

Installation & User Manual

Obyn Keypad - IP Access Control Terminal



The information in this document may be changed as we always strive to improve the product.
Trust that the information provided is accurate at the time of document release.

Table of Contents

Table of Contents	2
Technical Specifications	5
Packing Contents	7
Optional Extra Equipment	7
Installation Information	8
1. Site Survey & Bench Testing	8
2. Installation	8
3. Wiring Diagram	9
4. Relay Connections	10
5. Power	11
a. 12v DC	11
b. 48v POE	11
6. Network Connection	11
a. Ethernet	11
b. 4G Router	12
Setup - Select Mode	13
Cloud Mode (Default)	13
Standalone Mode	13
Cloud Mode Setup	14
Getting Started	14
1. Account Creation	15
2. Create a company	15
3. Create a site	16
4. Create a block	16
5. Create a device	17
6. Setup Users	18
7. Licenses	19
Standalone Mode Setup	20
Getting Started	20
1: Enter Programming Mode	20
2: Set a New Engineer Code	20
3: Enable Standalone Mode	21
Note: Changing from Standalone Mode to Cloud Mode will delete all data currently stored on the device.	21
Keypad Operation	22
LED Indicators	22
Unlocking Methods	22
Function Codes	23
Manual Factory Reset	29
Management Portal Operation	30
1. Company Dashboard	30
a. Sites	30

b. Company Admin	30
c. Purchase Record	31
2. Site Dashboard	31
a. Blocks	31
b. Devices	32
c. Site Users	34
d. Operation Log	39
e. Device Log	39
f. Site Licences	40
g. Payments	40
h. Notice	41
i. User Messages	42
App Operation	44
1. Add Intercom to Device	44
2. Devices (Home Page)	44
a. Relay Activation & Bluetooth Activation	44
b. Pin Apartment	44
c. Add Apartment	44
d. Apartment Settings	44
e. Device Settings	45
f. Lift Control	45
g. Guard	45
h. Activity	45
i. Settings	45
3. Apartment Settings	45
a. Apartment Name	45
b. Service Renewal	46
c. Share Settings	46
d. Available devices	47
e. User Profile Settings	47
f. Access Settings	48
g. Quick Unlock Setting	50
4. Device Settings	51
a. Device Name	51
b. Device Detail	51
c. Notification Settings	52
d. Advanced Settings	52
e. Local Settings	54
5. Activity Log	55
6. Settings	55
a. Account	55
b. Share	56
c. Album	56
d. Tool	57

e. Mobile Data Reminder	57
f. Call Settings	57
g. Site Management	58
h. User Help	60
i. About	60
Local Web Interface Operation	61
Local Config	61
User Management	62
Maintenance	62
App Updates	62
Firmware Updates	62
Warranty	62
Certifications	63
CE-RED	63
FCC	63

Technical Specifications

GENERAL	
Material	Powder-coated Aluminium & Toughened Glass
Weatherproof	IP65
Impact Rating	IK08
Approvals	CE-RED, FCC, ROHS, RED_DA
Dimensions	<u>EU</u> 139mm (H), 50mm (W), 27mm (D) <u>US</u> 5.5in (H), 2in (W), 1.1in (D)
Operating Temperature	-30 ~ +65
Operating Humidity	10 ~ 90%
Power Supply	12v DC / 48v POE (802.3af)
Power Consumption	Max 2W
Relays	1
Relay Type	N/C & N/O
Relay Load	2A, 30v DC/250AC
Operating System	Linux
Alarms	Anti-vandal/Tamper
System Requirements	Minimum 1.5MB/s Upload Speed
Storage	2GB Flash
Illumination	White, Green, Blue, Red LED
CAMERA	
Camera Strength	2 Megapixels
Lens	35° (H), 60° (V), 70° (D)
BUILT-IN CARD READER	
Frequency	13.56MHz (MIFARE & NFC) - 24bit

WIEGAND	
Protocol	Wiegand 26 & 34
Functions	Reader & Controller
AUDIO	
Audio Components	Speaker
NETWORK	
Ethernet	IEEE 802.3
Supported Protocols	TCP/UDP/RTP/RTSP/HTTPS

Packing Contents

- 1x Obyn-Keypad
- 1x PoE Plug
- 1x IEC Lead (Kettle Lead)
- 1x Accessory Bag (Screws, Connectors etc)

Optional Extra Equipment

- Ethernet Cable



- External 4G Router (Optional for when 4G connection is required)



- AES Branded MiFare Cards



Installation Information

Proper installation is essential for optimal system performance and the best user experience. Ensure all instructions in this section are followed carefully.

1. Site Survey & Bench Testing

It's important to make sure the site where the system will be installed is suitable. To determine this, we need to ensure certain requirements are met like network speeds, cable distance (DC Power & POE). For more information proceed to the next section.

We also recommend performing a “**Bench Test**” of the system before installing. This will ensure the system is working as it should before it's fully installed. Follow the setup steps below to get started and ensure to default/reset the system once you are done.

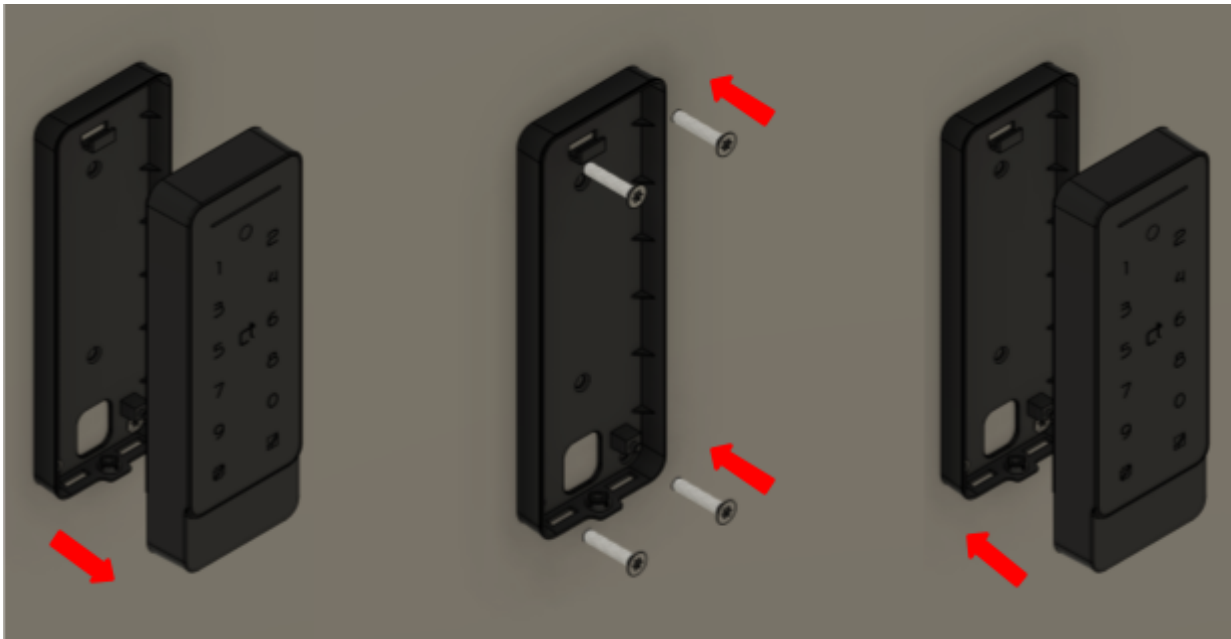
2. Installation

Ethernet can travel up to roughly 100m/320ft on CAT5/CAT6 cable. Longer distances require a switch every 100m/320ft unless using any specialist equipment.



MAX DISTANCE 100m (320ft) (LAN)
This can be extended by using an ethernet cable extender
(purchased separately)

Surface Mount - Installation



- 1) Remove the fastening screw located at the bottom of the keypad to detach the front panel.
- 2) Mount the back plate to the desired surface using any of the 6 available mounting holes.
- 3) Pull any required cables through the mounting surface and connect them to the front panel.
- 4) Reattach the front panel and secure it by re-inserting the fastening screw.

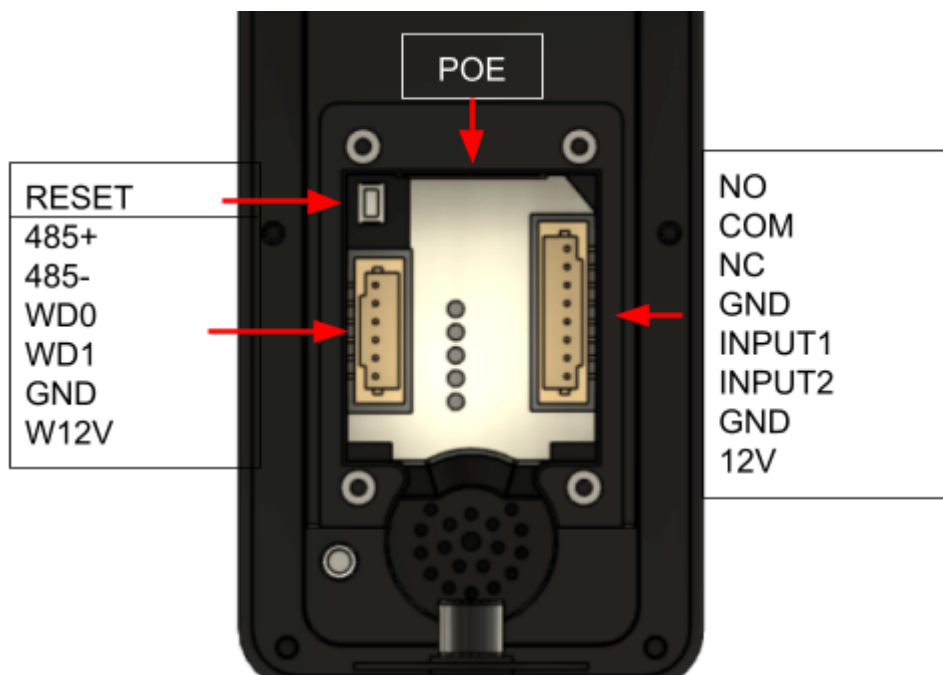
INGRESS PROTECTION



We recommend sealing all entry holes for prevention of insects that can cause issues with a risk of shorting out components.

To maintain the IP65 rating please follow the sealing instructions. (available online)

3. Wiring Diagram



POE: Can provide both power and network.

RST: Reset button, used to factory reset the device.

485+/-: *Not in use*

W_D1/0: Wiegand interface for wiegand access control.

GND/W12V: Wiegand device power supply.

NO/COM/NC: Relay Terminals.

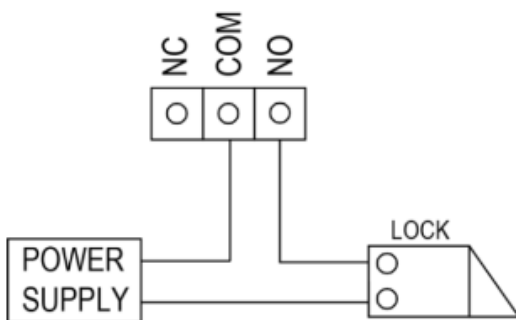
GND/INPUT1: Exit Button

INPUT2: *Not in use*

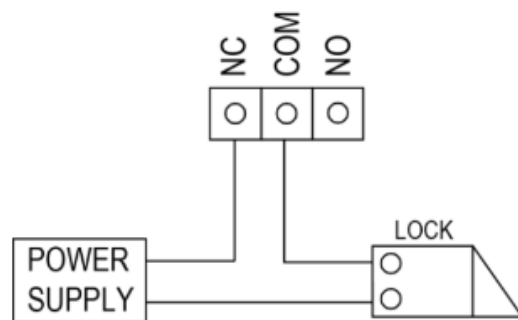
12V/GND: Power supply when POE is not being used

4. Relay Connections

Type 1: Power-on-to-unlock



Type 2: Power-off-to-unlock



Note:

- An external power supply must be used according to the lock.
- The relay is limited to 30V, 2A.

5. Power

Powering the device can be done either via 12v DC or 48v POE. Both of which AES can supply.

a. 12v DC

When using DC power it is required to stay within a certain distance depending on the type or thickness of cable used. Our general recommendations are as follows:

Up to 2 metres (6 feet) - Use minimum 0.5mm²/ 22 gauge cable.

Up to 4 metres (12 feet) - Use minimum 1mm² / 20 gauge cable.

Up to 8 metres (25 feet) - Use minimum 1.5mm² / 18 gauge cable.

b. 48v POE

When using POE to power the system it's important to note that the max distance Ethernet can travel is 100m/320ft. This means the distance between the power source and the device cannot be greater than this.

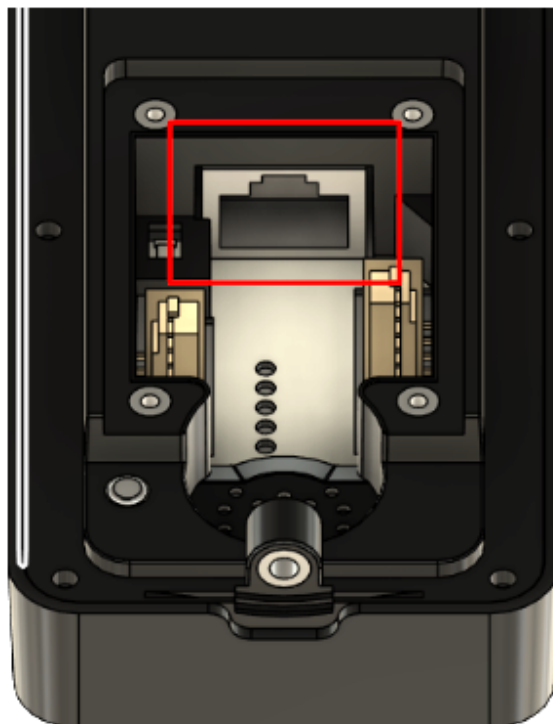
6. Network Connection

When it comes to connecting the device to a network this can be done in two ways.

a. Ethernet

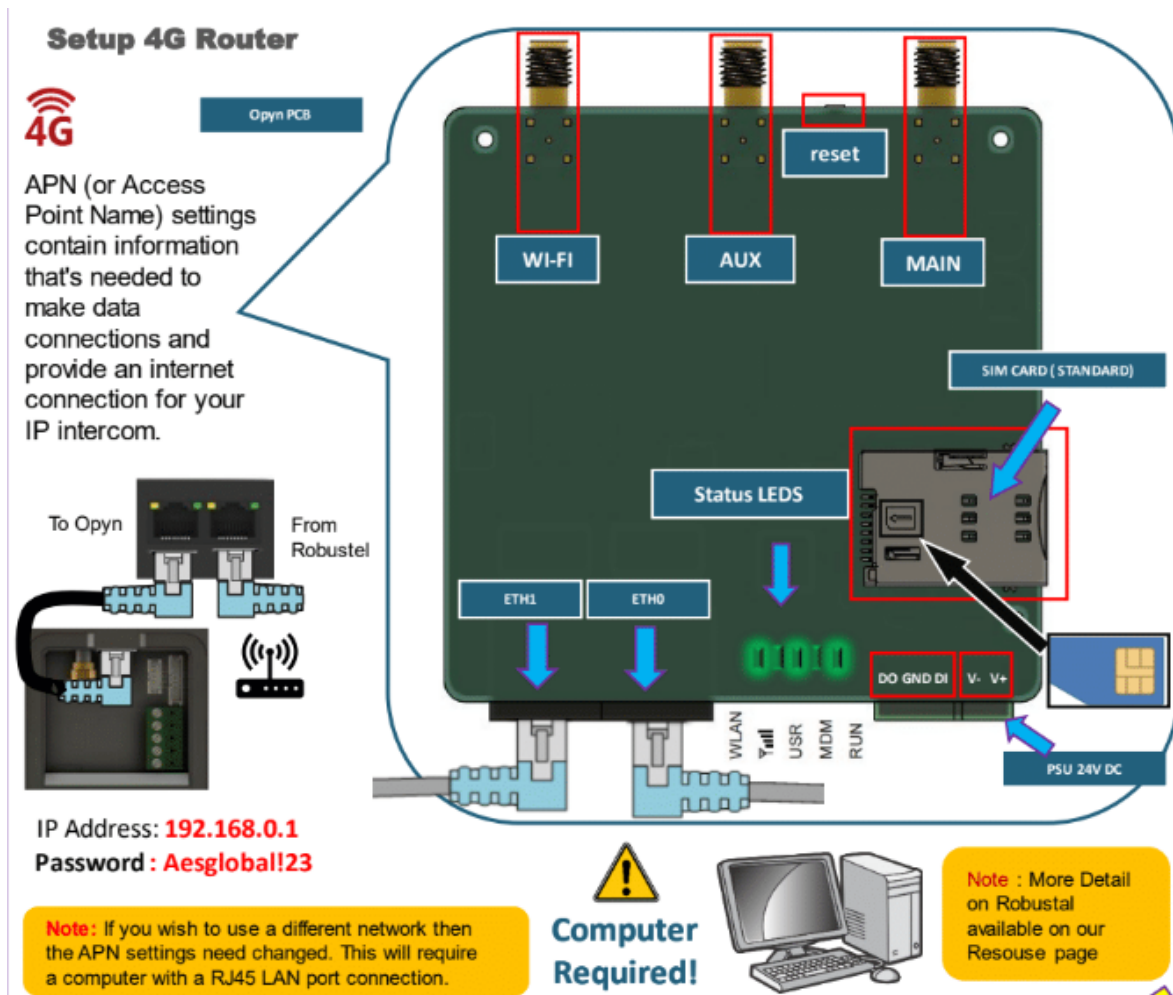
You can connect an ethernet cable directly into one of the RJ45 ports that the device has. Both of these ports support DHCP, and if you wish you may also enable static IP for both. It does not matter which of the two ports you use.

Note: Ethernet can travel up to roughly 100m/320ft on CAT5/CAT6 cable. Longer distances require a switch every 100m/320ft unless using any specialist equipment.



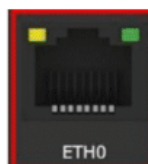
b. 4G Router

If a standard network connection is not possible, AES can offer an external 4G router that can provide a network connection to the device.



DATA TRANSFER LEDS

The 2 LEDs behind LAN 1 Port will flash **GREEN** when you have connection activity.



PCB BOOT STATUS LEDS

When the PCB has successfully booted up you should have activity on all 3 LEDs:

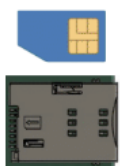


RUN: Constant ON = **Initializing** | Blinking - Working Constant OFF = **PCB Powered OFF**
MDM: Steady solid = **Working** | Blinking = Data sent/ recieved Constant OFF = **Not Connected**
USR: Steady solid = **Working** | Blinking = Data sent/ recieved Constant OFF = **Not Connected**
RSSI (Represented by five bars signal.) : Steady solid = **Strong signal** | Blinking = Medium signal Constant OFF = **Low/no Signal**
WLAN: Steady solid = **Wi-Fi is working** Constant OFF = **Not Connected**

SIM ORIENTATION

ALWAYS ensure that the system is switched **OFF** any time you are adding or removing the SIM card and also ensure that the orientation is correct before powering the router back on.

STANDARD SIM SIZE ONLY



- ATTENTION! -

This module will come the APN pre-set for the AES SIM that is provided with the unit. Once the SIM has been setup with a data package then this module will provide an internet connection for the main PCB.

Setup - Select Mode

The system supports two primary operating modes: **Cloud Mode** (default) and **Standalone Mode**. Each mode offers different features and installation benefits.

Cloud Mode (Default)

Cloud Mode allows the system to be fully managed remotely via the “Opyin Management Portal”.

Key Features:

- Complete management via the cloud portal or mobile app
- No wired communication required between additional devices (e.g., additional keypads or Opyin Multi intercom devices)
- Unlimited keypads can be added to a site using wireless connectivity
- Requires:
 - Power
 - Network connection
 - Relay connection to the entry point

This mode is ideally suited to installations with multiple entry points or where remote management functionality is required.

Standalone Mode

In Standalone Mode all management is done physically on the keypad.

Key Features:

- Configuration and management performed locally on the device
- Supports additional operating configurations:
 - **Controller Mode (Default)** – Can physically connect to a slave device via Wiegand
 - **Reader Mode** – Operates as a slave device, physically connected to a controller device via Wiegand
- Requires:
 - Power
 - Relay connection to the entry point
 - Wiegand connection (If applicable)

This mode is suitable for single-door or two-door installations, where cloud connectivity is not required, or where there is no network connection available.

Note: For detailed configuration instructions for each operating mode, refer to the **Keypad Operation** section of this manual.

Cloud Mode Setup

Before starting, ensure the system has been installed correctly and has a working network connection. If the keypad is set to Standalone Mode you can change it back to Cloud Mode by following the steps in the **Keypad Operation** section.

Getting Started

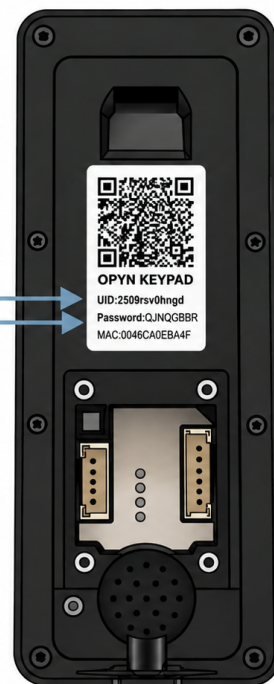
1. Apply power to the system.
2. After a few seconds, the system will emit a beep.
3. A steady white LED will illuminate, indicating the system is in **Standby Mode**.
4. Make note of the devices **Serial Number & Security Code** located on a sticker at the back of the keypad. (See *image below*)
5. Now you can proceed to the **Opyn Multi Management Portal**.

Device Details

Your device **serial number** and **security code** can be found on the sticker located on the back of the device itself.

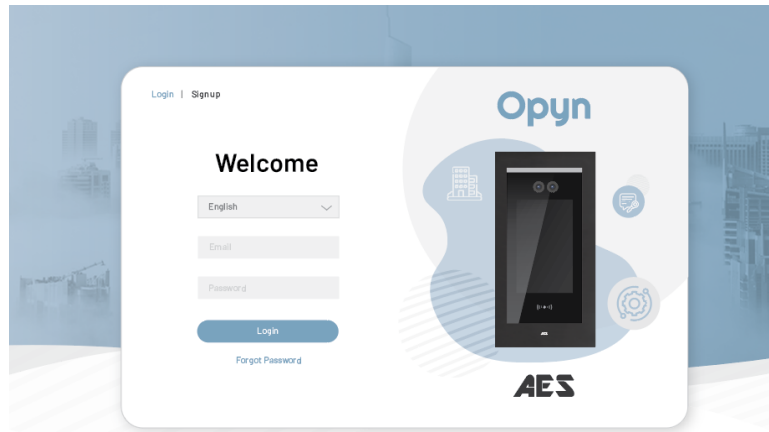
The information on the sticker is the **default** serial number and security code for your device.

It will be labelled as **UID** (Serial Number) and **Password** (Security Code).



1. Account Creation

Once the keypad has been installed & powered up you can start the cloud setup process. To get started you will need to navigate to our management portal and create an account: [Opyin Multi - Management Portal](#)



2. Create a company

First you will need to create a company. You may create additional companies later if needed.

Create Company ×

Company Name *

Cancel Confirm

3. Create a site

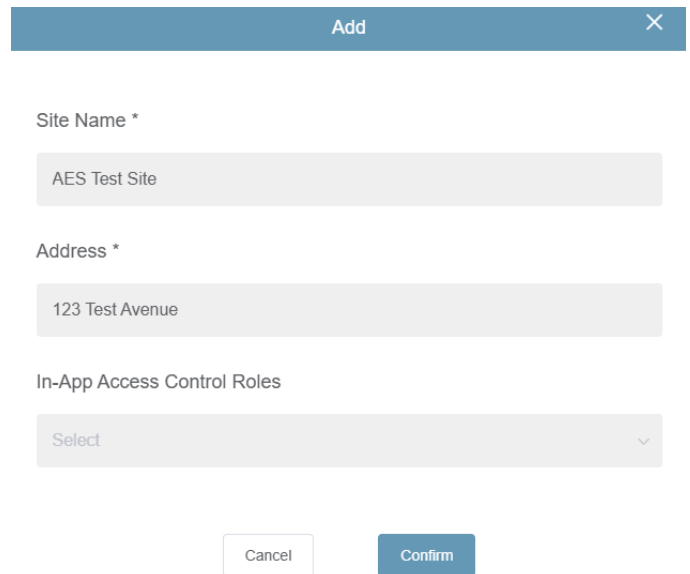
A site covers the entire installation project. You can think of it in the context of a business park or an apartment complex, where the site encompasses all the devices & users within. Enter a site name and address then set the In-App Access Control Roles.

In-App Access Control Roles –

Programming permissions are managed at a site level. Choose here which roles you would like to have programming permissions.

If the User role is listed here, anyone assigned that role will have the ability to program via the app as a licensed user via the “Access Settings” page such as create their own QR codes, Keypad Codes and Facial Recognition IDs. Further permissions can be managed later in the process such as the ability to unlock relay, accept an incoming call & preview the live camera feed.

If you do not wish any user to have this access via the app then remove all roles from this text box.



The screenshot shows a modal window titled 'Add' with a close button (X). It contains three input fields: 'Site Name *' with the value 'AES Test Site', 'Address *' with the value '123 Test Avenue', and 'In-App Access Control Roles' with a dropdown menu showing 'Select'. At the bottom, there are two buttons: 'Cancel' and 'Confirm'.

4. Create a block

A block or several blocks can now be added depending on the requirements of the site. It's easiest to think of a “block” as an apartment block, a unit in a business park or a house/property within a gated community.

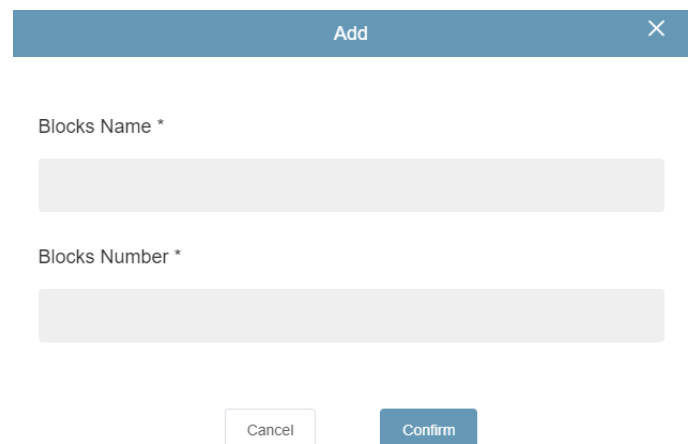
You will need to enter a name and a number for each block. This information can be edited at a later time.

Example:

Blocks Name - Unit 1A or Unit 1B

Block Number - 1 or 2

Note: The block number can only contain numerals and cannot start with a 0.



The screenshot shows a modal window titled 'Add' with a close button (X). It contains two input fields: 'Blocks Name *' and 'Blocks Number *'. At the bottom, there are two buttons: 'Cancel' and 'Confirm'.

5. Create a device

Attaching a Device

1. Click “Create New Device” and select “Keypad”.
2. Enter the required keypad information and assign it to a “**Block**”. This gives all users in the block access to the device.
3. To make the keypad available to the entire site, select “**Sites**” from the dropdown instead of a specific block. This allows all site users to access the keypad.

The screenshot shows a navigation bar with 'Blocks', 'Devices', and 'Site Users' tabs, and a 'Create New Device' button. Below is a modal titled 'Create New Device' with a close button. It contains a 'Device Type *' dropdown menu with 'Keypad' selected. At the bottom are 'Cancel' and 'Confirm' buttons.

Adjusting User Permissions

You can configure the following permissions for user roles:

- Unlock the intercom relays

Floor Number - If using elevator control. Set the floor the device is located on.

Data Sync - Copy the programming from another keypad.

Most of this information can be updated later if needed.

The screenshot shows a modal titled 'Create New Keypad' with a close button. It is divided into two columns. The left column contains: 'Device Serial Number *' with a text input and a link 'if you can't find serial number please click here >>'; 'Device Security Code *' with a text input and a link 'if you can't find security code please click here >>'; 'Device Name *' with a text input; and 'Site Or Blocks *' with a dropdown menu showing 'Site/Blocks'. The right column contains: 'Role Permission Control' with a table of permissions for Site User, Site Employee, and Site Other; 'Floor Number' with a dropdown menu; and 'Data Sync' with a link icon and a text input. At the bottom are 'Cancel' and 'Confirm' buttons.

Role	View	Lock	Relay
Site User			
Site Employee			
Site Other			

6. Setup Users

Adding Users to the Keypad

1. Fill in the user's details and select their block, house/apartment number, floor number (for elevator control) and user role.

Note: Users with the “Admin” role do not require an active license to operate the keypad.

2. Assign a licence if already purchased (or do this later after reading the “Licences” section).

Block Assignment:

- Select “**Sites**” to make the user a “site user,” granting access only to site devices.
- Assign them to a “**Block**” to provide access to their block’s devices and site devices.

User Onboarding:

- After saving, an email invite is sent to the user.
- The email includes instructions to download the AES Opyin app, create an account, and scan a QR code or click a link.
- Scanning the QR code or using the link prompts the user to accept the invitation to the site. Once accepted, the user is added to the device’s contact list and can operate the system. User will need to create an account in the AES Opyin app.

Note: You can use the batch import function to add up to 200 users at once.

Add Site User

User email *

User Role *

User Role

First Name *

Surname

Floor Number

Floor Number

SiteOrBlocks *

Site/Blocks

Available activation codes

☐ 30 Days

Remaining Quantity 122

☐ 1 Day

Remaining Quantity 18

Apartment Number *

Cancel

Confirm

*To operate the panel, users need an assigned licence. This applies even if no app access is needed and you intend on using SIP calling only.**

7. Licences

All users not with the role of “admin” need an active license to operate the keypad.

- **Purchasing Licences:** Buy licences directly from AES through the management portal under the “Payments” tab. For details, see the “Management Portal Operation” section.
- **Licence Duration:** The licence duration begins when assigned to a user, not at the time of purchase.
- **Assigning Licences:** Licences can be assigned:
 - When creating an apartment.
 - When editing an apartment.
 - Using the “service activation” feature.
- **Admin Monitoring:** Check each apartment's remaining licence duration in the management portal.
- **User Monitoring:** Users can view their licence duration in the mobile app.
- **Unbind/Bind:** You can unbind a user from an apartment and keep the license until a new user is bound to the apartment.
- **Delete License:** If a license is deleted it cannot be recovered and a new license will need to be purchased.

Note: Each apartment requires a licence assigned to the main user. The main user can share apartment access with others via the mobile app up to a maximum of 8. SIP credentials are a separate service.

The screenshot displays three main sections of the management portal interface:

- Add Site User:** A form for creating a new user. It includes fields for 'User email', 'User Role' (set to 'employee'), 'First Name', 'Surname', 'BloodChills', and 'House Number'. A red box highlights the 'Available activation codes' section, showing two options: '30 Days' (Remaining Quantity: 130) and '1 Day' (Remaining Quantity: 20). Buttons for 'Cancel' and 'Create' are at the bottom.
- User Detail:** A form for editing user information. It includes tabs for 'User Detail', 'Devices', 'App Settings', and 'Card Settings'. The 'User Detail' tab is active, showing 'Personal Info' and 'User Setting'. The 'User Setting' section has a red box around the 'Assign' button. The 'Service Status' is 'In Use' and 'Services Remaining' is '30 Days'.
- Service Activation:** A modal window for activating services. It has a search bar and a table with columns: '#', 'User Name', 'Service Status', and 'Services Remaining'. The table shows one entry: '1', 'Test Test', 'In Use', '30 Days'. A red box highlights the table. Below the table, there is a 'Total: 1' and 'Select: 0' summary. At the bottom, there are two license options: 'License Package (Basic Edition) for 30 days' (Remaining Quantity: 131) and 'License Package (Basic Edition) for 1 days' (Remaining Quantity: 20). Buttons for 'Cancel' and 'Activation' are at the bottom.

Standalone Mode Setup

Getting Started

1. Apply power to the system.
2. After a few seconds, the system will emit a beep.
3. A steady white LED will illuminate, indicating the system is in **Standby Mode**.
4. Upon initial setup, you must change the default engineer's code before accessing the keypad's system settings.

1: Enter Programming Mode

1. Enter the default engineers code (123456) using the following keypad sequence:

 ➡ 123456 ➡ 

If the code is entered correctly:

- The blue LED will flash flash.
- A single beep will sound.
- The system will enter code changing mode.

If the code is entered incorrectly:

- The red LED will flash illuminate.
- Three beeps will sound.
- The system will return to standby mode.

Note: Pressing  at any time during input will cancel the operation and return the system to standby mode.

2: Set a New Engineer Code

1. Enter a new 6-digit engineers code

Example: 654321 ➡ 

- A tone will sound prompting to confirm the code.

2. Re-enter the same 6-digit code

654321 ➡ 

If the code is entered correctly:

- The green LED will flash flash.
- A confirmation beep will sound.
- The system will return to standby mode.

If the entered codes do not match:

- The red LED will flash.
- Three beeps will sound.
- The system will return to standby mode.



3: Enable Standalone Mode

1. Enter the system settings using the following keypad sequence:

☐ ➡ Engineers Code ➡ ☒

Example: ☐ ➡ 123456 ➡ ☒

If the code is entered correctly:

- The green LED will flash continuously.
- A confirmation beep will sound

2. Access **Mode Selection** by entering: ☐4 ➡ ☒

- If the code is entered correctly:
 - The white LED will flash.
 - A confirmation beep will sound.

3. Select **Standalone Mode** by entering: ☐1 ➡ ☒

- If the code is entered correctly:
 - The green LED will flash.
 - A confirmation beep will sound
 - The system will reboot.

4. The keypad is now configured to **Standalone Mode** and can be managed and programmed locally. For detailed information on all management and programming options, refer to the **Keypad Operation** section of the manual.

Note: Changing from Standalone Mode to Cloud Mode will delete all data currently stored on the device.

Keypad Operation

LED Indicators

- Standby Mode = Steady White LED
- Settings Mode = Steady Flashing Green LED
- Success Scenarios = Flashing Green/Blue LED
- Failure Scenarios = Flashing Red LED

Unlocking Methods

There are methods of activating the relay/lock of the system. Below we will detail what they are and how you will program them and use them in both Cloud Mode and Standalone Mode.

Keypad Codes

- Programmed via Management Portal or Mobile App (Cloud Mode)
- Programmed directly on the keypad (Standalone Mode)
- Enter the code followed by √ to use.
- Example: **5656**√
- If the entered code is accepted the green LED will flash and a confirmation beep will sound.
- If the entered code is rejected the red LED will flash and a confirmation beep will sound.
- Wiegand Supported

IC Cards

- Programmed via Management Portal or Mobile App (Cloud Mode)
- Programmed directly on the keypad (Standalone Mode)
- Swipe on the keypad surface near the card icon.
- If the card is accepted the green LED will flash and a confirmation beep will sound.
- If the card is rejected the red LED will flash and a confirmation beep will sound.
- Wiegand Supported

QR Codes

- Programmed via Management Portal or Mobile App (Cloud Mode)
- Show the QR code to the keypad's camera at roughly a 30cm distance.
- If the code is accepted the green LED will flash and a confirmation beep will sound.
- If the code is rejected the red LED will flash and a confirmation beep will sound.

Bluetooth

- Programmed via Mobile App (Cloud Mode)
- Programmed directly on the keypad and via Mobile App (Standalone Mode)
- Press the Bluetooth icon on the Mobile app to activate relay.

Function Codes

Function codes are used to access the various settings options after entering **System Settings**. A complete list of function codes used to configure and program the keypad is provided below.

X =  √ = 

Code	Function	Description	Available in Standalone Mode	Available in Cloud Mode
X	System Settings	Enter the system settings using the following keypad sequence: X [Engineer Code] √ Example: X 260226 √ (Default Code: 123456) If the code is entered correctly the green LED will flash continuously.	Yes	Yes
1	Factory Reset	All parameters will be reset, including the engineer password, regardless of whether the device is in cloud mode or standalone mode. To complete this specific setting, press and hold the “√” key for 3 seconds.	Yes	Yes
2	User Reset	All settings will be reset except for the engineer password. To complete this specific setting, press and hold the “√” key for 3 seconds.	Yes	Yes
3√	Engineer Code	Enter a new 6-digit engineer code followed by “√”.	Yes	Yes
4√	Operation Mode Selection	After entering this setting, select the desired mode: - Press “1√” for standalone mode - Press “2√” for cloud mode The default setting is 2√ (Cloud mode). Note: Changing from Standalone Mode to Cloud Mode will delete all data currently stored on the device.	Yes	Yes
5√	Relay Activation Time	Value range is from 1 to 99 seconds. The default value is 2 seconds.	Yes	Yes

		Example command: 5√ (sets the time to 5 seconds)		
6√	Device Mode Selection	After entering this setting, select the desired mode: • Press “1√” for controller mode • Press “2√” to set the device as a Wiegand 26 keypad (Slave device) • Press “3√” to set the device as a Wiegand 34 keypad (Slave device) The default value is 1√ (Controller mode). Note: Wiegand 26 and Wiegand 34 are used for card unlocking only, while Wiegand 4 is fixed for password unlocking.	Yes	No
7√	Tone Setting	Select the keypad beep setting: • Press “1√” to disable the keypad sound • Press “2√” to enable the keypad sound The default value is 2√ (Sound enabled).	Yes	Yes
8√	Bluetooth Configuration	Select the Bluetooth setting: • Press “1√” to activate device and phone Bluetooth pairing mode • Press “2√” to deactivate device and phone Bluetooth pairing mode • Press “3√” to delete all paired phones Note: This setting will time out after 60 seconds. Only one Bluetooth phone can be connected at a time, and up to 20 phones can be paired.	Yes	No
9√	Relay Operation Mode	Select the relay and “Hold Open” keypad code settings: • Press “1√” to set relay as always closed • Press “2√” to set relay as always open • Press “3√” to enter the “Hold Open” keypad code addition mode • Press “4√” to enter the “Hold Open” keypad code deletion mode The default value is Relay always closed.	Yes	No

Hold Open Keypad Code Setup

1. Enter **3√** to add or **4√** to delete a keypad code.
2. The blue light will remain steady, indicating you are in keypad code setup mode.
3. Enter the hold-open keypad code you wish to add or delete, ending with **√**.
4. The blue light will flash once, prompting you to re-enter the same keypad code, ending with **√**.
5. Successful setup: the green light stays on for 1 second and a single “beep di” is heard.
6. Failed setup: the red light stays on for 1 second and three “beep dididi” sounds are heard. This occurs if:
 - Deleting a keypad code not in the database
 - Adding a keypad code that does not meet length requirements

After successfully setting a keypad code, the system automatically returns to Setup Mode 9 (white light flashing slowly). To add or delete another keypad code, enter **3√** or **4√** again.

- If no operation occurs within 30 seconds, the system exits the setup mode and returns to standby mode (white light steady).
- Press ***** to manually exit the keypad code addition or deletion mode.

Notes

1. The “Hold Open” keypad code works as follows: Enter the code in standby mode, ending with **√**, to activate the relay. Enter the same code again to deactivate the relay.
2. Only one “Hold Open” keypad code can be set.
3. Keypad code conflicts:
 - Adding a “Hold Open” keypad code that matches an existing unlock keypad code will fail.
 - Adding a regular unlock keypad code that matches the “Hold Open” keypad code will also fail.
4. This feature is **not supported in Cloud mode**. Future support is planned.

10√	Exit-Button Unlock Delay Time	The time unit is 0.5 seconds, with a range from 0.5s to 10s. Input values correspond as follows: • 0√ = 0.5s • 1√ = 1s • 2√ = 1.5s • 3√ = 2s • ... • 19√ = 10s The default value is 3√ (2 seconds).	Yes	Yes
11√	Tone Volume	Select the volume level: • Press “1√” for low volume • Press “2√” for medium volume • Press “3√” for high volume The default value is 2√ (Medium volume).	Yes	Yes

12✓	IC Card Configuration	Select the IC card mode: ● Press “1✓” to activate card addition mode ● Press “2✓” to activate card deletion mode ● Press “3✓” to delete all cards IC Card Add/Remove Mode 1. After entering this mode successfully, the blue light remains steady. 2. Place the card to be added or removed on the card-swiping area. 3. Successful operation: green light stays on for 1 second and a single beep is heard. 4. Failed operation: red light stays on for 1 second and three beeps (beep dididi) are heard. 5. Repeat the process for all cards to be added or removed. 6. The system automatically exits the card addition/removal mode after 30 seconds of inactivity, returning to standby mode (white light steady). 7. Press * to exit card addition/removal mode immediately. Card Encryption ● Supports encrypted or unencrypted card swiping. Default is unencrypted. ● Encryption levels: Unencrypted / SL1 / SL3 (Priority 2, currently unsupported) Notes 1. Locally added cards have permanent validity and unlimited usage. 2. Supports up to 10,000 cards. 3. Duplicate cards can be successfully added or deleted. 4. Cards are read based on the 24-digit card number: ○ With QV 24-digit card-face IC cards, this applies only in unencrypted mode. ○ SL1 or SL3 encryption requires specific Mifare card types for addition and swipe-to-unlock operations. 5. Currently supports IC cards only; ID cards are	Yes	Yes
-----	-----------------------	---	-----	-----

		not supported.		
13√	Keypad Code Configuration	Select the keypad password mode: ● Press “1√” to activate password addition mode ● Press “2√” to activate password deletion mode ● Press “3√” to delete all passwords Password Add/Delete Mode 1. Press 1√, 2√ or 3√ to select your mode. 2. The blue light will remain steady, indicating the system is in password setup mode. 3. Enter the desired password to add or delete, ending with √. 4. The blue light will flash once, prompting you to re-enter the same password, ending with √. 5. Successful setup: the green light stays on for 1 second and a single beep (di) is heard. 6. Failed setup: the red light stays on for 1 second and three beeps (dididi) are heard. Failure occurs if: ○ Deleting a password not in the database ○ Adding a password that does not meet length requirements After successfully setting a password, the system automatically returns to password setup mode (white light slow-flashing). To add or delete additional passwords, re-enter 1√ or 2√ as appropriate. ● The system automatically exits the current password mode after 30 seconds of inactivity, returning to standby (white light steady). ● Press * to exit the password addition/deletion mode manually. Notes 1. Locally added passwords have permanent validity and unlimited usage. 2. Supports up to 10,000 passwords. 3. Password length: 4–12 characters. 4. Supports adding or deleting duplicate passwords successfully.	Yes	Yes

14√	Tamper Alarm	Select the tamper setting: - Press “2√” to enable tamper detection - Press “1√” to disable tamper detection The default value is 1√ (Tamper disabled).	Yes	Yes
15√	Continuous Input Error Protection	Select the Continuous Input Error protection setting: - Press “2√” to activate protection against Continuous Input Errors - Press “1√” to deactivate protection The default value is 1√ (protection deactivated). Note: Continuous Input Errors include incorrect or unauthorized attempts via card, password, QR code, or BLE unlock.	Yes	Yes
16√	IC Card Encryption Level	Select the card encryption mode: - Press “1√” for unencrypted cards - Press “2√” for SL1 encryption cards - Press “3√” for SL3 encryption cards The default value is 1√ (unencrypted). Note: This feature is not supported in Phase 1 development.	Yes	Yes
17√	Device Unbinding	Press “1√” to manually unbind the device from the site.	No	Yes

Manual Factory Reset

Press and hold the reset button for 5 seconds.

The panel will confirm reset mode with:

- 1 green light flash (1 second)
- 1 beep

Within 20 seconds, enter: X 357896321 √

The reset will then complete, confirmed by:

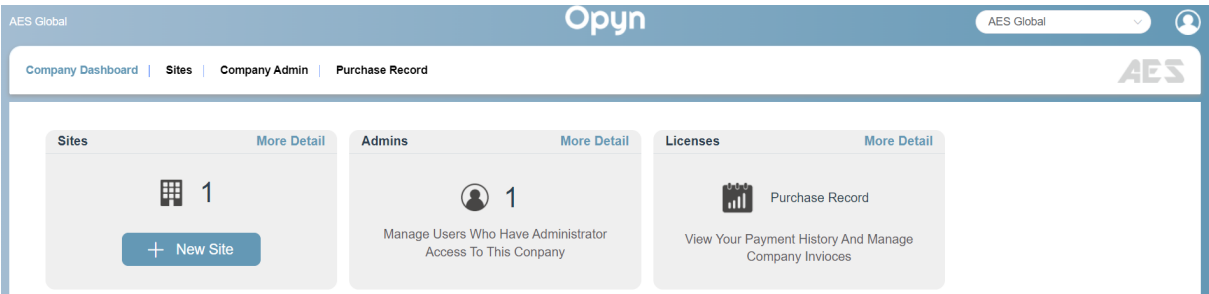
- 1 green light flash (1 second)
- 1 beep

Management Portal Operation

1. Company Dashboard

Link: [Opyn Multi - Management Portal](#)

This is the homepage of the portal. Here you can see all your sites, create additional admins and look at your purchase records for any licences. You can also create additional companies and swap between them using the drop-down menu in the top right corner.



a. Sites

View, edit or delete current sites or create new ones. Set in-app access control roles.

Create New Sites

Kilcronagh Business Park

Cookstown

Add

Site Name *

AES Test Site

Address *

123 Test Avenue

In-App Access Control Roles

Select

Cancel

Confirm

b. Company Admin

Here you have the ability to edit or delete any current admins while also adding new ones.

Add Admin				
Admin Name	Account	Role	Create Date	...
AES Thor	Jane.Doe@email.com	admin	2024-07-01 16:09:42	 

Add Admin ✕

Email Account *

Please Enter The Registered Account

User Role Company Admin:
Manages All Sites And Site Admins.
Makes Payments And Has Access To Billing Info.

Cancel

Search

c. Purchase Record

Keep track of all your licence purchases here. Filter by site or time frame.

Sites

Start Time

End Time

Search

Sites	License Name	Quantity	Amount	Admin Name	Create Date
Kilcronagh Business Park	License Package (Basic Edition) for 30 days	50	\$50		2024-07-01 16:18:42

2. Site Dashboard

From the site dashboard you have many options, which we will cover individually but here you can get a good overview of the blocks, devices and users for the site.

Site Dashboard

Block

Panels

Site Users

Operation Log

Panel Log

Site Licenses

Payments

Notices

User Messages

AES

Block

More Detail

12

Added Devices

Create New Panel

15

Added User

Add Users

13

Active Licences

2

Expired Licences

--

Not Opened

0

Not Accepted

+ Buy Licenses

a. Blocks

In the blocks section we can edit the block name and block number. You will also be able to see any devices assigned to this block along with any users assigned to these devices.

Block Detail

Panels

Users

Lift Relay Settings

Block Detail - See and edit block name and number.

Devices - See all devices attached to the block.

Users - See all users attached to the block.

Lift Relay Settings - Enable and configure elevator control.

b. Devices

In the devices section we have access to several settings, these include being able to edit the panel details, configure the role permissions, add a “SIP” server, change the DTMF settings and add “Guards”. We can also “delete” and “bind” and “unbind” devices.

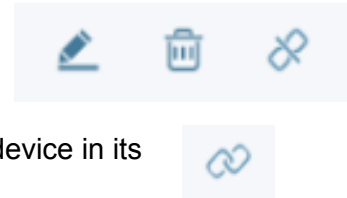
Device Actions:

Edit - Change information & settings of the device.

Delete - Remove the device from the management portal.

Unbind - Remove the existing device from the portal but keep information, settings & programming in place.

Bind - If a device has been “unbound” you can bind a new device in its place to inherit information, settings and programming.



Device Detail	Access Control	Guard Settings	Automatic Opening Times	General Settings
Device Name	4 - Test Keypad		Device Mode	Opyn Keypad
Site Or Blocks	Testing		Serial Number	24079yeifhu4
Floor Number	1		Device Version	V100.R260.A137.00.G0122.B413
Device Status	Offline		Bluetooth Version	401001011
			MCU Version	512
			BLE MAC	d4:39:82:c6:70:65
			IP Address	192.168.0.107

Device Details - See device info and edit name, block and floor number.

Access Control - Adjust the role permissions here as you wish.

Guard Settings - Here you can add guards to the device. You can add several guards which can call each other via the mobile app.

Automatic Opening Times - Configure times/days where the device relay will momentarily activate, or hold open.

Select “Lock”, “Mode” and “Day(s)” followed by the exact “Time”, then apply to all or several days if needed.

Lock Name	Lock 1
Mode Selection	Hold Open
Day	Thursday

Plan 1	⌚ Select 1	⌚ Select 1
Plan 2	⌚ Select 1	⌚ Select 1
Plan 3	⌚ Select 1	⌚ Select 1
Plan 4	⌚ Select 1	⌚ Select 1
Plan 5	⌚ Select 1	⌚ Select 1
Plan 6	⌚ Select 1	⌚ Select 1

Day Selection

☐ All

☐ Mon

☐ Tue

☐ Wed

☒ Thu

☐ Fri

☐ Sat

☐ Sun

General Settings - Change key settings of the keypad.

Master Code - See/Edit the device “Engineers Code”.

Relay Activation Time - Adjust the relay activation time.

Button Beep - Enable/Disable button beeps on the keypad.

Exit Button Unlock Time - Adjust the delay time of the exit button.

Tone Volume - Adjust the tone volume of the keypad.

Tamper Alarm - Enable/Disable the tamper/anti-vandalism alarm.

Continuous Input Error Protection - Disable the keypad for X minutes after X amount of attempted inputs.

Time Zone - Device time zone used for automatic opening times, time restricted codes/cards and logs.

Master Code	
Relay Activation Time	5
Button Beep	ON
Exit Button Unlock Time	3
Tone Volume	2
Tamper Alarm	OFF
Continuous Input Error Pr...	OFF
Time Zone	GMT00 London,Lisbon,Dublin

c. Site Users

In this section we can edit the user details, update the users licence, add codes & cards and more.

Admin users can add up to **250** of each unlocking method, while other types of users are limited to **20** per method. These methods being *Keypad Codes*, *QR Codes* and *IC Cards*.

Note: Some menu options are only available for use with the **Opyin-Multi** intercom system and will not be covered below. For example: *SIP & Facial Recognition*.

User Detail Devices SIP Settings Card Settings Car Plate Settings Face Unlock Password Unlock QR Code Unlock Sharing Management

User Details - You can edit most of the user's information including the block they are assigned to and their house/apartment number. Licences can also be assigned to a user from this page.

Devices - See all the devices the user has access to. There is also a toggle here for "Access Status" if you need to remove access for a time without having to delete them from the system.

Card Settings - Here you can add your cards to the different users. When adding a card you will need to input a name to make it easily distinguishable, followed by the full card number (8-10 digits) and which relay/lock to operate. There are a couple of ways to add the card number:

1. Manual Input (Full Card Number) - If you know the full digit card number you can enter this here and confirm to add.

Note: In some cases when entering a 10 digit ID you may need to use the "Reverse" button which will convert the ID differently. Only use this if having issues without it.

Add Card

☒ Full Card Number

☐ Facility Code&Card Number

Cancel

Confirm

2. Manual Input (Facility Code & Card Number) - If you only know the 3 digit facility code and the 5 digit card number add this in here to calculate your full card number.

Add Card

×

☐ Full Card Number

☒ Facility Code&Card Number

-

Cancel

Confirm

3. Reader - Connect a reader to your computer in order to scan the card and get the full card number. You need to make sure to have the correct drivers installed to operate the keypad. This can be downloaded from the portal. The reader can be purchased from AES.

Add Card

×



Reader is not detected, Please check your driver installation or Cable Connection !

Download Driver

Test Driver

Add Card



Please place a card on the reader

After adding the above you will then need to select how many uses this card will have before it expires, and also set a validity time. The final part of the adding process is choosing which devices to sync it to. You can select 1 or more devices that you have access to in which this card will be added to. The number of uses and the validity time can be toggled to “Unlimited” and “Forever” to make the card work permanently.

Add Card Number

×

Name *

Full Card Number *

Unlock Option *

Please Select

▼

Manual Input

Reader

Limited

Unlimited

Numbe Of Uses

Validity Time

⌚ Start Time

~

⌚ End Time

Forever

Panel Sync

☐ Production
☐ Engineering
☐ Entrance

Cancel

Confirm

4. - Batch Import - Add up to 20 cards/tags at once using CSV import. Download the file using the “Export” button, fill in the information as explained in the document and then click the “Import” button and upload the file.

Batch Import

×

This feature is designed to make it easier for installers to import target data. Please use the "Export" function before each batch import operation and carefully review the usage notes inside the table.




Note: The system uses 24-bits as its standard, if your card is 32-bit it will be converted to 24-bit and the ID displayed on this portal will be different from what may be printed on your card.

Password Unlock - Add and manage Keypad Codes for each apartment/user. Enter the required information such as name, keypad code, lock, number of uses and validity time and which device(s) to sync to. Then click “Confirm” to add.

Add Password Unlock

Name *

Unlock Password *

Unlock Option *

Please Select

Limited

Unlimited

Validity Time

Start Time

~

End Time

Forever

Panel Sync

☐ AES HQ Test

☐ Technical Test

Cancel

Confirm

QR Code Unlock - Add and manage QR Codes for each apartment/user. Enter the required information such as name, lock, number of uses and validity time and which device(s) to sync to. Then click “Confirm” to add.

Add QR Code Unlock

Name *

Unlock QR Code

Click To Display

Unlock Option *

Please Select

Limited

Unlimited

Validity Time

Start Time

~

End Time

Forever

Panel Sync

☐ AES HQ Test

☐ Technical Test

Cancel

Confirm

Sharing Management - See and manage the users that the apartment has been shared with.

Invite - Add a new user to share the apartment with.

Delete - Remove a user's access to the apartment.

Re-Invite - Send another sharing message to the user's mobile app.

Note: *An apartment can only be shared with 8 users.*

Sharing Management

×

Please Enter The Account You Want To Share With

Q

d. Operation Log

This log keeps track of all managerial operations done on the portal. It will give you the user name of the person who carried out the operation along with the operation type and the time.

-

User Name	Operation module	Operation Content	Create Date
--	Notice	Release device notice	2024-09-04 12:39:31
--	Notice	Create device notice	2024-09-04 12:39:28
--	Site Licenses	Buy Licenses	2024-09-04 12:34:02
--	Notice	Withdraw device notice	2024-07-16 08:32:33
Jane Doe	Panels	Delete Ddevice guard config	2024-07-16 08:31:53
Sagland Thor	Panels	Create Ddevice guard config	2024-07-16 08:31:27
Jane Doe	Panels	Update Panels	2024-07-16 08:26:17
--	Panels	Binding Panels	2024-07-16 08:25:52
--	Notice	Release device notice	2024-07-16 08:09:27
--	Notice	Create device notice	2024-07-16 08:09:18

< 1 2 3 4 >

Go to 1

e. Device Log

The device log is separated into 3 categories. You can export all these logs as “.xlsx” files.

Call Log - Displays both answered and unanswered calls along with who the call was for and a snapshot.

Access Log - Displays unlock events such as keypad code, qr code or facial recognition.

Tamper Log - Displays any tamper alarm events that may have been set off.

Call Log Access Log Tamper Log

-

Panel	Blocks/Sites	Apartment Number	User Name	Unlock Type	Status	Time
Test 2	Unit 4C	1	Jane Doe	Unlock Password	Success	2024-09-09 10:20:14
Test	Unit 4C	1	Jane Doe	Unlock Password	Success	2024-09-09 10:20:13
Test 2	Unit 4C	1	Jane Doe	Unlock Password	Success	2024-09-09 10:20:09
Test	Unit 4C	1	Jane Doe	Unlock Password	Success	2024-09-09 10:20:07
Test	Unit 4C	1	Jane Doe	QR Code	Success	2024-09-09 10:19:32
Test 2	Unit 4C	1	Jane Doe	QR Code	Success	2024-09-09 10:19:27

f. Site Licences

Here you can keep track of how many licences you have remaining available to your site. If you wish to may also buy more from this page, but this can also be done from the “Payments” page.

Service Licenses

Activation Records



License Package (Basic Edition) for 30 days

131

Remaining Quantity

Buy More



License Package (Basic Edition) for 1 days

20

Remaining Quantity

Buy More

You can also view the records for all activations within your site. Search directly by user name or by licence type to help filter the records as you wish.

Service Licenses

Activation Records

User Name

Licenses Name

Search

Licenses Name	Code	Users	Blocks Name	Create Date
License Package (Basic Edition) for 30 days	--	Test Test	Unit 4 (AES)	2024-11-05 15:11:57

g. Payments

Here you can purchase licences to be added to your site.

Service Licenses

Purchase Record



License Package (Basic Edition) for 7 days

\$1 /Person

Buy Now



License Package (Basic Edition) for 30 days

\$1 /Person

Buy Now



License Package (Basic Edition) for 1 days

\$1 /Person

Buy Now

Buy Licenses

 License Package (Basic Edition) for 30 days \$1 /Person

Buy Quantity :

10

20

50

Custom Quantity

Pay Platform : ☐  ☐ 

Pay Amount : \$10

Pay

When buying licences you will need to enter the quantity you want and be sure to select “Stripe” as the payment platform. You will then be prompted with a check-out page which will require you to enter details such as card number and expiry date. After the payment is successful the licences are immediately added to your site.

Note: Prices shown in this manual do not reflect actual prices for licences.

h. Notice

In this section we can create notices to be sent either to the app users of your site or to the devices. They are divided into 2 separate pages “App Notice” and “Device Notice”.

App Notice - This notice type lets you send out a notification to all the app users in your site or you can select specific users. Simply select “Broadcast” or “Private Message”. After this, fill out the required information and click “Create Notice”. The notice will then appear on the “App Notice” list after which you can choose to release, withdraw or delete it.

We recommend uploading pictures with a 16:9 ratio.

*Reception Device:

Broadcast

Private Message

Selected User Number: 0/10

*Title:

The title length must be 1-50digits

*Title Picture:

Note: it is suggest to upload in image width 16:9 ratio.

*Content:

0/2000

Content can only be entered with a maximum of 2000 characters

End Time

🕒 End Time

Create Notice

Cancel

License Package (Basic Edition) for 1 days
\$10.00
 Qty 10, \$1.00 each

G Pay

Or pay with card

Email

Card information

1234 1234 1234 1234

VISA

MasterCard

Amex

MM / YY

CVC

Cardholder name

Full name on card

Country or region

United Kingdom

Postal code

☐ Securely save my information for 1-click checkout
 Pay faster on this site and everywhere Link is accepted.

Pay

Device Notice (Opyn-Multi Only) - This notice type lets you send out a notice either to all devices in your site or you can choose a specific device. Choose between “Broadcast” or “Choose Device”. Afterwards make sure to fill out all the required information. The notice will then appear in the “Device Notice” list after which you can choose to release, withdraw or delete it.

We recommend uploading pictures with a 9:16 ratio and 600 x 1024 pixels.

*Reception Device: Broadcast Choose Device Selected Device Number: 0/10

*Title: The title length must be 1-50digits

*Title Picture: 

Note: it is suggest to upload in image width 9:16 ratio.

Time Range: Start Time - End Time

Create Notice Cancel

i. User Messages

This section allows for communication directly between residents and management via the app and management portal.

As you will see this “ticketing system” allows requests/questions from the residents to easily be collected and managed in one place.

Please enter title Country Issue type Release Status Start Time - End Time Search

Users	Country	Email/Phone	Title	Issue type	Status	Creation Date	...
Sagland Thor			When will elevator be fixed?	Question	Pending	2025-07-10 07:46:53	More

View Message

By clicking “**More**” on a message you will be taken to a different screen where you can see the initial message and all its details such as the user name, and if provided also email/phone, country.

Title: When will elevator be fixed? Name: Sagland Thor Email/Phone: Country: Picture:
Description: ✎ Wonder when elevator will be fixed

Reply to message

1. To reply to a message locate the options at the bottom of the page and hit “**Reply**”



2. After doing so a new screen will appear that will allow you to enter a message you can send back to the user. Just simply enter your message and click “**Submit**”.

Reply Contents

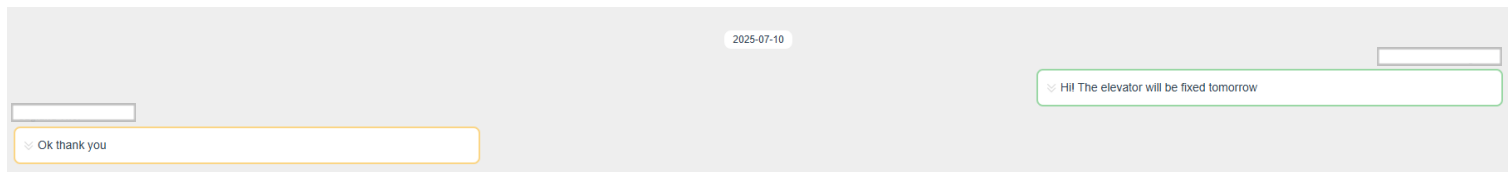
Please enter reply contents

0/2000

Submit

Cancel

3. Once the reply has been sent you can see your reply and any further messages from the user on this topic appear as a chat.



Change status

If you want to change the status of this message simply use the options on the bottom of the page

Denied - Will reject the request/question.

Finished - Will mark it as completed.

Processing - Signifies that this request/question is being processed.

Return - Will return you to the previous page.

The updated status will be displayed to the user and appear on their app.

Note: The users point of view for this function can be found in the “App Operation” section.



App Operation

The AES Opyn mobile app is crucial for users of the system. It allows users to remotely add and manage keypad codes, qr codes and cards/tags. You can also invite other users, activate the locks of the device and more. We will be covering these essential features below.

1. Add Intercom to Device

To add an Opyn Keypad to your AES Opyn app you need to be invited to a site. The management of the site needs to create you as a user in the management portal, after which an email will be sent out containing a QR code & link you can use after you have downloaded the app and signed in.

Note: This email may appear in your spam folder, and must be moved to your main inbox in order to view the QR code.

After using the QR code or link you will be prompted with the invitation pop-up asking if you wish to accept or decline. Should you choose to accept, the site and all devices within will automatically populate inside your app.

2. Devices (Home Page)

The “Devices” page functions as the app’s home page. From here we can access settings, activate relays and more.

a. Relay Activation & Bluetooth Activation

Trigger relays from this screen if you wish. Simply tap the icon for the relay you want to activate and this will momentarily trigger the relay.

Activate the relay manually via bluetooth. (if enabled and configured)

b. Pin Apartment

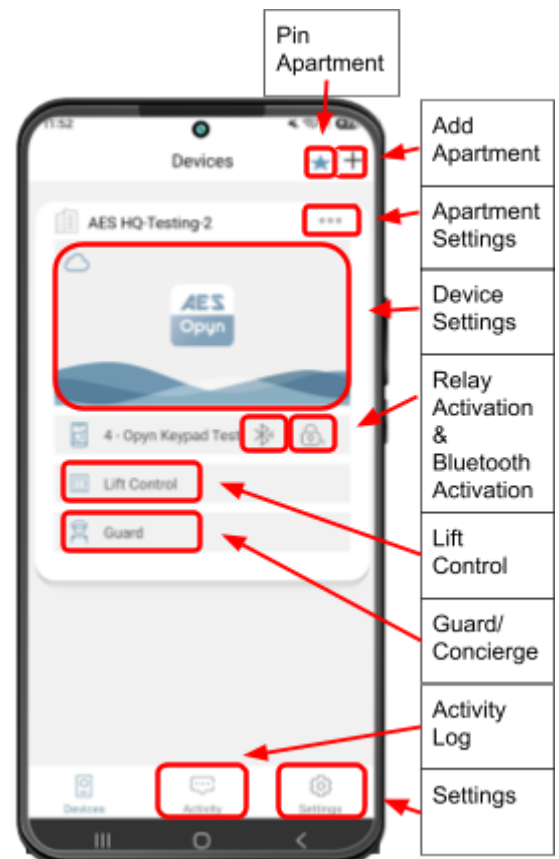
Select one or more apartments to pin to the top of your device list. The most recently pinned apartment will appear first.

c. Add Apartment

You can scan a site QR using the “+” signs located on this page.

d. Apartment Settings

Clicking the three dots on this page will open up a menu that can take you to the apartment settings.



e. Device Settings

Click the thumbnail (AES Opyn logo) to enter keypad settings.

f. Lift Control

Call the elevator to your assigned floor. (If elevator control is in use)

g. Guard

Call the guard/concierge from your app. Or if you are a guard/concierge, call residents. (If configured)

h. Activity

The activity log can be navigated to by the bottom menu. More info on this feature below.

i. Settings

Settings related mainly to the app and calls, more info on this below.

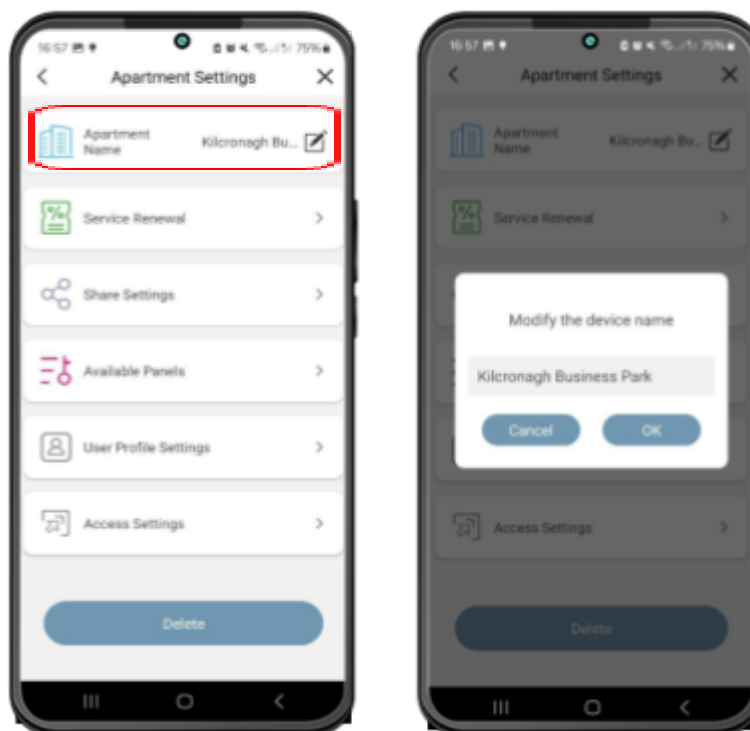
**Additional Banners for IP Camera, Lift Control & Guard will only show if they have been configured on the management portal.*

3. Apartment Settings

Within this section of the app you will find settings that affect the apartment and all the devices this apartment has access to.

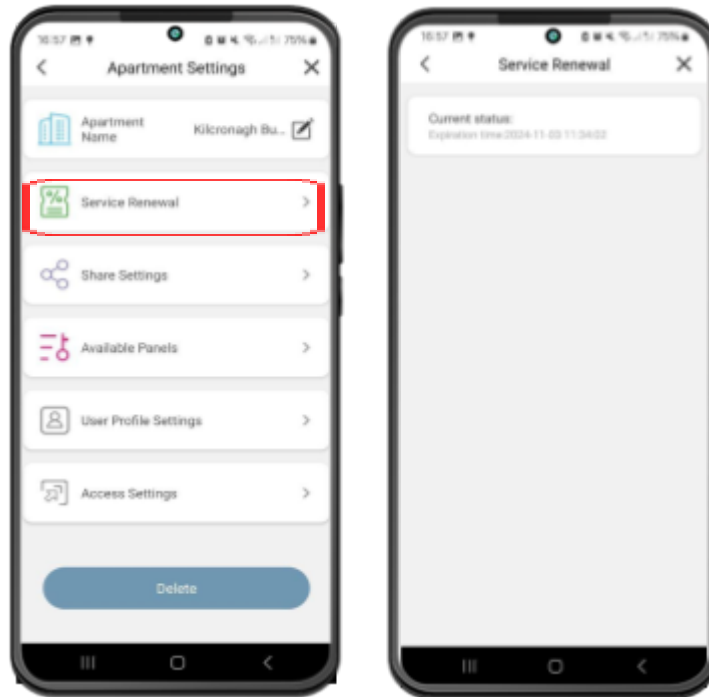
a. Apartment Name

Change the name of your apartment/site as you please. This only changes for your app account.



b. Service Renewal

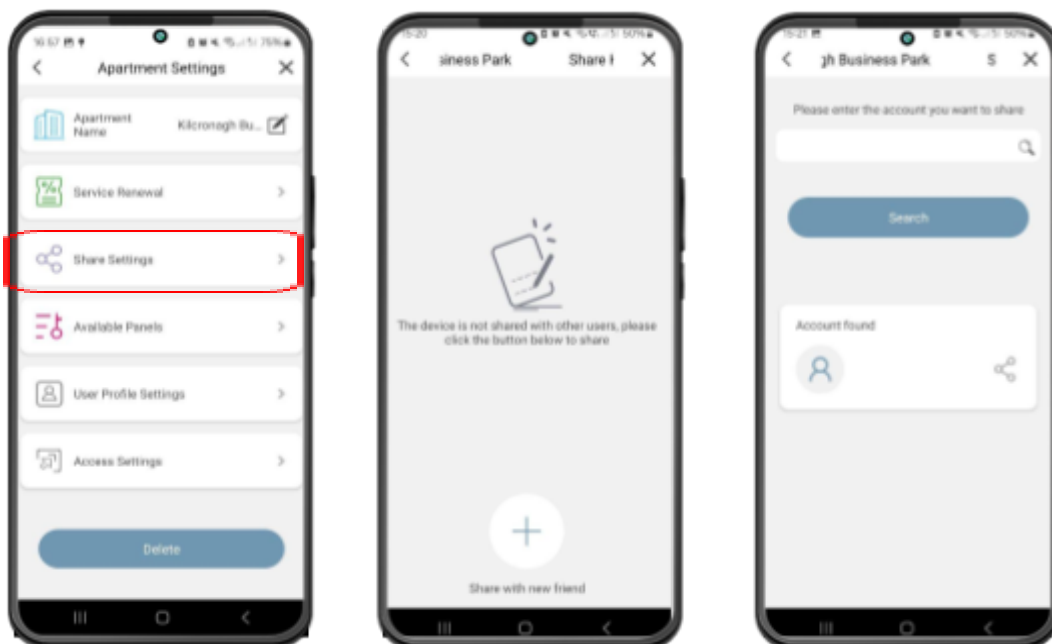
Keep track of when the licence for your apartment is going to expire. It is up to management to give you a new one should yours expire.



c. Share Settings

Share access to your apartment. All that is required is that the person you are sharing with has an AES Opyn account and app. You can then search for them using the email they signed up with and send an invite. They will need to accept this on their app and will be given “user” access”.

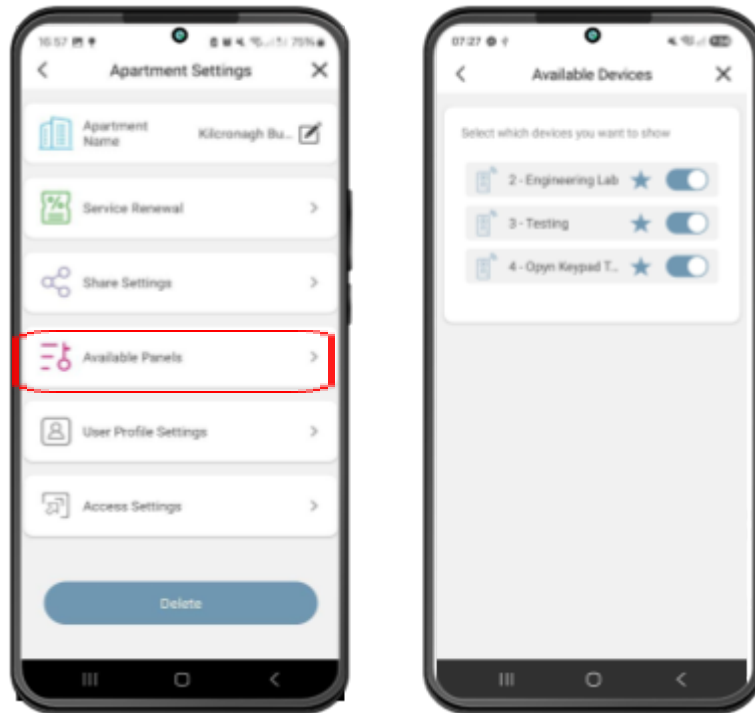
Note: An apartment can only be shared with 8 users.



d. Available devices

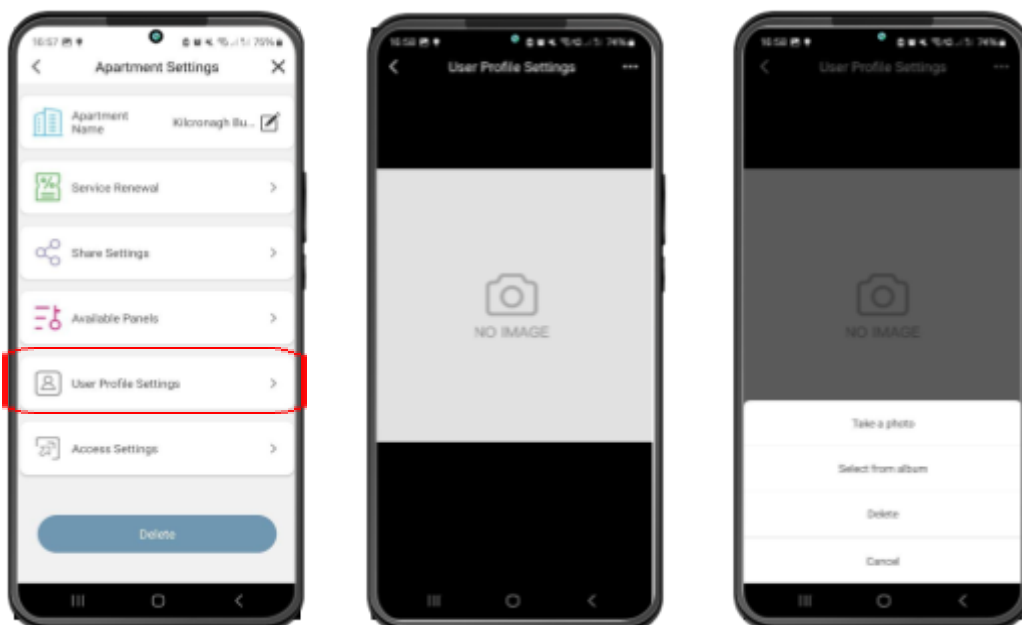
See a list of the devices you have access to. You can choose to enable or disable them being displayed on your “Devices” page.

You can also pin the devices to appear at the top of the device list for your apartment. The most recently pinned device will appear first.



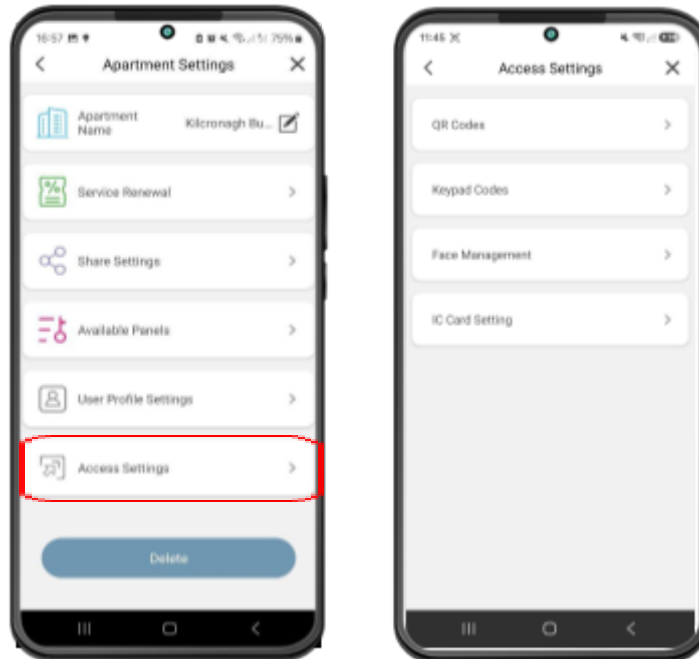
e. User Profile Settings

Here you can upload a picture for your user profile. This picture is what will be displayed in the contact list of all devices you have access to and on the management portal.



f. Access Settings

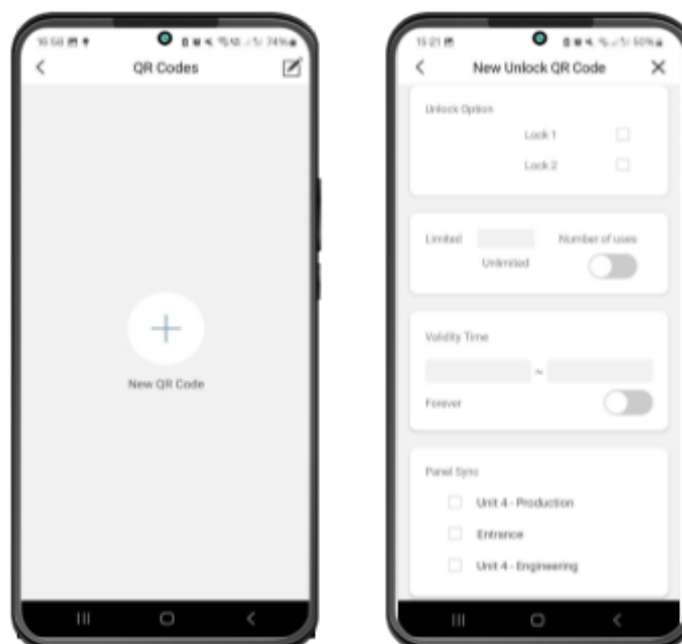
In this section of the app you can add QR Codes, Keypad Codes and Face ID's to operate the relays/locks of the device(s).



QR Codes

To add a QR you need to first give it a name. You then need to select the “Lock” you want it to operate followed by the “Number of uses” and “Validity Time”. Both the numbers of users and validity time can be adjusted to suit the needs of the user. They can also be set to “unlimited” and “forever” by pressing the toggles.

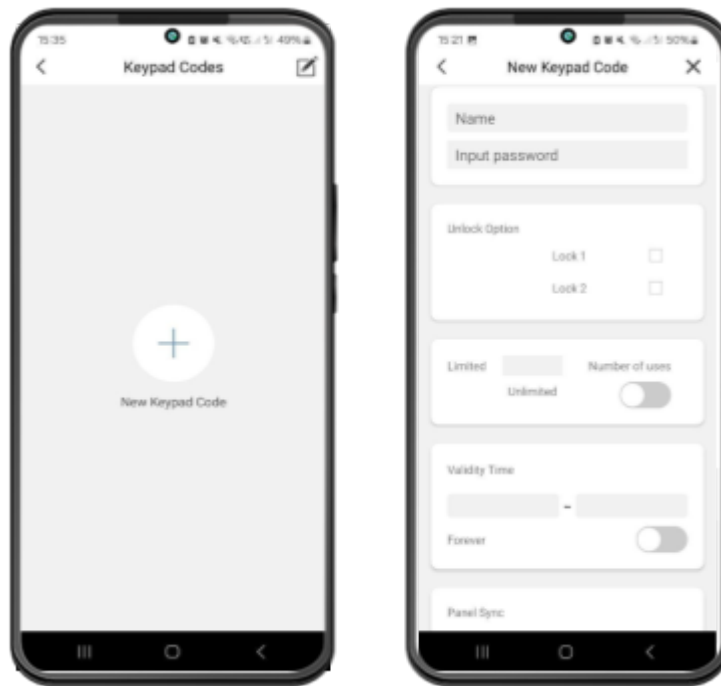
Lastly you have the “Device Sync”. Here you can see all the devices you can add this code to. After you have filled in all the information and selected device(s) hit “OK”. This will sync the code to all the devices selected.



Keypad Codes

To add a keypad code you need to first give it a name. You then need to input what you want the code to be, followed by selecting the “Lock” you want it to operate followed by the “Number of uses” and “Validity Time”. Both the numbers of users and validity time can be adjusted to suit the needs of the user. They can also be set to “unlimited” and “forever” by pressing the toggles.

Lastly you have the “device Sync”. Here you can see all the devices you can add this code to. After you have filled in all the information and selected device(s) hit “OK”. This will sync the code to all the devices selected.

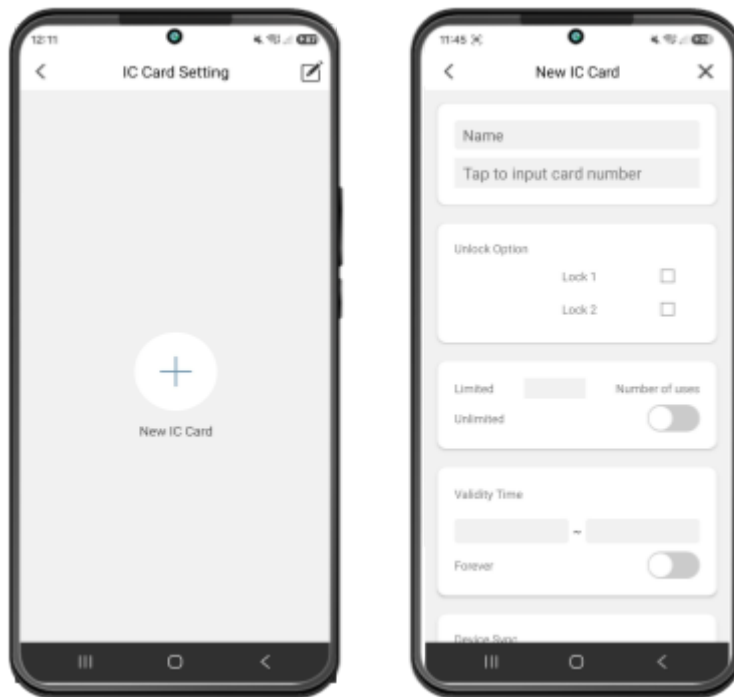


Face Management (Not available on the Oryn Keypad)

IC Card Settings

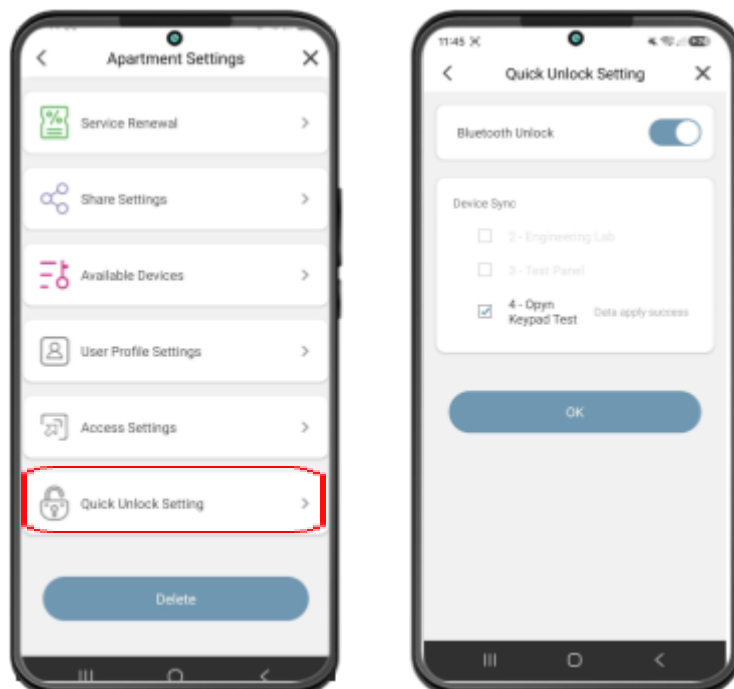
To add a card/tag you need to first give it a name. You then need to input the cards/tags ID, followed by selecting the “Lock” you want it to operate followed by the “Number of uses” and “Validity Time”. Both the numbers of users and validity time can be adjusted to suit the needs of the user. They can also be set to “unlimited” and “forever” by pressing the toggles.

Lastly you have the “Device Sync”. Here you can see all the devices you can add this code to. After you have filled in all the information and selected device(s) hit “OK”. This will sync the card/tag to all the devices selected.



g. Quick Unlock Setting

Configure the manual bluetooth unlocking option within the app. Enable the bluetooth unlock and select the device the function should be set for.

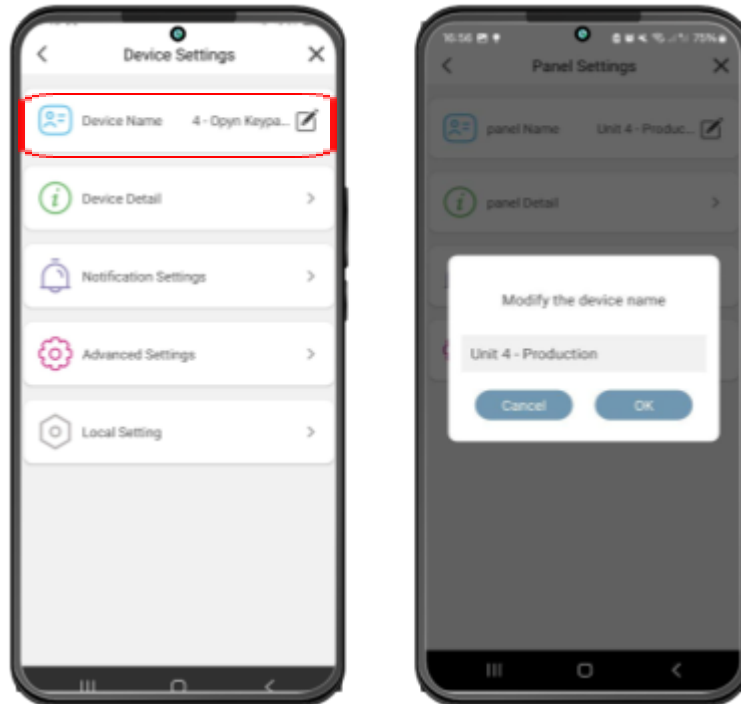


4. Device Settings

Within this section of the app you will find settings that affect the individual device accessed to reach this section.

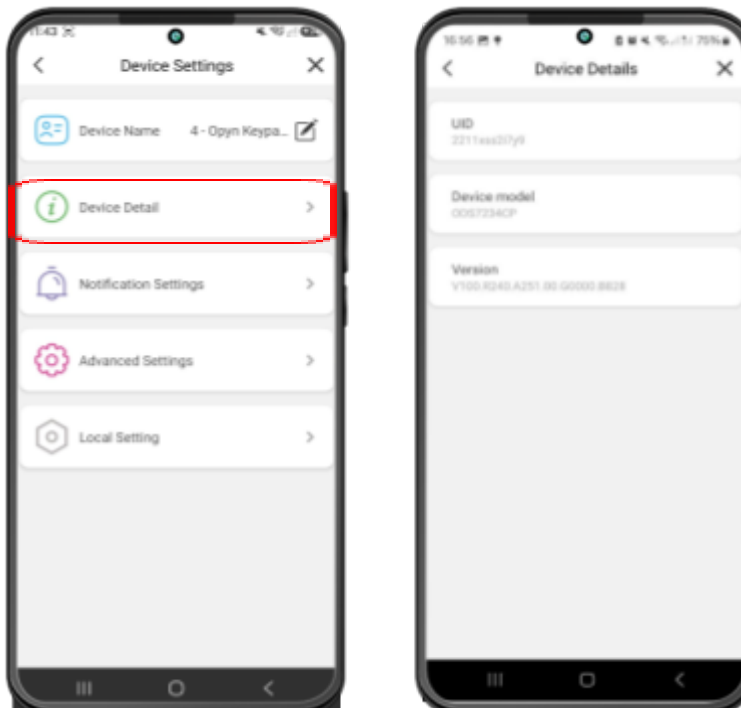
a. Device Name

Change the name of your apartment/site as you please. This only changes for your app account.



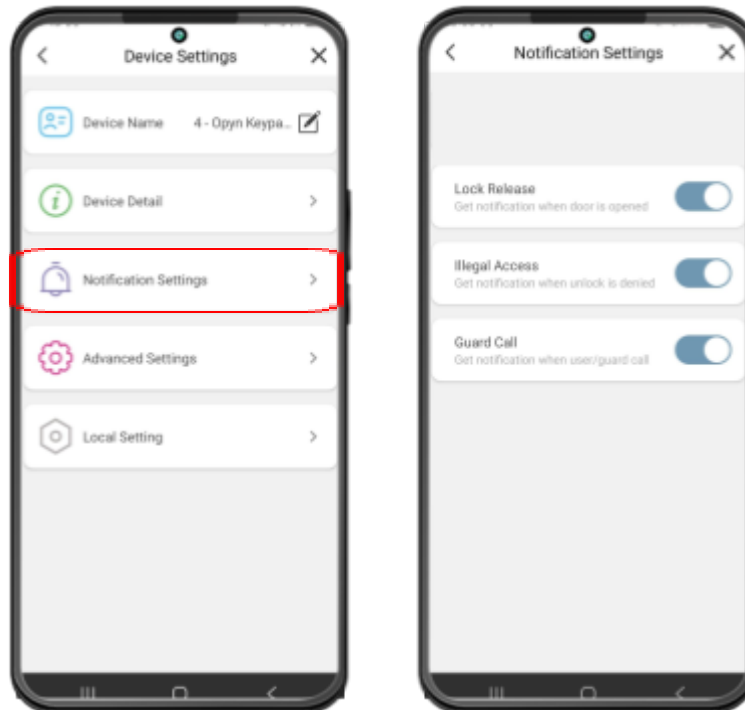
b. Device Detail

View details specific to this device such as its UID, model and software version.



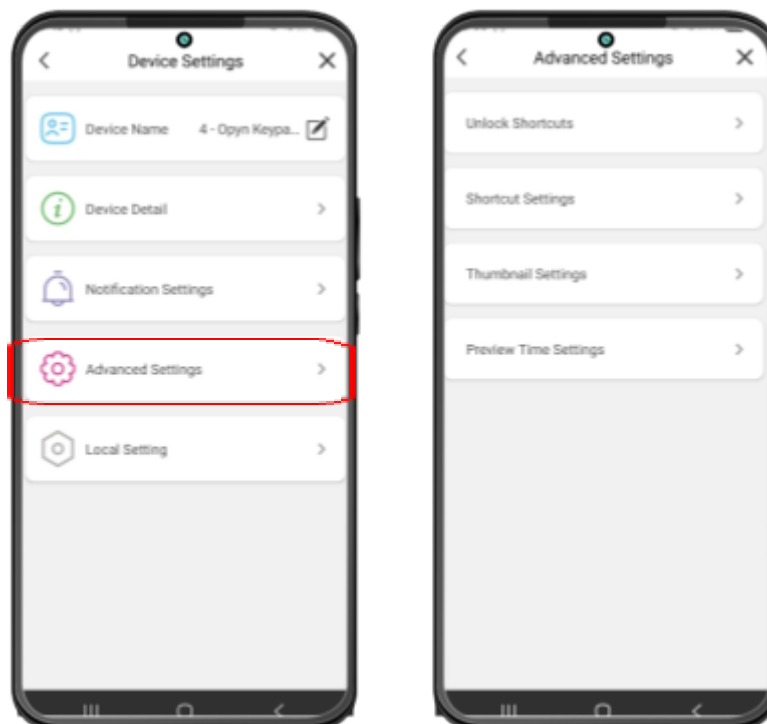
c. Notification Settings

Enable and disable the different types of notifications you will receive for this device.



d. Advanced Settings

This section gives you access to additional features such as creating “Unlock Shortcuts”. Adjusting the “Devices” page shortcuts, changing the “thumbnail” for the devices and more.



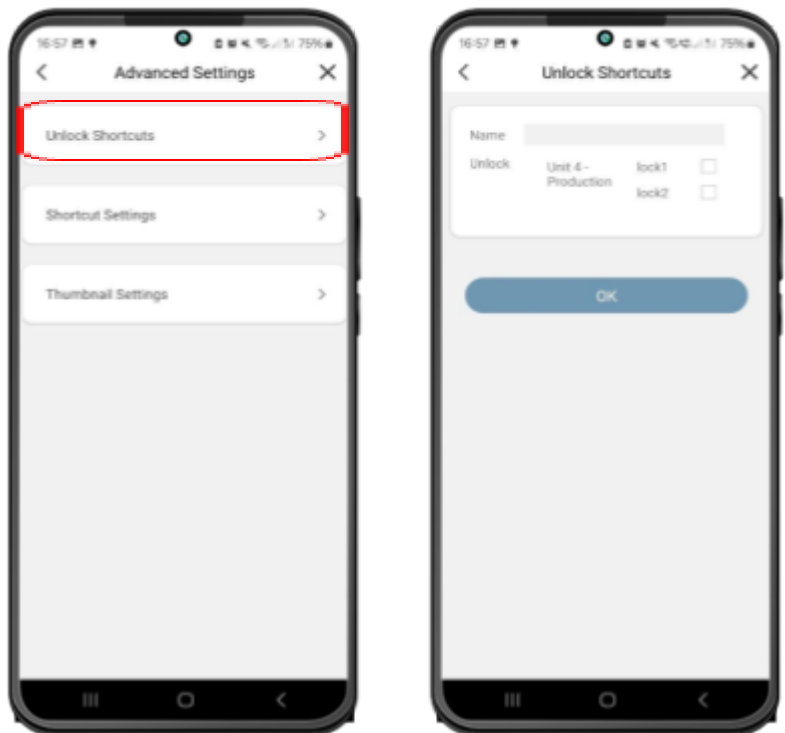
Unlock Shortcuts

Create a shortcut that will allow quick and easy activation of the device's relays/locks.

Simply name the shortcut and select the lock you wish to operate then depending on your phone's operating system it will work in 1 of 2 ways.

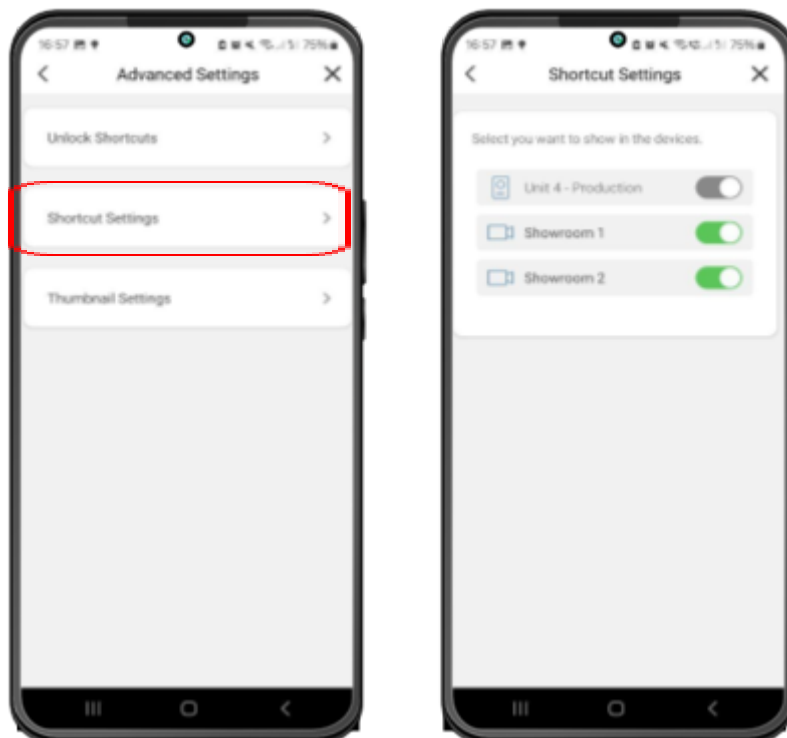
Android: Will create a widget to go on the home screen of your phone. Upon pressing this widget the app will open and automatically activate the chosen lock.

iOS: Will create SIRI command that can be used by speaking the phrase "Hey siri, [Shortcut name]". This again will open the app and automatically activate the chosen lock.



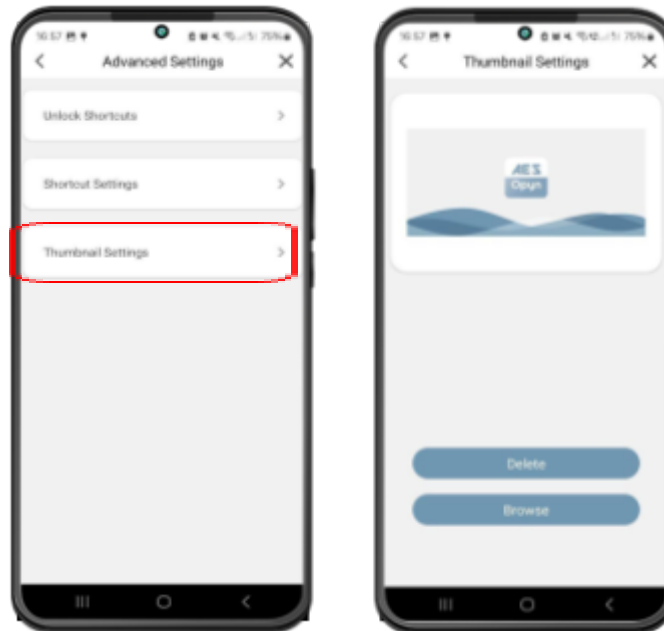
Shortcut Settings

Here you can enable and disable devices being shown on the "Devices" page inside the app.



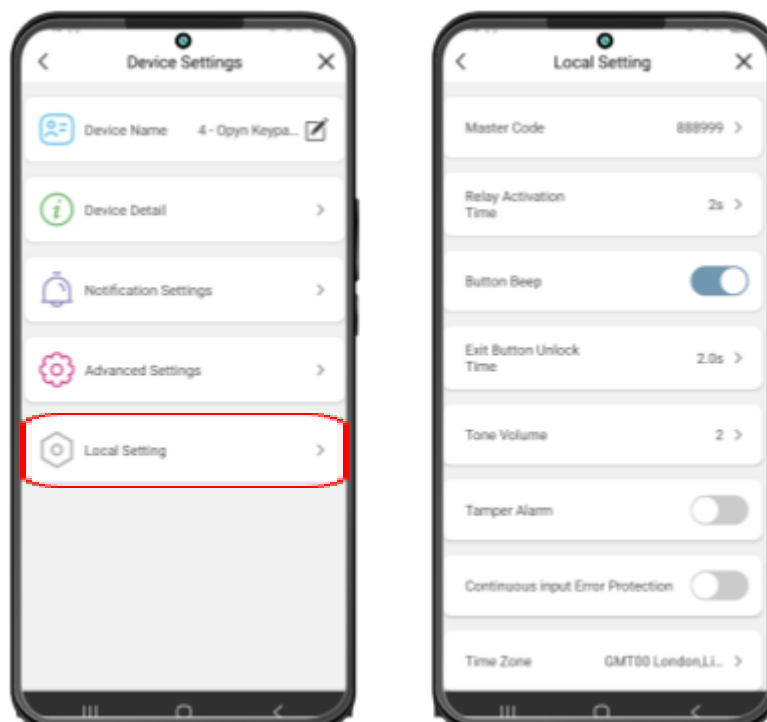
Thumbnail Settings

Add or delete a thumbnail to be added to the device. The purpose of a thumbnail is to always be shown on the “Devices” page rather than a snapshot from the last video session.



e. Local Settings

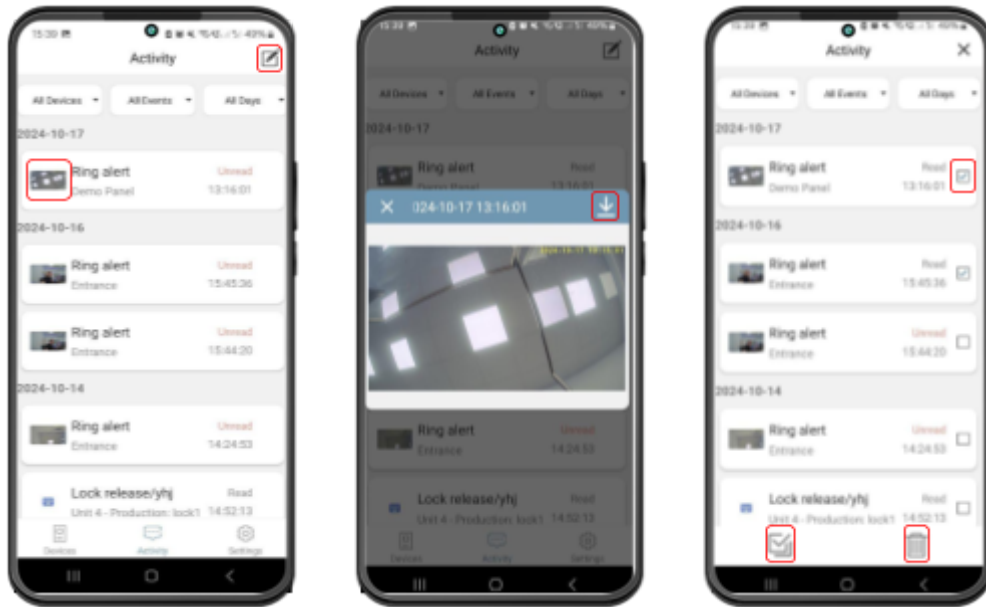
This section lets you change several settings for the Opyn Keypad, such as engineers code, relay activation time, time zone, **automatic opening times** and more.



5. Activity Log

From this page you can view the events relevant to your apartments. Be that qr codes, keypad codes and face IDs registered to your apartment. You can view a snapshot of the user taken at the moment of the entry method being used by clicking the thumbnail. You can also save this to your app album.

You also have the ability to delete events. You start this process by using the icon in the top right corner. Then you can either delete individual events or select all and delete.

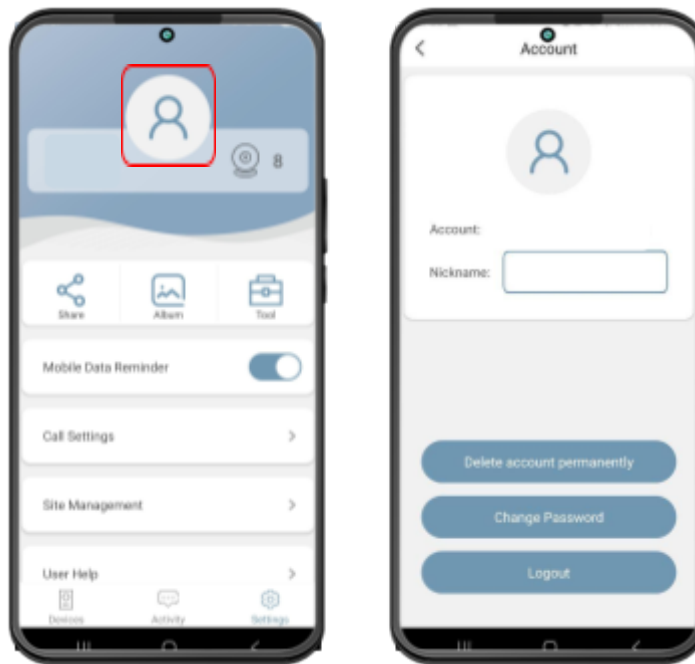


6. Settings

In this section of the app you will find general settings regarding your account, app and more.

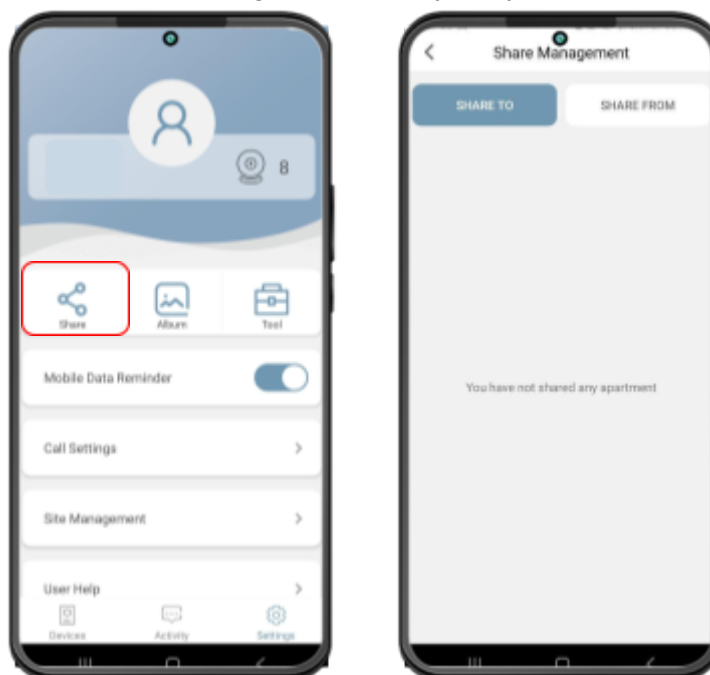
a. Account

The accounts page lets you change your “nickname”, delete your account and change the login password. You can also logout from this page.



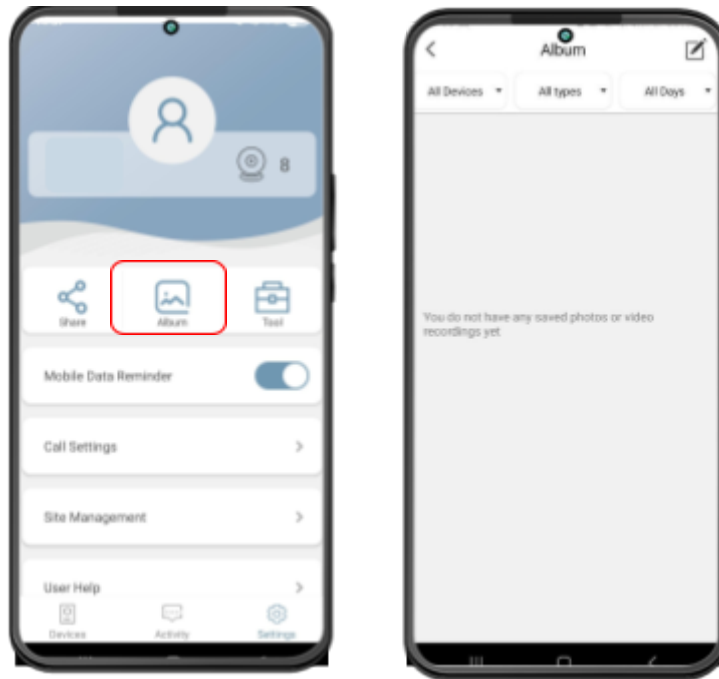
b. Share

This page will display all the users you are sharing your apartment with, but also show all the apartments that are being shared with you by other users.



c. Album

The album will display photos and videos saved either from the activity log or directly from the camera preview page. You can save these directly to your phone from here or delete them. These are saved in the device app memory.



d. Tool

This section's features do not affect the “Opyn Keypad” system. Instead it is meant to work with the standard AES Opyn single button intercom system.

e. Mobile Data Reminder

This reminder will appear when your device is using mobile data while viewing the camera. The purpose behind this reminder is to avoid you using up all your mobile data unintentionally.

f. Call Settings

This page lets you adjust settings specific to the incoming calls. These settings include:

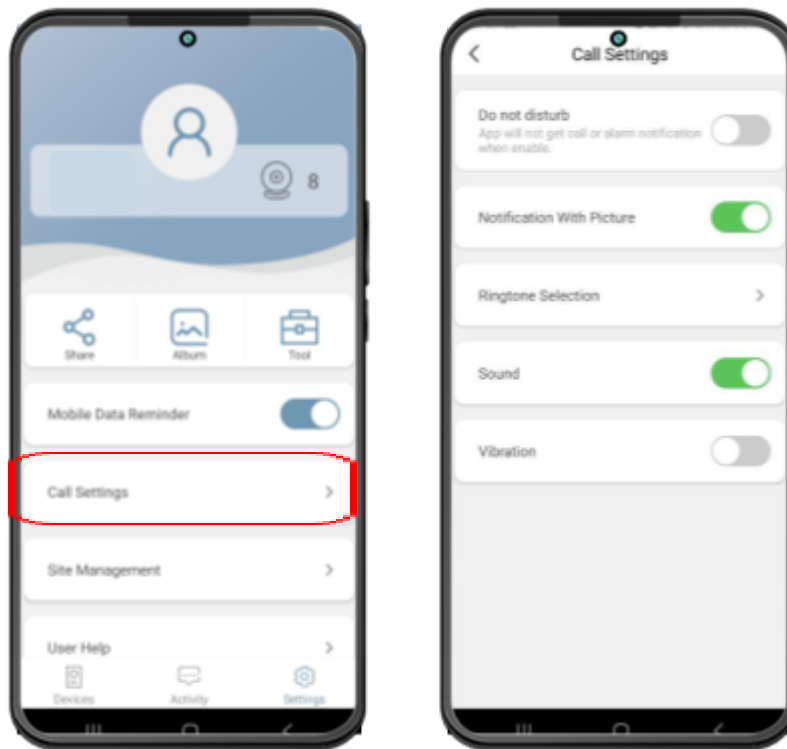
Do not disturb - Which will disable all notifications from the app when enabled.

Notification with picture - Relates to calls, motion, alarm notifications. Enabling this allows you to see a snapshot in the notification banner taken by the camera at the time of the event.

Ringtone Selection - Change the ringtone for incoming calls.

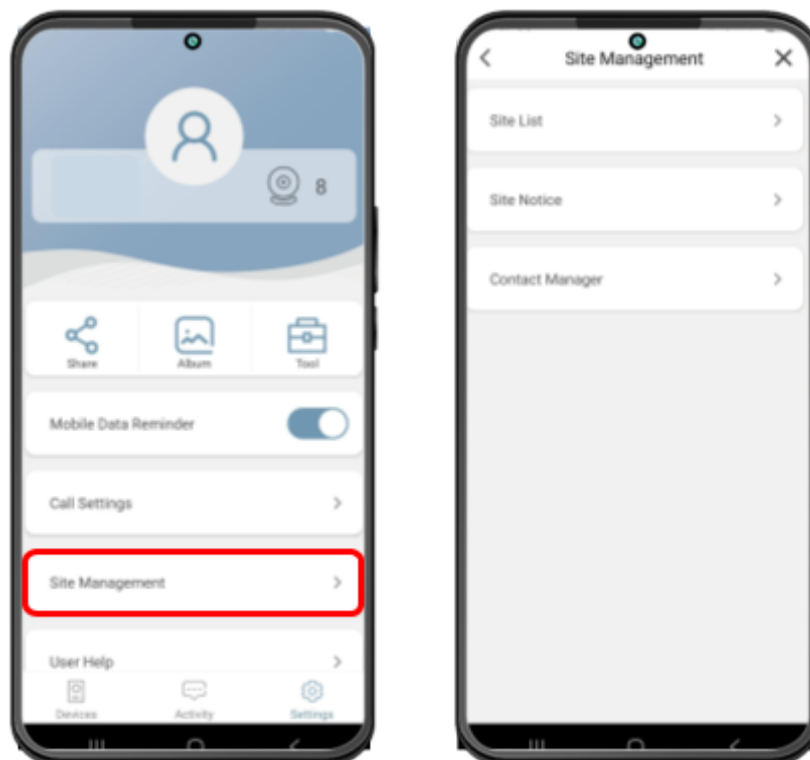
Sound - Enabling or disabling this will determine if incoming calls will have a ringtone or be silent.

Vibration - Enabling or disabling this will determine if incoming calls have vibration or not.



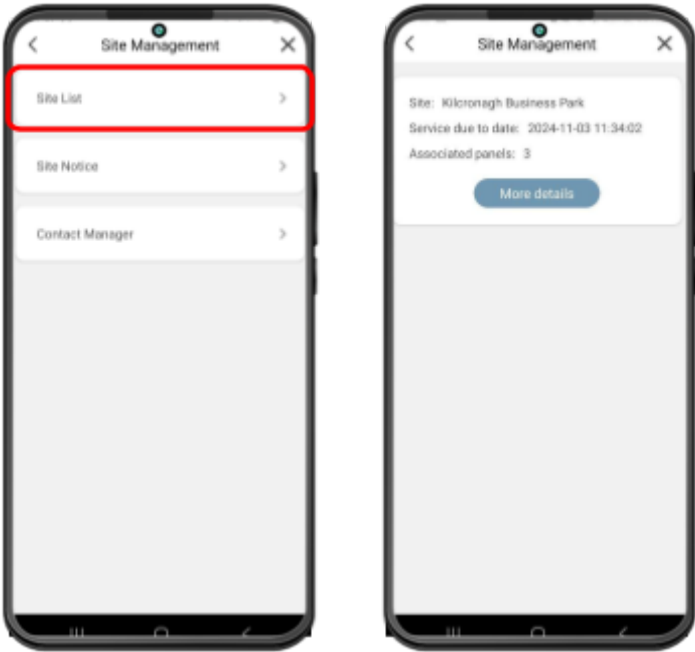
g. Site Management

This page lets you manage different parts of your sites via features such as “Site List”, “Site Notice” & “Contact Manager”.



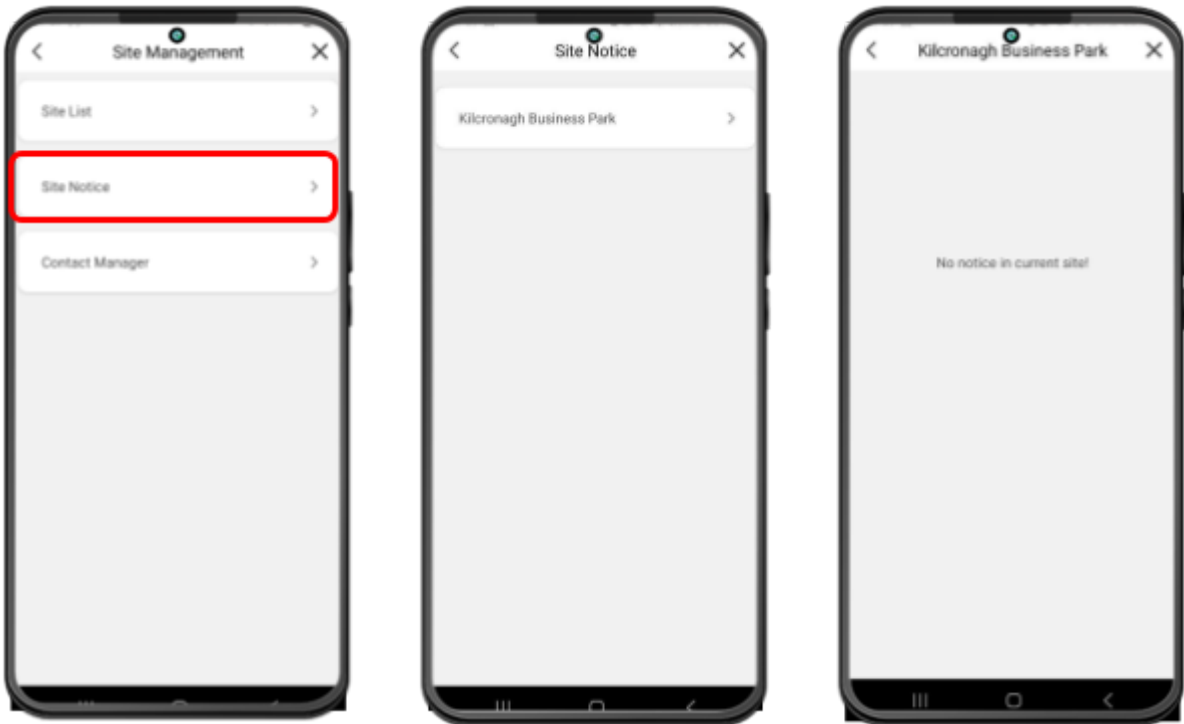
Site List

This page lets you see all the apartments you have access to, when your licence will expire for each and how many devices in each apartment gives you access to. Using the “More details” button will take you to “Apartment Settings”.



Site Notice

Management has the ability to send out notices that can be for all users within the site or also specific apartments. If you get a notice it will firstly appear for you as a push notification but can also be viewed in full within the app from this page as long as it has not been removed by management or expired.

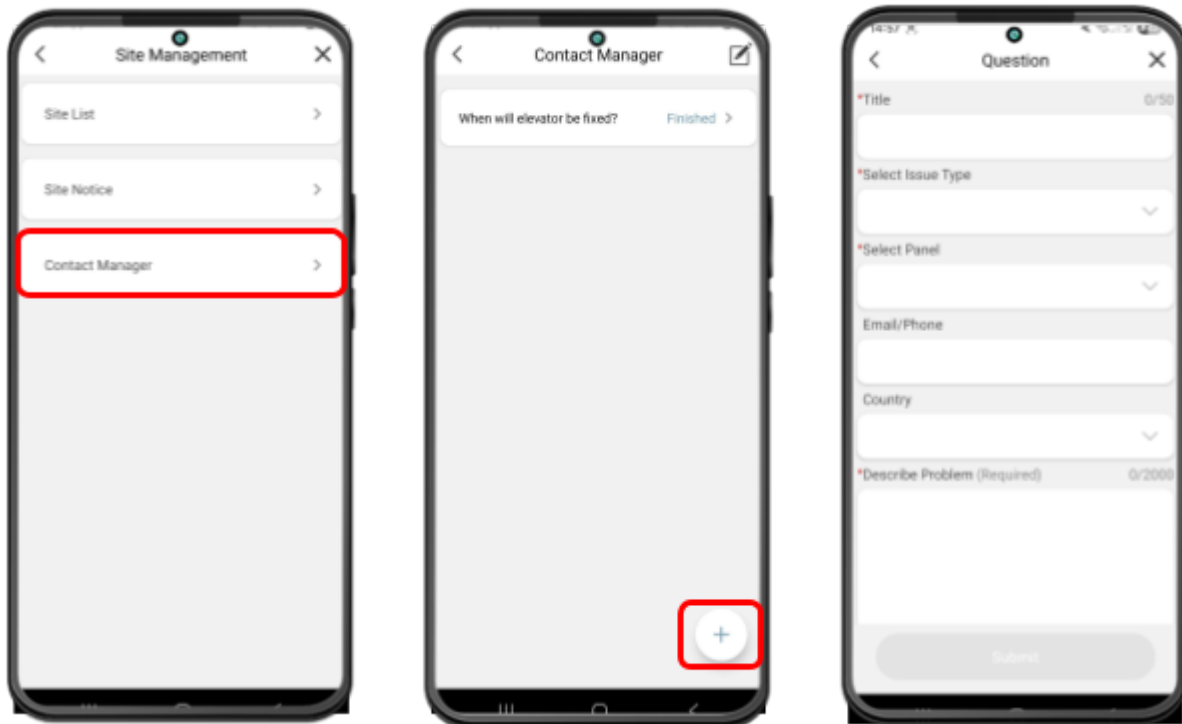


Contact Manager

Send tickets to management with questions or issues related to the intercom system, app or other topics.

Create a new ticket by clicking the “+” icon in the bottom right. Simply enter the information that is required and send it to management.

You can see existing tickets that have been closed or are still open, and continue these as chats.



h. User Help

We have added a built-in “User Help” section into the app which will answer several frequently asked questions around your account, device setup, playback features and more. We hope that users will find this helpful and prevent them from having to go look for the answer elsewhere.

i. About

This page will give you information about the app version and the date it was released along with access to our T&Cs and Privacy Policy.

Local Web Interface Operation

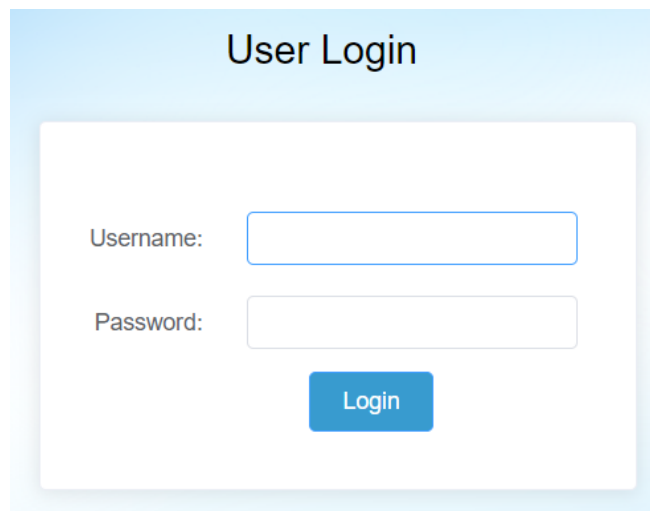
There are also some additional features that can only be accessed by connecting to the device via the local-area-network. This means that both the device and the computer accessing this page need to be on the same network (IP scheme). We will only cover the essential features here and do not recommend adjusting any settings not covered in this manual.

To access this page you will need to enter the IP address of your device into your browser. The IP can be found via the device itself in the “Device Information” page that can be accessed from “Settings”.

The default login credentials are:

Username: *admin*

Password: *123456* (Same as engineers code)

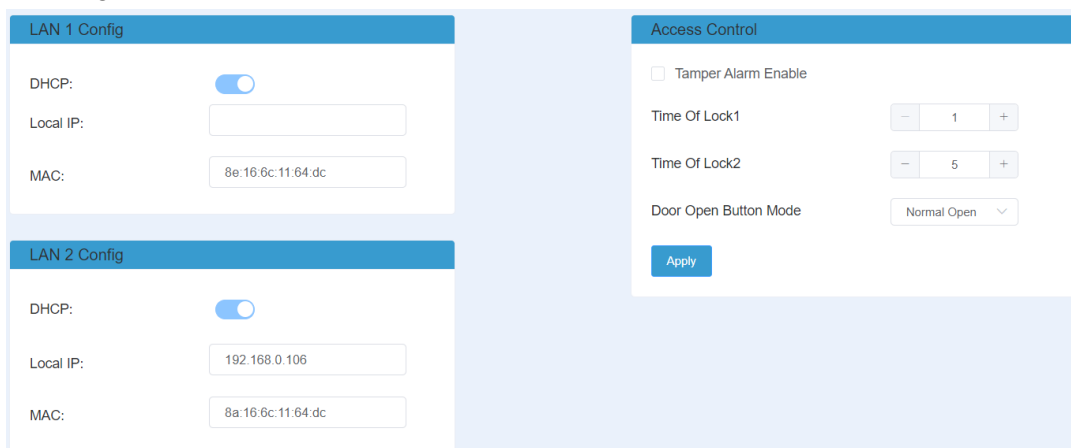


The image shows a 'User Login' form with a light blue header. Below the header is a white box containing the login fields. The 'Username' field is a text input with a blue border. The 'Password' field is a text input with a grey border. Below the password field is a blue 'Login' button.

Local Config

The features on this page include:

- View device IP & MAC address
- Enable or disable tamper alarm
- Adjust unlock time for lock 1 or lock 2
- Change default state of exit button



The image shows the 'Local Config' interface with two main sections: 'LAN 1 Config', 'LAN 2 Config', and 'Access Control'. The 'LAN 1 Config' section has a blue header and contains fields for 'DHCP' (a toggle switch), 'Local IP' (a text input), and 'MAC' (a text input). The 'LAN 2 Config' section also has a blue header and contains fields for 'DHCP' (a toggle switch), 'Local IP' (a text input), and 'MAC' (a text input). The 'Access Control' section has a blue header and contains a 'Tamper Alarm Enable' checkbox, 'Time Of Lock1' and 'Time Of Lock2' (each with a numeric input and '+'/'-' buttons), and a 'Door Open Button Mode' dropdown menu. An 'Apply' button is at the bottom of the 'Access Control' section.

User Management

This allows you to change the default login details for this page.

Note: The password is the same as the Master/Engineer's code of the device.

UserName	Remarks	Operation
admin		Edit

Maintenance

Here we can see device information such as its software version, hardware version and the **Cloud UID** and **Cloud Outer Auth Code** which are used for adding the device to the management portal. We can also update the firmware or reboot the device from here.

Device Model:	Opyn Keypad
Software Version:	Apr 13 2026 10:00:51
Mcu1 Version:	401001011
Mcu2 Version:	512
Bluetooth Mac:	d4:39:82:c6:70:65
Hardware Version:	ver.c
Cloud Uid:	24079yeifhu4
Cloud Outer Auth Code:	BYLFYAKP
	Refresh

[Update](#)[Reboot Device](#)[Diagnosis](#)

[Backup Device](#)[Restore Device](#)[Cloud Unbind](#)

App Updates

We will continually monitor the app's performance and release updates to enhance the user's experience and/or fix any issues that arise over time. These updates will be available via the iOS App Store or the Google Play Store.

Firmware Updates

Firmware updates will be released to fix any bugs or to add additional features where possible throughout the product's lifetime. The firmware version your system is using can be seen via the app.

Warranty

Please note by installing this product, you are accepting our warranty terms. This warranty is a "return to base" 2-year manufacturer's warranty.

For full warranty terms and conditions contact the AES Technical Support Team.

Certifications

This product is designed in accordance with the EU General Data Protection Regulation (GDPR) and incorporates privacy-by-design principles.

CE-RED

Manufacturer: Advanced Electronic Solutions Global Ltd

Address: Unit 4C, Kilcronagh Business Park, Cookstown, Co Tyrone, BT809HJ, United Kingdom

Complies with the following essential requirements for:

EN 301 489-1 V2.2.0 (2017-03) (Electro-Magnetic Compliance)

EN 301 489-17 V3.2.0 (2017-03) (Electro-Magnetic Compliance)

EN 62479:2010 (Assessment of RF exposure / Maximum Output Power)

EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013 (Electrical Safety)

EN 18031 (Cybersecurity requirements for radio equipment – protection of network integrity, personal data and privacy, and prevention of fraud in accordance with Article 3(3) of the Radio Equipment Directive)



Notified body: Shenzhen HUAK Testing Technology Co., Ltd.

CNAS Number: L9589

This declaration is issued under the sole responsibility of the manufacturer.

Signed by:

Paul Creighton, Managing Director. Date: 18th October 2024

FCC

FCC ID: 2ALPX-OPYNKEYPAD

Grantee: Advanced Electronic Solutions Global Ltd.



This device complies with Part 15 of 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. Output power listed is conducted. This device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

RF Exposure Statement

To maintain compliance with FCC's RF Exposure guidelines, This equipment should be installed and operated with a minimum distance of 20cm from all persons. This device and its antenna(s) must not be co-located or operated in conjunction with any other antenna or transmitter.



sales@aesglobalonline.com
technical@aesglobalonline.com
TEL: +44 (0) 288 6390 693

www.aesglobalonline.com



sales@aesglobalus.com
technical@aesglobalus.com
TEL: +1 (321) 900 4599

www.aesglobalus.com



support@aesglobaltelecom.com
TEL UK-EU: +44 (0) 288 6390 693
TEL USA: +1 (321) 900 4599

www.aesglobaltelecom.com