

## CONTENTS

|                                      |          |                                                    |           |
|--------------------------------------|----------|----------------------------------------------------|-----------|
| <b>1. General Introduction</b>       | <b>1</b> | <b>4.5 Removing a Gateway from Your Account</b>    | <b>8</b>  |
| 1.1 Product Layout                   | 1        | <b>4.6 Dashboard</b>                               | <b>8</b>  |
| <b>2. Gateway Hardware Setup</b>     | <b>2</b> | <b>4.7 Partitions</b>                              | <b>9</b>  |
| 2.1 Internal connection              | 2        | <b>4.8 Rooms</b>                                   | <b>10</b> |
| 2.2 Siren and Relay Output Operation | 3        | <b>4.9 Device list</b>                             | <b>10</b> |
| 2.3 LED Indicator Definition         | 4        | <b>5. Setting up the System for the First Time</b> | <b>12</b> |
| 2.4 Powering Up                      | 4        | 5.1 Creating Partitions                            | 12        |
| 2.5 LTE 4G Backup Connection         | 5        | 5.2 Creating Rooms                                 | 12        |
| <b>3. Mounting the Unit</b>          | <b>5</b> | 5.3 Creating Devices                               | 13        |
| 3.1 Location Selection Guidelines    | 5        | 5.4 Sensor Information Page                        | 13        |
| 3.2 Mounting                         | 6        | 5.5 Testing Devices RF Signal Strength             | 14        |
| <b>4. VIAS App overview</b>          | <b>6</b> | 5.6 Users and access                               | 15        |
| 4.1 Setting up an Account            | 6        | 5.7 Members                                        | 15        |
| 4.2 Setting Face ID / Touch ID       | 7        | 5.8 Users                                          | 16        |
| 4.3 Gateway List                     | 7        | 5.9 Customized permissions                         | 18        |
| 4.4 Adding a Gateway to Your Account | 8        | 5.10 Alarm Modes Workflow                          | 20        |
|                                      |          | 5.11 Alarm System Settings                         | 24        |
|                                      |          | 5.12 Viewing the Event Logs                        | 25        |
|                                      |          | <b>6. Surveillance Settings</b>                    | <b>25</b> |

|     |                                        |           |                                                             |    |
|-----|----------------------------------------|-----------|-------------------------------------------------------------|----|
| 6.1 | <i>Adding Cameras Manually</i>         | 25        | 10. Firmware Upgrade                                        | 41 |
| 6.2 | <i>Adding Cameras Automatically</i>    | 26        | 11. Reboot or Reset Gateways                                | 42 |
| 6.3 | <i>Surveillance Setting Page</i>       | 26        | 11.1 Reboot gateways                                        | 42 |
| 6.4 | <i>Recording Modes</i>                 | 26        | 11.2 Reset Gateways                                         | 42 |
| 6.5 | <i>Camera Operation</i>                | 28        | 11.3 Reset Gateway's Users                                  | 42 |
| 7.  | <b>Gateway Configurations</b>          | <b>34</b> | 12. Backup and Transfer                                     | 43 |
| 7.1 | <i>General Information</i>             | 34        | 12.1 Transferring Data from an Old Gateway to a New Gateway | 43 |
| 7.2 | <i>Monitoring Center connection</i>    | 34        | 12.2 Gateway Transfer to Itself                             | 44 |
| 7.3 | <i>Connection to 4G</i>                | 35        | 13. VIAS Web Interface                                      | 45 |
| 7.4 | <i>Network Communication Interface</i> | 36        | 14. Specifications                                          | 45 |
| 7.5 | <i>Duress</i>                          | 36        | 14.1 Hardware Specification                                 | 45 |
| 8.  | <b>Automations</b>                     | <b>37</b> | 14.2 Functional Specifications                              | 46 |
| 8.1 | <i>SC115 Automation Setting</i>        | 37        | 15. Certifications                                          | 46 |
| 9.  | <b>Notifications</b>                   | <b>37</b> |                                                             |    |
| 9.1 | <i>Email Notification</i>              | 37        |                                                             |    |
| 9.2 | <i>SMS Notification</i>                | 39        |                                                             |    |
| 9.3 | <i>Voice Call Notification</i>         | 39        |                                                             |    |
| 9.4 | <i>Critical Alerts</i>                 | 40        |                                                             |    |

# 1. General Introduction

VIAS (Video IOT Alarm System) is an all-in-one solution that combines Alarm, Video Surveillance and Home Automation into a single platform. The system architecture comprises three core components: the gateway, a robust cloud platform, and a range of U-Net wireless sensors.

At the center of the VIAS system is the gateway, which functions as the primary control hub. It enables wireless communication, real-time monitoring, and centralized management of all U-Net family devices.

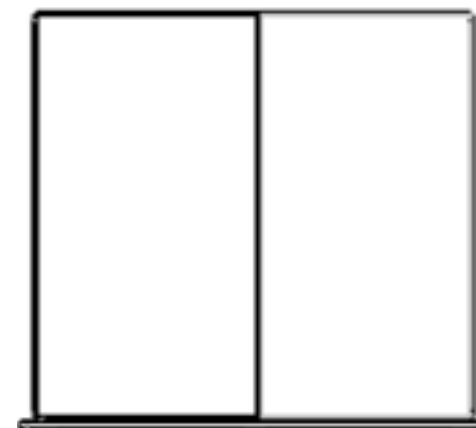
Main features:

- EN50131-compliant security alarm with home automation function.
- Manage / supervise a wireless network of sensor and devices.
- Alarm event reporting via SIA-IP protocol.
- Local video storage (24/7) with built-in hard drive bay.
- Alarm-triggered video verification.
- Rechargeable backup battery.
- Tamper protection for enclosure and wall mount.
- System backup and restore functionality.
- Support one relay output (SC115 only).

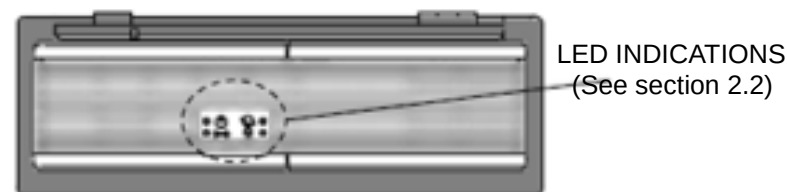
Model Description:

- SC109: 4CH NVR Control Panel (4G LTE, 24/7, Event Recording)
- SC109L: 4CH Video Control Panel (4G LTE, Event Recording)
- SC109C: 4CH Video Control Panel (Event Recording)
- SC115: 8CH NVR Control Panel (4G LTE, 24/7, Event Recording)

## 1.1 Product Layout



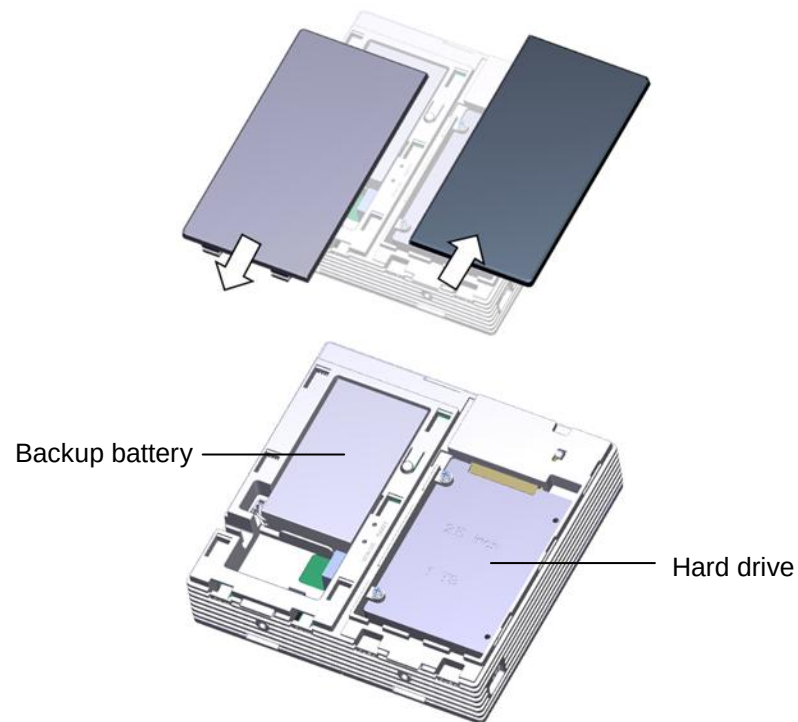
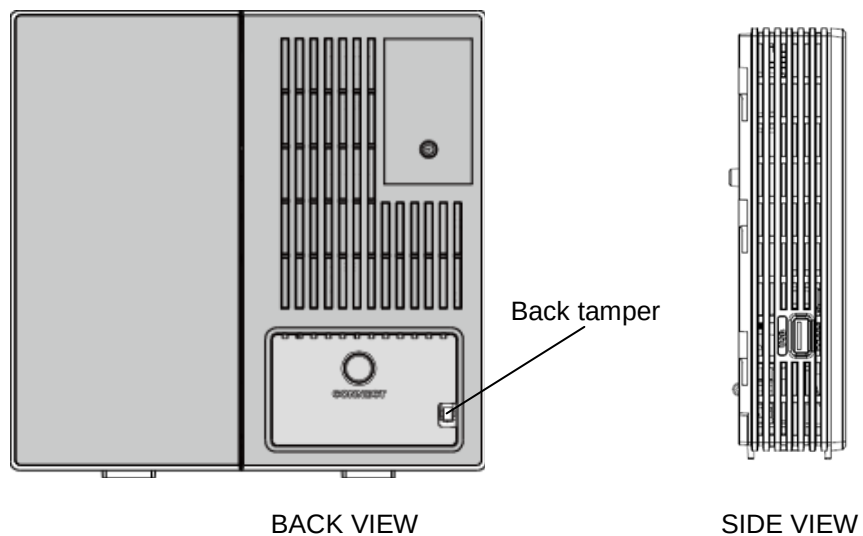
FRONT VIEW



TOP VIEW



REAR VIEW (Wall bracket)

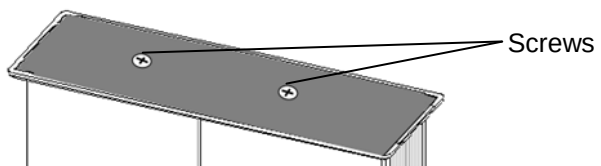


## 2. Gateway Hardware Setup

### 2.1 Internal connection

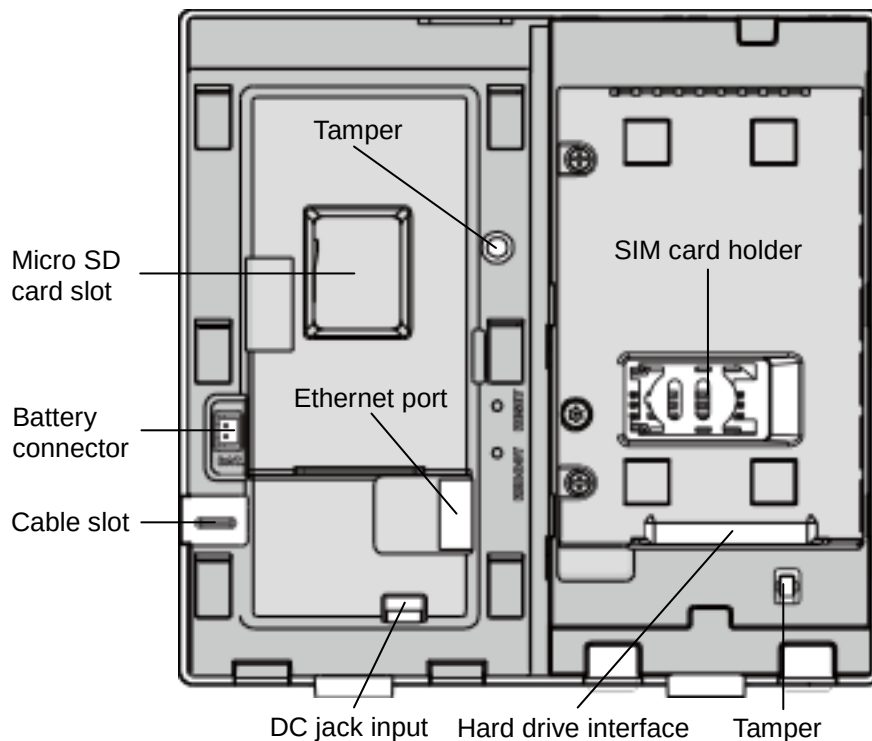
To access the internal connectors, first remove the wall bracket, then detach the top cover.

1. Remove the wall bracket by unscrewing the bottom screws.



2. Slide open the front covers. For the left cover, lift the clips and pull downwards; for the right cover, push upwards.

3. Remove the battery and hard drive to reveal the connectors.



4. To store video recording, the panel utilizes an SSD, HDD or Micro SD card, depending on the required recording feature:
  - Use SSD or HDD for 24-hour continuous recording and event clips.
  - Use Micro SD card for event clips only.

**Note:** The interface for SSD or HDD supports SATA 2.5-inch under 9.5 mm thick.

Format the Micro SD card as one partition with FAT32 or exFAT.

Before installing SIM card, SSD, HDD, or Micro SD, power off the panel and remove the backup battery.

At first installation, the gateway checks if SSD or HDD is formatted for recording.

The power LED blinks orange during checking, then turns steady green when done.

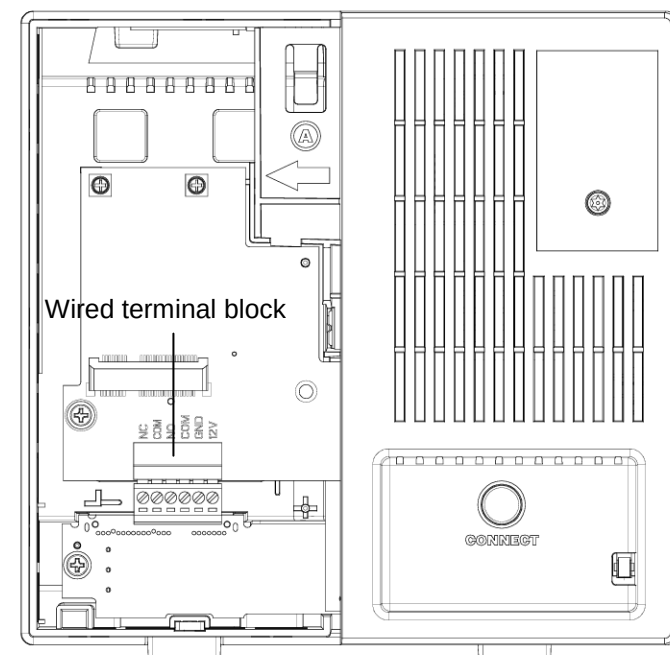
5. To enable 4G LTE internet backup, insert a valid SIM card with active internet service.

**Note:** Please disable the SIM card's PIN lock and use the app to set the APN (Menu > Gateway Configuration > Modem) before inserting the SIM card.

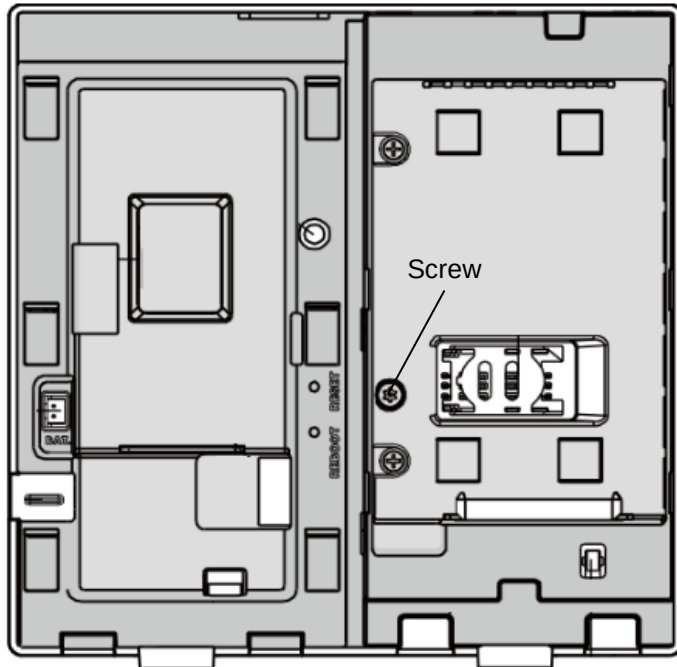
When both wired and 4G connections are available, the wired connection will be used by default.

## 2.2 Siren and Relay Output Operation

The gateway provides one siren output and one relay output, which can be used to trigger an external siren (SC115 only).



1. Remove the screw next to the SIM card slot and detach the back cover.



SC115 provides a siren output (12V, 0.7A. Requires a boost circuit. Connect the wires to the 12V and GND on the terminal block.) and relay output (NO/NC/COM), both of which can be controlled through the AUTOMATION in the VIAS app (see Section 8.1 – SC115 Automation Setting).

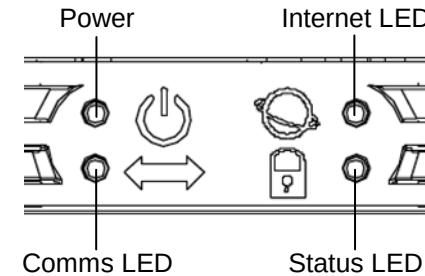
**Note:**

Ensure the connected siren's power consumption does not exceed the specified output.

If higher current is required, use an external power relay.

Wiring should only be performed by a qualified installer.

## 2.3 LED Indicator Definition



Power LED: Shows power status and errors.

| Color  | Meaning            |
|--------|--------------------|
| Green  | DC power.          |
| Red    | Battery operation. |
| Orange | Firmware upgrade.  |

Comms LED: shows the type of external connection

| Color | Meaning                         |
|-------|---------------------------------|
| Green | Connected by Ethernet.          |
| Red   | 3G / 4G connection established. |

Internet LED: Shows status of external connection and RF binding.

| Color          | Meaning                                           |
|----------------|---------------------------------------------------|
| Green          | Connected to server.<br>And Gateway has an Owner. |
| Red            | Unable to connect to server                       |
| Blinking green | Connected to server but Gateway has no Owner.     |

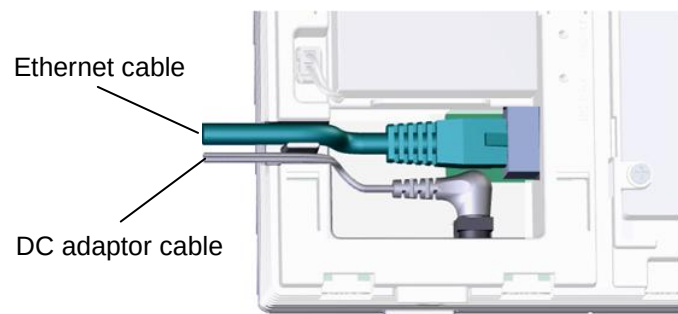
Status LED: shows alarm status

| Color         | Meaning                       |
|---------------|-------------------------------|
| Red           | System Armed.                 |
| Orange        | System Part-Armed.            |
| Green         | System Disarmed.              |
| Green flashes | Panel is pairing with device. |

## 2.4 Powering Up

1. Connect the Ethernet cable and the supplied DC adapter to the

Gateway to power it on.



2. Wait until all four LEDs on the Gateway turn green (this may take about 40 secs on the first connection).
3. The Ethernet port has two LEDs:
  - The left LED stays solid orange when the Ethernet cable is plugged in.
  - The right LED flashes green when network data is transmitting.
4. Connect the backup battery to the Gateway to keep the alarm working during power outages. Backup lasts about 12 hours.
5. Tuck the cables into the cable slots.
6. Reattach the left cover to the gateway.

Note: If the Internet LED suddenly turns red, it means the panel cannot connect to the server VIAS will send a notification after 3 minutes. Once the gateway is back online, a notification will be sent immediately.

## 2.5 LTE 4G Backup Connection

The gateway will switch to 4G LTE internet backup when connection is lost, either due to the Ethernet cable being unplugged or the upstream router's WAN connection is failing.

The system will send notifications indicating the gateway is offline and then back online after one to two minutes. This means the network has switched to the SIM card, and the Comms LED on the gateway will turn red.

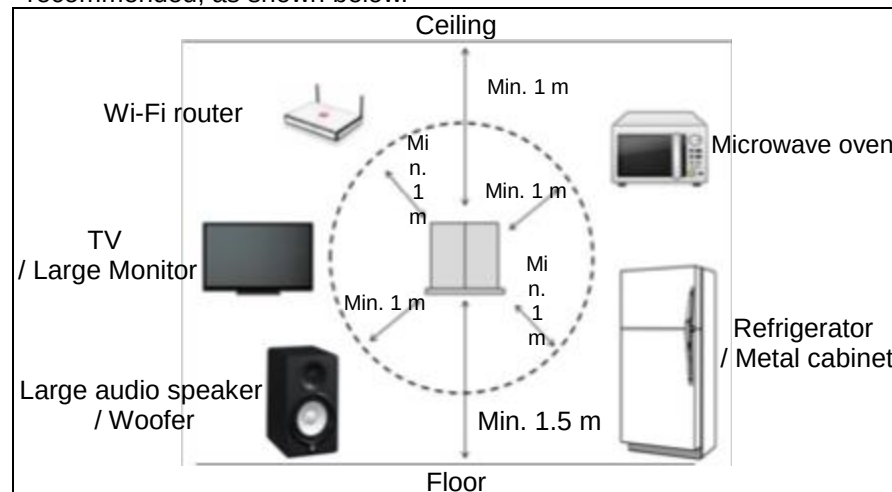
Normally, the system continues to operate, and recorded videos can still be accessed through the App.

To keep watching live video streams during 4G internet backup, make sure the cameras and gateway are on the same network, and that the router remains operational.

## 3. Mounting the Unit

### 3.1 Location Selection Guidelines

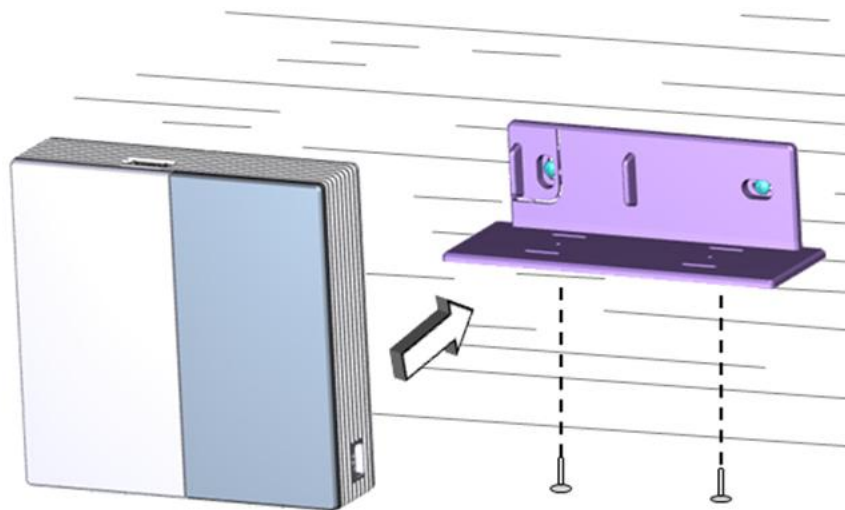
The gateway should ideally be mounted on a wall at a height of 1.5 meters. Avoid placing the gateway near large electrical appliances, large metal objects, or devices that emit radio frequency signals such as routers and microwave ovens, as these can interfere with its RF performance. A minimum clearance of 1 meter radius around the gateway is recommended, as shown below.



### 3.2 Mounting

1. Before mounting the gateway, securely attach the wall bracket to the wall using the provided screws.
2. Once the bracket is in place, mount the gateway onto it and fasten the bottom screws to lock it.

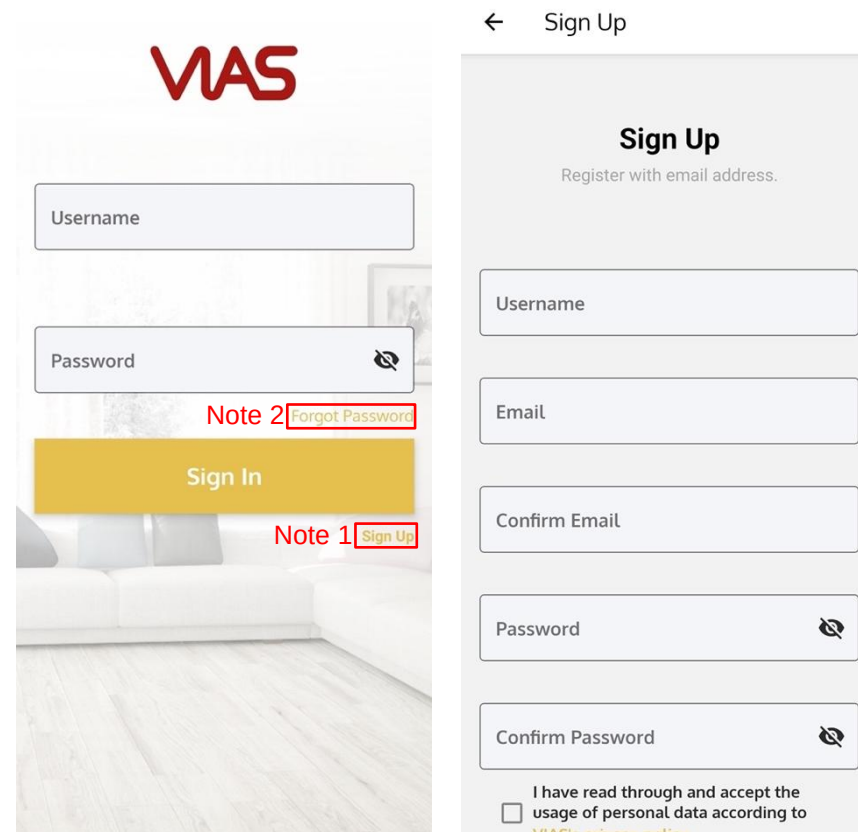
Note: Removing the gateway from the wall bracket will trigger a tamper event and may activate any connected wireless siren.



#### 4. VIAS App overview

## 4.1 Setting up an Account

1. Search for the “VIAS” App on the App Store (iOS) or Google Play (Android), and install it.



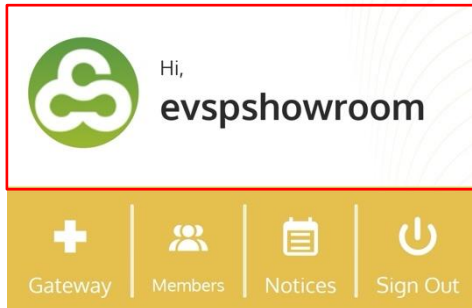
2. Open the app and tap **Sign in** (see Note 1) to register a new account.
3. A verification email will be sent to the address you entered. Click the link in the email to complete registration.
4. Return to the **Sign in** page, enter your username and password, then tap **Sign in** to access the Gateway list.
5. If you forget the password after registration, tap **Forgot Password** on the Sign in page (see Note 2).
6. Enter your username, and a verification code will be sent to your email. Then, enter the code and set a new password.

## 4.2 Setting Face ID / Touch ID

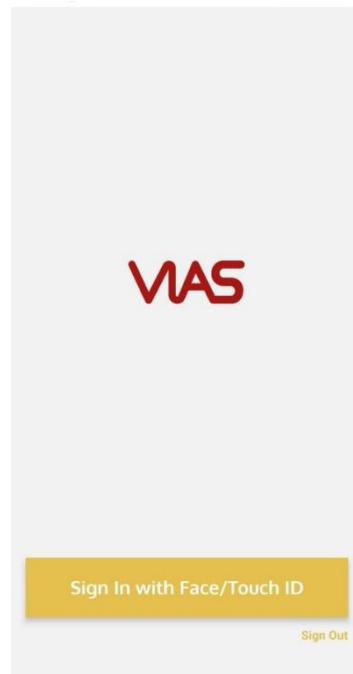
Location: [Dashboard](#) > [Gateways](#)

Using Face ID or Touch ID adds extra security each time you open the app.

1. Tap the top area.



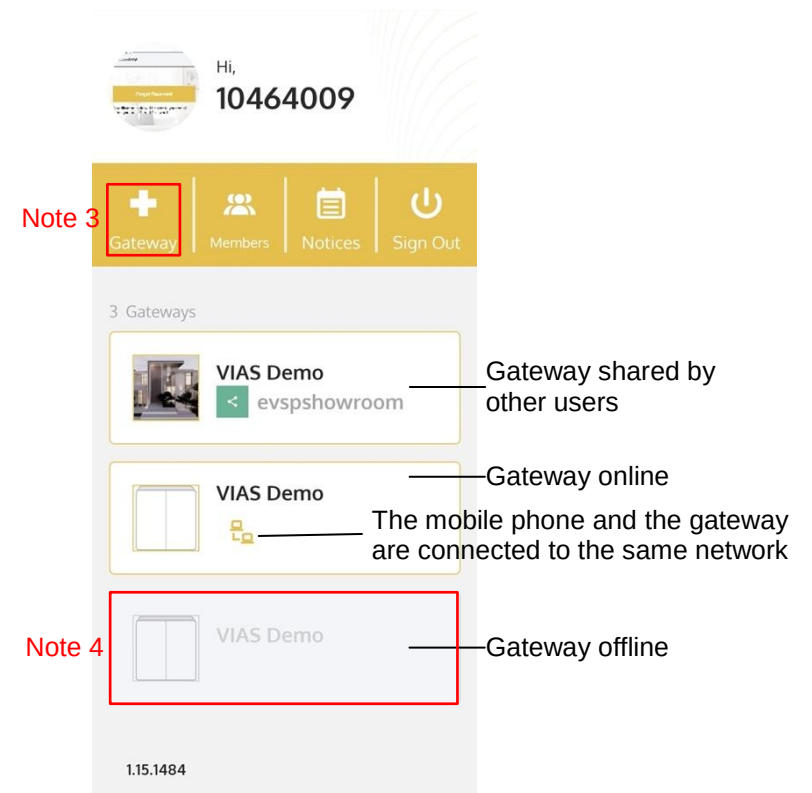
2. Please tap **Enable Face/Touch ID**.

A screenshot of the 'User Information' screen. At the top, there is a back arrow, the text 'User Information', and a checkmark. Below this is a section titled 'Press to select photo' with a circular placeholder containing the 'VIAS' logo. Underneath is a toggle switch for 'Enable Face/Touch ID'. Below the toggle are five input fields: 'Name' (containing 'evspshowroom'), 'Email' (containing 'desmond.chen@everspring.com'), 'Phone', 'Notify Phone', and 'Notify Email'. At the bottom, there is a 'Created At' field showing '2021-11-04 03:58:55'.

## 4.3 Gateway List

After signing in, the first page displayed is the **Gateway List**. This page allows you to efficiently manage all gateways associated with your account. You can add new gateways, remove existing ones, and view their connection statuses at a glance.

Additionally, VIAS allows other users to share their gateways with your account (see Section 5.8.1 – *Adding Users*). Any shared gateways will also be listed in your Gateway List.



Apart from managing gateways, this page also allows you to manage your members. You can invite new members, remove existing ones, and accept invitations from other users to join their member lists.

The Notices tab displays notification not only from your own gateways but also from members' gateways shared with you.  
For example, you will receive a push notification from VIAS whenever any gateway goes offline or comes back online.

#### 4.4 Adding a Gateway to Your Account

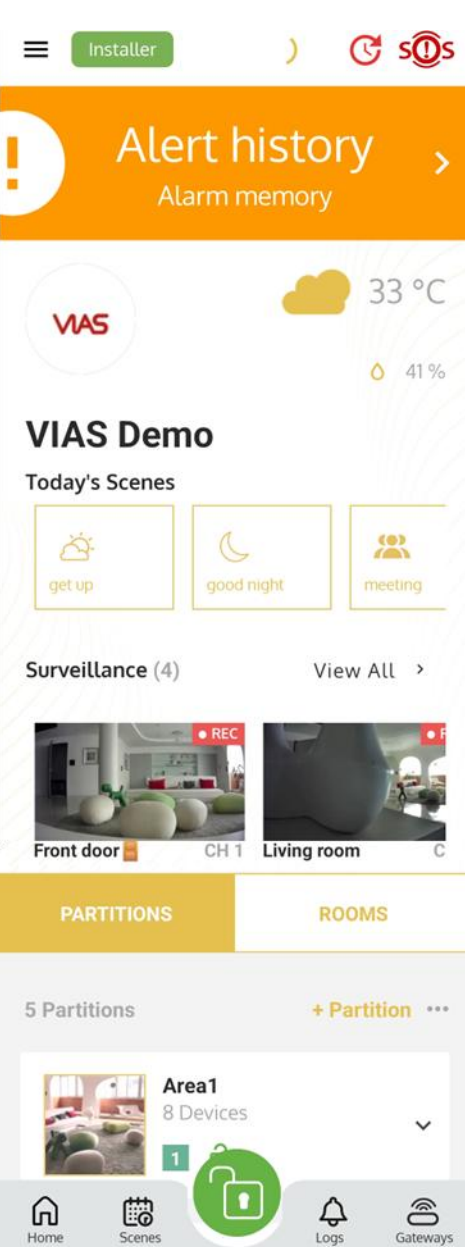
1. Sign in to your account and go to the **Gateway List** page. Then tap **+ Gateway** (see Note 3).
2. Scan the QR code located on the back side of the gateway., the QR code is also located near the SIM card slot inside the gateway.
3. Enter a name for the gateway.
4. Once registered, the gateway will appear in the Gateway list.
5. Tap the newly added gateway to open its **Dashboard** page.
6. Repeat the steps to add additional gateways if needed.

#### 4.5 Removing a Gateway from Your Account

1. Sign in to your account and go to the **Gateway List** page. Press and hold the gateway you wish to remove (see Note 4).
2. Tap the Delete button to confirm and permanently remove the selected gateway.

#### 4.6 Dashboard

Tap on a gateway to open its **Dashboard** view. The dashboard serves as the main interface for each gateway. Its contents will vary depending on the configuration and features of the specific gateway.



The screenshot shows the VIAS Demo mobile app interface. At the top, there's a navigation bar with an 'Installer' button, a menu icon, and a status icon. Below this is an 'Alert history' section with a sub-header 'Alarm memory'. The main area displays 'VIAS Demo' with weather information (33 °C, 41% humidity) and 'Today's Scenes' (get up, good night, meeting). Below that is a 'Surveillance (4)' section showing video snapshots of 'Front door' and 'Living room'. The bottom section is titled 'PARTITIONS' and 'ROOMS', showing '5 Partitions' and a '+ Partition' button. At the very bottom is a 'Bottom Tabs' bar with icons for Home, Scenes, a central alarm control button, Logs, and Gateways.

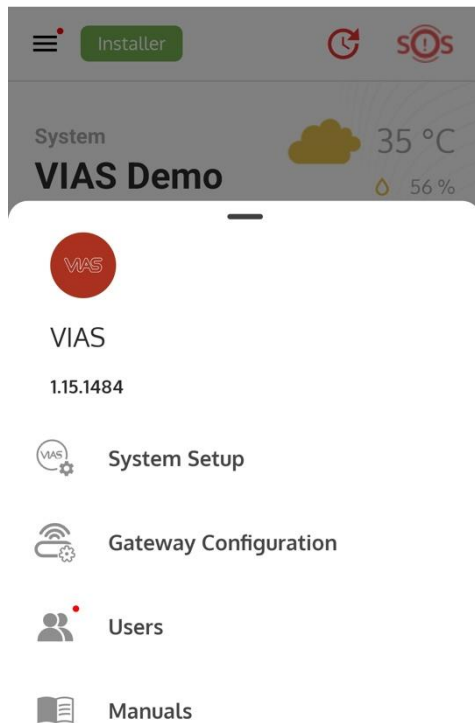
- Menu
- Role
- Refresh
- Update firmware
- SOS panic button
- Notify
  - Alarm alert
  - Alert history
  - Entry / exit delay
- Gateway Information
  - Gateway name
  - Temperature & humidity
- Scenes Section
  - Favorite personal scenes
- Surveillance Section
  - Video snapshots update every 15 mins
- Security Section
  - Partitions
  - Rooms
- Bottom Tabs
  - Central alarm control button
  - Switch other pages

**Note:** A menu icon with a red dot in the top-right corner indicates that the installer has been granted **Allow Access** permission (see Section 5.8.1 – *Editing a User*).

Next to the menu, a green label with white text reading **"Installer"** will appear only when the current user's role is **Installer**.

The **Update Firmware** function can be performed only by users with the roles of **Supervisor** or **Installer**. However, if the Installer disables the Supervisor's panel permission (see Section 5.9 – *Customized Permissions*), then the Supervisor will no longer be able to operate this function.

Tapping the Menu button will display the settings list.



The lower part of the Dashboard is divided into two main tabs: **Partitions**

and **Rooms**. For more details, refer to the next section.

## 4.7 Partitions

Where: [Dashboard > PARTITIONS](#)

In VIAS, a **partition** represents a large, security-protected area that can be armed or disarmed independently. For example, it could be a single floor of a building or a specific area in a home. Typically, the owner creates multiple partitions to logically map the physical structure of the property. In a typical household, you might have separate partitions for the upper floor, lower floor, attic, basement, garage, etc.

Each partition consists of several **zones**, with each zone corresponding to a single device. When a new device is added to VIAS, it is automatically assigned a zone number.

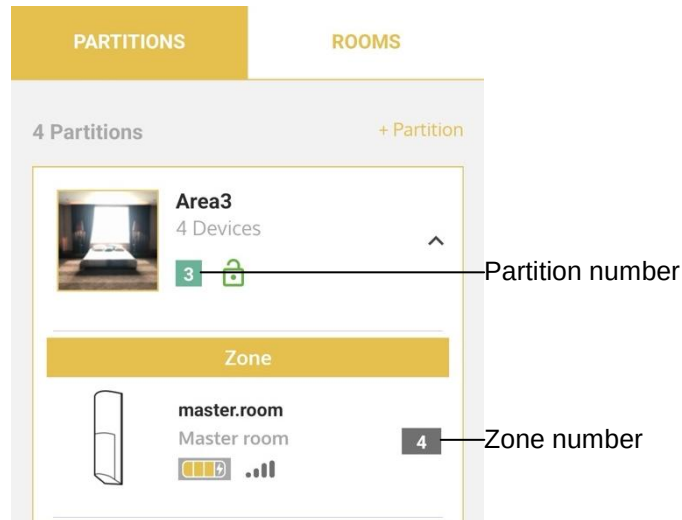
Partitions operate independently, meaning they can be armed or disarmed separately or grouped for simultaneous control. When a partition is armed, all the zones within it are also armed.

**Note:** More advanced configurations are possible. For instance, a *common zone* can be created between partitions to secure shared spaces such as lobbies, hallways, elevators, waiting areas, or parking lots.

Partitions are also linked to user access rights. If a user has restricted access to specific partitions, they will not be able to view or control other partitions. Only the **owner** has full visibility and control over all partitions.

**Note:** For convenience, VIAS provides one default partition upon initial setup.

Partitions and their zones are displayed in the VIAS App under the PARTITIONS section as shown below:



**Note:** Automation devices will not appear under **PARTITIONS**. Instead, they are categorized under **Rooms** or **Devices** within the automation sections.

## 4.8 Rooms

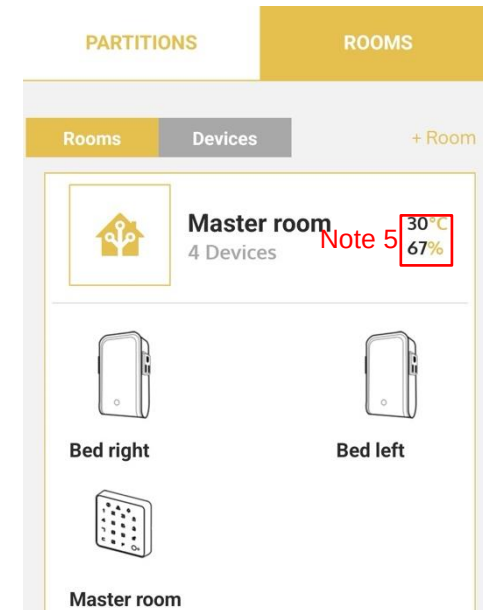
Where: [Dashboard > ROOMS > Rooms](#)

Unlike partitions, a room is a non-security-based grouping of devices designed for home automation purposes. It helps organize devices based on their physical placement within the home, corresponding to real-world room layouts.

Automation devices—such as smart plugs or temperature sensors—that do not participate in alarm functions play an active role in home automation **scenes** and **rules** created under the Scenes section. Some alarm devices, such as door contacts or motion sensors, while primarily assigned to partitions for security purposes, can also be included in rooms for automation use.

**Note:** For convenience, VIAS provides four preset rooms during the initial setup. These rooms can be edited or deleted as needed.

Rooms are displayed on the VIAS App under the **ROOMS** section, as shown below:

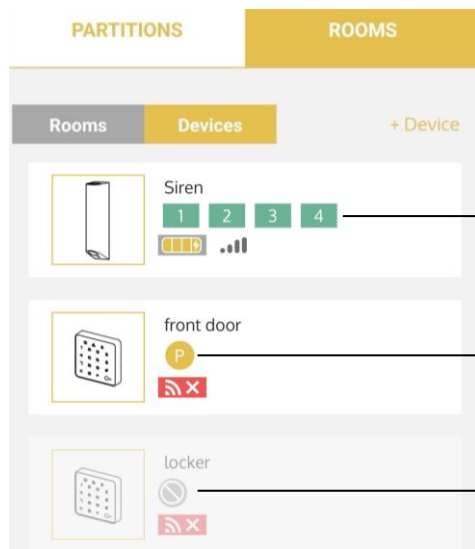


If temperature or humidity sensors are added, their readings will be displayed under each room (see Note 5).

## 4.9 Device list

Where: [Dashboard > ROOMS > Devices](#)

All devices in the system are listed in this section. For each device, you can view its **trigger status**, **signal strength**, and **battery level**.



Indicates the partition number to which this device is assigned.

A device assigned to multiple partition numbers, it's considered part of a **common zone**.

Device isn't assigned to a partition.

The device is temporarily disabled.

The dashboard displays the device status using icons, as shown below:

| Icon | Explanation                            |
|------|----------------------------------------|
|      | Alert triggered.                       |
|      | Tamper detected (ceiling mount).       |
|      | Device is turned on.                   |
|      | Device is turned off.                  |
|      | PIR camera is ready to capture images. |
|      | PIR camera is capturing images.        |
|      | PIR camera is sending images.          |
|      | Motion detected by PIR or camera.      |

| Icon | Explanation                             |
|------|-----------------------------------------|
|      | Smoke detected by smoke detector.       |
|      | Smoke detector siren is active.         |
|      | Smoke detector siren is disabled.       |
|      | Curtain roll up/down level.             |
|      | Curtain tilts level.                    |
|      | Thermostatic radiator in locked mode.   |
|      | Thermostatic radiator in frost mode.    |
|      | Thermostatic radiator in heating mode.  |
|      | Thermostatic radiator window-open mode. |
|      | Battery level.                          |
|      | Low battery level.                      |
|      | AC adapter connected.                   |
|      | Zone is closed.                         |
|      | Intruder alert.                         |
|      | Tamper – cover removed.                 |
|      | RF signal level.                        |
|      | No RF signals.                          |
|      | Device is offline.                      |

## 5. Setting up the System for the First Time

Where: [Dashboard > Menu > System Setup](#)

This page guides you through the **five essential steps** required to properly set up the VIAS system. Tapping each item on the list will take you directly to its respective configuration page.



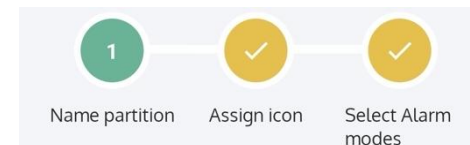
Note: The system must be in **disarmed mode** during configuration. Setup is **not allowed** while the system is armed.

### 5.1 Creating Partitions

#### 5.1.1 Adding Partitions

Where: [Dashboard > Menu > System Setup > ADD PARTITION](#)  
(Alternate path: [Dashboard > PARTITIONS > + Partition](#))

Follow the three-step to complete partition setup.



Note: In Step 2, pressing **Select Photo** allows you to upload a custom image, adjust its angle, resize, and crop it as desired.

#### 5.1.2 Editing a Partition

Where: [Dashboard > PARTITIONS](#)

1. Press and hold the partition you want to edit.
2. Tap the **Save** icon in the upper-right corner to apply changes.

#### 5.1.3 Removing a Partition

Where: [Dashboard > PARTITIONS](#)

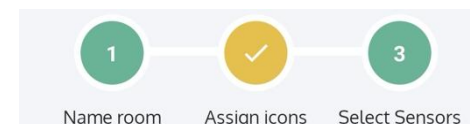
1. Press and hold the partition you want to remove.
2. Tap the **Delete Partition** button to confirm deletion.

### 5.2 Creating Rooms

#### 5.2.1 Adding Rooms

Where: [Dashboard > Menu > System Setup > ADD ROOM](#)  
(Alternate path: [Dashboard > ROOMS > Rooms > + Room](#))

Follow the three-step process to complete room setup.



Note: In Step 2 of adding a partition or room, tapping **Select Photo** allows

you to upload your own image, then adjust the **angle**, **size**, and **crop** as needed.

### 5.2.2 Editing a Room

Where: [Dashboard > ROOMS > Rooms](#)

1. Press and hold the room you wish to edit.
2. Tap the **Save** icon in the top-right corner to apply changes.

### 5.2.3 Removing a Room

Where: [Dashboard > ROOMS > Rooms](#)

1. Press and hold the room you wish to remove.
2. Tap the **Delete Room** button to confirm deletion.

## 5.3 Creating Devices

### 5.3.1 Adding Devices

Where: [Dashboard > Menu > System Setup > ADD DEVICE](#)

(Alternate path: [Dashboard > ROOMS > Devices > + Device](#))

All wireless devices follow a standard binding process that is quick and easy. This typically involves pressing a button on the device and observing the LED indicator.

Steps:

1. Select the device model and follow the instructions shown.
2. After detection, configure the device settings:
3. Enter the **device name** (required).
4. A **zone number** will be assigned automatically.
5. Set the **ZONE TYPE** and **ZONE BEHAVIOR** (see section 5.4).
6. Assign the device to a **partition** and a **room** from the dropdown lists.
7. Tap **SUBMIT** to save the configuration.
8. Return to *Dashboard > ROOMS > Devices*. The new device will appear in the list.

### 5.3.2 Editing a Device

Where: [Dashboard > ROOMS > Devices](#)

1. Tap the device you want to edit.
2. Tap the **SAVE** button to apply changes.

### 5.3.3 Removing a Device

Where: [Dashboard > ROOMS > Devices](#)

1. Tap the device you want to remove.
2. Tap the **DELETE** button to confirm.

## 5.4 Sensor Information Page

Where: [Dashboard > ROOMS > Devices > any device](#)

Each device has a dedicated configuration page. From here, you can adjust which **partitions** and **rooms** the device is assigned to. For **security sensors**, this is also where **zone configuration** is managed.

### 5.4.1 ZONE TYPE:

- **ENTRY:** Entry delay allows time to disarm the system when entering.
- **EXIT:** Exit delay provides time to leave after arming the system.
- **ENTRY AND EXIT:** Combines both delays for the same zone.
- **FOLLOW ZONE:** This zone does not trigger an alarm if a "Entry/Exit" zone has previously activated the entry delay time. An immediate alarm is triggered if no entry delay has previously been activated. Use this zone type for a motion detector in the entrance area, directed at the entrance door (which is fitted with a magnetic contact), for example. • If an instant zone was triggered, or nothing was triggered before, it should also work as an instant zone.
- **INSTANT:** Alarm is triggered immediately when the zone is activated.
- **DAY ZONE:**
  - If system is armed: triggers alarm and creates event log.
  - If disarmed: sends a notification, but no event is logged.
- **24 HOUR BURGLARY:** Always active, regardless of system arming state.
- **24 HOUR FLOOD:** Triggers an instant alarm when flood is detected.
- **24 HOUR SMOKE:** Triggers an instant alarm when smoke is detected.
- **LOCK MONITORING:**
  - Prevents arming if zone is open.
  - Does **not** trigger alarm if opened while system is armed.

Note: To activate the siren when a zone is triggered, make sure **Siren Audible** is enabled under ZONE BEHAVIOR.

#### 5.4.2 ZONE BEHAVIOR

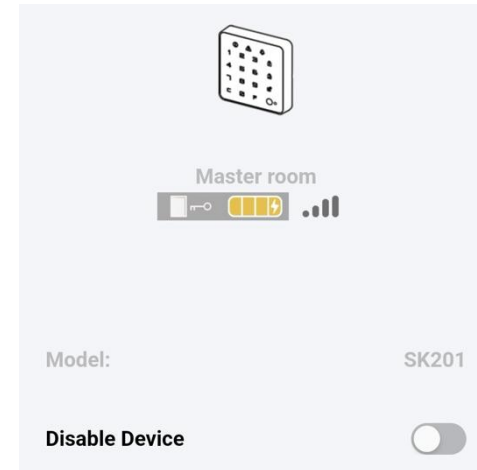
- **Bypass Enable:** When this setting is enabled, the zone can be manually bypassed. If disabled, the zone must be ready in order for the system to be armed.  
For zones configured as **EXIT** or **ENTRY AND EXIT**, the gateway will only check the device's status at the end of the delay period.  
  
If the device is not ready and Bypass Enable is ON, the system will force arm and ignore any activity in this zone.  
If the device is not ready and Bypass Enable is OFF, the system will remain in disarmed mode.
- **Transmission Delay:** When enabled, zone alarms will be delayed for a programmed time before being sent to the system.
- **Siren Audible:** When enabled, the zone will trigger the siren sound during an alarm event.

Note: By default, all zones have Siren Audible enabled.

#### 5.4.3 DISABLE DEVICE

VIAS allows a device to be temporarily disabled for maintenance purposes. Once disabled:

- The device will appear in light grey on the dashboard.
- The alarm system will ignore it, even when the system is armed.
- Any event or trigger from this device will not activate an alarm.



#### 5.4.4.4. LAST RSSI

This section displays the Last RSSI (Received Signal Strength Indicator) for the device, measured in (dB). This value helps assess the wireless communication strength between the device and the gateway.

### 5.5 Testing Devices RF Signal Strength

Where: [Dashboard](#) > [ROOMS](#) > [Devices](#) > any device

According to EN50131 certification, alarm systems must include a signal test mode with reduced transmission power to ensure stable operation, even in environments with poor RF conditions. This test applies specifically to security devices such as door contacts, motion sensors, and sirens.

1. Press the START RF LINK TEST button to begin the signal strength test.
2. When prompted by the app, trigger the sensor. The device will then transmit a signal every 5 seconds.
3. Move the sensor to different locations and observe how the Last RSSI values change.
4. Press the STOP button to exit the test mode.

Please refer to the chart below for RSSI values, bar display, RF bar color, and installation recommendations:

| RSSI value | Bar display | RF bar color | Remark                   |
|------------|-------------|--------------|--------------------------|
| > -100     | 0 bar       | Red          | Unstable, do not install |

| RSSI value | Bar display | RF bar color | Remark                |
|------------|-------------|--------------|-----------------------|
| -96 ~ -100 | 1 bar       | Yellow       | Weak, do not install  |
| -91 ~ -95  | 2 bar       | Green        | Low, stable operation |
| -86 ~ -90  | 3 bar       | Black        | Good                  |
| < -86      | 4 bar       | Black        | Excellent             |

Note: The system will automatically exit test mode after 5 mins.

## 5.6 Users and access

### 5.6.1 Overview

VIAS APP is designed for installers to set up and register gateways for users. Once a user registers an account and the installer can hand over the gateway by add the User after installation. The first user to receive the shared gateway becomes the highest privilege owner of that gateway, with full control. This owner supervisor can add other users to access the gateway and assign them different User Types. Additionally, they can restrict access or include other installers to provide ongoing services and configuration.

There are 4 types of users:

1. Installer: Installers who set up the panels and make configuration **except Zone bypass**. Installer can test the system after set up the configuration while the owner of panel can limit the right for installer to access and operate the system.
2. Owner Supervisor (Red): The one who scans the QR code when adding the gateway which has most highest level of configuration rights including shared the gateway and assign different access rights to the users. The owner (Supervisor in Red color) always possesses the right to operate the system.  
While configuration right can be enabled or disabled by the Installer.
3. Supervisor (Green): The Users has been set by owner as Supervisor to operate partly or full operation of system except they are not able to adding the Users.
4. Local User: Created by Owner to operate the system only through remote keyfob and keypad, and there are email and mobile can be set to receive notification as well. The local user is for the ones who don't need to use the APP to be a temporarily visitor to operate the system.

### 5.6.2 Members

Where: [Dashboard > Gateways > Members](#)

Members function similarly to a friend list and are mainly used to select users when adding new members to a gateway. In the members list, you can view who has invited you to join as a member, track invitations you have sent, and see which gateways have been shared with you.

### 5.6.3 Users

Where: [Dashboard > Menu > Users](#)

The gateway owner can add users via email, from the member list, or locally. Users can be assigned different access rights, such as supervisor or installer, allowing them to arm or disarm the system, view cameras, or only receive notifications.

The person who scans the QR code on the gateway during the initial installation becomes the owner. The system allows only one owner, and only the owner can add or remove users.

## 5.7 Members

### 5.7.1 Inviting Members

Where: [Dashboard > Gateways > Members](#)

VIAS allows you to invite users who have a registered account to join your member list.

1. Tap the add icon at the top right corner.
2. Enter the user's email address and press the search icon.
3. The invitation will appear in the Invite section.

Note: If the email address has not been registered before, the system will automatically send an invitation email to that address.

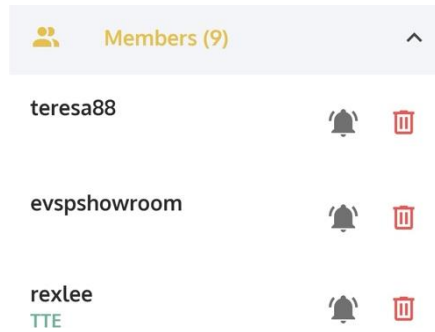
4. To cancel an invitation, press the cancel icon next to the invitation in the Invite section, then confirm by pressing the Cancel button.

### 5.7.2 Accepting Invitation

Where: [Dashboard > Gateways > Members](#)

To accept an invitation, please press the accept icon on the right side in the Invited section. If you do not wish to join, you can also reject the invitation.

Once accepted, you will appear in the Members section.



The green text indicates the gateways that have been shared with you by the member.

### 5.7.3 Muting Notifications

Where: [Dashboard > Gateways > Members](#)

If you prefer not to receive push notifications from a member who is sharing their gateways, or from a specific user, you can simply tap the alert icon to mute them. This setting overrides the notification preferences configured under: (Dashboard > Menu > Users > any user > Settings).

### 5.7.4 Removing Members

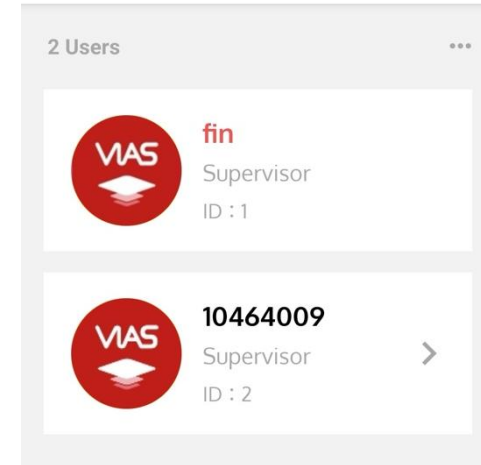
Where: [Dashboard > Gateways > Members](#)

1. To remove a member, tap the trash icon next to the member you want to remove.
2. Confirm the action by pressing the **Delete** button if you are sure you want to remove this member.

Note: Any gateways previously shared with you by this member will be removed once the member is deleted.

## 5.8 Users

Only the account owner, indicated in red, has permission to add or delete users. Installers are indicated in green. User IDs start from ID 1.



### 5.8.1 Adding Users

Where: [Dashboard > Menu > System Setup > ADD USER](#)  
(Other way: [Dashboard > Menu > Users > Add User button](#))

There are three ways to add a user:

1. Invite a New User
  - 1.1 Enter the user's email in the **Search New User** field.
  - 1.2 Select a permission type in the **Permission** section (see section 5.6.3 Users).
  - 1.3 If the user is already registered, they will be added to the gateway. If not, they will receive an invitation to create an account.
  - 1.4 Tap the **Save** icon in the top-right corner, then confirm by pressing **Yes**.
2. Choose from My Members
  - 2.1 Select a permission type in the **Permission** section (see section 5.6.2 Users).
  - 2.2 Select a member under **Share Gateway to Member**.
  - 2.3 Tap the **Save** icon in the top-right corner, then press **Yes** to confirm.
3. Create a Local User
  - 3.1 Enter the user's name.
  - 3.2 Optionally, enter an email address and phone number to enable SMS, email, and voice call notifications.

Note: To add members to the member list, see section 5.7 Members.

3.3 Tap the **Save** icon in the top-right corner, then confirm by pressing **Yes**.

### 5.8.2 Editing a User

Where: [Dashboard](#) > [Menu](#) > [Users](#) > any user

On the user editing page, settings are divided into three sections, described as follows:

1. **Permission** – Defines the user's access level for this gateway. For advanced settings, refer to section 5.9 *Permissions*.
2. **PIN Code** – Grants the user the ability to arm/disarm the system via keypad. The PIN must be 4 digits and numeric only.
3. **Allow Access** – Determines whether the user is allowed to access the gateway. This option is enabled by default. If an installer has access allowed, a red dot will appear next to their name, as shown below:

Where: Dashboard



Where: Menu



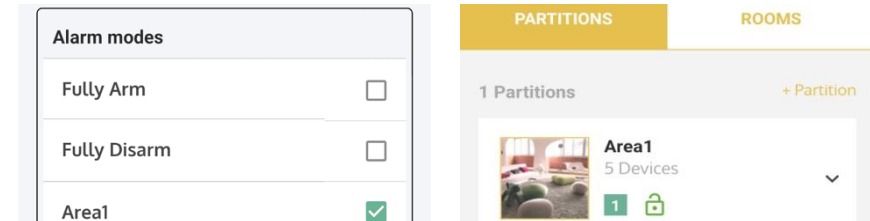
Where: [Dashboard](#) > [Menu](#) > [Users](#)



Where: [Dashboard](#) > [Menu](#) > [Users](#) > user with installer permission



4. **Voice Call Enable** – Please refer to section 9.3 *Voice Call Notification*.
5. **Notification Catalogs** – Please refer to section 9 *Notifications*.
6. **Alarm Modes** – Defines which partition(s) the user can view, arm, and disarm. If you wish to restrict the user to only view specific areas, please disable Fully Arm and Fully Disarm, as shown below:



### 5.8.3 Removing a User

Where: [Dashboard](#) > [Menu](#) > [Users](#) > any user

1. To remove a user, tap the Delete User button next to the user you wish to remove.
2. Confirm the deletion by pressing **Yes** if you are sure you want to remove this user.

### 5.8.4 Ownership transfer process

To help you better understand how gateway users sharing according to our system operation, here are two key scenarios:

1. When Sharing the Gateway

First user binding the gateway as Installer will be the owner of panel (Installer A in Red).

In the meantime, he can add more installers where can be seen on the user list.

After the installation is done and the Installer A sharing the gateway to a user as Supervisor (User E)

→ The ownership will be transferred to the Supervisor as owner of gateway (User E).

After the transfer:

Only users who are members of the new Owner (User E) will be able to see the gateway.

Users not related to User E (e.g., User D) will no longer see the gateway on their gateway list.

User E the owner still can invite Installer B and C back to be installers on the User list after transfer.

If the Installer B and C are already the members of the User E on the member list. They still can see the panel on gateway list after transferred.

Example:

| User    | Relationship to User E | Gateway Visibility |
|---------|------------------------|--------------------|
| A, B, C | Members of User E      | Visible            |
| D       | Not a member           | Disappeared        |

## 2. When Deleting the Gateway

### a. If the Owner is a Supervisor (User E):

When the Owner Supervisor deletes the gateway:

→ Ownership will be transferred to the last shared Installer (e.g., User D).

→ All other users (except local users) will be removed from the gateway.

Example:

| User    | Permission                    | Gateway Visibility |
|---------|-------------------------------|--------------------|
| A, B, C | Installer                     | Removed            |
| D       | Installer (added as last one) | Owner              |
| E       | Supervisor (Owner)            | Removed            |
| Local   | Local User                    | Not Affected       |

### b. If the Owner is an Installer:

When the Installer deletes the gateway:

→ All users will be removed (except local users).

→ The gateway will go back to an unbound state.

Example:

| User       | Permission        | Gateway Visibility |
|------------|-------------------|--------------------|
| A, B, C, D | Installer         | Removed            |
| E          | Installer (Owner) | Removed            |
| Local      | Local User        | Not Affected       |

## 5.9 Customized permissions

You can customize each permission type based on your requirements. By default, the supervisor always has full access to operating system such as arming/disarming, controlling devices, and run automation. The installer

always can configure system settings. Before introducing the available operations, we will first explain the functions can be set by each permission type for installer and supervisor.

### 5.9.1 Supervisor Permission Configuration by Installer

Where: [Dashboard > Menu > Users > Setting icon \(top right corner\)](#)

| Permission            | Description                                                                                                                                                                                                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Panel                 | Enable or disable: <ul style="list-style-type: none"> <li>Backup.</li> <li>Firmware Updates.</li> <li>Access to the System Setup page (Dashboard &gt; Menu).</li> <li>Editing settings for Gateway Configuration and Permission Types.</li> <li>Adding, editing, and removing Partitions, Rooms, and Alarm Modes.</li> </ul> |
| Security Devices      | Enable or disable adding, editing, and removing devices (e.g., Magnetic Sensor, Keypad, and Siren).                                                                                                                                                                                                                          |
| Smart Home Devices    | Enable or disable adding, editing, and removing devices (e.g., Switch, Plug, and Module).                                                                                                                                                                                                                                    |
| Automation and Scenes | Enable or disable adding, editing, and removing Scenes.                                                                                                                                                                                                                                                                      |

Note: Only installers can configure a supervisor's permissions. The "+Device" button (located at [Dashboard > ROOMS > Devices](#)) will be hidden when both Security Devices and Smart Home Devices permissions are disabled.

### 5.9.2 Installer Permission Configuration by Supervisor

Where: [Dashboard > Menu > Users > Setting icon \(top right corner\)](#)

| Permission                     | Description                                                                                                                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scenes And Devices Executive   | Enable or disable the operation of Devices and Scenes.                                                                                                                                                                           |
| Security with / without Bypass | Allows zones to be bypassed manually. However, installers cannot perform bypass operations themselves.                                                                                                                           |
| Camera                         | Enable or disable: <ul style="list-style-type: none"> <li>Displaying channels on the dashboard.</li> <li>Viewing video from push event notifications.</li> <li>Adding and editing push-event video actions in scenes.</li> </ul> |

| Permission | Description                                          |
|------------|------------------------------------------------------|
| PIRCAM     | Enable or disable viewing of photos for each PIRCAM. |

Note: Only a supervisor can assign permissions to an installer.

### 5.9.3 Customized Permissions

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [Setting icon \(top right corner\)](#)

| Permission                     | Description                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scenes And Devices Executive   | Allows enabling or disabling the operation of Devices and Scenes.                                                                                                                                                   |
| Security with / without Bypass | Permits manual bypass of the zone, with or without bypass mode.                                                                                                                                                     |
| Camera                         | Allows enabling or disabling the following features: <ul style="list-style-type: none"> <li>• Displaying camera channels on the dashboard.</li> <li>• Viewing video from push event video notifications.</li> </ul> |
| PIRCAM                         | Enable or disable viewing of photos for each PIRCAM.                                                                                                                                                                |

Note: Customized permission do not allow adding, editing, or deleting Partitions, Rooms, Devices, or Scenes.

### 5.9.4 Permanent Permissions

When configuring different permission types, some functions remain unaffected. For example, users with customized permissions can still arm or disarm the system and trigger a panic alert.

Please refer to the table below for detailed function availability across permission types:

| Function                               | Supervisor | Installer | Customized |
|----------------------------------------|------------|-----------|------------|
| Arming and Disarming                   | O          | O         | O          |
| Panic Alert                            | O          | O         | O          |
| Bypass Alert                           | O          | △         | △          |
| Operating Devices and Scenes           | O          | △         | △          |
| Showing Camera Channels                | O          | △         | △          |
| Viewing Push Event Video Notifications | O          | △         | △          |

| Function                                                                      | Supervisor | Installer | Customized |
|-------------------------------------------------------------------------------|------------|-----------|------------|
| Adding, Editing, Removing Push Event Video Notification Actions within Scenes | O          | △         | △          |
| Updating Firmware                                                             | △          | O         | △          |
| Accessing the System Setup Page                                               | △          | O         | △          |
| Editing Gateway Configuration and Permission Type Settings                    | △          | O         | △          |
| Adding, Editing, Removing Partitions, Rooms, Alarm Modes, Devices, and Scenes | △          | O         | △          |

### 5.9.5 Creating Permission Types

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [Setting icon \(top right corner\)](#)

Steps:

1. Tap the Create Permission Type button.
2. Enter a name for the new permission type.
3. Select the required functions, then tap the Save icon at the top right.

### 5.9.6 Editing Permission Types

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [Setting icon \(top right corner\)](#) > [Select any existing permission type](#)

Steps:

1. Tap the permission type you wish to edit.
2. Select or deselect the necessary functions.
3. Tap the Save icon at the top right to apply changes.

Note: The name of a permission type **cannot be edited** once it has been created. Only function selection is allowed.

### 5.9.7 Removing Permission Types

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [Setting icon \(top right corner\)](#) > [Select any existing permission type](#)

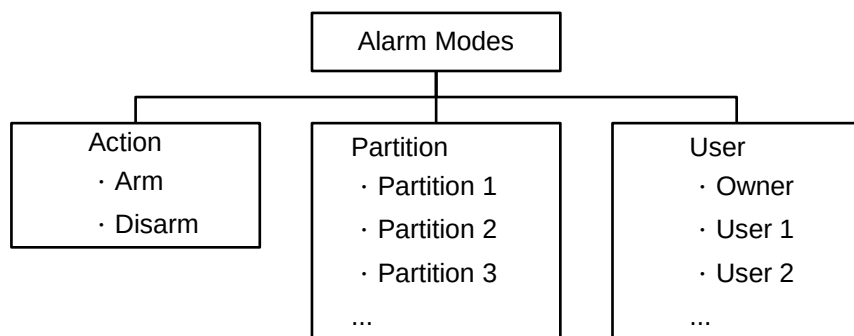
Steps:

1. Tap the permission type you wish to remove.
2. If you are sure you want to delete it, tap the Delete Permission Type button.

## 5.10 Alarm Modes Workflow

### 5.10.1 Overview

Alarm modes are the foundation of the VIAS alarm system. Each alarm mode defines a specific relationship between users and partitions, determining which users have permission to arm or disarm which partitions.



When a user arms or disarms the system, they are activating a specific alarm mode.

For example:

- Triggering a part-arm from the keypad.
- Pressing a button on the remote keyfob (that has been assigned to a particular alarm mode) will activate that alarm mode.

You can create multiple alarm modes to suit different combinations of users and partitions. Users assigned to a particular alarm mode will only have visibility and control over the specific partitions included in that mode. This functionality is useful for environments where multiple organizations share the same system (e.g., separating staff from two different companies operating under a single gateway).

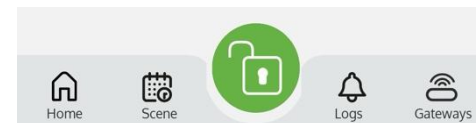
**Note:** VIAS includes two preset alarm modes— Fully Arm and Fully Disarm—which always include all partitions in the system.

### 5.10.2 Executing an Alarm Mode

Where: [Dashboard](#) > [Central Alarm Control Button](#)

Steps:

1. The central alarm control button on the dashboard displays the system's current status: Armed, Disarmed, or Part-Armed.



2. Tap the button to reveal the available alarm modes. Then, select any alarm mode (e.g., Disarm, Part-Arm, or Arm) to execute it.



Disarm



Part-Arm

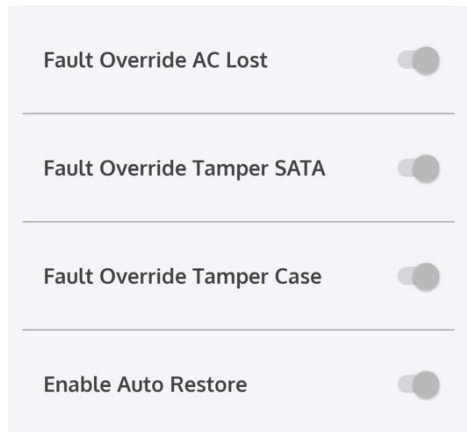


Arm

System Behavior:

- In Arm mode:  
If a sensor is triggered, the dashboard will show an Alarm Alert, and users will receive a push notification.
- In Disarm mode:  
Users can view the Alert History, including sensors that haven't been restored, and logs related to panic, tamper, flood, smoke, and other events.

By default, when devices are restored, their records will be automatically cleared from Alert History. If you prefer to keep these logs, you can disable auto-clearing by toggling the Enable Auto Restore option:  
[Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [Settings icon \(top right\)](#) > [Alarm](#).



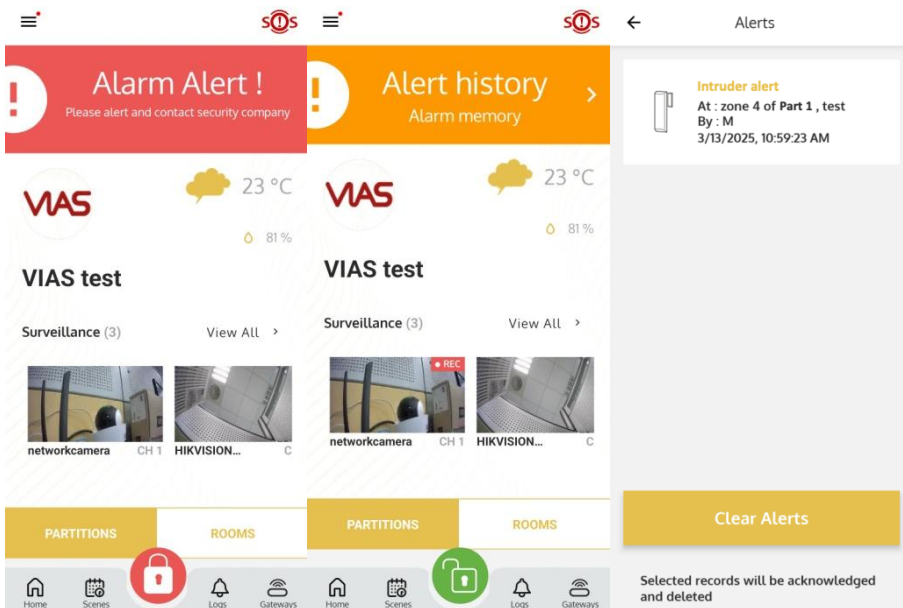
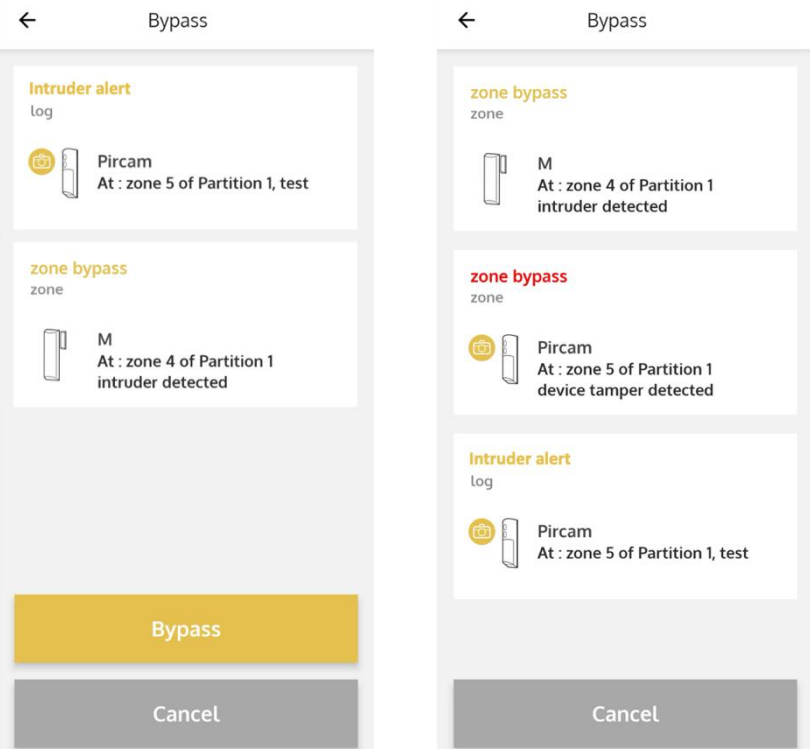
- A sensor is malfunctioning.
- A user wants to leave a window or door open during arming.

Steps:

1. On the Sensor Information page (see Section 5.4), tap the Bypass Enable option for the sensor you wish to bypass.
2. Return to the dashboard and press any desired alarm mode to arm the system.

Bypass Page Behavior:

- The Bypass page shows:
  - Alert History entries that haven't been cleared.
  - Sensors that have been triggered.
- If a sensor has bypass capability enabled, a Bypass button will be shown next to it.
- If a sensor cannot be bypassed, it will appear in red in the list.



### 5.10.3 Bypassing Sensors

Where: [Dashboard](#) > [Central alarm control button](#)

Bypassing a sensor allows VIAS to ignore a specific sensor when arming the system. All other sensors will still be monitored. This feature is useful when:

Note: Installers do not have permission to bypass sensors.

#### 5.10.4 Force Arming

The key difference between Force Arming and Bypassing is that Force Arming skips the manual bypass process, allowing the system to arm immediately, even if certain sensors are open or triggered.

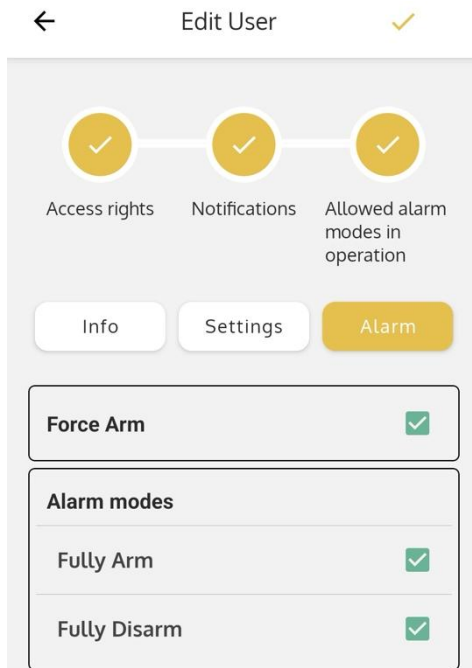
This can be done via the App, Keypad, or Keyfob.

- Using the App

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [Select a User](#) > [Alarm](#)

Steps:

1. Enable the Force Arm toggle.



2. Tap the Save icon (top right).
3. Return to the dashboard and press any Alarm Mode to execute it.

Note: Installers cannot bypass sensors or use Force Arm.

- Using the Keypad

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [Settings icon \(top right\)](#) > [Duress](#)

Steps:

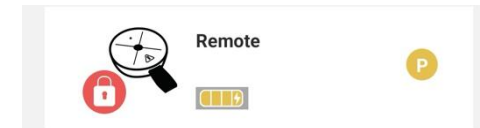
1. Enter a 3-digit Force Arm Code.
2. Tap the Save icon.
3. On the keypad, enter your 4-digit PIN code, then press the Force Arm code to arm.
4. To activate Stay Mode using Force Arm:  
Enter 4-digit PIN code + 3-digit Force Arm code + Part-Arm icon + Alarm Mode ID.

- Using the Keyfob

Where: [Dashboard](#) > [ROOMS](#) > [Devices](#) > [Select a Keyfob](#)

Steps:

1. Toggle the Force Arm switch to enable.
2. Tap the **SAVE** button.
3. The keyfob will display a lock icon, indicating Force Arm is active.



#### 5.10.5 Creating an Alarm Mode

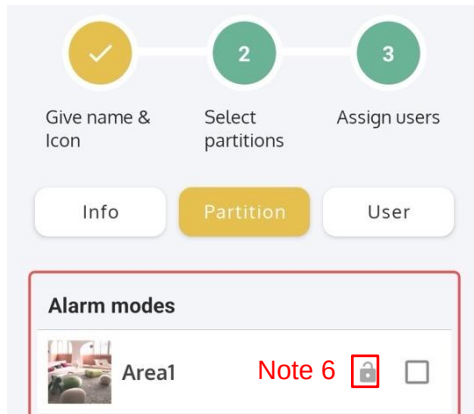
Where: [Dashboard](#) > [Menu](#) > [System Setup](#) > [ADD ALARM MODE](#)  
(Alternate path: [Dashboard](#) > [Central Alarm Control Button](#) > [Settings Icon \(top right\)](#) > [Add Alarm Mode](#))

In addition to the default Fully Arm and Fully Disarm modes, VIAS allows you to create custom alarm modes that can arm or disarm specific groups of partitions.

Steps:

1. Enter a name for the new alarm mode.
2. Select the partitions to be included in this mode.
3. Next to each selected partition, tap the lock icon (see Note 6) to

toggle its behavior between arm or disarm.



4. Select the users who will have permission to operate this alarm mode.
5. Tap the Save icon (top right) to complete the setup.

**Note:** Only users who have been previously invited will appear in the user list. Only selected users will see this alarm mode in the Alarm Modes page.

#### 5.10.6 Editing an Alarm Mode

**Where:** Dashboard > Central alarm control button > Settings Icon (top right)

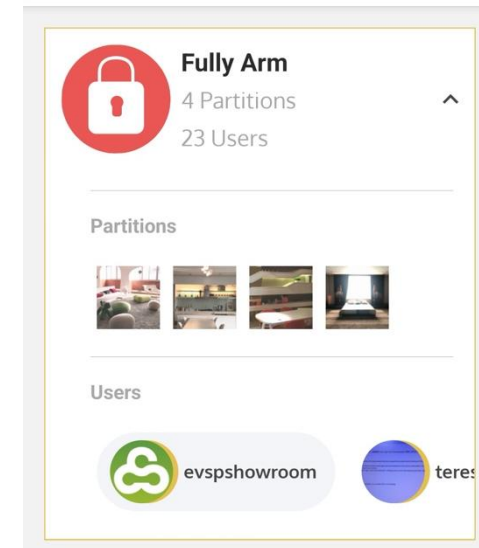
This page displays all the available alarm modes.

Tap on any folded block to view the details including:

- The partitions associated with the alarm mode.
- The users who have permission to operate it.

From here, you can review and edit each mode as needed.

← Alarm Modes Manage



Steps:

1. Tap and hold the alarm mode you want to edit.
2. Make any necessary changes.
3. Press the Save icon (top right) to apply the changes.

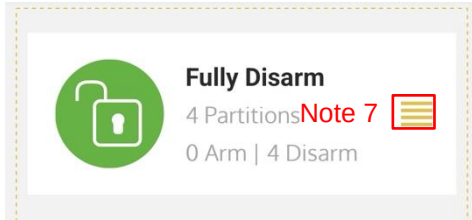
You can also modify the list of partitions and users under each alarm mode: Tap and hold on the relevant section to access its settings page.

**Note:** The default alarm modes— Fully Arm and Fully Disarm—cannot be edited.

#### 5.10.7 Adjusting Alert Mode Sequences

**Where:** Dashboard > Central Alarm Control Button

1. To edit the alert mode sequences, tap the arrow icon on the top right corner.
2. Press and hold the alignment icon on the right (see Note 7), then drag it to your desired position.



3. To exit edit mode, tap the arrow icon on the top right corner again.

#### 5.10.8 Removing an Alarm Mode

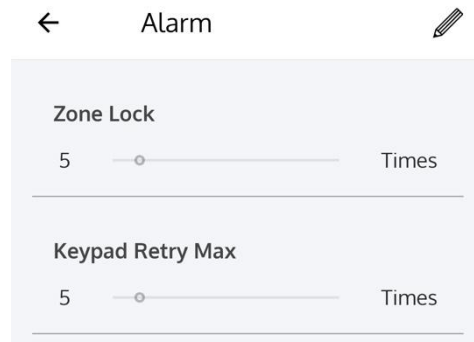
Where: [Dashboard](#) > [Central Alarm Control Button](#) > [Settings Icon \(Top Right\)](#)

1. To remove an alarm mode, press and hold the alarm mode you wish to delete.
2. If you are sure you want to remove this alarm mode, tap the **Delete Alarm** button.

### 5.11 Alarm System Settings

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [Settings Icon \(Top Right\)](#) > [Alarm](#)

This section allows you to configure various security-related settings.



The following options can be configured:

- **Zone Lock:** When the same alarm is triggered more times than the specified limit, it will stop activating. No notifications or records will be generated until the alarms are cleared from the alarm history. Default:

5 times.



- **Keypad Retry Max:** If the number of incorrect keypad entries exceeds the limit, the keypad will be locked. The lock duration depends on the Keypad Timeout setting. Default: 5 times.
- **Keypad Timeout:** Duration of keypad lock after exceeding the retry limit. Default: 30 seconds.
- **Entry Delay:** Delay before alarm activation when a device is triggered in arm mode. Default: 10 seconds.
- **Exit Delay:** Delay before the system enters arm mode. Default: 30 seconds.
- **Transmission Delay:** If enabled, the reporting of zone alarms will be delayed by the configured time.
- **Power Loss Report Delay:** Reports a power outage after the defined delay. Default: 0 minutes.
- **Intruder Siren:** Enabled by default. Duration: 60 seconds.
- **Tamper Siren:** Enabled by default. Duration: 60 seconds.
- **Panic Siren:** Enabled by default. Duration: 60 seconds.
- **Flood Siren:** Enabled by default. Duration: 60 seconds.
- **Smoke Siren:** Enabled by default. Duration: 60 seconds.
- **SOS Siren:** Enabled by default. Duration: 60 seconds.
- **Fault Override:** When disabled, the system cannot be armed if faults are present. Default: Disabled.
- **Maintenance:** When enabled, this mode prevents alarms or tamper triggers during system maintenance. The system must be disarmed before activating this mode. Default: Disabled.

To edit these settings, tap the edit icon in the top right corner. After making your changes, tap the icon again to save.

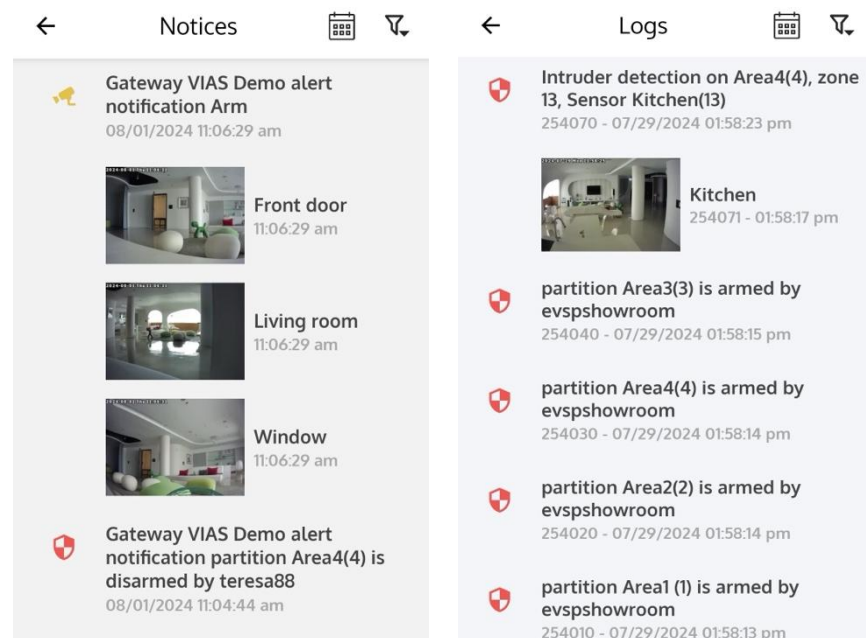
Note: Entry / Exit Delay can be set separately by zones on sensor information page.

## 5.12 Viewing the Event Logs

VIAS provides two locations where event logs can be accessed:

1. Dashboard > Gateways > Notices.
2. Dashboard > Logs.

The key difference is that the first option displays event logs from **all gateways**, while the second shows logs for a **specific gateway** only. Both views support filtering by event type and date.



Event logs are stored in the gateway and will be automatically overwritten once the number of entries exceeds 10,000.

## 6. Surveillance Settings

VIAS alarm system seamlessly integrates with any IP camera that supports the ONVIF standard, providing high-quality video monitoring and flexibility in camera selection.

**Note:** If the camera supports Wi-Fi, it must first be connected to the home

router via Wi-Fi before it can be detected by VIAS.

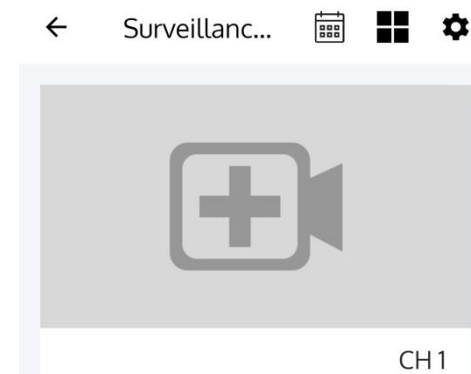
For some camera brands, such as Hikvision and Dahua, ONVIF is disabled by default. Please make sure to enable ONVIF in the camera settings before using it with VIAS. Refer to the camera's user manual for detailed instructions.

The username and password entered here are the credentials used to access the camera via ONVIF. In some cases, these credentials may differ from the ones used to log into the camera's main setup interface.

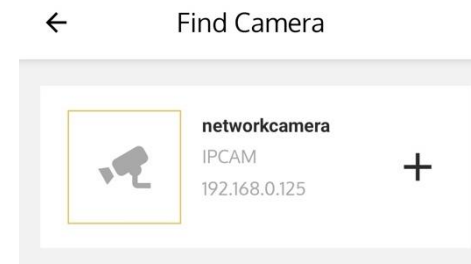
## 6.1 Adding Cameras Manually

Where: [Dashboard](#)

1. Tap **View All** in the Surveillance section, then select any camera with the **add icon**.



2. The system will display all automatically detected cameras.

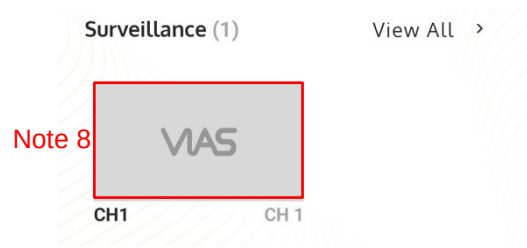


3. Tap the **add icon** on the right side of the desired camera.
4. On the channel setup page, enter the **Camera Name**, **Username**, and **Password**.
5. Tap the **save icon** in the top right corner to save the settings and return to the dashboard.
6. Once the camera is successfully added, a snapshot from the video feed will appear on the screen.

## 6.2 Adding Cameras Automatically

Where: [Dashboard](#)

When the gateway is bound for the first time, cameras on the same network will be automatically detected.



1. Tap the snapshot icon (see Note 8).
2. On the channel setup page, enter your Camera Name, Username, and Password.
3. Tap the save icon in the top right corner to save the settings and return to the dashboard.
4. Once the camera is successfully added, a video snapshot will appear on the screen.

## 6.3 Surveillance Setting Page

Where: [Dashboard](#) > [View All On Surveillance Section](#) > [Settings Icon \(Top Right\)](#)

- **Auto Search Camera:** Scans for cameras on the same network and adds them automatically to the gateway. Default setting: Enabled.  
*Note: If any cameras are removed, this setting will be disabled.*
- **File Retention:** Sets the number of days to retain video files, as long

as the hard drive has available space.

*Note: Videos are recorded 24/7 on the SSD or HDD. Older files will be overwritten when storage is full.*

- **Download Stream Type:** Choose between Main Stream and Sub Stream for video downloads.
- **Disconnect Debounce:** Reduces the frequency of online/offline status updates when brief disconnections occur.

## 6.4 Recording Modes

VIAS system offers four types of video recording:

1. **24-Hour Recording:** Continuous recording from all camera channels, regardless of alarm status. Recording starts automatically when the gateway is powered on.
2. **Arm Record Only:** Records video only when the corresponding partition is in **arm** mode.
3. **Record on Event Only:** Stores a short 15-second video clip when an alarm event occurs (5 seconds before and 10 seconds after the event).
4. **No Recording:** Disables video recording entirely.

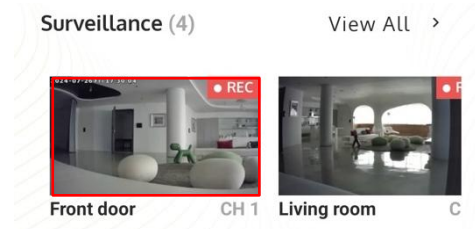
### 6.4.1 Assigning Partitions

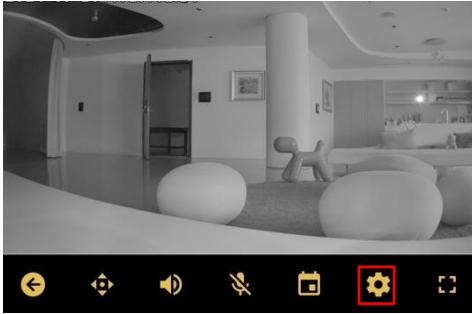
Where: [Dashboard](#)

Before setting up recording modes, two preliminary steps must be completed.

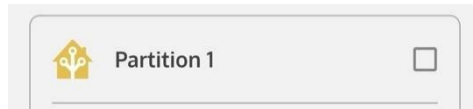
First, cameras must be assigned to different partitions in order to manage recording independently.

1. Tap the camera you want to configure, then press the setting icon.





2. Select the partition(s) where you want to assign the camera for recording.



3. Press the SAVE button to apply the changes.

#### 6.4.2 Installing Storages

The gateway records video onto SSD or HDD storage devices.

**Note:** MicroSD cards only support "Record on Event" mode.

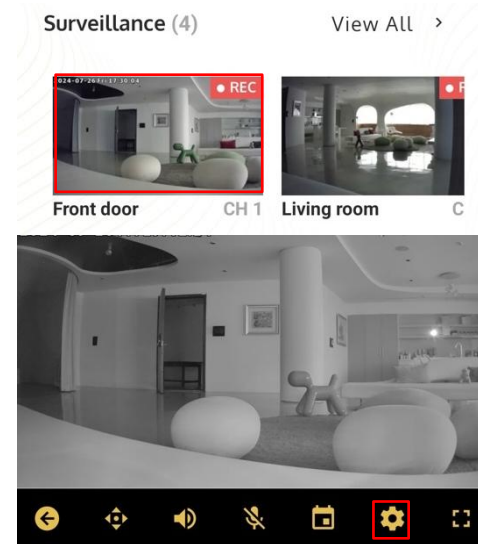
Please ensure both the power and backup battery is disconnected before installing the SSD or HDD. Once powered on, the gateway will automatically detect and check the format of the storage device.

- During this process, the Power LED will blink orange to indicate the formatting check.
- When complete, the Power LED will turn solid green.
- You can then view the storage information via:  
Dashboard > Menu > Gateway Configuration > Settings Icon (Top Right) > General Information

#### Setting Recording Modes

Where: [Dashboard](#)

1. Tap the camera you want to configure, then press the settings icon.



2. Tap the settings icon in the top right corner.
3. Select the desired Recording Mode.
4. Tap the save icon in the top right to apply the changes.

The Main Stream and Sub Stream determine the camera's video quality for live viewing, storage, and downloading. Below are the maximum and recommended settings for different numbers of connected cameras:

1. SC109 Maximum Settings

- Main Stream

| Number of Cameras | Bit rate (kbps) | FPS | GOV |
|-------------------|-----------------|-----|-----|
| 1                 | 4096            | 30  | 30  |
| 2                 | 2048            | 30  | 30  |
| 3                 | 1365            | 30  | 30  |
| 4                 | 1024            | 30  | 30  |

- Sub Stream

| Number of Cameras | Resolution | Bit rate (kbps) | FPS | GOV |
|-------------------|------------|-----------------|-----|-----|
| 1                 | 352 x 240  | 1536            | 30  | 30  |
| 2                 | 352 x 240  | 768             | 30  | 30  |
| 3                 | 352 x 240  | 512             | 30  | 30  |
| 4                 | 352 x 240  | 384             | 30  | 30  |

## 2. SC109 Recommend Settings

- Main Stream

| Number of Cameras | Resolution | Bit rate (kbps) | FPS | GOV |
|-------------------|------------|-----------------|-----|-----|
| 1                 | 1280 x 720 | 2048            | 30  | 30  |
| 2                 | 1280 x 720 | 1024            | 15  | 15  |
| 3                 | 1280 x 720 | 768             | 15  | 30  |
| 4                 | 1280 x 720 | 512             | 15  | 30  |

- Sub Stream

| Number of Cameras | Resolution | Bit rate (kbps) | FPS | GOV |
|-------------------|------------|-----------------|-----|-----|
| 1                 | 352 x 240  | 768             | 15  | 15  |
| 2                 | 352 x 240  | 512             | 15  | 15  |
| 3                 | 352 x 240  | 384             | 15  | 30  |
| 4                 | 352 x 240  | 384             | 15  | 30  |

## 3. SC115 Maximum Settings

- Main Stream

| Number of Cameras | Bit rate (kbps) | FPS | GOV |
|-------------------|-----------------|-----|-----|
| 1                 | 8192            | 30  | 30  |
| 2                 | 8192            | 25  | 25  |
| 3                 | 8192            | 16  | 16  |
| 4                 | 8192            | 12  | 12  |
| 5                 | 6144            | 10  | 10  |
| 6                 | 5120            | 8   | 8   |
| 7                 | 4096            | 7   | 7   |
| 8                 | 4096            | 6   | 6   |

- Sub Stream

| Number of Cameras | Resolution | Bit rate (kbps) | FPS | GOV |
|-------------------|------------|-----------------|-----|-----|
| 1                 | 1280 x 720 | 2048            | 30  | 30  |
| 2                 | 1280 x 720 | 2048            | 30  | 30  |
| 3                 | 1280 x 720 | 2048            | 30  | 30  |
| 4                 | 1280 x 720 | 2048            | 30  | 30  |
| 5                 | 1280 x 720 | 2048            | 30  | 30  |
| 6                 | 1280 x 720 | 2048            | 30  | 30  |
| 7                 | 1280 x 720 | 2048            | 30  | 30  |
| 8                 | 1280 x 720 | 2048            | 30  | 30  |

## 4. SC115 Recommend Settings

- Main Stream

| Number of Cameras | Resolution  | Bit rate (kbps) | FPS | GOV |
|-------------------|-------------|-----------------|-----|-----|
| 1                 | 1920 x 1080 | 4096            | 30  | 30  |
| 2                 | 1920 x 1080 | 4096            | 30  | 30  |
| 3                 | 1920 x 1080 | 4096            | 30  | 30  |
| 4                 | 1920 x 1080 | 4096            | 30  | 30  |
| 5                 | 1920 x 1080 | 4096            | 30  | 30  |
| 6                 | 1920 x 1080 | 4096            | 30  | 30  |
| 7                 | 1920 x 1080 | 4096            | 28  | 28  |
| 8                 | 1920 x 1080 | 4096            | 25  | 25  |

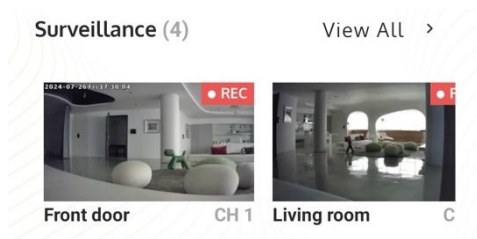
- Sub Stream

| Number of Cameras | Resolution | Bit rate (kbps) | FPS | GOV |
|-------------------|------------|-----------------|-----|-----|
| 1                 | 640 x 480  | 1024            | 30  | 30  |
| 2                 | 640 x 480  | 1024            | 30  | 30  |
| 3                 | 640 x 480  | 1024            | 30  | 30  |
| 4                 | 640 x 480  | 1024            | 30  | 30  |
| 5                 | 640 x 480  | 1024            | 30  | 30  |
| 6                 | 640 x 480  | 1024            | 30  | 30  |
| 7                 | 640 x 480  | 1024            | 30  | 30  |
| 8                 | 640 x 480  | 1024            | 30  | 30  |

## 6.5 Camera Operation

Where: [Dashboard](#)

The Surveillance section of the dashboard displays a snapshot preview for each camera channel, which updates automatically every 15 minutes.



VIAS supports both single-channel and multi-channel live video viewing:

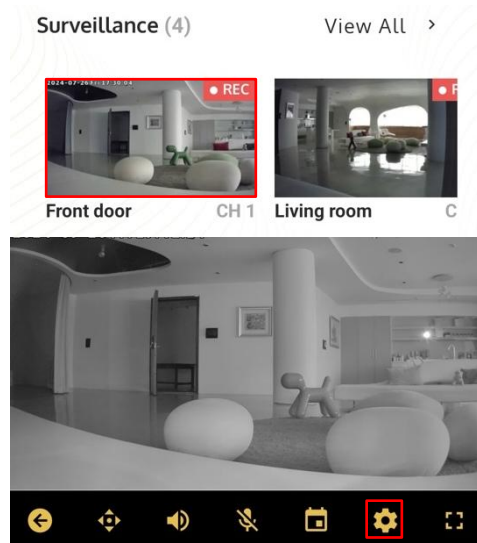
- Single-channel view uses the Main Stream.
- Multi-channel view uses the Sub Stream.

For stream settings, please refer to section 6.4.3 Setting Recording Modes.

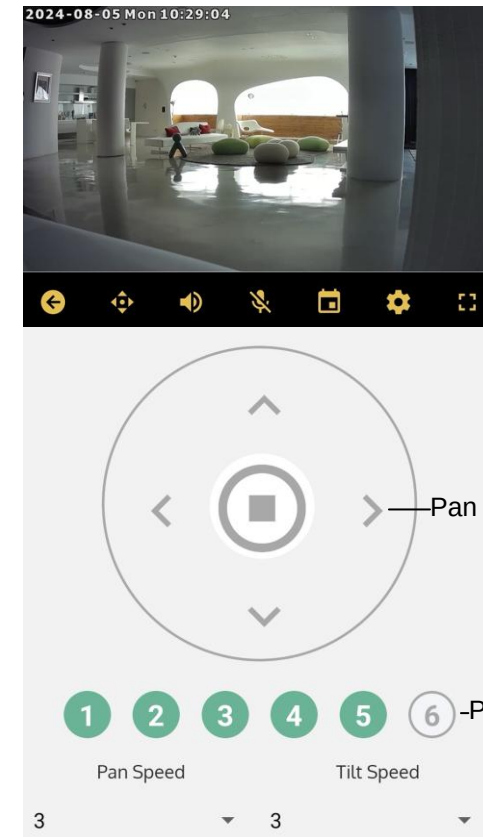
### 6.5.1 Single-channel

Where: [Dashboard](#)

1. Please press the camera you wish to view.



You will see seven buttons for various functions:  
Back, Pan and Tilt, Audio, Speaker, Playback Recording, Channel Settings, and Full Screen.



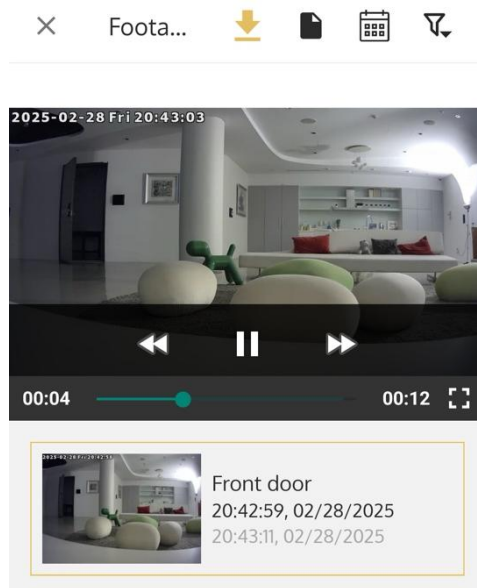
Button Descriptions:

- Back: Returns to dashboard.
- Pan and tilt: Allows movement of the camera. VIAS provides six preset buttons; a green button indicates that a preset position is stored. Pressing the button moves the camera to that position.
  - To store a new preset, press and hold a white button for 3 seconds.

- You can also adjust the movement speed.
- Preset points can be linked with scenes (e.g., when the door opens, the camera moves to the entrance). See section 8 Automation.

**Note:** The camera must support pan and tilt functionality.

- Audio: Toggles the incoming sound from the camera on or off.
- Speaker: Enables or disables speaking to the camera.
- Playback Recording: Displays recordings in chronological order. Each clip lasts up to 15 minutes.



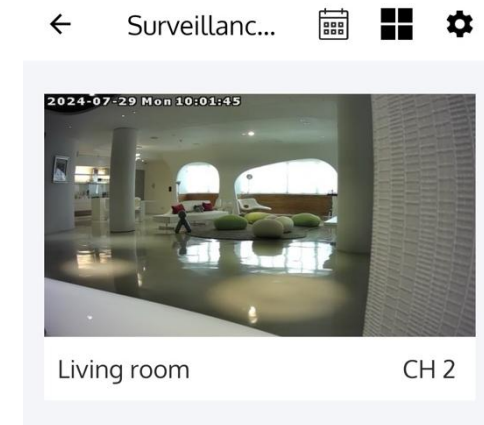
- During playback, you can scrub the time bar, view full screen, or download the video.
- Use the calendar to locate recordings from specific dates. Tap the calendar icon to show/hide it. You can filter the playback list by camera.
- Channel Settings:  
On this page you can:
  - Enable or disable the camera.
  - Change the camera display name.
  - Assign the camera to partitions.

- Enable motion detection (functions as a zone sensor – see 6.5.3).
- Sync camera time with the gateway.
- Adjust Network Caching Time:
  - Shorter time: less real-time delay, but requires a stable network.
  - Longer time: more delay, but works better on weaker networks.

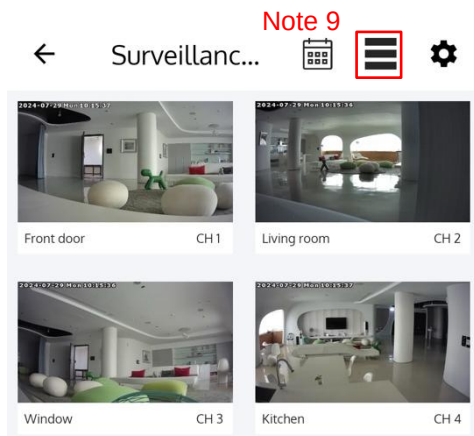
## 6.5.2 Multi-channel

Where: [Dashboard](#)

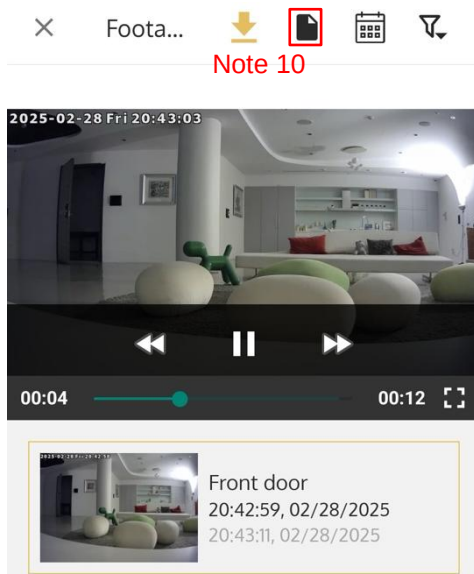
1. Please press View All.



2. You can press the display icon (see note 9) to switch the display mode.



The calendar shows the playback list sorted by recording date and time, with which clip lasting up to 15 minutes. By default, only event recording clips are displayed. You can press the second icon (see note 10) to toggle between 24-hour continuous recording and armed recording clips.



During playback, you can drag the time bar to move forward or backward, switch to full-screen mode, or download the video.

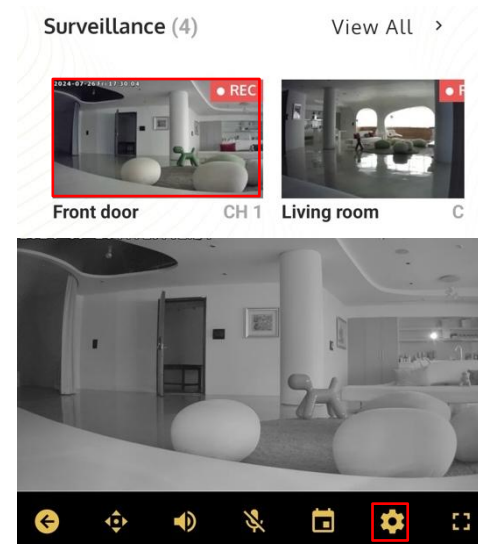
You can also use the calendar to search for past recordings. Press the calendar icon to show or hide the calendar, and use the filter to view the playback list by selected cameras.

### 6.5.3 Motion Detection

Where: [Dashboard](#)

When this feature is enabled, the camera functions as a sensor. Additionally, when Motion Alarm is activated, an alarm will trigger if movement is detected while in arm mode.

1. Please select the camera and press the setting icon.

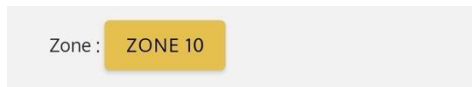


2. Enable Motion Detection, then press the save icon at the top right to apply the changes.

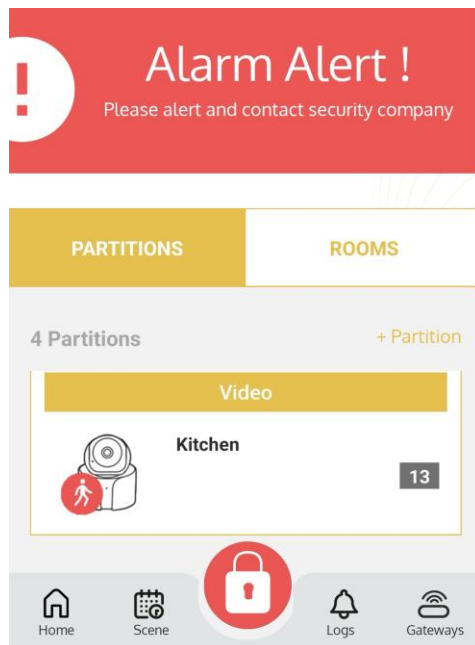


Note: Cameras must be assigned to partitions for managing monitoring and video verification.

- Press the yellow area to be redirected to the device's setting page.



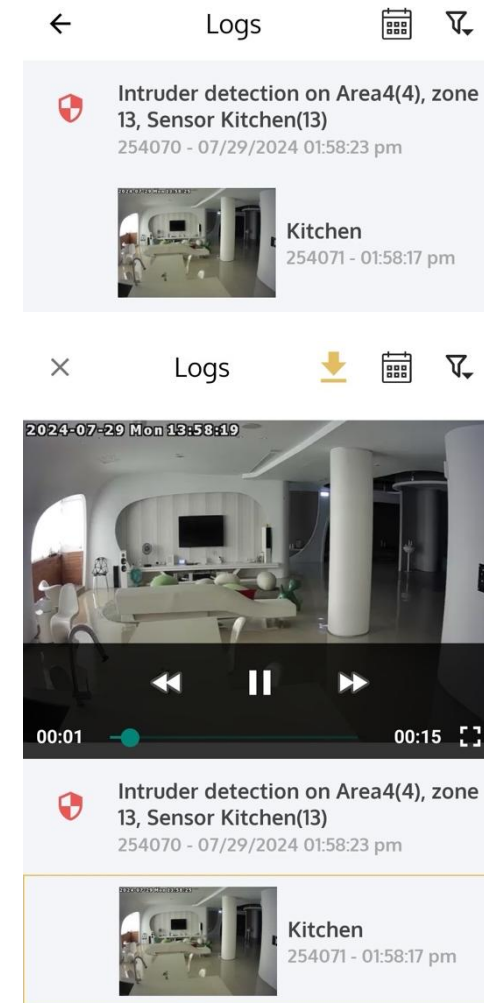
- Enable Motion Alarm, then press the SAVE button to apply the changes.
- When motion is detected, the camera will display a red moving icon and trigger an alarm event.



- You can view the video clip on the Logs page at Dashboard > Logs. Each clip includes 5 seconds of pre-recording and 10 seconds of event recording.

During playback, you can drag the time bar to move forward or backward, switch to full-screen mode, or download the video.

You can also use the calendar to search for past recordings. Press the calendar icon to show or hide the calendar, and use the filter to view the playback list by selected cameras.



- Users who share access to the gateway can also view video clips on the Notices page at Dashboard > Gateways > Notices. All functions here are similar to those on the Logs page.

#### 6.5.4 Push Event Video

When an alert or automatic scene is triggered, sends a push notification with video clips of the recording along with the event notification to users in the assigned partitions. Simply pressing the push message will immediately play the video clip.

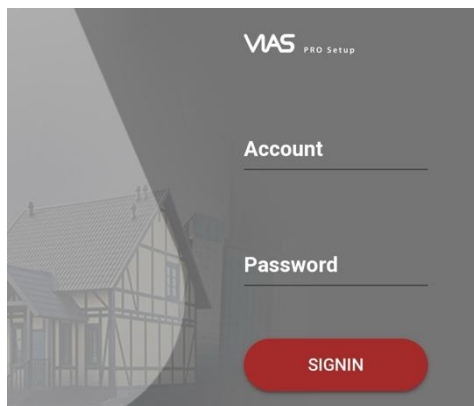
You can also view the video clip through the mailbox:

1. Press the screenshot of the video you want to view.

Intruder detection on Area4(4), zone 13,  
Sensor Kitchen(13)



2. Enter your Account and Password, then press the SIGN IN button.



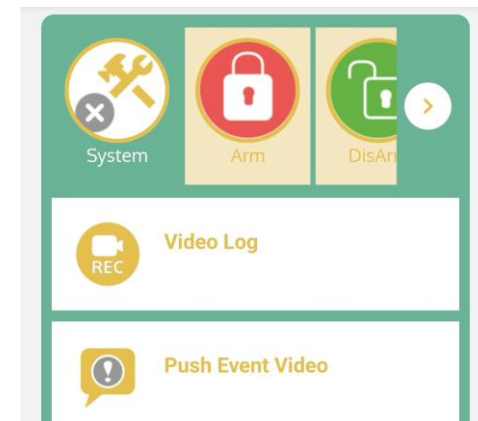
3. Once signed in successfully, you will be able to watch the video clip.



In addition to alarm event push notifications, VIAS allows you to share customized event video notifications with your friends or neighbors via advanced settings.

This can be configured in SCENES and AUTOMATION at Dashboard > Scenes:

1. Press + Add Scenes or + Add Automation.
2. Press + Add Actions in the third step.
3. Select System, then choose the Push Event Video.



4. Enter the Push Event Video Message.
5. Select the users to whom you want to send the message and choose the cameras.
6. Press the add icon on the right and then the save icon on the top right to apply the changes.



## 7. Gateway Configurations

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#)

This page displays the operating status of the gateway. You can:

- Edit the Gateway Name.
- Change the gateway's photo.
- Check the Network connection via Wire or 4G.
- Check the modem status, including SIM card detection, GSM voice call support in the area, and signal strength to the base station.
- View the IMEI number.
- See the current firmware version and update to a new version when available.

### 7.1 General Information

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [General Information](#)

This page shows the storage status and date & time.

### 7.2 Monitoring Center connection

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [SIA CD-09](#)

Add or edit information required for reporting to the monitoring center using the SIA DC-09 protocol.

Note: If multiple SIA settings exist, the system will prioritize the first SIA setting.

#### 7.2.1 Adding a SIA Setting

1. Press the Add SIA button.
2. Enter the Service Name.
3. Enter the Account, IP and Port provided by the service provider.
4. Press the save icon on the top right.

Note: Some providers may require AES encryption or need Receive Number or Account Prefix. Please configure according to your provider's instructions.

#### 7.2.2 Editing a SIA Setting

1. To edit a SIA setting, select the SIA you want to edit.
2. Press the save icon (top right).

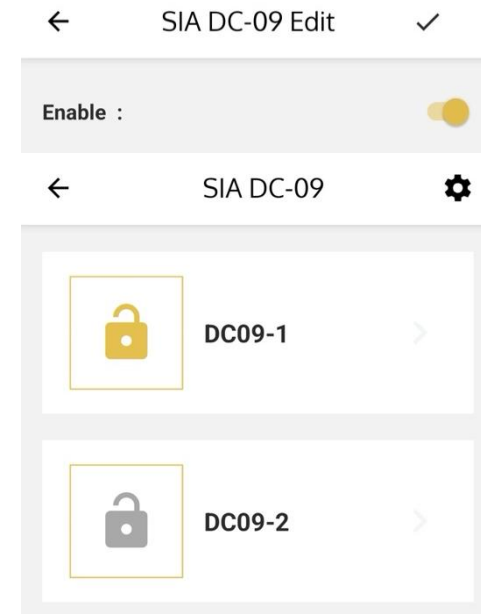
#### 7.2.3 Removing a SIA Setting

1. To remove a SIA setting, select the SIA you want to delete.
2. Press the Delete SIA button to confirm removal.

#### 7.2.4 Disabling a SIA Setting

VIAS allows disabling a SIA setting for maintenance, temporarily suspending its function in the system.

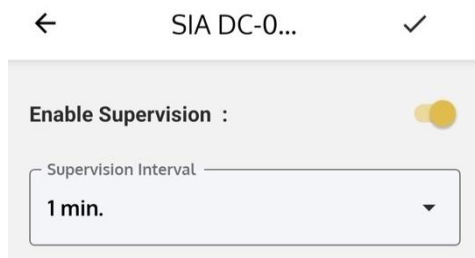
Once disabled, the SIA setting will be shown with a light lock icon in the list.



## Heartbeat

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > settings icon (top right) > SIA CD-09 > settings icon (top right)

When connected to the monitoring center, the system periodically sends signals to confirm the connection is active.

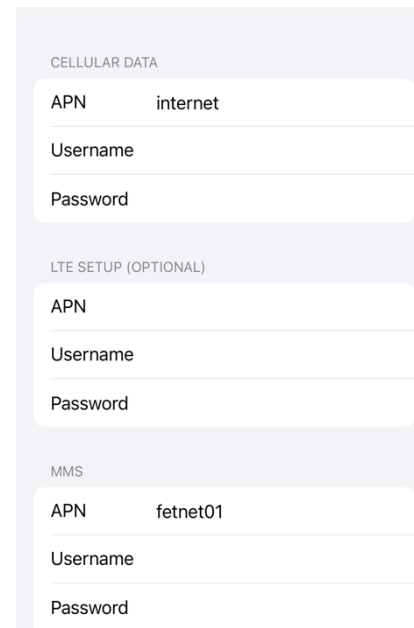


## 7.3 Connection to 4G

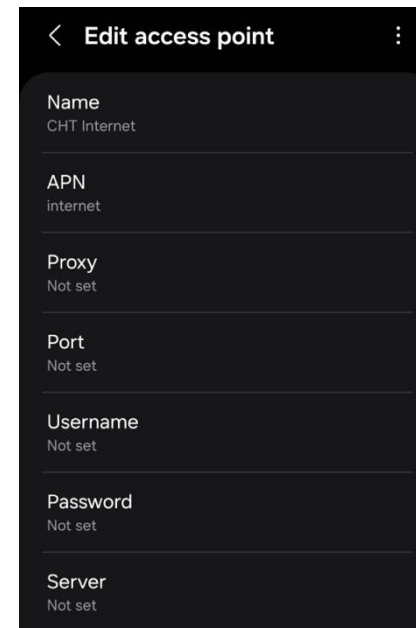
Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > settings icon (top right) > Modem

Please place the SIM card in the slot to enable 4G connectivity for controlling the system, and make sure to turn off the PIN code before inserting the SIM card.

Please type the APN, User Name and Password. For information related to the APN, please refer to the images below:



iOS: Settings > Cellular > SIM card provider > Cellular Data Network



Android: Settings > Connections > Mobile networks > Access Point Names

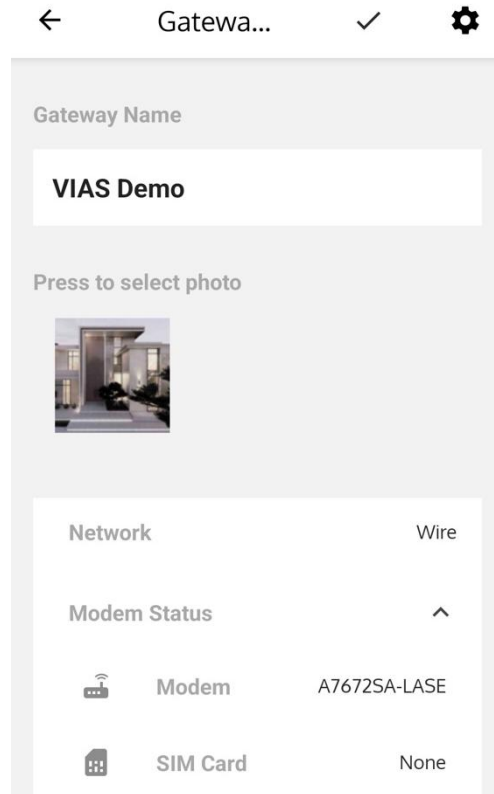
**Note:** Some may require APN authentication. Please configure according to the SIM card provider's instructions.

The connection status can be checked in [Dashboard](#) > [Gateway Configuration](#) > [Modem Status](#) > [SIM Card](#) will display OK when it is installed successfully; otherwise, it will show None.

### 7.3.1 LET Function

In this setting page, you can also disable the Enable option to turn off the LET function. The system will log who disabled this function and will not display network failure messages if the SIM card is used for SMS instead of internet.

We suggest keeping this function enabled because of the security alarm EN50131.



When both wired and 4G connections are available, the wired connection will take precedence, and the network status will show Wire; otherwise, it will show 4G.

Note: Please insert the SIM card into the slot before powering on the gateway, and power it off if you want to replace the SIM card. The gateway will detect the SIM card when it is powered on.

## 7.4 Network Communication Interface

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [Network](#)

There are three methods of network connection:

1. Static: A static Internet Protocol (IP) address is a fixed address

permanently assigned by an Internet Service Provider (ISP). Please enter the required information on the page, then press the save icon on the top right to confirm the settings.

2. DHCP: Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that automatically assigns an IP address and other related configuration information to a device. This is the default setting.
3. PPPoE: Point-to-Point Protocol over Ethernet is a network protocol that connects via an ISP and requires a username and password. Please enter the username and password, then press the save icon on the top right to confirm the settings.

Note: Incorrect static IP settings will prevent the panel from connecting to the network, making it unreachable through the app. If this occurs, press and hold the CONNECT button on the panel for 10 seconds, then release it. The panel will reboot and reset the network settings to default DHCP.



## 7.5 Duress

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [Duress](#)

Disarm under duress is used when an intruder forces you to disarm the system. Duress can be triggered while disarming via the keypad.

When activated, the system will disarm as usual but will also send duress disarm report to the monitoring center, log the event, and notify other users connected to the same gateway.

### 7.5.1 Duress through Keypad

1. Create a 3-digit duress code. The default setting is 911.
2. Press the save icon on the top right to apply.
3. To activate duress mode, enter this code immediately after your PIN on the keypad.

### 7.5.2 Force Arming Through Keypad

Please follow the same steps as described in section 5.10.4 Force arming.

## 8. Automations

Where: [Dashboard > Scenes](#)

VIAS provides more than 100 customizable automation combinations, allowing flexible setup tailored to your needs.

The Scenes page contains two sections:

1. SCENES: Automation scenes that can be triggered immediately.
2. AUTOMATION: Rules that are activated by time or specific events.

Please refer to the instructional video for guidance on setting up automation.



### 8.1 SC115 Automation Setting

Where: [Dashboard > Scenes](#)

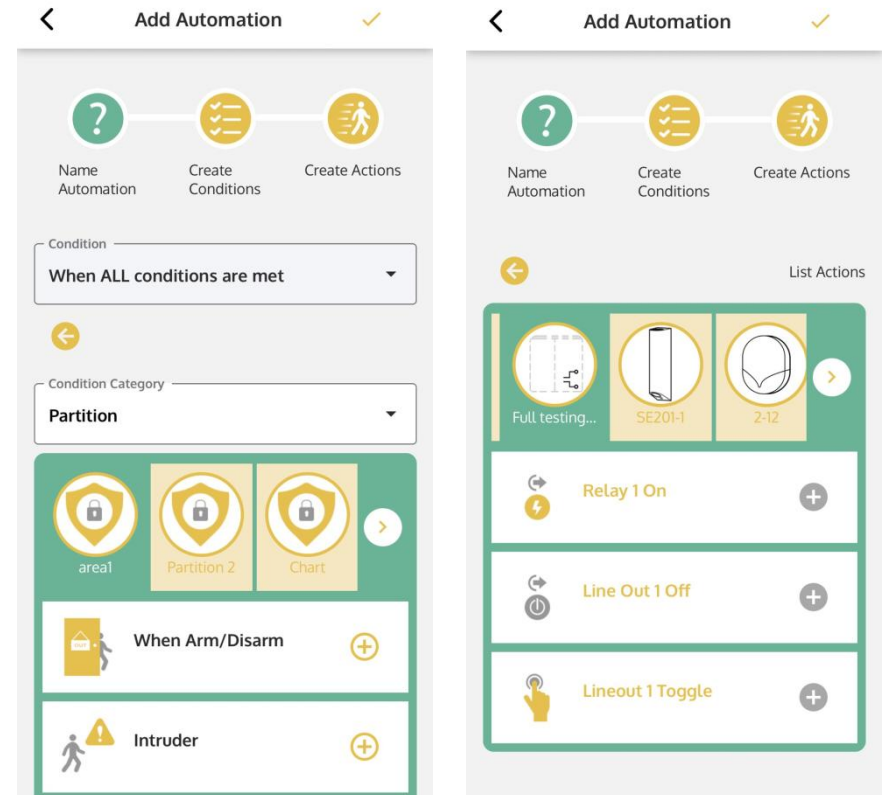
The SC115 supports triggering relay operations through scenes and automations. Available actions include Relay 1 on, line out 1 off, line out toggle.

For example, if you would like a wired internal siren to sound for 2 minutes when a partition is intruded, and then stop automatically after 120 seconds,

you can set this up by adding an automation.

Please go to “+Automation”, create a condition for when the partition is intruded, and then set the following actions in sequence:

1. Activate Line Out 1 to trigger the siren.
2. Add 120 second delay (Actions > System > Delay).
3. Turn off Line Out 1 to stop the siren.



## 9. Notifications

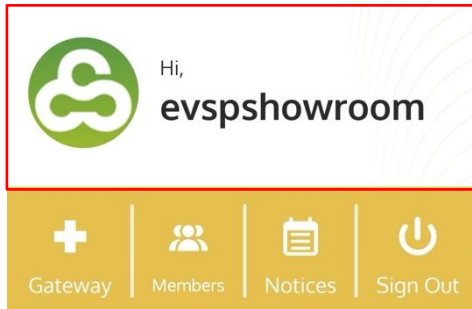
### 9.1 Email Notification

To receive email notifications, you must configure your Notify Email settings. You can also set up your own mail server and choose the specific types of event notifications you wish to receive.

### 9.1.1 Editing Notify Email

Where: [Dashboard](#) > [Gateways](#)

1. Press the top area.

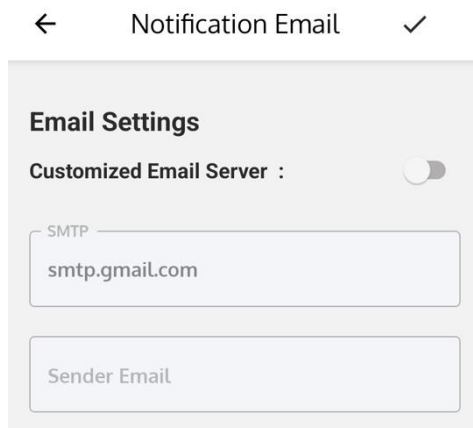


2. Enter the email address in Notify Email.
3. Press the save icon on the top right to apply the changes.

### 9.1.2 Setting Own Mail Server

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [Notification Email](#)

The system includes a built-in mail server to send notifications to users, but you may also configure your own mail server.



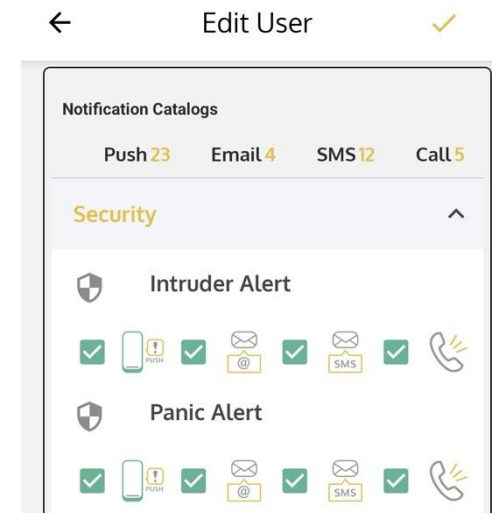
1. Enable Customized Email Server and enter the details of the email account to be used, such as SMTP server, port, username, and password.
2. Press the Email Test button. A test email will be sent to your notify email address. If successful, a confirmation will appear. If it times out, the settings may be incorrect.

Note: The gateway must have a valid email address to send notifications on behalf of the user. SMTP settings vary depending on the service provider.

### 9.1.3 User Notification Preference

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [any user](#) > [Settings](#)

On this page, you can choose which types of notifications each user will receive, such as security, power, and communication events.



Note: The user must first enter their Notify Email on the User Information page, as described in section 9.1.1.

In the notification catalogue, some items may be marked with an X, which indicates that the notification is not available.

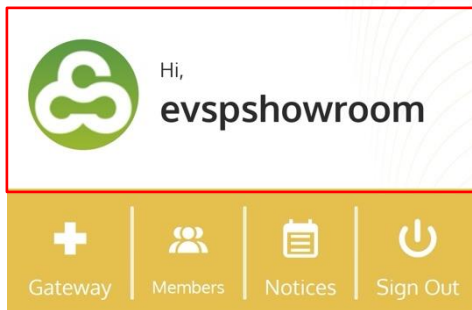
## 9.2 SMS Notification

To receive SMS notifications, you must configure your Notify Phone. You can also choose which event notifications you want to receive.

### 9.2.1 Editing Notify Phone

Where: [Dashboard](#) > [Gateways](#)

1. Press the top area.



2. Enter the phone number in Notify Phone.
3. Press the save icon on the top right to apply the changes.

### 9.2.2 User Notification Preference

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [any user](#) > [Settings](#)

On this page, you can select which notifications each user will receive, such as security, power, and communication events.

**Note:** Please ensure that the SIM card has been installed in the gateway in advance.

In the notification catalogue, some items are marked with an X, which means that the notification is not available.

### 9.2.3 Notification Delay

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [Notification delay](#)

On this page, there are two options for setting notification delays:

1. **Server Notification Delay:** When the gateway cannot connect to the server, the system will send a notification to the user by default after 10 seconds. Users can choose to extend this delay, up to a maximum of 600 seconds.
2. **Client Notification Delay:** When the gateway's internet connection is lost, the system sends an immediate notification. Users can choose to delay this notification, up to a maximum of 600 seconds.

If you do not want to receive these notifications, you can disable them in the Edit User page:

[Dashboard](#) > [Menu](#) > [Users](#) > [Any User](#) > [Settings](#) > [Notification](#) > [Communication](#):

1. **Server Connection Lost:** Disable this option to stop receiving notifications about the gateway failing to connect to the server.
2. **Internet Lost / Restore:** Disable this option to stop receiving notifications about loss and restoration of internet connection.

## 9.3 Voice Call Notification

To receive voice call notifications, you must complete three steps: configure your Notify Phone, set up Notification Voice, and enable the user's Voice Call option. You can also choose which event notifications you want to receive.

### 9.3.1 Editing Notify Phone

Please follow the same steps as described in 9.2.1 Editing notify phone.

### 9.3.2 Setting Voice Call Notification

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [settings icon \(top right\)](#) > [Notification Voice](#)

Here you can add up to three users to receive calls for selected notification events. When a security event occurs, calls will be made to users listed in Priority 1, 2, and 3.

You can also configure the number of retry attempts and the ringing duration for each call. The default duration is 15 seconds.

**Note:** Please ensure that the SIM card has been installed in the gateway in advance.

### 9.3.3 Enabling User Voice Call

Where: [Dashboard](#) > [Menu](#) > [Users](#) > [any user](#) > [Settings](#)

Enable the Voice Call option. You can also select which notifications each user will receive, such as security, power, and communication events.

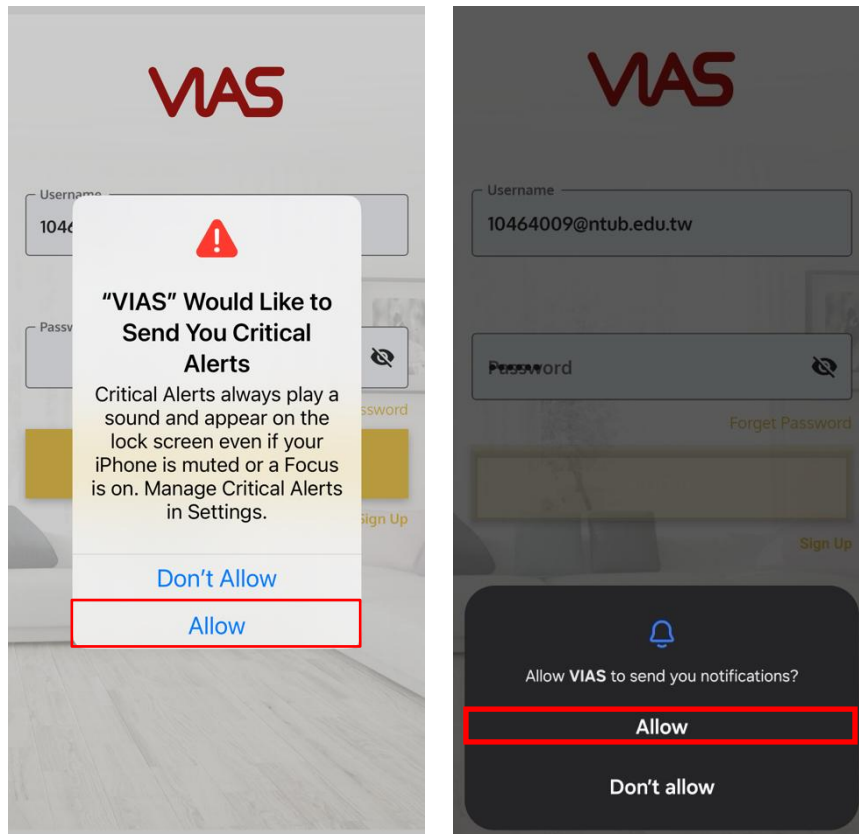
**Note:** In the notification catalogue, some items are marked with an X, which means the notification is not available.

## 9.4 Critical Alerts

Critical alerts are intended for high-priority notifications. These alerts appear at the top of the lock screen and play a sound that cannot be ignored. Examples include intruder, smoke, flood, panic, or tamper alarms.

On iOS devices, critical alerts will be received even if the phone is muted or in Do Not Disturb mode. On Android, critical alerts are also supported; please make sure that system sound is enabled and that the phone is not in Do Not Disturb mode.

If you do not receive critical alerts, reinstall the app to activate this feature, as the latest version includes the required permissions and settings



If you do not want to receive critical alerts, you can change the settings as follows:

1. On iOS, go to Settings > Notifications > VIAS > Critical Alerts and disable the feature.
2. On Android, mute the system sound by going to Settings > Sounds and vibration > System sound.

## 10. Firmware Upgrade

1. The firmware upgrade icon will automatically appear at the top of the dashboard, or "Update Available" will be shown on Dashboard > Menu > Gateway Configuration when a new firmware version is available for the gateway.

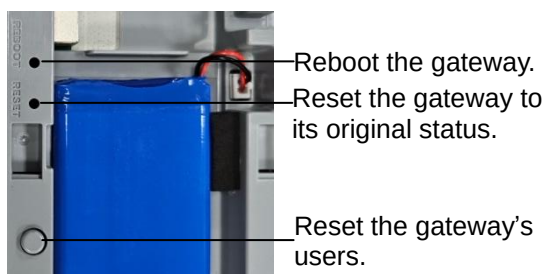


2. Please press the icon or text to display the update information.
3. Press the Upgrade button to start the update procedure.
4. During the firmware update, the power LED will flash orange. Please do not power off the gateway during this process to avoid errors.
5. After the update is complete, the gateway will restart. Please wait until all four LEDs on the top light up green again. This process takes about 30 seconds. You will receive a push notification when the gateway is back online, indicating that the update is complete.
6. To check the firmware version, go to Dashboard > Menu > Gateway Configuration and press the firmware option to view the current version.

Note: Only supervisors and installers can perform firmware upgrades. However, installers can enable or disable panel permissions for supervisors (see section 5.9 Customized permissions) to allow firmware upgrades.

## 11. Reboot or Reset Gateways

The factory default button can clear previous settings, reset the gateway to its original status, or reset the gateway's users. The reboot button can restart the gateway.



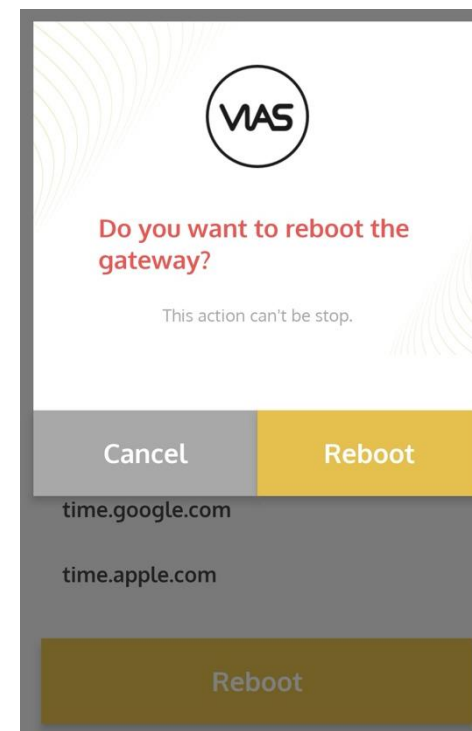
### 11.1 Reboot gateways

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [setting icon on the top right](#) > [General Information](#)

Press the REBOOT button. The four LED indicators on the top will turn off for about 30 seconds before turning back on.

You can also reboot the gateway via the app:

1. Press the Reboot button.
2. Confirm the reboot to proceed.



Wait until all four LEDs are illuminated, indicating that the process is complete. You will receive a push notification when the gateway is back online and powered on.

### 11.2 Reset Gateways

Press and hold the reset button for 10 seconds, then release it. The four LED indicators on the top will turn off for about 30 seconds before turning back on. Wait until all four LEDs are illuminated, indicating the process is complete. You will receive a push notification when the gateway is back online and powered on.

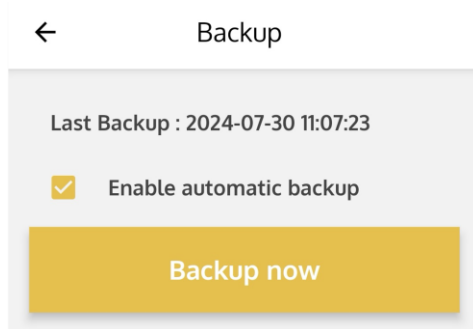
### 11.3 Reset Gateway's Users

Press the reset button five times within five seconds. The Internet LED will blink green, then blink orange, and return to blinking green. This indicates that the gateway's users have been reset.

## 12. Backup and Transfer

Where: [Dashboard](#) > [Menu](#) > [Gateway Configuration](#) > [setting icon on the top right](#) > [Backup](#)

To prevent system failures or data loss, VIAS automatically backs up system data to the cloud every week. This includes users, devices, partitions, cameras, scenes, and configurations. Once backed up, the data remains in the cloud even if the gateway is reset.



On this page, you can view the time of the last backup, enable or disable automatic backups, and perform manual backups.

**Note:** Only supervisors and installers can back up system data. However, installers can enable or disable supervisor panel permissions (see section 5.9 Customized permissions) to perform backups.

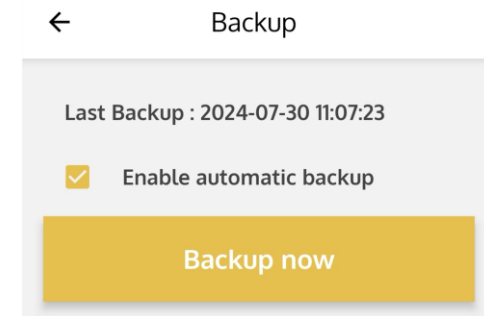
### 12.1 Transferring Data from an Old Gateway to a New Gateway

VIAS allows backup data to be transferred to a new gateway, subject to the following requirements:

1. At least one backup must have been performed.
2. The old gateway must have at least one user; otherwise, the Internet LED will blink green, indicating no owner.
3. If a designated installer will assist with the transfer, the old gateway must be shared with that installer.
4. It is recommended to reset the new gateway if previously used, and wait five minutes before proceeding.

Follow these steps to transfer backup data to the new system:

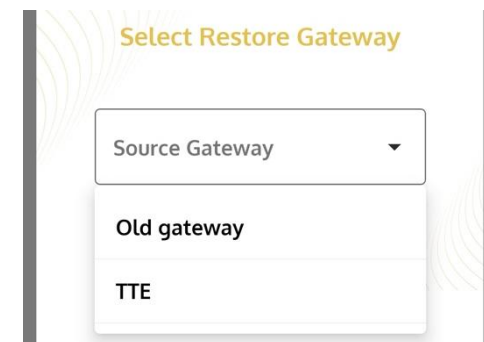
1. Press the Backup Now button.



2. Reset the new gateway if it has been used before.
3. Go to [Dashboard](#) > [Gateways](#) > [Gateway](#) (yellow section), then press the Backup Import button.



4. Scan the QR code of the new gateway.
5. Select the source gateway to transfer data from.

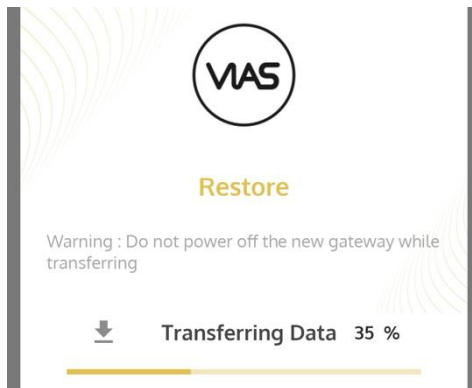


Note: The list of source gateways is based on gateways owned by or shared with your account.

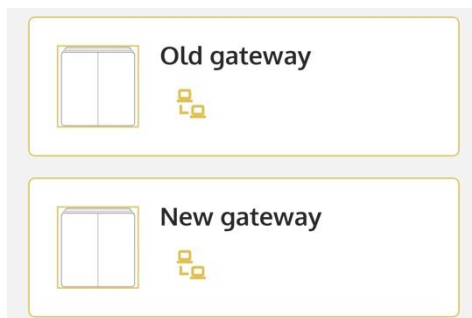
6. Enter the Target Gateway Name.

Note: If “Add Gateway & Upgrade” appears, the backup data is not affected by the firmware version.

7. A verification code will be sent to the owner of the source gateway.
8. Enter the Transfer Confirmation Code, then press Start.
9. The system will begin transferring data.



10. When the progress bar reaches 100%, press the Close button.
11. After transfer, the backup data remains on the old gateway but it will no longer be operational.



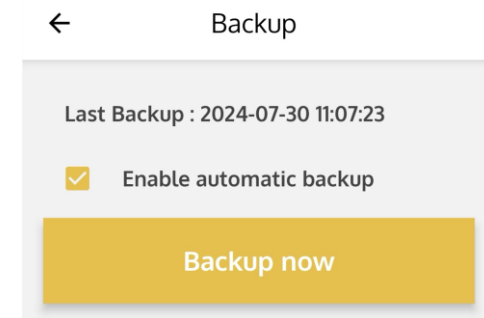
## 12.2 Gateway Transfer to Itself

The gateway can restore backup data to itself. Before initiating the process, ensure the following conditions are met:

1. At least one backup must have been successfully completed.
2. It is strongly recommended to reset the gateway and wait five minutes before beginning the transfer.

Steps to Restore Backup Data to the Same Gateway:

1. Click the **Backup Now** button.



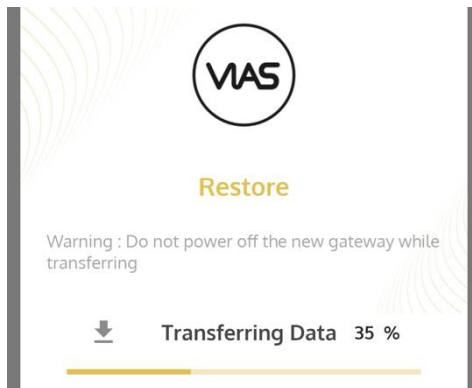
2. Reset the gateway.
3. Navigate to Dashboard > Gateways, select the gateway highlighted in yellow, and click the Backup Restore button.



4. Scan the gateway's QR code.
5. Enter the Target Gateway Name.

Note: If the message Add Gateway & Upgrade appears, the backup data will not be affected by the firmware version.

6. The system will begin transferring the data.



7. Once the progress bar reaches 100%, click the CLOSE button.

## 13. VIAS Web Interface

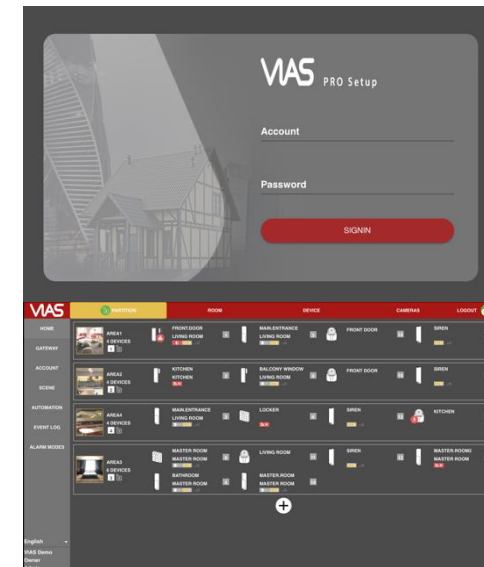
In addition to the mobile app, VIAS also offers a web interface that allows users to configure settings through a web browser. The available settings on the web interface are identical to those found in the app.

There are two ways to access the VIAS web interface:

1. <https://my.vias-system.com>
2. <http://192.168.x.x/#/dashboard>

**Note:** You can find the IP address from Dashboard > Menu > Gateway Configuration > setting icon on the top right > Network.

3. Enter the Account and Password of a user with access to the selected gateway.



## 14. Specifications

### 14.1 Hardware Specification

| System             | Processor                 | High-performance Embedded CPU                                                                                          |
|--------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------|
| Indicators         | LED indicators            | Power LED, Internet LED, Comms LED, Status LED                                                                         |
| Buttons / Switches | Internal (inside housing) | Reboot button, Reset to factory default button                                                                         |
|                    | Tamper Switches           | 1 x Wall-remove tamper, 2 x housing-open tamper                                                                        |
| Slots / Connector  | External                  | USB port (SC109 only)                                                                                                  |
|                    | Internal (inside housing) | DC-jack, RJ45(LAN), 1 x SATA connector, SIM card slot, Micro SD slot (SC109L/SC109C does not include a SATA connector) |
|                    | Extender board            | Wired terminal block (SC115 only): 1 x relay: NC, NO, COM                                                              |

| System                   | Processor             | High-performance Embedded CPU                                                                                          |
|--------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------|
|                          |                       | 1 x siren output: 12V, 0.7A (need boost circuit)                                                                       |
| Power                    | Primary Power         | DC adaptor 12V, 2A                                                                                                     |
|                          | Backup Power          | SC109 LiPO Battery, 7.4V 2500mAh for > 12 hrs battery life<br>SC115 LiPO battery, 7.4V 3000mAh for >12hrs battery life |
| Sensor & Devices Network | Protocol              | Wireless U-Net 2-way communication                                                                                     |
|                          | Frequency             | 868.0-868.6 MHz (EU)<br>921.0-925.0 MHz (US)                                                                           |
| Communication            | Main network          | Ethernet: 1 x 10/100 LAN port                                                                                          |
|                          | Backup Mobile Network | 4G LTE                                                                                                                 |
|                          | SMS and Voice         | 2G GSM                                                                                                                 |
| Storage                  | SSD Interface         | 1 x SATA2 port for video storage (not available on SC109L)                                                             |
|                          | SD card               | Micro SD slot (supports SD-XC format)                                                                                  |
| Alarm Reporting          | IP Protocol           | SIA DC09                                                                                                               |
| Operating Environment    | Temperature           | SC109: -10°C ~ +40 °C<br>SC115: 0° till +40 °C                                                                         |
|                          | Humidity              | Max. 85% RH                                                                                                            |
| Mechanical               | Dimensions            | 165.4 mm (W) X 61.2 mm (D) X 165 mm (H)                                                                                |
|                          | Weight                | 596 g (including backup battery, without hard drive)                                                                   |
| Installation             | Location              | Indoor use only                                                                                                        |
|                          | Mounting Options      | Wall mount with bracket, or tabletop placement                                                                         |

## 14.2 Functional Specifications

### 14.2.1 General Specifications

|                      |                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------|
| Number of Zones      | 160                                                                                                    |
| Number of devices    | 160                                                                                                    |
| Number of Partitions | 40                                                                                                     |
| Number of Users      | Owner: 1, Users: 50,                                                                                   |
| Keypad PIN Codes     | 100                                                                                                    |
| Remote Keyfobs       | 50                                                                                                     |
| Video Recording      | SC109 / SC115: 24/7 + Event Recording,<br>SC109L: Event Recording Only<br>SC109C: Event Recording Only |

### 14.2.2 Alarm Specifications

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| Entry / Exit Delay | 5 to 45 seconds                                            |
| Override / Bypass  | Available for zones with open, fault, or tamper conditions |
| Zone Lock Count    | 5 to 20 attempts                                           |
| Event Log Capacity | Stores up to 10,000 events                                 |

Note: Specifications are subject to change and improvement without prior notice.

## 15. Certifications

### CE Certified

- Security Grade 2, Environmental Class II
- EN50131-1:2006/A1:2009/A2:2017/A3:2020
- EN50131-3:2009
- EN50131-6:2017
- EN50131-10:2014
- EN50136-1:2012/A1:2018
- EN50136-2:2013
- EN50131-5-3:2017

## FCC Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.

## RF Exposure Information

The device has been evaluated to meet general RF exposure requirement. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.