,0,0,0,0,0</P14308>
  <P14309>profile10@0,0,0,0,0,0</P14309>
</Configuration>
```

Set:

`http://<servername>/goform/config?cmd=set&<parameter>=<value>...`

<parameter>=<value>	Values	Description
P14300=<string>		e.g.: <P14300>profile1@0,0,0,0,0,0</P14300>



P14301=<string>		profile1 is revisable name of alarm action, Max. Length = 20
P14302=<string>		
P14303=<string>		1 st digit after @ represents whether "Upload to Alarm Center": 0: Disable 1: Enable
P14304=<string>		2 nd digit after @ represents whether "Sound Alarm" 0: Disable 1: Enable
P14305=<string>		3 rd digit after @ represents whether "Voice Alarm to SIP Phone"
P14306=<string>		0: Disable 1: Enable
P14307=<string>		4 th digit after @ represents whether "Alarm Output" 0: Disable 1: Enable
P14308=<string>		5 th digit after @ represents whether "Send Email" 0: Disable 1: Enable
P14309=<string>		6 th digit after @ represents whether "Upload JPEG" snapshot 0: Disable 1: Enable
test_alarm_action=<int>	1-10	Test for Alarm Action



21. Alarm Phone List

Supported Devices: **GDS3710/GDS3705**

Support **cmd = get/add/del**

Get:

http://<servername>/goform/config?cmd=get&type=sip

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P10459>111</P10459>
  <P10459>aaa</P10459>
</Configuration>
```

Add:

http://<servername>/goform/config?cmd=add&P10459=num1,num2, ...

<parameter>=<value>	Values	Description
P10459=<string>		Alarm Phone

Del:

http://<servername>/goform/config?cmd=del&P10459=num1,num2,num3, ...

<parameter>=<value>	Values	Description
P10459=<string>		(,) used as a separator when multiple alarm numbers deleted.



22.Email Settings

Supported Devices: **GDS3710/GDS370**

Support **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=sntp

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>

  <ResCode>0</ResCode>

  <RetMsg>OK</RetMsg>

  <P10120>0</P10120>

  <P10121>smtp.google.com</P10121>

  <P10122>25</P10122>

  <P10123>kevin@google.com</P10123>

  <P10124>kevin@google.com</P10124>

  <P14348>kevin@google.com</P14348>

  <P14349>kevin@google.com</P14349>

  <P10127>kevin</P10127>

  <P10129>0</P10129>

  <P10128r>123</P10128r>

  <P10128>Y</P10128>

</Configuration>
```



Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value>	Values	Description
P10121=<string>		SMTP Mail Server
P10122=<string>		Port of SMTP Server
P10123=<string>		Sender's email address. Max. Length = 127
P10127=<string>		Sender's User Name, Max. Length = 63
P10128=<string>		Sender's email password, Max. Length = 63
P14348=<string>		Alarm to email address 1, Max. Length = 127
P14349=<string>		Alarm to email address 2, Max. Length = 127
P10129=<int>	<0 1>	SSL Encryption 0: Disable 1: Enable



23.FTP Settings

Supported Devices: **GDS3710 only**

Supported Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=ftp

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P12054>1</P12054>
  <P10140>1</P10140>
  <P14113>1</P14113>
  <P14114/>
  <P14115>21</P14115>
  <P14116/>
  <P14118>/</P14118>
  <P14330/>
  <P14332/>
  <P14117/>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set<parameter>=<value>...

<parameter>=<value>	Values	Description
P14113=<int>	<0 1>	Storage Server Type 0: FTP



		1: Central Storage (GDSManager Configure)
P14114=<string>		FTP Server IP or FQDN, Max. Length = 255
P14115=<int>		FTP Server Port, Max. Length = 5
P14116=<string>		FTP User Name, Max. Length = 63
P14118=<string>		FTP Path, Max. Length = 255



24. Upgrade Configuration

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

```
http://<servername>/goform/config?cmd=get&type=upgrade
```

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>

<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P12054>1</P12054>
  <P6767>1</P6767>
  <P192>fm.grandstream.com/gs</P192>
  <P6768/>
  <P232/>
  <P233/>
  <P212>2</P212>
  <P237>fm.grandstream.com/gs</P237>
  <P1360/>
  <P234/>
  <P235/>
  <P6769/>
  <P1361/>
  <P1359/>
  <version_limit>1.0.3.1</version_limit>
  <P193>10080</P193>
  <P194>1</P194>
  <P145>1</P145>
  <P1414>0</P1414>
```



```
<P8463>0</P8463>
</Configuration>
```

Set:

```
http://<servername>/goform/config?cmd=set<parameter>=<value>...
```

<parameter>=<value>	Values	Description
P6767=<int>	<0 1 2>	Firmware Upgrade Method 0: TFTP 1: HTTP 2: HTTPS
P192=<string>		Firmware Server Path
P6768=<string>		Firmware HTTP/HTTPS User Name
P6769=<string>		Firmware HTTP/HTTPS Password
P232=<string>		Firmware Upgrade File Prefix
P233=<string>		Firmware Upgrade File Postfix
P193=<int>	60 - 525600	Automatic Upgrade Interval (Minutes)
P194=<int>	<0 1 2 3>	Automatic Upgrade 0: No 1: Yes, check for periodic 2: Yes, check for every day 3: Yes, check for every week
P212=<int>	<0 1 2>	Upgrade Method: 0: TFTP 1: HTTP 2: HTTPS
P237=<string>		Config Server Path
P1360=<string>		Config HTTP/HTTPS User Name
P1361=<string>		Config HTTP/HTTPS Password
P234=<string>		Config Upgrade File Prefix
P235=<string>		Config Upgrade File Postfix
P1359=<string>		XML Config File Password
P145=<int>	<0 1>	DHCP Option 66 Override Server 0: Disable 1: Enable
P1414=<int>	<0 1>	Zero Config (for UCM Provisioning)



		0: Disable 1: Enable
P8458=<int>	<0 1>	Randomized Automatic Upgrade 0: Disable 1: Enable
P285=<int>	<0-23>	Hour of the Day – Start Time
P8459=<int>	<0-23>	Hour of the Day – End Time
P286=<int>	<0-6>	Day of the Week – Week
P1411=<int>	<0 1>	DHCP Option 120 Override SIP Server 0: Disable 1: Enable
P8463=<int>	<0 1>	Validate Server Certificates 0: Disable 1: Enable
P4428=<int>	<0 1>	Disable SIP NOTIFY Authentication 0: Disable 1: Enable

25. Reboot & Reset

Supported Devices: **GDS3710/GDS3705**

Support **cmd = reboot/reset**

Reboot:

http://<servername>/goform/config?cmd=reboot

Reset:

http://<servername>/goform/config?cmd=reset&P12055=<value>

<parameter>=<value>	Values	Description
---------------------	--------	-------------



P12055=<int>	<0 1 2 3>	Type of Reset Operation: 0: Clear All Data 1: Retain Network Data Only 2: Retain Only Card Information 3: Retain Network Data and Card Information
--------------	-----------	--

Get:

http://<servername>/goform/config?cmd=get&type=reset_reboot

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P15540>1</P15540>
  <P15541>0</P15541>
  <P15542>1210</P15542>
  <P14117/>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set<parameter>=<value>...

<parameter>=<value>	Values	Description
P15540=<int>	<0 1>	Auto Reboot Enable: 0: Disable 1: Enable
P15542=<string>		Auto Reboot Enable Time (Hour and Minutes): Example: 23:12 -> 2312, 08:06 -> 0806
P15541=<int>		Auto Reboot Enable Time (Week) 0: Everyday 1: Sunday



		2: Monday
		3: Tuesday
		4: Wednesday
		5: Thursday
		6: Friday
		7: Saturday



26.Syslog or Debug

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

`http://<servername>/goform/config?cmd=get&type=debug`

Example:

```
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P207>192.168.1.10</P207>
  <P208>0</P208>
</Configuration>
```

Set:

`http://<servername>/goform/config?cmd=set&<parameter>=<value>...`

<parameter>=<value>	Values	Description
P207=<string>		Debug Log Server IP or FQDN
P208=<int>	<0 1 2 3 4>	Debug Log Level: 0: None 1: Debug 2: Info 3: Warning 4: Error



27.Data Maintenance

Supported Devices: **GDS3710/GDS3705**

Support Methods: **cmd = export/upload**

Export:

http://<servername>/goform/config?cmd=export&type=0&data_type=0

<parameter>=<value>	Values	Description
data_type=<int>	<0 1>	The type of system config file. 0: System Config Data (No include password) 1: System Config Data (include password)

Upload:

http://<servername>/goform/config?cmd=upload&type=1

28.System Health Alert

Supported Devices: **GDS3710/GDS3705**

Support Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=sys_health_alert

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P15490>0</P15490>
```



```

<P15491>0</P15491>

<P15492>5</P15492>

<P15496></P15496>

<P15493>0</P15493>

<P15494>0</P15494>

<P15495>0</P15495>

</Configuration>

```

Set:

```
http://<servername>/goform/config?cmd=set&<parameter>=<value>...
```

<parameter>=<value>	Values	Description
P15900=<int>	<0 1>	Enable System Health Alert 0: Disable 1: Enable
P15491=<int>	<0 1>	Delivery Method 1: Real-time 2: Periodic
P15492=<int>	<1-10080>	Alert Interval(m)
P15496=<string>		Email Title Max. Length=256
P15493=<int>	<0 1>	SIP Registration Status 0: Disable 1: Enable
P15494=<int>	<0 1>	System Running Status 0: Disable 1: Enable
P15494=<int>	<0 1>	System Temperature 0: Disable 1: Enable

29.Event Notification

Supported Devices: **GDS3710/GDS3705**



Supported Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=log

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P15410>1</P15410>
  <P15413>http://192.168.1.2:80</P15413>
  <P15414>admin</P15414>
  <P15415>admin</P15415>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value>	Values	Description
P15410=<int>	<0 1>	Enable Event Notification 0: Disable 1: Enable
P15417=<int>	<1 2>	Via Type 1: HTTP 2: HTTPS
P15553=<int>	<0 1>	Event Notification HTTP Method 0: POST 1: GET
P15413=<string>		HTTP Server URL: Format ip:port/path .



		Example: 192.168.1.2:80/ Max. Length=256
P15414=<string>		HTTP Server Username: If don't need the Username & Password to access the HTTP server, please keep empty. Max. Length=128
P15415=<string>		HTTP Server Password: If don't need the Username & Password to access the HTTP server, please keep empty. Max. Length=128
P15416=<string>		URL Template Default: <pre>{ "mac": "\${MAC}", "content": "\${WARNING_MSG}" }</pre>



30.Certificates

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get/set**

Get:

http://<servername>/goform/config?cmd=get&type=trustedca

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P8433></P8433>
  <P8433></P8434>
  <P8433></P8435>
  <P8433></P8436>
  <P8433></P8437>
  <P8433></P8438>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>=<value>	Values	Description
P8433=<string>		Trusted CA Certificates
P8434=<string>		
P8435=<string>		
P8436=<string>		
P8437=<string>		
P8438=<string>		
P8475=<string>		Custom Certificate



31. System Status

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get**

Get:

http://<servername>/goform/config?cmd=get&type=sysinfo

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>

  <ResCode>0</ResCode>

  <RetMsg>OK</RetMsg>

  <P89>GDS3710</P89>

  <P917>V1.6A</P917>

  <P1397>9650001416A</P1397>

  <P70>1.0.3.31</P70>

  <P45>1.0.3.31</P45>

  <P68>1.0.3.31</P68>

  <P15009>2 hours 44 minutes</P15009>

  <P499>0</P499>

</Configuration>
```

<parameter>=<value>	Model Supported	Values	Description
P89=<string>	GDS3710/GDS3705		Product Model
P208=<int>	GDS3710/GDS3705	<0 1 2 3 4>	Hardware Version
P1397=<string>	GDS3710/GDS3705		Part Number
P70=<string>	GDS3710/GDS3705		Core Version
P45=<string>	GDS3710/GDS3705		Base Version
P68=<string>	GDS3710/GDS3705		Prog Version
P69	GDS3710/GDS3705		Boot Version
P15009=<string>	GDS3710/GDS3705		System Up Time



Pfw_available_version =<string>	GDS3710/GDS3705		Firmware available version
Systemp=<string>	GDS3710/GDS3705		System Temperature
atp_in=<int>	GDS3710/GDS3705	<0 1>	Tamper Sensor 0: Untriggered 1: Triggered
doorctrl0=<int>	GDS3710/GDS3705	<0 1>	Door Ctrl [1] 0: Untriggered 1: Triggered
doorctrl0=<int>	GDS3710/GDS3705	<0 1>	Door Ctrl 2 0: Untriggered 1: Triggered
doorctrl1=<int>	GDS3710/GDS3705	<0 1>	Door Ctrl 0: Untriggered 1: Triggered
do=<int>	GDS3710/GDS3705	<0 1>	Digit Output 0: Untriggered 1: Triggered
di0=<int>	GDS3710/GDS3705	<0 1>	Digit Input 1 0: Untriggered 1: Triggered
di1=<int>	GDS3710/GDS3705	<0 1>	Digit Input 2 0: Untriggered 1: Triggered



32. Network Status

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd = get**

Get:

```
http://<servername>/goform/config?cmd=get&type=net
```

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P67>00:0B:82:B9:A9:1C</P67>
  <P8>0</P8>
  <P9>192</P9>
  <P10>168</P10>
  <P11>5</P11>
  <P12>202</P12>
  <P13>255</P13>
  <P14>255</P14>
  <P15>255</P15>
  <P16>0</P16>
  <P17>192</P17>
  <P18>168</P18>
  <P19>5</P19>
  <P20>1</P20>
  <P10107>0</P10107>
  <P21>192</P21>
```



```

<P22>168</P22>

<P23>5</P23>

<P24>1</P24>

<P25>192</P25>

<P26>168</P26>

<P27>5</P27>

<P28>1</P28>

<P1684>1</P1684>

<P51>0</P51>

<P87>0</P87>

</Configuration>

```

<parameter>=<value>	Values	Description
P8=<int>	<0 1>	IP Address Mode 0: DHCP 1: Static IP
P9=<int>	0 - 255	IP Address: P9. P10. P11. P12.
P10=<int>	0 - 255	
P11=<int>	0 - 255	
P12=<int>	0 - 255	
P13=<int>	0 - 255	Subnet Mask: P13. P14. P15. P16.
P14=<int>	0 - 255	
P15=<int>	0 - 255	
P16=<int>	0 - 255	
P17=<int>	0 - 255	Gateway: P17. P18. P19.
P18=<int>	0 - 255	
P19=<int>	0 - 255	
P20=<int>	0 - 255	



		P20.
P10107=<iint>	<0 1>	DNS
P21=<int>	0 - 255	DNS Server 1
P22=<int>	0 - 255	
P23=<int>	0 - 255	P21.
P24=<int>	0 - 255	P22.
		P23.
		P24.
P25=<int>	0 - 255	DNS Server 2
P26=<int>	0 - 255	
P27=<int>	0 - 255	P25.
P28=<int>	0 - 255	P26.
		P27.
		P28.

33.Firmware Available Version Check

Supported Devices: **GDS3710/GDS3705**

Supported Methods: **cmd= fw_upgrade**

fw_upgrade:

http://<servername>/goform/config?cmd=fw_upgrade&type=num

<parameter>=<value>	Values	Description
P8=<int>	<0 1>	Operate type 0: check firmware available version 1: firmware upgrade



34. Card Data Import/Export

Supported Devices: **GDS3710/ GDS3705**

Supported Methods:

cmd= export/upload (GDS3710)
cmd= export/upload (GDS3705)

Export:

http://<servername>/goform/config?cmd=export&type=1&data_type=num

Import:

http://<servername>/goform/config?cmd=upload&type=0&dupopt=num

<parameter>=<value>	Values	Description
type=<int>		Type: export type = 1 upload type = 0 (GDS3705 only)
data_type	<0 1>	Export data type: 0 - .gs 1 - .csv (GDS3705)
Dupopt	<0 1>	On Duplicate Entry operate type 0 - skip 1- update information

35. OpenVPN Settings

Supported Devices: GDS3710/ GDS3705

Support **cmd= get/set/upload/del**

Get:

http://<servername>/goform/config?cmd=get&type=openvpn



Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
  <P7050>1</P7050>

  <P7051>192.168.86.158</P7051>

  <P7052>1194</P7052>

  <P2912>0</P2912>

  <P9902>1</P9902>

  <P9903>1</P9903>

  <P9904>1</P9904>

  <P8396>0</P8396>

  <P8394/>

  <P8395></P8395>

  <P8460/>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set<parameter>=<value>...

- P7050/ P7051/ P7052/ P2912/ P8396/ P8394/ P8395/ P8460

SET:

http://<servername>/goform/config?cmd=set&Pxxx=<value>

- P9902/ P9903/ P9904

UPLOAD:

http://<servername>/goform/config?cmd= upload&type=4&index=x (x=0/1/2)

DEL:

http://<servername>/goform/config?cmd= del&openvpn=x (x=0/1/2)



<parameter>=<value>	Values	Description
P7050=<int>	0, 1	OpenVPN® Enable 0- Disable Enable
P7051=<string>	String	OpenVPN® Server Address Max. Length = 256
P7052=<int>	Integer: 0 - 65535	OpenVPN® Port Range: 0 ~ 65535
P2912=<int>	0, 1	OpenVPN® Transport 0- UDP TCP
P9902	String	System_Settings.OpenVPN® Settings.Openvpn_CA Max. Length = 8192
P9903	String	System_Settings.OpenVPN® Settings.Openvpn_Client_ Certificate Max. Length = 8192
P9904	String	System_Settings.OpenVPN® Settings.Openvpn_Client_Key Max. Length = 8192
P8394	String	OpenVPN® Username Max. Length = 256
P8395	String	OpenVPN® Password Max. Length = 256
P8396	0, 1, 2, 3	System_Settings. OpenVPN® Settings.Openvpn_Cipher_Method 0: Blowfish; 1: AES-128; 2: AES-256; 3: Triple-DES
P8460	String	System_Settings.OpenVPN® Settings.Additional_Options Max. Length = 1024

36. TR069 Settings

Supported Devices: GDS3705

Support **cmd= get/set**

Get:

<http://<servername>/goform/config?cmd=get&type=tr069>



Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <P1409>1</P1409>

  <P4503>https://acs-test.gdms.cloud</P4503>

  <P4506>1</P4506>

  <P4507>86400</P4507>

  <P4511>000B82XXXXXX</P4511>

  <P4518>7547</P4518>
</Configuration>
```

Set:

http://<servername>/goform/config?cmd=set<parameter>=<value>...

- P1409/P4503/P4504/P4505/P4506/P4507/P4511/P4512/P4518/P8220/P8221

SET:

http://<servername>/goform/config?cmd=set&Pxxx=<value>

<parameter>=<value>	Values	Description
P1409=<int>	0, 1	Enable TR-069 0- Disable 1- Enable
P4503=<string>	String	ACS URL Max. Length = 1024
P4504=<string>	String	ACS Username Max. Length = 1024
P4505=<string>	String	ACS Password Max. Length = 128
P4506=<int>	0, 1	Periodic Inform Enable 0- Disable 1- Enable
P4507=<int>	0, 9999999999	Periodic Inform Interval (s)
P4511=<string>	String	Connection Request Username Max. Length = 1024
P4512=<string>	String	Connection Request Password Max. Length = 1024



P4518=<int>	1-65535	Connection Request Port
P8220=<string>	String	CPE Cert File Max. Length = 2048
P8221=<string>	String	CPE Cert Key Max. Length = 2048



HTTP API APPLICATION EXAMPLES

Now we provide three examples for reference:

- 1) General parameter revision, e.g.: change the “Unlocking Latency”
- 2) Obtain Snapshot
- 3) Obtain MJPEG stream

1. General Parameter Revision

Login Authentication: The authentication is using Challenge / Response encryption mode. After the successful authentication by the administrator, each later on operations will be accepted and successful ONLY when the correct authentication information is included inside the HTTP/HTTPS request header.

The authentication process is as following:

Step 1:

Client → Server

(Type=0 means login authentication verification required).

```
https://<servername>/goform/login?cmd=login&user=admin&type=0
```

The Wireshark Capture Listed Below:

POST /goform/login HTTP/1.1

Host: 192.168.86.3

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0

Accept: application/xml, text/xml, */*; q=0.01

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

If-Modified-Since: 0

X-Requested-With: XMLHttpRequest

Referer: http://192.168.1.3/login.html

Content-Length: 27



Connection: keep-alive

cmd=login&user=admin&type=0

Server → Client (Server sending ChallengeCode to Client after receiving the request from Client)

HTTP/1.0 200 OK Content-Type: text/xml; charset=UTF-8

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <ChallengeCode>6243b032c7468a9e384e49933914e880</ChallengeCode>
  <LoginType>0</LoginType>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step 2: Client → Server

(Client received ChallengeCode,
via **authcodestring** =md5(**ChallengeCode**:GDS3710IZpRsFzCbM:password);
generating the **authcodestring**. Then sending this authcode string back to the Server)

https://<servername>/goform/login?cmd=login&user=admin&authcode=<authcodestring>&type=0

The Wireshark Capture Listed Below:

POST /goform/login HTTP/1.1

Host: 192.168.86.3

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0

Accept: application/xml, text/xml, */*; q=0.01

Accept-Language: zh-CN, zh; q=0.8,en-US; q=0.5,en; q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

If-Modified-Since: 0

X-Requested-With: XMLHttpRequest

Referer: http://192.168.1.3/login.html

Content-Length: 69



Connection: keep-alive

cmd=login&user=admin&authcode=6d990a5f8f4f7e61635732febae3496f&type=0

NOTE:

The rule for authcodestring listed below:

authcodestring = md5(ChallengeCode:GDS3710IZpRsFzCbM:password);

- The “ChallengeString” is the returned string from Server in **Step 1**.
- Password is the web login password of the device (GDS37xx)
- Authcode string length must be 32 in lowercase hex as in MD5 hash.

Server ➔ Client

HTTP/1.0 200 OK

Content-Type: text/xml; charset=UTF-8

Set-Cookie: session=6d990a5f8f4f7e61635732febae3496f; path=/;

Set-Cookie: uname=admin; path=/;

Set-Cookie: level=1; path=/;

<?xml version="1.0" encoding="UTF-8" ?>

<Configuration>

<ResCode>0</ResCode>

<LoginType>0</LoginType>

<RetMsg>OK</RetMsg>

</Configuration>

Note:

- The **red** part is the authentication information returned by the Server after successful authentication.
- This part of the information must exist in the message header before all later on operations can run normally.



Example: Adjust “Unlocking Latency” and “Unlock Hold Time” via HTTP API:

Client → Server

```
POST /goform/config HTTP/1.1
Host: 192.168.86.3
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101
Firefox/51.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN, zh; q=0.8, en-US; q=0.5,en; q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
If-Modified-Since: 0
X-Requested-With: XMLHttpRequest
Referer: http://192.168.86.3/Pages/doorbasic.html?t=1496977082292
Content-Length: 299
Cookie: session=6d990a5f8f4f7e61635732febae3496f; uname=admin; level=1;
gdsauthkey80=6d990a5f8f4f7e61635732febae3496f; curpage=doorbasic.html
Connection: keep-alive

cmd=set&P14100=2&P14101=5
```

Note:

- The “P14100=2” means adjusting “Unlocking Latency” to 2 seconds.
- The “P14101=5” means adjusting “Unlock Hold Time” to 5 seconds.
- The red part “Cookie” is the returned verification message of the successful authentication in Login Verification at step 2.



Example: Request snapshot via HTTP API: (GDS3710)

Step 1: Client → Server (Client sending request to Server, trying to get ChallengeCode)

```
POST /goform/login HTTP/1.1
Host: 192.168.86.3

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101
Firefox/51.0

Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN, zh; q=0.8, en-US; q=0.5,en; q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
If-Modified-Since: 0
X-Requested-With: XMLHttpRequest
Referer: http://192.168.86.3/jpeg/view.html
Content-Length: 27
Connection: keep-alive

cmd=login&user=admin&type=1
```

Step 2: Server → Client (Server sending ChallengeCode to Client after receiving the request)

```
HTTP/1.0 200 OK
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <ChallengeCode>b00cb908497b74848f94760d6a76c4aa</ChallengeCode>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step 3: Client → Server

(Client received ChallengeCode,

via **authcodestring** = md5(**ChallengeCode**:GDS3710IZpRsFzCbM:password);
generating **authcodestring**, then sending back the **authcodestring** to Server)



```
POST /goform/login HTTP/1.1
Host: 192.168.86.3
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN, zh; q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
If-Modified-Since: 0
X-Requested-With: XMLHttpRequest
Referer: http://192.168.86.3/jpeg/view.html
Content-Length: 69
Connection: keep-alive

cmd=login&user=admin&authcode=931b58c7d24800e9d4b1aa39a01dc04a&type=1
```

Step 4: Server → Client (Server received the authcode from Client, successfully verified, Server will send below information to Client)

```
HTTP/1.0 200 OK
Content-Type: text/xml; charset=UTF-8
Set-Cookie: mjpeg_sess=d5e3f029fb7334b2bebd737ea77d09f7; path=/;
Set-Cookie: mjpeg_uname=admin; path=/;
Set-Cookie: mjpeg_level=1; path=/;

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step 5:

Later on interactions between Client and Server, the HTTP header should contain strings like “mjpeg_sess, mjpeg_uname, mjpeg_level”.



For example:

```
GET /snapshot/view0.jpg?0.9801228921400826 HTTP/1.1
Host: 192.168.86.3
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101
Firefox/51.0
Accept: */*
Accept-Language: zh-CN, zh; q=0.8,en-US; q=0.5,en; q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.86.3/jpeg/view.html
Cookie: mjpeg_sess=931b58c7d24800e9d4b1aa39a01dc04a; mjpeg_uname=admin;
mjpeg_level=1
Connection: keep-alive
```

Note:

- “mjpeg_sess” is string from Server to Client after successful authentication, used for all later on request.
- “mjpeg_uname” is User Name or ID
- “mjpeg_level” is fixed as “1”
- The above **RED** part “Cookie” is the returned verification message of the successful authentication in Login Verification at Step 4.



2. JPEG (Snapshot)

Supported Devices: **GDS3710 only**

Login Authentication: The authentication is using Challenge / Response encryption mode. After the successful authentication by the administrator, each later on operations will be accepted and successful ONLY when the correct authentication information is included inside the request header.

The authentication process is as following:

Step 1:

Client → Server

(Type=1 means MJPEG/JPEG obtain login authentication verification)

```
https://<servername>/goform/login?cmd=login&user=admin&type=1
```

Server → Client

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <ChallengeCode>ChallengeString</ChallengeCode>
  <LoginType>0</LoginType>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step2:

Client → Server

```
https://<servername>/goform/login?cmd=login&user=admin&authcode=<authcodestring>&type=1
```

NOTE:

The rule for authcodestring listed below:

- **authcodestring** = md5(ChallengeString:GDS3710IDyTIHwNgZ:password);
- The "ChallengeString" is the returned string from Server in **Step 1**.
- password is the login password of the device (GDS37xx)
- Authcode string length must be 32 in lowercase hex as in MD5 hash.



Server → Client

```
HTTP/1.0 200 OK Content-Type: text/xml; charset=UTF-8
Set-Cookie: mjpeg_sess=396a6328e70f3b1b984f7d6f08159a49; path=/;
Set-Cookie: mjpeg_uname=admin; path=/;
Set-Cookie: mjpeg_level=1; path=/;

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Note:

- The red part is the authentication information returned by the Server after successful authentication.
- This part of the information must exist in the message header before all later on operations can run normally.

Step3:

Client → Server

```
https://<servername>/snapshot/view.jpeg
```

NOTE:

- Step 3 should be finished within 30 seconds after authentication OK, or the authentication will be invalid.
- The timer that records authentication valid time will refresh if Step3 executes successfully.
- The timer when using **https://<servername>/snapshot/view.jpeg** to obtain snapshot will start counting from 0, within 30 seconds if the same request is asking for snapshot again, the timer will reset; otherwise the request without verified message will be timed out and the verification will be voided. New verification is required to obtain snapshot again.
- The snapshot is using internal 4th stream, with MJPEG video codec and fixed resolution 1280 x 720.

Below is an Example:

Step 1: Client → Server (Client sending login request to Server, trying to get ChallengeCode)

```
POST /goform/login HTTP/1.1
```



Host: 192.168.86.3
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN, zh; q=0.8,en-US; q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
If-Modified-Since: 0
X-Requested-With: XMLHttpRequest
Referer: http://192.168.86.3/jpeg/mjpeg.html
Content-Length: 27
Connection: keep-alive

cmd=login&user=admin&type=1

Step 2: Server → Client (Server sending ChallengeCode to Client after receiving the request from Client)

HTTP/1.0 200 OK
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
 <ResCode>0</ResCode>
 <ChallengeCode>c1cd724b1fc2d552652bba09a56f6f3c</ChallengeCode>
 <RetMsg>OK</RetMsg>
</Configuration>

Step 3: Client → Server (Client receiving ChallengeCode,
via **authcodestring** = md5(**ChallengeCode**: GDS3710IDyTIHwNgZ:password);
generating **authcodestring**, then sending this **authcodestring** back to Server)

POST /goform/login HTTP/1.1
Host: 192.168.86.3
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN, zh; q=0.8,en-US; q=0.5,en;q=0.3



```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
If-Modified-Since: 0
X-Requested-With: XMLHttpRequest
Referer: http://192.168.86.3/jpeg/mjpeg.html
Content-Length: 69
Connection: keep-alive

cmd=login&user=admin&authcode=a7539fbd022664d07c23f736a643be55&type=1
```

Step 4: Server → Client (Server received the authcode from Client, successfully verified,
Server will send below information to Client)

```
HTTP/1.0 200 OK
Content-Type: text/xml; charset=UTF-8
Set-Cookie: mjpeg_sess=a7539fbd022664d07c23f736a643be55; path=/;
Set-Cookie: mjpeg_uname=admin; path=/;
Set-Cookie: mjpeg_level=1; path=/;

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step 5: Later on interactions between Client and Server, the HTTP header should contain strings like “mjpeg_sess, mjpeg_uname, mjpeg_level”.

For example :

```
GET /snapshot/view0.jpg?0.9801228921400826 HTTP/1.1
Host: 192.168.86.3
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101
Firefox/51.0
Accept: */*
Accept-Language: zh-CN, zh; q=0.8,en-US; q=0.5,en; q=0.3
Accept-Encoding: gzip, deflate
```



Referer: http://192.168.86.3/jpeg/mjpeg.html

Cookie: **mjpeg_sess=a7539fbd022664d07c23f736a643be55; mjpeg_uname=admin; mjpeg_level=1**

Connection: keep-alive

NOTE:

- “mjpeg_sess” is string from Server to Client after successful authentication, used for all later on request.
- “mjpeg_uname” is User Name or ID
- “mjpeg_level” is fixed as “1”
- The **red** part “Cookie” is the returned verification message of the successful authentication in Login Verification at Step 4.

3. MJPEG Stream (Challenge Mode or Basic Mode)

Supported Devices: **GDS3710 only**

The authentication is using either Challenge / Response encryption mode or Basic authentication. After the successful authentication by the administrator, each later on operations will be accepted and successful ONLY when the correct authentication information is included inside the request header.

The GDS3710 supports MJPEG Stream live viewing via HTTP API commands, this can be used without installing the Live view browser plugin. Users can deploy two methods to retrieve MJPEG stream depending on MJPEG Authentication Mode, which can be set under following path:

Web UI → System Settings → Access Settings

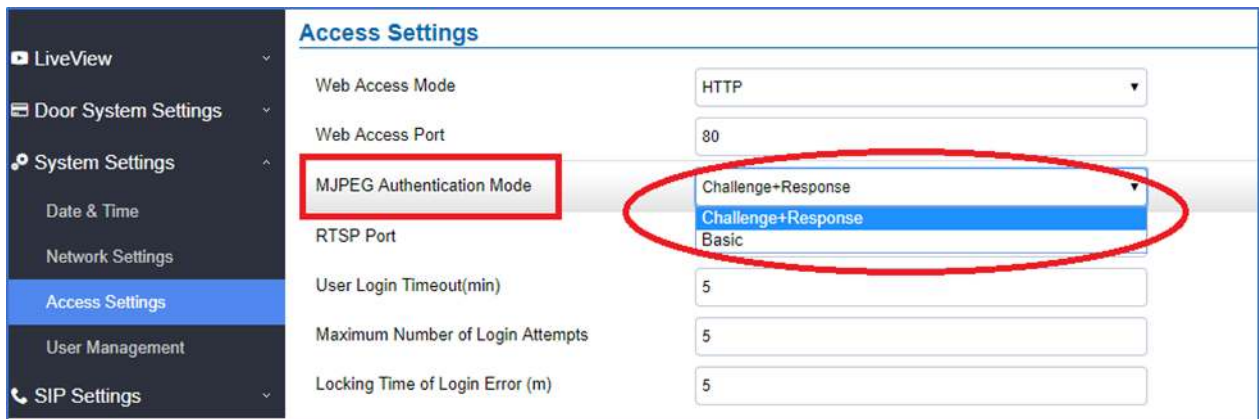


Figure 1: MJPEG Authentication Mode

1) Challenge+Response MJPEG Authentication for Default Mode:

Select “Challenge+Response” from WebUI: “System Settings → Access Settings → MJPEG Authentication Mode” to obtain the default MJPEG stream (internal 4th stream) with 1280x720 resolution.

Step 1:

Client → Server

```
<http|https>://<servername>/jpeg/stream?type=0&user=admin
```

Server → Client

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <ChallengeCode>ChallengeString</ChallengeCode>
  <IDCode>id_code</IDCode>
  <LoginType>0</LoginType>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step2:

Client → Server

```
<http|https>://<servername>/jpeg/stream?type=1&user=admin&authcode=<authcodestr
ing>&idcode=id_code
```

NOTE:

The rule for authcodestring listed below:

- **authcodestring** = md5(ChallengeString:GDS3710IDyTIHwNgZ:password);
- The “ChallengeString” is the returned string from Server in **Step 1**.
- password is the login password of the device (GDS37xx)
- Authcode string length must be 32 in lowercase hex as in MD5 hash.
- The **RED** part is the authentication message returned by the Server after successful authentication.
- This part of the information must exist in the message header before all later on operations can run normally.



Below is an Example:

Step 1: Client → Server (Client sending login request to Server, trying to get ChallengeCode)

```
GET /jpeg/stream?type=0&user=admin HTTP/1.1
Host: 192.168.100.123
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Step 2: Server → Client (Server sending ChallengeCode to Client after receiving the request from Client)

```
HTTP/1.0 200 OK
Content-Type: text/xml;charset=UTF-8

<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>OK</RetMsg>
  <ChallengeCode>9c07f92ea2ab55c2d7ef433e5fa163a0</ChallengeCode>
  <IDCode>QDOJBDBQT8MJ7WRVCZ7L</IDCode>
</Configuration>
```

Step 3: Client → Server (Client receiving ChallengeCode,
via `authcodestring = md5(ChallengeCode:GDS3710IDyTIHwNgZ:password);`
generating `authcodestring`, then sending this `authcodestring` back to Server)

```
GET
/jpeg/stream?type=1&user=admin&authcode=b10e713c68ee31ac5500359969496907&idcode=QDOJBDBQT8
MJ7WRVCZ7L HTTP/1.1
Host: 192.168.100.123
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
```



Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

Accept-Encoding: gzip, deflate

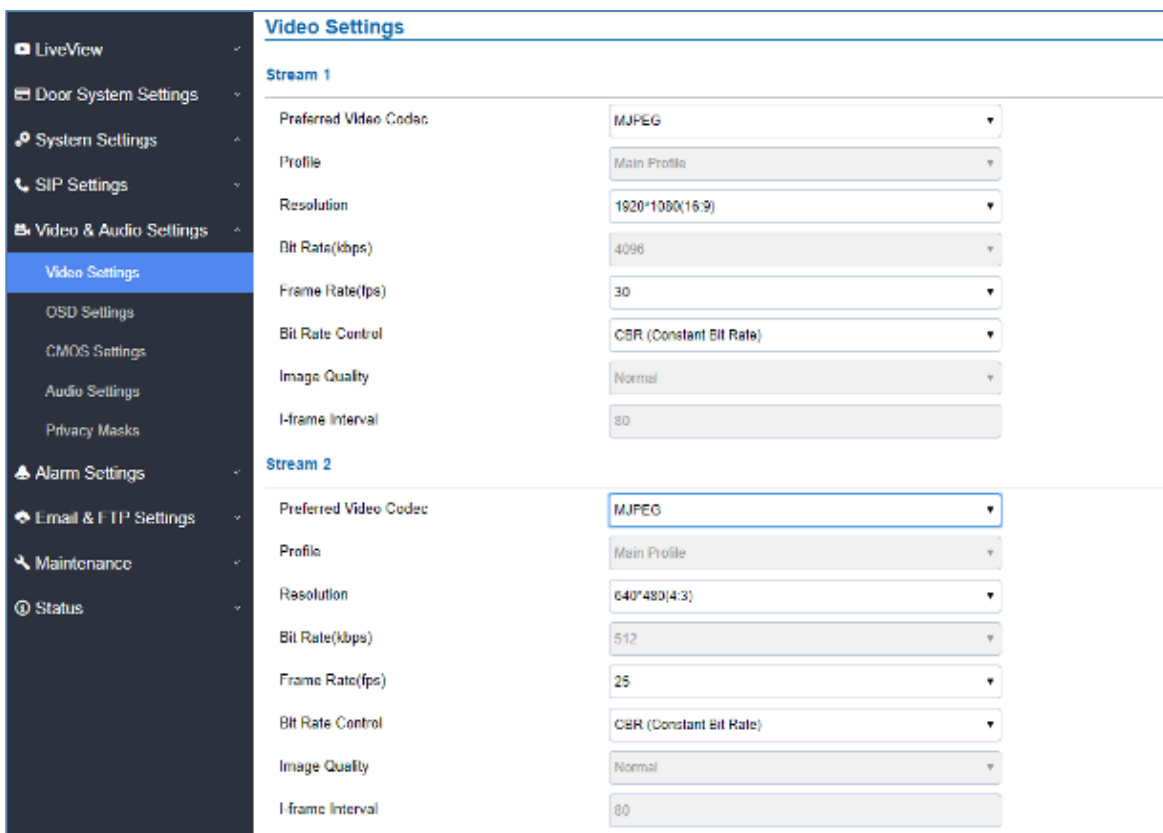
Accept-Language: zh-CN,zh;q=0.9

Then the MJPEG stream will be retrieved.

2) Challenge+Response MJPEG Authentication for Recommended Method: (MJPEG Video Codec)

The video codec in this option should be set to “MJPEG” for the specific stream that we want to retrieve under:

Web UI → Video & Audio Settings → Video Settings



Video Settings	
Stream 1	
Preferred Video Codec	MJPEG
Profile	Main Profile
Resolution	1920*1080(16:9)
Bit Rate(kbps)	4096
Frame Rate(fps)	30
Bit Rate Control	CBR (Constant Bit Rate)
Image Quality	Normal
I-frame Interval	80
Stream 2	
Preferred Video Codec	MJPEG
Profile	Main Profile
Resolution	640*480(4:3)
Bit Rate(kbps)	512
Frame Rate(fps)	25
Bit Rate Control	CBR (Constant Bit Rate)
Image Quality	Normal
I-frame Interval	80

Figure 2: Video Settings

The authentication process is as following:

Step 1:

Client → Server

<http/https>://<servername>/jpeg/stream?type=0&user=admin&stream=X

Where **X= 0,1,2** corresponded to **1st, 2nd and 3rd** MJPEG stream respectively.



Server → Client

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <ChallengeCode>ChallengeString</ChallengeCode>
  <IDCode>id_code</IDCode>
  <LoginType>0</LoginType>
  <RetMsg>OK</RetMsg>
</Configuration>
```

Step2:

Client → Server

```
<http|https>://<servername>/jpeg/stream?type=1&user=admin&stream=X&authcode=<authcodestring>
&idcode=id_code
```

Where X= 0,1,2 corresponded to 1st, 2nd and 3rd MJPEG stream respectively.

NOTE:

The rule for authcodestring listed below:

- **authcodestring** = md5(ChallengeString:GDS3710IDyTIHwNgZ:password);
- The "ChallengeString" is the returned string from Server in **Step 1**.
- Password is the login password of the device (GDS37xx)
- Authcode string length must be 32 in lowercase hex as in MD5 hash.
- The RED part is the authentication message returned by the Server after successful authentication.
- This part of the message must exist in the message header before all later on operations can run successfully.

Below is an Example to get 2nd MJPEG Stream

Step 1: Client → Server (Client sending login request to Server, trying to get ChallengeCode)

```
GET /jpeg/stream?type=0&user=admin&stream=1 HTTP/1.1
Host: 192.168.100.123
Connection: keep-alive
Cache-Control: max-age=0
```



Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Step 2: Server → Client (Server sending ChallengeCode to Client after receiving the request from Client)

HTTP/1.0 200 OK

Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8" ?>

<Configuration>

<ResCode>0</ResCode>

<RetMsg></RetMsg>

<ChallengeCode>ceab1fac2056be0f889ed634716b466b</ChallengeCode>

<IDCode>LS79DELW7W7987NK87XO</IDCode>

</Configuration>

Step 3: Client → Server (Client receiving ChallengeCode,

via **authcodestring** = md5(**ChallengeCode**:GDS3710IDyTIHwNgZ:password);

generating **authcodestring**, then sending this **authcodestring** back to Server)

GET

/jpeg/stream?type=1&user=admin&stream=1&authcode=c73472591063ca6159f082a8138f46e4&idcode=LS79DELW7W7987NK87XO HTTP/1.1

Host: 192.168.100.123

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/66.0.3359.139 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

Accept-Encoding: gzip, deflate



Accept-Language: zh-CN,zh;q=0.9

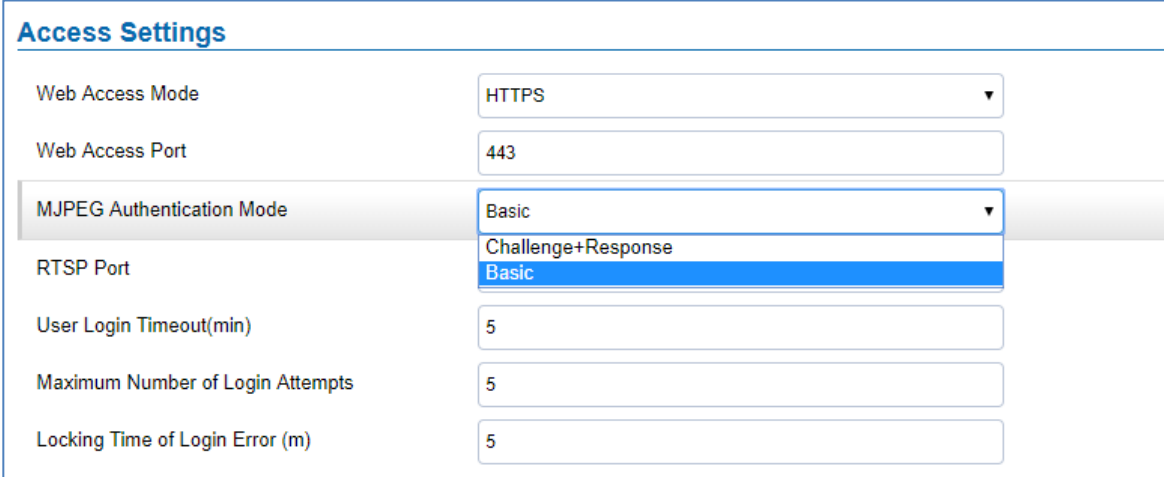
Then the MJPEG stream will be retrieved.

3) Basic MJPEG Authentication for Default Method

Select "Basic" from WebUI: "System Settings → Access Settings → MJPEG Authentication Mode" to obtain the default MJPEG stream (internal 4th stream) with 1280x720 resolution.

NOTE:

- MJPEG must be selected in the Preferred Video Codec for this to work



Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Basic
RTSP Port	
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5

Figure 3: Basic MJPEG Authentication

Client → Server

`<http|https>://username:password@<servername>/jpeg/stream`

NOTE:

- username: web login username
- password is the web login password of the device (GDS37xx)

Below is an Example:

Step 1: Client → Server (Client sending GET request to Server, trying to get MJPEG Stream)

GET /jpeg/stream HTTP/1.1

Host: 192.168.100.123



Connection: keep-alive

Authorization: Basic YWRtaW46YWRtaW4=

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

Accept-Encoding: gzip, deflate

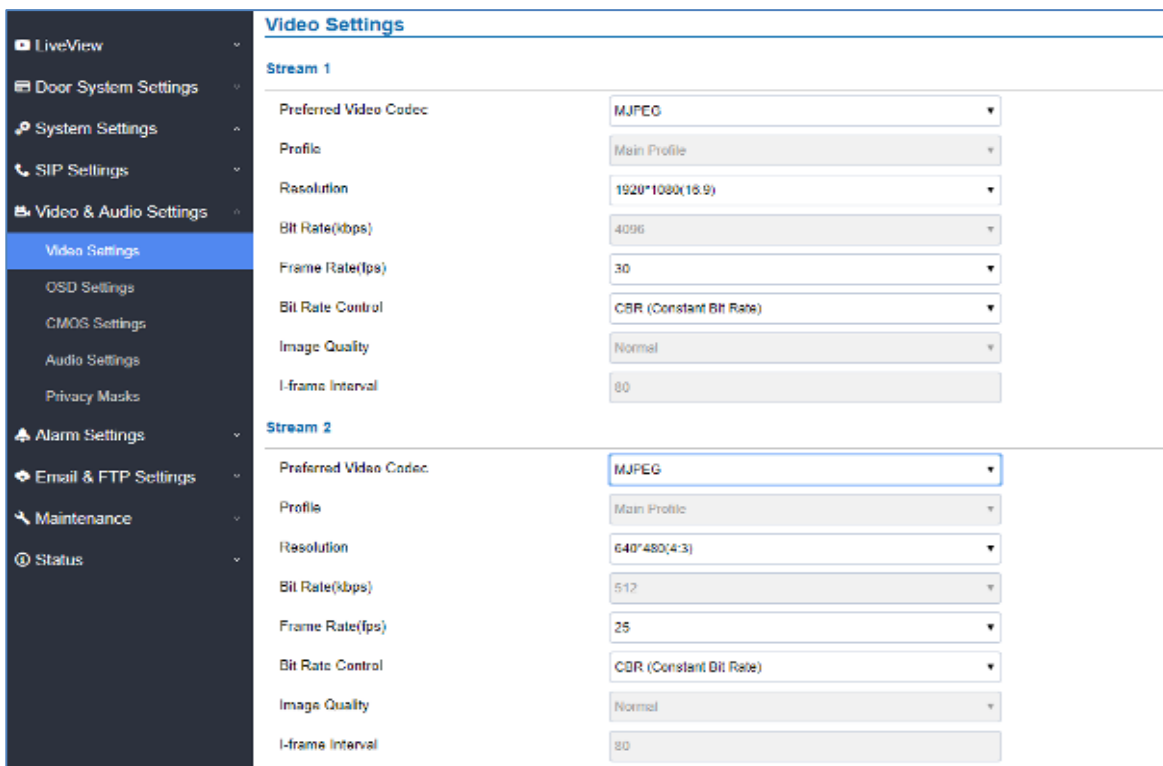
Accept-Language: zh-CN,zh;q=0.9

Then the MJPEG stream will be retrieved.

4) **Basic MJPEG Authentication for Recommended Method: (MJPEG Video Codec)**

The video codec in this option should be set to “MJPEG” for the specific stream that we want to retrieve under:

Web UI → Video & Audio Settings → Video Settings



Video Settings	
Stream 1	
Preferred Video Codec	MJPEG
Profile	Main Profile
Resolution	1920*1080(18.9)
Bit Rate(kbps)	4096
Frame Rate(fps)	30
Bit Rate Control	CBR (Constant Bit Rate)
Image Quality	Normal
I-frame Interval	80
Stream 2	
Preferred Video Codec	MJPEG
Profile	Main Profile
Resolution	640*480(4.3)
Bit Rate(kbps)	512
Frame Rate(fps)	25
Bit Rate Control	CBR (Constant Bit Rate)
Image Quality	Normal
I-frame Interval	80

Figure 4: Video settings

Client → Server

<http|https>://username:password@<servername>/jpeg/stream=X

Where **X= 0,1,2** corresponded to **1st, 2nd and 3rd** MJPEG stream respectively.

NOTE:

- username: web login username
- password is the web login password of the device (GDS37xx)

Below is an Example to get 2nd MJPEG Stream:

Step 1: Client → Server (Client sending GET request to Server, trying to get MJPEG Stream)

```
GET /jpeg/stream=1 HTTP/1.1
Host: 192.168.100.123
Connection: keep-alive
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Then the 2nd MJPEG stream will be retrieved.

- **Basic authentication of MJPEG snapshot image via HTTP API to easy 3rd party System Integration, similar to GS IP Camera implementation.**

For easy system integration (with the cost of less secure), once the feature enabled (default is disabled), user can send HTTP API with correct credentials to retrieve MJPEG/JPEG snapshot from GDS3710, similar to the behavior of Grandstream IP Cameras.

The HTTP API or CLI command listed as below:

MJPEG: [http\(s\)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html](http(s)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html)

JPEG: [http\(s\)://admin:password@IP_GDS3710:Port/jpeg/view.html](http(s)://admin:password@IP_GDS3710:Port/jpeg/view.html)

NOTE:

- MJPEG is continuously grab JPEG snapshots.
- Similar command can be applied to open source application like **VLC MediaPlayer** to retrieve H.264 video stream with better quality:

rtsp://admin:password@IP_GDS3710:Port/X



where X= 0, 4, 8 corresponded to 1st, 2nd and 3rd video stream where 2nd recommended.

- **Anonymous LiveView / Snapshot:**

From WEB UI -> Access Enable "Enable Anonymous LiveView" in the "Access Settings" WebUI page

When enabled, user can display the camera stream from GDS without admin credentials using the following URL scheme:

MJPEG Video: `http(s)://GDS3710_IP:port/videoview.html`

Users can also retrieve a real-time snapshot without admin credentials using the following URL:

JPEG Snapshot: `http(s)://IP_GDS3710:Port/anonymous/snapshot/view.html`

`http(s)://IP_GDS3710:Port/anonymous/snapshot/view.jpg`

NOTE:

- MJPEG stream may feel like animation due to the compromise of video quality and bandwidth.
- Similar command can be applied to open source application like VLC MediaPlayer to retrieve H.264 video stream with better quality:

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

(X= 0, 4, 8 corresponded to 1st, 2nd and 3rd video stream where 2nd stream recommended)



4. HTTP API to Open Door

HTTP API Open Door Authentication: The authentication is using Challenge/Response encryption mode. After the successful authentication by the administrator, each later on operations will be accepted and successful ONLY when the correct authentication information is included inside the request header.

<parameter>=<value>	Values	Description
cmd=<int>	<0 1>	0: Step 1 1: Step 2
authcodestring=<string>	md5(ChallengeString:remote_pin:password);	
idcodestring=<string>	From authentication' step 1	
opt_type=<int>	<1 2>	1: open door 2: close door

The authentication process is as following:

Step 1:

Client → Server

```
[http/https]://<servername>/goform/apicmd?cmd=0&user=admin
```

Server → Client

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg></RetMsg>
  <ChallengeCode>5c0e1f55b54be2d0c56004ba349fb726</ChallengeCode>
  <IDCode>UM1NWDJYC19LOEYQRWNA</IDCode>
</Configuration>
```

Step2:

Client → Server

```
[http/https]://<servername>/goform/apicmd?cmd=1&user=admin&authcode=<authcodes
tring>&idcode=<idcodestring>&type=opt_type
```



NOTE:

The rule for authcodestring listed below:

authcodestring = md5(ChallengeCode:remote_pin:password);

idcodestring = The node value of "IDCode", such as "UM1NWDJYC19LOEYQRWNA"
above example.

opt_type = 1: open door, 2: close door

- The "ChallengeCode" is the returned string from Server in **Step 1**.
- Remote_pin is "Remote PIN to Open Door"
- Password is the login password of the device (GDS37xx).
- Authcodestring must be length of 32 in lowercase hex as in MD5 hash.
- The **RED** part is the authentication message returned by the Server after successful authentication.
- This part of the message must exist in the message header before all later on operations can run successfully.

If authentication OK, the return message like this:

HTTP/1.0 200 OK Content-Type: text/xml; charset=UTF-8

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>0</ResCode>
  <RetMsg>Authentication OK</RetMsg>
</Configuration>
```

If authentication Failed, the return message like this:

HTTP/1.0 200 OK Content-Type: text/xml; charset=UTF-8

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
  <ResCode>1</ResCode>
  <RetMsg>Authentication error</RetMsg>
</Configuration>
```



If the HTTP API to open door disable, then the return message like this:

```
HTTP/1.0 200 OK Content-Type: text/xml;charset=UTF-8
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>1</ResCode>
  <RetMsg>HTTP API open door function is disable</RetMsg>
</Configuration>
```

If the remote open door PIN is null, then the return message like this:

```
HTTP/1.0 200 OK Content-Type: text/xml;charset=UTF-8
<?xml version="1.0"encoding="UTF-8" ?>
<Configuration>
  <ResCode>1</ResCode>
  <RetMsg>Authentication error. Remote PIN is null</RetMsg>
</Configuration>
```

Notes:

- The **RED** part is the authentication information returned by the Server after successful authentication.
- This part of the information must exist in the message header before all later on operations can run normally.
- The user must be “admin”, others do not have the privilege.
- Default Validity of the **idcodestring** come from step 1 is 30 seconds, it is mean that user must finish the step 2 in 30 seconds, or the idcodestring will timeout and invalid. (This parameter can **ONLY** be configured via P Value which is **P15428**)

For example, if you want to set it to 150 seconds, you will need to apply this command:

http://<servername>/goform/config?cmd=set&P15428=150

- The “type=1” means that the HTTP API is for open door.
- Authcode string length must be 32 in lowercase hex as in MD5 hash.

