HSGW Series

IP Alarm System

User Manual

June 2020

Table of Contents

1. INTRODUCTION **1**

1.1. SYSTEM SPECIFICATION 2

2. PANEL INFORMATION **5**

2.1. IDENTIFYING THE PARTS: 5

2.2. THE POWER SUPPLY: 6

2.3. SYSTEM REQUIREMENTS: 6

3. GETTING STARTED **7**

3.1. SYSTEM DEPLOYMENT 7

3.2. HARDWARE INSTALLATION 7

3.3. SOFTWARE INSTALLATION 10

4. CONNECTION TO PANEL WEBPAGE **13**

5. DEVICE MANAGEMENT **15**

5.1. LEARNING 15

5.2. ADD RF DEVICE 22

5.3. LEARN RULE 23

5.4. WALK TEST 25

5.5. EXCLUSION 26

5.6. Z-WAVE TOOL 27

5.7. PSS CONTROL 28

5.8. UPIC CONTROL 29

5.9. SURVEILLANCE 30

5.10. GROUP CONTROL 31

5.11. SOUND/SIREN SETTING 32

6. PROGRAM THE SYSTEM **36**

6.1. PANEL CONDITION 36

6.2. PANEL SETTINGS 39

6.3. PIN CODE 43

7. NETWORK SETTINGS **44**

7.1. GSM (HSGW-MAX8 ONLY) 44

7.2. NETWORK 47

7.3. WIRELESS 48

7.4. UPNP 49

8. SYSTEM SETTINGS **50**

8.1. Administrator Setting 50
8.2. Home Automation 51
8.3. Scene 56
8.4. Reporting 58
8.5. Code Settings 61
8.6. SMTP Setting 63
8.7. Media Upload 64
8.8. Polling 65
8.9. XMPP 66
8.10. Date & Time 67
8.11. Dynamic DNS 68
8.12. Test IP 69
8.13. Firmware Upgrade 70
8.14. RF Firmware Upgrade 71
8.15. Factory Reset 72
8.16. Backup & Restore 74
8.17. System Log 75

***9. EVENT & HISTORY* 76**

9.1. Captured Events 76
9.2. Reported Events 77
9.3. Event Log 78
9.4. Device History 79

***10. APPENDIX* 80**

10.1. Fault Event Description 80
10.2. Control Panel Mode and Response Table 81
10.3. Cross Zone Verification 83
10.4. Fire Verification 83
10.5. Contact-ID Protocol & Format 84
10.6. Event Code 85

1. Introduction

This section covers unpacking your IP Security System with HSGW Series IP Panel and Security Sensors. Refer to later chapters for information on setting up and configuring the system over the Web Page in more detail.

The advanced IP Security System with fully integrated TCP/IP technology and Ethernet connectivity is able to take full advantage of new advances in IP Home Security and Home Automation and multi-path signalling.

1.1. System Specification

Function		
Control Facilities	Remote Keypad & Remote Controller	
Alarm Transmission Path	Built-in Module: RF + RJ45 port (IP Connection) + 4G*	
Report Destinations	20 Monitoring Stations or mobile number	
Arming Modes	Away, Home 1, Home 2, Home 3	
Alarm Type	Burglar, Panic, Fire, Medical, Emergency, Water, Silent	
Supervision	Programmable time frame for inactivity alert	
GSM Standards	Compiles with CE & FCC standards.	
Specifications		
CPU, RAM	CPU: i.MX 6ULL MCIMX6Y1DVM05AB NXP RAM: DDR3L SDRAM MT41K256M16TW (4Gbit)	
Flash	Flash: NOR FLASH MT25QL256ABA 256Mbit and eMMC 4GBytes	
Electrical		
External AC adaptor	Input: AC 100-240V, 50 / 60Hz, Output: DC 12V 1A	
Backup Battery	1600mAh, Ni-MH rechargeable battery pack	
Battery Recharge Time	72 hours	
Battery Backup Time	30 hours**	
Current Drain	AC Powered	Approx. 126mA / 12V standby
	Battery Powered	Approx. 44mA / 7.2V Suspend
Wireless		

RF (one of these three possibilities for different country)	Frequency: 868MHz Modulation: FSK Antenna type: Monopole antenna Antenna gain: 1.75dBi Protocol: Climax Encryption: Private Encryption Method
	Frequency: 915MHz Modulation: FSK Antenna type: Monopole antenna Antenna gain: 1.75dBi Protocol: Climax Encryption: Private Encryption Method
	Frequency: 920MHz Modulation: FSK Antenna type: Monopole antenna Antenna gain: 1.75dBi Protocol: Climax Encryption: Private Encryption Method
4G* (one of these two possibilities for different country)	(Quectel EC21-E) GSM: 900 / 1800MHz WCDMA: B1 / B5 / B8 LTE: FDD: B1 / B3 / B5 / B7 / B8 / B20
	(Quectel EC21-AU) GSM: 850 / 900 / 1800 / 1900MHz

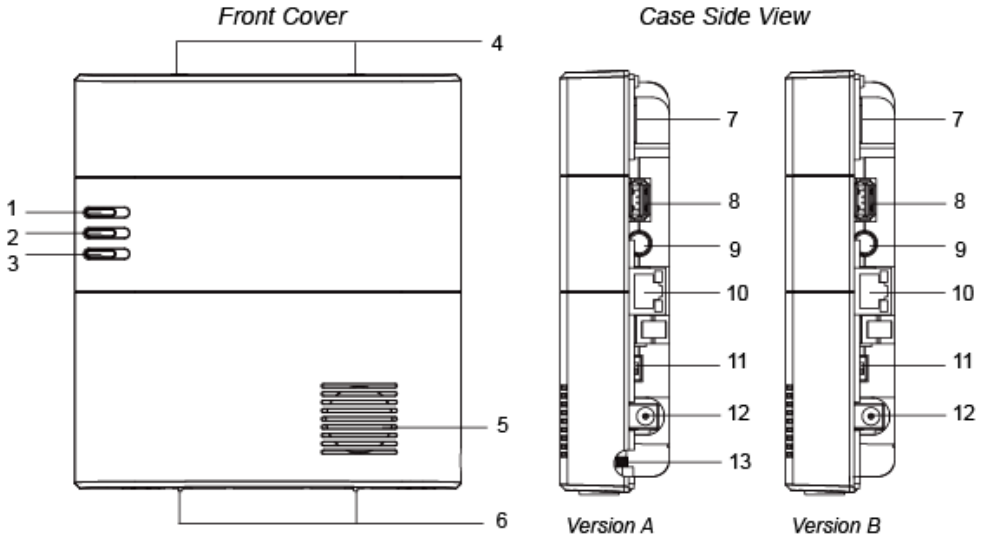
	WCDMA: B1 / B2 / B5 / B8 LTE: FDD: B1 / B2 / B3 / B4 / B5 / B7 / B8 / B28, TDD: B40
Antenna Type	Main: Monopole Aux: Dipole
Protocol	Climax
Physical Properties	
Operating Temperature	-10°C ~ 45°C
Operating Humidity	85% relative humidity @23°C (non-condensing)
Dimensions	150mm x 140mm x 42.3mm
Weight	430g

**Note: 4G with fallback compatibility to 3G and 2G.*

*** Note: The actual battery life may vary with product settings, usage patterns and operating environment.*

2. Panel Information

2.1. Identifying the parts:



1 LED 1 (Red/Green)

Red LED ON – Area 1 in exit delay of Full Arm Mode.

Red LED Flash – Area 1 in exit delay of Home 1/2/3 Mode.

Green LED ON - System in the learning mode.

Green LED Flash - System in the Walk Test mode.

2 LED 2 (Red/Green)

Red LED ON – Area 2 in exit delay of Full Arm mode

Red LED Flash – Area 2 in exit delay of Home 1/Home 2/Home 3 mode

Green LED On – System in the learning mode

Green LED Flash – System in the Walk Test mode

3 LED 3 (Red/Yellow)

Red LED ON – Alarm in memory.

Red LED Flash – Alarm

Yellow LED ON – system fault

4 Top Fixing Screw x 2 (for Version A only)

5 Buzzer

6 Bottom Fixing Screw x 2

7 Micro SIM Card Compartment

8 USB Port

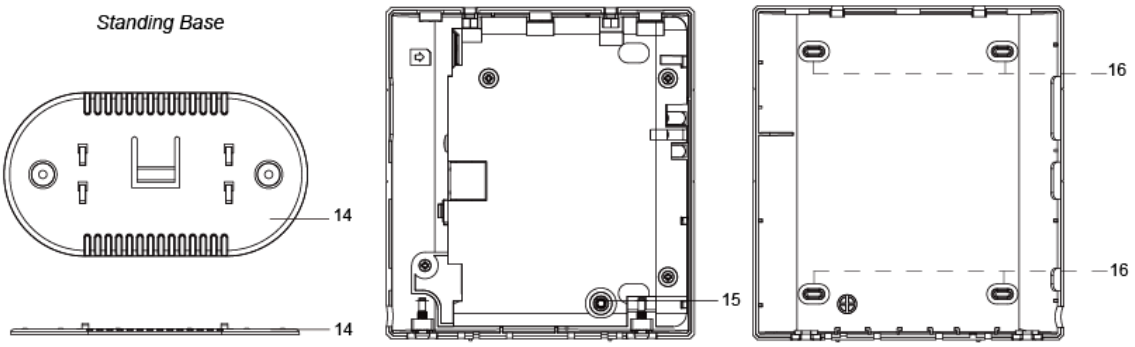
9 Learn/ResetButton

10 Ethernet Port (pre punched hole for Version B only)

11 Battery Switch (slide to "ON" to meet requirements of the applicable EN standard.)

12 DC Jack

13 Pre Punched Hole for Wiring (for Version A only)



14 Standing Base (for desktop deployment)

15 Tamper Switch

16 Wall Mounting Knockouts x 4

2.2. The Power Supply:

An AC power adapter is required to connect to a wall outlet. Be sure only to use an adapter with the appropriate AC voltage rating to prevent component damage. A DC 12V 1A switching power is used to power the Control Panel with 7.2V 1600mAh, Ni-mH rechargeable battery pack.

Rechargeable Battery

- The Control Panel has rechargeable battery pack of 1600mAh.
- In addition to the adapter, there is a rechargeable battery inside the Control Panel, which serves as a backup in case of a power failure.
- During normal operation, the AC power adapter is used to supply power to the Control Panel and at the same time recharge the battery. Slide the Battery Switch to ON to activate and charge the battery. It takes approximately 72 hours to fully charge the battery
- The battery status information is displayed in the Panel section of local area webpage.

2.3. System Requirements:

The system requires a TCP/IP network environment for you to connect to the Control Panel for system programming. Hardware requirement for programming the panel vial Local Area Network (LAN) webpage:

- Microsoft Windows 8 or Windows 10 operating system.
- Microsoft Internet Explorer 6.x, or later and Mozilla Firefox 3.0 compatible.
- CPU: Intel Pentium II 266MHz or above
- Memory: 32MB (64MB recommended)
- VGA resolution: 800x600 or above

3. Getting Started

Read this section of the manual to learn how to set up your Control Panel and program System Settings over the Web page.

3.1. System Deployment

Follow guidelines below when planning installation location:

- The Control Panel requires Ethernet connection.
- The Control Panel should be installed at a location that is hidden from outside view.
- Avoid mounting the Control Panel near large metal objects which may affect wireless radio strength.
- The Control Panel should be protected by sensors so that no intruder can reach the Control Panel without first activating a sensor.
- When using **ZigBee routers** to improve ZigBee network coverage, remember to use only ZigBee Router with backup batteries for security sensors. If you use a Router without backup battery for security sensors, the Router will be powered down in case of AC failure, and you security sensors will lose connection with the ZigBee network.
- Home Automation devices (Power Switches…etc) do not have this limit and can be used with any Router.

3.2. Hardware Installation

The panel can be either fixed on the wall or placed on deskop. Remove the bottom standing base to reveal the bottom cover fixing screw. (Figure 1)

1 (Case Version A for example) The panel casing is secured by 4 screws, 2 at top and 2 at bottom, remove the top 2 screws and loosen the bottom 2 screws. (Figure 2)

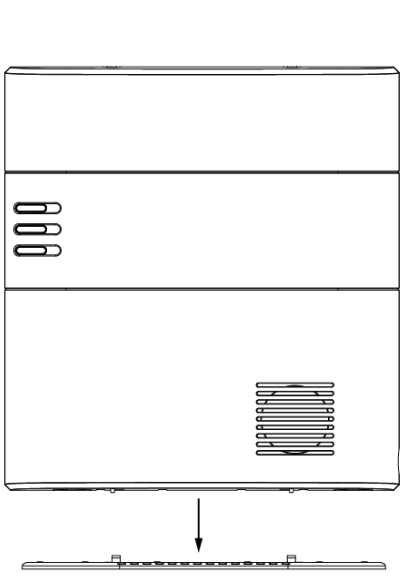


Figure 1

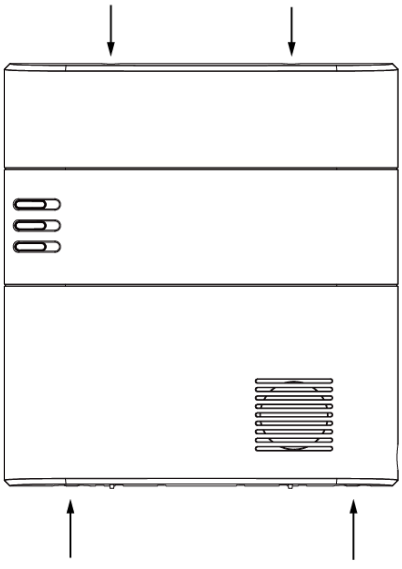


Figure 2

2 To remove the back cover, first lift the cover partially from the bottom, then push inward from the top to disconnect the back cover from panel main body.

3 Remove the 4 screws securing the internal cover.

4 Replace the internal cover for setup:

I. Connect Ethernet cable to panel Ethernet port.

II. Insert a functional micro SIM Card into Micro SIM Card Compartment, the SIM Card PIN Code must be disabled first.

III. Slide Battery Switch to ON position.

IV. Plug in AC adaptor to power on the panel.

5 Wire the Ethernet and AC power cable, close the cover and choose to install the panel on desktop, or mount on the wall.

When closing the cover, first attach the back cover to main body from the top, then close the cover from bottom.

Desktop:

I. Replace the back cover, wire the cable through the side hole and tighten the 4 fixing screws. (figure 3)

II. Replace the standing base. (figure 4)

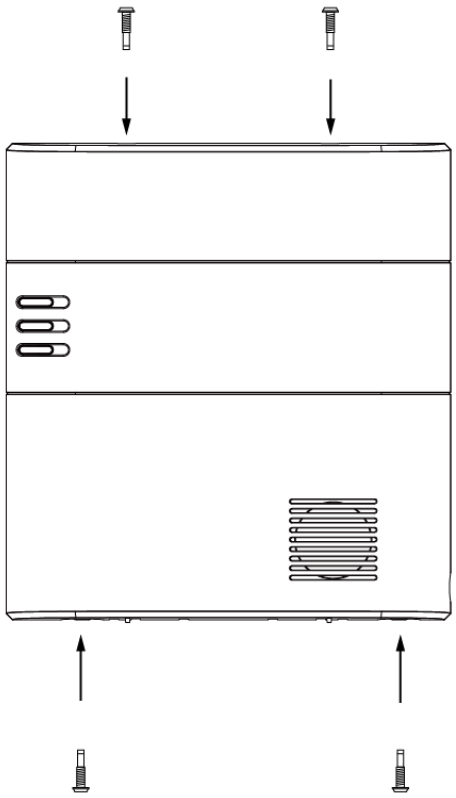


Figure 3

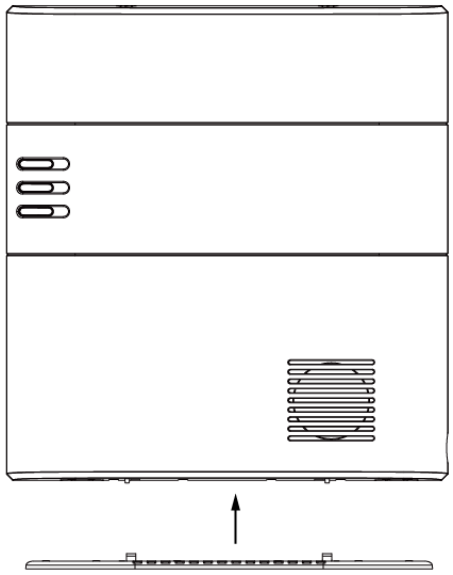


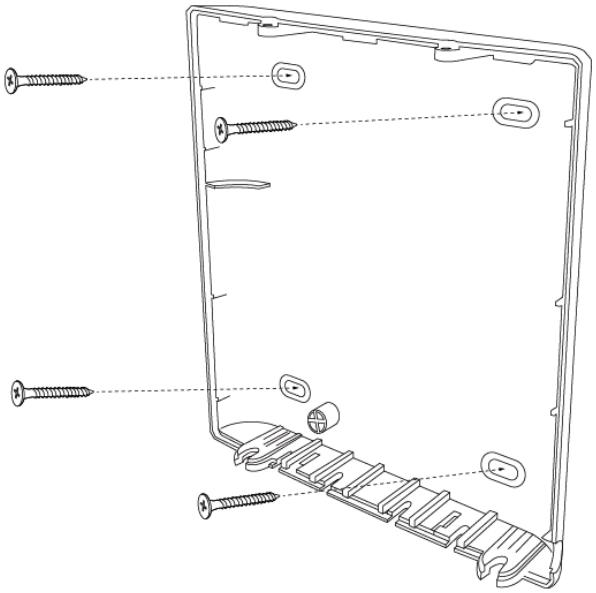
Figure 4

III. Put the panel at desired location to finish installation.

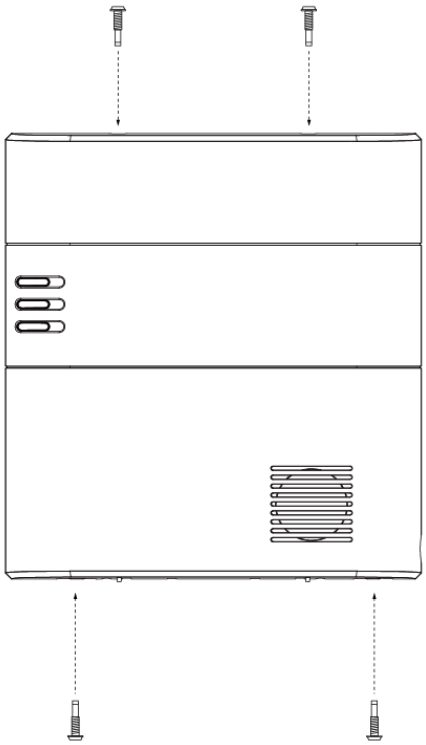
Wall Mounting:

I. Break through the 4 Wall Mounting Knockouts.

II. Use the knockouts as template, mark mounting locations on the wall.



III. Replace the panel onto the back cover and tighten the 4 fixing screws to complete installation.



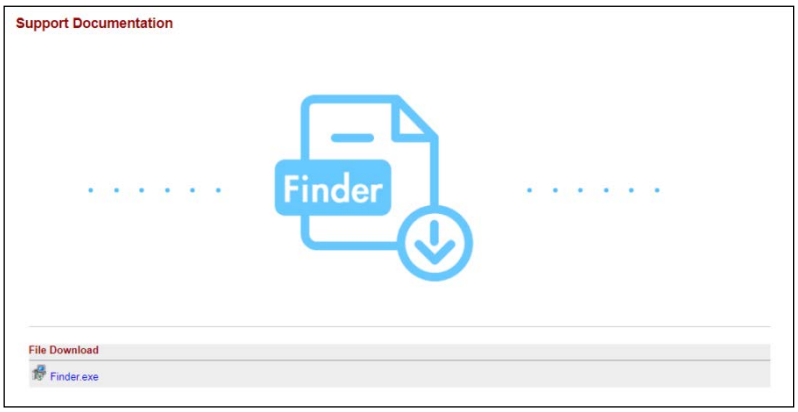
3.3. Software Installation

※ THIS INSTALLATION IS ONLY REQUIRED FOR FIRST TIME USER ※

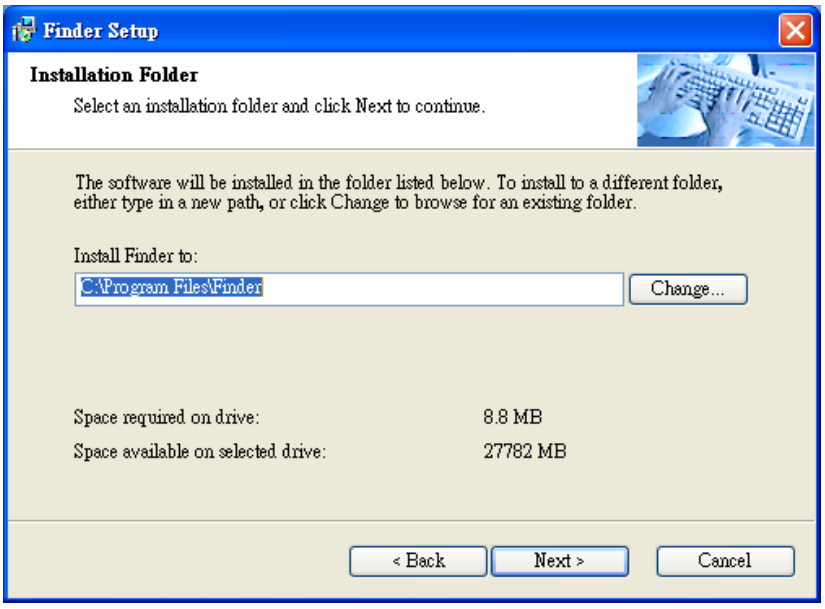
1. RUNNING THE FINDER SOFTWARE

The Finder software is required for your computer to identify the control panel on the LAN.

Step 1. To download Finder software, open your browser and type below URL in the address bar: http://www.climax.com.tw/climax-download-finder.html.



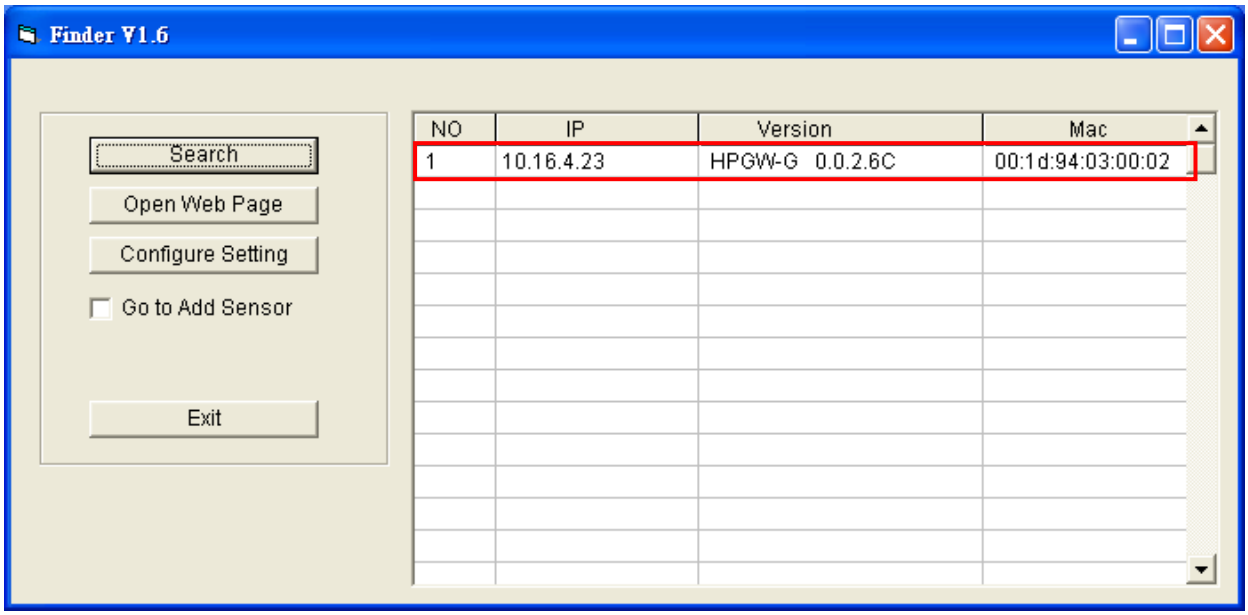
Step 2. After download, install the software and follow on-screen instructions to complete installation.



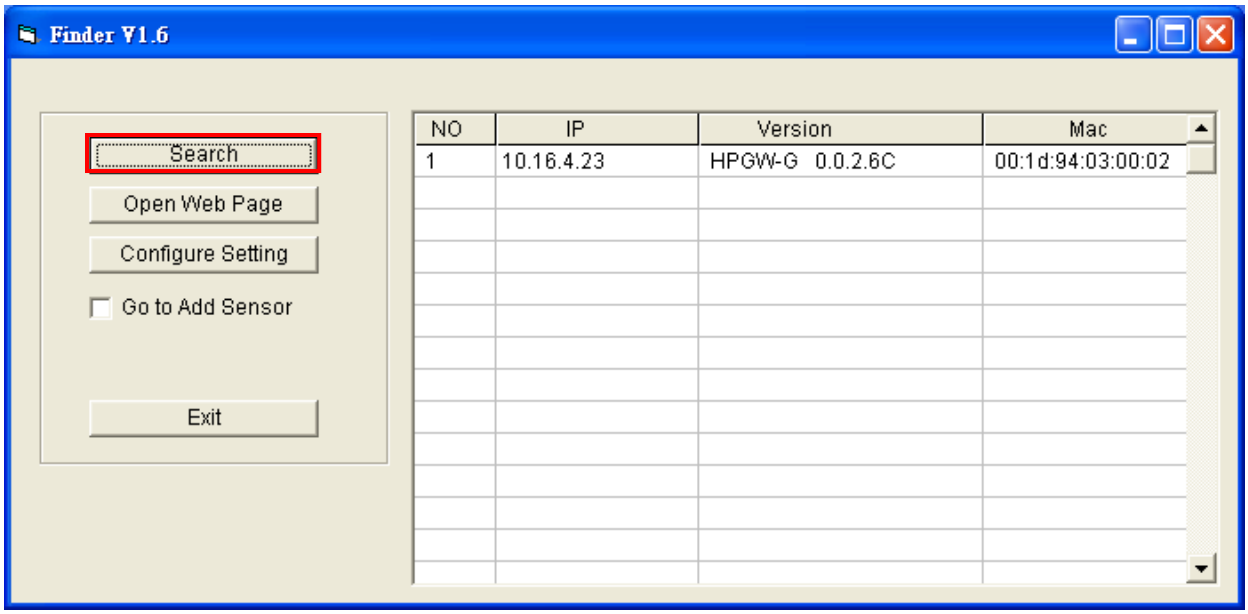
Step 3. Follow on screen instruction to complete installation

Step 4. Once complete, the Finder icon will be displayed on your desktop.

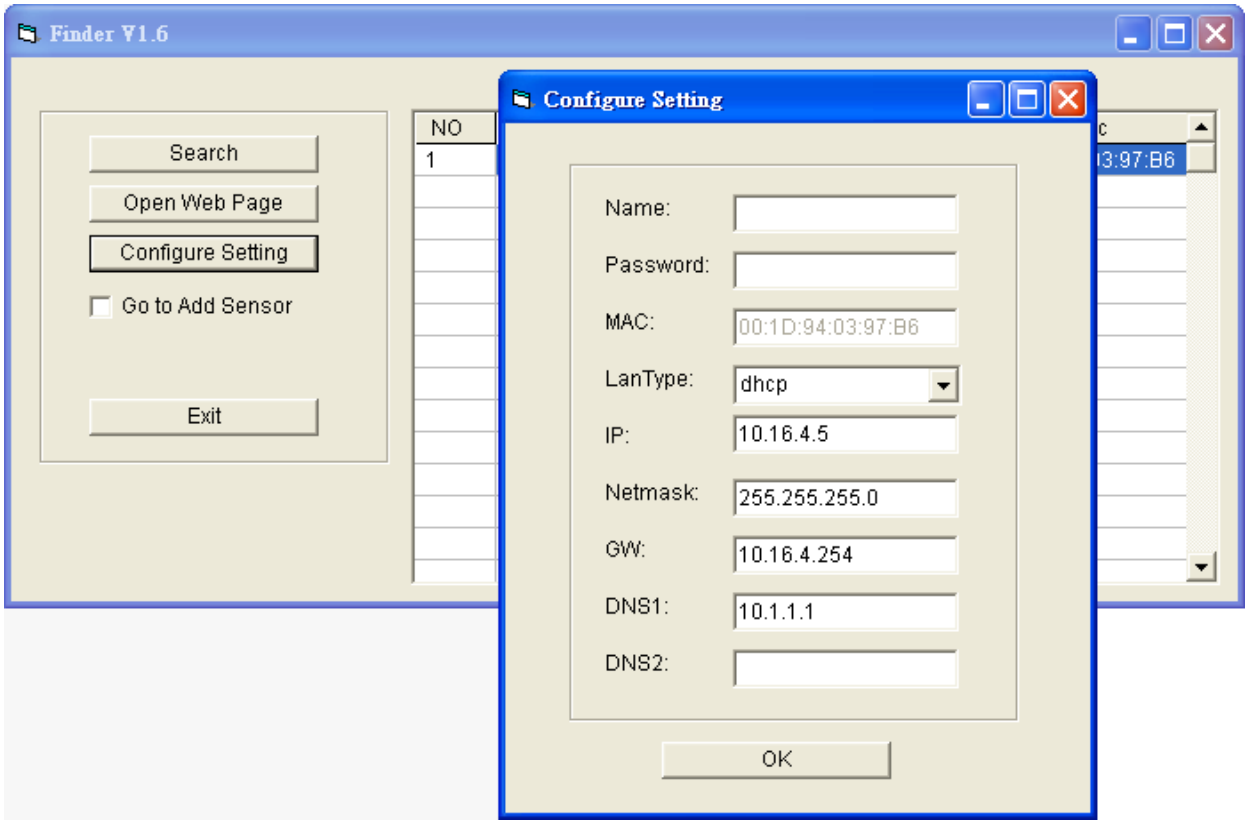
Step 5. Double click on the "**Finder.exe**" to start the software. Finder will automatically search for control panel on the LAN and display its information. If available, the panel's LAN IP address, Firmware version and MAC address will be displayed



Step 6. If the panel information is not displayed, check panel power and Ethernet connection and click on "**Search**" to update the panel information.



Step 7. **(Optional)**You can choose to edit the panel's network setting by clicking on the panel column, then click "Configure Setting"



The LanType is default to **DHCP** and does not require manual input of IP/Netmask/Gateawy/DNS setting. If you wish to configure these setting manually, change LanType to **Static**.

After finish changing network setting, enter the user name (default: **admin**) and password (default: **cX+HsA*7F1**) then click **OK** to confirm. The user name and password can be changed later in panel configuration webpage

Step 8. Click the panel information column and click on "**Open Web Page**", or double click on the panel column to link to the panel configuration webpage. Your default browser will start automatically to connect to the LAN IP displayed in Finder.

4. *Connection to Panel Webpage*

For first time setup, webpage connection is only available within 1 hour after the panel is powered on; if the panel has been powered on for more than 1 hour. Webpage access will be disabled. Reboot the panel to enable webpage function again.

Change default password after login to gain unrestricted webpage access.

Step 1. Select the Control Panel in the Finder software and click on “Open Webpage” to connect to panel webpage.

Alternatively, enter the Control Panel IP address displayed in Finder into your browser’s address section and proceed.

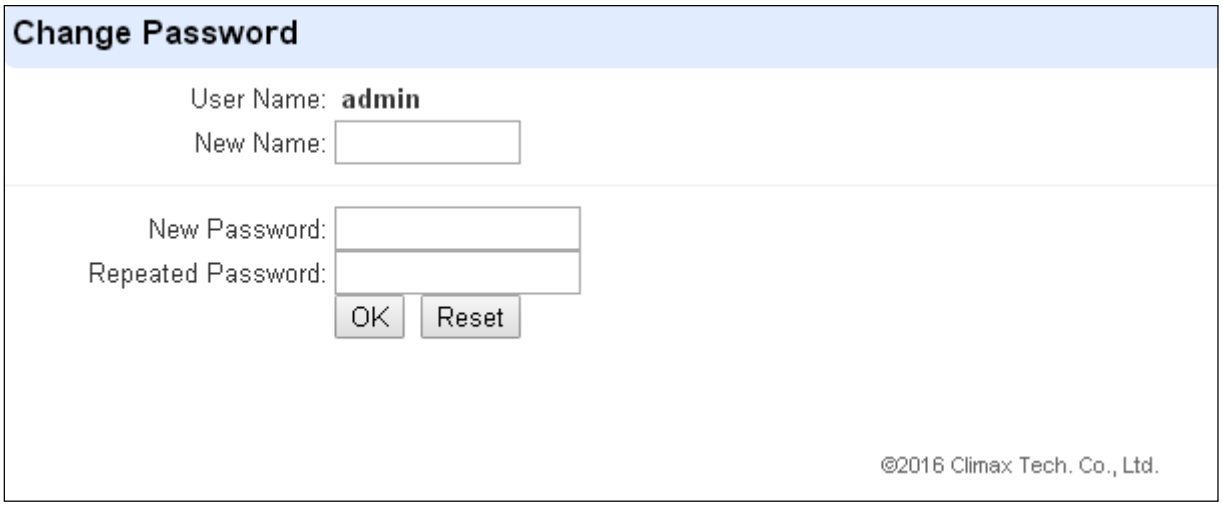
Step 2. Enter the User name & Password to proceed

Default user name: **admin**

Default password: **cX+HsA*7F1**

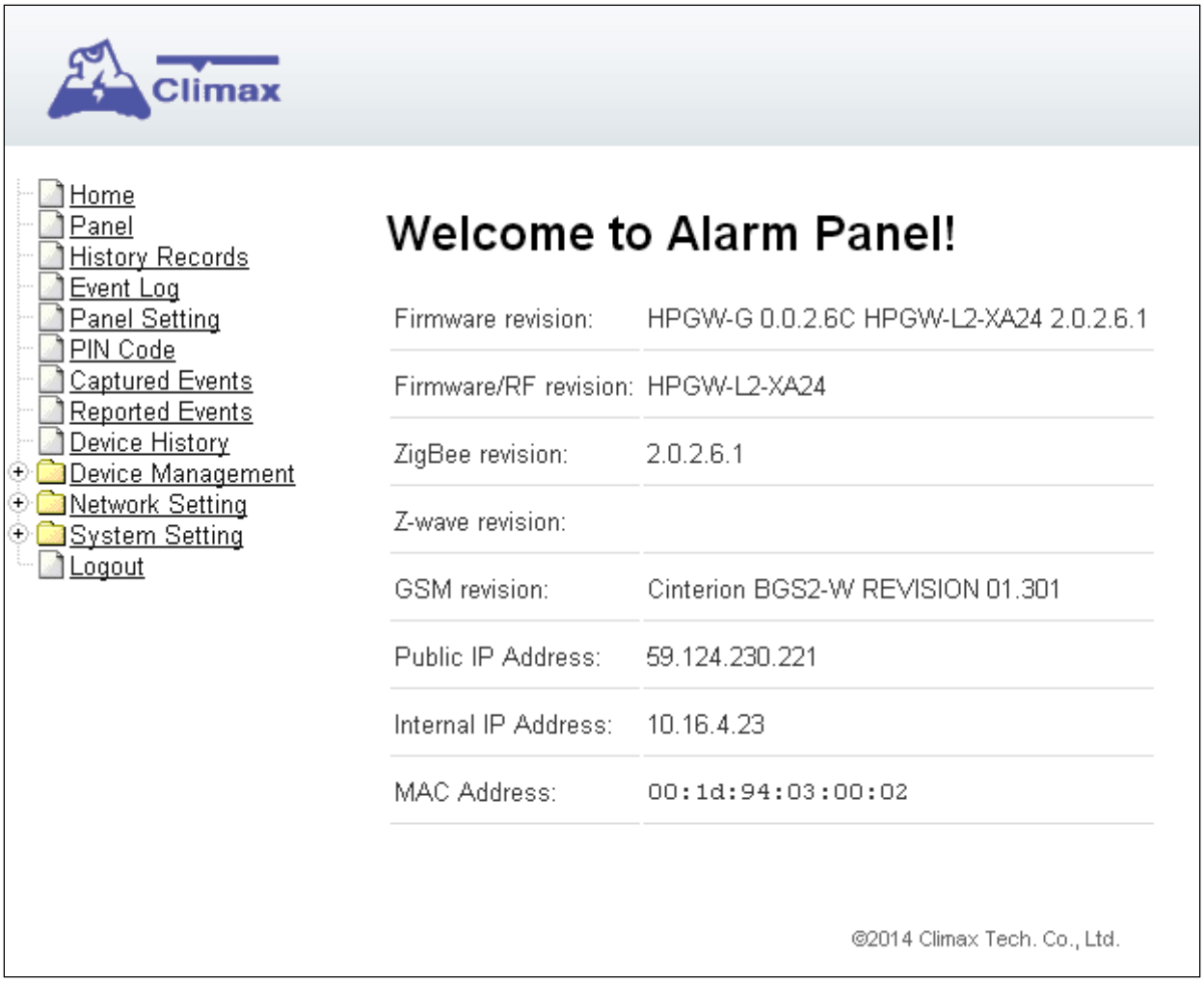
(If wrong user name and password are entered for **5** times, the local webpage login will be disabled for **5** minutes.)

Step 3. You will enter change password page. Enter and repeat a new password (username change is optional), take care that both username and password are case sensitive. Click OK to confirm.



Step 4. Upon confirming new username and password. You will enter panel Welcome page. The panel will prompt you to re login with new username and password.

Step 5. You will enter panel Welcome page. The Control Panel’s information will be displayed. Click on the pages and folders on the left to access the Control Panel’s various functions



The Welcome page displays current control panel firmware version information according to different panel model and MAC address.

<IMPORTANT NOTE>

☞ If the default login password is not changed, webpage access will be disabled 1 hour after power on. Reboot the panel and changed password to allow unrestricted webpage access.

5. Device Management

The Device Management section allows you to learn in, edit, control and view all available accessory devices that can be included in the HSGW Control Panel.

5.1. Learning

Use this function to add new devices into the Control Panel. HSGW supports up to 160 zones of accessory devices, in 2 areas, up to 80 zones each area.

The following types of accessory devices are supported:

- **RF device:** All Climax RF devices are supported. (For ZigBee only model, RF devices are not supported.)
- **ZigBee device:** All ZigBee device with ZigBee Home Automation 1.2 profile are supported.

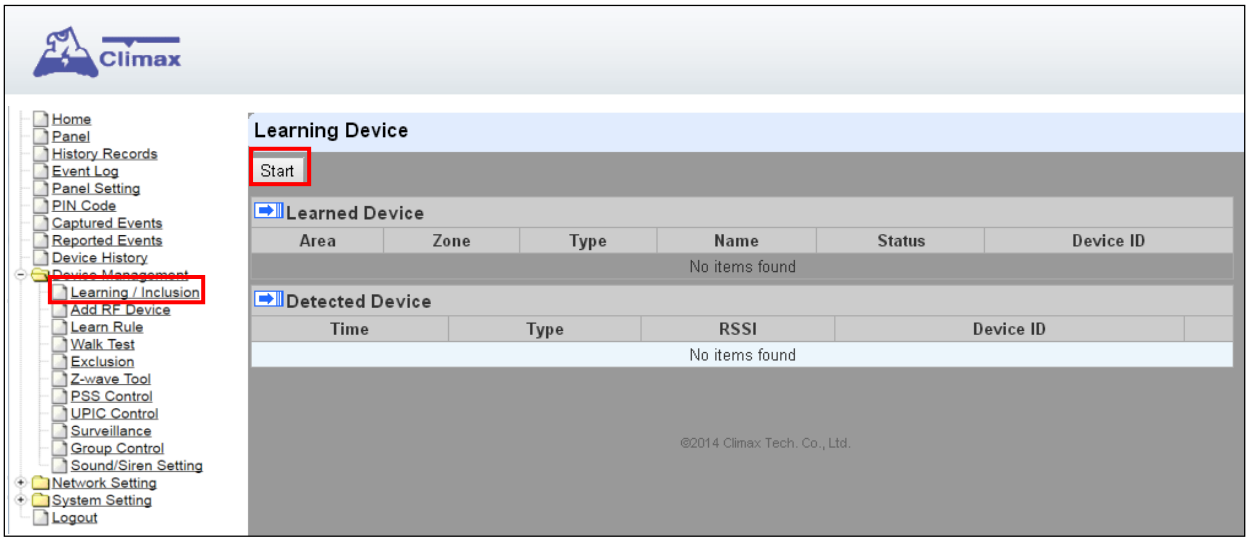
<IMPORTANT NOTE>

☞ The Control Panel built-in ZigBee module supports up to **40** ZigBee devices by itself. If you wish to include more than 40 ZigBee devices into the Control Panel, you must add extra ZigBee Routers into the Control Panel's ZigBee network to increase the network's maximum device capacity.

- **IP Cameras:** The Control Panel is compatible with Climax VST-1818 Series IP Camera. Up to 6 IP Cameras are supported.
- **Z-Wave Device:** Available for Z-Wave modules only, other modules requires additional USB Z-Wave Dongle.

5.1.1. Add Sensor

Step 1. Click on "**Learning**" to enter learn page.



Step 2. Click on "**Start**" to enter learning mode.

Step 3. Press the test or learn button on the each device or any button on the Remote Controller. (Please refer to each sensor's user manual for test or learn button position).

<NOTE>

☞ For ZigBee sensors, press and hold the learn button for 10~12 seconds to transmit a

learn code.

☞ For IP Camera VST-1818 Series, press and hold the Privacy button for 10 seconds.

Step 4. When the system received the signal transmitted from device, the screen will display its information for selection.

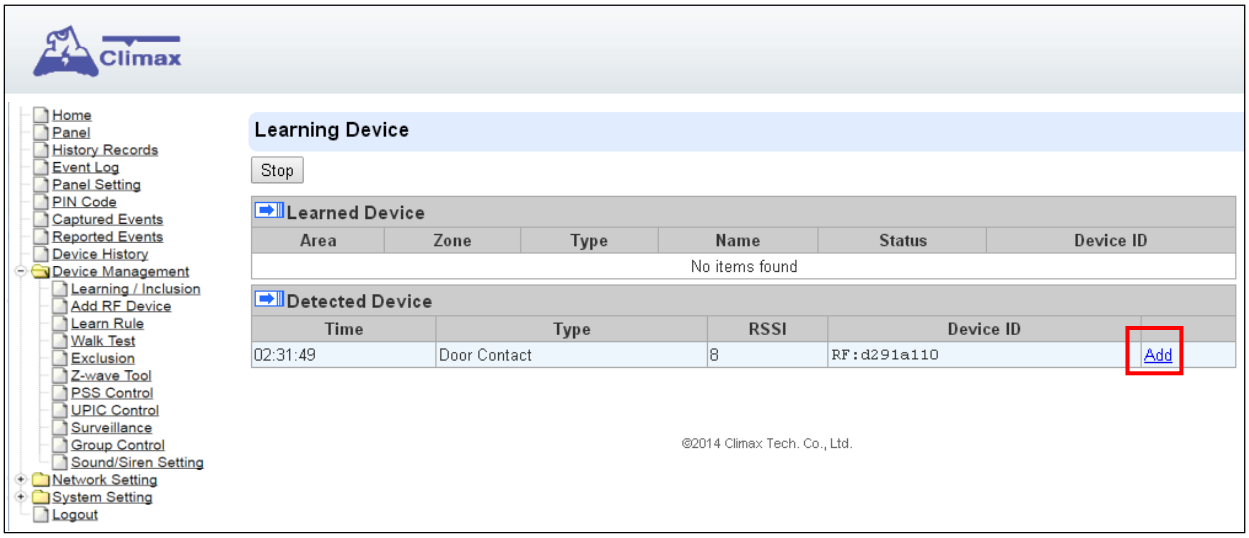
<NOTE>

☞ It takes 5-10 seconds for the Control Panel to receive a learn code from ZigBee or Z-Wave Sensor.

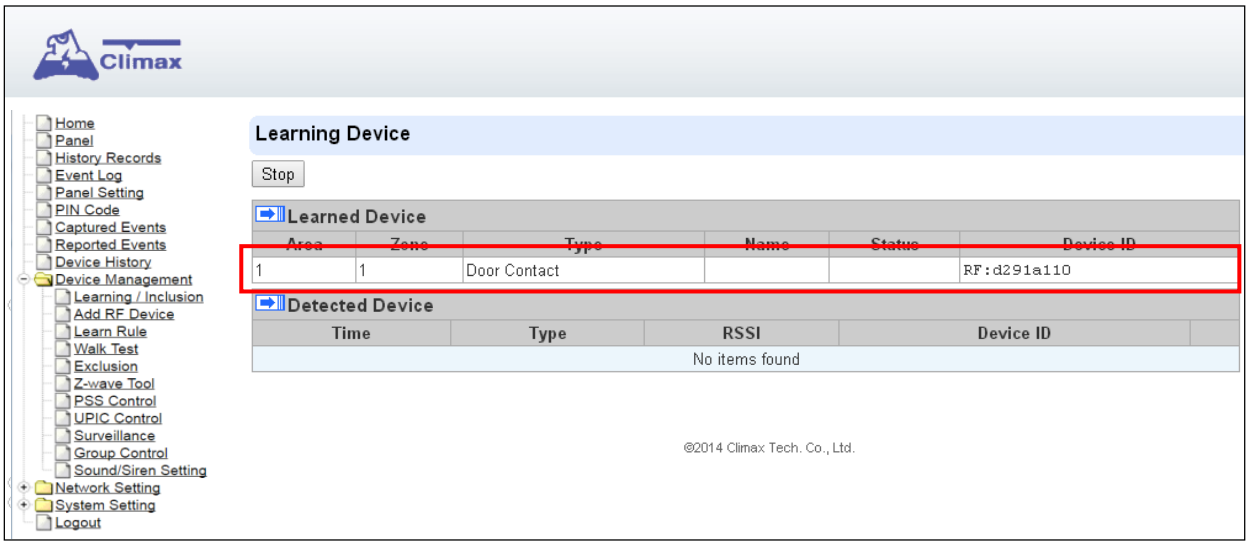
Step 5. Click "**Add**" to include selected device into panel. If the sensor you wish to learn into already exists in the system, the sensor information will be displayed in the **Learned Device** section. If not, the sensor information will be displayed in the **Detected Device** section.

<NOTE>

☞ For VST-862 F1 devices, press and hold the learn button for 3 seconds for the Control Panel to receive a learn code, and then click "**Add**" within 30 seconds.



Step 6. If the device is successfully learnt into the system, the added device will be displayed in the "**Learned Device**" section.



Step 7. Repeat Step 3~5 to learn in all device, click Stop to exit learn mode when complete. The system will automatically exit Learn mode if left idle for 5 minutes.

5.1.2. Local Learning

Instead of learning devices via configuration webpage, you can also learn in devices by using the learn button located on the back of Control Panel.

Step 1. Press and hold the **Learn** Button on the back of Control Panel for 10 seconds, release when the Control Panel emits one short beep. LED 1 Green will turn ON to indicate the Control Panel is now in learning mode

Step 2. Press the test or learn button on each device to transmit signal, refer to device manual for detail.

Step 3. When the Control Panel receives signal from device, it will emit 2 beeps to confirm. The device will be included in the panel automatically.

Step 4. After finish learning all devices, press and holde the Learn button for 1 second. The Control Panel will emit 2 short beeps to indicate it has returned to normal mode. LED1 will dim.

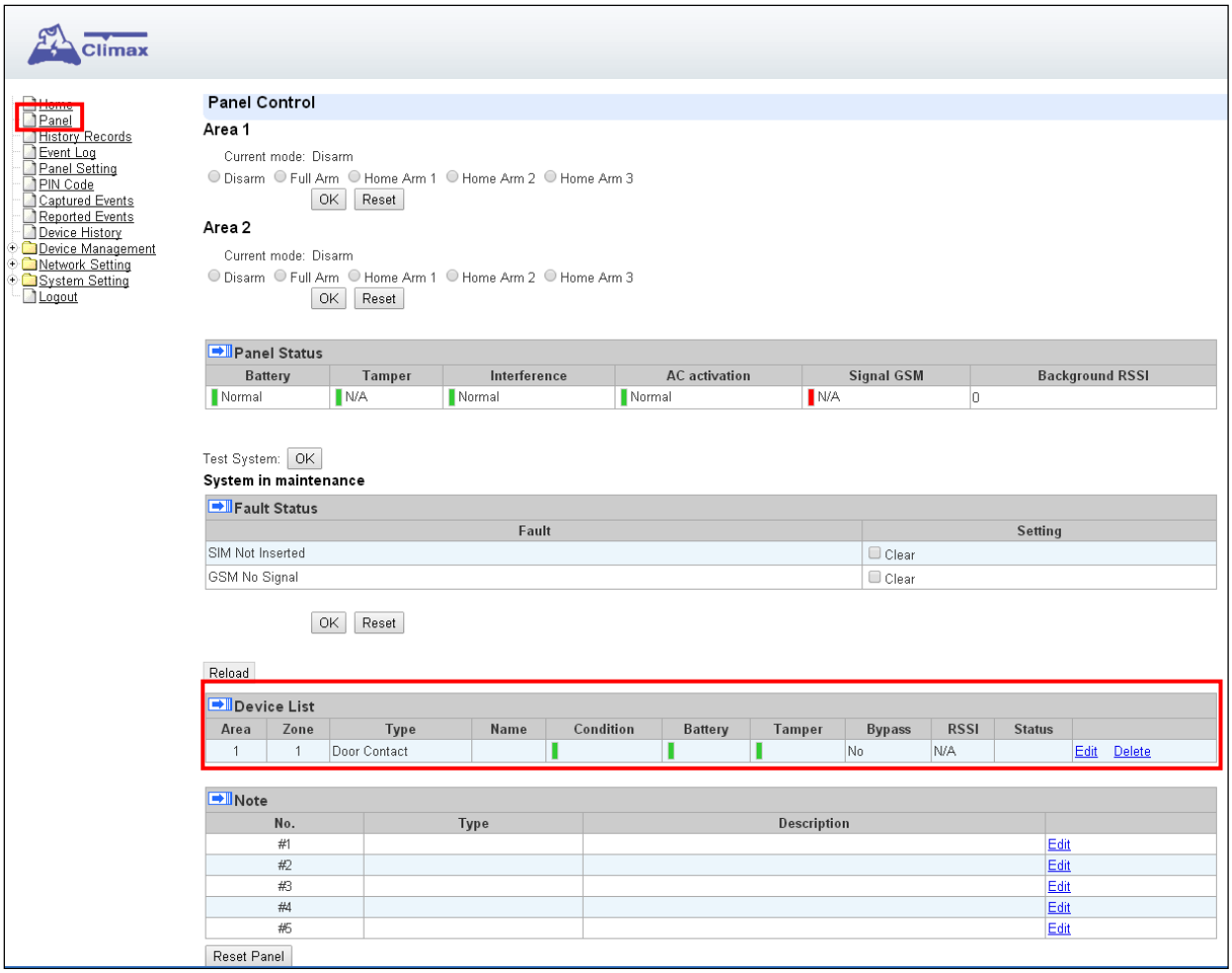
<NOTE>

- ☞ Device learnt in via Local Learning will be assigned to Area 1 only, which is limited to 80 devices.
- ☞ The Control Panel cannot enter learning mode when under Away Arm/Home Arm or Walk Test mode. The Control Panel will emit 5 beeps to indicate error.

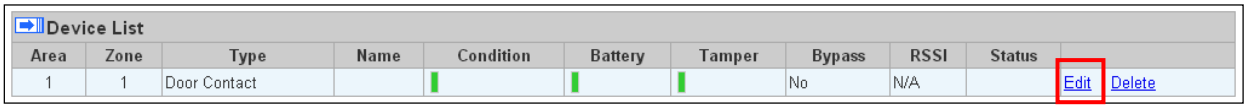
5.1.3. Edit Devices

After finish learning devices, proceed to edit the device setting.

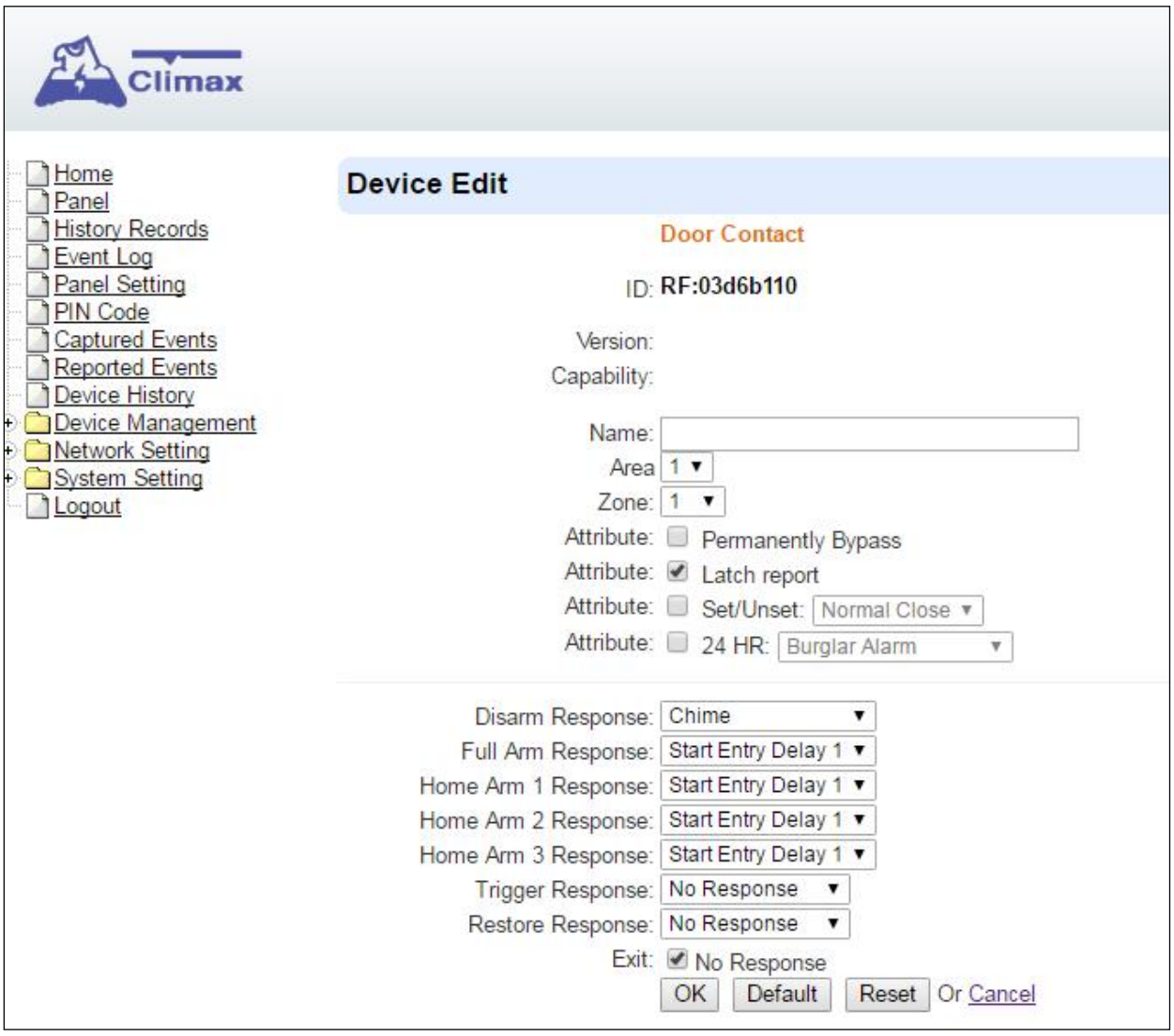
Step 1. Click **Panel** to enter Panel webpage. All learnt in devices will be displayed under **Device List** section.



Step 1. To edit the device setting or information, click "**Edit**" at end of device entry.



Step 2. You will enter Device Edit webpage



Step 3. Edit your device setting and information according to instruction below. Click "**OK**" to save your new changes when finished. Alternatively, click "**Default**" to reset all parameters to default values or click "**Reset**" to re-enter all the information.

- **Name:** Enter a name for the device.
- **Area:** Select the area which the device belongs to.
- **Zone:** Select the Device zone number.

- **Attribute List:**

  The attribute list determines panel behaviour when the panel receives trigger signal from the device. There are

  General Attribute:

  ☞ ***Permanentlyt Bypass***

  This function allows user to permanently deactivate (bypass) the selected device.

  - If bypassed, then the Control Panel will not respond at all when the sensor is

triggered.

- If bypassed, the system can be armed directly regardless the device's fault situation. However, its fault situation will still be monitored, logged and displayed in the webpage.

☞ ***Latch report***

This function **ONLY** applies to Remote Control or Door Contact with Set/Unset attribute enabled.

- Latch Report **ON:** When the device is used to change systm arm mode, the Control Panel will report the arm/disarm action by the particular device.
- Latch Report **OFF:** When the device is used to change systm arm mode, the Control Panel will not report the arm/disarm action by the particular device.

☞ ***Set/Unset***

This function is for Door Contact only. This function allows Door Contact to control system mode.

- **Normal Close:** The system will be armed when the Door Contact is opened, and disarmed when Door Contact is closed.
- **Normal Open**: The system will be armed when the Door Contact is closed, and disarmed when Door Contact is open.

☞ ***24HR***

This function enables the device to activated selected alarm event whenever it is triggered regardless of system mode. System mode response will be disabled if 24HR attribute is enabled.

System Mode Attributes:

The System Mode Attributes determines system behavior under particular arming mode when the sensor is triggered.

☞ ***No Response***

- When a sensor with **No Response** is triggered, the Control Panel will not respond.

☞ ***Start Entry Delay 1/ Start Entry Delay 2***

- When the system is under Full Arm or Home Arm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, Control Panel will start an entry countdown period to give enough time to disarm the system.
- When the Control Panel is in the Disarm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, the Control Panel will immediately report a burglar interior alarm (**CID code: 132**).
- When the Control Panel is in the Full Arm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, the Entry Delay 1/2 timer starts counting down. If no correct pin code is entered during the entry delay timer to disarm the system, the Control Panel will report a burglar perimeter alarm (**CID code:131**) immediately after entry delay timer 1/2 expires.
- When the Control Panel is in the Home Arm 1/2/3 mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, the Entry Delay 1/2 timer starts counting down. If no correct pin code is entered during the entry delay period to disam the system, the Control Panel will report a burglar interior alarm (**CID code: 132**) immediately after entry delay timer 1/2 expires.

☞ ***Chime***

- When the system is in Arm/ Home Arm 1/ Home Arm 2/ Home Arm 3 mode, if a sensor set to Chime is triggered, the Control Panel will sound a Door Chime (Ding-Dong Sound).

☞ ***Burglar Follow***

- When the system is in Full Arm or Home Arm mode mode, if a sensor set to **Burglar Follow** is triggered, the Control Panel will report a burglar alarm immediately.
- When a Start Entry sensor is triggered and the system is under Entry Delay Timer countdown, if a sensor set to **Burglar Follow** is triggered, the Control Panel will wait until the Entry Delay Timer expires before activating a burglar alarm. If the system is disarmed before the timer expires, the Control Panel will not activate alarm.

☞ ***Burglar Instant***

- When the system is under Full arm or Home Arm/ Disarm / Entry Time mode, if a sensor set to **Burglar Instant** is triggered, the Control Panel will report a burglar alarm immediately.

☞ ***Burglar Outdoor***

- When the system is in Full Arm or Home Arm / Disarm / / Entry Time mode, if a sensor set to **Burglar Outdoor** is triggered, the Control Panel will report a burglar outdoor event immediately.

☞ ***Cross Zone***

- See **12.2 Appendix – Cross Zone Verification** for detail.

☞ ***Apply Scene***

- This function is only avaiable for Remote Keypad and Remote Control.
- Select a Home Automation Scene number for a Remote Keypad or Remote Control button. When the button is pressed, the Control Panel will execute the actions programming in the Scene accordingly. For more information, please refer to **8.3. Scene**.

Home Automation Attributes:

The Home Automation Attributes allows a device to control Home Automation function.

☞ ***Trigger Response***

- When the device is triggered, the Control Panel will activated selected Home Automation Scene number. Please refer to **8.3. Scene** webpage for detail.

☞ ***Restore Response***

- When the device transmits restore signal after trigger, the Control Panel will activate selected Home Automation Scene number.

Other Attributes:

☞ ***Permanent Bypass***

- When checked, the panel will completely ignore all signal received from this device. A bypassed device will be unable to trigger any response, including alarm or fault from the Control Panel. All other attribute settings will be also be ignored.

☞ ***Exit (No Response)***

- If checked, the panel will ignore trigger signal from this sensor during Exit Time countdown. If deselected, the panel will activated burglar alarm and report immediately when the sensor triggered during Exit Delay Timer.

☞ ***24HR***

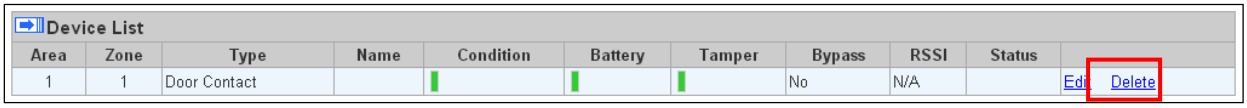
- A sensor set to 24HR attribute will ignore Disarm, Full Arm, Home are and Exit response setting. The panel will activate selected alarm when this sensor is triggered regardless of system mode under any time.

<NOTE>

☞ Some devices have their own unique functions and will have its own attribute setting which is not listed in this section. Please refer to the device manual for its setting detail.

5.1.4. Delete Devices

Step 1. To delete a sensor, click "**Delete**" under "**Device List**"

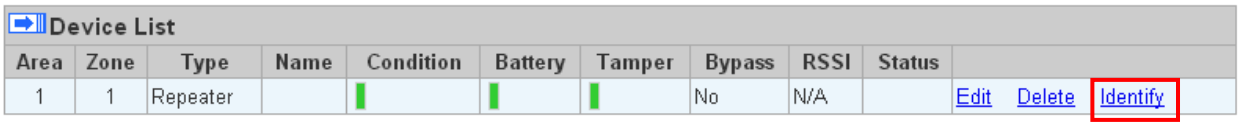


Step 2. A message "**Delete success**" is displayed and the sensor you choose is deleted successfully.

5.1.5. Identify ZigBee Device

The Identify function is available for ZigBee device only, it can be used to locate ZigBee devices after learning.
For battery powered ZigBee devices, the identify fuction should be used within 1 minute after pressing device button, or 3 minute after learning in the device. Otherwise due to ZigBee network mechanisms, the device may not be able to receive signal successfullly from panel.
AC powered ZigBee devices do not have such limits and you can use Identify function anytime.

Step 1. Click "Identify" under the Device List after the device column entry.



Step 2. If the ZigBee device receives signal successfully, the webpage will display a success message and the ZigBee device LED indicator will flash 10 times to confirm.

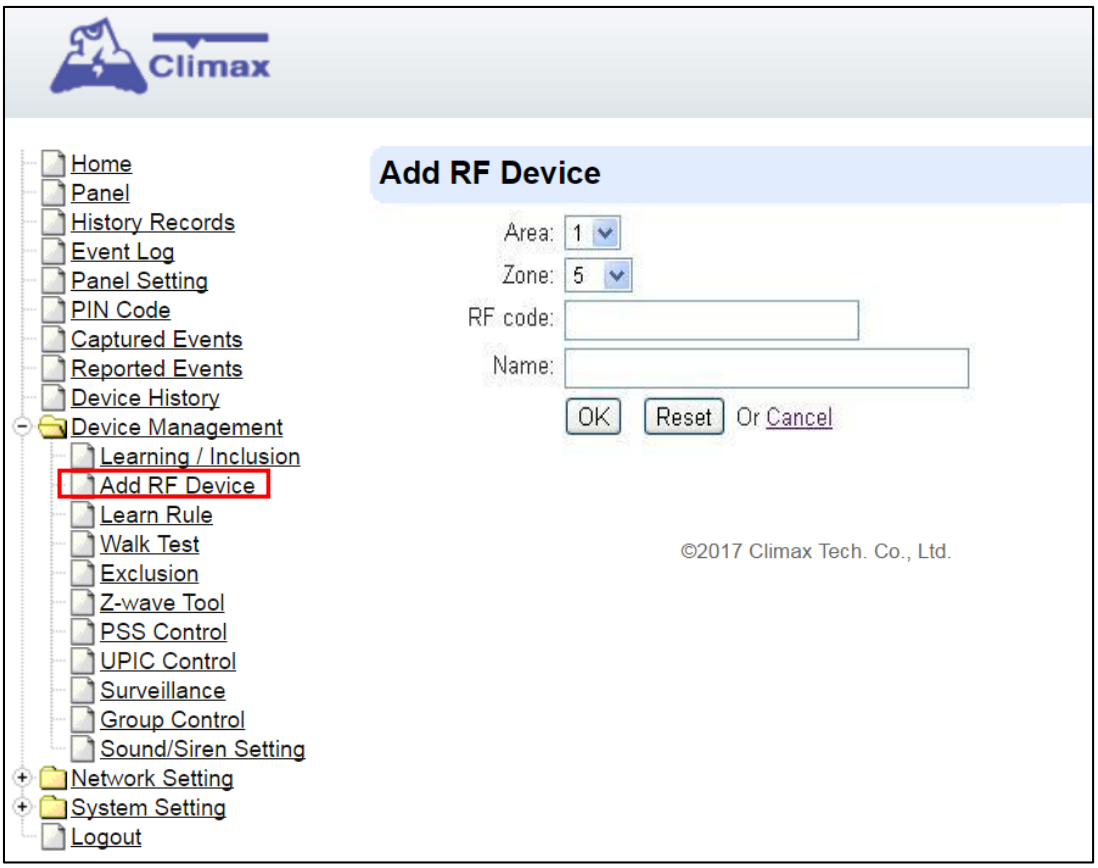
<NOTE>

☞ If a timeout message is displayed on webpage, it means the device did not receive signal from Control Panel, please check ZigBee device range from panel and make sure to follow instruction above about Identifying battery powered ZigBee devices.

5.2. Add RF Device

Besides learning, you can also add RF devices into the system by entering its RF code into the system with **Add RF Device** function.

Step 1. Click **Add RF Device**.



Step 2. Select Area and Zone number for the device you wish to add into system.

Step 3. Enter the device RF code, and preferred device name (up to 31 characters)

Step 4. Press “OK” to save

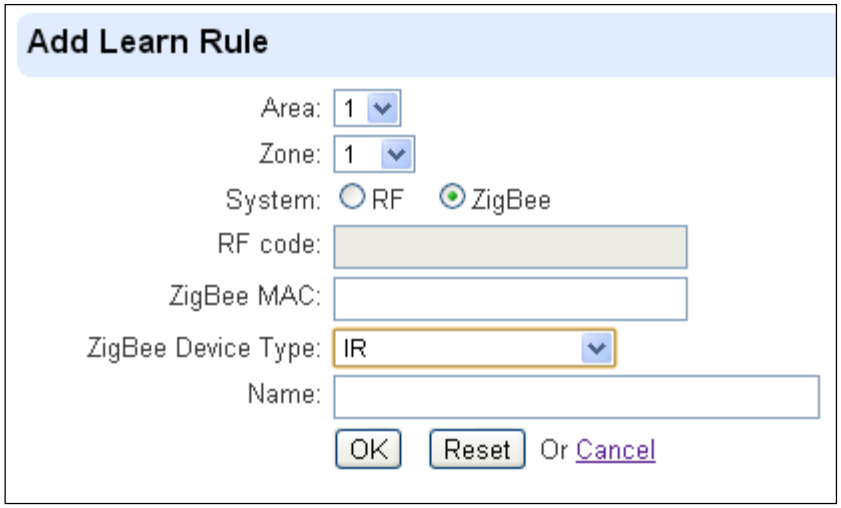
Step 5. If the RF code you entered is valid, the device will be added into the system according to the Area and Zone number. You do not need to learn the device as instructed in **5.1.1. Add Sensor**.

5.3. Learn Rule

You can enter the sensor RF code or ZigBee MAC address manually to assign area and zone number to this sensor. Sensors learned with pre-assigned rule will be put under the area and zone number you specified. This function does not work with Z-Wave devices and DECT device.

Step 1. Click **Learn Rule**.

Step 2. You will see the **Add Learn Rule** menu.



Step 3. Select **Area** and **Zone** number for this device.

Step 4. Select **RF** or **ZigBee**.

Step 5. Key in the RF code or ZigBee MAC info

Step 6. For ZigBee device, select a ZigBee Device Type

Step 7. Enter a preferred name for sensor (up to 31 letters or numbers).

Step 8. Press “OK” to save.

Step 9. If the process is successful, the screen will display “**Updated Successfully**.” You can then check, edit or delete the rule under the **Learn Rule** menu.

Step 10 Repeat the steps to add more rules.

Step 11. Learn in the sensors you have entered rules for according to **5.1.1 Add Sensor**.

<NOTE>

☞ Learn rule function is only used to pre-assign area and zone number to sensors before learning. To add senor to control panel, you still need to follow the instruction in **5.1.1 Add Sensor** to complete the learning process.

- **Backup Device List to Learn Rule**

You can choose to import learn rule from current learnt in ZigBee devices

Step 1. Click “Backup Device List to Learn Rule”.

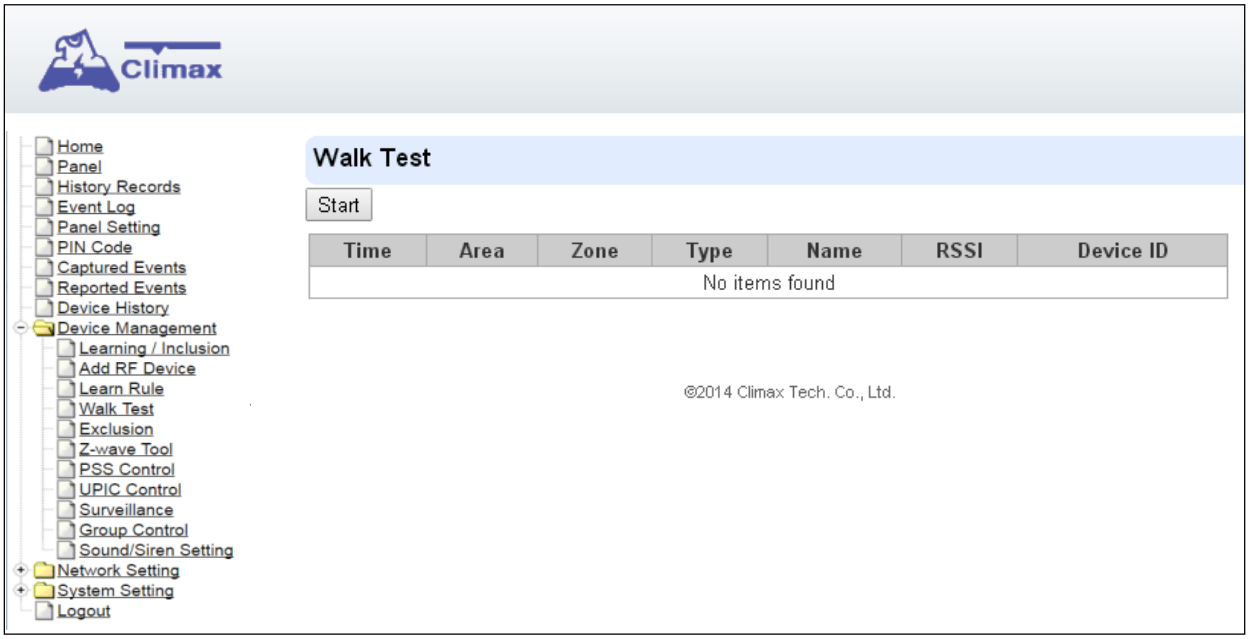
Step 2. Click OK to confirm.

Step 3. The Learn Rule page will be updated with new rules according to current ZigBee device list information. Z-wave device and IP Camera will not be included.

5.4. Walk Test

This is to test the sensor operation range for installation purpose.

Step 1. Click "**Start**" to enter Walk Test mode.



Step 2. Press the test button on the sensor(s) or any button on the Remote Controller or triggering the sensor.

Step 3. When the Control Panel receives a signal, it will show as below and a 2-tone beep will be heard to indicate that it is safe to install the particular sensor in the location.

- **Time**: time informaiton
- **Area**: operation area
- **Zone**: device zone
- **Type**: device type
- **Name**: device name
- **Rssi**: the RF signal strength between Control Panel and sensor. The Rssi value here must be higher than the Rssi value of Panel's background noise (please refer to *6.1 Panel Condition section for details*). If not, you may still learn in the sensor; however, please relocate the sensor and use Walk test to find a more suitable location.
- **DeviceID**: device's unique identification code.

Step 4. Once all sensors are tested, click on "**Stop**" to exit Walk Test mode. The system will automatically exit Walk Test mode if left idle for 5 minutes.

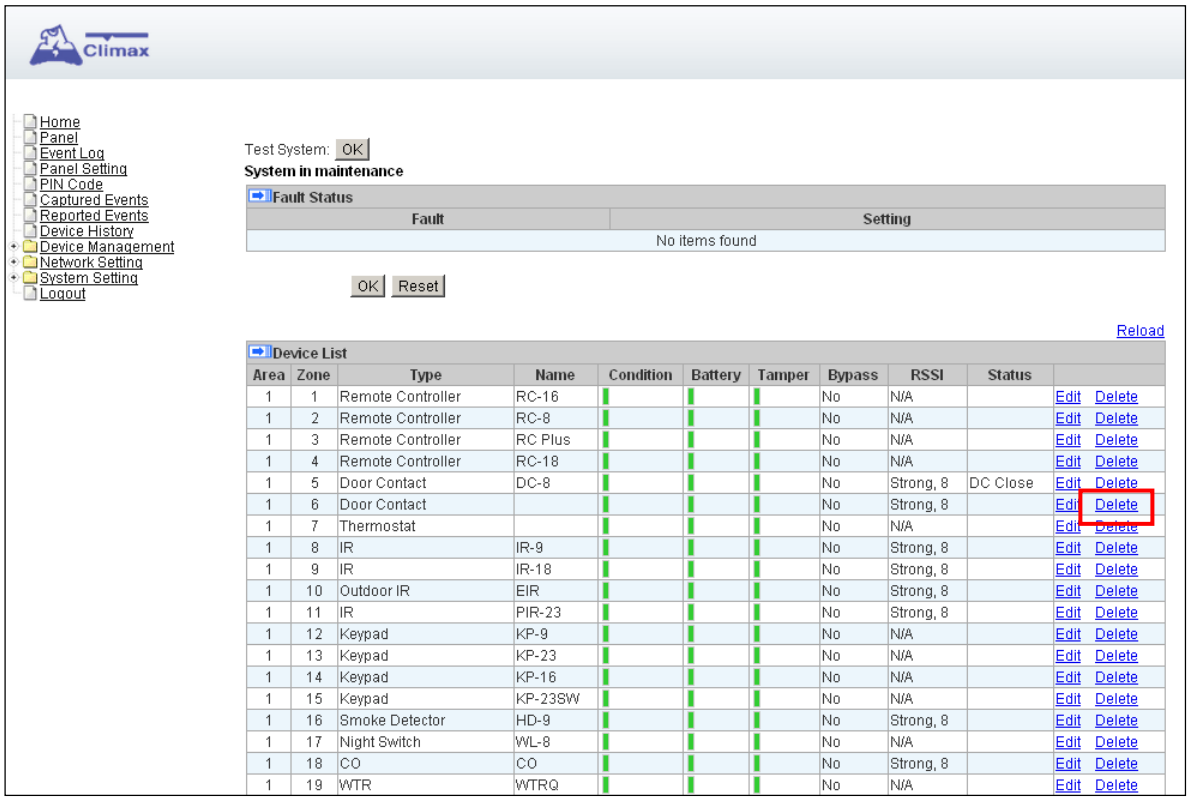
5.5. Exclusion

This feature is only available for Z-Wave modules only, or when a Z-wave dongle is inserted into the Control Panel. This feature is for you to remove Z-Wave device only.

Step 1. Click on "**Exclusion**" and click on "**Start**" to start the procedure. Then the Panel will enter the removing mode.

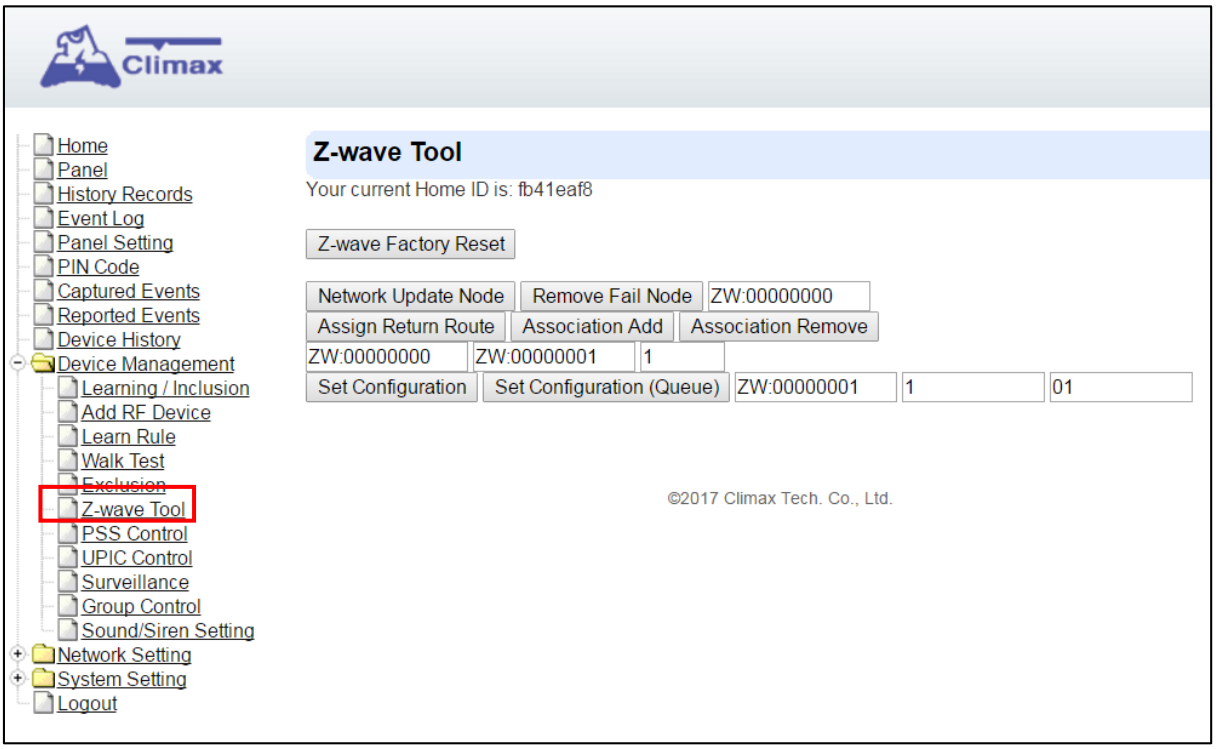
Step 2. Refer to the Z-Wave device manual to transmit signal.

Step 3. Select the desired Z-Wave and click **delete** to remove it from the Z-wave list under **Device List** section (**Panel)**. Then the Control Panel will remove the Z-Wave device.



5.6. Z-Wave Tool

The Z-wave Tool is used to reset Z-wave module to factory default and remove all Z-wave devices, or change routing setting.



Step 1. Click "**Z-Wave Factory Reset**", the Z-Wave module is reset to factory default and all Z-Wave devices will be removed automatically. The Control Panel Home ID will also be changed automatically for a newly added Z-Wave device to recognize.

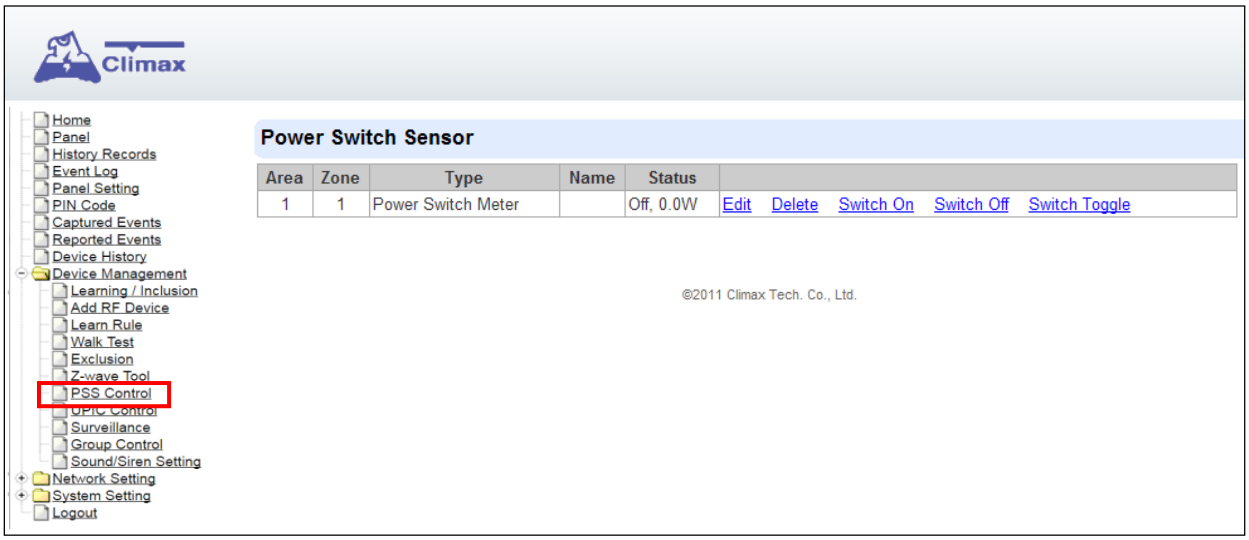
Step 2. The list of Z-Wave devices is still displayed in the **Panel** webpage. Please go to panel webpage and remove all Z-wave devices.

- **Change Z-Wave Routing Setting**

Use the other functions to configure your Z-Wave routing settings.

5.7. PSS Control

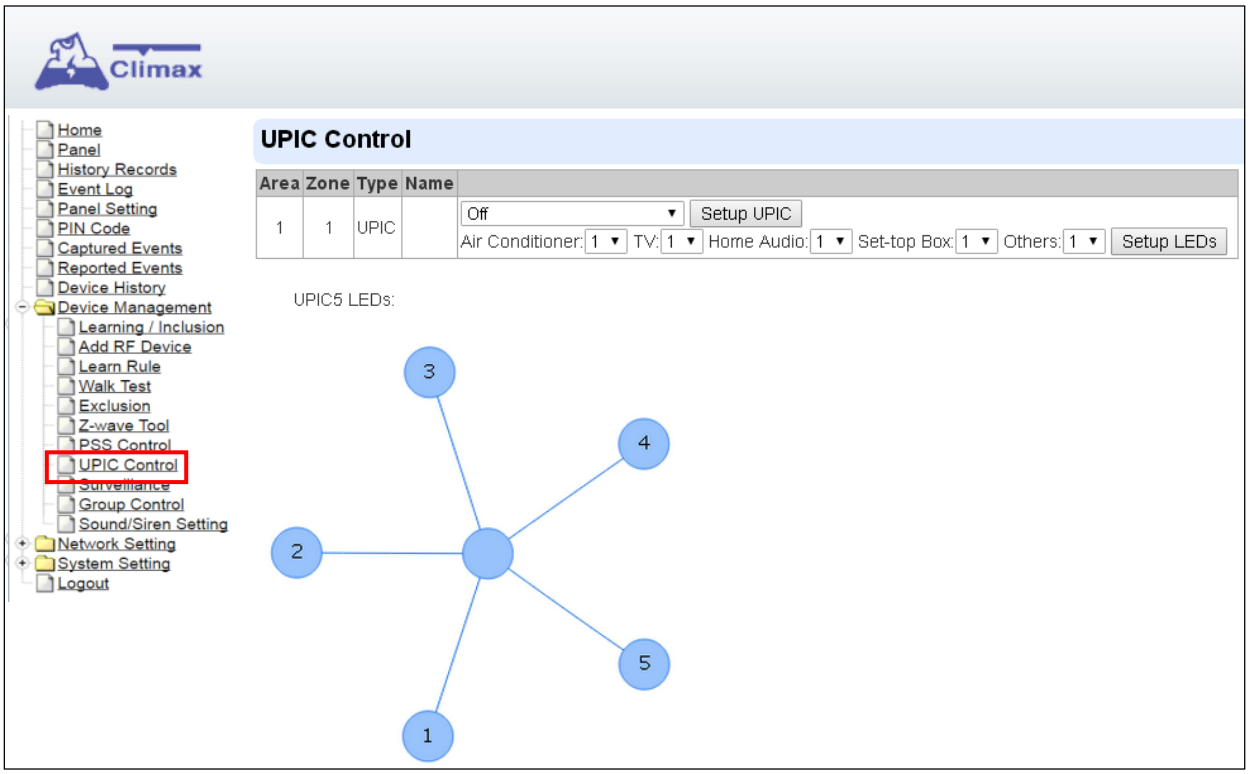
This feature is designed to control/edit/delete Power Switches included in the panel.



- Click **Edit** to edit attributes of power switches.
- Click **Delete** to remove power switch from panel.
- Click **Switch On/Switch Off** to turn on/off power switches. Or click **Switch Toggle** to toggle between on/off status. For Power Switch Dimmer, you can also set its power output level with the slide down menu.

5.8. UPIC Control

UPIC Control webpage allows you to control UPIC IR Transmitter included in Control Panel



- **Transmit IR Signal**

Depending on the UPIC model number, select the function to be performed in the drop down menu, then click “Setup UPIC” for the UPIC to transmit IR Signal.

- **UPIC5 LED Setup (UPIC5 only)**

UPIC5 has 6 IR LEDs, a central one and 5 surrounding ones. The central LED will always transmit IR signal when activated; besides the central LED, one of the 5 surrounding LEDs can be selected to activate upon IR signal transmission to increase the IR signal coverage.

Step 1: Refer to the diagram on the webpage and UPIC5 manual to determine which LED should be used for signal transmission to each particular home appliance.

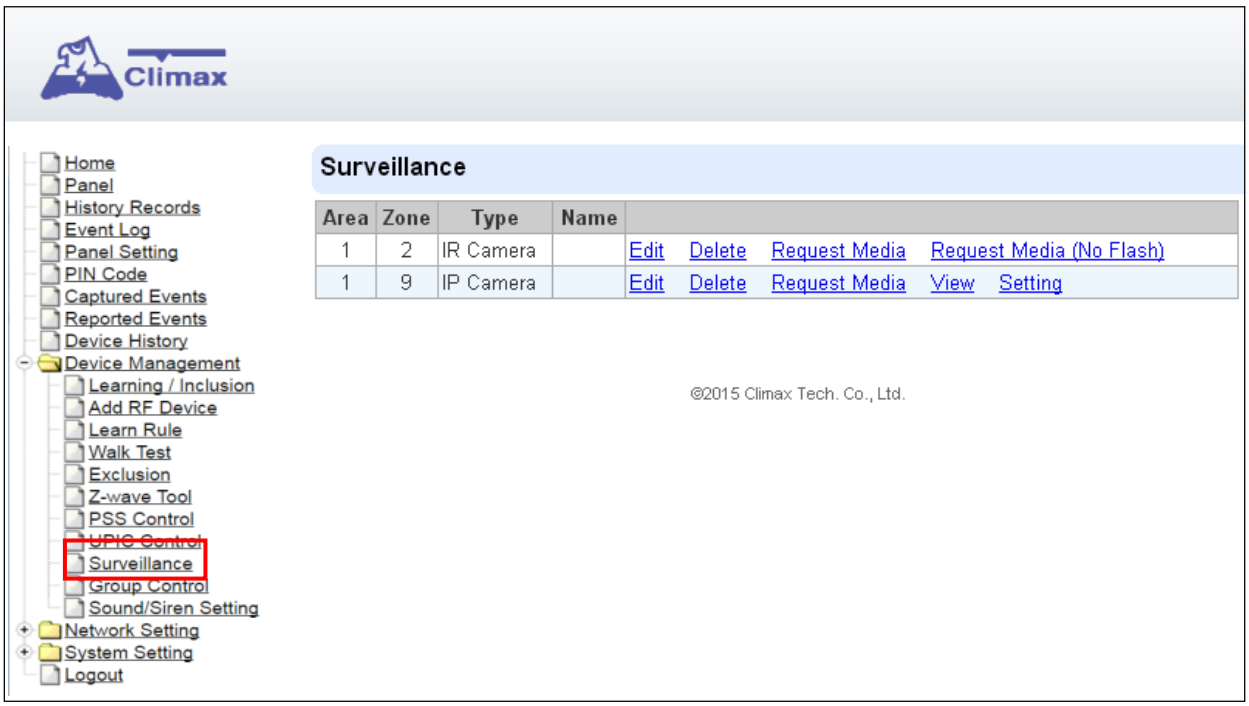
Step 2: Select the LED number from the drop down menu for each appliance type, then click “Setup LED” to confirm. Please refer to UPIC5 manual for more information.

<EXAMPLE>

- ☞ If “Air Conditioner” is set to LED 1, UPIC5 will transmit all Air Condition functions with both Central LED and LED1.
- ☞ If “TV” is set to LED 5, UPIC5 will transmit all Air Condition functions with both Central LED and LED5.

5.9. Surveillance

The PIR Camera/Video Cameras and IP Cameras are listed under **Surveillance** for separate control.



- Click **Edit** to edit camera attributes.
- Click **Delete** to remove device from panel.
- Click **Request Media** to capture a picture or vide
  - PIR camera: A picture will be captured upon request
  - PIR Video Camera: A 10-second video will be recorded upon request
  - IP Camera: The IP Camera will record a video according to its video length setting (Please refer to IP Camera manual for detail.)
  - For PIR Camera/Video Camera, you can choose to take the picture/video without activating the camera's flash.

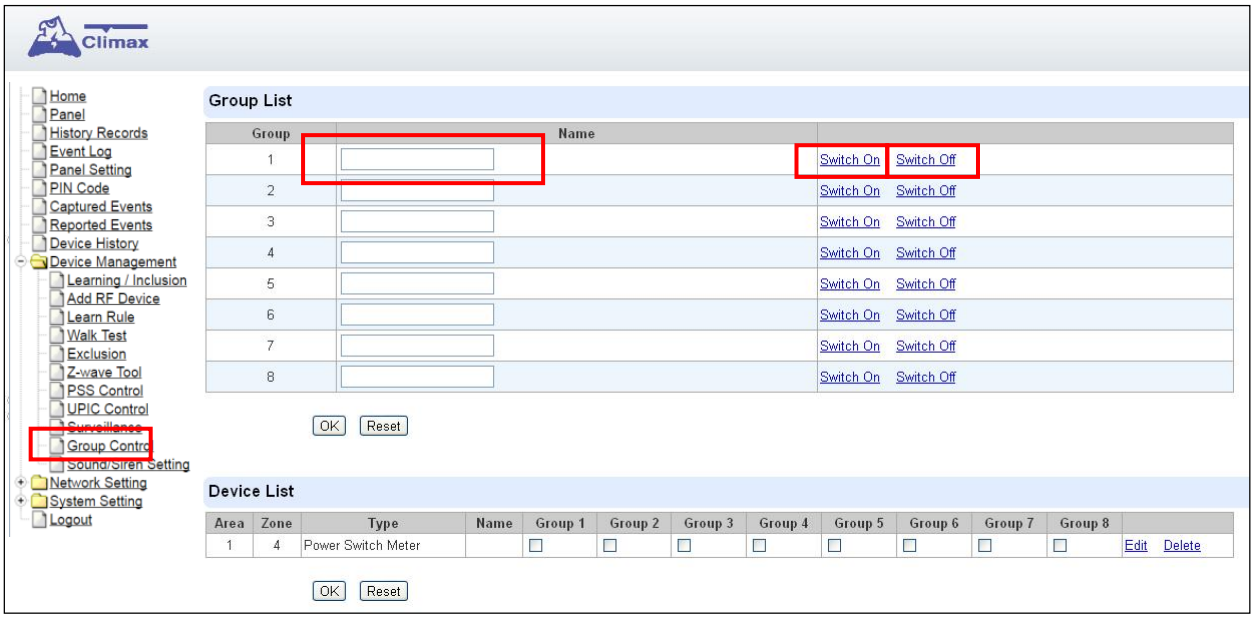
  Picture and video captured by PIR Camera and PIR Video Camera will be stored under the **Captured Event** webpage. Video Recorded by IP Camera will be stored in the IP Camera, please refer to IP Camera manual to view the video
- For IP Camera, click "View" or "Setting" to access IP Camera webpage for video streaming or setting configuration. A new webpage will open and you will be required to enter the username and password for the IP Camera to access streaming or setting.

5.10. Group Control

This feature is designed for you to edit a name of group, switch on or off a group of Power Switches. You can also assign Power Switches to groups you desire.

5.10.1. Group Control/Edit

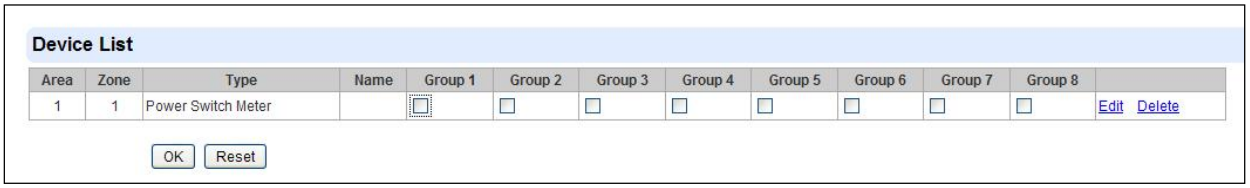
Step 1. Specify a new name for a group.



Step 2. Click Switch On or Switch Off to turn on or off one group of power switches.

5.10.2 Device Edit/Delete

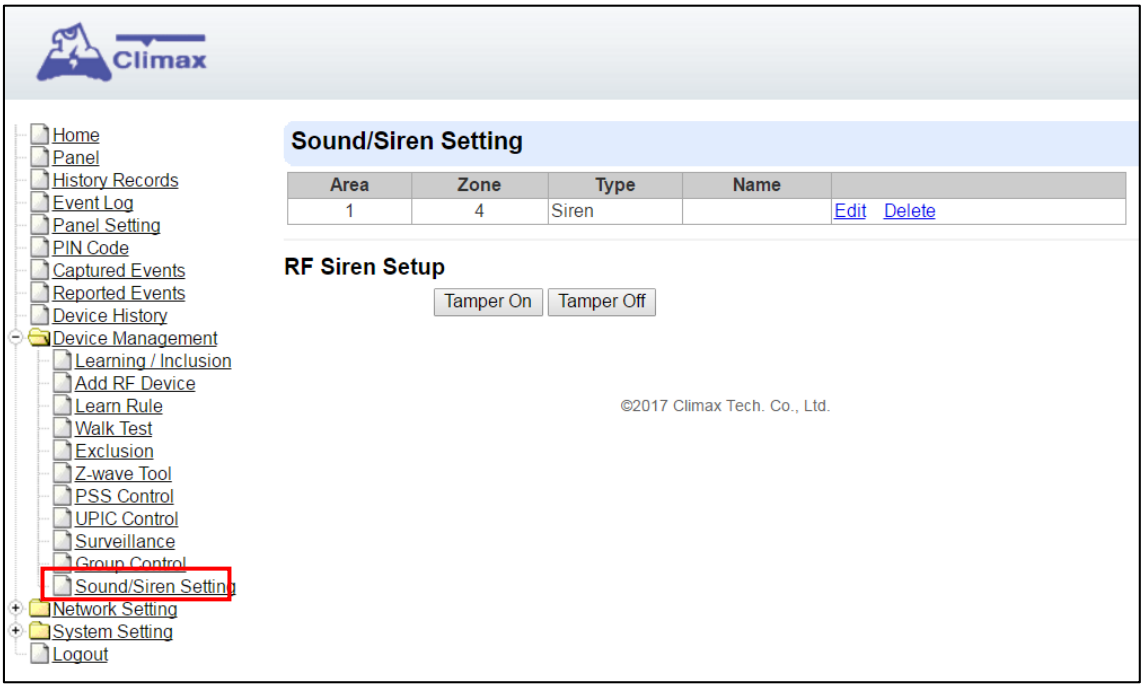
Step 1. Check on the groups you wish to assign the Power Switch. This is a multiple-choice field and you can assign one Power Switch to multiple groups. Whenever one of the assigned groups receives request to turn on/off, all Power Switches belonging to the group will be activated accordingly.



Step 2. Click **Edit** to edit attributes of an added power switch or power switch meter or **Delete** to delete this device.

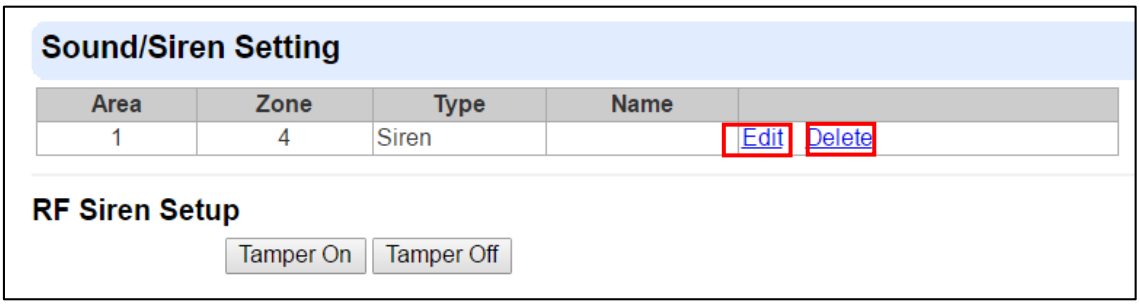
5.11. Sound/Siren Setting

The Sound/Siren Setting page includes setting Siren configuration function.

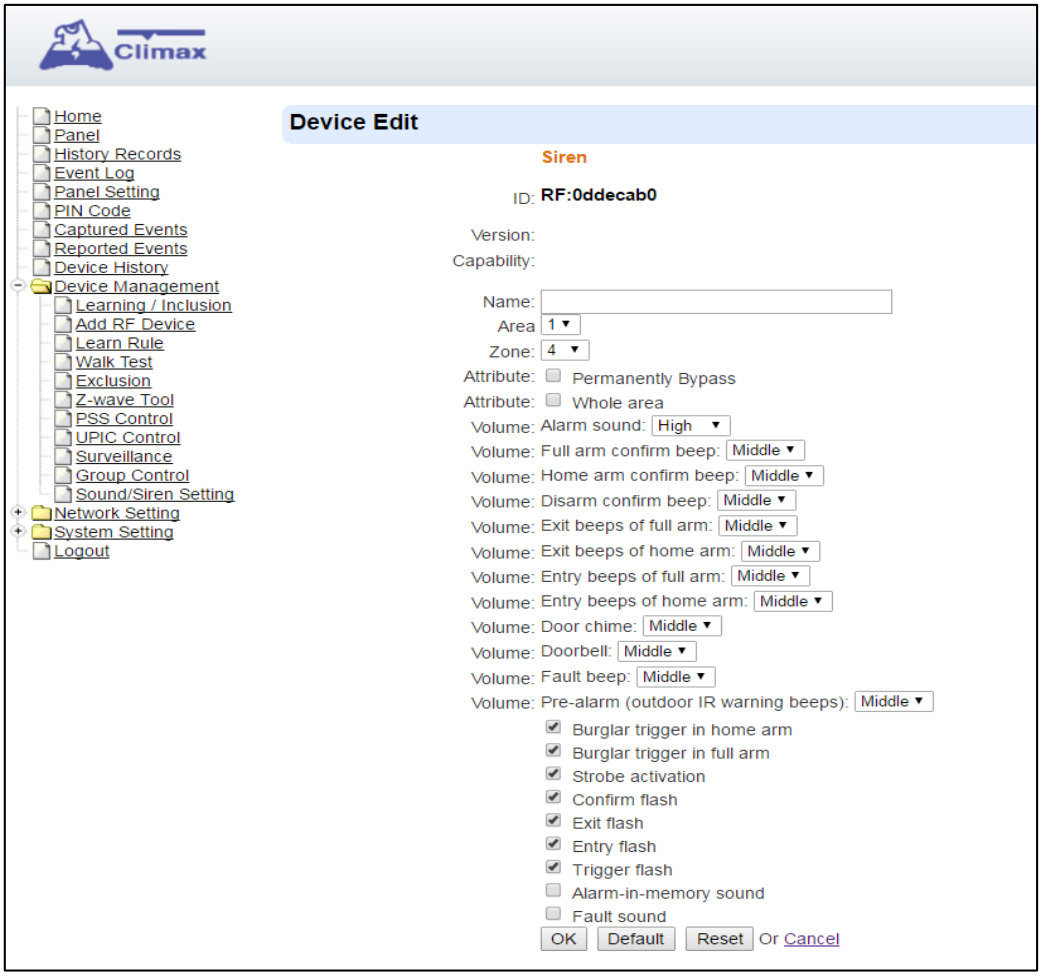


5.11.1. Device Edit/Delete

Click **Edit** to edit the Siren's attribute, volume and voice settings, or **Delete** to delete the Siren.



After clicking **Edit**, you will be directed to the Device Edit page:



<NOTE>

☞ The Device Edit page is only available for the newest BX/Siren series and BX series **without DIP Switch**.

Edit your Siren setting and information accordingly to instruction below. Click "**OK**" to save your new changes when finished. Alternatively, click "**Default**" to reset all parameters to default values or click "**Reset**" to re-enter all the information.

- **Name:** Enter a name for the Siren.
- **Area:** Select the area which the Siren belongs to.
- **Zone:** Select the Siren zone number.

☞ ***Attribute:***

- **Permanently Bypass:** If checked, the Control Panel will completely ignore all signal received from the Siren. A bypassed Siren will not be able to trigger any response, including alarm or fault from the Control Panel. All other attribute settings will also be ignored.
- **Whole Area:** if checked, all the Volume, Voice and Behavior functions will be simultaneously enabled in Area 1 and Area 2.

☞ ***Volume:***

- **Alarm Sound:** set the volume of the alarm sound of the Siren when alarming.
- **Full arm confirm beep:** set the volume of the confirm beep sound of the Siren when

Control Panel is put into Full Arm Mode.

- **Home arm confirm beep:** set the volume of the confirm beep sound of the Siren when Control Panel is put into Home Arm Mode.
- **Disarm confirm beep:** set the volume of the confirm beep sound of the Siren when Control Panel is put into Disarm Mode.
- **Exit beeps of full arm:** set exit countdown beep volume under Full Arm Mode.
- **Exit beeps of home arm:** set exit countdown beep volume under Home Arm Mode.
- **Entry beeps of full arm:** set entry countdown beep volume under Full Arm Mode.
- **Entry beeps of home arm:** set entry countdown beep volume under Home Arm Mode.
- **Door Chime:** set the volume of the Door Chime sound (Ding-Dong Sound).

☞ ***Voice:***

*(The following functions are only available for **SRV** devices):*

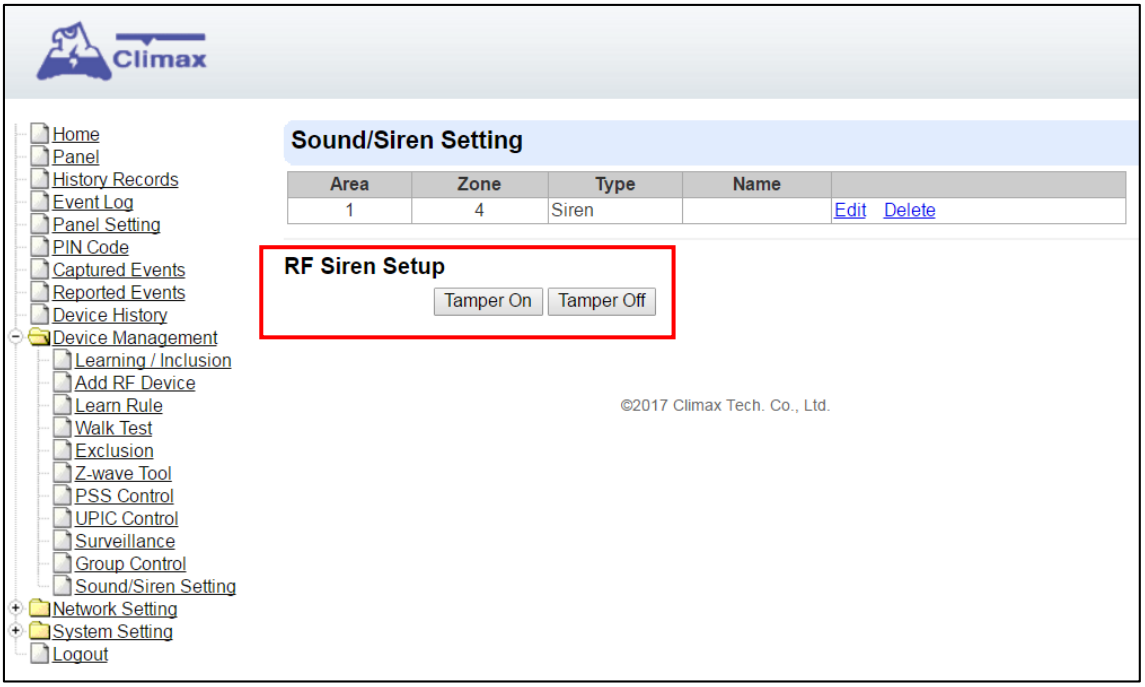
- **Doorbell:** set the volume of the ring tone when pressing the button on the Video Door Phone (VDP).
- **Fault beep:** set the volume of the voice played when system is force armed under fault conditions.
- **Pre-alarm (outdoor IR warning beeps):** set the volume of the voice played when an outdoor burglar sensor(Door Contact, IR) is triggered.

☞ ***Behavior***

*(The following functions are only available for **RF modules**):*

- **Burglar trigger in home arm:** Enable or Disable whether Siren is activated when an alarm is triggered under Home Arm.
- **Burglar trigger in full arm:** Enable or Disable whether Siren is activated when an alarm is triggered under Full Arm.
- **Strobe activation:** Enable or Disable Siren LED strobe activation.
- **Confirm flash:** Enable or Disable Siren LED flash when system Armed/Disarmed.
- **Exit flash:** Enable or Disable Siren LED flash during an exit countdown period.
- **Entry flash:** Enable or Disable Siren LED flash during an entry countdown period.
- **Trigger flash:** Enable or Disable the flashing from the Siren LED when alarming.
- **Alarm-in-memory sound:** Enable or Disable Alarm in Memory sound.
- **Fault sound:** Enable or Disable system fault sounds.

5.11.2. RF Siren Setup



- **Tamper On/Off**

  You can enable/disable all RF Sirens tamper protection with this function. Select to turn on or off the sirens tamper function.

<NOTE>

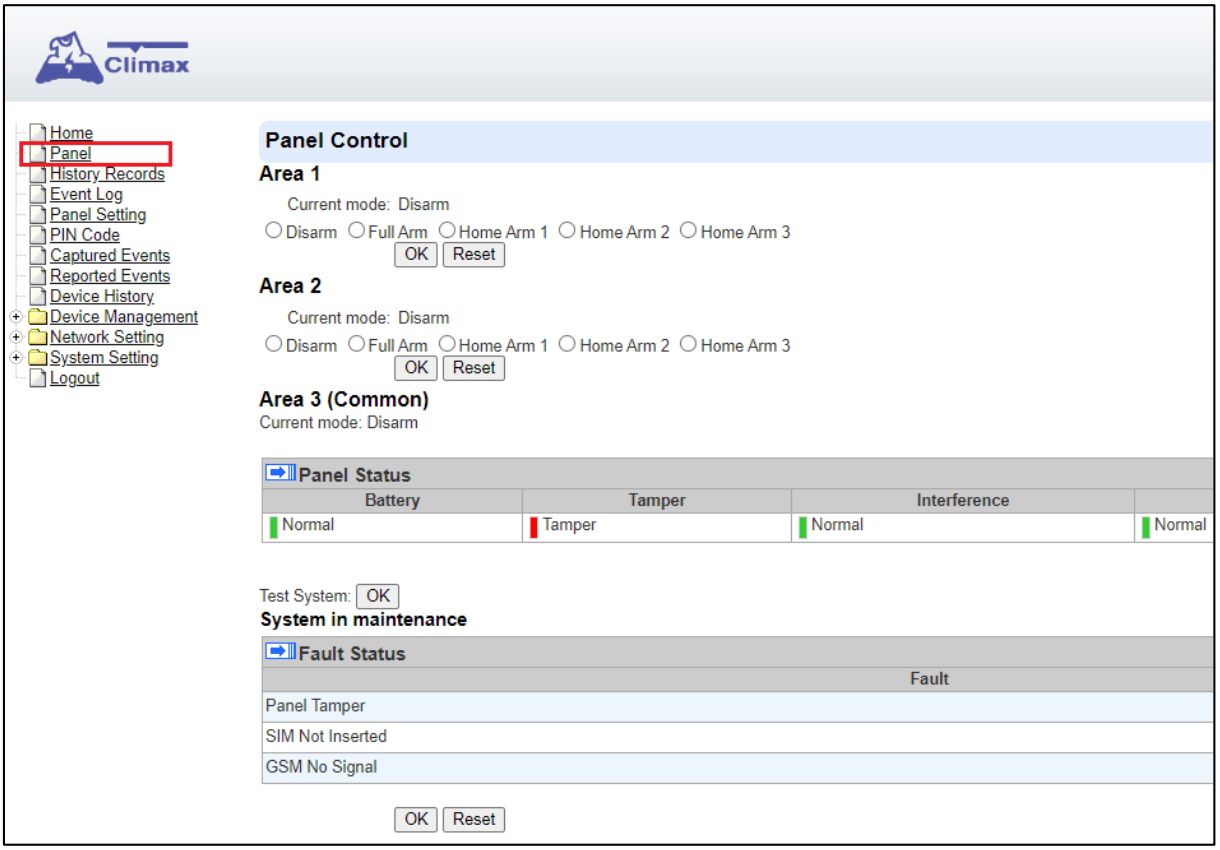
☞ When turned off, if siren tamper will be enabled again automatically after one hour if not turn on manually during the one hour period.

6. Program the System

After the initial set-up, you can then program your system by clicking on the left menu to set them individually.

6.1. Panel Condition

In the **Panel** Section, user can arm, disarm or partially arm the system. Besides, it displays the current **Panel Status** & **Device Information**.



Panel Control

Select a choice to arm, disarm or partially arm the system.

Panel Status

The Control Panel will update the panel status periodically. However, in order to show the current status, you must reload the screen to refresh the display.

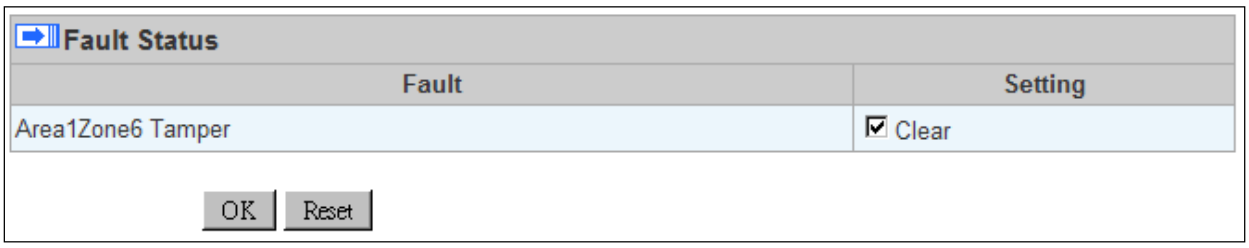
- **Battery**: When battery is running low, a “low battery” message will be displayed to inform you to recharge the battery.
- **Tamper**: (reserved)
- **Interference:** This is for you to check whether the Control Panel is purposely interfered. The jamming period detected will be accumulated, and when the total period exceeds 30 seconds within 1 minute, a “Jamming” message will be shown and reported to the Central Monitoring Station accordingly.
- **AC activation**: To check whether AC power is connected. If not, it will show “AC Failure”.
- **Background RSSI**: Rssi value is for you to check the RF environment around the

Control Panel. It ranges from 0 to 9, where 0 refers to the weakest and 9 refers to the strongest background noise. Therefore, the lower the Rssi value, the better the environment.

Test System

The function is designed to send a command to sever over the polling or XMPP protocol.

Fault Status



The fault events that exist in the alarm system is displayed under this section. When fault event exists in system, the control panel Fault LED will light up to indicate fault status under Disarm or Home Arm mode (The Fault LED will not light up under Arm mode).

When fault event exists, and you attempt to arm the system, the arming action will be prohibited and the panel will display fault information on the webpage. If you still want to arm the system, perform the arming action again to force arm.

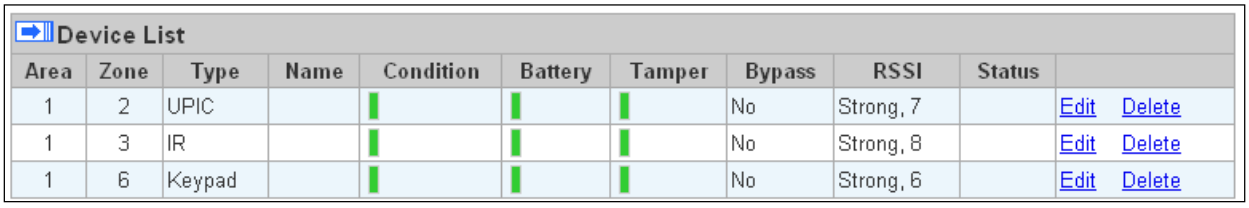
You can check the “Clear” box in the setting column then click “OK” to ignore the fault event. Cleared fault event will not cause the Fault LED to light up, nor prohibit arming.

Device List

1. The Control Panel will update the device information periodically. However, in order to show the current status, you must **reload** the screen to refresh the display.

- **Area**: operation area
  - **Zone**: device zone
  - **Type**: device type
  - **Name**: device title
  - **Status**: device’s current status, such as tamper status, battery status, out of order condition or DC open. If PSM is added into the system, the data of PSM, such as On/Off status, voltage, electric current and watt, will be displayed.

2. Under **Device**, you could further **edit** or **delete** an added device (please refer to **5.1.3** and **5.1.4** for details). Beside, you can reset Panel settings or clear the system faults by pressing **Reset Panel**.



- After pressing **Reset Panel**, the Control Panel will restart in 60 seconds and all configured values will be kept without any change.

Note

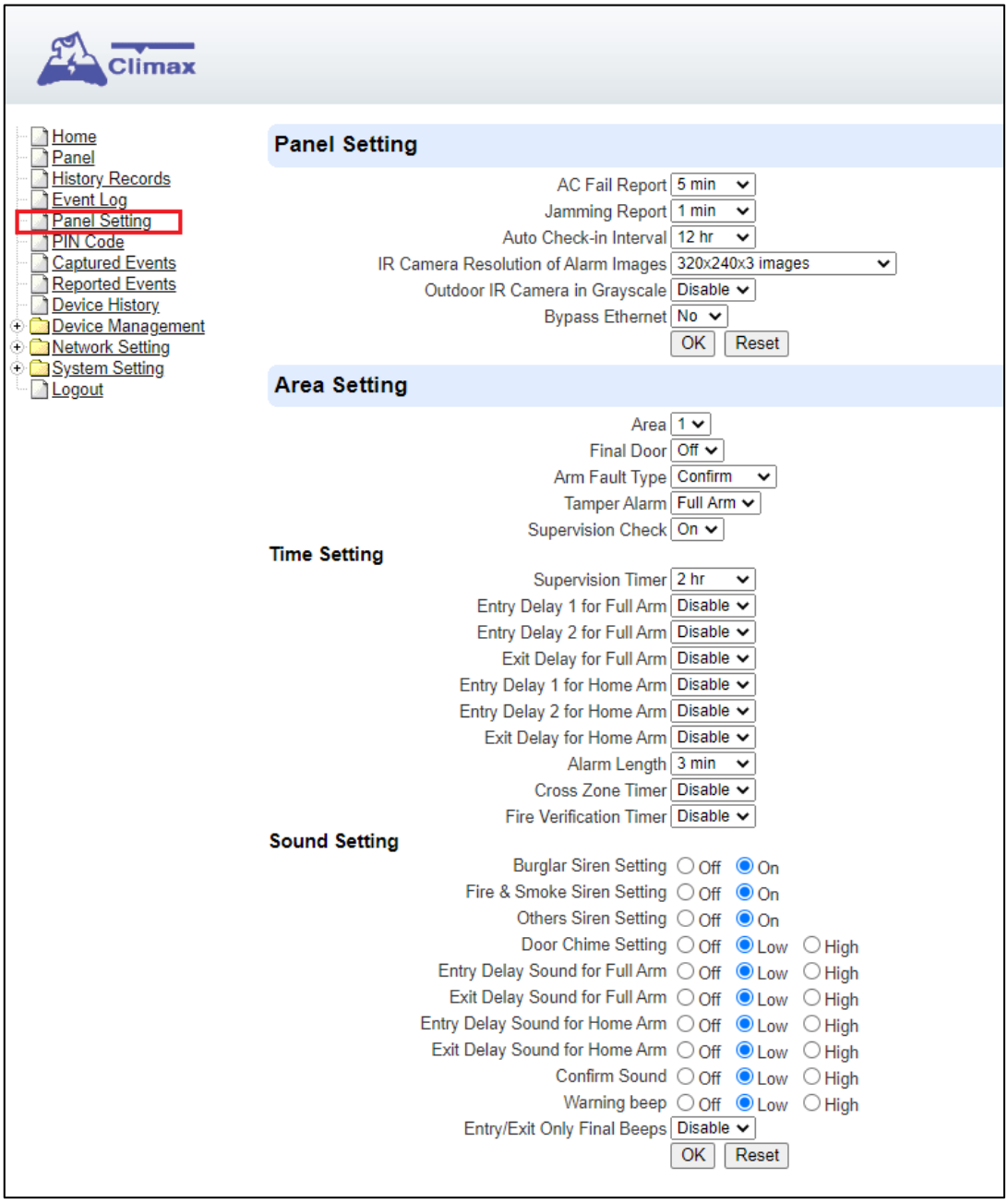
Note

No.	Type	Description	
#1			Edit
#2			Edit
#3			Edit
#4			Edit
#5			Edit

The function is designed for installer to make a note for each control panel. The note you make here can be delivered to a server over XMPP or polling protocol.

6.2. Panel Settings

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



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**: this function is reserved.
- **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 Greysclae**: This is to select whether pictures from Outdoor PIR Camera should be taken in greyscale 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 Arm: 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

- **Burglar Siren setting**: this is for you to decide whether the Control Panel sounds when there is a burglar alarm.
- **Fire & Smoke Siren setting**: this is for you to decide whether the Control Panel sounds when there is a fire alarm, smoke alarm, or gas alarm.
- **Others Siren setting**: this is for you to decide whether the Control Panel sounds when there is a panic alarm, water alarm, emergency alarm, etc.
- **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**.

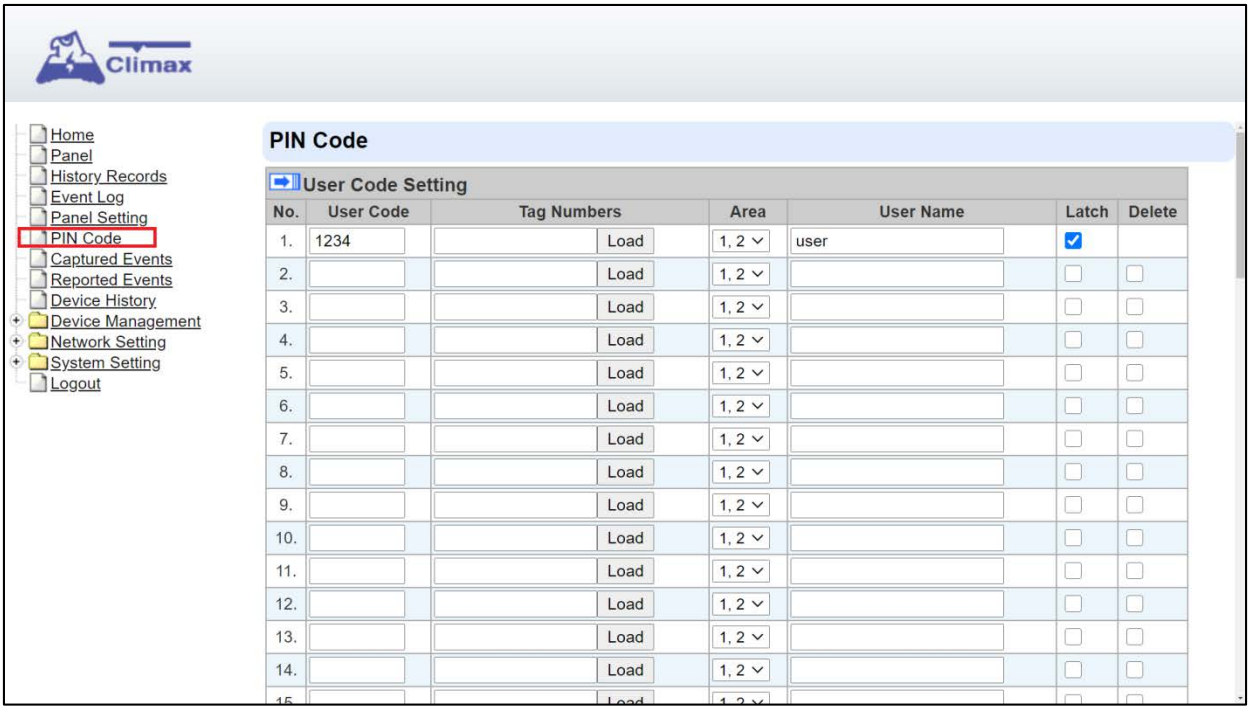
  The Control Panel sounds a Door Chime (Ding-Dong Sound) while the DC and/or IR is activated in Disarm / Full / Home / Entry mode.
- **Entry Delay Sound for Full Arm**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the entry delay time in the full 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. The 2 areas in the control panel have 60 User PIN Codes available for setting. Each consists of 4-6 digits (numeric number 0~9), no disallowed PIN code. User PIN code #1 is always activated factory default.

User PIN #1 in Area 1, 2

Password: **1234**



User Code Setting

- **User Code**: Enter the 4-digit code in the field.
- **Tag Number**: The number indicates the tag which is associated to the user code. By applying a tag to the tag sensor zone of Remote Keypad and clicking the **Load** button, the corresponding tag number will be loaded.
- **Area**: Select the area for setting User PIN Code.
- **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.

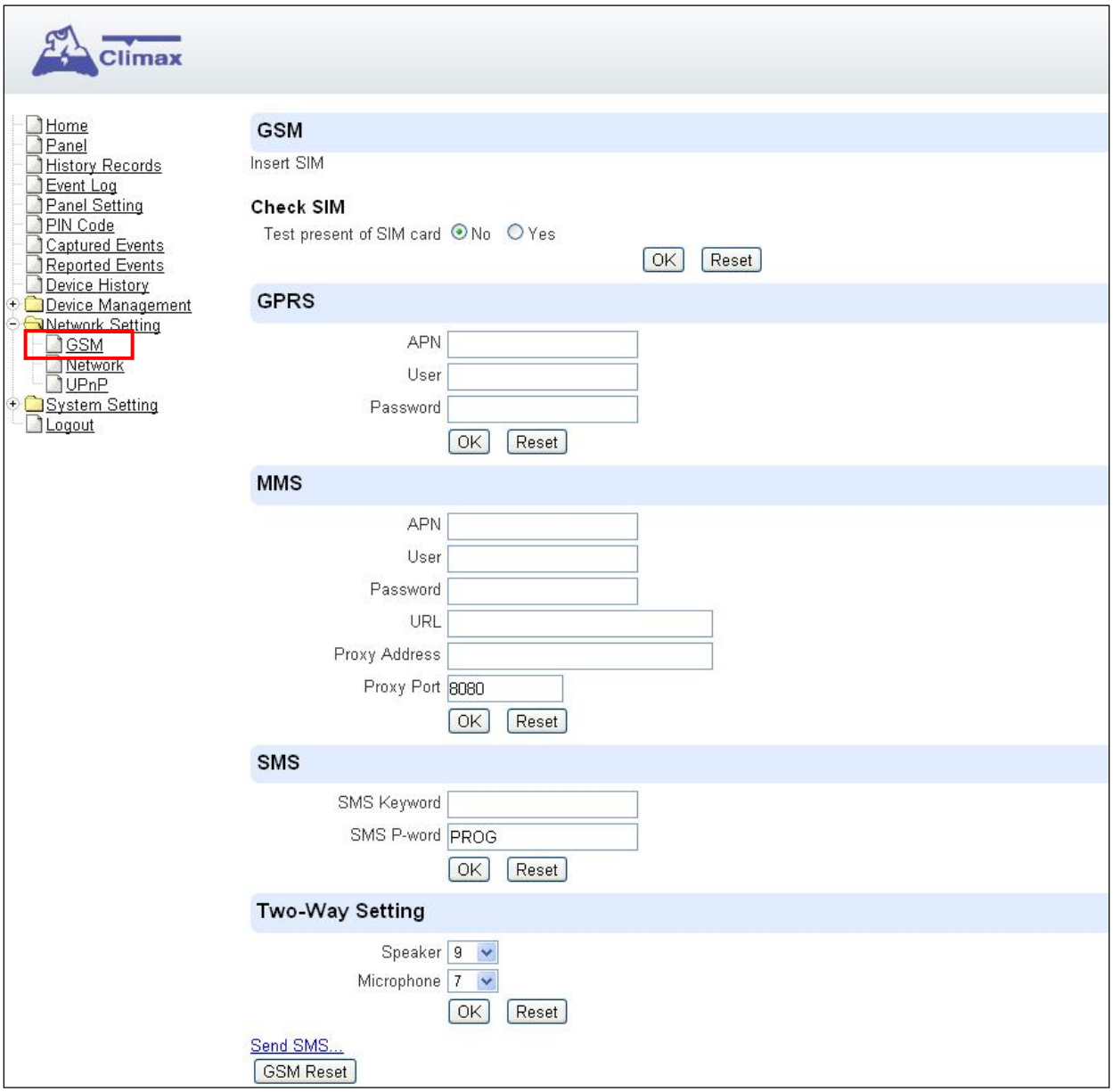
  ☐ Latch → **Latch Report OFF** = When the User PIN Code is used to change system mode, the panel will not report the event.

- **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 (HSGW-MAX8 only)



Check SIM

This is designed for the system to check the SIM card 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.***)

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 both Areas 1 & 2.

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**

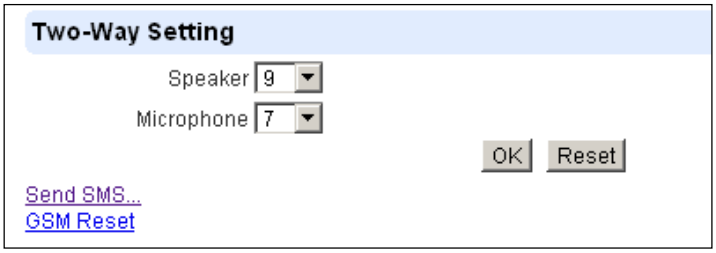
  For sending remote commands to system via SMS message, a personalized password is required for the Control Panel to recognize your authority.

- **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

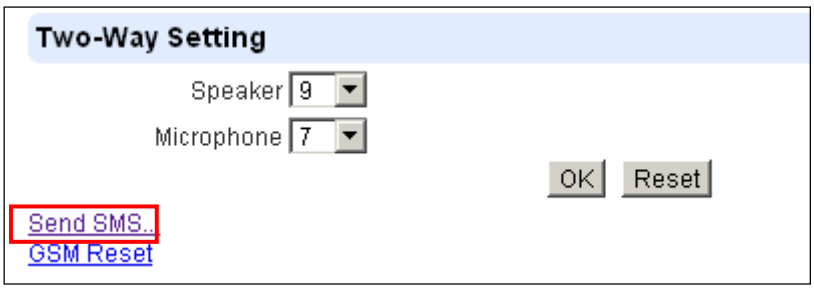
The two-way setting is designed to adjust speaker volume and microphone sensitivity on DECT device for two-way communication.



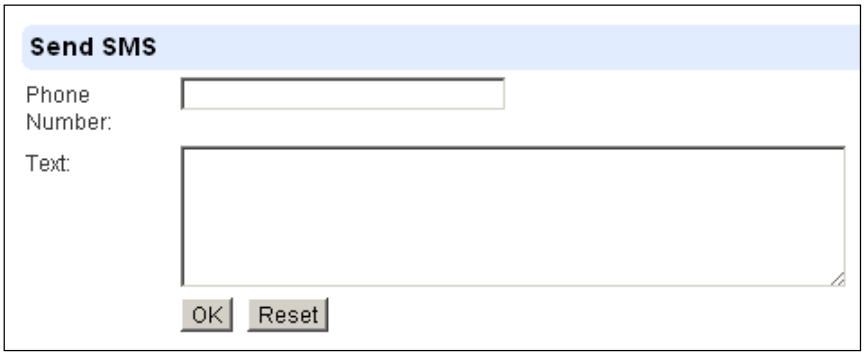
Send SMS Message

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

Step 1. Click **Send SMS**.



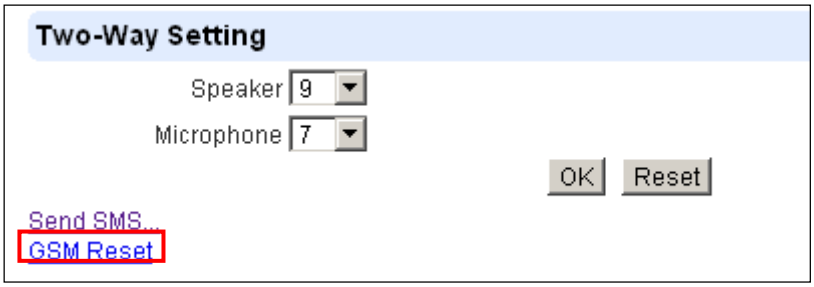
Step 2. Enter a desired phone number and text message.



Reset GSM

This feature is designed for you to reset GSM module.

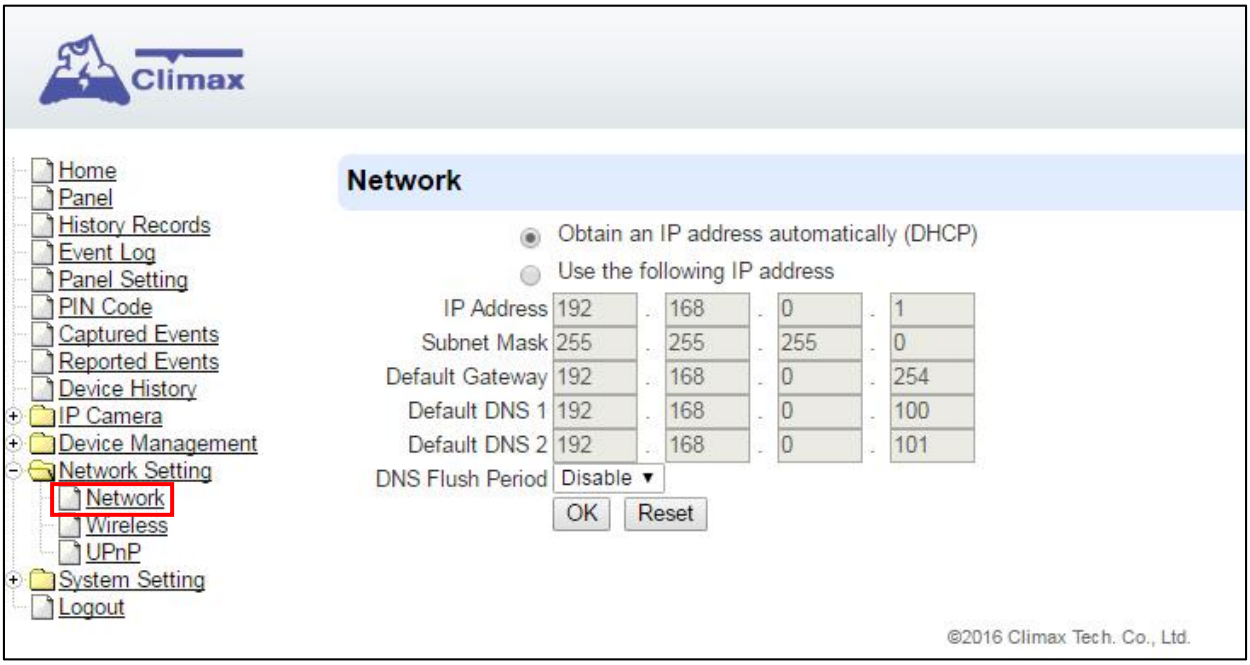
Step 1. Click **GSM Reset.**



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.



- **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.

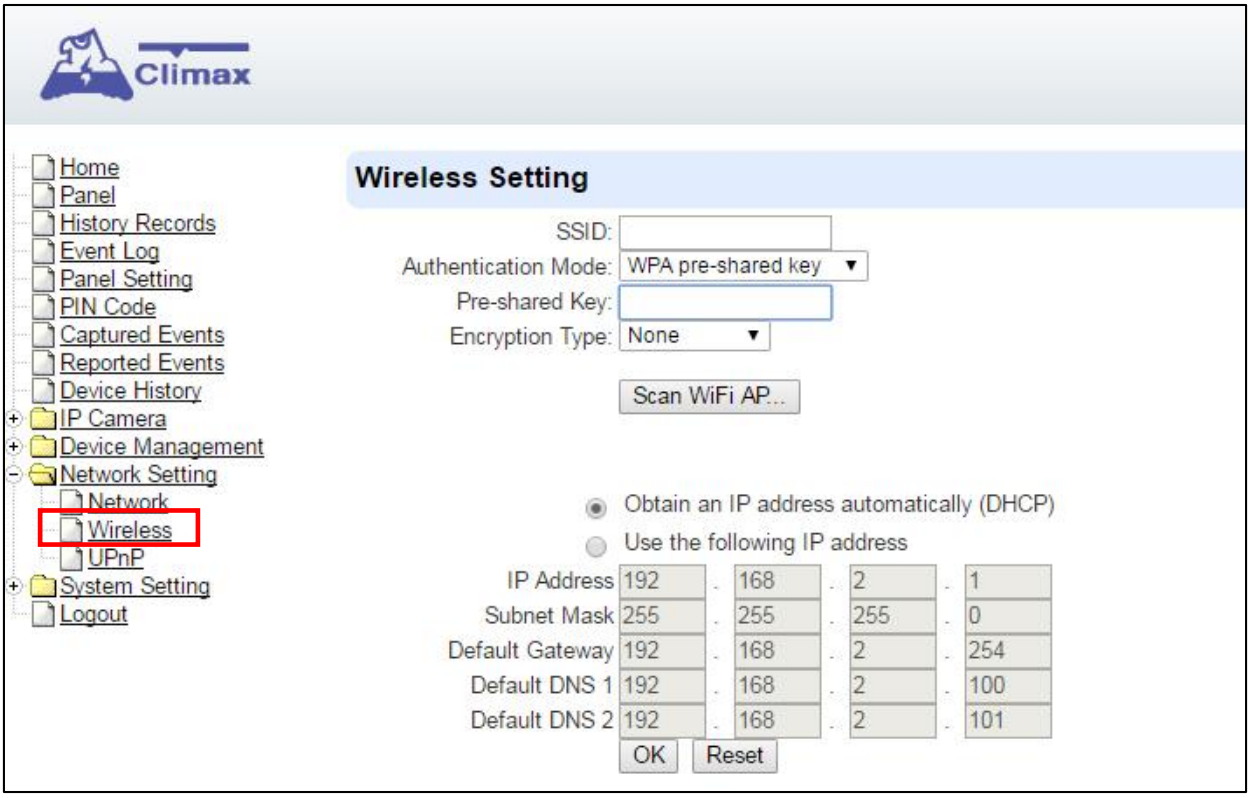
  Please make sure that you have obtained all required values according to your Network environment. Please contact your network administrator and/or internet service provider for more information.

- **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.

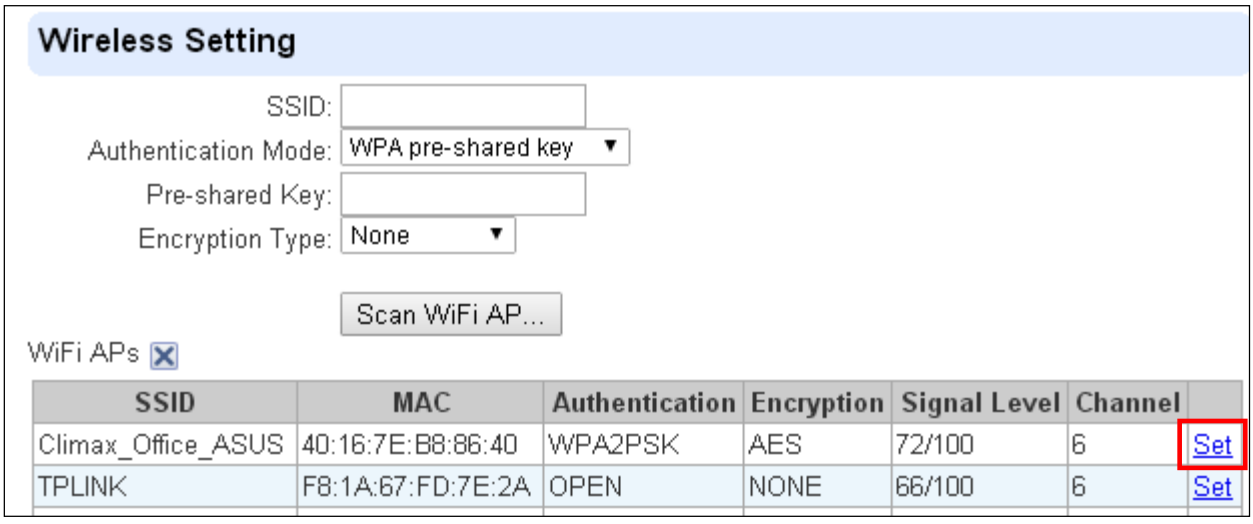
7.3. Wireless

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



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

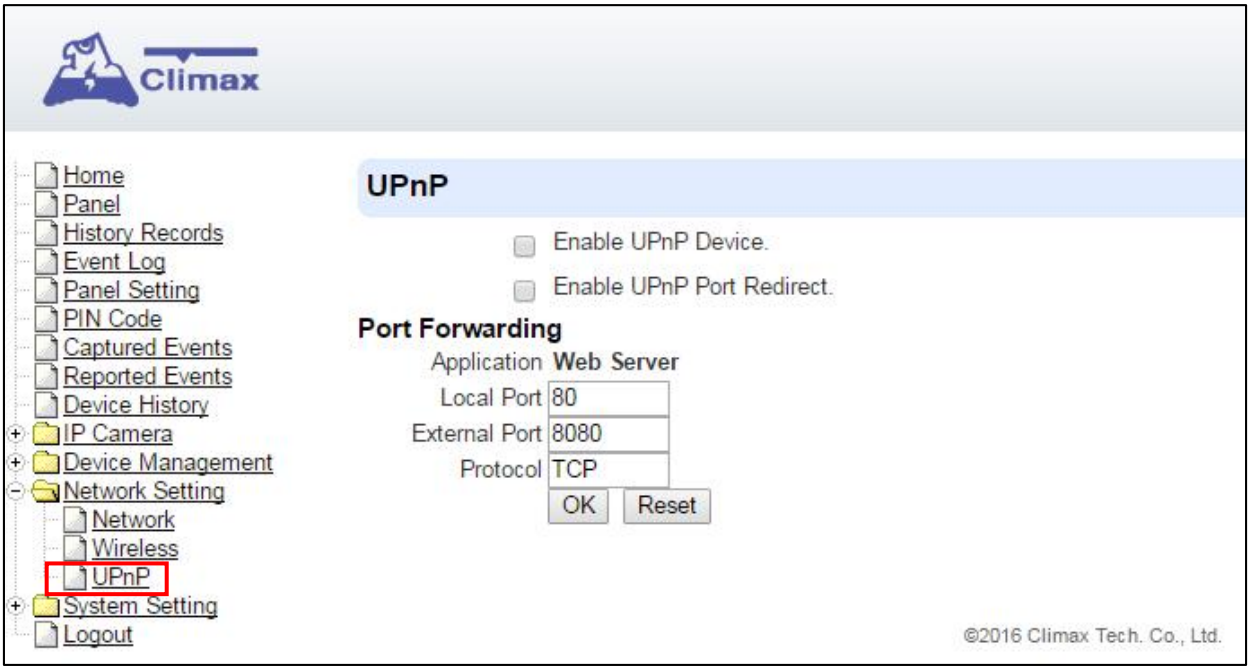
1. Search for WiFi AP: Click “**Scan WiFi AP**” to search for available wireless network Select the available Wireless APs from the list by clicking “**Set**” after AP info column and enter the required information (pre-shared key, etc.) and click the “**OK**” button.



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.



- **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.

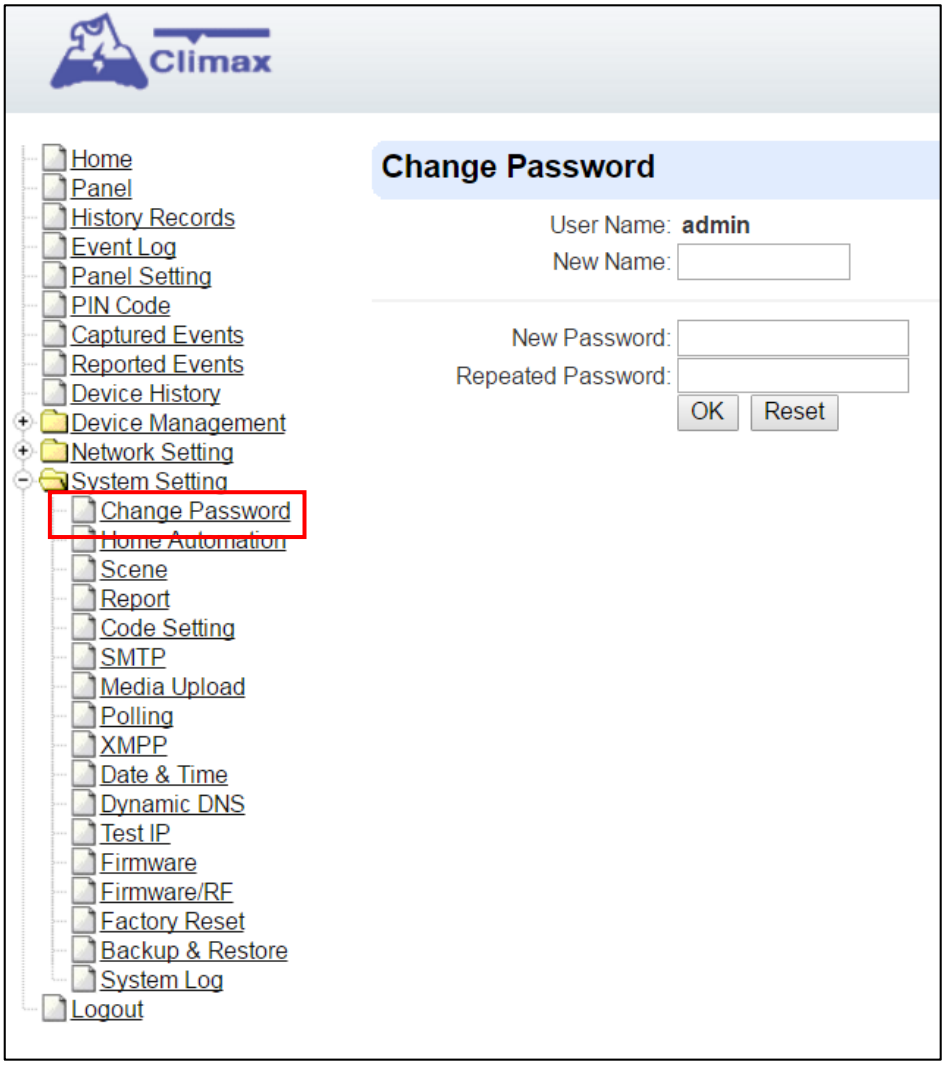
8. System Settings

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.



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.

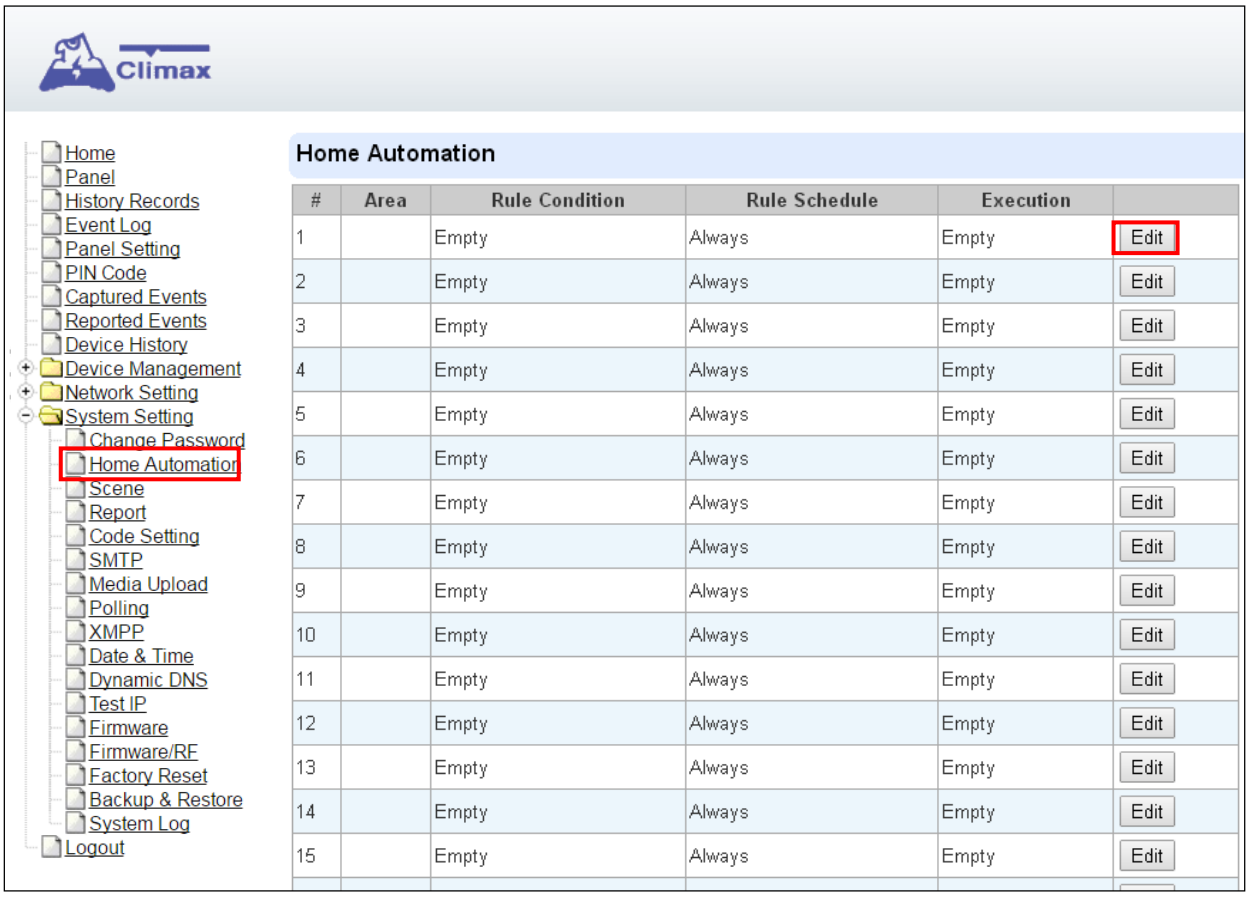
Step 1. Click on **Edit**.

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.



- **Area**

  Select an opeartion area.

- **Rule Condition**

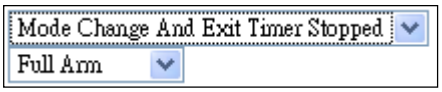
  The rule condition determines under which circumstances the rule should be activated.

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

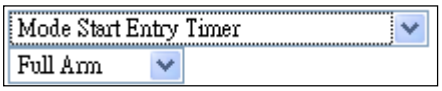
  ☞ ***Trigger Alarm*** : When set as **Trigger Alarm**, if the specified alarm event (Burglar/Some/Medical/Water/Silent Panic/Panic/Emergency/Fire /CO Alarm) is triggered, the rule will be activated according to rule schedule and execution setting.

  ☞ ***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 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.



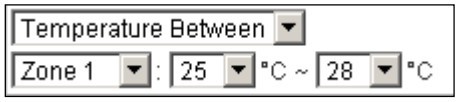
☞ ***Mode Start Entry Timer*** : When set as **Mode Start Entry Timer**, when the system begins to countdown Entry Delay, the rule will be activated according to rule schedule and execution setting.



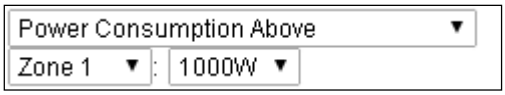
☞ ***Temperature Below*** : When set as **Temperature Below**, if the temperature detected by specified temperature sensor drops below set threshold, the rule will be activated according to rule schedule and execution setting.

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

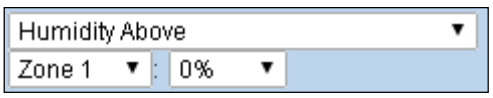
☞ ***Temperature Between*** : When set as **Temperature Between**, if the temperature detected by specified temperature sensor falls within the range specified, the rule will be activated according to rule schedule and execution setting.



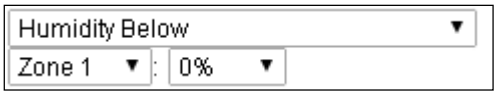
☞ ***High Power Consumption*** : When set as **Power Consumption Above**, if the power output watt from a specific Power Switch exceeds, the rule will be activated according to rule schedule and execution setting.



☞ ***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.



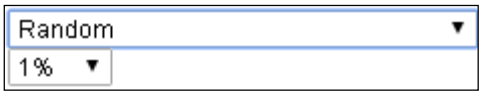
☞ ***Humidity Below*** : When set as **Humidity Below**,if the humidity reading from specified room sensor falls below the level specified, the rule will be activated according to rule schedule and execution setting.



☞ ***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**

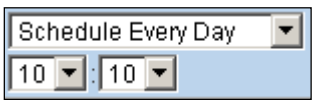
☞ ***Always*** : When set as **Always**, the rule can be activated anytime.

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

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

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

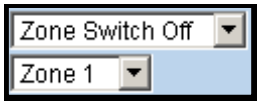
☞ ***Schedule Every Day*** : When set as **Schedule Every Day**, the system will follow the the rule condition and execute rule according to time specified every day



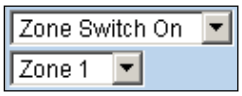
- **Execution**

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

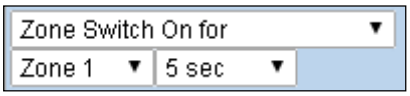
☞ ***Zone Switch Off:*** Turn on the Power Switch at specified zone.



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



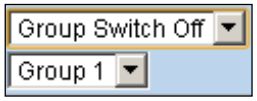
☞ ***Zone Swich On For*** : Turn on the Power Switch at specified zone for a set duration.



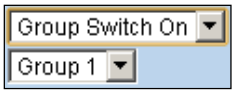
☞ ***Zone Switch Level:***: Change the power output level for Dimmer at specified zone.

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

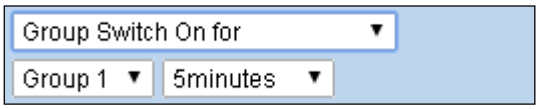
☞ ***Group Switch Off*** : Turn off all Power Switches assigned to specified group.



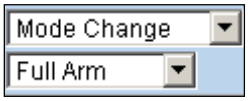
☞ ***Group Switch On*** : Turn on all Power Switches assigned to specified group.



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

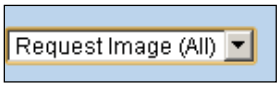


☞ ***Mode Change*** : The system will change to the mode as you specified.

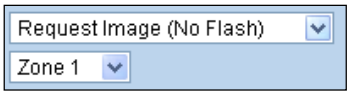


☞ ***Request Image*** : The PIR Camera in specified zone will take a picture.

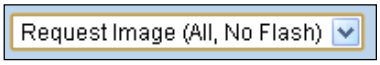
☞ ***Request Image (All)*** : All PIR Cameras in the system will take a picture.



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



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

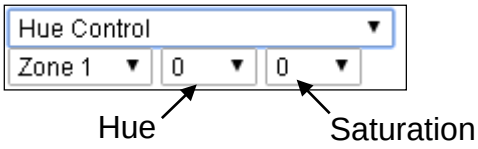


☞ ***Request Video*** : The PIR Video Camera or IP Camera in specified zone will record a video.

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

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

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

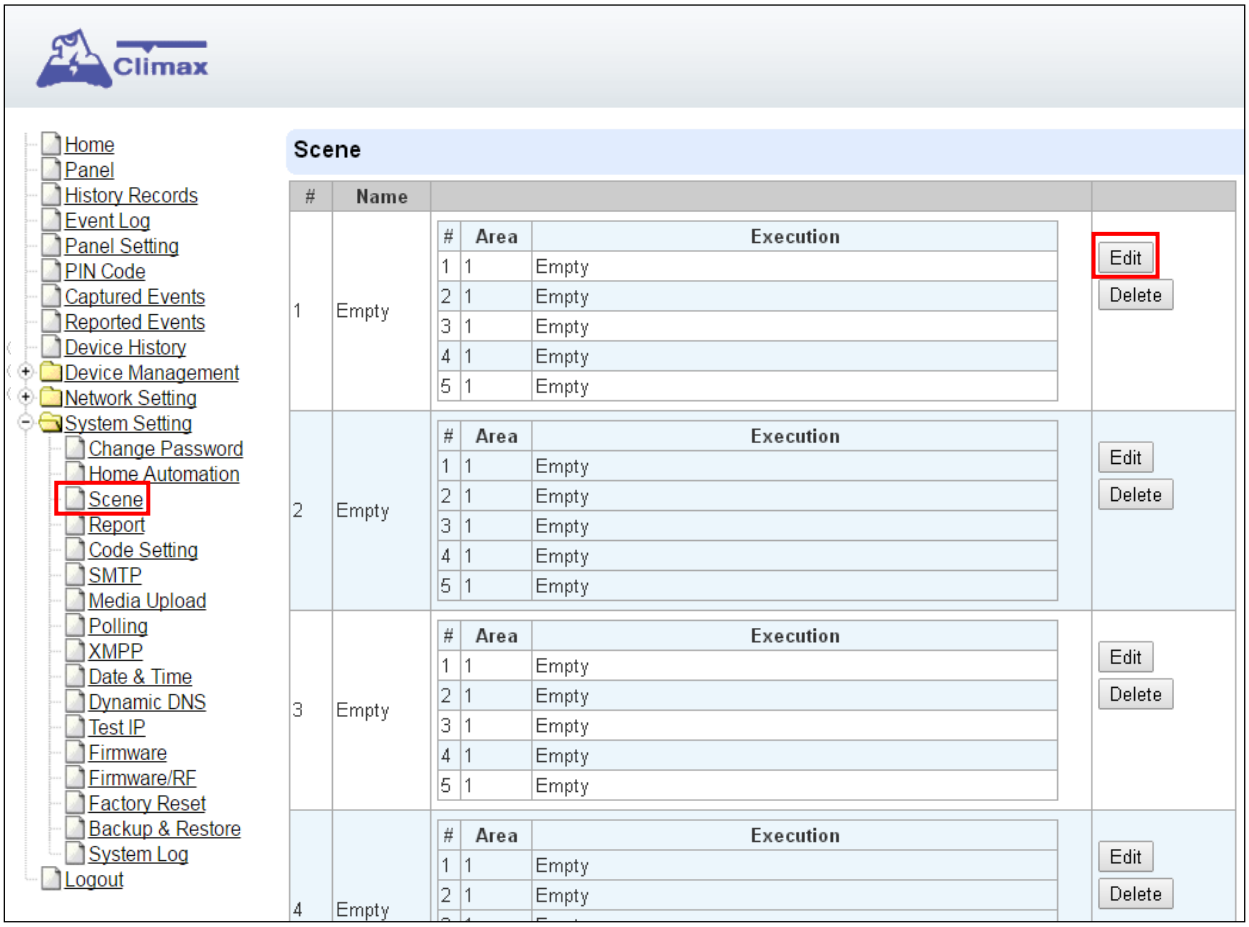


☞ ***Trigger Alarm:*** Choose to activate one of the following alarms: High Temperature Alarm, Low Temperature Alarm, High Power Consumption Alarm, High Humidity Alarm and Low Humidity Alarm

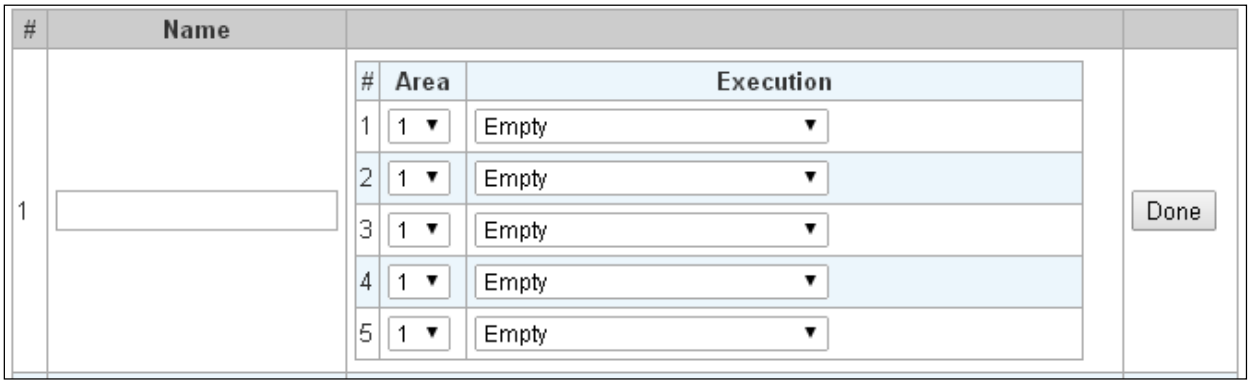
☞ ***Apply Scene:***: the system will execute preprogrammed Scene number. Please refer to **8.3. Scene** for detail.

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**l), 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.



Step 1. Click on **Edit**.



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.

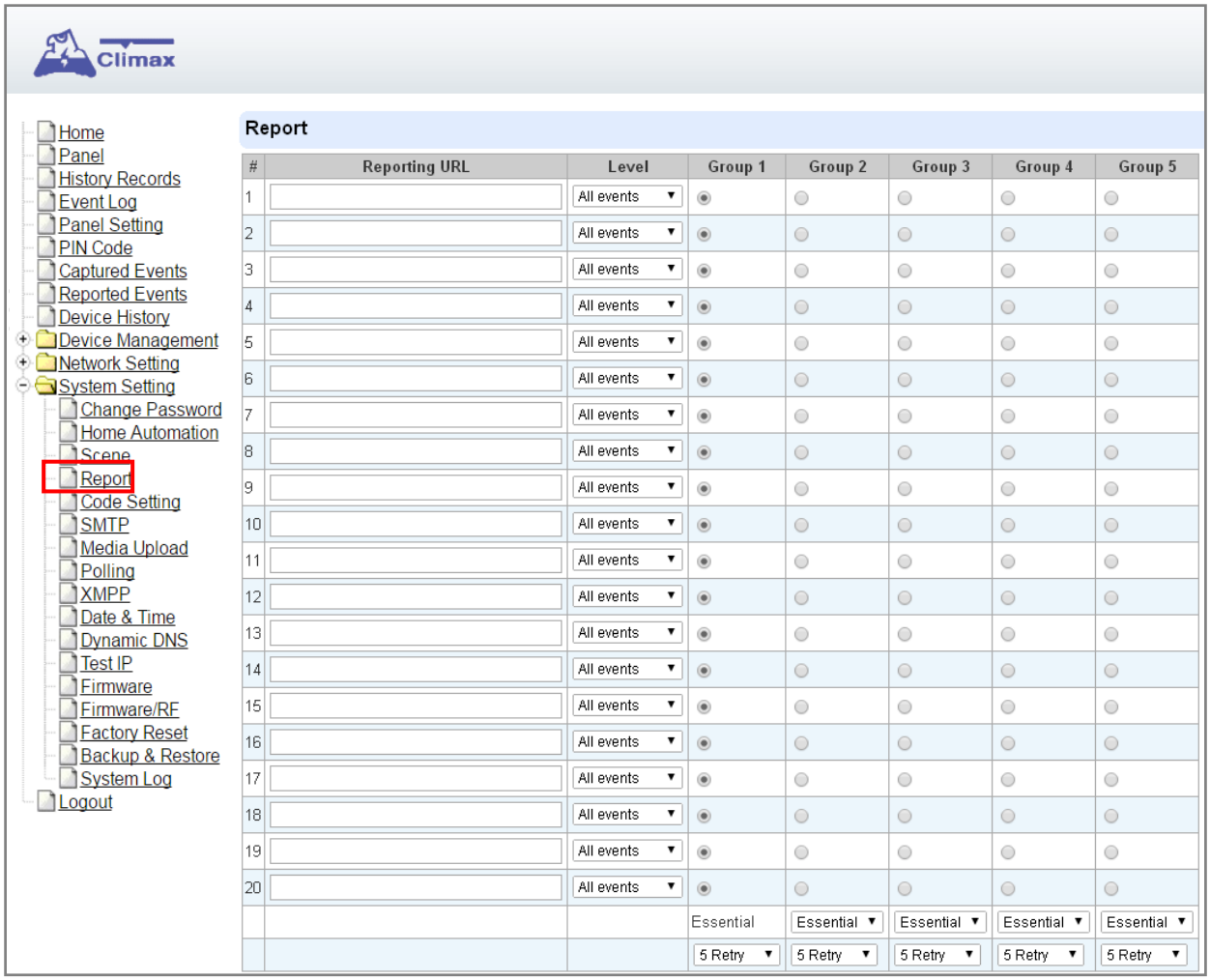
Step 5. Repeat Step 2-3 to setup the execution you wanted. As many as 5 executions can be included in one scene.

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.



- **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.

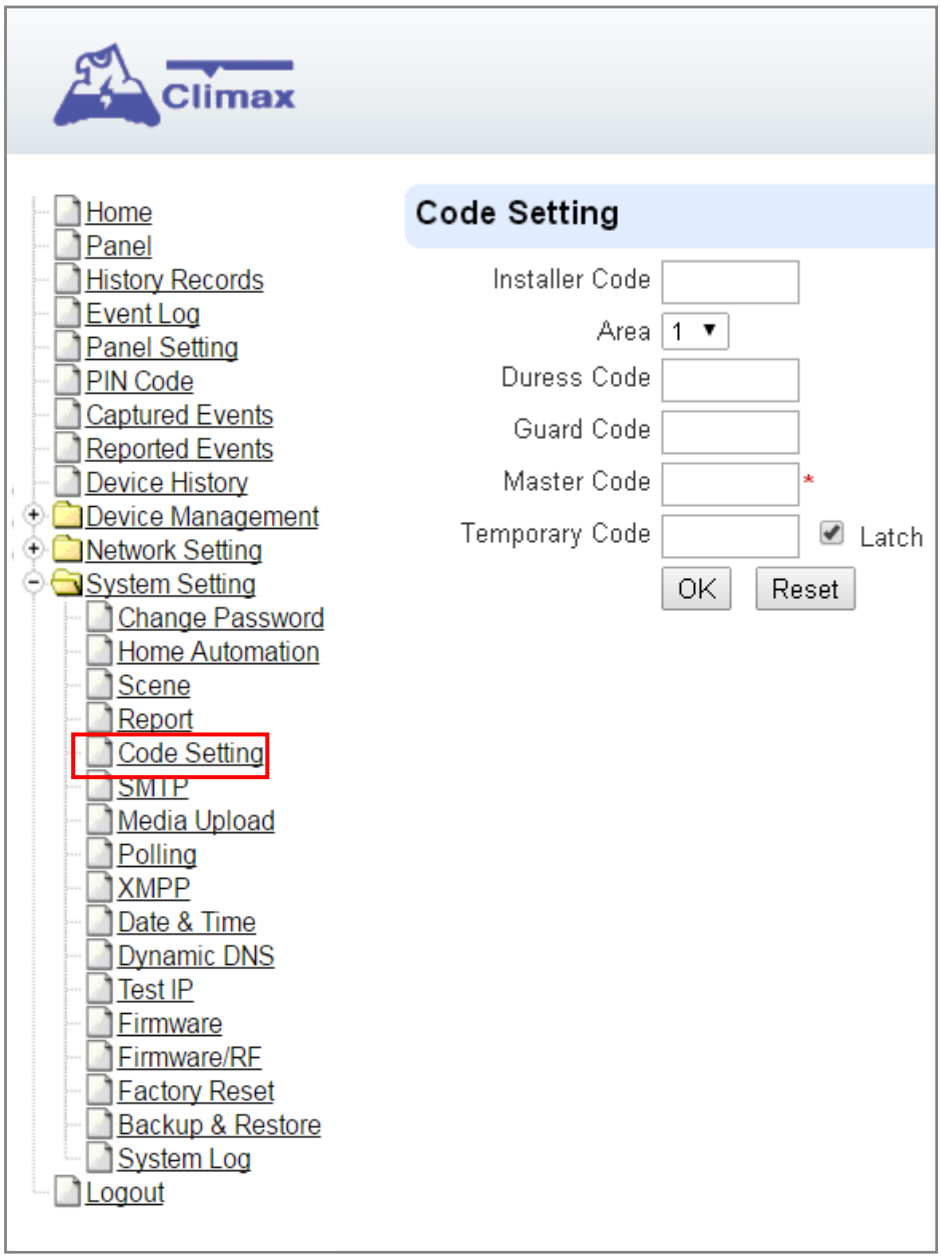
<NOTE>

- ☞ 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**.



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.

- **Master Code**

  This function is currently disabled.

- **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.

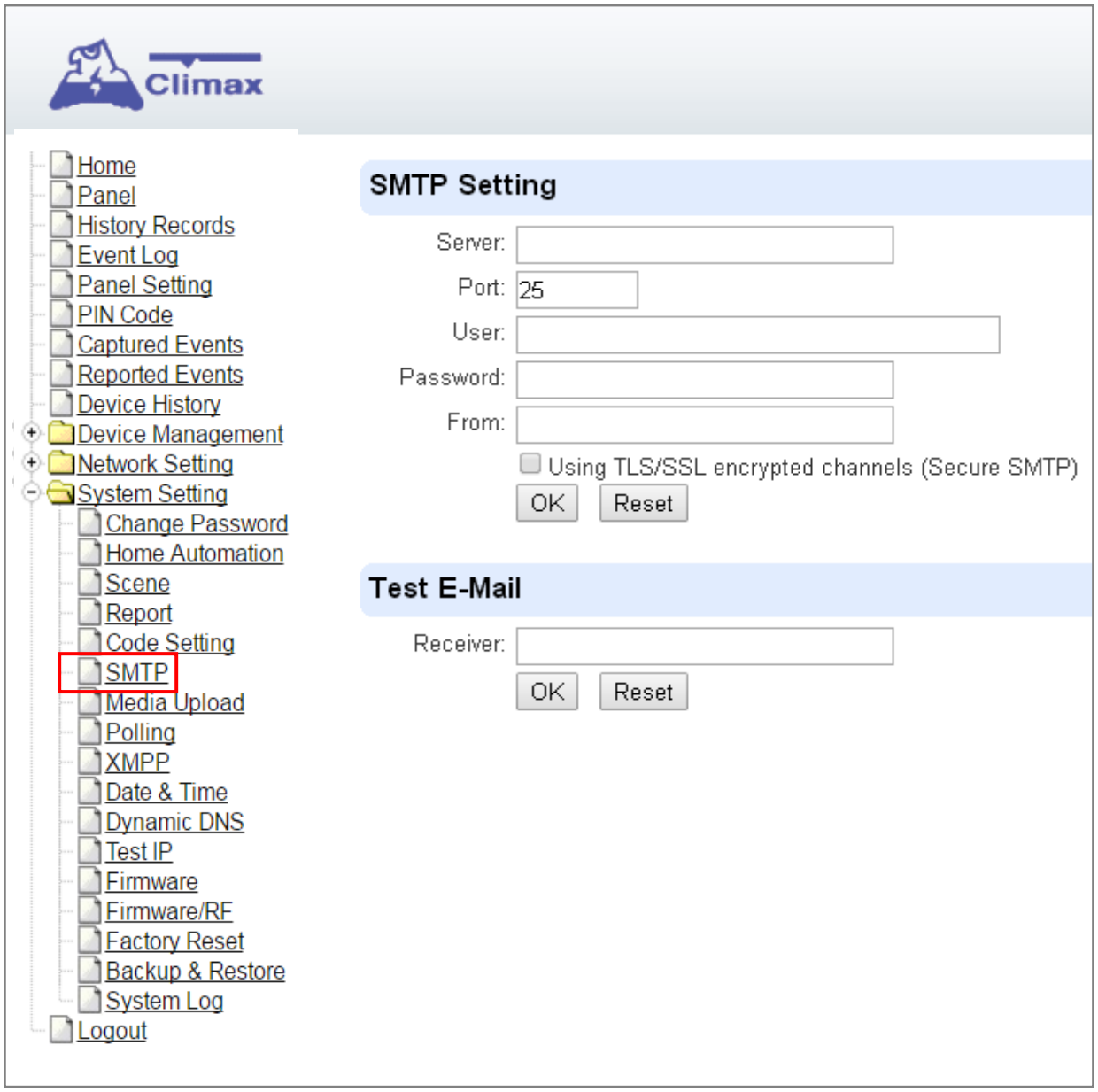
  ☐ Latch → **Latch Reprot OFF** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will NOT transmit reporting(s) to notify the Central Monitoring Station.

- **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.



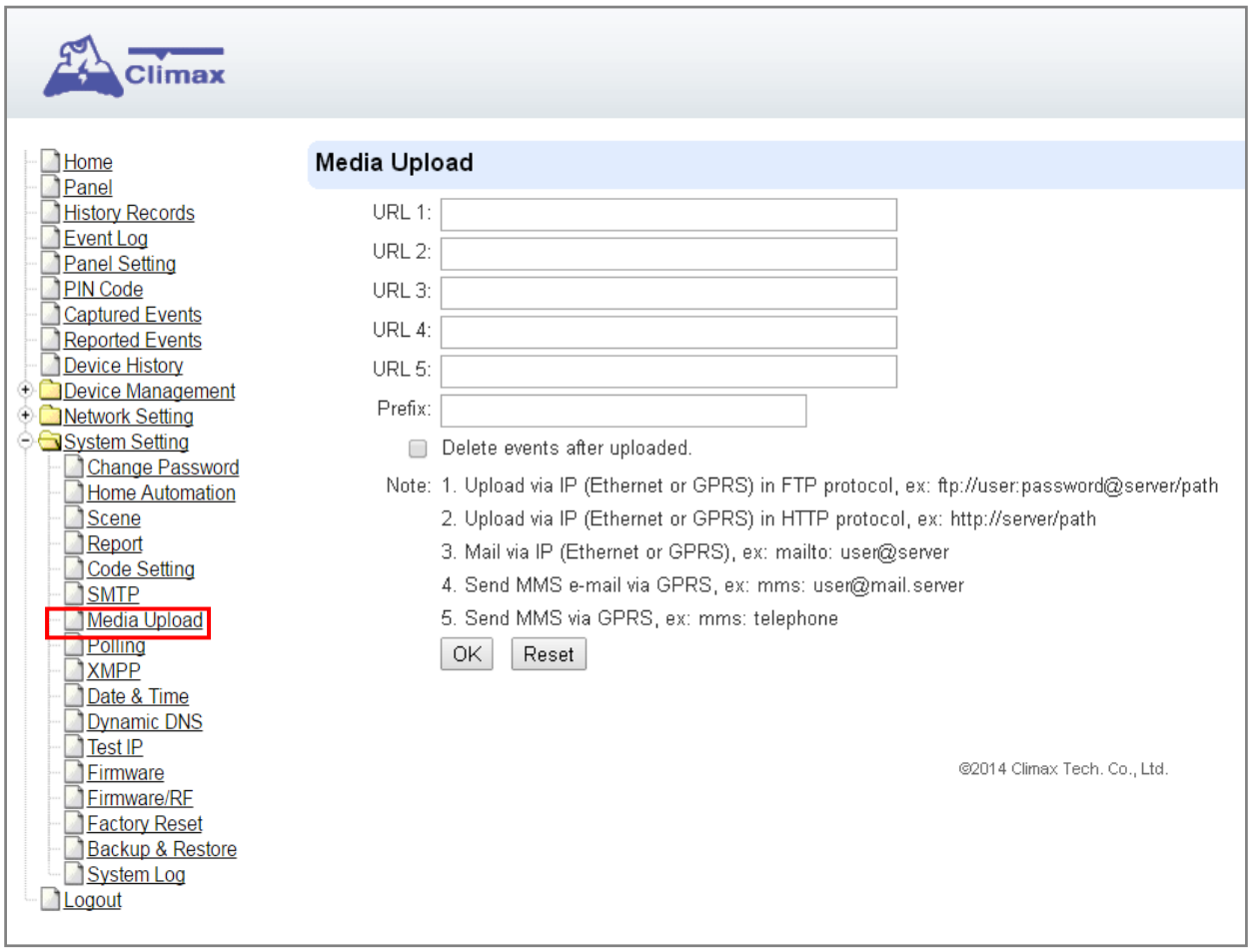
Step 1. Enter the following settings:

- **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.



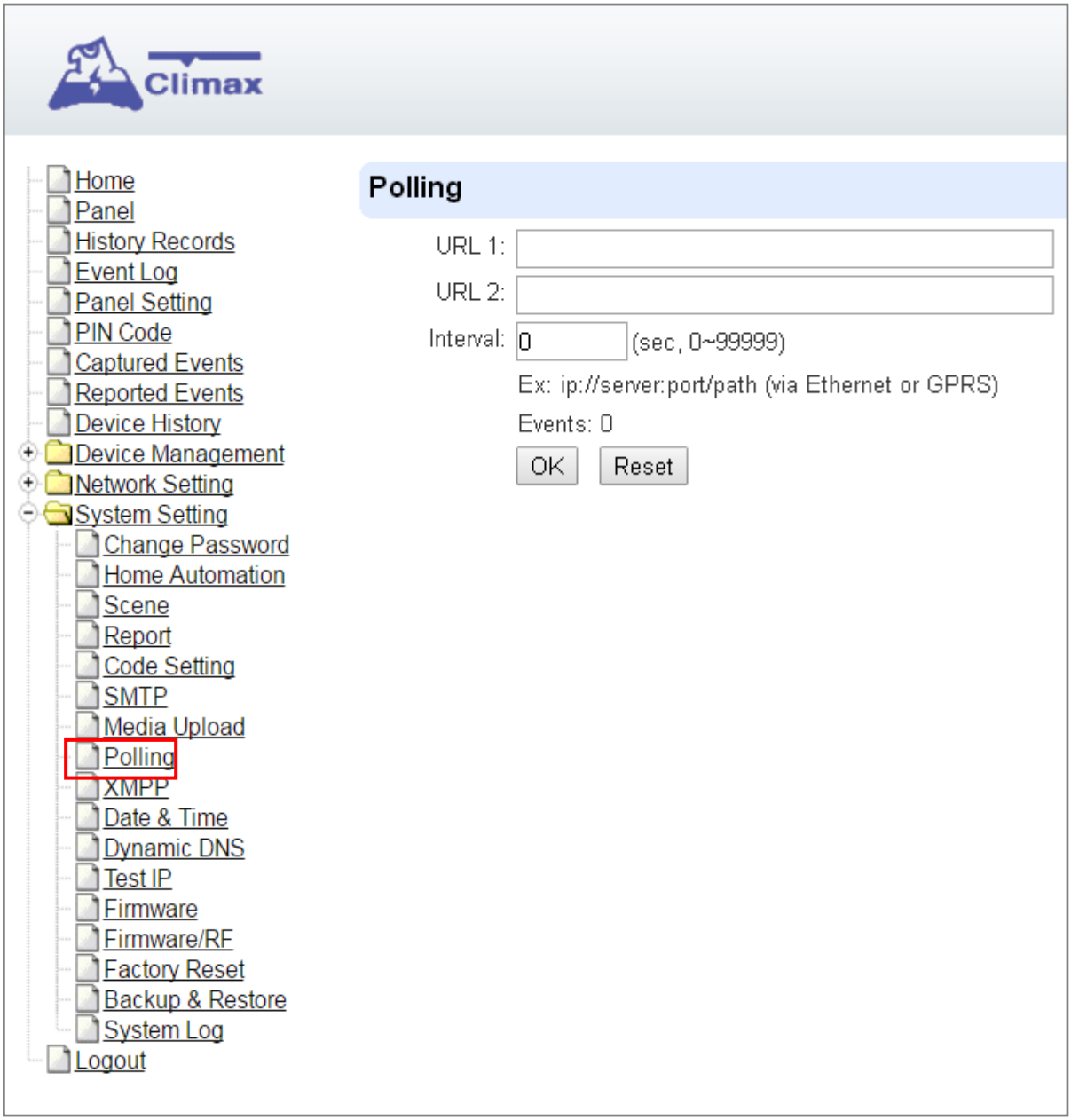
- **FTP:** ftp://user.password@server/path
- **HTTP:** http://ip:port/path
- **Email**: mailto:user@server (transmitting an alarm image over Ethernet)
- **Manitou**: manitou://user@server:port
- **MMS via Telephone**: mms: telephone number
- **MMS via GPRS**: mms: user@mail.server (transmitting an alarm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

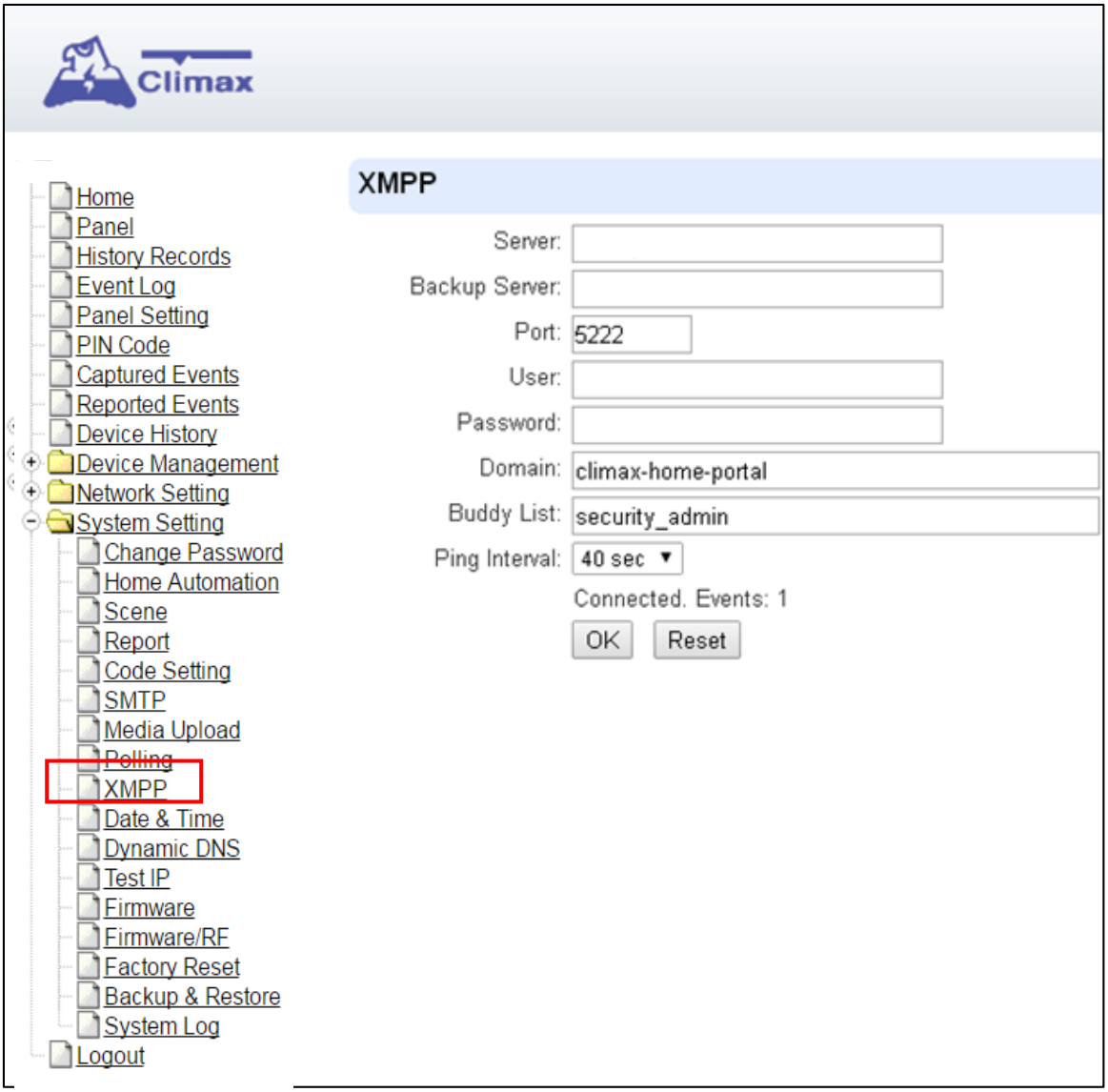
The polling function enables the Control Panel to query the destiation you set (URL1 or URL2) in turn as to whether it has any data to transmit.



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

8.9. XMPP

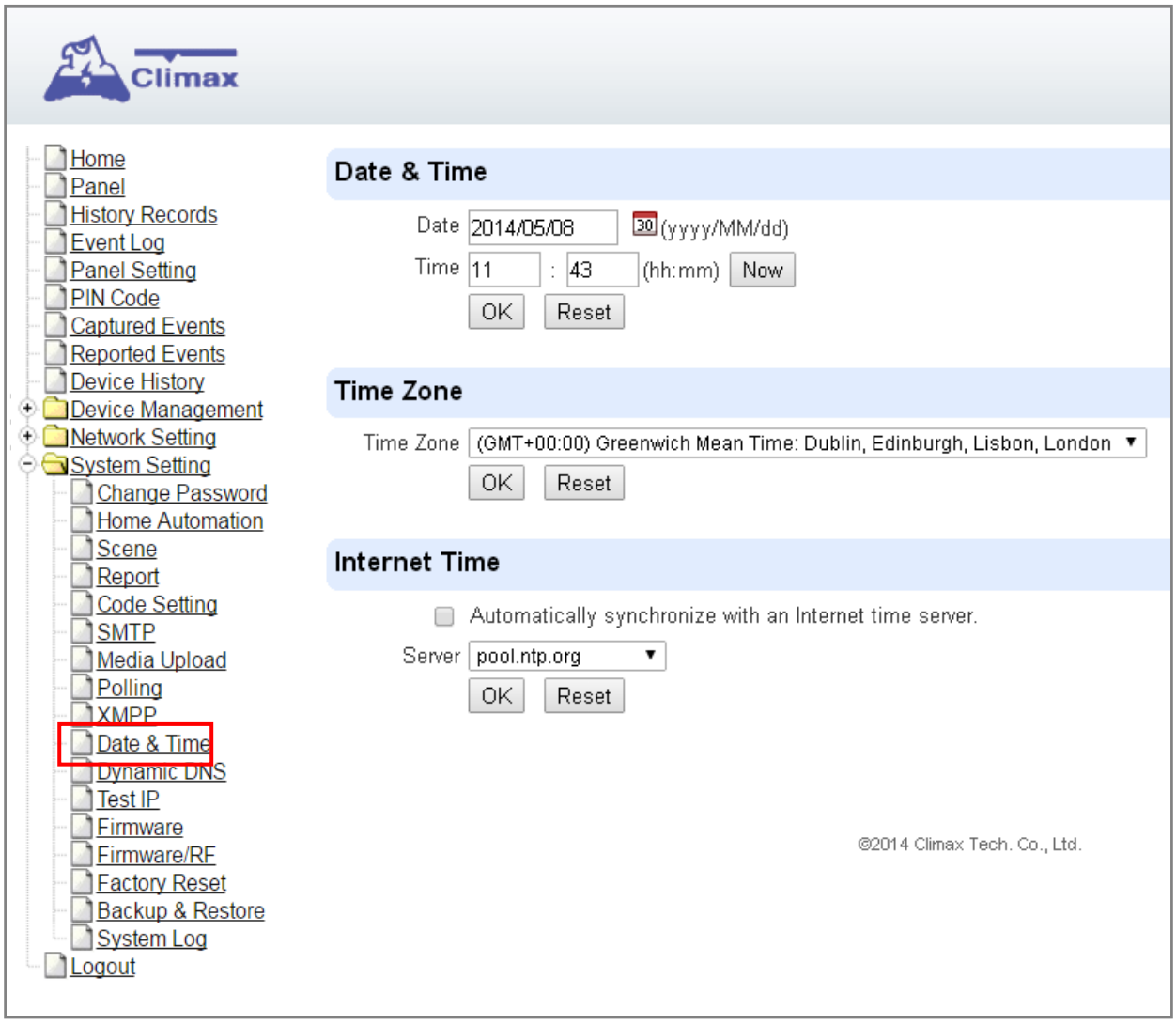
XMPP setting enables the Control Panel to query the set destination. This setting is required for the Control Panel to connect to Climax's Home Portal Server for remote control. If the panel is disconnected from the server, it will retry connection every 3 minutes.



- **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

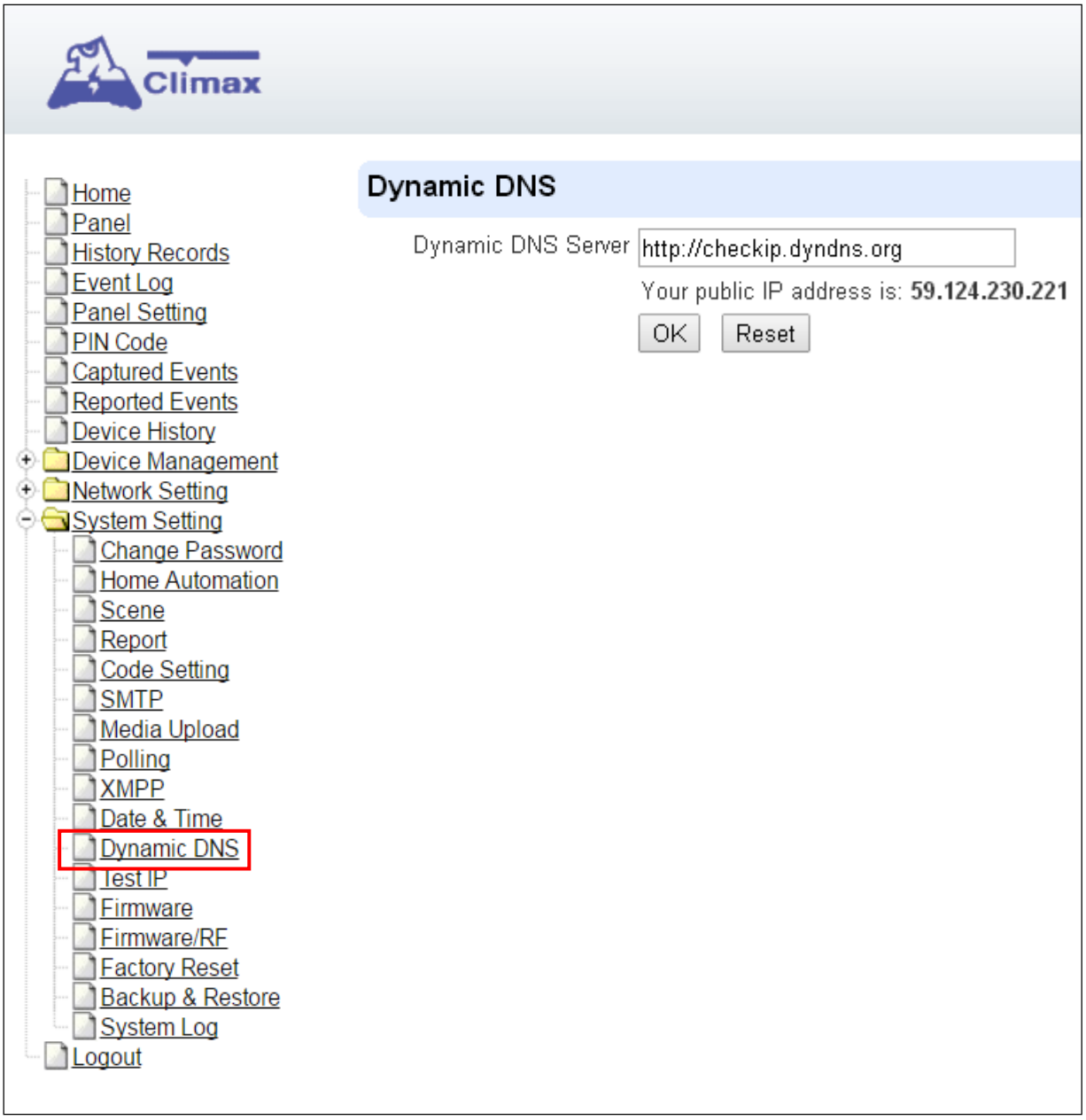
Program the current **Date** & **Time** and set automatic synchronization with internet time server.



- **Date & Time:** 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

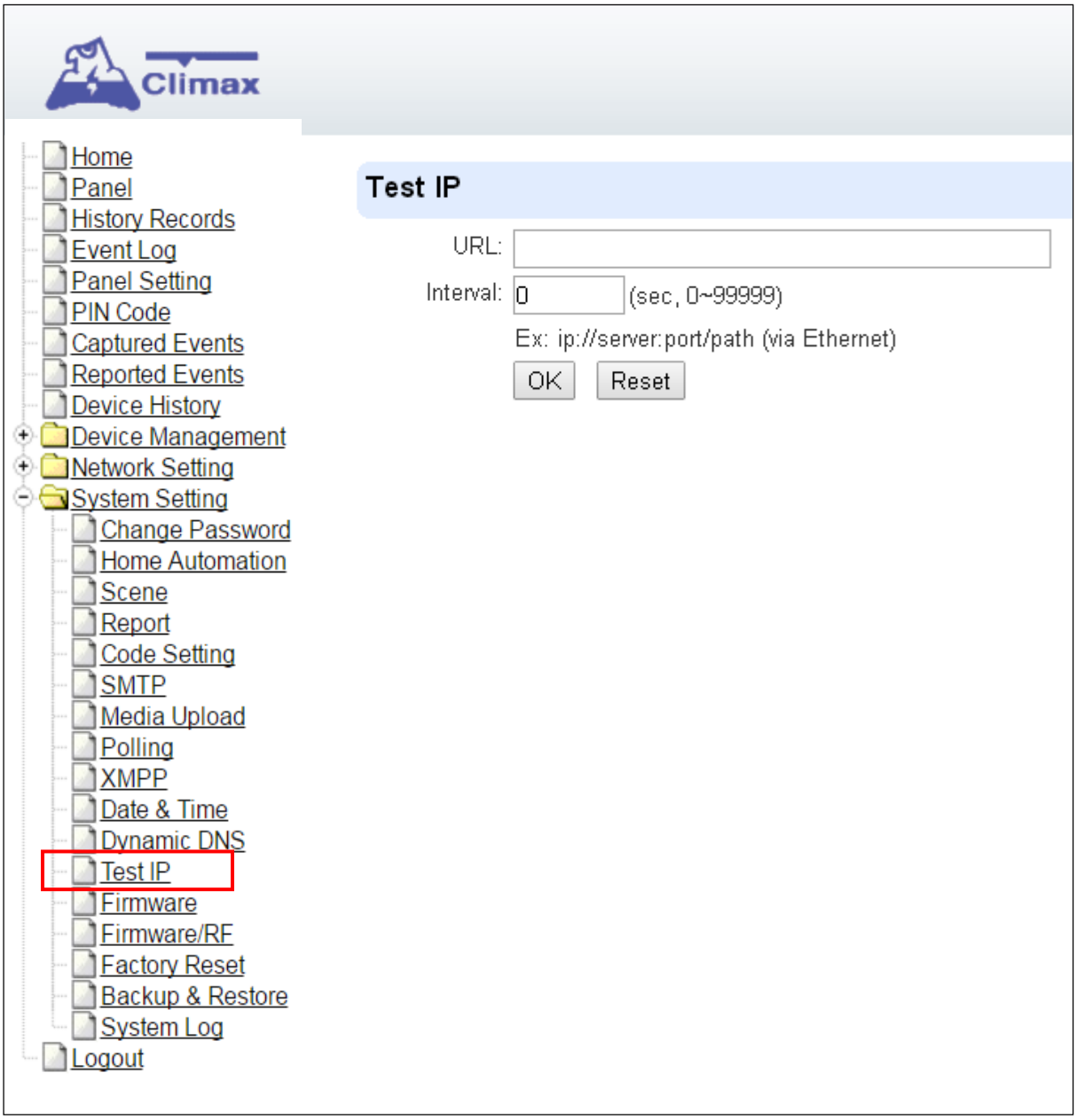
This page is used to provide you the Control Panel's current public IP address.



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

8.12. Test IP

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



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

Step 2. Enter the test interval.

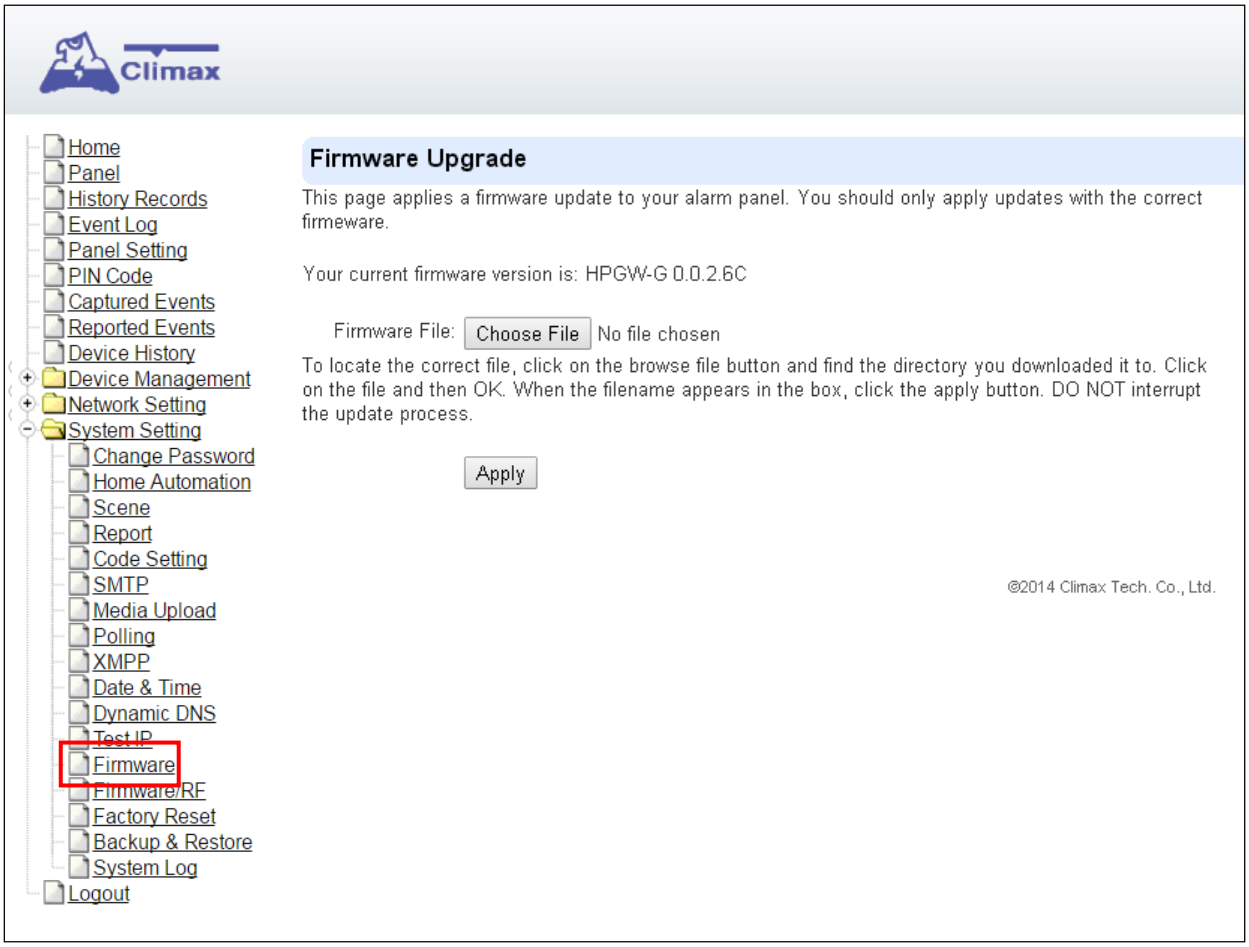
Step 3. Click “OK”

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 "**Browse**" and locate the latest firmware file ("**unzipped image.bin**" file) in your PC.



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

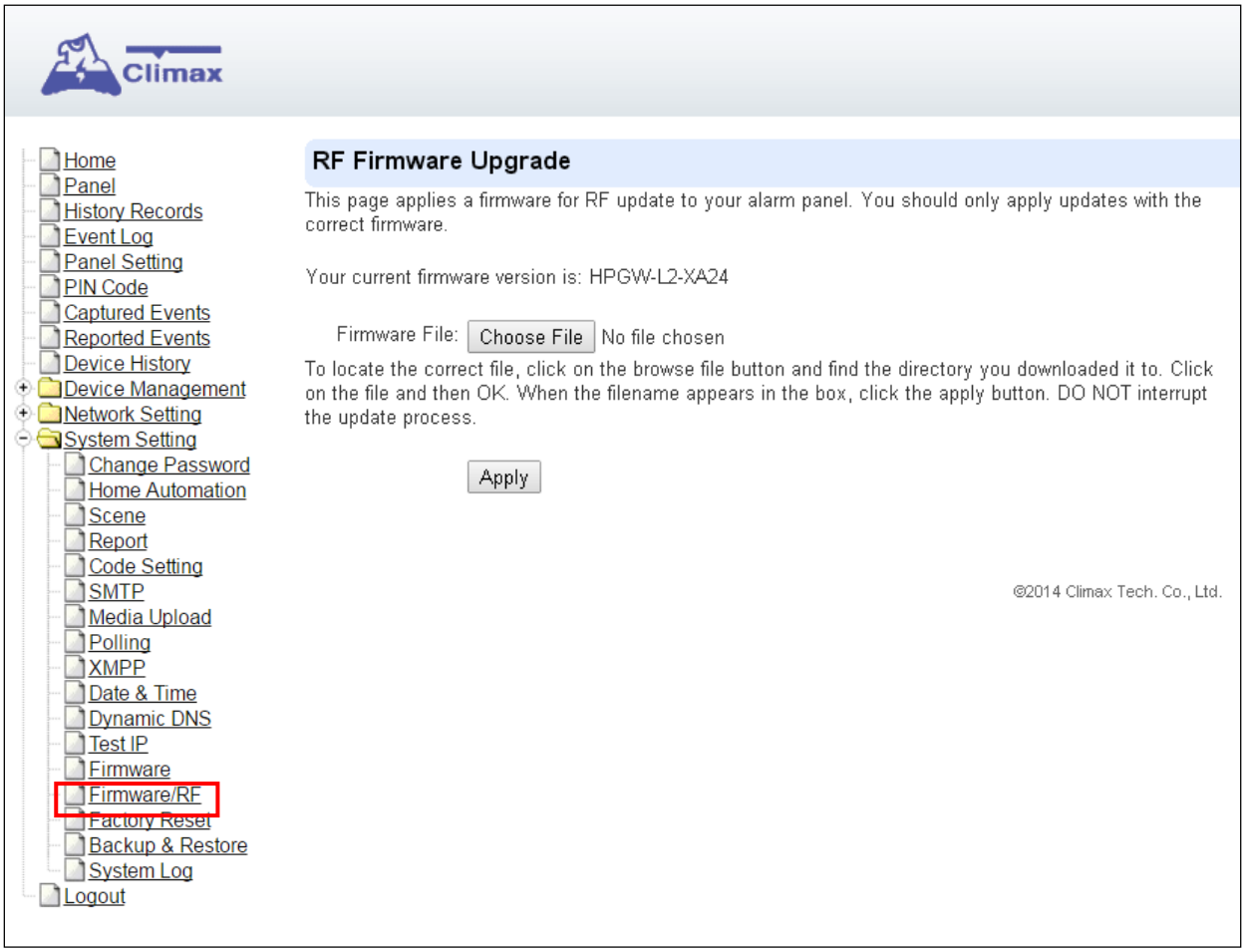
Step 3. Wait for 1 min and do NOT power off during this time.

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 "**Browse**" and locate the latest firmware file ("**unzipped image.bin**" file) in your PC.



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. 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.

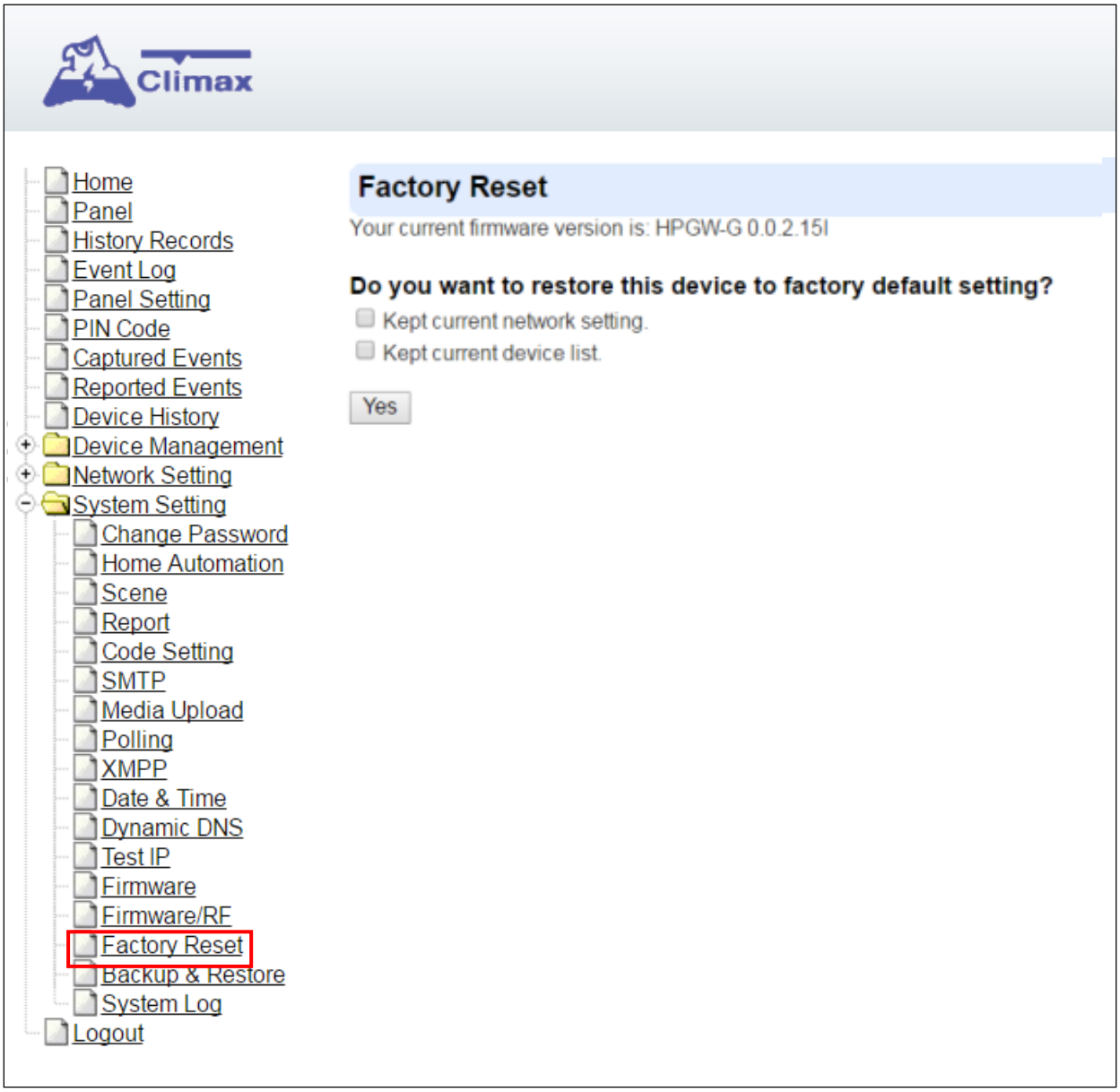
Remote Reset

Step 1. Tick the **Kept current network setting** or **Kept current device list** box 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.



Local Reset

Step 1. Disconnect the AC adaptor, slide battery switch to OFF.

Step 2. Press and hold the reset button and connect the AC adaptor to the Control Panel. DO NOT release the button yet.

Step 3. Keep holding the reset button for about 45 seconds then release until you hear one long beep. The 3 LEDs will flash 3 times.

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

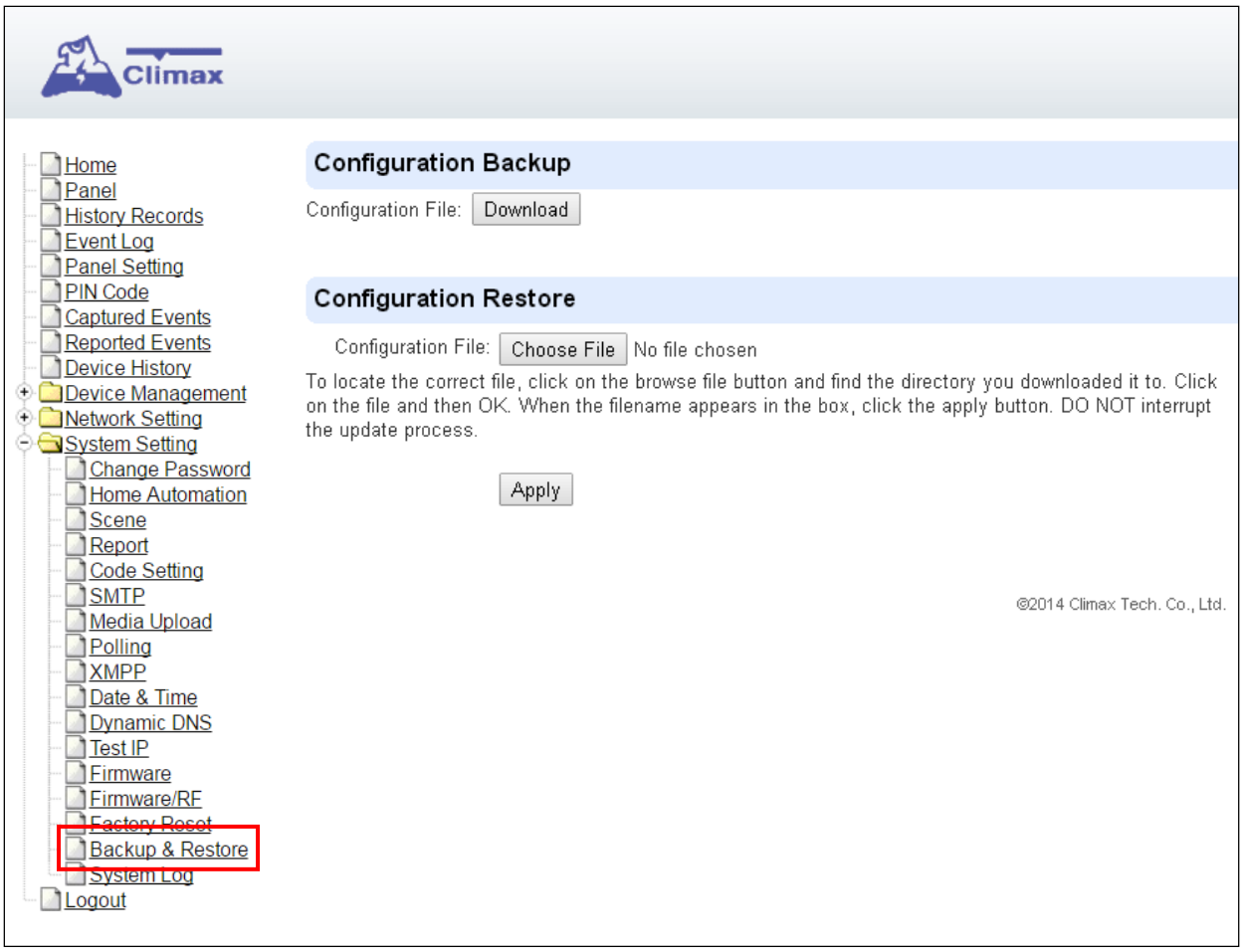
8.16. Backup & Restore

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

8.16.1 Backup Data

Yan can backup all programmed data and save these programmed values into a file.

Step 1. Click **Download configuration file**.



Step 2. Click **Download configuration file**.

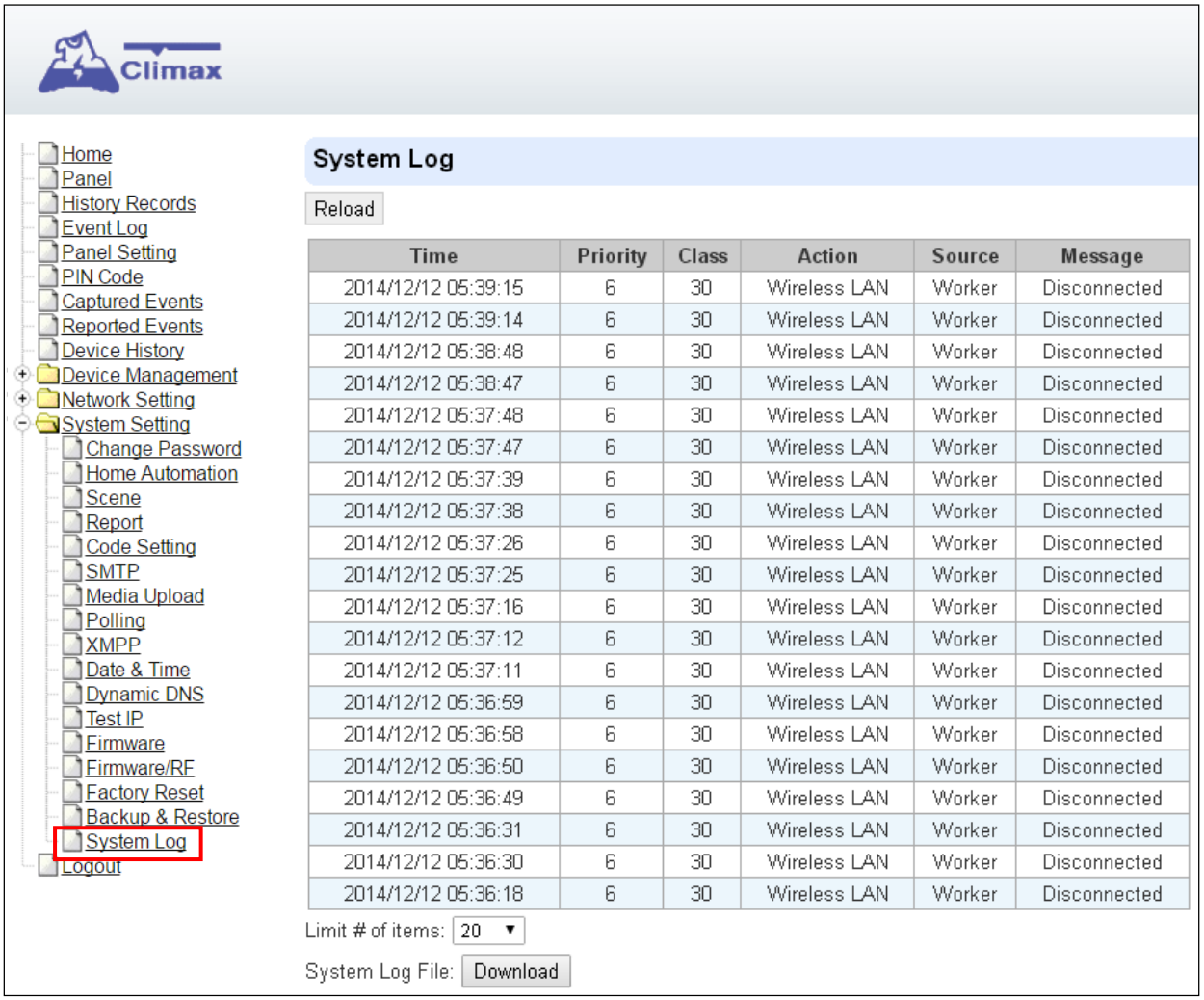
8.16.2 Restore Settings

Step 1. Click **Browse**, select a saved file.

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

8.17. System Log

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



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

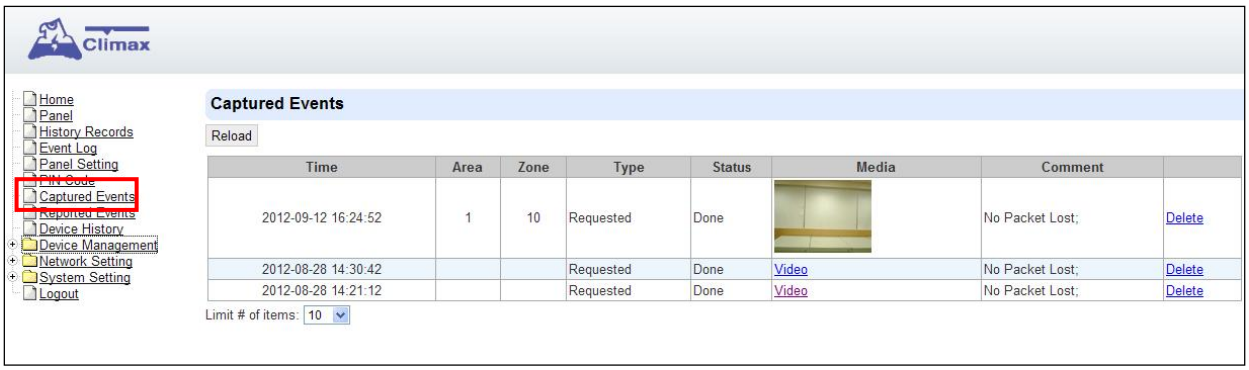
9. Event & History

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.

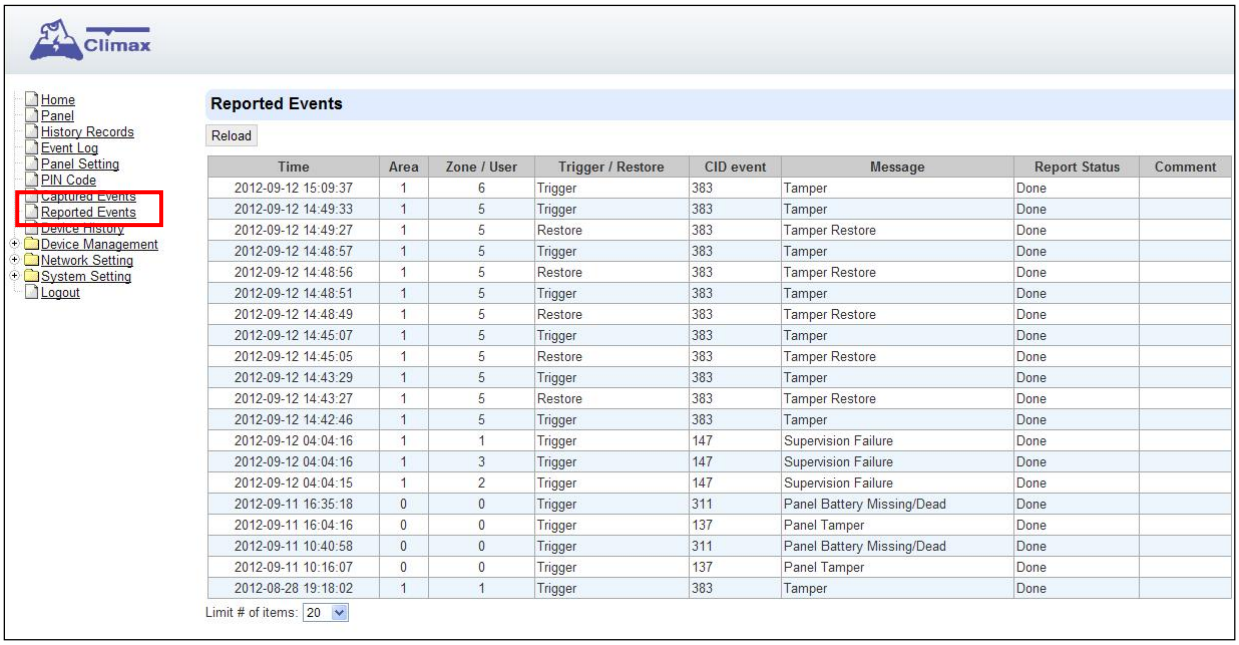
Caputred events will be displayed in this page with their information for you to view. Simply click on the picture or video to view them. You can also click **Delete** to delete the event.



- **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.

9.2. Reported Events

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



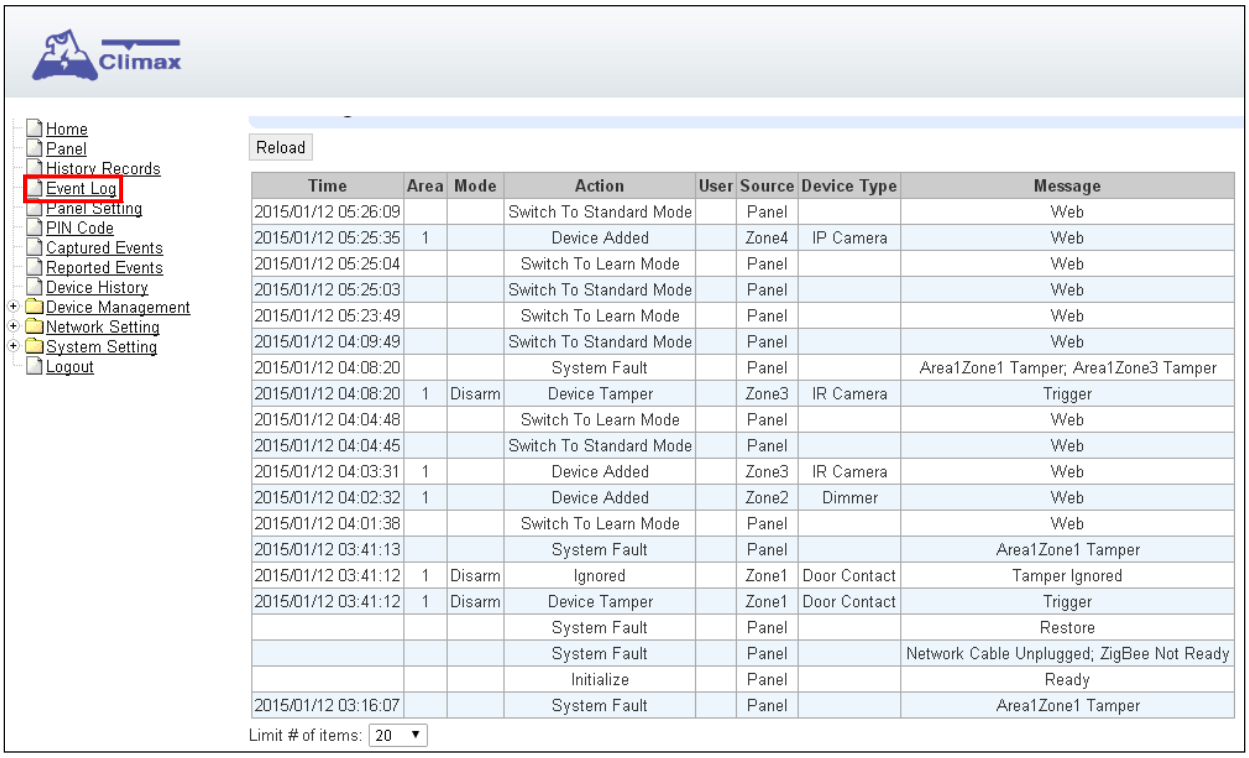
Time	Area	Zone / User	Trigger / Restore	CID event	Message	Report Status	Comment
2012-09-12 15:09:37	1	6	Trigger	383	Tamper	Done	
2012-09-12 14:49:33	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:49:27	1	5	Restore	383	Tamper Restore	Done	
2012-09-12 14:48:57	1	5	Trigger	383	Tamper	Done	
2012-09-12 14:48:56	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.

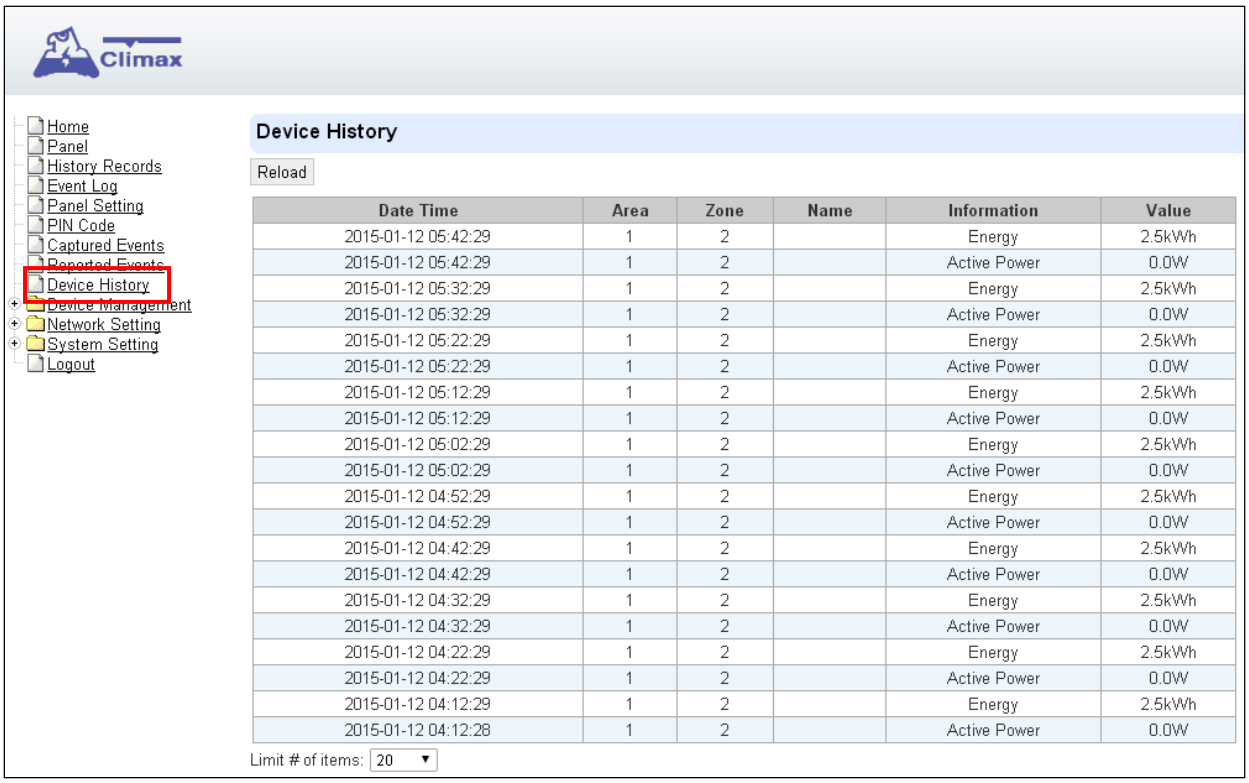


Time	Area	Mode	Action	User	Source	Device Type	Message
2015/01/12 05:26:09			Switch To Standard Mode		Panel		Web
2015/01/12 05:25:35	1		Device Added		Zone4	IP Camera	Web
2015/01/12 05:25:04			Switch To Learn Mode		Panel		Web
2015/01/12 05:25:03			Switch To Standard Mode		Panel		Web
2015/01/12 05:23:49			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

- **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**).



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

- **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/Z-wave/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 Alarm	Instant Smoke Alarm	Instant Smoke Alarm	Instant Smoke Alarm	Instant Smoke Alarm	Instant Smoke 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

Where		**ACCT MT QXYZ GG $C_1C_2C_3$**
ACCT	=	4 Digit Account number (0-9, B-F)
MT	=	Message Type, 18H.
Q	=	Event qualifier, which gives specific event information:
XYZ	=	Event code (3 Hex digits 0-9, B-F)
GG	=	Group, Partition number (00H), or Area Number - 00 = panel - 01= area 1……..xx= area xx
$C_1C_2C_3$	=	1. For devices: zone

$C_1C_2C_3$ = Zone number
001, Zone 1
002, Zone 2
……..
XXX Zone XXX

2. For Panel: code

$C_1C_2C_3$ =	
User PIN Code 1	001
User PIN Code 2	002
User PIN Code 3	003
User PIN Code 4	004
User PIN Code 5	005
User PIN Code 6	006
Temporary Code	997
Duress Code	998
000= Control Panel	

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.

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 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 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.