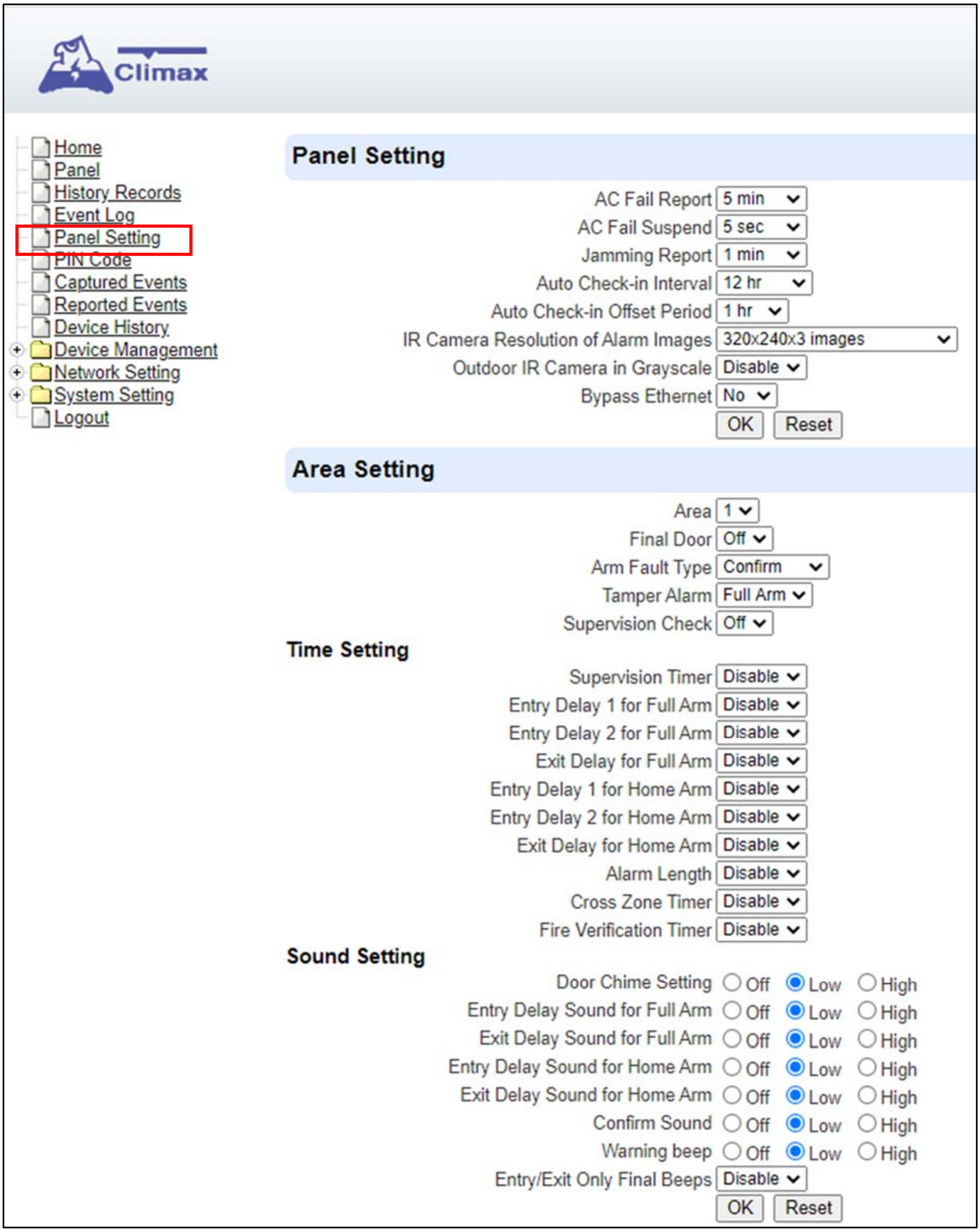
6.2. Panel Settings

Program the **Panel, Time** and **Sound Settings** at your discretion.



Panel Setting

AC Fail Report: 5 min
AC Fail Suspend: 5 sec
Jamming Report: 1 min
Auto Check-in Interval: 12 hr
Auto Check-in Offset Period: 1 hr
IR Camera Resolution of Alarm Images: 320x240x3 images
Outdoor IR Camera in Grayscale: Disable
Bypass Ethernet: No

Area Setting

Area: 1
Final Door: Off
Arm Fault Type: Confirm
Tamper Alarm: Full Arm
Supervision Check: Off

Time Setting

Supervision Timer: Disable
Entry Delay 1 for Full Arm: Disable
Entry Delay 2 for Full Arm: Disable
Exit Delay for Full Arm: Disable
Entry Delay 1 for Home Arm: Disable
Entry Delay 2 for Home Arm: Disable
Exit Delay for Home Arm: Disable
Alarm Length: Disable
Cross Zone Timer: Disable
Fire Verification Timer: Disable

Sound Setting

Door Chime Setting: ○ Off ● Low ○ High
Entry Delay Sound for Full Arm: ○ Off ● Low ○ High
Exit Delay Sound for Full Arm: ○ Off ● Low ○ High
Entry Delay Sound for Home Arm: ○ Off ● Low ○ High
Exit Delay Sound for Home Arm: ○ Off ● Low ○ High
Confirm Sound: ○ Off ● Low ○ High
Warning beep: ○ Off ● Low ○ High
Entry/Exit Only Final Beeps: Disable

Panel Setting

- **AC Fail Report**: When an AC power failure is detected, your Control Panel will report to the Central Monitoring Station according to the duration set under AC Fail Report. If 5 minutes is set, the event will be automatically reported to the CMS after 5 minutes. Your Control Panel will start to use its battery power instead of the mains power until the fault even is cleared.
- **AC Fail Suspend**: After an AC power failure event is reported, the Control Panel will

convert to sleep mode to conserve battery power. During this period, both GSM and Ethernet port will be powered off, while the RF and ZigBee modules will keep working. If 5 seconds is set, both GSM and Ethernet port will be powered off after 5 seconds. In order to send messages to the CMS, the Control Panel will power on its GSM and Ethernet temporarily.

- **Jamming Report**: Jamming period is specified as background RSSI level detected exceeding the threshold for a period.of time. The jamming period detected will be accumulated.

  3 options: Disable, 1 minute and 2 minutes are provided . If 1 minute is set, once the total jamming period exceeds 30 seconds within 1 minute, a "Jamming" message will be reported to the Central Monitoring Station . If 2 minutes is set, once the total jamming period exceeds 60 seconds within 2 minutes, a Jamming message will be reported to the Central Monitoring Station. If Diable is set, the control panel will not send a jamming report to the Central Monitoring Station if a jamming fault is detected.

- **Auto Check-in**: this is to select whether the Control Panel needs to send check-in reporting to the Central Station automatically and to select the period of time between check-in reports. Options available are **Disable**, **1 hour**, **2 hours**, **3 hours… up to 4 Weeks**.

- **Auto Check-in Offset Period**: This is to set the time delay before the first **Auto Check-In** report is made. After power is supplied or re-supplied to the Control Panel, a test report will be sent to the Central Monitoring Station (CMS) based on the Offset Period. This is used to test whether the CMS is able to receive the report from the Panel accurately.

  After this test report is sent, the Control Panel will then send reports at regular interval based on the setting of the Auto Check-in Report.

  For example, if **Offset Period** is set to 2 Hours, and **Auto Check-in Report** is set to 12 hours, the Control Panel will transmit an event code 602 to the CMS after 2 hours, and then report 602 event code periodically at a regular intervals of 12 hours.

- **IR Camera Resolution of Alarm Images**: This is to select the resolution and number of pictures taken by PIR Camera when the camera detects a movement in armed mode.

  Options available are **320x240x3 images (Default), 320x240x6 images and 640x320x3 images.**

- **Outdoor IR Camera in Grayscale**: This is to select whether pictures from Outdoor PIR Camera should be taken in grayscale instead of color pictures.

  Options available are: **Disable** (Color Picture) and **Enable** (Greyscale picture)

- **Bypass Ethernet:** Select to enable or disable Bypass Ethernet function. When **YES** is selected, the Control Panel will bypass connection fault when Ethernet cable unplugged status is detected.

Area Setting

- **Area**: Select operation area to apply setting.

- **Final Door**: If set to **On**: When the system is Away Armed and under exit timer countdown, if a opened Door Contact set to Entry attribute is closed, the system will automatically arm the system even if the exit delay timer has not expired yet.

- **Arm Fault Type**: Select how the system should respond when it is being armed under fault condition.

  ✓ Confirm: The panel will first display a "Mode Change Fault" message and emit 2 beeps. Arming again within 10 seconds will force arm the system.

  ✓ Direct Confirm: The system will be force armed directly without displaying fault message and report an event.

- **Tamper Alarm**: Select whether the siren should sound alarm when the tamper is triggered.
  - ✓ Full Arm: when tamper is triggered under Full arm mode, Control Panel raises a local alarm and sends report to the monitoring center. While under Home Arm or Disarm modes no alarm will be activated, nor report sent.
  - ✓ Always: Control Panel raises a local alarm and send report for tamper-trigger in all modes.
- **Supervision Check**: Select to enable or disable system supervision function. When **ON** is selected, the Control Panel will monitor the accessory devices according to the supervision signal received.

Time Setting

- **Supervision Timer**: The Control Panel monitors accessory devices according to the supervision signal transmitted regularly from the device. User this option to set a time period for receiving supervision signals. If the Control Panel fails to receive supervision signal from a device within this duration, it will consider the device out of order and report the event accordingly.
- **Entry Delay 1 for Full Arm**: Set Entry Delay Timer 1 for full arm mode. When a sensor set to Start Entry Delay 1 is triggered under Full Arm mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.
- **Entry Delay 2 for Full Arm**: Set Entry Delay Timer 2 for full arm mode. When a sensor set to Start Entry Delay 2 is triggered under Full Arm mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.
- **Exit Delay for Full Arm**: Set the Exit Delay Timer when entering Full Arm mode. When the user changes system mode to Full Arm, the panel will begin Exit Delay Timer Countdown and enter Full Arm mode when the timer expires. The user must leave area protected by sensors before the timer expires, otherwise an alarm will be activated with the sensor is triggered.
- **Entry Delay 1 for Home Arm**: Set Entry Delay Timer 1 for Home Arm mode. When a sensor set to Start Entry Delay 1 is triggered under Home Arm mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.
- **Entry Delay 2 for Home Arm**: Set Entry Delay Timer 2 for Home Arm mode. When a sensor set to Start Entry Delay 2 is triggered under Home Arm mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.
- **Exit Delay for Home Arm**: Set Exit Delay Timer for Home Arm mode. When the user changes system mode to Home Arm, the panel will begin Exit Delay Timer Countdown

and enter Home Arm mode when the timer expires. The user must leave area protected by sensors before the timer expires, otherwise an alarm will be activated with the sensor is triggered (Default as 10 seconds).

- **Alarm Length**: Set the duration the external siren should sound when an alarm is activated.
- **Cross Zone Timer**: Please refer to ***10.3 Cross Zone Timer*** for details
- **Fire Verification Time**: Please refer to ***10.4 Fire Verification Timer*** below for details.

Sound Setting

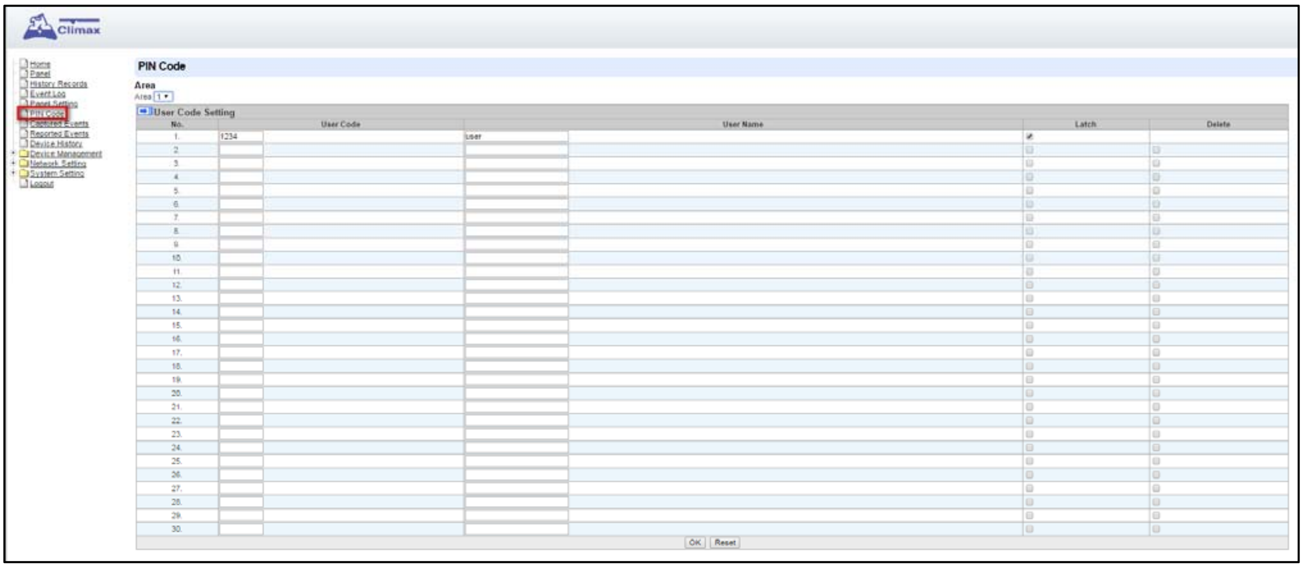
- **Door Chime Setting**: this function is available only when the attribute of Door Contact **(DC)** and/or PIR detector **(IR)** is set as **Door Chime**.

  The Control Panel sounds a Door Chime (Ding-Dong Sound) while the DC and/or IR is activated in Disarm / Full / Home / Entry mode.
- **Entry Delay Sound for Full Arm**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the entry delay time in the full arm mode.
- **Exit Delay Sound for Full Arm**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the exit delay timer in the full arm mode.
- **Entry Delay Sound for Home Arm**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the entry delay time in the home arm mode.
- **Exit Delay Sound for Home Arm**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the exit delay timer in the home arm mode.
- **Confirm Sound:** this is for you to decide whether to turn off/or adjust Control Panel beeping sounds when changing Arm/Home Arm/Disarm mode.
- **Warning beep**: this is for you to decide whether the Control Panel will sound a warning beep whenever a fault condition has been detected and displayed. The warning beep will be silenced after the Fault message has been read by the user. When a new fault condition is detected, it will then again emit a warning beep every 30 sec.
- **Entry/ Exit Only Final Beeps:** This is for you to determine when the Control Panel should start warning beep during Entry or Exit countdown timer. For example, if the setting is set to 5 seconds, the Control Panel will only stat warning beep during the last 5 seconds of Entry or Exit countdown timer. When set to Disable, the Control Panel will sound warning beep during the entire Entry or Exit countdown timer.

6.3. PIN Code

The User PIN Codes are used by Remote Keypad accessory to control system mode remotely. You may set up the PIN Codes available for the areas in the control panel. Each consists of 4-6 digits (numeric number 0~9), no disallowed PIN code. User PIN code #1 for each Area is always activated factory default.

User PIN #1 in Area 1	User PIN #1 in Area 2
Password: **1234**	Password: **4321**



PIN Code

Area

Area 1

User Code Setting

No.	User Code	User Name	Latch	Delete
1.	1234	user	☑	
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.			☐	☐
27.			☐	☐
28.			☐	☐
29.			☐	☐
30.			☐	☐

Area

Area: Select the area for setting User PIN Code.

User Code Setting

- **User Code**: Enter the 4-digit code in the field.
- **User Name**: Enter a user name for easy recognition of system events. Up to 17 alphanumerical characters are allow for each user name.
- **Latch**:

  ☑ Latch → **Latch Report ON** = Whenever the User PIN Code is used to change system mode, the panel will report the event.

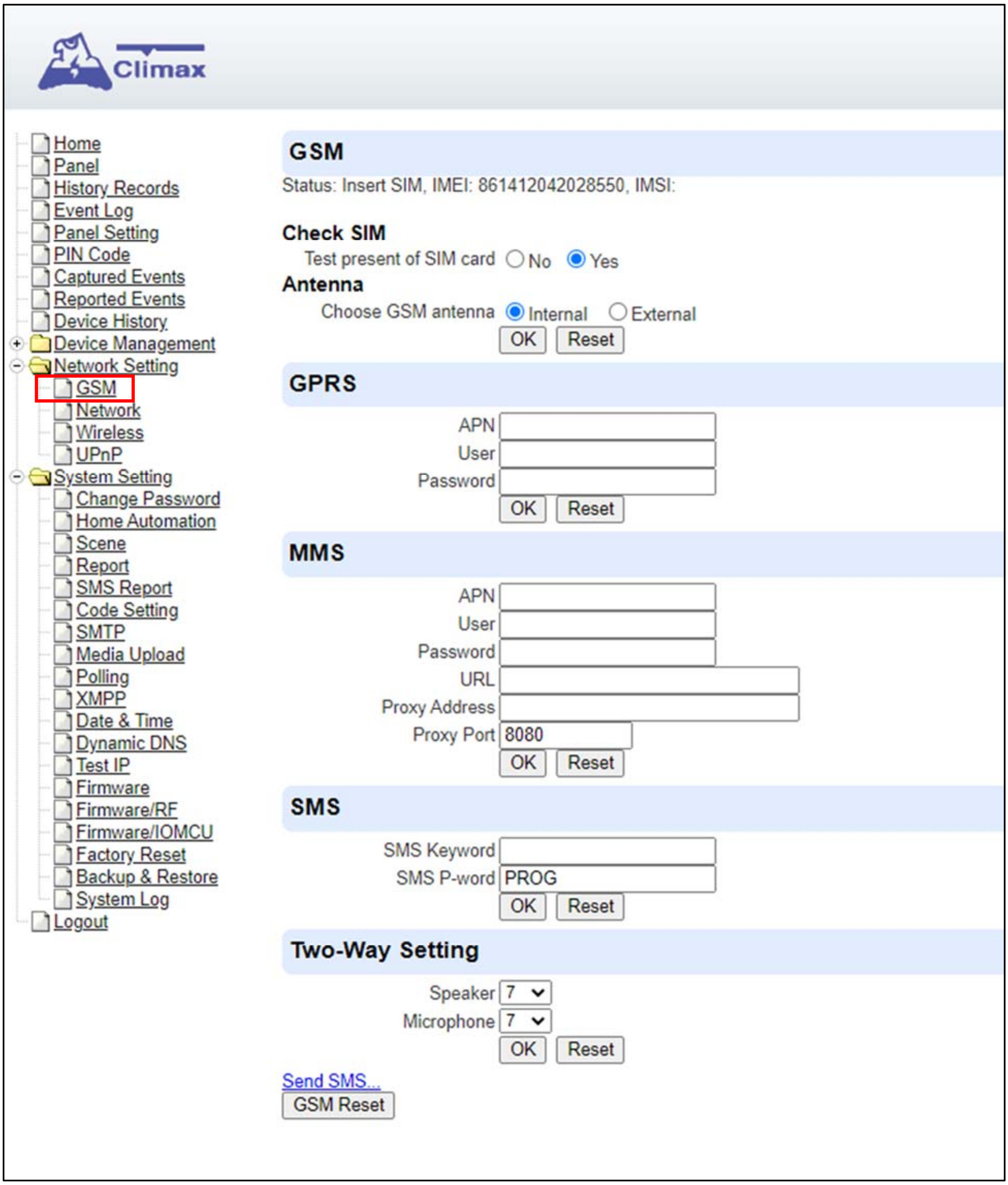
  ☐ Latch → **Latch Report OFF** = When the User PIN Code is used to change system mode, the panel will not report the event.

- **Delete**: Check the box if you want to delete selected user. User#1 in each area cannot be deleted

After finish all setting, click **OK** to confirm change.

7. Network Settings

7.1. GSM



GSM

Status: Insert SIM, IMEI: 861412042028550, IMSI:

Check SIM

Test present of SIM card ○ No ● Yes

Antenna

Choose GSM antenna ● Internal ○ External

GPRS

APN

User

Password

MMS

APN

User

Password

URL

Proxy Address

Proxy Port 8080

SMS

SMS Keyword

SMS P-word PROG

Two-Way Setting

Speaker 7

Microphone 7

Check SIM

This is designed for the system to check if the SIM card is inserted or not. (***If users do not intend to use the GSM funciton, please tick “NO” to ensure the system will not check if the SIM card is inserted or not and it will not display the GSM fault by LED flashing.***)

Antenna

This option is for the user to choose between using the internal or external antenna.

GPRS

In order to allow GPRS to serve as a back-up IP Reporting method, this section will need to be programmed before reporting.

- **APN (Access Point) Name**

  It is the name of an access point for GPRS. Please inquire your service provider for an APN. When APN is set, the system becomes valid for internet connection.

- **User (GPRS)**

  It is the Log-in name to input before accessing the GPRS feature. Please inquire your service provider.

- **Password (GPRS)**

  It is the User Password to input before accessing the GPRS feature. Please inquire your service provider.

<NOTE>

- All values will be applied to all Areas.

MMS

The MMS settings are offered by your telecom service provider. Before configuring this function, contact your service provider for correct MMS setting information of the inserted SIM card.

- **APN (Access Point) Name**

  Enter a MMS APN name provided by your service provider.

- **User**

  Enter the Log-in name for accessing the MMS feature provided by your telecom service provider.

- **Password**

  Enter the password for accessing the MMS feature provided by your telecom service provider.

- **URL**

  Enter the MMS APN URL provided by your telecom service provider.

- **Proxy Address**

  Enter the MMS Proxy Address provided by your telecom service provider.

- **Proxy Port**

  Enter the MMS Proxy Port provided by your telecom service provider.

SMS

- **SMS Keyword**

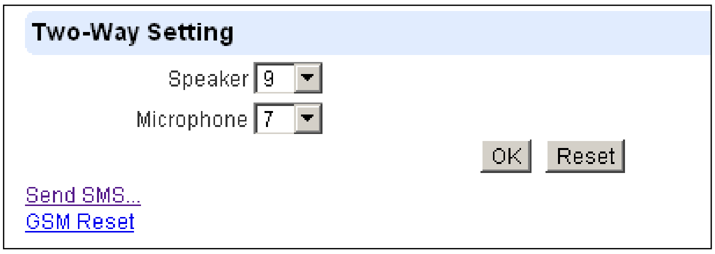
  For sending remote commands to system via SMS message, a personalized password is required for the Control Panel to recognize your authority.

- **SMS P-Word**

  Program Keyword is used to recognize the identity of a valid user; and to give authority for Remote Installing (through SMS Text) or Remote Upgrading purposes (through GPRS). This keyword will need to be inserted whenever the Remote Setting or Remote Upgrading is required. A maximum of 15 characters is allowed.

Two Way Setting

The two-way setting is designed to adjust speaker volume and microphone sensitivity on DECT device for two-way communication.



Two-Way Setting

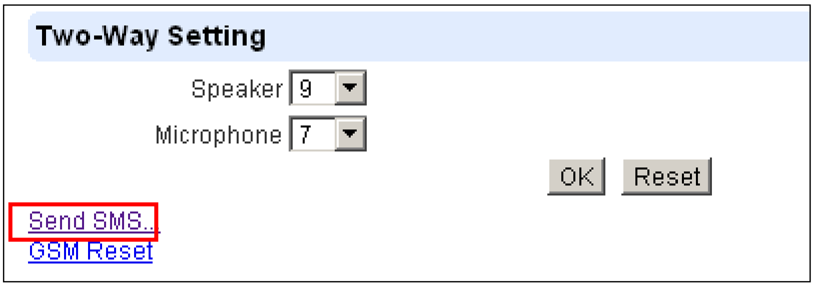
Speaker 9

Microphone 7

Send SMS Message

This feature is designed for you to send a SMS message on this web configuration page.

Step 1. Click **Send SMS**.

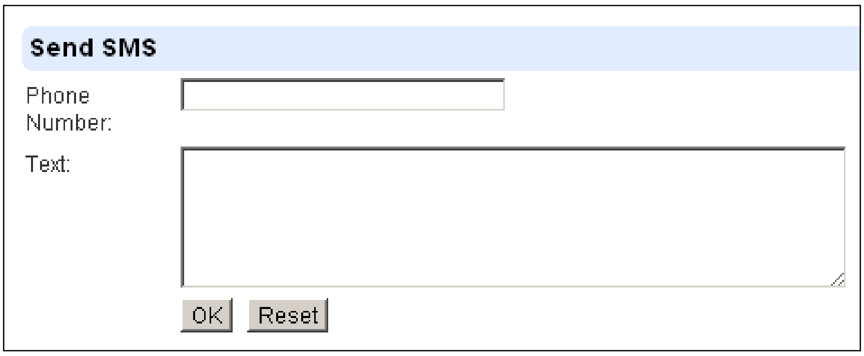


Two-Way Setting

Speaker 9

Microphone 7

Step 2. Enter a desired phone number and text message.



Send SMS

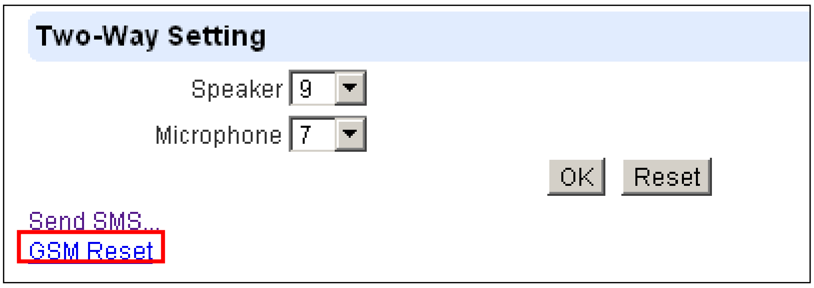
Phone Number:

Text:

Reset GSM

This feature is designed for you to reset GSM module.

Step 1. Click **GSM Reset.**



Two-Way Setting

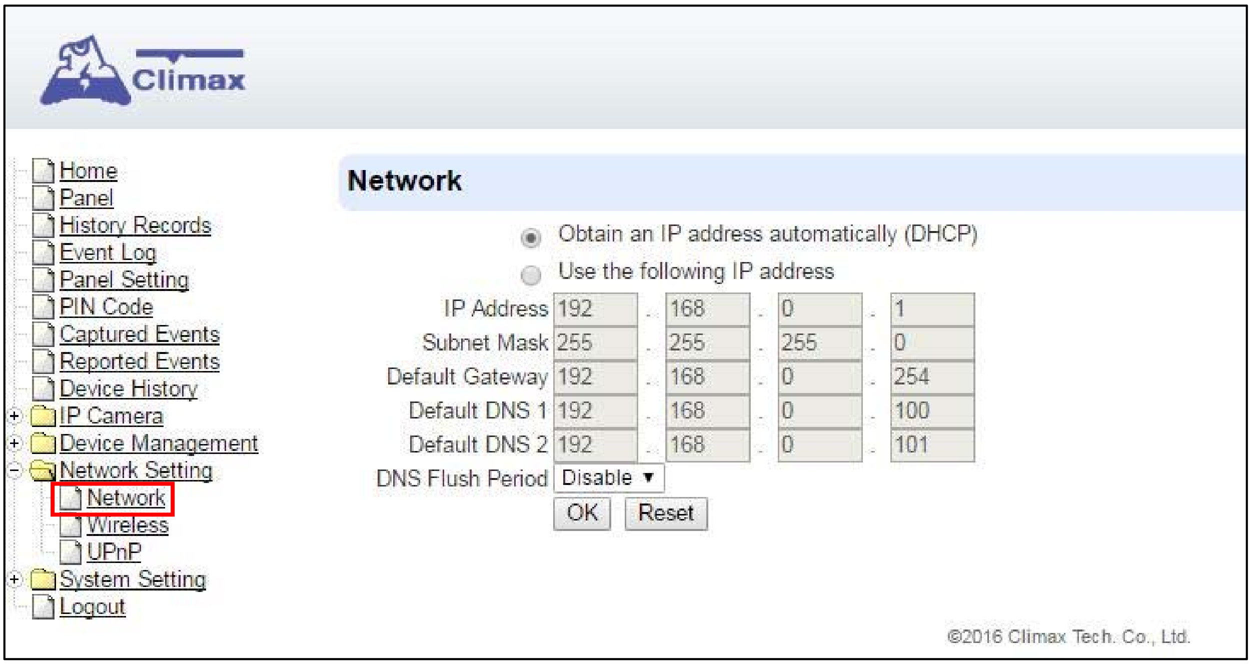
Speaker 9

Microphone 7

Step 2. A pop-out message "Are you sure?" is displayed. Click **Yes** to confirm resetting.

7.2. Network

This is for you to program the Network for IP connection.



Network

● Obtain an IP address automatically (DHCP)

○ Use the following IP address

IP Address 192 . 168 . 0 . 1

Subnet Mask 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 0 . 254

Default DNS 1 192 . 168 . 0 . 100

Default DNS 2 192 . 168 . 0 . 101

DNS Flush Period Disable ▾

- **Obtain an IP address automatically (DHCP)**

  If DHCP is selected, the Network will obtain an IP address automatically with a valid Network DHCP Server. Therefore, manual settings are not required.

  This is only to be chosen if your Network environment supports DHCP. It will automatically generate all information.

- **Use following IP address**

  You can also enter the Network information manually for IP Address, Subnet Mask, Default Gateway, Default DNS 1 and Default DNS 2.

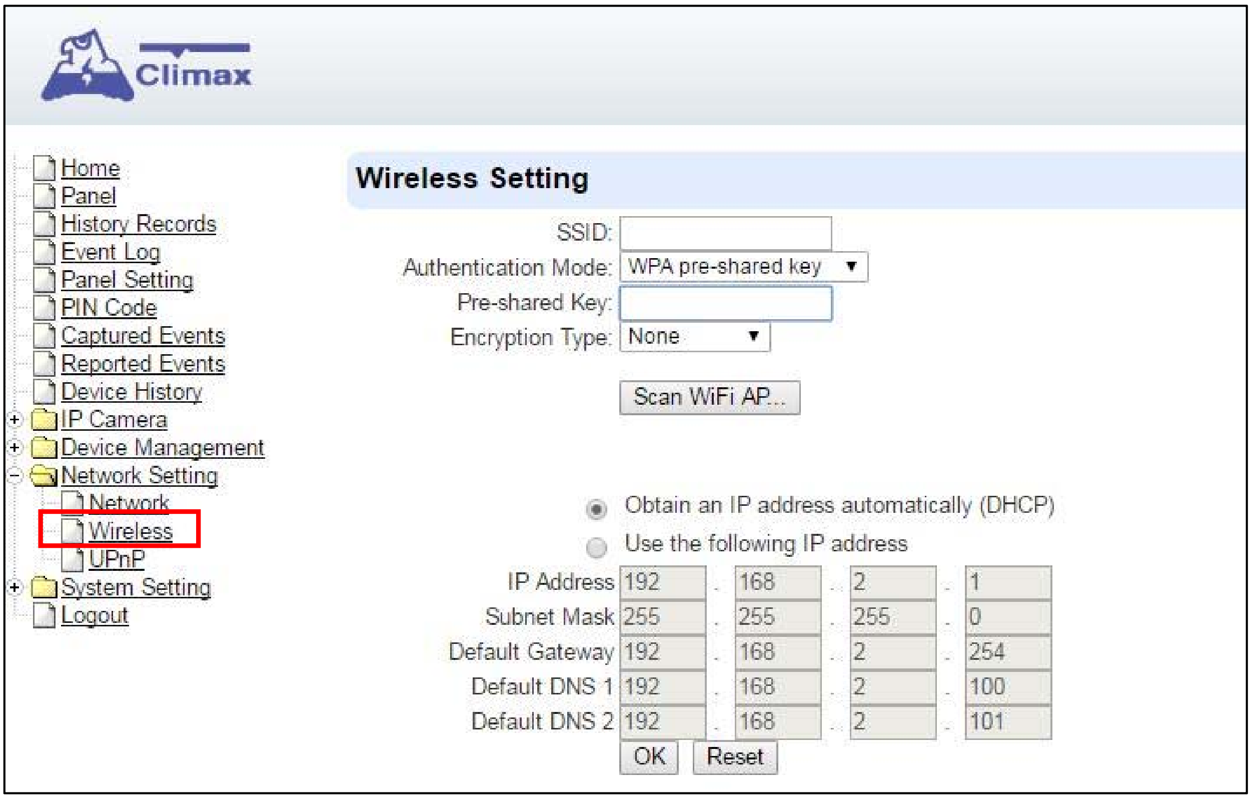
  Please make sure that you have obtained all required values according to your Network environment. Please contact your network administrator and/or internet service provider for more information.

- **DNS Flush Period**

  You can set the system to clear current DNS resolution records for all entered URL settings (Reporting, Upload, XMPP…etc.) after a set time period. The system will then resolve the Domain Name again and acquire new IP address for the URL settings. This function is disabled by default.

7.3. Wireless

Use “**Wireless**” webpage to setup the panel’s WiFi setting



Wireless Setting

SSID:

Authentication Mode: WPA pre-shared key

Pre-shared Key:

Encryption Type: None

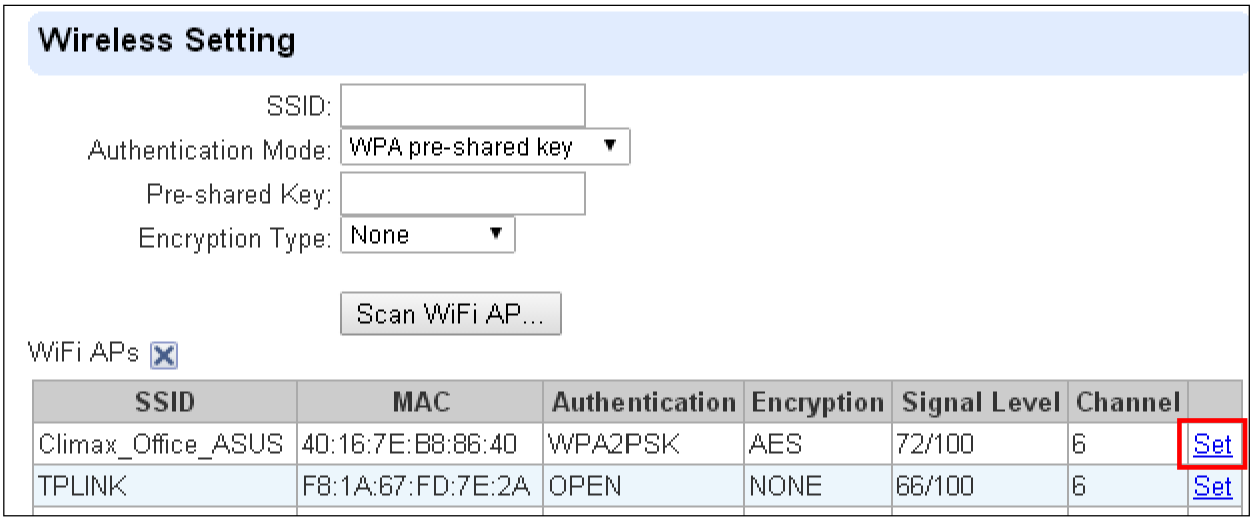
● Obtain an IP address automatically (DHCP)

○ Use the following IP address

IP Address	192	168	2	1
Subnet Mask	255	255	255	0
Default Gateway	192	168	2	254
Default DNS 1	192	168	2	100
Default DNS 2	192	168	2	101

There are 3 ways you can connect to the wireless network.

1. Search for WiFi AP: Click “**Scan WiFi AP**” to search for available wireless network Select the available Wireless APs from the list by clicking “**Set**” after AP info column and enter the required information (pre-shared key, etc.) and click the “**OK**” button.



Wireless Setting

SSID:

Authentication Mode: WPA pre-shared key

Pre-shared Key:

Encryption Type: None

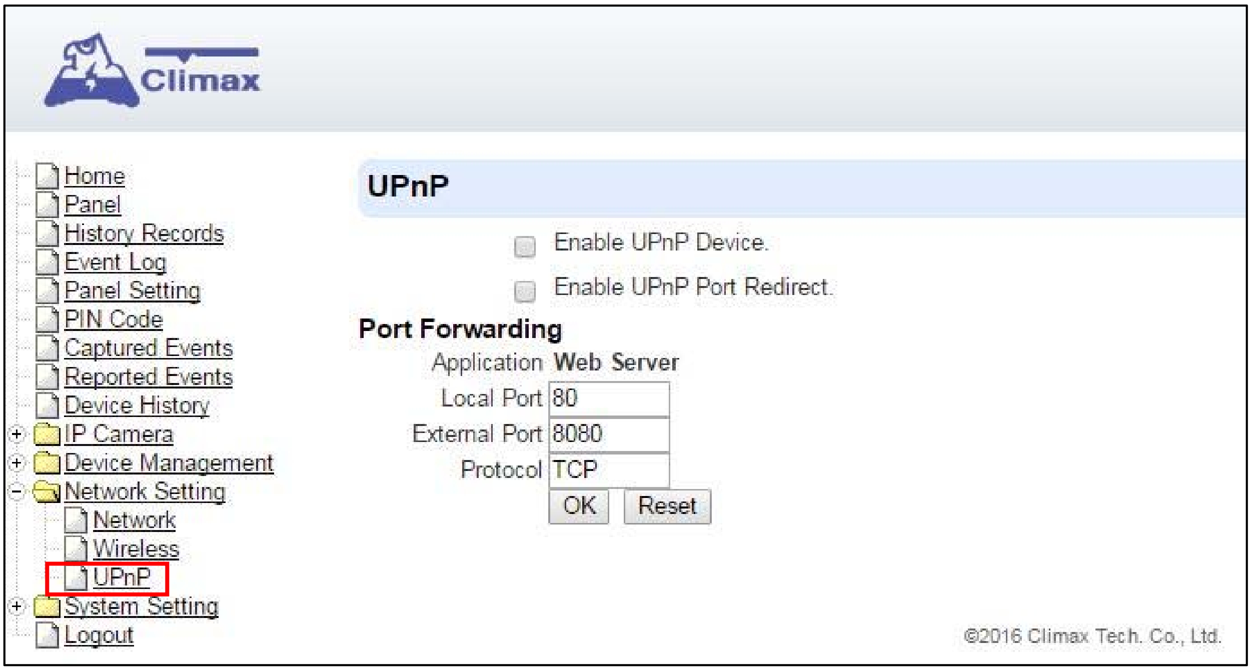
WiFi APs ☒

SSID	MAC	Authentication	Encryption	Signal Level	Channel	
Climax_Office_ASUS	40:16:7E:B8:86:40	WPA2PSK	AES	72/100	6	Set
TPLINK	F8:1A:67:FD:7E:2A	OPEN	NONE	66/100	6	Set

2. Enter the Wireless information manually and click “**OK**” to connect.

7.4. UPnP

UPnP is Universal Plug and Play, which opens networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.



UPnP

□ Enable UPnP Device.

□ Enable UPnP Port Redirect.

Port Forwarding

Application Web Server
Local Port 80
External Port 8080
Protocol TCP

©2016 Climax Tech. Co., Ltd.

- **Enable UPnP Device:**

  When enabled, you will be able to see this device via any UPnP discovery tool

- **Enable UPnP Port Redirect:**

  The device will try to find an UPnP-supported router and set up the port to redirect to the router.

- **Port Forwarding:**

  Port forwarding function allows you to configure specific communication ports to be routed to your system over the Internet for users to access their IP camera(s) remotely.

  1. **Local Port:** type 80.
  2. **External Port:** type 8080.
  3. **Protocol:** type TCP.

  After port forwarding has been set up, the router will forward incoming requests on port that your IP Camera users. To set up port forwarding on your router, please refer to your router’s instruction manuals for detail.

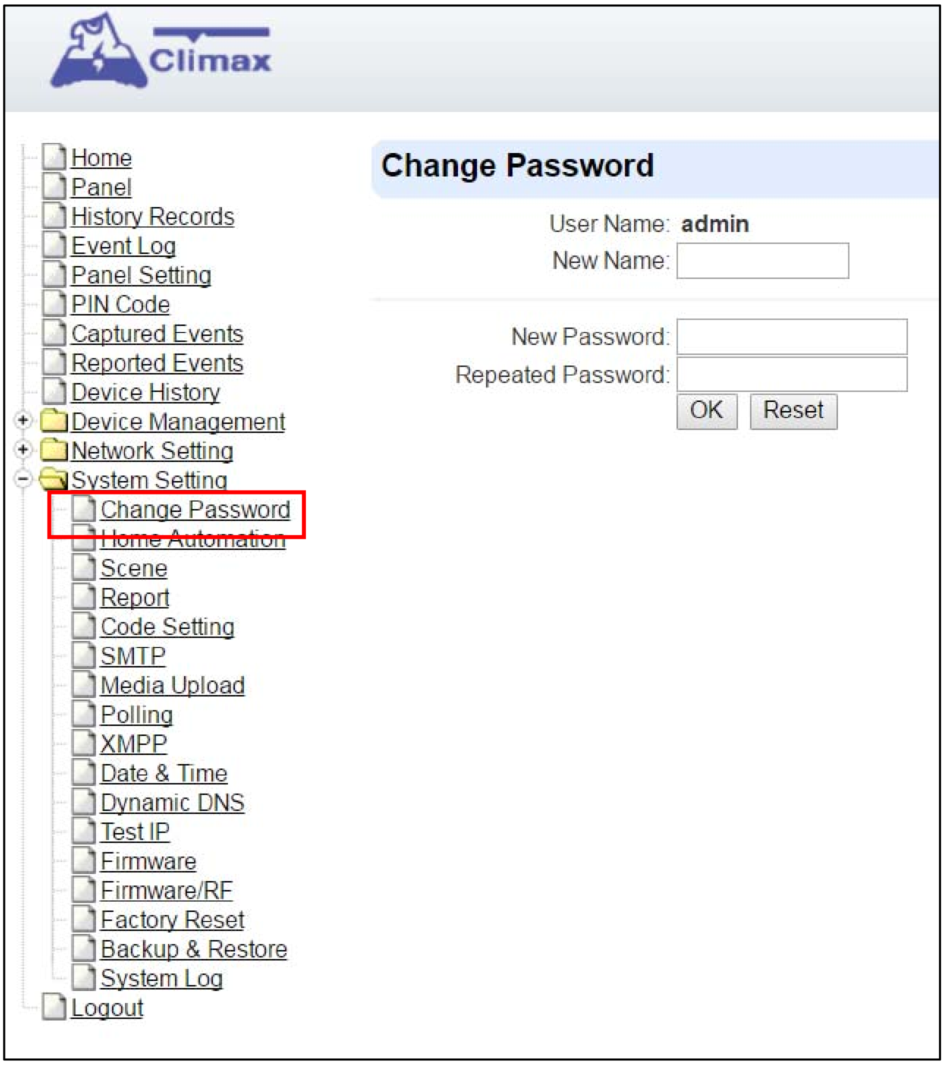
8. *System Settings*

8.1. Administrator Setting

For setting new Administrator Log-in Name and Password. Please note both User Name and Password are ***case sensitive***.

Step 1. Enter the preferred **User Name**.

Step 2. Enter the preferred **Password** in the "New Password" field and repeat the same Password in the **Repeat Password** field.



Change Password

User Name: **admin**

New Name:

New Password:

Repeated Password:

8.2. Home Automation

It is used to set Home Automation rules to control sensors and home appliances. You can set up to 100 rules.

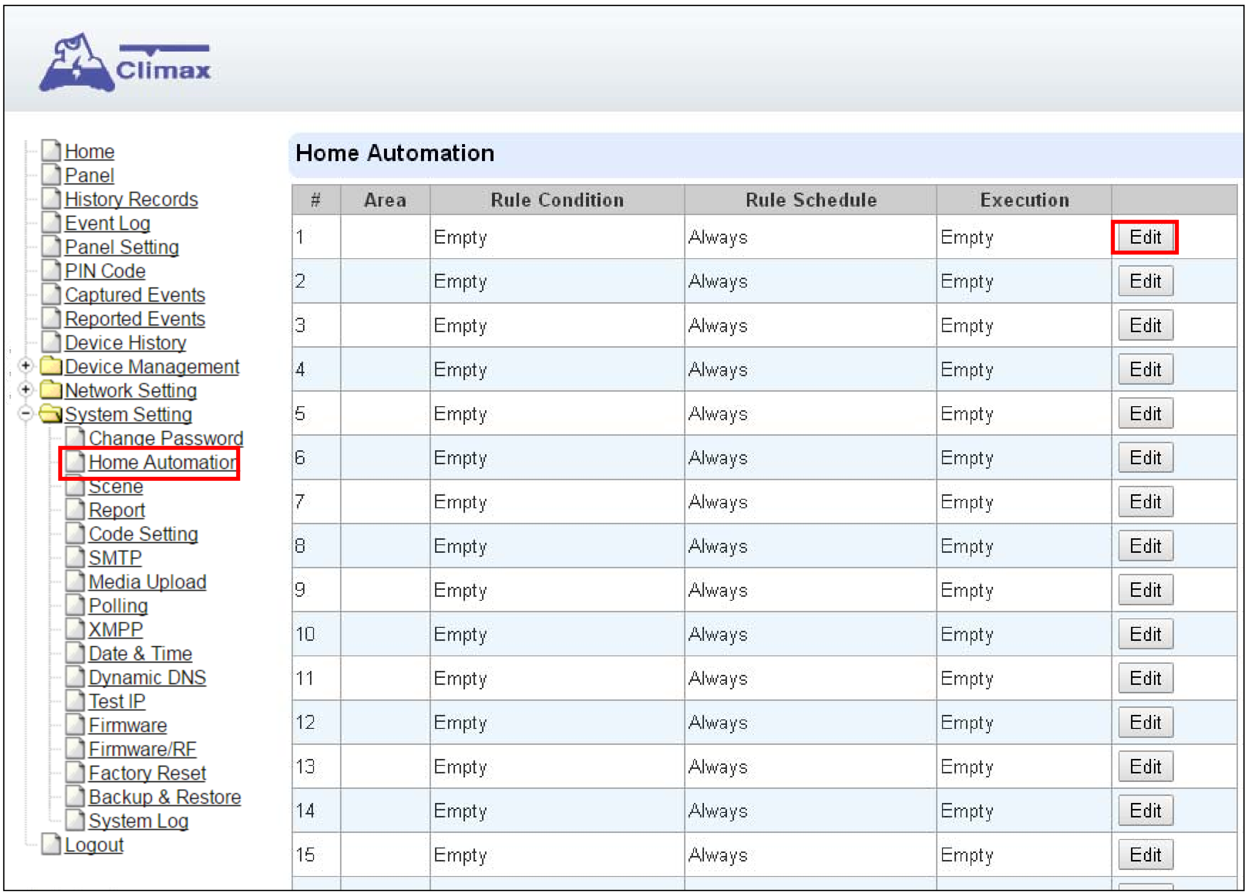
Step 1. Click on **Edit**.

Step 2. Select an operation area.

Step 3. Set a rule condition.

Step 4. Set a rule schedule.

Step 5. Select the corresponding action rules in the **Execution** field.



Home Automation

#	Area	Rule Condition	Rule Schedule	Execution	
1		Empty	Always	Empty	Edit
2		Empty	Always	Empty	Edit
3		Empty	Always	Empty	Edit
4		Empty	Always	Empty	Edit
5		Empty	Always	Empty	Edit
6		Empty	Always	Empty	Edit
7		Empty	Always	Empty	Edit
8		Empty	Always	Empty	Edit
9		Empty	Always	Empty	Edit
10		Empty	Always	Empty	Edit
11		Empty	Always	Empty	Edit
12		Empty	Always	Empty	Edit
13		Empty	Always	Empty	Edit
14		Empty	Always	Empty	Edit
15		Empty	Always	Empty	Edit

- **Area**

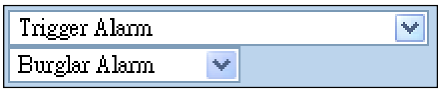
  Select an opeartion area.

- **Rule Condition**

  The rule condition determines under which circumstances the rule should be activated.

☞ ***Empty*** **:** When set as **Empty**, the system will follow the schedule time and execution rule to respond accordingly.

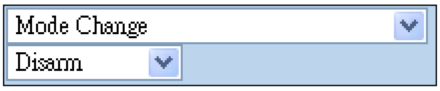
☞ ***Trigger Alarm*** : When set as **Trigger Alarm**, if the specified alarm event (Burglar/Smoke/Medical/Water/Silent Panic/Panic/Emergency/Fire/CO Alarm/Gas/Heat) or any alarm is triggered, the rule will be activated according to rule schedule and execution setting.



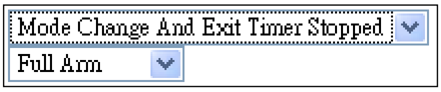
Trigger Alarm

Burglar Alarm

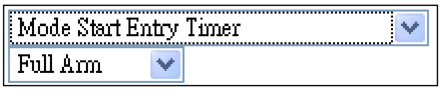
☞ ***Mode Change*** : When set as **Mode Change**, when the system enters specified mode, the rule will be activated according to rule schedule and execution setting.


Mode Change
Disarm

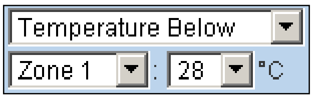
☞ ***Mode Change and Exit Timer Stopped*** : When set as **Mode Change and Exit Timer Stopped**, when the system changes mode to and Exit Delay Timer expires, , the rule will be activated according to rule schedule and execution setting.


Mode Change And Exit Timer Stopped
Full Arm

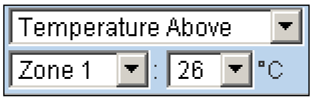
☞ ***Mode Start Entry Timer*** : When set as **Mode Start Entry Timer**, when the system begins to countdown Entry Delay, the rule will be activated according to rule schedule and execution setting.


Mode Start Entry Timer
Full Arm

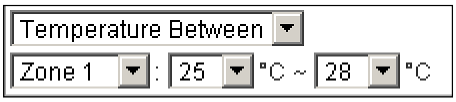
☞ ***Temperature Below*** : When set as **Temperature Below**, if the temperature detected by specified temperature sensor drops below set threshold, the rule will be activated according to rule schedule and execution setting.


Temperature Below
Zone 1 : 28 °C

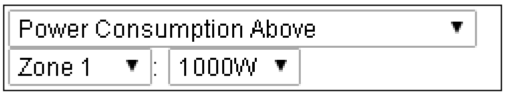
☞ ***Temperature Above*** : When set as **Temperature Above**, if the temperature detected by specified temperature sensor exceeds set threshold, the rule will be activated according to rule schedule and execution setting.


Temperature Above
Zone 1 : 26 °C

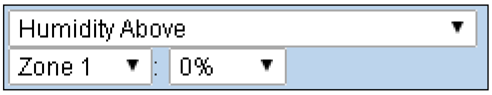
☞ ***Temperature Between*** : When set as **Temperature Between**, if the temperature detected by specified temperature sensor falls within the range specified, the rule will be activated according to rule schedule and execution setting.


Temperature Between
Zone 1 : 25 °C ~ 28 °C

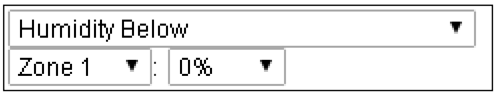
☞ ***High Power Consumption*** : When set as **Power Consumption Above**, if the power output watt from a specific Power Switch exceeds, the rule will be activated according to rule schedule and execution setting.


Power Consumption Above
Zone 1 : 1000W

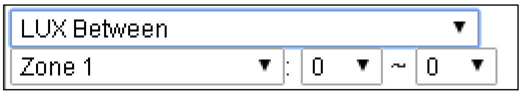
☞ ***Humidity Above*** : When set as **Humidity Above**,if the humidity reading from specified room sensor rises above the level specified, the rule will be activated according to rule schedule and execution setting.


Humidity Above
Zone 1 : 0%

☞ ***Humidity Below*** : When set as **Humidity Below**,if the humidity reading from specified room sensor falls below the level specified, the rule will be activated according to rule schedule and execution setting.

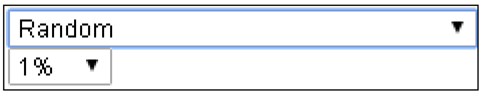

Humidity Below
Zone 1 : 0%

☞ ***LUX Between*** : When set as **LUX Between**, if the lux reading from specified light sensor falls below the level specified, the rule will be activated according to rule schedule and execution setting.



☞ ***Random*** : The **Random** condition must be used along with Rule Schedule setting. Set a percentace from 1 to 10%. When the panel time reaches programmed Rule Schedule time. The Panel will activate rule according to set chance.

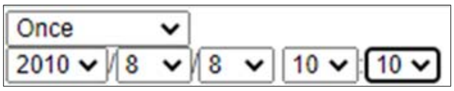
Example: If set as 10%, whenever the panel reaches programmed Rule Schedule time, there will be a 10% chance the rule is activated.



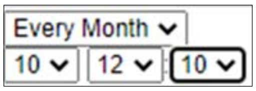
- **Rule Schedule**

☞ ***Always*** : When set as **Always**, the rule can be activated anytime.

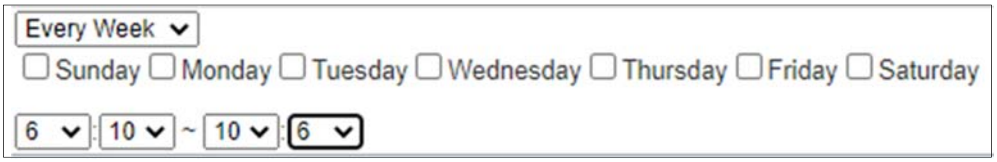
☞ ***Once*** : When set as **Once**, the system will follow the rule condition and execute rule according to the exact date and time specifed..



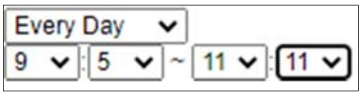
☞ ***Every Month*** : When set as **Every Month**, the system will follow the rule condition and execute rule according to date and time specified every month.



☞ ***Every Week*** : When set as **Every Week**, the system will follow the rule condition and execute rule according to day of the week and time specified every week.


Every Week
□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
6
10
~
10
6

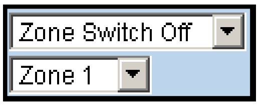
☞ ***Every Day*** : When set as **Every Day**, the system will follow the the rule condition and execute rule according to time specified every day



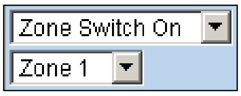
- **Execution**

Execution is the actual action performed by Control Panel when both Rule Condition and Rule Schedule requirements are met

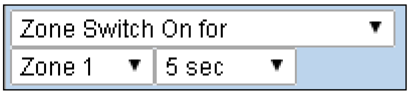
☞ ***Zone Switch Off:*** Turn on the Power Switch at specified zone.



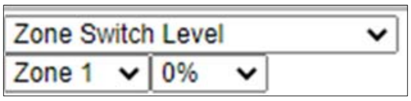
☞ ***Zone Swich On*** : Turn on the Power Switch at specified zone.


Zone Switch On
Zone 1

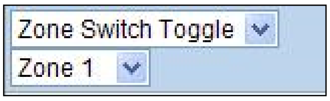
☞ ***Zone Swich On For*** : Turn on the Power Switch at specified zone for a set duration.


Zone Switch On for
Zone 1 | 5 sec

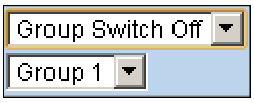
☞ ***Zone Switch Level:***: Change the power output level for Dimmer at specified zone.


Zone Switch Level
Zone 1 | 0%

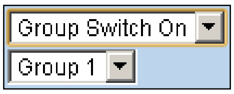
☞ ***Zone Swich Toggle*** : Toggle on/off the Power Switch at specified zone.


Zone Switch Toggle
Zone 1

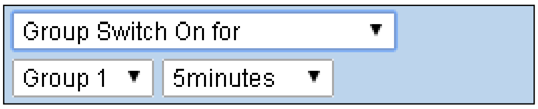
☞ ***Group Switch Off*** : Turn off all Power Switches assigned to specified group.


Group Switch Off
Group 1

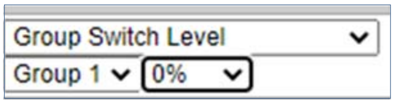
☞ ***Group Switch On*** : Turn on all Power Switches assigned to specified group.


Group Switch On
Group 1

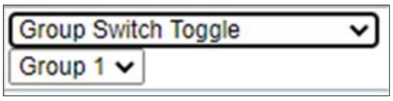
☞ ***Group Switch On For*** : Turn on all Power Switches assigned to specified group for a set duration.


Group Switch On for
Group 1 | 5minutes

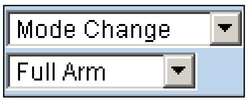
☞ ***Group Switch Level*** : Change the power output level for Dimmer at specified group.


Group Switch Level
Group 1 | 0%

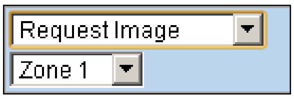
☞ ***Group Switch Toggle*** : Toggle on/off the Power Switch at specified group.


Group Switch Toggle
Group 1

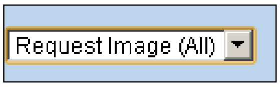
☞ ***Mode Change*** : The system will change to the mode as you specified.


Mode Change
Full Arm

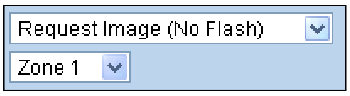
☞ ***Request Image*** : The PIR Camera in specified zone will take a picture.


Request Image
Zone 1

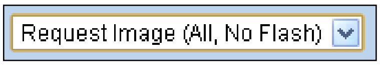
☞ ***Request Image (All)*** : All PIR Cameras in the system will take a picture.


Request Image (All)

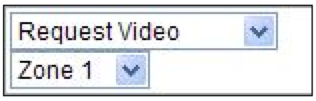
☞ ***Request Image (No Flash)***: The PIR Camera in specified zone will take a picture.without activating its LED flash.


Request Image (No Flash)
Zone 1

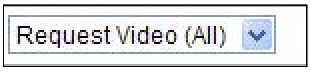
☞ ***Request Image (All, No Flash)*** : All PIR Cameras in the system will take a picture without activating LED Flash.


Request Image (All, No Flash)

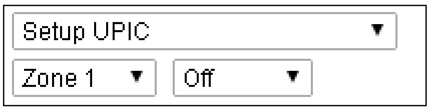
☞ ***Request Video*** : The PIR Video Camera or IP Camera in specified zone will record a video.


Request Video
Zone 1

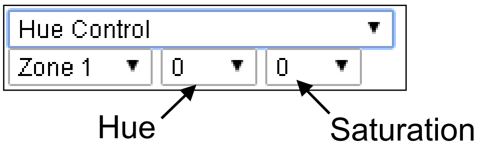
☞ ***Request Video (All)*** : All PIR Video Cameras and IP Cameras in the system will record a video.


Request Video (All)

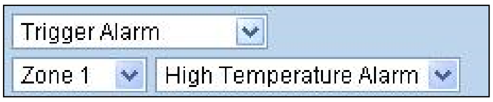
☞ ***Setup UPIC:***: The UPIC and specified zone will transmit Off/Heat/Cool command to the air conditioner as programmed.


Setup UPIC
Zone 1
Off

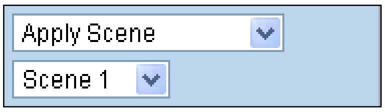
☞ ***Hue Control:***: Adjust the hue and saturation of the Philips Hue at sepecified zone as programmed.


Hue Control
Zone 1
0
0

☞ ***Trigger Alarm:*** Choose to activate one of the following alarms: High Temperature Alarm, Low Temperature Alarm, High Power Consumption Alarm, High Humidity Alarm and Low Humidity Alarm

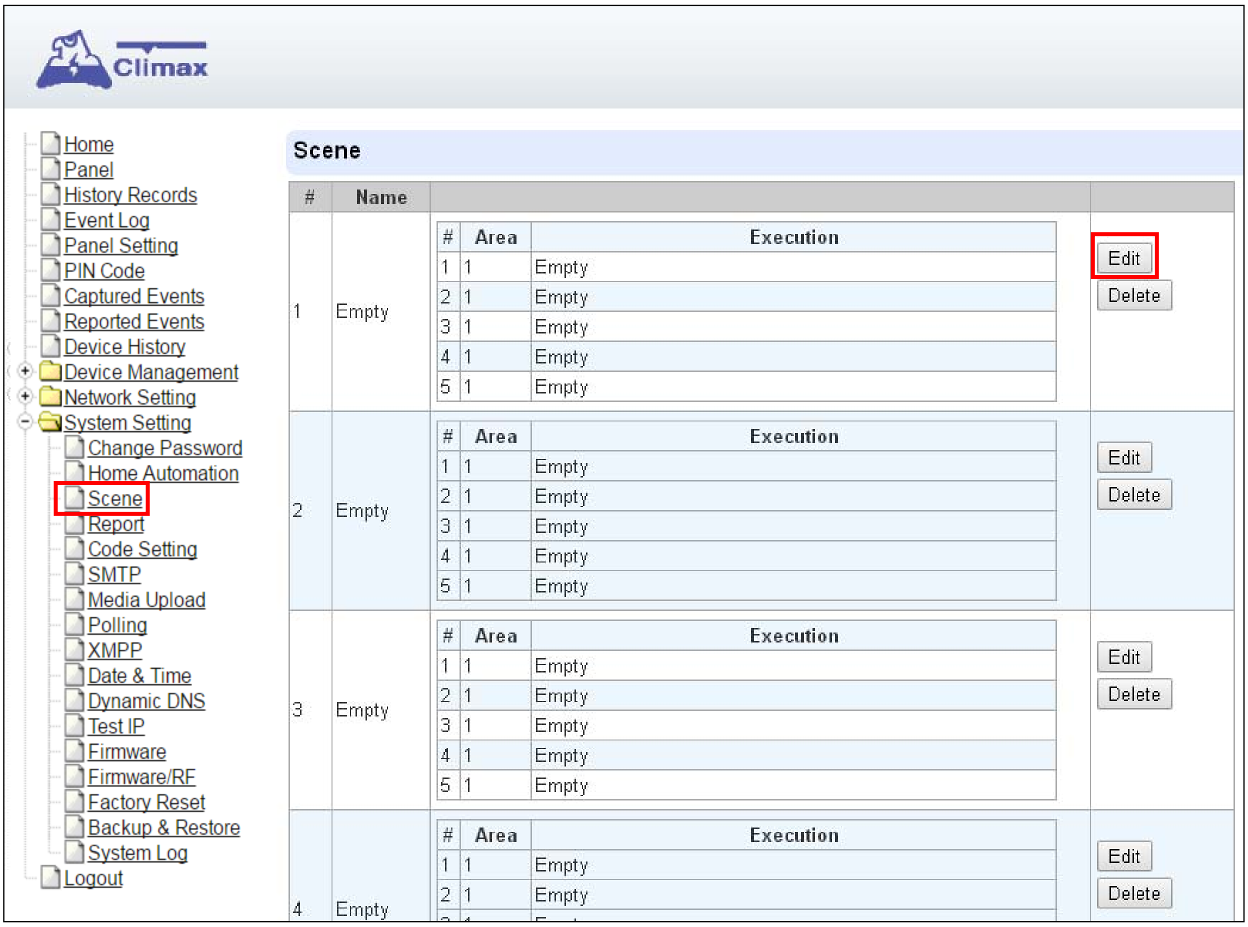

Trigger Alarm
Zone 1
High Temperature Alarm

☞ ***Apply Scene:***: the system will execute preprogrammed Scene number. Please refer to **8.3. Scene** for detail.


Apply Scene
Scene 1

8.3. Scene

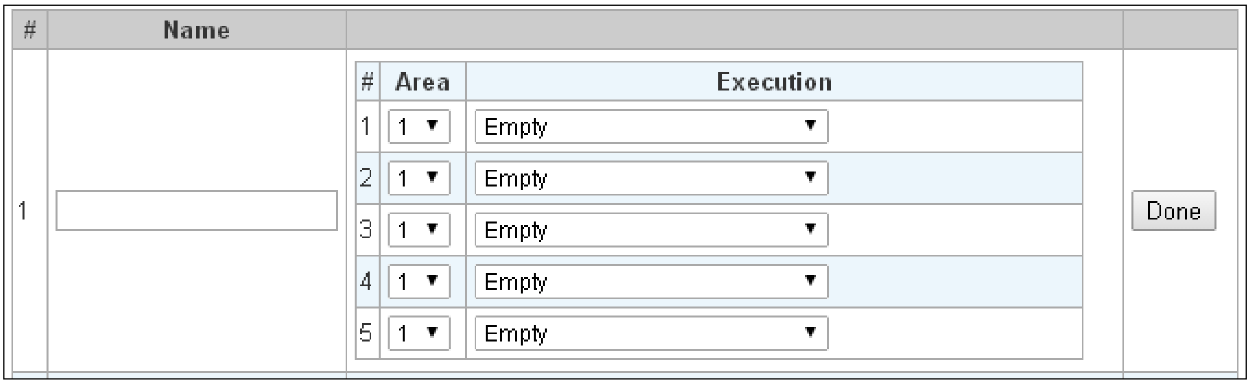
The Scene setting allows you to customize a series of actions with your devices, such as Power Switch control, image/video request, mode change and trigger alarm. The programmed scene can be set to activated when a device is triggered. (See **5.1.3. Edit Devices**), or when a Home Automation Rule is excecuted. (See **8.2. Home Automation**) For example, you can set a scene to control multiple lightings, then set your Remote Controller to activate the scene when the button is pressed, or set a Home Automation Rule to activate the scene.



Scene

#	Name	#	Area	Execution
1	Empty	1	1	Empty
		2	1	Empty
		3	1	Empty
		4	1	Empty
		5	1	Empty
2	Empty	1	1	Empty
		2	1	Empty
		3	1	Empty
		4	1	Empty
		5	1	Empty
3	Empty	1	1	Empty
		2	1	Empty
		3	1	Empty
		4	1	Empty
		5	1	Empty
4	Empty	1	1	Empty
		2	1	Empty

Step 1. Click on **Edit**.



#	Name	#	Area	Execution
1		1	1 ▼	Empty ▼
		2	1 ▼	Empty ▼
		3	1 ▼	Empty ▼
		4	1 ▼	Empty ▼
		5	1 ▼	Empty ▼

Step 2. Enter a name for the scene.

Step 3. Select an Area

Step 4. Select an action to be executed when the scene is activated. Refer to the Rule Execution section in ***8.2. Home Automation*** for detail.

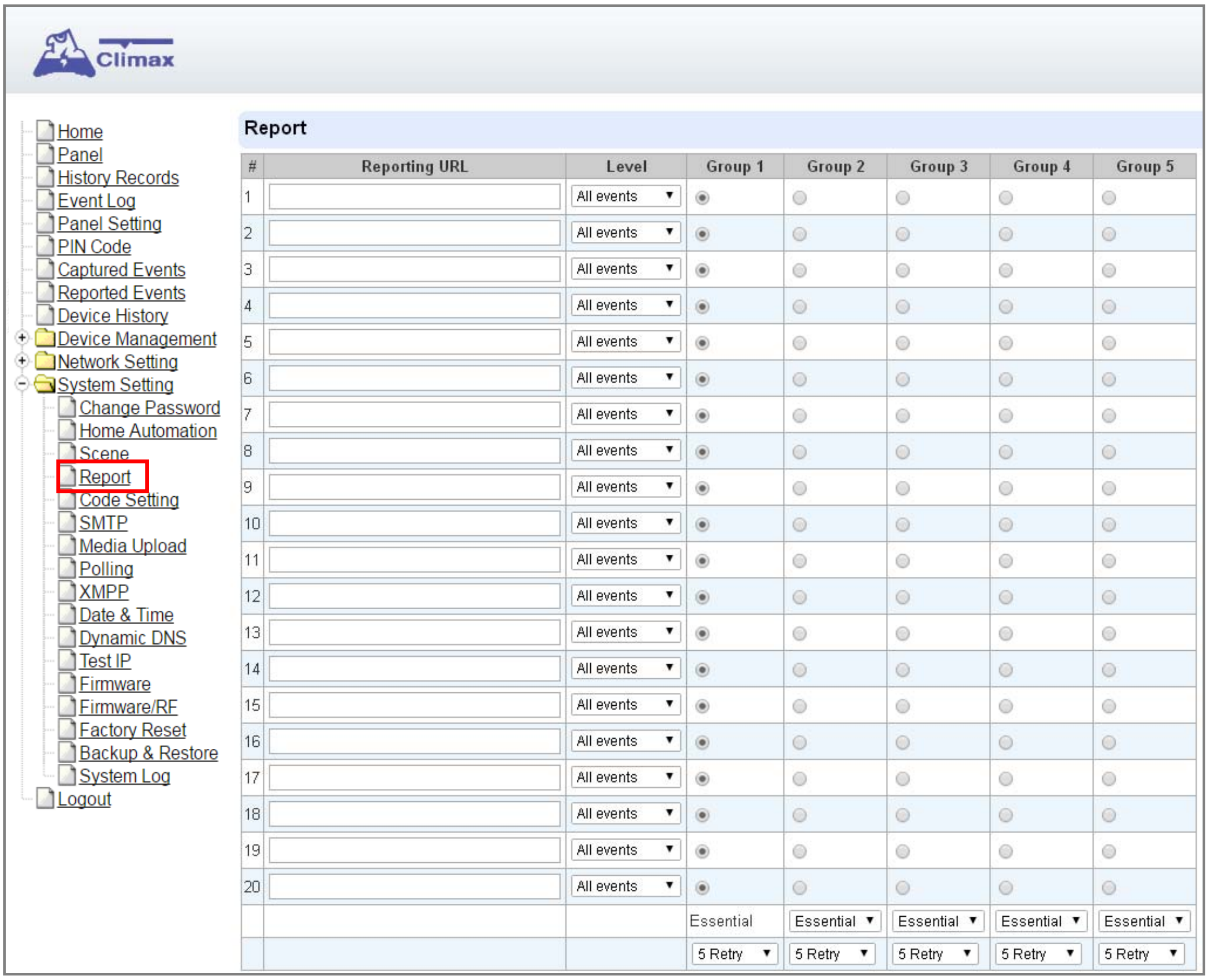
Step 5. Repeat Step 2-3 to setup the execution you wanted. As many as 5 executions can be included in one scene.

Step 6. Click “**Done**”.

Step 7. Click “**OK**” at bottom of webpage to confirm the new scene setting..

8.4. Reporting

This is used for installer to program/ set all requirements for reporting purposes.



Report

#	Reporting URL	Level	Group 1	Group 2	Group 3	Group 4	Group 5
1		All events ▼	●	○	○	○	○
2		All events ▼	●	○	○	○	○
3		All events ▼	●	○	○	○	○
4		All events ▼	●	○	○	○	○
5		All events ▼	●	○	○	○	○
6		All events ▼	●	○	○	○	○
7		All events ▼	●	○	○	○	○
8		All events ▼	●	○	○	○	○
9		All events ▼	●	○	○	○	○
10		All events ▼	●	○	○	○	○
11		All events ▼	●	○	○	○	○
12		All events ▼	●	○	○	○	○
13		All events ▼	●	○	○	○	○
14		All events ▼	●	○	○	○	○
15		All events ▼	●	○	○	○	○
16		All events ▼	●	○	○	○	○
17		All events ▼	●	○	○	○	○
18		All events ▼	●	○	○	○	○
19		All events ▼	●	○	○	○	○
20		All events ▼	●	○	○	○	○
			Essential	Essential ▼	Essential ▼	Essential ▼	Essential ▼
			5 Retry ▼	5 Retry ▼	5 Retry ▼	5 Retry ▼	5 Retry ▼

- **Reporting URL**

  This is used for installer to program report destinations.

  1 Climax CID protocol via IP

  Format: ip://(Account Number)@(server ip):(port)/CID

  Example: ip://1234@54.183.182.247:8080/CID

  2 SIA DC-09 protocol via IP

  Format: ip://(Account Number)@(server ip):(port)/SIA

  Example: ip://1234@54.183.182.247:8080/SIA

  3 SIA DC-09 protocol via IP with AES encryption

  Format: ip//(Account Number)@(server ip):(port)/SIA/KEY/(128,196 or 256 bits Key)

  Example:

  ip://1234@54.183.182.247:8080/SIA/KEY/ 4A46321737F890F654D632103F86B4F3

  4 SIA DC-09 protocol using CID event code via IP

  Format: ip://(Account Number)@(server ip):(port)/CID_SIA

  Example: ip://1234@54.183.182.247:8080/CID_SIA

  5 SIA DC-09 protocol using CID event code via IP, with HEX encryption.

  Format: ip//(Account Number)@(server ip):(port)/CID_SIA/KEY/(HEX)

  Example:

ip://1234@54.183.182.247:8080/CID_SIA/KEY/4A46321737F890F654D632103F86B4F3

6 **CSV protocol via IP**

Format: ip//(Account Number)@(server ip):(port)/CSV

Example: ip://1234@54.183.182.247:8080/CSV

7 **CSV protocol via IP including username and password**

Format: ip//(Account Number)@(server ip):(port)/CSV/User/Pasword

Example: ip://1234@54.183.182.247:8080/CSV/abcd/1357

8 **Email**

Format: mailto:user@example.com

Example: mailto:john@gmail.com

- **Level**

  Select a reporting condition:

  All events: The system will report all events to this destination.

  Alarm events: The system will only report alarm event to this destination.

  Status events: The system will only report status event(non-alarm events) to this destination.

- **Group**

  Select a group for your report destination The system will make report according to the following principle:

  ☞ Group with higher priority will be reported first: Ex: Group 1 → Group 2 → Group 3….

  ☞ If reporting to the first destination in a group fails, the system will move on to the next report destination in the group.

  ☞ If reporting to one of the report destinations in a group is successful, the system will consider reporting to this group successful and stop reporting to rest of the destinations in the group. It will then move on to report to the next group.

  ☞ If reporting to all destinations in a group fails, the system will retry report to group according to retry times set below. If reporting is still unsuccessful after retries, the system will move on to report the the next group according to Essential/Optional setting below.

  ☞ After completing a round of reporting (From Group 1 → Group 2 ….. →Group5), If there is any group set as Essential which has not received report successfully, the system will restart the reporting cycle to retry reporting until every group set as Essential is reported successfully.

- **Essential/Optional**

  Essential: the system will report to all groups set as **Essential**. The system will never give up trying to report to any group set as Essential until at least one of the destinations in every Essential group successfully receives the report. Group 1 is always set as **Essential** and cannot be changed.

  Optional: The system will only report to group set as **Optional** when reporting to its previous group fails. For example: if Group 3 is set is optional, the Control Panel will only report to Group 3 if reporting to Group 2 fails.

- **1 Retry/ 3 Retry/ 5 Retry/ 10 Retry/ 99 Retry:**

If reporting to all destinations in a group fails, the system will retry reporting to the group according to the retries times set here.

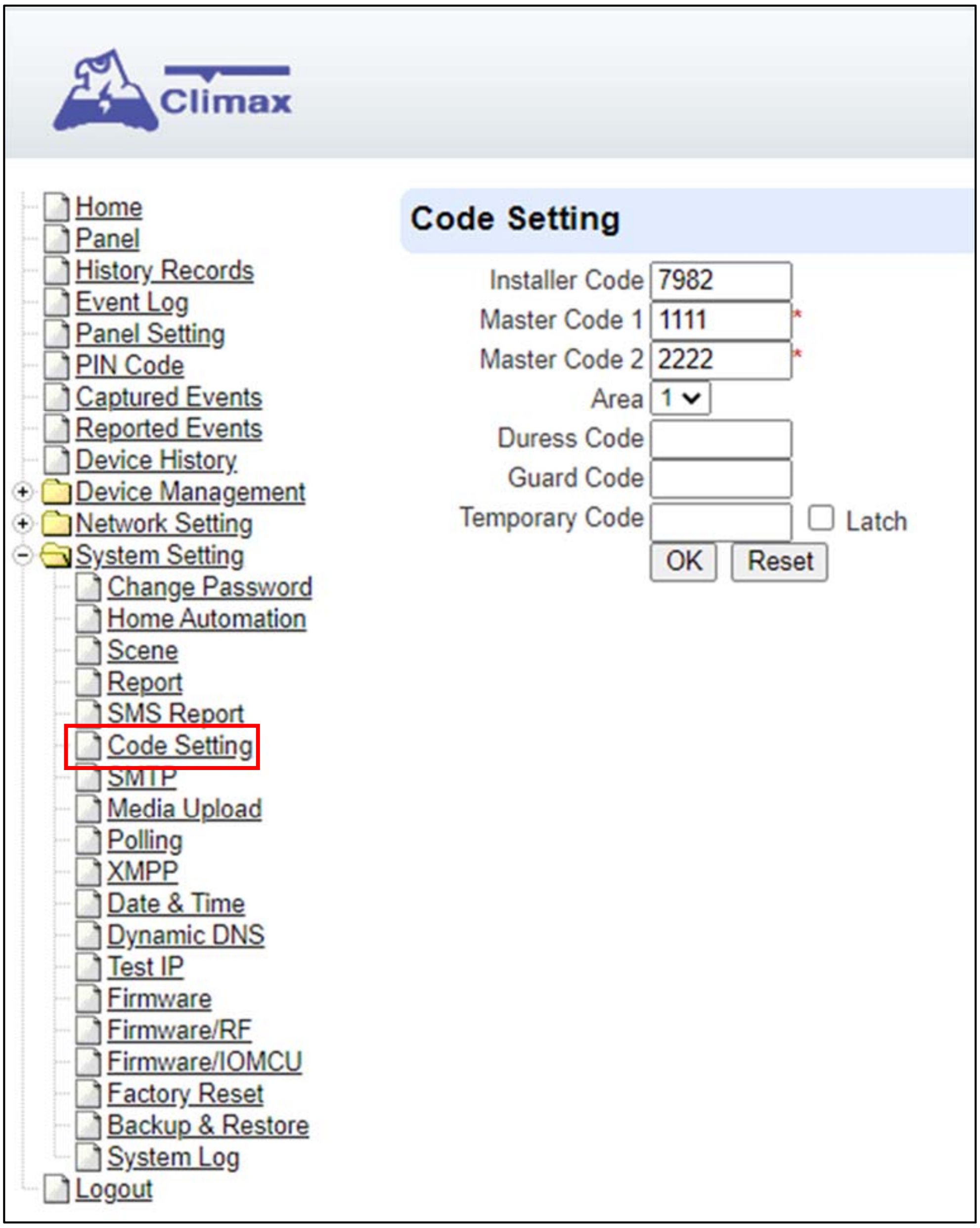
<NOTE>

- When the panel is registered into Climax's Home Portal Server, URL1 will be filled in with Home Portal Server report information. Do not change the information once registration is complete or reporting to Home Portal Server may encounter error.
- After registering the panel in Home Portal Server, if you wish to set more reporting destination, the new report destination should be set to different group than URL1 otherwise it may not be able to receive report successfully.

8.5. Code Settings

The Duress Code, Master Code & Temporary Code adds the flexibility of different security level for operation in **Code Settings** menu.

Step 1. Key in your preferred 4-6 digit **Installer Code**, **Duress Code**, **Master Code**, and/or **Temporary Code**.



Code Setting

Installer Code 7982

Master Code 1 1111 *

Master Code 2 2222 *

Area 1

Duress Code

Guard Code

Temporary Code □ Latch

Step 2. You can also choose to have Latch Option On / Off for Temporary Code by tick the Latch Option box and press **OK** to confirm the settings.

- **Installer Code**

  The Installer Code is used for SMS Remote Programming, when sending a remote programming message, the user needs to enter Installer Code in the message to be able to program the system. The default Installer code is: **7982**.

- **Master Code**

  The default Master Code for Area 1 and Area 2 are: 1111 and 2222 respectively.

- **Area**

  Each Area has different Duress Code, Master Code, and Temporary Code. Select the Area to program the code setting in this area.

- **Duress Code**

  The Duress Code is designed for transmitting a secret & silence alarm.

  When Duress Code is used for accessing the system, the Control Panel will report a secret alarm message without sounding the siren to the Central Monitoring Station to indicate of a **Duress Situation in Progress**.

  The Duress Code consists of 4-6 digits and is not activated as default by the factory.

- **Guard Code**

  The Guard Code is designed for security patrol personnel to arm/disarm the system. It can be set the same as a User PIN Code.

  The Guard Code consists of 4-6 digits and is not activated as default by the factory.

- **Temporary Code**

  Temporary Code is also used to arm/disarm the system, but it is for a temporary user. The temporary Code is **ONLY** valid for one-access per arming and disarming. Afterwards, the Temporary Code will be automatically erased and needs to be reset for a new Temporary user.

  The Temporary Code consists of 4-6 digits and is not activated as default by the factory.

- **Latch Option**

  This is to program the Latch Key Reporting feature for Temporary Code. Please click the box to select the options.

  ☑ Latch → **Latch Report ON** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will transmitt Contact ID code / SMS message / GPRS reporting (according to pre-setting) to notify the Central Monitoring Station.

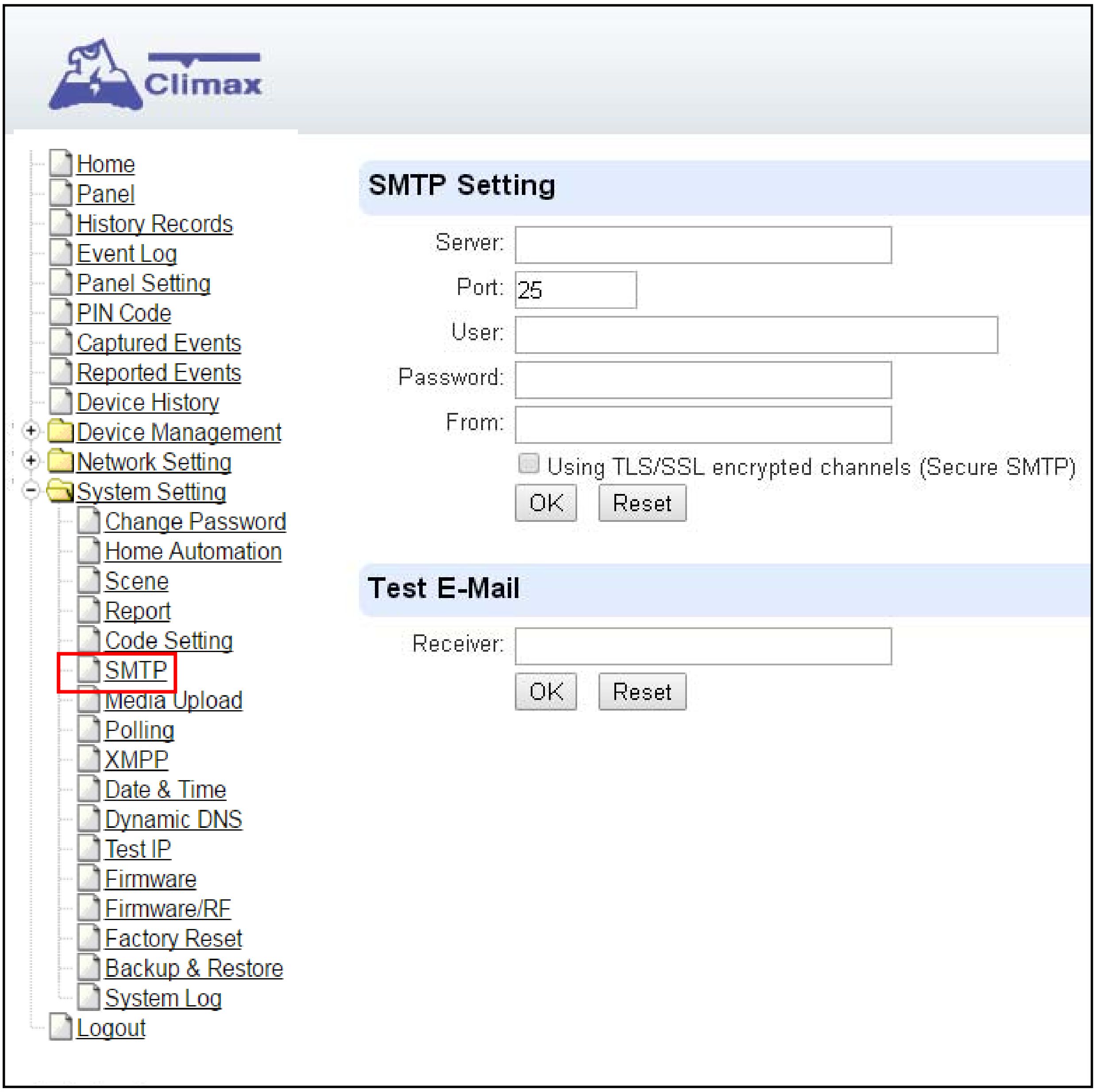
  □ Latch → **Latch Reprot OFF** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will NOT transmit reporting(s) to notify the Central Monitoring Station.

- **Delete**

  Except Master Code which can’t be disabled in any way, Temporary and Duress Code can be disabled by cleaning the code box and leaving the box as blank.

8.6. SMTP Setting

Program the mail server related settings. The email account you set here would be used to send report for events or picture and video clip captured by PIR Camera and PIR Video Camera.



SMTP Setting

Server:

Port: 25

User:

Password:

From:

□ Using TLS/SSL encrypted channels (Secure SMTP)

OK Reset

Test E-Mail

Receiver:

OK Reset

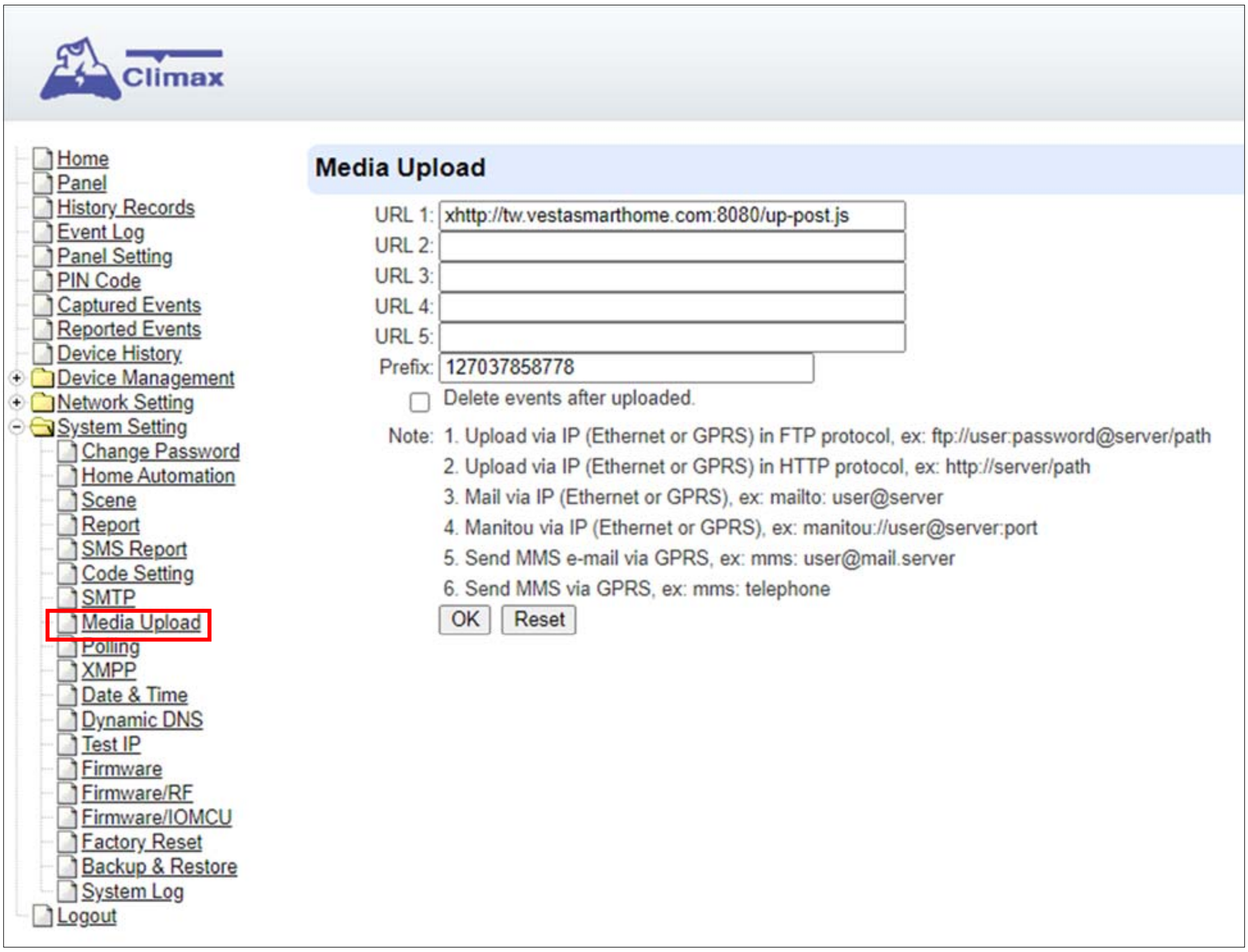
Step 1. Enter the following settings:

- **Server:** set the mail server (max. 60 digits/alphabets).
- **Port**: set the port number (max. 5 digits/alphabets).
- **User:** set the mail account name (max. 30 digits/alphabets).
- **Password:** set the password corresponding to the mail account name (max. 30 digits/alphabets).
- **From:** set the email address according to your mail sever and account name. If your mail server supports other email address, you can enter the email address here. (max. 30 digits/alphabets).
- **Using TLS/SSL encrypted channels (Secure SMTP):**If your mail server uses TLS or SSL encryption method for secure transfer, please click the box to enable the setting

Step 2. Click **OK** to confirm the setting.

8.7. Media Upload

The system can deliver captured images and video clips captured by PIR Cameras and PIR Video Camera to cell phone, email or FTP.



Media Upload

URL 1: xhttp://tw.vestasmarthome.com:8080/up-post.js

URL 2:

URL 3:

URL 4:

URL 5:

Prefix: 127037858778

□ Delete events after uploaded.

Note: 1. Upload via IP (Ethernet or GPRS) in FTP protocol, ex: ftp://user:password@server/path

2. Upload via IP (Ethernet or GPRS) in HTTP protocol, ex: http://server/path

3. Mail via IP (Ethernet or GPRS), ex: mailto: user@server

4. Manitou via IP (Ethernet or GPRS), ex: manitou://user@server:port

5. Send MMS e-mail via GPRS, ex: mms: user@mail.server

6. Send MMS via GPRS, ex: mms: telephone

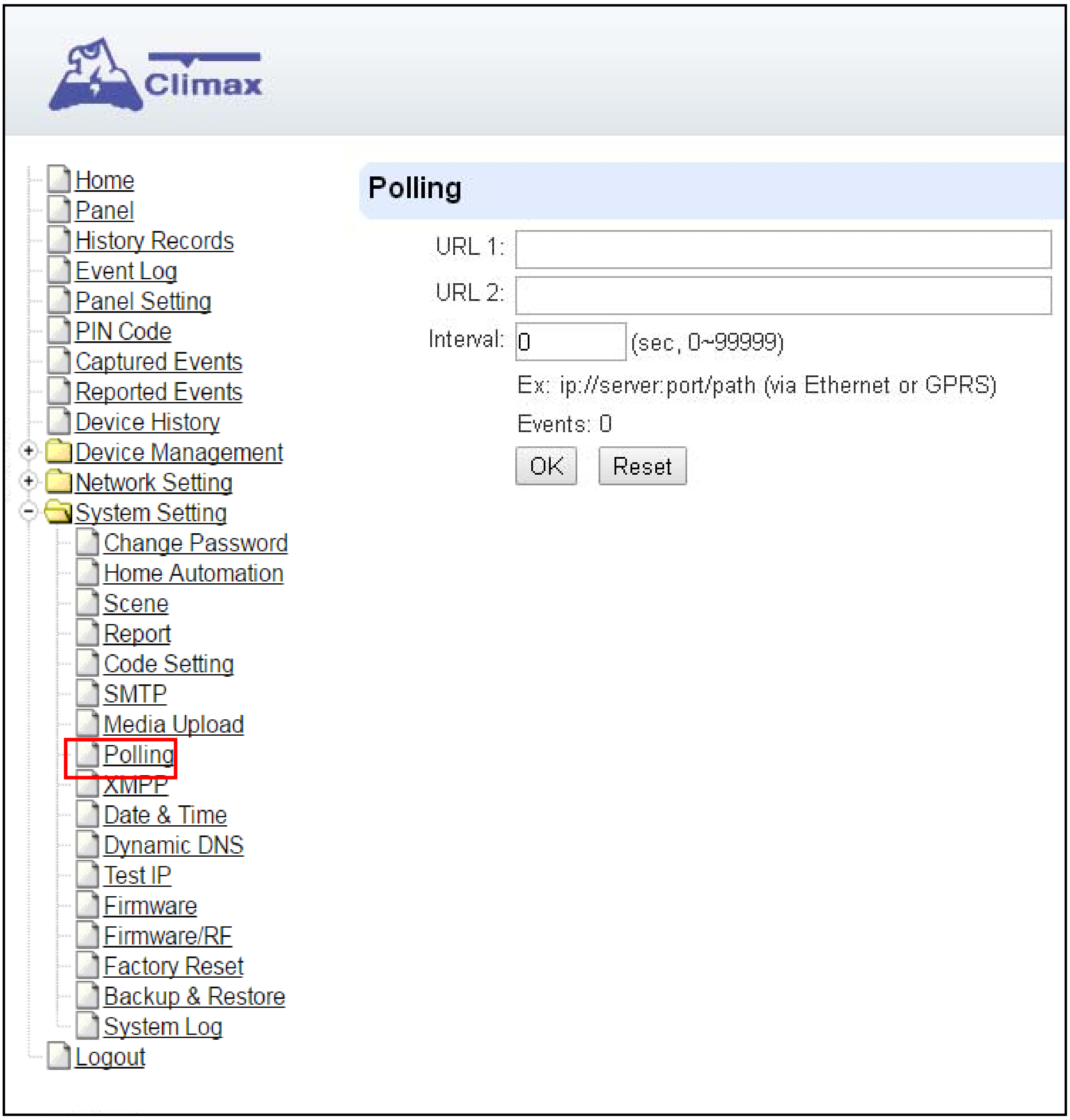
- **FTP:** ftp://user.password@server/path
- **HTTP:** http://ip:port/path
- **Email**: mailto:user@server (transmitting an alarm image over Ethernet)
- **Manitou**: manitou://user@server:port
- **MMS via Telephone**: mms: telephone number
- **MMS via GPRS**: mms: user@mail.server (transmitting an alarm image over MMS)

<NOTE>

- If “**Deleted events after uploaded**” is checked, the system will automatically clear all captured images which are displayed in the Captured Events menu after it successfully sends out those captured images to preset reporting destinations.

8.8. Polling

The polling function enables the Control Panel to query the destiation you set (URL1 or URL2) in turn as to whether it has any data to transmit.



Polling

URL 1:

URL 2:

Interval: 0 (sec, 0~99999)

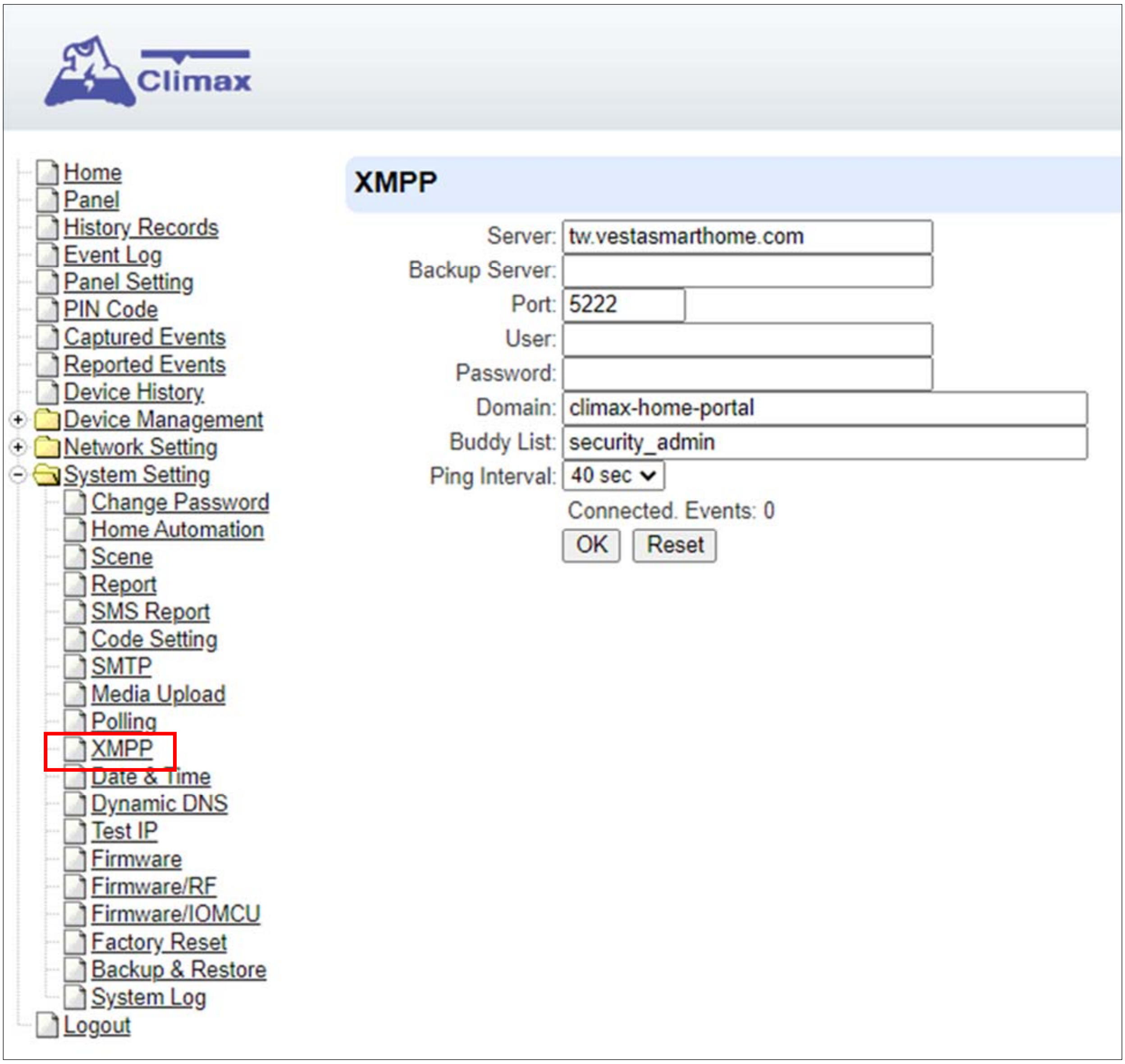
Ex: ip://server:port/path (via Ethernet or GPRS)

Events: 0

- **URL/URL2:** ip://server:port/path
- **Interval :** interval time of polling

8.9. XMPP

XMPP setting enables the Control Panel to query the set destination. This setting is required for the Control Panel to connect to Climax's Home Portal Server for remote control. If the panel is disconnected from the server, it will retry connection every 3 minutes.



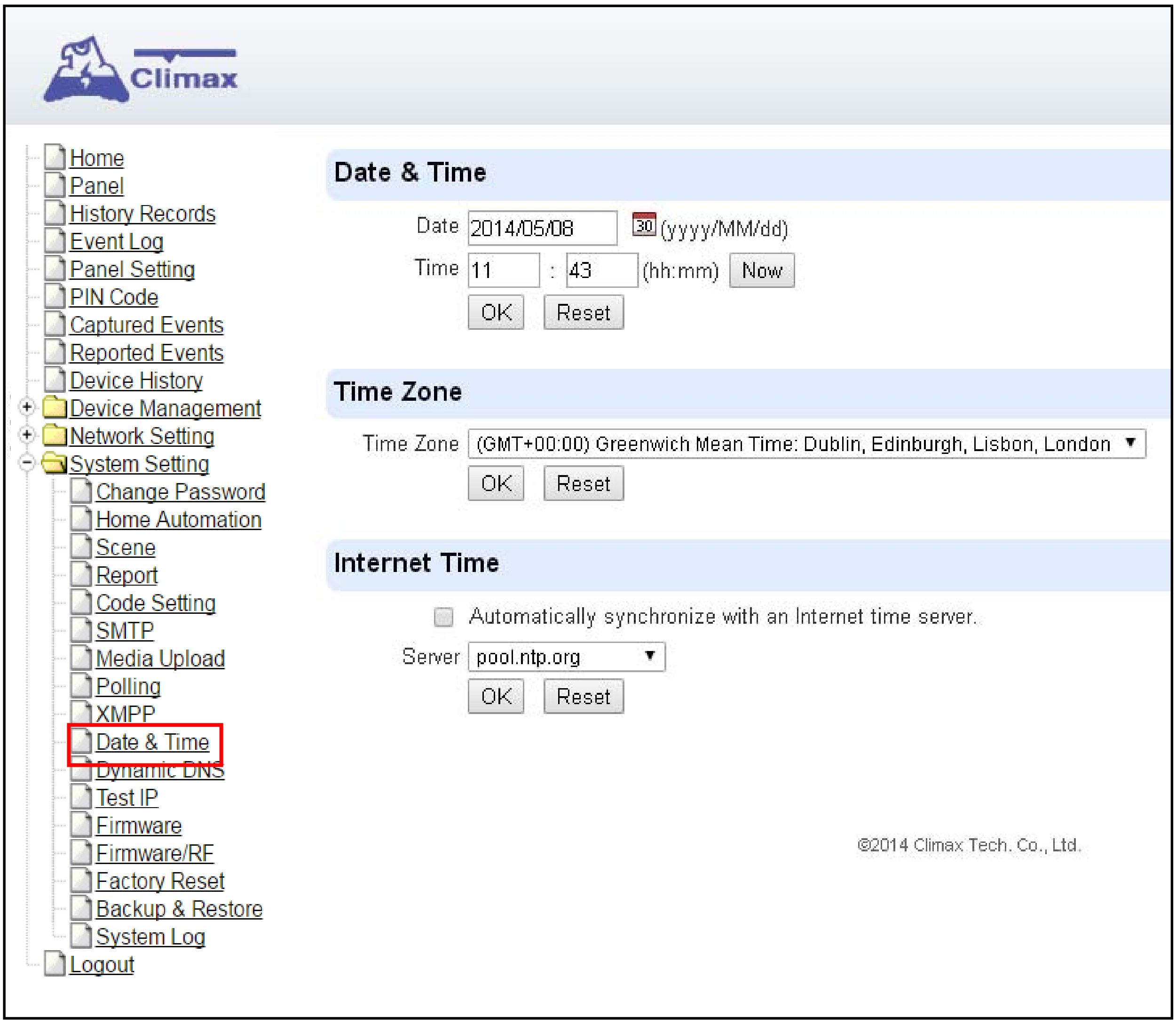
XMPP

Server: tw.vestasmarthome.com
Backup Server:
Port: 5222
User:
Password:
Domain: climax-home-portal
Buddy List: security_admin
Ping Interval: 40 sec
Connected. Events: 0

- **Server: server address** (dependent upon default firmware)
  US server: us.vestasmarthome.com
  EU server: eu.vestasmarthome.com
  Taiwan server: tw.vestasmarthome.com
- **Port**: server's port number
- **User**: authorized user account name
- **Password**: authorized user password
- **Domain**: domain address
- **Buddy List**: contact destination
- **Ping Interval**: server connection test interval

8.10. Date & Time

Program the current **Date** & **Time** and set automatic synchronization with internet time server.



Date & Time

Date 2014/05/08 (yyyy/MM/dd)

Time 11 : 43 (hh:mm)

Time Zone

Time Zone (GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Internet Time

□ Automatically synchronize with an Internet time server.

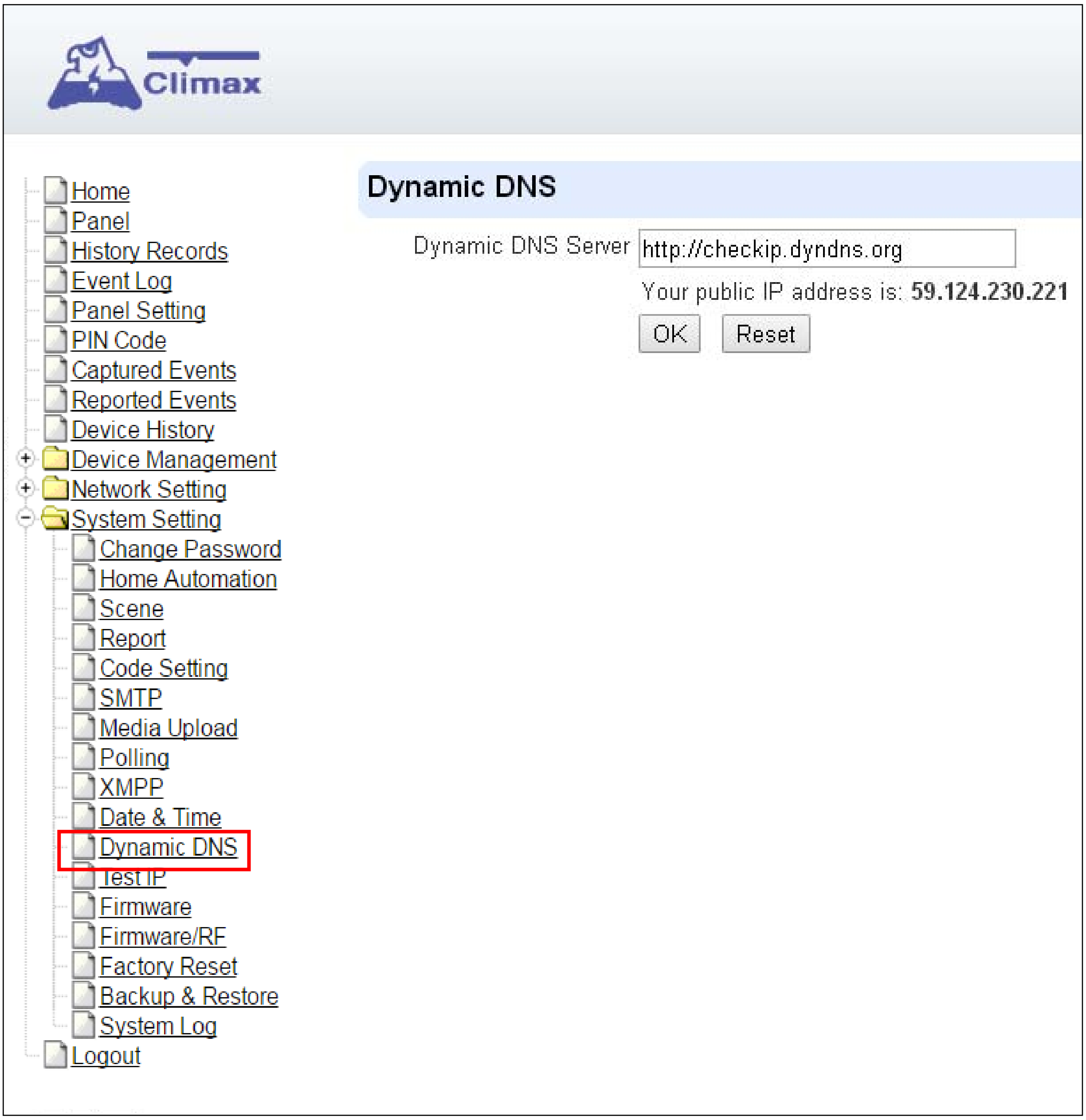
Server pool.ntp.org

©2014 Climax Tech. Co., Ltd.

- **Date & Time:** set current month, date and time.
- **Time Zone:** choose your time zone, and then the system will calculate the daylight saving time automatically (if necessary).
- **Internet Time:** the system will automatically synchronize with an internet time server. Tick the check box to enable this function. Available options: time1.google.com, pool.ntp.org, time.nist.gov and tick.usno.navy.mil.

8.11. Dynamic DNS

This page is used to provide you the Control Panel's current public IP address.



Dynamic DNS

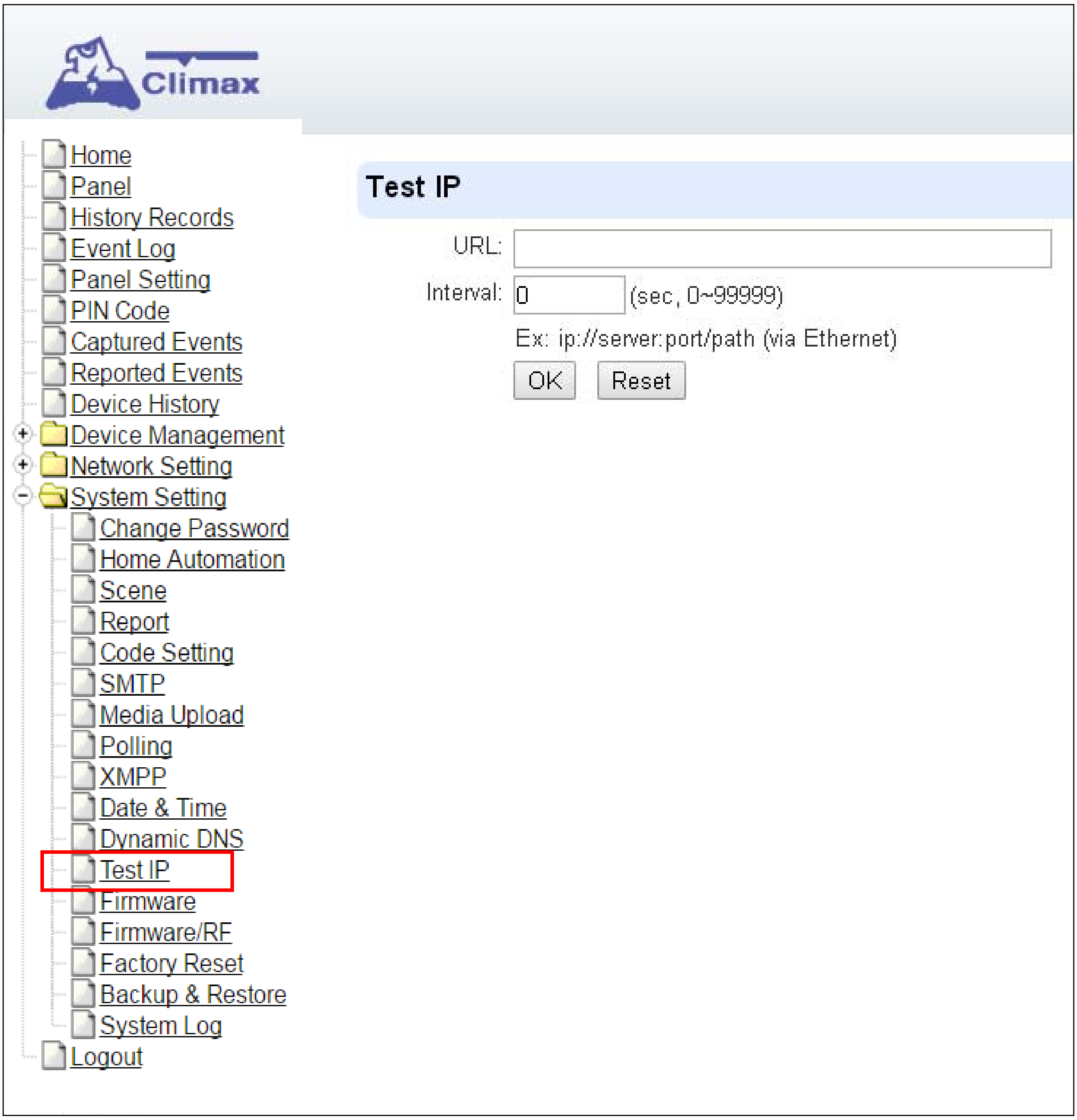
Dynamic DNS Server: http://checkip.dyndns.org

Your public IP address is: **59.124.230.221**

- **Dynamic DNS Server:** http://checkip.dyndns.org

8.12. Test IP

This is for you to test the Control Panel internet connection.



Test IP

URL:

Interval: 0 (sec, 0~99999)

Ex: ip://server:port/path (via Ethernet)

Step 1. Enter the URL destination you want to test connection to.

Step 2. Enter the test interval.

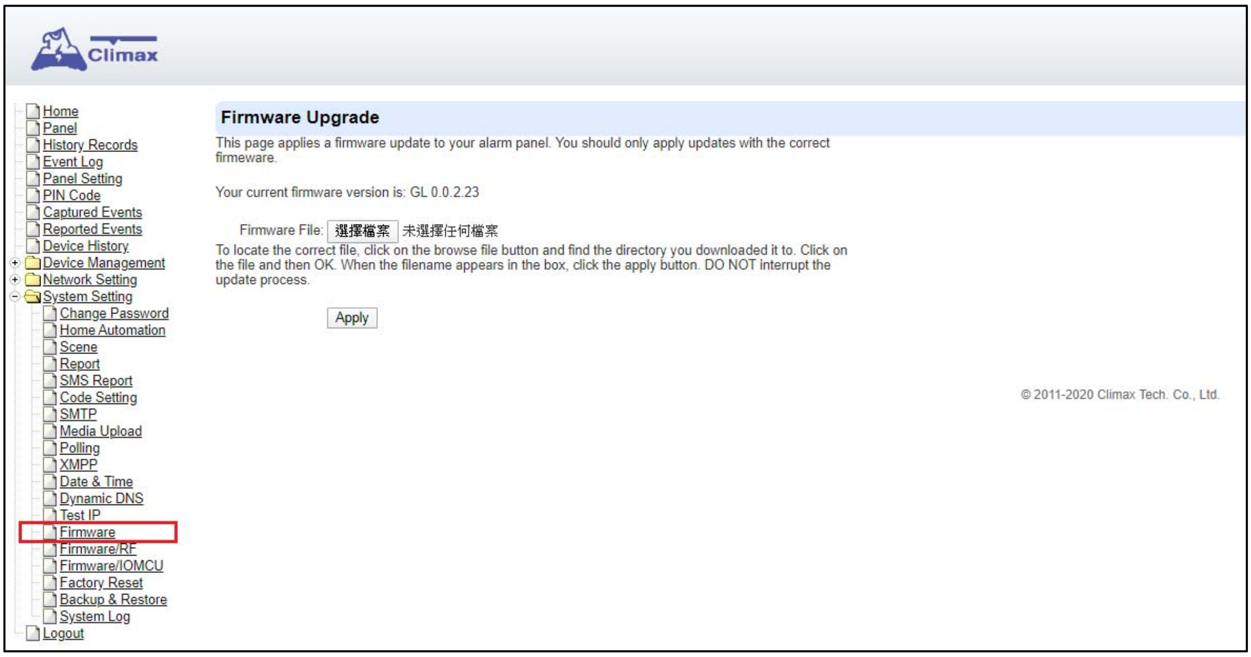
Step 3. Click “OK”

You can check the test connect result in **System Log**.

8.13 Firmware Upgrade

You can update the firmware via this web page.

Step 1. Click on “**Choose File**” and locate the latest firmware file in your PC.



Firmware Upgrade

This page applies a firmware update to your alarm panel. You should only apply updates with the correct firmeware.

Your current firmware version is: GL 0.0.2.23

Firmware File: 未選擇任何檔案

To locate the correct file, click on the browse file button and find the directory you downloaded it to. Click on the file and then OK. When the filename appears in the box, click the apply button. DO NOT interrupt the update process.

© 2011-2020 Climax Tech. Co., Ltd.

Step 2. Press “**Apply**” to upload the latest firmware to Control Panel

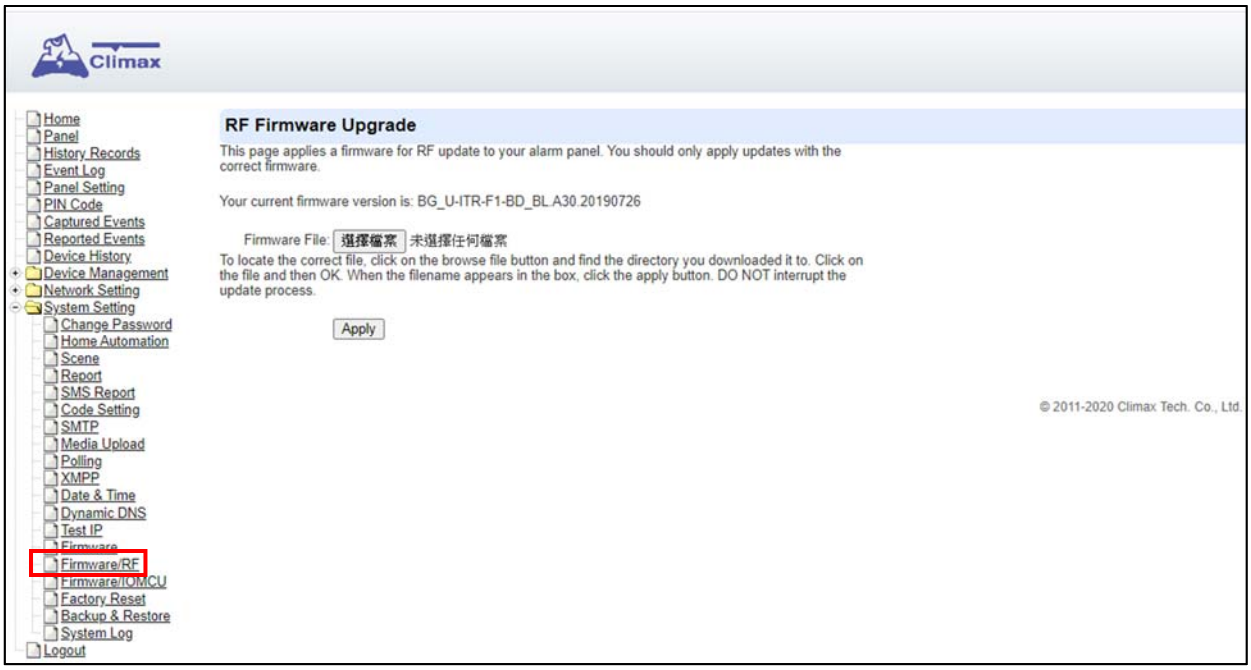
Step 3. Wait for 1 min and do NOT power off during this time.

Step 4. Once Firmware upgrading is complete, the Control Panel will reboot automatically

8.14. RF Firmware Upgrade

You can update the Control Panel's RF firmware via this web page.

Step 1. Click on "**Choose File**" and locate the latest firmware file ("**unzipped image.bin**" file) in your PC.



RF Firmware Upgrade

This page applies a firmware for RF update to your alarm panel. You should only apply updates with the correct firmware.

Your current firmware version is: BG_U-ITR-F1-BD_BL.A30.20190726

Firmware File: 未選擇任何檔案

To locate the correct file, click on the browse file button and find the directory you downloaded it to. Click on the file and then OK. When the filename appears in the box, click the apply button. DO NOT interrupt the update process.

© 2011-2020 Climax Tech. Co., Ltd.

Step 2. Press "**Apply**" to upload the latest firmware to Control Panel

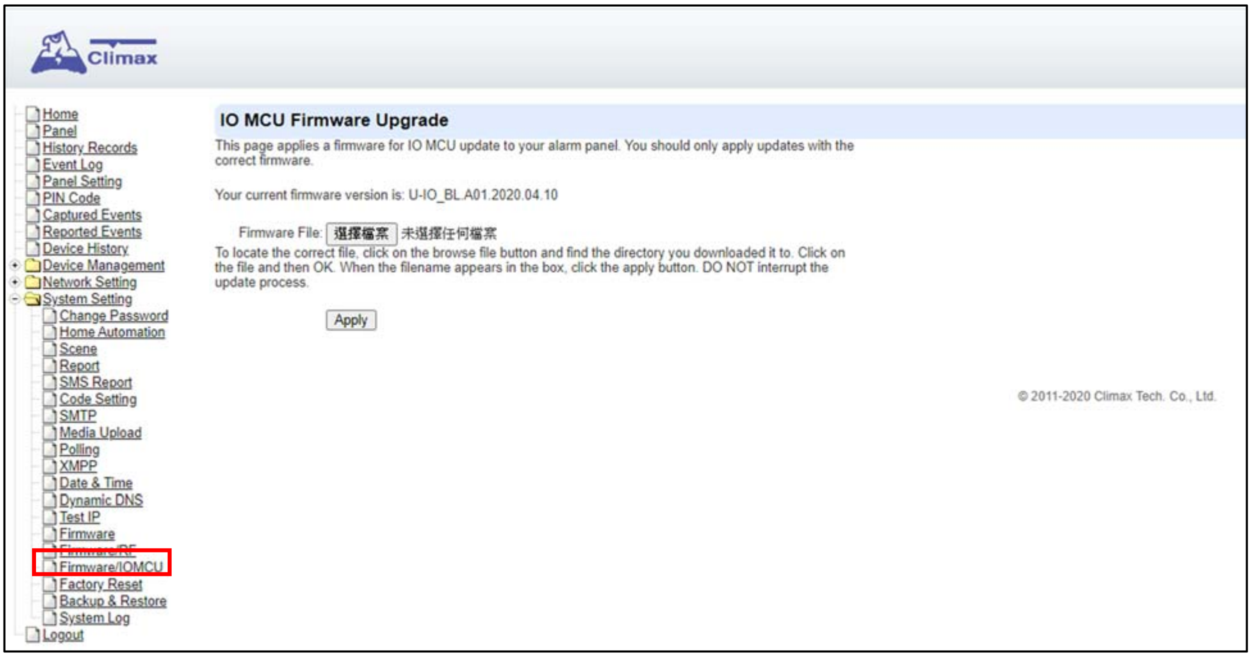
Step 3. Wait for 1 min and do NOT power off during this time.

Step 4. Once Firmware upgrading is complete, the Control Panel will reboot automatically

8.15. IO MCU Firmware Upgrade

Step 1. Click “**Firmware/IOMCU**” to enter this page.

Step 2. Click on “**Choose File**” and locate the latest firmware file in your PC.



IO MCU Firmware Upgrade

This page applies a firmware for IO MCU update to your alarm panel. You should only apply updates with the correct firmware.

Your current firmware version is: U-IO_BL.A01.2020.04.10

Firmware File: 選擇檔案 未選擇任何檔案

To locate the correct file, click on the browse file button and find the directory you downloaded it to. Click on the file and then OK. When the filename appears in the box, click the apply button. DO NOT interrupt the update process.

Apply

© 2011-2020 Climax Tech. Co., Ltd.

Step 3. Press “**Apply**” to upload the latest firmware to Control Panel

Step 4. Wait for 1 min and DO NOT power off during this time.

Step 5. Once Firmware upgrading is complete, the Panel will reboot automatically.

8.16. Factory Reset

Yan can clear all programmed parameters in the Control Panel and reset it to Factory Default.

Once the **Factory Reset** is executed, all the programmed settings will returned to its default value, and all the learnt-in devices will be removed. You will need to restart the programming and learning process again.

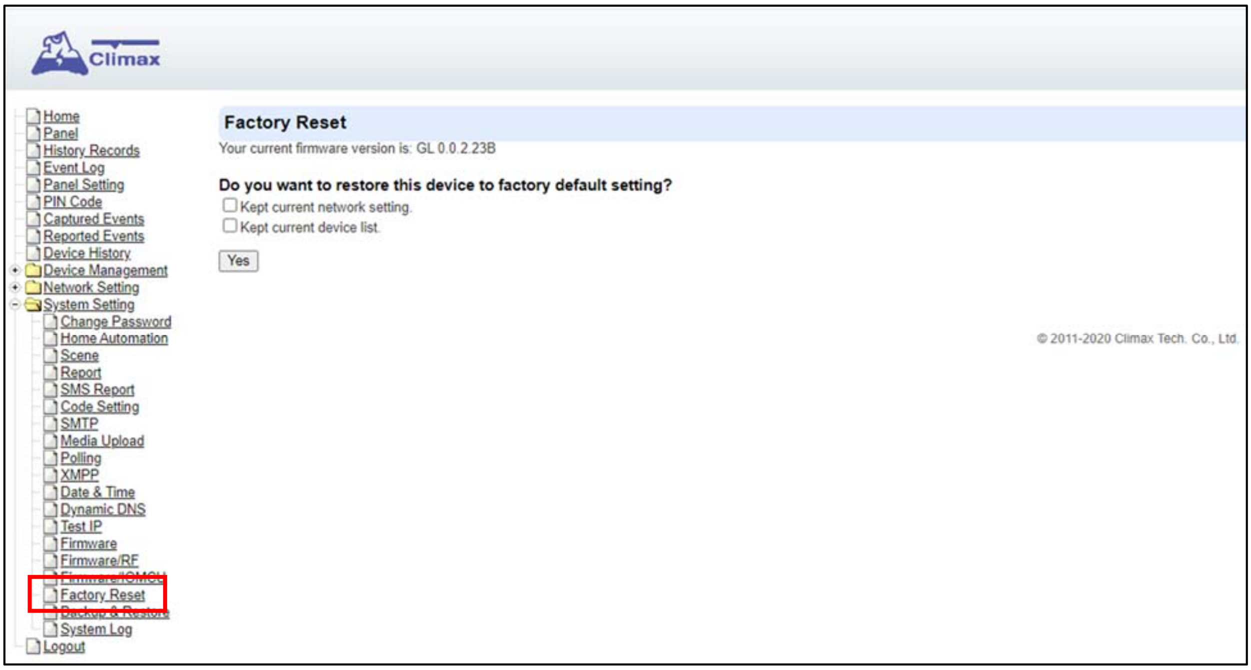
8.16.1 Remote Reset

Step 1. Tick the **Kept current network setting** to keep the current Network settings. Otherwise, the system will reset its value back to factory default. Tick the **Kept current device list** box to keep the current learnt-in devices. Otherwise, the system will reset its value back to factory default.

Step 2. Press **Yes** to continue the Reset procedure.

Step 3. Wait for 1 min and do NOT power off during this time.

Step 4. Once reset is complete, it will automatically reboot the main unit.



Factory Reset

Your current firmware version is: GL 0.0.2.23B

Do you want to restore this device to factory default setting?

□ Kept current network setting.

□ Kept current device list.

8.16.2 Local Reset

Step 1. Slide battery switch to OFF.

Step 2. Press and hold the learn button.

Step 3. Keep holding the reset button until you hear continuous beeps. The 3 LEDs will flash 3 times.

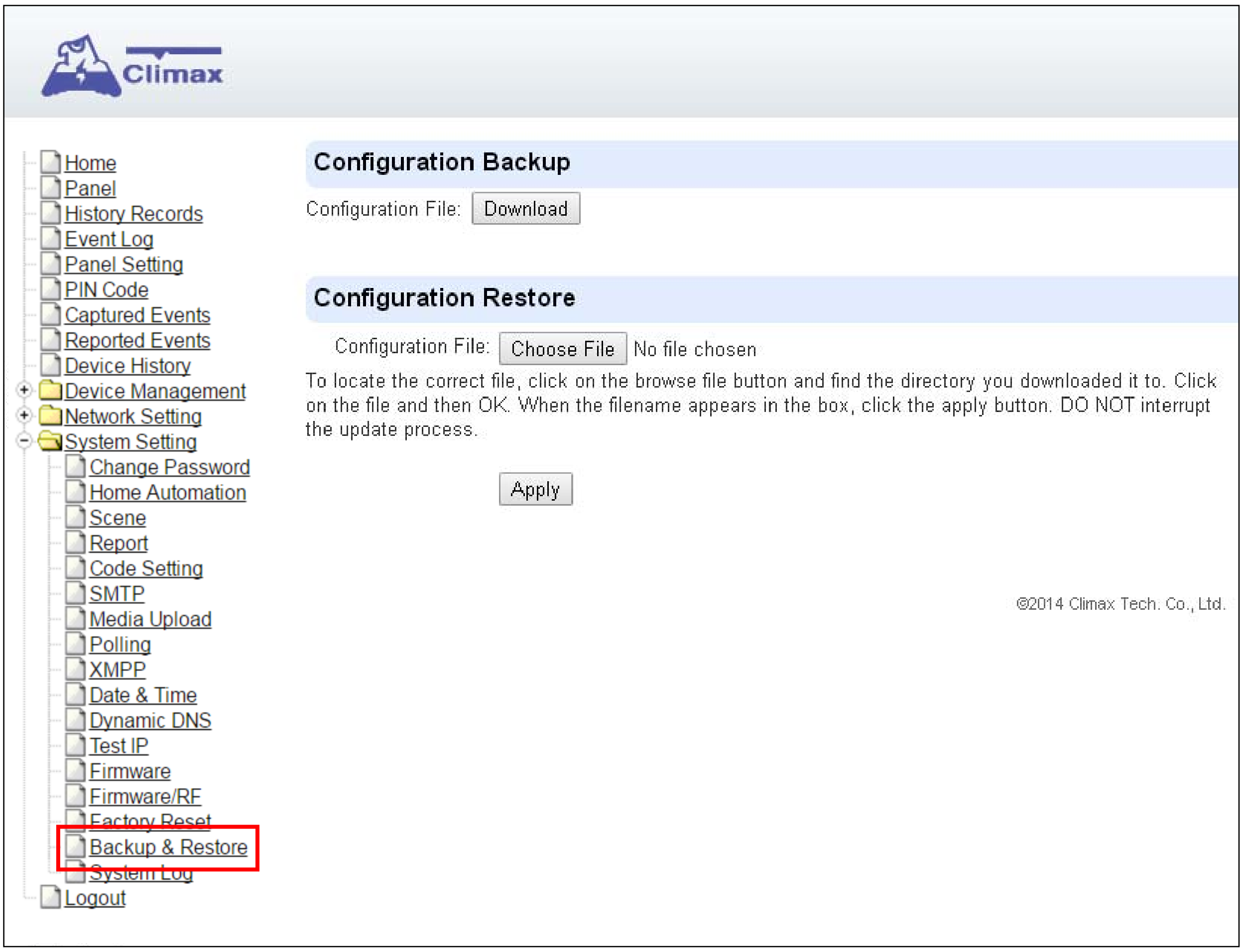
Step 4. Release the button and wait for the Control Panel to reboot.

8.17. Backup & Restore

Yan can back up all programmed parameters and save these programmed values into a file. Besides, you also can restore pre-programmed settings.

8.17.1 Backup Data

Click **Download**, and you can back up all programmed data and save these programmed values into a file.



To locate the correct file, click on the browse file button and find the directory you downloaded it to. Click on the file and then OK. When the filename appears in the box, click the apply button. DO NOT interrupt the update process.

©2014 Climax Tech. Co., Ltd.

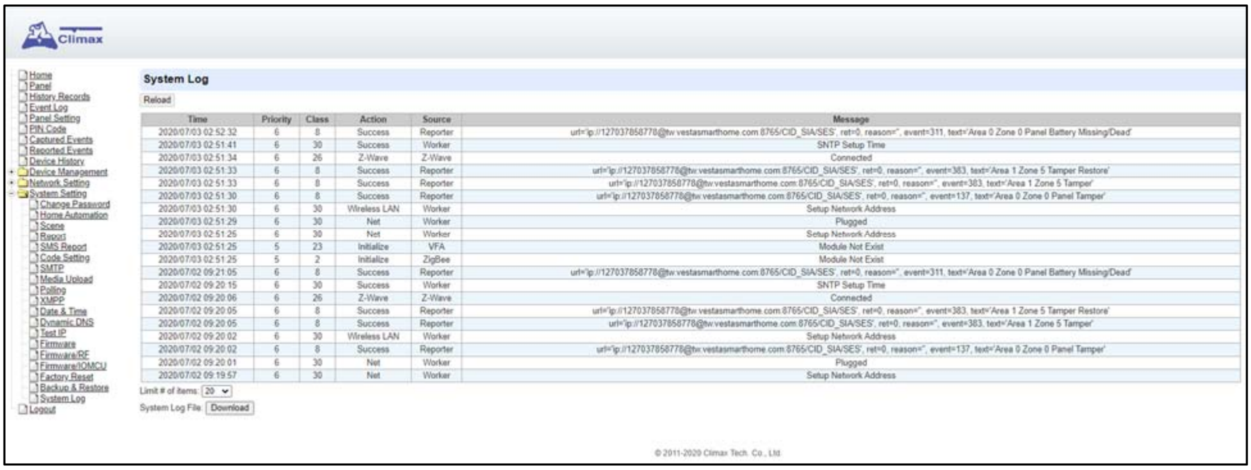
8.17.2 Restore Settings

Step 1. Click **Choose File**, select a saved file.

Step 2. Click **Apply** to apply the pre-programmed values to the main unit.

8.18. System Log

The sytem log webpage logs the control panel's detail system operation history.



System Log

Time	Priority	Class	Action	Source	Message
2020/07/03 02:52:32	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=311, text='Area 0 Zone 0 Panel Battery Missing/Dead'
2020/07/03 02:51:41	6	30	Success	Worker	SNTP Setup Time
2020/07/03 02:51:34	6	26	Z-Wave	Z-Wave	Connected
2020/07/03 02:51:33	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=383, text='Area 1 Zone 5 Tamper Restore'
2020/07/03 02:51:33	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=383, text='Area 1 Zone 5 Tamper'
2020/07/03 02:51:30	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=137, text='Area 0 Zone 0 Panel Tamper'
2020/07/03 02:51:30	6	30	Wireless LAN	Worker	Setup Network Address
2020/07/03 02:51:29	6	30	Net	Worker	Plugged
2020/07/03 02:51:26	6	30	Net	Worker	Setup Network Address
2020/07/03 02:51:25	5	23	Initialize	VFA	Module Not Exist
2020/07/03 02:51:25	5	2	Initialize	ZigBee	Module Not Exist
2020/07/02 09:21:05	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=311, text='Area 0 Zone 0 Panel Battery Missing/Dead'
2020/07/02 09:20:15	6	30	Success	Worker	SNTP Setup Time
2020/07/02 09:20:06	6	26	Z-Wave	Z-Wave	Connected
2020/07/02 09:20:05	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=383, text='Area 1 Zone 5 Tamper Restore'
2020/07/02 09:20:05	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=383, text='Area 1 Zone 5 Tamper'
2020/07/02 09:20:02	6	30	Wireless LAN	Worker	Setup Network Address
2020/07/02 09:20:02	6	8	Success	Reporter	url='ip://127037858778@tw.vestasmarthome.com:8765/CID_SIA/SES', ret=0, reason='', event=137, text='Area 0 Zone 0 Panel Tamper'
2020/07/02 09:20:01	6	30	Net	Worker	Plugged
2020/07/02 09:19:57	6	30	Net	Worker	Setup Network Address

Limit # of items: 20

System Log File: Download

© 2011-2020 Climax Tech. Co., Ltd.

- **System Log File Download**: Click to download a detail log files into your computer for more information.

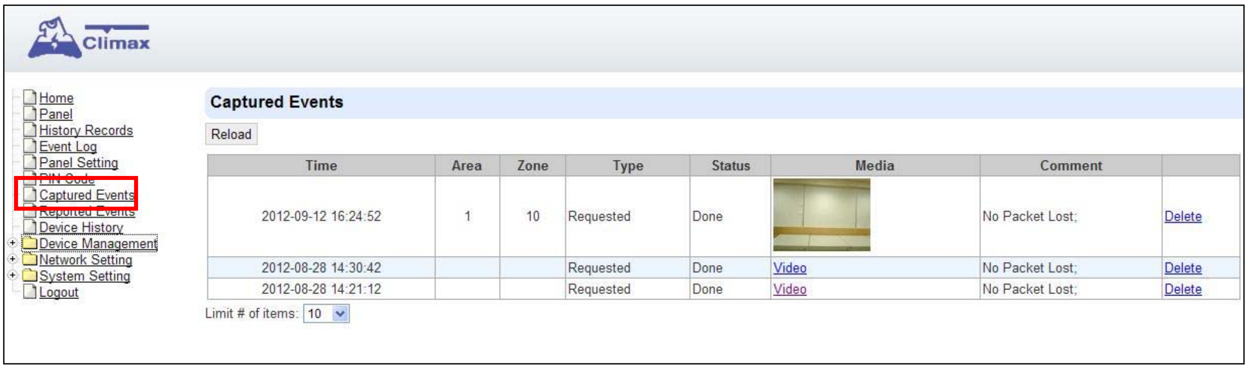
9. Event & History

This section introduces event history of the system.

9.1. Captured Events

This page stores all captured pictures and videos by PIR Camera and PIR Video Camera. When a PIR Camera is triggered, it will take 3 pictures in quick succession, when a PIR Video Camera is triggered, it will take a 10-second video clip. You can also request the PIR Camera to take a picture and PIR Video Camera to take a 10-second video clip manually.

Caputred events will be displayed in this page with their information for you to view. Simply click on the picture or video to view them. You can also click **Delete** to delete the event.



Captured Events

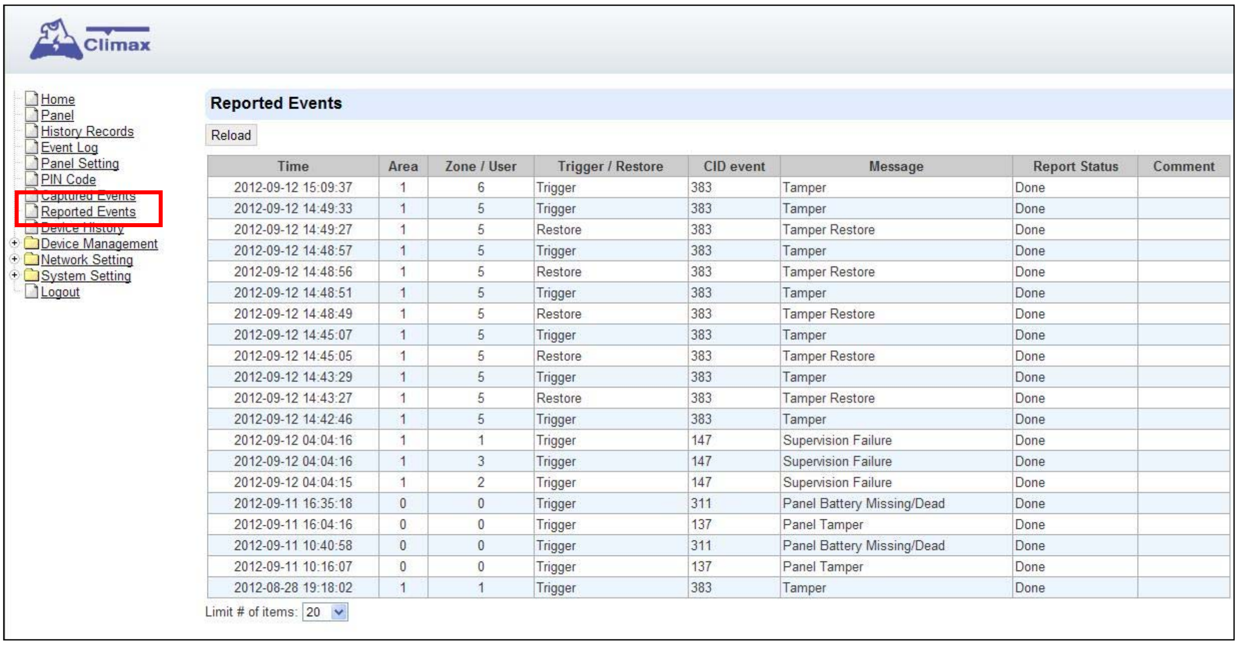
Time	Area	Zone	Type	Status	Media	Comment	
2012-09-12 16:24:52	1	10	Requested	Done		No Packet Lost;	Delete
2012-08-28 14:30:42			Requested	Done	Video	No Packet Lost;	Delete
2012-08-28 14:21:12			Requested	Done	Video	No Packet Lost;	Delete

Limit # of items: 10

- **Reload :** Click to refresh the page content
- **Limit # of Items:** Click the drop down menu on the page to select the numbers of captured events you want to display.

9.2. Reported Events

This page stores all triggered events by the control panel by recording the events' CID event code and report status.



Reported Events

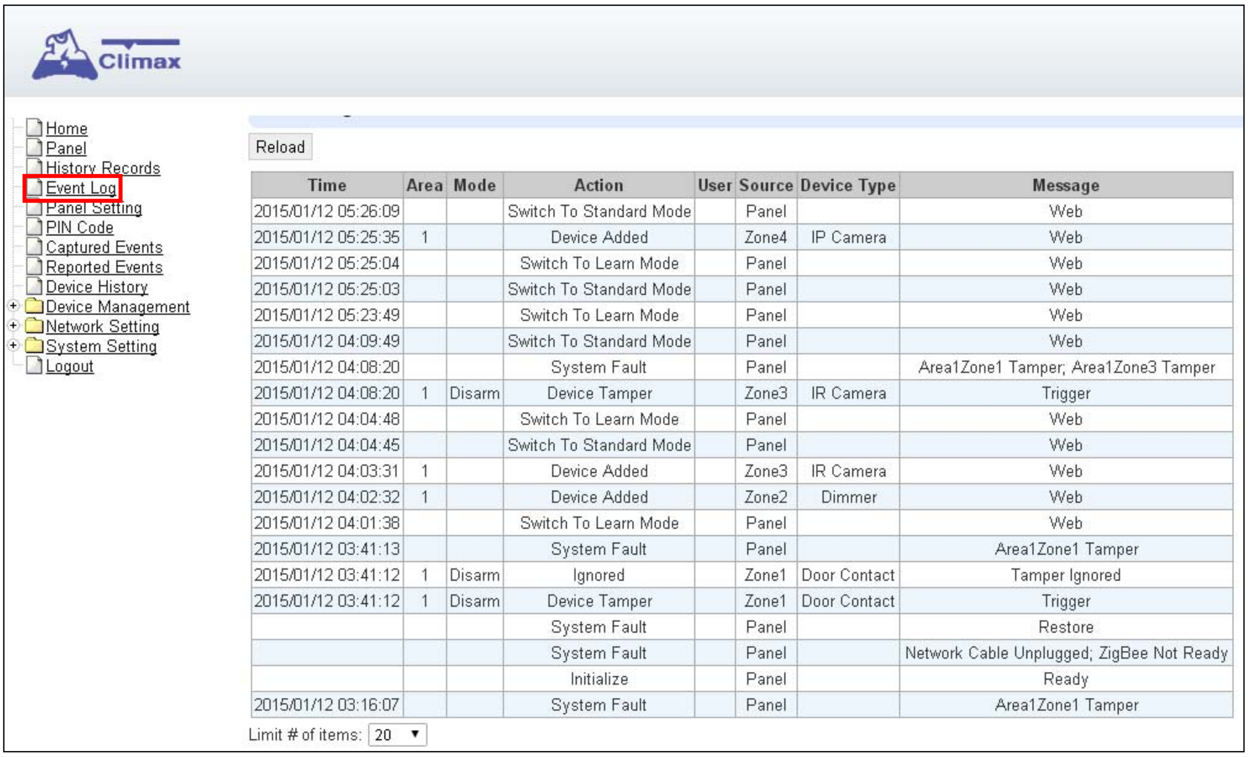
Time	Area	Zone / User	Trigger / Restore	CID event	Message	Report Status	Comment
2012-09-12 15:09:37	1	6	Trigger	383	Tamper	Done	
2012-09-12 14:49:33	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:49:27	1	5	Restore	383	Tamper Restore	Done	
2012-09-12 14:48:57	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:48:56	1	5	Restore	383	Tamper Restore	Done	
2012-09-12 14:48:51	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:48:49	1	5	Restore	383	Tamper Restore	Done	
2012-09-12 14:45:07	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:45:05	1	5	Restore	383	Tamper Restore	Done	
2012-09-12 14:43:29	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:43:27	1	5	Restore	383	Tamper Restore	Done	
2012-09-12 14:42:46	1	5	Trigger	383	Tamper	Done	
2012-09-12 04:04:16	1	1	Trigger	147	Supervision Failure	Done	
2012-09-12 04:04:16	1	3	Trigger	147	Supervision Failure	Done	
2012-09-12 04:04:15	1	2	Trigger	147	Supervision Failure	Done	
2012-09-11 16:35:18	0	0	Trigger	311	Panel Battery Missing/Dead	Done	
2012-09-11 16:04:16	0	0	Trigger	137	Panel Tamper	Done	
2012-09-11 10:40:58	0	0	Trigger	311	Panel Battery Missing/Dead	Done	
2012-09-11 10:16:07	0	0	Trigger	137	Panel Tamper	Done	
2012-08-28 19:18:02	1	1	Trigger	383	Tamper	Done	

Limit # of items: 20

- **Reload :** Click to refresh the page content
- **Limit # of Items:** Click the drop down menu on the pageto select the numbers of captured events you want to display.

9.3. Event Log

The Event Log page records specific actions performed by the Control Panel and accessory devices.



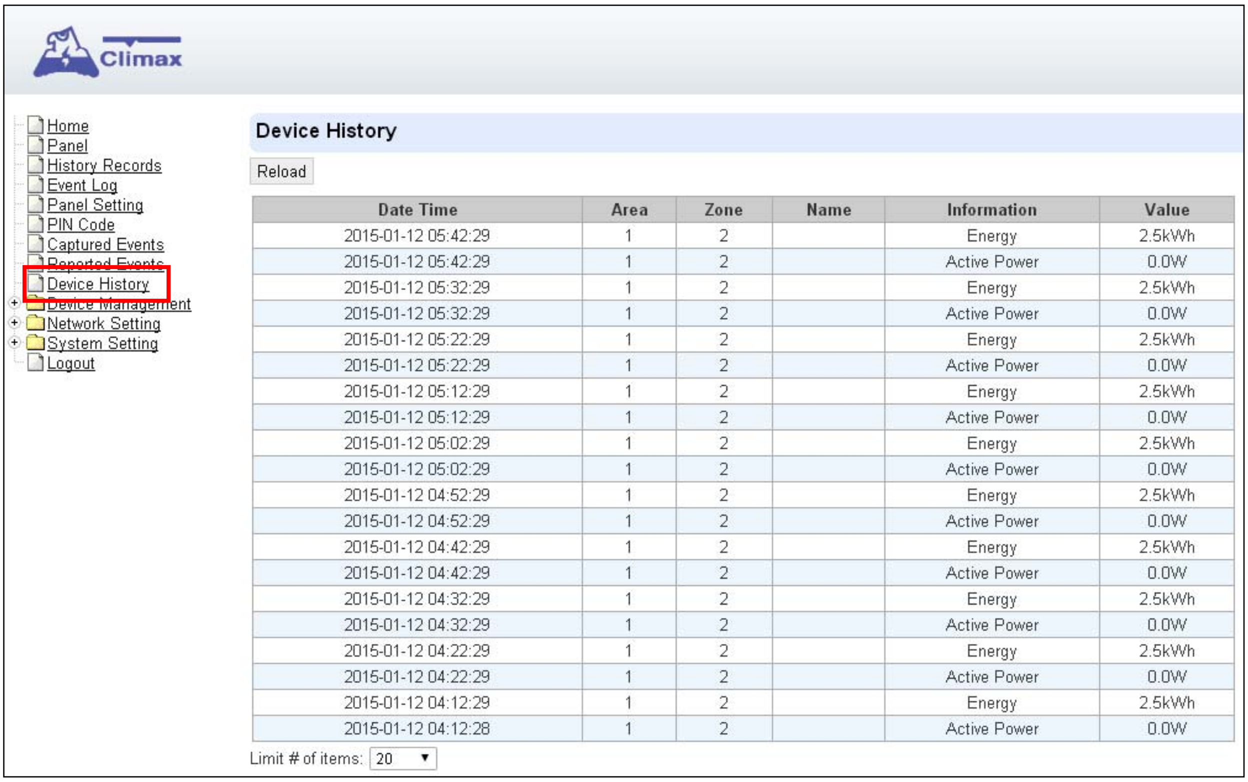
Time	Area	Mode	Action	User	Source	Device Type	Message
2015/01/12 05:26:09			Switch To Standard Mode		Panel		Web
2015/01/12 05:25:35	1		Device Added		Zone4	IP Camera	Web
2015/01/12 05:25:04			Switch To Learn Mode		Panel		Web
2015/01/12 05:25:03			Switch To Standard Mode		Panel		Web
2015/01/12 05:23:49			Switch To Learn Mode		Panel		Web
2015/01/12 04:09:49			Switch To Standard Mode		Panel		Web
2015/01/12 04:08:20			System Fault		Panel		Area1Zone1 Tamper; Area1Zone3 Tamper
2015/01/12 04:08:20	1	Disarm	Device Tamper		Zone3	IR Camera	Trigger
2015/01/12 04:04:48			Switch To Learn Mode		Panel		Web
2015/01/12 04:04:45			Switch To Standard Mode		Panel		Web
2015/01/12 04:03:31	1		Device Added		Zone3	IR Camera	Web
2015/01/12 04:02:32	1		Device Added		Zone2	Dimmer	Web
2015/01/12 04:01:38			Switch To Learn Mode		Panel		Web
2015/01/12 03:41:13			System Fault		Panel		Area1Zone1 Tamper
2015/01/12 03:41:12	1	Disarm	Ignored		Zone1	Door Contact	Tamper Ignored
2015/01/12 03:41:12	1	Disarm	Device Tamper		Zone1	Door Contact	Trigger
			System Fault		Panel		Restore
			System Fault		Panel		Network Cable Unplugged; ZigBee Not Ready
			Initialize		Panel		Ready
2015/01/12 03:16:07			System Fault		Panel		Area1Zone1 Tamper

Limit # of items: 20

- **Reload :** Click to refresh the page content
- **Limit # of Items:** Click the drop down menu on the pageto select the numbers of captured events you want to display.

9.4. Device History

You can track your ZigBee accessory device status history under **Device History**. For Power Switch Meter or Temperature Sensor, the update history power consumption or temperature ireading will be displayed under this page (the current info is also displayed under **Panel** and **PSS Control**).



Device History

Date Time	Area	Zone	Name	Information	Value
2015-01-12 05:42:29	1	2		Energy	2.5kWh
2015-01-12 05:42:29	1	2		Active Power	0.0W
2015-01-12 05:32:29	1	2		Energy	2.5kWh
2015-01-12 05:32:29	1	2		Active Power	0.0W
2015-01-12 05:22:29	1	2		Energy	2.5kWh
2015-01-12 05:22:29	1	2		Active Power	0.0W
2015-01-12 05:12:29	1	2		Energy	2.5kWh
2015-01-12 05:12:29	1	2		Active Power	0.0W
2015-01-12 05:02:29	1	2		Energy	2.5kWh
2015-01-12 05:02:29	1	2		Active Power	0.0W
2015-01-12 04:52:29	1	2		Energy	2.5kWh
2015-01-12 04:52:29	1	2		Active Power	0.0W
2015-01-12 04:42:29	1	2		Energy	2.5kWh
2015-01-12 04:42:29	1	2		Active Power	0.0W
2015-01-12 04:32:29	1	2		Energy	2.5kWh
2015-01-12 04:32:29	1	2		Active Power	0.0W
2015-01-12 04:22:29	1	2		Energy	2.5kWh
2015-01-12 04:22:29	1	2		Active Power	0.0W
2015-01-12 04:12:29	1	2		Energy	2.5kWh
2015-01-12 04:12:28	1	2		Active Power	0.0W

Limit # of items: 20

- **Reload :** Click to refresh the page content
- **Limit # of Items:** Click the drop down menu on the pageto select the numbers of captured events you want to display.

10. Appendix

10.1. Fault Event Description

During operation, when the panel detects faulty events, the panel will log the event and make reports. When fault events exist in the system, the panel Fault LED will light up and the panel will emit a beep every 30 seconds.

- **Fault Event Table**

Fault Event	Descriptions
Panel AC Failure	The Control Panel's AC power is disconnected When AC failure is detected, the panel will turn off both Ethernet and mobile network functions when idle to conserve power. Ethernet and mobile network will be activated temporarily when an event is detected by the panel (i.e. alarm trigger) to send report, and will turn off again after finishing report. Accessing the panel via remote server XMPP connection is disabled during AC failure.
Panel Low Battery	The panel's backup battery is only used when AC failure is detected. When the backup battery voltage is low, the panel low battery event is generated
Panel Tamper	The tamper switch on back of the panel is not compressed against the back cover. This means the panel's cover is opened and not properly sealed.
Battery Dead/Missing	The panel cannot detect backup battery, this means the battery is either dysfunctional, or the battery switch is not slid to ON position.
Interference/Jamming	The panel detects radio frequency jamming, which will affect its ability to receive signal from RF devices (Does not include ZigBee/Shutter Control/Wi-fi signal)
Device Low Battery	The accessory device at indicated zone number is low on battery
Device AC Failure	The accessory device at indicated zone number does not have AC power connection.
Device Tamper	The tamper switch of the device at indicated zone number is open
Device Supervision Failure	The panel was unable to receive supervision signal sent from accessory device at indicated zone number for the duration of Supervision Timer programmed. (i.e. If Supervision Timer is set to 12 hours, the panel will generate supervision failure event after failing to receive supervision signal for 12 hours)

10.2. Control Panel Mode and Response Table

For Alarm Activation by Events and Control Panel Responses, please refer to the following table:

Attribute	System Mode / Status					
	Disarm	Full Arm	Home Arm	Under Exit Timer	Under Exit Timer (No Response)	Under Entry Timer
No Response	No Response	No Response	No Response	Instant Burglar Alarm	No Response	No Response
Start Entry Delay 1	Instant Burglar Alarm (Interior)	Start Entry 1 → Burglar Alarm (Perimeter)	Start Entry 1 → Burglar Alarm (Interior)	Instant Burglar Alarm	No Response	Delayed Burglar Alarm
Start Entry Delay 2	Instant Burglar Alarm (Interior)	Start Entry 2 → Burglar Alarm (Perimeter)	Start Entry 2 → Burglar Alarm (Interior)	Instant Burglar Alarm	No Response	Delayed Burglar Alarm
Chime	Door Chime	Door Chime	Door Chime	Instant Burglar Alarm	No Response	Door Chime
Burglar Follow	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	No Response	Delayed Burglar Alarm
Burglar Instant	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	No Response	Instant Burglar Alarm
Burglar Outdoor	Instant Burglar Outdoor Alarm	Instant Burglar Outdoor Alarm	Instant Burglar Outdoor Alarm	Instant Burglar Alarm	No Response	Instant Burglar Outdoor Alarm
Cross Zone	**See 10.3. Appendix – Cross Zone Verification**			Instant Burglar Alarm	No Response	Delayed Burglar Alarm
Set/Unset (Opening)	Full Arm	No Response	Full Arm	Full Arm	No Response	No Response
Set/Unset (Closing)	No Response	Disarm	Disarm	Disarm	Disarm	Disarm
24H – Burglar	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm	Instant Burglar Alarm
24H – Smoke	Instant Smoke	Instant Smoke	Instant Smoke	Instant Smoke	Instant Smoke	Instant Smoke Alarm

	Alarm	Alarm	Alarm	Alarm	Alarm	
24H – Medical	Instant Medical Alarm	Instant Medical Alarm	Instant Medical Alarm	Instant Medical Alarm	Instant Medical Alarm	Instant Medical Alarm
24H – Fire	Instant Fire Alarm	Instant Fire Alarm	Instant Fire Alarm	Instant Fire Alarm	Instant Fire Alarm	Instant Fire Alarm
24H – Water	Instant Water Alarm	Instant Water Alarm	Instant Water Alarm	Instant Water Alarm	Instant Water Alarm	Instant Water Alarm
24H – CO	Instant CO Alarm	Instant CO Alarm	Instant CO Alarm	Instant CO Alarm	Instant CO Alarm	Instant CO Alarm
24H – Gas	Instant Gas Alarm	Instant Gas Alarm	Instant Gas Alarm	Instant Gas Alarm	Instant Gas Alarm	Instant Gas Alarm
24H – Heat	Instant Heat Alarm	Instant Heat Alarm	Instant Heat Alarm	Instant Heat Alarm	Instant Heat Alarm	Instant Heat Alarm
24H – Silent Panic	Instant Silent Panic Alarm	Instant Silent Panic Alarm	Instant Silent Panic Alarm	Instant Silent Panic Alarm	Instant Silent Panic Alarm	Instant Silent Panic Alarm
24H – Panic	Instant Panic Alarm	Instant Panic Alarm	Instant Panic Alarm	Instant Panic Alarm	Instant Panic Alarm	Instant Panic Alarm
24H – Emergency	Instant Emergency Alarm	Instant Emergency Alarm	Instant Emergency Alarm	Instant Emergency Alarm	Instant Emergency Alarm	Instant Emergency Alarm
24H – Emergency (Quiet)	Instant Silent Emergency Alarm	Instant Silent Emergency Alarm	Instant Silent Emergency Alarm	Instant Silent Emergency Alarm	Instant Silent Emergency Alarm	Instant Silent Emergency Alarm
24H – Fire with Verification	See **10.4. Appendix – Fire Verification**					
Trigger Scene	Trigger Scene Number	Trigger Scene Number	Trigger Scene Number	Trigger Scene Number	Trigger Scene Number	Trigger Scene Number

<NOTE>

☞ "**Delayed Burglar Alarm**" reponse means the Control Panel will wait for the Entry Time to expire. If the Enty Time expires without disarming the system, the Control Panel will activate a Burglar Alarm after Entry Time expiry.

☞ **"Silent Panic Alarm"**, **"Silent Emergency Alarm"** and "**Burglar Outdoor Alarm**" does not activate any audible alarm. The Control Panel will report the alarm event silently without any warning sound.

10.3. Cross Zone Verification

Cross Zone Verification is use to setup cross verification for intrusion sensors.

To use Cross Zone Verification, the following sensor and panel setting must be adjusted:

1 At least **1** intrusion sensor must be set to **Cross Zone** attribute.

2 The **Cross Zone Timer** option under Panel Setting webpage must be enabled.

Cross Zone Verification Rule

- Cross Zone function does not activate under Exit and Entry Time.
- When a sensor set to Cross Zone attribute is triggered, the panel begins to sound alarm, counts down Cross Zone Timer and reports a Cross Zone First Trip event (CID 693).
  - If the Cross Zone Timer expires without any other sensor trigger, the panel reports Cross Zone Trouble event (CID 378) when the timer expires.
  - If the same sensor is triggered again during Cross Zone Timers, the Cross Zone Timer is reset and extended.
  - If another sensor is triggered during the timer:
    - The Panel report Burglar (CID 130) for both sensors.
    - If the newly triggered sensor is set to Cross Zone attribute, the Panel also report Burglar Verified (CID 139) for this sensor.
    - The Cross Zone Timer is reset and extended.
    - When the Cross Zone Timer expires, the panel reports Cross Zone Timeout (CID 694).

10.4. Fire Verification

Fire Verification is use to setup verification for Smoke Detector.

To use Fire Verification, the following sensor and panel setting must be adjusted:

1 At least **1** Smoke Detector must be set to **24 HR – Fire with Verification** attribute.

2 The **Fire Verification Timer** option under Panel Setting webpage must be enabled.

Fire Verification Rule

- When a Smoke Detector set to Fire Verification attribute is triggered, the panel begins to sound alarm, counts down Fire Verification Timer and reports a Near Alarm event (CID 118).
  - Triggering any Smoke Detector with Fire Verification attribute (including the original Some Detector) during Fire Verification Timer will prompt panel to report Smoke Alarm event (CID 111), the timer will be reset and extended.
  - Triggering a regular Smoke Detector with Smoke attribute during the Fire Verification Timer will prompt panel to report Smoke Alarm event (CID 111), the timer will not be reset..
  - When the Fire Verification Timer expires, the panel reports Fire Verification Timeout event (CID 695).

10.5. Contact-ID Protocol & Format

<table>
<tr><td>Where</td><td></td><td><b>ACCT MT QXYZ GG $C_1C_2C_3$</b></td></tr>
<tr><td>ACCT</td><td>=</td><td>4 Digit Account number (0-9, B-F)</td></tr>
<tr><td>MT</td><td>=</td><td>Message Type, 18H.</td></tr>
<tr><td>Q</td><td>=</td><td>Event qualifier, which gives specific event information:</td></tr>
<tr><td>XYZ</td><td>=</td><td>Event code (3 Hex digits 0-9, B-F)</td></tr>
<tr><td>GG</td><td>=</td><td>Group, Partition number (00H), or Area Number
- 00 = panel
- 01= area 1……..xx= area xx</td></tr>
<tr><td>$C_1C_2C_3$</td><td>=</td><td>1. For devices: zone
<table>
<tr><th><b>$C_1C_2C_3$ = Zone number</b></th></tr>
<tr><td>001, Zone 1</td></tr>
<tr><td>002, Zone 2</td></tr>
<tr><td>……………………</td></tr>
<tr><td>XXX Zone XXX</td></tr>
</table>
2. For Panel: code
<table>
<tr><th><b>$C_1C_2C_3$ =</b></th><th></th></tr>
<tr><td>User PIN Code 1</td><td>001</td></tr>
<tr><td>User PIN Code 2</td><td>002</td></tr>
<tr><td>User PIN Code 3</td><td>003</td></tr>
<tr><td>User PIN Code 4</td><td>004</td></tr>
<tr><td>User PIN Code 5</td><td>005</td></tr>
<tr><td>User PIN Code 6</td><td>006</td></tr>
<tr><td>Temporary Code</td><td>997</td></tr>
<tr><td>Duress Code</td><td>998</td></tr>
<tr><td colspan="2">000= Control Panel</td></tr>
</table>
</td></tr>
</table>

10.6. Event Code

- **100 – Medical**
  - When a device set to Medical attribute is triggered.
- **101 – Personal emergency**
  - When a device set to Personal Emergency attribute is triggered.
- **110 – Fire**
  - When a device set to Fire attribute is triggered.
- **111 – Smoke**
  - When the Smoke Detector (SD) set to Smoke Alarm is triggered.
  - When the Smoke Detector (SD) set to Fire Verification verifies an alarm during Fire Verification Time.
- **118 – Near Alarm**
  - When the Smoke Detector (SD) set to Fire Verification is triggered.
- **120 – Panic**
  - When a device set to Panic attribute is pressed.
- **121 – Duress**
  - When the Duress Code is entered to disarm or arm the system.
- **122 –Silent Panic**
  - When a device set to Silent Panic is pressed.
- **130 – Burglar**
  - Whenever a device set as Burglar Instant is triggered.
  - Whenever a device set as Burglar Instant is triggered under **Disarm**, **Full Arm** or **Home Arm** mode.
- **131 – Burglar Perimeter**
  - When a device set as **Entry** is triggered in Full Arm mode.
  - When a device set as **Burglar Follow** is triggered during Full Arm Entry Time and the system is not disarmed before entry time expiry.
- **132 – Burglar Interior**
  - When a device set at **Entry** is triggered in Home Arm mode.
  - When a device set as **Burglar Follow** is triggered during Home Arm Entry Time and the system is not disarmed before entry time expiry.
- **136 – Burglar Outdoor**
  - Whenever a device set at **Burglar Outdoor** is triggered.
- **137 – Panel Tamper/ Panel Tamper Restore**
  - When the panel’s tamper protection is triggered.
  - When the panel’s tamper function is restored.
- **139 – Burglar Verified.**
  - When a sensor set to Cross Zone attribute verifies an alarm.
- **147 – Sensor Supervision Failure/ Sensor Supervision Restore**
  - When the panel fails to receive supervision signal from a device within preset supervision timer.

- ◆ When the panel receives signal again from sensor that previously failed supervision.
- **154 – Water leakage**
  - ◆ When the Water Sensor connected to Door Contact set at **Wate**r (@**W**) is triggered.
- **158 – High Temperature Alarm**
  - ◆ When high temperature alarm is triggered.
- **159 – Low Temperature Alarm**
  - ◆ When low temperature alarm is triggered.
- **162 – CO Alarm**
- **170 – High Power Consumption**
  - ◆ When high power consumption alarm is triggered.
- **171 – High Humidity Alarm**
  - ◆ When high humidity alarm is triggered.
- **172 – Low Humidity Alarm**
  - ◆ When low humidity alarm is triggered.
- **301 – AC Failure/ AC Power Restore**
  - ◆ When the AC power fails for more than 10 sec.
  - ◆ Restore from AC power failure.
- **302 – Low battery/ Battery Normal**
  - ◆ When the battery voltage of the Panel is low.
  - ◆ When the panel battery restores voltage.
- **311 – Battery Disconnection/ Battery Reconnected**
- **344 – Interference/ Interference problem solved**
- **358 – Network Cable Unplugged**
  - ◆ When the Ethernet cable is disconnected.
- **374 – Force Arm**
  - ◆ When the system is armed with existing fault events
- **693 – Cross Zone Trouble**
  - ◆ When Cross Zone Timer expires without alarm verification.
- **380 – Device AC Failure**
  - ◆ When an AC power device loses AC power connection.
- **383 – Sensor Tamper/ Sensor Tamper Restore**
  - ◆ When any sensor's tamper protection is triggered.
  - ◆ When the sensor's tamper function is restored.
- **384 – Sensor Low battery/ Sensor Battery Normal**
  - ◆ When a device detects low battery voltage.
  - ◆ When a device's low battery condition is restored.
- **400 – Arm/Disarm (by Remote Controller)**
  - ◆ When the system is armed or disarmed by using the Remote Controller.
- **401 – Remote Arm/Disarm**
  - ◆ When the system is armed or disarmed by SMS message or web access

- **407 – Disarm/Away Arm/Home Arm by Remote Keypad**
- **408 – Set/Unset Arm/Disarm**
  - ◆ When the DC set at Set\Unset is triggered.
- **456 - Partial Arm**
  - ◆ When partially arm the system from Disarm to Home arm
- **570 – Device out of order/ Door Contact Not Closed**
  - ◆ When arm fault type is set as Direct Arm, any device is out of order after the preset exit delay time is reached
  - ◆ When arm fault type is set as Direct Arm, Door Contact is not closed after the preset exit delay time is reached.
- **602 – Periodic test report**
  - ◆ When the control panel makes periodic Check-in reporting.
- **616 – Call Request**
  - ◆ When the service call is activated by VST-809.
- **693 – Cross Zone First Trip**
  - ◆ When a sensor set to Cross Zone is triggered to start Cross Zone Timers.
- **694 – Cross Zone Timeout**
  - ◆ When Cross Zone Timer expires after the alarm has been verified.
- **695 – Fire Verification Timeout**
  - ◆ When Fire Verification Timer expires.

I. Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15, Part 22, Part 24, and Part 27 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:
. Reorient or relocate the receiving antenna.
. Increase the separation between the equipment and receiver.
. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15, Part 22, Part 24, and Part 27 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.