EDEN INNOVATIONS

Access control

OPTIMA Box®

ONE Pass

ONE **PASS**

Table of contents

1- Compatibilites

- OPTIMA Box in version 4.12.0 minimum with the “ONE Pass” additional module activated
- At least one C485-IP-SSCP interface connected to the same IP network as the OPTIMA Box
- At least one STID ARC-W33 SSCP master reader (update reader) connected by Bus to the C485-IP-SSCP interface
- Offline readers compatible in offline mode with the “offline standard” OSS standard. Configuration and update: software and/or configuration badges required by the manufacturer
- ONE Pass tablet consisting of a display screen and an update reader connected to the C485-IP-SSCP interface (optional)
- MIFARE DESFire® badges 2K minimum

2- ONE Pass Module

To activate the **ONE Pass** module, press ‘*Activate’* in the Configuration/Installation administration/Additional modules menu. You will be asked for an activation code.

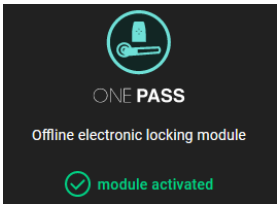


Fig. 1: ONE Pass Additional module.

Please contact your sales department to get the appropriate code.

3- Specifications

3.1 Principle of operation

Installation in Offline mode (offline) with OPTIMA ONE Pass requires offline compatible readers, badges and one or more master reader(s) connected to the OPTIMA Box.

The badges are used directly on door handles or on compatible cylinders in offline mode, depending on access rights, validity dates and authorized time slots.
No need for wiring or an access control unit.

Given that the readers are not configured online to issue the rights or not, a refresh frequency can be configured for each of the badges to encourage badge holders to update their access rights.

When the update date has passed, badges are no longer authorized on all readers: it is necessary to update the deadline, as well as the user rights by passing the badge over the master reader provided.

In addition to updating the deadline when switching to the master reader, the following actions are carried out:

- Updating of all rights if they have been modified in the meantime by the Administrator.
- Recovery of passage events on readers.
- Deletion of events recorded in the badge.

The ONE Pass module allows you to configure badge update rules and offers the possibility of creating or editing badges by encoding on the master reader.

The technology chosen for the badges is MIFARE DESFire®.

3.2 Update rule

The minimum frequency for updating badges is 24 hours.

- A compromise concerning the refresh frequency must be configured: the lower it is, the more users must refresh regularly: the more frequently rights and events are refreshed.
- Time slots are used to restrict access to specific times during the defined period before the next refresh.
- Validity dates can be configured to block badge access until a given date.

3.3 Update reader

Role of the update reader

The update reader is required:

- For the site administrator to create each new badge by encoding with specific rights.
- To retrieve badge swipe events.
- For the badge holder in order to update his rights and the deadline.
- To retrieve badge swipe events.

Master reader location

Several update readers can be connected to the OPTIMA Box.
To ensure that the master reader is always physically accessible to modify rights and to retrieve events:

- The update reader is located inside a building: access to this building must be via standard access control (online).
- The update reader is outside a building: readers giving access to the building must be close to the master reader.

The protocol chosen for communication with the reader is SSCP® for maximum security.

3.4 Forbidden badges

If you wish to quickly block access to a badge, and this before the next update date (stolen/lost badge, or other, etc.) for which the rights are restricted, you can register it on the list of prohibited badges from the Optima software.

A specific badge containing the list of badges to be denied access must be encoded from the ONE Pass interface using the update reader.

This badge **must then be passed over the doors concerned to block the desired badge(s)** for a period of prohibition to be specified (up to 256 badges).

4- General configuration

4.1 Configuring the update reader and card settings

ONE Pass menu / General configuration 

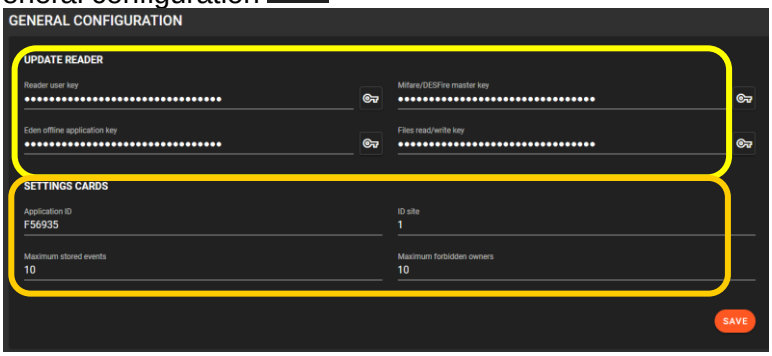


Fig. 3: Configuring update reader.

Keys configuration

For all of your update readers, define the keys in terms of:

- Reader user key
- Mifare®/DESFire® master key
- Eden offline application key
- Files read/write key

These keys must consist of 32 characters in hexadecimal format.
Keys ensure reader authentication.
Any loss of these leads to the drive being returned to the manufacturer to reset it to factory mode.

Card settings

For all of your update readers, define the settings in terms of:

- Application ID
- Site ID
- Maximum stored events
- Maximum forbidden owners

User guide : https://www.optimabox.fr/doc/produits/notices/spinel/en_US/modules/C485-IP-SSCP.pdf

The user or the Administrator must keep the values of each key in an independent file which remains under his responsibility.
EDEN Innovations is not responsible for any loss.

4.2 Configuring update reader

Configure the IP address of each C485-IP-SSCP interface (default: 192.168.3.140 / port 10001).
Also fill in the associated company(ies) and the parameters related to tear-out management.
Select at least one reader as the encoding reader.

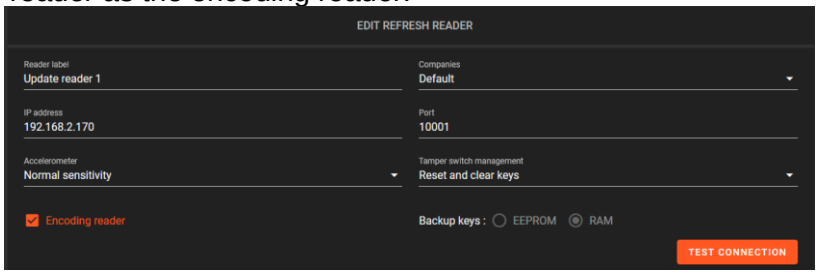


Fig. 4: Configuring settings for an update reader.

Tamper swith management
Depending on the movements detected by the player's accelerometer, adjust the sensitivity level to perform the following operations:

- None
- Reset reader
- Clear keys
- Reset and clear keys

It is recommended that the removal management setting be set to "Key reset and clear keys" to ensure maximum security.
The next connection to the reader saves the keys necessary for its connection.

It is necessary to take into account the type of DESfire cards (1K, 2K, 8K, etc.) according to the number of events desired to be recorded by considering the number of readers in your installation and the refresh rate.
Access to the doors is still authorized but the event will not be recorded in the badge if the size is insufficient.

4.3 Establishing the connection with the master reader

After configuring the reader and card settings, you can press the button TEST CONNECTION to verify the connection of each reader.

Communication with the master reader is established: the "**Receive**" and "**Transmit**" diodes of the C485-IP-SSCP interface flash continuously.

In the event of a connection failure, a disconnection notification is displayed in the OPTIMA information menu bar.

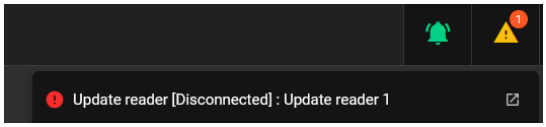


Fig 5. Update reader disconnect notification.

5- Configuring offline readers and offline groups

Authorization on a door is done by giving access to the reader **or** group belonging to the door.
The configuration of readers and offline groups is only available by connecting to OPTIMA with the user profile in Administrator mode.

Configuration of offline readers and groups is only available by connecting to OPTIMA with the user profile in Administrator mode.

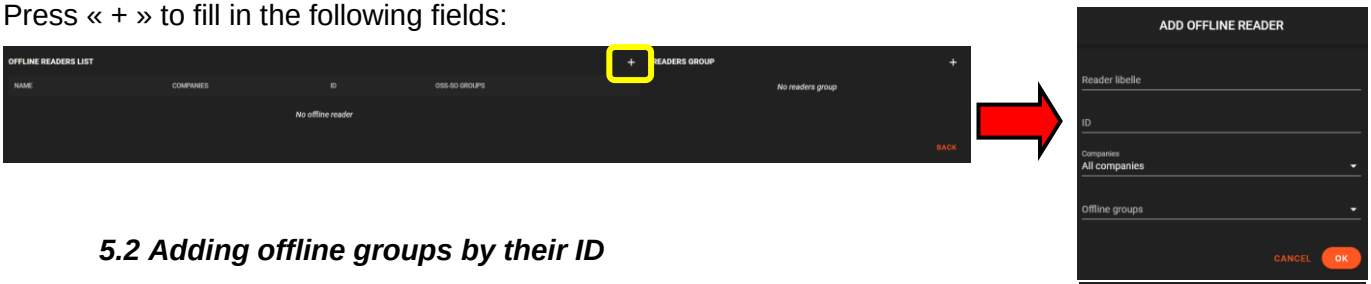
From the Offline readers menu  , add:

- The readers corresponding to your installation by setting their identifier.
- The groups corresponding to your installation by setting their identifier.

Please refer to the "*Configuration_offline_U&Z*" manual for the configuration of U&Z brand offline readers available here :
https://www.optimabox.fr/doc/produits/notices/spinel/en_US/logiciels/Configuration_offline_U&Z.pdf
The "*Configuration_offline_APERIO*" manual for the configuration of APERIO brand offline readers available here :
https://www.optimabox.fr/doc/produits/notices/spinel/en_US/logiciels/Configuration_offline_APERIO.pdf
The "*Configuration_offline_dormakaba*" manual for the configuration of dormakaba brand offline readers available here :
https://www.optimabox.fr/doc/produits/notices/spinel/en_US/logiciels/Configuration_offline_dormakaba.pdf

5.1 Adding offline readers by their ID

Press « + » to fill in the following fields:



5.2 Adding offline groups by their ID

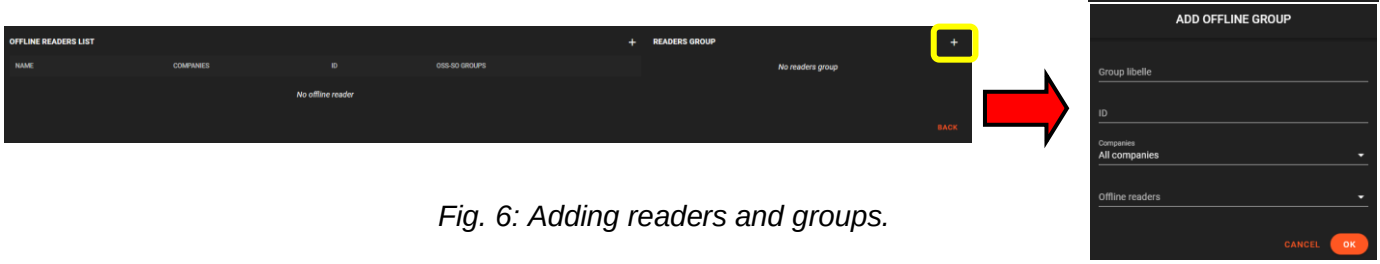


Fig. 6: Adding readers and groups.

The list of readers in the offline Group is purely **informative**.
This list is to be completed according to the initial configuration of the readers to a given group.
Readers belonging to this list are not authorized by default.

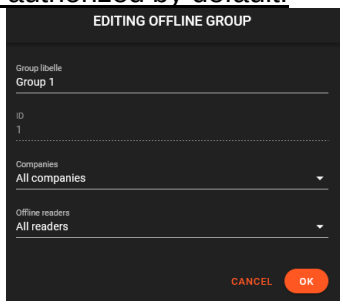


Fig. 7: Configuring offline group 1 with ID 1 & 2.

5.3 Deletion of readers

Delete readers by clicking on  .

Deleting a reader leads to the deletion of reader labels in the event history. Access to deleted readers is no longer authorized after updating the rights.

6- Configuring badges

This menu allows you to establish a “standard” configuration to apply to your badges, in terms of:

- Permission to access
- Type of event to write in the badge
- Update rule

6.1 Access rights

Select authorized readers and/or groups with offline time slots.
It is possible to assign up to 4 offline time slots per reader.

By default, or if no time slot is selected, access is permanent.

For each of them, choose the Toggle function and/or Extended opening option.
To work, the options Toggle mode (= Permanent free passage mode) and "Extended unlock time" must be activated on the readers concerned.

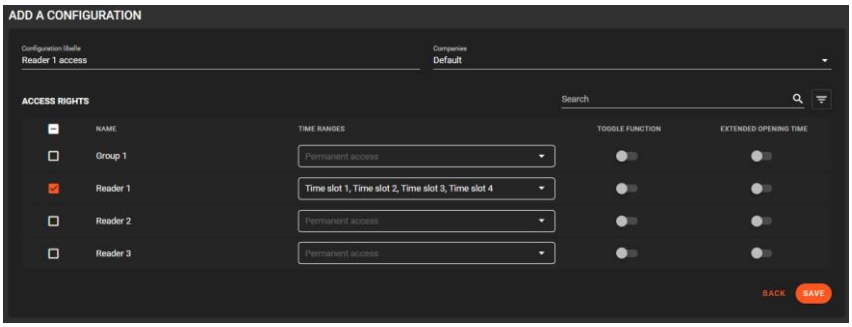


Fig. 8: Configuring access rights.

6.2 Events type

Create "standard" configurations to apply to your badges to record or not certain types of events passing through the readers.

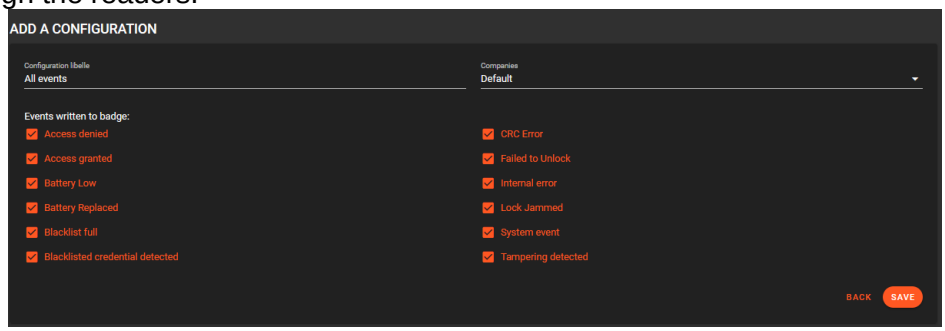


Fig. 8: Types of events to record in badges.

6.3 Update rules

The update date is the only way to force users to pass their badge on the update reader.
After this date, badges are **no longer authorized on all readers**.
The update frequency therefore conditions the frequency with which badges are passed over the update reader to renew rights and to recover events.

- The lowest possible frequency is 24 hours.

- The date is updated by adding the number of days/weeks/months in relation to the last date the badge was updated.

- Event retrieval transfers events to the OPTIMA database, then empties the card of all recorded events.

- It is recommended to configure update rules for all badges, including badges for guests, employees, administrators, or trustees.

- In fact, in the event of loss or theft, or departure of the badge holder from the company, the badge will be automatically blocked on all readers once the update date has passed.

- Choose the days of Saturday and/or Sunday to exclude if you do not wish to include them in the update frequency (feature available in "Day" frequency only).

- At a minimum, it is recommended to configure a validity date to block badges after a given date.

Disabling the update rule is strongly discouraged.
In this case, the badge holder will have unlimited access to the readers included in his access rights.
(Except passage of the "Badge forbidden" on the readers whose access must be blocked).

Tip! A daily update is recommended if you want finer management of access rights and if you want to obtain the most up-to-date events.

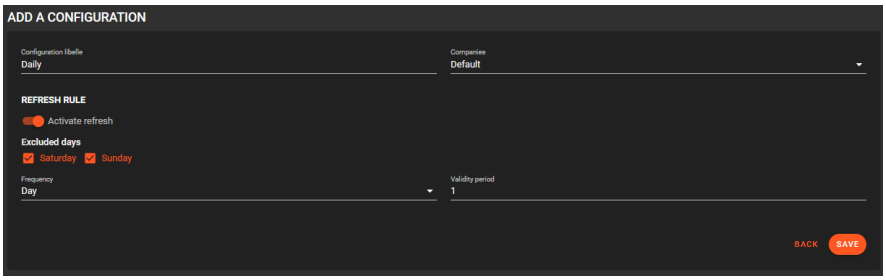


Fig. 10: Daily update rule not counting weekends.

Practical cases of updating:
• The user passes his badge on the update reader at 1:00 p.m. for an update frequency of 1 day. Access is authorized **until the next day at 1:00 p.m.**
After this time, the user must pass his badge on the update reader to issue access again for an additional 24 hours.
• Saturday excluded: if the badge has an update frequency of 3 days with the last update on Friday at 8:00 a.m., the user must update **after the following Tuesday from 8:00 a.m.** to obtain access again.

7- Event settings

Modify the events here in terms of:
- Label in the list of events
- Label color in the list of events
- Purge recurrence (90 days by default)

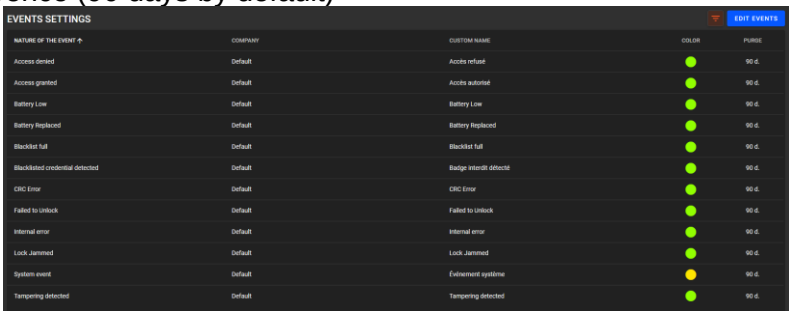


Fig. 11: Events settings.

8- Access control rights

Give your badges detailed rights or apply existing configurations.
The configuration must be detailed if no configuration has been selected regarding access rights, event configuration and refresh configuration.

8.1 Time slots

Users' offline time slots are available from the Access rights / Time slots menu in the Configuration menu of the OPTIMA interface with the option "*Time slot used in the ONE Pass module*" checked.

These are identified by the symbol  .

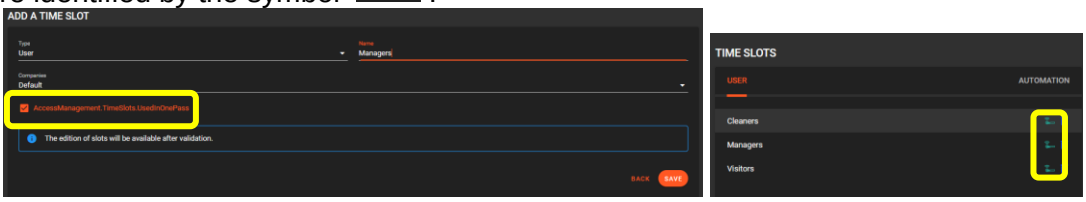


Fig. 12: Configuration of offline time slots for users.

It is possible to associate up to 4 time slots per day.
Existing access control time slots (online) are not compatible with offline time slots.

8.2 Validity

The user's validity period is available in the "Access rights" tab of the User file from the main OPTIMA interface.

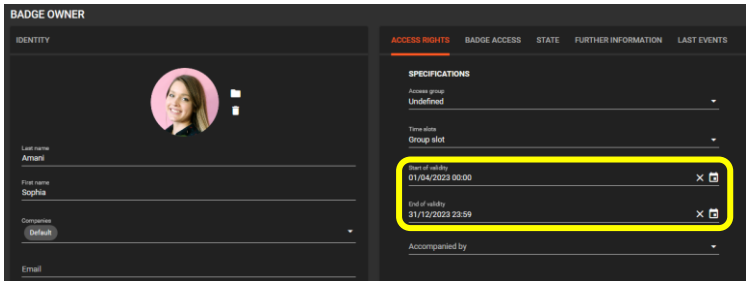


Fig. 13: Configuration of validity dates from the main OPTIMA interface.

9- Creation of badges by encoding

To assign the badges to the users it is necessary to encode them.

The list of offline users corresponds to the list of access control users.
Only the rights in terms of time slots (offline) and in terms of validity dates are applied from the access control.
Encoding a badge requires it to be configured first: click on the badge to choose its configuration of access rights, events and update rules.

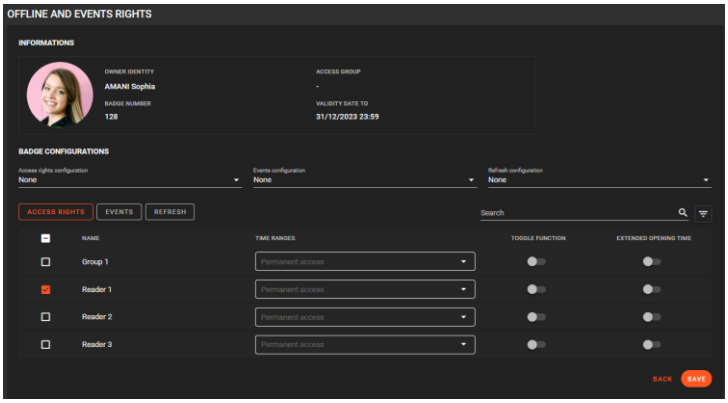


Fig. 14: Configuration of offline events and offline rights.

From the User rights menu  , choose the user whose badge has not yet been encoded: they are identified by the symbol  .

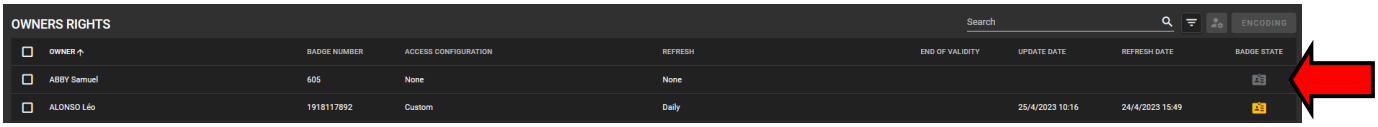


Fig. 13: Selection of a user for encoding.

Then click on the button **ENCODE** and present the Mifare®/DESFire® badge to the update reader until the LEDs on the reader light up green and the message "**Encoding completed successfully**" appears.

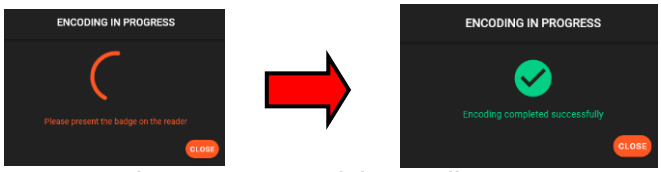


Fig. 16: Successful encoding.

Note: It is impossible to associate a user with a badge already encoded with another existing user.
If you wish to encode a badge already associated with an existing user:

- Identify it beforehand when passing the badge over the update reader in the Logbook (see Logbook section).
- Depending on the user identified in the Logbook, delete it from the OPTIMA interface.

10- Owners rights

View user properties from the menu  .

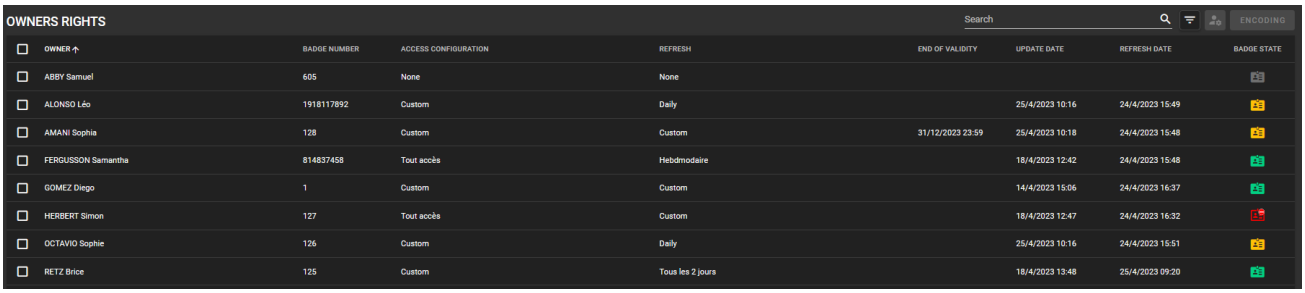


Fig. 17: Owners rights.

10.1 Badge status

On the date of consultation of the badges, check the status of all the badges. They can have the status:

- Unencoded badge  : no association of the user with an encoded badge.
- Valid badge  : the user badge valid at the time of the consultation.
- Badge with different configuration  : the badge configuration was changed after the last update.
- Forbidden badge  : the badge belongs to the list of prohibited badges.

   It is effectively prohibited after encoding the prohibited badge and passing it over the readers concerned (see Section “*Prohibited badges*”).

- Badge not valid  : the expiry date of the badge has passed.
- Badge out of refrech cycle  : the badge has exceeded its update date: it is refused on all readers.

  It must necessarily be updated by passing on the update reader (update of the deadline).

10.2 Filter

Click on the filter icon  to bring up the data filtering menu in order to select the user(s) according to the desired criteria.

Filter criteria:

- Valdity dates
- Rights configuration
- Update settings
- Badge state

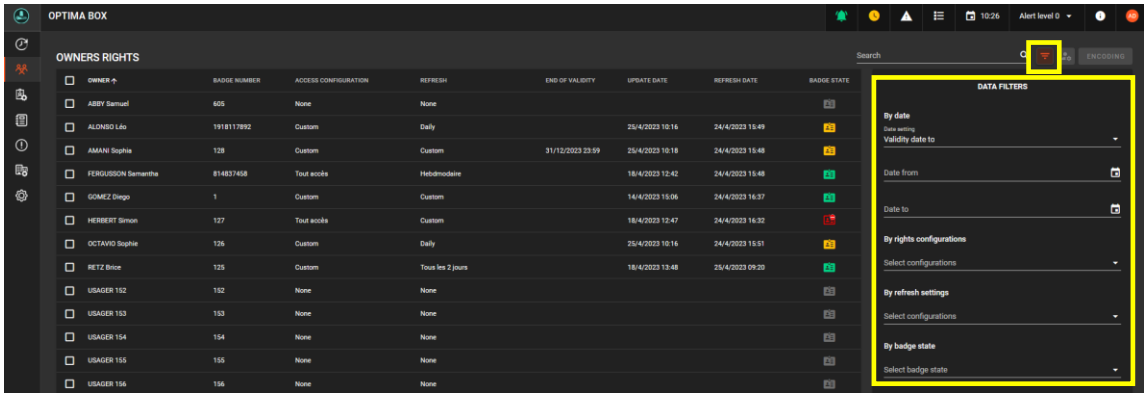


Fig. 16: Filter data.

10.3 Apply configurations

Apply a configuration change to badge selection in terms of:

- Access rights configuration
- Events configuration
- Refresh configuration

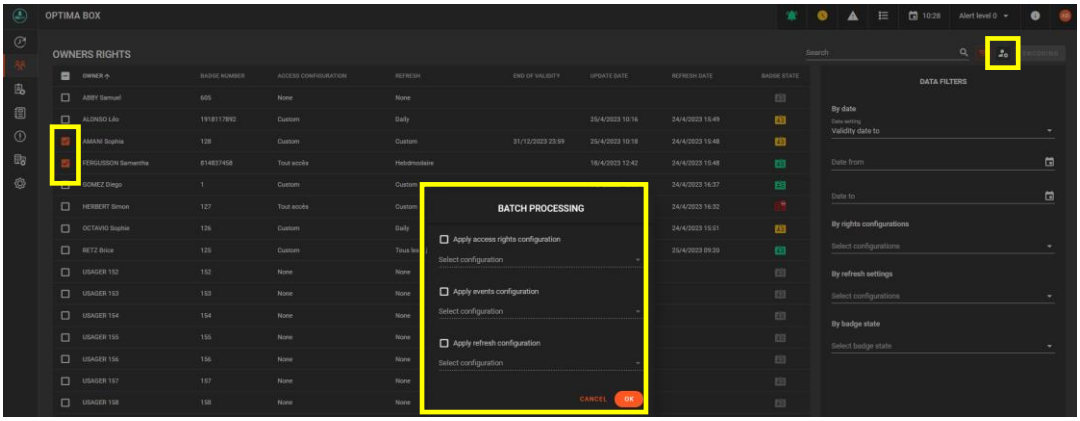


Fig. 19: Appy configurations.

11- Forbidden badges

If you want to quickly restrict a user's access in the following cases:

- The deadline has not passed
- The end of validity is not exceeded
- The offline time range is valid

It is possible to create a badge containing the badge or badges for which access must be prohibited.
All readers must be updated by presenting the encoded badge with the list of prohibited users.

11.1 Update access rights

It is advisable to change the access rights in order to restrict subsequent access to badge readers.
Click on the user file to deselect the readers/group in the access rights.

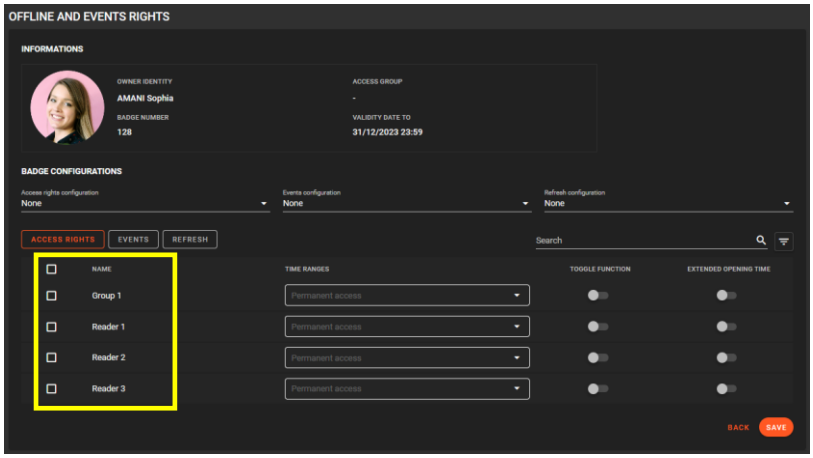
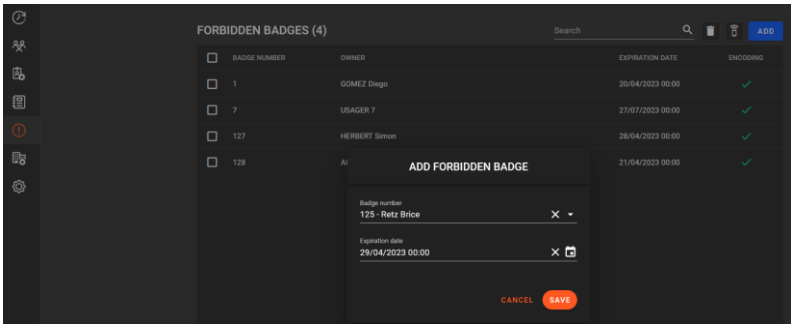


Fig. 20: Readers and groups are disabled.

11-2 Creation of the forbidden badge

Click on ADD from the “Badges prohibited” menu  to select the user (enter the letters of the user to search for) and select an expiration date.
The expiry date must correspond to a date later than the next update date of the badge (if existing).



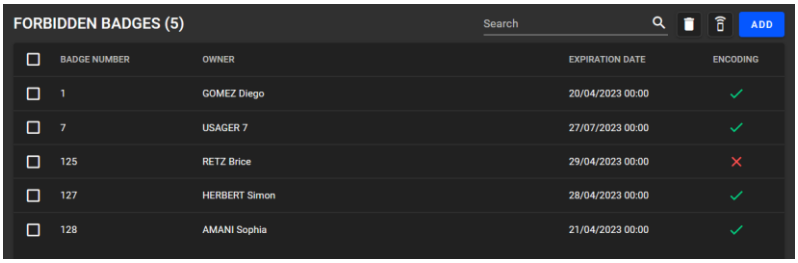


Fig. 21: Adding user to ban.

11.3 Encoding forbidden badge

Then click on the "Encode" button  and present a Mifare®/DESFire® badge to the update reader.

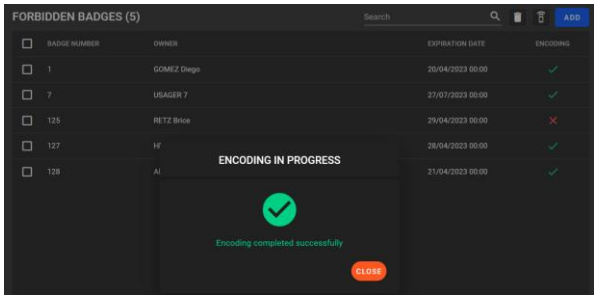


Fig. 22: Forbidden badge encoding.

11.4 Updating readers

Then present the badge on all readers to configure blocking.

It is possible to configure up to 256 prohibited users.
It is important to reduce the expiry date as much as possible in order to free up memory space for later adding badges to be prohibited.

The maximum number of users on the forbidden list can be configured from the general configuration  .

12- Logbook

Access information about the update reader.
These are the passing of badges and the connection/disconnection.

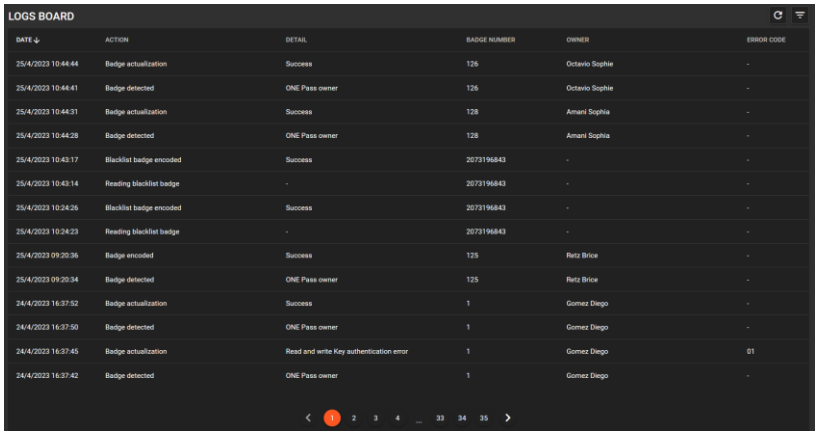


Fig. 23: Logbook.

The list is updated by clicking on the button 

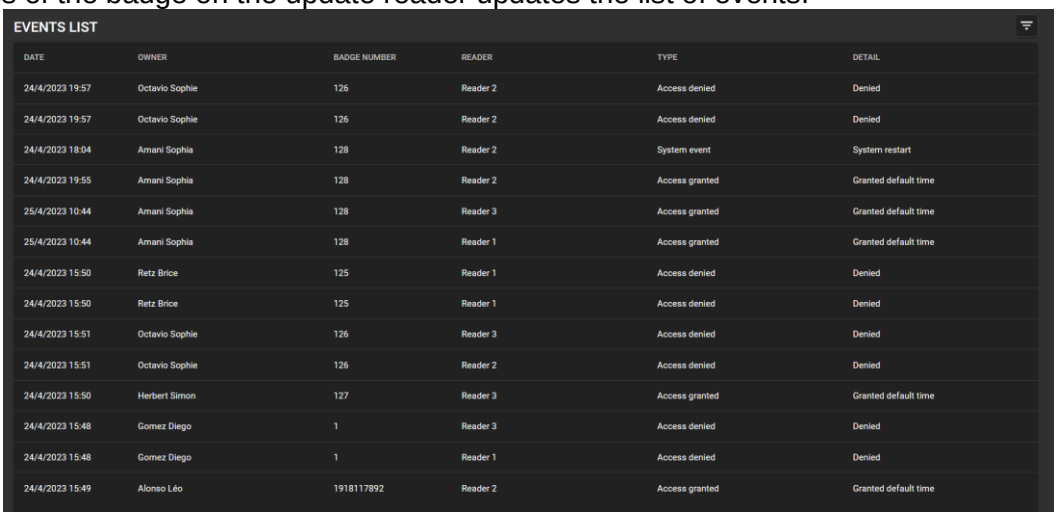
You can filter  the data according to the :

- Period
- Event types
- Update reader
- Owner

Export the entire logbook data by pressing the button  .

13- Operation

Each pass of the badge on the update reader updates the list of events.



EVENTS LIST

DATE	OWNER	BADGE NUMBER	READER	TYPE	DETAIL
24/4/2023 19:57	Octavio Sophie	126	Reader 2	Access denied	Denied
24/4/2023 19:57	Octavio Sophie	126	Reader 2	Access denied	Denied
24/4/2023 18:04	Amani Sophia	128	Reader 2	System event	System restart
24/4/2023 19:55	Amani Sophia	128	Reader 2	Access granted	Granted default time
25/4/2023 10:44	Amani Sophia	128	Reader 3	Access granted	Granted default time
25/4/2023 10:44	Amani Sophia	128	Reader 1	Access granted	Granted default time
24/4/2023 15:50	Retz Brice	125	Reader 1	Access denied	Denied
24/4/2023 15:50	Retz Brice	125	Reader 1	Access denied	Denied
24/4/2023 15:51	Octavio Sophie	126	Reader 3	Access denied	Denied
24/4/2023 15:51	Octavio Sophie	126	Reader 2	Access denied	Denied
24/4/2023 15:50	Herbert Simon	127	Reader 3	Access granted	Granted default time
24/4/2023 15:48	Gomez Diego	1	Reader 3	Access denied	Denied
24/4/2023 15:48	Gomez Diego	1	Reader 1	Access denied	Denied
24/4/2023 15:49	Alonso Léo	1918117892	Reader 2	Access granted	Granted default time

Fig. 24: Events list.

Past events are available by applying a filter  .

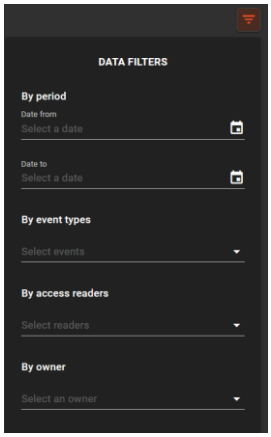


Fig. 25: Events list.

In addition to the period, filter according to:

- Event types
- Access reader
- Owner

Zone Commerciale et Artisanale
670, route de Berre
13510 EGUILLES
France
www.eden-innovations.com