VISIOTECH

AJAX SETUP STEP BY STEP

AJAX

1. DOWNLOAD SMARTHPONE APP AND PC SOFTWARE

Ajax has two apps for smartphones (Android and iOS)

Ajax Security System → End-users

Ajax PRO: Tool for Engineers → Installer and security professionals

Ajax Security System: Download iOS (From iOS 13.0)

Ajax PRO: Tool For Engineers: Download iOS (From iOS 13.0)

Ajax Security System: Download Android (From Android 5.0)

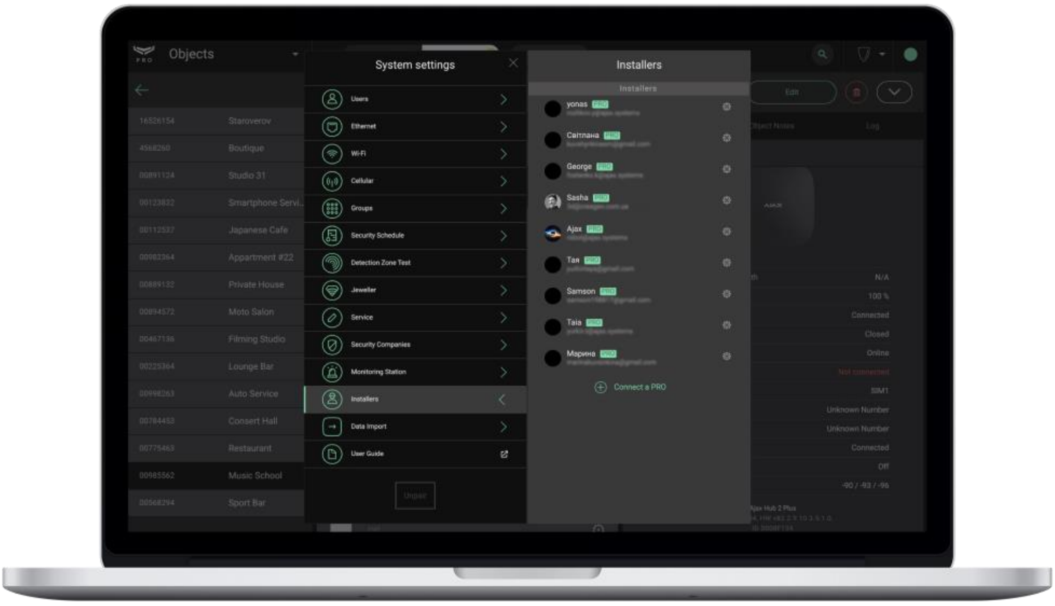
Ajax PRO: Tool For Engineers: Download Android (From Android 5.0)

There is also a desktop version, PRO Desktop, to manage directly from a PC. It is designed for administration and monitoring of the alarms of the Ajax security system

Download Windows

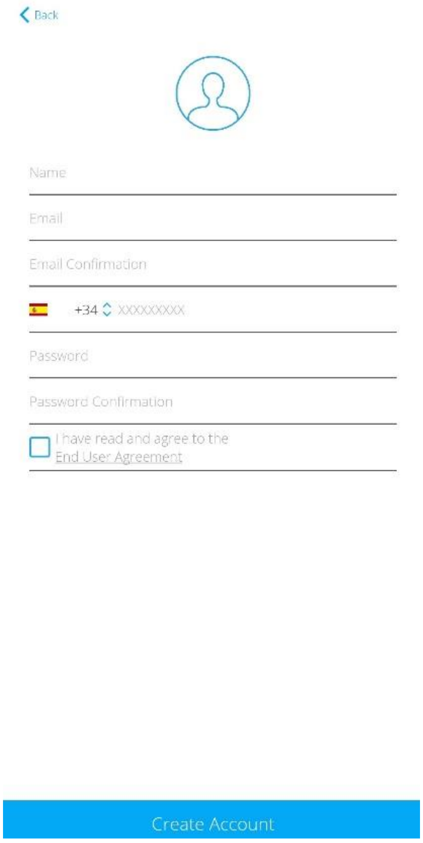
Download macOS

User Manual



2. CREATE ACCOUNT

To create an account, it is necessary to fill in all the fields in the image below.



< Back

Name

Email

Email Confirmation

+34 XXXXXXXXX

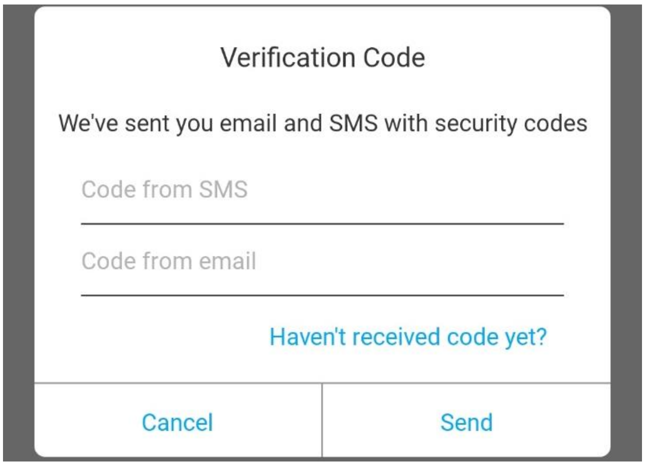
Password

Password Confirmation

□ I have read and agree to the End User Agreement

Create Account

Once an account is created, a confirmation code by SMS and another by e-mail. Write both codes in the following screen to validate your account.



Verification Code

We've sent you email and SMS with security codes

Code from SMS

Code from email

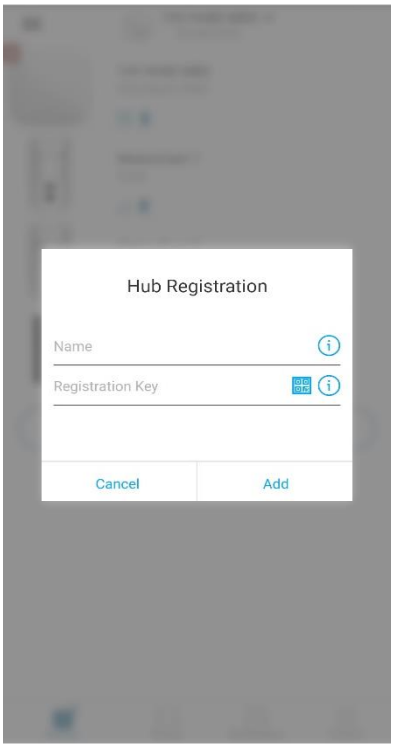
Haven't received code yet?

Cancel Send

3. ADD HUB

Ajax has a configuration assistant step-by-step. It is also possible to carry out this task manually.

Fill in the following fields. You can scan the QR code or introduce the identification number.



Hub Registration

Name

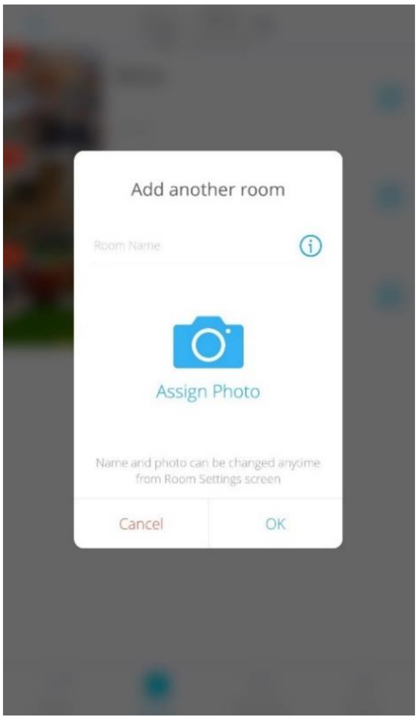
Registration Key

4. ADD ROOM

Assign name and photo.

The rooms are used to categorize the devices and to localize them within the installation. In this way, through the notifications, we know where events are taking place.

Moreover, it is possible to see the average temperature thanks to the Ajax temperature sensors found in some of the devices.

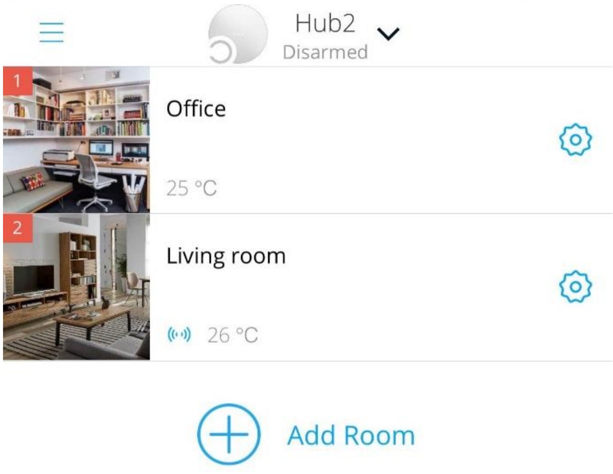


Add another room

Room Name

Assign Photo

Name and photo can be changed anytime from Room Settings screen

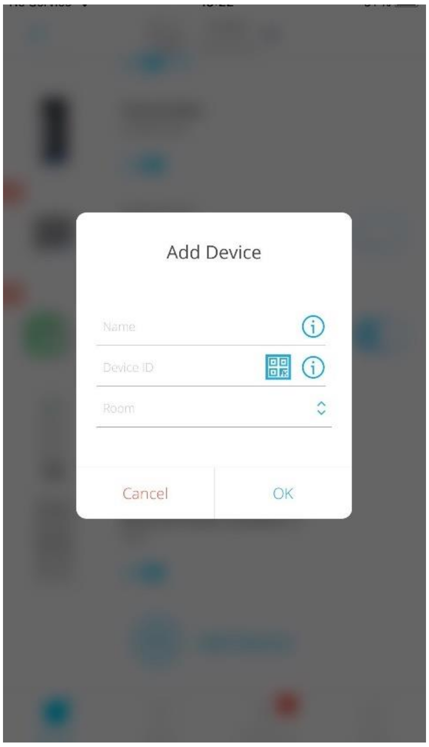


Hub2
Disarmed

1	Office	25 °C
2	Living room	26 °C

5. ADD DEVICES

To add devices, it is necessary to introduce a name, scan the QR code of the device and localize it in a room. If the device is turned on, it is necessary to restart it for adding it. In case the device is turned off, then turn it on.



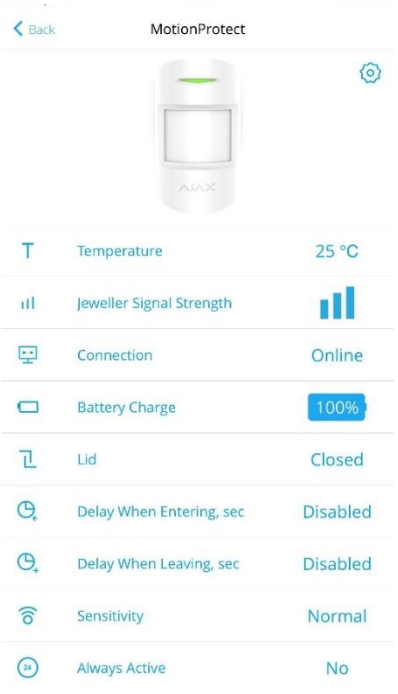
Add Device

Name

Device ID

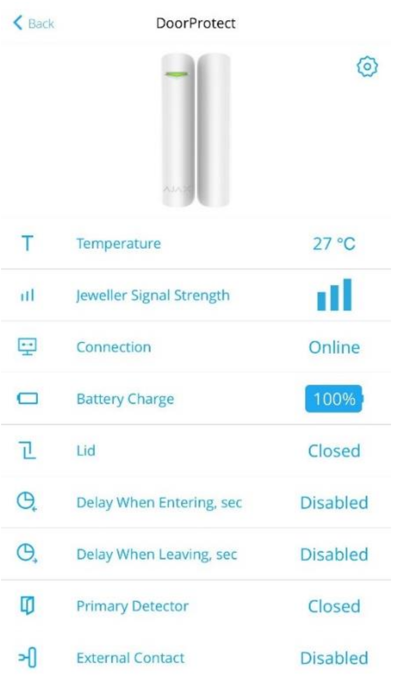
Room

Moreover, you can have a quick overview of different indicators of the device.



MotionProtect

Temperature	25 °C
Jeweller Signal Strength	▮▮▮
Connection	Online
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	Disabled
Delay When Leaving, sec	Disabled
Sensitivity	Normal
Always Active	No

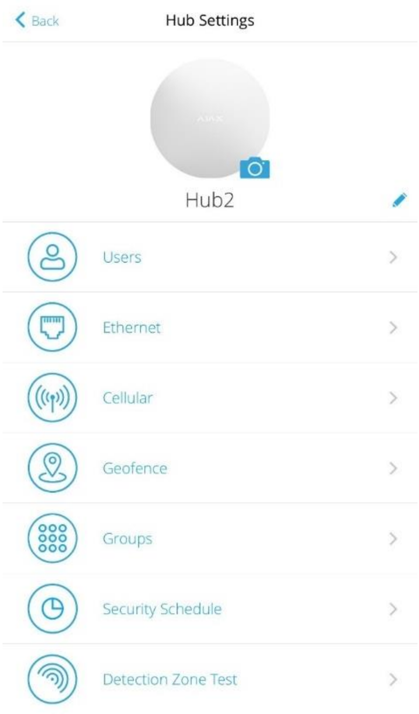


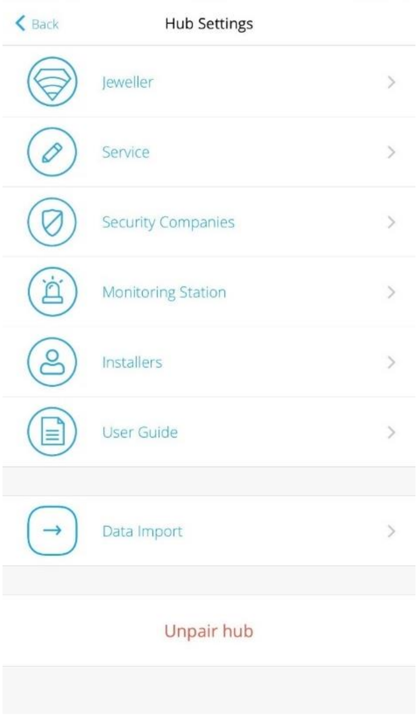
DoorProtect

Temperature	27 °C
Jeweller Signal Strength	▮▮▮
Connection	Online
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	Disabled
Delay When Leaving, sec	Disabled
Primary Detector	Closed
External Contact	Disabled

6. HUB CONFIGURATION

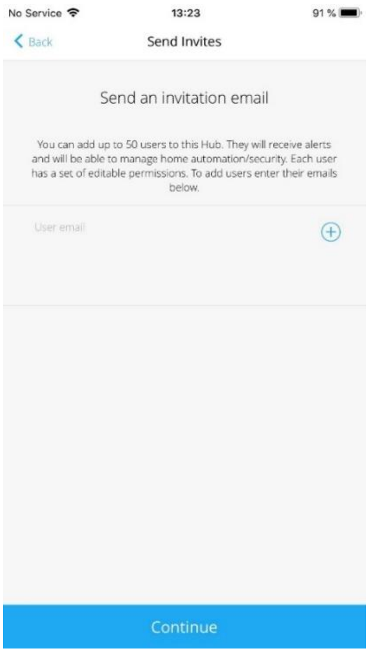
In the following step we show how to configure the HUB with the following parameters:





6.1. USERS

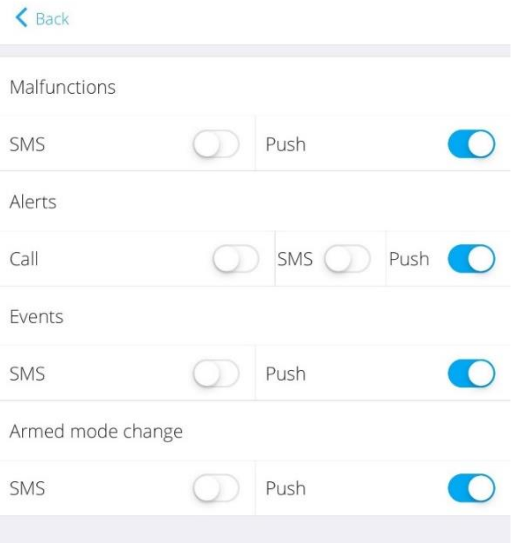
In this option you can add users allowed by the Hub that are registered in the app Ajax security System.



Send an invitation email

You can add up to 50 users to this Hub. They will receive alerts and will be able to manage home automation/security. Each user has a set of editable permissions. To add users enter their emails below.

También se puede configurar las notificaciones para que, dependiendo de la incidencia, se reciba de la manera que cada usuario elija.



Malfunctions

SMS ○ Push ●

Alerts

Call ○ SMS ○ Push ●

Events

SMS ○ Push ●

Armed mode change

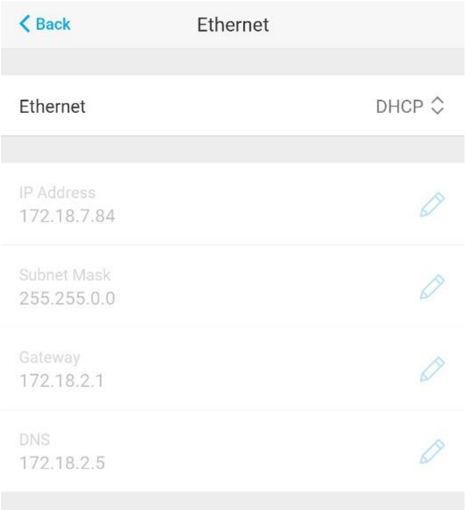
SMS ○ Push ●

As shown in the previous image, it is possible to allow an option for receiving calls in the case alarm to all users. These calls are carried out if the Hub has a SIM-card with sufficient balance.

6.2. ETHERNET

When it comes to the Ethernet configuration, it is possible to deactivate it in case it should communicate through GPRS.

It is possible to configure DHCP or static IP. Fill in the fields in the following image if choosing static IP.



< Back Ethernet

Ethernet: DHCP

IP Address: 172.18.7.84

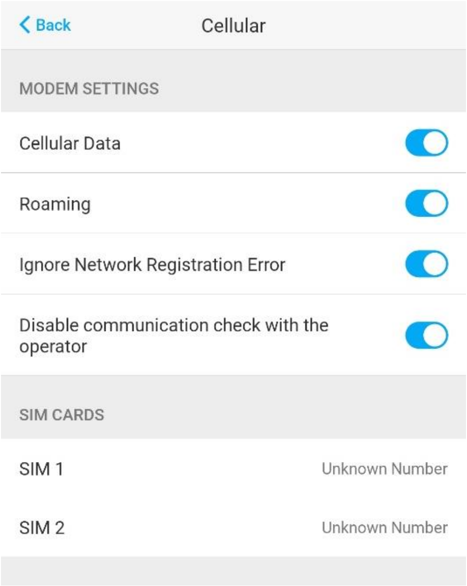
Subnet Mask: 255.255.0.0

Gateway: 172.18.2.1

DNS: 172.18.2.5

6.3. MOBILE NETWORK

For GPRS communication it is possible to activate or deactivate this type of connection. Moreover, it is necessary to introduce the APN from the operator of the SIM card.



< Back Cellular

MODEM SETTINGS

Cellular Data: on

Roaming: on

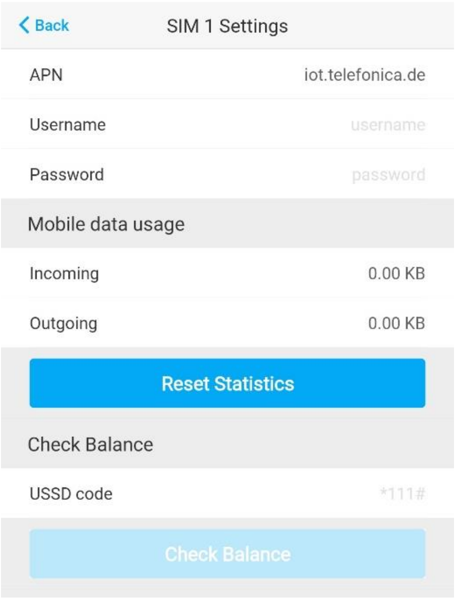
Ignore Network Registration Error: on

Disable communication check with the operator: on

SIM CARDS

SIM 1: Unknown Number

SIM 2: Unknown Number



< Back SIM 1 Settings

APN: iot.telefonica.de

Username: username

Password: password

Mobile data usage

Incoming: 0.00 KB

Outgoing: 0.00 KB

Reset Statistics

Check Balance

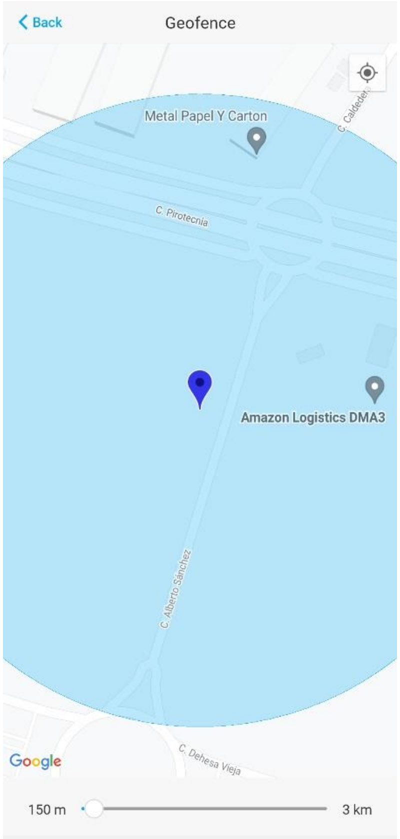
USSD code: *111#

Check Balance

6.4. GEOFENCE

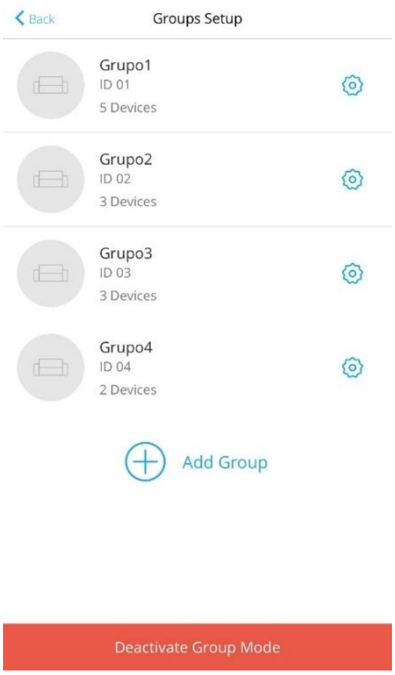
Geofence is a tool using geolocation from a smartphone, establishing a radius (configurable between 100m and 3000m) from a selected point. From this point a reminder is sent to arm for leaving the area or disarm when getting closer.

This tool as well as the reminders could be deactivated.



6.5. GROUPS

More than just creating rooms, you can also create groups. The difference is that groups allows you to arm/disarm the group(s) of your choice.



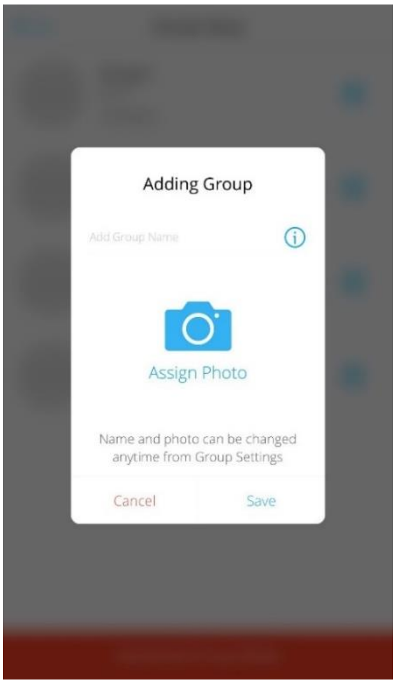
Groups Setup

Grupo1
ID 01
5 Devices

Grupo2
ID 02
3 Devices

Grupo3
ID 03
3 Devices

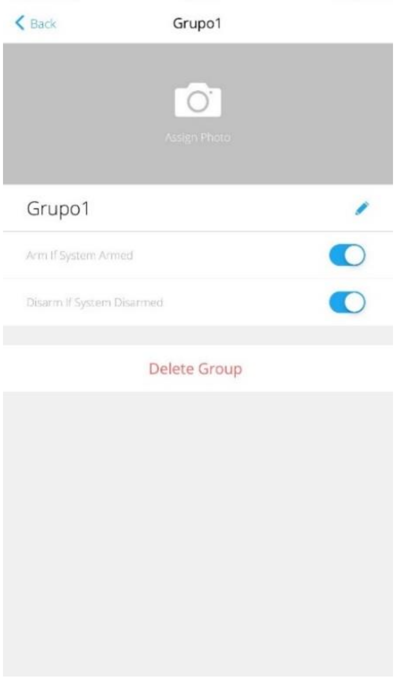
Grupo4
ID 04
2 Devices



Adding Group

Add Group Name

Name and photo can be changed anytime from Group Settings



Grupo1

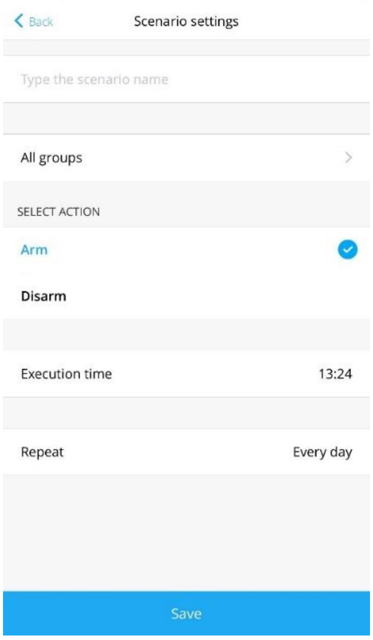
Grupo1

Arm If System Armed

Disarm If System Disarmed

6.6. SCENARIO SETTINGS

With this option, you can automatically set the arm/disarm process selecting groups or the complete Hub, choosing the time and days.



Scenario settings

Type the scenario name

All groups

SELECT ACTION

Arm ✓

Disarm

Execution time 13:24

Repeat Every day

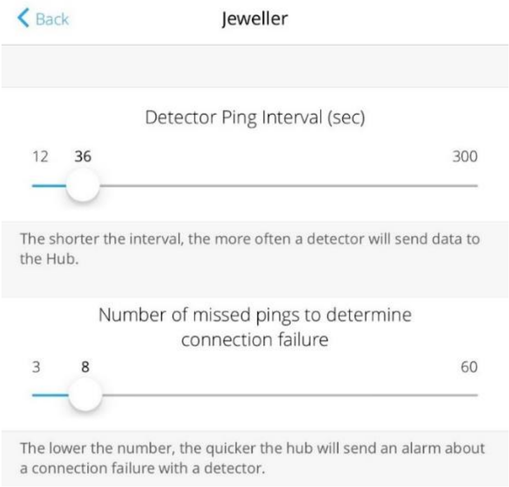
6.7. DETECTION TEST ZONE

This test consists of determining the operational distance of each device individually. It is recommended to generate alarms in each detector to verify their functionality. During the test it lights up continuously and turns of during the alarm.

6.8. JEWELLER

In this part, the communication between devices and the Hub is monitored. The different patameters are:

- . Ping Interval, which is the time of sending data from a detector to a Hub
- Number of missed pings to determine connection failure. When this number is reached, an alarm indicating a connection failure is sent.



Detector Ping Interval (sec)

The shorter the interval, the more often a detector will send data to the Hub.

Number of missed pings to determine connection failure

The lower the number, the quicker the hub will send an alarm about a connection failure with a detector.

For example, with the following values:

36 seconds of ping interval * 8 pings missed = 5 minutes

The possible connection failure is detected in 5 minutes.

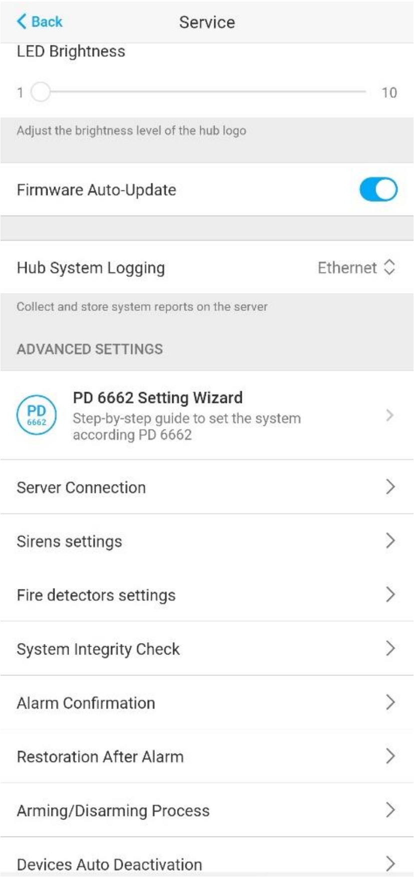
6.9. SERVICE

Here, various options are configured

- LED light
- Firmware update
  - Connection settings with the server: it is posible to configure the monitoring time for the communication between the Hub and Ajax cloud, through these parameters:
  - Delay in the server connection failure alarm.
  - Ping Interval between server and hub: it is the time established for the hub to notify a conection error with the server. tervalo de ping entre servidor y el hub: es el intervalo de tiempo que se establece para que el hub notique su fallo de conexión con el servidor.

(Ping Interval * 3) + Delay

Moreover, it is possible to customize notifications of lost connection for a specific channel. For example, if the Hub is connected through various channels and one channel is lost, a notification is sent with a configurable delay between 3 and 30 minutes. If all connection channels are lost, the shortest communication delay is chosen. (Between the alarm failure Interval and the Hub-Sever polling interval)



Back Service

LED Brightness

1 10

Adjust the brightness level of the hub logo

Firmware Auto-Update

Hub System Logging Ethernet

Collect and store system reports on the server

ADVANCED SETTINGS

PD 6662 Setting Wizard
Step-by-step guide to set the system according PD 6662

Server Connection

Sirens settings

Fire detectors settings

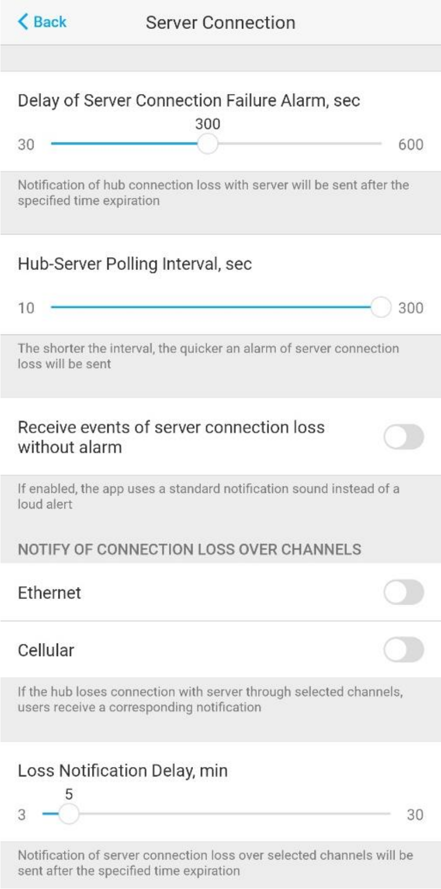
System Integrity Check

Alarm Confirmation

Restoration After Alarm

Arming/Disarming Process

Devices Auto Deactivation



Back Server Connection

Delay of Server Connection Failure Alarm, sec

300

30 600

Notification of hub connection loss with server will be sent after the specified time expiration

Hub-Server Polling Interval, sec

10 300

The shorter the interval, the quicker an alarm of server connection loss will be sent

Receive events of server connection loss without alarm

If enabled, the app uses a standard notification sound instead of a loud alert

NOTIFY OF CONNECTION LOSS OVER CHANNELS

Ethernet

Cellular

If the hub loses connection with server through selected channels, users receive a corresponding notification

Loss Notification Delay, min

5

3 30

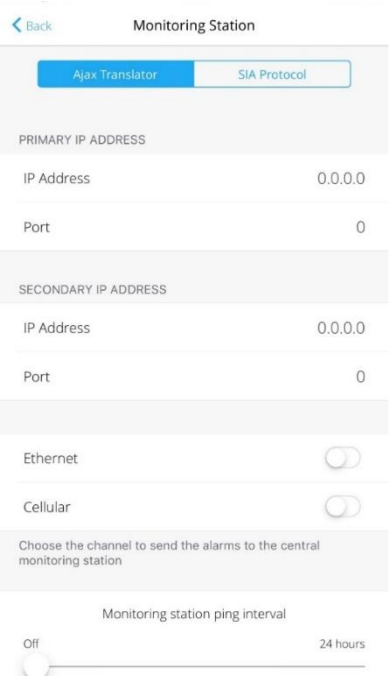
Notification of server connection loss over selected channels will be sent after the specified time expiration

- Siren configuration: you can select which action will activate the siren or which events it will indicate with double flashes.
- Fire detector settings: the connection between fire detectors can be configured to activate when at least one of them is triggered or that the first smoke detection alarm should be ignored during the first 30 seconds.
- System integrity check: you configure the different states of the hub that are included in the integrity check and activate or deactivate the permission to arm on failure of the system.
- Alarm settings: you can configure the robbery alarm settings when a button or two different buttons are pressed twice.

6.10. MONITORING STATION

Configuration to directly communicate the Hub with the Alarm Receiving Center (ARC). This configuration will be carried out after adding the Hub to the ARC (section 6.12 Security companies)

Set the IP address and port of the PC where Ajax Translator is located. These parameters must be provided by the Alarm Receiving Center.



PRIMARY IP ADDRESS

IP Address 0.0.0.0

Port 0

SECONDARY IP ADDRESS

IP Address 0.0.0.0

Port 0

Ethernet ○

Cellular ○

Choose the channel to send the alarms to the central monitoring station

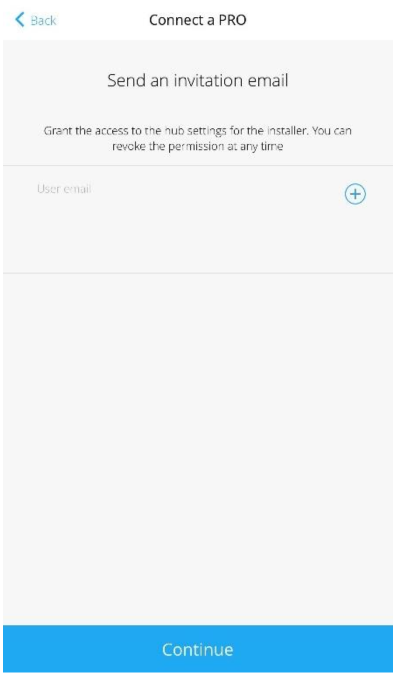
Monitoring station ping interval

Off 24 hours

6.11. PRO / INSTALLERS

In this section, an invitation code can be sent to the installer so that he has access to the alarm system and can make settings or manage the alarms. The available permissions that can be given to the installer are night mode activation, panic button activation, access to cameras and automation controls. You can also manage which groups you have access to.

The users invited from this section are those created in the Ajax PRO App: Tool for Engineers or in the Ajax PRO Desktop software.



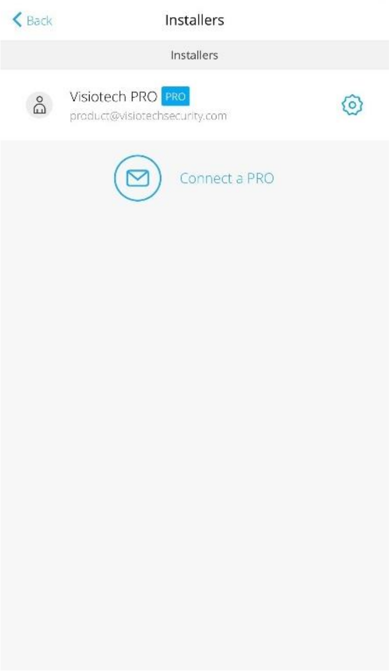
< Back Connect a PRO

Send an invitation email

Grant the access to the hub settings for the installer. You can revoke the permission at any time

User email

Continue

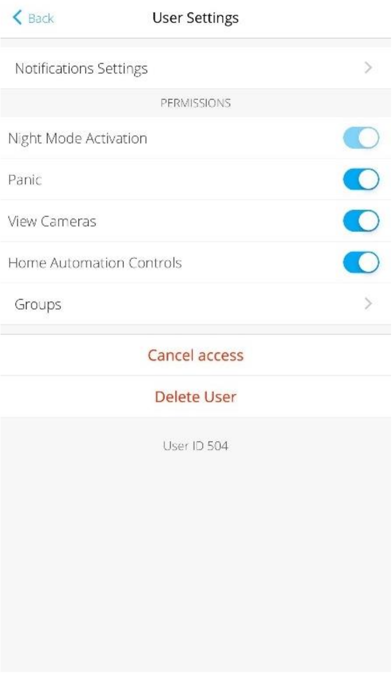


< Back Installers

Installers

Visiotech PRO PRO
product@visiotechsecurity.com

Connect a PRO



< Back User Settings

Notifications Settings

PERMISSIONS

Night Mode Activation

Panic

View Cameras

Home Automation Controls

Groups

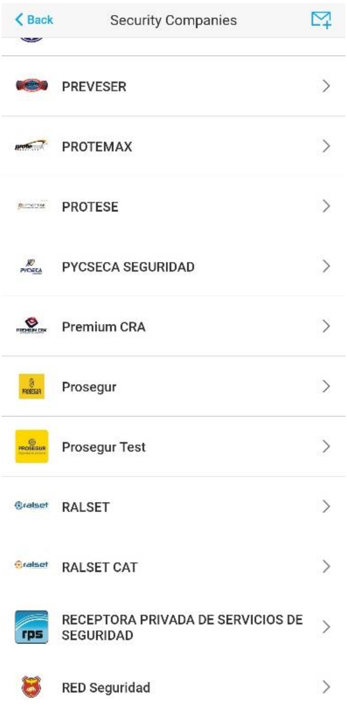
Cancel access

Delete User

User ID 504

6.12. SECURITY COMPANIES

In this section there is a list of Alarm Receiving Centers (ARC) to request adding the Hub panel to the ARC. Once the ARC has been selected, click on 'Apply'.



< Back Security Companies

PREVESER

PROTEMAX

PROTESE

PYCSECA SEGURIDAD

Premium CRA

Prosegur

Prosegur Test

RALSET

RALSET CAT

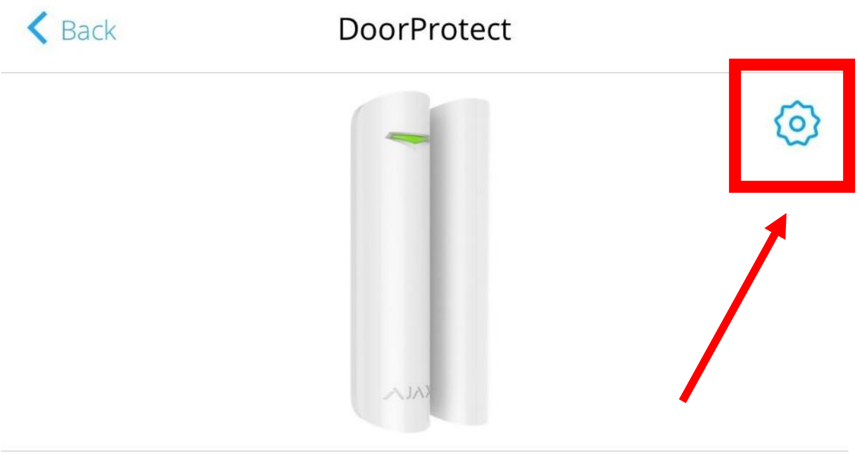
RECEPTORA PRIVADA DE SERVICIOS DE SEGURIDAD

RED Seguridad

7. CONFIGURATION OF DEVICES

To access the configuration of the devices it is necessary that the alarm system is disarmed. This menu is located in the devices tab:

The configuration of each product is located at the top of it, in the icon ⚙ as can be seen in the following image.

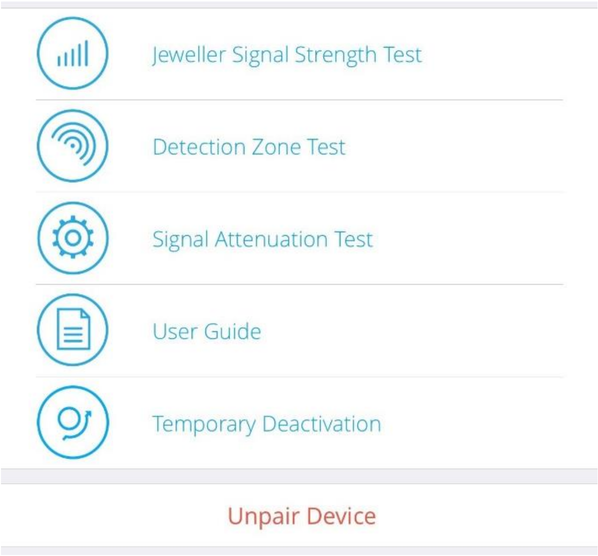


For all AJAX devices it is possible to carry out a signal intensity test (via Jeweler radio) and a signal attenuation test from its configuration.

All detectors (movement, magnetic, glass breakage) offer the possibility of carrying out a test of the detection zone.

In addition, there is a quick user guide in each of them.

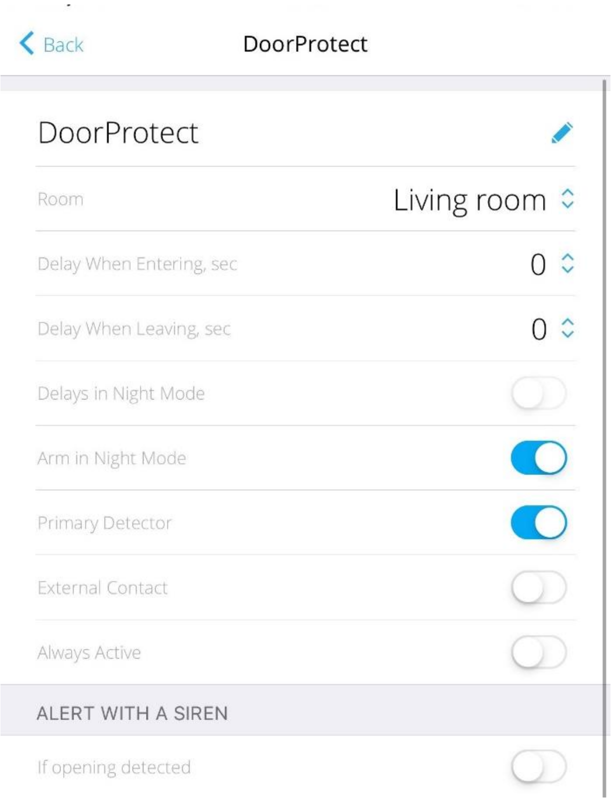
The option to unpair the device from the HUB is located at the end of the configuration.



Some examples of different device configurations are below:

AJ-DOORPROTECT-B

AJ-DOORPROTECT-W



< Back DoorProtect

DoorProtect

Room: Living room

Delay When Entering, sec: 0

Delay When Leaving, sec: 0

Delays in Night Mode ○

Arm in Night Mode ●

Primary Detector ●

External Contact ○

Always Active ○

ALERT WITH A SIREN

If opening detected ○

-Name

- room

select.

- Delay when entering

0-120 sec

- Delay when leaving

0-120 sec

-Always active

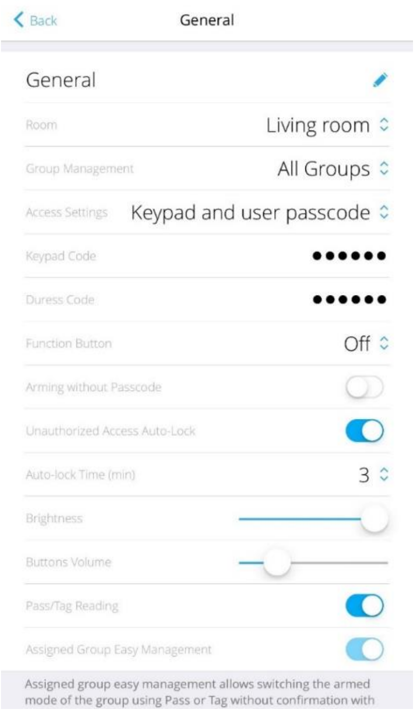
24h mode

- Alert with a siren

Select if you want the system sirens to sound with the detection of the detector that is being configured.

AJ-KEYPADPLUS-W

AJ-KEYPADPLUS-B



General

Room	Living room
Group Management	All Groups
Access Settings	Keypad and user passcode
Keypad Code	••••••
Duress Code	••••••
Function Button	Off
Arming without Passcode	○
Unauthorized Access Auto-Lock	●
Auto-lock Time (min)	3
Brightness	
Buttons Volume	
Pass/Tag Reading	●
Assigned Group Easy Management	●

Assigned group easy management allows switching the armed mode of the group using Pass or Tag without confirmation with

- Access settings

Keypad code only (general), user code only (unique for each user on the system), or both.

-Keypad code

Disarm Password

- Duress code

Disarm code under duress. ARC will be notified of disarming under duress.

- Function button:

Assign action to button (*): emergency, silence siren of smoke detectors or no function**.**

- Arm without passcode

- Unauthorized Access Auto-Lock

After three attempts, the keypad is locked until the configured time has elapsed or from the unlock app.

- Autolock Time (min)

Time that must elapse before being able to use the keypad after 3 incorrect password attempts.

-Brightness

-Buttons Volume

- Tag/Pass reading

- Alert with siren

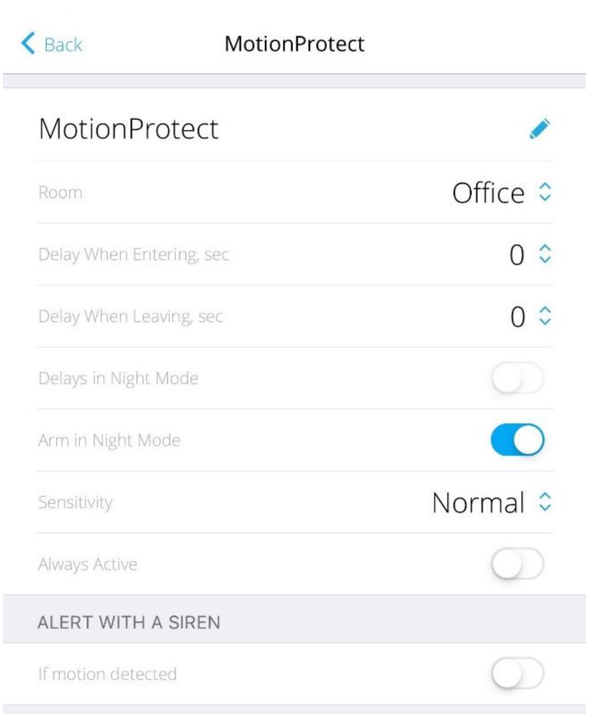
Enable/disable siren when pressing panic button.

AJ-MOTIONRPOTECT-B

AJ-MOTIONRPOTECT-W

- **Delay when entering**
0-120 sec
- **Delay when leaving**
0-120 sec
- **Delay in night mode**

-**Sensitivity**
High, normal and low



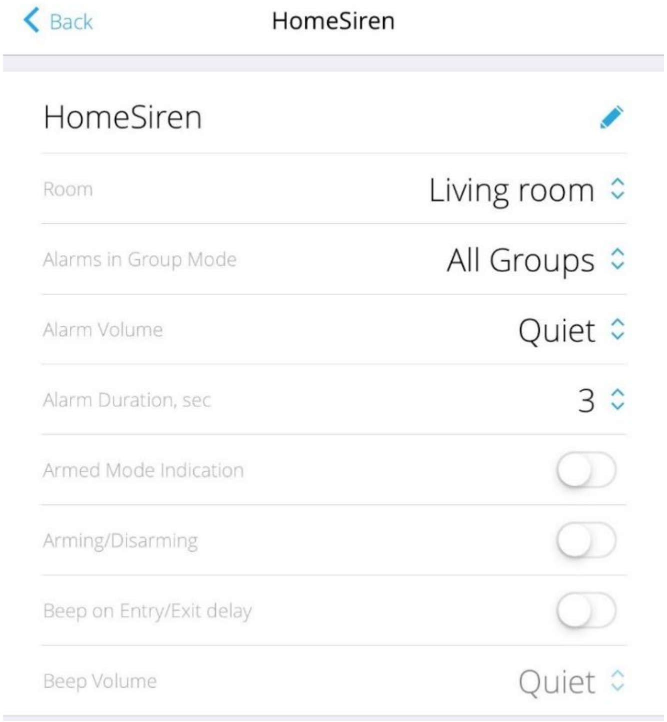
< Back MotionProtect

MotionProtect ✎

Room	Office ⇕
Delay When Entering, sec	0 ⇕
Delay When Leaving, sec	0 ⇕
Delays in Night Mode	○
Arm in Night Mode	●
Sensitivity	Normal ⇕
Always Active	○

ALERT WITH A SIREN

If motion detected	○



< Back HomeSiren

HomeSiren ✎

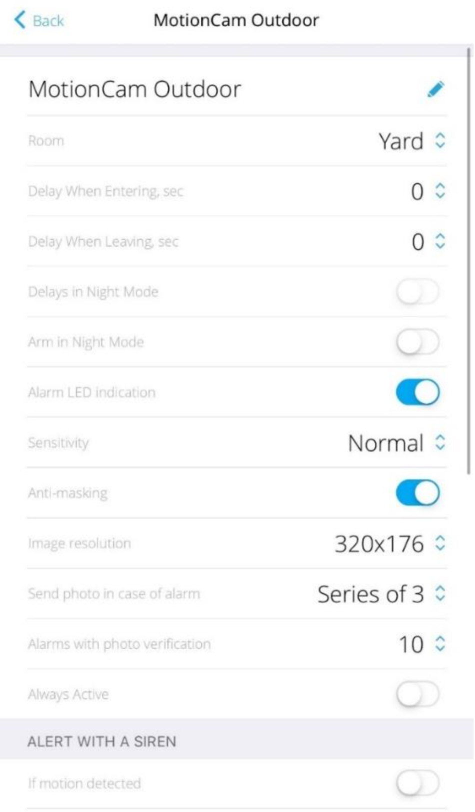
Room	Living room ⇕
Alarms in Group Mode	All Groups ⇕
Alarm Volume	Quiet ⇕
Alarm Duration, sec	3 ⇕
Armed Mode Indication	○
Arming/Disarming	○
Beep on Entry/Exit delay	○
Beep Volume	Quiet ⇕

AJ-HOMESIREN-W

AJ-HOMESIREN-B

- **Alarm duration**
3-180 sec
- **Alarm volume**
- **Armed mode indication**
- **Arming/Disarming**
- **Beep on entering/exiting delay**
- **Beep volume**

AJ-MOTIONCAMOUTDOOR-W



< Back MotionCam Outdoor

MotionCam Outdoor

Room	Yard ⇕
Delay When Entering, sec	0 ⇕
Delay When Leaving, sec	0 ⇕
Delays in Night Mode	○
Arm in Night Mode	○
Alarm LED indication	●
Sensitivity	Normal ⇕
Anti-masking	●
Image resolution	320x176 ⇕
Send photo in case of alarm	Series of 3 ⇕
Alarms with photo verification	10 ⇕
Always Active	○

ALERT WITH A SIREN

If motion detected	○

- Delay when entering

0-120 sec

- Delay when exiting

0-120 sec

- Delay in night mode

- Arm in night mode

-Sensitivity

high, normal and low

- Anti-masking sensor

- Image resolution

640x352 or 320x176

- Number of photos per alarm

0-5

- Alarms with photo verification

Number of detections included in the images. 1-10 or all

-Always active