

Grandstream Networks, Inc.

GDS37xx

HTTP API Guide



GDS37xx - HTTP API

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 has to be executed before any operation to the related parameter configuration.

Software Version Requirement

- All current official firmware of the Grandstream GDS37xx are supported.

Syntax: Client => Server

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

NOTE:

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

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>
```

NOTE:

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

- *authcodestring = md5(ChallengeString:GDS3710IzRsFzCbM: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 has to be existed 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:

- o 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:

- o In most situation, parameters fetched by using "GET" can be revised by using "SET", except Status or Display parameter information.
- o 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.
- o Please refer to related WebGUI page for reference if unsure about the HTTP API.

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

XML Returned by Device

Response Code	Response Text	Description
0	OK	Success
1		User does not exist
2		Password error
3		Maximum login or maximum whitelist 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 password
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

Card Management

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

Get:

[http|https]://<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> <!-- username -->
<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|https]://<servername>/goform/config?cmd=<add|set>&<parameter>=<value>...

NOTE:

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)*

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

<parameter> = <value>	Model Supported	Values	Description
ID= <int>	GDS3710/GDS3705	Numeric Digits	RFID card number. Unique and cannot be empty
room_num = <int>	GDS3710/GDS3705	Numeric Digits	Virtual Number (Room Number). Cannot be empty
sip_num = <string>	GDS3710/GDS3705	Numeric Digits	SIP extension number (max. length: 20) Binding via SIP
username = <string>	GDS3710/GDS3705	Character Strings	Name (max. 32 characters). Cannot be empty
passwd = <string>	GDS3710/GDS3705	Numeric Digits	PIN to open door (max. length: 12)
gender = <int>	GDS3710/GDS3705	<0 1>	Gender: 0: Male (Default); 1: Female
identify_num = <string>	GDS3710/GDS3705		ID Number (max. length: 20)
cellphone_num = <int>	GDS3710/GDS3705		Cell Number (max. length: 16)
SOD = <int>	GDS3710/GDS3705		Valid Start Date Format: Default: 20991231 20171001 (YYYYMMDD)

EOD = <int>	GDS3710/GDS3705		Valid End Date Format: Default: 20991231 20171001 (YYYYMMDD)
enable_card = <int>	GDS3710/GDS3705	<0 1>	Enable the RFID card 0: Disable (Default); 1: Enable
ID= <string>	GDS3710/GDS3705		Delete ID number. "," used as separator; Max. 20 can be deleted one time
account	GDS3710/GDS3705	<0 1 2 3 4>	Call Out Account 0: Auto 1: Account 1 2: Account 2 3: Account 3 4: Account 4
group_id	GDS3710/GDS3705	<0-50>	Group: The group id must exist, or group_id=0
sch_id	GDS3710/GDS3705	<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|https]://<servername>/goform/config?cmd=del&ID=ID1,ID2,ID3,ID4,...

NOTE:

- To delete a card, you need only to mention the ID number which is the Card Number.

- o *Maximum 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>
```

Door System Basic Settings

Support **cmd=get / set**

Get:

[http|https]://<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>

<P10462/>

<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|https]://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter> = <value>	Model Supported	Values	Description
P15440= <int>	GDS3710/G DS3705 GDS3712/G DS3702	GDS3710/GDS3705: <0 1 2 3> GDS3712/GDS3702: <0 1 2 3>	Door Relay Options (GDS3710/GDS3705) 0:Local Relay 1:Webrelay 2:GSC3570 Relay 3: Send Wiegand Code on Remote Open Door Actions Door Relay Options (GDS3712/GDS3702) 0:Local Relay 1:Webrelay 2:GSC3570 Relay 3: Send Wiegand Code on Remote Open Door Actions
P15441= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Webrelay ON URL (Max. Length=1024)
P15447= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Webrelay OFF ULR (Max. Length=1024)
P15442= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Webrelay Username (Max. Length=128)
P15443= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Webrelay Password (Max. Length=128)

P15444=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<1 2 3 4>	Choose Open Door Account 1: Account 1 2: Account 2 3: Account 3 4: Account 4
P15445= <string>	GDS3710/G DS3705 GDS3712/G DS3702		GSC3570 Phone Number (Max. Length=128)
P15446= <string>	GDS3710/G DS3705 GDS3712/G DS3702		GSC3570 Door Password (Max. Length=128)
P15450=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	ALMOUT1 Feature 0: Alarm Output 1: Open Door
P15470=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	ALMOUT1 Status 0: Normal Close 1: Normal Open
P15467=<int>	GDS3710/G DS3705 GDS3702	<0 1 2 3>	Control Options 0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P15468=<int>	GDS3710/G D3705	<0 1 2 3>	Wiegand Control Options 0: Door 1 1: Door 2 2: Door 1 & Door 2 3: None
P14100=<int>	GDS3710/G DS3705 GDS3712/G DS3702	0 – 20	Delay before Unlock (s)

P15465=<int>	GDS3710/G D3705 GDS3712/G DS3702	0 – 20	Door 2 Delay before Unlock (s)
P14101=<int>	GDS3710/G DS3705 GDS3712/G DS3702	1 – 1800	Unlock Hold Time (s)
P15466=<int>	GDS3710/G D3705 GDS3712/G DS3702	1 – 1800	Door 2 Unlock Hold Time (s)
P14829=<int>	GDS3710/G DS3705	0 – 2000	Minimum Interval of Swiping Card (ms)
P15593	GDS3705/G DS3702	<0 1>	Email Notification When Door Opened 0: Disable 1: Enable
P15474=<int>	GDS3710 GDS3712	0 – 4 and no more than 'Unlock Hold Time (s) (For the second door)' value.	Number of Snapshots when Door Opened
P15475=<int>	GDS3710 GDS3712	0 – 4 and no more than second 'Unlock Hold Time (s) (For the second door)' value.	Number of Snapshots when Door 2 Opened
P14103=<int>	GDS3710 GDS3712	<0 1>	Snapshot when Door Opened — via FTP: 0: No; 1: Yes
P15471=<int>	GDS3710 GDS3712	<0 1>	Snapshot when Door Opened — via Email: 0: No; 1: Yes
P15420=<int>	GDS3710 GDS3712	<0 1>	Snapshot when Doorbell Pressed — via FTP: 0: No; 1: Yes
P15409=<int>	GDS3710 GDS3712	<0 1>	Snapshot when Doorbell Pressed — via Email: 0: No; 1: Yes
P15583	GDS3710/G DS3712 GDS3705/G DS3702	0-10	Snapshot Delay When Door Opened (s)

P15584	GDS3710/G DS3712 GDS3705/G DS3702	0-10	Snapshot Delay When Doorbell Pressed (s)
P14856=<int>	GDS3710/G DS3705 GDS3702	<0 1 >	Call Mode: 0: Virtual Number (Or Room Number) 1: SIP Number
P10470	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2 3 4>	Doorbell Call Out Account: 0: Auto 1: Account 1 2: Account 2 3: Account 3 4: Account 4
P14827=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Doorbell Mode: 0: Call Doorbell Number 1: Doorbell Output Control (DO1) 2: Both Above
P15434	GDS3710/G D3705 GDS3712/G DS3702	<0 1>	Number(s) Called When Door Bell Pressed 0: Serial Hunting 1: Parallel Hunting
P15418=<int>	GDS3710/G DS3705 GDS3712/G DS3702	0 — 10	Press Doorbell Schedule 1
P10462= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Number 1 Called When Door Bell Pressed (Max. Length=255)
P15557=<int>	GDS3710/G DS3705 GDS3712/G DS3702	0 — 10	Press Doorbell Schedule 2

P15556= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Number 2 Called When Door Bell Pressed (Max. Length=255)
P15559= <int>	GDS3710/G DS3705 GDS3712/G DS3702	0 — 10	Press Doorbell Schedule 3
P15558= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Number 3 Called When Door Bell Pressed (Max. Length=255)
P15561= <int>	GDS3710/G DS3705 GDS3712/G DS3702	0 — 10	Press Doorbell Schedule 4
P15560= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Number 4 Called When Door Bell Pressed (Max. Length=255)
P15419= <int>	GDS3710/G D3705	0 — 20	Maximum Number of Dialed Digits
P15436= <int>	GDS3710/G D3705	1 – 15	No Key Input Timeout (s)
P10457= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Remote PIN to Open Door. Max. length = 8
P15460= <string>	GDS3710/G D3705 GDS3712/G DS3702		Remote PIN to Open Door 2. Max. length = 8
P10464= <int>	GDS3710/G DS3705	<0 1 2>	Local PIN Type: 0: Private PIN 1: Universal PIN 2: Card & private PIN

P15461=<int>	GDS3710/G DS3705	<0 1 2 3>	Unified PIN Open Door Options: 0: Door 1 1: Door 2 2: Door 3 3: none
P15498= <string>	GDS3710/G DS3705	<0 10>	Local PIN to Open the Door Schdule
P14850=<int>	GDS3710/G DS3705 GDS3702	<0 1>	Enable Guest PIN: 0: Disable 1: Enable
P15462=<int>	GDS3710/G DS3705	<0 1 2 3>	Guest PIN Open Door Options: 0: Door 1 1: Door 2 2: Door 3 3: none
P10463= <string>	GDS3710/G DS3705		Local PIN to Open Door (all digits value)
P14858=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Enable DTMF Open Door 0: Enable; 1: Disable (Default)
P14851= <string>	GDS3710/G DS3705		Guest PIN: Numerical Digits. Max. Length = 8
P14852= <string>	GDS3710/G DS3705	e.g.: 2017/06/14 00:00:00	Guest PIN starting time
P14853= <string>	GDS3710/G DS3705	e.g.: 2017/06/14 02:02:10	Guest PIN ending time
P14580=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Disable Auto-Answer 0: Disable (Default); 1: Enable
P14582=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Enable Doorbell Button to End Call 0: Disable (Default) 1: Enable

P15421=<int>	GDS3710/G DS3705 GDS3702	<0 1>	Disable Keypad (except Doorbell Button) 0: Disable (Default); 1: Enable
P15422=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Hang up Call After Remote Door Opened 0: Disable (Default); 1: Enable
P15582=<int>	GDS3710/G DS3705 GDS3712/G DS3702	3-1800	Onhook Timer After Remote Open Door (s)
P15424=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Enable HTTP API Remote Open Door 0: Disable (Default); 1: Challenge + Response Authentication. 2: Basic Authentication
P1573=<int>	GDS3710/G DS3705	<0 1>	HTTP API Open Door Compatibility Mode 0: Disable (Default); 1: Enable
P15433=<int>	GDS3710/G DS3705	<0 1>	Disable Keypad SIP Number Dialing 0: Disable (Default); 1: Enable
P15543=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	One-way Interlocking Doors Mode 0: Disable (Default); 1: Enable
P10465=<int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Enable Card Issuing Mode 0: Disable (Default); 1: Enable
P15423=<int>	GDS3710/G DS3705	1-1440	Card Issuing State Expire Time (m)
P14800=<int>	GDS3710/G DS3705	<0 1>	Enable Key Blue Light 0: Disable; 1: Enable
P15428=<int>	GDS3710 GDS3712	5 — 300	Open Door Valid Time

P14801=<int>	GDS3710	<0 1>	Enable White LED Back Light 0: Disable; 1: Enable
P15591=<int>	GDS3710	1-255	Blue Light Brightness(Time Interval)
P15592=<int>	GDS3710	1-255	Blue Light Brightness(Key Pressed)
P15301=<int>	GDS3710/GDS3705	<0 1>	Central Mode 0: Disable (Default); 1: Enable
P15544=<int>	GDS3710	<0 1>	Key Sensitivity Level 0: Default 1:High
P14340=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<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 GDS3712/GDS3702		Start time turning on the Blue Door Bell Light Digit string like "1459". The first two digit is 24 hour format, las two is minutes 00 <= hour <=23; 00 <= minute <= 59
P14561=<string>	GDS3710/GDS3705 GDS3712/GDS3702		End time turning on the Blue Door Bell Light Digit string like "1459". The first two digit is 24 hour format, las two is minutes 00 <= hour <=23 00 <= minute <= 59
P14562=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Door Bell Blue Light 0: Disable 1: Enable

P15500=<int>	GDS3710/GDS370 5	<0 1>	Enable Keypad Blue Light 0: Disable 1: Enable
P15501=<int>	GDS3710		Start time turning on the Blue Keypad Light Digit string like "1459". The first two digit is 24 hour format, las two is minutes 00 <= hour <=23; 00 <= minute <= 59

P15502=<int>	GDS3710/GDS370 5		End time turning on the Blue Keypad Light Digit string like "1459". The first two digit is 24 hour format, las two is minutes 00 <= hour <=23 00 <= minute <= 59
P15594=<int>	GDS3710	<0 1>	Enable White Backlight on Time Interval 0: Disable 1: Enable
P15595=<int>	GDS3710		Start time turning on the White Backlight Digit string like "1459". The first two digit is 24 hour format, las two is minutes 00 <= hour <=23; 00 <= minute <= 59
P15596=<int>	GDS3710		End time turning on the White Backlight Digit string like "1459". The first two digit is 24 hour format, las two is minutes 00 <= hour <=23 00 <= minute <= 59
P15514	GDS3710/GDS370 5 GDS3712/GDS370 2	<0 1>	System_Settings.Access_Settings.Enable_PIN_Password_Display_HTTPS 0: Disable; 1: Enable.

- o **P15514**

GET:[http|https]://<servername>/goform/config?cmd=get&type=access

SET:[http|https]://<servername>/goform/config?cmd=set&P15514=<value>

- o **P15440/ P15441/ P15442/ P15443**

GET:[http|https]://<servername>/goform/config?cmd=get&type=door

SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

Keep Door Open

Support **cmd=get / set**

Get:

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

<parameter> = <value>	Model Supported	Values	Description
P15429 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 2	Keep Door Open 0: Disable 1: Immediate Open Door 2: Schedule Open Door
P15435 = <digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Emergency PIN to Disable Keep Door Open
P15585 = <digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Emergency PIN to Re-enable Keep Door Open
P15430 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	5 – 480	Duration to Keep Door Open (m)
P15211 = <digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Schedule Start Time

P15212=<digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Schedule End Time
P15571=<int>	GDS3710/GDS3712	0-10	Schedule
P15506=<int>	GDS3710 GDS3712	0 – 10	Holiday Mode
P15213=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Schedule Table Format: door_sch,index@start_time@end_time Example: P15213=door_sch,0@0000@2359
P15455=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 2	Keep Door Open 0: Disable 1: Immediate Open Door 2: Schedule Open Door
P15472=<digital string>	GDS3710/GDS3712 GDS3705/GDS3702		Emergency PIN to Disable Keep Door Open (Door 2)
P15586=<digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Emergency PIN to Re-enable Keep Door Open (Door 2)
P15456=<int>	GDS3710/GDS3705 GDS3712/GDS3702	5 – 480	Duration to Keep Door Open (m) (Door 2)
P15457=<digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Schedule Start Time (Door 2)
P15458=<digital string>	GDS3710/GDS3705 GDS3712/GDS3702		Schedule End Time (Door 2)
P15572=<int>	GDS3710/GDS3712	0-10	Schedule (Door 2)
P15507=<int>	GDS3710 GDS3712	0-10	Holiday Mode (For the second door)
P15459=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Schedule Table (Door 2) Format: door_sch,index@start_time@end_time Example: P15459=door_sch,0@0000@2359

Group

Devices: **GDS3710/GDS3705**

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

Get:

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

<para>= <value>	Model Supported	Values	Description
groupname= <string>&schid= <int>	GDS3710/GDS3705	groupname: string	Group Name, Max. Length=64
	schid: 1 — 10	Time Schedule Index	

Set:

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

<parameter>= <value>	Model Supported	Value s	Description
<para1>= <value1>&<para2>= <value2>&<para3>= <value3>groupid= <int>&groupname= <string>&schid= <int>	GDS3710/GDS305	groupid: 1-10 schid: 1-10	group name. Max. Length=64 schid: Time Schedule Index groupid: Group Index.

Del:

[http|https]://<servername>/goform/config?cmd=del&<para1>= <value1>

<parameter>= <value>	Model Supported	Values	Description
groupid= <int>	GDS3710/GDS3705	1 — 10	groupid: Group Index.

Schedule

Support **cmd=get / set**

Get:

[http|https]://<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|https]://<servername>/goform/config?cmd=set&<paramter>=<value>...

<parameter>= <value>	Model Supported	Values	Description

P15200=<string>			Value format:
P15201=<string>			name@holiday_mode,weekday0@start_time0@end_time0,weekday1@start_time1@end_time1,...
P15202=<string>			Use (,) as separator when set multiple numbers.
P15203=<string>			e.g.:
P15204=<string>	GDS3710/GDS3705		AAA@0,0@0830 @1459 ,0@1600@1800,
P15205=<string>	GDS3712/GDS3702		AAA is a revisable name for a schedule, Max. Length = 64
P15206=<string>			1 st @ represent holiday mode, 0-10.
P15207=<string>			2 st @ represent date of the week, 0-6, Sunday to Saturday
P15208=<string>			3 nd @ the pre-four digits represent start time of that period, 0830 represent 08:30 in 24 hour format;
P15209=<string>			2 nd @ the post-four digits represent end time of that period, 1459 represent 14:59 in 24 hour format.

NOTE:

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

Holiday

Support **cmd=get / set**

Get:

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

<parameter>=<value>	Model Supported	Values	Description
P15250=<string>			
P15251=<string>			
P15252=<string>			Value format:
P15253=<string>			name,start_date0@end_date0, start_date1@end_date1,
P15254=<string>	GDS3710/GDS3705		Use (,) as separator when set multiple dates.
P15255=<string>	GDS3712/GDS3702		e.g.:
P15256=<string>			schedule_1,20180405@20180420, 20180421@20180425,
P15257=<string>			schedule_1 is a revisable name for a schedule, Max. Length = 64
P15258=<string>			
P15259=<string>			

NOTE:

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

Date and Time

Devices: **GDS3710/GDS3705**

Support **cmd= get/set**

Get:

[http|https]://<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></P10005/>
<P10008>0</P10008>
<P14040>2017</P14040>
<P14041>6</P14041>
<P14042>3</P14042>
<P14043>9</P14043>
<P14044>37</P14044>
<P14045>33</P14045>
</Configuration>
```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P144= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Allow DHCP Option 42 to override NTP server
P143= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Allow DHCP Option 2 to Override Time Zone Setting

P64=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 38 and 55,56	<p>Time Zone:</p> <p>1:GMT-12 (Eniwetok, Kwajalein)</p> <p>2:GMT-11 (Midway Isl., Samoa)</p> <p>3:GMT-10 (Hawaii, Aleutian Isl.)</p> <p>4:GMT-09 (Alaska)</p> <p>5:GMT-08 (Las Vegas, San Francisco, Vancouver)</p> <p>6:GMT-07 (Calgary, Denver, Salt Lake City)</p> <p>7:GMT-06 (Chicago, Dallas, Mexico City)</p> <p>8:GMT-05 (Cuba)</p> <p>9:GMT-05 (New York, Toronto, Washington DC)</p> <p>10:GMT-04 (Paraguay)</p> <p>11:GMT-04 (Chile)</p> <p>12:GMT-04 (Charlottetown, Manaus)</p> <p>55:GMT-04:30 (Caracas)</p> <p>39:GMT-03:30 (Newfoundland)</p> <p>13:GMT-03 (Brasilia, Sao Paulo)</p> <p>14:GMT-02 (Noronha, Mid-Atlantic)</p> <p>15:GMT-01 (Azores, Cap Verde Isl.)</p> <p>16:GMT (Dublin, Lisbon, London, Reykjavik)</p> <p>17:GMT+01 (Amsterdam, Berlin, Rome, Stockholm)</p> <p>18:GMT+02 (Athens, Helsinki, Istanbul, Riga)</p> <p>19:GMT+02 (Egypt)</p> <p>20:GMT+02 (Israel)</p> <p>21:GMT+02 (Lebanon)</p> <p>22:GMT+02 (Syria)</p> <p>23:GMT+03 (Moscow, Riyadh)</p> <p>24:GMT+03 (Iraq)</p> <p>25:GMT+03:30 (Iran)</p> <p>26:GMT+04 (Abu Dubai, Baku)</p> <p>27:GMT+04:30 (Kabul)</p> <p>28:GMT+05 (Islamabad, Karachi, Tashkent)</p> <p>29:GMT+05:30 (Bombay, Calcutta, New Delhi)</p> <p>30:GMT+06 (Novosibirsk, Omsk)</p>
-----------	--	------------------	---

			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 GDS3712/GDS3702	<0 1>	Enable Daylight Saving Time 0: Disable 1: Enable
P10005=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Daylight Saving Time
P5006=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable NTP 0: Disable 1: Enable
P30=<string>	GDS3710/GDS3705 GDS3712/GDS3702		NTP Server
P10006=<int>	GDS3710/GDS3705 GDS3712/GDS3702	60 – 1440	Update Interval (m)

Network Settings

Devices: **GDS3710/GDS3705**

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

Get:

[http|https]://<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:AB:CC:BA</P67>
<P8>0</P8>
<P9>192</P9>
<P10>168</P10>
<P11>86</P11>
<P12>3</P12>
<P13>255</P13>
<P14>255</P14>
<P15>255</P15>
<P16>0</P16>
<P17>192</P17>
<P18>168</P18>
<P19>86</P19>
<P20>1</P20>
<P10107>0</P10107>
<P21>192</P21>
<P22>168</P22>
<P23>84</P23>
<P24>217</P24>
<P25>192</P25>
<P26>168</P26>
<P27>10</P27>
<P28>253</P28>
</Configuration>

```

Set:

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

- o **P8439/ P8440**

UPLOAD:

[http|https]://<servername>/goform/config?cmd= upload&type=6&index=x (x=0/1; 0: 802.1X CA Certificate, 1: 802.1X Client Certificate)

DEL:

[http|https]://<servername>/goform/config?cmd= del& 8021x=x (x=0/1; 0: 802.1X CA Certificate, 1: 802.1X Client Certificate)

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

P8= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	IP Address Mode 0: DHCP 1: Static IP
P9= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	IP Address: P9.P10.P11.P12
P10= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P11= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P12= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P13= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	Subnet Mask: P13.P14.P15.P16
P14= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P15= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P16= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P17= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	Gateway: P17.P18.P19.P20
P18= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P19= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P20= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P10107= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	DNS

P21=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	DNS Server 1 P21.P22.P23.P24
P22=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P23=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P24=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P25=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	DNS Server 2 P25.P26.P27.P28
P26=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P27=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P28=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P1684=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0,1	Enable LLDP 0: Disable 1: Enable
P27004=<int>	GDS3705 GDS3702	0,1	Enable VLAN 0: Disable 1: Enable
P51=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0-4094	Layer 2 QoS 802.1Q/VLAN Tag
P87=<int>	GDS3710/GDS3705 GDS3712/GDS3702		Layer 2 QoS 802.1p Priority Value
P5038=<int>	GDS3705 GDS3702	0-7	Layer 2 QoS 802.1p Priority Value
P5042=<int>	GDS3705 GDS3702	0-7	Layer 2 QoS 802.1p Priority value for RTP media

P7901= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0-3	802.1X Mode 0:Disable 1:EAP_MD5 2:EAP-TLS 3:EAP-PEAPv0/MSCHAPv2
P7902= <string>	GDS3710/GDS3705 GDS3712/GDS3702		802.1X Identity MAX length is 512
P7903= <string>	GDS3710/GDS3705 GDS3712/GDS3702		MD5 Password MAX length is 512
P8439= <string>	GDS3710/GDS3705 GDS3712/GDS3702		802.1X CA Certificate Max. Length = 8192
P8440= <string>	GDS3710/GDS3705 GDS3712/GDS3702		802.1X Client Certificate Max. Length = 8192

Access Settings

Devices: **GDS3710/GDS3705**

Support **cmd=get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=access

Example:

```

<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P12054>0</P12054>
<P901>80</P901>
<P903>554</P903>
<P12056>60</P12056>
<P14832>5</P14832>
<P14834>5</P14834>
<P12052>1</P12052>
<P12053>1</P12053>
<P276>1</P276>
<P27006>22</P27006>
<P15505></P15505>
<P15512></P15512>
</Configuration>

```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P12054 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Web Access Mode 0: HTTP 1: HTTPS
P901 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	HTTP: 80 – 65535 HTTPS: 443 – 65535	Web Port
P903 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	554 – 65535	RTSP Port
P12056 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	3 – 60	Time Out for Login (minute)
P14832 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	3 – 10	Max. continuous errors for Login Lock
P14834 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	5 – 60	Login error lockout time (minute)

P15473= <int>	GDS3710 GDS3712	<0 1>	Disable Web Access 0: Disable 1: Enable
P12053= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable UPnP Search 0: Disable 1: Enable
P15469= <int>	GDS3710 GDS3712	<0 1>	Enable Anonymous LiveView 0: Disable 1: Enable
P276= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable SSH 0: Disable 1: Enable
P27006= <int>	GDS3710/GDS3705 GDS3712/GDS3702	22 – 65535	SSH Port
P22293= <int>	GDS3710/GDS3705 GDS3712/GDS3702	10-12	Minimum TLS Version 10: TLS_1.0 11: TLS_1.1 12: TLS_1.2
P22293= <int>	GDS3710/GDS3705 GDS3712/GDS3702	10-12, 99	Minimum TLS Version 10: TLS_1.0 11: TLS_1.1 12: TLS_1.2 99: Unlimited
P15505= <string>	GDS3710/GDS3705 GDS3712/GDS3702		GDSManager Configuration Password MIN length is 1 MAX length is 32
P15512= <string>	GDS3710 GDS3712		RTSP Password MIN length is 1 MAX length is 32

User Management

Devices: **GDS3710/GDS3705**

Support **cmd=set**

Set:

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

<parameter> = <value>	Model Supported	Values	Description
oldpwd=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Oldpwd: Old Password, Max. Length = 32 Newpwd: New Password Max. Length = 32 cfmnewpwd: Confirmed New Password; Max. Length = 32 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.
Newpwd= <string>	GDS3710/GDS3705 GDS3712/GDS3702		
cfmnewpwd= <string>	GDS3710/GDS3705 GDS3712/GDS3702		
P10124=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Password Recovery Email Address

SIP Settings

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=sip

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P499>0</P499>
<P407></P407>
<P402></P402>
<P2412></P2412>
<P403></P403>
<P2433></P2433>
<P404></P404>
<P405></P405>
<P409>0</P409>
<P76></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>
<PIpCallSave>1</PIpCallSave>
<P10454>0</P10454>
<P8001>0</P8001>
<P8003>0</P8003>
<P411>0</P411>
<P443>0</P443>
<P15427>0</P15427>
<P15476>0</P15476>
<P424>100</P424>
<P406>N</P406>
<P281>Y</P281>
</Configuration>
```

Set:

[[http](#)][https](#)://<servername>/goform/config?cmd=set&<parameter>=<value>...

FOR GDS3710/GDS3712/GDS3705/GDS3702 ACCOUNT SETTINGS

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	Model Supported	Values	Description
P271= <int>	P401= <int>	P501= <int>	P601= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Account Active (In Use). 0:No 1:Yes
P210= <int>	P499= <int>	P599= <int>	P699= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	SIP Registration Status(Read Only)
P3= <string>	P407= <string>	P507= <string>	P607= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Account Name Max. Length = 64
P47= <string>	P402= <string>	P502= <string>	P602= <string>	GDS3710/G DS3705 GDS3712/G DS3702		SIP Server Max. Length = 255
P2312= <string>	P2412= <string>	P2512= <string>	P2612= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Secondary SIP Server Max. Length = 255
P48= <string>	P403= <string>	P503= <string>	P603= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Outbound Proxy Max. Length = 255
P2333= <string>	P2433= <string>	P2533= <string>	P2633= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Backup Outbound Proxy Max. Length = 255
P103= <int>	P408= <int>	P508= <int>	P608= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	DNS Mode 0:A Record 1:SRV 2:NAPTR/SRV

P35= <string>	P404= <string>	P504= <string>	P604= <string>	GDS3710/G DS3705 GDS3712/G DS3702		SIP User ID Max. Length = 255
P36= <string>	P405= <string>	P505= <string>	P605= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Authenticate ID Max. Length = 255
P34= <string>	P406= <string>	P506= <string>	P606= <string>	GDS3710/G DS3705 GDS3712/G DS3702		Authenticate password Max. Length = 255
P63=<int>	P409= <int>	P509= <int>	P609= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Tel URI 0: Disabled 1: User = Phone 2: Enable
P32=<int>	P412= <int>	P512= <int>	P612= <int>	GDS3710/G DS3705 GDS3712/G DS3702	1 – 64800	Registration Expiration (m)
P2330= <int>	P2430= <int>	P2530= <int>	P2630= <int>	GDS3710/G DS3705 GDS3712/G DS3702	0 – 64800	Re-register before Expiration (s)
P40=<int>	P413= <int>	P513= <int>	P613= <int>	GDS3710/G DS3705 GDS3712/G DS3702	1 – 65535	Local SIP Port
P130= <int>	P448= <int>	P548= <int>	P648= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	SIP Transport 0: UDP 1: TCP 2: TLS/TCP
P2311= <int>	P2411= <int>	P2511= <int>	P2611= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Check Domain Certificates 0: Disable 1: Enable

P15480= <int>	P8000= <int>	P15481= <int>	P15482= <int>	GDS3710 GDS3712	<0 1 2>	Stream 0: Stream 1 1: Stream 2 2: Stream 3
P2302= <int>	P2402= <int>	P2502= <int>	P2602= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Enable DTMF RFC2833 0: Disable 1: Enable
P2303= <int>	P2403= <int>	P2503= <int>	P2603= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Enable DTMF SIP INFO 0: Disable 1: Enable
P79= <int>	P496= <int>	P596= <int>	P696= <int>	GDS3710/G DS3705 GDS3712/G DS3702	96-127	DTMF Payload Type
P490= <int>	P1309= <int>	P590= <int>	P690= <int>	GDS3705 GDS3702	<0 1>	Enable Keep-Alive 0: Disable 1: Enable
P52= <int>	P414= <int>	P514= <int>	P614= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2 3 4>	NAT Traversal 0:No 1:Stun 2:Keep-Alive 3:UPnP 4:Auto 5:VPN
P43064= <int>	P43065= <int>	P43066= <int>	P43067= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	UPnP NAT Traversal 0: Disable 1: Enable
P81= <int>	P411= <int>	P511= <int>	P611= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Unregister on Reboot 0: Disable 1: Enable

P183= <int>	P443= <int>	P543= <int>	P643= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Enable SRTP 0: Disable 1: Enable but not Forced 2: Enable and Forced
P2383= <int>	P2483= <int>	P2583= <int>	P2683= <int>	GDS3710/G DS3712	<0 1 2>	SRTP Key Length 0: AES 128&256 bit 1: AES 128 bit 2: AES 256 bit
P198= <int>	P424= <int>	P524= <int>	P624= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<100 102 12 2 129>	Special Feature 100: Standard 102: Broadsoft 122: Metaswitch 129: Telefonica Spain
P191= <int>	P420= <int>	P520= <int>	P620= <int>	GDS3710/G DS3712		Enable Local Call Features 0: Disable 1: Enable
P2305= <int>	P2405= <int>	P2505= <int>	P2605= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Outbound Proxy Mode 0:in route 1:not in route 2:always send to
P2306= <int>	P2406= <int>	P2506= <int>	P2606= <int>	GDS3705 GDS3702	<0 1>	Validate Incoming Messages(0:No 1:Yes
P2392= <int>	P2492= <int>	P2592= <int>	P2692= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Enable RTCP 0: Disable 1: RTCP 2: RTCP-XR
P2347= <int>	P2447= <int>	P2547= <int>	P2647= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Accept Incoming SIP from Proxy Only 0: Disable 1: Enable

P2327= <int>	P2427= <int>	P2527= <int>	P2627= <int>	GDS3710 GDS3712	<0 1>	Enable RFC6184 0: Disable 1: Enable
P26058= <int>	P26158= <int>	P26258= <int>	P26358= <int>	GDS3705 GDS3702	<0 1>	Use P-Access-Network-Info Header 0: Disable 1: Enable
P26061= <int>	P26161= <int>	P26261= <int>	P26361= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1 2>	Add MAC in User-Agent 0: No 1: Yes, except REGISTER 2: Yes to all SIP
P293= <int>	P462= <int>	P562= <int>	P662= <int>	GDS3710 GDS3712	<96-127 & !=101>	H.264 Payload Type
P29061= <int>	P29161= <int>	P29261= <int>	P29361= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 1>	Codec Negotiation Priority: 0: Caller 1: Callee
P37= <int>	P486= <int>	P586= <int>	P686= <int>	GDS3710/G DS3705 GDS3712/G DS3702	1 – 64	Voice Frames Per TX
P2329= <int>	P2429= <int>	P2529= <int>	P2629= <int>	GDS3710 GDS3712	<0 1>	SIP URI Scheme When Using TLS 0: sip 1: sips
P288= <int>	P489= <int>	P589= <int>	P689= <int>	GDS3710 GDS3712	<0 1>	Support SIP Instance ID 0: Disable 1: Enable
P57= <int>	P451= <int>	P551= <int>	P651= <int>	GDS3710/G DS3705 GDS3712/G DS3702	<0 8 9 18>	Preferred Vocoder 1 0: PCMU 8: PCMA 9: G.722 18: G729A/B

P58= <int>	P452= <int>	P552= <int>	P652= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 8 9 18>	Preferred Vocoder 2 0: PCMU 8: PCMA 9: G.722 18: G729A/B
P59= <int>	P453= <int>	P553= <int>	P653= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 8 9 18>	Preferred Vocoder 3 0: PCMU 8: PCMA 9: G.722 18: G729A/B
P60= <int>	P454= <int>	P554= <int>	P654= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 8 9 18>	Preferred Vocoder 4 0: PCMU 8: PCMA 9: G.722 18: G729A/B
P2395= <int>	P2495= <int>	P2595= <int>	P2695= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Session Timer 0: Disable 1: Enable

FOR GDS3710/GDS3712/GDS3705/GDS3702 SIP ADVANCED SETTINGS

<parameter> = <value>	Model Supported	Values	Description
P76= <string>	GDS3710/GDS3705 GDS3712/GDS3702		STUN Server
P39= <int>	GDS3710/GDS3705 GDS3712/GDS3702	1 – 65535	Local SIP Port
P10451= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 65535	Auto On-Hook Timer (s)
P29610= <int>	GDS3710/GDS3705 GDS3712/GDS3702	48-10000	Use Random Port

P14847=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 90	Ringing Timeout (s)
P4208	GDS3710/GDS3705 GDS3712/GDS3702	1 – 1440	DNS Cache Expiration (m)
P28160	GDS3710/GDS3705 GDS3712/GDS3702	0 – 1440	DNS Cache Duration (m)
P280=<string>	GDS3710/GDS3705 GDS3712/GDS3702		SIP TLS Certificate
P279=<string>	GDS3710/GDS3705 GDS3712/GDS3702		SIP TLS Private Key
P281=<string>	GDS3710/GDS3705 GDS3712/GDS3702		SIP TLS Private Key Password
P10453=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Direct IP Call 0: Disable 1: Enable
P8001=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Two-way SIP Calling 0: Disable 1: Enable
P8003=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	SIP Proxy Compatibility Mode 1: Disable 0: Enable
P957=<int>	GDS3710 GDS3712	<0 1>	SIP Packetization Compatibility Mode 1: Disable 0: Enable
P15427	GDS3710/GDS3705 GDS3702	<0 1>	Enable Multi-channel Call Mode: 0: Disable 1: Enable
P15476=<int>	GDS3705 GDS3702	<0 1>	Allow Reset via SIP NOTIFY 0: Disable (default) 1: Enable

Whitelist

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

Get:

[http|https]://<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|https]://<servername>/goform/config?cmd=set&P10460=num

Add:

[http|https]://<servername>/goform/config?cmd=add&P10460=num

Del:

[http|https]://<servername>/goform/config?cmd=del&P10460=num1,num2,num3, ...

Account 1 Whitelist

<parameter> = <value>	Model Supported	Values	Description
P10410= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Whitelist 0: Disable 1: Enable
P10411= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Use (,) as separator when deleting multiple numbers. Up to 200 numbers.

Account 2 Whitelist

<parameter> = <value>	Model Supported	Values	Description
P10454= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Whitelist 0: Disable 1: Enable

P10460=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Use (,) as separator when deleting multiple numbers. Up to 200 numbers.
-----------------	------------------------------------	--	--

Account 3 Whitelist

<parameter> = <value>	Model Supported	Values	Description
P10420=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Whitelist 0: Disable 1: Enable
P10421=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Use (,) as separator when deleting multiple numbers. Up to 200 numbers.

Account 4 Whitelist

<parameter> = <value>	Model Supported	Values	Description
P10430=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Whitelist 0: Disable 1: Enable
P10431=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Use (,) as separator when deleting multiple numbers. Up to 200 numbers.

<parameter> = <value>	Model Supported	Values	Description
P15434=<int>	GDS3710 GDS3705 GDS3712/GDS3702	<0 1>	Door Bell Call Mode 0: Serial Hunting 1: Parallel Hunting

Example:

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

Video Settings

Devices: **GDS3710 Only**

Support **cmd= get/set**

Get:

[http|https]://<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>60</P12312>
<P12706>96</P12706>
<P12713>1</P12713>
<P12707>1022</P12707>
<P12708>512</P12708>
<P12709>25</P12709>
<P12710>0</P12710>
<P12711>2</P12711>
<P12712>50</P12712>
<P13106>96</P13106>
<P13113>1</P13113>
<P13107>0</P13107>
<P13108>256</P13108>
<P13109>30</P13109>
<P13110>0</P13110>
<P13111>2</P13111>
<P13112>60</P13112>
</Configuration>
```

Get:

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

Stream 1			
<parameter>=<value>	Model Supported	Values	Description
P12306=<int>	GDS3710 GDS3712	<26 96>	Video Codec: 26: H.264 96: MJPEG
P12313	GDS3710 GDS3712	<0 1 2>	Profile 0: Baseline 1: Main Profile 2: High Profile
P12307=<int>	GDS3710 GDS3712	<1022 1025>	Resolution: 1025: 1920*1080 (16:9) 1022: 1280*720 (16:9)
P12315=<int>	GDS3710 GDS3712	<1024 2048 4096>	Video Bit Rate (kbps) 1024: 1024kb 2048: 2048kb 4096: 4096kb
P12904=<int>	GDS3710 GDS3712	<5 10 15 20 25 30>	Max. Frame Rate (fps) 5: 5fps 10: 10fps 15: 15fps 20: 20fps 25: 25fps 30: 30fps
P12924=<int>	GDS3710 GDS3712	<0 1>	Video Bit Rate Control 0: Constant Bit Rate (CBR) 1: Variable Bit Rate (VBR)

P12311=<int>	GDS3710 GDS3712	<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>	GDS3710 GDS3712	1 – 100	I-Frame Interval

Stream 2			
<parameter> = <value>	Model Supported	Values	Description
P12706=<int>	GDS3710 GDS3712	<26 96>	Video Codec: 26: H.264 96: MJPEG
P12713	GDS3710 GDS3712	<0 1 2>	Profile 0: Baseline 1: Main Profile 2: High Profile
P12707=<int>	GDS3710 GDS3712	<1022 1 1010>	Resolution: 1022: 1280*720 (16:9) 1: 640*480 (4:3) 1010: 480*272 (16:9)
P12708=<int>	GDS3710 GDS3712	<256 512 1024>	Video Bit Rate (kbps) 256: 256kb 512: 512kb 1024: 1024kb

P12709=<int>	GDS3710 GDS3712	<5 10 15 20 25>	Max. Frame Rate (fps) 5: 5fps 10: 10fps 15: 15fps 20: 20fps 25: 25fps
P12710=<int>	GDS3710 GDS3712	<0 1>	Video Bit Rate Control 0: Constant Bit Rate (CBR) 1: Variable Bit Rate (VBR)
P12711=<int>	GDS3710 GDS3712	<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>	GDS3710 GDS3712	1 – 100	I-Frame Interval

Stream 3			
<parameter> = <value>	Model Supported	Values	Description
P13106=<int>	GDS3710 GDS3712	<26 96>	Video Codec: 26: H.264 96: MJPEG
P13113=<int>	GDS3710 GDS3712	<0 1 2>	Profile 0: Baseline 1: Main Profile 2: High Profile
P13107=<int>	GDS3710 GDS3712	<0 1008>	Resolution: 1008: 352*240 (CIF) 0: 320*240 (4:3)

P13108=<int>	GDS3710 GDS3712	<128 256 512>	Video Bit Rate (kbps) 128: 128kb 256: 256kb 512: 512kb
P13109=<int>	GDS3710 GDS3712	<5 10 15 20 25 30>	Max. Frame Rate (fps) 5: 5fps 10: 10fps 15: 15fps 20: 20fps 25: 25fps 30: 30fps
P13110=<int>	GDS3710 GDS3712	<0 1>	Video Bit Rate Control 0: Constant Bit Rate (CBR) 1: Variable Bit Rate (VBR)
P13111=<int>	GDS3710 GDS3712	<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>	GDS3710 GDS3712	1 – 100	I-Frame Interval

On Screen Display (OSD) Settings

Devices: **GDS3710/GDS3712 Only**

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

Get:

[http|https]://<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></P10040>
<P10041>0</P10041>
<P10046>0</P10046>
</Configuration>

```

Set:

[[http|https](http://<servername>/goform/config?cmd=set&<parameter>=<value>...)://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter> = <value>	Model Supported	Values	Description
P10044= <int>	GDS3710 GDS3712	<0 1>	Display Time 0: Disable 1: Enable
P10045= <int>	GDS3710 GDS3712	<0 1>	Display Text 0: Disable 1: Enable
P10001= <int>	GDS3710 GDS3712	<0 1 2>	OSD Date Format 0: Year – Month – Date 1: Month – Date – Year 2: Date – Month – Year
P10007= <int>	GDS3710 GDS3712	<0 1>	OSD Time Format 0: 24 hours 1: 12 hours
P10040= <string>	GDS3710 GDS3712		OSD Text Length Max. Length = 25

P10041=<int>	GDS3710 GDS3712	<0 1 2 3>	OSD Position for Date/Time 0: Top Left 1: Bottom Left 2: Top Right 3: Bottom Right
P10046=<int>	GDS3710 GDS3712	<0 1 2 3>	OSD Position for Text 0: Top Left 1: Bottom Left 2: Top Right 3: Bottom Right

CMOS Settings

Devices: **GDS3710 Only**

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

Get:

[[http](#)][https](#)://<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>
<P12314>1</P12314>
<P10503>0</P10503>
</Configuration>
```

Set:

[[http](#)][https](#)://<servername>/goform/config?cmd=set&<parameter>=<value>...

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

P10572=<int>	GDS3710 GDS3712	<1 2>	Mode 1: Normal 2: Low Light
P10573=<int>	GDS3710 GDS3712	<0 1>	LDC (Lens Distortion Correction) 0: Disable / OFF 1: Enable / ON
P12314=<int>	GDS3710 GDS3712	<0 1>	Power Frequency (For Avoiding Video Flicker) 0: 50Hz 1: 60Hz
P10503=<int>	GDS3710 GDS3712	<0 30 60 125 250 500 1000 2000 5000 10000>	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

Audio Settings

Support **cmd= get/set**

Get:

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

<parameter> = <value>	Model Supported	Values	Description
P14000 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	<1 2 4>	Audio Codec 1: PCMU 2: PCMA 4: G.722
P14003 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	GDS3710: 0 -6 GDS3705: 0-7	System Volume
P14835 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	GDS3710: 0 -6 GDS3705: 0-7	Door Bell Volume
P15499 = <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Custom Doorbell Ringtone 0: Disable 1: Enable
P15554 = <int>	GDS3710 GDS3712	1-1440	Audio Loopback Test Expiration (m) Note: Reserved Field

Privacy Masks

Devices: **GDS3710 Only**

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

Get:

[http|https]://<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>

```

Get:

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

<parameter>= <value>	Model Supported	Values	Description
P14225=<string>	GDS3710 GDS3712		<p>Region for Privacy Masks</p> <p>Format:</p> <p>Enable @Top Left x1 coordinates, Top Left y1 coordinates; Bottom Right x2 coordinates, Bottom Right y2 coordinates.</p> <p>e.g.: 0@0,0,0,0; 0@0,0,0,0; 0@0,0,0,0; 0@0,0,0,0;</p> <p>Digit before @ represents function, 0: Disable/Hide 1: Enable/Display</p> <p>Coordinates are separated by (,)</p> <p>Region is separated by (;)</p> <p>Please Do remember the last; and configure the 4 regions at the same time all at once.</p> <p>Rules:</p> <p>0 <= x1, x2 <= 704; 0 <= y1, y2 <= 576; x1 <= x2; y1 <= y2</p>

Alarm Config

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=event

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<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>123</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,</P14300>
<P14301>profile2@0,0,0,0,0,</P14301>
<P14302>profile3@0,0,0,0,0,</P14302>
<P14303>profile4@0,0,0,0,0,</P14303>
<P14304>profile5@0,0,0,0,0,</P14304>
<P14305>profile6@0,0,0,0,0,</P14305>
<P14306>profile7@0,0,0,0,0,</P14306>
<P14307>profile8@0,0,0,0,0,</P14307>
<P14308>profile9@0,0,0,0,0,</P14308>
<P14309>profile10@0,0,0,0,0,</P14309>
<P10467>0</P10467>
<P10466>N</P10466>
<P14341>5</P14341>
```

```

<P10468>1</P10468>
<P10469></P10469>
<P14350>0</P14350>
<P14355>1</P14355>
<P14354></P14354>
<P14825>1</P14825>
<P14826>1</P14826>
<P15407>1</P15407>
<P15408>1</P15408>
</Configuration>

```

Get:

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

<parameter> = <value>	Model Supported	Values	Description
P10250=<int>	GDS3710 GDS3712	<0 1>	Enable Motion Detection Alarm 0: Disable 1: Enable
P14223=<int>	GDS3710 GDS3712	0 – 100	Sensitivity of Motion Detection

<p>P14224=<string></p>	<p>GDS3710 GDS3712</p>		<p>Region of Motion Detection</p> <p>Format:</p> <p>[Top Left x1 coordinates, Top Left y1 coordinates, Bottom Right x2 coordinates, Bottom Right y2 coordinates]</p> <p>e.g.:</p> <p>[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]</p> <p>Coordinates are separated by (,)</p> <p>Region is separated by (;)</p> <p>The 8 regions must be configured at the same time all at once.</p> <p>Rules:</p> <p>0 <= x1, x2 <= 704; 0 <= y1, y2 <= 576;</p> <p>x1 <= x2; y1 <= y2</p>
<p>P14221=<int></p>	<p>GDS3710 GDS3712</p>	<p><0 1 2 3 4 5 6 7 8 9 10></p>	<p>Select Alarm Schedule</p> <p>0: All Day</p> <p>1: Schedule1</p> <p>2: Schedule2</p> <p>3: Schedule3</p> <p>4: Schedule4</p> <p>5: Schedule5</p> <p>6: Schedule6</p> <p>7: Schedule7</p> <p>8: Schedule8</p> <p>9: Schedule9</p> <p>10: Schedule10</p>

P14222=<int>	GDS3710 GDS3712	<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 GDS3712/GDS3702	<0 1 2 3 4>	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 GDS3712/GDS3702	<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 GDS3712/GDS3702	<0 1>	Digit Input 1 Door Control Abnormal Options 0: Door 1 1: Door 2
P15431=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Digit Input 1 Status 0:Normal Open 1:Normal Close

P14321=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2 3 4 5 6 7 8 9>	<p>Select Alarm Schedule 1</p> <p>0: All Day</p> <p>1: Schedule1</p> <p>2: Schedule2</p> <p>3: Schedule3</p> <p>4: Schedule4</p> <p>5: Schedule5</p> <p>6: Schedule6</p> <p>7: Schedule7</p> <p>8: Schedule8</p> <p>9: Schedule9</p> <p>10: Schedule10</p>
P14322=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<1 2 3 4 5 6 7 8 9 10>	<p>Select Alarm Action Profile 1</p> <p>1: profile1</p> <p>2: profile2</p> <p>3: profile3</p> <p>4: profile4</p> <p>5: profile5</p> <p>6: profile6</p> <p>7: profile7</p> <p>8: profile8</p> <p>9: profile9</p> <p>10: profile10</p>
P14325=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2 3 4>	<p>Action of Alarm Input Channel 1</p> <p>0: Disable</p> <p>1: Alarm Input</p> <p>2: Open Door</p> <p>3: Abnormal Door Control</p> <p>4: Door Status Check</p>

P15452=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<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 GDS3712/GDS3702	<0 1>	Digit Input 2 Door Control Abnormal Options 0: Door 1 1: Door 2
P15432=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Digit Input 2 Status 0:Normal Open 1:Normal Close
P14326=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<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 GDS3712/GDS3702	<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 GDS3712/GDS3702	<0 1 2 3 4 5 10 15 20 25 30 60 300 900>	Alarm Output Duration (Seconds) 0: Always 1: 1s 2: 2s 3: 3s 4: 4s 5: 5s (Default) 10: 10s 15: 15s 20: 20s 25: 25s 30: 30s 60: 60s 300: 300s 900: 900s
P15581=<int>	GDS3705/GDS3702	<0 1>	Turn Off Alarm Output After Hang up Alarm Call 0: Disable 1: Enable
P10467=<int>	GDS3710/GDS3705	<0 1>	Enable Hostage Code 0: Disable 1: Enable

P10466= <string>	GDS3710/GDS3705		Hostage Code: All digits string Max. Length = 10
P10468= <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
P14350= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Tamper Alarm 0: Disable 1: Enable
P14355= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<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/GDS3705	<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>	<p>Select Alarm Action Profile</p> <p>1: profile1</p> <p>2: profile2</p> <p>3: profile3</p> <p>4: profile4</p> <p>5: profile5</p> <p>6: profile6</p> <p>7: profile7</p> <p>8: profile8</p> <p>9: profile9</p> <p>10: profile10</p>
P15407=<int>	GDS3710/GDS3705	<0 1>	<p>Enable Non-scheduled Access Alarm</p> <p>0: Disable</p> <p>1: Enable</p>
P15408=<int>	GDS3710/GDS3705	<1 2 3 4 5 6 7 8 9 10>	<p>Select Alarm Action Profile</p> <p>1: profile1</p> <p>2: profile2</p> <p>3: profile3</p> <p>4: profile4</p> <p>5: profile5</p> <p>6: profile6</p> <p>7: profile7</p> <p>8: profile8</p> <p>9: profile9</p> <p>10: profile10</p>
P15515=<int>	GDS3710/GDS3705	<0 1>	<p>Enable Unauthorized Door Opening Attempt Alarm</p> <p>0: Disable</p> <p>1: Enable</p>
P15610=<int>	GDS3705/GDS3702	<0 1>	<p>Enable SIP Calling Trigger Alarm Output</p> <p>0: Disable</p> <p>1: Enable</p>

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
--------------	-----------------	------------------------	---

Alarm Schedule Configuration

Support **cmd= get/set**

Get:

[[http](#)][https](#)://<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](#)][https](#)://<servername>/goform/config?cmd=set&<parameter>=<value>...

<parameter>= <value>	Model Supported	Valu es	Description
P14200=<string>			e.g.:
P14201=<string>			<P14201>schedule2,0@0830@1459,0@1500@1820,</P14201>
P14202=<string>			schedule2 is a revisable name for a time period, Max. Length = 20
P14203=<string>	GDS3710/GDS		1 st @ represent date of the week, 0-6, Sunday to Saturday
P14204=<string>	3705		2 nd @ the pre-four digits represent start time of that period, 0830 represent 08:30 in 24 hour format;
P14205=<string>	GDS3712/GDS		2 nd @ the post-four digits represent end time of that period, 1459 represent 14:59 in 24 hour format.
P14206=<string>	3702		
P14207=<string>			NOTE:
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.

Alarm Action Configuration

Support **cmd= get/set**

Get:

[[http|https](http://<servername>/goform/config?cmd=get&type=alarm_profile)://<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@0,0,0,0,0,0,0</P14300>
<P14301>profile2@0,0,0,0,0,0,0,</P14301>
<P14302>profile3@0,0,0,0,0,0,0,</P14302>
<P14303>profile4@0,0,0,0,0,0,0,</P14303>
<P14304>profile5@0,0,0,0,0,0,0,</P14304>
<P14305>profile6@0,0,0,0,0,0,0,</P14305>
<P14306>profile7@0,0,0,0,0,0,0,</P14306>
<P14307>profile8@0,0,0,0,0,0,0,</P14307>
<P14308>profile9@0,0,0,0,0,0,0,</P14308>
<P14309>profile10@0,0,0,0,0,0,0,</P14309>
</Configuration>
```

Set:

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

<parameter>= <value>	Model Supported	Values	Description
P14300=<string> P14301=<string> P14302=<string> P14303=<string> P14304=<string> P14305=<string> P14306=<string> P14307=<string> P14308=<string> P14309=<string>	GDS3710/GDS3705 GDS3712/GDS3702		<p>e.g.: <P14300>profile1@0,0,0,0,0,0</P14300></p> <p>Profile1 is revisable name of alarm action, Max. Length = 20</p> <p>1st digit after @ represents whether "Upload to Alarm Center": 0: Disable 1: Enable</p> <p>2nd digit after @ represents whether "Sound Alarm" 0: Disable 1: Enable</p> <p>3rd digit after @ represents whether "Voice Alarm to SIP Phone" 0: Disable 1: Enable</p> <p>4th digit after @ represents whether "Alarm Output" 0: Disable 1: Enable</p> <p>5th digit after @ represents whether "Send Email" 0: Disable 1: Enable</p> <p>6th digit after @ represents whether "Upload JPEG" Snapshot 0: Disable 1: Enable</p>
test_alarm_action=< int >	GDS3710/GDS3705 GDS3712/GDS3702	1-10	Test for Alarm Action

Alarm Phone List

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

Get:

[http|https]://<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>
```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P10471= <string>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2 3 4>	Alarm Phone List 1 0: Auto 1: Account 1 2: Account 2 3: Account 3 4: Account 4
P10459= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Alarm Phone List 1
P15575= <string>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2 3 4>	Alarm Phone List 2 0: Auto 1: Account 1 2: Account 2 3: Account 3 4: Account 4
P15576= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Alarm Phone List 2

Email Settings

Support cmd= get/set

Get:

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

<parameter>= <value>	Model Supported	Values	Description
P10121= <string>	GDS3710/GDS3705 GDS3712/GDS3702		SMTP Mail Server
P10122= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Port of SMTP Server
P10123= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Sender's email address. Max. Length = 127
P10127= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Sender's Username, Max. Length = 63
P10128= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Sender's email password, Max. Length = 63
P14348= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Alarm to email address 1, Max. Length = 127
P14349= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Alarm to email address 2, Max. Length = 127

P10129=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	SSL Encryption 0: Disable 1: Enable
P10131=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Email Subject Max.length=512
P10132=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Email Content Max.length=2048

FTP Settings

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=ftp

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P10140>1</P10140>
<P14113>0</P14113>
<P14114>192.168.1.10</P14114>
<P14115>21</P14115>
<P14116>kevin</P14116>
<P14118>/</P14118>
</Configuration>
```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P14113=<int>	GDS3710 GDS3712	<0 1>	Storage Server Type 0: FTP 1: Central Storage (GDSManager Configure)

P14114=<string>	GDS3710 GDS3712		FTP Server IP or FQDN, Max. Length = 255
P14115=<int>	GDS3710 GDS3712		FTP Server Port, Max. Length = 5
P14116=<string>	GDS3710 GDS3712		FTP Username, Max. Length = 63
P14118=<string>	GDS3710 GDS3712		FTP Path, Max. Length = 255

Upgrade Configuration

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=upgrade

Set:

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

Example:

```

<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P6767>1</P6767>
<P192>fm.grandstream.com/gs</P192>
<P6768></P6768>
<P232></P232>
<P233></P233>
<P212>1</P212>
<P237>fm.grandstream.com/gs</P237>
<P1360></P1360>
<P234></P234>
<P235></P235>
<P6769></P6769>
<P1361></P1361>
<P1359></P1359>
<version_limit>1.0.3.1</version_limit>
<P193>10080</P193>
<P194>1</P194>
<P8463>1</P8463>
<P145>0</P145>
<P1414>0</P1414>
</Configuration>

```

o **P4428**

GET:[http|https]://<servername>/goform/config?cmd=get&type=upgrade

SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

<parameter> = <value>	Model Supported	Values	Description
P6767= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2>	Firmware Upgrade Method 0: TFTP 1: HTTP 2: HTTPS
P192= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Firmware Server Path
P6768= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Firmware HTTP/HTTPS Username

P6769= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Firmware HTTP/HTTPS Password
P232= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Firmware Upgrade File Prefix
P233= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Firmware Upgrade File Postfix
P193= <int>	GDS3710/GDS3705 GDS3712/GDS3702	60 – 525600	Automatic Upgrade Interval (m)
P194= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<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>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2>	Config Upgrade Method 0: TFTP 1: HTTP 2: HTTPS
P237= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Config Server Path
P1360= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Config HTTP/HTTPS Username
P1361= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Config HTTP/HTTPS Password
P234= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Config Upgrade File Prefix
P235= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Config Upgrade File Postfix
P1359= <string>	GDS3710/GDS3705 GDS3712/GDS3702		XML Config File Password
P145= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	DHCP Option 66 Override Server 0: Disable 1: Enable

P1414= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	3CX Auto Provision (for UCM Provisioning) 0: Disable 1: Enable
P8458= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Start Upgrade at Random Time 0: Disable 1: Enable
P285= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0-23>	Hour of the Day – Start Time
P8459= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0-23>	Hour of the Day – End Time
P286= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0-6>	Day of the Week – Week
P1411= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	DHCP Option 120 Override SIP Server 0: Disable 1: Enable
P8463= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Validate Server Certificates 0: Disable 1: Enable
P4428= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable SIP NOTIFY Authentication 0: Disable 1: Enable

Reboot & Reset

Support **cmd= reboot/reset/get/set**

Reboot:

[http|https]://<servername>/goform/config?cmd=reboot

Reset:

[http|https]://<servername>/goform/config?cmd=reset&P12055=<value>

<parameter> = <value>	Model Supported	Values	Description
P12055= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<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|https]://<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>
</Configuration>
```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P15540= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Auto Reboot Enable: 0: Disable 1: Enable
P15541= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0-7	Auto Reboot Enable Time (Week) 0: Everyday 1: Sunday 2: Monday 3: Tuesday 4: Wednesday 5: Thursday 6: Friday 7: Saturday
P15542= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Auto Reboot Enable Time (Hour and Minutes): Example: 23:12 -> 2312, 08:06 -> 0806

Syslog or Debug

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=debug

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P8402>0</P8402>
<P207>192.168.1.10</P207>
<P208>0</P208>
<P1387>0</P1387>
</Configuration>
```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P8402= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Syslog Protocol 0:UDP 1:SSL/TSL
P207= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Syslog Server IP or FQDN
P208= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2 3 4>	Syslog Level: 0: None 1: Debug 2: Info 3: Warning 4: Error
P1387= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Send SIP Log 0:No 1:Yes

Data Maintenance

Support **cmd=export/upload**

Export:

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

<parameter>= <value>	Model Supported	Values	Description
data_type= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	The type of system config file. 0: System Config Data(No include password) 1: System Config Data(Include password)

Upload:

[http|https]://<servername>/goform/config?cmd=upload&type=1

System Health Alert

Support **cmd= get/set**

Get:

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

<parameter>= <value>	Model Supported	Values	Description
P15900= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable System Health Alert 0: Disable 1: Enable

P15491=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Delivery Method 0: Real-time 1: Periodic
P15492=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<1-10080>	Alert Interval (m)
P15496=<string>	GDS3710/GDS3705 GDS3712/GDS3702		Email Title Max. Length=256
P15493=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	SIP Registration Status 0: Disable 1: Enable
P15494=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	System Running Status 0: Disable 1: Enable

Event Notification

Support **cmd= get/set**

Get:

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

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

P15410=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Enable Event Notification 0: Disable 1: Enable
P15417=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<1 2>	Via Type 1:HTTP 2:HTTPS
P15553=<int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	HTTP Method 0: POST 1: GET
P15413=<string>	GDS3710/GDS3705 GDS3712/GDS3702		HTTP Server URL: Format ip:port/path . Example: 192.168.1.2:80/ Max. Length=256
P15414=<string>	GDS3710/GDS3705 GDS3712/GDS3702		HTTP Server Username: If don't need the Username & Password to access the HTTP server, please keep empty. Max. Length=128
P15415=<string>	GDS3710/GDS3705 GDS3712/GDS3702		HTTP Server Password: If don't need the Username & Password to access the HTTP server, please keep empty. Max. Length=128
P15416=<string>	GDS3710/GDS3705 GDS3712/GDS3702		URL Template Default: {"mac":"\${MAC}","content":"\${WARNING_MSG}"}

Trusted CA Certificates

Support **cmd= get/set**

Get:

[http|https]://<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>

<P8475></P8475>

</Configuration>

```

Set:

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

<parameter> = <value>	Model Supported	Values	Description
P8433= <string> P8434= <string> P8435= <string> P8436= <string> P8437= <string> P8438= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Trusted CA Certificates
P8475= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Custom Certificate

System Status

Support **cmd= get**

Get:

[http|https]://<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>V1.5A</P917>
```

```
<P1397>9650001415A</P1397>
```

```
<P70>1.0.2.61</P70>
```

```
<P45>1.0.2.61</P45>
```

```
<P68>1.0.2.61</P68>
```

```
<P15009>1 hour 31 minutes</P15009>
```

```
<P499>0</P499>
```

```
</Configuration>
```

<parameter> = <value>	Model Supported	Values	Description
P89= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Product Model
P208= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1 2 3 4>	Hardware Version
P1397= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Part Number
P69= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Boot Version
P70= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Core Version
P45= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Base Version
P68= <string>	GDS3710/GDS3705 GDS3712/GDS3702		Program Version
P15009= <string>	GDS3710/GDS3705 GDS3712/GDS3702		System Up Time

P499= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	SIP Registered Status 0: Unregistered 1: Registered
Pfw_available_version = <string>	GDS3710/GDS3705 GDS3712/GDS3702		Firmware available version
Systemp= <string>	GDS3710/GDS3705 GDS3712/GDS3702		System Temperature
atp_in= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Tamper Sensor 0: Untriggered 1: Triggered
doorctrl0= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Door Control [1] 0: Untriggered 1: Triggered
doorctrl0= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Door Control 2 0: Untriggered 1: Triggered
doorctrl1= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Door Control 0: Untriggered 1: Triggered
do= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Digit Output 0: Untriggered 1: Triggered
di0= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Digit Input 1 0: Untriggered 1: Triggered
di1= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Digit Input 2 0: Untriggered 1: Triggered

Network Status

Support **cmd= get**

Get:

[http|https]://<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:AB:CC:BA</P67>
<P8>0</P8>
<P9>192</P9>
<P10>168</P10>
<P11>86</P11>
<P12>3</P12>
<P13>255</P13>
<P14>255</P14>
<P15>255</P15>
<P16>0</P16>
<P17>192</P17>
<P18>168</P18>
<P19>86</P19>
<P20>1</P20>
<P10107>0</P10107>
<P21>192</P21>
<P22>168</P22>
<P23>84</P23>
<P24>217</P24>
<P25>192</P25>
<P26>168</P26>
<P27>10</P27>
<P28>253</P28>
</Configuration>
```

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

P8= <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	IP Address Mode 0: DHCP 1: Static IP
P9= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	IP Address: P9. P10. P11. P12.
P10= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P11= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P12= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P13= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	Subnet Mask: P13. P14. P15. P16.
P14= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P15= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P16= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P17= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	Gateway: P17. P18. P19. P20.

P18=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P19=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P20=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P10107=<iint>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	DNS
P21=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	DNS Server 1 P21. P22. P23. P24.
P22=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P23=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P24=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P25=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	DNS Server 2 P25. P26. P27. P28.
P26=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P27=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	
P28=<int>	GDS3710/GDS3705 GDS3712/GDS3702	0 – 255	

Firmware Available Version Check

Support **cmd= fw_upgrade**

fw_upgrade:

[http|https]://<servername>/goform/config?cmd=fw_upgrade&type=num

<parameter> = <value>	Model Supported	Values	Description
type = <int>	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Operate type 0: check firmware available version 1: firmware upgrade

Card Data Import/Export

Support **cmd= export/upload**

Export:

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

Import:

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

<parameter> = <value>	Model Supported	Values	Description
type = <int>	GDS3710/GDS3705 GDS3712/GDS3702		type export type = 1 upload type = 0
data_type	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	Export data type 0 – .gs 1 – .csv
dupopt	GDS3710/GDS3705 GDS3712/GDS3702	<0 1>	For Duplicated Record operate type 0 – Skip 1- Overwrite

OpenVPN Settings

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

Get:

[http|https]://<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|https]://<servername>/goform/config?cmd=set<¶meter>=<value>...

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

SET:

[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

- o **P9902/ P9903/ P9904**

UPLOAD:

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

DEL:

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

<parameter> = <value>	Model Supported	Values	Description
P7050= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0, 1	OpenVPN® Enable 1. Disable 2. Enable

P7051= <string>	GDS3710/GDS3705 GDS3712/GDS3702	String	OpenVPN® Server Address Max. Length = 256
P7052= <int>	GDS3710/GDS3705 GDS3712/GDS3702	Integer: 0 – 65535	OpenVPN® Port Range: 0 ~ 65535
P2912= <int>	GDS3710/GDS3705 GDS3712/GDS3702	0, 1	OpenVPN® Transport 1. UDP 2. TCP
P9902	GDS3710/GDS3705 GDS3712/GDS3702	String	System_Settings.OpenVPN® Settings.Openvpn_CA Max. Length = 8192
P9903	GDS3710/GDS3705 GDS3712/GDS3702	String	System_Settings.OpenVPN® Settings.Openvpn_Client_Certificate Max. Length = 8192
P9904	GDS3710/GDS3705 GDS3712/GDS3702	String	System_Settings.OpenVPN® Settings.Openvpn_Client_Key Max. Length = 8192
P8394	GDS3710/GDS3705 GDS3712/GDS3702	String	OpenVPN® Username Max. Length = 256
P8395	GDS3710/GDS3705 GDS3712/GDS3702	String	OpenVPN® Password Max. Length = 256
P8396	GDS3710/GDS3705 GDS3712/GDS3702	0, 1, 2, 3	System_Settings. OpenVPN® Settings.Openvpn_Cipher_Method 0: Blowfish; 1: AES-128; 2: AES-256; 3: Triple-DES
P8460	GDS3710/GDS3705 GDS3712/GDS3702	String	System_Settings.OpenVPN® Settings.Additional_Options Max. Length = 1024

TR069 Settings

Support **cmd= get/set**

Get:

[http|https]://<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>
<P4504/>
<P4506>1</P4506>
<P4507>86400</P4507>
<P4511>000B829A8C95</P4511>
<P4518>7547</P4518>
<P8220/>
<P8221/>
<P4505/>
<P4512>000B829A8C95</P4512>
</Configuration>
```

Set:

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

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

SET:

[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

<parameter>=<value>	Model Supported	Values	Description
P1409=<int>	GDS3705/GDS3710 GDS3712/GDS3702	0, 1	Enable TR-069 0-Disable 1-Enable
P4503=<string>	GDS3705/GDS3710 GDS3712/GDS3702	String	ACS URL Max. Length = 1024

P4504= <string>	GDS3705/GDS3710 GDS3712/GDS3702	String	ACS Username Max. Length = 1024
P4505= <string>	GDS3705/GDS3710 GDS3712/GDS3702	String	ACS Password Max. Length = 128
P4506= <int>	GDS3705/GDS3710 GDS3712/GDS3702	0, 1	Periodic Inform Enable 0-Disable 1-Enable
P4507= <int>	GDS3705/GDS3710 GDS3712/GDS3702	0- 9999999999	Periodic Inform Interval (s)
P4511= <string>	GDS3705/GDS3710 GDS3712/GDS3702	String	Connection Request Username Max. Length = 1024
P4512= <string>	GDS3705/GDS3710 GDS3712/GDS3702	String	Connection Request Password Max. Length = 128
P4518= <string>	GDS3705/GDS3710 GDS3712/GDS3702	1-65535	Connection Request Port
P8220= <string>	GDS3705/GDS3710 GDS3712/GDS3702	String	CPE Cert File Max. Length = 2048
P8221= <string>	GDS3705/GDS3710 GDS3712/GDS3702	String	CPE Cert Key Max. Length = 2048

SNMP Settings

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type=snmp

Example:

```

<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P21896>1</ P21896>
<P21904>1</P21904>
</Configuration>

```

Set:

[http|https]://<servername>/goform/config?cmd=set<¶meter>=<value>...

SET:

[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

<parameter> = <value>	Model Supported	Values	Description
P21896= <int>	GDS3710/GDS3712	<0 1>	Enable SNMP 0: Disable 1: Enable
P21904= <int>	GDS3710/GDS3712	<1 2 3>	SNMP Version 1: Version 1 2: Version 2 3: Version 3
P21903= <int>	GDS3710/GDS3712	161 or 1025-65535	SNMP Port
P21902= <string>	GDS3710/GDS3712		SNMPv1/v2 Community Max. Length =64
P21899= <int>	GDS3710/GDS3712	<1 2 3>	SNMP Trap Version 1: Version 1 2: Version 2 3: Version 3
P21897= <string>	GDS3710/GDS3712		SNMP Trap IP Address Max.length=16
P21898= <int>	GDS3710/GDS3712	162 or 1025-65535	SNMP Trap Port
P21901= <int>	GDS3710/GDS3712	1-1440	SNMP Trap Inerval

P21900=<string>	GDS3710/GDS3712		SNMPv1/v2 Trap Community Max.length=64
P21905=<string>	GDS3710/GDS3712		SNMPv3 Username Max.length=128
P21910=<int>	GDS3710/GDS3712	<0 1 2>	SNMPv3 Security Level 0: noAuthUser 1: authUser 2: privUser
P21906=<int>	GDS3710/GDS3712	<0 1 2>	SNMPv3 Authentication Protocol 0: None 1: MD5 2: SHA
P21907=<int>	GDS3710/GDS3712	<0 1 2>	SNMPv3 Privacy Protocol 0: None 1: DES 2: AES
P21908=<string>	GDS3710/GDS3712		SNMPv3 Authentication Key Max.length=2048
P21909=<string>	GDS3710/GDS3712		SNMPv3 Privacy Key Max.length=2048
P21911=<string>	GDS3710/GDS3712		SNMPv3 Trap Username Max.length=128
P21916=<int>	GDS3710/GDS3712	<0 1 2>	SNMPv3 Trap Security Level 0: noAuthUser 1: authUser 2: privUser
P21912=<int>	GDS3710/GDS3712	<0 1 2>	SNMPv3 Trap Authentication Protocol 0: None 1: MD5 2: SHA

P21913	GDS3710/GDS3712	<0 1 2>	SNMPv3 Trap Privacy Protocol 0: None 1: DES 2: AES
P21914	GDS3710/GDS3712		SNMPv3 Trap Authentication Key Max.lenth=2048
P21915	GDS3710/GDS3712		SNMPv3 Trap privacy Key Max.lenth=2048

Packet Capture

Support **cmd= get/set**

Get:

[http|https]://<servername>/goform/config?cmd=get&type= capture

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
<ResCode>0</ResCode>
<RetMsg>OK</RetMsg>
<P6008>0</P6008>
<P22419>0</ P22419>
</Configuration>
```

Set:

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

SET:

[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

<parameter>=<value>	Model Supported	Values	Description
P6008=<int>	GDS3710/GDS3712	<0 1>	With RTP Packets 0: No 1: Yes

P22419=<int>	GDS3710/GDS3712	<0 1>	With Secret Key Information 0: No 1: Yes
--------------	-----------------	-------	--

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

General Parameter Revision

Authentication verification required First

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 (**NOTE:** *type=0 means login authentication verification required*)

```
[http|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)

```
[http|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 "ChallengeCode" is the returned string from Server in **Step 1**.
- password is the web login password of the device (GDS37xx)
- Authcode string must be length of 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.*

Parameters can ONLY be adjusted after successful authentication verification

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 above RED part "Cookie" is the returned verification message of the successful authentication in Login Verification at **Step 2**.

Snapshots

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: (NOTE: type=1 means MJPEG/JPEG obtain login authentication verification)

Client → Server

```
[http|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 must be length of 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_undef=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 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.

Step3:

Client → Server

[http|https]://<servername>/snapshot/view

[http|https]://<servername>/snapshot/view?res=stream_flag

NOTE:

- **Step 3** should be finish within **30 seconds** after authentication OK, otherwise the authentication will be invalid.
- The timer that records authentication valid time will refresh if **Step 3** executes successfully.
- The timer when using `https://<servername>/snapshot/view.jpg` to obtain snapshot will start counting from 0, within 30 seconds if the same request asking for snapshot again, the timer will reset; otherwise the request without verified message will be timed out and the verification will be void. New verification is required when obtain snapshot again.
- The snapshot is using internal 4th stream, with MJPEG video codec and fixed resolution 1280 x 720
- Stream_flag mean resolution: 1/2/other. 1mean 1920*1080 2:640*480, other: 1280*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:GDS3710DyTIHwNgZ: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 as shown below:

```
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 Username 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**.

MJPEG Stream (Encryption Mode or Basic Mode)

MJPEG Authentication: 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.

MJPEG Challenge/Response Authentication at Default Mode

Select "Challenge + Response" from WebUI: "System Settings → Access Settings → MJPEG Authentication Mode" to obtain the default MJPEG stream (internal 4th stream) with 1280×720 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=<authcodestring>&idcode=id_code
```

NOTE:

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

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></RetMsg>
<ChallengeCode> 9c07f92ea2ab55c2d7ef433e5fa163a0</ChallengeCode>
<IDCode> QDOJBDQBT8MJ7WRVCZ7L</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=QDOJBDQBT8MJ7WRVCZ7L
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 successfully retrieved.

Obtain MJPEG stream at specified stream channel

Select "Challenge + Response" from WebUI: "System Settings → Access Settings → MJPEG Authentication Mode" to obtain the specified channel stream.

NOTE:

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

Step 1:

Client → Server

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

X: 0/1/2 (0 means 1st MJPEG stream, 1 means 2nd and 2 means 3rd MJPEG stream.)

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
```

X: 0/1/2 (0 means 1st MJPEG stream, 1 means 2nd and 2 means 3rd MJPEG stream.)

NOTE:

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

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 successfully.

MJPEG Basic 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 1280×720 resolution.

Client → Server

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

NOTE:

- Username: web login username; password: web login password

Below is an **Example**:

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.

MJPEG Basic Authentication For Recommended Method

Select "Basic" from WebUI: "System Settings → Access Settings → MJPEG Authentication Mode" to obtain the specified channel stream.

NOTE:

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

Client → Server

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

X: 0/1/2 (0 means 1st MJPEG stream, 1 means 2nd and 2 means 3rd MJPEG stream.)

NOTE:

- o Username: web login username; password: web login password
- o Below is an Example to get 2nd MJPEG Stream:
- o 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

MJPEG video or Snapshot image via HTTP API to 3rd party System Integration

For easy system integration (with the cost of less secure), once the feature enabled (default is disabled), user can send HTTP API with correct credentials to retrieve MJPEG video or JPEG snapshot from GDS371X, similar to the behavior of Grandstream IP Cameras.

The HTTP API or CLI command listed as below:

MJPEG Video:

[http\(s\)://admin:password@IP_GDS371X:Port/jpeg/mjpeg.html](http(s)://admin:password@IP_GDS371X:Port/jpeg/mjpeg.html)

JPEG Snapshot:

[http\(s\)://admin:password@IP_GDS371X:Port/jpeg/view.html](http(s)://admin:password@IP_GDS371X:Port/jpeg/view.html)

Anonymous Liveview / Snapshot/Stream

Enable "Enable Anonymous LiveView" in the "Access Settings" WebUI page

MJPEG Video:

[http\(s\)://IP_GDS371X:Port/videoview.html](http(s)://IP_GDS371X:Port/videoview.html)

JPEG Snapshot:

[http\(s\)://IP_GDS371X:Port/anonymous/snapshot/view.html](http(s)://IP_GDS371X:Port/anonymous/snapshot/view.html)

http(s)://IP_GDS371X:Port/anonymous/snapshot/view?res=stream_flag

stream_flag mean resolution: 1/2/other, 1mean 1920*1080, 2 mean 640*480, the value mean 1280*720

MJPEG Stream:

http(s)://IP_GDS371X:Port/anonymous/jpeg/stream=X

X: 0/1/2 (0 means 1st MJPEG stream, 1 means 2nd and 2 means 3rd MJPEG stream. MJPEG must be selected in the Preferred Video Codec for this to work.)

X: 3 (3 means the default MJPEG stream (internal 4th stream) with 1280×720 resolution)

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_GDS371X:Port/X

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

HTTP API to Open Door

Note

HTTP API Open Door settings require the option "Enable HTTP API Remote Open Door" Under **Door System Settings => Basic Settings** to be set to Challenge + Response Authentication.
This option is disabled by default

HTTP API Open Door basic on Challenge + Response 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.

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=<authcodestring>&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 message 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 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.

Server → Client

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>
```

NOTE:

- The RED 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 successfully.
- The user must be "admin", others do not have the privilege.
- Default validity of the idcodestring come from step 1 is 30 second, it is mean that user must finish the step 2 in 30 second, or the idcodestring will timeout and invalid. **(This parameter can only be configured via P value)**
- The "type=1" mean that the HTTP API is for open door.
- Authcode string must be length of 32 in lowercase hex as in MD5 hash.

HTTP API Open Door basic on Basic Authentication: The authentication is using simple username and password.

Client → Server

```
<http|https>://username:password@<servername>/goform/apicmd?remotepin=PIN_string&type=opt_type
```

NOTE:

- Username: web login username; password: web login password
- PIN_string: Remote PIN to Open Door
- opt_type: **opt_type = 1: open door, 2: close door**

Direct Login

GDS371X support HTTP API direct login

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

The header of response message:

```
HTTP/1.0 302 OK
Content-Type: text/xml;charset=UTF-8
Location: index.html
Set-Cookie: session=33d4d8f24c57313dd385a722e079c451;path=/;
Set-Cookie: uname=admin;path=/;
```

The RED is the authentication message need include in require header for next time.

HTTP SIP DIAL

cmd= <string>	call	http sip call cmd
call_type= <int>	<0 1>	0:end call 1:call
call_num= <string>		call num or IP

CHANGE LOG

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

Firmware Version 1.0.0.46

- Added "[Enable White Backlight on Time Interval](#)"

Firmware Version 1.0.0.45

- Added "Email Notification When Door Opened" ([P15593](#))
- Added "Onhook Timer After Remote Open Door" ([P15582](#))
- Updated "Alarm Output Duration (s)" ([P14341](#))

Firmware Version 1.0.0.44

- Added "[Emergency PIN to Re-enable Keep Door Open](#)"
- Added "[Snapshot Delay When Door Opened/Doorbell Pressed \(s\)](#)"
- Added "[Minimum TLS Version](#)" && "[Maximum TLS Version](#)"
- Added "[HTTP API Open Door Compatibility Mode](#)"

Firmware Version 1.0.0.43

- Added "[Check Domain Certificates](#)"
- Added Schedule for "[Keep Door Open](#)"

Firmware Version 1.0.0.42

- Added [SNMP](#)

Firmware Version 1.0.0.41

- Added: [Number 2/3/4 Called When Door Bell Pressed](#)

Firmware Version 1.0.0.40

- Added option to Enable/Disable [SIP NOTIFY Authentication](#)

Firmware Version 1.0.0.39

- Added SIP URI Scheme When Using TLS ([P2329/P2429/P2529/P2629](#))
- Added Support SIP Instance ID ([P288/P489/P589/P69](#))

Firmware Version 1.0.0.38

- Added [TR-069](#) for GDS3710

Firmware Version 1.0.0.37

- Added "Add MAC in User-Agent" ([P26061/P26161/P26261/P26361](#))
- Added "Codec Negotiation Priority" ([P29061/P29161/P29261/P29361](#))
- Added Event Notification HTTP Method ([P15553](#))

Firmware Version 1.0.0.36

- Added Key Sensitivity Level ([P15544](#)) for GDS3710
- Added One-way Interlocking Doors Mode ([P15543](#))
- Updated [P14320/P14325](#) value range.
- Added Configurable [Auto Reboot](#)

Firmware Version 1.0.0.35

- Updated the title "[P26058/P26158/P26258/P26358](#))

Firmware Version 1.0.0.34

- Updated [P15440](#) range to 0-2
- Added values [P15444/P15445/P15446](#)
- Added TR069 Pvalues: [P1409/P4503/P4504/P4505/P4506//P4507/P4511/P4512/P4518/P8220/P8221](#)

Firmware Version 1.0.0.33

- Added [P15515](#) Enable Unauthorized Door Opening Attempt Alarm.
- Add [P15516](#) Enable Unauthorized Door Opening Attempt Alarm Action Profile.

Firmware Version 1.0.0.32

- Added [P15514](#), Enable PIN/Password Display (HTTPS)

Firmware Version 1.0.0.31

- Added [P4428](#), for "Maintenance=> Upgrade=> Disable SIP NOTIFY Authentication"

Firmware Version 1.0.0.30

- Added [P7050/P7051/P7052/P2912/P9902/P9903/P9904/P8394/P8395/P8396/P8460](#)

Firmware Version 1.0.0.29

- Added [P15440/ P15441/ P15442/ P15443](#)

Firmware Version 1.0.0.28

- Added [P2395/P2595/P2695](#)

Firmware Version 1.0.0.27

- Updated [Unlock hold time](#), MAX to 1800

Firmware Version 1.0.0.26

- Added [RTSP Password](#).

Firmware Version 1.0.0.25

- Added "[Abnormal Door Control](#)"

Firmware Version 1.0.0.24

- Added "[Holiday Mode](#)" For "[Keep Door Open](#)"

Firmware Version 1.0.0.23

- Added SIP account "[Voice Frames Per TX](#)" & "[Re-register before Expiration](#)" & Preferred Vocoder "[DHCP Option 42](#)" & [Start Upgrade at Random Time](#) for GDS3705.

Firmware Version 1.0.0.22

- Deleted "[G.729A/B](#)" option at "[Preferred Audio Codec](#)"

Firmware Version 1.0.0.21

- Update P100 to [P198](#)

Firmware Version 1.0.0.20

- Updated [JPEG](#) (SNAPSHOT)

Firmware Version 1.0.0.19

- Added "[DHCP Option 120 Override SIP Server](#)" & "[Voice Frames Per TX](#)"

Firmware Version 1.0.0.18

- Added "[DTMF Payload Type](#)"

Firmware Version 1.0.0.17

- Updated title string

Firmware Version 1.0.0.16

- Added [Multi-SIP account](#).

Firmware Version 1.0.0.15

- Added "[Authcode string must be lowercase](#)"

Firmware Version 1.0.0.14

- Mark red color for some key word about HTTP API.

Firmware Version 1.0.0.13

- Updated [P15436](#) (No Key Input Timeout (s)) for GDS3710.
- Added [P2305/P2405/P2505/P2605](#)(Outbound Proxy Mode) for GDS3705
- Added [P15476](#) (Allow/disallow Reset via SIP NOTIFY) for GDS3705

Firmware Version 1.0.0.12

- Added [P15476](#) (Allow/disallow Reset via SIP NOTIFY) for GDS3710

Firmware Version 1.0.0.11

- Added [Alarm Out](#) P value for GDS3710

Firmware Version 1.0.0.10

- Added [P15431](#), [P15432](#) and 4 SIP Accounts for GDS3705

Firmware Version 1.0.0.9

- Added "[fw_upgrade check](#)" API
- Added CSV file format support for [import/export card users](#)
- Added new P value [P15418](#) and [P15434](#)

Firmware Version 1.0.0.8

- Added [P2392](#), [P15419](#)
- Updated [P443](#)
- Updateed [JPEG & MJPEG](#) Stream

Firmware Version 1.0.0.7

- Added Methods to Get [MJPEG](#)

Firmware Version 1.0.0.5

- Added "[Keep Door Open, Non-scheduled Access Alarm, Test_Alarm_Action](#)"

Firmware Version 1.0.0.4

- Added support for GDS3705

Firmware Version 1.0.0.3

- Added option "[Validate Server Certificates](#)"

Firmware Version 1.0.0.2

- Added HTTP API Open Door

Firmware Version 1.0.0.1

- Card Issuing State Expire Time (m) — [P15423](#) (value:1-1440)

Firmware Version 1.0.0.0

- This is the initial version

Can't find the answer you're looking for? Don't worry we're here to help!

[CONTACT SUPPORT](#)