

OTS® Pulse



USER MANUAL

V1.1



ojmar®

INTELLIGENT LOCKING SYSTEMS

This document is for information only and is not contractually binding. The information may have undergone changes that have not yet been incorporated in the present document and we therefore suggest that if in doubt you please contact Ojmar to obtain updated information.

© Ojmar, S.A.

0. GENERAL DESCRIPTION.....	5
0.1. GENERAL DESCRIPTION	5
0.2. SYMBOLS USED IN THE USER MANUAL.....	5
0.3. GENERAL WARNINGS	5
0.4. REGULATORY INFORMATION USA	6
0.5. CLASS B DEVICE NOTICE.....	6
0.6. RF EXPOSURE SAFETY	6
0.7. TECHNICAL SUPPORT	7
1. OTS PULSE LOCKS.....	8
1.1. GENERAL DESCRIPTION	8
1.2. MEASUREMENTS AND FEATURES.....	8
1.2.1. TECHNICAL DRAWINGS.....	8
1.3. OPENING AND CLOSING	10
1.3.1. RFID OPERATION	10
1.3.2. SMARTPHONE OPERATION	10
1.4. LOCK TYPES	10
1.4.1. DEDICATED LOCK	10
1.4.2. FREE LOCK.....	11
1.4.3. RENTAL LOCK.....	11
2. GATEWAY	11
3. PROGRAMMER	12
4. INFOTERMINAL	13
5. SOFTWARE	14
5.1. SOFTWARE FEATURES	15
6. SYSTEM MANAGEMENT.....	16
6.1. SYSTEM ARCHITECTURE	16
6.2. SYSTEM SET-UP	17
6.2.1. LOG IN THE SOFTWARE	18
6.2.2. CHECK GATEWAYS CONNECTION.....	18
6.2.3. LOCKS CREATION	19
6.2.4. LOCK SET-UP	19
6.2.5. CHECK ONLINE COMMUNICATION.....	20
6.3. SYSTEM USAGE.....	21
6.3.1. REGISTER PERMISSIONS FOR THE FIRST TIME	21
6.3.2. REGISTER PERMISSIONS FOR THE FIRST TIME	22

6.3.3. MOBILE DEVICE CREDENTIALS – PHONES/TABLETS ETC	22
7. MAINTENANCE AND FAQS	23
7.1. DASHBOARD	23
7.2. BATTERIES REPLACEMENT	23
7.3. LED INDICATIONS OF OTS PULSE LOCKS	24
7.4. FAQS.....	25
	26

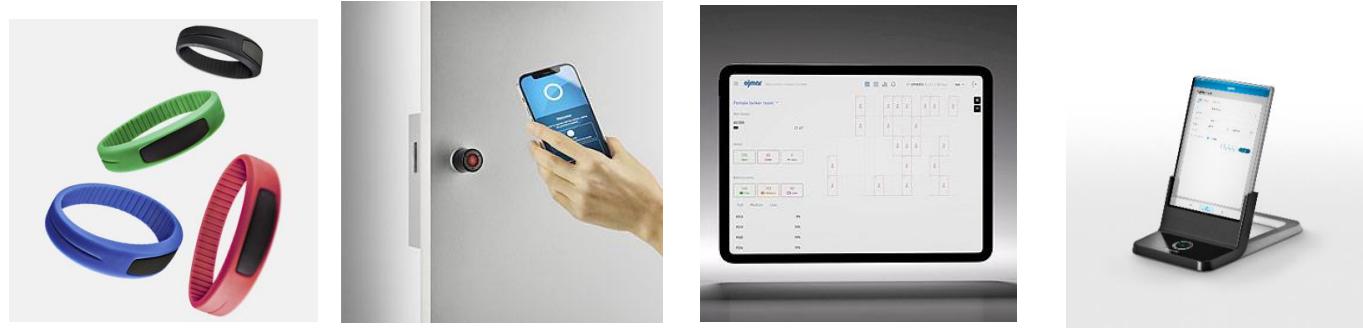
0. GENERAL DESCRIPTION

0.1. GENERAL DESCRIPTION

The OTS pulse is an online, wireless locking system. The locks can be operated using RFID credentials (wristbands, cards etc.) or using BLE-enabled tablets or phones (Android or IOS). Locks can be managed remotely anywhere in the world via internet.

The OTS Pulse system consists of the following key components:

1. **OTS Pulse lock:** An online lock that can be operated by RFID or BLE. The lock communicates wireless with the Gateway to operate.
2. **Gateway:** Proprietary device that communicates with the locks Wireless and with the Ojmar Cloud software via Ethernet. The Gateway stores the permissions and allows the lock to operate or not depending on the aforementioned permissions
3. **Programmer:** Device that is used to register the user cards for the first time and create the set-up card for the locks.
4. **Infoterminal (Optional):** Device that gives information of the user card (Locks that is occupying, permissions, etc.)
5. **User App (Optional):** Android and iOS App that can operate with the locks and rent a locker.
6. **Ojmar Cloud Software:** Cloud based software that monitors the facility in real time. Ojmar cloud can also reconfigure the locks and permissions and gives advanced stats of the locks.



0.2. SYMBOLS USED IN THE USER MANUAL

- NOTE: The notes are used to highlight information that is of particular importance or related interest that must be remembered.
- EXAMPLE: The examples are used to show a case study that may provide users with a better understanding of the explanation.
- WARNING: The warning boxes highlight the importance of the information described.

0.3. GENERAL WARNINGS

Please follow the rules below to ensure the correct working order of our product in your facility:

- WARNING: The product purchased must be installed and used according to the technical operating conditions described in the corresponding manual.
- WARNING: Where not specifically indicated, customers are responsible for the appropriate installation or use of the application.

- **WARNING:** On receiving the material, please inspect the packaging and the material for any signs of damage. Also check that the shipment is complete (accessories, documents, etc.).
- **WARNING:** If the packaging has been damaged during transport or you suspect that it may have been damaged or that it could be faulty, the material must not be used. Please contact us in this case.
- **WARNING:** Our products must be installed and handled by authorised personnel. More specifically, the electrical connections must be made by qualified specialists.
- **WARNING:** It is forbidden to make any replacements or remove the protective covers.
- **WARNING:** Do not attempt to repair any material in the event of a fault or damage and then re-start it. You must contact us in these cases.
- **WARNING:** No responsibility will be accepted for damage caused as a result of misuse.
- **WARNING:** In accordance with Royal Decree 106/2008, dated 1 February 2016, before leaving the devices in their pick-up installations, the batteries must be removed and left separately for their appropriate handling.



0.4. REGULATORY INFORMATION USA

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

0.5. CLASS B DEVICE NOTICE

- Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

0.6. RF EXPOSURE SAFETY

This product is a radio transmitter and receiver. The antenna must be installed and operated with a minimum distance of 20 cm between the radiator and your body.

It is designed not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

0.7. TECHNICAL SUPPORT

Should you wish to make any enquiries on our products, please contact the Ojmar technical department:

- Telephone: +34 943 748 484
- Fax: +34 943 748 490
- Website: www.ojmar.com

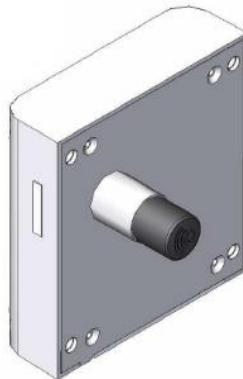
1. OTS PULSE LOCKS

1.1. GENERAL DESCRIPTION

OTS Pulse is an online real-time wireless electronic locking system with RFID and BLE technology.

The lock is fully controlled via wireless from Ojmar's cloud software, allowing to reconfigure and assign permissions remotely. The lock will ask for permission to the gateway and will operate once the answer is received.

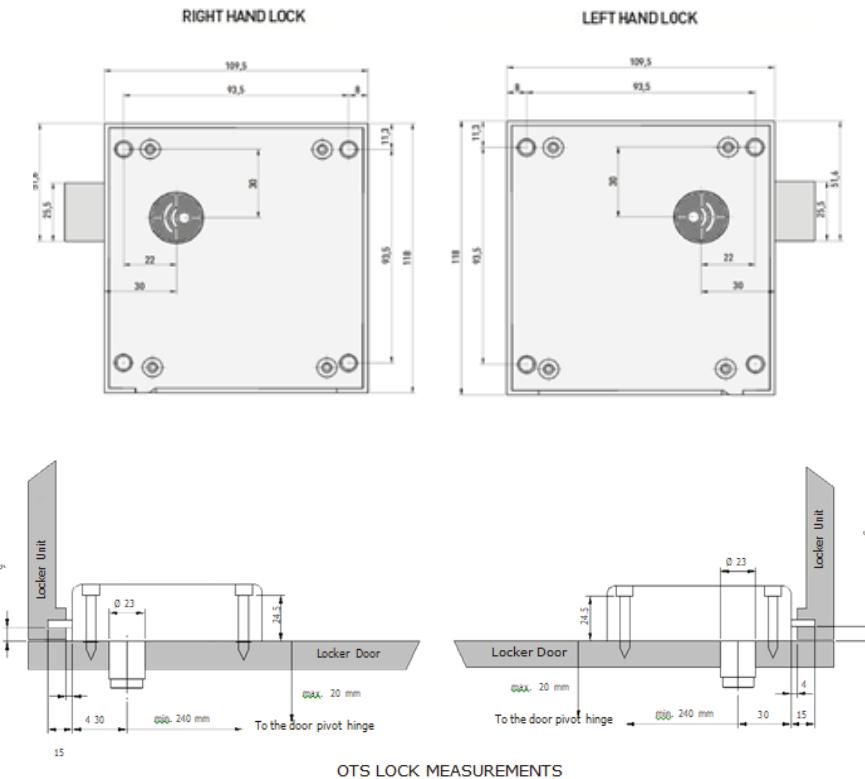
An offline mode is available in case network gets down, allowing operation in standalone mode and storing all the information, sending that information back to the cloud software once communication is reestablished.

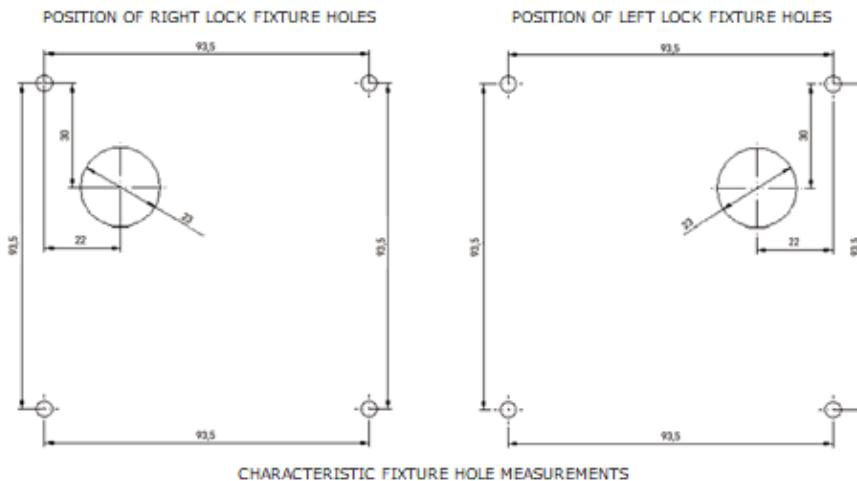


1.2. MEASUREMENTS AND FEATURES

The OTS proximity lock includes a fully autonomous power supply system and therefore does not require any type of wiring. Powered by 4 standard AA alkaline batteries, it has an approximate autonomy of 8 years.

1.2.1. TECHNICAL DRAWINGS





Technical Specifications

TECHNOLOGIES	Authentication mode	RFID, Bluetooth
	RFID standards	MIFARE® (DESFire EV1 & EV2, Ultralight, Ultralight C, Classic1K/4K 4B and 7B UID – ISO/IEC 14443), ISO 15693 (Incluye HID® Seos and HID® iClass)
	Reading	UID / Sector
	Wearables	RFID cards, wristbands, FOBs, Technogym key, Stickers & Transponders
	Bluetooth OS	Android & iOS
USAGE MODES	Free mode	Up to 3 locks simultaneously with just one wearable
	Dedicated mode	Up to 6 locks simultaneously with just one wearable
	Multifunction mode	Up to 3 free and 3 dedicated locks simultaneously with just one wearable
	Rental mode	Configurable in periods of 15 minutes
	Notifications	LED (Red, amber & green)
USER INTERFACES	Lock closed notifications	Nozzle in closed position Red LED blinking every 2 seconds (configurable) In Software and infoterminale in RT
	Alarms	Low battery warning High occupancy alert
COMMUNICATION INTERFACES	Communication standard	Wireless 2.4GHz proprietary stack
	Encryption mode	AES 256
	Reading field range (wireless)	Up to 50 m (depending on the layout)
POWER SUPPLY	Batteries (Type & quantity)	4 alkaline batteries VARTA Type AA
	Battery life	Up to 8 years at room temperature (Depending on usage and configuration)
MECHANICAL CHARACTERISTICS	Dimensions	119.5 mm x 35 mm x 118 mm
	Weight	375 gr
	Knob resistance	1000 N
	Housing	Black nozzle Black and green nozzle White nozzle

OTS PULSE v1.0

ENVIRONMENTAL CONDITIONS	Temperature	From -10°C to 42°C (interiors)
	Humidity	< 97% (Condensation free)
	Protection type	IK09 / IP55

1.3. OPENING AND CLOSING

The lock opening and closing process is as follows:

1.3.1. RFID OPERATION

OTS®PULSE

CLOSE



1. Place items in locker



2. Push the knob with your card or wristband



3. Locker locked



OPEN



1. Push the knob with your card or wristband



2. Locker opened



3. Remove items



INTELLIGENT LOCKING SYSTEMS

ojmar.com ojmar.us

1.3.2. SMARTPHONE OPERATION

Closing operation: Present phone to lock and press lock button on app whilst pressing lock nozzle.

Opening operation: Present phone to lock and press unlock button in app. Nozzle will open automatically.

1.4. LOCK TYPES

OTS locks can be configured in three different ways:

- Free.
- Dedicated.
- Rental.

These locks are set the first time with a set-up card.

- NOTE: Once the locks have been programmed they can be reconfigured via cloud using Ojmar's software

1.4.1. DEDICATED LOCK

The Dedicated lock mode allows for a certain member number to be assigned to a specific lock.

- EXAMPLE: A lock is reserved for a gym member and only he/she may use it.

Only the dedicated keys associated to the lock will have access to it.

As many keys as required can be created for each dedicated lock and they may all have access at the same time.

- EXAMPLE: A member with two dedicated keys may close a lock with one key and open the same lock with the other key.

1.4.2. FREE MODE LOCK

The "Free" operating mode allows for access to the lock by any programmed key of this type. It works as follows:

- A free key allows for any free lock that is not in use at the time to be opened and closed.
- As soon as the lock is in use, the key cannot be used in any other free lock until the first one has been freed.

1.4.3. RENTAL MODE LOCK

The "rental" operating mode allows members to rent a lock on the desired day and for the desired length of time.

The user will only be able to operate with the lock, only if he is using it, during the rental period.

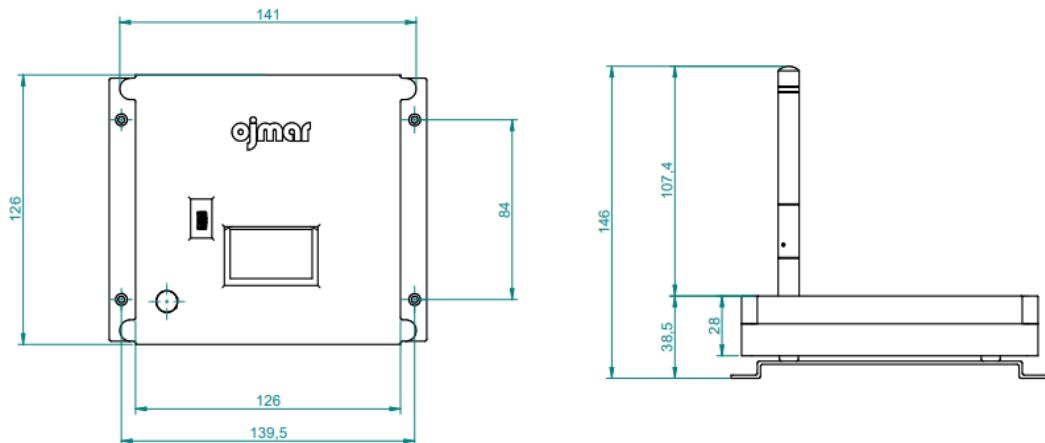
2. GATEWAY

The Gateway is a key device that communicates wirelessly with the locks and via ethernet with the Ojmar Cloud SW.

The device stores the configuration of the locks and user permissions and takes the decision whether the lock should operate or not. If the network goes down, the Gateway will continue working. The set consists of:

- Gateway.
- One Ethernet cable.
- PoE Injector available upon request.

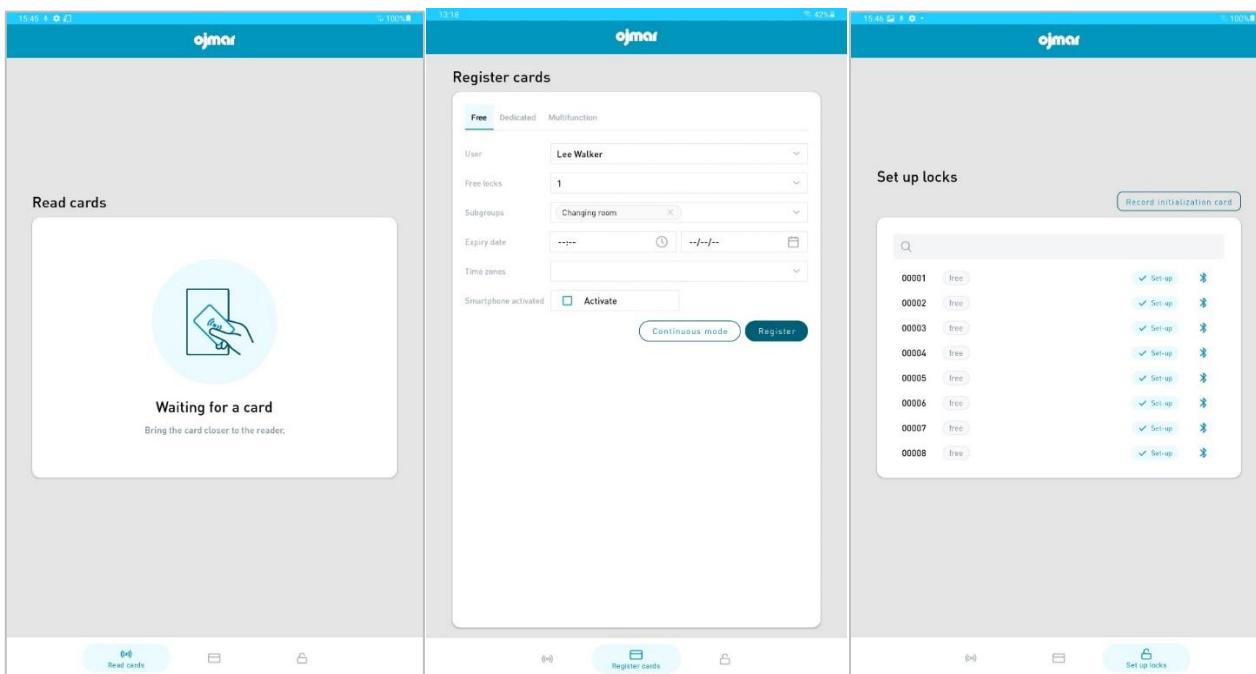




- NOTE: Internet connection to the device is required for proper operation. Ports 20870 and 1921 shall be opened.
- NOTE: Online status of the gateways can be check in Software menu, pressing "Peripherals/Gateways management"

3. PROGRAMMER

The Ojmar Programmer is a lock and credential configuration device. This device automatically downloads the configuration of the locks from the software and configures them for the first time via RFID. The programmer also has the option to register the RFID credential for the first time to give them a number.



Using the programmer, the installation administrator will be able to read information about the existing card, generate new user cards and create set-up cards.

4. INFOTERMINAL

The infoterminal is a device to inform the user in case they forget the locker number that is occupying. When approaching a key to the reading area indicated on the infoterminal, the number of the lock taken by that credential will be displayed on the screen, allowing the user to know which locker they have taken. It also includes real-time information on the status of the installation and information on the expected occupancy in the incoming hours as a

guide for users to know which lockers are available. This infoterminal is placed on a wall, allowing the user convenient access to key information. The set consists of:

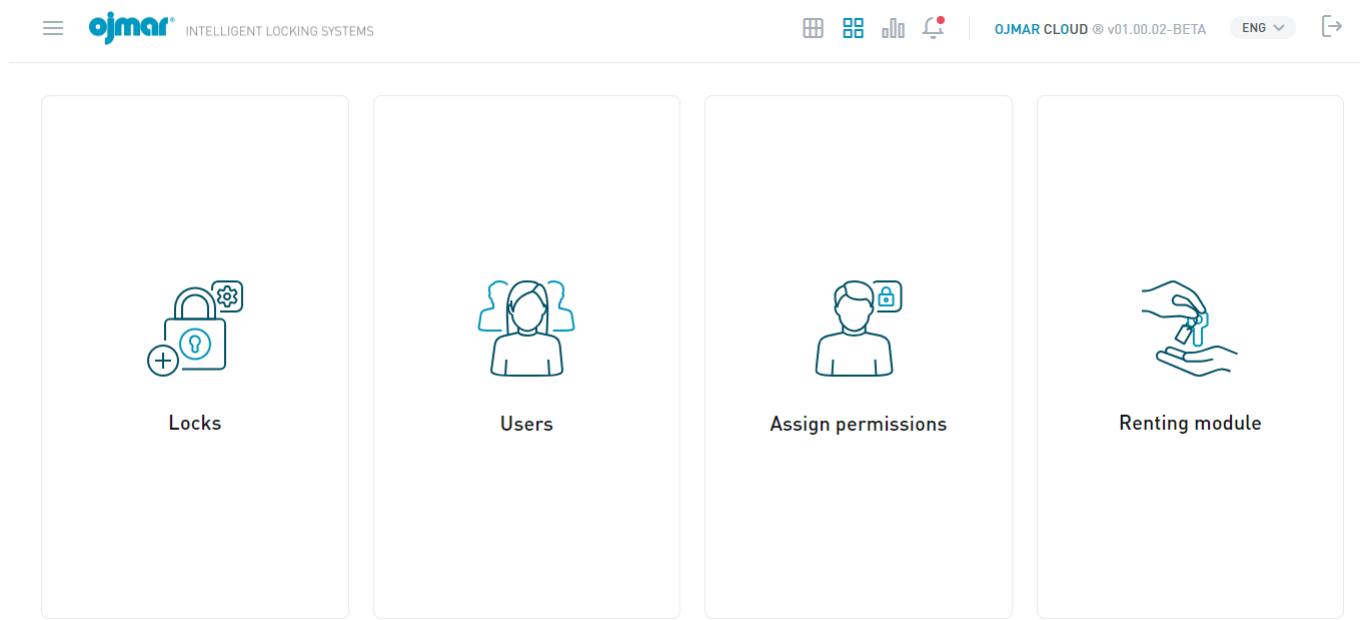
- Wall support.
- Infoterminal.
- USB power cable



5. SOFTWARE

OJMAR's cloud management SW can manage and/or monitor in real time the installation of OJMAR locks. It is a cloud-based application, so it is a multi-device, multi-platform, and scalable software. It can run on any device with any operating system installed, using the Google Chrome web browser. The SW is managed using the browser, and it is enough to go to the specific web page, provided by Ojmar.

The user will have a predefined operator profile or role, although the system allows to generate new ones with permissions. Each operator has a username and password to access his account.



5.1. SOFTWARE FEATURES

OJMAR's SW will be able to manage the following features:

- **Locks:** Access to the facility's locks list. Allows management: create/delete/edit (lock name, lock type and associated wall).
- **Subgroup:** Access to the facility's locks subgroups. Allows management: create/delete/edit (subgroup name).
- **Operators:** The user to be used when log-in. Each operator has an associated role. Allows to create/delete/edit (username, password) operators.
- **Roles:** Created set of permissions to assign later to operators.
- **Time zones:** Access to a list of configured time zones. Allows management: create/delete/edit (subgroup name). The user keys that don't have assigned any permission out of the time zone won't operate out of the determined time.
- **Automatic openings:** Access to configured automatic openings. Allows management: create/delete/edit (name, hour, subgroup and week/days). The established locks will automatically open on the given time (only for free type locks).
- **Walls:** Access to facility's walls list. Allows management: create/delete/edit (wall name, nº of rows, nº of columns, vertical/horizontal).
- **Advanced settings:** SW configuration parameters: domain name, UTC time, maximum rent time, etc.
- **Users:** Access to the facility's users. Allows management: create/delete/edit (username; email and phone optionals). It's possible to import users from a CSV file.
- **User permissions:** Access to the UIDs list and permissions. Allows permission management filtering by UID or users. Free/Dedicated/Multifunction.
- **Generic permissions:** Access to the list of created generic permits (permission profiles).
- **Facility in Real time:** Access to wall visualization (main screen).
- **Dashboard:** Access to statistics.
- **Data export:** Allows data export of events, users, locks and resources (CSV or EXCEL format).
- **Audit trail:** Registered system events.
- **Alarms:** Registered system alarms.
- **FW update:** Allow to update the FW version of locks, gateways and RF modules (of Gateway). Shows the list of devices with out-of-date FW versions.
- **Gateways management:** Access to facility's Gateways list. Allows to see its status and MAC address (also last communication and access rights update).
- **Infoterminal management:** Access to facility's Infoterminal list. Allows to see the associated wall, version and online status. It's also possible to edit Infoterminal's name and the wall it is pointing.

- **Programmer management:** Access to facility's Programmer list. Allows to see the associated wall, version and online status. It's also possible to edit Programmer's name.
- **Downloads:** Access to downloads. Allows to download the CSV template for user import.

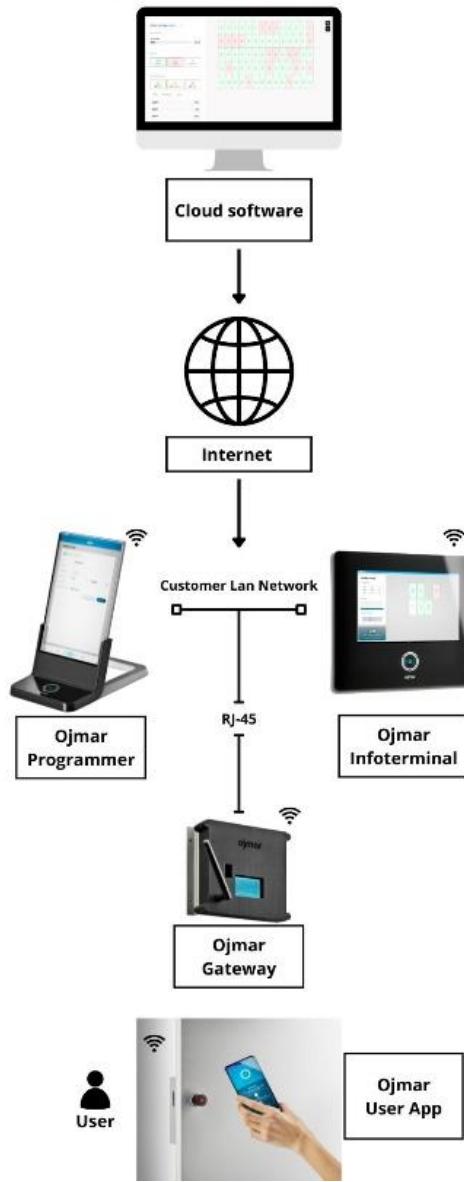
6. SYSTEM MANAGEMENT

6.1. SYSTEM ARCHITECTURE

System architecture is the following one:

OTS® PULSE

System architecture



Gateways will be connected by Ethernet to an internet connection (PoE available) via port 20870. Once connected, it will be automatically connected to the Ojmar Cloud software, deployed in the cloud.

Locks will be automatically connected to the Gateways with a 2.4GHz proprietary protocol, that will respond to the lock to operate.

Apart from that, programmer will be connected to the cloud via Wi-Fi and Infoterminal will be connected to the cloud via Ethernet, both by port 1921.

6.2. SYSTEM SET-UP

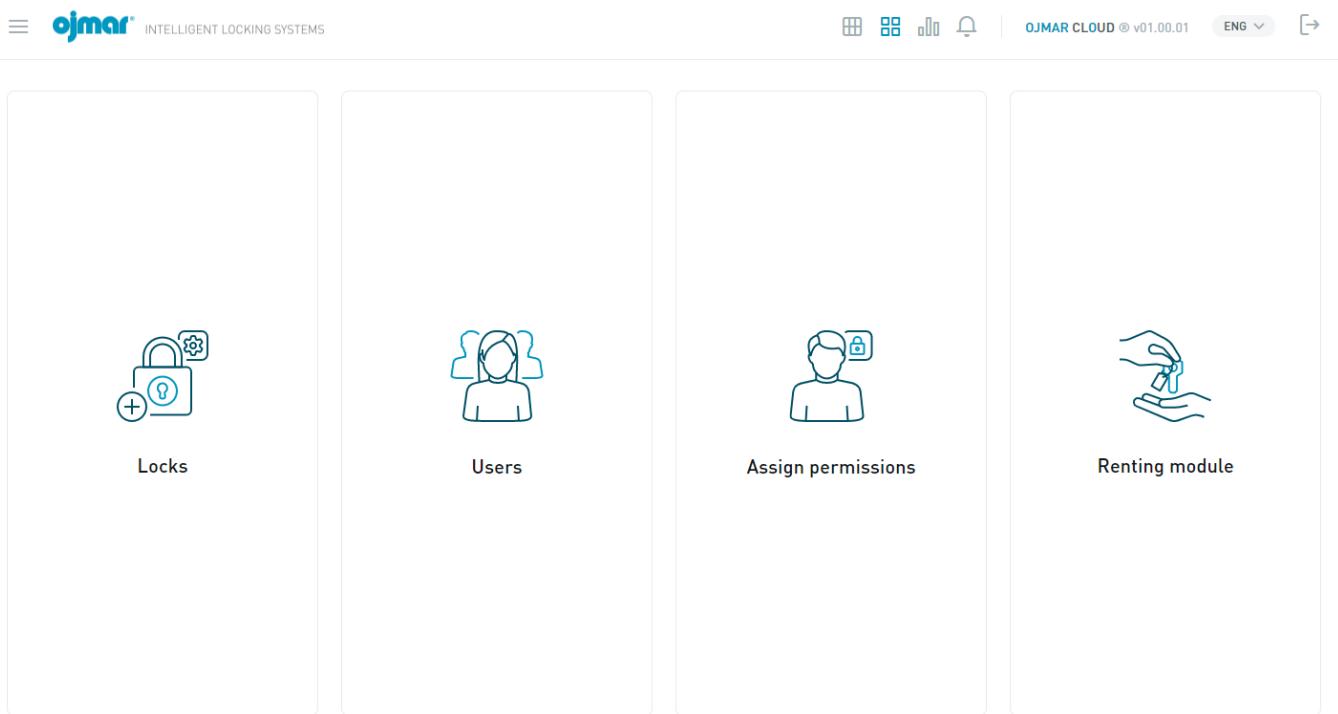
Following steps must be done to set-up the system:

- 1- Connect the gateways to internet (Check that port 20870 is opened outbound)
- 2- Log in to the software (See chapter 6.2.1)

- 3- Check on the software that gateways have been connected and that are online. (See chapter 6.2.2)
- 4- Create the locks and the walls on the software (See chapter 6.2.3)
- 5- Connect the programmer to the WiFi network (Check that port 1921 is opened)
- 6- Create the set-up card and set the locks (See chapter 6.2.4)
- 7- Check online communication (See chapter 6.2.5)

6.2.1. LOG IN THE SOFTWARE

As part of the set-up procedure admin will receive an e-mail with a web page to access. Clicking on the link will load the web page, and you will be prompted to enter a password for the “admin” user. Once entered, the user is logged in and will have access to the software.



To change the administrator username and password, left click on the three horizontal bars at the top left of the screen, then select “Configuration/operators” and press the edit button of admin operator in order to change username and password.

- NOTE: Different credentials can be created in "Configuration/Credential" to limit the modification and viewing permissions of different operators.
- NOTE: New operators can be added in "Configuration/Operators" and have assigned an specific credential to each one

6.2.2. CHECK GATEWAYS CONNECTION

Select the icon on the upper left side, and go to Peripherals → Gateway Management

Gateway Example	8034285D0A10		06/07/2023 13:02:38	07/07/2023 12:16:45	
-----------------	--------------	--	---------------------	---------------------	--

For each Gateway, a “Yes” has to appear in the Online option. This option will mean that Gateways are getting connected to the software.

- NOTE: If “No” appears on Gateway connection, please check that port 20870 is opened in the network. If problem persists, contact Ojmar.

6.2.3. LOCKS CREATION

In the main menu select option Locks, and the choose "Add".

Locks / Add lock

Add lock

Save

Lock information

Name: Prefix 1 Suffix

Amount:

Type: Select an option

Subgroup: Select an option

Create subgroup

Wall: Select an option

Create wall

Following options will need to be filled for the locks' creation.

- Name: Name of the first lock that is going to be created. A prefix (Up to 2 characters) and a suffix (Up to 2 characters) can be added to the name.
- Amount: Quantity of locks that will be created in a consecutive way
- Type: Type of lock (It can be chosen between Free, Dedicated or rental). See Chapter 1.4 for further information.
- Subgroup: Only available for free locks. Subgroups can be used to differentiate between different groups of locks. Each subgroup can have its own automatic openings and time zones. You can also limit user permissions by providing access to some subgroups and not providing access to others.
- Locker Walls: Virtual structures in which the locks will be installed and give each lock an specific position on the wall. For each wall, the name of the wall, the rows, columns and the orientation of the numeration can be defined.

Once created, press save and following screen will be shown and information will automatically be downloaded to the programmer.

6.2.4. LOCK SET-UP

- NOTE: If the locks have not been initialized from the factory, it is necessary to initialize them.

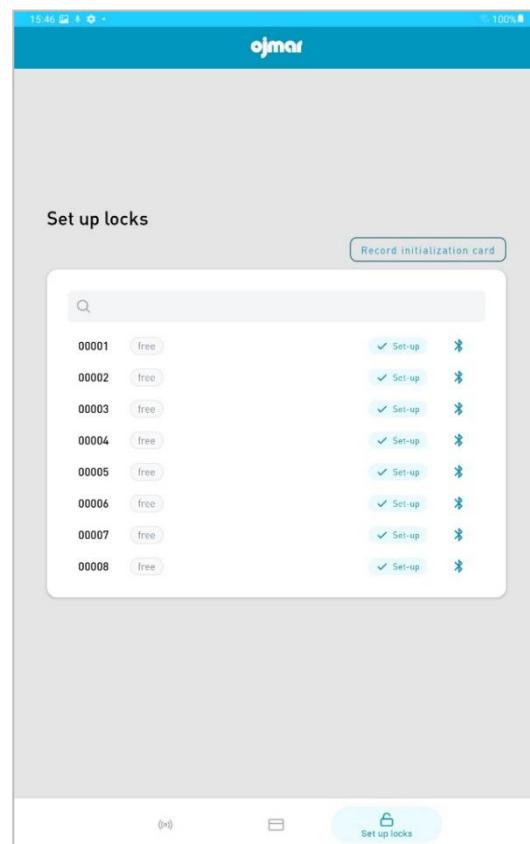
- NOTE: If the locks have been initialized from the factory, the activation card must be swiped in order for them to start working online.

Once locks have been created in the software, it is necessary to use the programmer to set up the locks:

Using programmer, select the padlock symbol at the bottom right (Set up locks):

- Choose the option "Record initialization card".
- The lock group (if any) is selected.
- Place the set-up card (delivered by Ojmar) on top of the programmer and press record.
- Push the lock nozzle with the card. The lock will buzz and will make 3 amber and 2 green blinks, confirming successful initialization.

- NOTE: This operation is only necessary for the first time after receiving the locks. Any configuration changes can be made from the Ojmar Cloud SW.



To test the communication with the Ojmar Cloud SW, use the master key provided by Ojmar to close and open each lock. Ojmar Cloud SW should record "Master card closing" and "Master card opening" events for each lock.

6.2.5. CHECK ONLINE COMMUNICATION

Once locks are set, choose icon and walls will appear. At first sight, locks will appear in grey. In order to cycle with the master card and locks will turn in green.



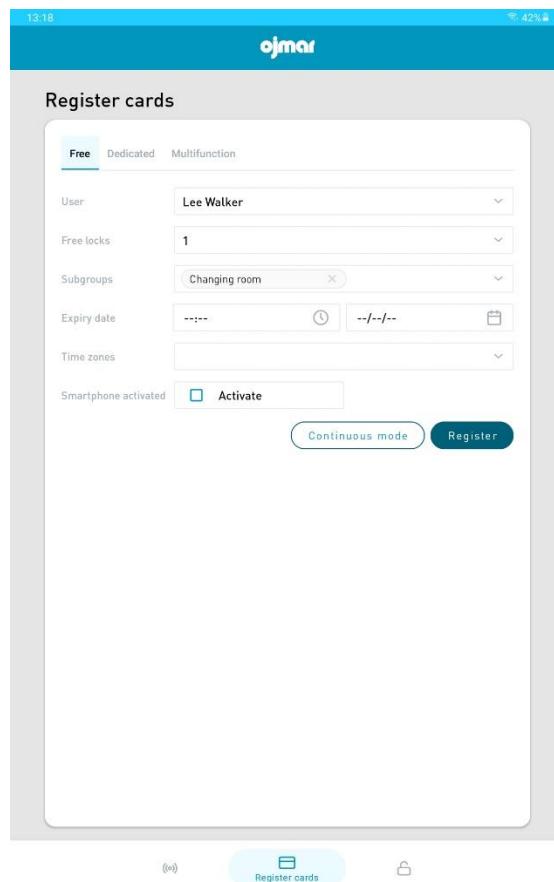
6.3. SYSTEM USE

6.3.1. REGISTER PERMISSIONS FOR THE FIRST TIME

Cards must be registered for the first time in the system. In this case, programmer's second option has to be chosen "Register Cards".

Following fields must be filled:

- Type of permit: Between free, dedicated and multifunction (free mode and dedicated at the same time).
- Fill the rest of the fields as desired.
- Place the card on top of the programmer and press record.
- Pass it through the lock with permissions and lock will get closed.



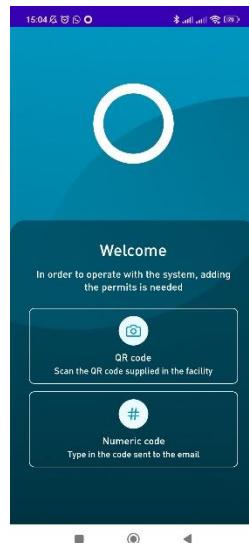
6.3.2. REGISTER PERMISSIONS FOR THE FIRST TIME

Once cards are registered for the first time, permissions can be reassigned directly from the software. To do this, go to the “Assign permissions” option.

The user (OR key) is chosen, and the configuration is changed as required. Press save, and the data will be updated in real-time.

6.3.3. MOBILE DEVICE CREDENTIALS – PHONES/TABLETS ETC

Once permission is given to the customer's smartphone, customer will need to download the App “Ojmar Cloud” from the Google Store/App Store.



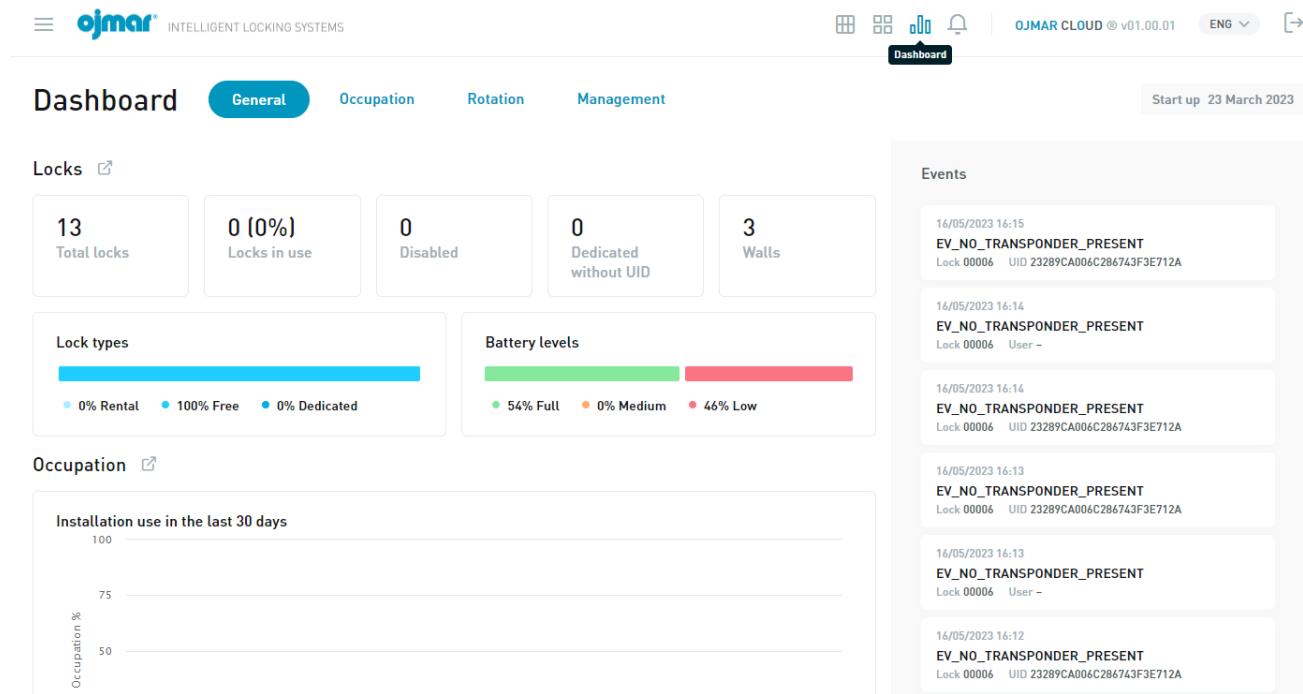
- Customer will be able to type a 9 digit code received by email or read a QR code in order to download the permissions to the Smartphone.
- Once downloaded, press operate, choose the desired lock and:
 - Closing operation: present phone to lock and press lock button on app whilst pressing lock nozzle.
 - Opening operation: present phone to lock and press unlock button in app. Nozzle will open automatically.

7. MAINTENANCE AND FAQS

OTS.Pulse automatically detects low battery levels. The Software will warn you when a lock is low on battery power. Up to 9 open and close cycles once the low battery is detected. On the tenth cycle, the lock can only be opened (never closed). This prevents a locker from getting stuck with no batteries.

7.1. DASHBOARD

By clicking on the graph symbol at the top of the Ojmar Cloud SW, you can access the dashboard area that contains all the information generated in the facility such as lock events, percentages of lock occupancy, number of cycles, battery status.....



7.2. BATTERIES REPLACEMENT

For battery replacement, follow the steps below:

1. Remove the torx screw.
2. Open the battery cover.
3. Remove the battery holder.
4. Replace the four AA batteries (two on each side of the support).
5. Insert the battery holder. The cover should fit easily. To do so, first insert the wire and then the battery holder.
6. Fit the cover and tighten the torx screw.

1



2



3



4



5



6



NOTE: It's advisable to make a closing and opening cycle with master card in order to test that the lock remains connected to Ojmar Cloud SW.

WARNING: During replacement of the batteries, maintain some model of batteries in order to assure correct function of the lock.

WARNING: Do not leave batteries in extreme conditions, such as hot temperatures, abnormal pressures, as they could suffer chemical damages

WARNING: Do not cut the batteries

7.3. LED INDICATIONS OF OTS PULSE LOCKS

The OTS Pulse incorporates a three color LED light to signal lock status and programming indication as follows:

Description	LED Sequence	Duration
Communication fault	●	1 s/flash
Mechanical error	●●●●●●	100 ms/flash
Low battery detection. Change batteries.	●●●	400 ms/flash
Definite low battery. Change batteries.	●●●	2 s/flash

Lock unusable until batteries changed.		
Set-up Correct		400 ms/flash
Key deleting OK		400 ms/flash
Date and time recorded correctly on the lock		2 s/flash
Winter-summer time changes correctly recorded on the lock		2 s/flash

7.4. FAQS

QUESTION	CAUSE	SOLUTION
The lock displays 3 amber flashes or does not flash.	The lock has detected flat battery level.	Replace the lock batteries and test its working status using a free mode credential
The Credential does not work on the locks.	The Credential is being used in another lock or it has never been registered.	Check whether the credential is or not in use (via programmer or software). If in use, clear it using the Management Software or by closing and opening the corresponding lock. If it not in use or registered in the system, record the credential using the programmer or via Software.



INTELLIGENT LOCKING SYSTEMS

Polígono Industrial de Lerun, s/n 20870 Elgoibar · Spain

T. +34 943 748484

www.ojmar.com

