



SECURING YOUR WORLD

USER MANUAL

VP360MPOE

Contents

Chapter 1	Device Connection	5
Chapter 2	Web Login	5
Chapter 3	Dashboard	6
Chapter 4	Device Settings	9
4.1	Device Info	9
4.2	System Time	9
4.3	Firmware Upgrade	10
4.4	Configuration	11
4.5	IP Address	12
4.6	WiFi Configuration	12
4.7	RTSP Settings	12
4.8	Function Testing	13
Chapter 5	User Management	14
Chapter 6	Resources	14
6.1	RTSP Logo / Resource	14
6.2	Audio Files	15
6.3	LED (Color & Pattern)	16
6.4	Email Template	16
Chapter 7	Alarm Settings	17
7.1	Event Settings	17
7.2	Action Settings	18
Chapter 8	Platform Integration	19
8.1	TCP / MQTT	19
8.2	HTTP	20
8.3	Heartbeat	21
8.4	SMTP (Email)	21
Chapter 9	History	24
9.1	Data Log	24
9.2	Event Log	24
Chapter 10	Installation	25
10.1	Pendant Mount	25
10.2	Ceiling / Surface Mount	26
Chapter 11	Important Notes	31
11.1	Power Supply	32
11.2	TVOC Sensor	32
11.3	Maintenance	32
11.4	Testing	32
11.5	Monitoring Area	32

Chapter 1 Device Connection

The VP360MPOE is a Power-over-Ethernet air-quality and vape detector. Before configuration, connect the unit to your network and locate it on the local segment.

The detector ships with DHCP enabled, so it requests an address automatically the moment it is powered. Follow the steps below to bring it online and open its web interface.

1. Connect the VP360MPOE to a PoE switch. Once power is applied, the detector obtains an IP address from your DHCP server automatically.
2. Your computer need to be connected in the same network segment, 192.168.1.100.

NOTE Your computer must reside on the same network segment as the detector. If the VP360MPOE is at 192.168.1.100, your PC must use an address in the 192.168.1.x range before the web interface will load.

Chapter 2 Web Login

Sign in to the web interface with the factory credentials: user name **admin** and password **111111**.

For security, the interface requires you to replace the default password on first login. Enter a new password when prompted and click **Confirm** to save it.

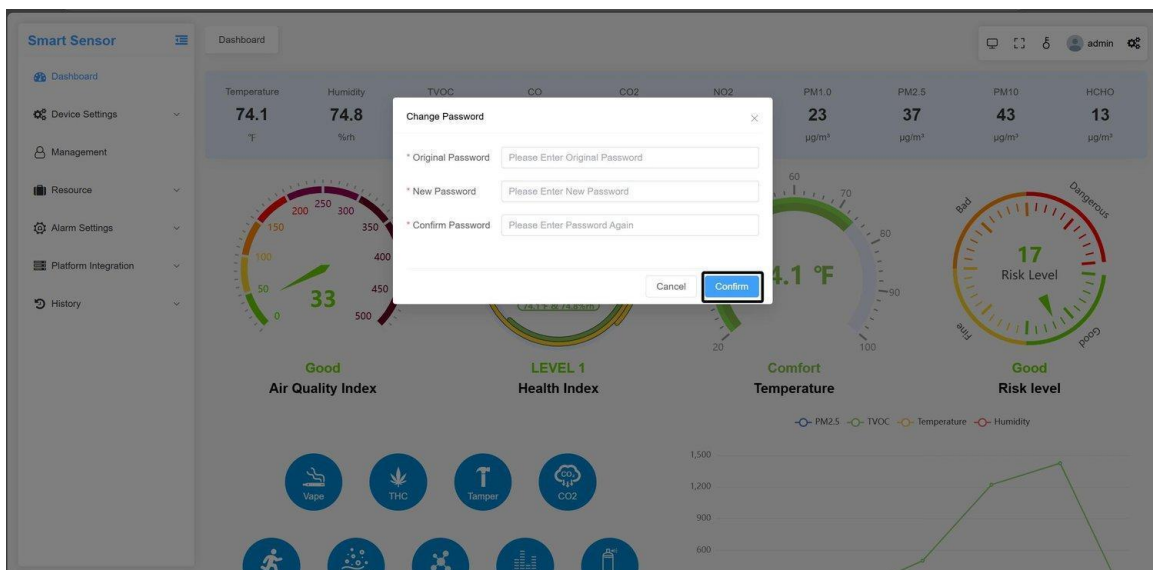


Figure 2-1. The mandatory change-password prompt presented the first time you sign in.

TIP Record the new password in a safe place. It is required for every subsequent login and for access to the configuration pages.

Chapter 3 Dashboard

The dashboard is the detector's home page. It presents live readings from every built-in sensor alongside the current event and risk status.

The following sensors report their real-time and reference values on the dashboard:

- Temperature and humidity
- TVOC
- CO
- CO2
- NO2
- PM1.0, PM2.5, and PM10
- HCHO
- Tamper sensor
- Motion sensor

The dashboard also summarizes event status for Vape/THC, Tamper, CO2, Motion, PM2.5, TVOC, Sound, Masking, AQI, HI, and Temperature, together with an overall Risk Level.



Figure 3-1. The live dashboard, presenting AQI, Health Index, temperature, risk level, and the individual sensor gauges.

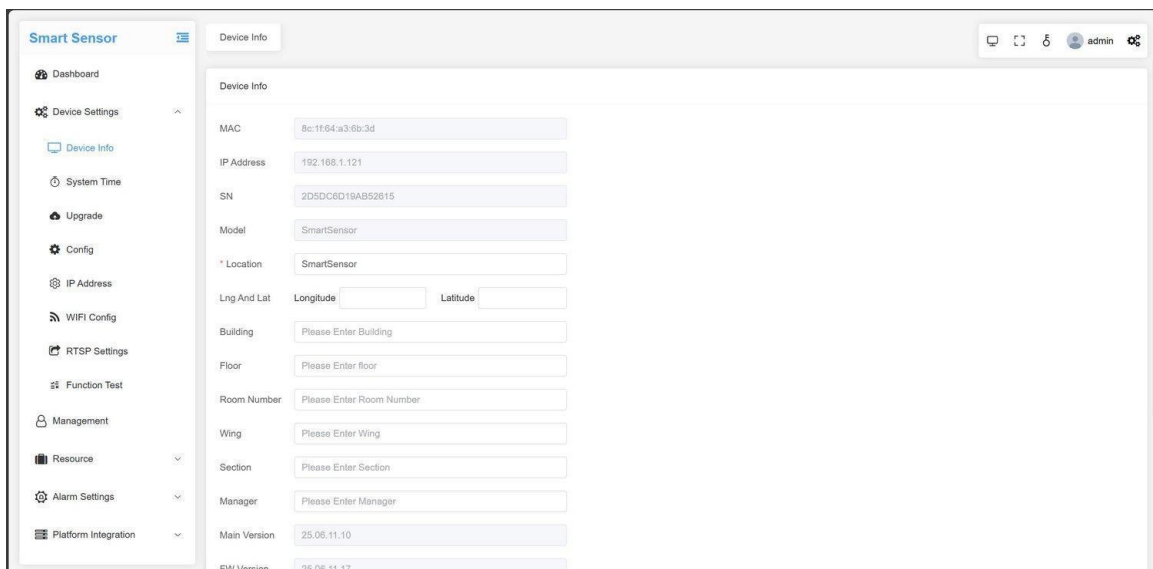
NOTE Each event indicator is shown as a blue icon under normal conditions. When an event is detected, the corresponding icon turns yellow or red to draw attention to the change.

Chapter 4 Device Settings

The Device Settings pages cover identification, timekeeping, firmware, network, and hardware verification for the VP360MPOE.

4.1 Device Info

Use this page to describe the detector in detail, which makes it easier to recognize where each unit is installed.



The screenshot shows the 'Smart Sensor' web interface. On the left is a sidebar menu with options: Dashboard, Device Settings (expanded), Device Info (selected), System Time, Upgrade, Config, IP Address, WIFI Config, RTSP Settings, Function Test, Management, Resource, Alarm Settings, and Platform Integration. The main content area is titled 'Device Info' and contains the following fields: MAC (8c:1f:64:a3:6b:3d), IP Address (192.168.1.121), SN (2D5DC6D19AB52615), Model (SmartSensor), Location (SmartSensor), Longitude and Latitude (empty), Building (Please Enter Building), Floor (Please Enter floor), Room Number (Please Enter Room Number), Wing (Please Enter Wing), Section (Please Enter Section), Manager (Please Enter Manager), Main Version (25.06.11.10), and FW Version (25.06.11.17). The 'Location' field is highlighted with a red box.

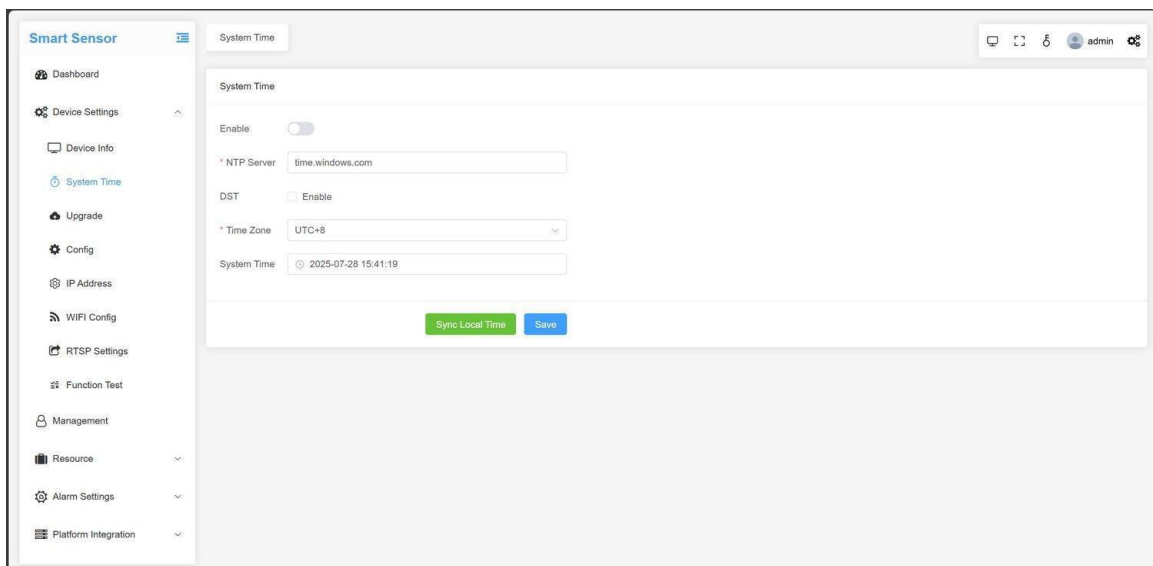
Figure 4-1. The Device Info page, where descriptive details such as name and location are entered.

TIP The value you enter in **Location** is overlaid on the RTSP video stream. This usually lets you identify a detector from the video alone, without opening its web interface again.

4.2 System Time

After installation, set the detector's time zone so its clock matches the rest of your local network. Accurate time keeps logs and event records consistent across devices.

The default NTP server is **time.windows.com**. Daylight saving time (DST) is supported for the USA and Canada.



The screenshot shows the 'Smart Sensor' web interface. On the left is a sidebar menu with options: Dashboard, Device Settings (expanded), Device Info, System Time (selected), Upgrade, Config, IP Address, WIFI Config, RTSP Settings, Function Test, Management, Resource, Alarm Settings, and Platform Integration. The main content area is titled 'System Time' and contains the following fields: Enable (toggle switch), NTP Server (time.windows.com), DST (Enable checkbox), Time Zone (UTC+8 dropdown), and System Time (2025-07-28 15:41:19). The 'NTP Server' field is highlighted with a red box. At the bottom are 'Sync Local Time' and 'Save' buttons.

Figure 4-2. The System Time page, showing NTP server and time-zone selection.

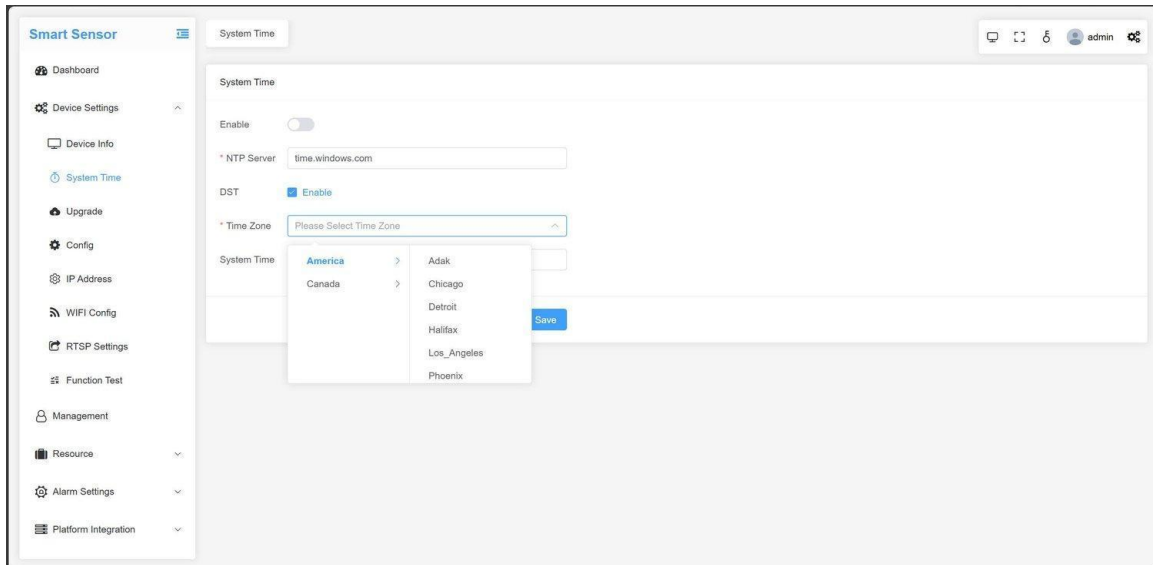


Figure 4-3. Daylight saving time options for the USA and Canada.

4.3 Firmware Upgrade

This page updates the detector's firmware (FW).

1. Click **Upload** and select the firmware file.
2. Once the upload finishes, click **Operate** to begin the upgrade.

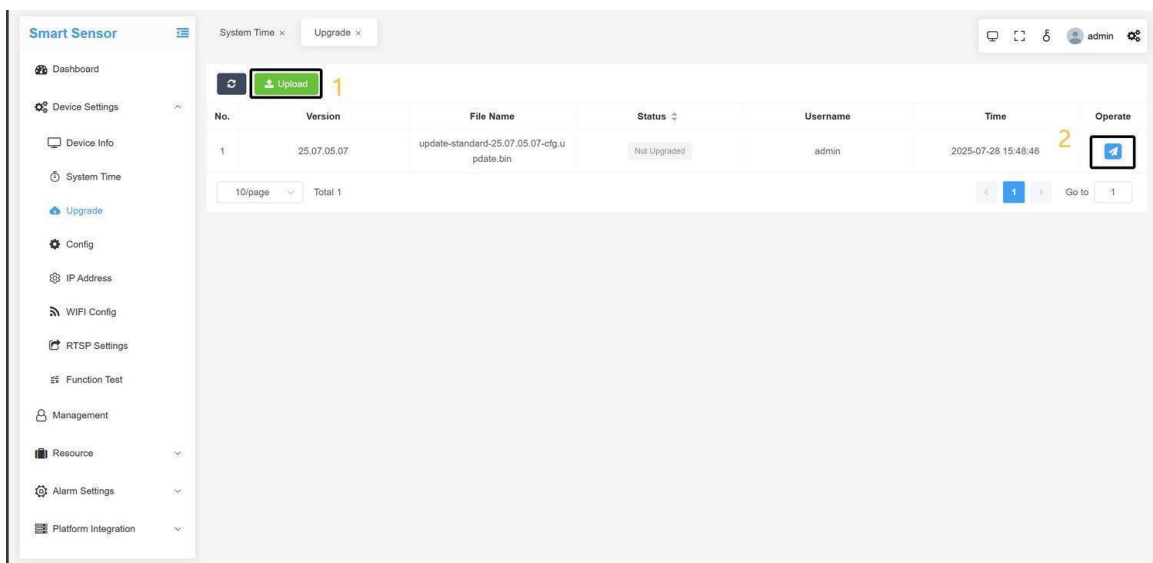


Figure 4-4. The Firmware Upgrade page, with the upload and operate controls.

CAUTION A firmware upgrade normally takes about three minutes. Keep the detector powered for the entire process; interrupting power during the upgrade can leave the unit unusable.

4.4 Configuration

This page groups the detector's operating options and maintenance actions:

- **Data Post** — forwards all measured data to a third-party platform for analysis and algorithm development. Enable it only when your deployment specifically requires it.
- **Temp Type** — selects whether temperature is displayed in Celsius or Fahrenheit.
- **Health Index Calc** — the calculation method for the Health Index; the default uses an average value.
- **Download / Upload Config** — exports one detector's configuration and applies it to others, saving time when installing multiple units.
- **Default** — restores the factory settings.
- **Reboot** — restarts the detector.

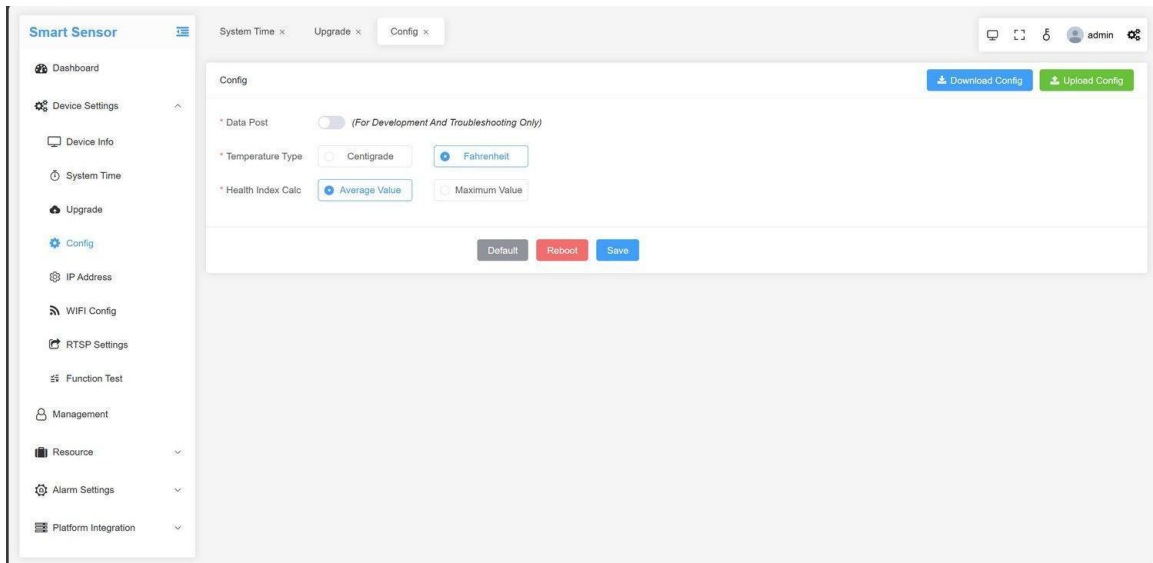
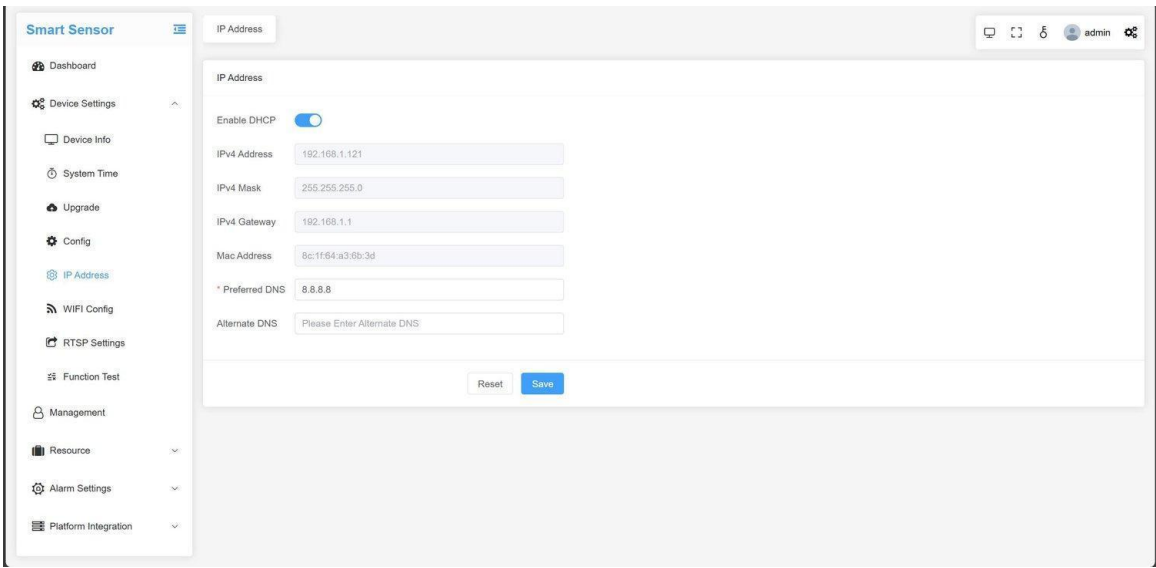


Figure 4-5. The Configuration page: Data Post, Temp Type, Health Index Calc, configuration import/export, Default, and Reboot.

CAUTION Do not enable **Data Post** unless you have a specific need for it. When active, every reading the detector produces is transmitted off-device to the connected platform.

4.5 IP Address

This page adjusts the detector's network address and toggles DHCP on or off. The IPv4 subnet mask is **255.255.255.0**.

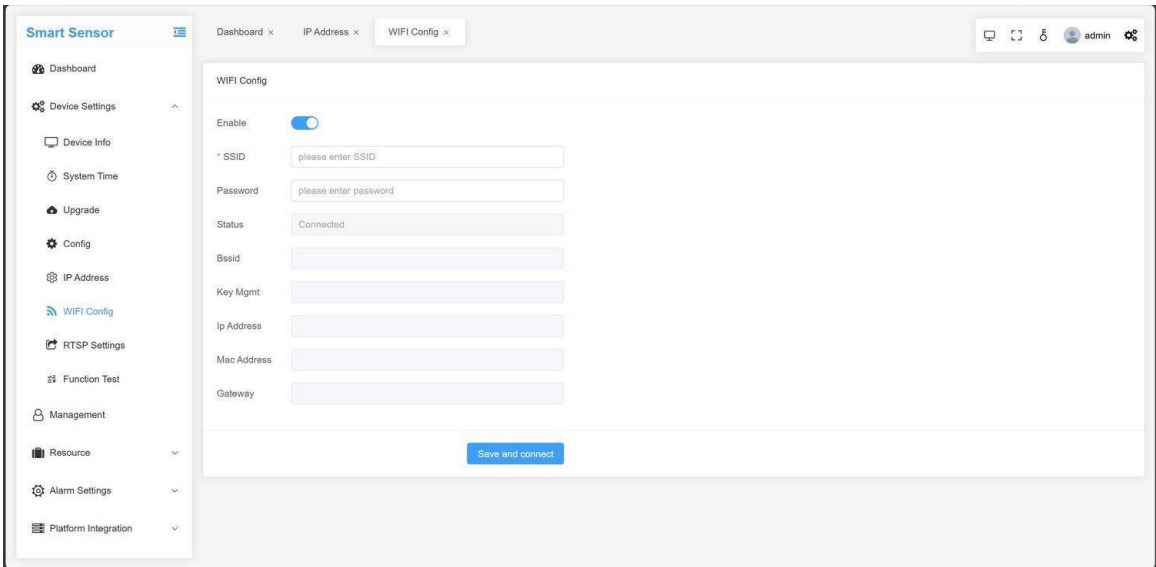


The screenshot shows the 'Smart Sensor' web interface with the 'IP Address' tab selected. The left sidebar contains a menu with options: Dashboard, Device Settings, Device Info, System Time, Upgrade, Config, IP Address (highlighted), WIFI Config, RTSP Settings, Function Test, Management, Resource, Alarm Settings, and Platform Integration. The main content area is titled 'IP Address' and features a toggle for 'Enable DHCP' which is currently turned on. Below this are input fields for 'IPv4 Address' (192.168.1.121), 'IPv4 Mask' (255.255.255.0), 'IPv4 Gateway' (192.168.1.1), 'Mac Address' (8c:1f:64:a3:6b:3d), '* Preferred DNS' (8.8.8.8), and 'Alternate DNS' (Please Enter Alternate DNS). At the bottom right of the form are 'Reset' and 'Save' buttons.

Figure 4-6. The IP Address page, with DHCP toggle and manual address entry.

4.6 WiFi Configuration

Enter the correct SSID and password to connect the VP360MPOE to a wireless network.



The screenshot shows the 'Smart Sensor' web interface with the 'WIFI Config' tab selected. The left sidebar is identical to the previous screenshot, with 'WIFI Config' highlighted. The main content area is titled 'WIFI Config' and features an 'Enable' toggle which is turned on. Below this are input fields for '* SSID' (placeholder: please enter SSID), 'Password' (placeholder: please enter password), 'Status' (Connected), 'Bssid', 'Key Mgmt', 'Ip Address', 'Mac Address', and 'Gateway'. At the bottom right of the form is a 'Save and connect' button.

Figure 4-7. The WiFi configuration page, with SSID and password fields.

4.7 RTSP Settings

The detector publishes a video stream at **rtsp://<ip address>:554**. You can overlay the device date and time, the device name, and a custom logo on this stream.

Upload the logo from **Resource – RTSP Config** first, then select it here.

- **Screen** — chooses the video resolution from three sizes: 1920x1080, 1280x720, and 640x360.
- **Frame Rate** — selectable from 1 to 5 fps.

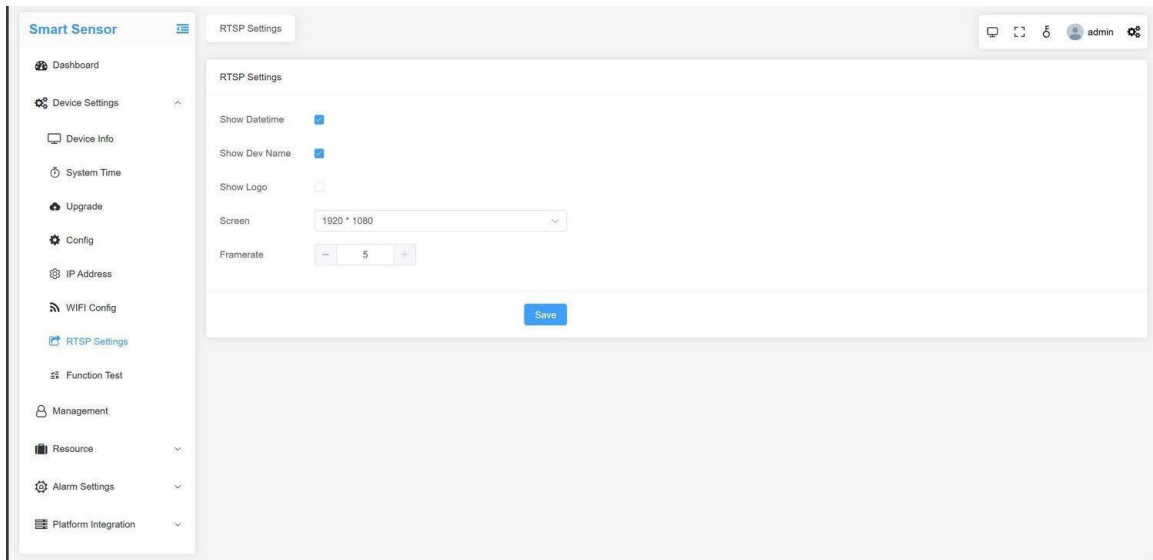


Figure 4-8. The RTSP Settings page: stream address, overlay options, resolution, and frame rate.

4.8 Function Testing

This page verifies that individual hardware components operate correctly, including the audio output, alarm output, fan, and RGB lights.

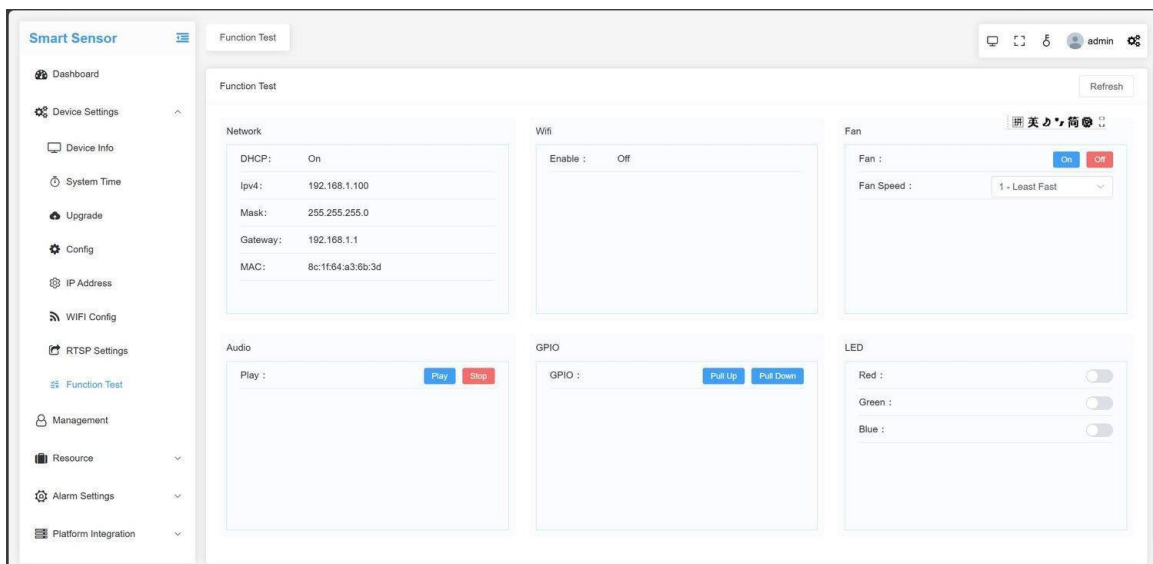


Figure 4-9. The Function Testing page, used to exercise the audio, alarm output, fan, and RGB lights.

CAUTION The fan must remain on at all times. Never switch it off; continuous airflow is required for the sensors to operate correctly.

Chapter 5 User Management

To grant additional people access to the web interface, click **Add** and create an account. Each account is assigned a **Level** of either admin or viewer.

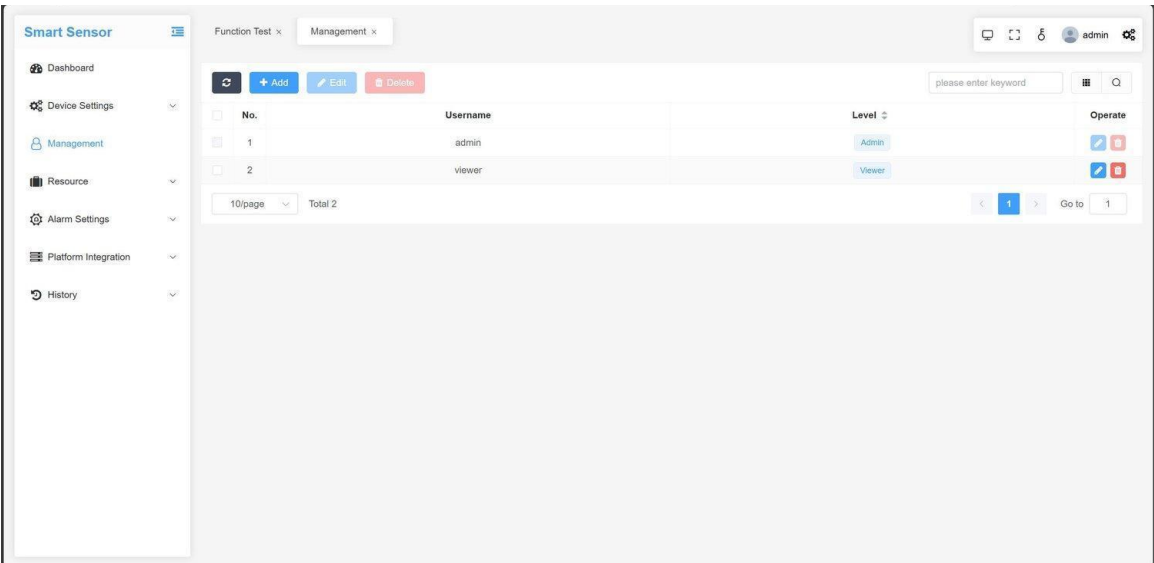


Figure 5-1. The user list, showing each account and its assigned access level.

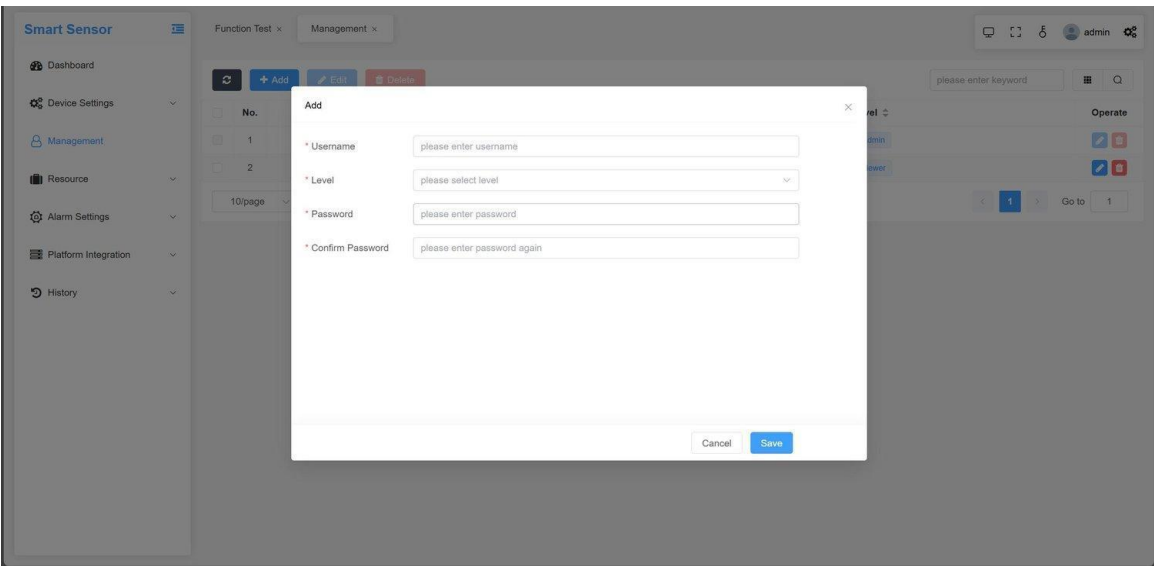


Figure 5-2. The add-user dialog, where a new account and its level are defined.

Chapter 6 Resources

The Resources section stores the media and templates the detector draws on: the RTSP logo, audio clips, LED colors and patterns, and the notification email templates.

6.1 RTSP Logo / Resource

Upload your custom logo here. To display it on the video stream, go to **Device Settings – RTSP Settings** and select the uploaded logo.

The logo must be a PNG image measuring 500 pixels wide by 100 pixels high.

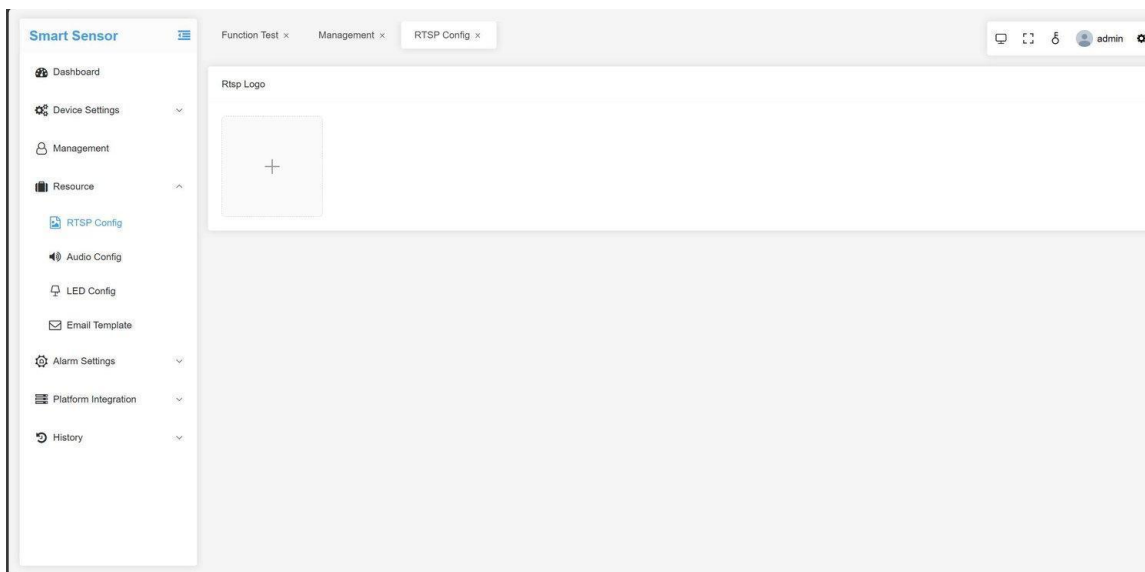


Figure 6-1. The RTSP logo resource page, where the overlay logo is uploaded.

6.2 Audio Files

The VP360MPOE includes eight built-in audio files, and you can upload additional pre-recorded clips. Uploaded files must meet the following requirements:

Property	Requirement
Format	WAV
Maximum file size	10 MB
Channel type	Mono
Sampling rate	16k
Bit rate	256 Kbps
Maximum total audio storage	17 MB

To add a clip, click **Custom** and then **Upload**.

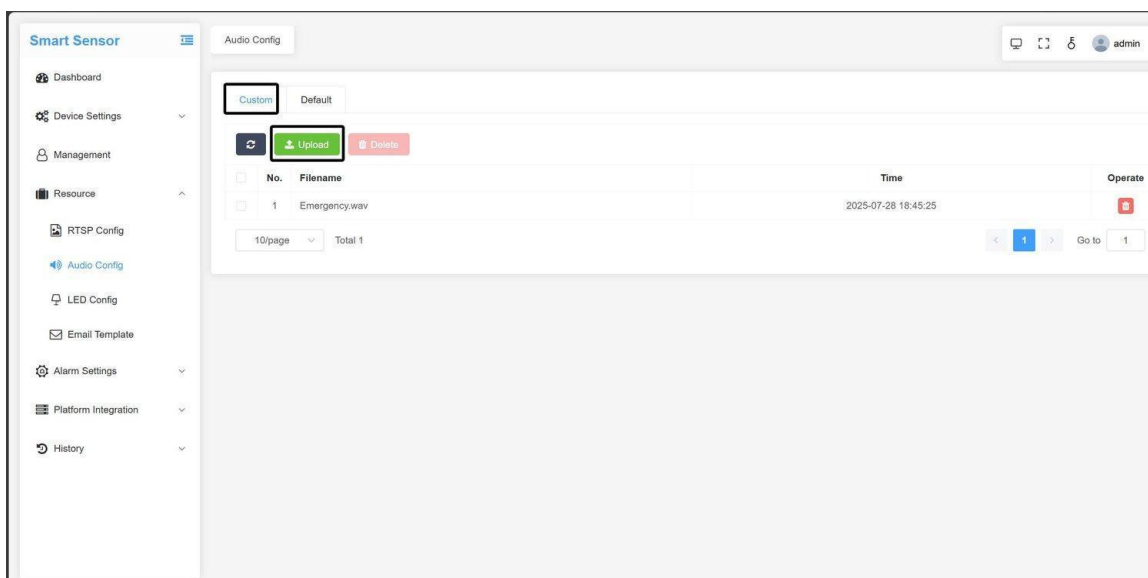


Figure 6-2. The audio configuration page, listing built-in clips and the upload control for custom audio.

6.3 LED (Color & Pattern)

Configure which LED colors and blink patterns are available for use:

- **Color** — seven colors are supported: red, green, blue, yellow, violet, cyan, and white. Disabled colors do not appear as options when configuring the LED.
- **Pattern** — thirteen patterns are available. As with colors, any pattern you disable becomes unavailable for selection.

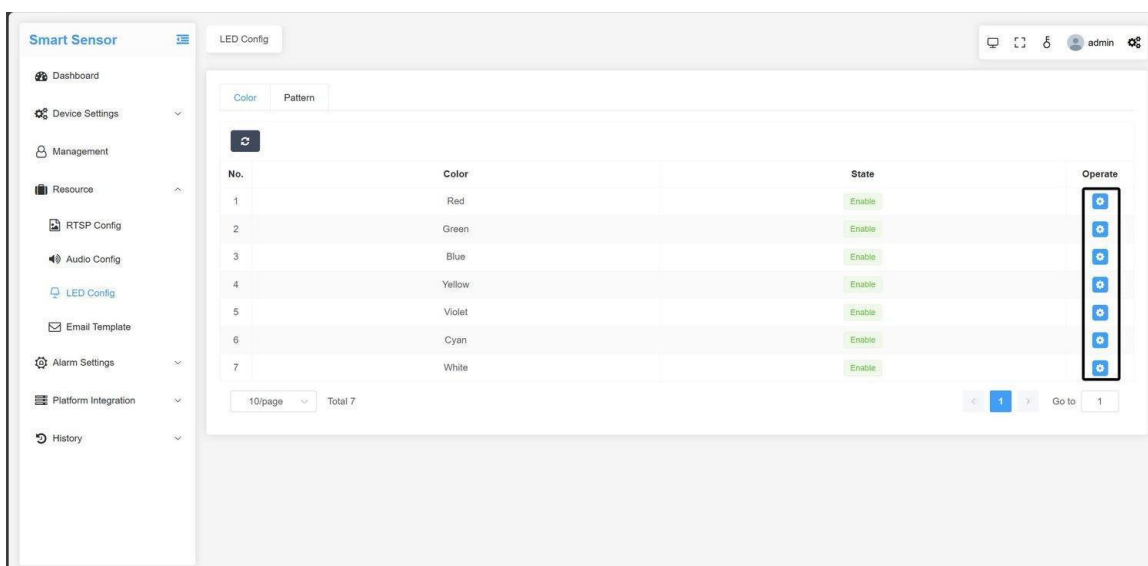


Figure 6-3. LED color configuration, enabling or disabling each of the seven colors.

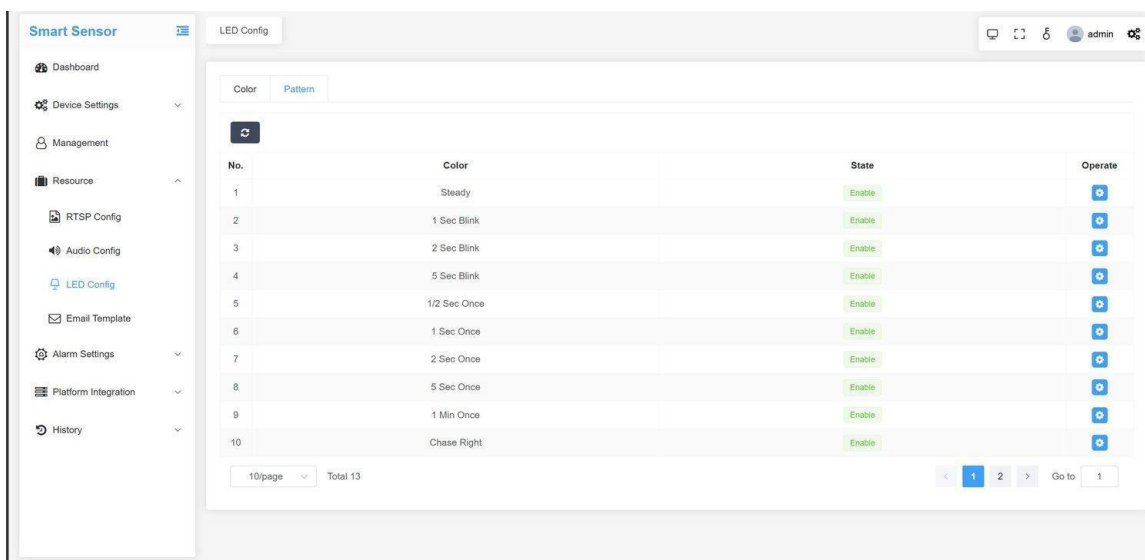


Figure 6-4. LED pattern configuration, enabling or disabling each of the thirteen patterns.

6.4 Email Template

When an event occurs, the detector can send an email to notify recipients, and it can send a second email when the event clears. This page defines the content of those messages.

- **Email Template Set** — the content sent when an event is triggered.
- **Email Template Reset** — the content sent when an event is released.
- **Subject** — the email subject line. Type it manually, or insert the wildcards listed alongside the field to build it automatically.

Wildcards make composition easier: to include a specific piece of information when an event is triggered or released, click the corresponding wildcard and it is inserted into the message body automatically.

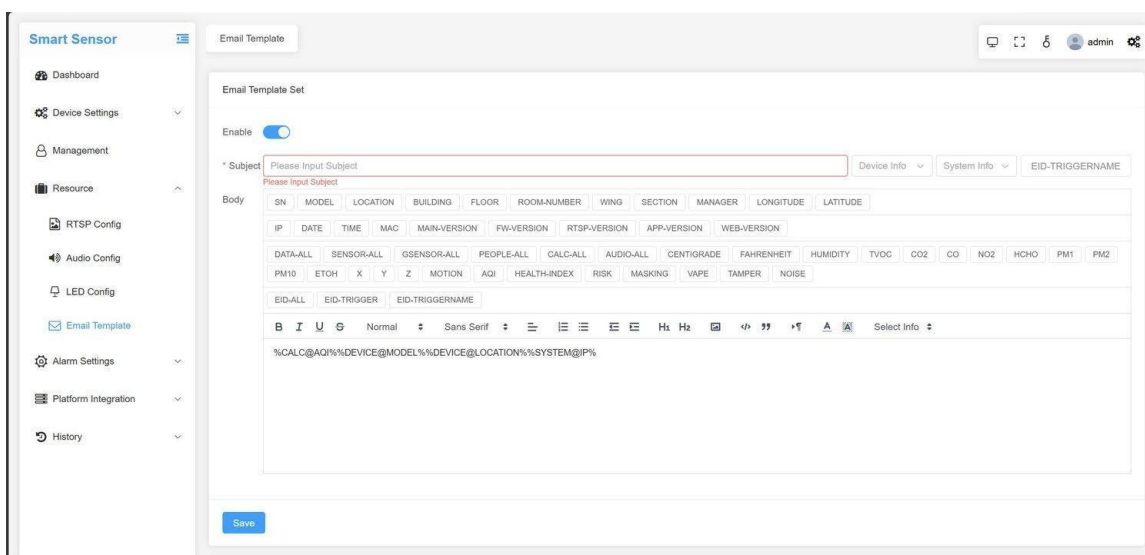


Figure 6-5. The Email Template Set page, defining the message sent when an event is triggered.

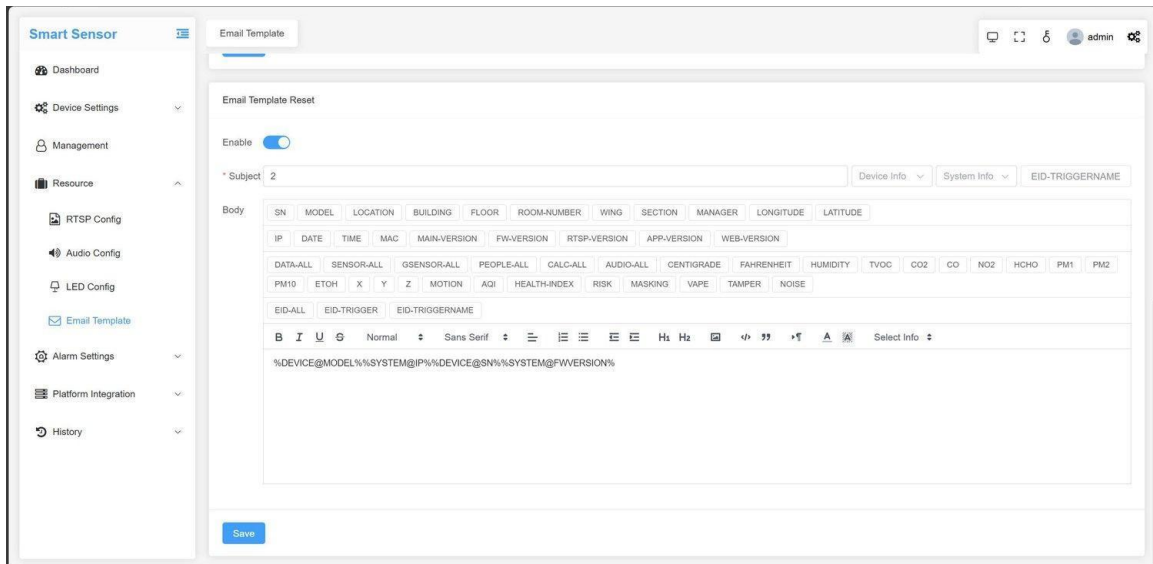


Figure 6-6. The Email Template Reset page, defining the message sent when an event is released.

Chapter 7 Alarm Settings

Alarm settings determine when each event fires and how the detector responds when it does.

7.1 Event Settings

Each event is defined by an Event Identifier (EID), a data source, its trigger and release conditions, an alarm interval, and an advanced schedule. The EID is editable, but the data source is fixed and should not be changed.

Available EIDs include Vape, Masking, Aggression, Tamper, Motion, Health-Index, AQI, PM2.5, PM10, TVOC, CO2, Humidity, HCHO, ETOH, Noise, Temp-C, and Temp-F.

- **Trigger Alarm** — the condition under which the event fires. Vape, Masking, and Motion use fixed algorithms with no configurable threshold; the remaining EIDs offer a data range you can set.
- **Release Alarm** — the condition under which the event clears. For example, if the Vape reset time is set to 60 seconds, the alarm clears once the detector goes 60 seconds without detecting vape again.
- **Alarm Interval** — the minimum gap between consecutive alarms. Set to 300 seconds, a new alarm cannot fire until 300 seconds after the previous one.
- **Advanced** — a time schedule for the event. For instance, setting Monday 06:30 to 20:00 restricts the event to that window.

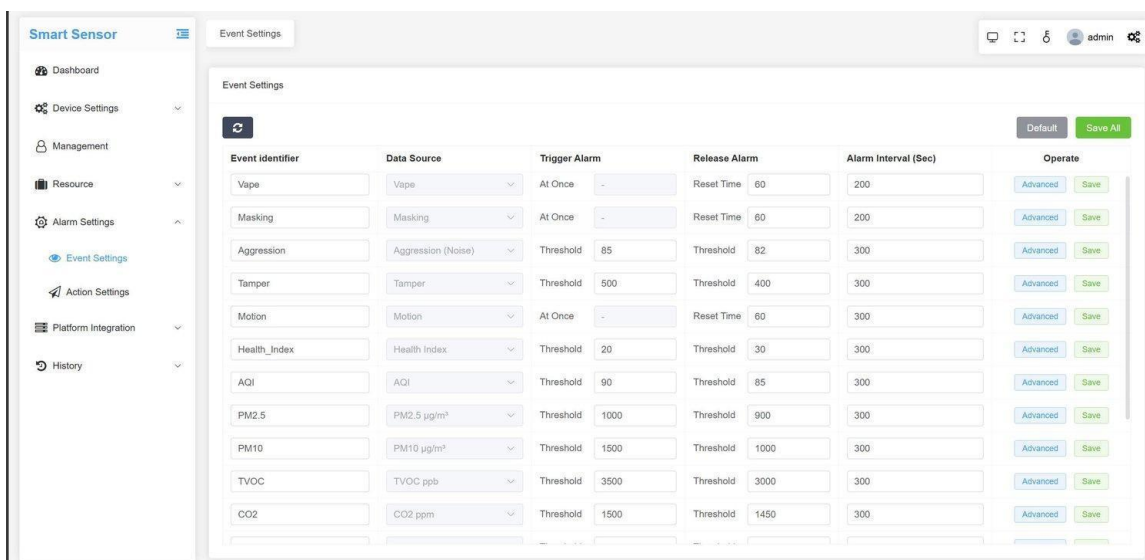


Figure 7-1. The Event Settings page: EID, data source, trigger and release conditions, and alarm interval.

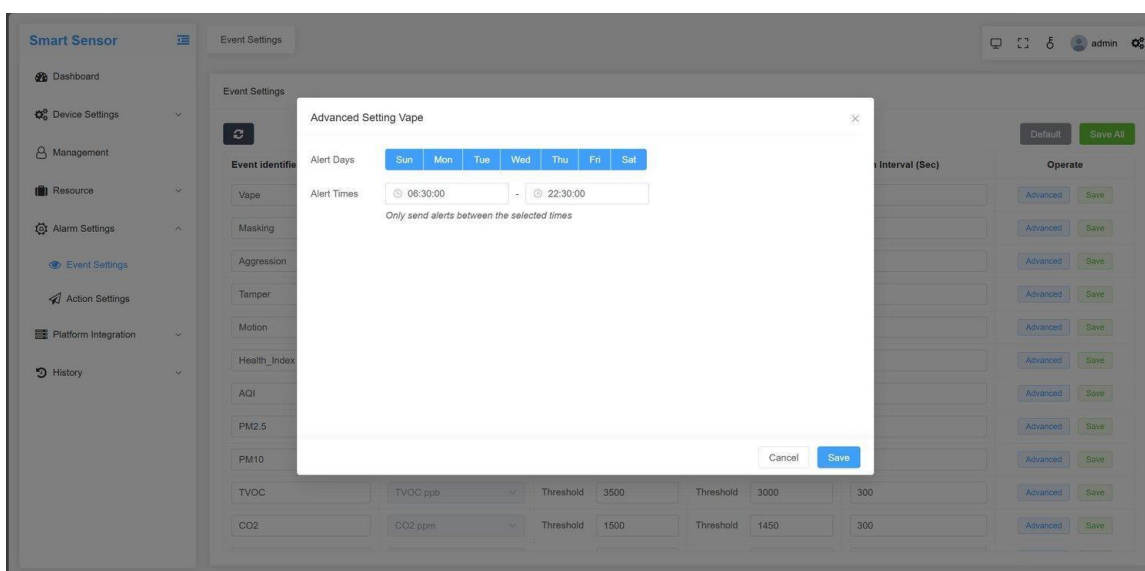


Figure 7-2. The advanced schedule, restricting an event to specific days and times.

7.2 Action Settings

Action settings define what the detector does when an event is triggered or released. The available responses are:

- Sending the set or reset notification email.
- Reporting the event to a third-party platform over HTTP, TCP/IP, or MQTT.
- Activating the wired alarm output for a defined duration.
- Driving a specific LED color and pattern.
- Playing an audio clip.

Because the detector handles many events, each one can be assigned a **Priority** of High, 2, 3, 4, 5, 6, 7, or 8.

- **Save** — stores the configured actions.
- **Test** — simulates the event so you can confirm the configured actions perform as expected.

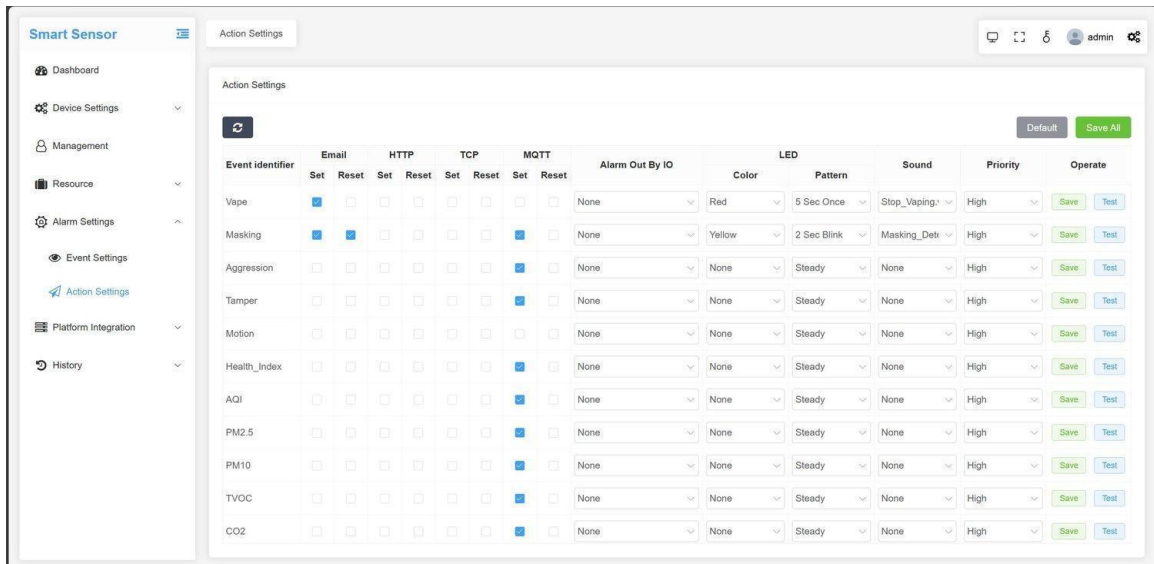


Figure 7-3. The Action Settings page, mapping each event to notifications, outputs, LED, audio, and priority.

Chapter 8 Platform Integration

The VP360MPOE can push event data to external systems over several protocols and send periodic heartbeats to confirm it remains online.

8.1 TCP / MQTT

When an event occurs, the detector can send its details to a third-party platform over TCP or MQTT. The payload can be formatted as plain text or JSON.

- **Set String** — the message sent to the platform when an alarm is raised.
- **Reset String** — the message that notifies the platform the alarm has cleared.

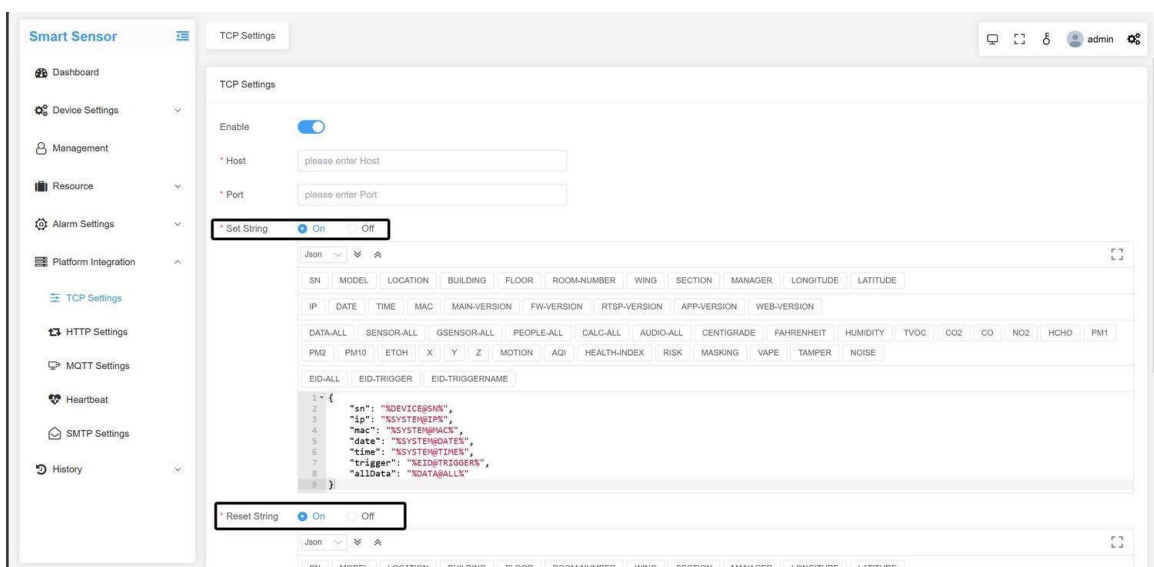


Figure 8-1. The TCP/MQTT settings page, with server details and payload format.

Smart Sensor

MQTT Settings x Heartbeat x

MQTT Settings

Enable ☒

* Server:

* Port:

Client Id:

User:

Password:

* Topic: Quick Input

* QoS:

* set string ☒ On ☐ Off

Json

SN	MODEL	LOCATION	BUILDING	FLOOR	ROOM-NUMBER	WING	SECTION	MANAGER	LONGITUDE	LATITUDE
IP	DATE	TIME	MAC	MAIN-VERSION	FW-VERSION	RTSP-VERSION	APP-VERSION	WEB-VERSION		
DATA-ALL	SENSOR-ALL	SENSOR-ALL	PEOPLE-ALL	CALC-ALL	AUDIO-ALL	CENTIGRADE	FAHRENHEIT	HUMIDITY	TVOC	CO2
PM2	PM10	ETOH	X	Y	Z	MOTION	AQI	HEALTH-INDEX	RISK	MASKING
EID-ALL	EID-TRIGGER	EID-TRIGGERNAME								

Figure 8-2. The Set String and Reset String definitions for TCP/MQTT reporting.

8.2 HTTP

The detector can also report event details to a third-party platform over HTTP, again using either plain text or JSON.

- **Set String** — the message sent when an alarm is raised.
- **Reset String** — the message that notifies the platform the alarm has cleared.
- **Test** — confirms that the settings are correct.

Smart Sensor

HTTP Settings

HTTP Settings

Enable ☒

* Server:

* Method:

* Content Type:

* Auth Method:

* set string

Private Key Value Pairs

Bearer Token

Basic Auth

NX OAuth2.0

NUMBER	WING	SECTION	MANAGER	LONGITUDE	LATITUDE
RTSP-VERSION	APP-VERSION	WEB-VERSION			
CALC-ALL	AUDIO-ALL	CENTIGRADE	FAHRENHEIT	HUMIDITY	TVOC
PM2	PM10	ETOH	X	Y	Z
MOTION	AQI	HEALTH-INDEX	RISK	MASKING	VAPE
TAMPER	NOISE				

```

1 {
2   "sn": "800000000000",
3   "ip": "192.168.1.1",
4   "mac": "800000000000",
5   "date": "2023-07-26 10:00:00",
6   "time": "2023-07-26 10:00:00",
7   "trigger": "800000000000",
8   "allData": "800000000000"
9 }

```

Figure 8-3. The HTTP settings page, with endpoint and payload configuration.

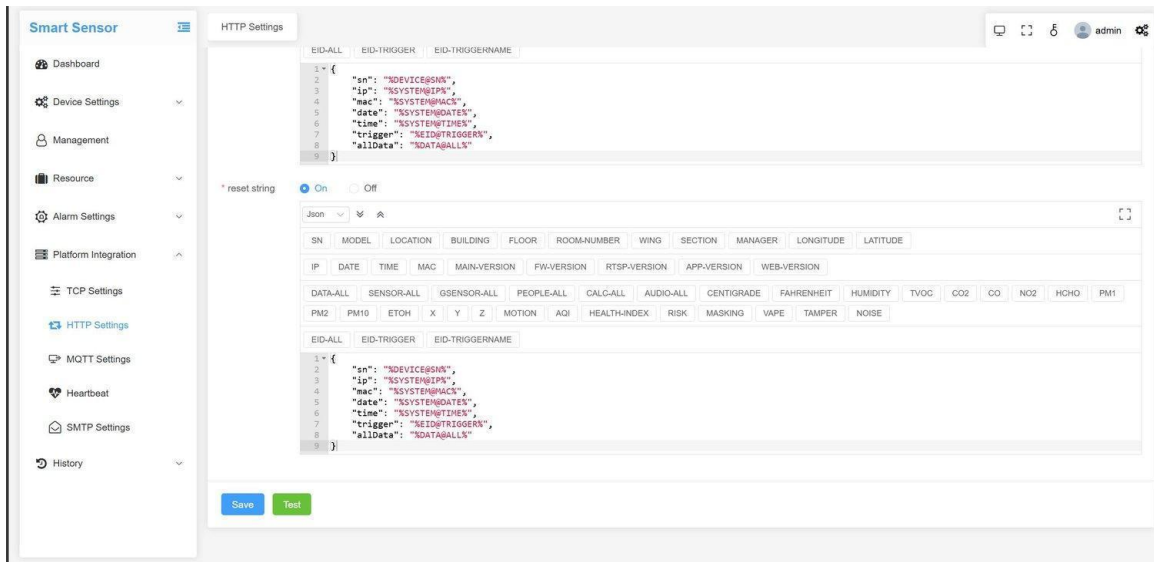


Figure 8-4. The Set String and Reset String definitions for HTTP reporting.

8.3 Heartbeat

The heartbeat function periodically sends data to your platform over HTTP, MQTT, or TCP. You choose the interval between heartbeats.

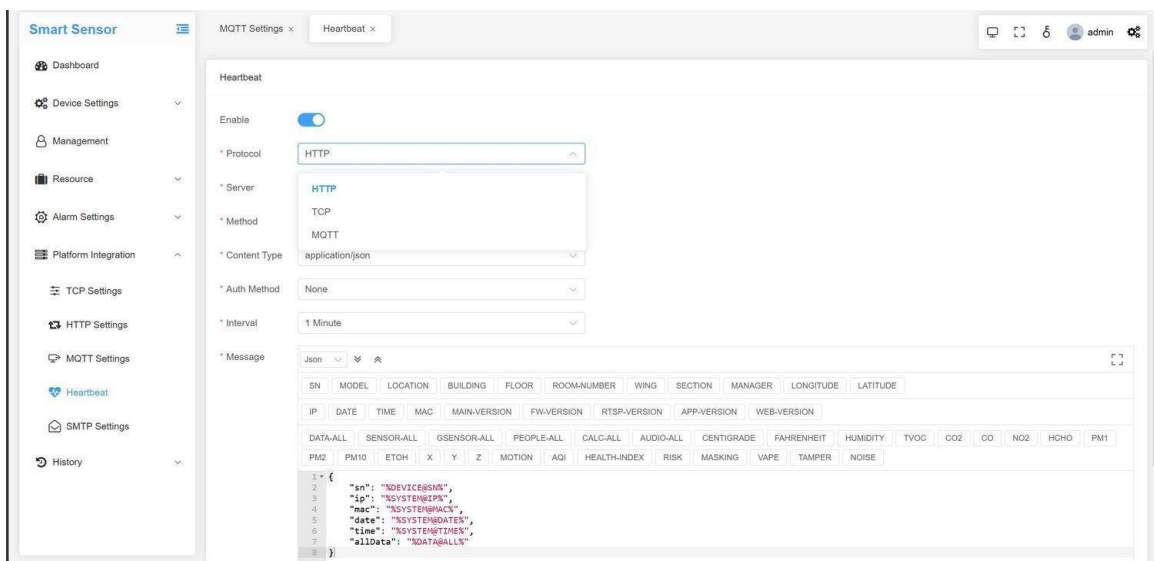


Figure 8-5. The Heartbeat page, selecting the transport protocol and interval.

8.4 SMTP (Email)

Before the detector can send notification emails, configure SMTP. The **Email Provider** field supports Gmail and Outlook; a Gmail example is shown below.

You can add several recipients. Enter each valid address, click the add control, and then click **Save**.

The screenshot displays the 'Smart Sensor' interface with the 'SMTP Settings' tab selected. On the left is a navigation menu with options: Dashboard, Device Settings, Management, Resource, Alarm Settings, Platform Integration, TCP Settings, HTTP Settings, MQTT Settings, Heartbeat, SMTP Settings (highlighted), and History. The main content area is titled 'SMTP Settings' and contains the following fields:

- Enable:** A toggle switch that is turned on.
- Email Provider:** A dropdown menu set to 'Gmail'.
- * Host:** A text input field containing 'smtp.gmail.com'.
- * Port:** A text input field containing '587'.
- * Security:** A dropdown menu set to 'TLS'.
- * User:** A text input field containing 'johnschuman90@gmail.com'.
- * Password:** A text input field with masked characters '*****' and a password icon.
- * Sender:** A text input field containing 'johnschuman90@gmail.com'.
- * Recipient1:** A text input field containing 'ej.colvill@invidtech.com', followed by a '+' button to add more recipients and a '-' button to remove them.

A blue 'Save' button is located at the bottom right of the settings form.

Figure 8-6. The SMTP settings page, showing provider selection and recipient entry using a Gmail example.

Chapter 9 History

The History section retains sensor readings and event records, both of which can be exported as reports.

9.1 Data Log

This page records sensor measurements over time. You can download the data as a report for a chosen time range, and enable or disable which measurements appear on the page.

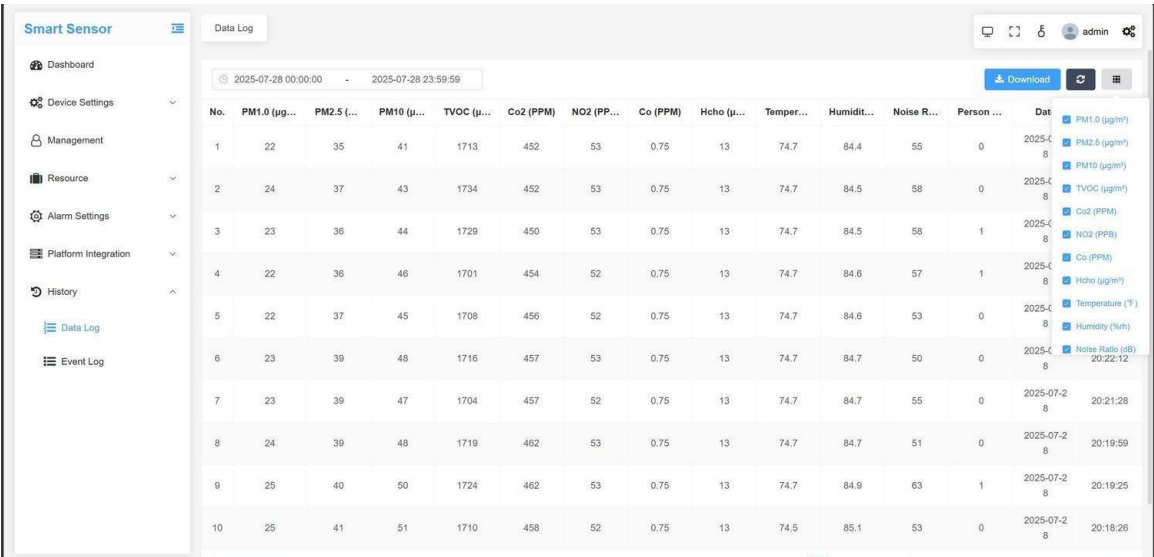


Figure 9-1. The Data Log page, with the sensor-measurement history and report download.

9.2 Event Log

This page records the detector's events. As with the Data Log, you can download the records as a report for a selected time range.

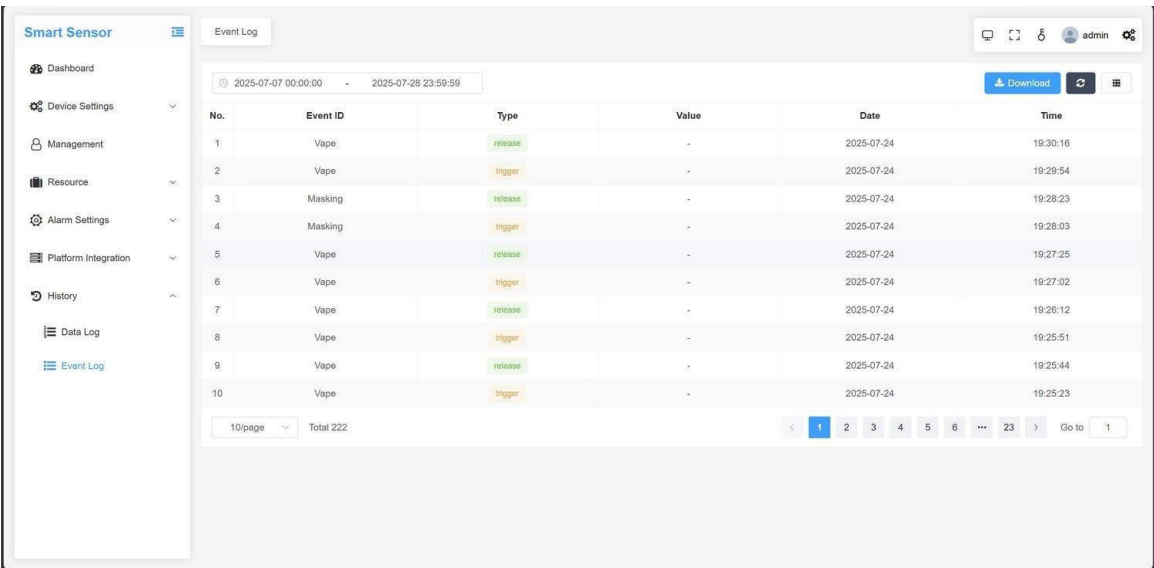


Figure 9-2. The Event Log page, listing recorded events with report download.

Chapter 10 Installation

The VP360MPOE can be pendant-mounted from a bracket or fixed directly to a ceiling or surface. Choose the method that suits the mounting location.

10.1 Pendant Mount

Use a pendant mount to suspend the detector from a bracket or drop rod, following the sequence shown below.

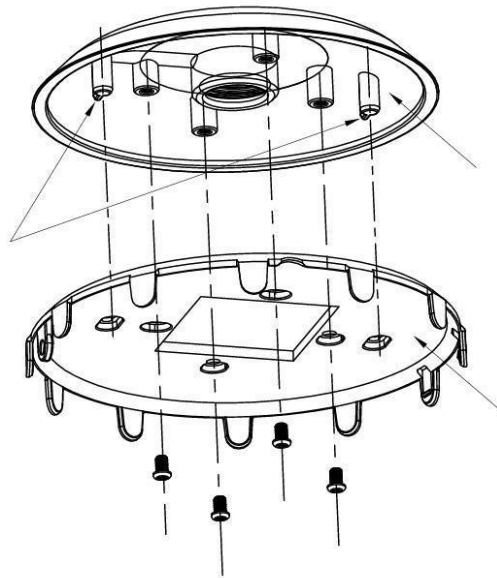


Figure 10-1. Pendant mount, step 1: preparing the bracket assembly.

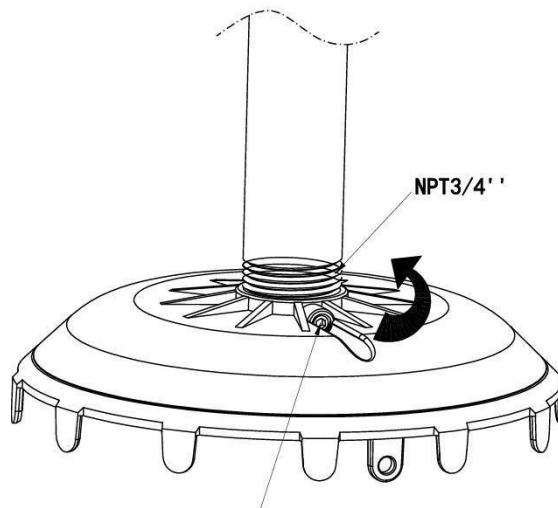


Figure 10-2. Pendant mount, step 2: securing the detector to the pendant.

10.2 Ceiling / Surface Mount

Use a ceiling or surface mount to attach the detector directly to a flat surface, following the sequence shown below.

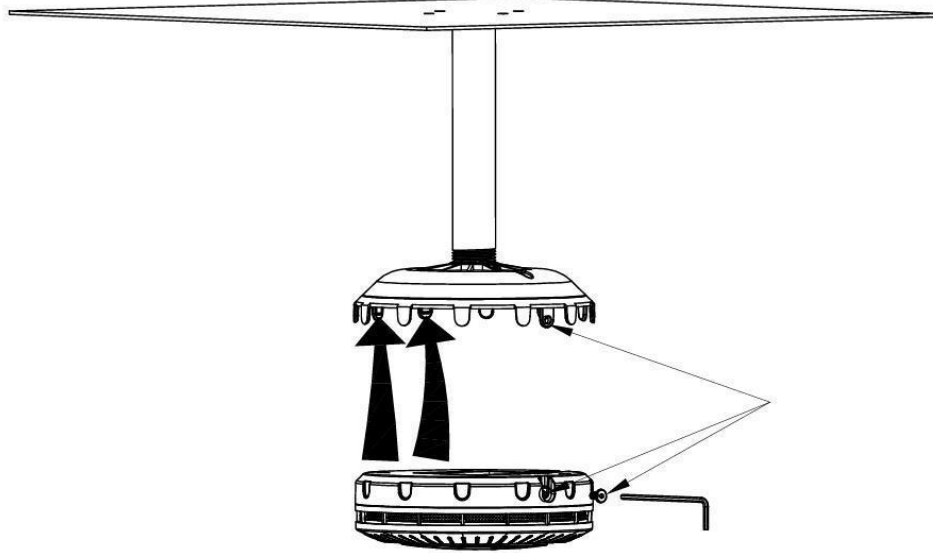


Figure 10-3. Ceiling mount, step 1: marking and preparing the mounting surface.

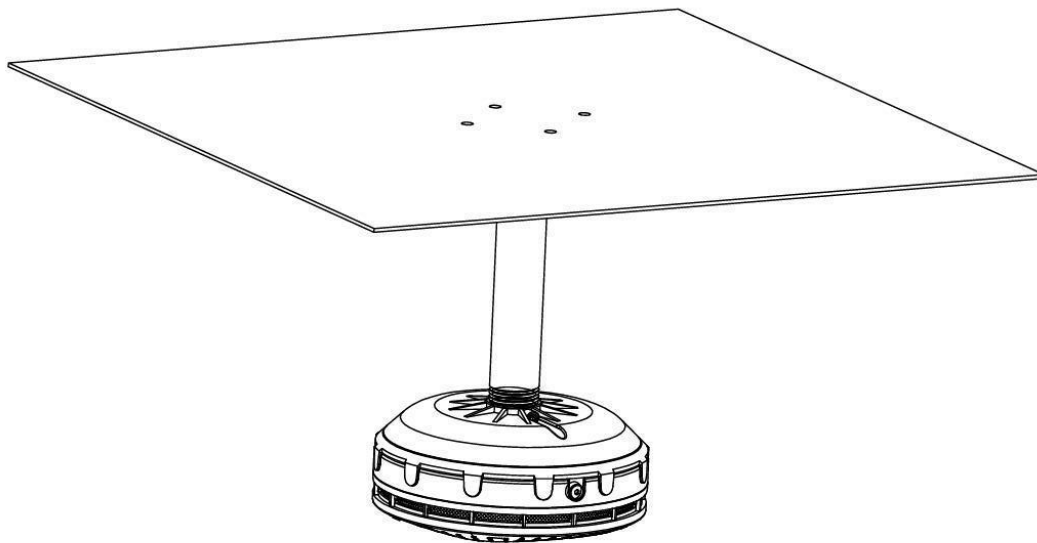


Figure 10-4. Ceiling mount, step 2: fitting the mounting base.

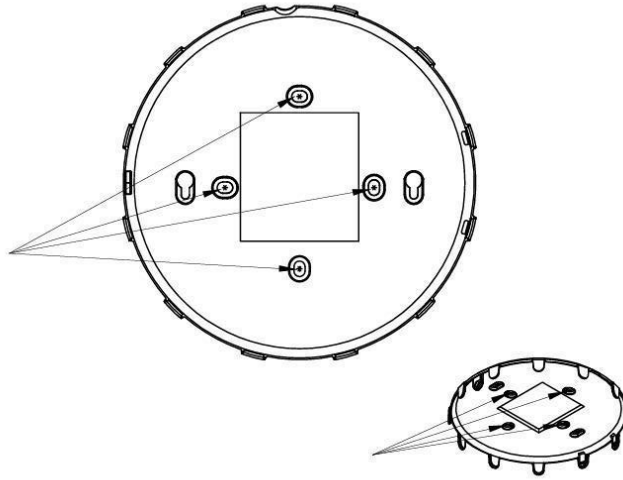


Figure 10-5. Ceiling mount, step 3: fastening the base to the surface.

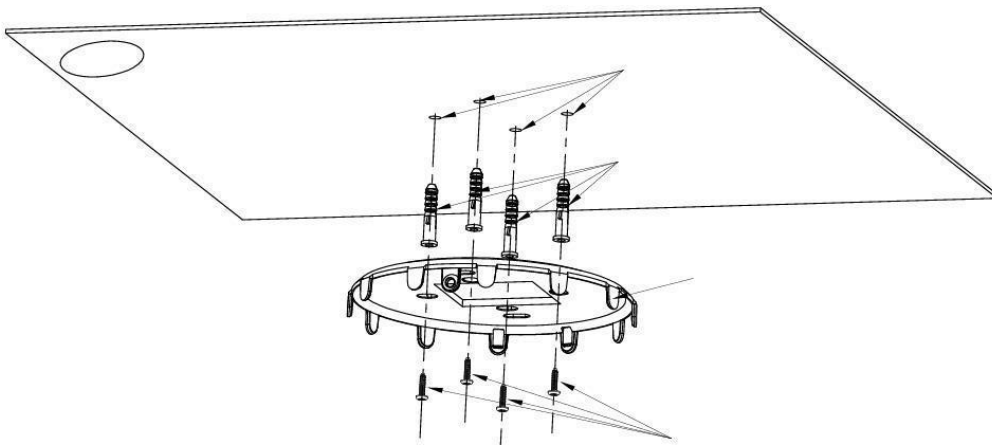


Figure 10-6. Ceiling mount, step 4: aligning the detector with the base.

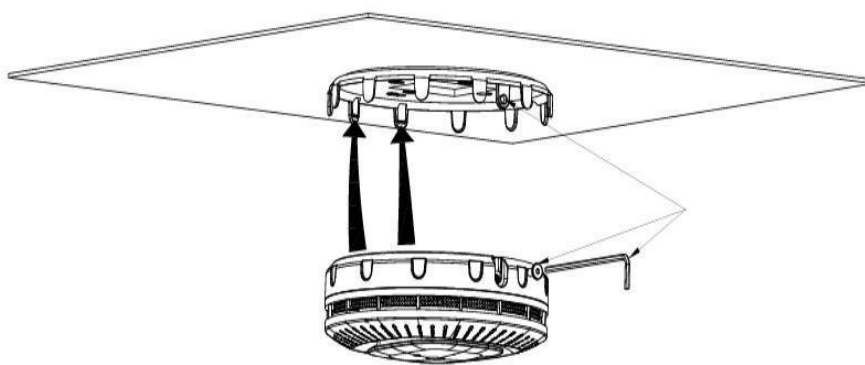


Figure 10-7. Ceiling mount, step 5: attaching the detector to the base.

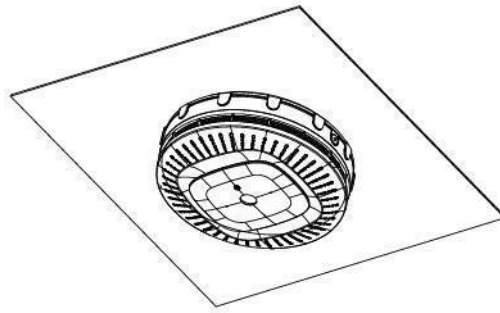


Figure 10-8. Ceiling mount, step 6: the completed installation.

Chapter 11 Important Notes

Observe the following points to keep the VP360MPOE accurate, reliable, and in good condition.

11.1 Power Supply

The detector accepts a DC12V input and can also be powered over Ethernet (PoE).

11.2 TVOC Sensor

Each time the detector is powered on or restarted, the TVOC sensor needs a warm-up period before its readings are reliable.

CAUTION After every power-up, wait about 40 minutes before relying on TVOC measurements. The sensor reaches a normal, accurate detection state only once this warm-up is complete.

11.3 Maintenance

Dust may accumulate on the surface over long periods of operation.

CAUTION Clean the detector only with a dry, clean cloth or a soft brush. Never use a damp cloth, alcohol, or dishwashing liquid, as these can damage the unit.

11.4 Testing

You may wish to test vape detection after installation.

CAUTION Never blow air directly onto the detector's surface. Doing so can damage the internal sensors, and the TVOC sensor in particular.

11.5 Monitoring Area

For the fastest response, keep the monitored area within a diameter of about 6 meters, and mount the detector no more than 3.3 m above the floor (measured from ceiling to ground).