GDS3705 Firmware Release Note

Table of Content

Table of Content 1

FIRMWARE VERSION 1.0.3.10 8

PRODUCT NAME 8
DATE 8
SUMMARY OF UPDATE 8
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 8
BUG FIX 9
ENHANCEMENT 10
KNOWN ISSUES 10
NEW HTTP API 11
NEW P-VALUE 11
NEW FEATURES OVERVIEW 12
TR069/GDMS SUPPORT 12

FIRMWARE VERSION 1.0.1.21 14

PRODUCT NAME 14
DATE 14
SUMMARY OF UPDATE 14
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 14
BUG FIX 14
ENHANCEMENT 15
KNOWN ISSUES 15
NEW HTTP API 16
NEW P-VALUE 17
NEW FEATURES OVERVIEW 18
CISCO WEBEX COMPATABIE 18
3CX IOT COMPATABLE 20
CONFIGURABLE KEYPAD BLUE LIGHT ON/OFF 21
UNAUTHORIZED CARD SWIPE (WIEGAND READER) ALERTED IN EVENT LOG 22
INCREASED WHITELIST IN EACH ACCOUNT 23

FIRMWARE VERSION 1.0.1.16 25

PRODUCT NAME 25

DATE 25
SUMMARY OF UPDATE 25
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 25
BUG FIX 25
ENHANCEMENT 26
KNOWN ISSUES 26
NEW HTTP API 27
NEW P-VALUE 27
NEW FEATURES OVERVIEW 28
PAIR WITH GSC3570 OPEN DOOR W/O SIP CALL 28
SCHEDULED AUTO REBOOT 31
ENHANCED OPEN DOOR VIA 3RD PARTY WEBRELAY WITH ON/OFF URL 32
ALARM ACTION WHEN ILLEGAL CARD SWIPED 34
MODIFIED CARD MANAGEMENT PAGE 35
WEBUI PASSWORD DISPLAY WITH SECUIRTY AND CONVENIENCE 36
GSC3570 SECURE OPEN DOOR BY PAIRING WITH GDS37XX 37
ADDED SIP ACCOUNT ACTIVE FEATURE 40
ADD "GMT-3:30" TIME ZONE SUPPORT 41

FIRMWARE VERSION 1.0.1.11 42

PRODUCT NAME 42
DATE 42
SUMMARY OF UPDATE 42
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 42
BUG FIX 42
ENHANCEMENT 43
KNOWN ISSUES 43
NEW HTTP API 44
NEW P-VALUE 44
MODIFIED P-VALUE 45
NEW FEATURES OVERVIEW 46
SUPPORT WEBRELAY OPEN DOOR 46
SUPPORT OPEN VPN 47
ADDED CALL TERMINATION BUTTON IN WEBUI 48
INCREASED UNLOK HOLDING TIME TO 30 MINUTES 49
CHANGED SIP ACCOUNT NAME TO DISPLAY NAME 50
ADDED REBOOT/RESYNC VIA SIP NOTIFY 51

FIRMWARE VERSION 1.0.1.6 52

PRODUCT NAME 52
DATE 52

SUMMARY OF UPDATE 52
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 52
BUG FIX 52
ENHANCEMENT 53
KNOWN ISSUES 53
NEW HTTP API 54
NEW P-VALUE 54
MODIFIED P-VALUE 54
NEW FEATURES OVERVIEW 55
SUPPORT FAILOVER MECHANISM ON DNS SRV 55
SIREN ALARMING WHEN DOOR OPENED ABNORMALLY (SPECIAL WIRING REQUIRED) 57
SUPPORT HOLIDAYS IN KEEP DOOR OPEN SCHEDULE 61
RESET FACTORY PASSWORD VIA SPECIAL KEY COMBINATION OPERATION 62

FIRMWARE VERSION 1.0.1.3 64

PRODUCT NAME 64
DATE 64
SUMMARY OF UPDATE 64
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 64
BUG FIX 64
ENHANCEMENT 65
KNOWN ISSUES 65
NEW HTTP API 66
NEW P-VALUE 67
MODIFIED P-VALUE 67
NEW FEATURES OVERVIEW 68
Advanced SIP Settings for ITSPs: Re-register & Accept incoming calls from Proxy Only 68
DHCP Option 42 69
DNS SRV Support 70
Multiple Audio Codecs and Voice Frame Per TX Support 71
Set Schedule for Upgrade/Provisioning 72
Separate Credentials for GDSManager 73

FIRMWARE VERSION 1.0.0.41 75

PRODUCT NAME 75
DATE 75
SUMMARY OF UPDATE 75
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 75
BUG FIX 75
ENHANCEMENT 76
KNOWN ISSUES 76

NEW HTTP API 77
NEW P-VALUE 78
MODIFIED P-VALUE 78
NEW FEATURES OVERVIEW 79
SYSTEM HEALTH ALERT 79
ENABLE/DISABLE WEB ACCESS 80
NO KEY INPUT TIMEOUT 81
OPEN DOOR VIA DIGITS ONLY PRIVATE PIN 83
SET SCHEDULE FOR LOCAL PIN OPEN DOOR 84
SYNCHRONIZE "KEEP DOOR OPEN" WITH GDSMANAGER 87
DTMF PAYLOAD AND RTCP/RTCP-XR 89
ALMOUT1 CONTROL DOOR2 91
NORMAL OPEN/CLOSE IN ALMOUT1 (COM1) DOOR2 CONTROL 96
ADDED BOOT VERSION IN "STATUS" PAGE 97

FIRMWARE VERSION 1.0.0.37 98

PRODUCT NAME 98
DATE 98
SUMMARY OF UPDATE 98
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 98
BUG FIX 98
ENHANCEMENT 98
KNOWN ISSUES 99
NEW HTTP API 99
NEW P-VALUE 99
NEW FEATURES OVERVIEW 100
OPTION OF OUTBOUND PROXY MODE 100
CONFIG FIRMWARE OR CONFIGURATION SERVER PATH AND ICMP TEST VIA SSH 101

FIRMWARE VERSION 1.0.0.36 103

PRODUCT NAME 103
DATE 103
SUMMARY OF UPDATE 103
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 103
BUG FIX 103
ENHANCEMENT 103
KNOWN ISSUES 104
NEW HTTP API 104
NEW P-VALUE 104
NEW FEATURES OVERVIEW 105
CUSTOM CERTIFICATE 105

INVISIBLE SIP PASSWORD *106*
SPECIAL SIP USER ID *107*
EXTENDED VLAN RANGE 0 ~ 4094 ..... *108*
DISPLAY TEMPERATURE IN FAHRENHEIT *109*

FIRMWARE VERSION 1.0.0.35 110

PRODUCT NAME 110
DATE 110
SUMMARY OF UPDATE 110
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 110
BUG FIX 110
ENHANCEMENT 111
KNOWN ISSUES 111
NEW HTTP API 112
NEW P-VALUE 113
NEW FEATURES OVERVIEW 117
MULTIPLE SIP ACCOUNTS *117*

FIRMWARE VERSION 1.0.0.31 130

PRODUCT NAME 130
DATE 130
SUMMARY OF UPDATE 130
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 130
BUG FIX 130
ENHANCEMENT 131
KNOWN ISSUES 131
NEW HTTP API/P-VALUE 131

FIRMWARE VERSION 1.0.0.28 132

PRODUCT NAME 132
DATE 132
SUMMARY OF UPDATE 132
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 132
BUG FIX 132
ENHANCEMENT 132
KNOWN ISSUES 133
NEW HTTP API/P-VALUE 133
NEW FEATURES OVERVIEW 134
HTTP API OPEN DOOR *134*
NON-SCHEDULED ACCESS ALARM *135*
"TEST" BUTTON IN ALARM ACTION *136*

LOG NOTIFICATION TYPE *137*
OPEN DOOR BY CONFIGURED SCHEDULE OR TIME WINDOW *138*
MORE INFORMAITON IN SYSTEM INFO PAGE *139*

FIRMWARE VERSION 1.0.0.26 140

PRODUCT NAME 140
DATE 140
SUMMARY OF UPDATE 140
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 140
BUG FIX 140
ENHANCEMENT 140
KNOWN ISSUES 141
NEW P-VALUE 141
NEW HTTP API 142
NEW FEATURES OVERVIEW 143
EVENT NOTIFICATION *143*
TRUSTED CA CERTIFICATES *144*
CARD MANAGEMENT – Valid Start/End Date for Card/User *145*
PASSWORD RECOVER EMAIL CONFIGURATION *146*

FIRMWARE VERSION 1.0.0.23 151

PRODUCT NAME 151
DATE 151
SUMMARY OF UPDATE 151
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 151
BUG FIX 151
ENHANCEMENT 151
KNOWN ISSUES 151
NEW P-VALUE 152
NEW HTTP API 152
NEW FEATURES OVERVIEW 153
EVENT NOTIFICATION *153*
SYSTEM INFO *154*

FIRMWARE VERSION 1.0.0.20 156

PRODUCT NAME 156
DATE 156
SUMMARY OF UPDATE 156
FIRMWARE APPLIES TO BELOW HW VERSION ONLY 156
BUG FIX 156
KNOWN ISSUES 156

NEW P-VALUE 157
NEW HTTP API 157

FIRMWARE VERSION 1.0.3.10

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B, 3.0A, 3.1A, 3.2A**)*

DATE

03/28/2022

SUMMARY OF UPDATE

This firmware of GDS3705 is mainly for bug fixes, feature enhancement, and new HW support.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal WebUI or missing parameters in the GUI. Please backup the data and configuration before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version, not able to downgrade
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version, not able to downgrade
GDS3705 HW3.0A	YES	
GDS3705 HW3.1A	YES	FW1.0.1.21 as Initial Version for this HW version, not able to downgrade
GDS3705 HW3.2A	YES	FW1.0.1.21 as Initial Version for this HW version, not able to downgrade

BUG FIX

- Fixed system health alert enabled but device will not trigger email alert in probability after reboot.
- Fixed system health alert interval option is invalid.
- Fixed system health alert email only contains the info of sip account.
- Fixed alarm triggered but device failed to send out email.
- Fixed “Disable SIP NOTIFY Authentication” needs reboot to take effect.
- Fixed GDMS: device should not reboot during call
- Fixed the wrong prompt when device is saving data.
- Fixed default value of HTTP method is POST.
- Fixed doorbell value set to “0” cannot be saved.
- Fixed swiping legal card in unauthorized schedule will trigger both Non-scheduled Access Alarm and Non-authorized RFID Card Access Alarm (this one should not be triggered).
- Fixed login error prompt incorrect.
- Fixed DUT not sending out system health alert after revise/update SIP account information.
- Fixed non-scheduled access not logged in event log.
- Fixed when “Disable Keypad SIP Number Dialing” enabled, device cannot open door when private PIN is more than 9 digits.
- Fixed non-scheduled access alarm call can be cancelled by pressing the doorbell key.
- Fixed some parameters not able to configure successfully via GDMS.
- Fixed when set DI_1 to abnormal door control and DI_2 disabled, DI_2 still has door1/door2 displayed.
- Fixed group name more than 63 characters should be able to be chopped and saved.
- Fixed GDMS templated value not matching webUI value not updated.
- Fixed wrong default value of “Disable SIP NOTIFY Authentication”, make it consistent with all devices
- Fixed device initial response to RFID/PIN very slow after reboot or idle for a while.
- Fixed the ringing timeout P value in GDMS template is wrong.
- Fixed alarm triggered but device not sending alarm email to “Alarm-To Email Address 2”
- Fixed enable whitelist the device will lose key tone after reject the call by replying 486.
- Fixed device reboot during DTMF open door performance testing.
- Fixed device cannot apply config file via UCM Zero Config.
- Fixed using custom certificate would fail the upgrade.
- Fixed wrong prompt when configure/save a holiday name already exist.

ENHANCEMENT

- Added TR069/GDMS support

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping even after pressing phone's keypad which supposedly should stop the siren audio at SIP phone side.

NEW HTTP API

- **N/A**

NEW P-VALUE

- **N/A**

NEW FEATURES OVERVIEW

This section lists major new features or improvement and advise customers how to use them.

TR069/GDMS SUPPORT

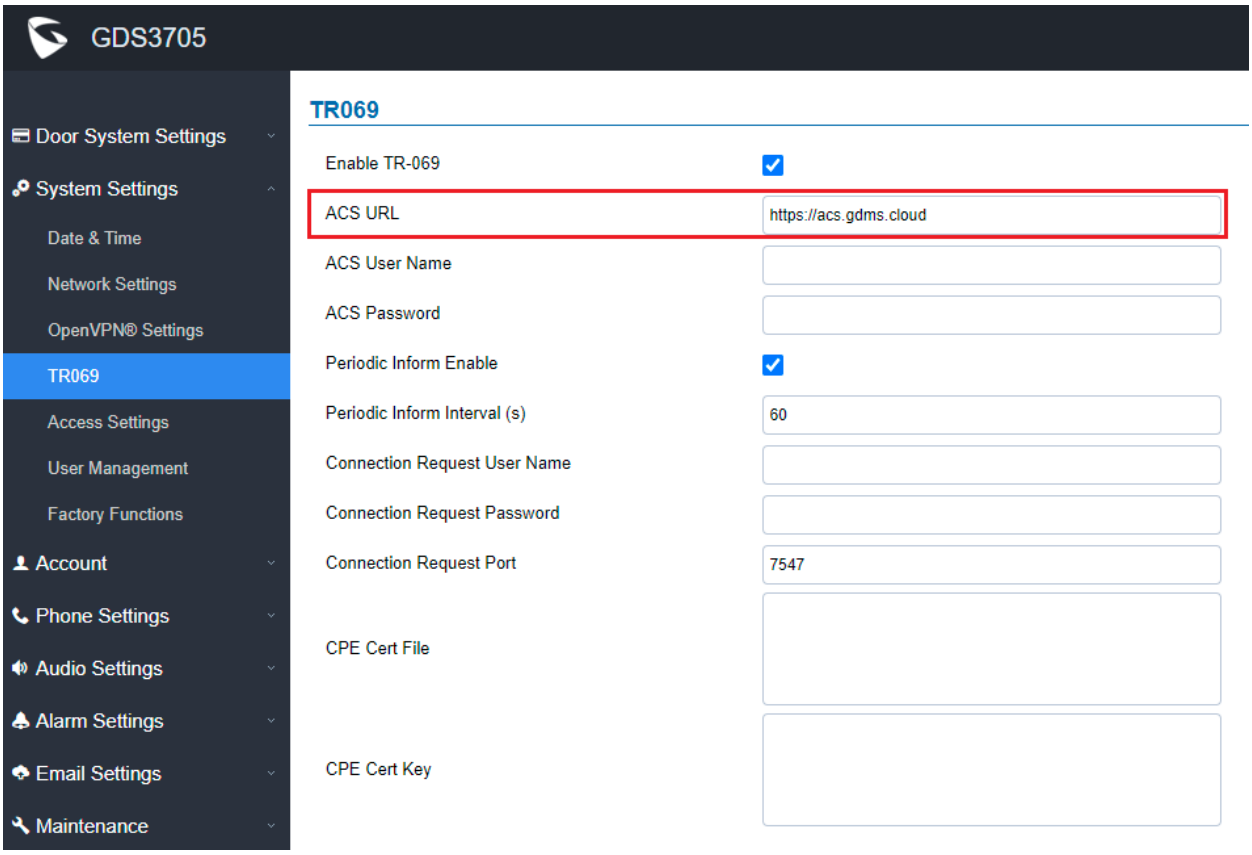
This new feature is implemented so the GDS3705 can be configured and provisioned via TR069/GDMS.

- **Functionality**

When enabled and configured, the GDS3705 will be configured and provisioned via TR069/GDMS.

- **Web Configuration**

This setup can be found under device web UI → System Settings → TR069:



If service providers support TR069 provisioning, or users have account of GDMS service, the GDS3705 can be configured via using related configuration template in the TR069 server or GDMS server side, then provisioning it over the Internet (Cloud Service).

Details please check out GDMS:
https://www.grandstream.com/products/device-management/gdms/product/gdms

For detailed information, please refer to User Manual and Resource Center:

- **GDS3705 User Manual:**
  http://www.grandstream.com/sites/default/files/Resources/GDS3705_UserManual.pdf

- **HOW-TO Guide**
  http://www.grandstream.com/support/resources/?title=GDS3705

- **GDMS**
  https://www.grandstream.com/products/device-management/gdms/product/gdms

FIRMWARE VERSION 1.0.1.21

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B, 3.0A, 3.1A**)*

DATE

12/10/2021

SUMMARY OF UPDATE

This firmware of GDS3705 is mainly for feature enhancement, bug fixes and new HW support.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal WebUI or missing parameters in the GUI. Please backup the data and configuration before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW3.0A	YES	FW1.0.1.21 as Initial Version for this HW version
GDS3705 HW3.1A	YES	FW1.0.1.21 as Initial Version for this HW version

BUG FIX

- 3CX IOT: fixed not sending REGISTER to configured port in SIP Server field when using STUN
- Fixed changing access mode to HTTPS with port 80 will be saved which should not
- Fixed no alarm email when “Non-authorized RFID Card Access Alarm” enabled
- Fixed DTMF door opening performance a while will sometimes cause the device failing to send registration to server and reboot required to recover.

ENHANCEMENT

- Added HW3.0A, HW3.1A support. (**The initial firmware is 1.0.1.21 and NOT able to downgradable**)
- Cisco WebEx IOT: Added Web UI Option “SIP URI Scheme When Using TLS”
- Cisco WebEx IOT: Added Web UI Option “Support SIP Instance ID”
- Added support for configurable keypad blue light On/Off.
- Added unauthorized card swiped on wired external 3rd party Wiegand reader will also have alert message in event Log
- Increased Whitelist Number to maximum 200 in each Account
- Added prompt “Alarm Schedule Name” and “Alarm Action Profile Name” cannot be blank.
- 3CX IOT: Support “Add MAC in User-Agent”
- 3CX IOT: Added “Codec Negotiation Priority” configuration
- Added option to choose HTTP method to either GET or POST request
- Added error prompt if illegal port value is set to web access

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping even after pressing phone’s keypad which supposedly should stop the siren audio at SIP phone side.

NEW HTTP API

GET:[http|https]://<servername>/goform/config?cmd=get&type=sip
SET:[http|https]://<servername>/goform/config?cmd=set&P2329=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P2429=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P2529=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P2629=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P288=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P489=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P589=<value>
SET:[http|https]://<servername>/goform/config?cmd=set&P689=<value>

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

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

GET:[http|https]://<servername>/goform/config?cmd=get&type=log
SET:[http|https]://<servername>/goform/config?cmd=set& P15553 =<value>

NEW P-VALUE

P2329	Account.Account_1.SIP_URI_Scheme_When_Using_TLS (Value: 0 / 1; 0: sip 1: sips)
P2429	Account.Account_2.SIP_URI_Scheme_When_Using_TLS (Value: 0 / 1; 0: sip 1: sips)
P2529	Account.Account_3.SIP_URI_Scheme_When_Using_TLS (Value: 0 / 1; 0: sip 1: sips)
P2629	Account.Account_4.SIP_URI_Scheme_When_Using_TLS (Value: 0 / 1; 0: sip 1: sips)
P288	Account.Account_1.Support_SIP_Instance_ID (Value: 0 / 1; 0: Disable 1: Enable)
P489	Account.Account_2.Support_SIP_Instance_ID (Value: 0 / 1; 0: Disable 1: Enable)
P589	Account.Account_3.Support_SIP_Instance_ID (Value: 0 / 1; 0: Disable 1: Enable)
P689	Account.Account_4.Support_SIP_Instance_ID (Value: 0 / 1; 0: Disable 1: Enable)
P15500	Door_System_Settings.Basic_Settings.Enable_Bule_Keypad_Light (Value: 0 / 1; 0: Disable 1: Enable)
P15501	Door_System_Settings.Basic_Settings.Bule_Keypad_Light_Start_Time (Value: String; Example: 125900)
P15502	Door_System_Settings.Basic_Settings.Bule_Keypad_Light_End_Time (Value: String; Example: 145930)
P26061	Account.Account1.Add_MAC_in_User-Agent (Value: 0 / 1 / 2; 0: No 1: Yes except REGISTER 2:Yes to all SIP)
P26161	Account.Account2.Add_MAC_in_User-Agent (Value: 0 / 1 / 2; 0: No 1: Yes except REGISTER 2:Yes to all SIP)
P26261	Account.Account3.Add_MAC_in_User-Agent (Value: 0 / 1 / 2; 0: No 1: Yes except REGISTER 2:Yes to all SIP)
P26361	Account.Account4.Add_MAC_in_User-Agent (Value: 0 / 1 / 2; 0: No 1: Yes except REGISTER 2:Yes to all SIP)
P29061	Account.Account1.Codec_Negotiation_Priority (Value: 0 / 1; 0: Caller 1: Callee)
P29161	Account.Account2.Codec_Negotiation_Priority (Value: 0 / 1; 0: Caller 1: Callee)
P29261	Account.Account3.Codec_Negotiation_Priority (Value: 0 / 1; 0: Caller 1: Callee)
P29361	Account.Account4.Codec_Negotiation_Priority (Value: 0 / 1; 0: Caller 1: Callee)
P15553	Maintenance.Event.Notification.HTTP_Method (Value: 0 / 1; 0: POST 1: GET)

NEW FEATURES OVERVIEW

This section lists major new features or improvement and advise customers how to use them.

CISCO WEBEX COMPATABIE

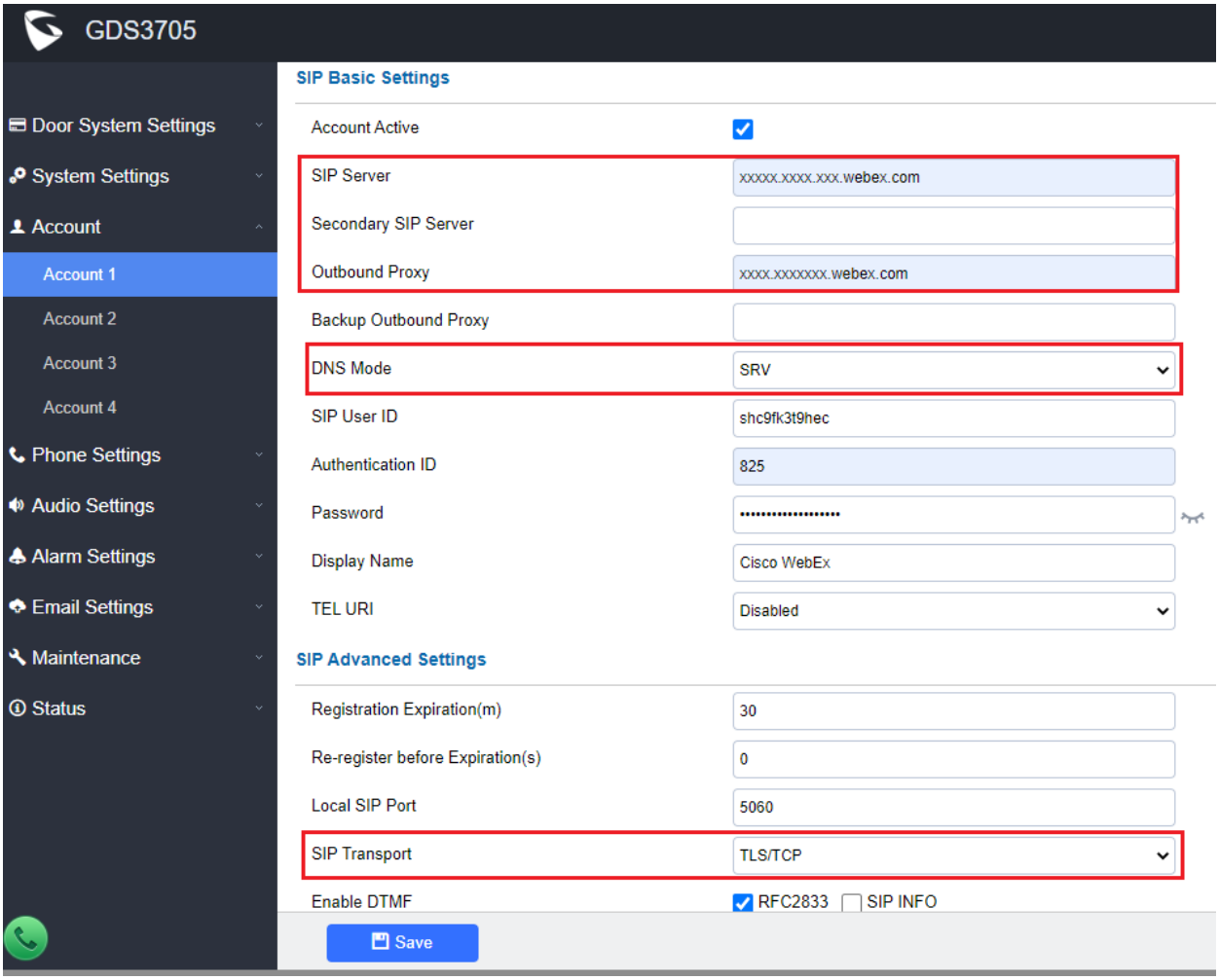
This new feature is implemented so the GDS3705 can be running in Cisco WebEx Service.

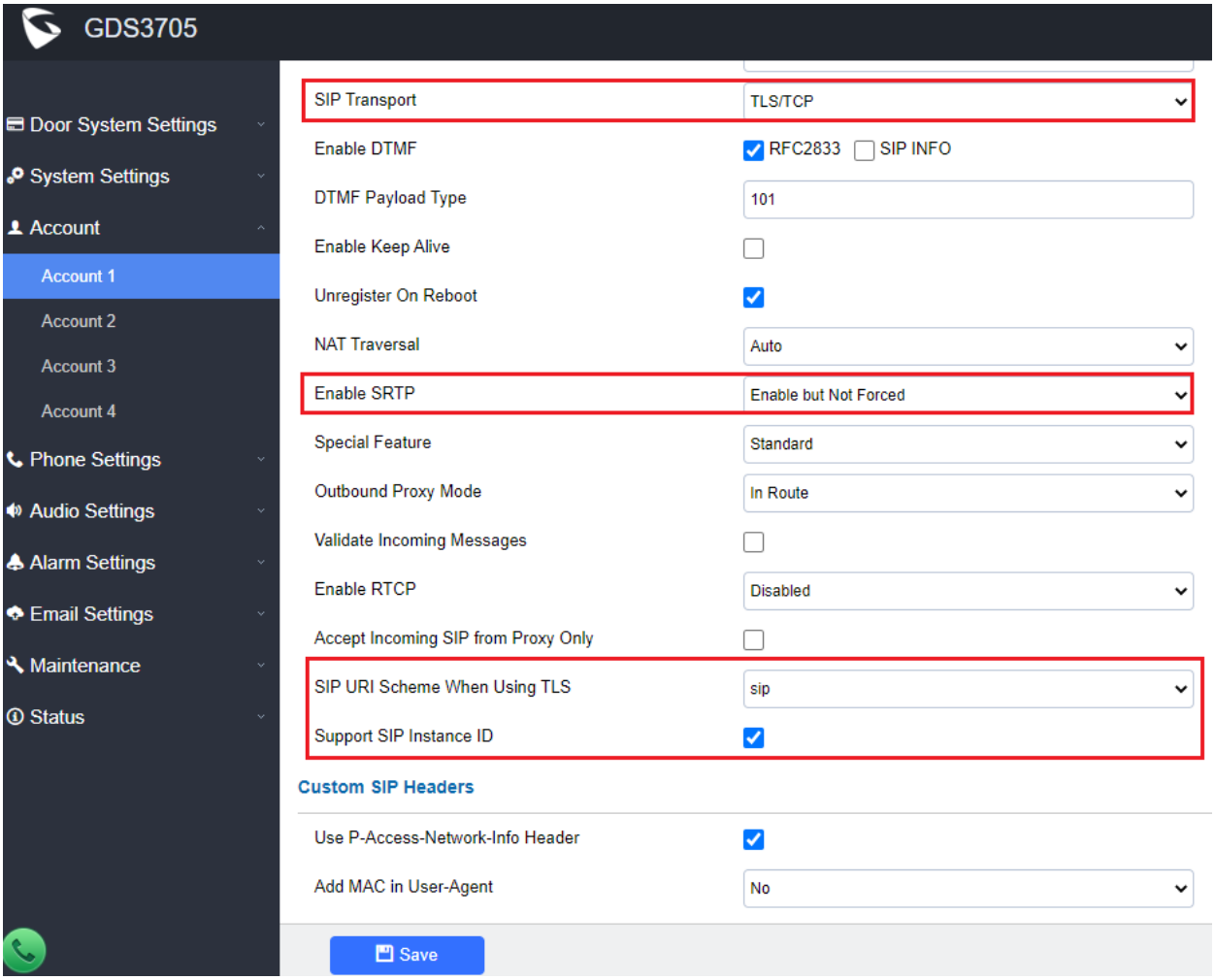
- **Functionality**

When enabled and configured this feature, the GDS3705 will register and work in Cisco WebEx Service.

- **Web Configuration**

This setup can be found under device web UI → Account → Account X:



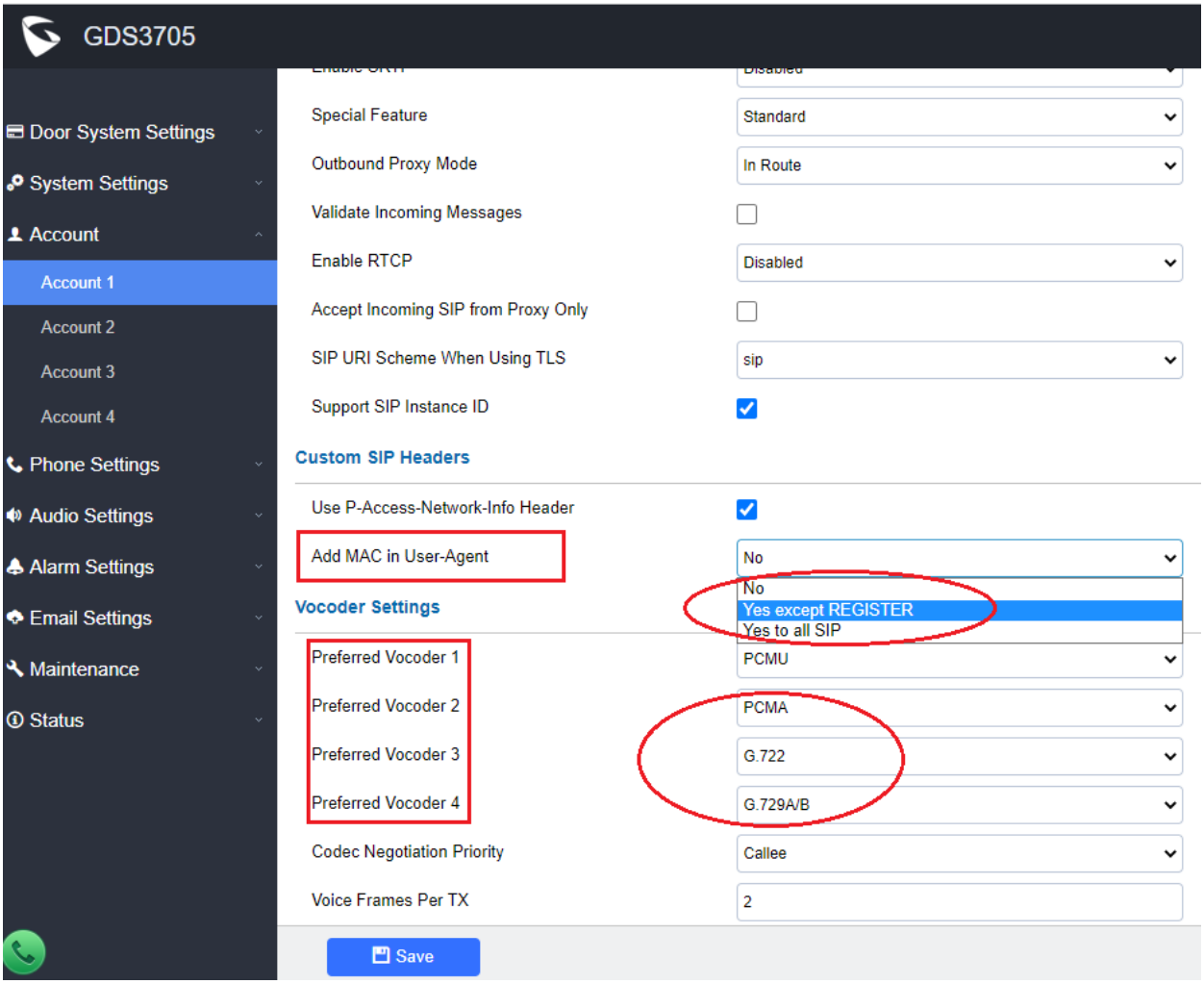


If user has Cisco WebEx service, the GDS3705 can be configured using above screenshots as reference, so the GDS3705 can be registered and running in Cisco WebEx Service.

3CX IOT COMPATABLE

- **Web Configuration**

This option can be found under device web UI → Account → Account X:



- **Functionality**

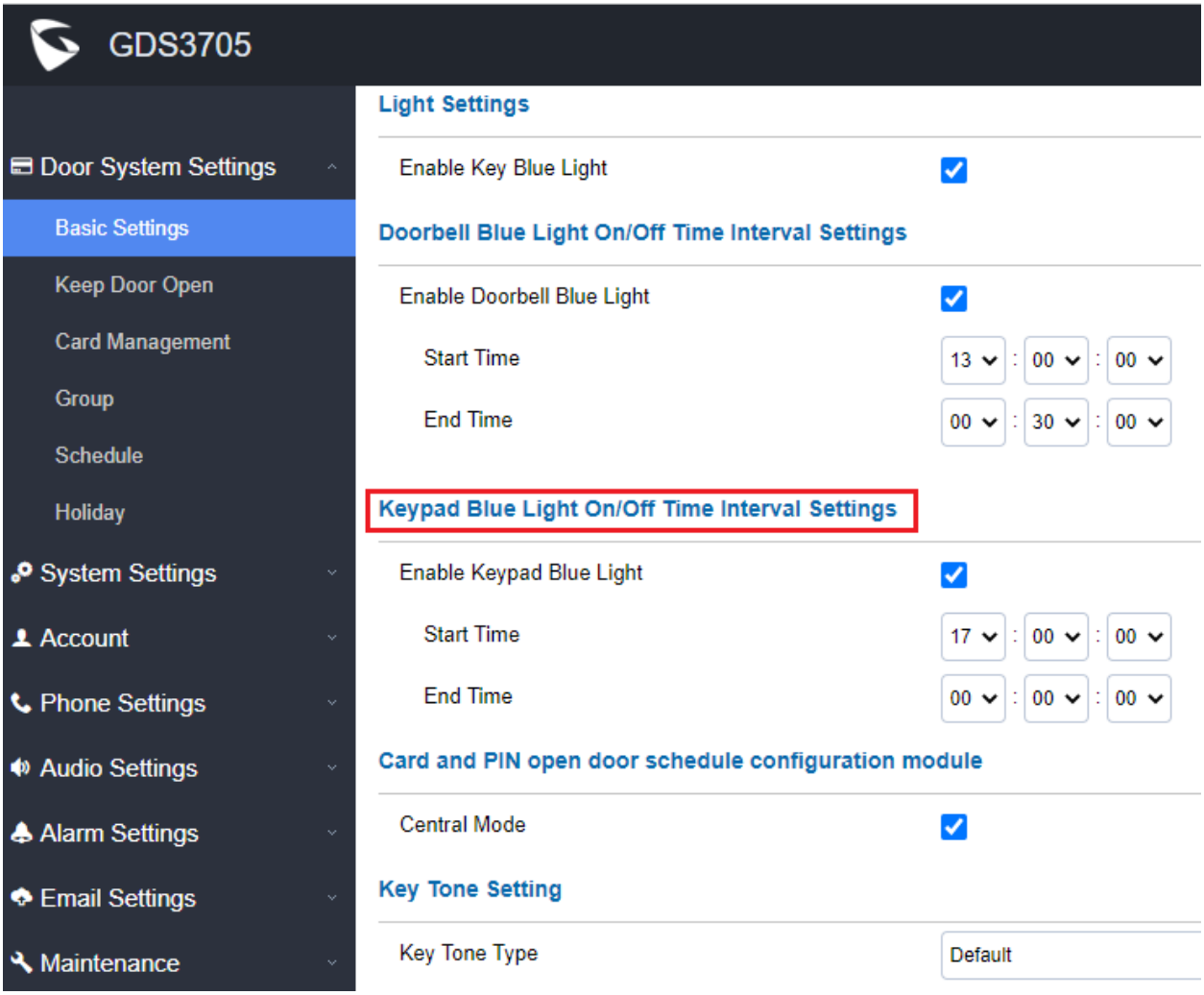
With this feature implemented, customers can conveniently select and configure related parameters so the GDS3705 can be registered and running in 3CX Solution, or be provisioned by 3CX Server.

The above screenshot of configuration is for 3CX configuration reference only.

CONFIGURABLE KEYPAD BLUE LIGHT ON/OFF

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



- **Functionality**

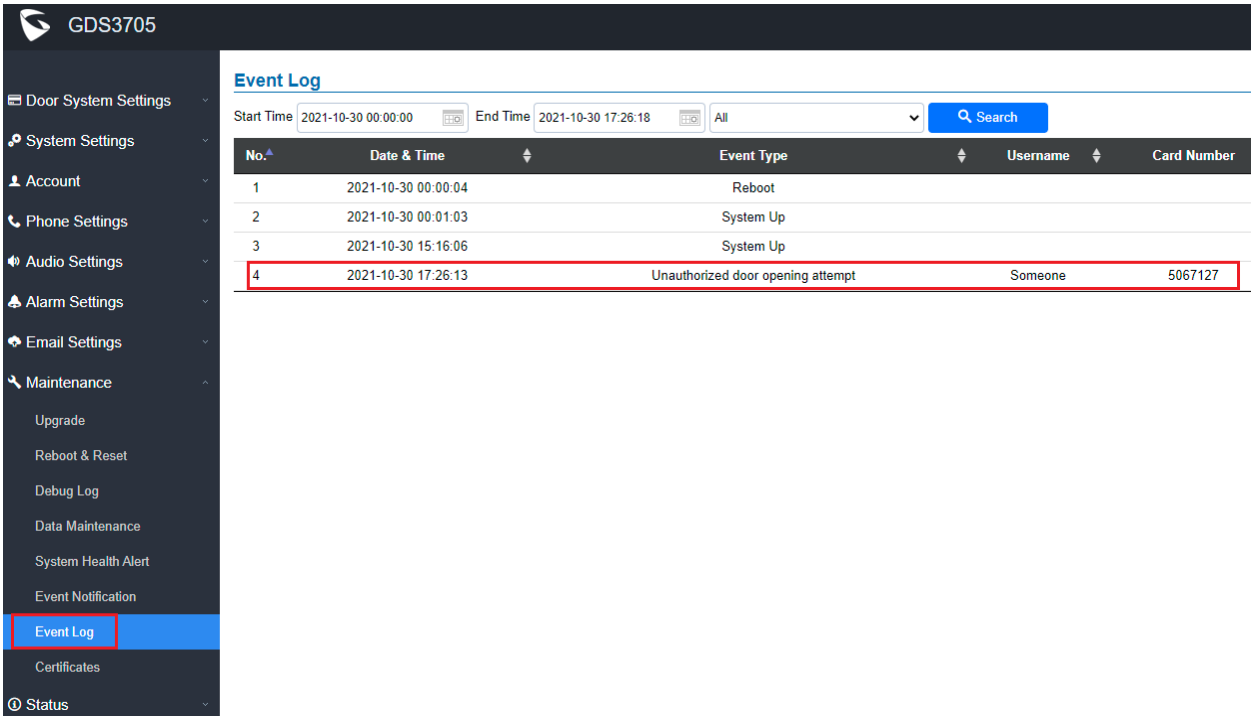
This feature enhancement is response to field request from customers.

By configure the keypad blue light ON/OFF based on specific time in a day, the GDS3705 can light up the keypad using blue LED light in the dark or night environment, so the visitors can clearly see the keypad and press the keypad to call or input PIN to open door without making mistakes.

UNAUTHORIZED CARD SWIPE (WIEGAND READER) ALERTED IN EVENT LOG

- **Web Configuration**

This option can be found under device web UI → Maintenance → Event Log:



- **Functionality**

This feature is implemented based on feedback from customers.

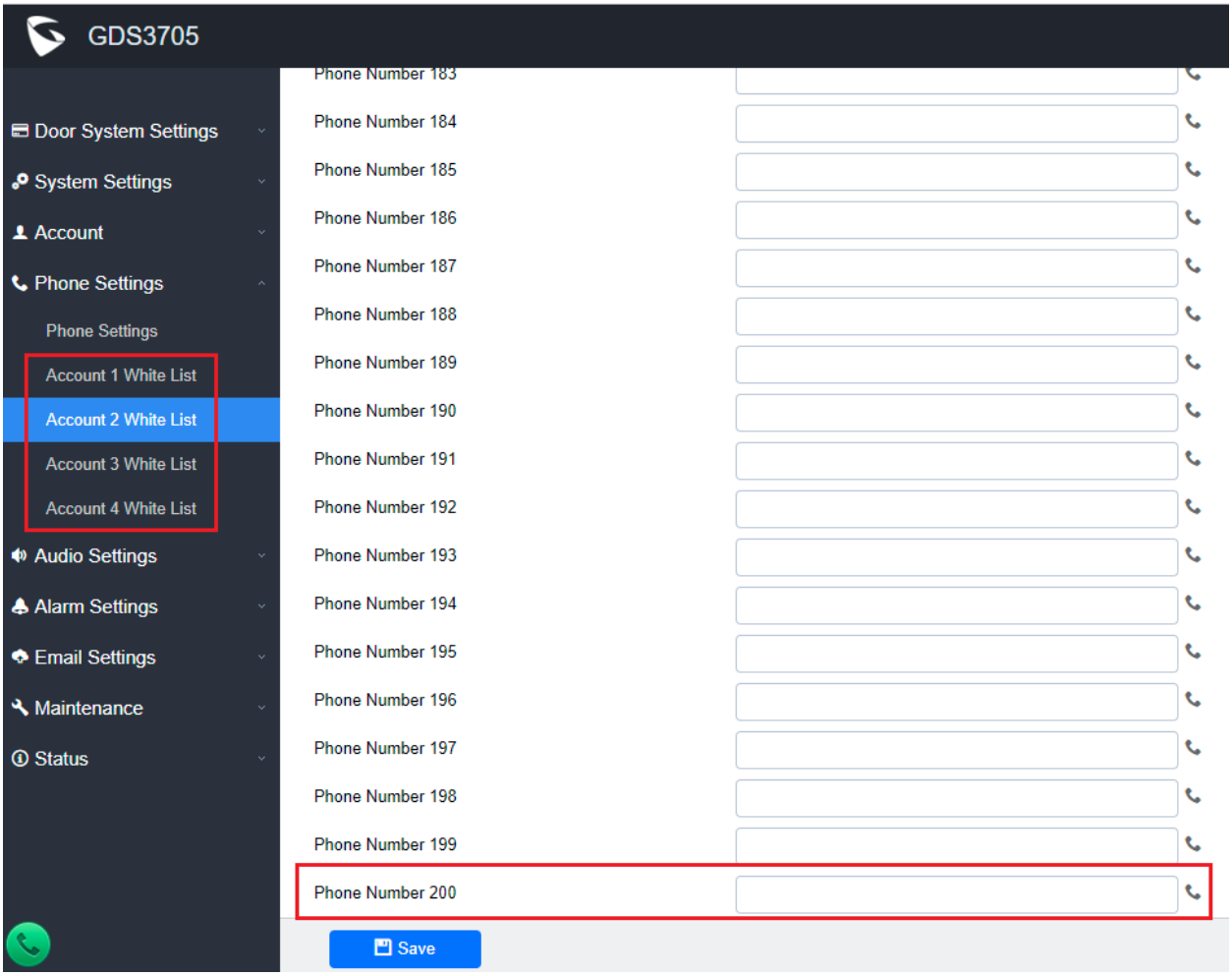
This feature previously only works when RFID card swiped at the GDS3705. If 3rd party card reader installed and wired into the Wiegand port of GDS3705, the illegal card swiped would not be able to be logged in the Event Log.

With this feature implemented, the illegal RFID card swiped via the 3rd party card reader will also be logged and alerted in the Event Log of the GDS3705, as shown in above screenshot.

INCREASED WHITELIST IN EACH ACCOUNT

- **Web Configuration**

This option can be found under device web UI → Phone Settings → Account X White List:



- **Functionality**

This feature enhancement is based on customers from field.

Some customers integrated GDS3705 with IPPBX and interconnected with POT Lines, so the visitors can call the user's cell phone number asking remote open door if user is not at the location.

Previously the White List has limitation so the list will full very quickly if the location is an apartment building. Now the list is boosted to maximum 200 in each Account. This will solve customer's problem and make the application solution feasible.

For detailed information, please refer to User Manual and Resource Center:

- **GDS3705 User Manual:**
  http://www.grandstream.com/sites/default/files/Resources/GDS3705_UserManual.pdf

- **HOW-TO Guide**
  http://www.grandstream.com/support/resources/?title=GDS3705

FIRMWARE VERSION 1.0.1.16

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

03/12/2021

SUMMARY OF UPDATE

This firmware update of GDS3705 is mainly for feature enhancement and bug fixes.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI. Please backup the data and configuration before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed half time zone the daylight saving time is invalid.
- Fixed unauthorized card swiped at Wiegand reader the event log not display related event.
- Fixed keypad locked if doorbell pressed or wrong PIN entered quickly too many times.
- Fixed NAPRT not used in DNS/SRV mode.
- Fixed call failure when disable key blue light with more than 6 second “no key input timeout” setting.
- Fixed doorbell audio played during the call.
- Fixed in Data Maintenance Mode, import the exported file will fail with prompt “illegal certificate”.
- Fixed error display issue when the certificate imported is valid for more than 2038.
- Fixed device reboot when import unmodified certificates in XML.
- Fixed device not check all PAI to match with whitelist number (ITSP Telefonica).
- Fixed cannot dial using Virtual Number.

ENHANCEMENT

- Added Secure Open Door with GDS37xx/GSC3570 Pairing and door lock/strike wired to GSC3570 Alarm_Out port and controlled by GSC3570 (located inside) instead of GDS37xx (located outside).
- Added pairing with GSC3570 open door without SIP call.
- Added Card Number limitation with maximum number to be **2147483647**.
- Added Web Relay ON/OFF URL configuration field for some 3rd party Web Relay Door Controlling.
- Added configurable Scheduled Auto Reboot (to keep a healthy system running).
- Added SIP Account Active feature.
- Added ability to disable P-Access-Network-Info Header for ITSP (e.g.: Telefonica).
- Added support to trigger Alarm Action when illegal card swiped.
- Added support to allow IP addresses in whitelist to call the GDS37xx and bypass the setting of "Accept Incoming SIP from Proxy Only"
- Added protection schema to prevent device reboot during a call.
- Added "GMT-3 (Argentina, Uruguay, Brasilia, San Paulo)" in time zone settings.
- Added "GMT-3:30 (Newfoundland) in time zone settings.
- Enhanced webUI password display with security and convenience.
- Improved webUI error login prompt message.
- Enhanced Card Management / Private PIN display feature for better administration.
- Improved HTTP API Open Door by processing default value if missed in the API.
- Modified tips at Card Management Page
- Enhanced webUI password display with security and convenience.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping even after pressing phone's keypad which supposedly should stop the siren audio at SIP phone side.

NEW HTTP API

- **P15540/ P15541/ P15542**
  GET:[http|https]://<servername>/goform/config?cmd=get&type=reset_reboot
  SET:[http|https]://<servername>/goform/config?cmd=set&P15540=<value>
  SET:[http|https]://<servername>/goform/config?cmd=set&P15541=<value>
  SET:[http|https]://<servername>/goform/config?cmd=set&P15542=<value>

- **P15440/P15441/P15447/P15442/P15443/P15444/P15445/P15446**
  GET:[http|https]://<servername>/goform/config?cmd=get&type=door
  SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

- **P15515/P15516**
  GET:[http|https]://<servername>/goform/config?cmd=get&type=event
  SET:[http|https]://<servername>/goform/config?cmd=set&Pxxx=<value>

NEW P-VALUE

- P15540: Maintenance.Reboot_Reset.Auto_Reboot.Enable
  (value: 0:Disable; 1:Enable)
- P15541: Maintenance.Reboot_Reset.Auto_Reboot.Week
  (value: 0:Everyday 1:Sunday 2:Monday 3:Tuesday 4:Wednesday 5:Thurday 6:Friday 7:Saturday)
- P15542: Maintenance.Reboot_Reset.Auto_Reboot.Hour_Min
  (time string, example: 14:20 ->1420)
- P15440: Door_System_Settings. Basic_settings.Door_relay_options
  (value: 0:local relay; 1:webrelay; 2:gsc3570 relay)
- P15441: Door_System_Settings. Basic_settings.Webrelay_ON_URL
  (string, max.len=1024)
- P15447: Door_System_Settings. Basic_settings. Webrelay_OFF_URL
  (string; max.len=1024)
- P15442: Door_System_Settings. Basic_settings.Webrelay_username
  (string; max.len=128)
- P15443: Door_System_Settings. Basic_settings.Webrelay_password
  (string; max.len=128)
- P15444: Door_System_Settings. Basic_settings.gsc3570_Account_to_choose
  (value: 1:acc1; 2:acc2; 3:aac3; 3:acc4)
- P15445: Door_System_Settings. Basic_settings. gsc3570_phone_number
  (string; max.len=128)
- P15446: Door_System_Settings. Basic_settings. gsc3570_password
  (string; max.len=128)
- P15515: Alarm_Settings.Alarm_events_config.Alarm_config.Enable_Nonauthorized_RFID_Card_Access_Alarm
  (value: 0:disable; 1:enable)
- P15516: Alarm_Settings.Alarm_events_config.Alarm_config.Alarm_profile
  (value: 1-10: profile1-10)

NEW FEATURES OVERVIEW

This section lists major new features or improvement and advise customers how to use them.

PAIR WITH GSC3570 OPEN DOOR W/O SIP CALL

This new open door feature is a major enhancement to GDS37xx, but need to include GSC3570 paired to make it a whole solution. The GDS37xx/GSC3570 will be pairing together in LAN, and GDS37xx still controls the strike.

- **Functionality**

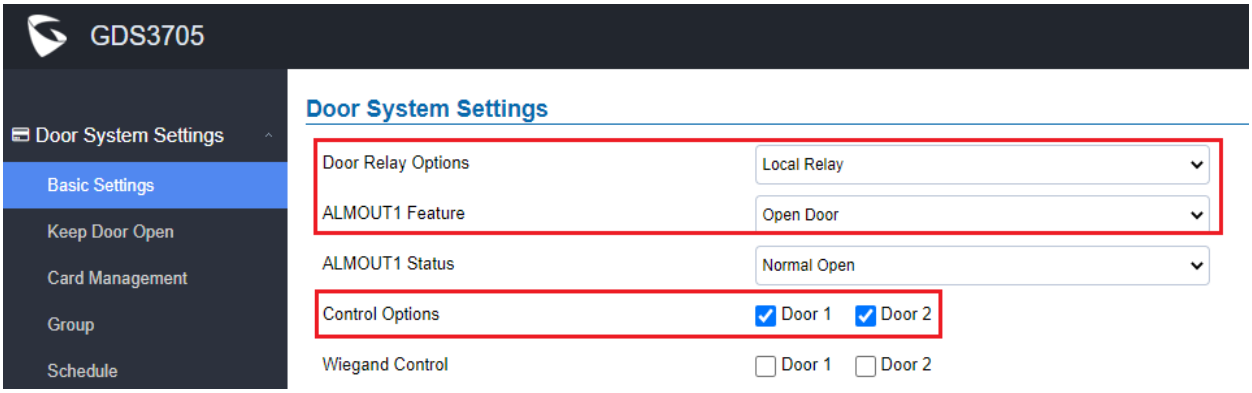
When enabled and configured this feature, the user will touch the GSC3570 and open the door directly via GDS37xx, without making SIP calls. This feature needs related matching GSC3570 firmware to work. The firmware required:

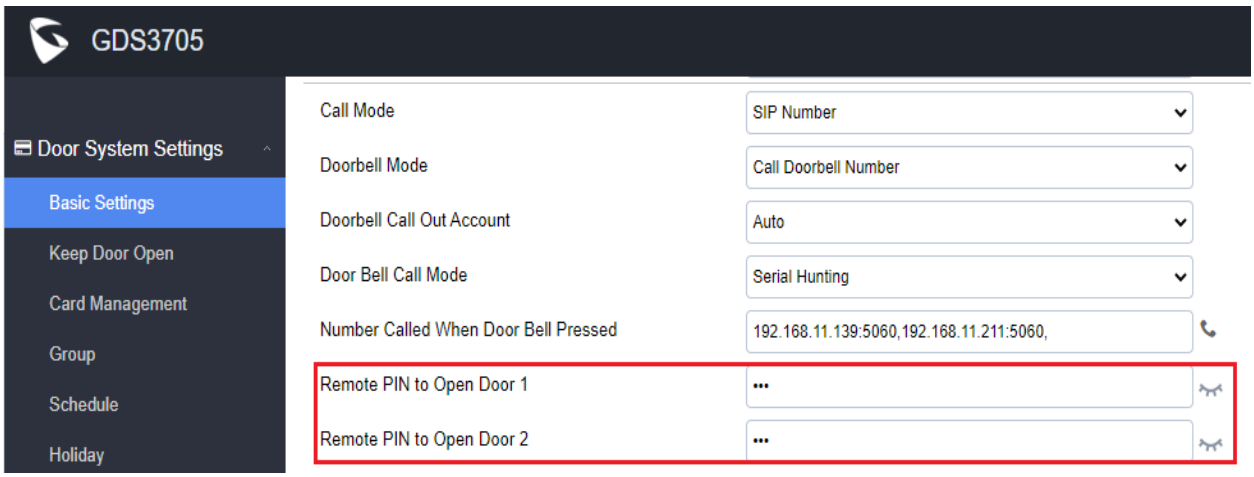
  - **GSC3570: 1.0.5.9 or above**

- **Web Configuration**

GDS3705: (FW: 1.0.1.16 or above)

This setup can be found under device web UI → Door System Settings → Basic Settings:

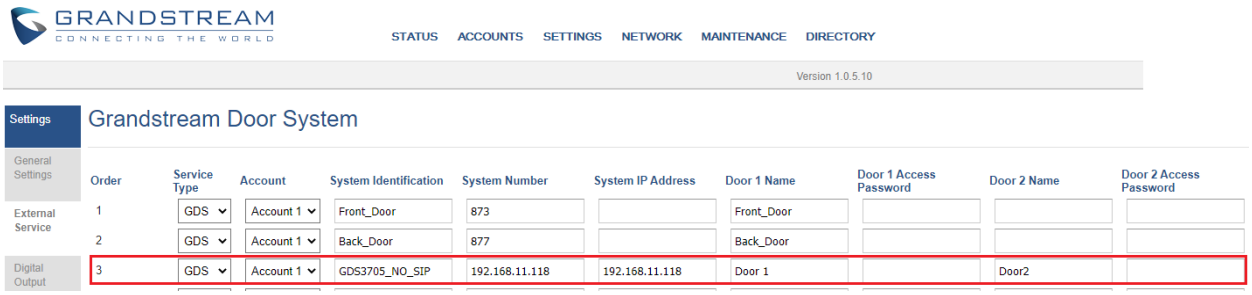




The GDS37xx is configured to control the relay/strike with “Door Relay Option” selected as “Local Relay”, where 1 door or 2 door used, depending on user’s configuration and installation.

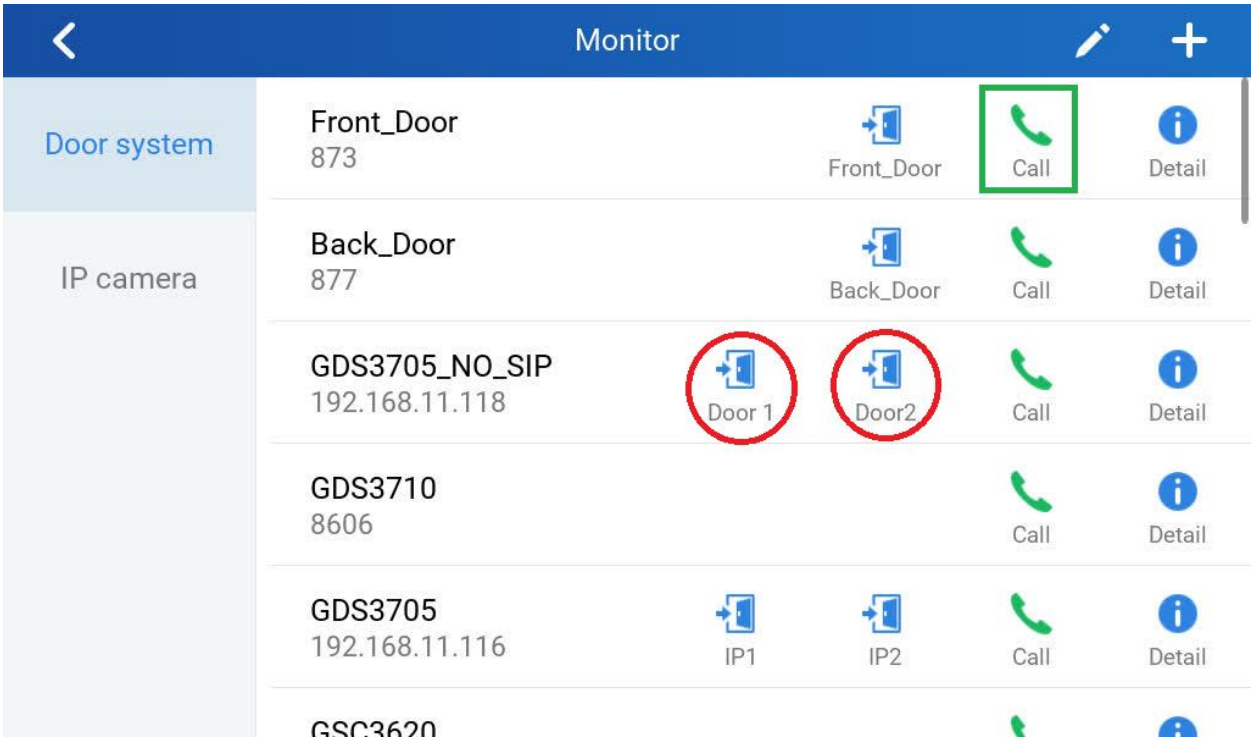
GSC3570: (FW: 1.0.5.9 or above)

The GSC3570 side also need to be configured according, like below:

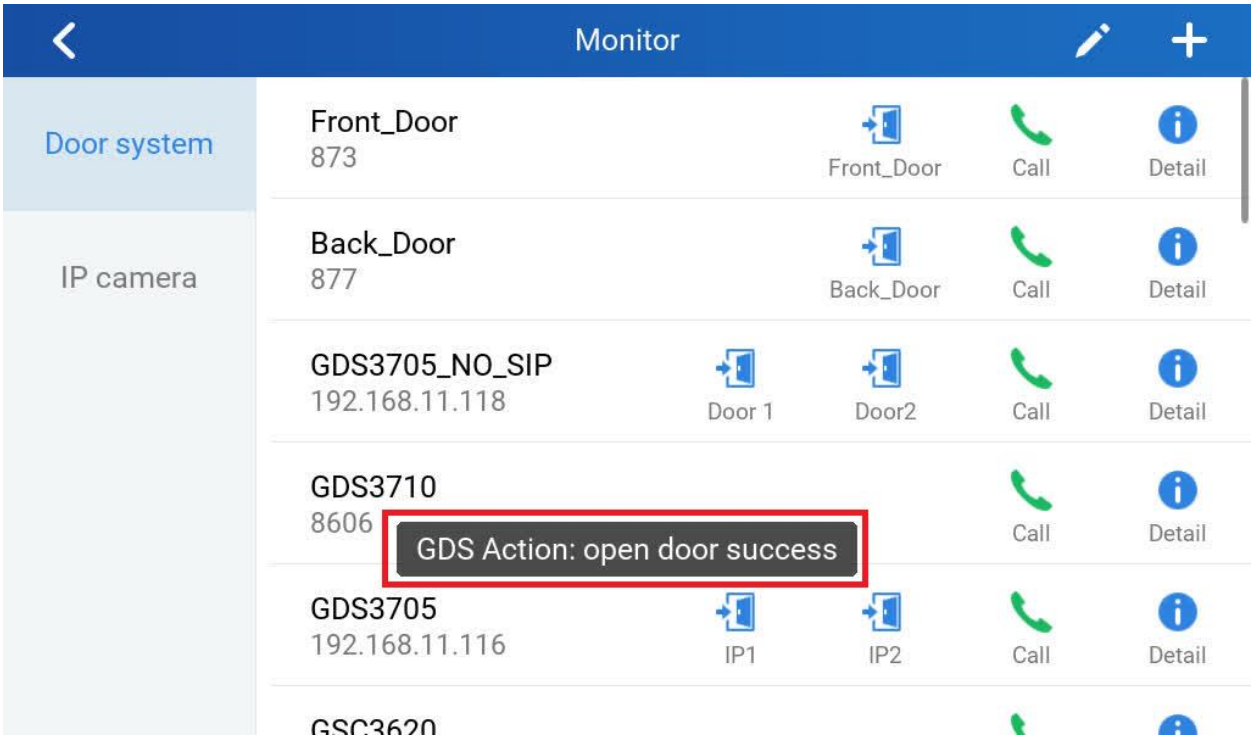


In the “SETTINGS → External Service”, input the IP address of GDS37xx where the GSC3570 paired with, and input the correct PIN for open related remote doors. The PIN should match with GDS37xx related remote PIN to open door.

Once configured successfully, in the touch screen UI of GSC3570, press “Monitor”, select “Door system”, will see UI like below:



Select the related door where the GSC3570 controlled, in this example, the “GDS3705_NO_SIP” located at right corner of top line is the one configured. Press the icon of open door (red circled one) will pop up another UI like below when door opened successfully:



Press related “Door 1” or “Door 2” icon (two doors configured in this example), the GDS37xx will operate the strike and open the correspondent door accordingly.

If press the “Phone” icon (green square illustrated above), then the GSC3570 will make SIP phone call to the configured GDS37xx and open door remotely via SIP phone call like as before.

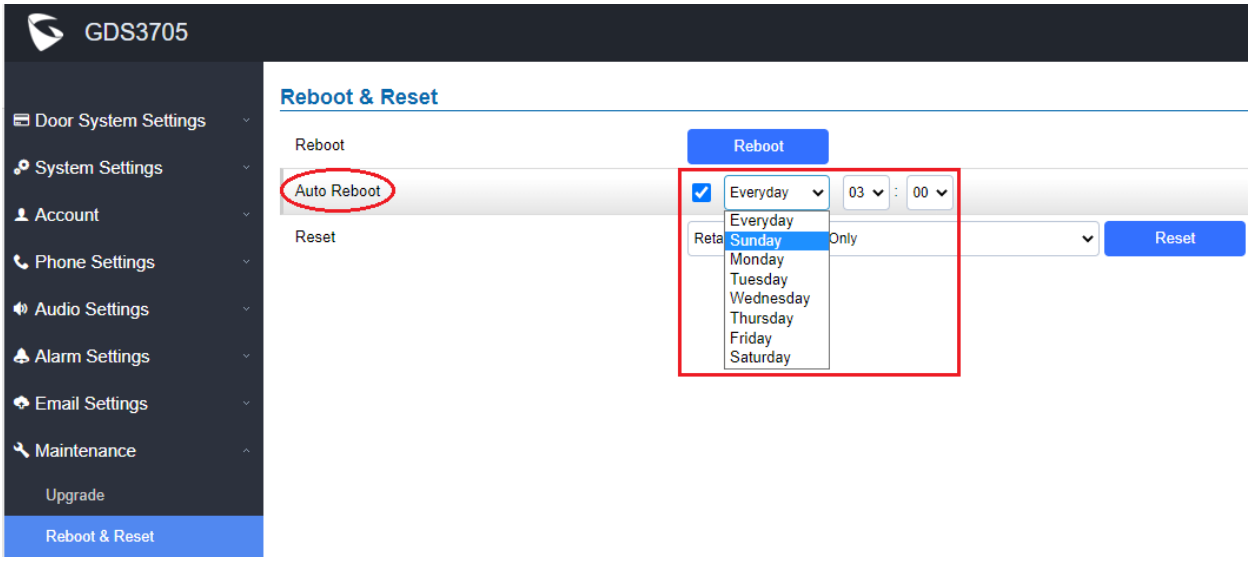
The application will help customers with installation scene where GSC3570 is located near Receptionist or related person, the user just use GSC3570 to operate GDS37xx to open door, without make a SIP phone call.

This application scene is good for hospital/clinic or senior house etc., environment where open door button or switch is NOT installed or wired, customer can just add a GSC3570 to open door from inside by related person (nurse or receptionist), to give convenience to their customers to come in or get out of the office or building.

SCHEDULED AUTO REBOOT

- **Web Configuration**

This option can be found under device web UI → Maintenance → Reboot & Reset:



- **Functionality**

With this feature implemented, customers can conveniently select a schedule to let the device reboot itself, per week or per day, to make a smooth and clean system, for the access control operation as well as to make sure the device is registered to SIP Proxy.

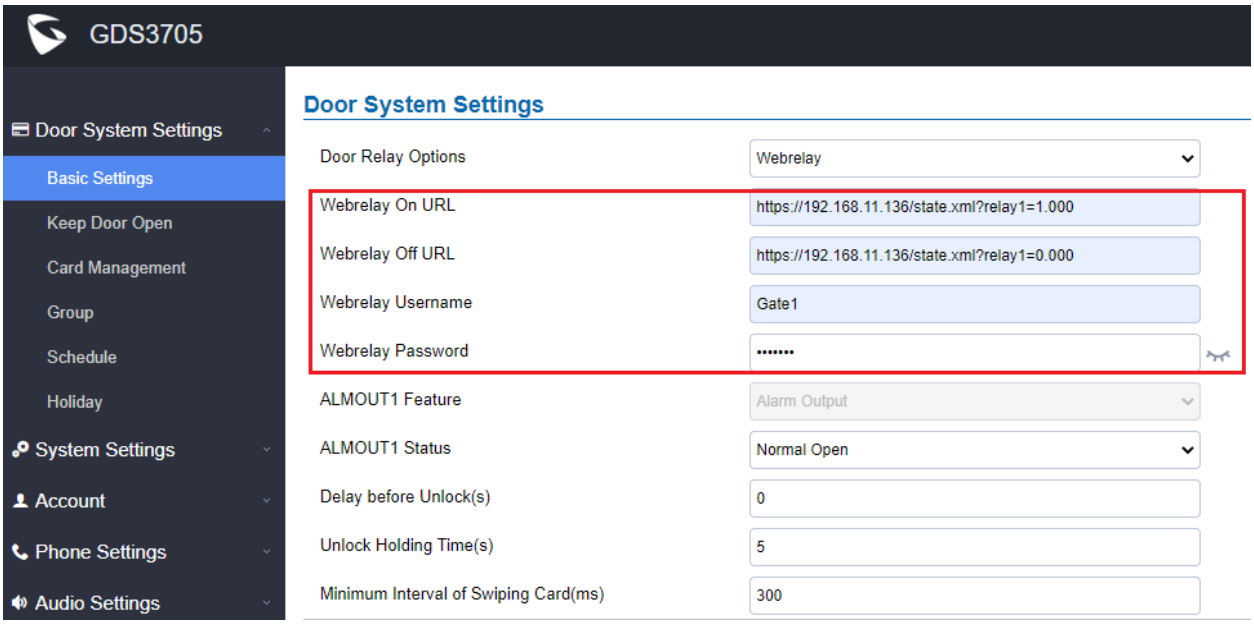
Before implement this feature, customers need to write their own scripts to reboot the device, or using SIP NOTIFY from SIP Server to reboot the device, or manually reboot the device when found the device lost registration to SIP Proxy.

Reliability is ensured by implement this new enhancement.

ENHANCED OPEN DOOR VIA 3RD PARTY WEBRELAY WITH ON/OFF URL

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



- **Functionality**

This feature enhancement is response to field request to integration with 3rd party Webrelay controller, to install the relay controller inside the build to enhance the security or apply in some industry application solution.

Now there are TWO Webrelay URL fields available, with On or Off URL command allowed or other usage URL command allowed. Also allow Username and Password configured if the 3rd party Webrelay requiring this security feature.

If some 3rd party Webrelay only support one URL command, then just leave another Off URL blank, or put whatever there as long as it is NOT a URL command.

- **3rd Party Webrelay**

When Webrelay is selected, customers need to continue configure the Webrelay IP address or domain name, together with credentials like Username and Password, as well as the URL commands used by the 3rd party Webrelay.

When legal open door event happened, the configured web relay will get the communication from GDS37xx, and will operate the strike to open door for the authenticated open door request. Or use that command to operate other industry application.

In web relay mode, the strike is wired to the web relay controller device.

The correct URL command, please refer to related 3rd party Webrelay User Manual or related documentation for details.

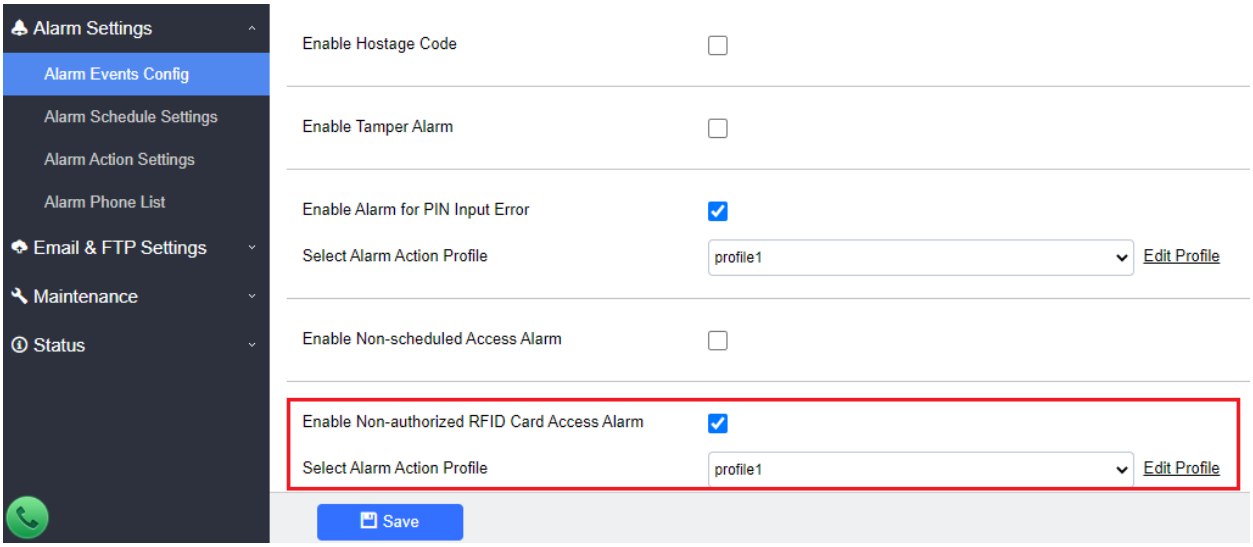
For more details about 3rd party Webrelay, please refer to below URL to get more information:

https://www.controlbyweb.com/webrelay/	*(Single/Dual/Quad, etc.)*
https://www.barix.com/barionet/	*(Universal programable I/O device)*

ALARM ACTION WHEN ILLEGAL CARD SWIPED

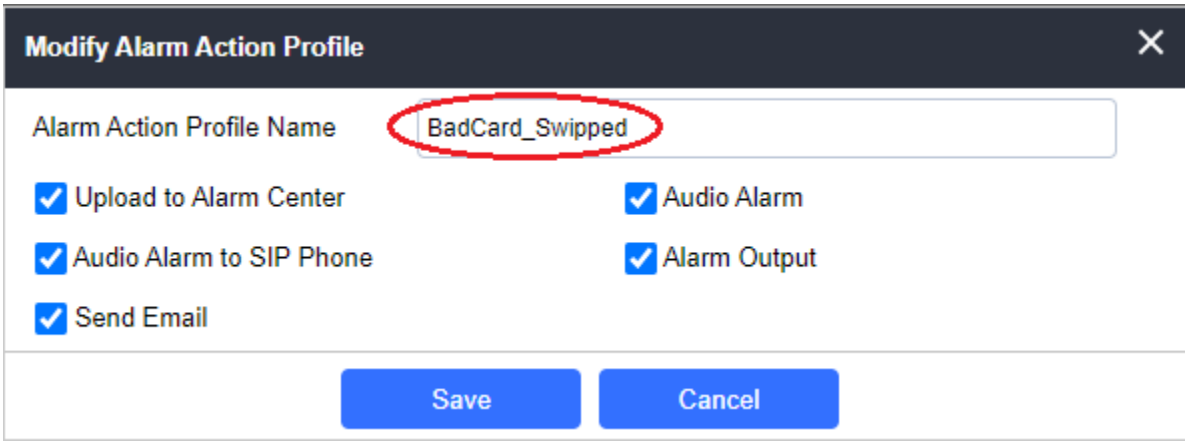
- **Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Event Config:



- **Functionality**

This feature enhancement is requested by customers from field. By enable this feature, any illegal card swiped trying to access the door will trigger alarm based on user's configuration, like below:

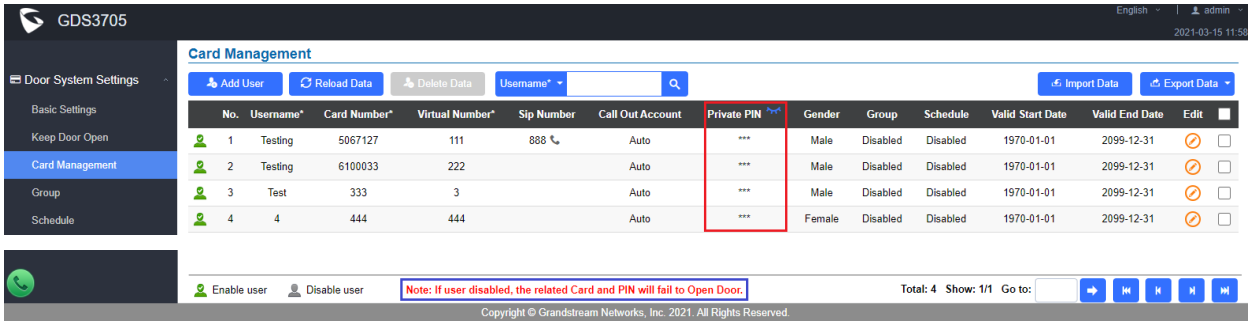


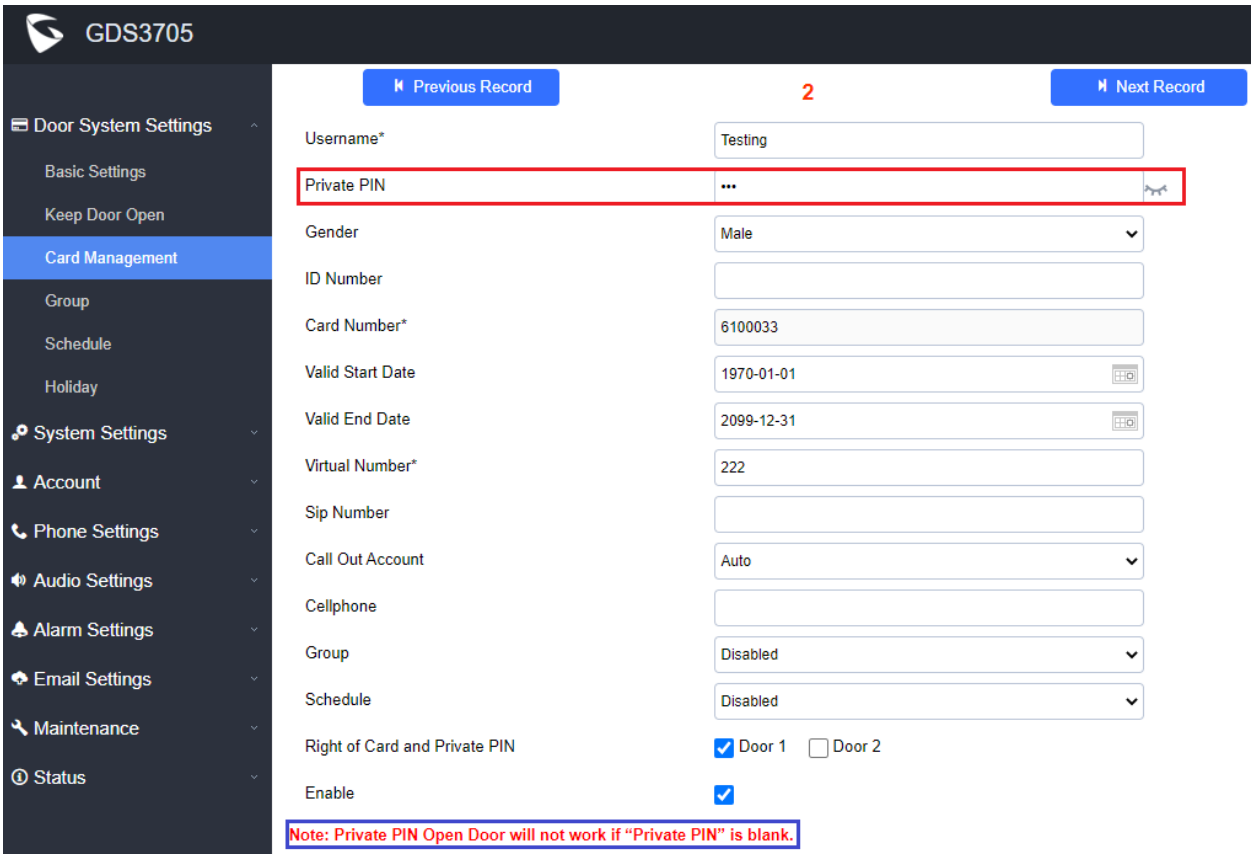
User will get email, snapshot, etc., based on the Alarm Action Profile configured, to enhance the security of access control.

MODIFIED CARD MANAGEMENT PAGE

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Card Management:





- **Functionality**

This enhancement is based on customer's feedback to increase the usability with friendly UI. The "Private PIN" now can be viewed in same page to help administration work when enabled. This is especially helpful when GDS3705 used to replace traditional analogue access control by using "PIN#" to open door.

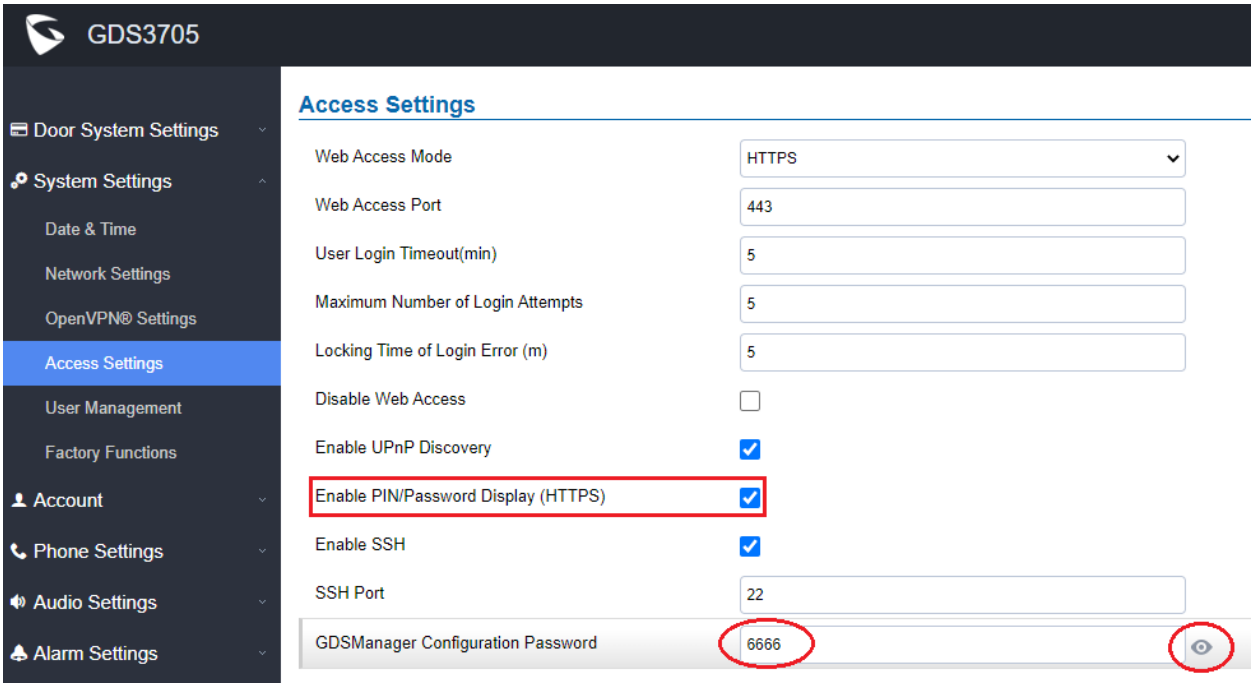
In the above screenshot, tips are added like:

- **Note: If user disabled, the related Card or PIN will fail to Open Door.**
- **Note: Private PIN Open Door will not work if "Private PIN" is blank.**

WEBUI PASSWORD DISPLAY WITH SECUIRTY AND CONVENIENCE

- **Web Configuration**

This option can be found under device web UI → System Settings → Access Settings:



- **Functionality**

This feature enhancement is a compromised solution to response the feedback from system integrators as well as the request from ITSP customers.

ITSP customer provisioning device and do not want end user to mess around the device, therefore requesting NO password should be displayed in webUI.

System integrators have different application scenes, therefore requesting password to be displayed once logged in as admin, just for configuration and management convenience.

This feature is enhanced to meet both requirements.

By default, the “Enable PIN/Password Display (HTTPS)” is disabled for ITSP customer. Service provider customers are using Configuration Template to provision the device, they can change related P values to change the configuration of the provisioned device.

System integrators can check and enable the PIN/Password Display in the “Access Setting”. Once enabled, there will be an “eye” icon displayed in the webUI, putting mouse cursor to the “eye” icon, the related password or PIN will be displayed at the webUI. Once mouse cursor moved away, the PIN/Password will be displayed as dot “.” as usual.

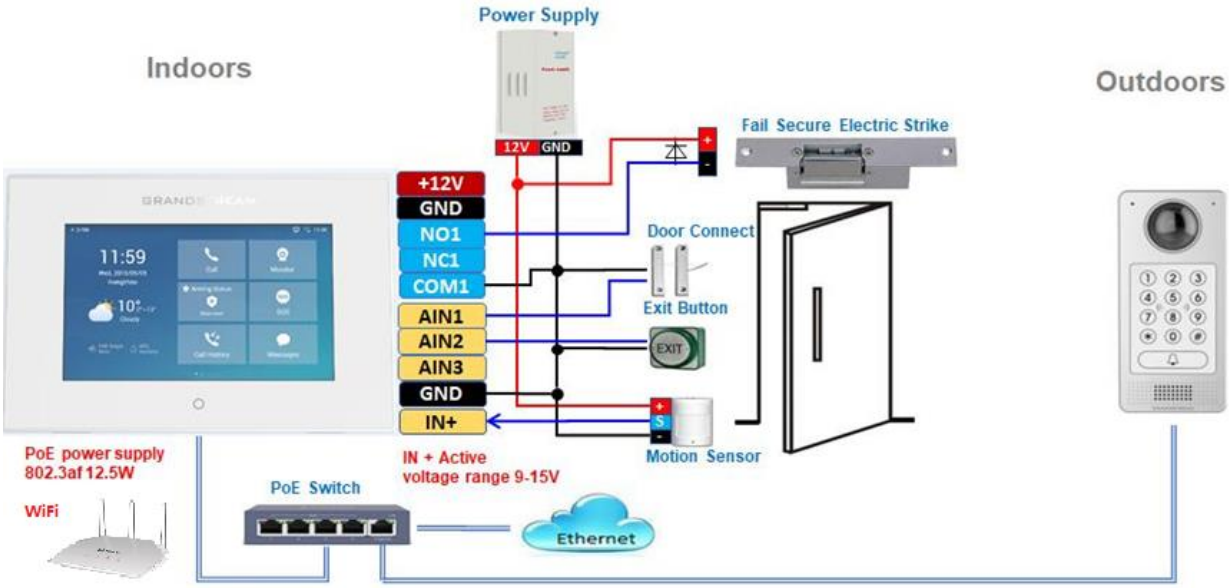
This feature ONLY works in HTTPS mode. Due to the insecurity of HTTP, PIN/Password will NOT be displayed. PIN/Password can ONLY be displayed in HTTPS mode.

GSC3570 SECURE OPEN DOOR BY PAIRING WITH GDS37XX

This secure open door new feature is a major enhancement to GDS37xx, but need to include GSC3570 to make it a whole solution. The GDS37xx/GSC3570 will be pairing together in LAN/WAN via IP/SIP, the door lock/strike will be wired to GSC3570 Alarm_Out port and controlled by GSC3570 (located inside) instead of GDS37xx (located outside). This way the strike control is inside the building with enhanced security.

- **Functionality**

This application scene will be similar like below:



Minimum firmware required for this to work:

- ***Outdoor Device:*** ***GDS3710 (FW1.0.7.19) / GDS3705 (FW1.0.1.16)***
- ***Indoor Device:*** ***GSC3570 (FW1.0.5.2)***

The GDS37xx can be powered via PoE; the GSC3570 can connect to same network via PoE or Wi-Fi.

For open door combination with GSC3570 and GDS37xx, if GSC3570 needs to control multiple GDS37xx, it has to use SIP and the related GDS37xx will control the strike/lock. The different GDS37xx doorbell call will have “One Button Open Door” displayed when in “Preview” (early media support) or when call established. The GSC3570 user will press the virtual button on touch screen to remotely open the door controlled by the related GDS37xx. There is no door limitation for such usage but only ONE DOOR can be opened at one time. It is just a SIP call open door application, but strike/lock control circuit is located outdoor.

For “Secure Open Door”, the GSC3570 is pairing with GDS37xx. The GSC3570 controlling the relay/strike/lock from inside the building (Unlike GDS37xx installed outside), but only ONE door can be controlled because GSC3570 only has one Relay Control circuit build in.
This pairing can be via LAN/WAN but LAN is recommended and actually most of the application scene are in LAN environment because most likely the GSC3570 and GDS37xx are in the same building.

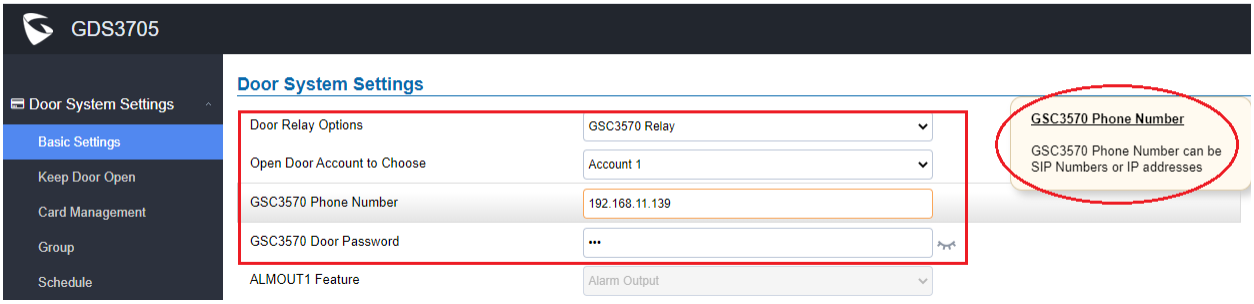
Although SIP/UCM over Internet/WAN also works, it is recommended to use static IP if the GSC3570 (inside) and GDS37xx (outside) are at same location in the same LAN. This setup is much simple and reliable in case there is network outage like Internet/UCM is down.

For the GSC3570 and GDS37xx pairing, it can be used via SIP only (Cloud or UCM); IP only (No SIP proxy or UCM but static IP address) and Mixed (SIP and fallback to IP if Proxy failed).

- **Web Configuration**

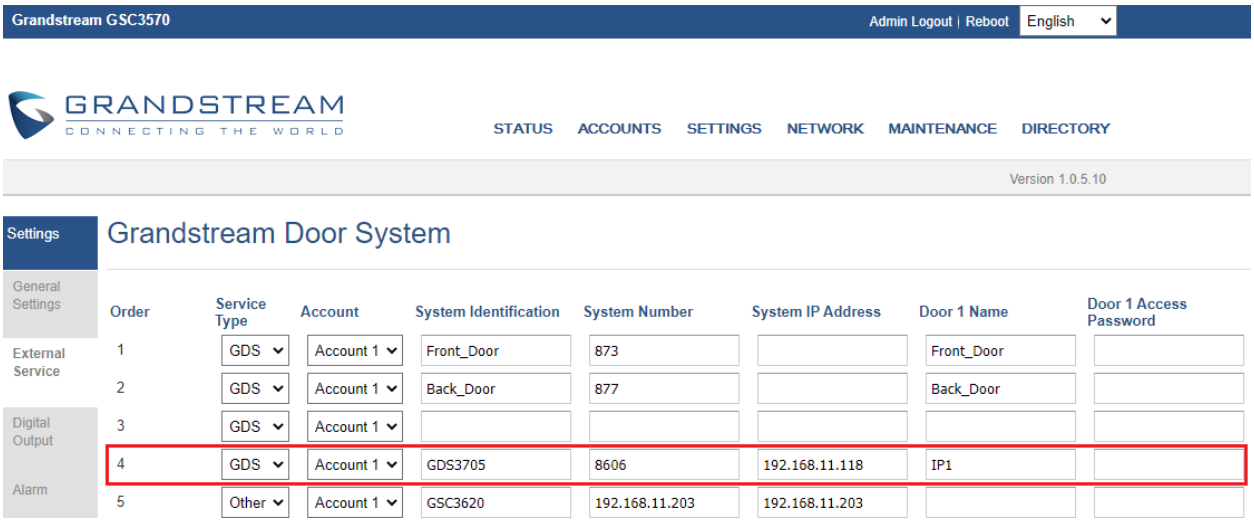
GDS3705: (FW: 1.0.1.16 or above)

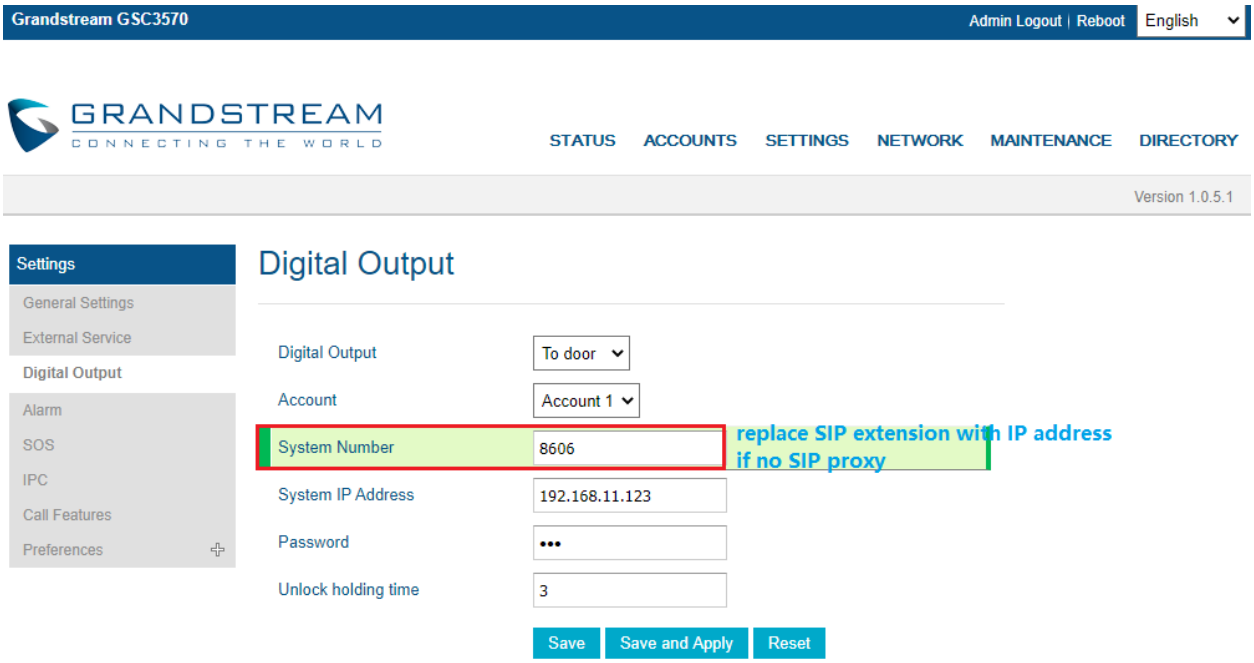
This setup can be found under device web UI → Door System Settings → Basic Settings:



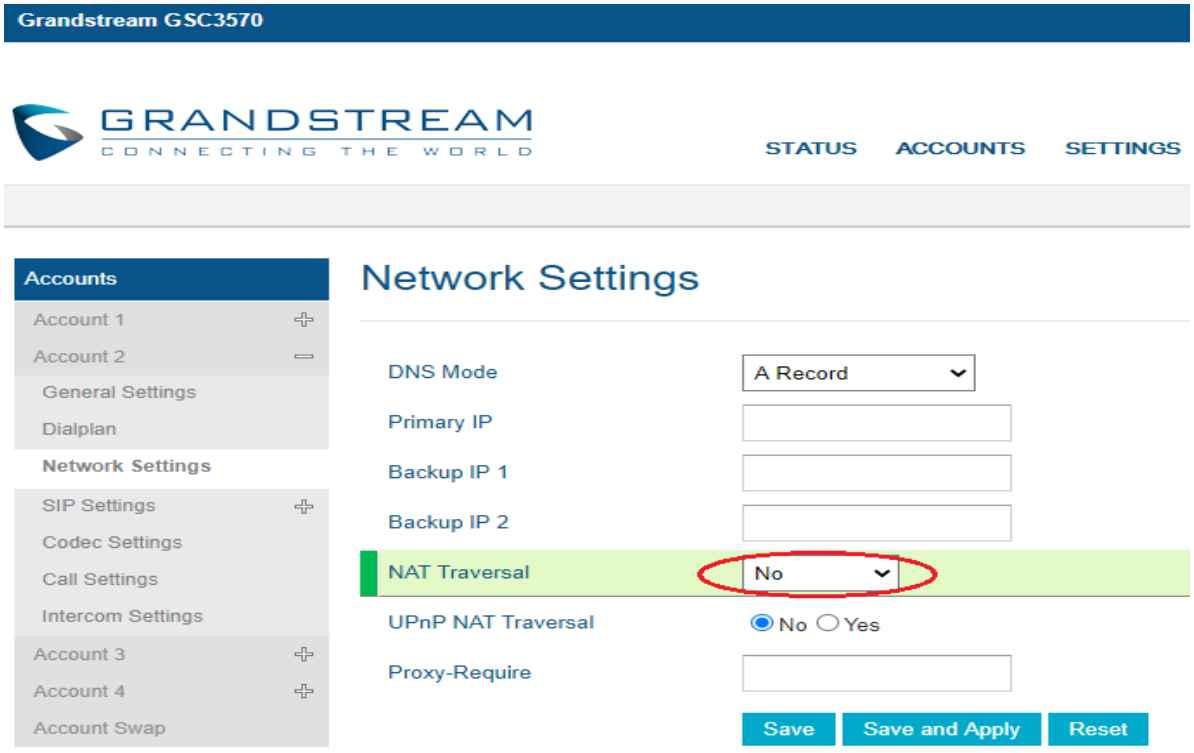
GSC3570: (FW: 1.0.5.2 or above)

The GSC3570 side also need to be configured according, like below:





If the solution/integration is using static IP address without SIP Proxy, all the devices involved (GDS/GSC/IP Phone) should choose "NAT Traversal" to "No" and should NOT "Use Random Port", otherwise will have problem of ghost call (SIP signaling working but NO media).

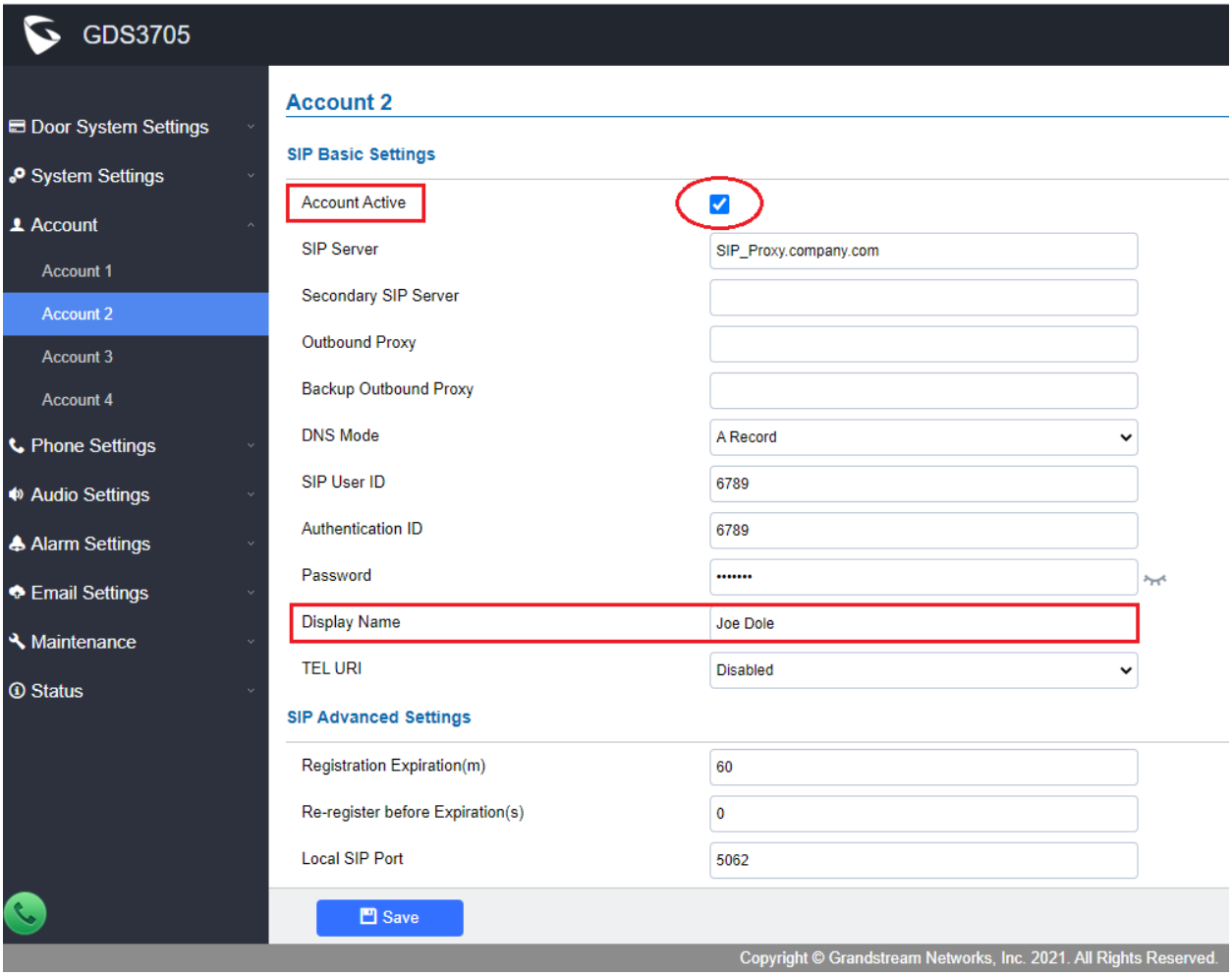


The IP phone or GSC3570 can use any empty SIP account, meaning it can be mixed if Account 1 registered to UCM/Proxy and Account 2 (blank) to use IP (but the account has to be configured as "Active").

ADDED SIP ACCOUNT ACTIVE FEATURE

- **Web Configuration**

This option can be found under device web UI → Account → Account X:



- **Functionality**

This feature enhancement is based on request and feedback from customers in field.

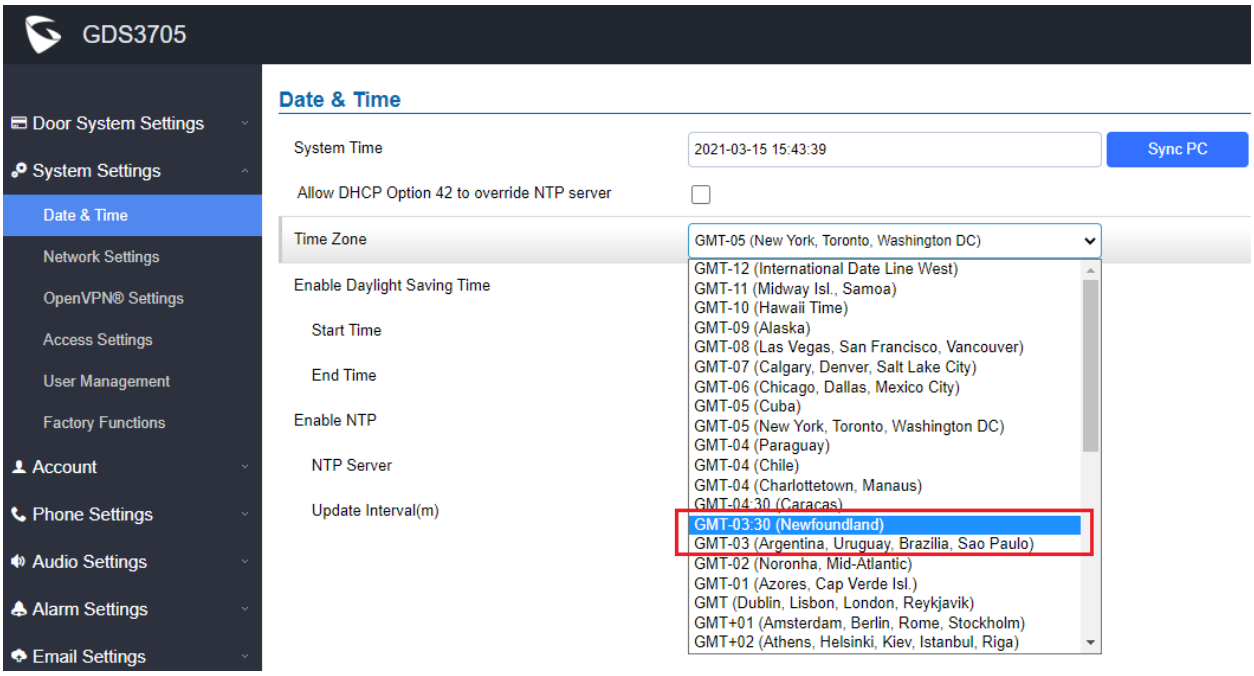
With this feature, the GDS3705 will behave and function the same as Grandstream IP Audio Phone.

When enable Account Active, but without configure SIP Server or User ID (leave those field blank), this feature will allow GDS3705 to receive calls via IP with different Account via different Port specified.

ADD "GMT-3:30" TIME ZONE SUPPORT

- **Web Configuration**

This option can be found under device web UI → System Settings → Date & Time:



:

- **Functionality**

This is a major security enhancement for GDS37xx (GDS3705/3710). With OpenVPN supporting, customer can link GDS37xx over VPN network, operating and controlling it.

For detailed information, please refer to User Manual and Resource Center:

- **GDS3705 User Manual:**
  http://www.grandstream.com/sites/default/files/Resources/GDS3705_UserManual.pdf

- **HOW-TO Guide**
  http://www.grandstream.com/support/resources/?title=GDS3705

FIRMWARE VERSION 1.0.1.11

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

07/01/2020

SUMMARY OF UPDATE

This firmware update of GDS3705 is mainly for feature enhancement and bug fixes.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI. Please backup the data and configuration before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed doorbell parallel hunting call one users reject the call will stop other group member ringing.
- Fixed Event Notification Logs still sending out when disabled or unauthorized card used to open door.
- Fixed device cannot be provisioned with general configuration file without MAC header of the unit
- Fixed doorbell call serial hunting will not move to next one if the first number rejected the call

ENHANCEMENT

- Added forcing user to change default password once default password used to log in
- Added WebRelay Open Door Feature
- Added OpenVPN support
- Added call termination button in the webUI
- Add configurable option to specify the cache time/refresh of DNS entries [Telefonica ITSP]
- Add ability to provision Card Management users [Telefonica ITSP]
- Added support for failover mechanism based on DNS SRV [Telefonica ITSP]
- Increased Unlock Holding Time to 30 minutes [Netia ITSP]
- Changed SIP Account Name to Display Name
- Added GDS37XX reboot/resync via SIP Notify
- Added ability in Event Log to display the attempts of unauthorized cards to open door
- Added support of User Name in HTTP Event Notification

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping even after pressing phone's keypad which supposedly should stop the siren audio at SIP phone side.

NEW HTTP API

- P4208
- P28160

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

- P15440 / P15441
- P15442 / P15443

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

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

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

- P9902 / P9903 / P9904

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

- P4428

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

NEW P-VALUE

- P4208: Phone_Settings.Phone_Settings.DNS_Cache_Expiration_Time. *(value range: 1 ~1440)*
- P28160: Phone_Settings.Phone_Settings.DNS_Cache_Duration. *(value range: 0 ~ 1440)*
- P15440: Door_System_Settings.Basic_Settings.Door_Relay_Options. *(value: 0: Local Relay; 1: WebRelay)*
- P15441: Door_System_Settings.Basic_Settings.Webrelay_IP_Address. *(Type: string; Max.length = 255)*
- P15442: Door_System_Settings.Basic_Settings. Webrelay_Username. *(Type: string; Max.length = 128)*
- P15443: Door_System_Settings.Basic_Settings. Webrelay_Password. *(Type: string; Max.length=128)*
- P7050: System_Settings. OpenVPN® Settings.Openvpn_Enable. *(value: 0: Disable; 1: Enable)*
- P7051: System_Settings. OpenVPN® Settings.Openvpn_Server_Address. *(Type: string. Max.length=256)*
- P7052: System_Settings. OpenVPN® Settings.Openvpn_Port *(value range: 0 ~ 65535)*
- P2912: System_Settings. OpenVPN® Settings.Openvpn_Transport *(value: 0: UDP; 1: TCP)*
- P9902: System_Settings. OpenVPN® Settings.Openvpn_ CA *(Type: string; Max length = 8192)*
- P9903: System_Settings. OpenVPN® Settings.Openvpn_ Client_Certificate *(Type: string; Max length = 8192)*
- P9904: System_Settings. OpenVPN® Settings.Openvpn_ Client_Key *(Type: string; Max length = 8192)*
- P8396: System_Settings. OpenVPN® Settings.Openvpn_Cipher_Method
  (value: 0: Blowfish; 1:AES-128; 2:AES-256; 3:Triple-DES)
- P8394: System_Settings. OpenVPN® Settings.Openvpn_ Username *(Type: string; Max.length=256)*
- P8395: System_Settings. OpenVPN® Settings.Openvpn_ Password *(Type: string; Max length is 256)*
- P8460: System_Settings. OpenVPN® Settings. Additional_Options *(Type: string; Max.length=1024)*
- P4428: Maintenance.Upgrade.Disable_SIP_NOTIFY_Authentication *(value: 0: disable; 1:enable)*

MODIFIED P-VALUE

- P14101: Unlock Action Holding Time *(value range updated from: 0 ~ 20 to 0 ~ 1800)*
- P15466: Door 2 Unlock Action Holding Time *(value range updated from: 0 ~ 20 to 0 ~ 1800)*

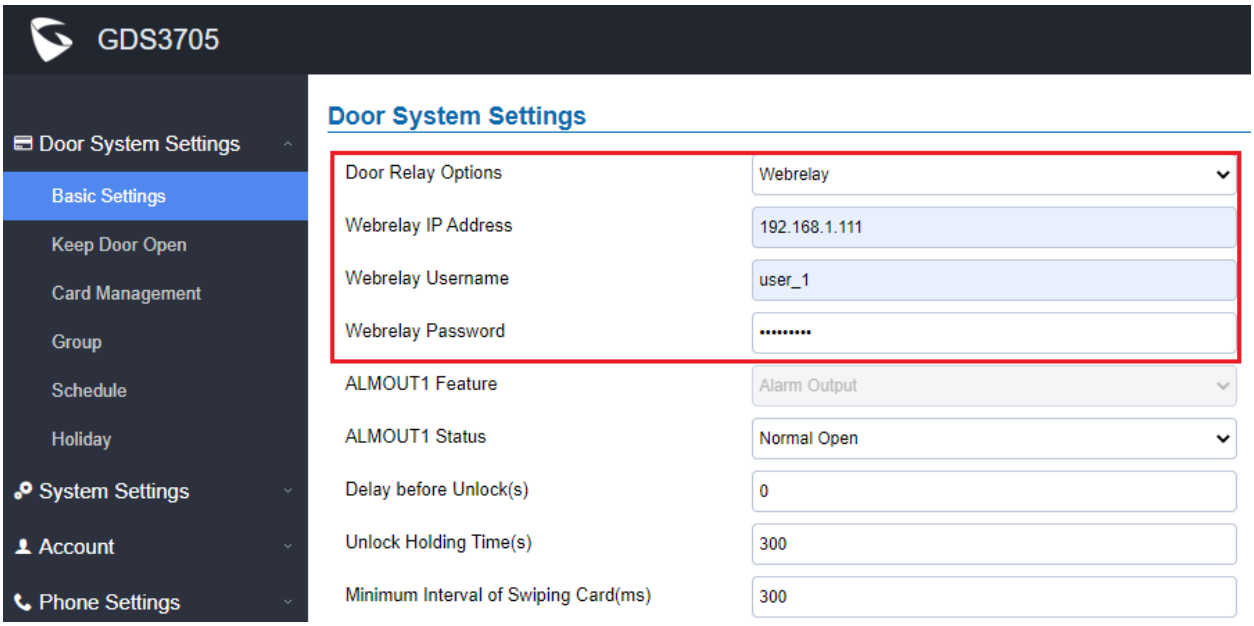
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

SUPPORT WEBRELAY OPEN DOOR

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings → Door Relay Options: Pull down UI has two choices, Local Relay or Webrelay



- **Functionality**

This is a major feature enhancement based on feedback from field. This feature allow customers to integrate GDS37XX with 3rd party webrelay to control door open over network, via script or other applications, to meet real application scene and enhance security.

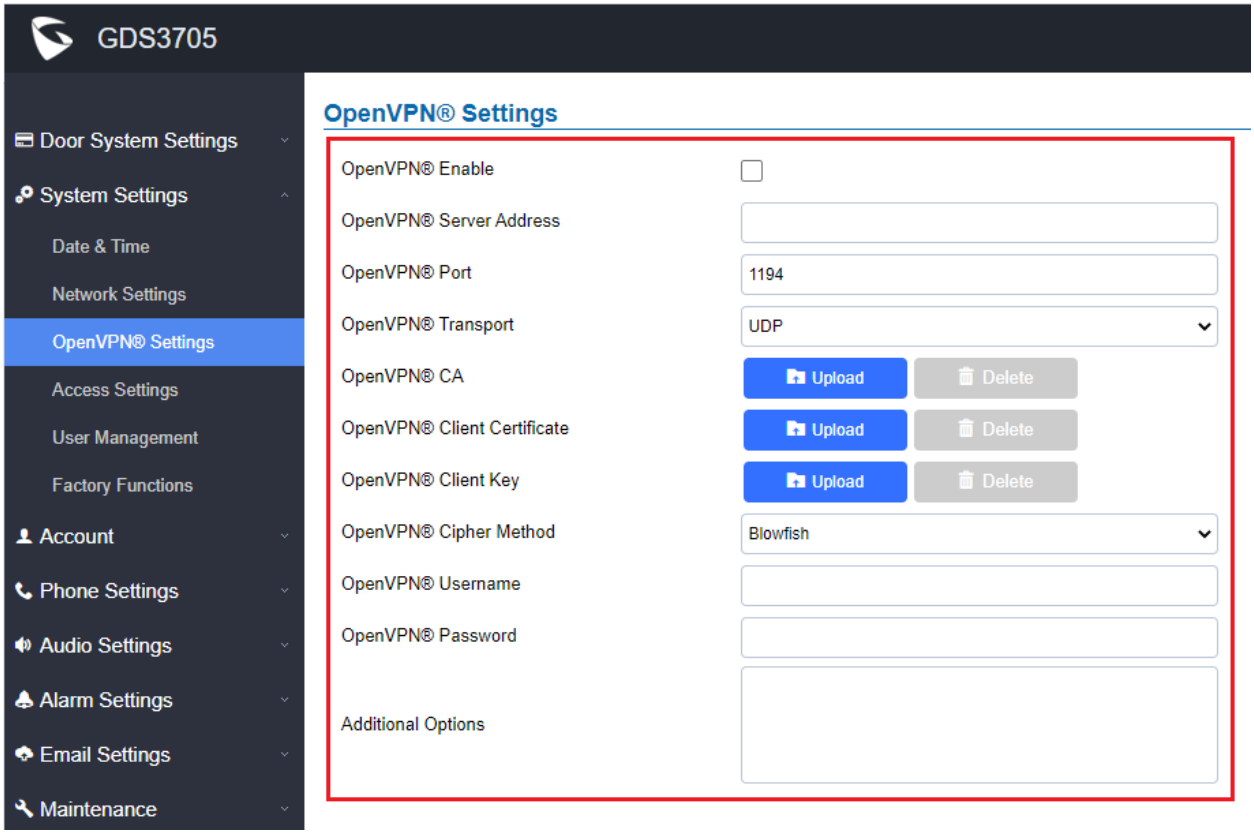
Users need to input webrelay IP address or domain name, as well as authentication information, to make this to work.

For details please refer to GDS37XX user manual, as well as the webrelay technical document and user manual.

SUPPORT OPEN VPN

- **Web Configuration**

This option can be found under device web UI → System Settings → OpenVPN Settings:



- **Functionality**

This is a major security enhancement for GDS37xx (GDS3705/3710). With OpenVPN supporting, customer can link GDS37xx over VPN network, operating and controlling it.

For detailed information, please refer to User Manual and Resource Center:

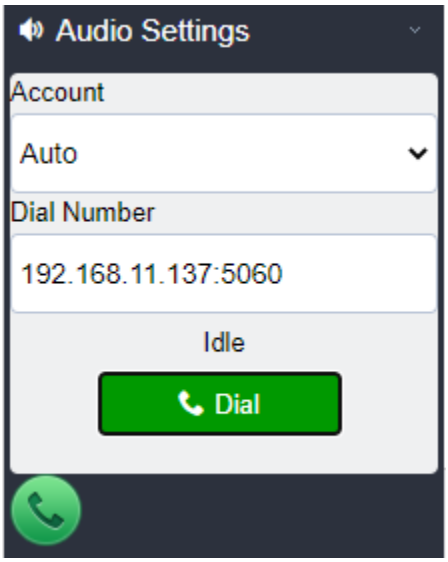
- GDS3705 User Manual:
  http://www.grandstream.com/sites/default/files/Resources/GDS3705_UserManual.pdf

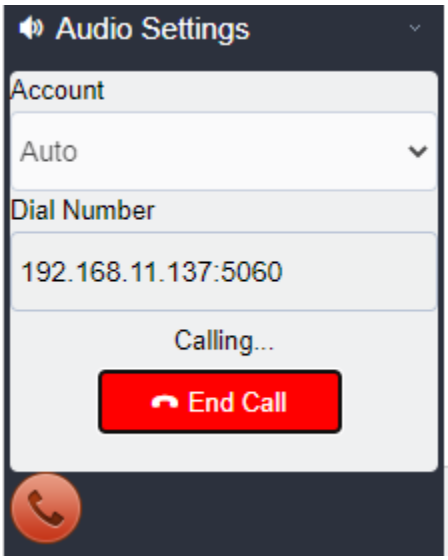
- HOW-TO Guide
  http://www.grandstream.com/support/resources/?title=GDS3705

ADDED CALL TERMINATION BUTTON IN WEBUI

- **Web Configuration**

This option can be found when log in to the webUI, displayed at lower left corner of the UI:





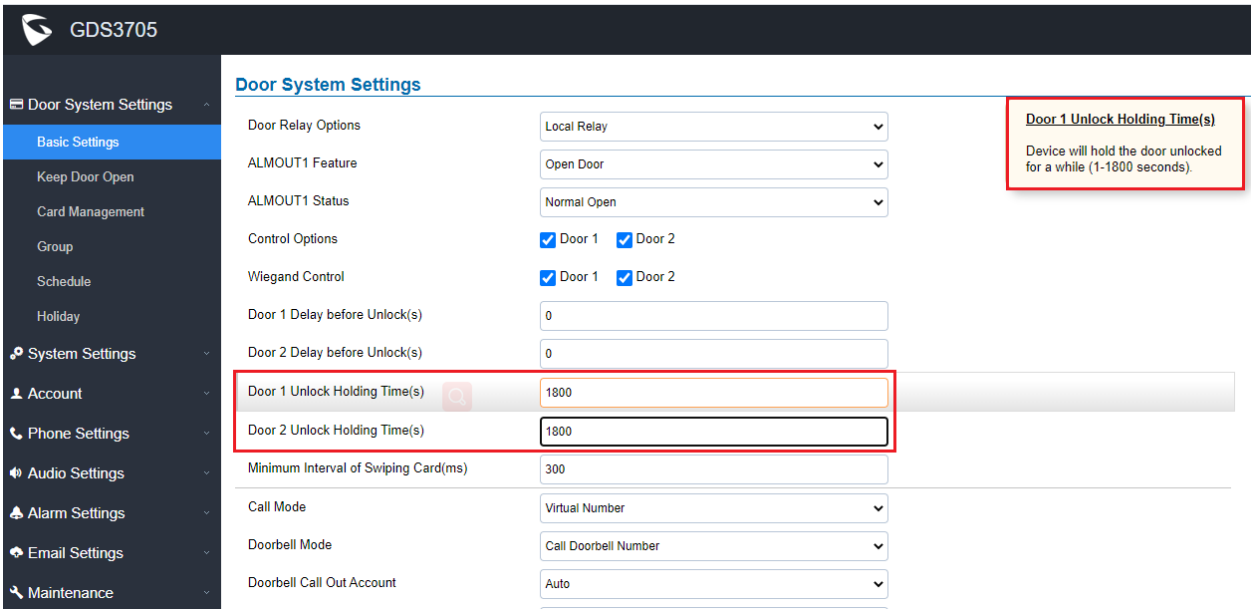
- **Functionality**

This feature allows user to make calls by input extension number or IP address, and terminate the calls from webUI, for user's convenience, like testing or verification.

INCREASED UNLOK HOLDING TIME TO 30 MINUTES

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



- **Functionality**

This feature enhancement is based on request and feedback from customers in field.

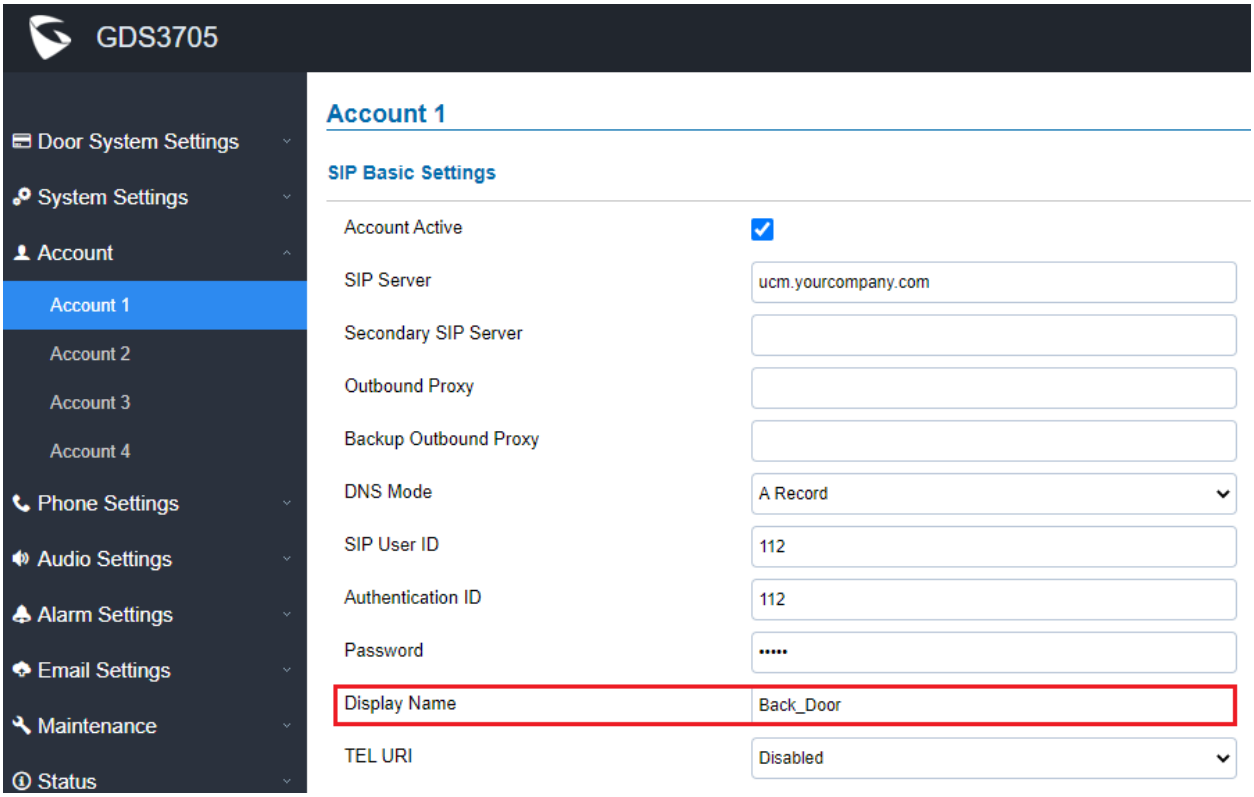
The Unlock Holding Time maximum value is increased from 20 seconds to 1800 seconds (or 30 minutes).

The request is raised by customers using GDS37XX in scenes like Senior House. This is special useful during COVID-19 pandemic period where Senior House is forbidden outside people visiting. Increase the unlock holding time so the people in wheelchair can push button to unlock the door, get outside to do some activities like pickup online ordering stuff, dropping trash, etc., and coming back, without other person involved. This will reduce human contract, and minimize the risk of COVID-19.

CHANGED SIP ACCOUNT NAME TO DISPLAY NAME

- **Web Configuration**

This option can be found under device web UI → Account → Account X:



- **Functionality**

The GDS3705 is an audio only device, unlike GDS3710, user cannot see who in at the door.

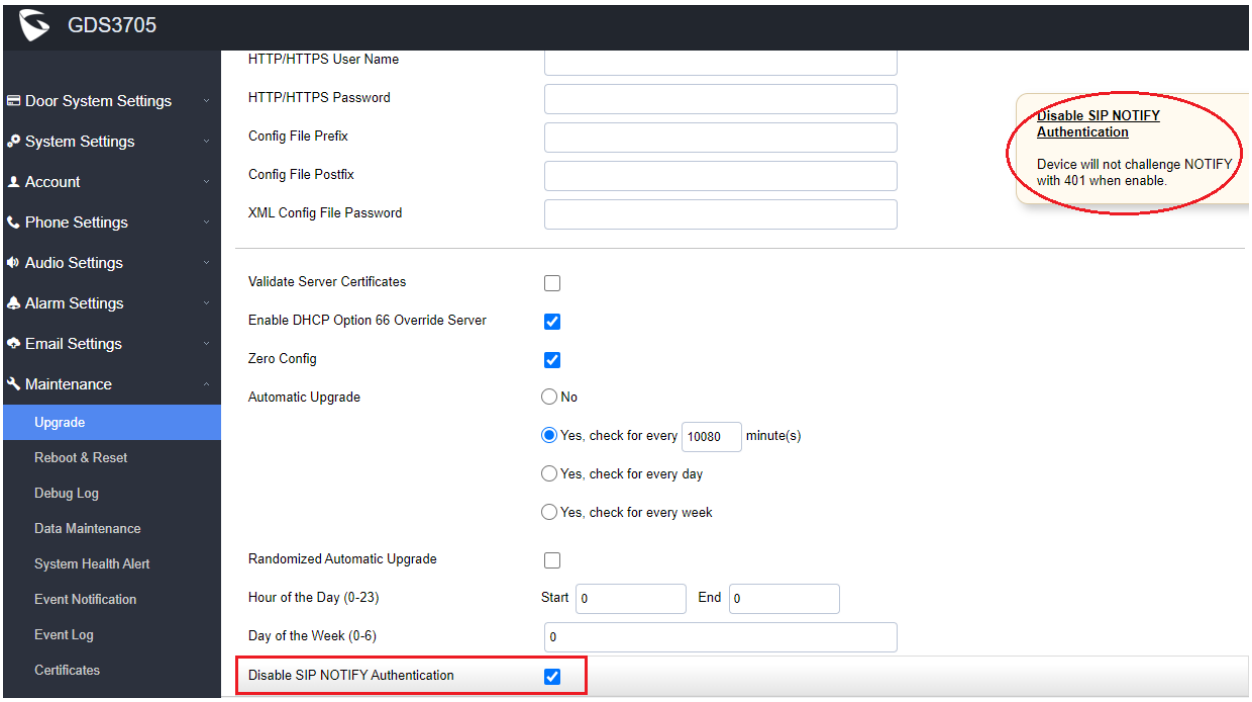
Adding this “Display Name” will also allow user receiving calls from GDS3705 knowing where the call is coming from (e.g.: which door or extension the call is made), improve user experience when user is using an IP phone with LCD display.

This feature enhancement is also in response to customer’s feedback from field.

ADDED REBOOT/RESYNC VIA SIP NOTIFY

- **Web Configuration**

This option can be found under device web UI → Maintenance → Upgrade:



- **Functionality**

This feature is disabled with security authentication previously based on request from ITSP customers, but lots of system integrators or system administrators still want to use this feature to remote reboot the GDS37xx for maintenance, firmware upgrade, re-provisioning, etc.

Based on feedback from customers in field, this feature is added back by a switch. By Default this feature is disabled with 401 Challenge NOTIFY.

Customer who need this feature to reboot device need manually check “Disable SIP NOTIFY Authentication” option (with understanding of potential security risk), then the device will response to the related SIP NOTIFY message to reboot the device (at some particular time with the control scripts from server), to do routine maintenance, firmware upgrade, etc., for the convenience of system administrator.

FIRMWARE VERSION 1.0.1.6

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

12/28/2019

SUMMARY OF UPDATE

This is a major feature update for GDS3705 as well as bug fixes, mainly for ITSP customers.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI. Please backup the data and configuration before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed abnormal open door sometimes alarm may not trigger issue
- Fixed virtual number peering call not working between GDS and SIP phone
- Fixed device cannot be re-provisioned when CFG file includes firmware upgrade and provisioning parameters
- Fixed rejecting call did not send 486 busy here (3CX IOT)
- Fixed 200 OK SDP out of order (3CX IOT)
- Fixed not recognizing DTMF input (3CX IOT)

ENHANCEMENT

- Added support for failover mechanism based on DNS SRV
- Added siren alarming function when door opened abnormally (special wiring required)
- Added including Holidays at Keep Door Open schedule
- Added reset/restore factory default password via special keypad combination operations

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping even after pressing phone's keypad which supposedly should stop the siren audio at SIP phone side.

NEW HTTP API

IP15508: (value: 0/1)	Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_1_Abnormal_Door_Control_Options GET: http://ip:port/goform/config?cmd=get&type=event SET: http://ip:port/goform/config?cmd=set&P15508=<value>
IP15509: (value: 0/1)	Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_2_Abnormal_Door_Control_Options GET: http://ip:port/goform/config?cmd=get&type=event SET: http://ip:port/goform/config?cmd=set&P15509=<value>

NEW P-VALUE

- P15508: *(value: 0/1)*
  Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_1_Abnormal_Door_Control_Options
- P15509: *(value: 0/1)*
  Alarm_Settings.Alarm_Events_Config.Digit_Input.Digit_Input_2_Abnormal_Door_Control_Options

MODIFIED P-VALUE

N/A

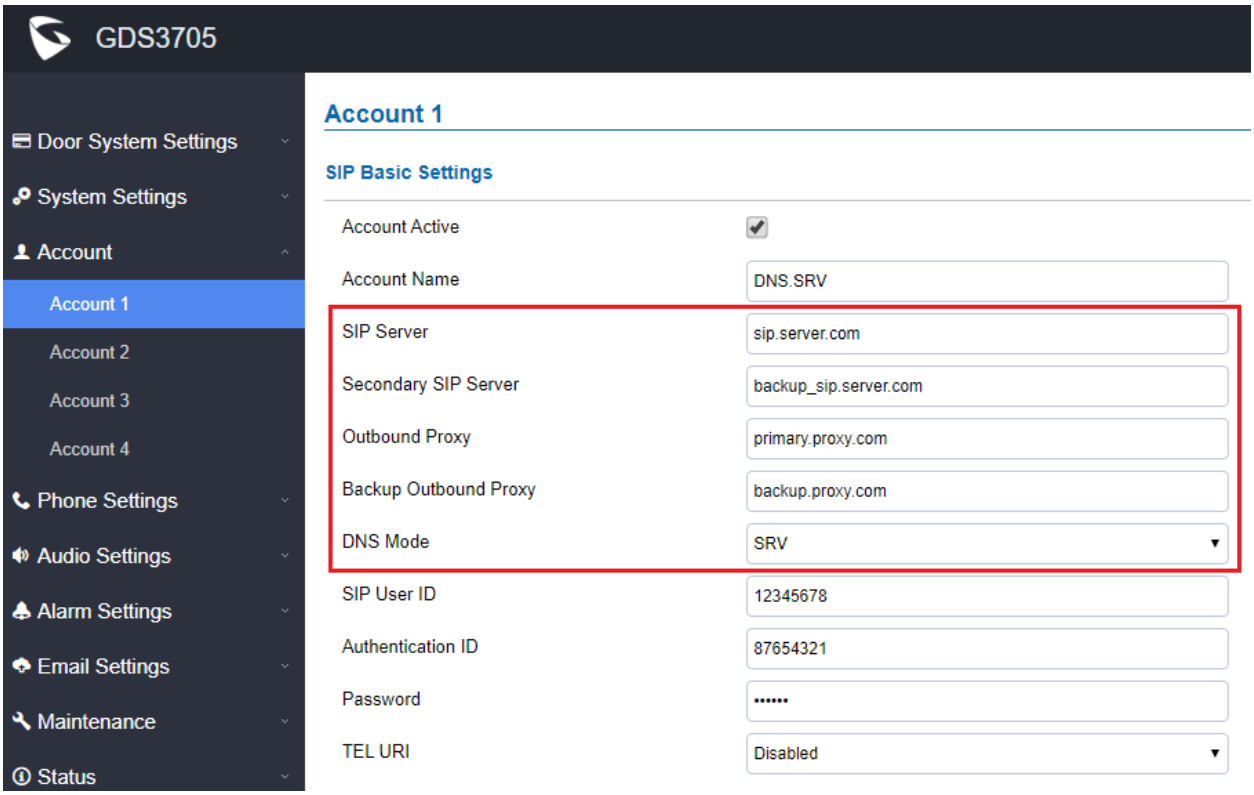
NEW FEATURES OVERVIEW

This section lists major new features or improvement and describes how to use them from the user's point of view.

SUPPORT FAILOVER MECHANISM ON DNS SRV

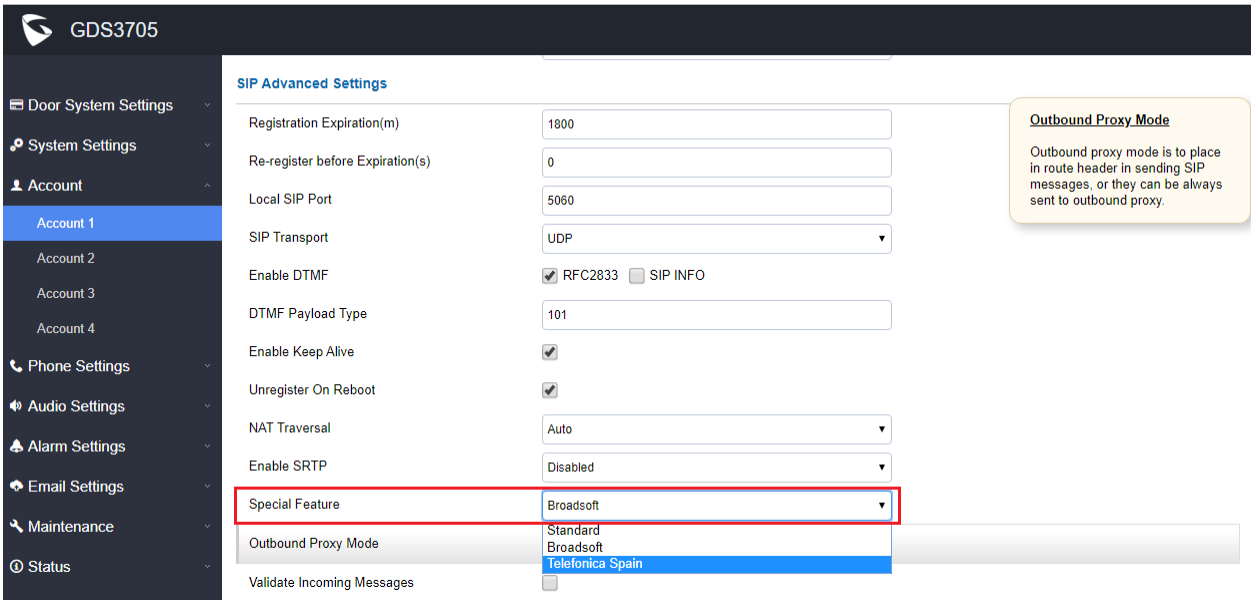
- **Web Configuration**

This option can be found under device web UI → Account → Account X (X=1, 2, 3, and 4):



- **Functionality**

This is a major feature enhancement for Service Provider, via DNS SRV (mainly for BroadSoft certified Soft Switch for major Internet Telephony Service Providers). Service providers can use this feature to provider smooth service transition backup in case service down.

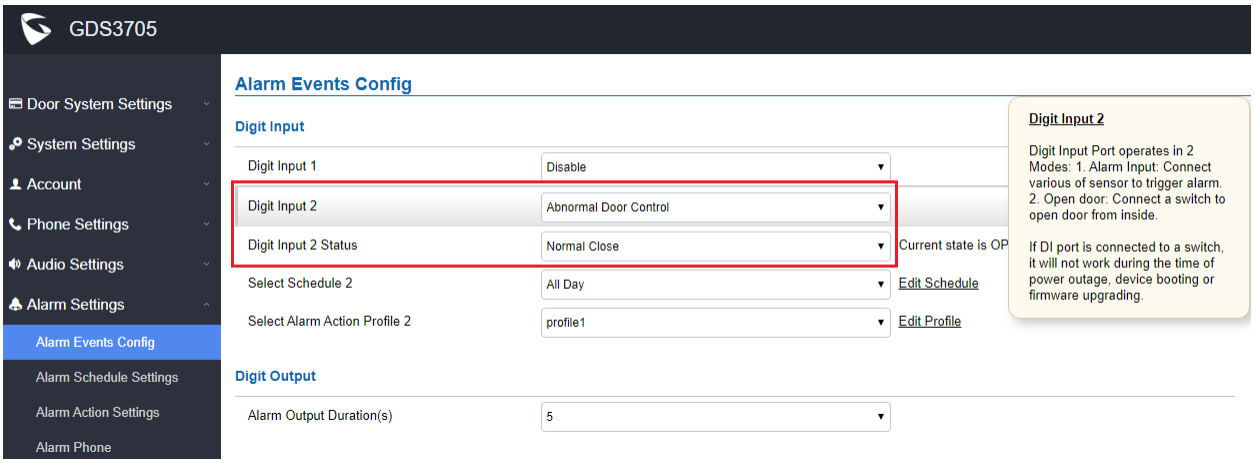


In the device web UI → Account X (X=1, 2, 3, and 4) → SIP Advanced Settings → Special Feature: There is a new feature specially designed for Telefonica Spain to match the service provided by Telefonica to their customers. Just need to enable this feature via either WebUI or Provisioning.

SIREN ALARMING WHEN DOOR OPENED ABNORMALLY (SPECIAL WIRING REQUIRED)

- **Web Configuration**

This option can be found under device web UI → Alarm Settings → Alarm Events Config → Digit Input:



- **Functionality**

This is a major security enhancement for GDS37xx (GDS3705/3710) when device be tampered to open the door abnormally.

When this feature enabled (**special wiring required, see below wiring diagram**), abnormal open door will be detected by DI port (Alarm_In2 or IN2 in below diagram showed) if wired correctly (connecting the COMx port to DIx port) therefore trigger **siren alarm**. Once abnormal open door alarm triggered, the **siren** will sound non-stop, until manually override by related person.

There are several ways to stop and disable the alarm:

1) Power cycle the GDS37xx
2) Pick up the Alarm Phone Call (if configured)
3) Open Door using PIN (either public PIN or private PIN)

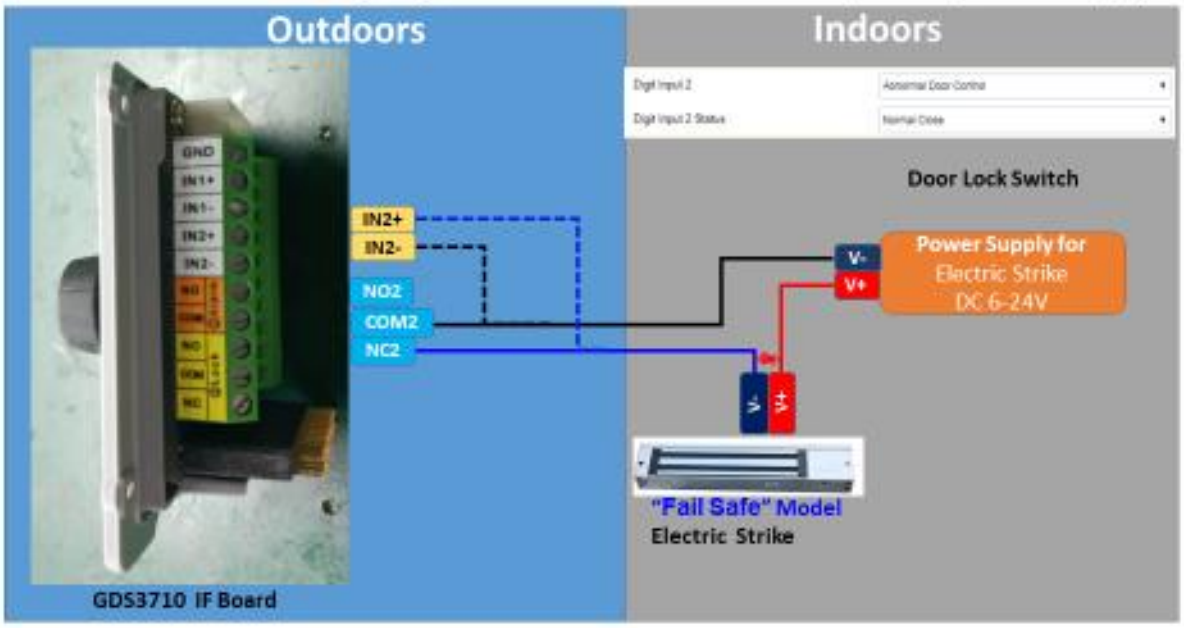
Once alarm triggered, the GDS3705 will play **siren** sound, send email to administrator (if configured SMTP); call the configured alarm SIP phone, send the alarm output (if connected). User will only be able to disable the siren using the 3 methods mentioned above.

Detailed action information please refer to GDS37xx User Manual, “Alarm Action Settings” configuration. Below are some diagrams showing the correct wiring to enable this new security enhancement feature.

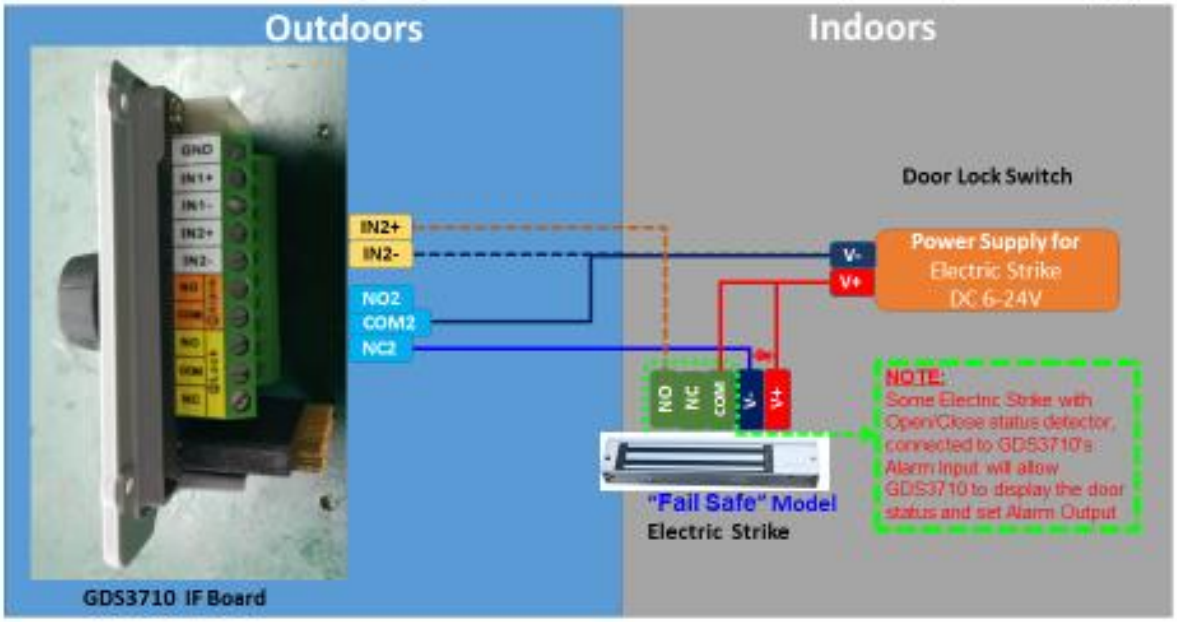
NOTE:

- *GDS3705 and GDS3710 sharing the SAME **interface backboard**. For convenience, the below diagrams are using GDS3710 as example.*
- *GDS3705 is exactly the same as GDS3710 in wiring for this feature. This means the interface backboard can be shared between GDS3705/3710. **Swap the device does NOT need to rewire**.*

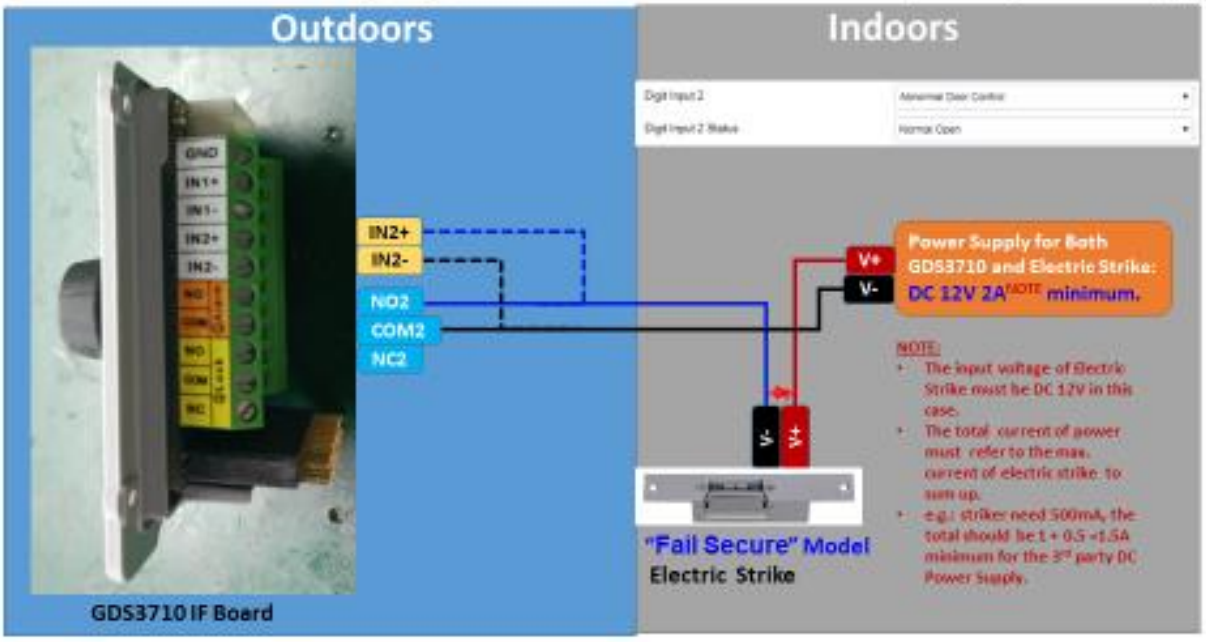
GDS3710 Connection & Wiring Diagrams ---- "Fail Safe" Electric Strike, 3rd Party Power Supply



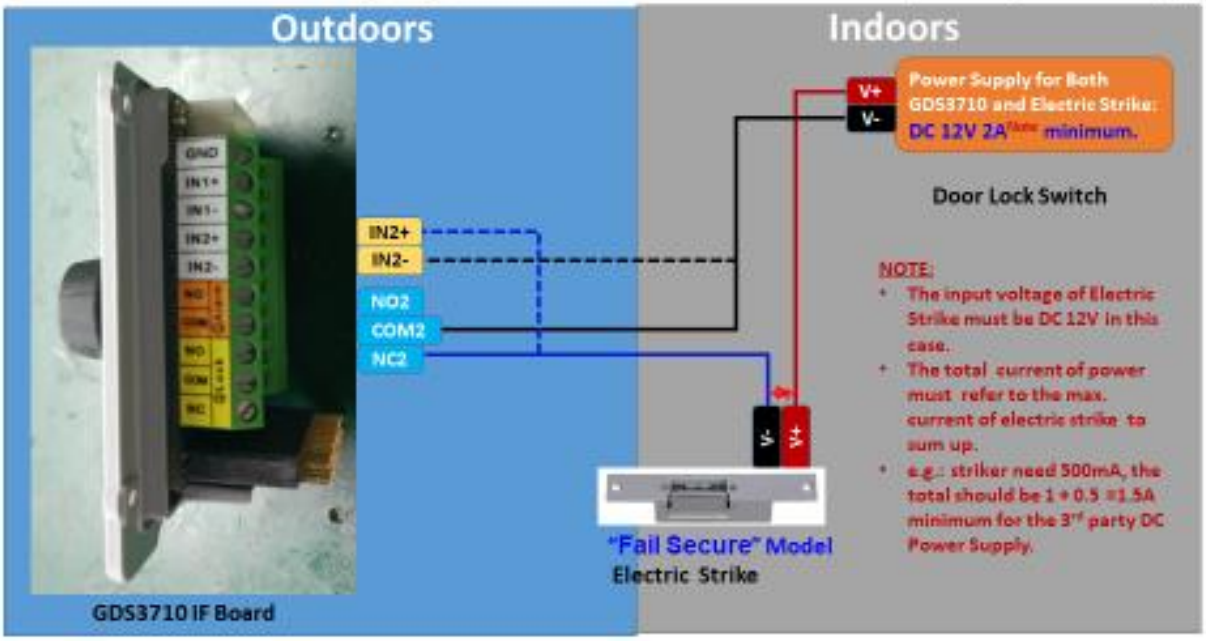
GDS3710 Connection & Wiring Diagrams ---- "Fail Safe" Electric Strike, 3rd Party Power Supply



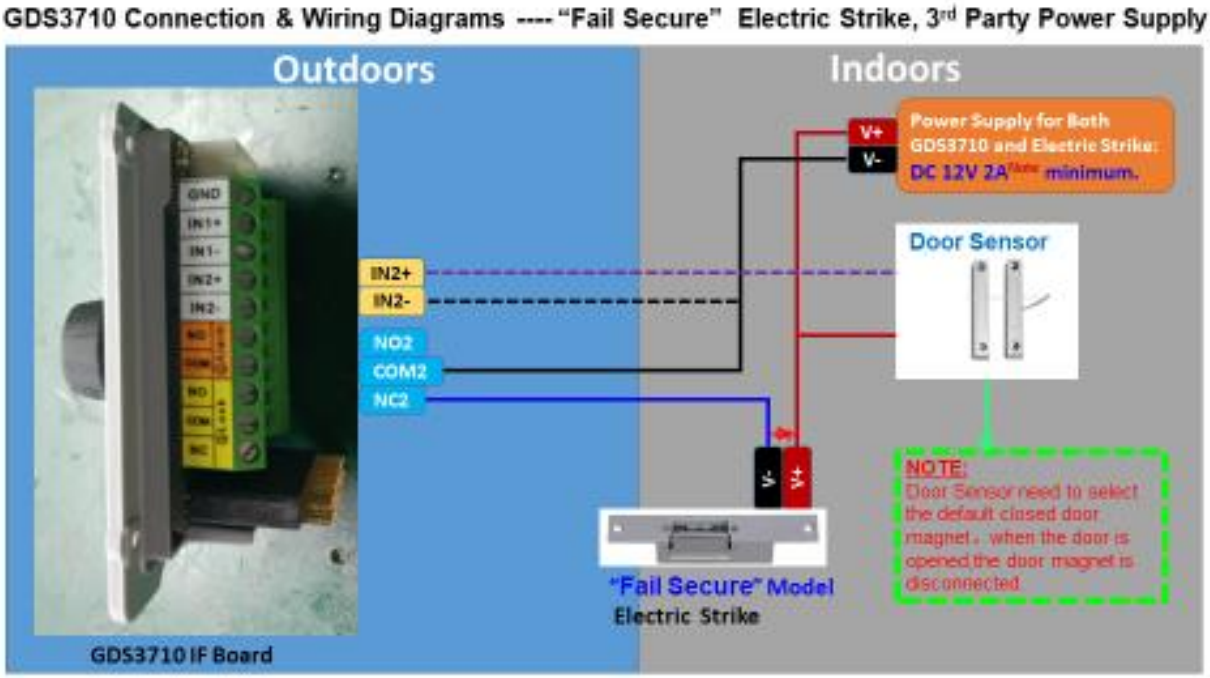
GDS3710 Connection & Wiring Diagrams ---- "Fail Secure" Electric Strike, 3rd Party Power Supply



GDS3710 Connection & Wiring Diagrams ---- "Fail Secure" Electric Strike, 3rd Party Power Supply



If 3rd party door sensor installed, customer could wire the door sensor signal directly into the DI port (DI2 in below example) to trigger the alarm if the door opened abnormal. See below diagram:



For detailed information, please refer to User Manual and Resource Center:

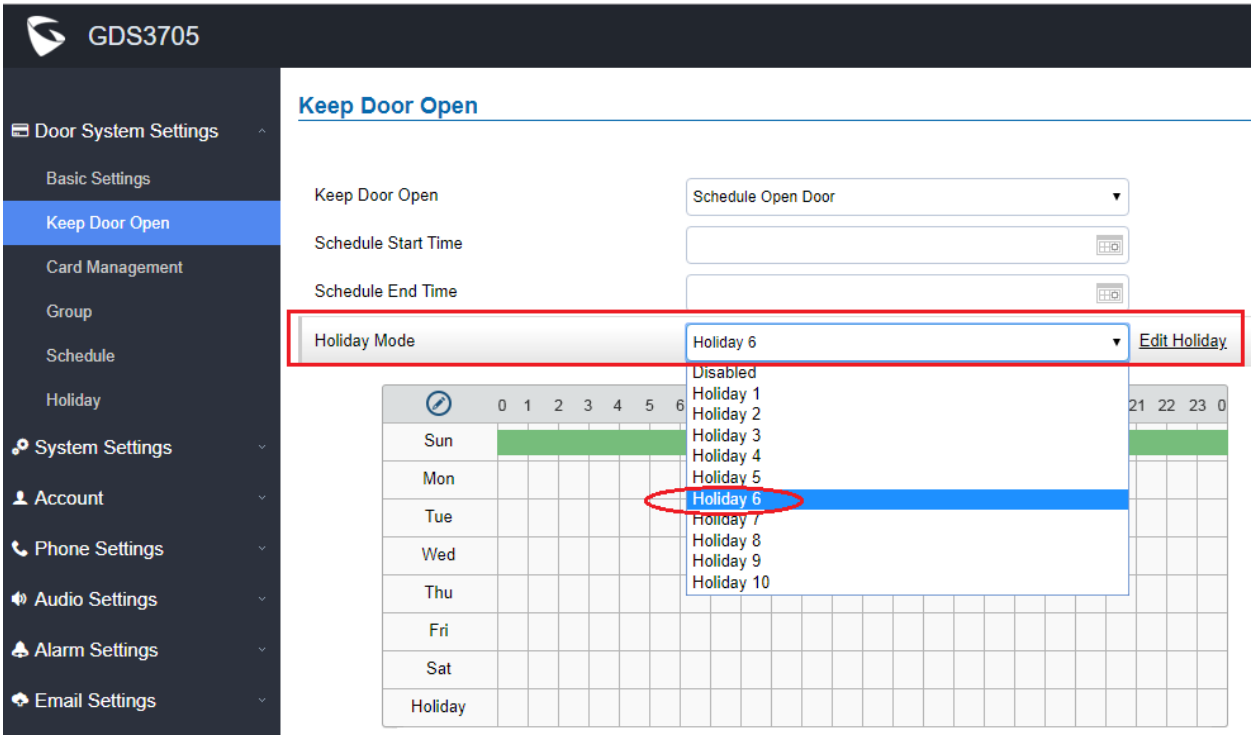
- GDS3705 User Manual:
  http://www.grandstream.com/sites/default/files/Resources/GDS3705_UserManual.pdf

- HOW-TO Guide
  http://www.grandstream.com/support/resources/?title=GDS3705

SUPPORT HOLIDAYS IN KEEP DOOR OPEN SCHEDULE

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Keep Door Open:



- **Functionality**

This feature is implemented based on field customer feedback either.

When configure Keep Door Open schedule, customers now can also specify which Holiday Schedule to be included into the Keep Door Open schedule, therefore make the GDS37xx more user friendly in such application scene configuration.

RESET FACTORY PASSWORD VIA SPECIAL KEY COMBINATION OPERATION

- **Functionality**

This is a new enhancement feature requested by ITSP service providers as well as lots of system integrators from Forum. This feature allows customers to reset the device administrator password to factory default via keypad operation through some special key combination.

When performing this operation, ONLY password will be reset back to factory default. All other setting or parameters will NOT be changed and will remain the same. This feature is specially designed for field engineers or technicians when dispatched in field but for some reason the administrator password is not available therefore not able to access the GDS37xx device to do the related maintenance.

Here are the steps to do such password reset operation via keypad:

Encoding Rules:

- Alphabet A – Z mapping to digit 1 – 26 respectively, no difference in lower or up case.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

NOTE:

- Suggest decoding the MAC and Password and write on paper before doing the reset operation.

Prerequisite condition:

1) MAC address of the GDS37xx (check the sticker at back of the device)
2) Default password of the GDS37xx (check the sticker at the back of the device)
3) Correct decoding the last 6 MAC address into digits (refer to encoding rule)
4) Correct decoding the default password into digits (refer to encoding rule)
5) Finish keypad input within 1 minute

Operation Steps:

1) When device is idle, input the special keypad combination with format: *****last_6_MAC**#**
2) Device will reach restore mode after correct digits in *Step 1)* entered. The backlight of keypad will flash quickly to tell operator the device is now in password reset/restore mode.
3) Operator will enter the correct decoded default password ending with # with format: **default_password_code#** via the keypad within 60 seconds.
4) If wrong code combination entered, the GDS37xx will beep with error sound (three short beeps) then exit the password reset mode, and the backlight will stop flashing.
5) If the correct default password decode entered within 60 seconds, GDS37xx will play a long beep sound (advising correct operation), the device will reboot itself automatically.
6) If keypad entry time out (not finish the input within 60 seconds), the device will exit this password reset mode automatically and stop the backlight flashing.

After successful password reset, operator will then be able to log into the GDS37xx webUI with default password, all the configuration inside the device will be the same and will NOT be changed.

For example:

Decoding the string into digits and write to paper before doing the operation:

Device with last 6 MAC address:	**33DDDD**
Decoding the last 6 MAC to digits would be:	***334444***
Default password is:	***xwpxz6AA***
Decoding the default password to digits would be:	***2423162426611***

1) Enter *****334444**#** via keypad, get into the password reset mode, the keypad backlight will flash quickly.
2) Within 60 seconds, enter **2423162426611#**, the device will play one long beep then reboot itself.
3) Wait the device finishing boot up, log in the webUI using the default password, **xwpxz6AA**

FIRMWARE VERSION 1.0.1.3

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

07/30/2019

SUMMARY OF UPDATE

This is a major feature update for GDS3705 as well as bug fixes, mainly for the ITSP features.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI. Please backup the data and configuration before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed audio setting customize ringtone has prompt in Chinese.
- Fixed reboot required to take effect when enable/disable DHCP Option 42.

ENHANCEMENT

- Added ITSP support: re-registration before expiration.
- Added “Only accept incoming SIP call from proxy server” to enhance security and prevent ghost calls.
- Added support for DHCP Option 42.
- Added support for Voice Frame Per TX at audio settings.
- Added support of separated webUI credentials for GDSManager.
- Added ability to enable multiple audio codecs simultaneously and specify priority of codecs.
- Added support for failover mechanism based on DNS SRV.
- Added support for schedule firmware upgrade/provisioning.
- Added support for G.729 audio codec.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping after pressing phone’s keypad.

NEW HTTP API

P37/P486/P586/P686	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P2330/P2430/P2530/2630	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P57/P58/P59/P60	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P451/P452/P453/P454	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P551/P552/P553/P554	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P651/P652/P653/P654	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P144	GET:[http|https]://<servername>/goform/config?cmd=get&type= date SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P8458/P285/P8459/P286	GET:[http|https]://<servername>/goform/config?cmd=get&type= upgrade SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>

NEW P-VALUE

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	**<parameter> =<value>**	**<parameter> =<value>**	**<parameter> =<value>**	**Model Supported**	**Values**	**Description**
P37=<int>	P486=<int>	P586=<int>	P686=<int>	GDS3710/GDS3705	<integer>	Voice Frame Per TX (1 - 64, Default 2)
P2330	P2430	P2530	P2630	GDS3710/GDS3705	<integer>	Re-register Before Expiration
P57/58/59/60	P451/452/453/454	P551/552/553/554	P651/652/653/654	GDS3710/GDS3705	String	Preferred Audio Code

- P144: System Settings/ Data&Time/ Allow DHCP Option 42 to override NTP server
- P8458: Maintenance/Upgrade/Randomized Automatic Upgrade
- P285: Maintenance/Upgrade/Hour of the Day (0-23)Start
- P8459: Maintenance/Upgrade/ Hour of the Day (0-23)end
- P286: Maintenance/Upgrade/ Day of the Week (0-6)

MODIFIED P-VALUE

N/A

NEW FEATURES OVERVIEW

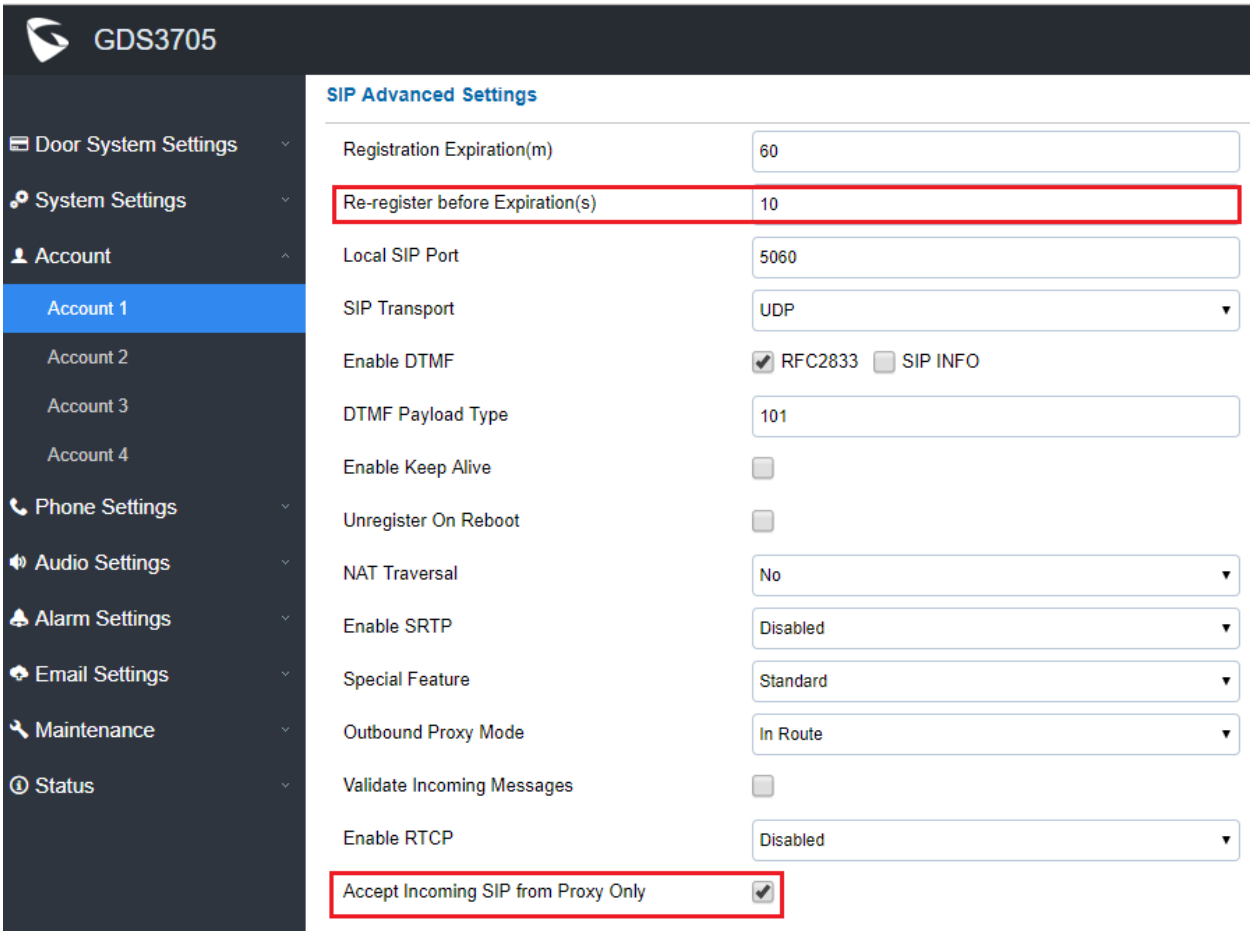
This section lists major new features and describes how to use them from the user's point of view.

Advanced SIP Settings for ITSPs: Re-register & Accept incoming calls from Proxy Only

- **Web Configuration**

New feature added in SIP Advanced Settings allows server providers (ITSP) to provide specified service to the customers.

This option can be found under device web UI: Account → Account X (X = 1, 2, 3 and 4):



- **Functionality**

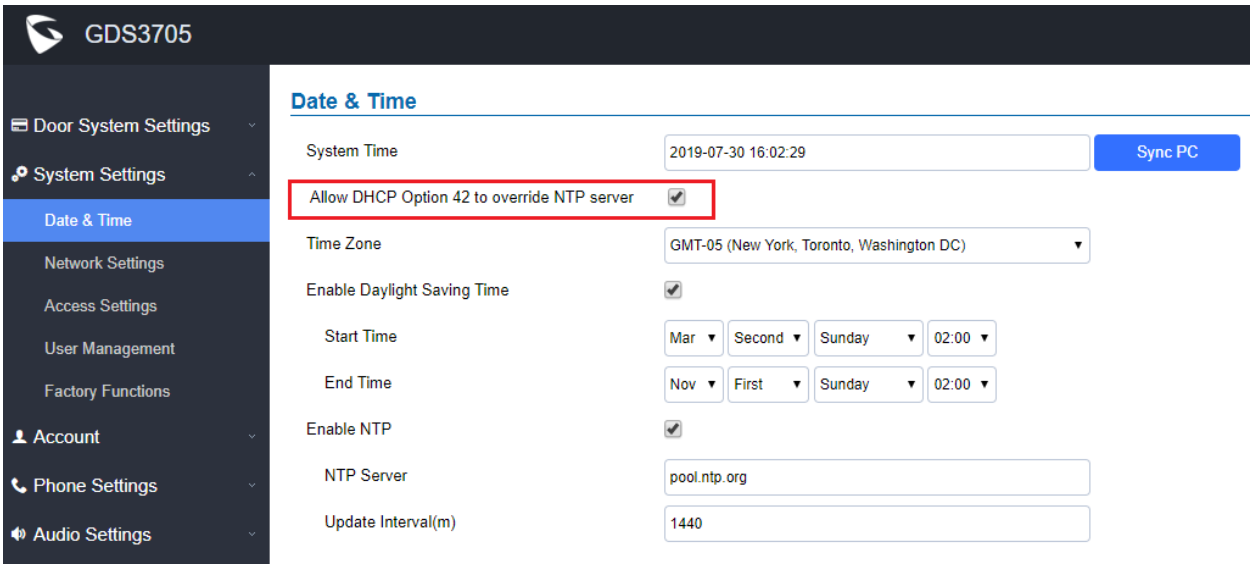
This feature is added to meet the requirement of ITSP customers. Service provider (ITSP) customers can configure the device to the customers.

DHCP Option 42

- **Web Configuration**

This feature is added to allow service providers (ITSPs) to configure system time based on DHCP server configuration.

The option of this webUI can be found: System Settings → Date & Time:



- **Functionality**

This feature is added to allow service provider customer to control system time via DHCP server.

NOTE:

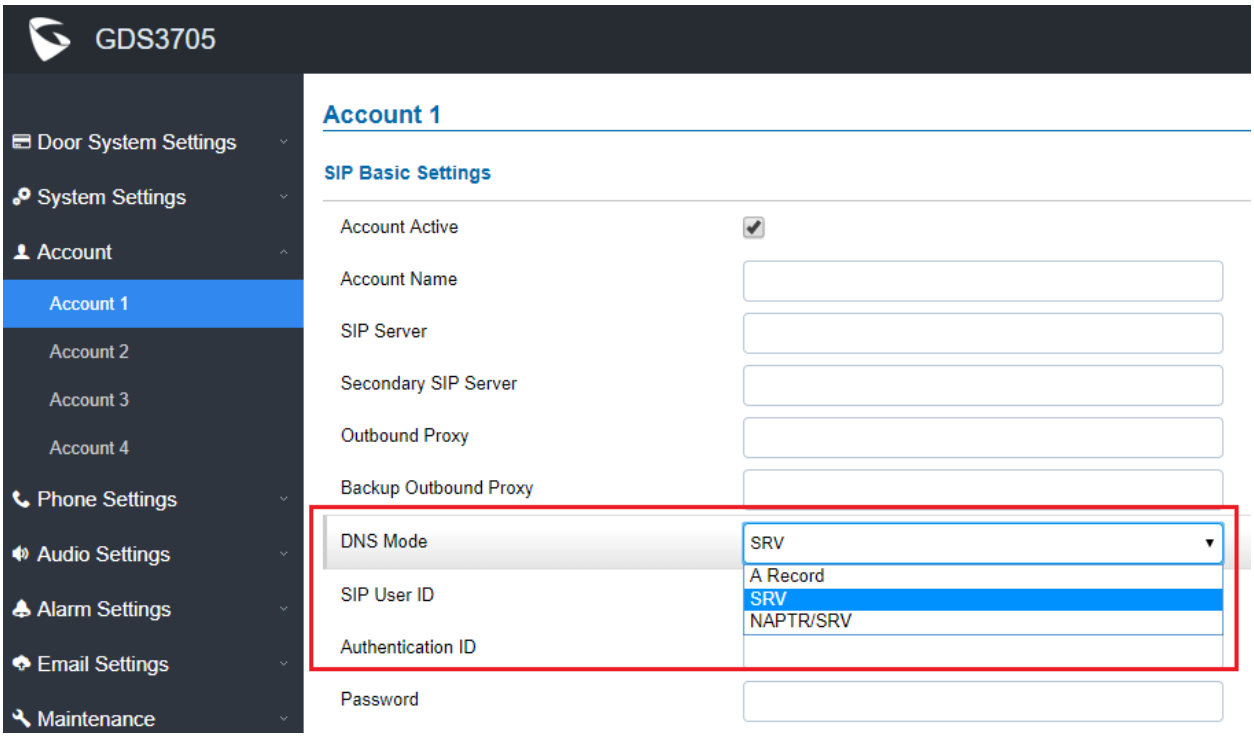
- This feature is designed for Service Provider, or Service Technician or Installers.
- End users without necessary knowledge are strongly discouraged to use it, avoiding incorrect system time caused by misconfiguration.

DNS SRV Support

- **Web Configuration**

This feature is added to allow service provider customers (ITSP) provide backup service in case there is an interruption. This is more like IP Phone feature from ITSPs.

The option of this webUI can be found: Account → Account X (X = 1, 2, 3 and 4)



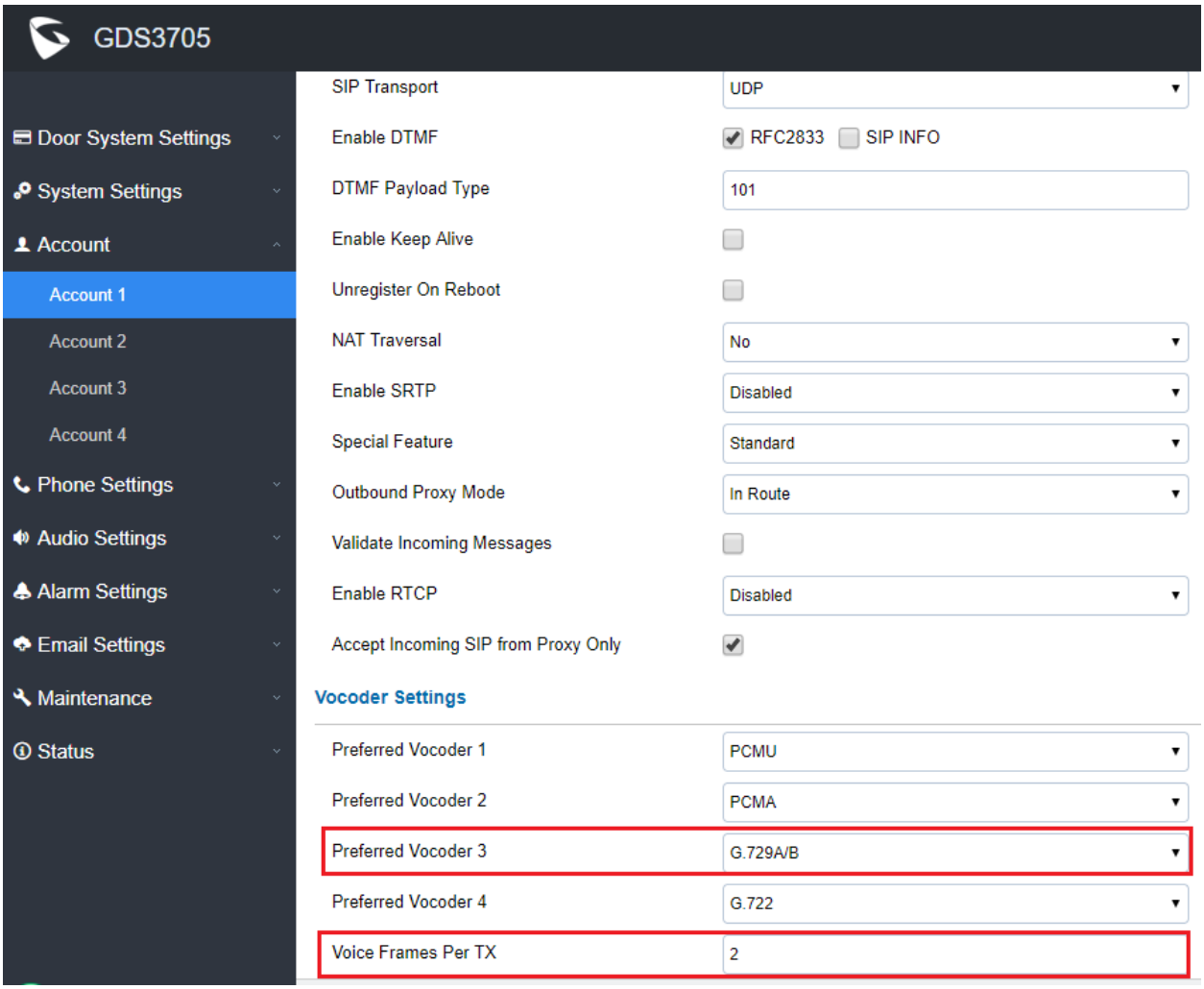
- **Functionality**

This is an enhancement for ITSP customers to support network backup service.

Multiple Audio Codecs and Voice Frame Per TX Support

- **Web Configuration**

The option can be found under device webUI: Account → Account X (X = 1, 2, 3 and 4):



- **Functionality**

This is an enhancement for an existing features after feedbacks from customers and installers, especially ITSP customers.

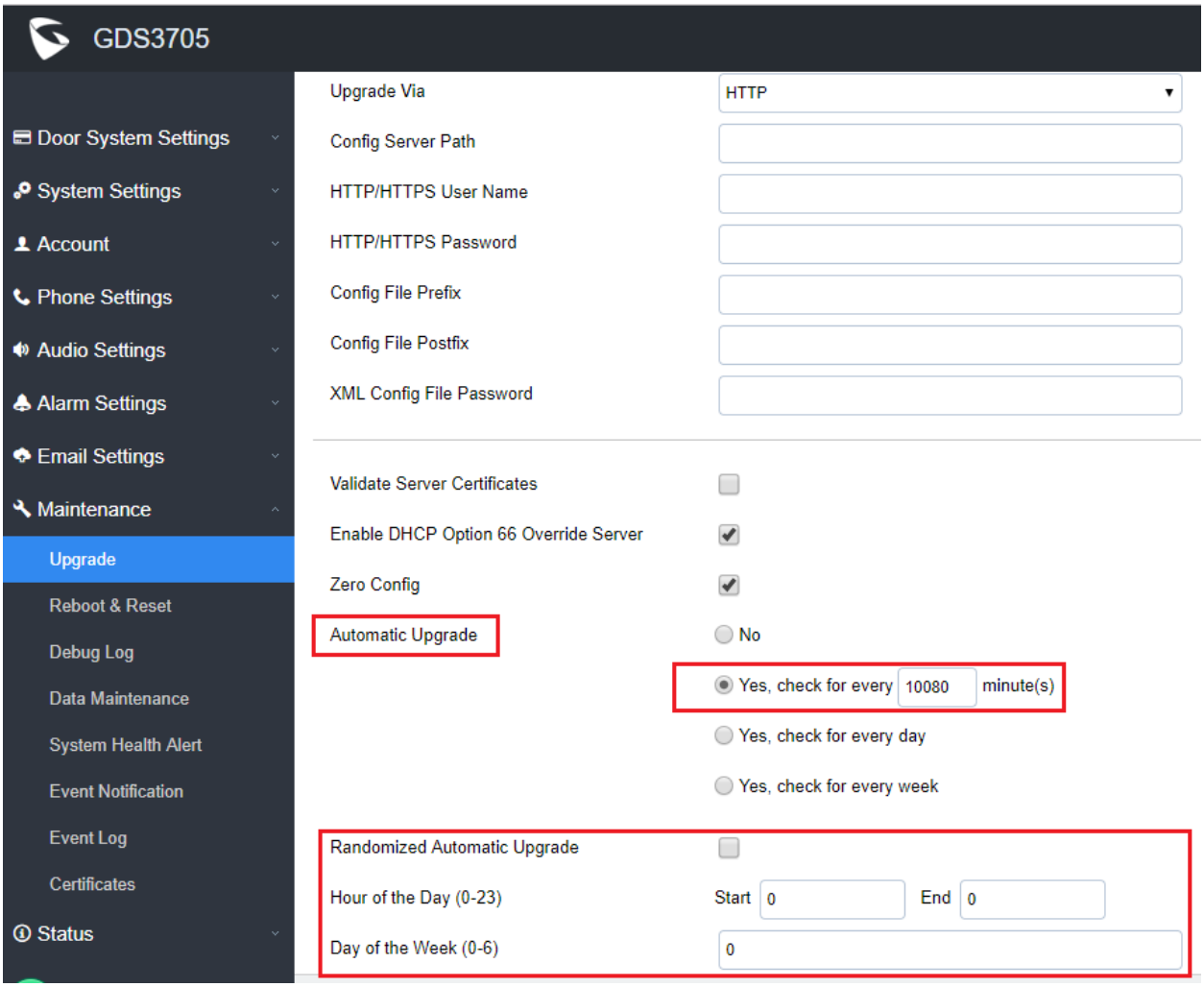
Added “Voice Frame Per TX” to allow ISTP customers configure the VoIP more efficiently.

Added G.729 audio codec support as well as multiple audio codecs simultaneously with specified priority.

Set Schedule for Upgrade/Provisioning

- **Web Configuration**

The option can be found under device webUI: Maintenance → Upgrade:



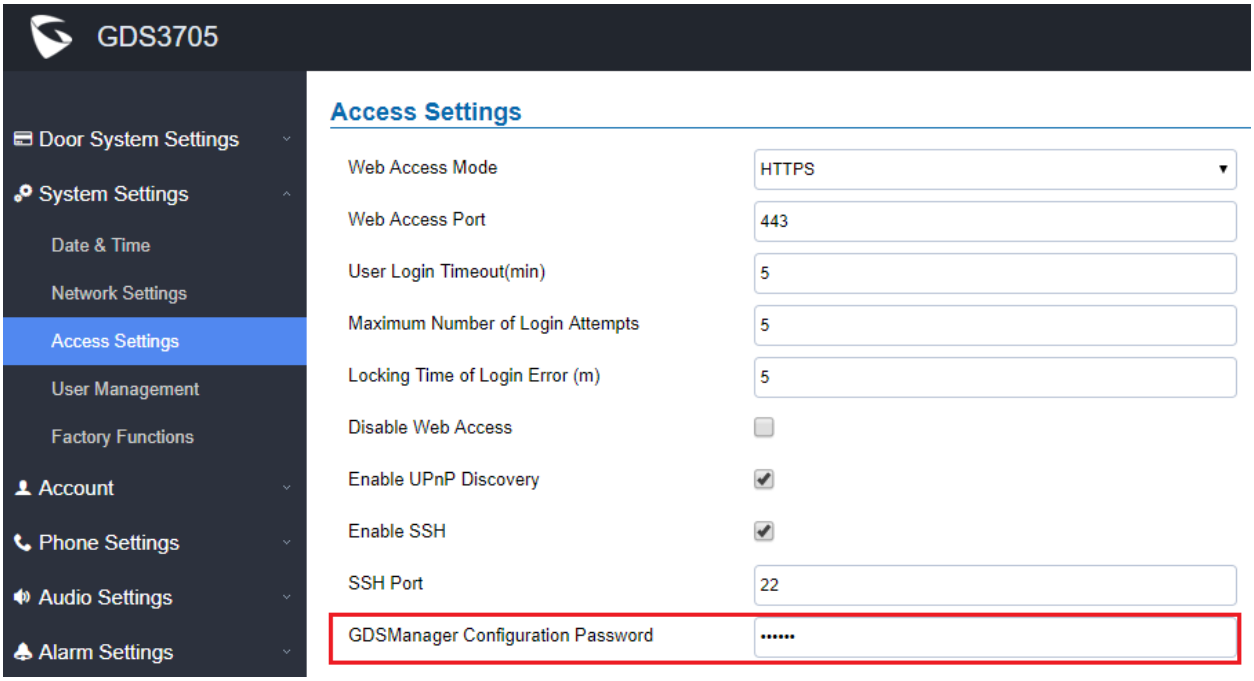
- **Functionality**

This is an enhancement for ITSP customers so scheduled or preconfigured firmware upgrade or configuration provisioning can be provided to the customers.

Separate Credentials for GDSManager

- **Web Configuration**

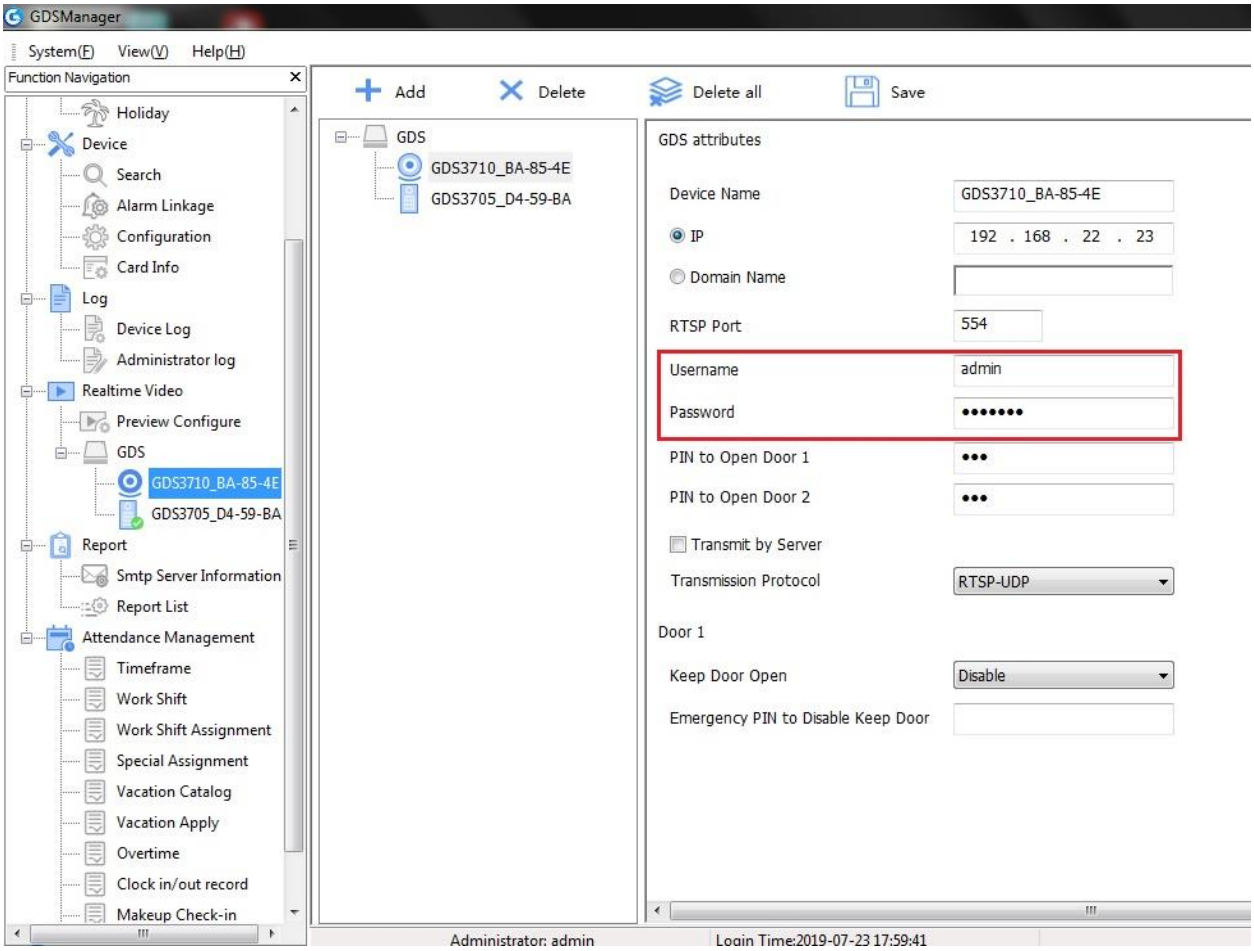
This option can be found under device web UI → System Settings → Access Settings:



- **Functionality**

This feature is implemented based on field customer feedback. Now separate credentials can be configured and used in GDSManager to communicate with GDS3705, instead of using GDS3705 webUI administrator's credentials. System administrators keep the admin password and use another password for GDSManager where usually operated by HR or other company staffs.

Make sure the correspondent password is configured in GDSManager like below:



NOTE:

- The password must match the password configured in the GDS3705 at above screenshot.
- This feature requires both GDS37xx and GDSManager to make it work.
- GDS37xx has to be configured in “Central Mode”
- GDSManager Version 1.0.1.1 or above is required to support this feature.

FIRMWARE VERSION 1.0.0.41

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

06/06/2019

SUMMARY OF UPDATE

This is a major feature update for GDS3705 as well as bug fixes. Two doors can be controlled starting from this version.

Factory Reset is recommended if upgrading from very old firmware, or experiencing abnormal webUI or missing parameters in the GUI. Please backup the configuration and data before factory reset, then import back after reset.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed only the 1st doorbell number can answer the call normally in Door Bell Call Mode.
- Fixed cannot answer the call after uploading an empty custom doorbell ringtone.
- Fixed GDSManager cannot open door2 via the remote PIN.
- Fixed Digit Input will not open Door1 when disable ALMOUT1 open door feature.
- Fixed alarm not activated even wrong private PIN inputted many times.
- Fixed no error prompt when saving “Door2 Unlock Holding Times(s)” to “0”.
- Fixed API cannot open Door2 remotely.
- Fixed cannot end the call by pressing doorbell button if the doorbell schedule not include current time
- Fixed Silent Alarm triggered the GDS3705 side has audio not muting on phone side.
- Fixed Digit Input 1 can only control open door1 when ALMOUT1 set as Open Door.
- Fixed wrong email theme used when testing alarm action.
- Fixed email failed to send out when non-schedule access alarm triggered.

- Fixed anyone knowing the DTMF PIN can open the door remotely if caller is GDS37xx, added the security limitation that only callees in the whitelist can open door remotely.
- Fixed if Hostage Alarm triggered the GDS3705 not sending audio but still sending alarm siren when far side phone pressed keypad to stop the siren.
- Fixed "Keep Door Open" by configured Schedule fail to work when Daylight Saving Time kicked in.
- Fixed pressing doorbell calling the 2nd callee in the list will not ring if the first number user rejected the open door request call (which supposedly should not happen like receptionist should not reject call)
- Fixed and forbidden user to upload custom doorbell ringtone with empty ring.bin audio.
- Fixed issue with decoding DNS (mDNS).
- Fixed Account Active not taking effect on Account1
- Fixed Event Log the SIP account number displayed incorrectly.
- Fixed no error prompt when saving SIP and RTP port with same number.
- Fixed clicking webUI to make doorbell call only the 1st number will be called.
- Fixed new uploaded certificate will not overwrite the previous certificate file.

ENHANCEMENT

- Synchronized Digit Input Status with GDS3710.
- Enhanced syslog messages and removed unnecessary details from the logs.
- Added sending System Health Alerts via email.
- Removed "SIP Proxy Compatibility Mode" as GDS3705 not support video.
- Added feature to Enable/Disable Web Access.
- Added feature option to configure "No Key Entry Timeout"
- Added feature to use Digits Only as Private PIN.
- Added option to set "schedule" for "Local PIN to Open Door".
- Added ability to configure "Keep Door Open" action from "Device Config" of GDSManager (Version: 1.0.1.1) and synchronize with GDS37xx, or vice versa from GDS37xx to GDSManager.
- Added option to set DTMF Payload value.
- Added RTCP/TRCP-XR support.
- Added reuse ALMOUT1 for Open Door function and interface.
- Added Digit Output support Normal Open or Normal Close setting.
- Added "Boot Version" displayed in "System Info" of "Status" UI page.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side not stopping after pressing phone's keypad.

NEW HTTP API

P2392/P2492/P2592/P2692/ P79/P496/P596/P696	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P15473	GET:[http|https]://<servername>/goform/config?cmd=get&type= access SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P15436/P15433/P15450/ P15460/P15461/P15462/ P15465/P15466/P15467/ P15468/P15470/P15498	GET:[http|https]://<servername>/goform/config?cmd=get&type= door SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P15451/P15452	GET:[http|https]://<servername>/goform/config?cmd=get&type= event SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P15455/P15456/P15457/ P15458/P15459/P15472	GET:[http|https]://<servername>/goform/config?cmd=get&type= sch_open_door SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P15490/P15491/P15492/ P15493/P15494/P15495/ P15496	GET:[http|https]://<servername>/goform/config?cmd=get&type= sys_health_alert SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>
P15499	GET:[http|https]://<servername>/goform/config?cmd=get&type= audio SET:[http|https]://<servername>/goform/config?cmd=set&Pname=<value>

NEW P-VALUE

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	**<parameter> =<value>**	**<parameter> =<value>**	**<parameter> =<value>**	**Model Supported**	**Values**	**Description**
P79=<int>	P496=<int>	P596=<int>	P696=<int>	GDS3710/GDS3705	<integer>	DTMF Payload Type
P2392	P2492	P2592	P2692	GDS3710/GDS3705	<0|1|2>	Enable RTCP 0: 1: RTCP 2: RTCP-XR

P15473 - System Settings/Access Settings/Disable Web Access
P15436 - Door System Settings/Basic Settings/No Key Input Timeout(s)
P15433 - Door System Settings/Basic Settings/Disable Keypad SIP Number Dialing
P15450 - Door System Settings/Basic Settings/ALMOUT1 Feature
P15451 - Alarm Settings/Alarm Events Config/Digit Input/Digit Input 1 Open Door Option
P15452 - Alarm Settings/Alarm Events Config/Digit Input/Digit Input 2 Open Door Option
P15455 - Door System Settings/Keep Door Open/Keep Door2 Open
P15456 - Door System Settings/Keep Door Open/Length (m) to Keep Door2 Open
P15457 - Door System Settings/Keep Door Open/Door2 Schedule Start Time
P15458 - Door System Settings/Keep Door Open/Door2 Schedule End Time
P15459 - Door System Settings/Keep Door Open/Door2 Schedule
P15472 - Door System Settings/Keep Door Open/Emergency PIN to Disable Keep Door2 Open
P15460 - Door System Settings/Basic Settings/Remote PIN to Open Door 2
P15461 - Door System Settings/Basic Settings/Unified PIN Open Door Options
P15462 - Door System Settings/Basic Settings/Guest PIN Open Door Options
P15465 - Door System Settings/Basic Settings/Door 2 Delay before Unlock(s)
P15466 - Door System Settings/Basic Settings/Door 2 Unlock Holding Time(s)
P15467 - Door System Settings/Basic Settings/ Control Options
P15468 - Door System Settings/Basic Settings/Wiegand Control
P15470 - Door System Settings/Basic Settings/DO1 Lock Status
P15498 - Door System Settings/Basic Settings/Local PIN to Open Door Schedule
P15490 - Maintenance/System Health Alert/Enable System Health Alert
P15491 - Maintenance/System Health Alert/Delivery Method
P15492 - Maintenance/System Health Alert/Interval Time
P15493 - Maintenance/System Health Alert/SIP Registration Status
P15494 - Maintenance/System Health Alert/ System Running Status
P15495 - Maintenance/System Health Alert/System Temperature
P15496 - Maintenance/System Health Alert/Email Title
P15499 - Audio Settings/Enable Custom Doorbell Ringtone

MODIFIED P-VALUE

P14835 - bell ring volume, default 5 -> 4

NEW FEATURES OVERVIEW

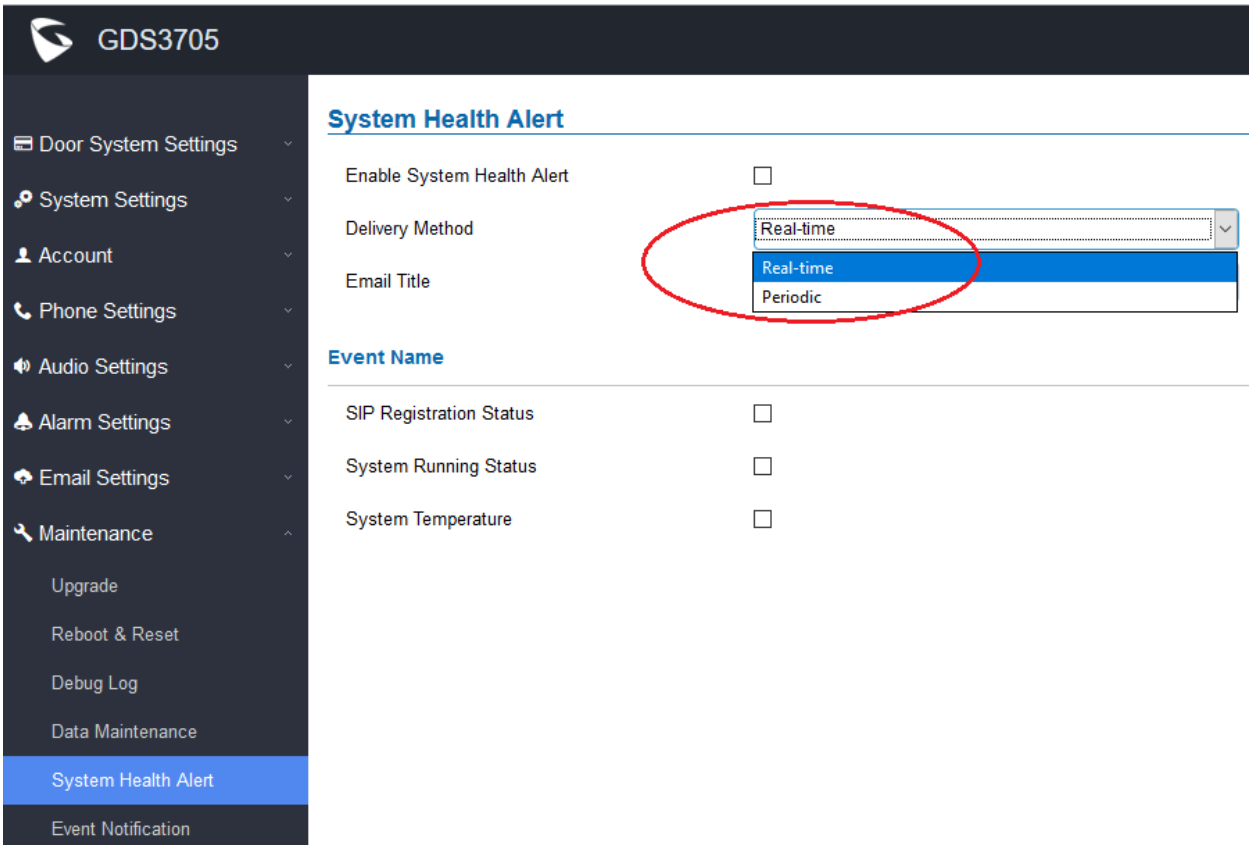
This section lists major new features and describes how to use them from the user's point of view.

SYSTEM HEALTH ALERT

- **Web Configuration**

New feature allows users to configure the device to send email report about system health information, like: Registration Status, Running Status, and Temperature. Email title can be written by users and also the sending frequency can be selected as either real-time or in period.

This option can be found under device web UI: Maintenance → System Health Alert:



- **Functionality**

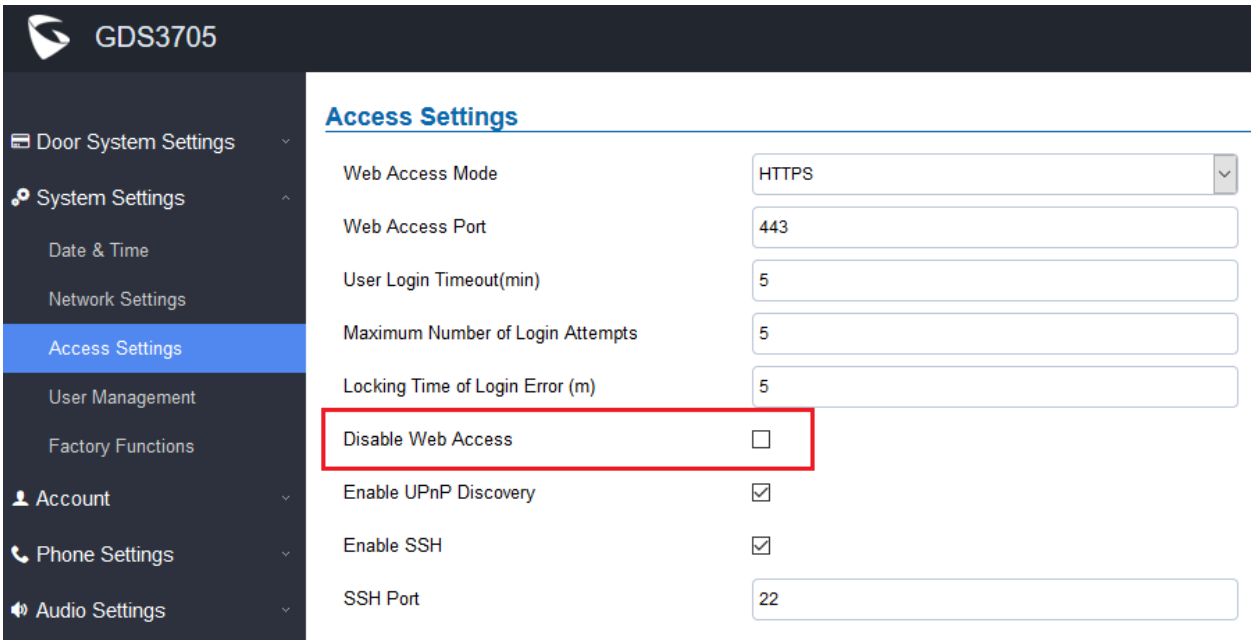
This feature is added to meet the requirement of ITSP customers. Service provider (ITSP) customers can configure the device to send out system health report to monitor the system health of the device to improve the service.

ENABLE/DISABLE WEB ACCESS

- **Web Configuration**

This feature is added to allow service provider to disable web access to enhance the security of the device.

The option of this webUI can be found: System Settings → Access Settings:



- **Functionality**

This feature is added to allow service provider customer to disable webUI for end users and improve the security of the device. By default is enabled.

NOTE:

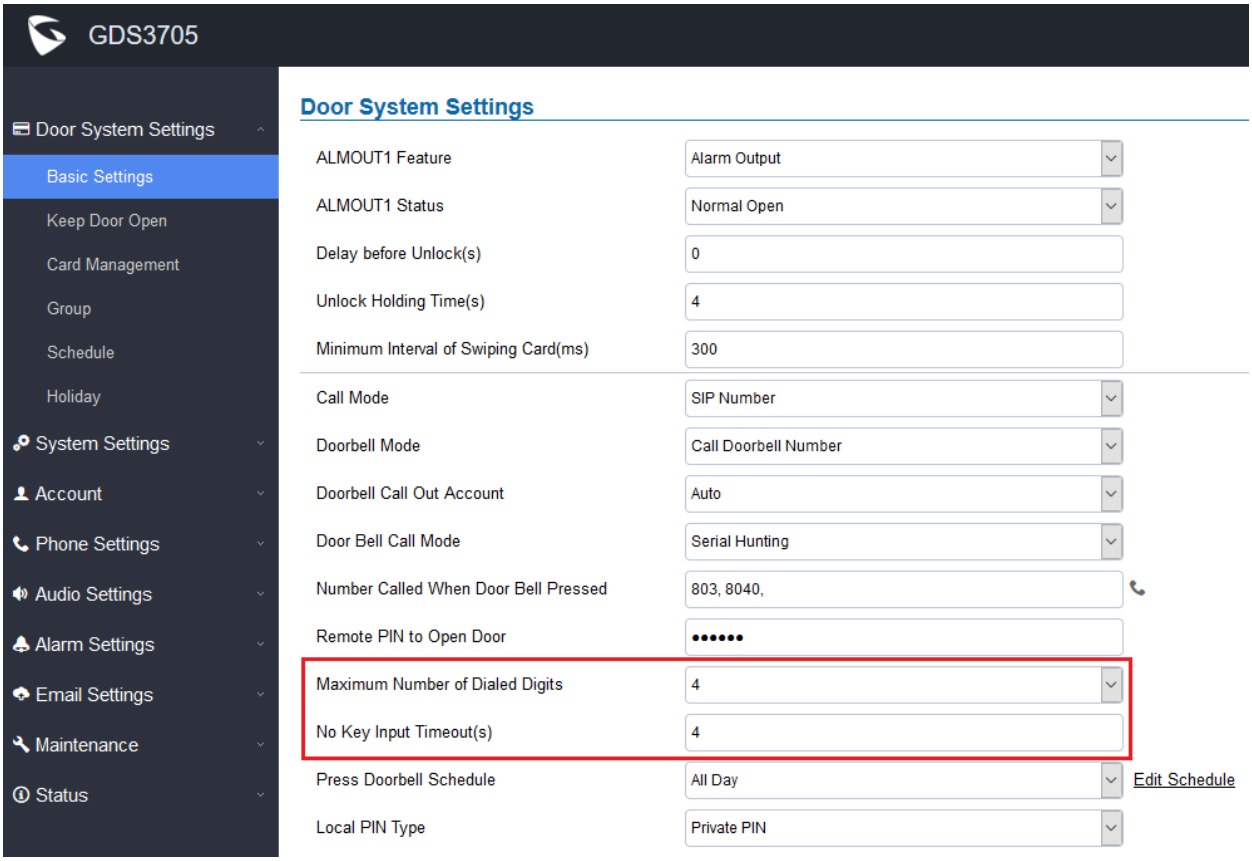
- This feature is designed for Service Provider, or Service Technician or Installers.
- End users without necessary knowledge are strongly discouraged to use it, avoiding lost access to the UI of the device.
- Once the webUI access is disabled, the UI can only be enabled again by either Provisioning, SSH (if enabled) or Factory Reset. This feature is NOT suggested to use by end users.
- If both Web Access and SSH are disabled, users will LOST access to the device. Only way to recover is re-provisioning the device, or HARD factory reset. Be very careful about disable BOTH, unless the device can be provisioned by configuration server.

NO KEY INPUT TIMEOUT

- **Web Configuration**

This feature is added to allow GDS3705 calling out automatically without pressing # key if stop input digits after the configured timer. This is more like IP Phone feature.

The option of this webUI can be found: Door System Settings → Basic Settings:



- **Functionality**

This is an enhancement for an existing features after feedbacks from customers.

This setting allows user to configure the timeout (in second) when no key input then sending out the SIP call automatically without press the “#” key. User can customize this parameter based on the environment this door phone installed.

For example in above screenshot:

"Maximum Number of Dialed Digits" is set to be "4":
This is good for an installation allowing the door phone call ONLY the internal extensions to open door.
The setting is 4, means once user input 4 digit to the GDS3705, it will immediately dial out (saying the internal extension is using 4 digits)

"No Key Input Timeout(s)" is set to be "4" (second).
This means if user input the digits (less than 4 digit in above example), then wait and not more key strike, after 4 seconds (this can be customized by user or installer in the installation scene), the SIP call will automatically dial out without the "#" pressed.

Same as above screenshot example, if user input less than 4 digits, say input only 1 digit ("0" for example), then followed by the "#" key, then the GDS3705 door phone will immediately dial out "0" to establish the call. (***"0"*** can be Operator or IVR depending on the IPPBX system configured)

This timer is in seconds, if no new digit input by user, the call will automatically be sending out and no "#" required to end the input.

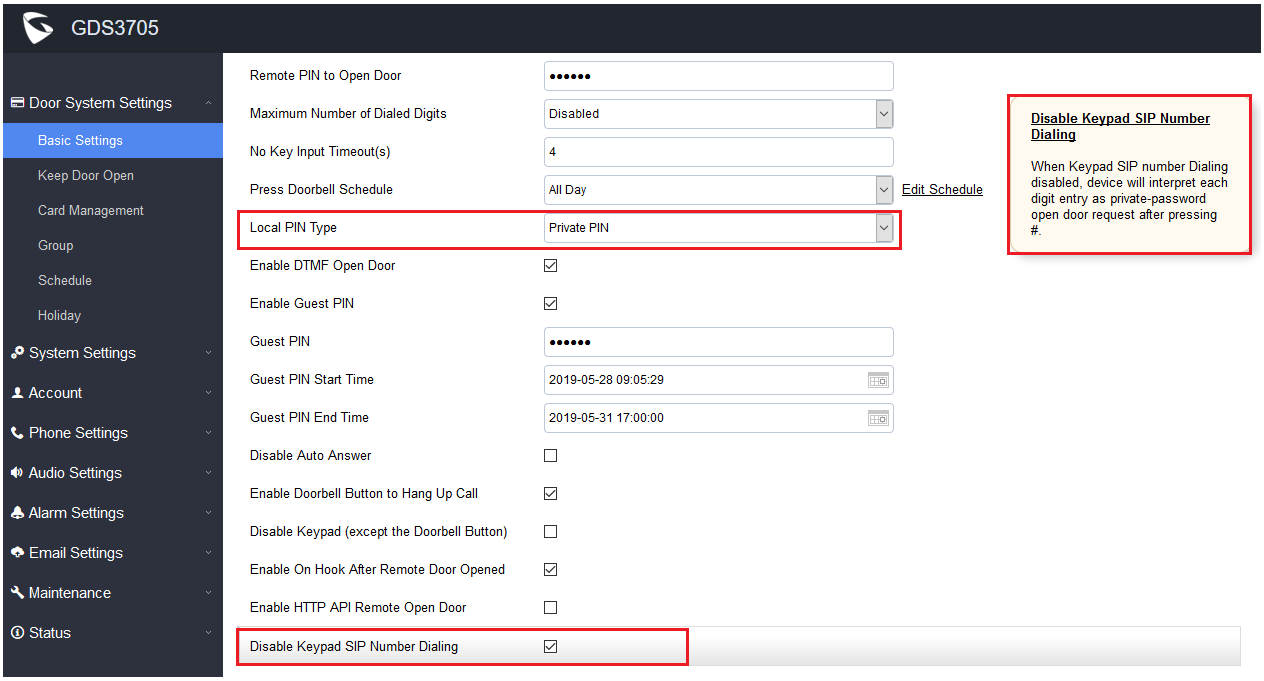
This is more a phone feature allowing users to simulate the traditional analogue phone dialing method.

Appropriate timer has to be configured to meet users' calling habit.

OPEN DOOR VIA DIGITS ONLY PRIVATE PIN

- **Web Configuration**

The option can be found under device webUI: Door System Settings → Basic Settings:



- **Functionality**

This is an enhancement for an existing features after feedbacks from customers and installers.

This setting allows user to use DIGIT ONLY private PIN to open door, with the cost of NOT be able to make any SIP calls (except for doorbell button call).

User just input **"PrivatePIN#"** to open door, more like traditional door access system. The PIN format is shorter and different with SIP call enabled mode (which PIN format is *"*VirtualNumber*PrivatePIN#")*. This makes the GDS3705 more like traditional access device.

NOTE:

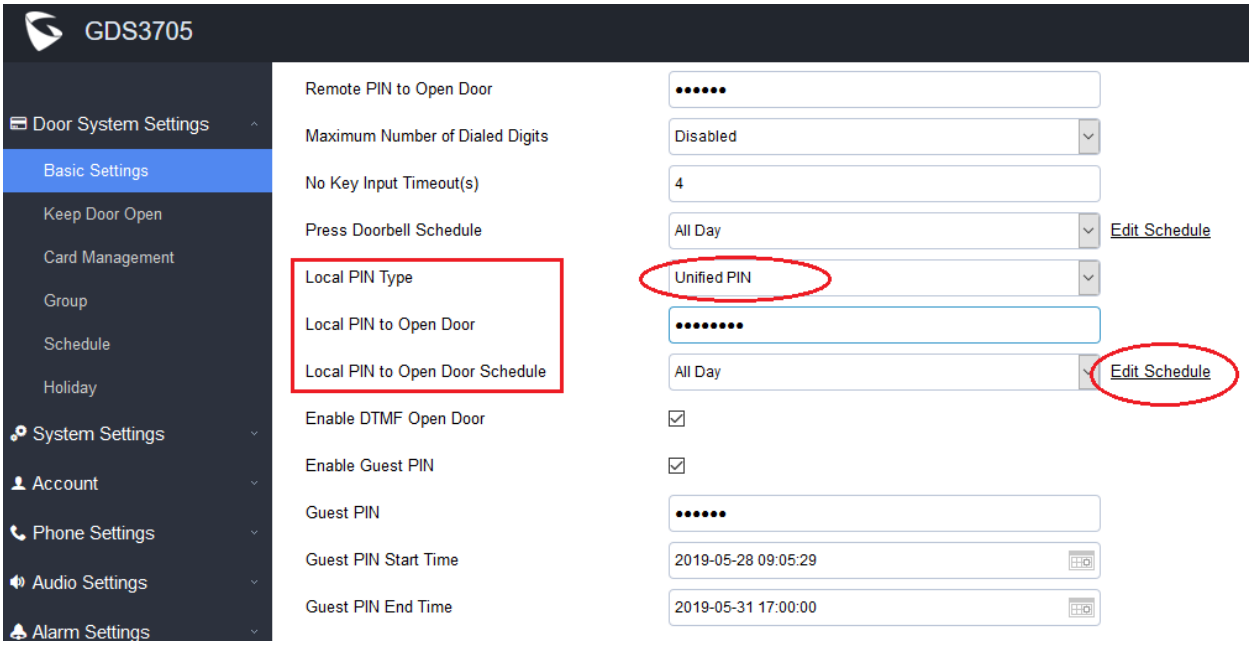
Following settings are required to make this feature working:

- "Disable Keypad SIP Number Calling" should be checked to enable this feature
- "Local PIN Type" should choose "Private PIN"
- Dial keypad to make SIP call will NOT work when above selected.
- PrivatePIN must be **UNIQUE** among users, otherwise the door will still open but log will NOT tell who opened the door due to duplicated PIN and whoever user last matched in the database with the PrivatePIN will be shown in the log.

SET SCHEDULE FOR LOCAL PIN OPEN DOOR

- **Web Configuration**

The option can be found under device webUI: Door System Settings → Access Settings:



- **Functionality**

This is an enhancement for “Unified PIN” access feature after feedbacks from customers. Currently, using Private PIN or RFID card, user can configure schedule in the “Card Management” database to control the time door can be accessed. But there is no schedule in the “Unified PIN”.

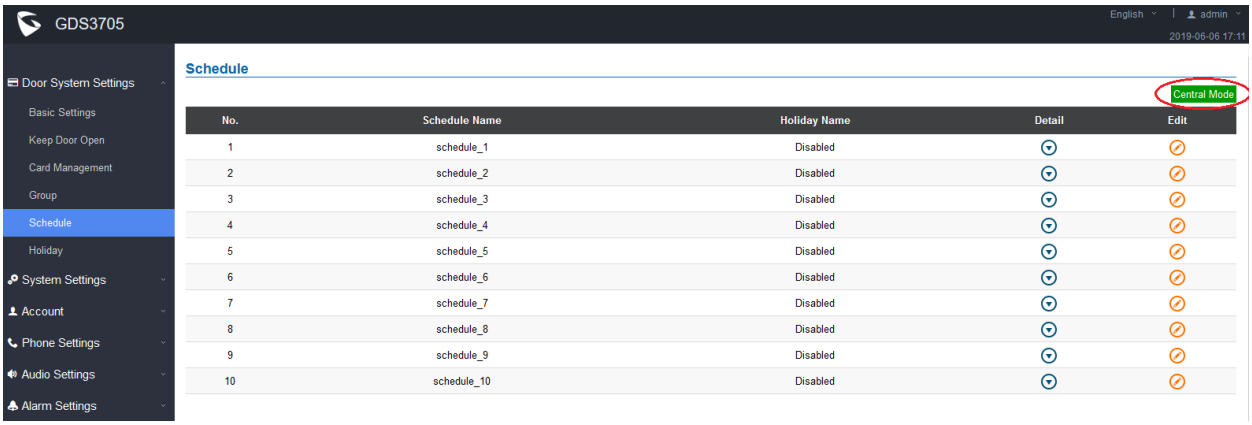
With this enhancement, users can now configure the “Schedule” to the “Unified PIN” so that the universal PIN also can be controlled by the Schedule, therefore door access can be controlled accordingly in the preconfigured time schedule.

The settings will appear only when “Unified PIN” selected in the “Local PIN Type”. User can click the “Edit Schedule” to get into schedule programming UI:

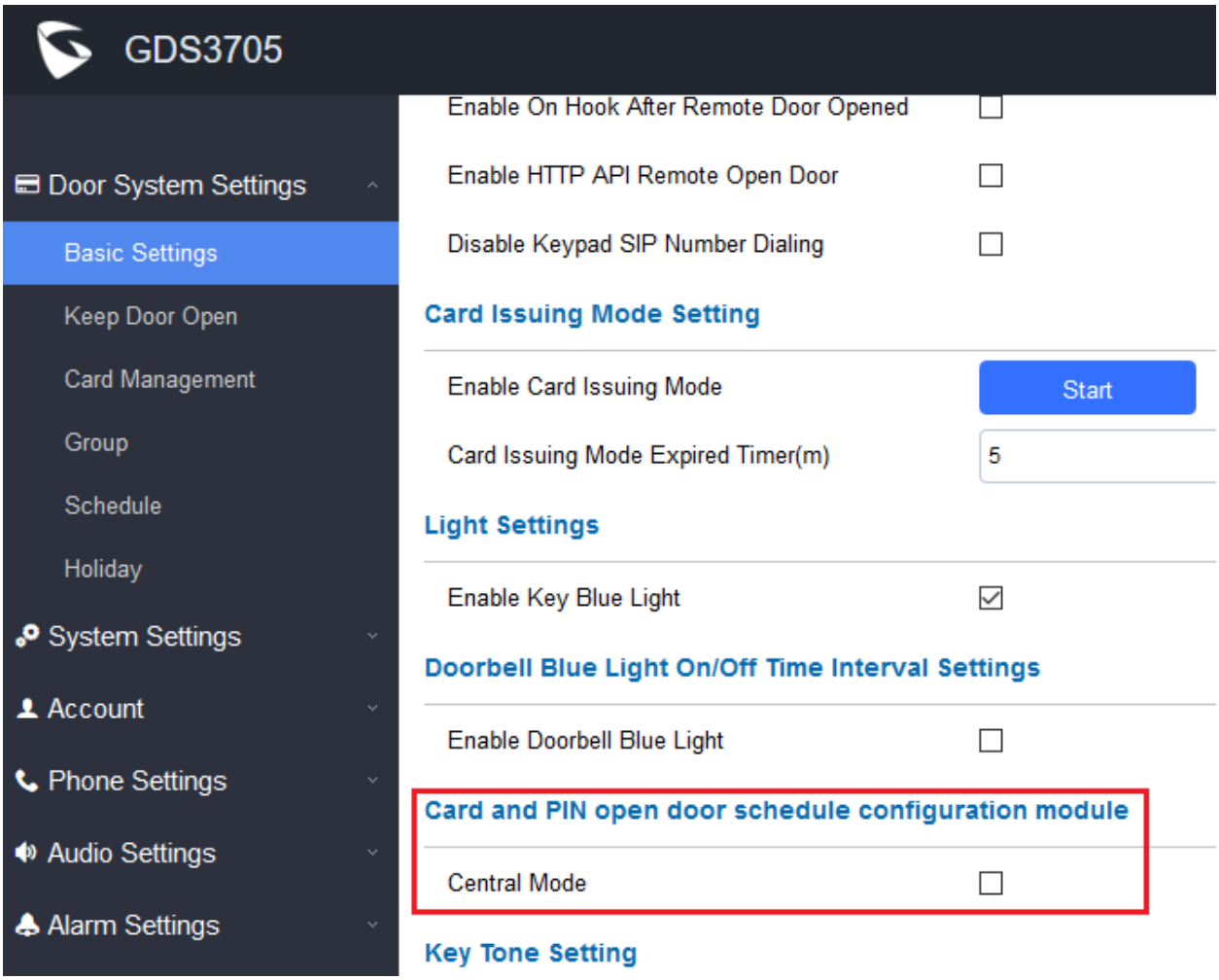
NOTE:

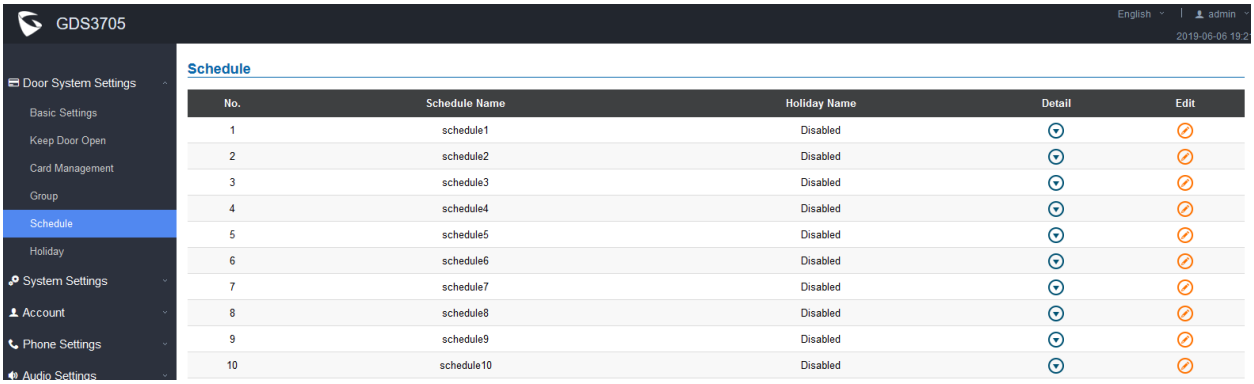
- The schedule can ONLY be edited when “Central Mode” disabled.
- If “Central Mode” enabled, the “Schedule” page is only viable and NOT editable. A green “Central Model” label will display in top right corner of the UI. (See below).
- When “Central Mode” enabled, the “Schedule” will be edited in GDSManager and synchronized by pulling from GDSManager down to GDS37xx device.

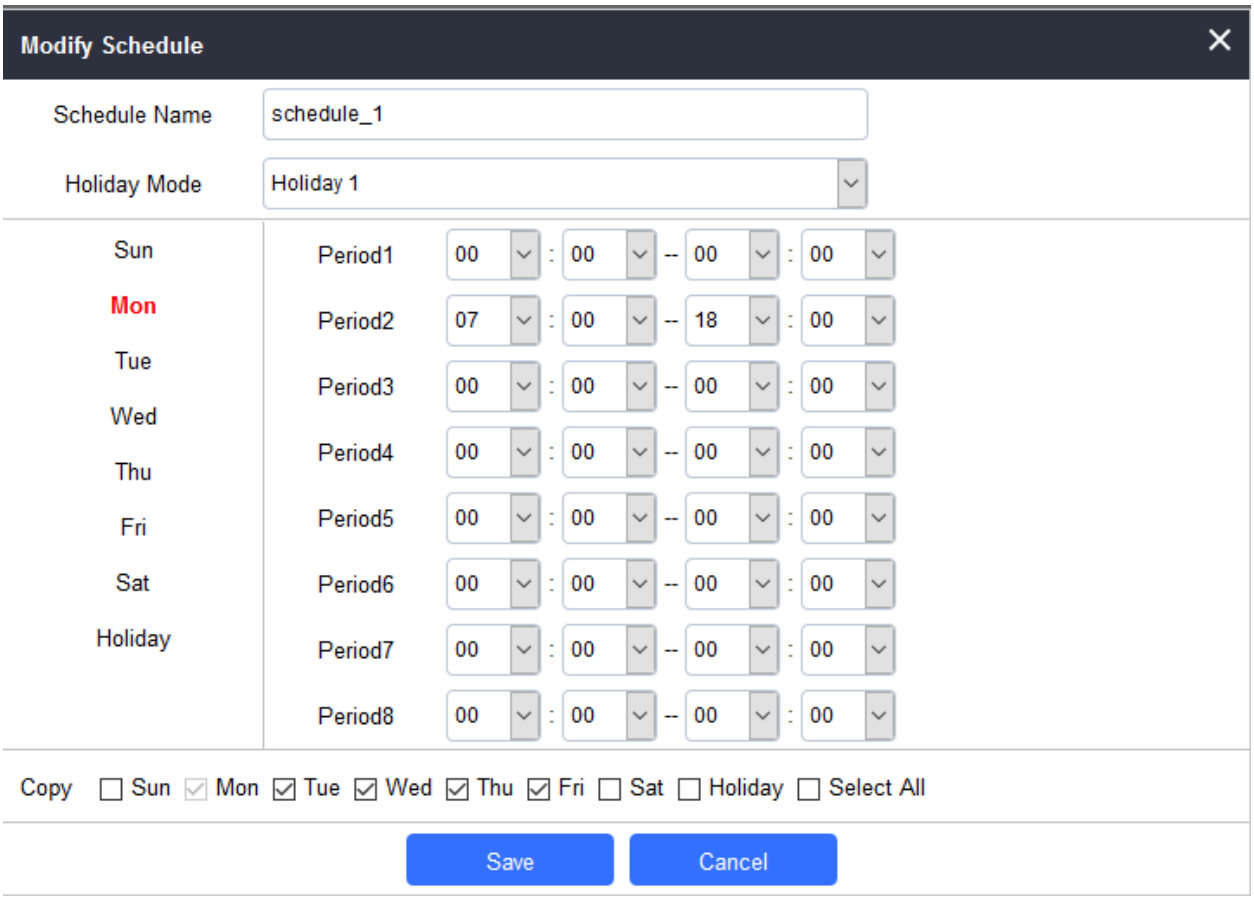
The “Schedule” UI page is only viewable and not editable with green label “Central Mode” displayed at top right corner:



When “Central Mode” NOT enabled, click the “Edit” on the “Schedule” UI will come out below screen to allow user to edit the schedule:




GDS3705
English
admin
2019-06-06 19:2
Door System Settings
Basic Settings
Keep Door Open
Card Management
Group
Schedule
Holiday
System Settings
Account
Phone Settings
Audio Settings
Schedule
No. Schedule Name Holiday Name Detail Edit
1 schedule1 Disabled
2 schedule2 Disabled
3 schedule3 Disabled
4 schedule4 Disabled
5 schedule5 Disabled
6 schedule6 Disabled
7 schedule7 Disabled
8 schedule8 Disabled
9 schedule9 Disabled
10 schedule10 Disabled

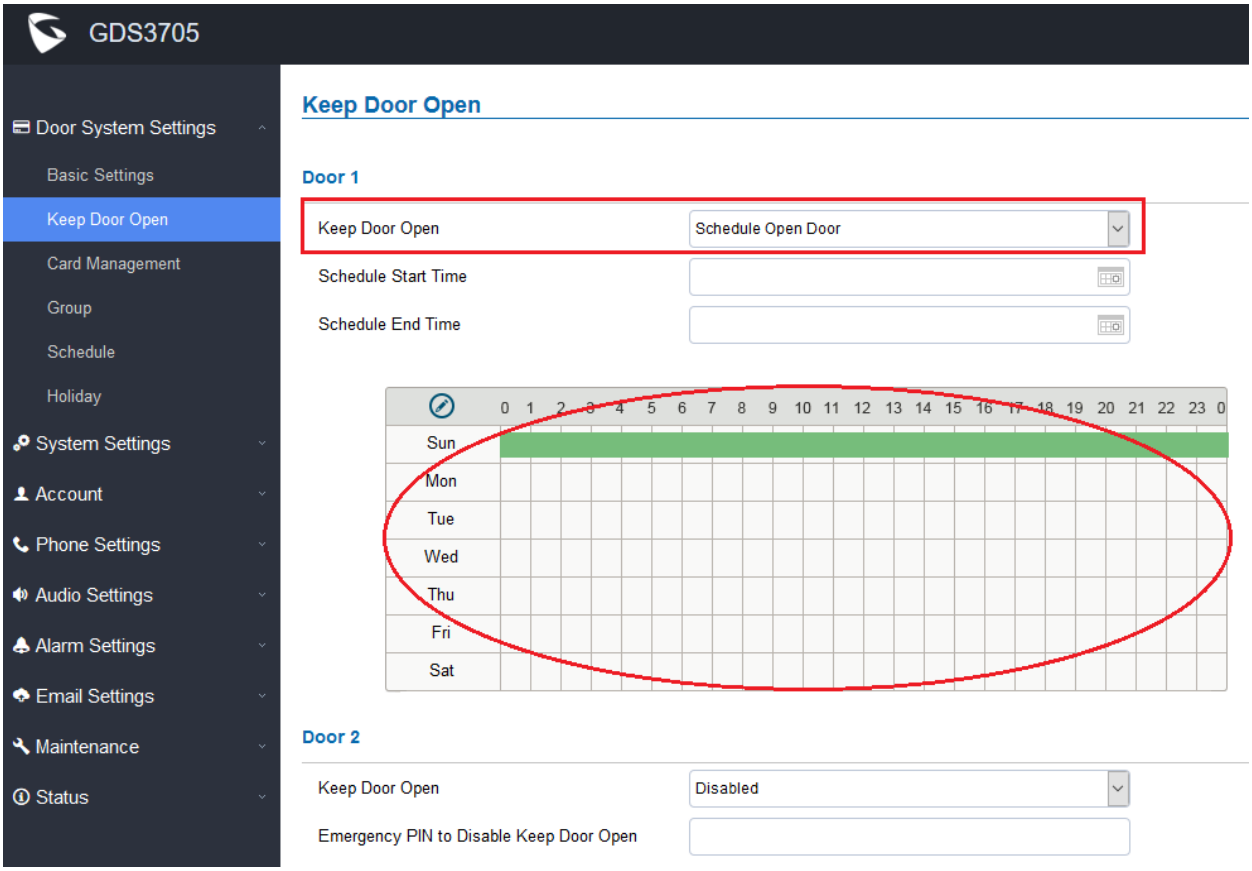

Modify Schedule
Schedule Name
schedule_1
Holiday Mode
Holiday 1
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Holiday
Period1 00 : 00 -- 00 : 00
Period2 07 : 00 -- 18 : 00
Period3 00 : 00 -- 00 : 00
Period4 00 : 00 -- 00 : 00
Period5 00 : 00 -- 00 : 00
Period6 00 : 00 -- 00 : 00
Period7 00 : 00 -- 00 : 00
Period8 00 : 00 -- 00 : 00
Copy Sun Mon Tue Wed Thu Fri Sat Holiday Select All
Save
Cancel

SYNCHRONIZE "KEEP DOOR OPEN" WITH GDSMANAGER

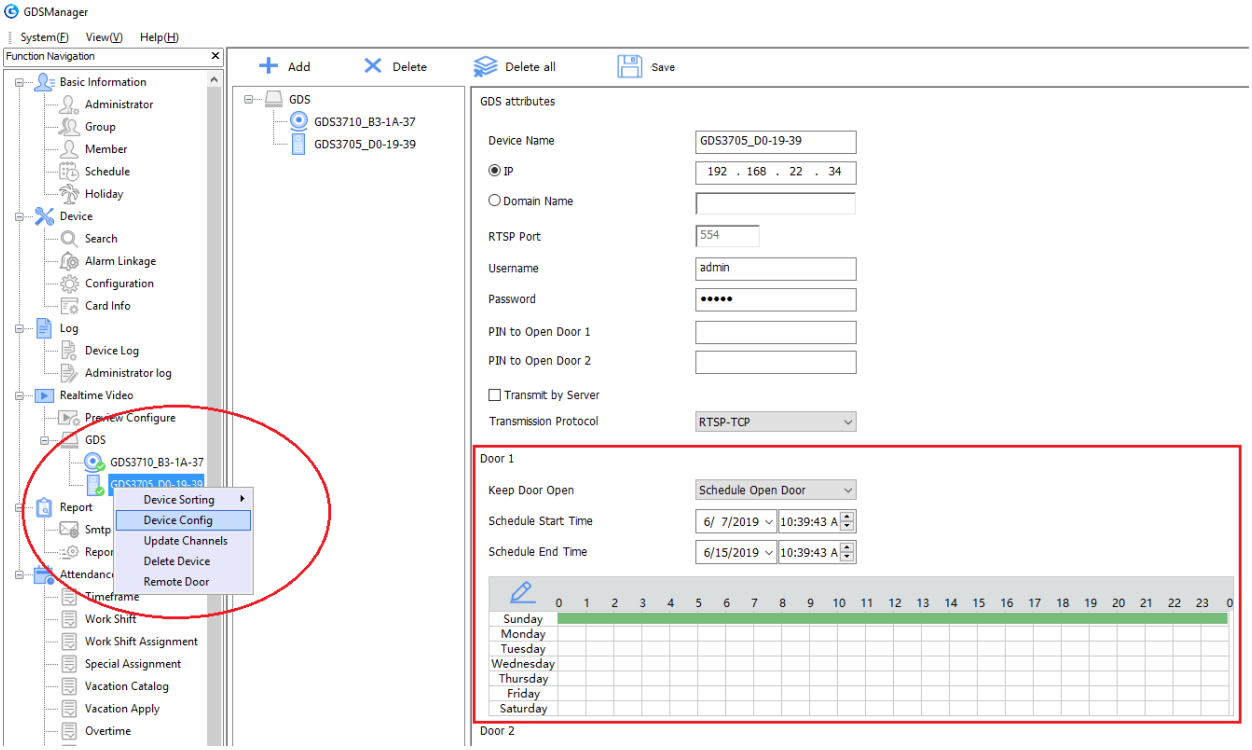
- **Web Configuration**

This feature is added to allow service provider to synchronize the schedule open door from GDSManager running at central office. GDSManager (Ver: 1.0.1.1 or later) required to work with this feature.

The webUI of GDS3701 can be found at: Door System Settings → Keep Door Open:



The webUI of GDSManager can be found at: Realtime Video → GDS: select related GDS37xx device and right click the selected GDS → Device Config:



- **Functionality**

This feature is added to allow service provider or system administrator or installer to synchronize the schedule open door from GDSManager running at Window based computer from central office. GDSManager (Ver: 1.0.1.1 or later) required to work with this feature.

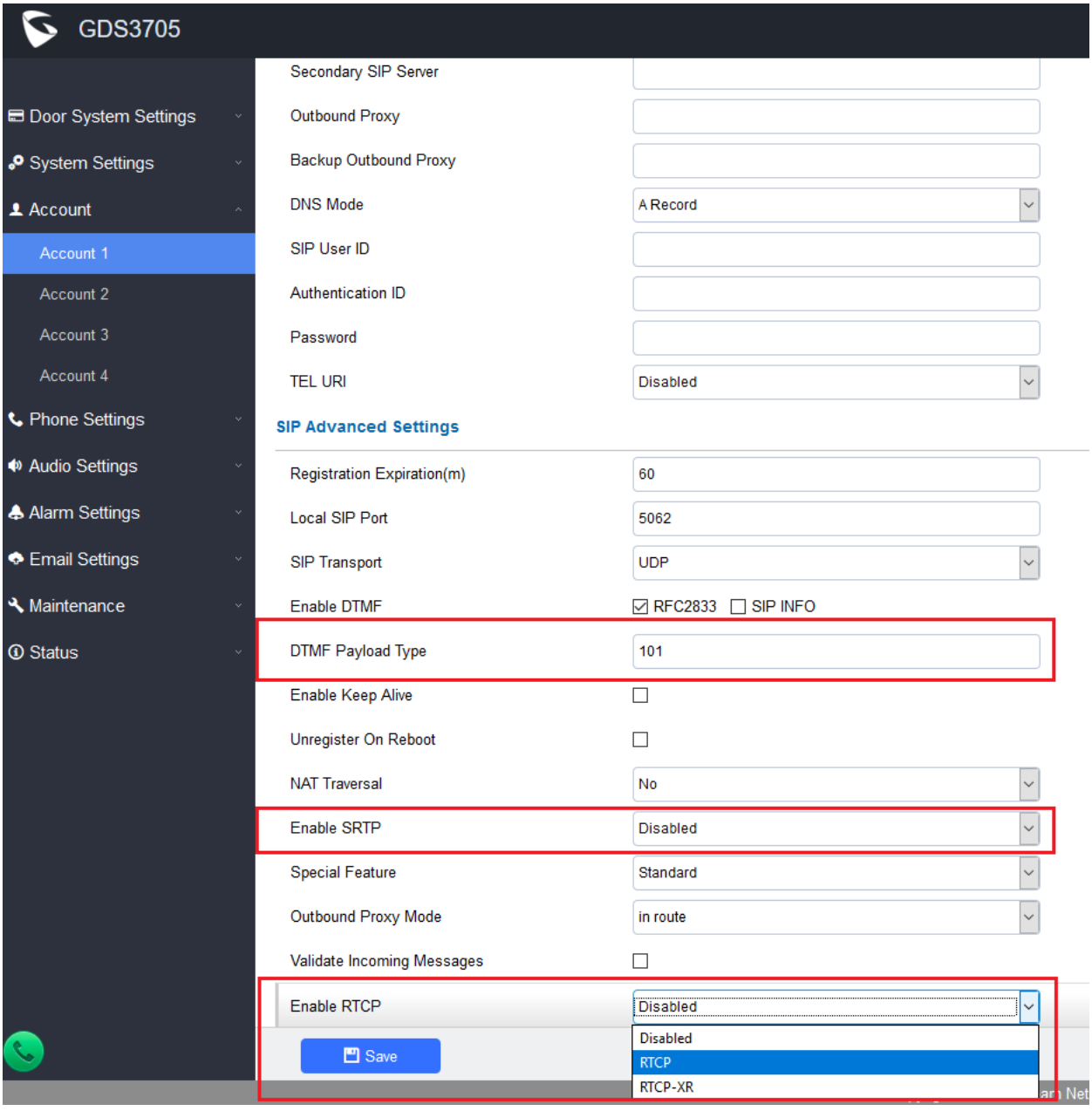
NOTE:

- This feature requires both GDS37xx and GDSManager to make it work.
- GDS37xx has to be configured in “Central Mode”
- GDSManager Version 1.0.1.1 or above is required to support this feature.

- **Web Configuration**

This option can be found under device web UI:

Account → Account X (X = 1 ~ 4) → SIP Advanced Settings:



- **Functionality**

These parameters are designed for more compatibility with 3rd parties SIP Proxy or IPPBX and good for ITSP service providers as well as System Integrators. The parameters can be adjusted by just fill in the corrected value or choose in pull-down menu selections.

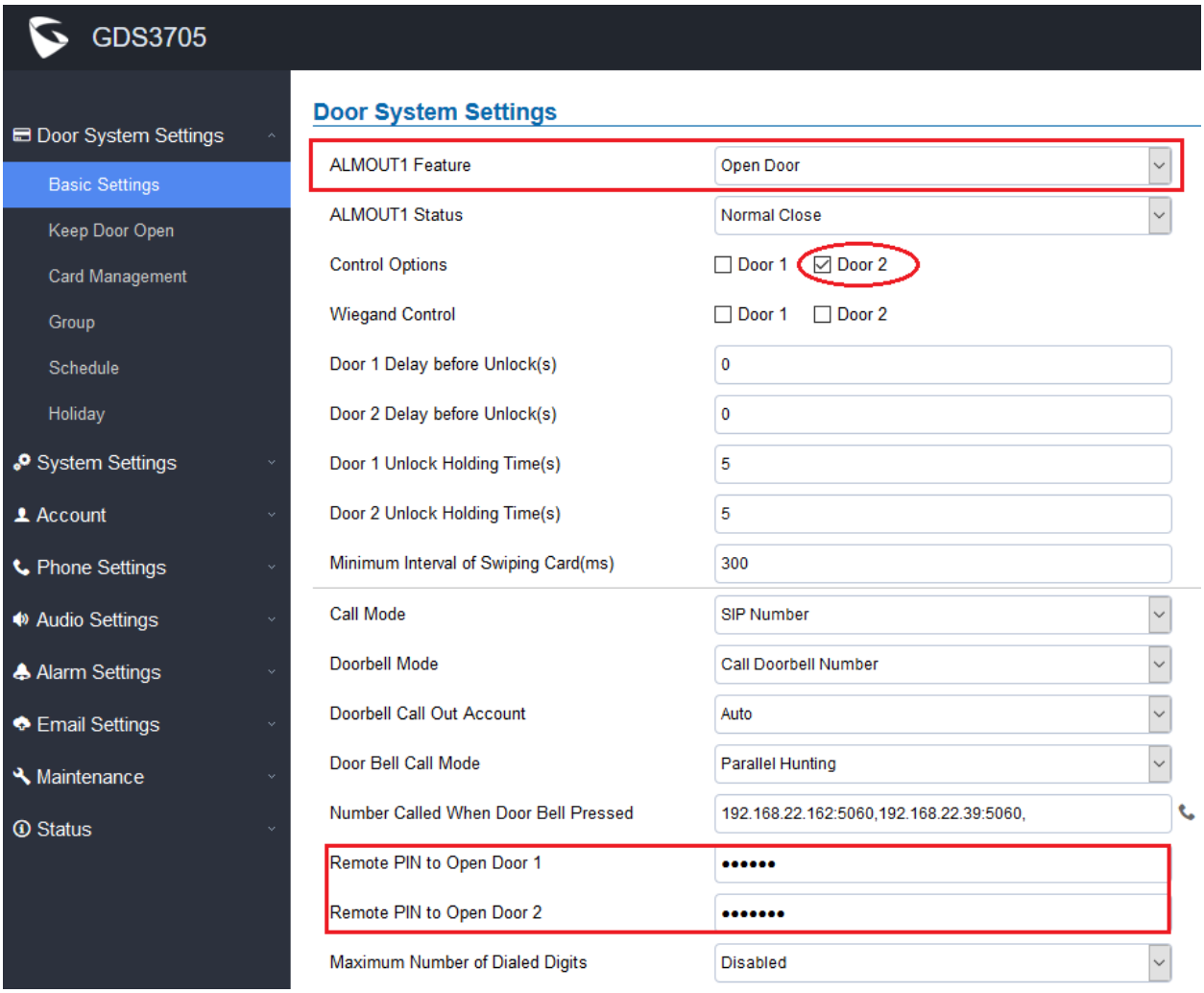
NOTE:

- Make sure correct value are filled in. Otherwise DTMF open door will fail, there will be no audio and sometimes the call will just fail to establish.
- If do not know the meaning or unsure the value adjusted, please use the default value.
- This feature is designed for Service Provider, or Service Technician or Installers.
- End users without necessary knowledge are strongly discouraged to change the parameters, avoiding the device not establish calls or not working properly.

ALMOUT1 CONTROL DOOR2

- **Web Configuration**

This feature is added to reuse ALMOUT1 port for DOOR2 Control. The option of this webUI can be found: Door System Settings → Basic Settings:



- **Functionality**

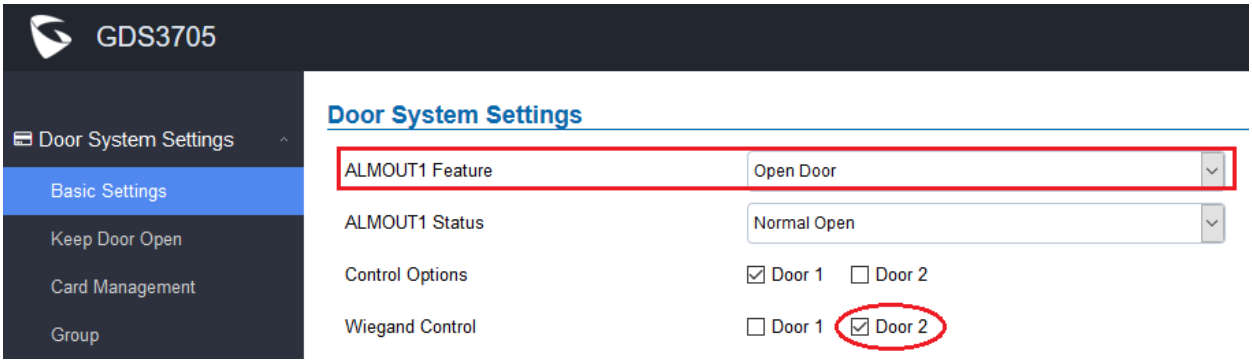
This is a major feature enhancement, by re-use ALMOUT1 (COM1) interface to be either as per original design as normal alarm out with 3rd party device, or control DOOR2 operation (the two functions are mutual-exclusive).

Customers can now use this ALMOUT1 (COM1) interface to control DOOR2, in additional to the existing Locker/COM2 interface (controlling DOOR1). This feature when selected, will enable GDS3705 to control the operation of TWO DOORS via RFID, local and remote PINs.

For example, a 3rd party Wiegand Input device can be installed at DOOR2 with related cable wired into the GDS3705 installed at DOOR1. Now the DOOR1 and DOOR2 can be configured to be opened by programmed RFID cards, related PINs either separately or both.

NOTE:

- **Interface for Door Control (Which Door can be OPEN):**

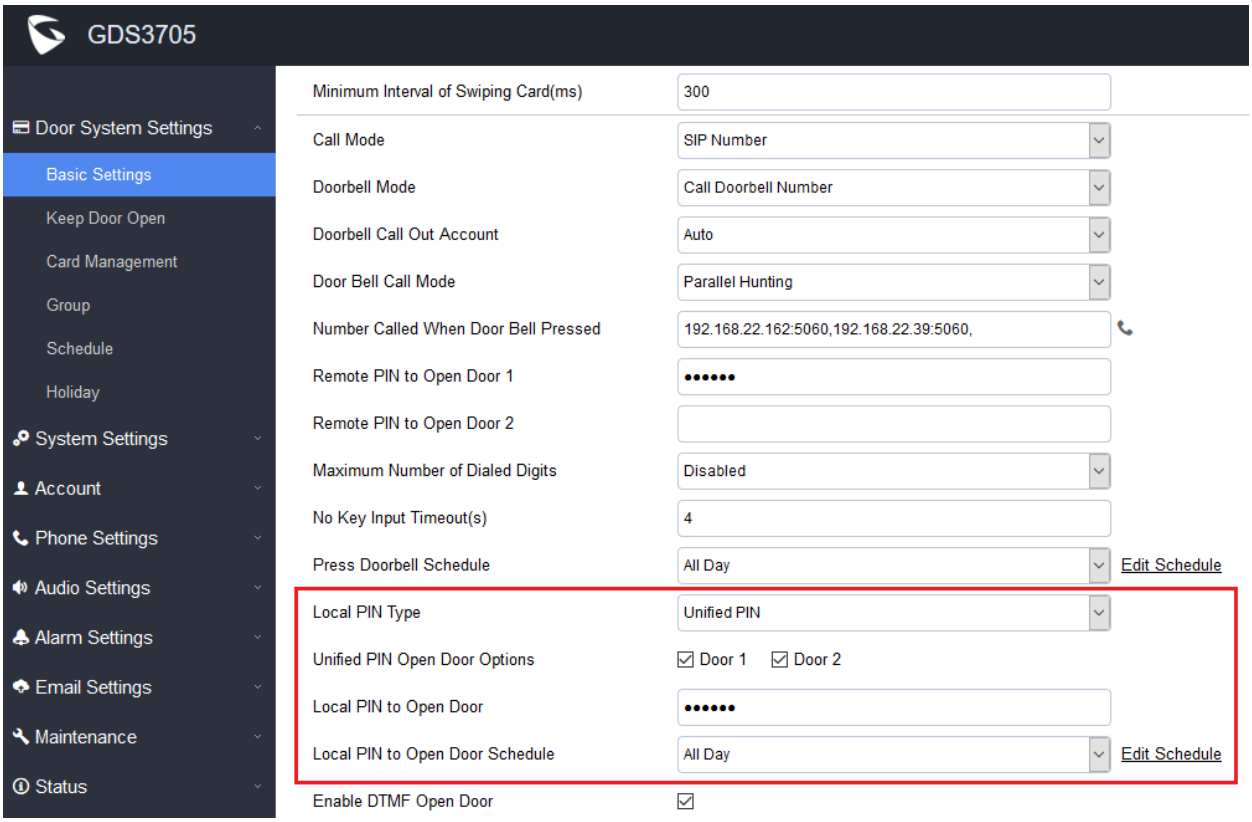


If ALMOUT1 (COM1) interface is set to control DOOR2 opening, “Lock Status” can be configured by choose “Normal Open” or “Normal Close” based on the strike used.

Unlike default COM2 which is designed for strike control and having three connecting sockets, the ALMOUT1 (COM1) only has two connecting sockets. Therefore correct lock mode has to be configured to make the strike working as expected.

For above example, the GDS3705 is configured to control DOOR1 (wiring to COM2 interface); the 3rd party Wiegand Input is set to control DOOR2 (wiring to COM1 interface).

- **Universal PIN for Operation of Doors:**

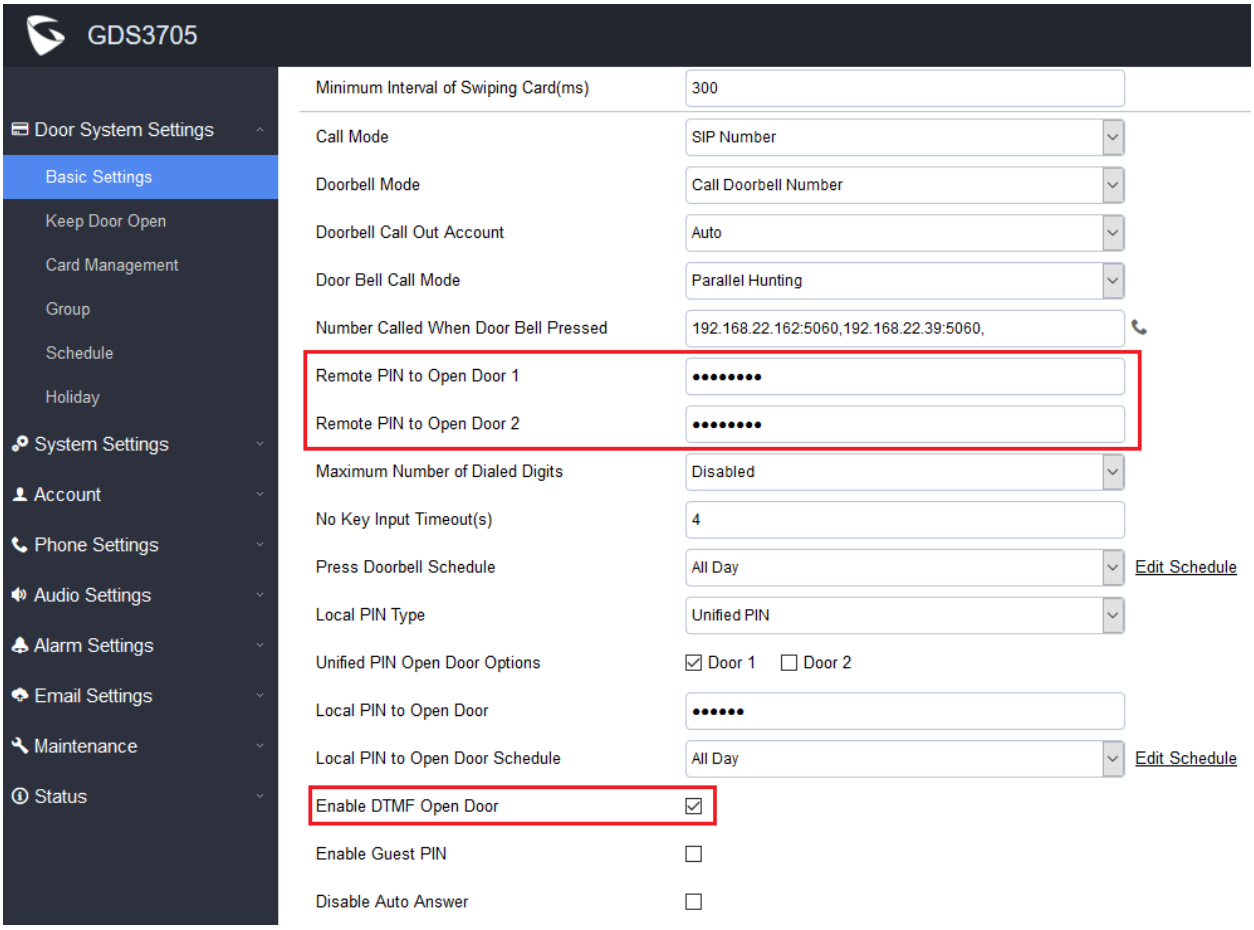


If Unified PIN (Universal PIN) is configured to open door, then which door can be controlled by the PIN is configured in the UI once “Unified PIN” selected.

For example, like above screenshot, if this universal PIN is set to open both DOO1 and DOOR2, but due to previous “Control Option” set to open Door1, and “Wiegand Control” set to open Door2, therefore the final result will be the **INTERSECT** result of both sets with condition qualified.

In above case, The PIN will only work at GDS3705 (DOOR1) and Wiegand Device (DOOR2) local input respectively. Meaning input PIN at GDS3705 will only open DOOR1 and will NOT open DOOR2.

- **Remote PIN to Operation of Doors:**

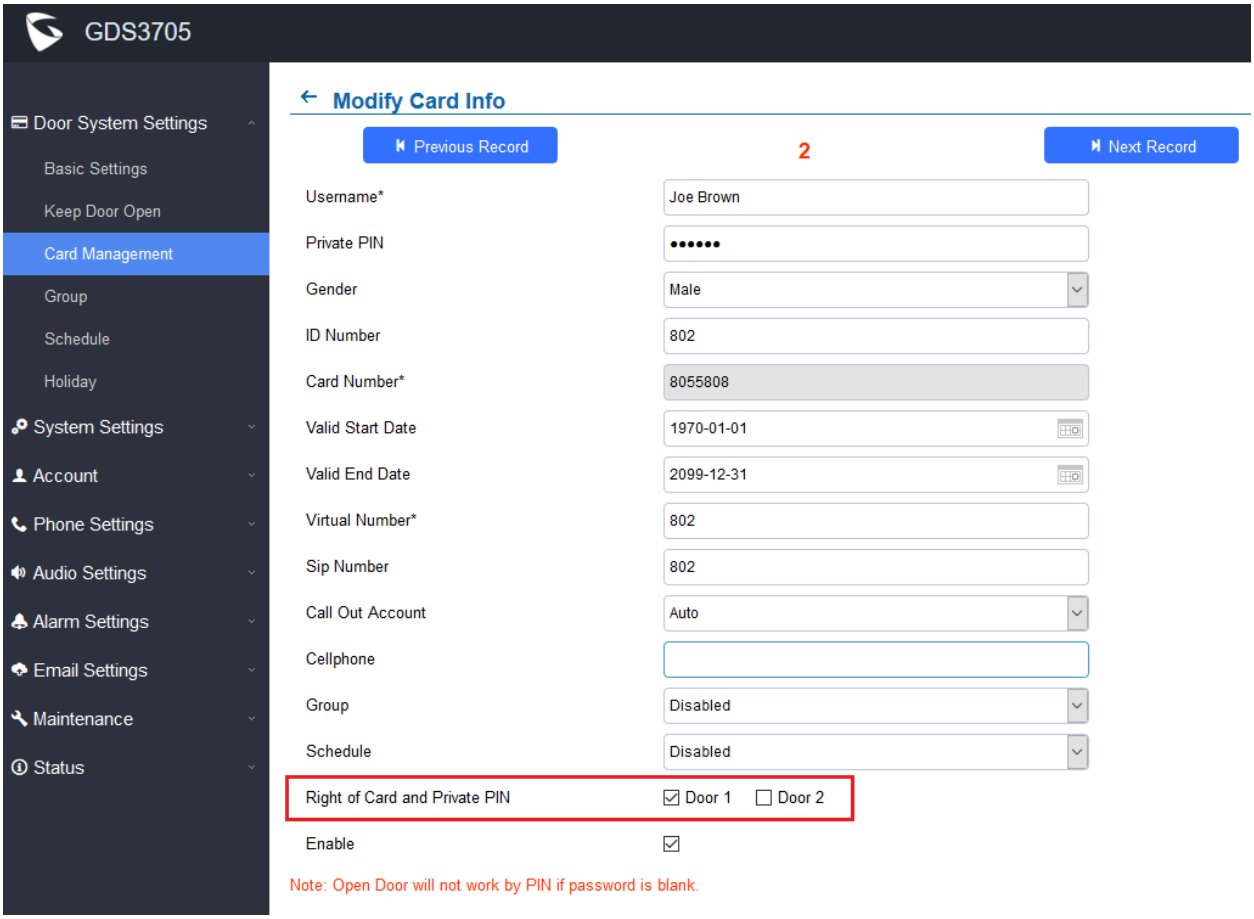


For remote PIN to open door, the PIN can be configured in above setting.

The PIN can be different for DOOR1 and DOOR2 and has to be configured correctly in related IP Phone which will be used to operate “One Key Open Door”.

If BOTH doors need to be opened at the same time, then both DOOR1 and DOOR2 has to be configured with exactly SAME password or PIN as DTMP open door.

- **Private PIN or Card & Private PIN:**



If using RFID card or Private PIN to open door, then which door can be opened by the RFID card or Private PIN is configured via “Card Management”, see above screenshot.

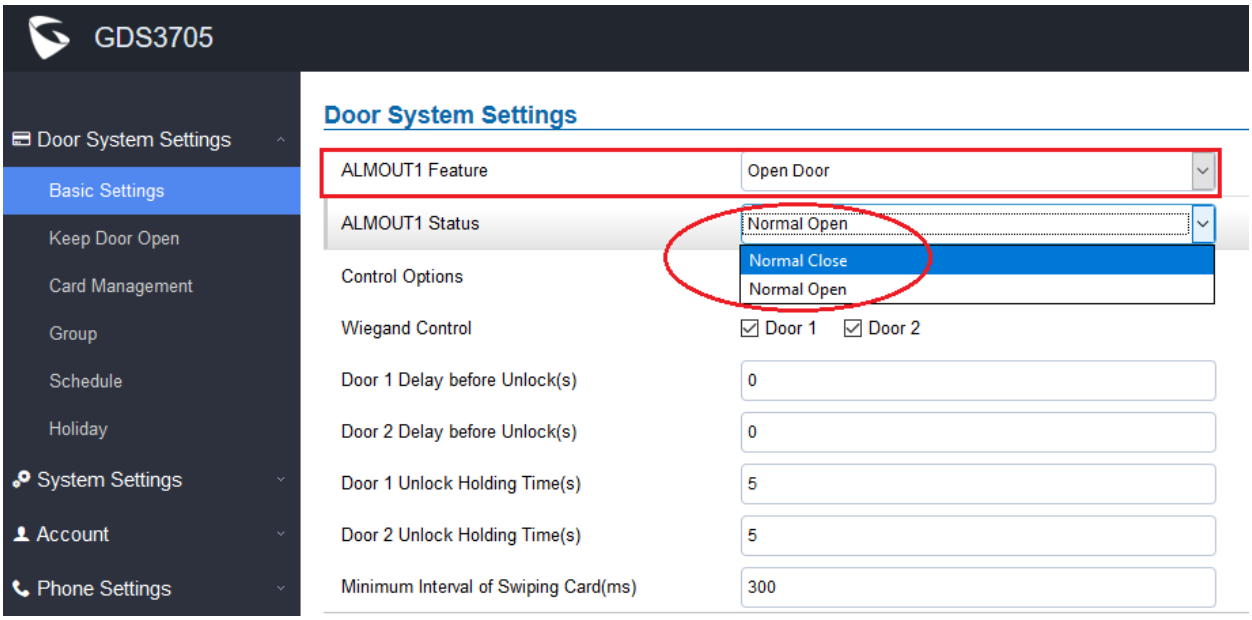
NOTE:

- For all the setting, the final result of which door can be opened is the **LOGIC INTERSECT OPERATION** of ALL the sets of condition qualified.
- Download the **DOOR OPEN LOGIC** document for more details about open Two Doors.
- Download the **TWO DOOR CONFIGURATION GUIDE** for detailed reference.
- Please refer to **GDS3705 USER MANUAL** for details about how to configure and control the DOOR1 and DOOR2 operation respectively.

NORMAL OPEN/CLOSE IN ALMOUT1 (COM1) DOOR2 CONTROL

- **Web Configuration**

This option can be found under device web UI → Door System Settings → Basic Settings:



- **Functionality**

This is an enhancement for an existing features after feedbacks from customers.

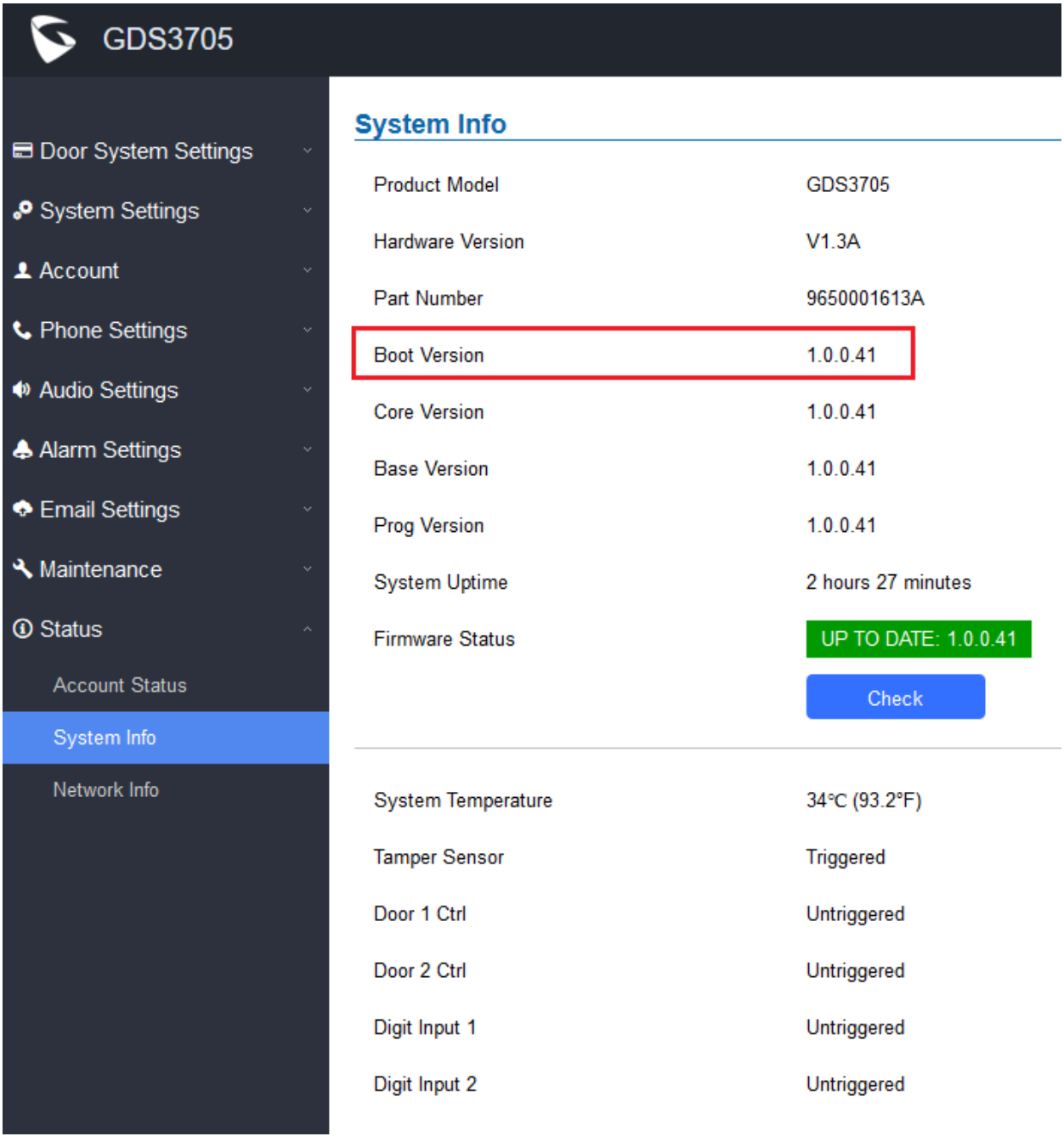
When re-using **ALMOUT1 (COM1)** interface to “Open Door” (controlling **DOOR2**) instead of “Alarm Output” (this feature is mutual exclusive, ONLY one choice will work), customers can choose “Normal Open” or “Normal Close” based on the electrical locker or striker used.

Please choose correctly based on the electrical locker or striker installed to avoid wrong operation.

ADDED BOOT VERSION IN "STATUS" PAGE

- **Web Configuration**

This option can be found under device web UI → Status → System Info:



- **Functionality**

This is an enhancement to display more technical information of GDS3705 in the "Status" page to help supporting users or customers when doing troubleshooting.

FIRMWARE VERSION 1.0.0.37

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

12/20/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and feature enhancement

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed reboot loop due to specific P-values.
- Fixed issue with ANATEL Certificate.

ENHANCEMENT

- Added ability to configure device with custom certificate signed by custom CA certificate
- Added event log showing users opening door via private PIN
- Added SIP NOTIFY to factory reset
- Added option to disable outbound proxy route header for both GDS3705/GDS3710
- Added CONFIG for firmware and configure server path and type via SSH.
- Added PING function in the CLI interface SSH.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side

NEW HTTP API

P15476	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&P15476=<value>	0: Disable 1: Enable
P2305/P2405/P2505/P2605	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Px=<value>	0: in route 1: not in route 2:always send to
P2306/P2406/P2506/P2606	GET:[http|https]://<servername>/goform/config?cmd=get&type=sip SET:[http|https]://<servername>/goform/config?cmd=set&Px=<value>	0: No 1: Yes

NEW P-VALUE

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	**<parameter> =<value>**	**<parameter> =<value>**	**<parameter> =<value>**	**Model Supported**	**Values**	**Description**
P2305=<int>	P2405=<int>	P2505=<int>	P2605=<int>	GDS3705	<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	<0|1>	Validate Incoming Messages 0: No 1: Yes

<parameter>=<value>	**Model Supported**	**Values**	**Description**
P15476	GDS3705	<0|1>	Allow Reset Via SIPNOTIFY 0: Disable (Default) 1: Enable

NEW FEATURES OVERVIEW

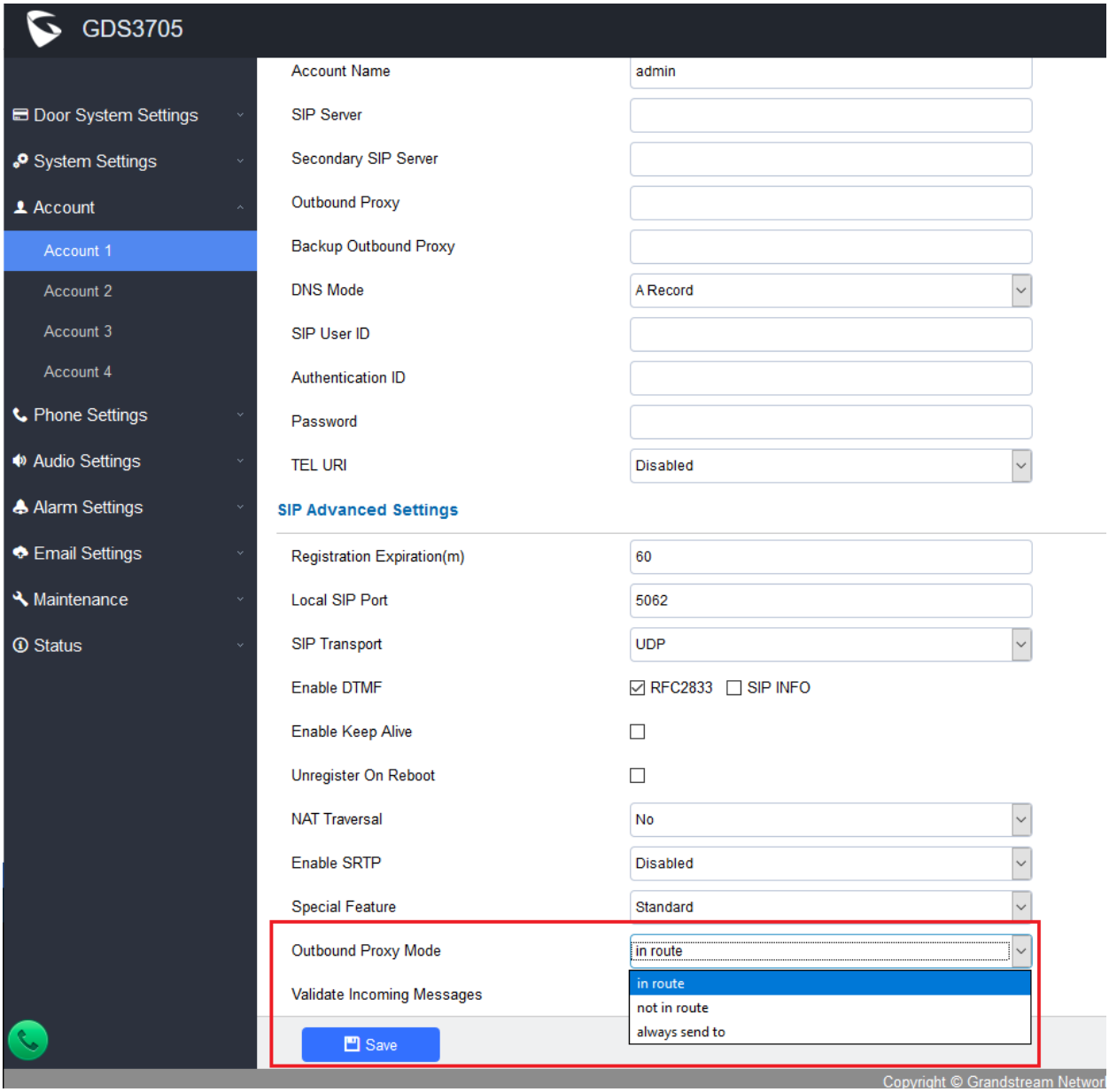
This section lists major new features and describes how to use them from the user's point of view.

OPTION OF OUTBOUND PROXY MODE

- **Web Configuration**

New feature added to allow users to configure the outbound proxy mode, as well as "Validate Incoming Message". This feature is very useful for ITSP service provider.

This option can be found under device web UI: Account X → SIP Advanced Settings:



- **Functionality**

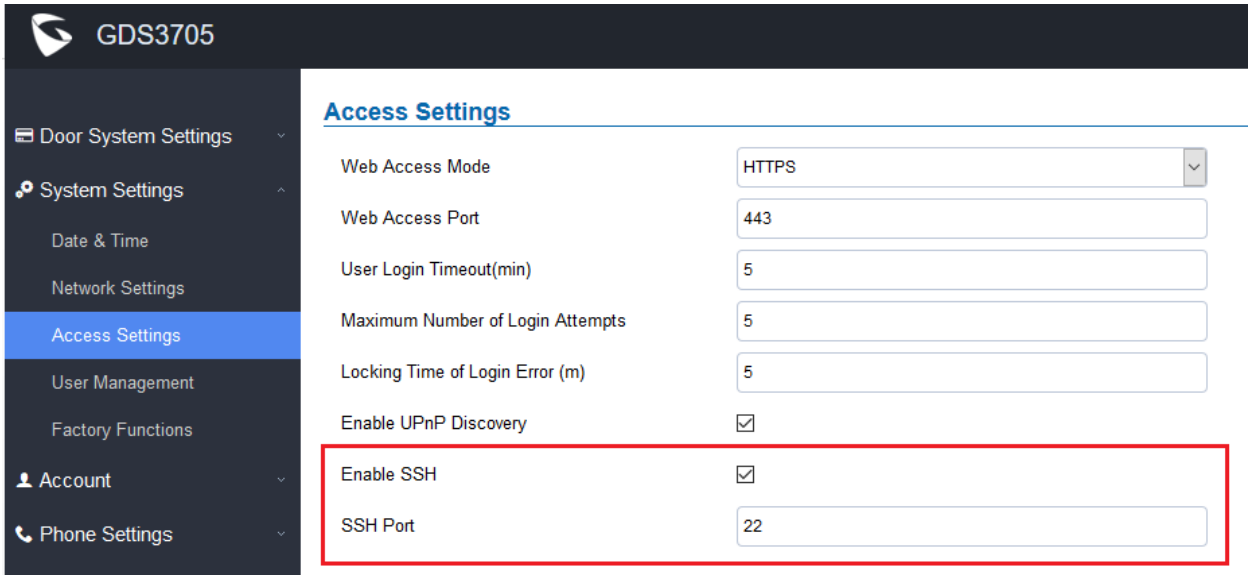
This feature is added to meet the requirement of ITSP customers. Service provider (ITSP) customers can make choosing different Outbound Proxy Mode for their customers to use the service based on different network environment.

CONFIG FIRMWARE OR CONFIGURATION SERVER PATH AND ICMP TEST VIA SSH

- **Web Configuration**

This feature is added to allow user to change firmware server path or configuration server path via SSH. This is very useful for ITSP or service contractors or installer to maintenance the device, for example, the webUI is purposed blocked, ITSP or Service Technician can use scripts in SSH to perform necessary configuration or maintenance, or upgrade firmware.

The SSH has to be enabled to use this feature. The option of this webUI can be found: System Settings → Access Settings:

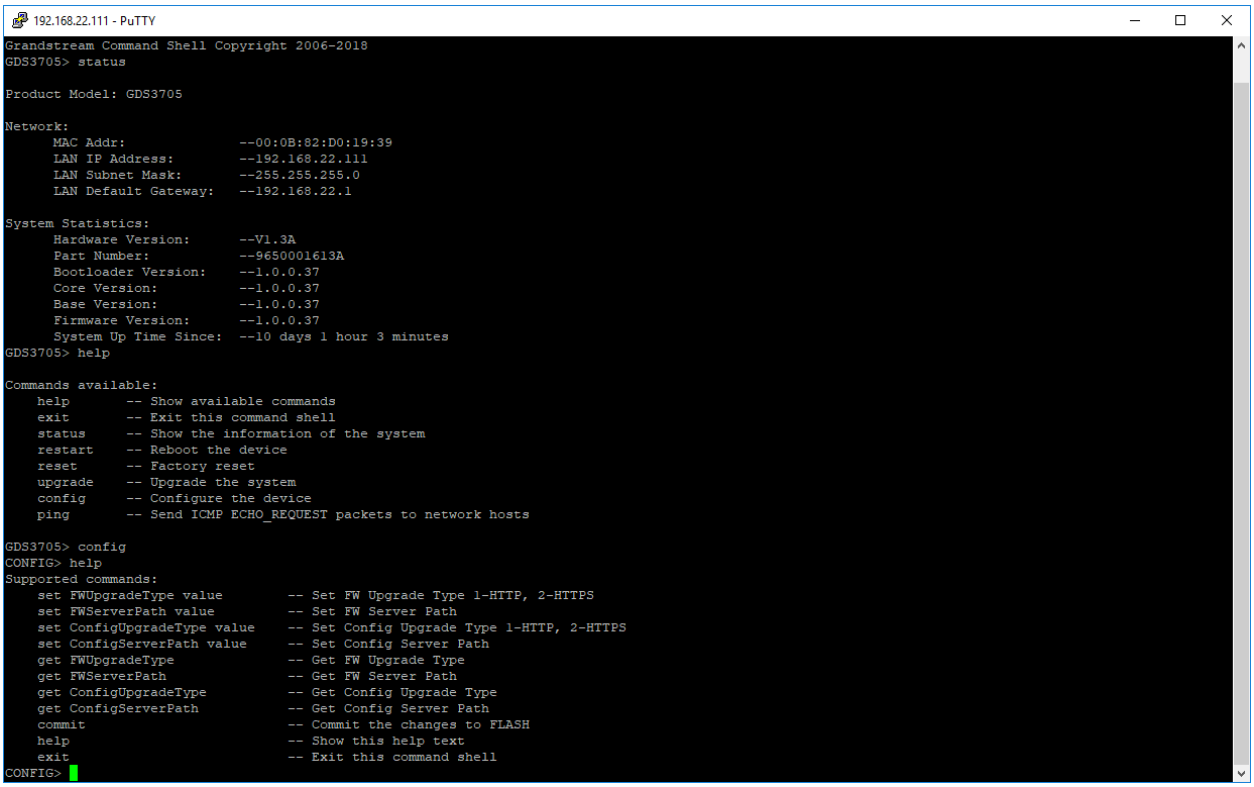


- **Functionality**

This feature is added to allow users (service technician, installer, etc.) to configure or change the firmware server or configuration server path via SSH, enhance the security of SIP accounts configured in GDS3705.

3rd party SSH application like PuTTY is required to use this feature.

For example, below is the screenshot of such CLI interface:



NOTE:

- This feature is designed for ITSP Service Provider, or Service Technician or Installers.
- End users without necessary knowledge are strongly discouraged to access it, avoiding damage the device or making the device not working properly.

FIRMWARE VERSION 1.0.0.36

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

11/06/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and feature enhancement

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed factory reset and configuration without another reboot the Wiegand port will not open door.
- Fixed data import in CSV format is not complete.
- Fixed confirmation tone not played when using SIP phone remote open door.
- Fixed parallel hunting preview mode the one key open door feature failed.
- Fixed cannot set strong admin password with special characters included.
- Fixed security vulnerability to compromise root access via SSH.

ENHANCEMENT

- Added ability to configure device with custom certificate signed by custom CA certificate
- Added SIP password hided and not visible in the WebUI
- Extended VLAN range from 0 ~ 55 to 0 ~ 4094
- Added option to display device temperature in Fahrenheit.
- Added support for special character “@” in the SIP User ID.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side

NEW HTTP API

N/A

NEW P-VALUE

N/A

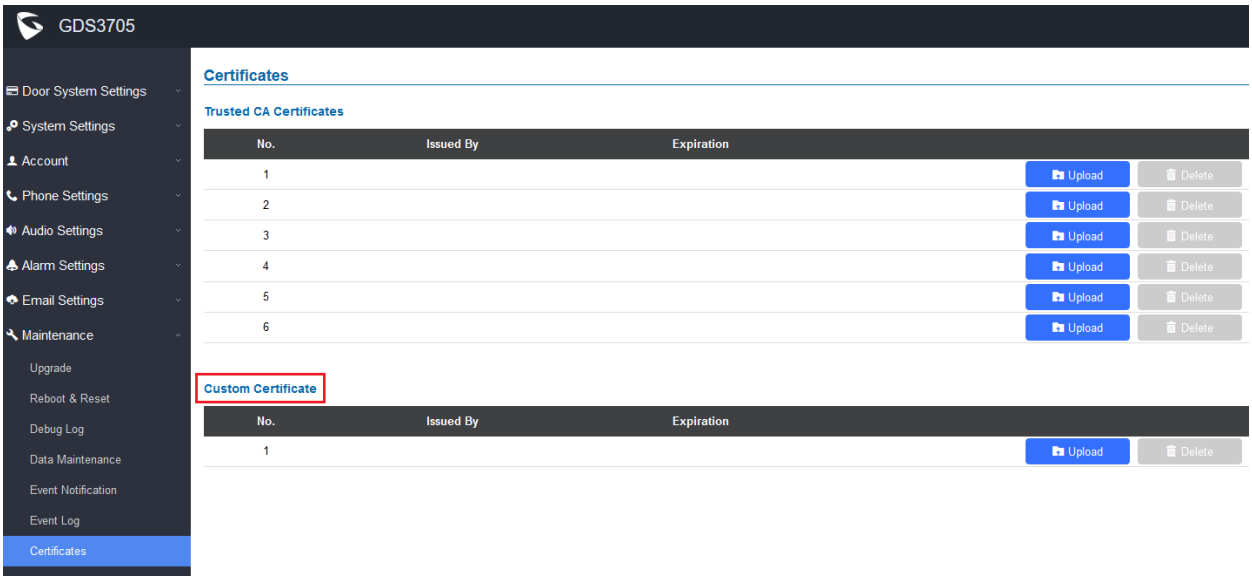
NEW FEATURES OVERVIEW

This section lists major new features and describes how to use them from the user's point of view.

CUSTOM CERTIFICATE

- **Web Configuration**

New feature added to allow users to configure the device with custom certificate signed by custom CA certificate. This option can be found under device web UI: Maintenance → Certificates like below:



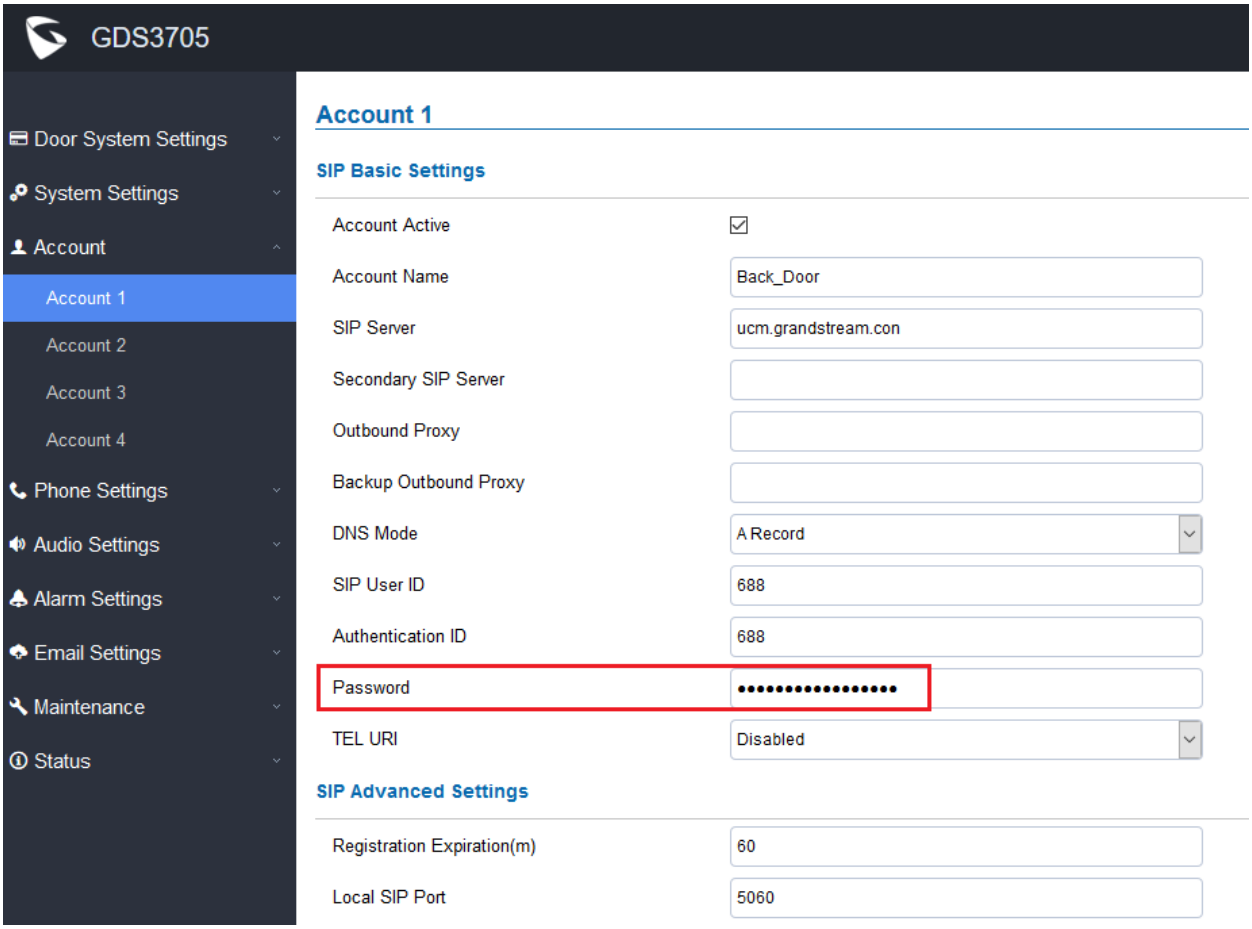
- **Functionality**

This feature is added to meet the requirement of ITSP customers. Service provider (ITSP) customers can make their own CA certificate and uploaded to the GDS device and provide service to their customers.

INVISIBLE SIP PASSWORD

- **Web Configuration**

This feature is added to enhance the security of SIP accounts configured in GDS3705. This can be found under device web UI: Account → Account X (where X: 1 ~ 4)



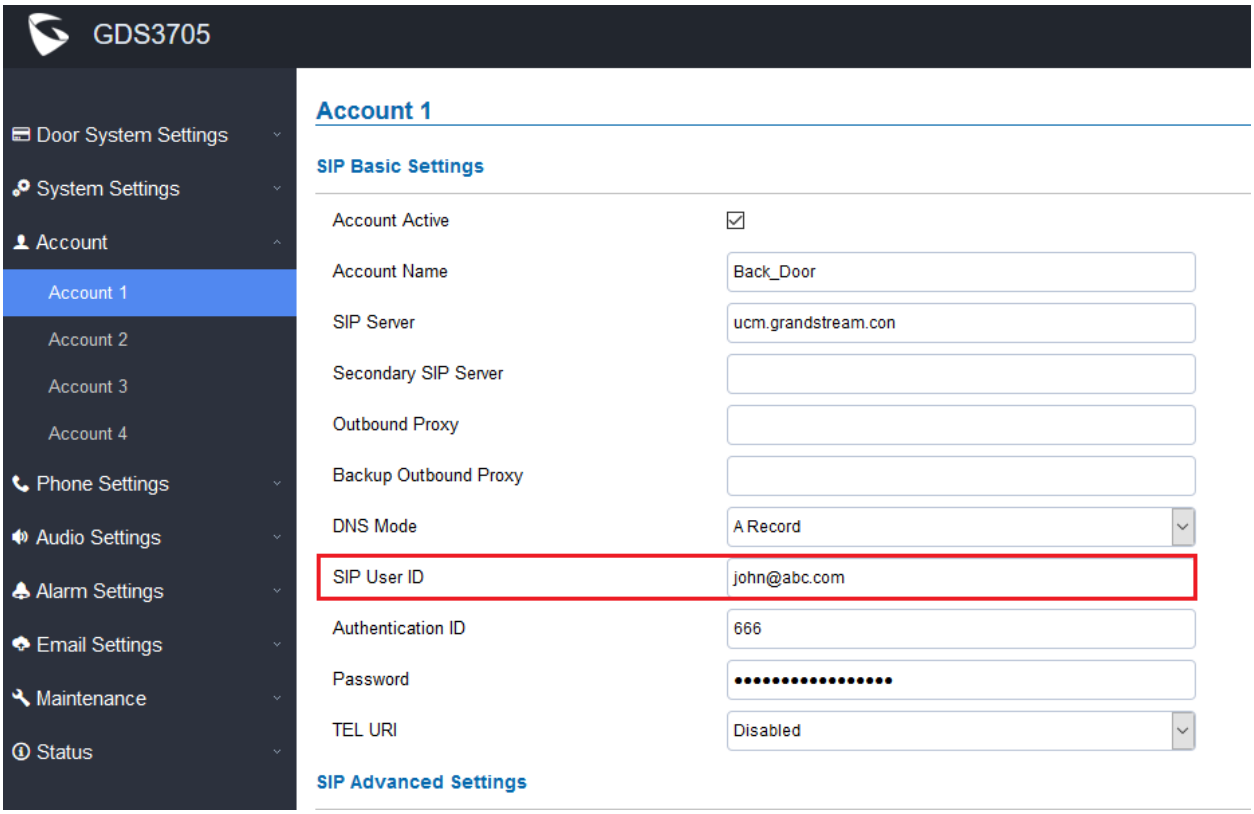
- **Functionality**

This feature is added to enhance the security of SIP accounts configured in GDS3705. Password is invisible from the webUI.

SPECIAL SIP USER ID

- **Web Configuration**

This feature is added to enhance the compatibility of GDS3705 with some SIP Proxys which using special characters like "@" as user ID. This can be found under device web UI: Account → Account X (where X: 1 ~ 4)



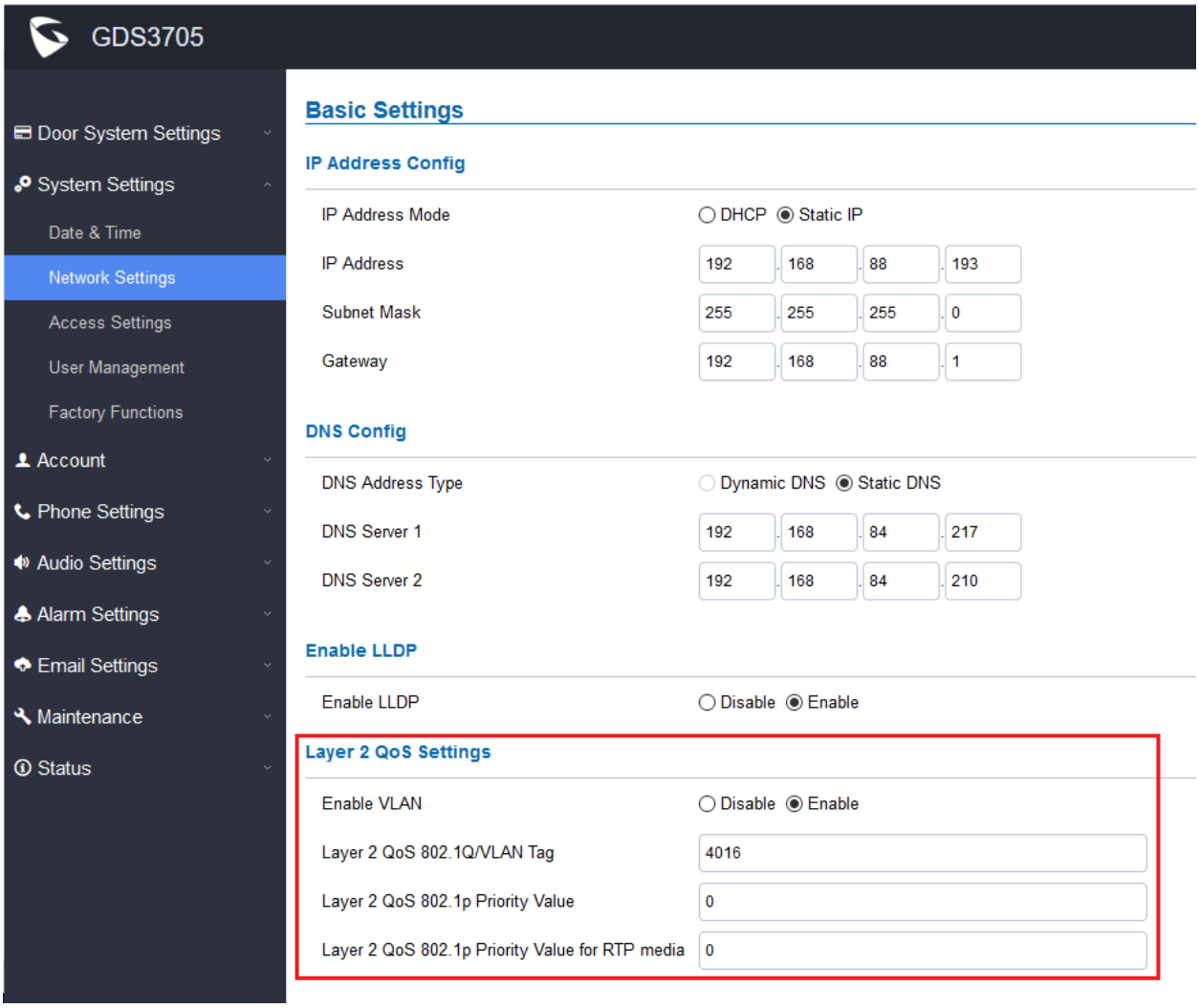
- **Functionality**

This feature is added to enhance the compatibility of GDS3705 with some SIP Proxys which using special characters like "@" as user ID.

EXTENDED VLAN RANGE 0 ~ 4094

- **Web Configuration**

This feature is added to enhance the VLAN range. This can be found under device web UI: System Settings → Network Settings → Layer 2 QoS Settings:



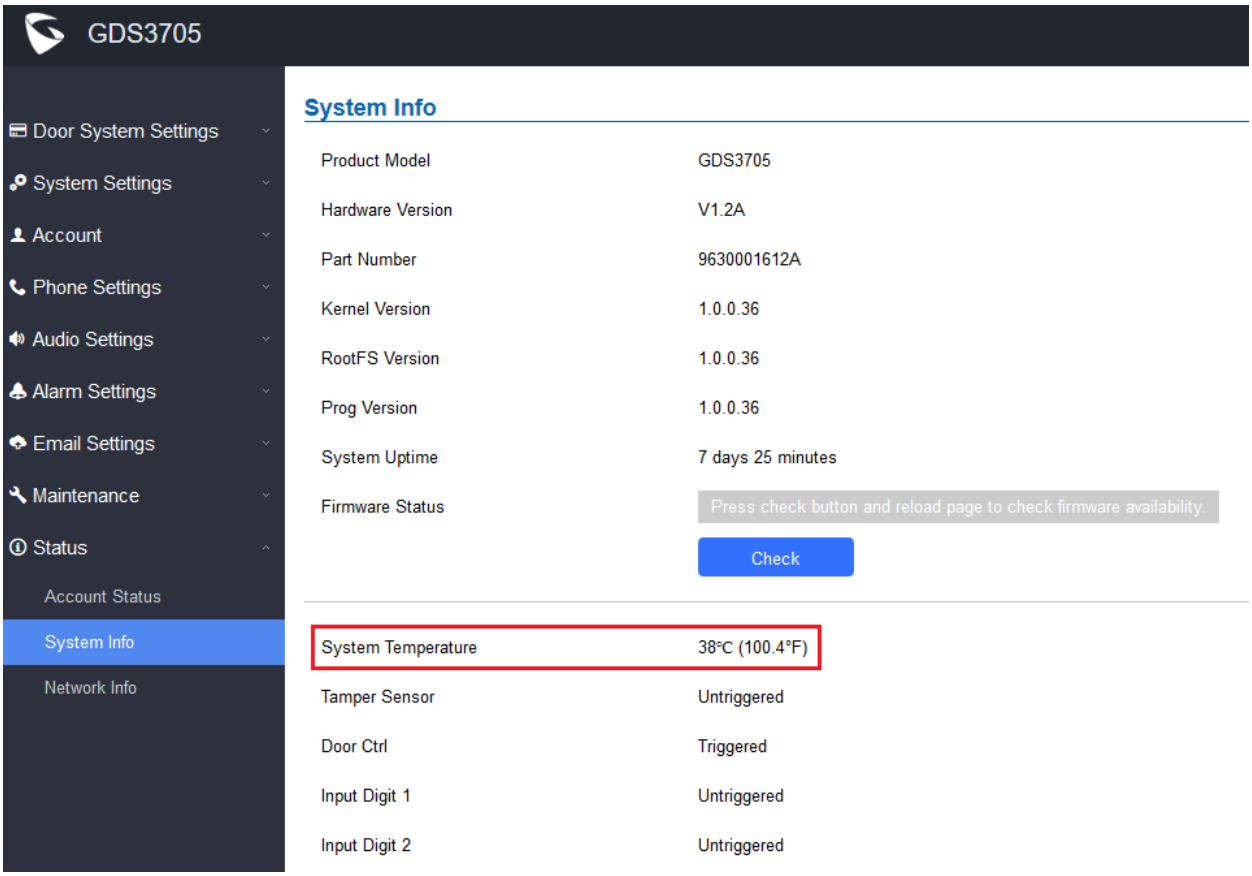
- **Functionality**

This feature is added to enhance the VLAN parameter settings. User can input the related VLAN parameters based on the appropriate network environment.

DISPLAY TEMPERATURE IN FAHRENHEIT

- **Web Configuration**

This feature is added to meet customers' requirement. This can be found under device web UI: Status → System Info:



- **Functionality**

This feature is added to meet customers' requirement and user habit.

FIRMWARE VERSION 1.0.0.35

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

09/21/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and feature enhancement since $1 Beta.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed digital input open door mode not functioning as expected.
- Fixed schedule cannot be saved when DI set to open door mode.
- Fixed Direct IP Call mode fail when SIP transmission set to TCP and TLS/TCP mode.
- Fixed no confirmation sound played when using GXP phone's "one key open door" feature to open the door without answering the call from GDS.
- Fixed STUN disabled the local SIP port incorrect.
- Fixed DTMF tone too short sounds like got cut off.
- Fixed when using RFC2833 the DTMF is incorrect.
- Fixed enable "Silent Alarm" mode when alarm triggered at schedule not configured the GDS not sending alarm sound.

ENHANCEMENT

- Added SIP extensions and/or IP addresses or combined “Parallel Hunting” (simultaneously ringing) mode when doorbell pressed.
- Added “Normal Open” and “Normal Close” state option in digit input “Alarm Input” mode.
- Added ability to configure schedule for “Alarm In” Open Door.
- Added option to send “call completed elsewhere” when door is opened successfully by GXP phone so other GXP phones in the open door list will not show “missed call” in the call history.
- Added multiple SIP account support (up to 4 SIP accounts).
- Added feature to support CSV format when import or export data.
- Added “Check for Update” firmware upgrade button like GXV phones to check the latest firmware.
- Added option to set maximum digits dialed so when the number of digit matched the call will immediately sending out by GDS without “#” pressed.
- Added ability to assign/configure a time schedule to the doorbell.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side

NEW HTTP API

P15419

GET：
<http|https>://<servername>/goform/config?cmd=get&type=door
SET：
<http|https>://<servername>/goform/config?cmd=set& P15419=<0-20>

P15418

GET：
<http|https>://<servername>/goform/config?cmd=get&type=door
SET：
<http|https>://<servername>/goform/config?cmd=set& P15418=<0-10>

P443

GET：
<http|https>://<servername>/goform/config?cmd=get&type=sip
SET：
<http|https>://<servername>/goform/config?cmd=set& P443=<0-20>

FW upgrade operate

fw_upgrade:
http://<servername>/goform/config?cmd=fw_upgrade&type=<0/1>

Card Data Import/Export

export:
http://<servername>/goform/config?cmd= export&type=1&data_type=<0/1>
upload:
http://<servername>/goform/config?cmd= upload&type=0&dupopt=<0/1>

Pfw_available_version

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

NEW P-VALUE

P-Value	Model Supported	Default Value	Comments
P15418=<int>	GDS3710/GDS3705	0 - 10	Press Doorbell Schedule
P15419=<int>	GDS3710/GDS3705	0 - 20	Maximum Number of Dialed Digits

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>	GDS3705	<0|1>	Account Active (In Use). 0:No 1:Yes
P210=<int>	P499=<int>	P599=<int>	P699=<int>	GDS3705	<0|1>	SIP Registration Status(Read Only)
P3=<string>	P407=<string>	P507=<string>	P607=<string>	GDS3705		Account Name Max. Length = 64
P47=<string>	P402=<string>	P502=<string>	P602=<string>	GDS3705		SIP Server Max. Length = 255
P2312=<string>	P2412=<string>	P2512=<string>	P2612=<string>	GDS3705		Secondary SIP Server Max. Length = 255
P48=<string>	P403=<string>	P503=<string>	P603=<string>	GDS3705		Outbound Proxy Max. Length = 255
P2333=<string>	P2433=<string>	P2533=<string>	P2633=<string>	GDS3705		Backup Outbound Proxy Max. Length = 255
P103=<int>	P408=<int>	P508=<int>	P608=<int>	GDS3705	<0|1|2>	DNS Mode 0:A Record 1:SRV 2:NAPTR/SRV

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	Model Supported	Values	Description
P35=<string>	P404=<string>	P504=<string>	P604=<string>	GDS3705		SIP User ID Max. Length = 255
P36=<string>	P405=<string>	P505=<string>	P605=<string>	GDS3705		Authenticate ID Max. Length = 255
P34=<string>	P406=<string>	P506=<string>	P606=<string>	GDS3705		Authenticate password Max. Length = 255
P63=<int>	P409=<int>	P509=<int>	P609=<int>	GDS3705	<0|1|2>	TEL URI 0: Disabled 1: User = Phone 2: Enable
P32=<int>	P412=<int>	P512=<int>	P612=<int>	GDS3705	60 - 64800	Registration Expiration(m)
P40=<int>	P413=<int>	P513=<int>	P613=<int>	GDS3705	1 - 65535	Local SIP Port
P130=<int>	P448=<int>	P548=<int>	P648=<int>	GDS3705	<0|1|2>	SIP Transport 0: UDP 1: TCP 2: TLS/TCP
P2302=<int>	P2402=<int>	P2502=<int>	P2602=<int>	GDS3705	<0|1>	Enable DTMF RFC2833 0: Disable 1: Enable
P2303=<int>	P2403=<int>	P2503=<int>	P2603=<int>	GDS3705	<0|1>	Enable DTMF SIP INFO 0: Disable 1: Enable
P490=<int>	P1309=<int>	P590=<int>	P690=<int>	GDS3705	<0|1>	Enable Keep Alive 0: Disable 1: Enable

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	**<parameter> =<value>**	**<parameter> =<value>**	**<parameter> =<value>**	**Model Supported**	**Values**	**Description**
P52=<int>	P414=<int>	P514=<int>	P614=<int>	GDS3705	<0|1|2|3|4>	NAT Traversal 0:No 1:Stun 2:Keep Alive 3:UPnP 4:Auto 5:VPN
P81=<int>	P411=<int>	P511=<int>	P611=<int>	GDS3705	<0|1>	Unregister On Reboot 0: Disable 1: Enable
P183=<int>	P443=<int>	P543=<int>	P643=<int>	GDS3705	<0|1|2>	Enable SRTP 0: Disable 1: Enable but not Forced 2: Enable and Forced
P100=<int>	P424=<int>	P524=<int>	P624=<int>	GDS3705	<100|102>	Special Feature 100: Standard 102: Broadsoft

<parameter>=<value>	Model Supported	Values	Description
P76=<string>	GDS3705		STUN Server
P39=<int>	GDS3705	1 - 65535	Local SIP Port
P10451=<int>	GDS3705	0 - 65535	Auto On-Hook Timer (Seconds)
P29610=<int>	GDS3705	48-10000	Use Random Port
P14847=<int>	GDS3705	0 - 90	Ring Timeout
P280=<string>	GDS3705		SIP TLS Certificate
P279=<string>	GDS3705		SIP TLS Private Key
P281=<string>	GDS3705		SIP TLS Private Key Password
P10453=<int>	GDS3705	<0|1>	Enable Direct IP Call 0: Disable 1: Enable
P8001=<int>	GDS3705	<0|1>	Enable two-way SIP Calling 0: Disable 1: Enable
P8003=<int>	GDS3705	<0|1>	SIP Proxy Compatibility Mode 0: Disable 1: Enable
P10410=<int>	GDS3705	<0|1>	Enable White List 0: Disable 1: Enable
P10411=<string>	GDS3705		Use (,) as separator when deleting multiple numbers.
P10420=<int>	GDS3705	<0|1>	Enable White List 0: Disable 1: Enable
P10421=<string>	GDS3705		Use (,) as separator when deleting multiple numbers.
P10430=<int>	GDS3705	<0|1>	Enable White List 0: Disable 1: Enable
P10431=<string>	GDS3705		Use (,) as separator when deleting multiple numbers.

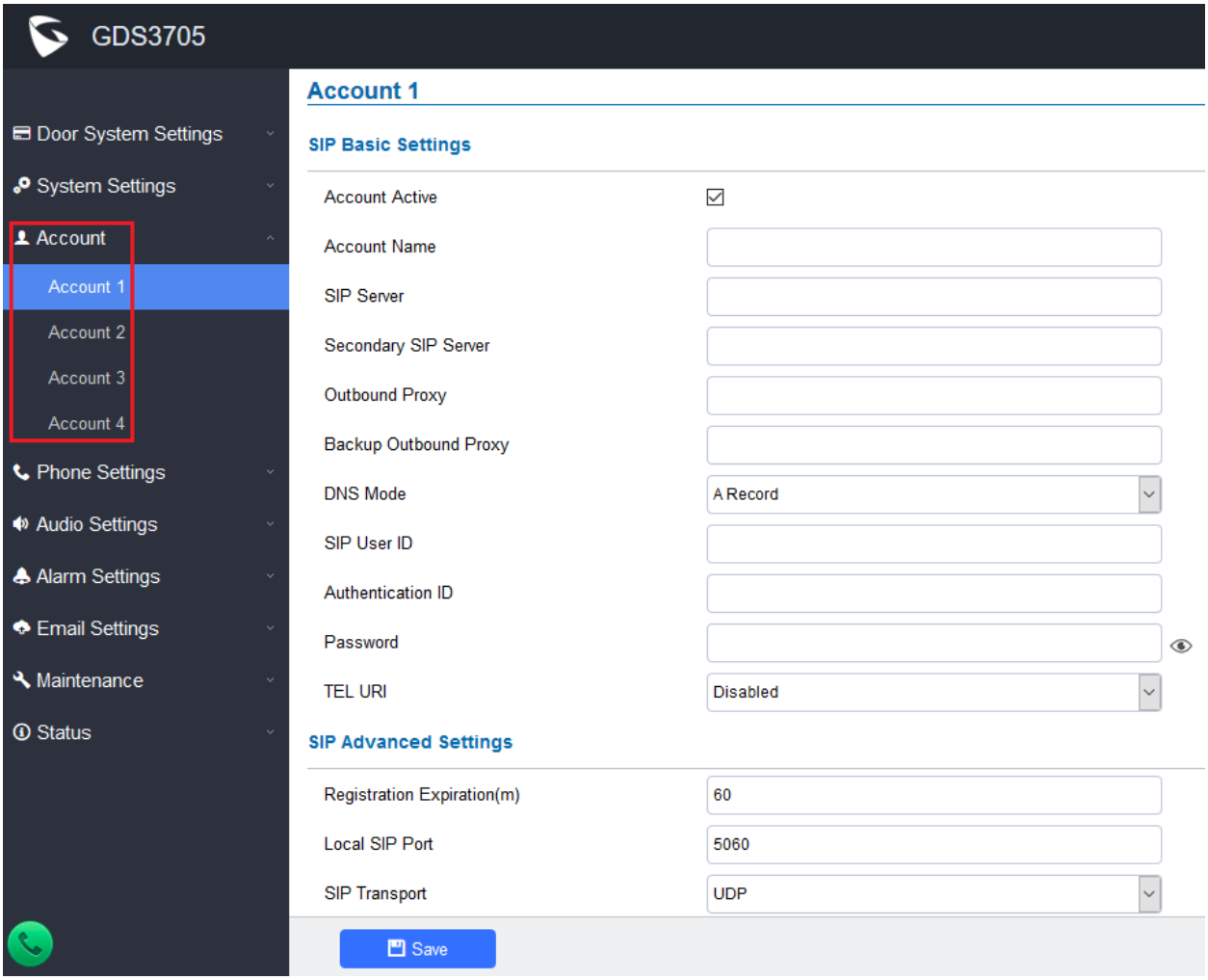
NEW FEATURES OVERVIEW

This section lists major new features and describes how to use them from the user's point of view.

MULTIPLE SIP ACCOUNTS

- **Web Configuration**

New feature added to support up to 4 SIP Accounts. This option can be found under device web UI → Account Settings page like below:



- **Functionality**

This feature added to meet the requirement of customers. Up to 4 SIP Proxy can be configured into GDS3705, solving application scenes like multiple companies or residents in one building but sharing the same entry door. The speed dial shortcut can be configured to help customers easily dial to related party to ask for open door.

- **New P-Value**

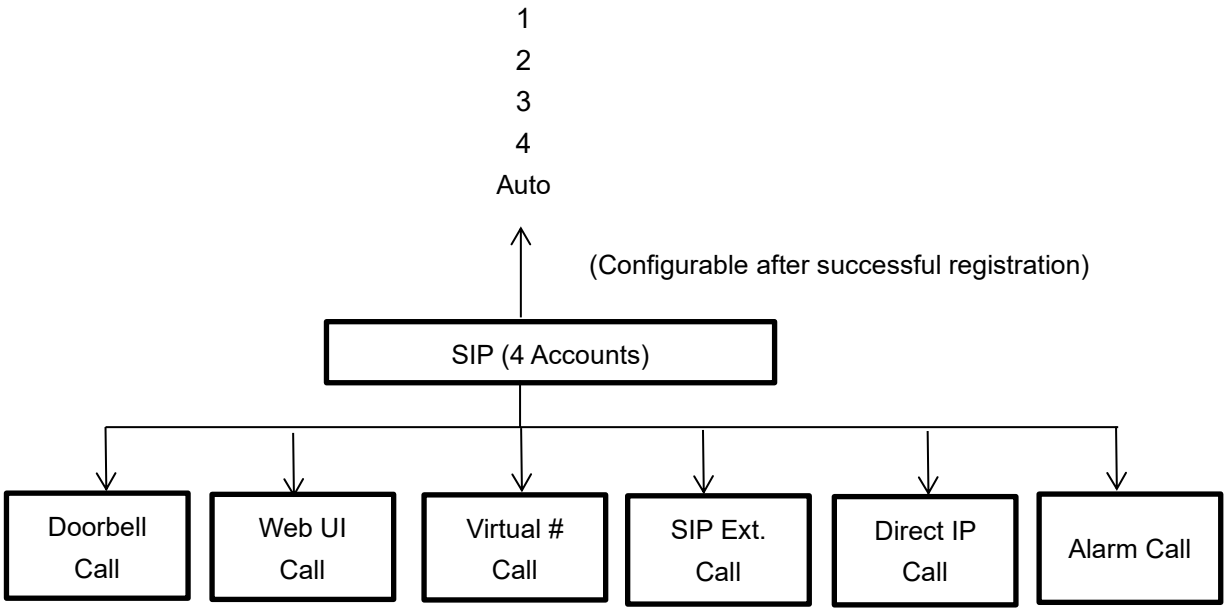
Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	**<parameter> =<value>**	**<parameter> =<value>**	**<parameter> =<value>**	**Model Supported**	**Values**	**Description**
P271=<int>	P401=<int>	P501=<int>	P601=<int>	GDS3705	<0|1>	Account Active (In Use). 0:No 1:Yes
P210=<int>	P499=<int>	P599=<int>	P699=<int>	GDS3705	<0|1>	SIP Registration Status(Read Only)
P3=<string>	P407=<string>	P507=<string>	P607=<string>	GDS3705		Account Name Max. Length = 64
P47=<string>	P402=<string>	P502=<string>	P602=<string>	GDS3705		SIP Server Max. Length = 255
P2312=<string>	P2412=<string>	P2512=<string>	P2612=<string>	GDS3705		Secondary SIP Server Max. Length = 255
P48=<string>	P403=<string>	P503=<string>	P603=<string>	GDS3705		Outbound Proxy Max. Length = 255
P2333=<string>	P2433=<string>	P2533=<string>	P2633=<string>	GDS3705		Backup Outbound Proxy Max. Length = 255
P103=<int>	P408=<int>	P508=<int>	P608=<int>	GDS3705	<0|1|2>	DNS Mode 0:A Record 1:SRV 2:NAPTR/SRV

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	Model Supported	Values	Description
P35=<string>	P404=<string>	P504=<string>	P604=<string>	GDS3705		SIP User ID Max. Length = 255
P36=<string>	P405=<string>	P505=<string>	P605=<string>	GDS3705		Authenticate ID Max. Length = 255
P34=<string>	P406=<string>	P506=<string>	P606=<string>	GDS3705		Authenticate password Max. Length = 255
P63=<int>	P409=<int>	P509=<int>	P609=<int>	GDS3705	<0|1|2>	TEL URI 0: Disabled 1: User = Phone 2: Enable
P32=<int>	P412=<int>	P512=<int>	P612=<int>	GDS3705	60 - 64800	Registration Expiration(m)
P40=<int>	P413=<int>	P513=<int>	P613=<int>	GDS3705	1 - 65535	Local SIP Port
P130=<int>	P448=<int>	P548=<int>	P648=<int>	GDS3705	<0|1|2>	SIP Transport 0: UDP 1: TCP 2: TLS/TCP
P2302=<int>	P2402=<int>	P2502=<int>	P2602=<int>	GDS3705	<0|1>	Enable DTMF RFC2833 0: Disable 1: Enable
P2303=<int>	P2403=<int>	P2503=<int>	P2603=<int>	GDS3705	<0|1>	Enable DTMF SIP INFO 0: Disable 1: Enable
P490=<int>	P1309=<int>	P590=<int>	P690=<int>	GDS3705	<0|1>	Enable Keep Alive 0: Disable 1: Enable

Account 1	Account 2	Account 3	Account 4			
<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	<parameter> =<value>	Model Supported	Values	Description
P52=<int>	P414=<int>	P514=<int>	P614=<int>	GDS3705	<0|1|2|3|4>	NAT Traversal 0:No 1:Stun 2:Keep Alive 3:UPnP 4:Auto 5:VPN
P81=<int>	P411=<int>	P511=<int>	P611=<int>	GDS3705	<0|1>	Unregister On Reboot 0: Disable 1: Enable
P183=<int>	P443=<int>	P543=<int>	P643=<int>	GDS3705	<0|1|2>	Enable SRTP 0: Disable 1: Enable but not Forced 2: Enable and Forced
P100=<int>	P424=<int>	P524=<int>	P624=<int>	GDS3705	<100|102>	Special Feature 100: Standard 102: Broadsoft

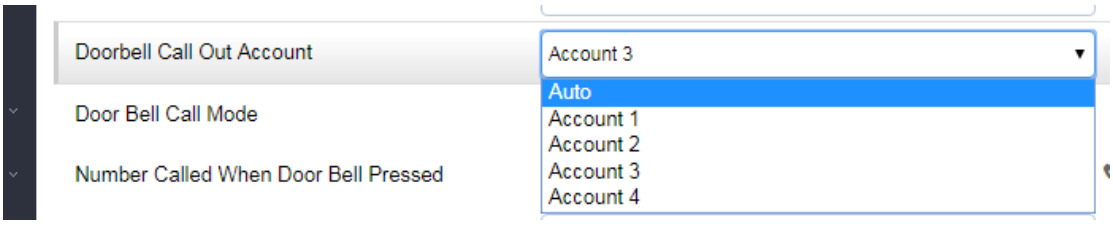
<parameter>=<value>	Model Supported	Values	Description
P76=<string>	GDS3705		STUN Server
P39=<int>	GDS3705	1 - 65535	Local SIP Port
P10451=<int>	GDS3705	0 - 65535	Auto On-Hook Timer (Seconds)
P29610=<int>	GDS3705	48-10000	Use Random Port
P14847=<int>	GDS3705	0 - 90	Ring Timeout
P280=<string>	GDS3705		SIP TLS Certificate
P279=<string>	GDS3705		SIP TLS Private Key
P281=<string>	GDS3705		SIP TLS Private Key Password
P10453=<int>	GDS3705	<0|1>	Enable Direct IP Call 0: Disable 1: Enable
P8001=<int>	GDS3705	<0|1>	Enable two-way SIP Calling 0: Disable 1: Enable
P8003=<int>	GDS3705	<0|1>	SIP Proxy Compatibility Mode 0: Disable 1: Enable
P10410=<int>	GDS3705	<0|1>	Enable White List 0: Disable 1: Enable
P10411=<string>	GDS3705		Use (,) as separator when deleting multiple numbers.
P10420=<int>	GDS3705	<0|1>	Enable White List 0: Disable 1: Enable
P10421=<string>	GDS3705		Use (,) as separator when deleting multiple numbers.
P10430=<int>	GDS3705	<0|1>	Enable White List 0: Disable 1: Enable
P10431=<string>	GDS3705		Use (,) as separator when deleting multiple numbers.

- **Flow Chart of Multiple SIP Account**



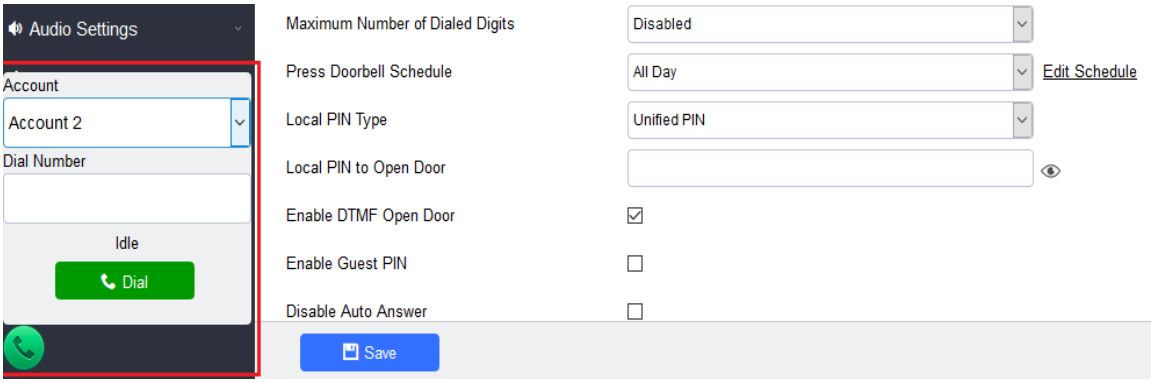
1) Doorbell Call:

Doorbell call can be configured to use maximum 4 SIP account line to call. The specific line used is configured in the "Card Management" settings. When configured as Auto (only works when related SIP proxy belong to one owner and function like fail-over), the GDS will check all the 4 accounts registered and call out using the first available registered account. Normal usage will be configured using selected account (in the "Card Management" page) to call out.



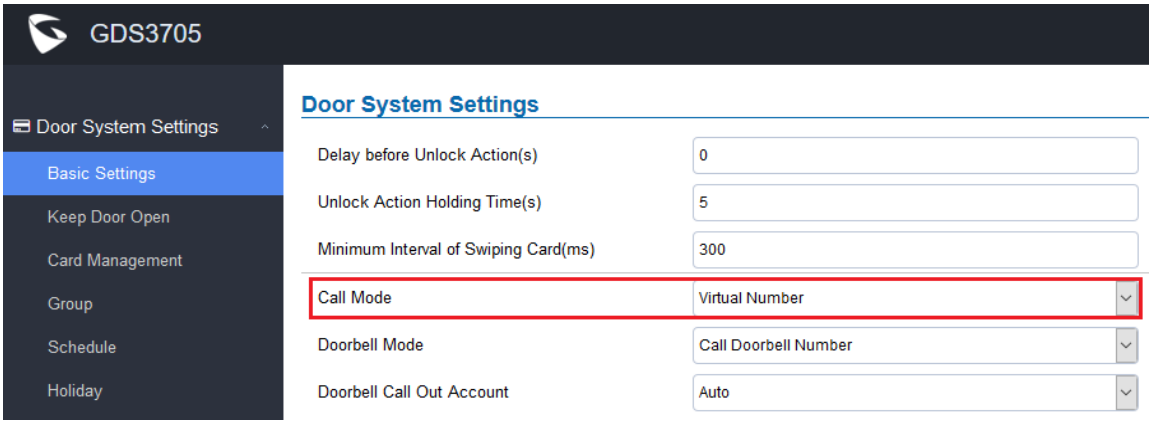
2) WebUI Call:

WebUI call is following the same calling protocol like 1). See below screenshot:

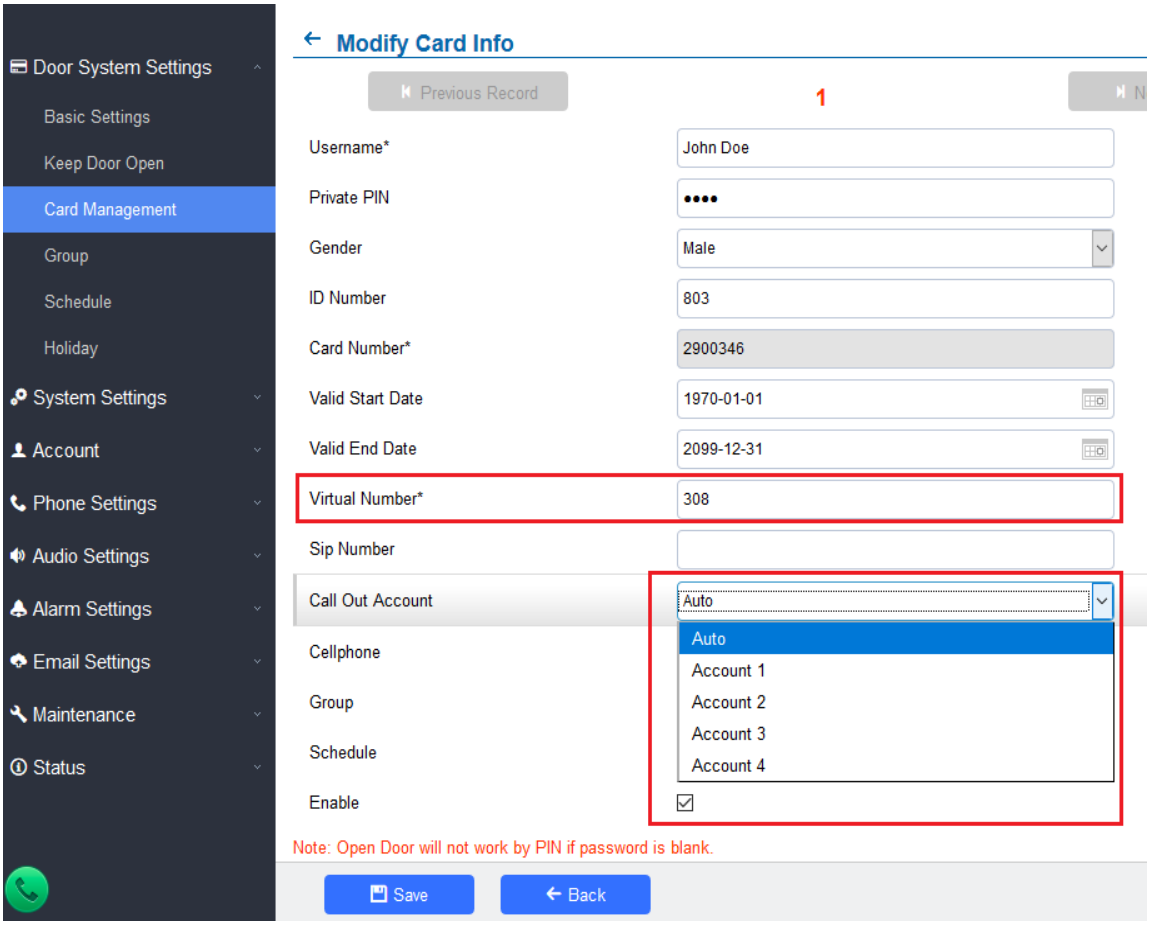


3) Virtual # Call:

Virtual # call can be configured in “Basic Settings” by choose “Call Mode” to be “Virtual Number” (default setting) like below:

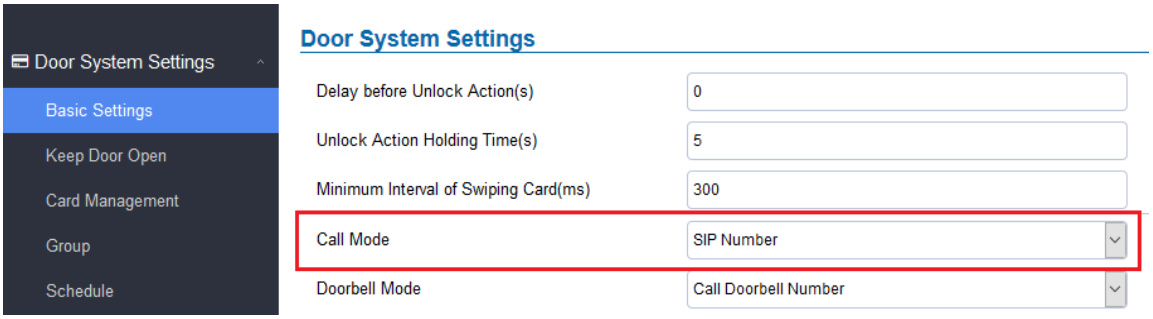


Then configure and select the “Call Out Account” in the “Card Management” page like below, by using select specific account to call out:

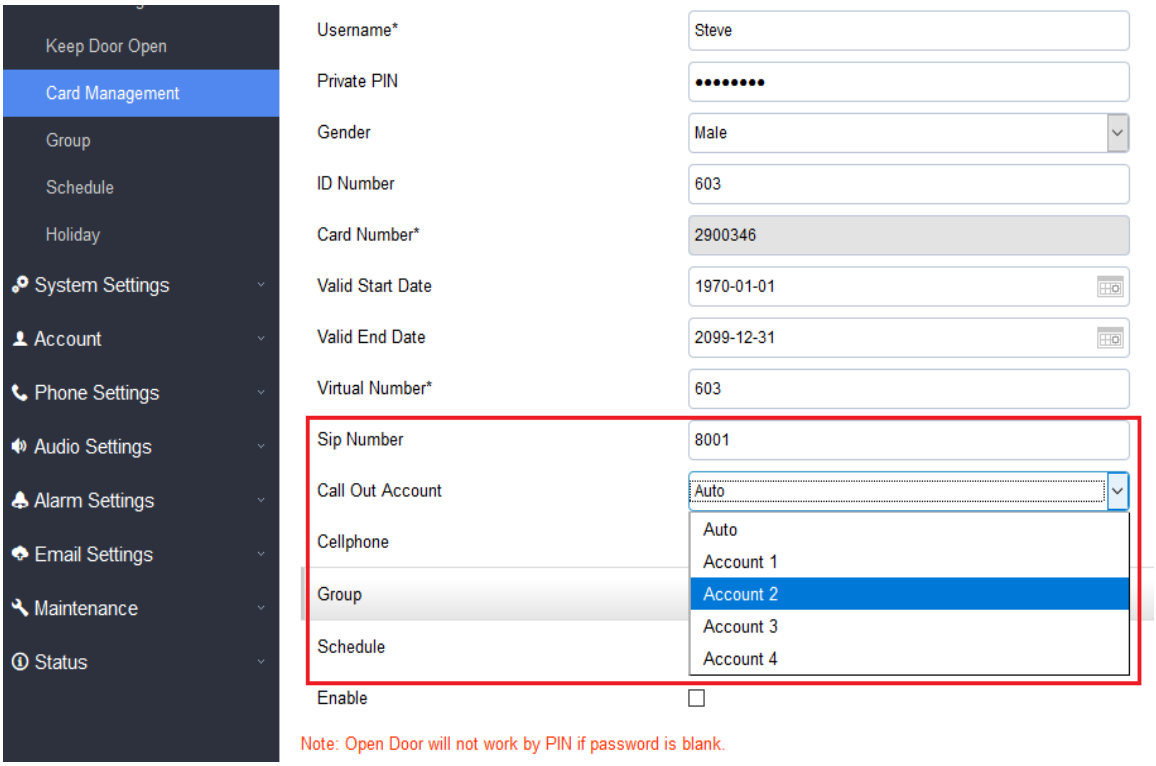


4) SIP Call:

Similar to "Virtual # Call", first configured in "Basic Settings" by choose "Call Mode" to be "SIP Number" (default setting) like below:



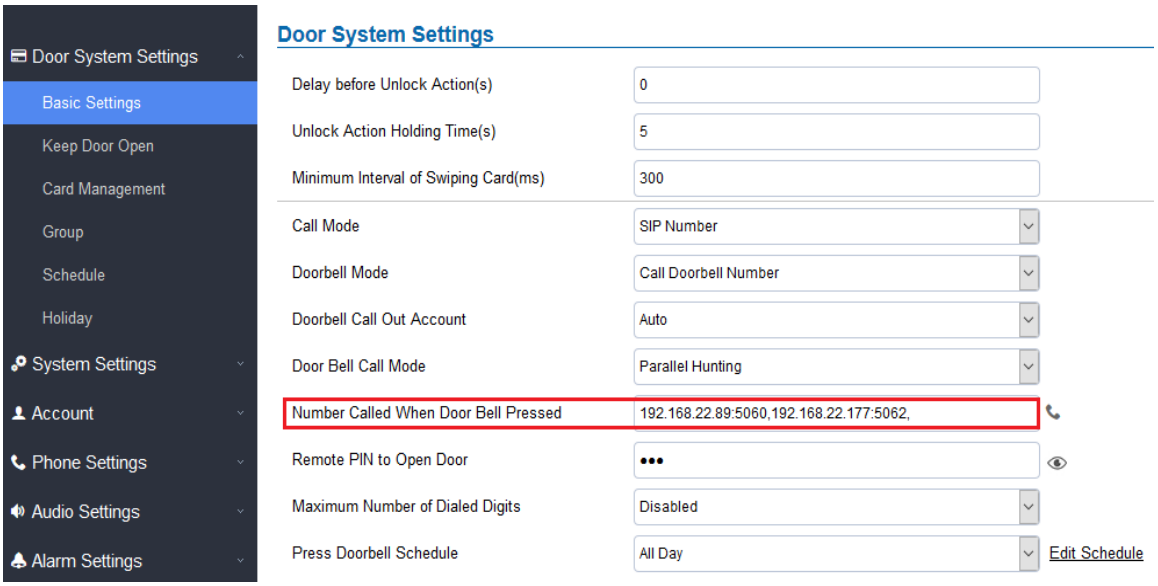
If the SIP extension has been configured in the "Card Management" page, then the call will send out using the account configured; if the SIP extension has not been configured in the "Card management" page, then default "Auto" will be used and call will send out via fist available registered SIP account.


Keep Door Open
Card Management
Group
Schedule
Holiday
System Settings
Account
Phone Settings
Audio Settings
Alarm Settings
Email Settings
Maintenance
Status
Username*
Steve
Private PIN
Gender
Male
ID Number
603
Card Number*
2900346
Valid Start Date
1970-01-01
Valid End Date
2099-12-31
Virtual Number*
603
Sip Number
8001
Call Out Account
Auto
Auto
Account 1
Account 2
Account 3
Account 4
Cellphone
Group
Schedule
Enable
Note: Open Door will not work by PIN if password is blank.

5) **Direct IP Call:**

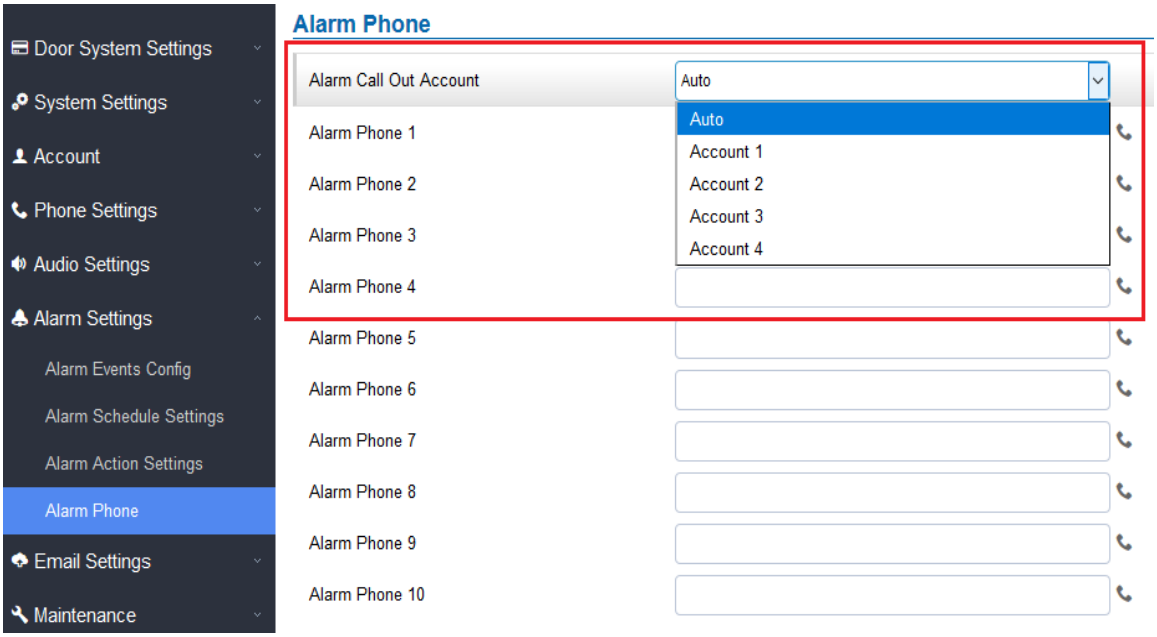
The “Direct IP Call” by default will always use “Account 1” to call out, using default port 5060. If different port or account used in the device at callee, it has to be configured according to ring at the correct port. For “Direct IP Call” the “User Random Port” has to be DISABLED in the device as callee.

By default “Enable Direct IP Call” is enabled in the “Phone Settings” of GDS.

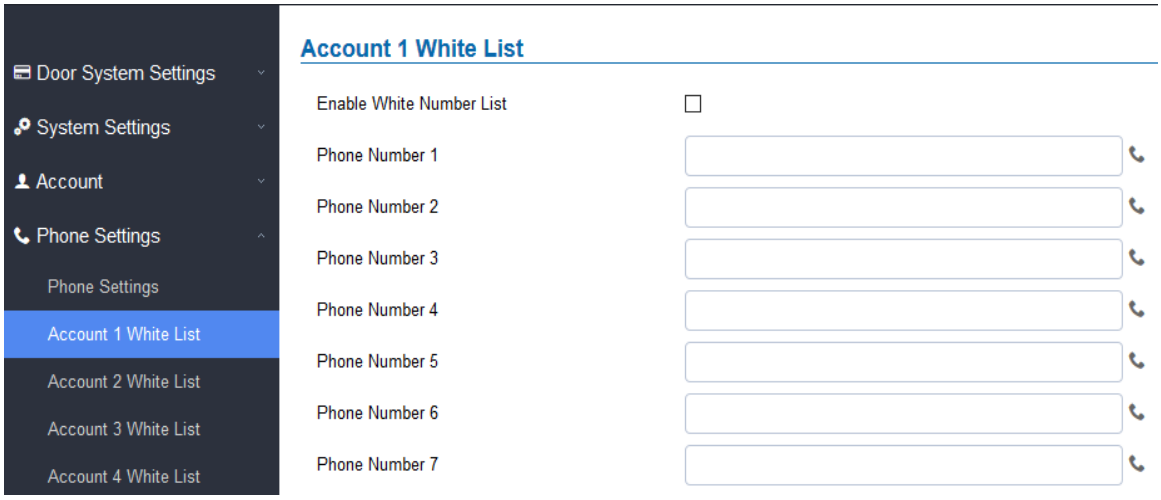


6) **Alarm Call:**

Alarm Call account selection can be configured in “Alarm Settings” by selecting “Alarm Phone” like below. The call out function is similar to doorbell call out function. If configured as “Auto”, the GDS will check all the 4 accounts registered and call out using 1st available registered account. Normally it will be configured to use particular account to call.



The “White List” configuration is under “Phone Settings” by choosing different SIP account configured.



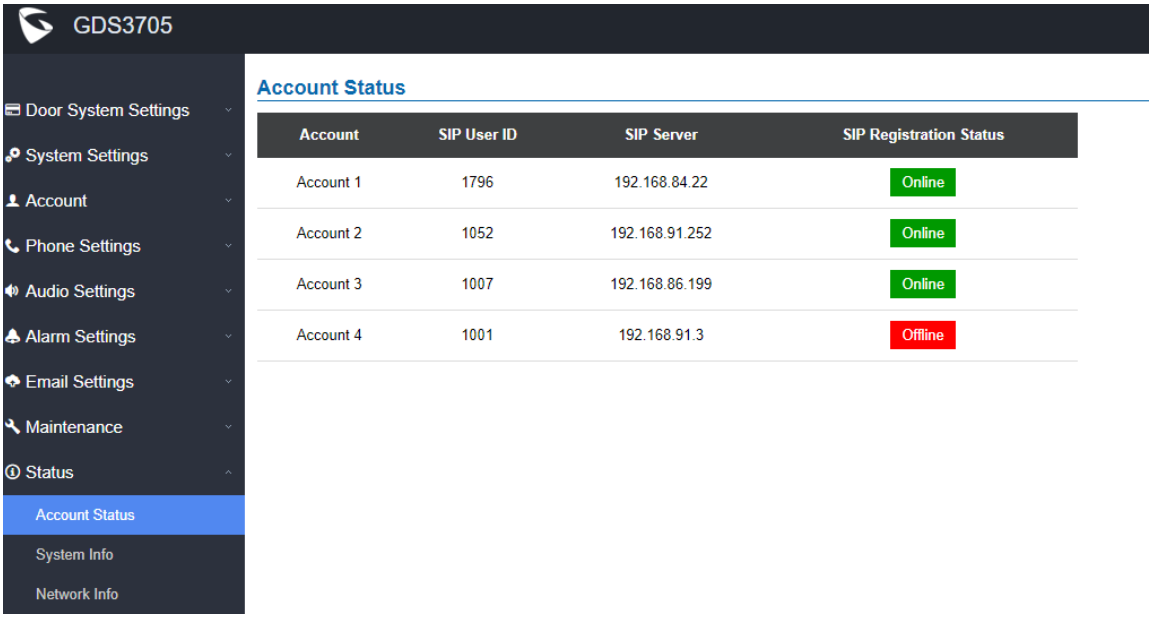
More detailed information, please refer to the User Manual of GDS37xx series, which can be found from Grandstream website:

http://www.grandstream.com/products/physical-security/facility-access-systems

- **Multiple SIP Account Call Functions**

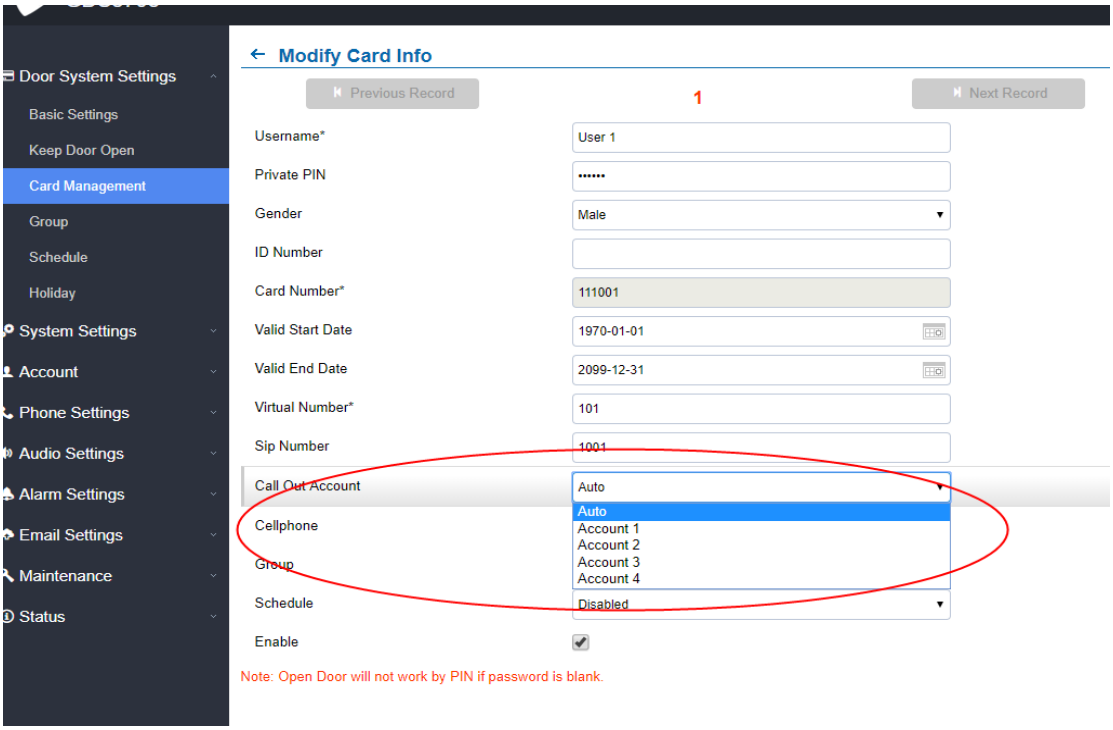
1) SIP Registration:

The 4 SIP accounts can be configured independently to work without interfering each other.



2) GDS as Caller (Virtual # Mode)

The related "Virtual #" and "Account" can be configured in the "Card Management" page. "Auto" means polling from account 1 to 4 using already registered account to call and fist available registered SIP account will be used.



The “Virtual #” is actually the “Speed Dial”. In above screenshot, virtual number “101” is speed dial shortcut for SIP number “1001”. When user dial “101”, the GDS will actually use the account configured in the “Card Management” page to call out. If user dial “101#”, GDS will call out via SIP number “1001” using related account.

For example, in a multi-tenant building, “virtual number” can be configured using the building room number, while actually “SIP number” can be mapped to different SIP Proxy using related SIP extension number(s).

3) **GDS as Caller (SIP Mode)**

When configured in this mode, the GDS will automatically choose from Account 1 to 4 and use the first available registered account to call out.

4) **GDS as Caller (Alarm Call)**

“Alarm Call” will use configured “Auto” or selected account to call out. If set to “Auto”, will use the first available successful registered proxy to call out.

5) **GDS as Callee (Auto Answer)**

The 1st incoming call will be answered automatically by default.

GDS3705 ONLY support one call at a particular time.

GDS3710 when enabled multiple call (maximum 4 calls simultaneously), digits “1”, “2”, “3” and “4’ are used to switch among different calls.

6) **Doorbell Call**

Support pre-configured calling number, maximum support 10 numbers.

7) **White List**

The “White List” under different SIP account is working independently.

FIRMWARE VERSION 1.0.0.31

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

08/06/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and enhancement since $1 Beta.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed device reboot after event alarm.
- Fixed device keep repeating registration.
- Fixed immediately Open Door issue when DST enabled.
- Fixed STUN process error.
- Fixed UI phone icon still showing “system busy” after the call.
- Fixed the key light not bright issue when using HTTP API to open door.
- Fixed SSH connection unauthorized after reboot when using static IP.
- Fixed “Expired Timer” in “Card Issuing Mode” cannot be saved.
- Fixed reboot issue when data exchanging with UCM.
- Fixed device cannot output key information when used as Wiegand output device.
- Fixed when configured SIP Alarm and Sound Alarm but continuously trigger alarms, the alarm sometime not sound but play door bell tone.

ENHANCEMENT

- Synchronization SRTP configuration UI with GDS3710, added “Enable but Not Forced; Enable and Forced” option.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side

NEW HTTP API/P-VALUE

- N/A

FIRMWARE VERSION 1.0.0.28

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A, 1.4B**)*

DATE

06/19/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and enhancement since $1 Beta.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version
GDS3705 HW1.4B	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed Import data exception.
- Fixed Wiegand as output device open door issue.
- Fixed Chime ring issue when Hostage Code Call Enabled.
- Fixed DNS analysis problem.
- Fixed the Valid Start Date input limit issue.
- Fixed "," in the group name causing UI display abnormal.
- Fixed ringing timeout set to "0" causes call failing to initiate.
- Fixed doorbell call failure if using IP peering but with no default port.

ENHANCEMENT

- Added HTTP Command to Open Door.
- Added 3CX compatibility features (e.g.: server side controlled UI automatic login)
- Added Optional Notification for out of schedule accessing attempts.
- Added Test Button for Alarm Action.
- Added missing Log Notification Type (Reboot/Reset/ConfigUpdate).

- Added Schedule Open Door Feature.
- Synchronized phone library with GXP phones with latest firmware.
- Added verification when importing configuration from UI.
- Added displaying SN number in the system information page.
- Added reboot protective schema when downloading interrupted or failed during upgrade process.

KNOWN ISSUES

- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- GDS Keypad input as Wiegand output still not working yet.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side

NEW HTTP API/P-VALUE

<parameter>=<value>	Page	Values	Comments
type=<string>	**Keep Door Open**	**sch_open_door**	**Get Keep Door Open Configs**
P15429=<int>	Keep Door Open	0,1,2	Keep Door Open Type
P15211 =<string>	Keep Door Open		Valid Schedule Start Time
P15212 =<string>	Keep Door Open		Valid Schedule End Time
P15213=<string>	Keep Door Open		Schedule
P15430=<int>	Keep Door Open	5-480	Interval of Keep Door Open(min)
P15424=<int>	Door System Basic Setting	0,1	Enable HTTP API Remote Open Door
test_alarm_action=< int >	**Alarm Action Settings**	**1-10**	**Test for Alarm action**
P15407=<int>		0,1	Enable Non-scheduled Access Alarm
P15408=<int>		1-10	Non-scheduled Access Alarm Profile

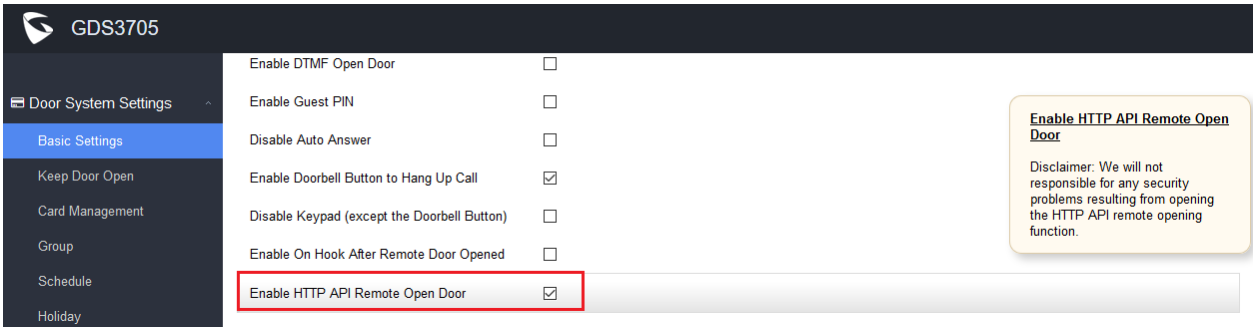
NEW FEATURES OVERVIEW

This section lists major new features and describes how to use it from the user's point of view.

HTTP API OPEN DOOR

- **Web Configuration**

New feature added and this option can be found under device web UI→Door System Settings → Basic Settings page like below:



- **Functionality**

This feature allow 3rd party system integrators to do 2nd stage development based on provided HTTP API. Once enabled, door can be remotely opened by customers who running some scripts from HTTP Server to remotely control the opening of the door.

- **New P-Value**

P-Value	Values	Default Value	Comments
P15424=<int>	Door System Basic Setting	0,1	Enable HTTP API Remote Open Door

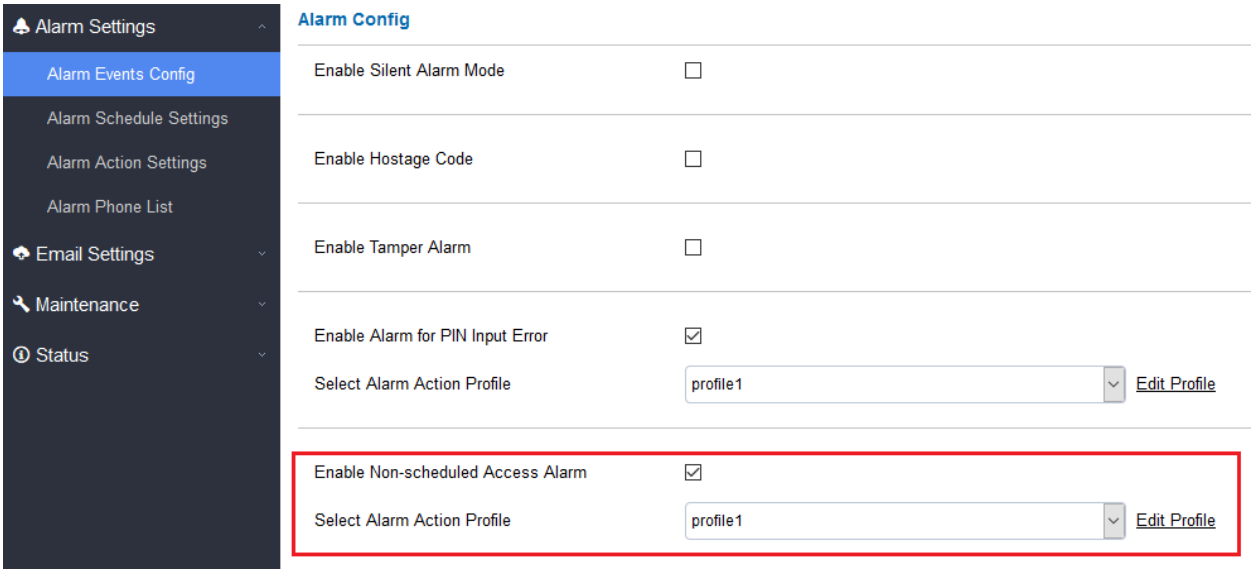
More detailed information, please refer to latest HTTP API documentation for GDS37xx series, which can be found from Grandstream website:

http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

NON-SCHEDULED ACCESS ALARM

- **Web Configuration**

This page can be found under “Alarm Settings” → “Alarm Events Config”



- **Functionality**

By default this feature is disabled. When configured and enabled, this feature will allow related building or office managers aware the abnormal activities when legitimated users access the door out of the allowed configured schedule. For example, entry during weekend or night at not working hours.

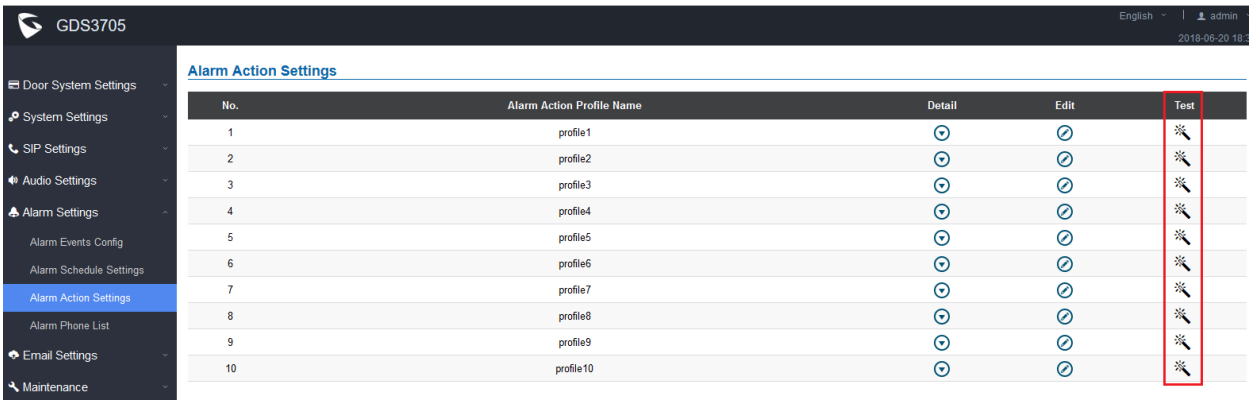
- **New Pvalue**

P-Value	Values	Default Value	Comments
P15408	1~10	1	Non-scheduled Access Alarm Action Profile

"TEST" BUTTON IN ALARM ACTION

- **Web Configuration**

This option can be found under device web UI "Alarm Settings" → Alarm Action Settings



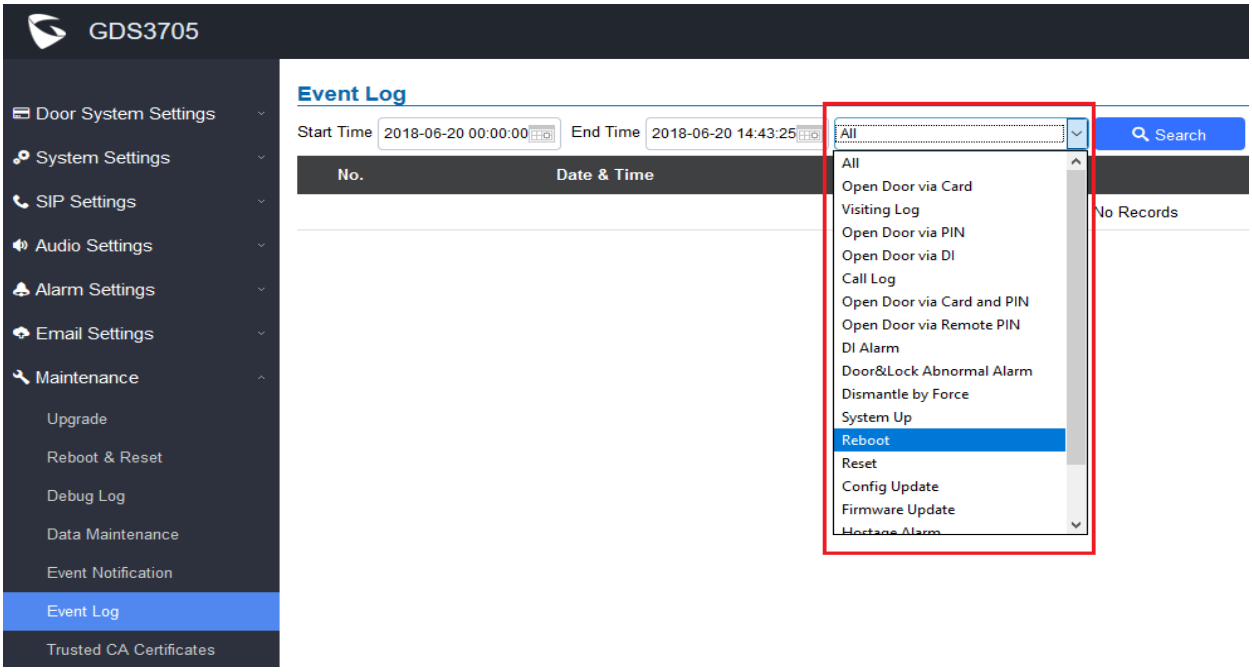
- **Functionality**

New feature added to allow use to click the "Test" button in the UI to test whether the configured Alarm Action working as expected during the configuration stage.

LOG NOTIFICATION TYPE

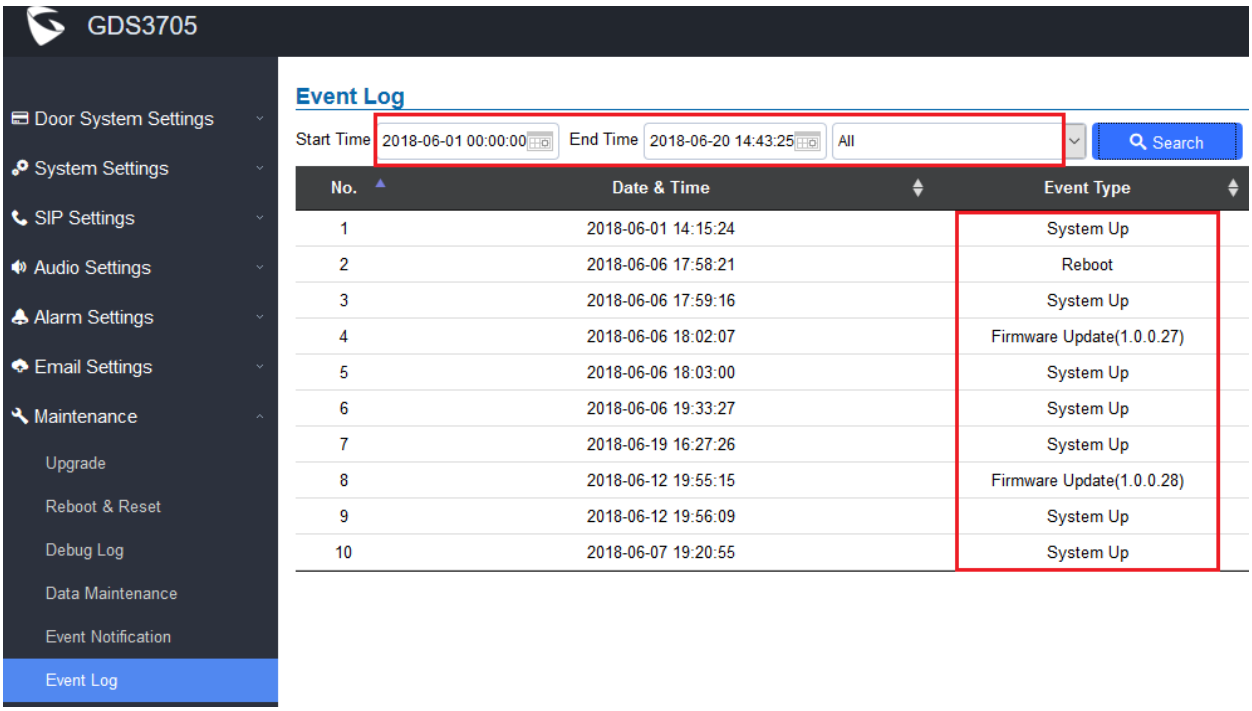
- **Web Configuration**

This page can be found under “Maintenance” → Event Log



- **Functionality**

Improved this feature to allow users or system administrator to search and display the related system logs in the webUI to understand the device operation history. See below example:

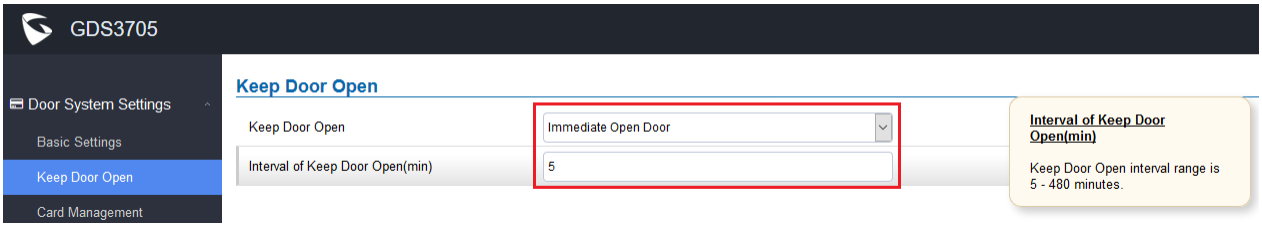


OPEN DOOR BY CONFIGURED SCHEDULE OR TIME WINDOW

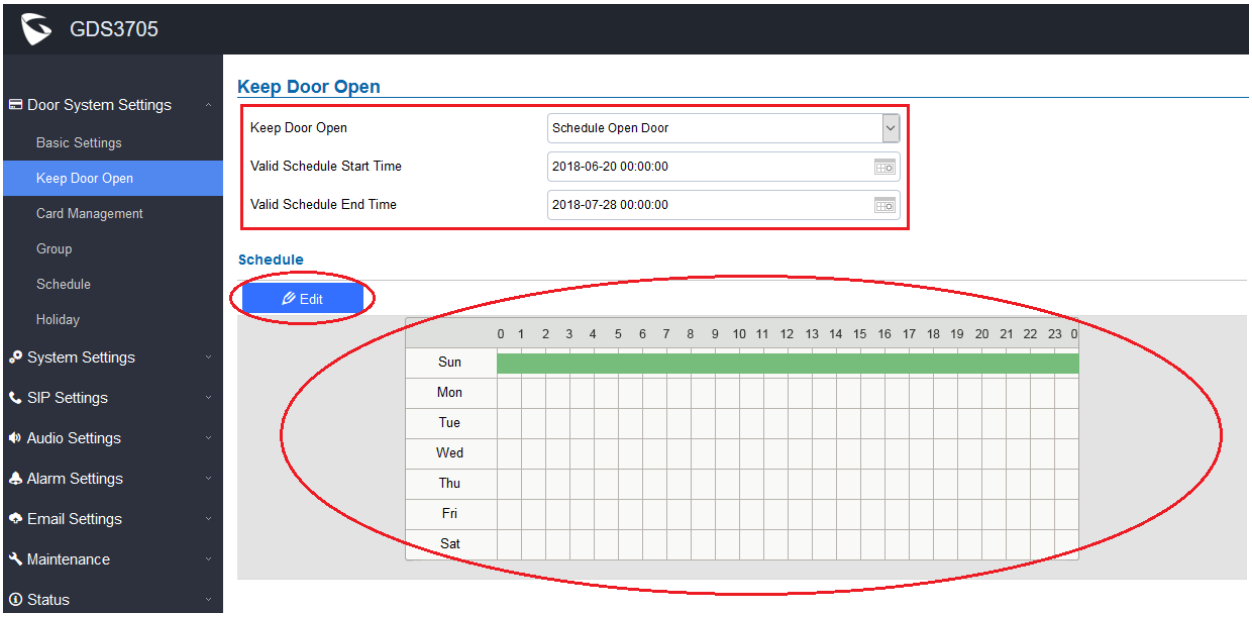
- **Web Configuration**

This option can be found under device web UI→ Door System Settings → Keep Door Open:
There are two modes:

1. Immediate Open Door (One Time Only Action)



2. Schedule Open Door (Repeated Action)



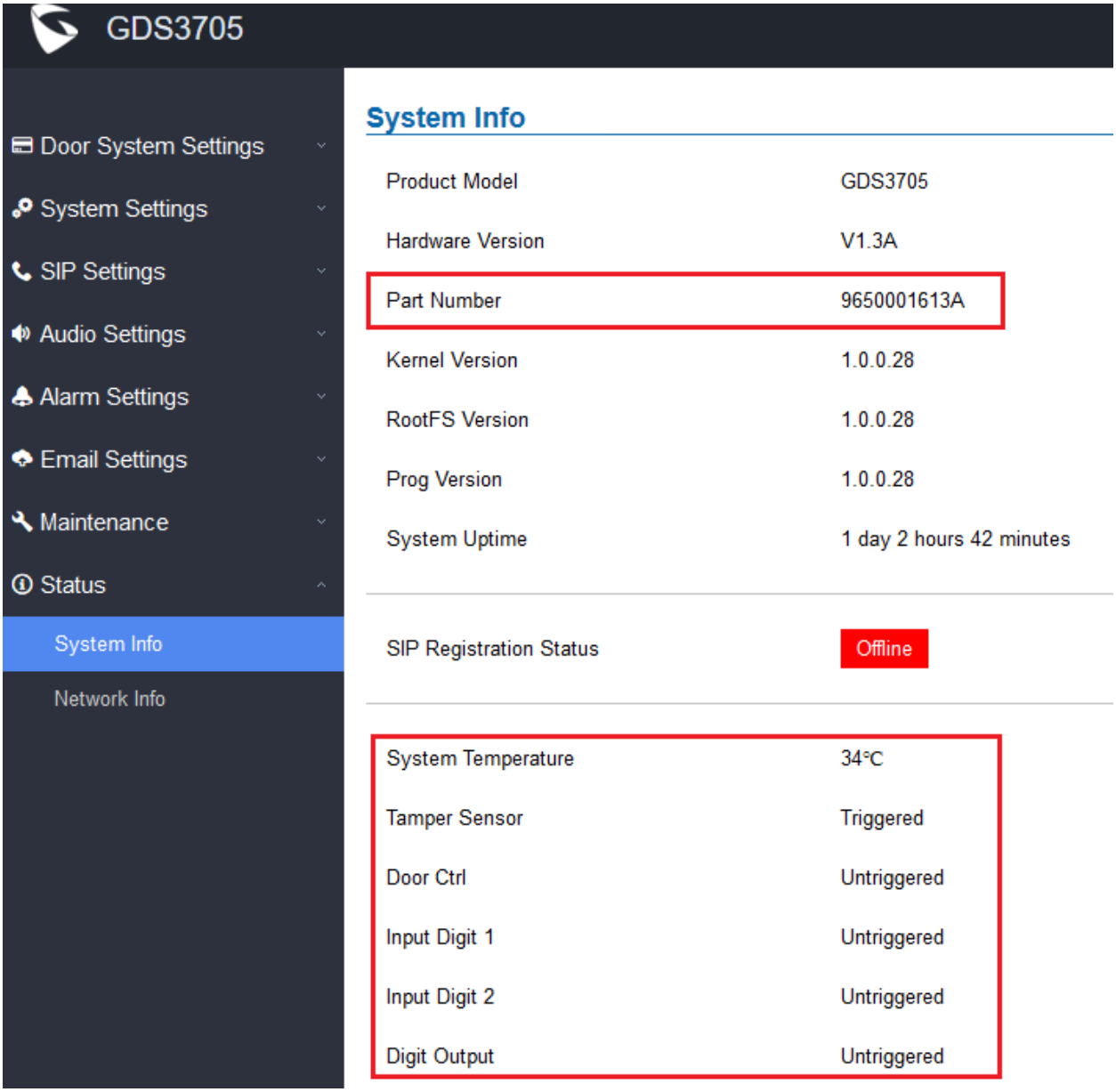
- **Functionality**

By default this feature is disabled. This feature when enabled will allow usage scene like schools or similar private or public places where the door needs to keep open at specific time window but closed otherwise. Also good for buildings or properties where a party or seminar need to be hosted for some period of time in a day (the door keeps open) then back to locked with authorized entry after that. Also good for lunch breaks in a factory or company where door open and no access log required.

MORE INFORMAITON IN SYSTEM INFO PAGE

- **Web Configuration**

This option can be found under device web UI "Status" → System Info



- **Functionality**

New feature added to allow use and system administrator to view more live operation information of GDS3705 device.

FIRMWARE VERSION 1.0.0.26

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A**)*

DATE

04/26/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and enhancement for $1 Beta.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed Door Chime still plays after call answered.
- Fixed BagRep. Kiev (capital of Ukraine) missing in time zone list.
- Fixed wrong log date for Wiegand reset.
- Fixed callee hang up the device still playing tone continuously.
- Fixed when ringing timeout set to “0” call cannot be initiated.
- Fixed WebGUI limitation for Alarm Phone List and White List is not applied to P value import files and no error report generated when limitation overflow during the file import or restore.
- Fixed log failed to get version number if there is power outage during upgrade process. (**Please avoid power and network outage during firmware upgrade process!**)

ENHANCEMENT

- Added displaying logs at device’s webUI.
- Added ability to disable certificate validation.
- Added log record for system Up/Reboot/Reset/ConfigUpdate/FirmwareUpdate.
- Added support for uploading Trusted CA Certificates.
- Optimized socket/fd close.
- Changed MAC address to lowercase in exported data.

- Added Factory Function for Audio Loopback and Certificate Verification.
- Improved if firmware upgrade happened during a call, the other processes will not exit until call end. (**not recommend** doing firmware upgrade during a call, **suggest** doing upgrade when device idle)
- Separate configuration parameters for firmware upgrade and configuration provisioning.
- Added Event Notification support for self-define URL Template, HTTPS and FQDN.
- Improved the style of Form Element.
- Added Valid Start/End Date for RFID Card for management convenience.
- Improved “Password Recovery Email” configuration and check validation based on feedback.

KNOWN ISSUES

- Zero Config Feature with UCM is not yet implemented.
- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Dual Mic function is invalid.
- When doorbell volume set to 0 still hearing the ring back tone.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- GDS Keypad input as Wiegand output still not working yet.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side

NEW P-VALUE

P-Value	Values	Default Value	Comments
P6767	1- HTTP; 2- HTTPS	1	Firmware Upgrade Via Type
P6768	<string> Max.length=512		Firmware Upgrade HTTP/HTTPS User Name
P6769	<string> Max.length=512		Firmware Upgrade HTTP/HTTPS Password
P8463	0 - Disable; 1 - Enable	0	Validate Server Certificates
P8433-P8438	<string> Max.length=4096		Trusted CA Certificates Files
P15416	<string> Max.length=1024	{"mac":"${MAC}","content":"${WARNING_MSG}"}	Event Notification URL Template
P15417	1- HTTP; 2- HTTPS	1	Event Notification Via Type

NEW HTTP API

<parameter>=<value>	Page	Values	Comments
P6767=<int>	Upgrade	1,2	Firmware Upgrade Via Type
P6768=< string >	Upgrade	string	Firmware Upgrade HTTP/HTTPS User Name
P6769=< string >	Upgrade	string	Firmware Upgrade HTTP/HTTPS Password
P8463=<int>	Upgrade	0,1	Validate Server Certificates
type=<string>	Trusted CA Certificates	trustedca	Get Trusted CA Certificates info
P8433-P8438=< string >	Trusted CA Certificates	string	Trusted CA Certificates Files
type=<string>	eventlog	eventlog	Get event log
Eventtype=<int>	eventlog	100-1408	Query event type
Logstartdate=<int>	eventlog		Query event log start date e.g. 20180330 - 2018-03-30
logenddate=<int>	eventlog		Query event log end date e.g. 20180330 - 2018-03-30
Logstarttime=<int>	eventlog		Query event log start time e.g. 121110 - 12:11:10
logendtime=<int>	eventlog		Query event log end time e.g. 121110 - 12:11:10
type=<sting>	Factory Functions	factfun	Get Factory Functions info
audiolb=<int>	Factory Functions	0,1	Audio Loopback Test: 1 – stop; 0 - start
P15416=< string >	Event Notification		Event Notification URL Template
P15417=< int >	Event Notification	1,2	Event Notification Via Type

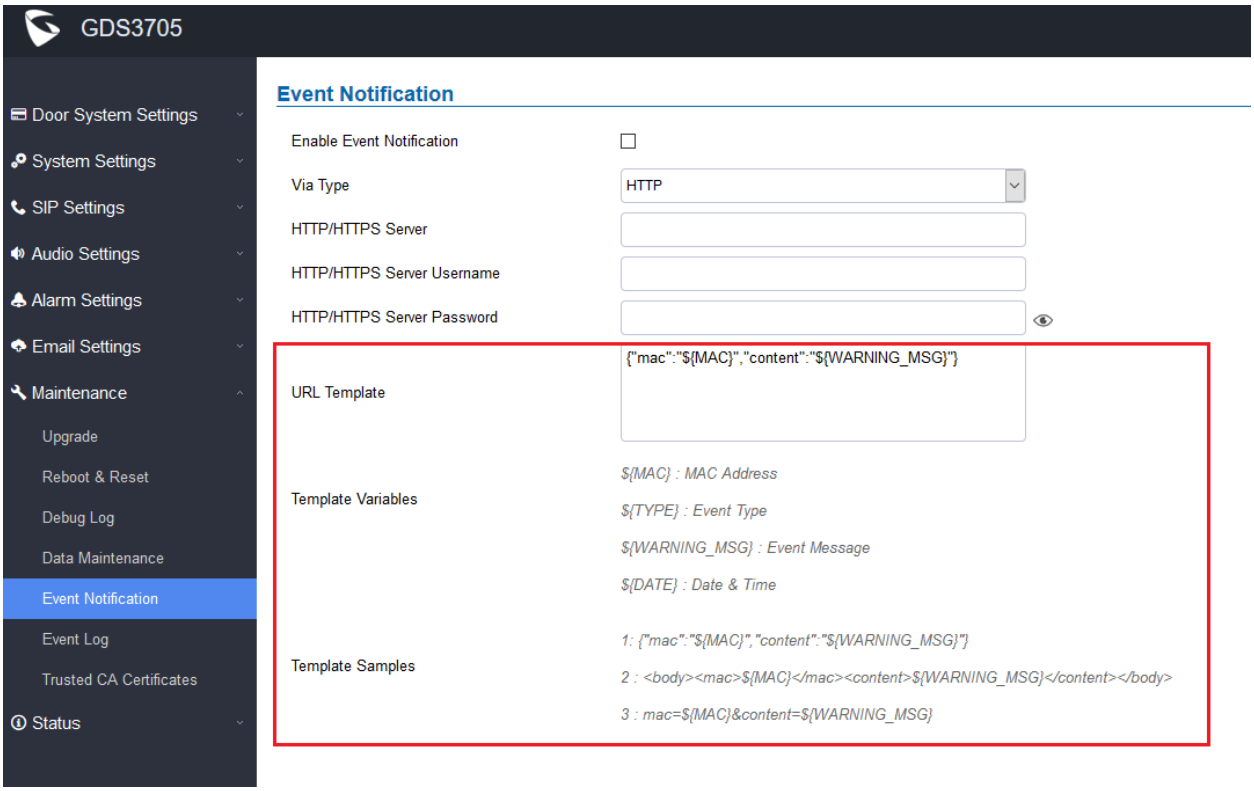
NEW FEATURES OVERVIEW

This section lists major new features and describes how to use it from the user's point of view.

EVENT NOTIFICATION

- **Web Configuration**

New feature added and this option can be found under device web UI→Maintenance →Event Notification.



- **Functionality**

This feature allow 3rd party HTTP Server to collect event notification lively from GDS3705. Server URL, Username and Password are required to authenticate the operation. Also 3rd party can use template to collect the operation status of the device, used for cloud solution.

- **New P-Value**

P-Value	Values	Default Value	Comments
P6767	1- HTTP; 2- HTTPS	1	Firmware Upgrade Via Type
P6768	<string> Max.length=512		Firmware Upgrade HTTP/HTTPS User Name
P6769	<string> Max.length=512		Firmware Upgrade HTTP/HTTPS Password

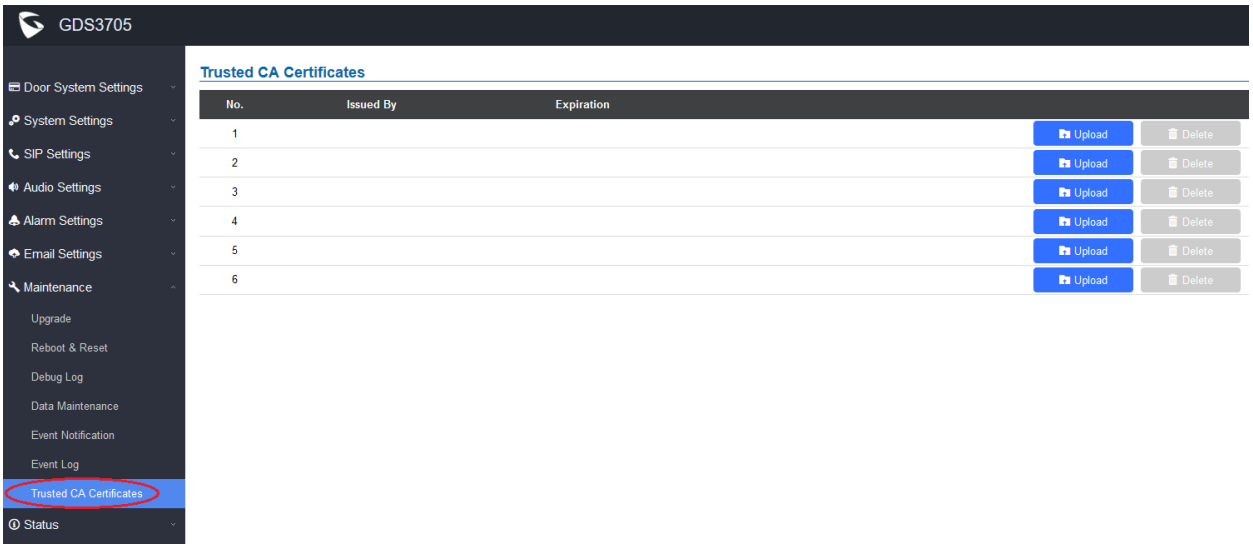
P8463	0 - Disable; 1 - Enable	0	Validate Server Certificates
P8433-P8438	<string> Max.length=4096		Trusted CA Certificates Files
P15416	<string> Max.length=1024	{"mac":"${MAC}","content":"${WARNING_MSG}"}	Event Notification URL Template
P15417	1- HTTP; 2- HTTPS	1	Event Notification Via Type

TRUSTED CA CERTIFICATES

- **Web Configuration**

Added “Upload” and “Delete” Trusted CA Certificates management.

This page can be found under “Maintenance” → Trusted CA Certificates



- **Functionality**

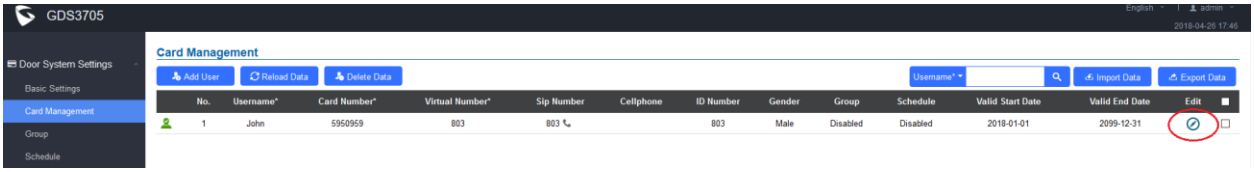
This feature allow the management of Trusted CA Certificates.

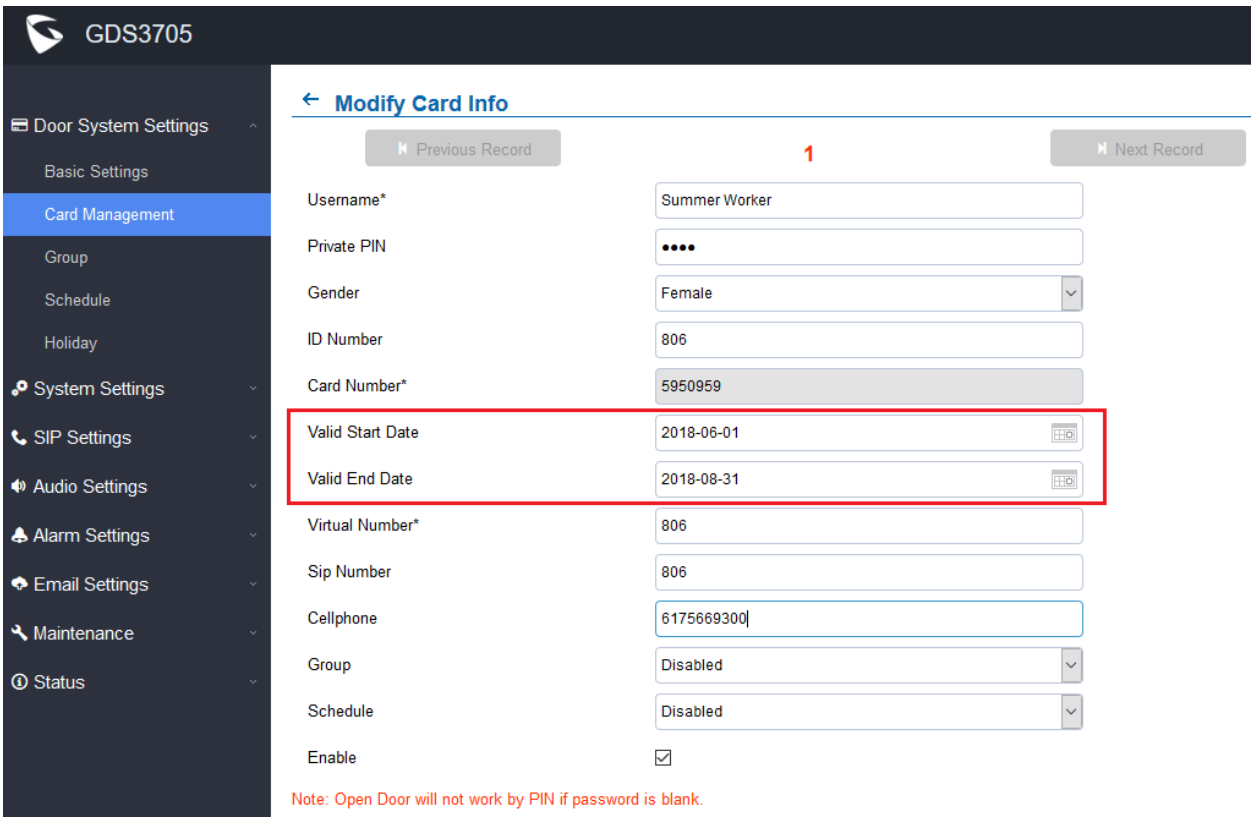
CARD MANAGEMENT – Valid Start/End Date for Card/User

- **Web Configuration**

New feature added the configuration of Start and End Date of the Card/User, implemented based of customer feedback. This helps the management and maintenance task of daily access system.

This option can be found under device web UI "Door System Settings" → Card Management → Click "Edit" to modify each Card/User.





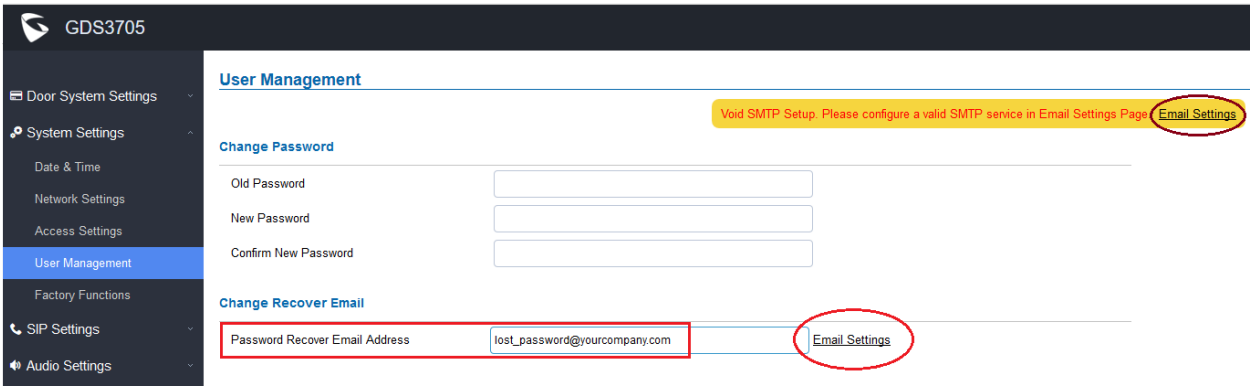
- **Functionality**

This helps the management and maintenance task of daily access system.
For example, customer can pre-configure the date of the cards for new employees or temporary seasoning workers and send out the cards before new employees coming to work.

PASSWORD RECOVER EMAIL CONFIGURATION

- **Web Configuration**

This page can be found under “System Settings” → User Management



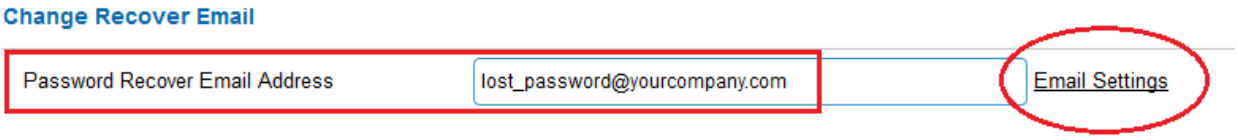
- **Functionality**

Improved this feature layout based on feedback. For security consideration, this device does not have hard reset key therefore administration password is very important. “Password Recover Email” is designed for user who lost password, but that has to be configured correctly before this can start function. Also whenever user changing the administrator password, this will also kick in to prompt user to configure the recover email. There are two pages involved this configuration or settings:

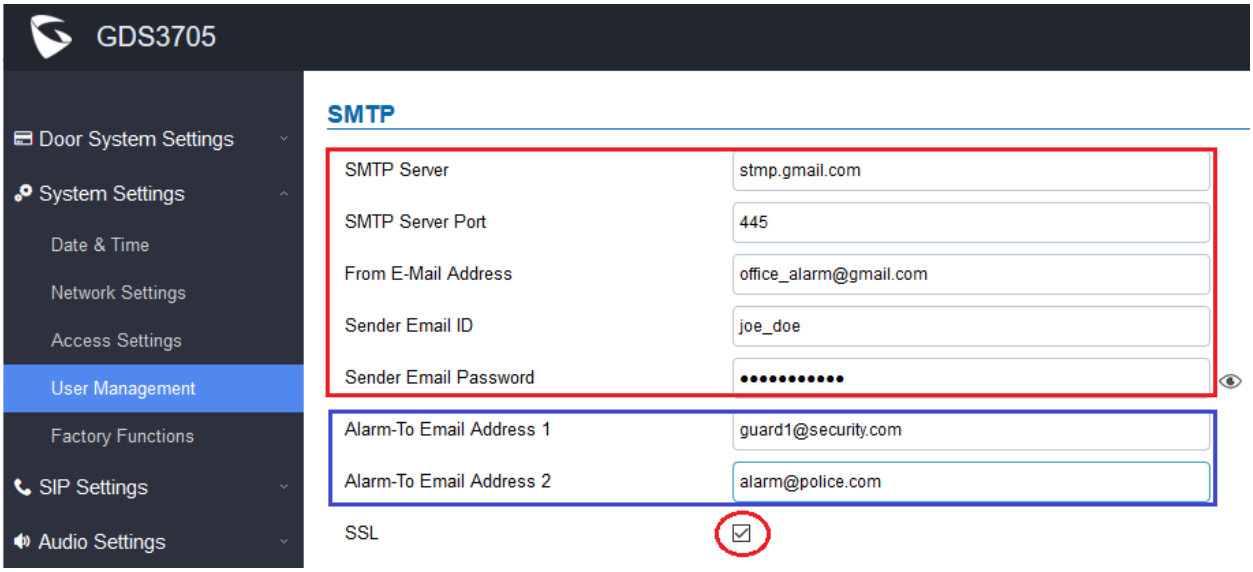
1) **User Management Page:**

As see in above screenshot, whenever change administrator password but SMTP setting is not configured, the “Void SMTP Setup. Please configure a valid SMTP service in Email Setting Page!” will prompt up, reminding user to setup the correct SMTP service.

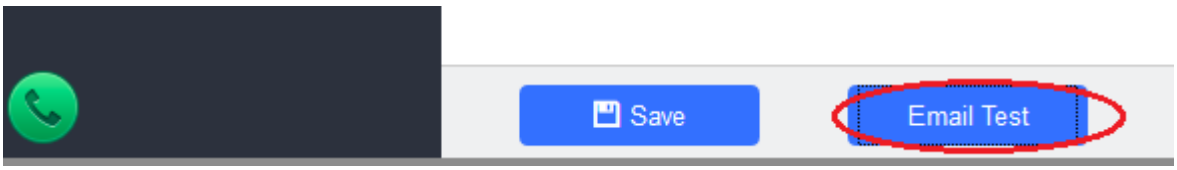
Users are strongly suggested to configure the “Password Recover Email Address”, similar to below:

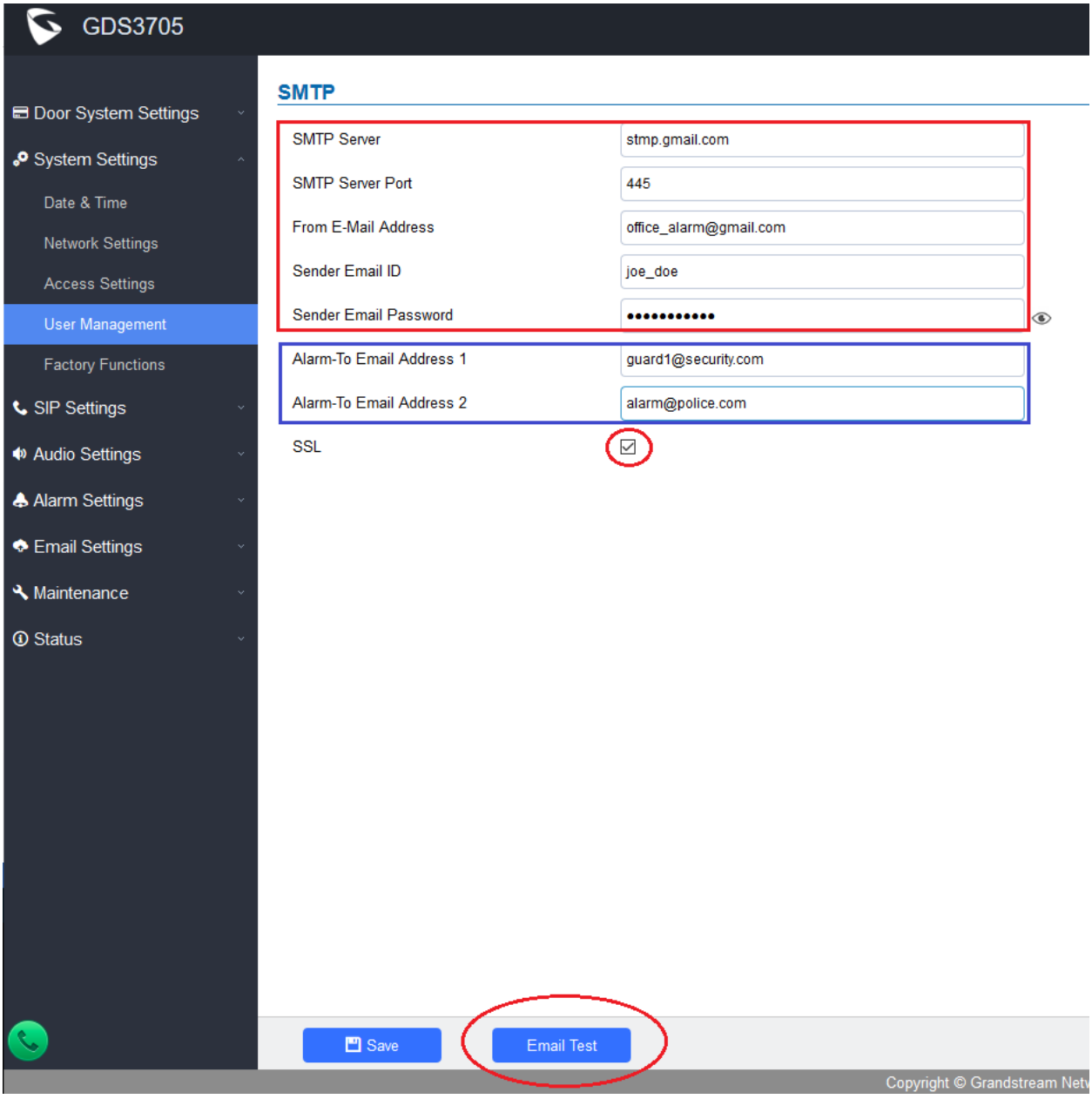


There are two “Email Settings” in the page, click any of them will be directed to following screen:

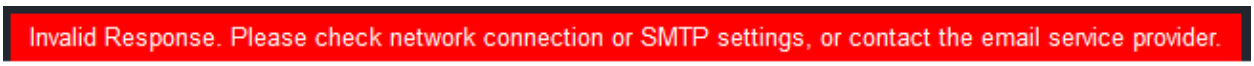


Once configured, user can click the “Email Test” button located at the bottom of this configuration page to test the validation of the configuration:



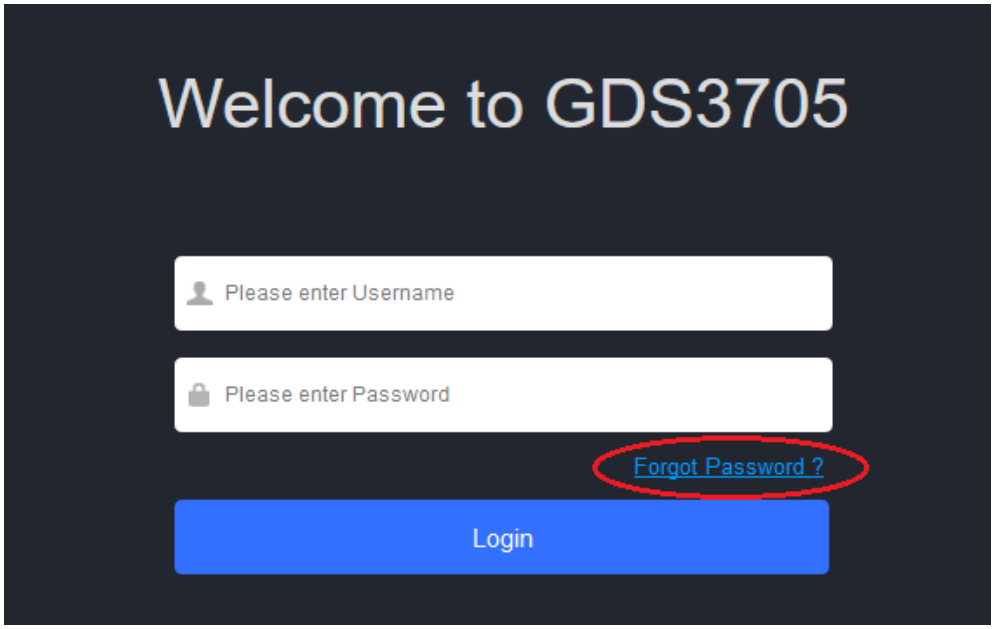


If the configuration is incorrect, following prompt will be displayed on screen:

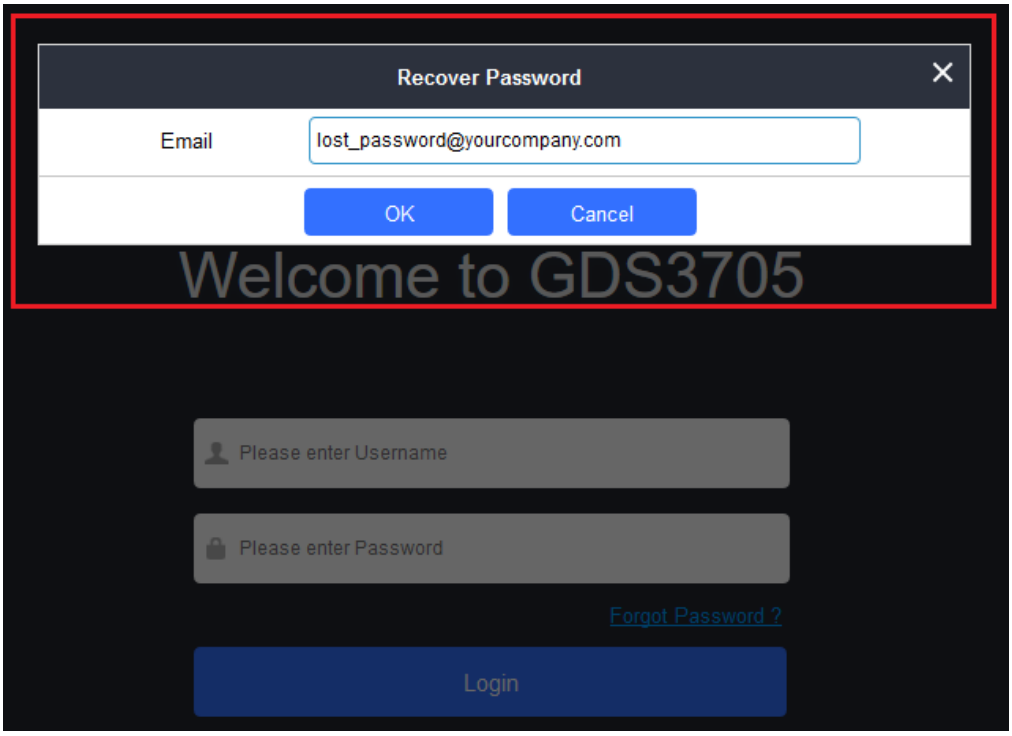


2) Login Page

At the login page, there is a link showing “Forgot Password ?”



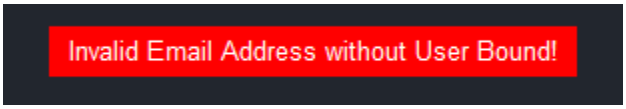
Click the link will pop up the following page to ask input the “Email Address” for the Recover Password to be sent to:



If the “Password Recover Email Address” and related SMTP is configured correctly, then click the “OK”

button the device will email the administrator password to the inputted email address, if the email address entered matches the pre-configured “Password Recover Email Address” inside the device and the device with working SMTP service configured.

Otherwise the device will prompt the following message at top of the UI page to advise user to configure the related parameters or service, to make this feature working. User can still click “Cancel” to omit these setting and continue the UI operation but this is bad operation behavior.



Grandstream strongly suggest user to configure a working email address as “Password Recover Email Address” and also configure a good SMTP service to the device. So if something happened, the administrator could get the password recover email to unlock the device.

Also with a working SMTP service configured, alarm emails can also be sent out. Snapshots of Alarm or snapshot when doorbell pressed can also be sent out as email attachment via the configured SMTP service to related receivers.

FIRMWARE VERSION 1.0.0.23

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A**)*

DATE

03/26/2018

SUMMARY OF UPDATE

The main purpose of this release is bug fix and enhancement for $1 Beta.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Dingdong door bell sound delayed playing out quite a lot comparing to GDS3710
- Fixed SIP number search not support “IP+Port” type
- Fixed without receiver, click “Test” and “Save” still show mail test successful
- Fixed doorbell sticky key (triggered twice) caused the initialized call hanging up
- Fixed enable Hostage Code the doorbell sound still played
- Fixed enable Silent Alarm Mode the doorbell sound still played
- Fixed Wiegand card open door the log information without card number

ENHANCEMENT

- Added UI showing Temperature/TamperSensor/DoorControl/DI/DO in the System Info Page
- Enhanced HTTP format to facilitate the 3rd party parsing Event Notification

KNOWN ISSUES

- Zero Config Feature with UCM is not yet implemented.
- When doorbell volume set to 0 still hearing the ring back tone.
- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.

- Dual Mic function is invalid.
- GDS Keypad input as Wiegand output still not working yet.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side
- WebGUI limitation for Alarm Phone List and White List is not applied to P value import files and no error report generated when limitation overflow during the file import or restore.

NEW P-VALUE

P-Value	Values	Default Value	Comments
P15410	0- Disable 1- Enable	0	Enable Log Reporting
P15413	<string> Max.length=256		HTTP Server URL
P15414	<string> Max.length=128		HTTP Server Username
P15415	<string> Max.length=128		HTTP Server Password

NEW HTTP API

<parameter>=<value>	Page	Values	Comments
type=<string>	System info	sysinfo	Get all log sysinfo parameter
doorctrl=<int>	System info	0,1, -1	Door Ctrl status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
atp_in =<int>	System info	0,1, -1	TamperSensor status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
di0 =<int>	System info	0,1, -1	DI0 status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
di1 =<int>	System info	0,1, -1	DI1 status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
do =<int>	System info	0,1, -1	DO status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
systemp =<int>	System info	0,1, -1	System Temperature (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown

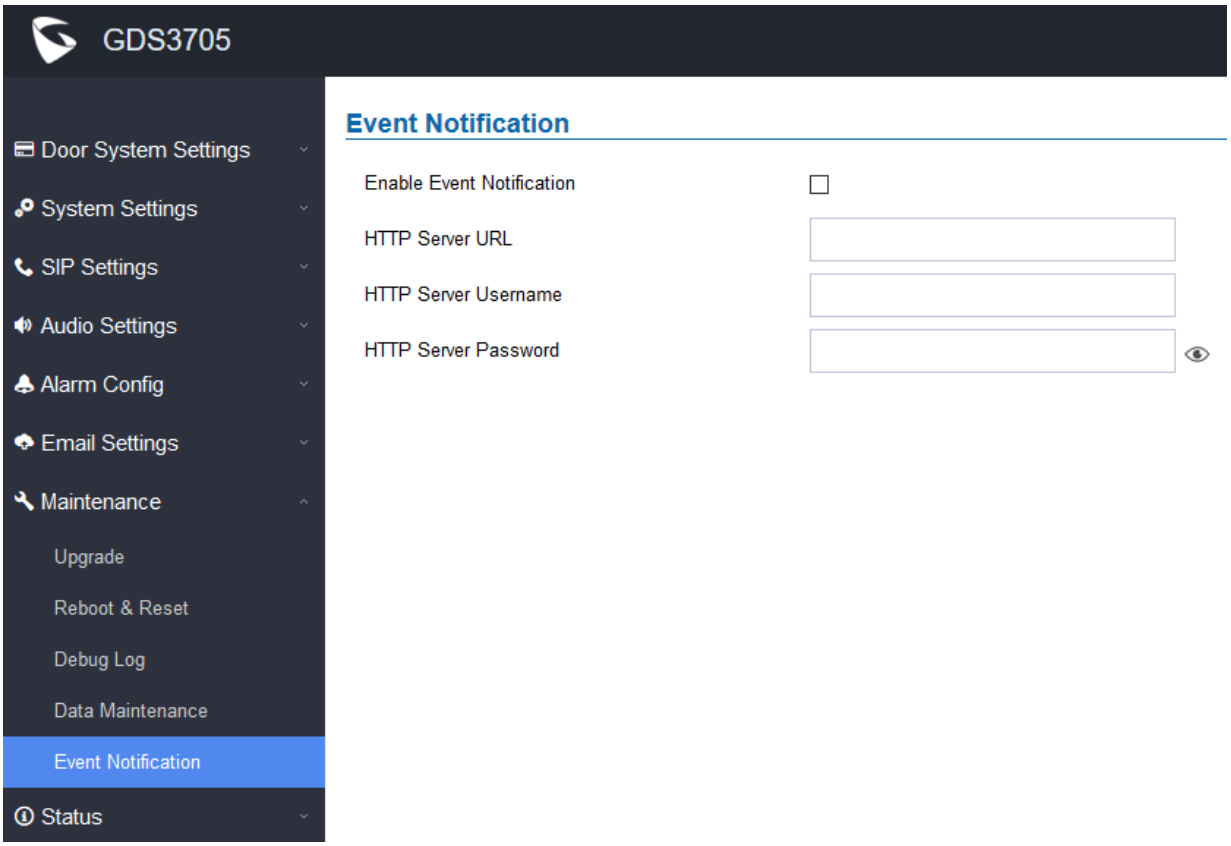
NEW FEATURES OVERVIEW

This section lists major new features and describes how to use it from the user's point of view.

EVENT NOTIFICATION

- **Web Configuration**

This option can be found under device web UI→Maintenance →Event Notification.



- **Functionality**

This feature allow 3rd party HTTP Server to collect event notification lively from GDS3705. Server URL, Username and Password are required to authenticate the operation.

- **New P-Value**

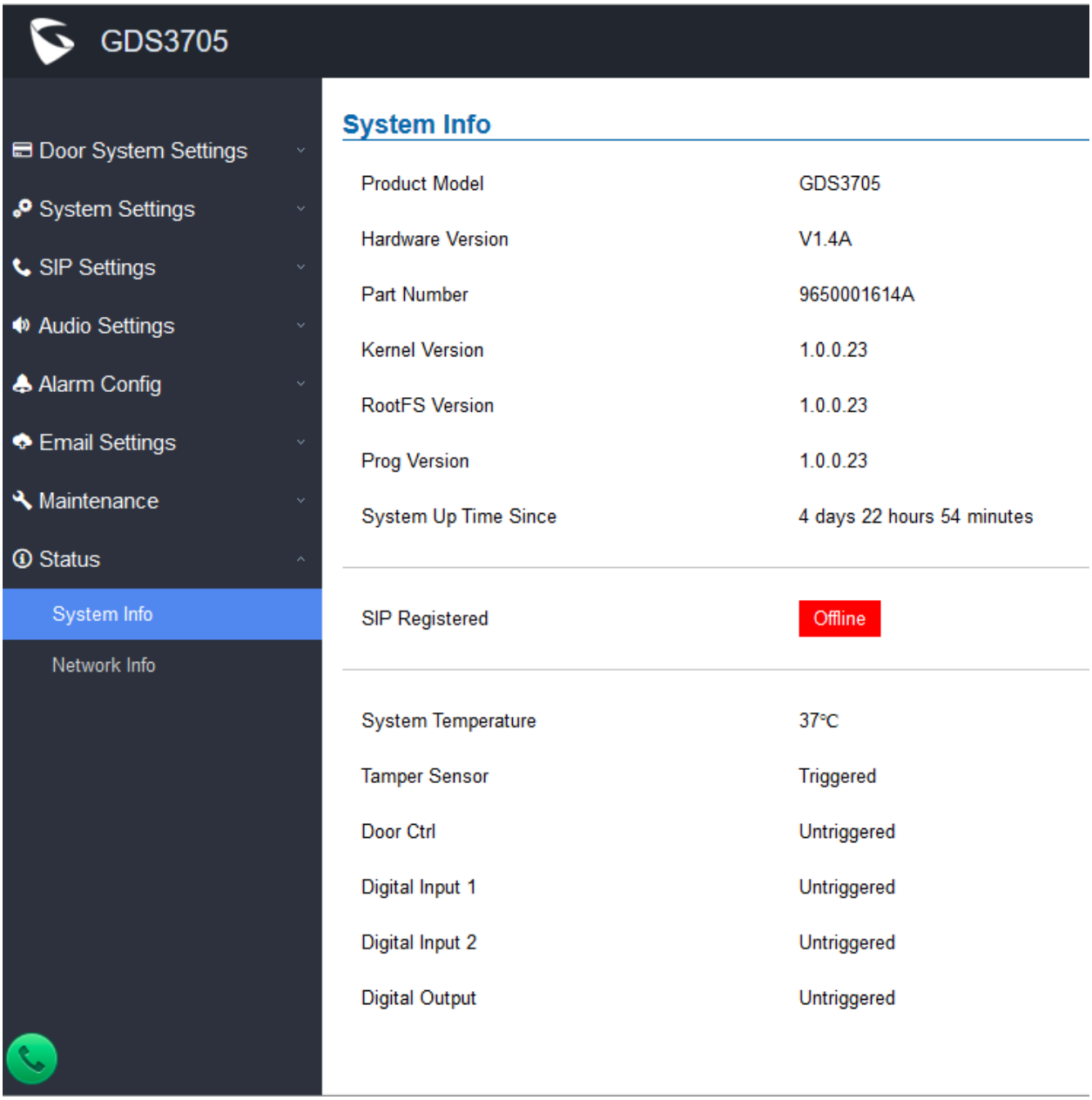
P-Value	Values	Default Value	Comments
P15410	0- Disable 1- Enable	0	Enable Log Reporting
P15413	<string> Max.length=256		HTTP Server URL
P15414	<string> Max.length=128		HTTP Server Username
P15415	<string> Max.length=128		HTTP Server Password

SYSTEM INFO

- **Web Configuration**

Added system information status for: *System Temperature, Tamper Sensor, Door Controller, Digital Input Interface 1, Digital Input Interface 2 and Digital Output*.

This page can be found under device web UI→ Status → System Info



- **Functionality**

This feature will notify user the operation status of GDS3705

- **New HTTP API**

<parameter>=<value>	Page	Values	Comments
type=<string>	System info	sysinfo	Get all log sysinfo parameter
doorctrl=<int>	System info	0,1, -1	Door Ctrl status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
atp_in =<int>	System info	0,1, -1	TamperSensor status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
di0 =<int>	System info	0,1, -1	DI0 status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
di1 =<int>	System info	0,1, -1	DI1 status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
do =<int>	System info	0,1, -1	DO status (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown
systemp =<int>	System info	0,1, -1	System Temperature (only get) 0 - Untriggered, 1 - Triggered, -1 - Unknown

FIRMWARE VERSION 1.0.0.20

PRODUCT NAME

GDS3705 *(HW Supported: **1.1A, 1.2A, 1.3A, 1.4A**)*

DATE

02/26/2018

SUMMARY OF UPDATE

Initial public release. The main purpose of this release is for $1 Beta.

FIRMWARE APPLIES TO BELOW HW VERSION ONLY

HW Version	FW	Comments
GDS3705 HW1.1A	YES	
GDS3705 HW1.2A	YES	
GDS3705 HW1.3A	YES	
GDS3705 HW1.4A	YES	FW1.0.0.20 as Initial Version for this HW version

BUG FIX

- Fixed alarm call no siren sound when enabled SRTP.

KNOWN ISSUES

- Zero Config Feature with UCM is not yet implemented.
- Dingdong door bell sound delayed playing out quite a lot comparing to GDS3710
- Continuously swiping invalid cards will sometime cause “pu” noise from speaker.
- When doorbell volume set to 0 still hearing the ring back tone.
- Playing Prompt Audio from Proxy/UCM sometimes distorted.
- Sending repeating registration packets to Server when receiving Terminate/Notify message.
- Dual Mic function is invalid.
- GDS Keypad input as Wiegand output still not working yet.
- Silent Alarm to SIP phone still playing siren at phone side after pressing keypad at phone side
- WebGUI limitation for Alarm Phone List and White List is not applied to P value import files and no error report generated when limitation overflow during the file import or restore.

NEW P-VALUE

- N/A

NEW HTTP API

- N/A