Vesta Series

Smart Anytime, Safe Anywhere

ESGW Series
IP Gateway
Installation Guide

November 28, 2019

Table of Contents

1. Introduction

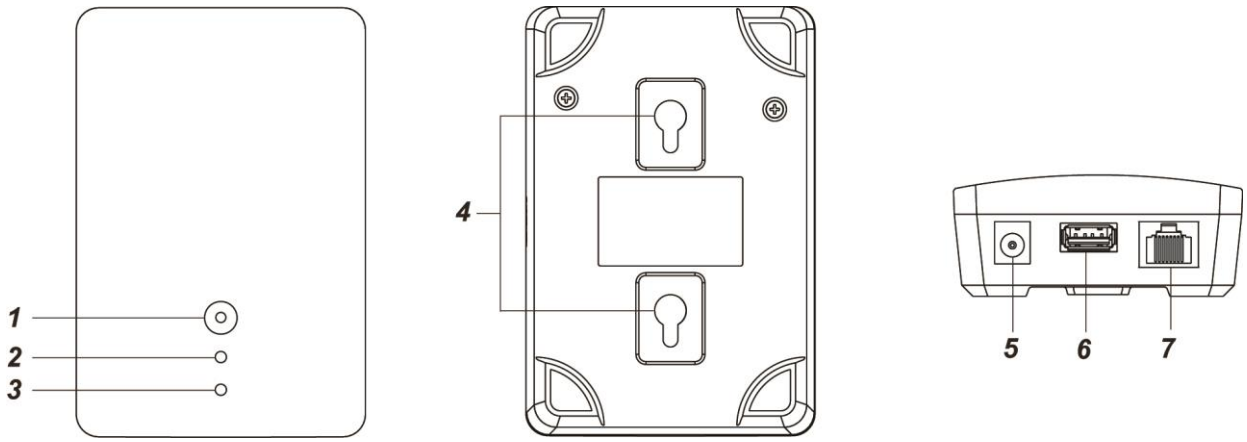
This section covers unpacking your ESGW IP Gateway Control Panel. Refer to later chapters for information on setting up and configuring the system over the Web Page in more detail.

The Control Panel utilizes ZigBee Pro Home Automation 1.2 profile is compatible with all ZigBee devices of same protocol on the market produced by other manufacturers. 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.

Remote Control of the panel is achieved by registering the panel in remote server to view panel status, receive alarm report and manage Home Automation in one complete solution.

2. Device Management

2.1. Identifying the parts:



1. Function Button & System Mode LED (Red/Blue)

Function Button:

Press and hold for 3 seconds – Enable WPS Protocol

Press and hold for 10 seconds – Enter Learning Mode

Press once under Learning Mode – Exit Learning Mode

Press and Hold then apply AC Power – Factory Reset

LED:

Red On – Away Arm

Red Flash – Home Arm

Blue On – Disarm

2. Network LED (Amber)

Amber On – Network Cable Unplugged and WiFi Disconnected

Amber Flash –Disconnected from Server

Off – Network Normal

3. System Status LED (Red/Amber)

Red On – System Alarming

Red Flash – Alarm In Memory

Amber On – Fault Exists in Sytem

Amber Flash – System under Learning Mode

Off – System Normal

4. Wall Mounting Holes

5. DC Jack

For connecting DC 5V 1A switching power

6. USB Port

- Z-Wave dongle USB port

7. Ethernet Port

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. DC 5V 1A switching power output adaptor is generally used to power the Control Panel for standard version.

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 ESGW series Control Panel and program System Settings over the Web page.

3.1. System Deployment

The Control Panel is designed to be placed on desktop, follow guidelines below when planning installation location:

- The Control Panel requires Ethernet connection for system programming, alarm reporting and remote control.
- The Control Panel should be installed at a location that is hidden from outside view.
- The Control Panel should be protected by sensors so that no intruder can reach the Control Panel without activating first activating sensor.

3.2. Installing the Control Panel

Step 1. For configuration and operation of Control Panel via Ethernet, connect the IP cable to the RJ-45 connector.

Step 2. Connect the Power Adaptor to a Wall Outlet and the other end to the Control Panel. After several seconds, the System Mode Blue LED will turn on to indicate system is now functional.

Step 3. The Control Panel can be mounted on wall with its wall mounting holes. Use the two holes to mark location on the wall, drill holes into wall and install screw at mounting location, then hang the Control Panel onto the screws.

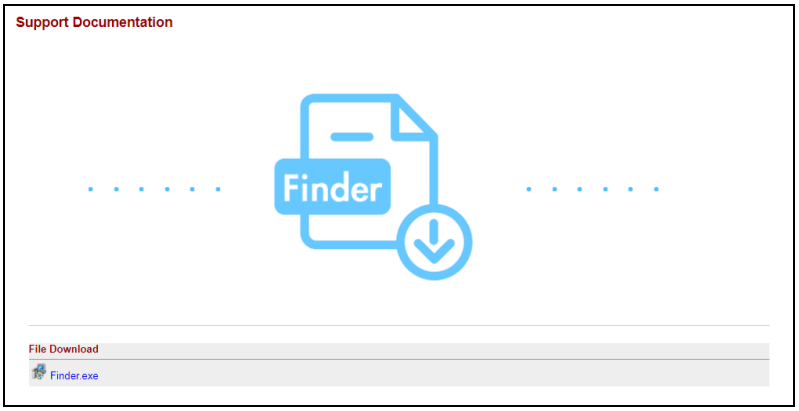
3.3. Software Installation

※ THIS INSTALLATION IS ONLY REQUIRED FOR FIRST TIME USER ※

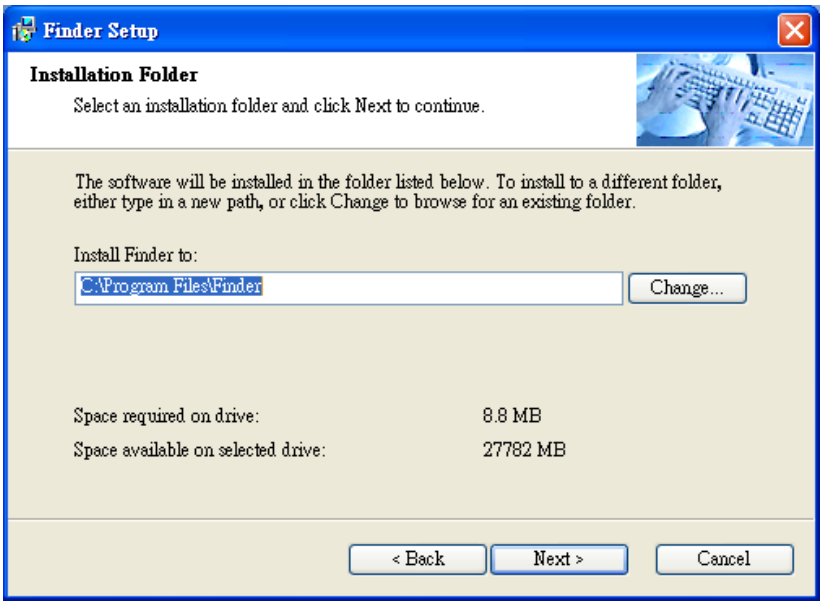
1. RUNNING THE FINDER SOFTWARE

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.



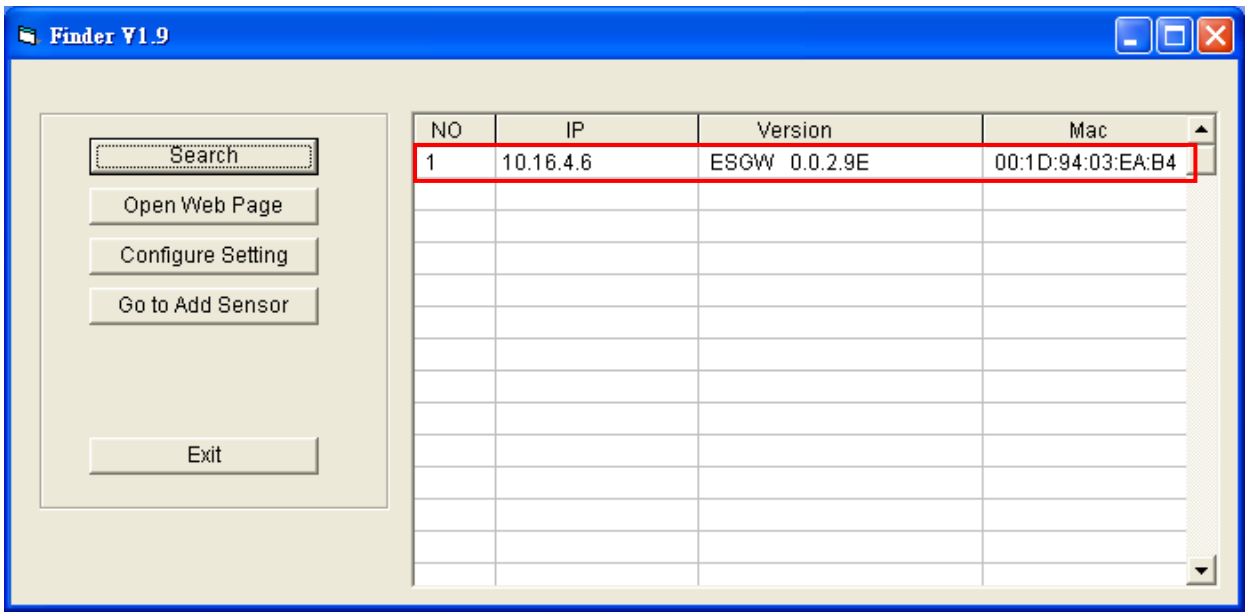
Step 2. After download, install the software and follow on-screen instructions to complete installation.



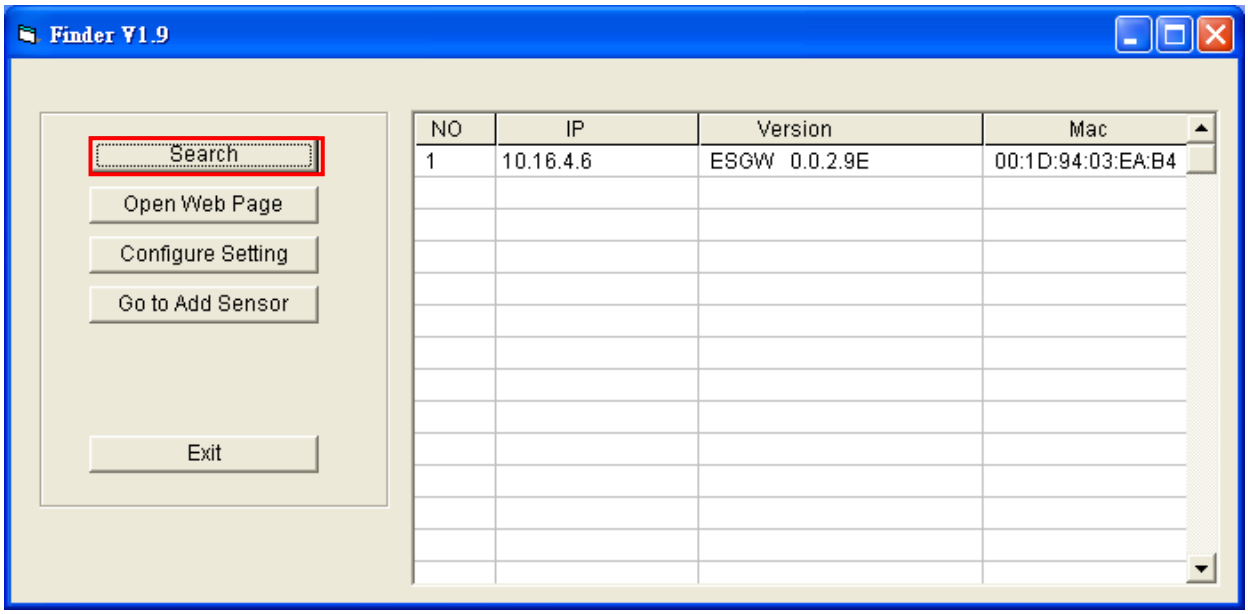
Step 3. Follow on screen instruction to complete installation

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

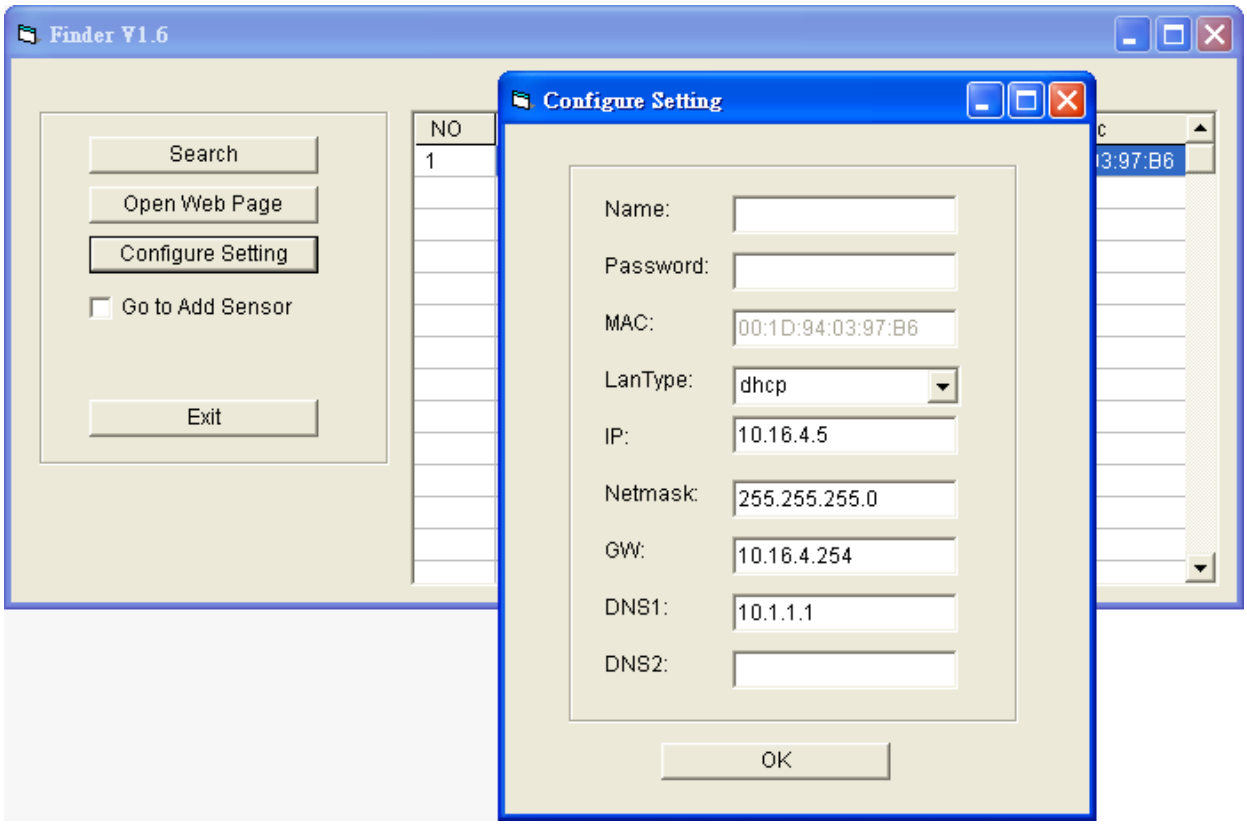
Step 5. Double click on the "**Finder.exe**" to start the software. Finder will automatically search for control panel on the LAN and display its information. If available, the panel's LAN IP address, Firmware version and MAC address will be displayed



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.

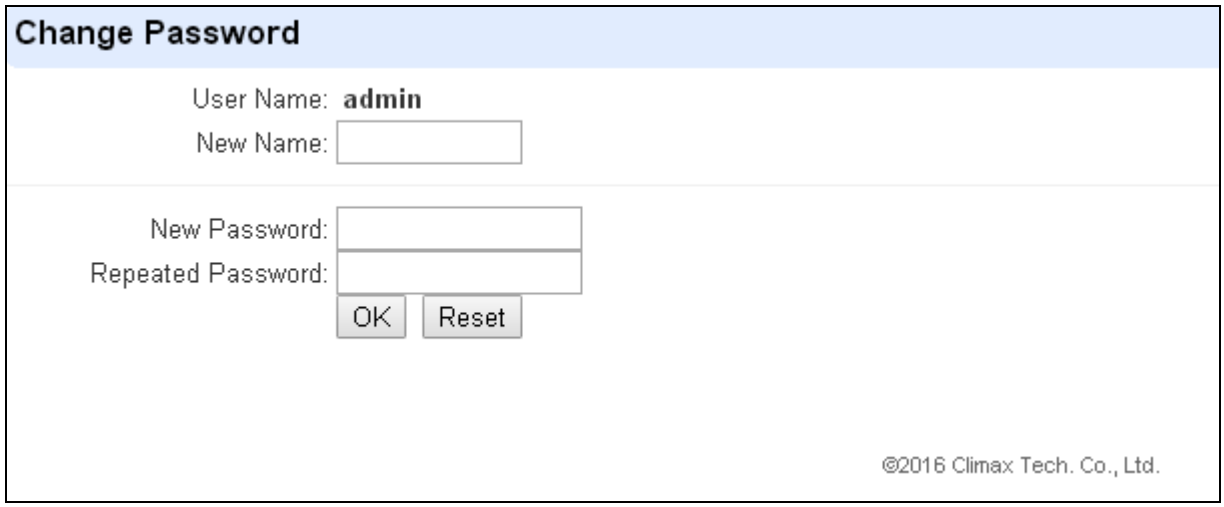
Alternatively, enter the Control Panel IP address displayed in Finder into your browser’s address section and proceed.

Step 2. Enter the User name & Password to proceed

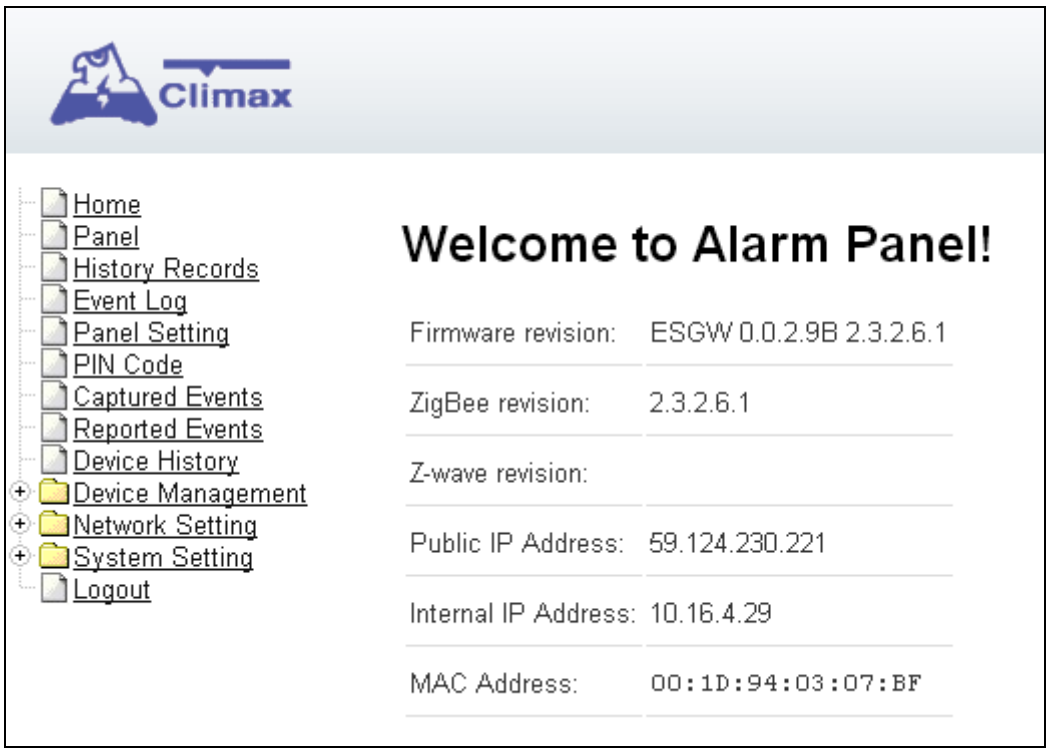
Default user name: **admin**

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

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.



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

5.1. Learning

This feature is for you to add new devices into the Control Panel.

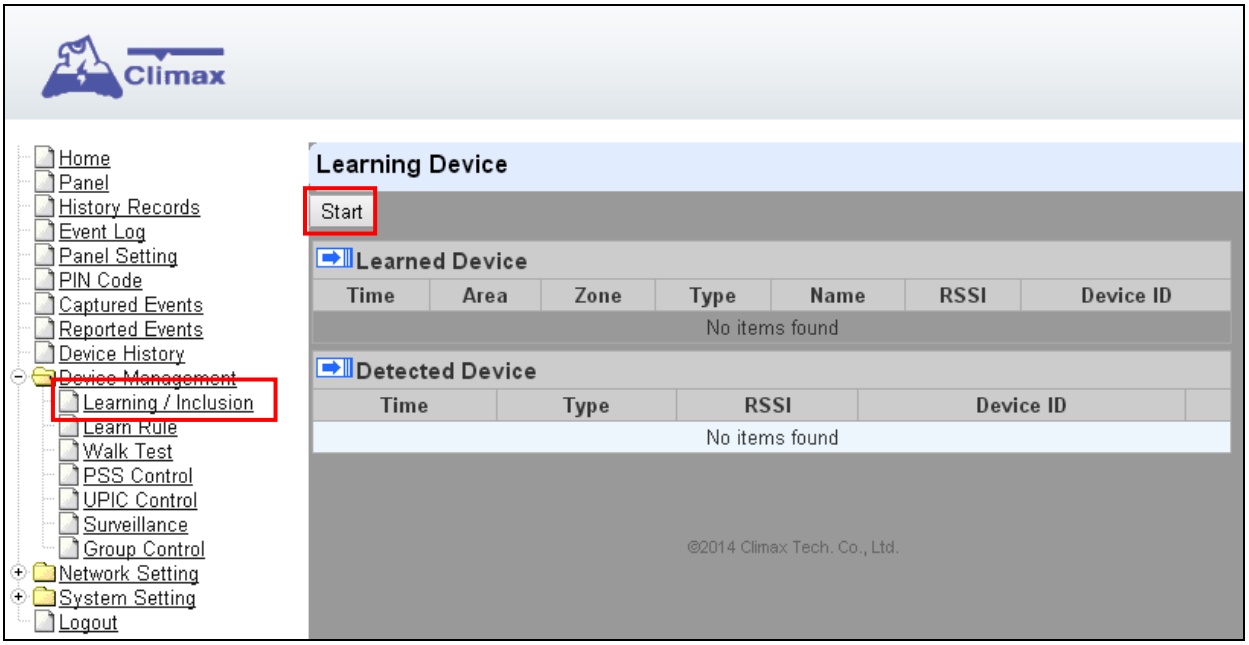
- The panel can support a maximum of 160 devices in two areas (80 devices each area.).
- Up to 6 IP Cameras can be included in the panel.
- If the panel has Z-Wave compatibility (with Z-Wave Dongle), it can also support Z-Wave devices

<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.

5.1.1. Add Sensor

Step 1. Click on "**Learning/Inclusion**" on the tool bar and then the following screen will be displayed.

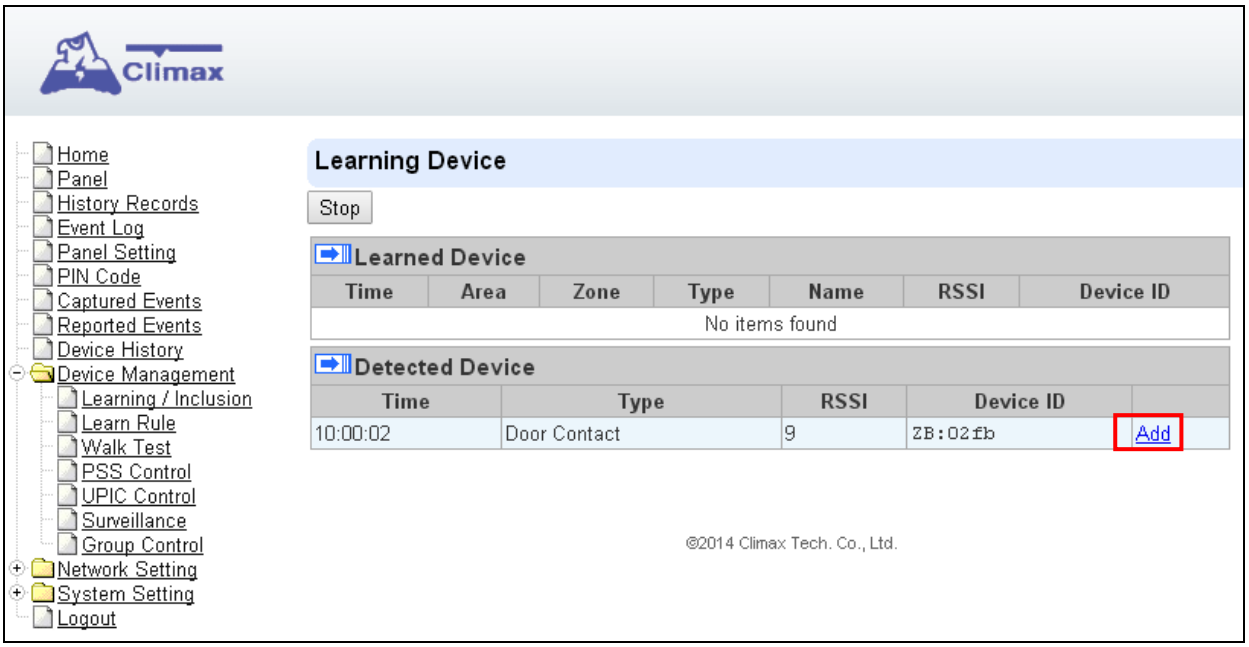


Step 2. Click on "**Start**"

Step 3. The Control Panel will automatically search for devices and include the device in the network. (Please refer to your device manual for detail). When the Control Panel successfully includes a new device in the network, the device information will be displayed accordingly on the webpage.

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

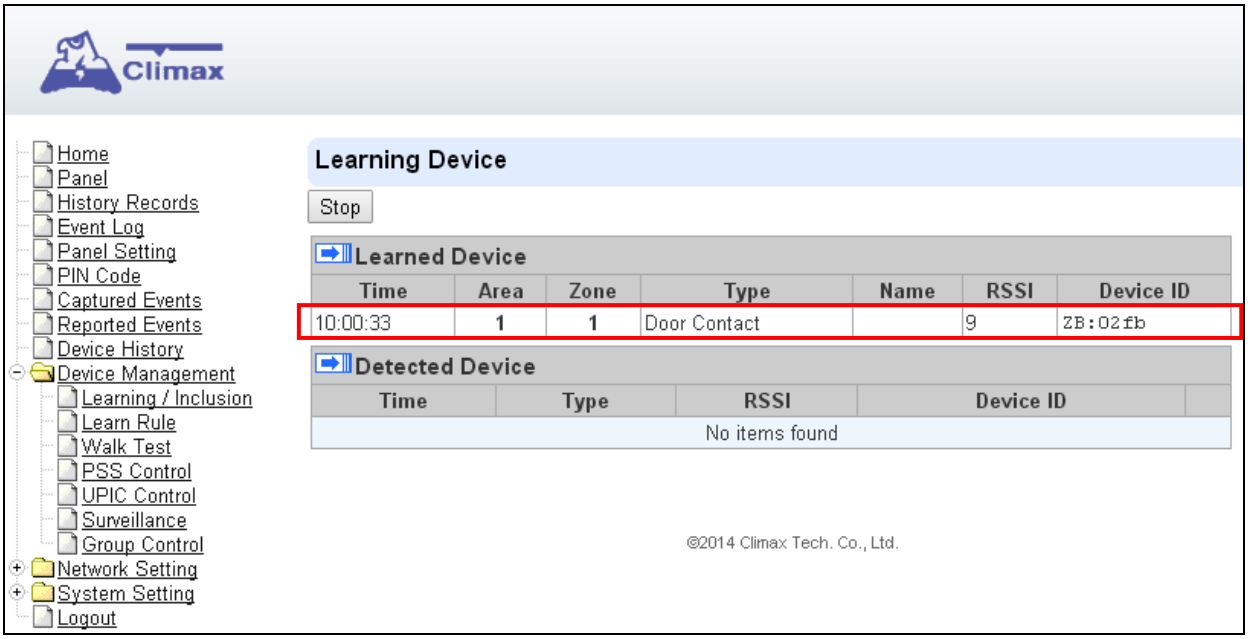
Step 5. Click "**Add**" (highlighted in red box) to include this particular sensor into the system. If the sensor you wish to learn into already exists in the system, the sensor information will be displayed in the **Learned Device** section. If not, the sensor information will be displayed in the **Detected Device** section.



<NOTE>

☞ Z-Wave devices requires an additional Z-Wave Dongle.

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

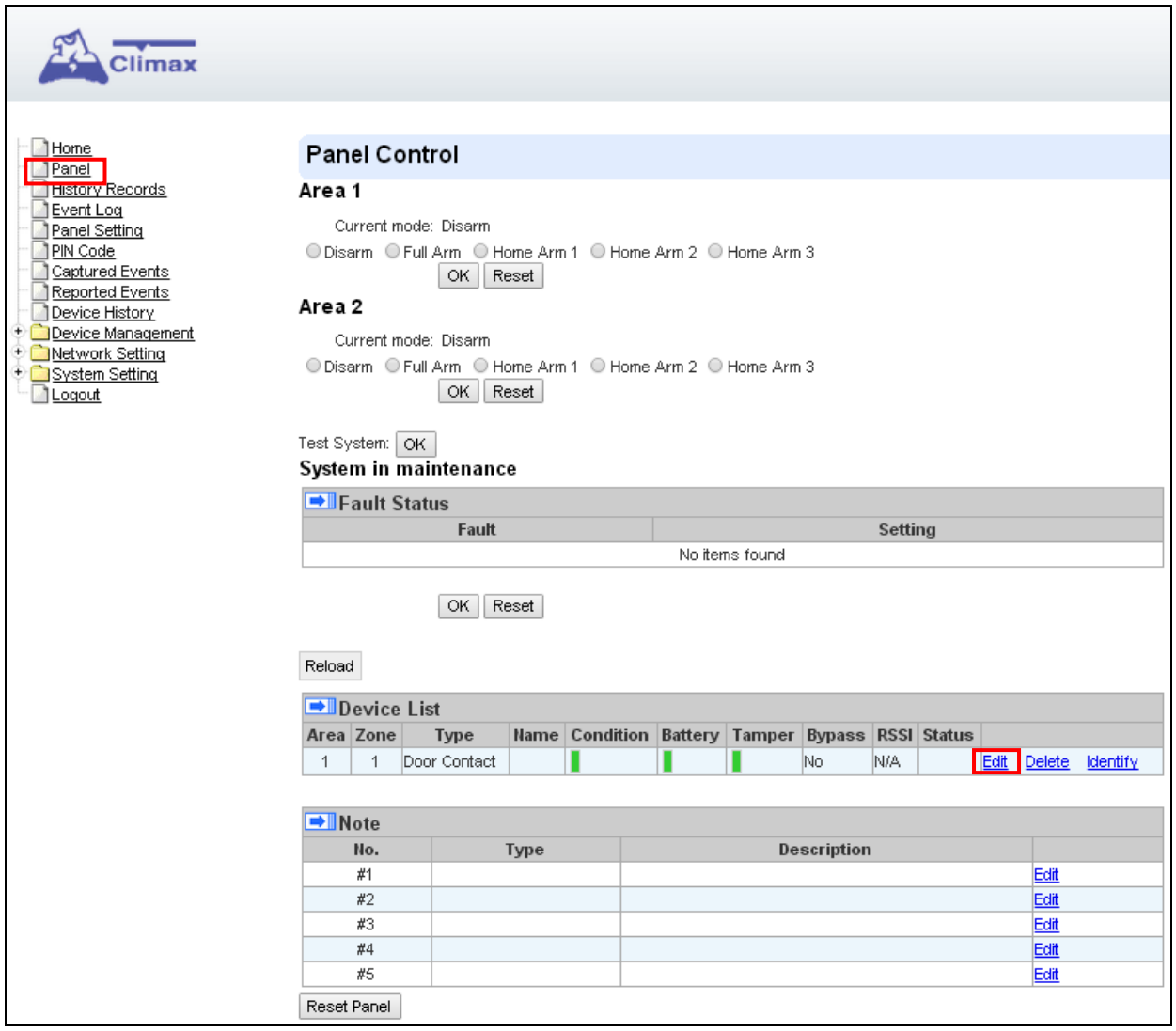


5.1.2. Local Learning

Press and hold the **Function** Button at the top of Control Panel for 10 seconds to enter learning mode, then transmit signal from your accessory devices. When the signal is received the panel will add the device into panel and assigned the device to to Area 1 automatically. To exit local learning mode, press the function Button once.

5.1.3. Edit Devices

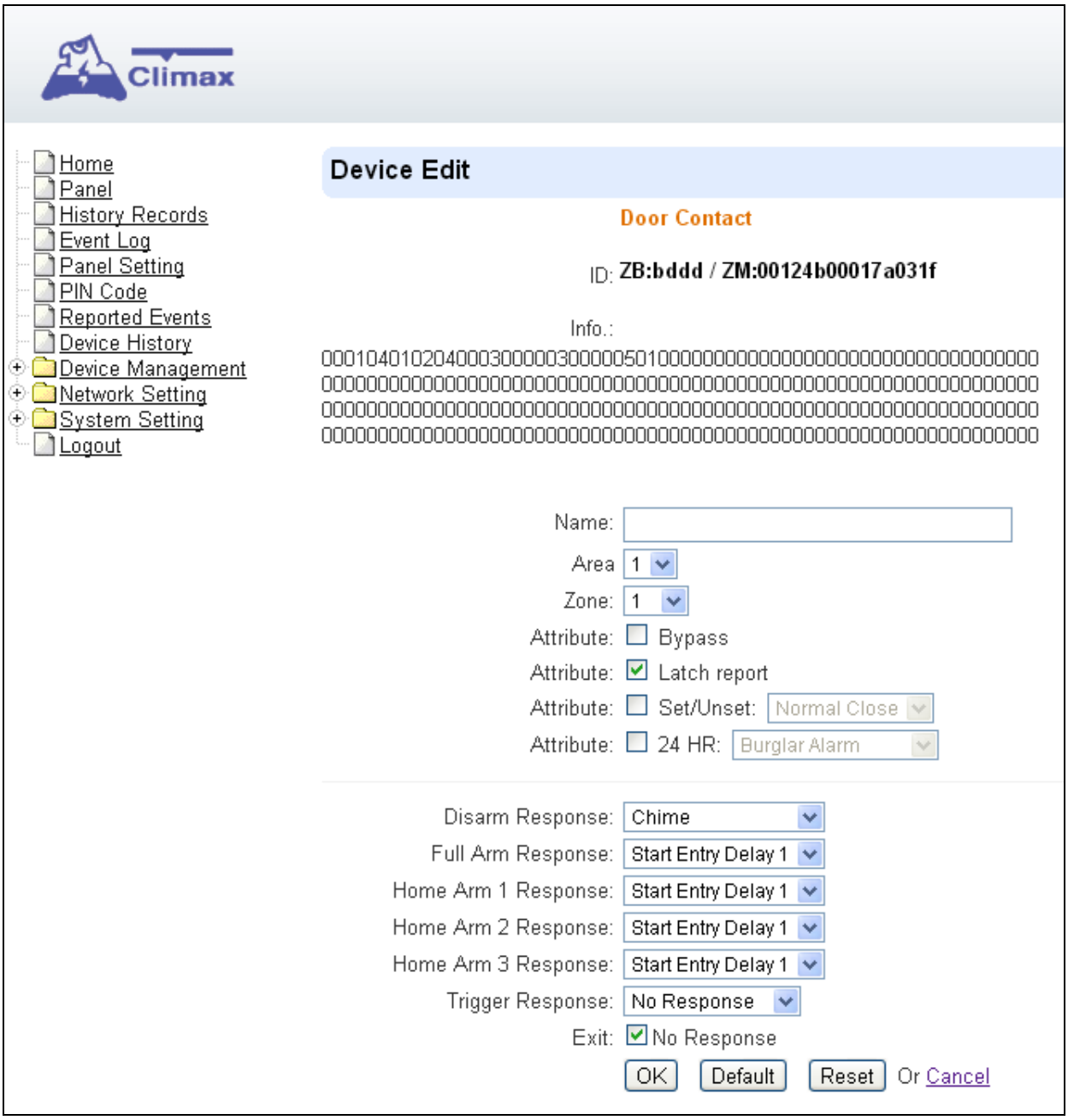
Step 1. To edit device setting, go to "**Panel**" webpage and click "**Edit**" after the device column under the Device List section.



Step 2. You device information and setting will be displayed. Programming the settings according to instructions below and click **OK** when completed to confirm change.

<NOTE>

- ☞ Press "**Default**" to reset all parameters to default values.
- ☞ Press "**Reset**" to re-enter all the information.
- ☞ Press "**Cancel**" to exit the screen and returns to Panel Condition Page.



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.
- Bybass: this function allows user to 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 history records webpage.
- Latch Report (Only for Remote Controller or Door Contact with Set/Unset attribute enabled):

  Latch Report ON = Whenever the system is armed, home armed or disarmed, the

Control Panel will report the arm/disarm event by the particular device

Latch Reprot OFF = Whenever the system is armed, home armed or disarmed, the Control Panel will NOT report the event.

- Set/Unset: 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.

- 24H: this function enables the sensor to report an selected alarm event whenever it is triggered regardless of system mode..
- Disarm/ Full/ Home 1/ Home 2/ Home 3 response: if the system is in the disarm / Full/home1//home2/home3 mode, when a sensor is triggered, it will respond according to the attribute you set.
- Trigger Response: When the device is triggered, the Control Panel will activated pre-programmed scene setting. Please refer to **Scene** webpage for detail.
- Exit: if **No Response** is ticked, the sensor does not repond to any trigger when the system under Exit Delay Time 1/2. If **No Response** is not ticked, the sensor will raise burglar alarm and report immediately when triggered during Exit Delay Timer.

- **Attribute List:**

  ☞ ***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, the system 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 system 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 a sensor set to **Chime** is activated, the system will sound a Ding-Dong Door Chime sound to indicate.

  ☞ ***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***

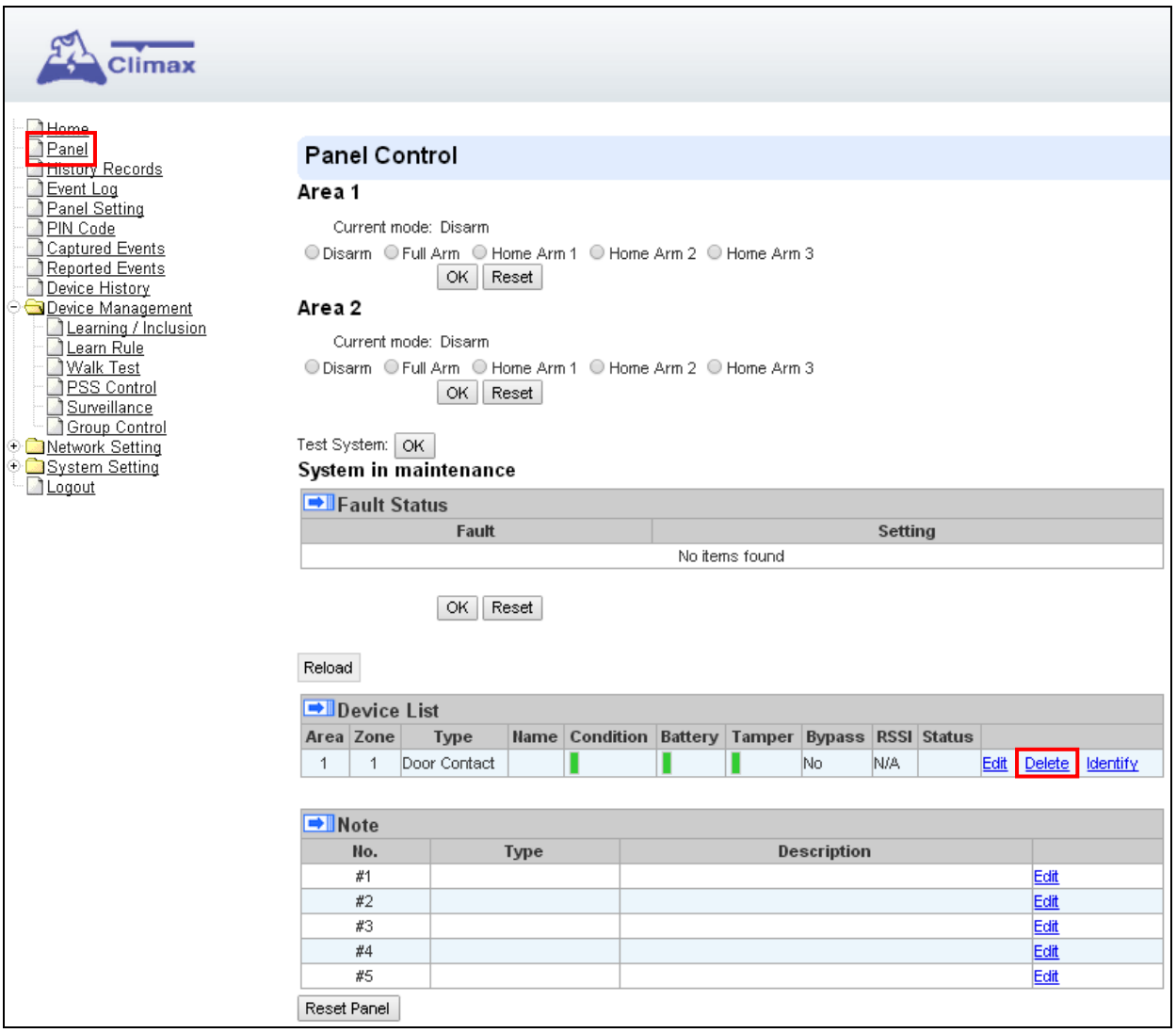
- When the system is in Full Arm or Home Arm / Disarm / / Entry Time mode, if a sensor set to **Burglar Outdoor** is triggered, the Control Panel will report a burglar outdoor event immediately.

☞ ***Apply Scene***

- The attribute is for Trigger Response only. You can select a Home Automation Scene number with this function. When the device is triggered/activated, the Control Panel will execute the actions programming in the Scene accordingly. For more information, please refer to **8.3. Scene**.

5.1.4. Delete Devices

Step 1. To delete a sensor, choose "**Delete**" under "**Panel**" section.



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

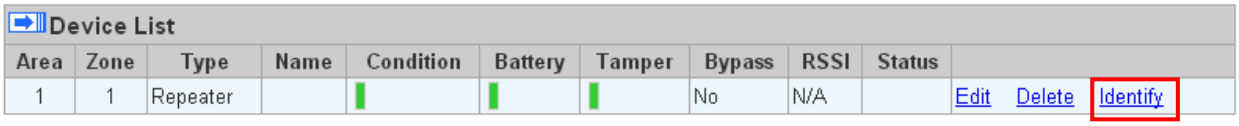
5.1.5. Identify ZigBee Device

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.

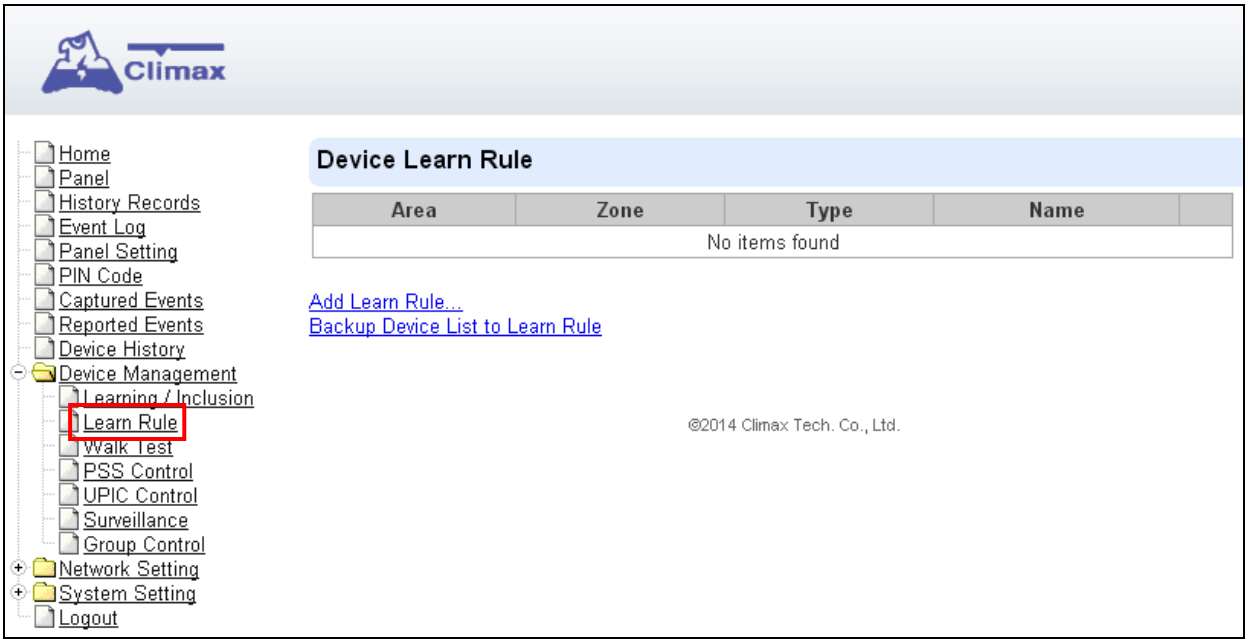
<NOTE>

☞ 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.

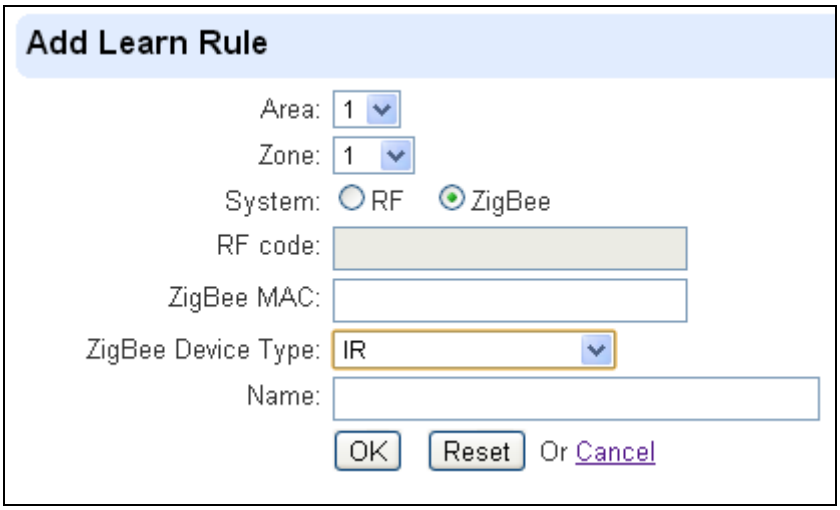
5.2. Learn Rule

You can enter the sensor 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 or IP Camera

Step 1. Under the **Learn Rule** menu, click **Add 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 **ZigBee**.

Step 5. Key in the ZigBee MAC info

Step 6. 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.

5.3. Walk Test

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

Step 1. Click on "**Start**". The system will automatically exit the test mode after 5 minutes

Step 2. Press the test button on the sensor(s) or any button on the Remote Controller (Please refer to your sensor manual for detail.)

Step 3. When the Control Panel receives a signal, it will show the information listed below to indicate that it is safe to install the particular sensor in the location.

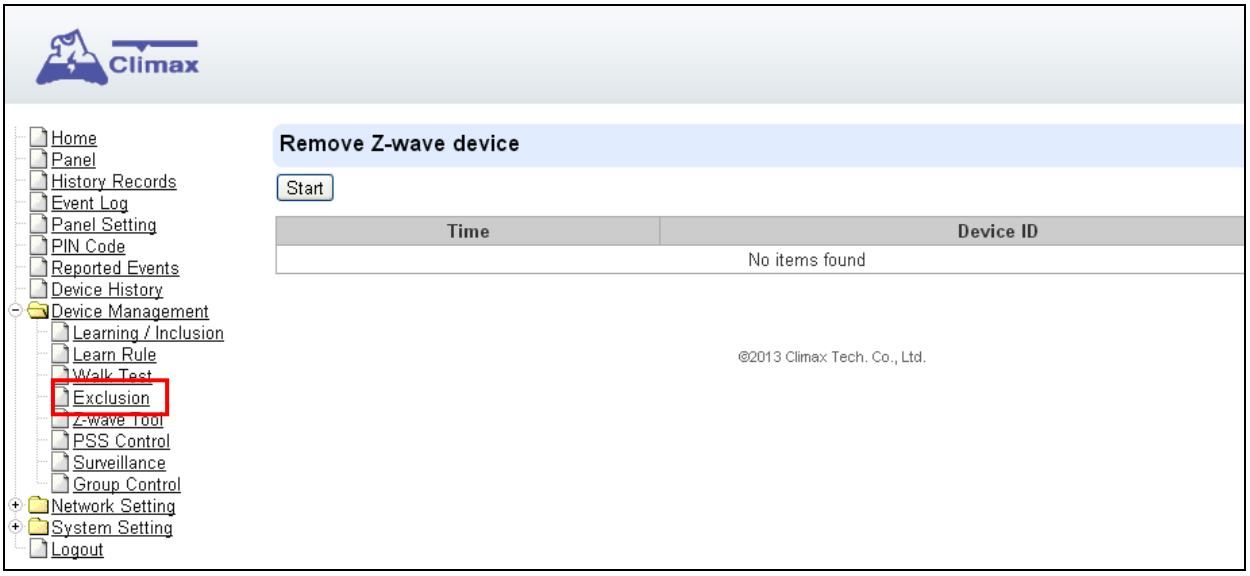
- **Time**: time informaiton
- **Area**: operation area
- **Zone**: device zone
- **Type**: device type
- **Name**: device name
- **Rssi**: the signal strength between Control Panel and sensor. The Rssi value here must be higher than the Rssi value of Panel's background noise (please refer to *6.1 Panel 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.

5.4. Exclusion

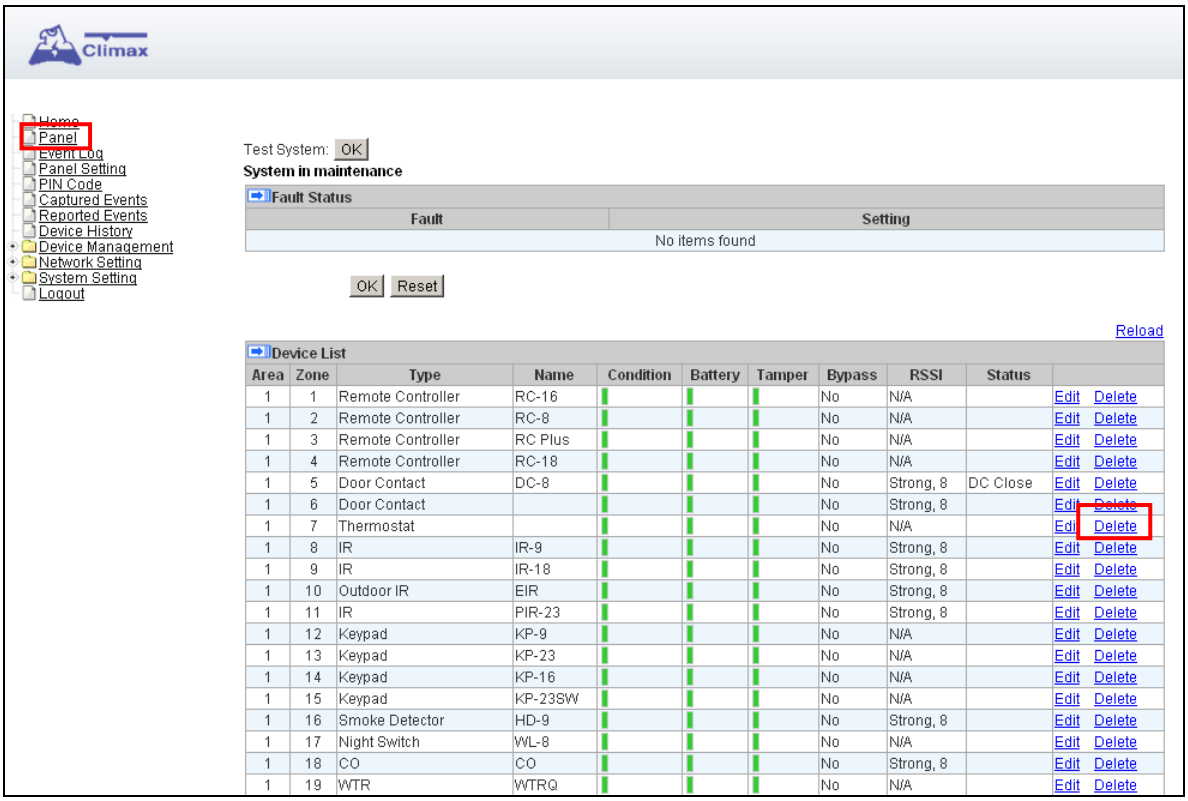
This feature is only available when Z-Wave dongle is inserted. This feature is for you to remove Z-Wave device only.

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



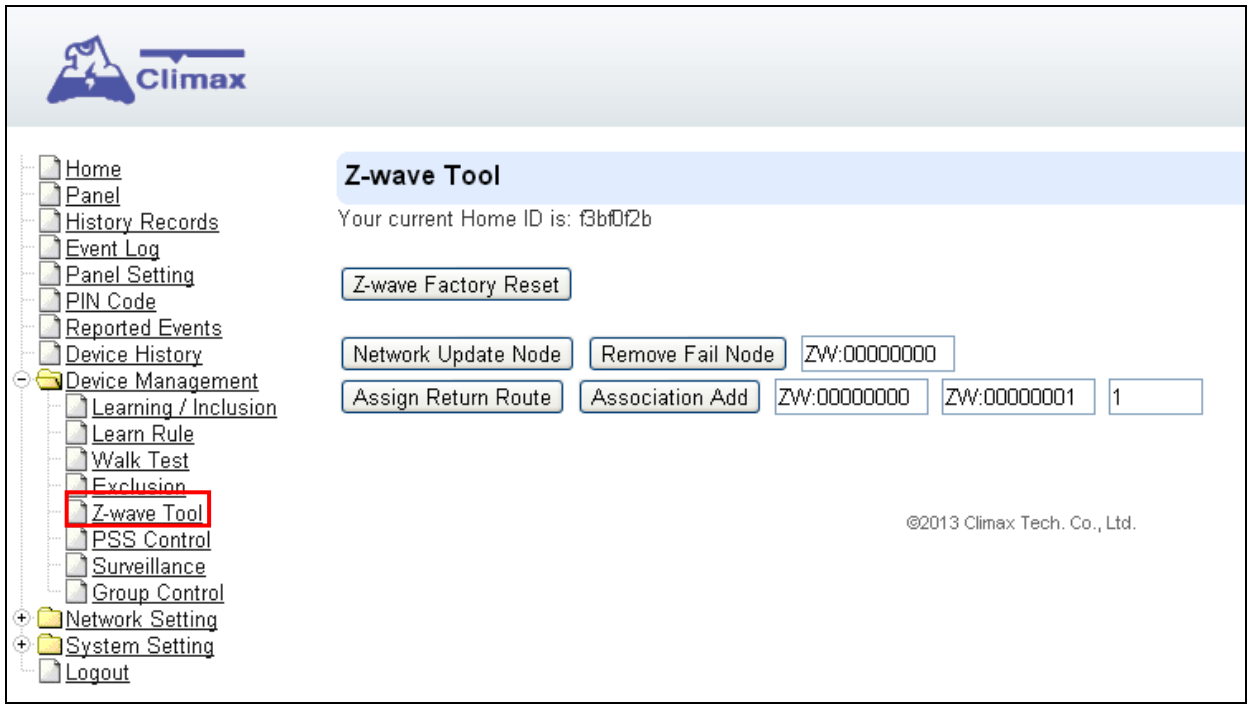
Step 2. Refer to the Z-Wave device manual to transmit signal.

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.



5.5. Z-Wave Tool

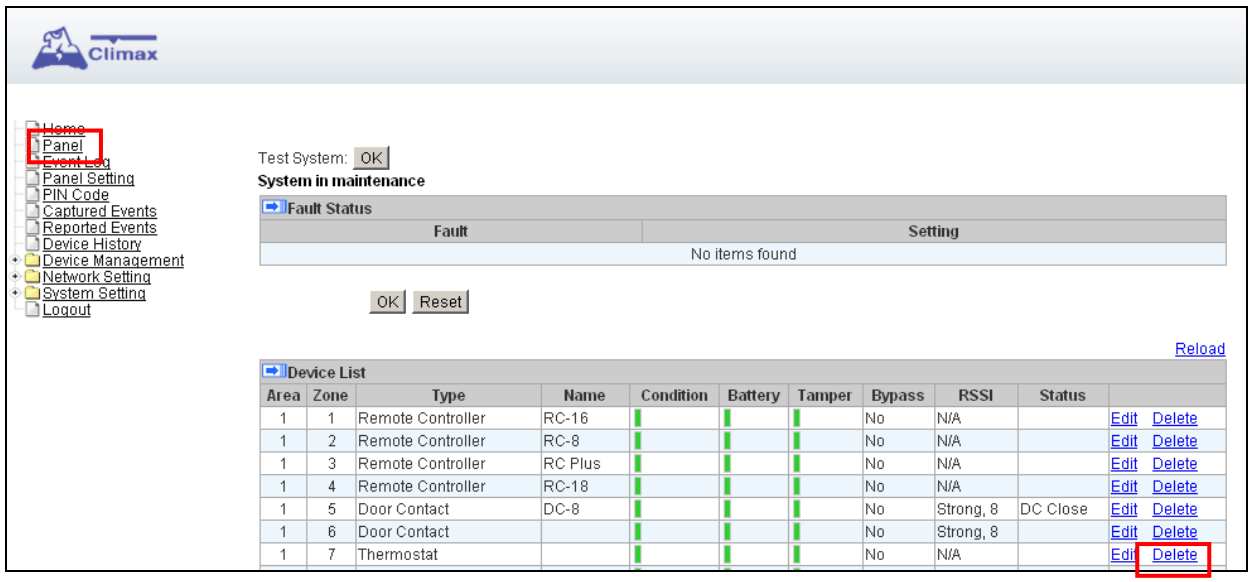
This feature is only available when Z-Wave dongle is inserted. This feature is for you to reset the Z-Wave dongle to factory default and remove all Z-Wave devices, or change routing setting.



- **Reset Z-Wave Dongle**

Step 1. Click "**Z-Wave Factory Reset**", Then the inserted Z-Wave dongle 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**. Please go to **Panel** and then **Device List**. Press **Delete** button to remove one by one.

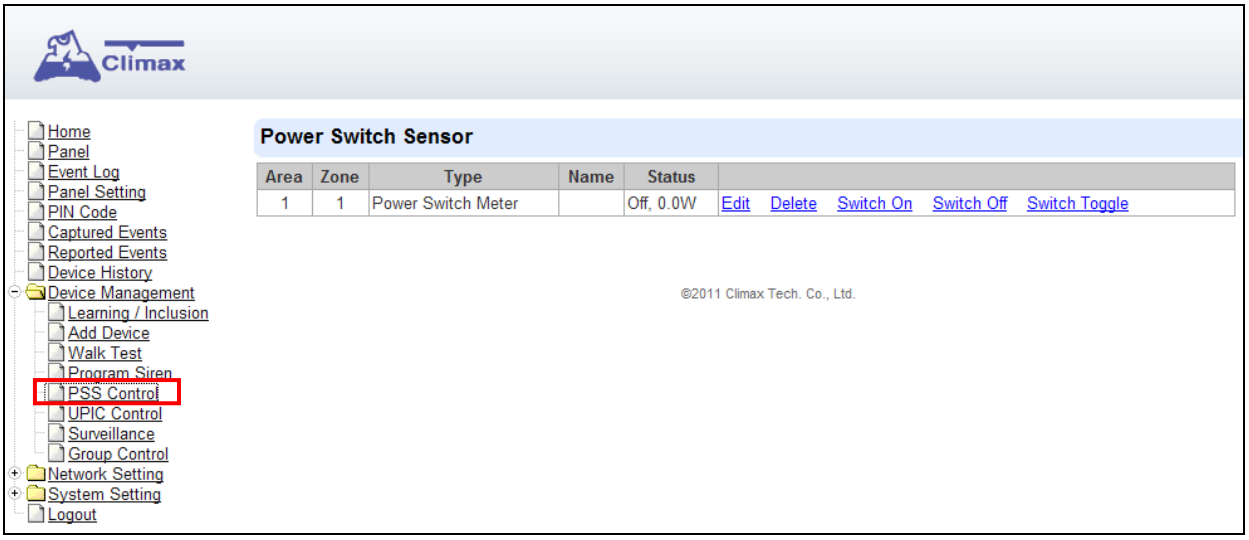


- **Change Z-Wave Routing Setting**

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

5.6. PSS Control

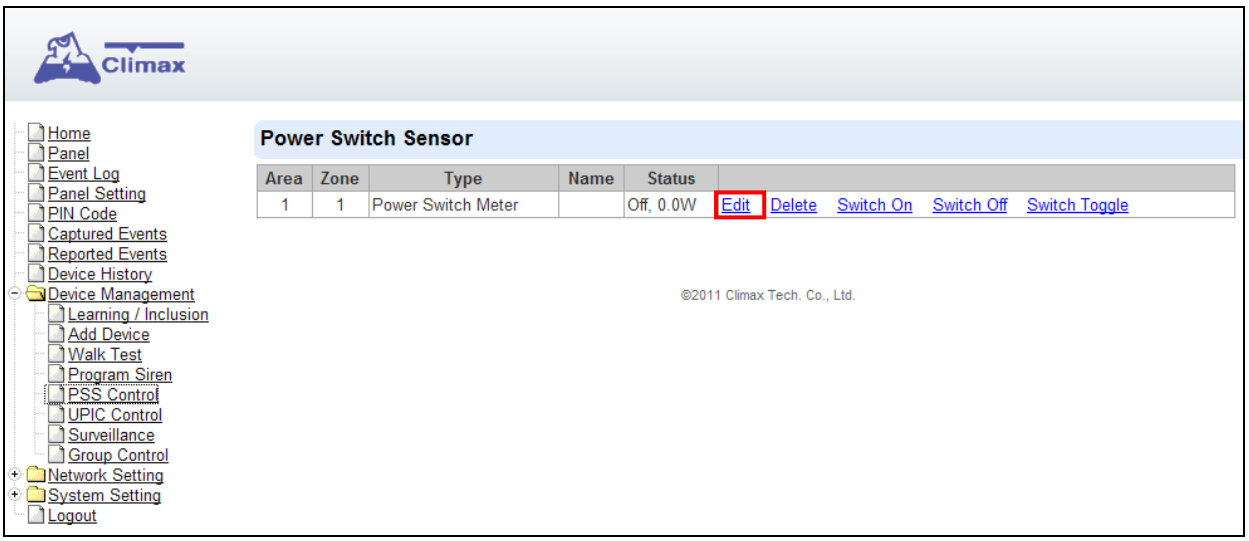
This feature is designed to control/edit/delete an added power switch.



5.6.1. Edit PSS

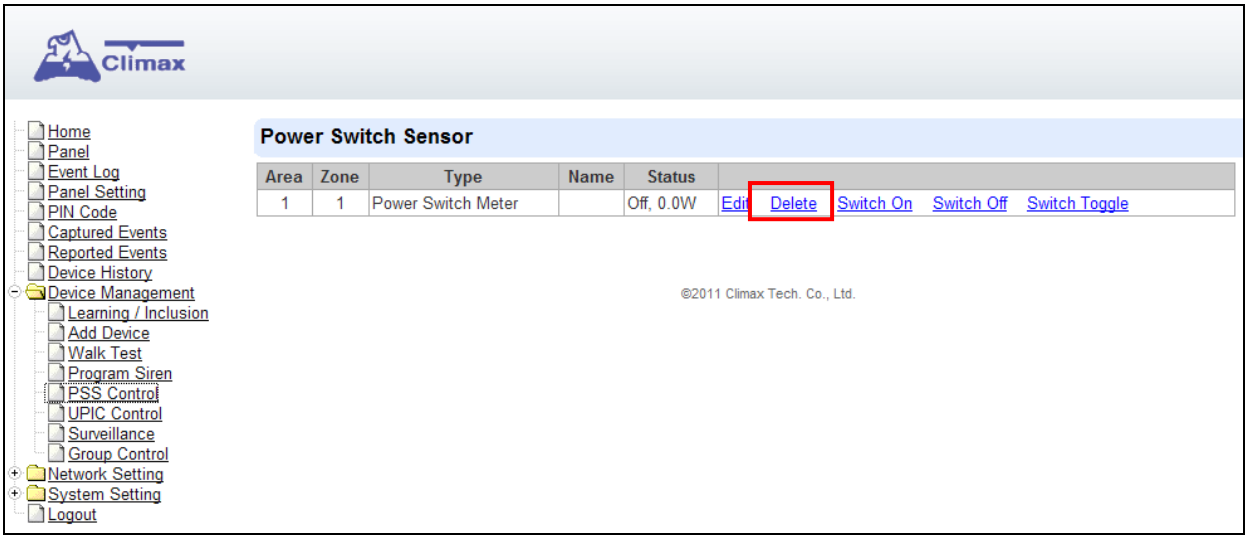
Click **Edit** to further edit attributes of power switches.

Step 1. To program the power switch, select **PSS Control** → **Edit** menu to edit the power switch's settings.



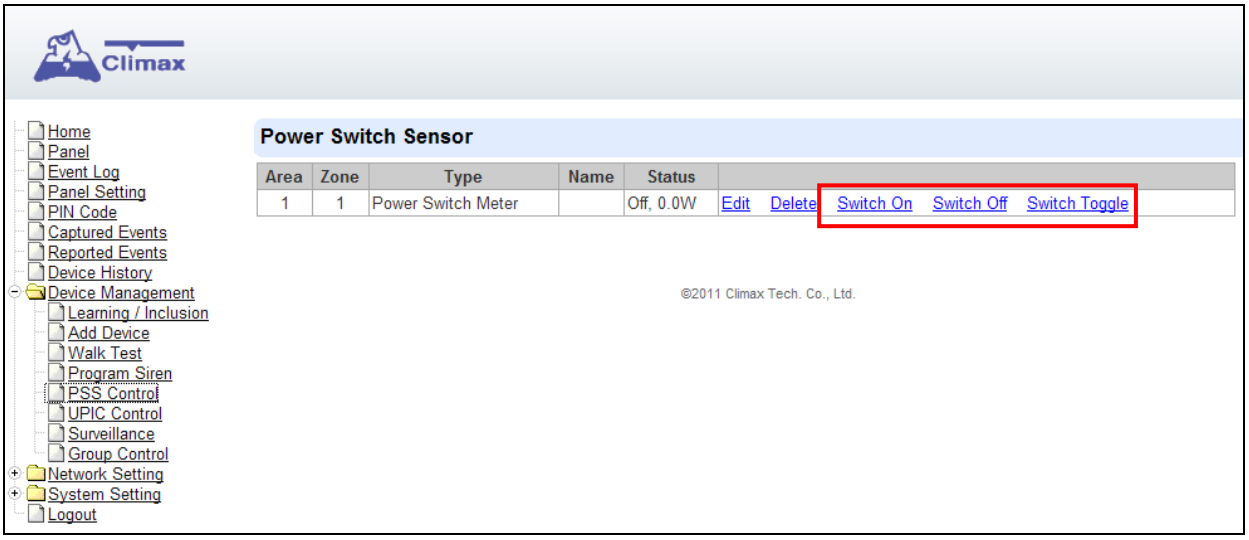
5.6.2. Delete PSS

Click **Delete** to delete power switches.



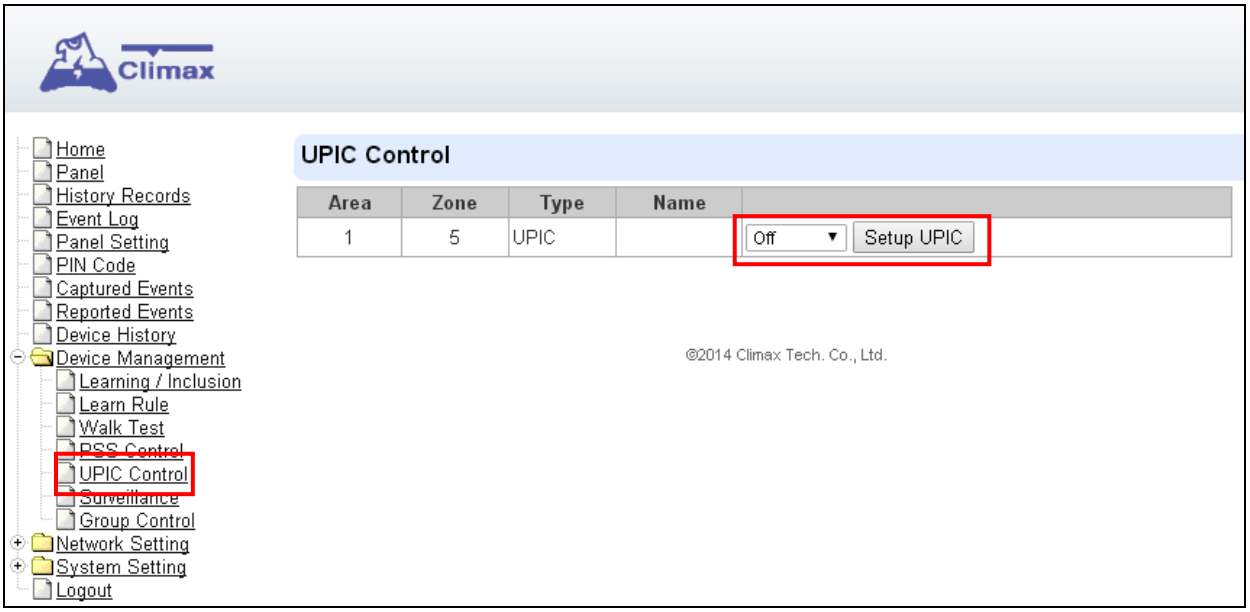
5.6.3. Control PSS

Click **Switch On/Switch Off** to turn on/off power switches. Or click **Switch Toggle** to control the power switch status.



5.7. UPIC Control

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

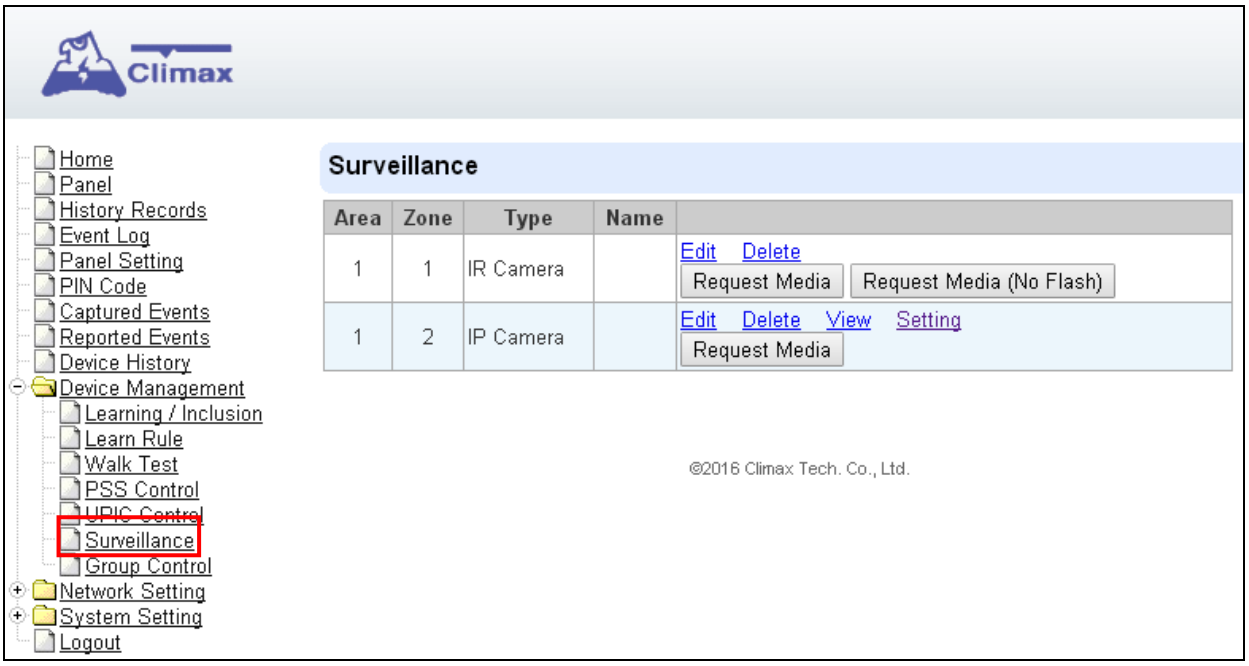


Step 1: Refer to UPIC manual to complete IR signal learning of “Off”, “Heating” and “Cooling” command for air conditioner.

Step 2: Use the drop down menu to select “Off”, “Heating” or “Cooling”. Then click “Setup UPIC” to transmit corresponding command to air conditioner with UPIC.

5.8. Surveillance

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

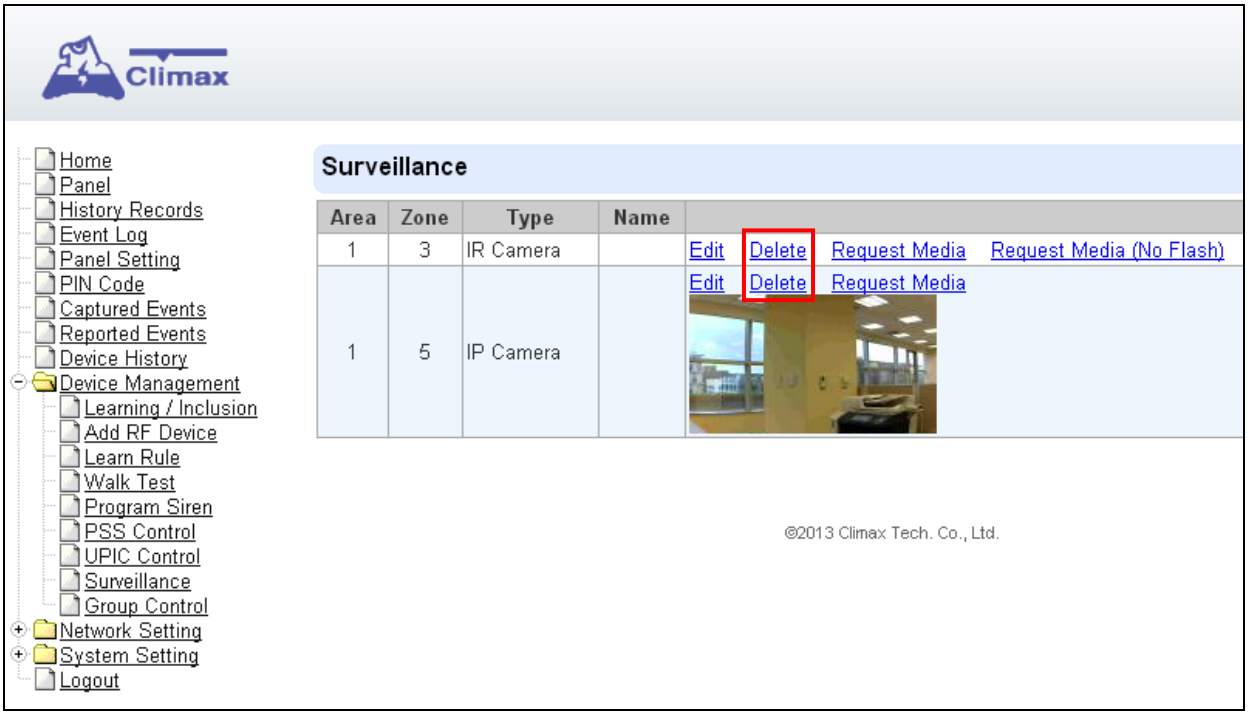


- Click **Edit** to edit camera attributes.
- Click **Delete** to remove device from panel.
- Click **Request Media** to capture a picture or vide
  - PIR camera: A picture will be captured upon request
  - PIR Video Camera: A 10-second video will be recorded upon request
  - IP Camera: The IP Camera 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.

5.8.2. Delete PIR Camera / PIR Video Camera

Click **Delete** to delete an existing PIR Camera / Video Camera/ IP Camera.



5.8.3. Request Images / Video

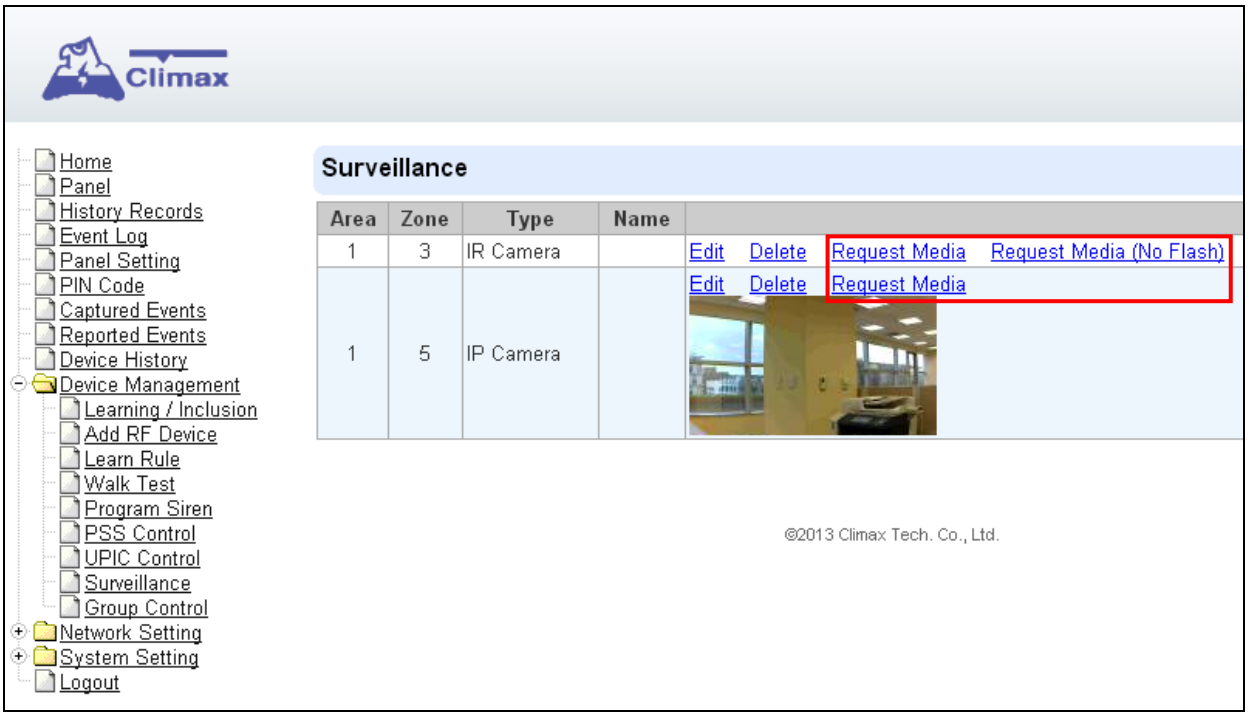
Step 1. Click **Request Media** to capture picture or video.

PIR camera: A picture will be captured upon request

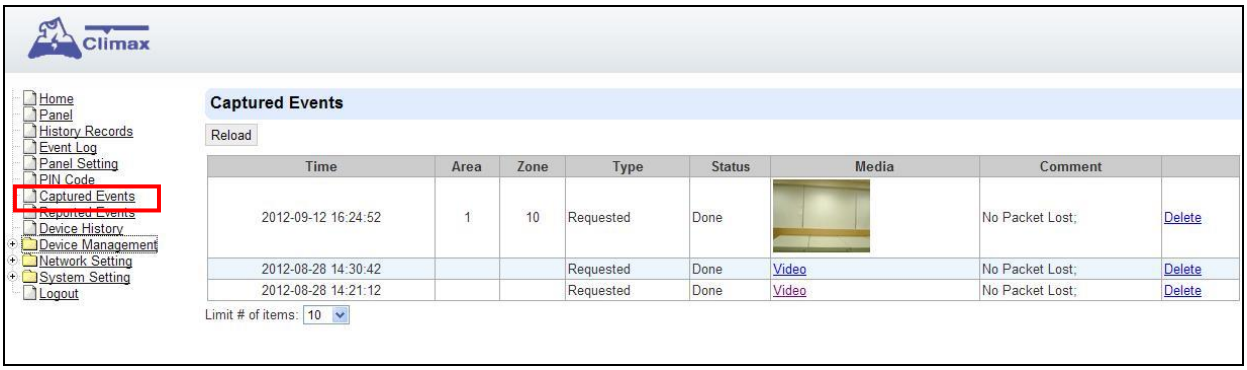
PIR Video Camera: A 10-second video will be recorded upon request

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.



Step 2: The captured image and video from PIR Camera/Video Camera will be displayed in the **Captured Events** section. To view captured image and video, select **Captured Events** to view details.



<NOTE>

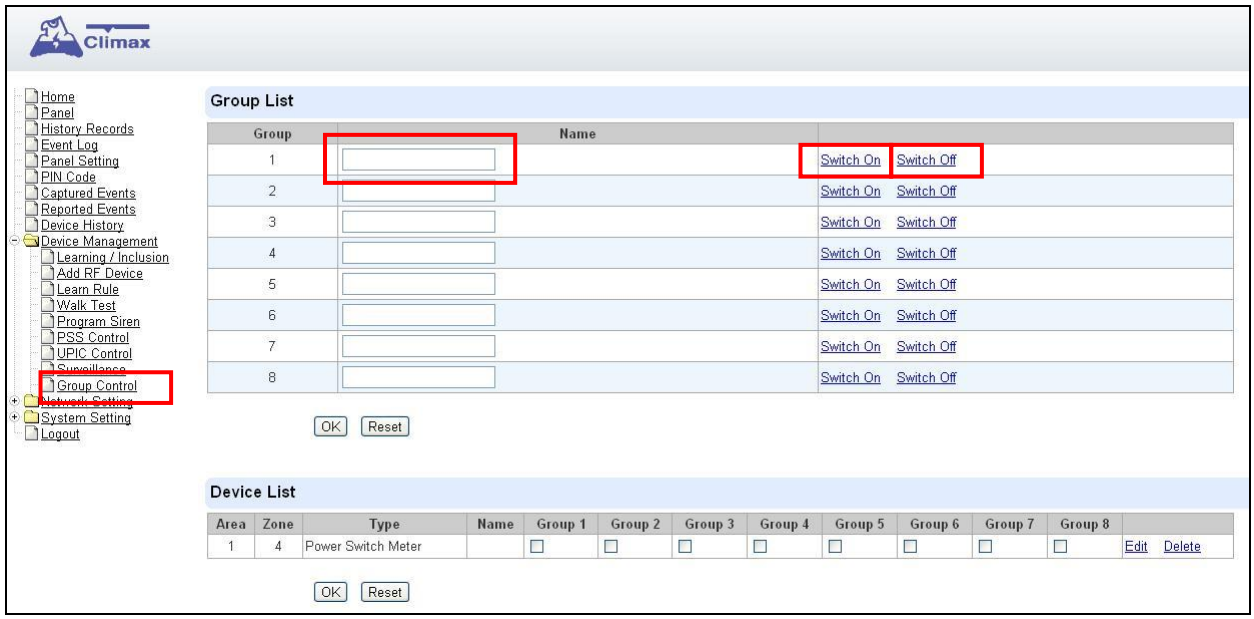
- ☞ If the number of captured events exceeds 100, the oldest record will be replaced the latest one.
- ☞ If users intend to receive captured pictures and video from IR cameras on cell phones, please refer to the **8.8. Media Upload** section for details.
- ☞ Video Recorded by IP Camera will be stored in the IP Camera, please refer to IP Camera manual to view the video.

5.9. Group Control

This feature is designed for you to edit a name of group, switch on or off a group of power switches. Besides, you also can assign power switches to a group you wish.

5.9.1. Group Control/Edit

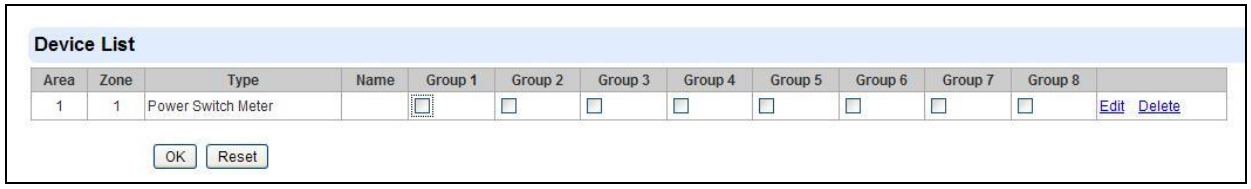
Step 1. Specify a new name for a group.



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

5.9.2 Device Edit/Delete

Step 1. Check the groups which you wish to assign the power switch. This is a multiple-choice field and you can assign one power switch to multiple groups. When you turn on/off the group, all power switches belong to the group will be activated accordingly.



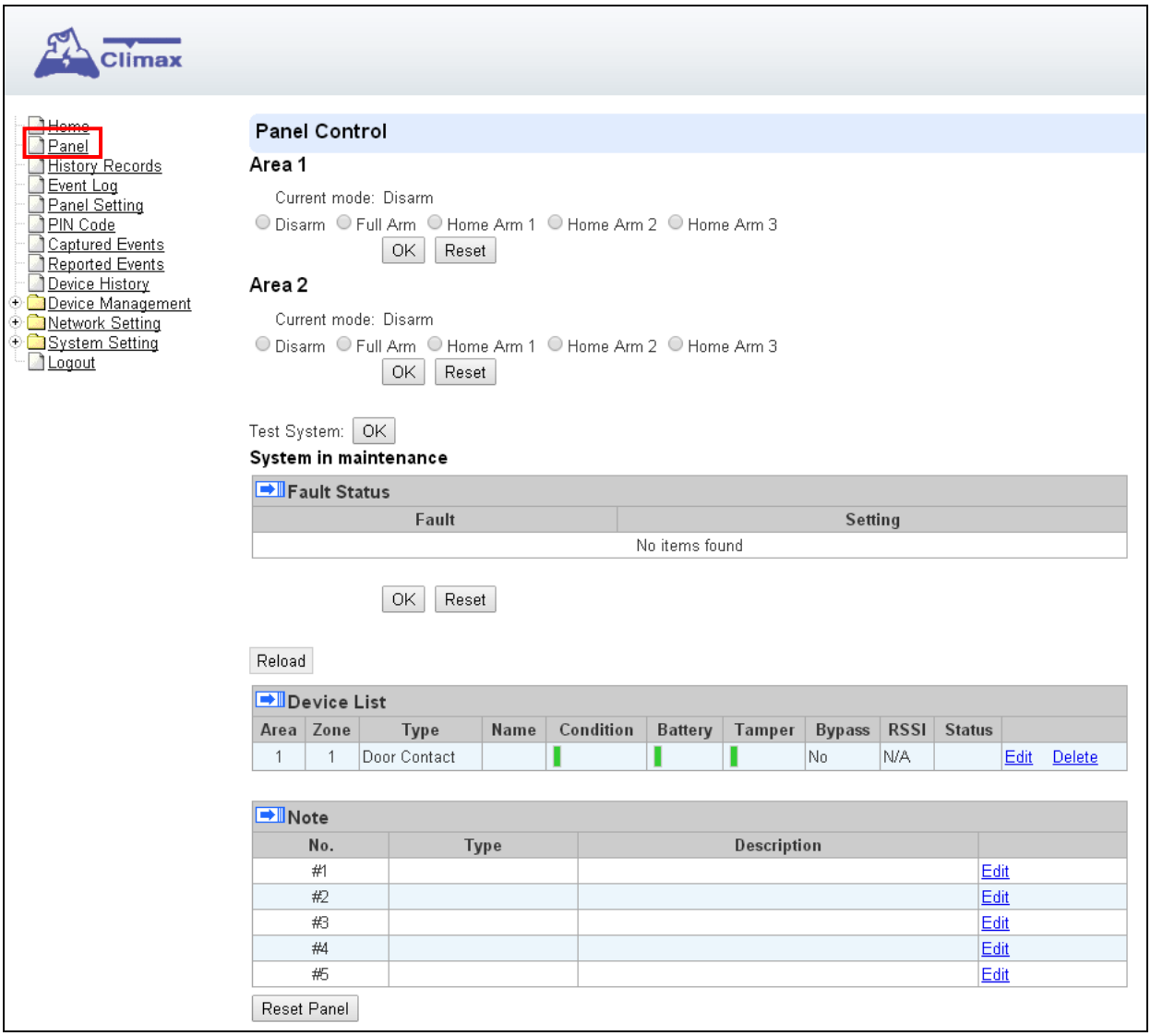
Step 2. Click **Edit** to edit attributes of power switch or **Delete** to delete this device.

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**.



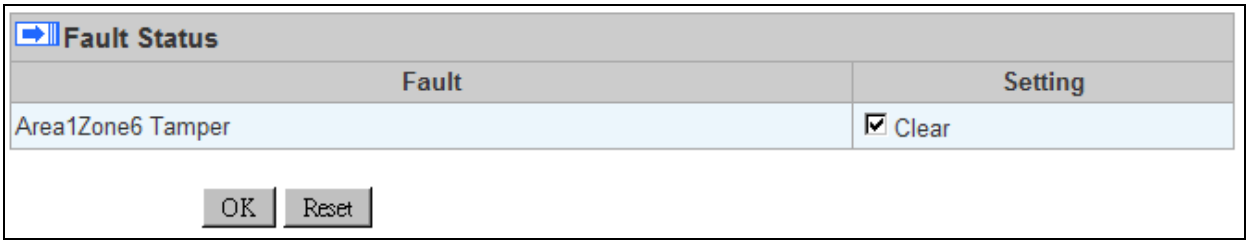
Panel Control

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

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

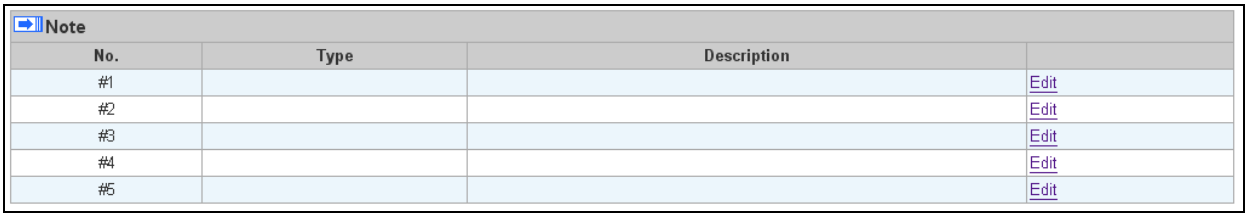
1. The Control Panel will update the device information periodically. However, in order to show the current status, you must **reload** the screen to refresh the display.

- **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.

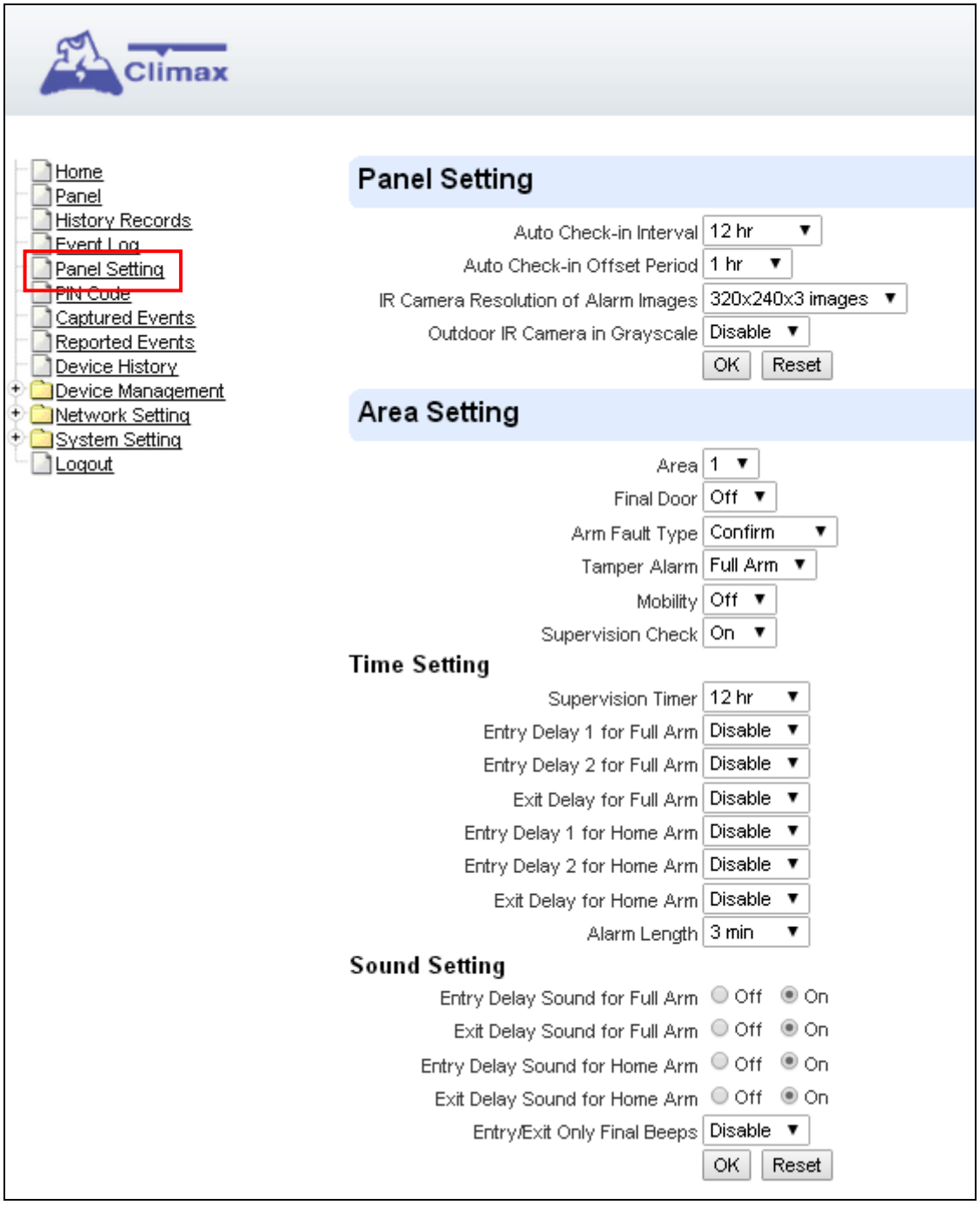
Note



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

- **Auto Check-in**: this is to select whether the Control Panel needs to do check-in reporting to the Central Station automatically and to select the period of time between check-in reports. Options available are **Disable**, **5 Min**, **10 Min**, **15 Min**,**… up to 4 Weeks**.
- **Auto Check-in Offset Period**: This is to set the time delay before the first **Auto Check-In** report to be 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 regular reports 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 3 Days, 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 3 days.

Options available are **1 Hour, 2 Hours, 3 Hours, 4 Hours, 6 Hours, 8 Hours, 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, 320x240x6 images and 640x320x3 images.(Default)**

- **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)

Area Setting

- **Area**: operation area
- **Final Door**: when the system is under away arming with Final Door set to On and a Door Contact set as Entry device, then, the system will automatically full arm the system once this Door Contact is detected as closed, event if the count-down period is not yet complete.
- **Arm Fault Type**: this option is for you to choose how the system should respond when it is being armed under fault condition.

  - Confirm: The panel will first display a “Mode Change Fault” message. Arming again within 10 seconds will force arm the system.

  - Direct Confirm: The system will be force armed directly and report an event.

- **Tamper Alarm**: this is for you to choose whether the learnt-in external 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 others modes (Home arm/ Alarm off modes, etc.), the siren does not sound nor any report will be sent

  - Always: Control Panel raises a local alarm for tamper-trigger in all modes.

- **Mobility**: this is for you to choose whether the Control Panel should report triggering of Door Contact and PIR Sensors under Disarm Mode.

  - On: Whenever a Door Contact or PIR Sensor is triggered under Disarm Mode, the Control Panel will send a report

  - Off: The Control Panel will not respond to Door Contact and PIR trigger under Disarm Mode.

- **Supervision Check**: this option is used to enable system supervision function. When **ON** is selected, the Control Panel will be able to receive the supervision signals from the devices to monitor their condition.

Time Setting

- **Supervision Timer**: this is for you to set a perdiod that the Control Panel should be able to receive the check-in signals form the devices. If the Control Panel fails to receive a supervision signal from a device within the preset period, it will report a CID event code (147) accordingly.
- **Entry Delay 1 for Full Arm**: this is for you to set Entry Delay Timer for full arm mode. It is allowed to use correct Pin code to disarm the full alarm mode and the alarm reporting

will not be sent during the time period you set in Entry Delay 1 for full arm mode. On the other hand, if the correct Pin code has not entered during the period, Control Panel raises an alarm and sends alarm report.

If Door Contact (DC) or PIR Detector (IR) is set as **Entry Delay 1 for Full Arm** attribute, the system will get into counting down period (Away entry timer) while the DC or IR is triggered under full arm mode.

- **Entry Delay 2 for Full Arm**: this is for you to set Entry Delay Timer. It is allowed to use correct Pin code to disarm the full alarm mode and the alarm reporting will not be sent during the time period you set in Entry Delay 2 for full arm mode. On the other hand, if the correct Pin code has not entered during the period, Control Panel raises an alarm and sends alarm report.

  If Door Contact (DC) or PIR Detector (IR) is set as **Entry Delay 2 for Full Arm** attribute, the system will get into counting down period (Away entry timer) while the DC or IR is triggered under full arm mode

- **Exit Delay for Full Arm**: this is for you to set Exit Delay Timer. While the system gets into **Away arm mode** by Control Panel, Remote Controller(RC) or Remote Keypad (KP), the Exit Delay timer starts counting down.

  During the counting down period, pressing the Arm Button of the RC can restart the counting. In addition, you can press Disarm Button of the RC to stop the counting and return to Alarm off mode.

- **Entry Delay 1 for Home Arm**: this is for you to set Entry Delay Timer. It is allowed to use correct Pin code to disarm the home alarm mode and the alarm reporting will not be sent during the time period you set in **Entry Delay 1 for Home Arm**. On the other hand, if the correct Pin code has not entered during the period, Control Panel raises an alarm and sends alarm report.

  If Door Contact (DC) or PIR Detector (IR) is set as **Entry Delay 1 for Home Arm** attribute, the system will get into counting down period (Away entry timer) while the DC or IR is triggered under full arm mode.

- **Entry Delay 2 for Home Arm**: this is for you to set Entry Delay Timer. It is allowed to use correct Pin code to disarm the home alarm mode and the alarm reporting will not be sent during the time period you set in **Entry Delay 2 for Home Arm.** On the other hand, if the correct Pin code has not entered during the period, Control Panel raises an alarm and sends alarm report.

  If Door Contact (DC) or PIR Detector (IR) is set as **Entry Delay 2 for Home Arm** attribute, the system will get into counting down period (Away entry timer) while the DC or IR is triggered under full arm mode

- **Alarm Length**: this is for you to select the external siren duration when an alarm is activated. Options are disable (no siren alarm) and 1-min to 15-min in 1- min increments.

Sound Setting

(The Control Panel does not have a built-in buzzer, the Sound Setting is used to control external siren or bellbox included in the system..)

- **Entry Delay Sound for Full Arm**: this is for you to decide whether the system should 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 system should 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 system should sounds count-down beeps and volume of beep during the entry delay time in the home

arm mode.

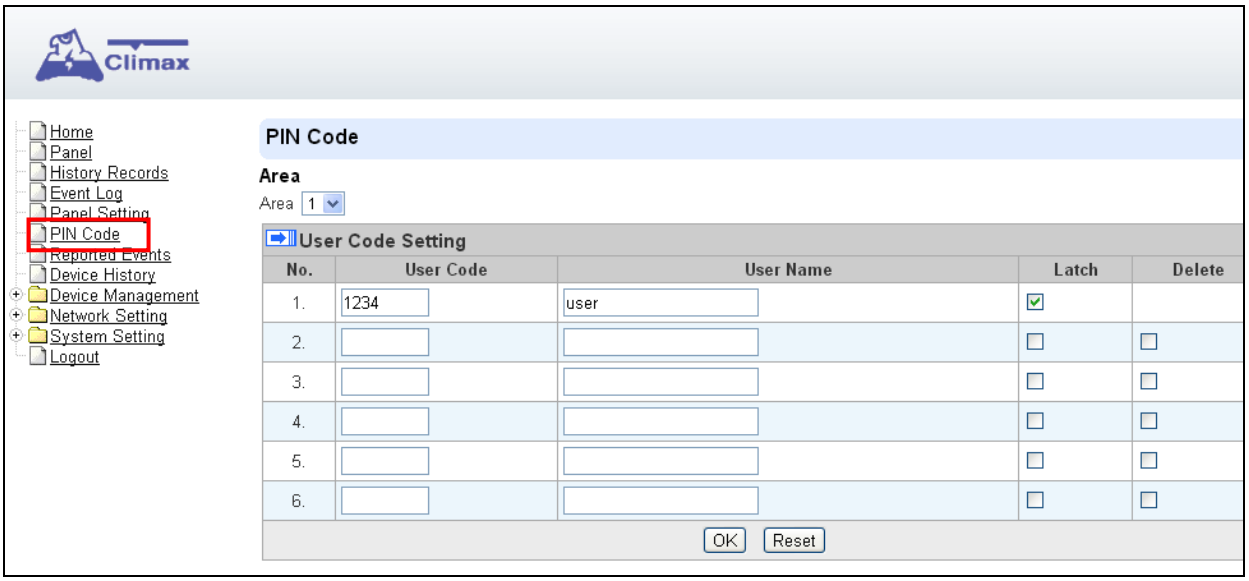
- **Exit Delay Sound for Home Arm**: this is for you to decide whether the system should sounds count-down beeps and volume of beep during the exit delay timer in the home arm mode.
- **Entry/ Exit Only Final Beeps:** This is for you to determine when the system should start warning beep during Entry or Exit countdown timer. For example, if the setting is set to 5 seconds, the system will only start 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

6 User PIN Codes are available in each Area. Each consists of 4 digits (only valid for numeric number 0~9). User PIN code #1 for each Area is always activated factory default.

All User PIN Codes are used to regularly arm/disarm the system and are allowed to access the Programming mode accompanied with the Master Code.

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



Area

Area: select an operation area.

User Code Setting

- **User Code**: an access code authorized for accessing the system.
- **User Name**: each individual User can be given a name for easy recognition when understanding system events. User Names can be named when first setting them or by editing them afterwards. The procedure is similar for both situations. 17 alphanumeric characters are available per name.
- **Latch**: this is to program the Latch Key Reporting feature for all users and any arming/disarming actions of the Remote Controllers of the system. Please click the box to select the options.

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

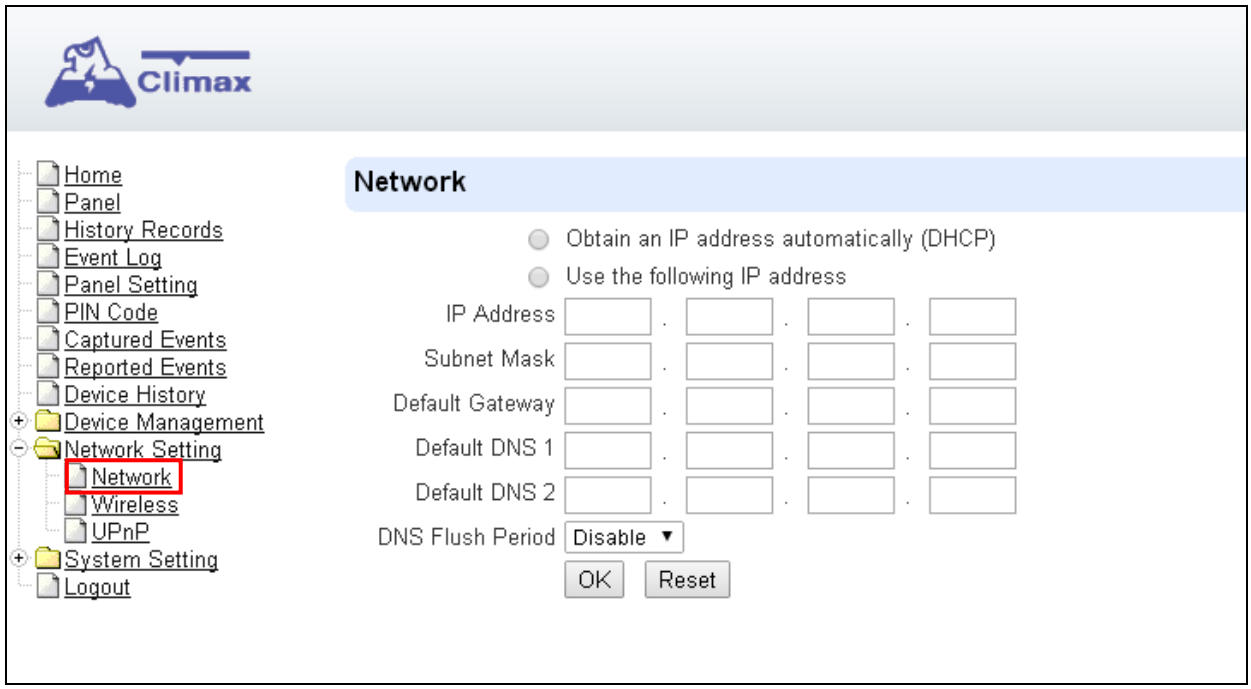
  ☐ Latch → **Latch Reprot OFF** = Whenever the system is armed, partially armed or disarmed, the Panel will NOT transmitt reporting(s) to notify the Central Monitoring Station.

- **Delete**: except User #1 can't be deleted in any way, User#2, 3, 4, 5, and 6 PIN codes can be deleted by clicking the Delete box. With a tick in the Delete check box, it means this particular PIN code will be deleted.

7. Network Settings

7.1. 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 the IP address**

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

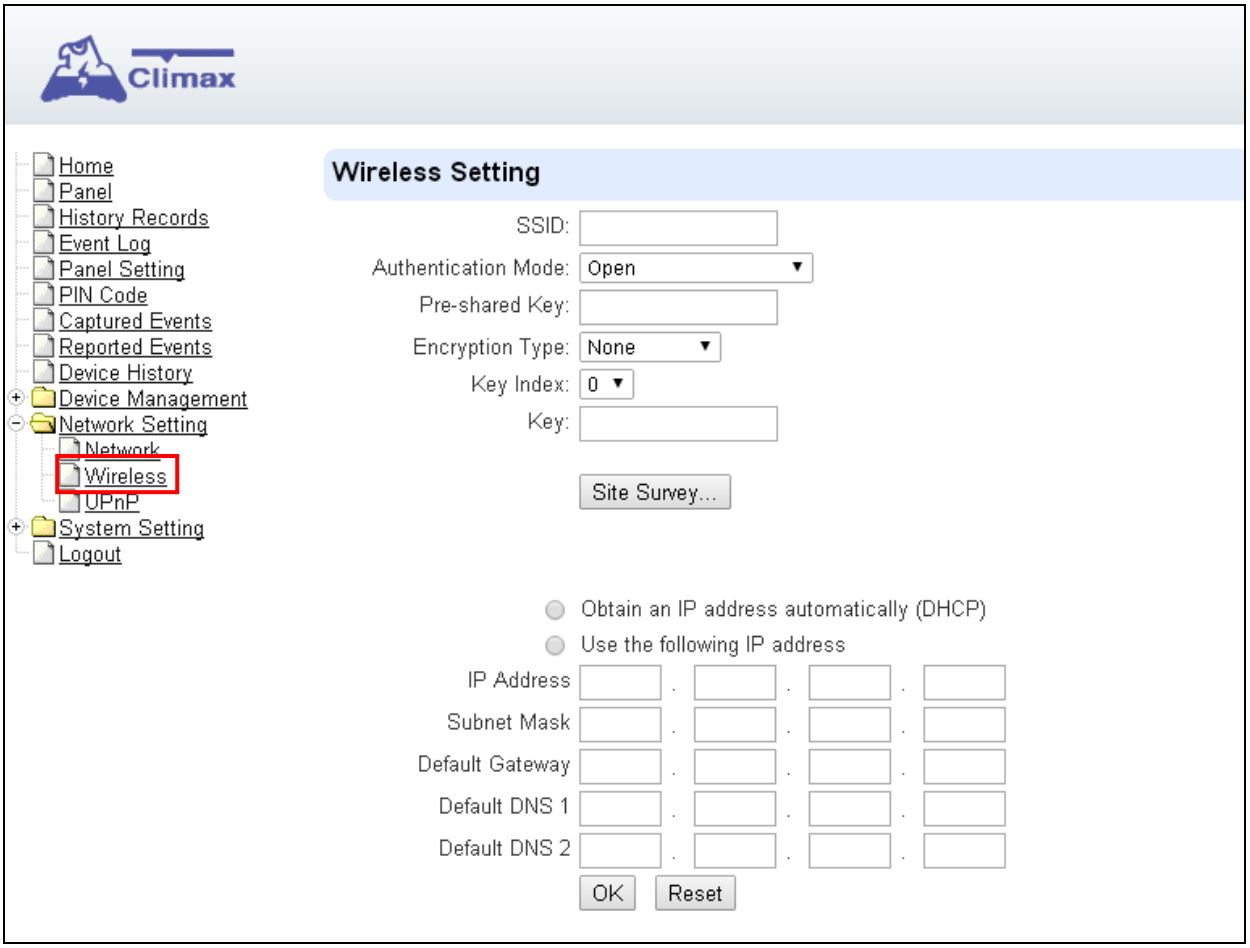
  Please make sure that you have obtained all required values according to your Network environment. Please contact your network administrator and/or internet service provider for more information.

- **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.

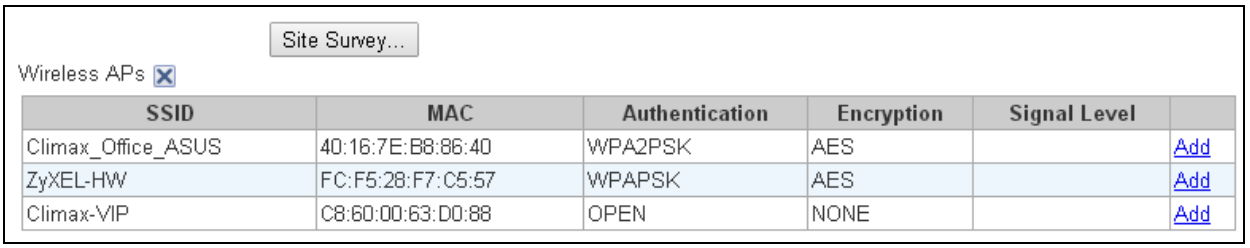
7.2. Wireless (Optional)

The Wireless page is only available to panel model with built-in wifi function.



There are 3 ways to connect to the wireless network.

1. Click "**Site Survey**" to search for available wireless access points. Select the desired access point and click "**Add**" to connect to wireless network.

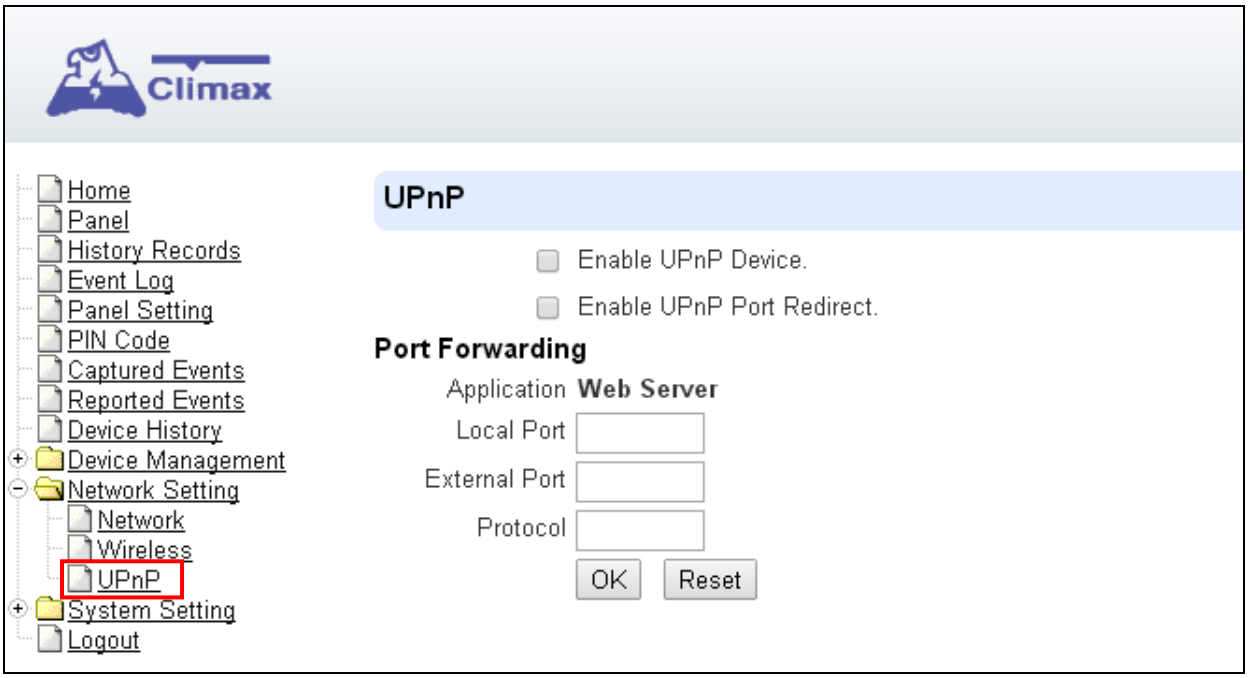


SSID	MAC	Authentication	Encryption	Signal Level	
Climax_Office_ASUS	40:16:7E:B8:86:40	WPA2PSK	AES		Add
ZyXEL-HW	FC:F5:28:F7:C5:57	WPAPSK	AES		Add
Climax-VIP	C8:60:00:63:D0:88	OPEN	NONE		Add

2. Enter the wireless information manually and click **OK** to connect.
3. Use the WPS function to connect to wireless network. Locate the Function Button at top of the Control Panel, press and hold the button for 3 seconds to enable WPS function. Refer to your wireless router setting to complete WPS setup.

7.3. 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 (e.g. Window XP).

- **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

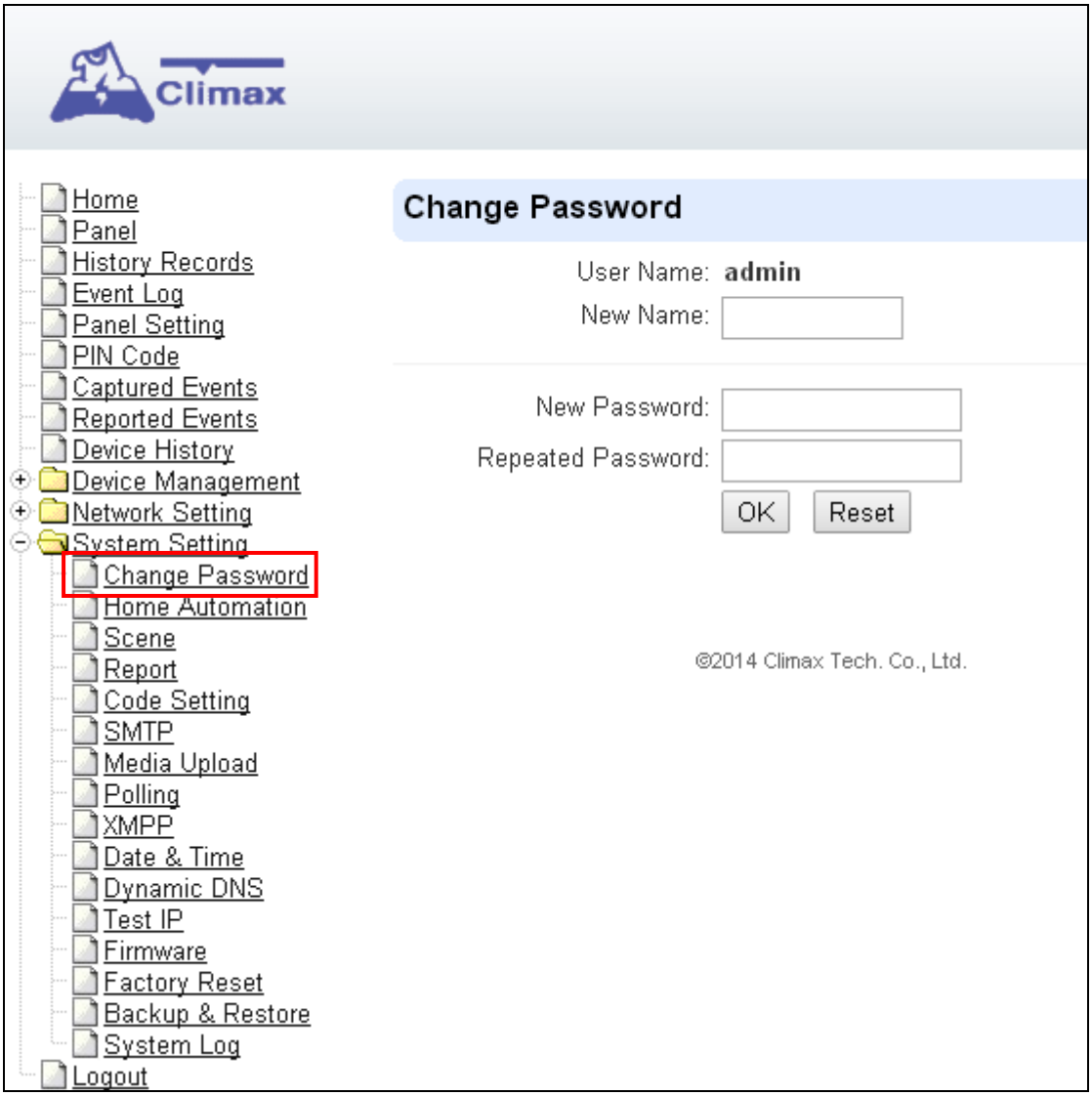
8.1. Administrator Setting

It is used to set new Administrator Log-in Name and Password when accessing this web page.

Please note the Caps for your Log-in Name and Password.

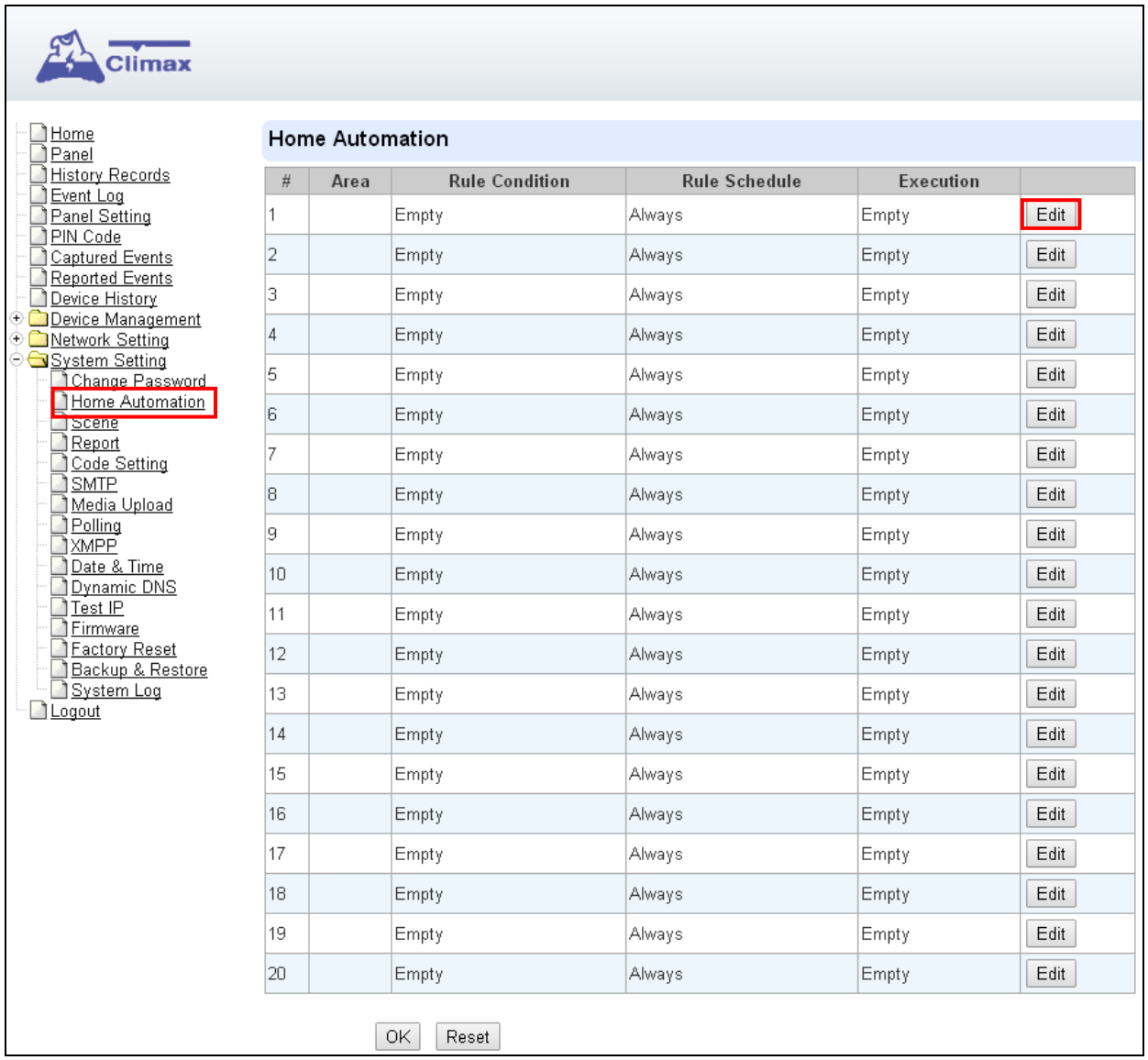
Step 1. Enter the preferred **Login-in Name**.

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 20 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 either Area 1 or Area 2

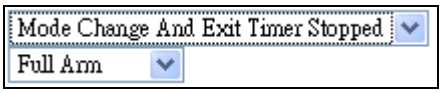
- **Rule Condition**

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

  ☞ ***Trigger Alarm*** : if the rule condition is set as **Trigger Alarm**, when the selected alarm event is triggered as you specify, the system will follow the schedule and execution rule to respond accordingly.

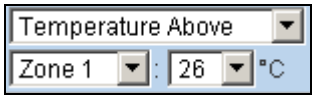
☞ ***Mode Change*** : if the rule condition is set as **Mode Change**, when the system changes to Disarm/ Full Arm/ Home Arm 1/ Home Arm 2/ Home Arm 3, the system will follow the schedule and execution rule to respond accordingly.

☞ ***Mode Change and Exit Timer Stopped*** : if the rule condition is set as **Mode Change and Exit Timer Stopped**, when the system changes to Full Arm/ Home Arm 1/ Home Arm 2/ Home Arm 3, the system will follow the schedule and execution rule to respond accordingly after the Exit Delay Timer expires.

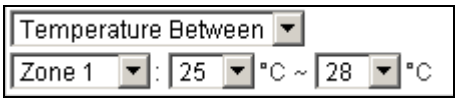


☞ ***Temperature Below*** : if the rule condition is set as **Temperature Below**, when the sensor specified by selecting the zone number, detects the temperature degree below the point that you select , the system will follow the schedule and execution rule to respond accordingly.

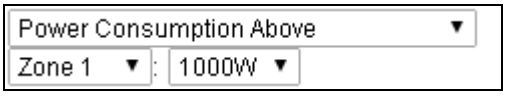
☞ ***Temperature Above*** : if the rule condition is set as **Temperature Above**, when the sensor specified by selecting the zone number, detects the temperature degree above the point that you select , the system will follow the schedule and execution rule to respond accordingly.



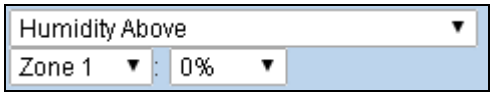
☞ ***Temperature Between*** : if the rule condition is set as **Temperature Between**, when the sensor specified by selecting the zone number detects the temperature degree among the range you speciify , the system will follow the schedule and execution rule to respond accordingly.



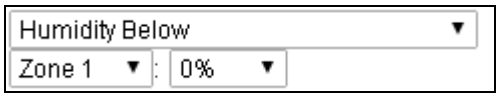
☞ ***High Power Consumption*** : When set as **Power Consumption Above**, if the power output watt from a specific Power Switch exceeds, the rule will be activated according to rule schedule and execution setting.



☞ ***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.



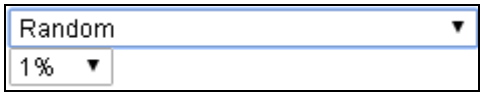
☞ ***Humidity Below*** : When set as **Humidity Below**,if the humidity reading from specified room sensor falls below the level specified, the rule will be activated according to rule schedule and execution setting.



☞ ***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*** : if the rule schedule is set as **Always**, the system will always follow rule schedule to respond accordingly.

☞ ***Schedule Once*** : if the rule condition is set as **Schedule Once**, the system will follow the rule condition and execution rule to respond accordingly for one time on the date and time, that you specifiy.

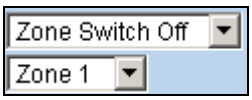
☞ ***Schedule Every Month*** : if the rule condition is set as **Schedule Every Month**, the system will follow the rule condition and execution rule to respond accordingly every month on the date and time, that you specifiy.

☞ ***Schedule Every Week*** : if the rule condition is set as **Schedule Every Week**, the system will follow the the rule condition and execution rule to respond accordingly every week on the date and time, that you specifiy.

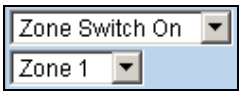
☞ ***Schedule Every Day*** : if the rule condition is set as **Schedule Every Day**, the system will follow the the rule condition and execution rule to respond accordingly every day on the time, that you specifiy.

- **Execution Rule**

☞ ***Zone Switch Off:*** a device in the zone which you specify will be switched off.



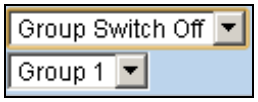
☞ ***Zone Swich On*** : a device in the zone which you specify will be switched on.



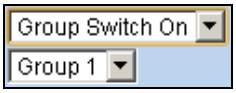
☞ ***Zone Switch Level:***: this function is used for Z-Wave device Dimmer only to control the output percentage.

☞ ***Zone Swich Toggle*** : a device in the zone which you specify will be toggled on/off.

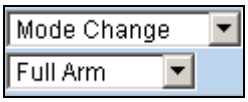
☞ ***Group Switch Off*** : devices belonging to the group selected select will be switched off.



☞ ***Group Switch On*** : devices belonging to the group selected will be switched on.



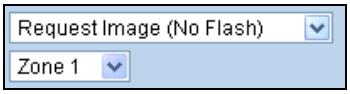
☞ ***Mode Change*** : the system will change to the mode (Disarm/ Full Arm/ Home Arm 1/ Home Arm 2/ Home Arm 3) as you specify.



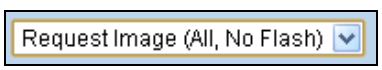
☞ ***Request Image*** : The PIR Camera in specified zone will take a picture.

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

☞ ***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.

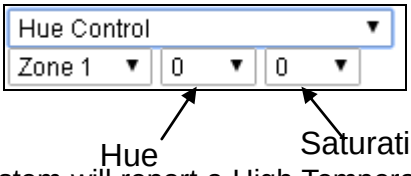


☞ ***Request Video*** : The PIR Video Camera or IP Camera in specified zone will record a video.

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

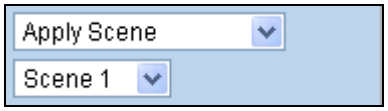
☞ ***Setup UPIC:***: The UPIC and specified zone will transmit Off/Heat/Cool command to the air conditioner as programmed.

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



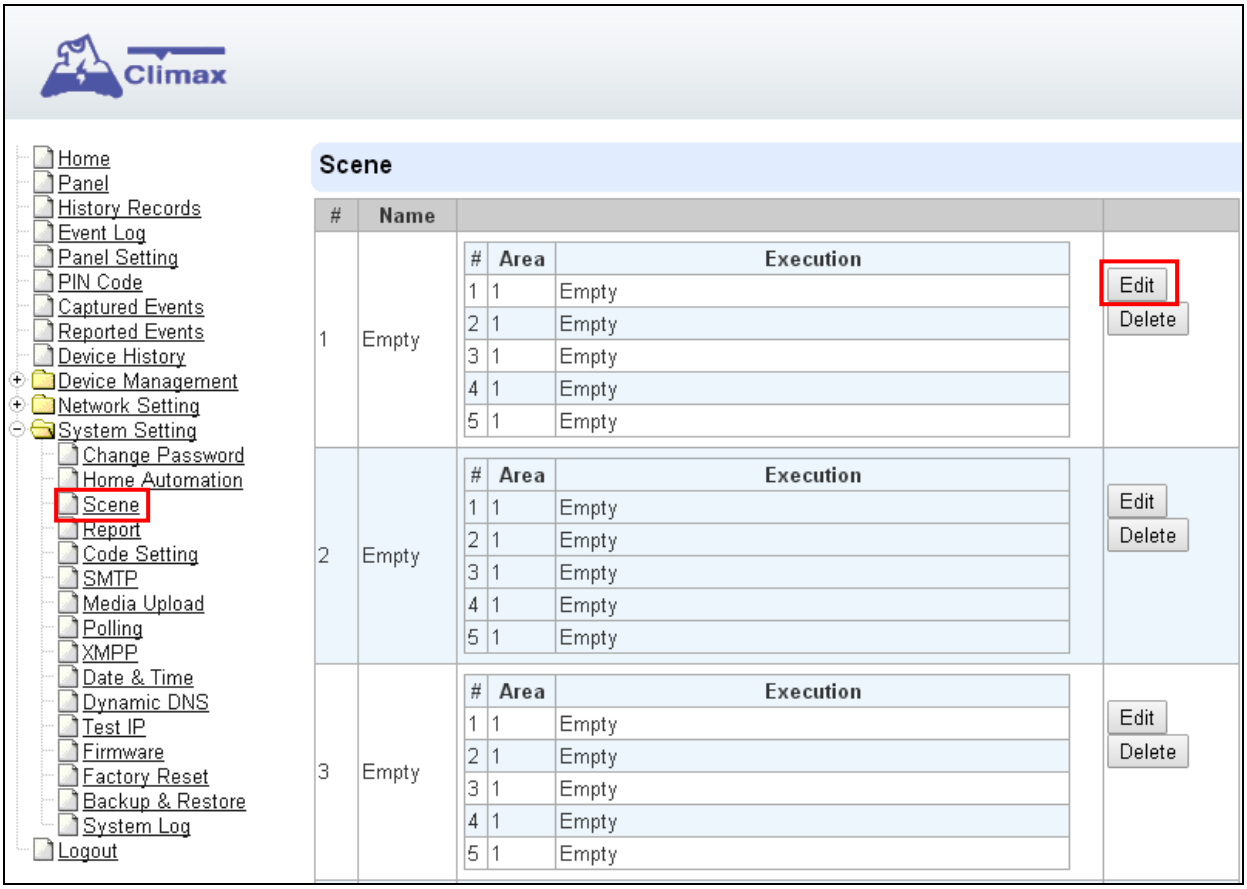
☞ ***Trigger Alarm:***: the system will report a High Temperature Alarm or Low Temperature Alarm.

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

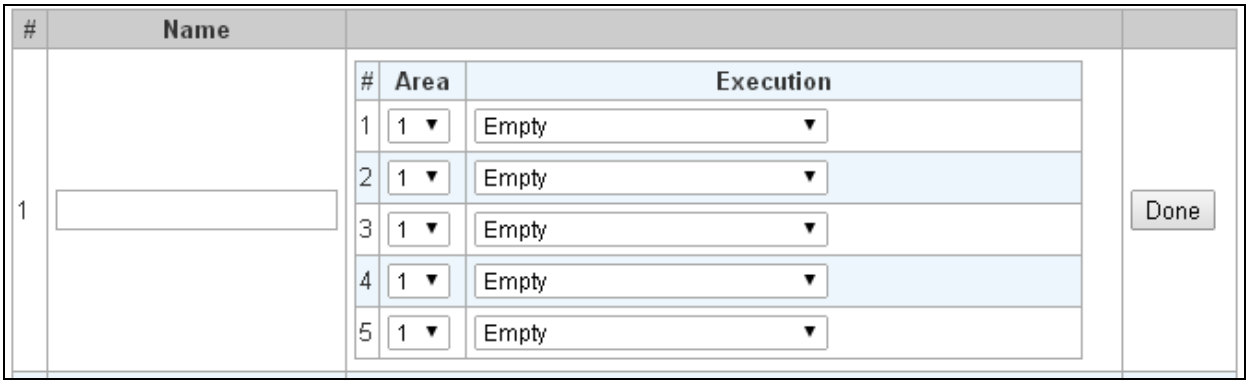


8.3. Scene

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 excuecuted. (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

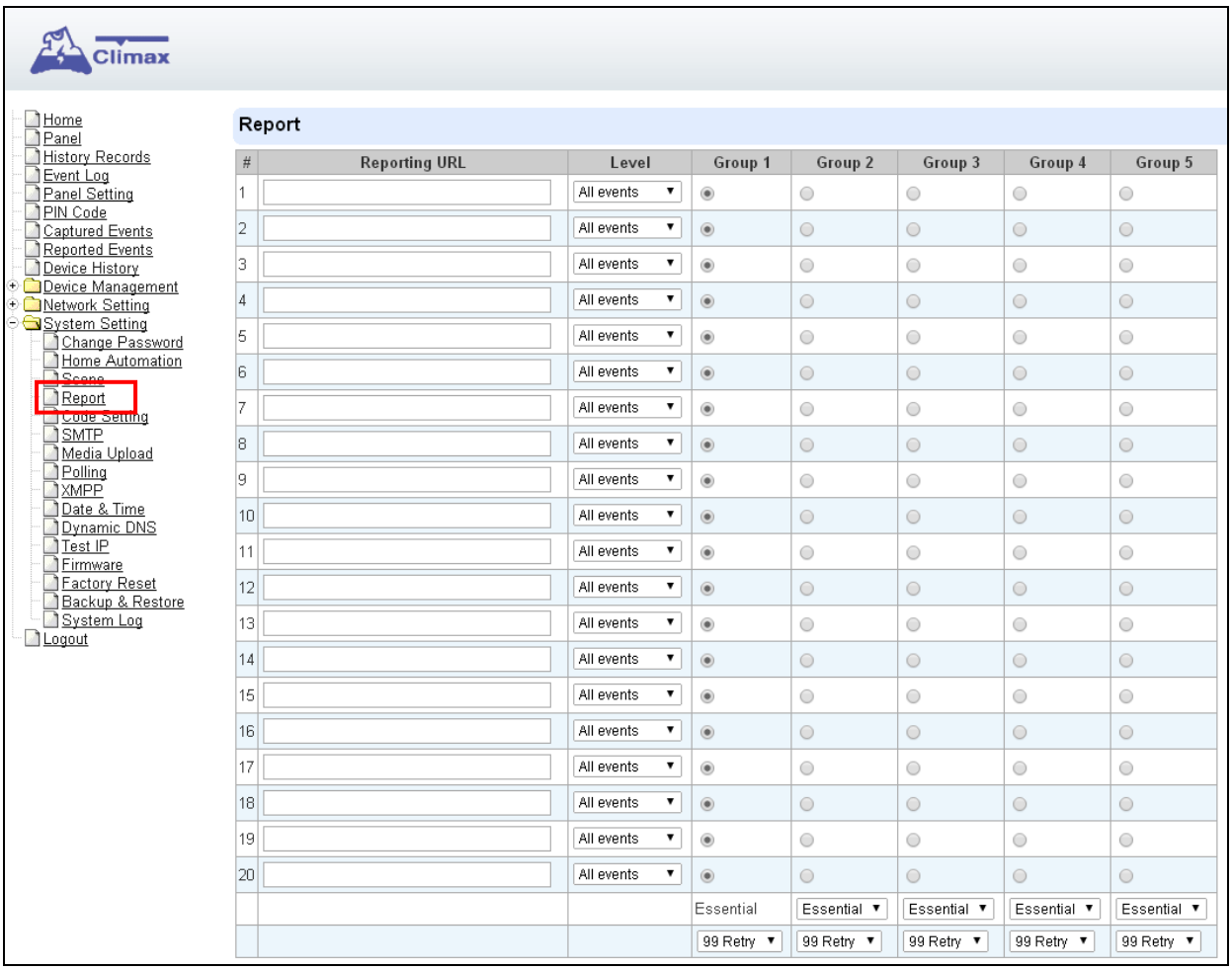
included in one scene.

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/ set all requirements for reporting purposes.

  ☞ Report via IP in CID format:

  ip://Account Number@server ip:port/CID

  ☞ Report via IP in SIA format:

  ip//Account Number @server ip:port/SIA

  ☞ Report via IP in CSV format:

  ip//Account Number @server ip:port/CSV

  ☞ Report via IP in CSV format including user name and password:

  ip//Account Number @server ip:port/CSV/User/Pasword

  <NOTE>

  ☞ Account number is 4 ~ 6 digits.

  ☞ Report via email (Requires SMTP setting)

  mailto: user@example.com

- **Level**

  Select a reporting condition:

All events: the system will report any event to this destination.

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

Status events: the system will only report status event(mode change /fault/auto cheeck-in..) to this destination.

- **Group**

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

  ☞ 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 the reporting 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 any group 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 failes. For example: if Group 3 is set is optional, the Control Panel will only report to Group 3 if reporting to Group 2 fails.

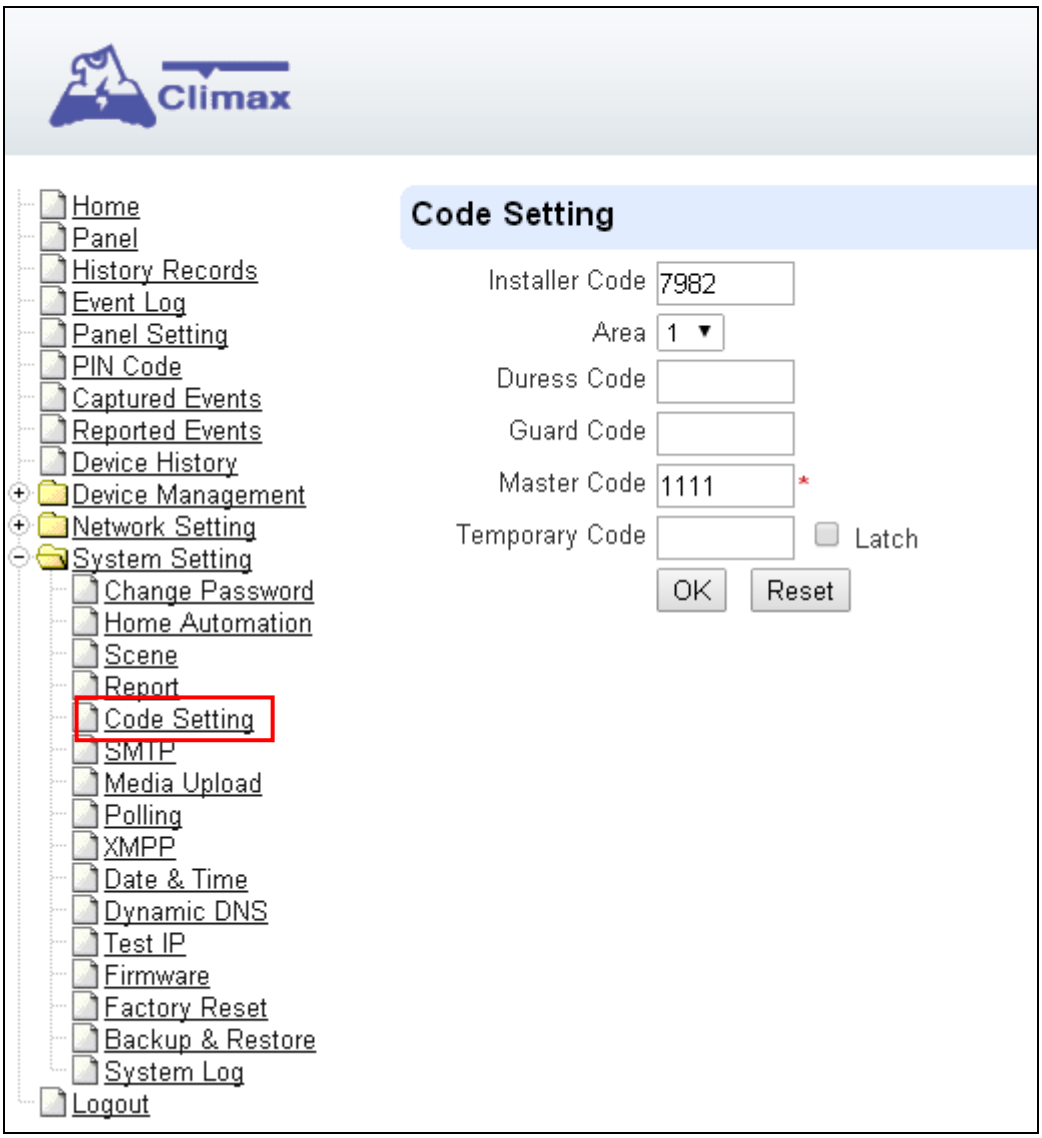
- **1 Retry/ 3 Retry/ 5 Retry/ 10 Retry/ 99 Retry:**

  If the no report destination in a group could be reached, the system will retry the report according to the retries times set here.

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 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**

  This function is currently disabled.

- **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 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 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 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.

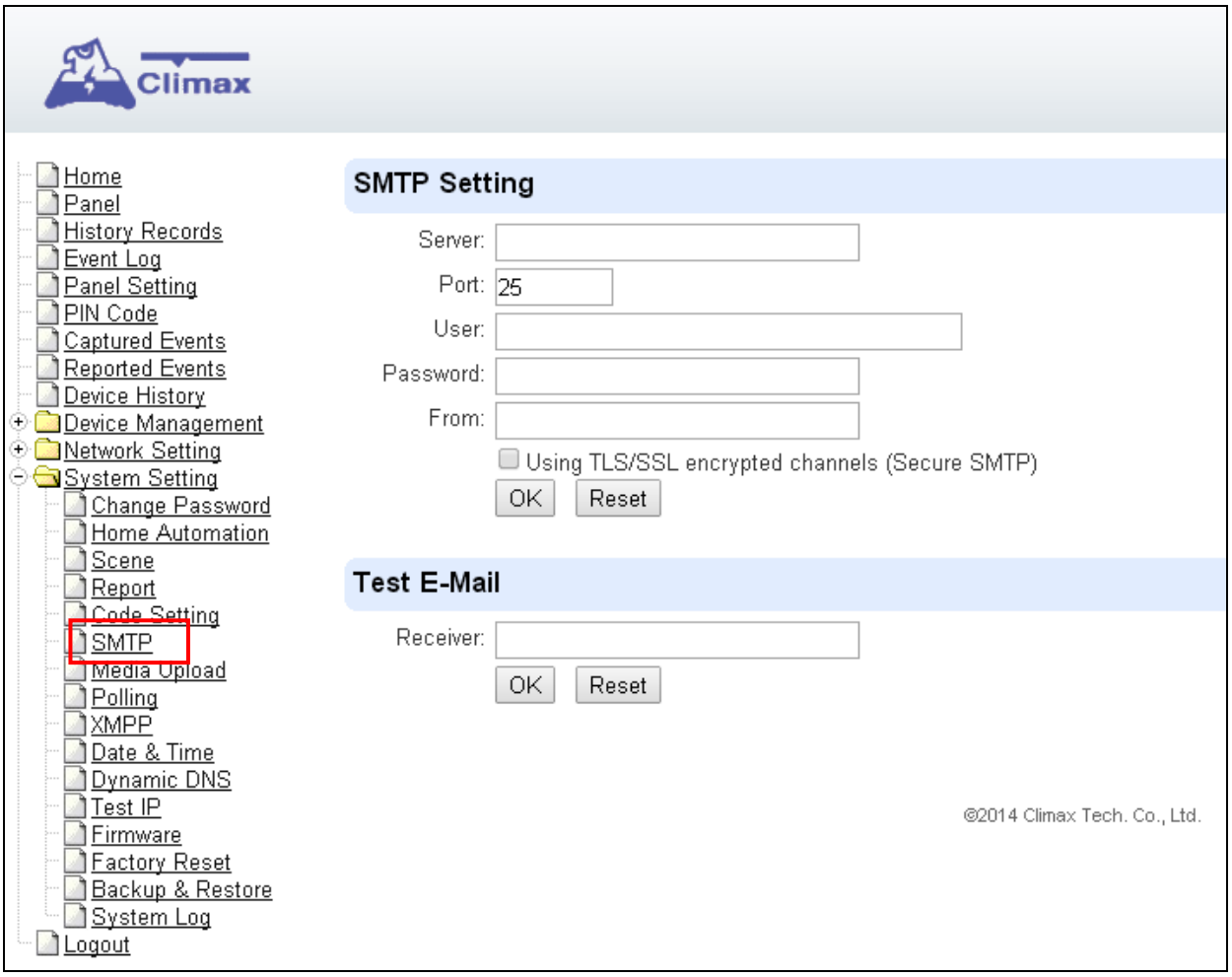
  ☐ Latch → **Latch Reprot OFF** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will NOT transmit reporting(s) to notify the Central Monitoring Station.

- **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



Step 1. Enter the following settings:

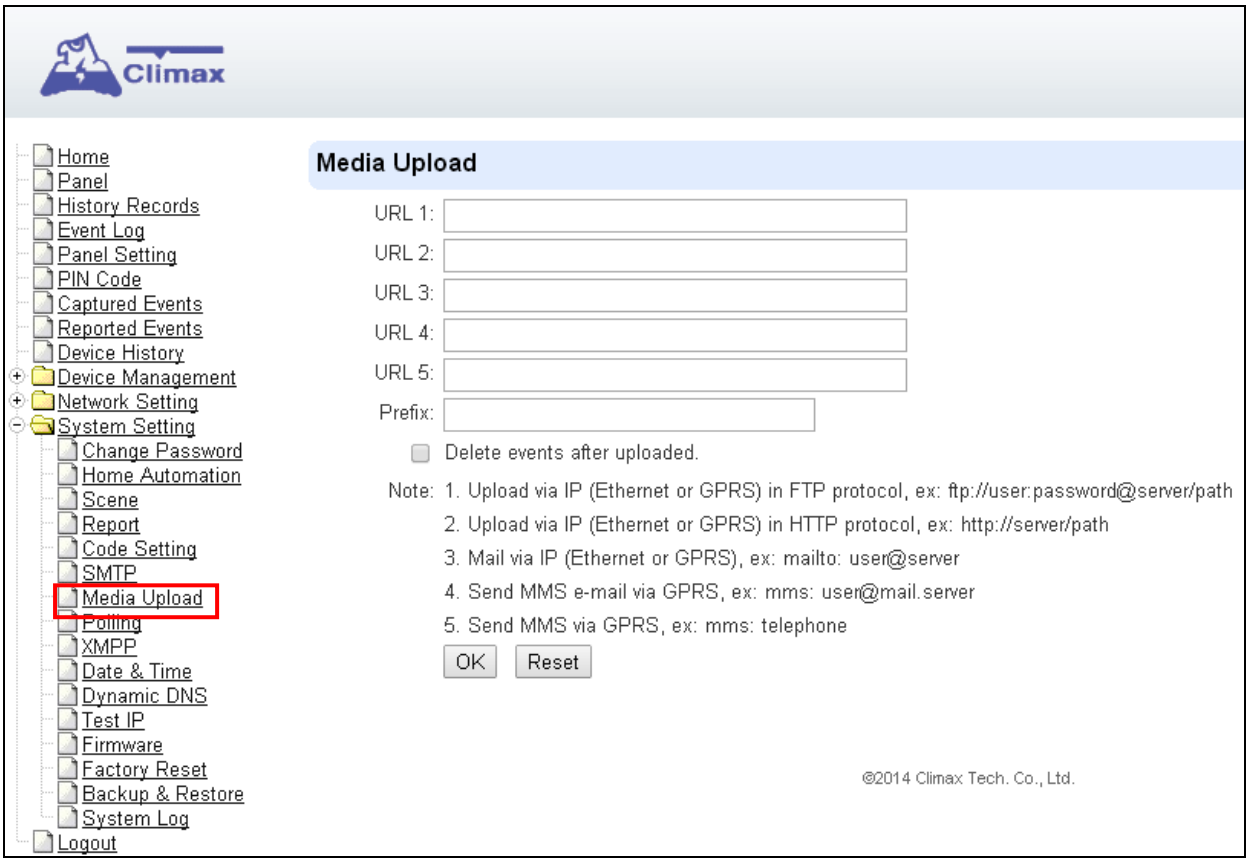
- **Server:** set the mail server (max. 60 digits/alphabets).
- **Port**: set the port number (max. 5 digits/alphabets).
- **User:** set the mail account name (max. 30 digits/alphabets).
- **Password:** set the password corresponding to the mail account name (max. 30 digits/alphabets).
- **From:** set 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.

Step 3. If you want to test the email setting, enter an email account under Test E-mail receiver field and click **OK** to send a test email .

8.7. Media Upload

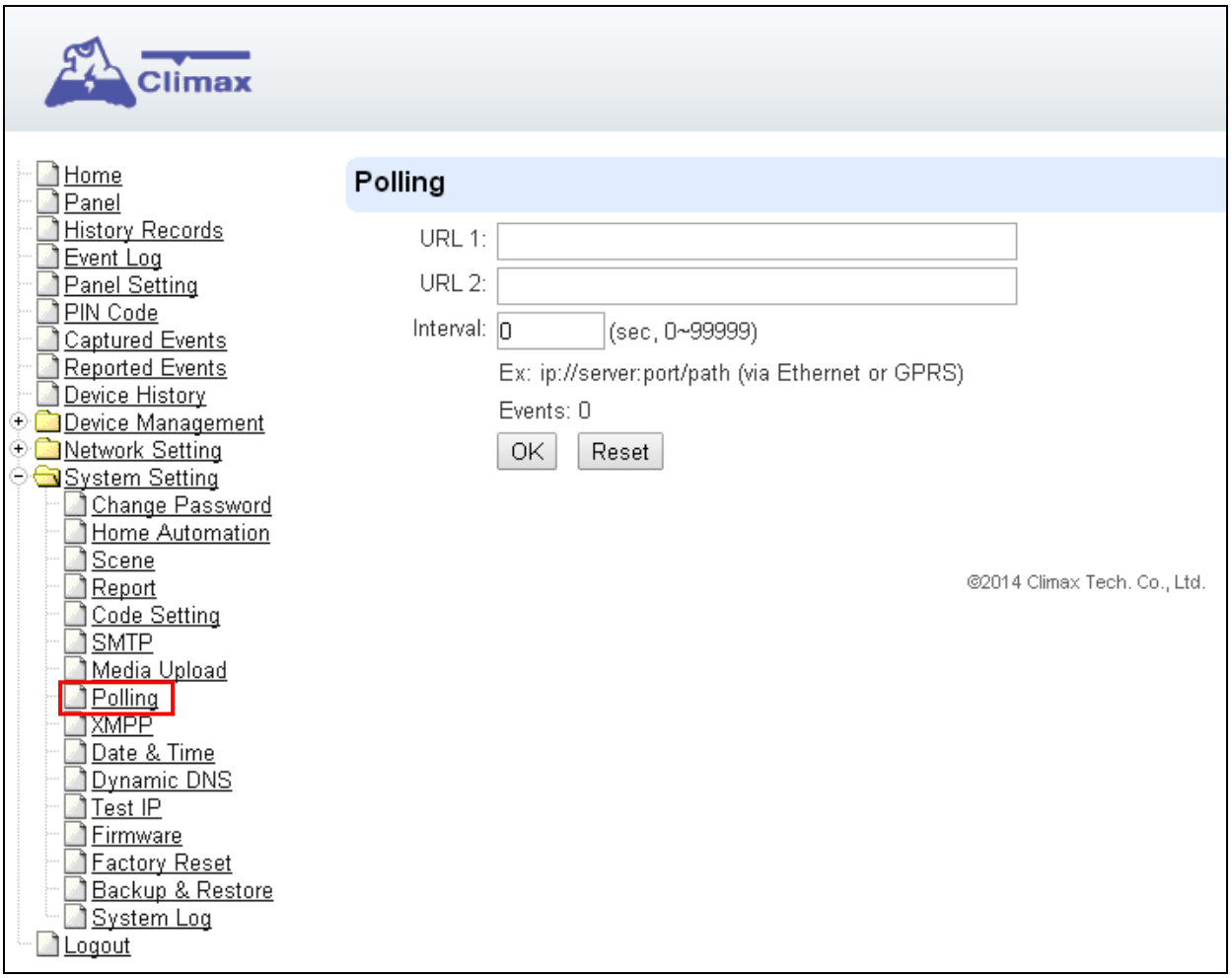
The Media Upload function sets the upload destination for video clips captured by IP Camera.



- **URL 1~5:** Upload destination for the video clips
- **Prefix**: The prefix assigned the file name of captured video clip for you to identify the file.

8.8. Polling

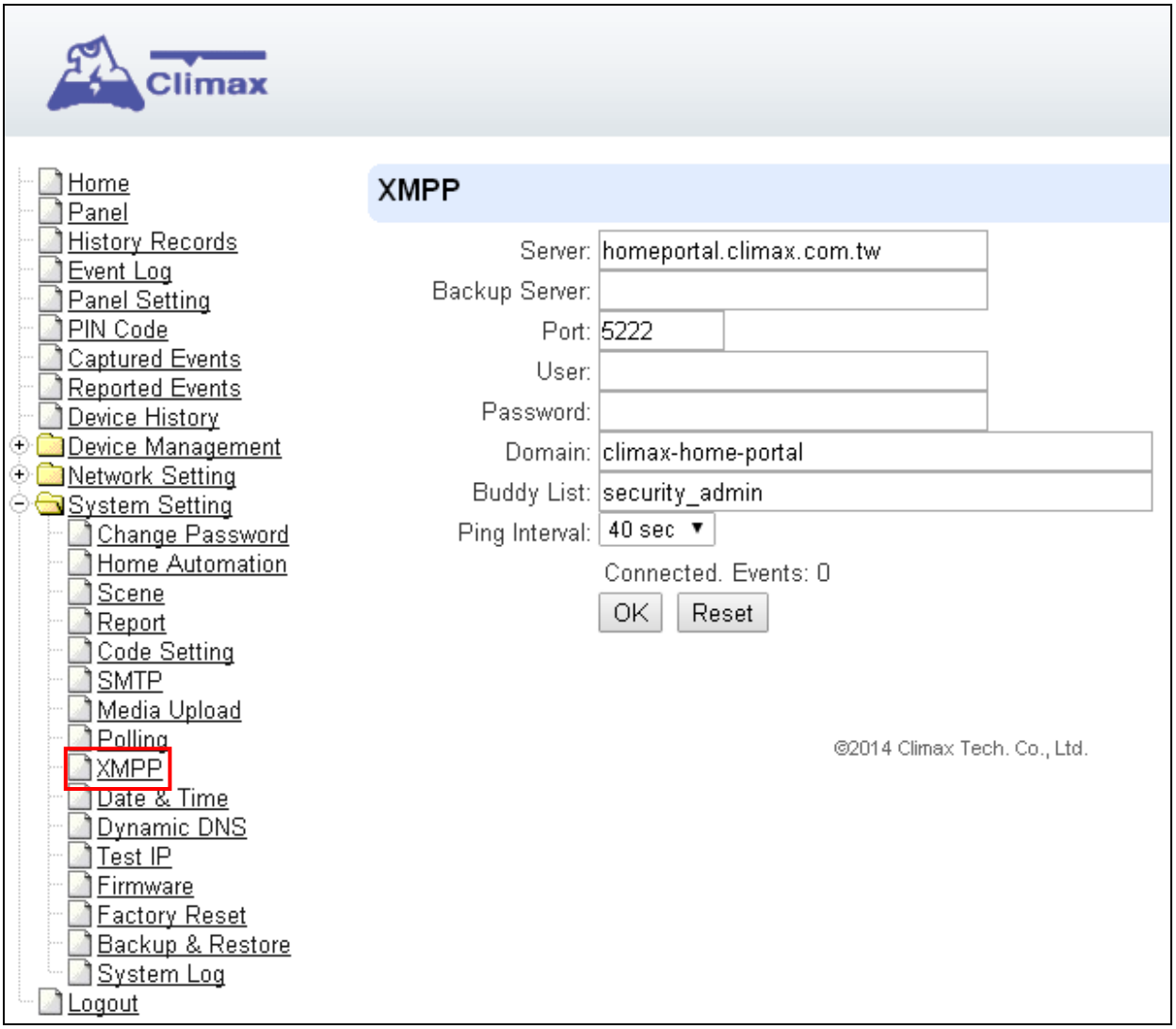
The polling function enables the Control Panel to query the destiation you set (URL1 or URL2) in turn as to whether it has any data to transmit.



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

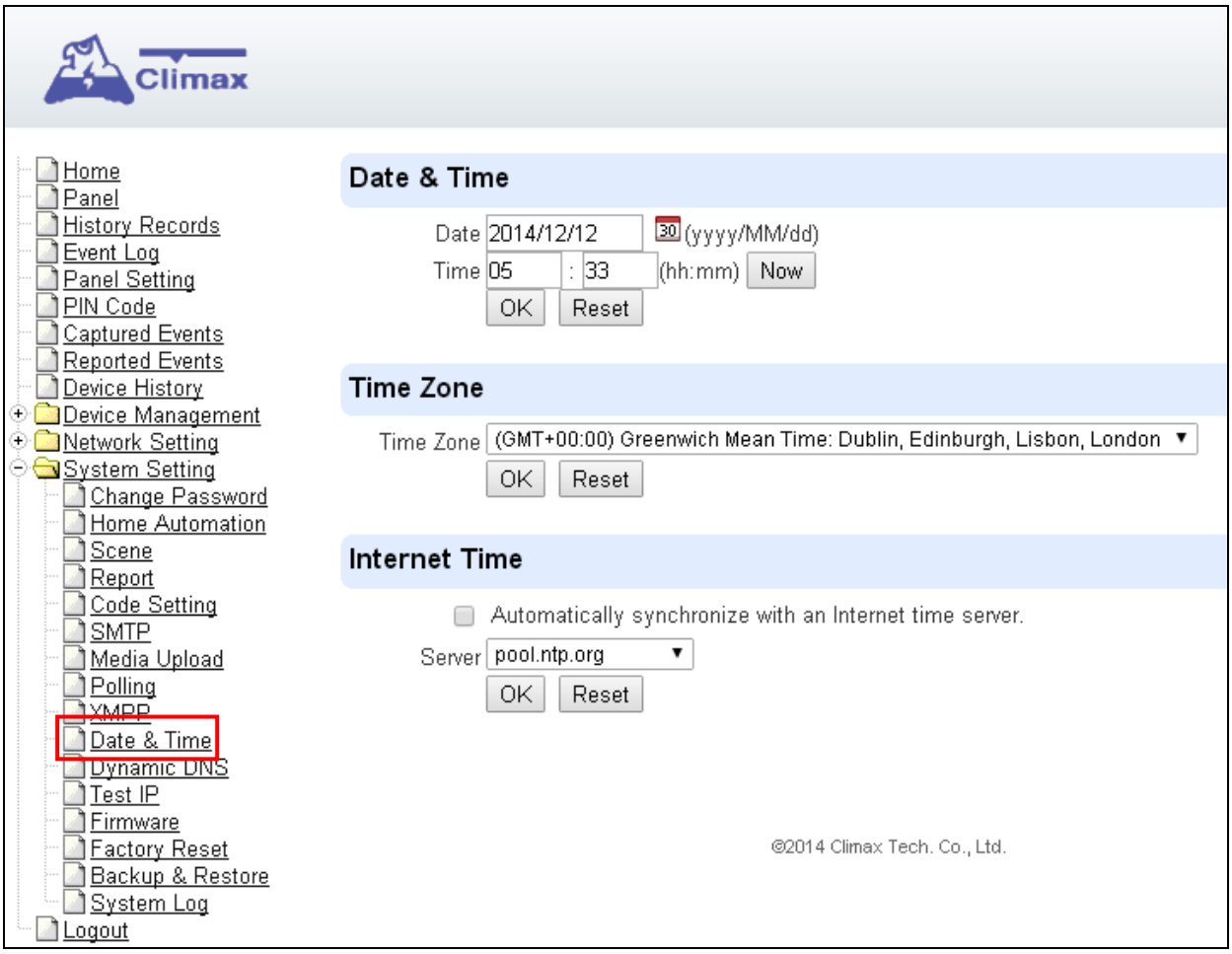
8.9. XMPP

XMPP setting enables the Control Panel to query the set destination. This setting is required for the Control Panel to connect to server for further remote control.



8.10. Date & Time

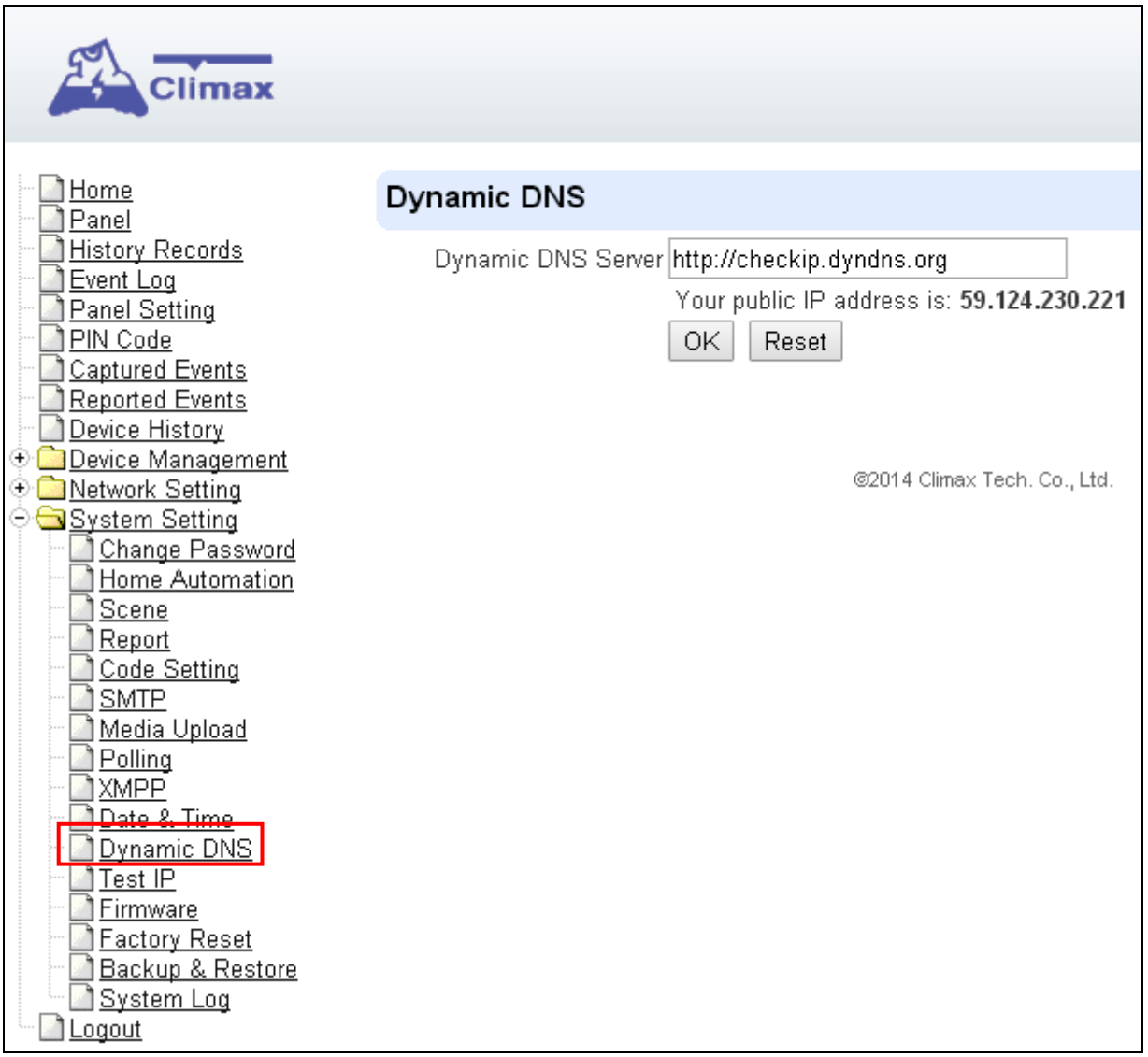
Program the current **Date** & **Time**. Normally this will automatically synchronize with Network Time Server with a valid internet connection.



- **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: pool.ntp.gov, time.nist.gov and tick.usno.navy.mil.

8.11. Dynamic DNS

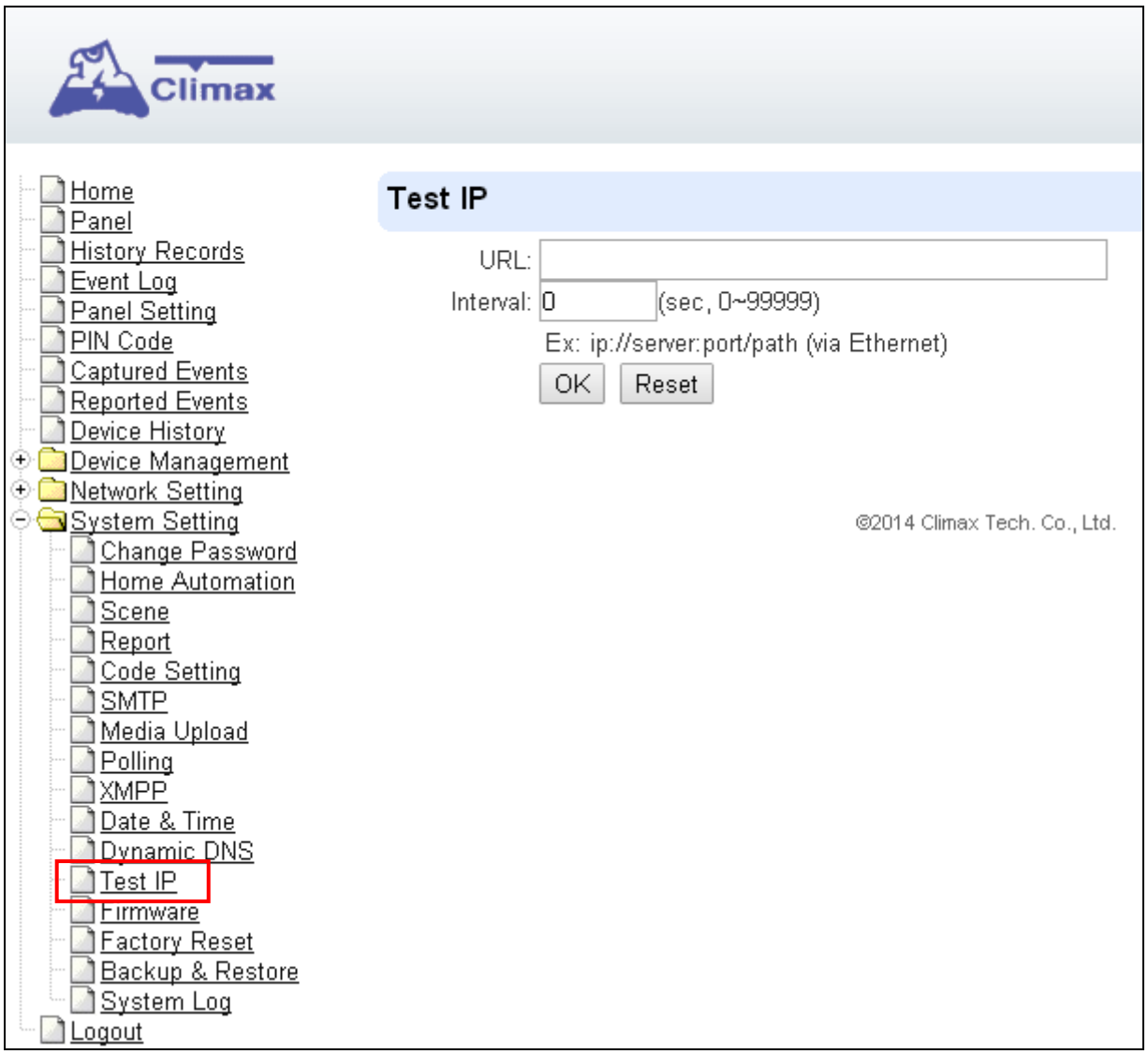
It is used to get your real public IP address on the internet.



- **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.

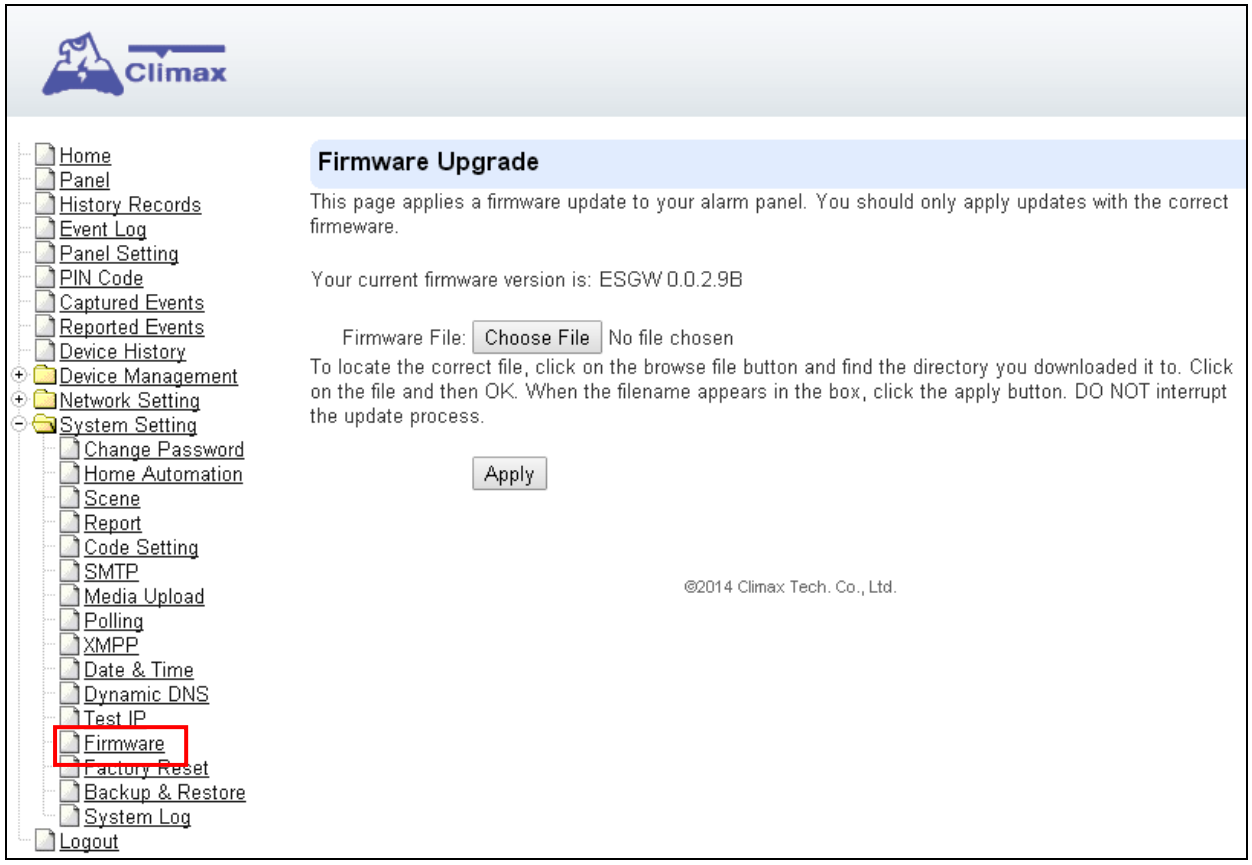
Step 3. Click “OK”

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. It will takes about 2~5 mins to load the file onto the Control Panel.

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

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

8.14. 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 data & IP values will returned to its default value, and all the learnt-in devices will be removed. You have to reprogram and learn in the device one by one again.

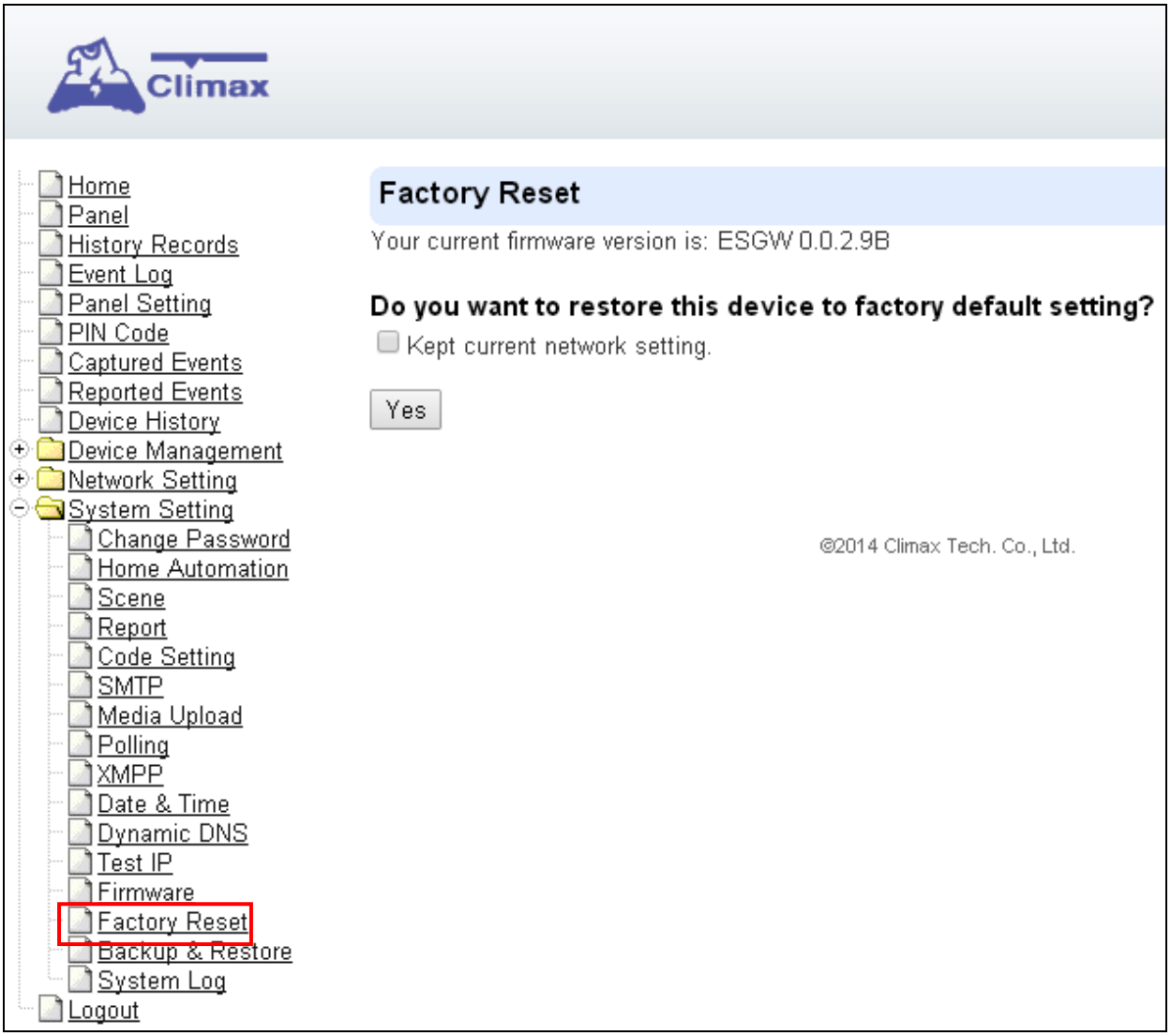
Remote Reset

Step 1. Tick the **Kept current network setting** box to keep the current Network settings. 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.

Step 2. Press and hold the Function Button at top of Control panel and connect the AC adaptor to the Control Panel. DO NOT release the Function Button.

Step 3. Keep holding the Function Button for about 45 seconds until all LEDS flashes 3 times.

Step 4. Release the Function Button and wait for the Control panel to reboot.

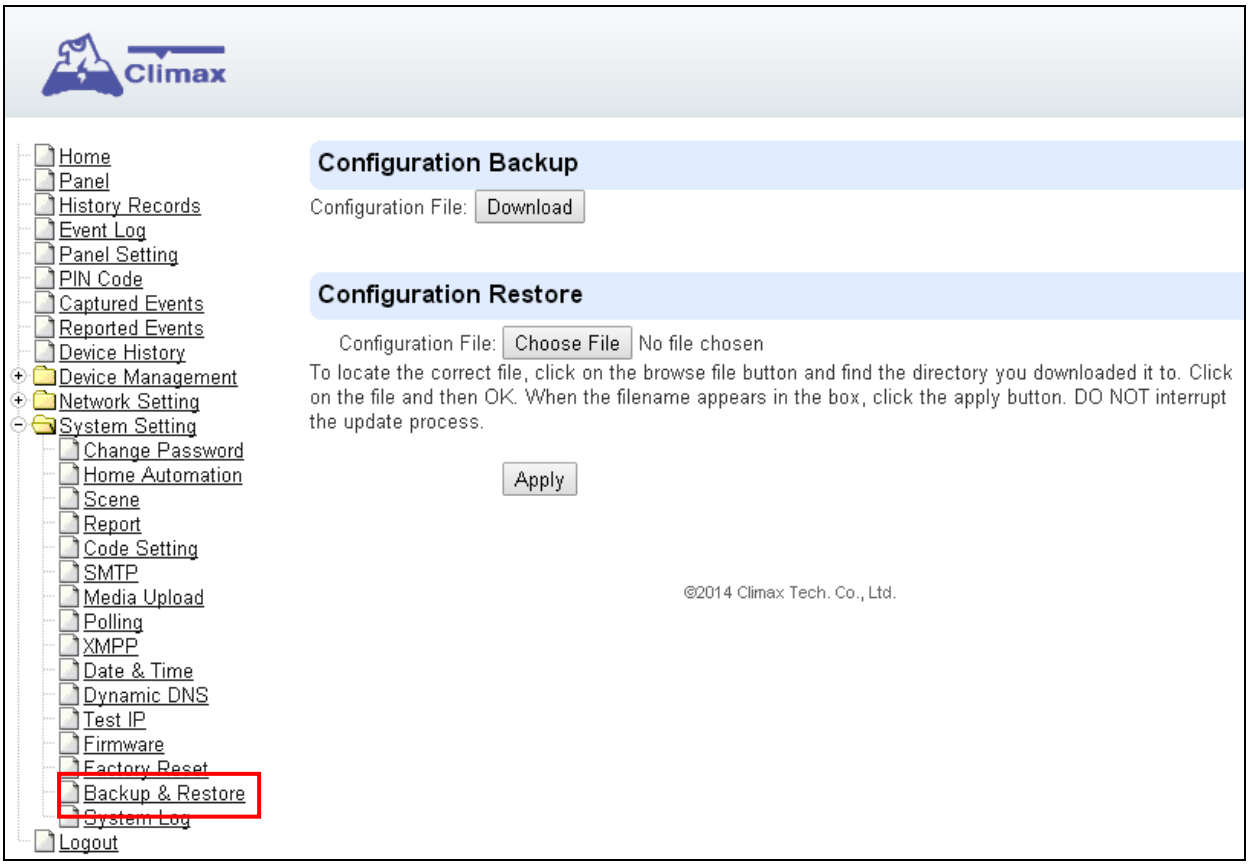
8.15. Backup & Restore

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

8.15.1 Backup Data

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

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



Step 2. A **.bin** file will be downloaded into your computer containing the panel's setting information..

8.15.2 Restore Settings

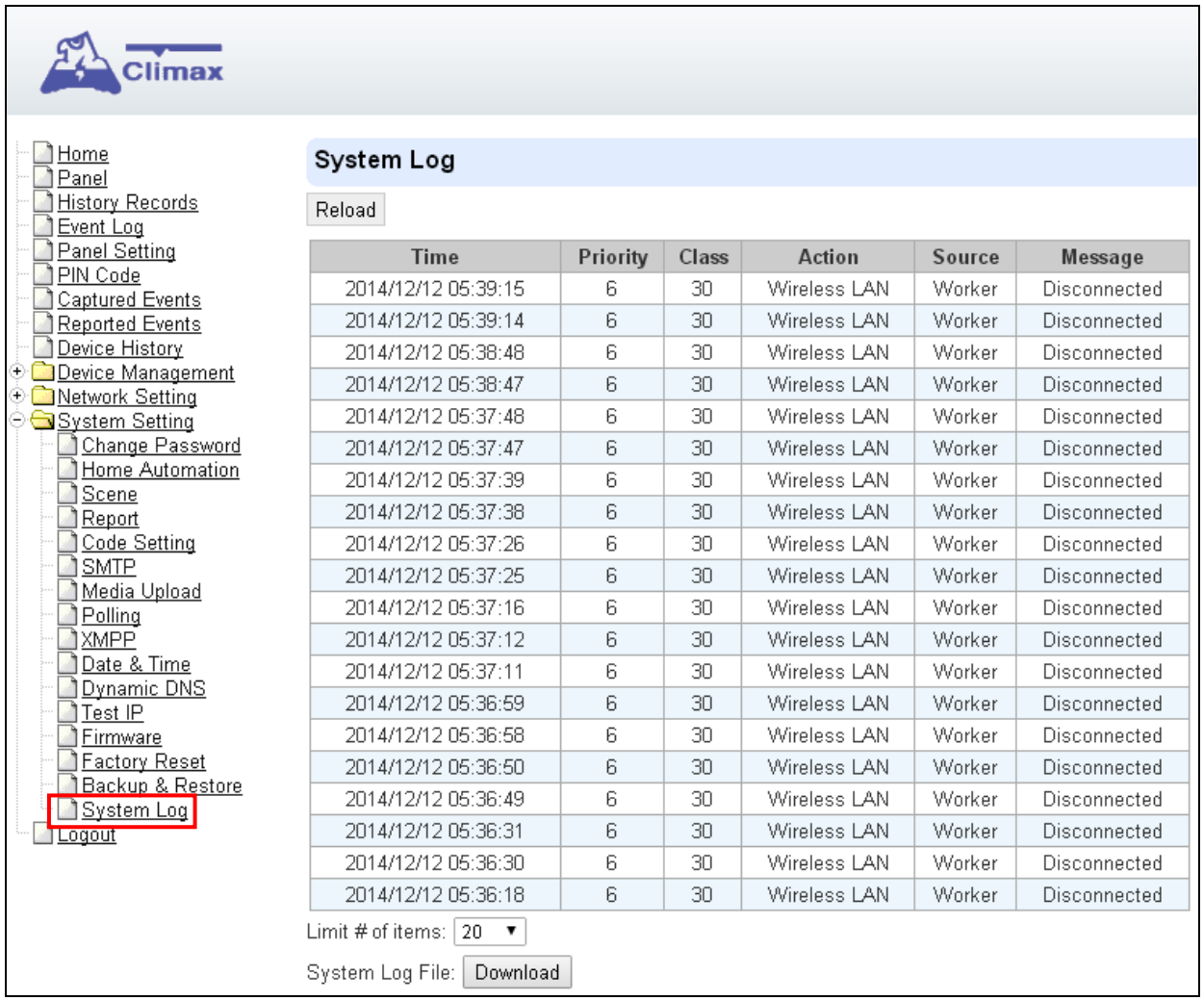
Step 1. Select a downloaded **.bin** file.

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

.

8.16. System Log

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



Time	Priority	Class	Action	Source	Message
2014/12/12 05:39:15	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:39:14	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:38:48	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:38:47	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:48	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:47	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:39	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:38	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:26	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:25	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:16	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:12	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:37:11	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:59	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:58	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:50	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:49	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:31	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:30	6	30	Wireless LAN	Worker	Disconnected
2014/12/12 05:36:18	6	30	Wireless LAN	Worker	Disconnected

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

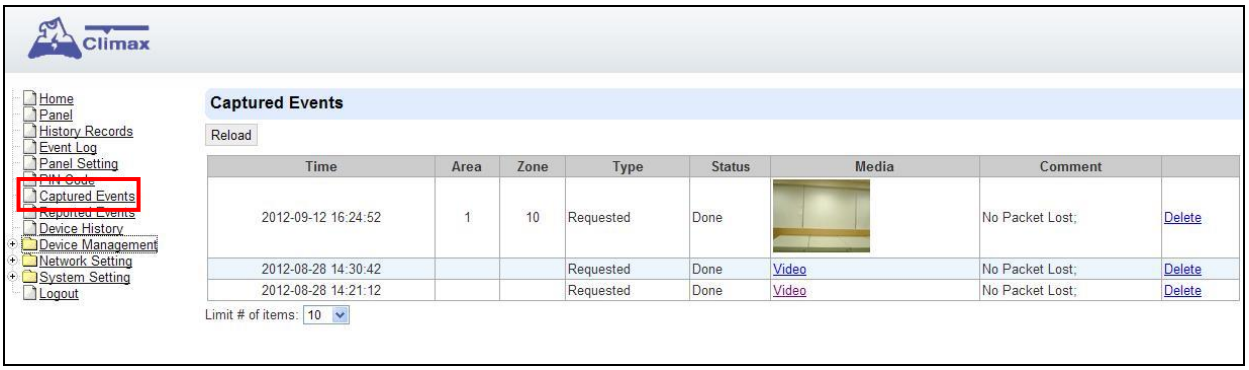
9. Event & History

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.

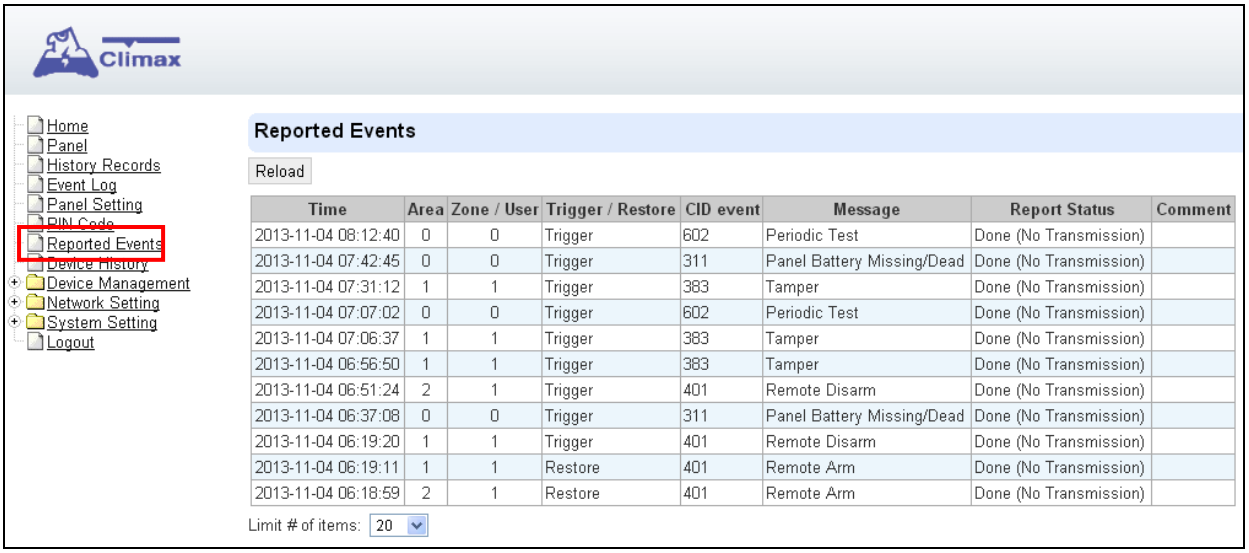
Caputred events will be displayed in this page with their information for you to view. Simply click on the picture or video to view them. You can also click **Delete** to delete the event.



- **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.

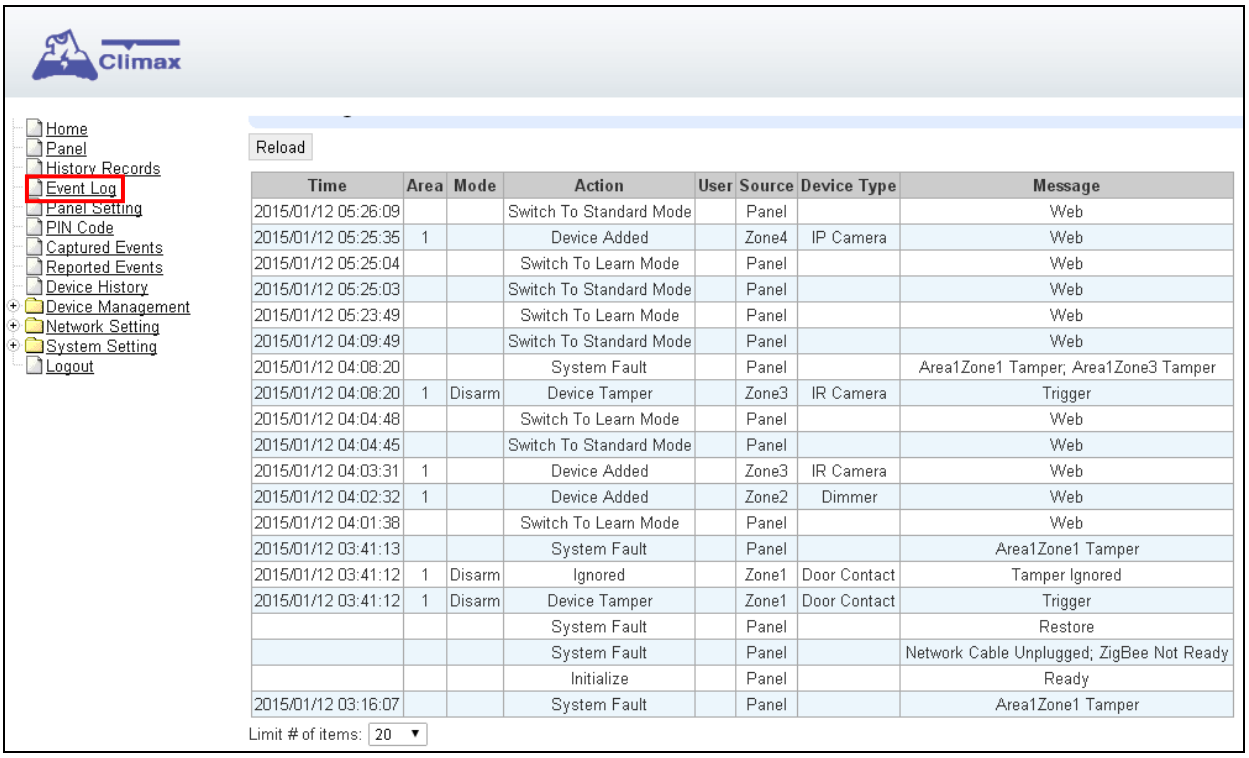


Time	Area	Zone / User	Trigger / Restore	CID event	Message	Report Status	Comment
2013-11-04 08:12:40	0	0	Trigger	602	Periodic Test	Done (No Transmission)	
2013-11-04 07:42:45	0	0	Trigger	311	Panel Battery Missing/Dead	Done (No Transmission)	
2013-11-04 07:31:12	1	1	Trigger	383	Tamper	Done (No Transmission)	
2013-11-04 07:07:02	0	0	Trigger	602	Periodic Test	Done (No Transmission)	
2013-11-04 07:06:37	1	1	Trigger	383	Tamper	Done (No Transmission)	
2013-11-04 06:56:50	1	1	Trigger	383	Tamper	Done (No Transmission)	
2013-11-04 06:51:24	2	1	Trigger	401	Remote Disarm	Done (No Transmission)	
2013-11-04 06:37:08	0	0	Trigger	311	Panel Battery Missing/Dead	Done (No Transmission)	
2013-11-04 06:19:20	1	1	Trigger	401	Remote Disarm	Done (No Transmission)	
2013-11-04 06:19:11	1	1	Restore	401	Remote Arm	Done (No Transmission)	
2013-11-04 06:18:59	2	1	Restore	401	Remote Arm	Done (No Transmission)	

- **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.

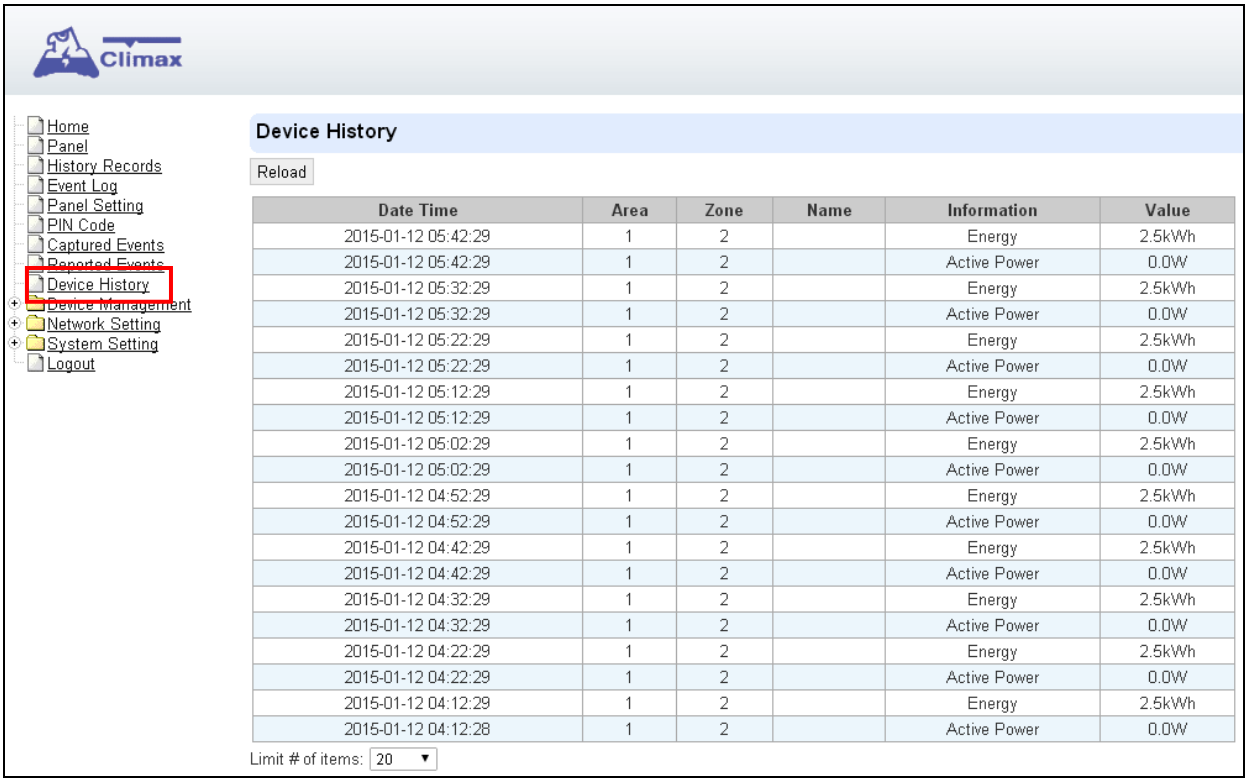


Time	Area	Mode	Action	User	Source	Device Type	Message
2015/01/12 05:26:09			Switch To Standard Mode		Panel		Web
2015/01/12 05:25:35	1		Device Added		Zone4	IP Camera	Web
2015/01/12 05:25:04			Switch To Learn Mode		Panel		Web
2015/01/12 05:25:03			Switch To Standard Mode		Panel		Web
2015/01/12 05:23:49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

The Control Panel communicates with Central Station receiver by using Contact-ID protocol.

The form of the message is:

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	

10.2. Event Code

- **100 – Medical**
- **101 – Personal emergency**
  - When the Wrist Transmitter (WTR) or Emergency Pendant (EP) is pressed.
- **110 – Fire**
- **111 – Smoke**
  - When the Smoke Detector (SD) is triggered.
- **114 – Heat**
  - When a Heat Detector is triggered.
  - When a Door Contact set as **Heat** is triggered.
- **120 – Panic**
  - When the Panic Button of the Remote Controller (RC) is pressed.
- **121 – Duress**
  - When the Duress Code is entered to disarm or arm the system.
- **122 –Silent Panic**
  - When the Panic Button of the Remote Controller 、WTR is pressed.
- **130 – Burglar**
  - When a device whose attribute is set as **Burglar** or **Burglar Follow** is triggered.
- **131 – Burglar Perimeter**
  - When a device set as **Entry** is triggered in the arm mode.
- **132 – Burglar Interior**
  - When a device set at **Entry** is triggered in the home mode.
- **136 – Burglar Outdoor**
  - When any 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.
- **147 – Sensor Supervision Failure/ Sensor Supervision Restore**
  - When the control panel can't receive the signal transmitted from any one of the devices individually for a preset time.
  - When the supervision function of sensor is restored.
- **151 – Gas**
  - When a Door Contact set at **Heat** is triggered.
- **154 – Water leakage**
  - When a Water Sensor is triggered
  - When a Door Contact set at **Wate**r is triggered.
- **158 – High Temperature Alarm**
  - When high temperature alarm is triggered

- **159 – Low Temperature Alarm**
  - When low temperature alarm is triggered
- **162 – CO detector**
- **344 – Interference / Interference Restore**
- **374 – Force Arm**
  - When “Arm Fault Type” in Panel Setting is set to “Confirm” and the panel is armed with existing fault event by confirming the arming action.
- **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 the battery voltage of any one of the devices is low.
  - When any device’s battery restores voltage.
- **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 - Bypass**
  - When “Arm Fault Type” in Panel Setting is set to “Direct” and the panel is armed with existing fault events.
- **602 – Periodic test report**
  - When the control panel makes periodic Check-in reporting.