golmar

iP–OPENER

END USER MANAGEMENT

USER MANUAL

TABLE OF CONTENTS

1. INTRODUCTION

This manual explains how the end user (site administrator) can use iP Opener Manager. For this, it is assumed that the installation administrator has granted permission to the software with the "Guardian" profile.

The "Guardian" software access profile is a profile with reduced permissions, which ensures that the configuration made by the site administrator (installer) will not be modified. At the same time, the end user (site administrator) can manage "schedules", "access profiles", "people" (users), and monitor "events".
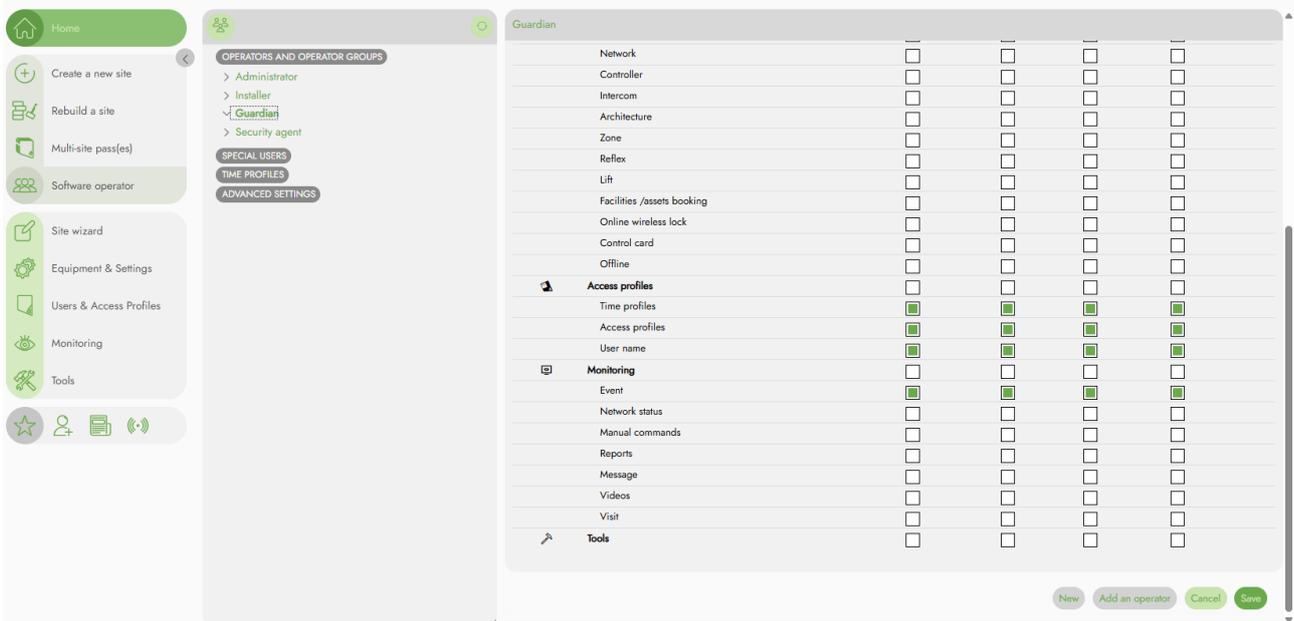
If you need additional functions, request higher permissions from the installation administrator.

2. LOGIN

Once the administrator (installer) has granted permission to the end user (site administrator), the administrator (installer) must provide the end user with the access credentials.

Once the end user (site administrator) has the credentials, they can log in by accessing www.ip-opener.com.
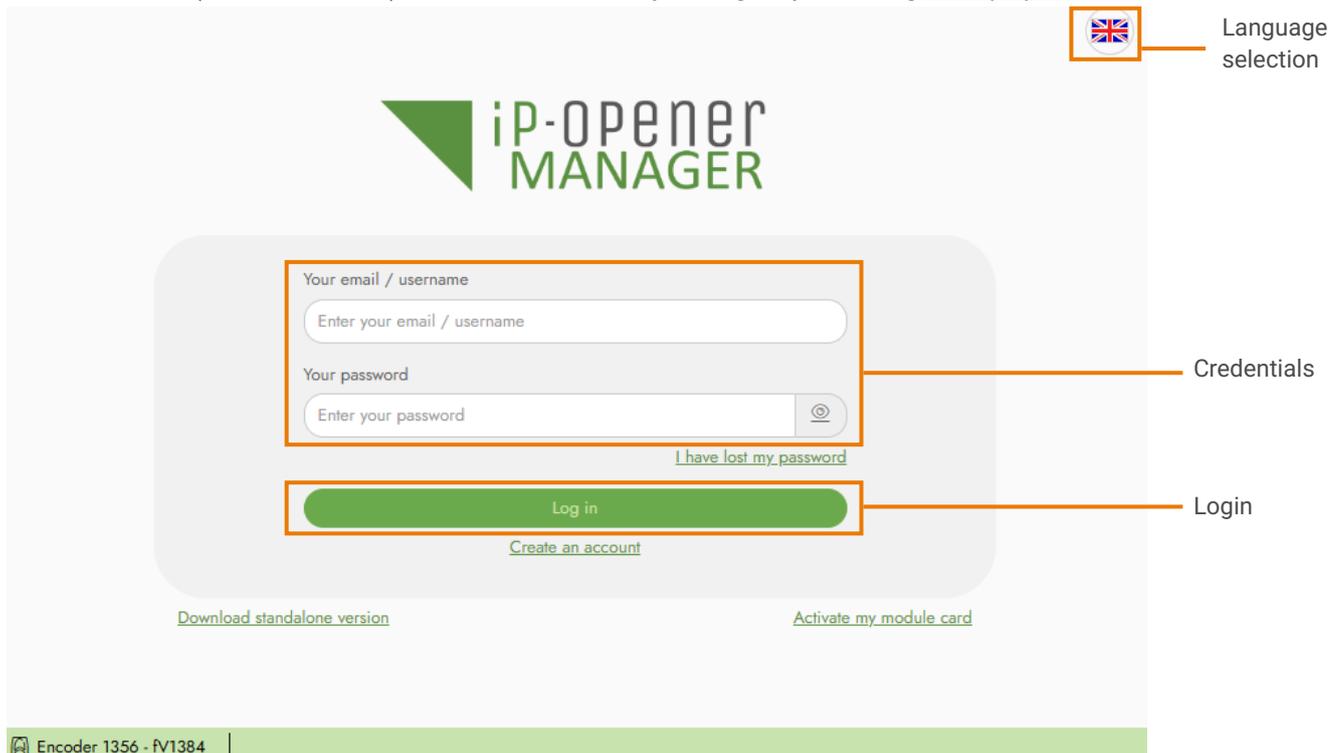
If the password is forgotten, click on the "Forgot password?" option. to restore it.

3. IP-OPENER HOME PAGE

Before reviewing the different steps to carry out a startup, see how the configuration environment is organized.

1 - Selected installation (site). The installation shown in this field is the one that will be modified.
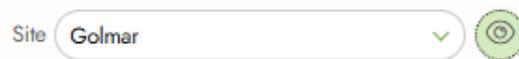
2 - Side menu.

Home page.

Create new installation (site).

Rebuild a site (function for standalone installations).

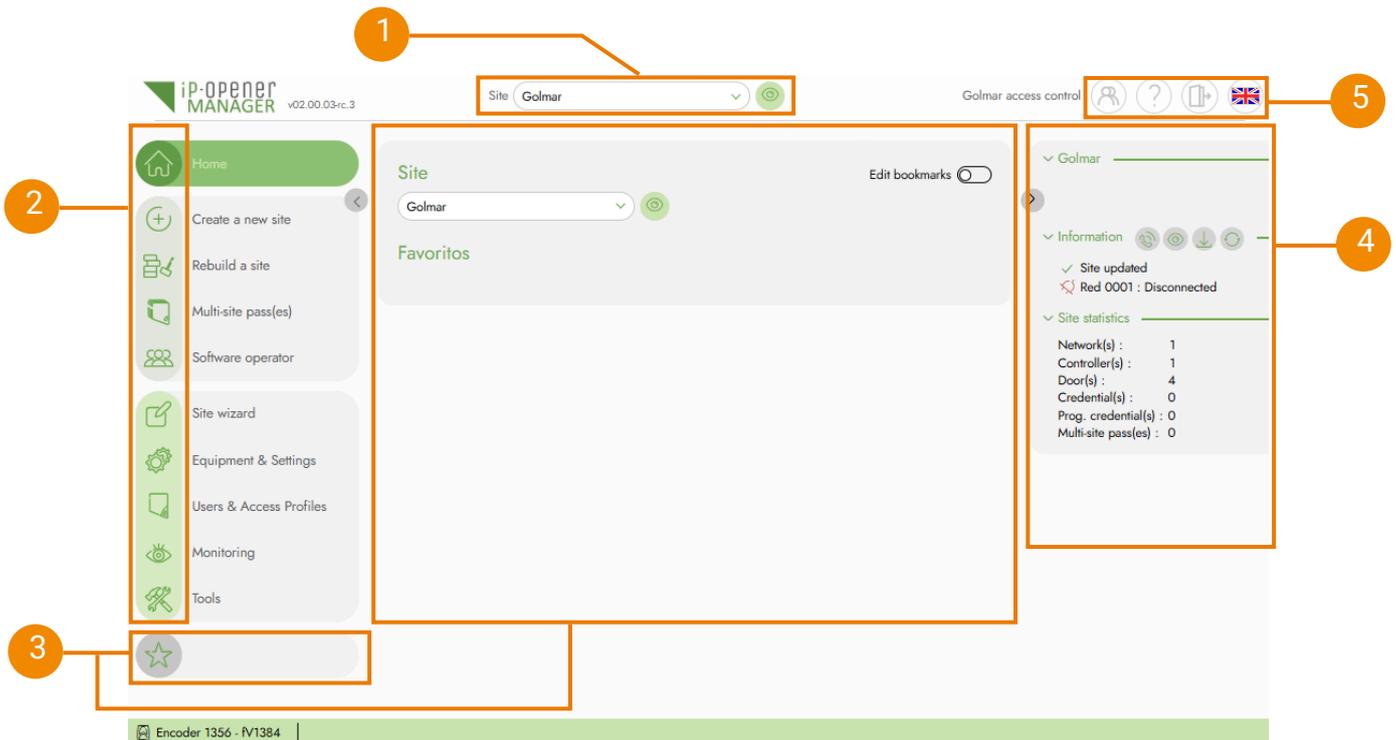Pass creation, a single card or credential allows access to different installations of the account.

Software access. Grant permissions to other users for full or partial use of the software.

Modify the site. The installation (site) to be modified will be the one selected (see point 1).

Material and configuration.
Allows you to adjust the configuration parameters of the different elements that make up the installation.

Access profiles and cards.
Allows the management of users and credentials who will have access to the installation.

Monitoring. Monitoring of the status and events of the installation.

Tools: Firmware update, Back Up, ...

Favorites, shortcuts.

3 - Favorites

You can add favorites from the "edit bookmarks" option on the home page. This allows you to add bookmarks, which will then appear on the home page and in the side menu.
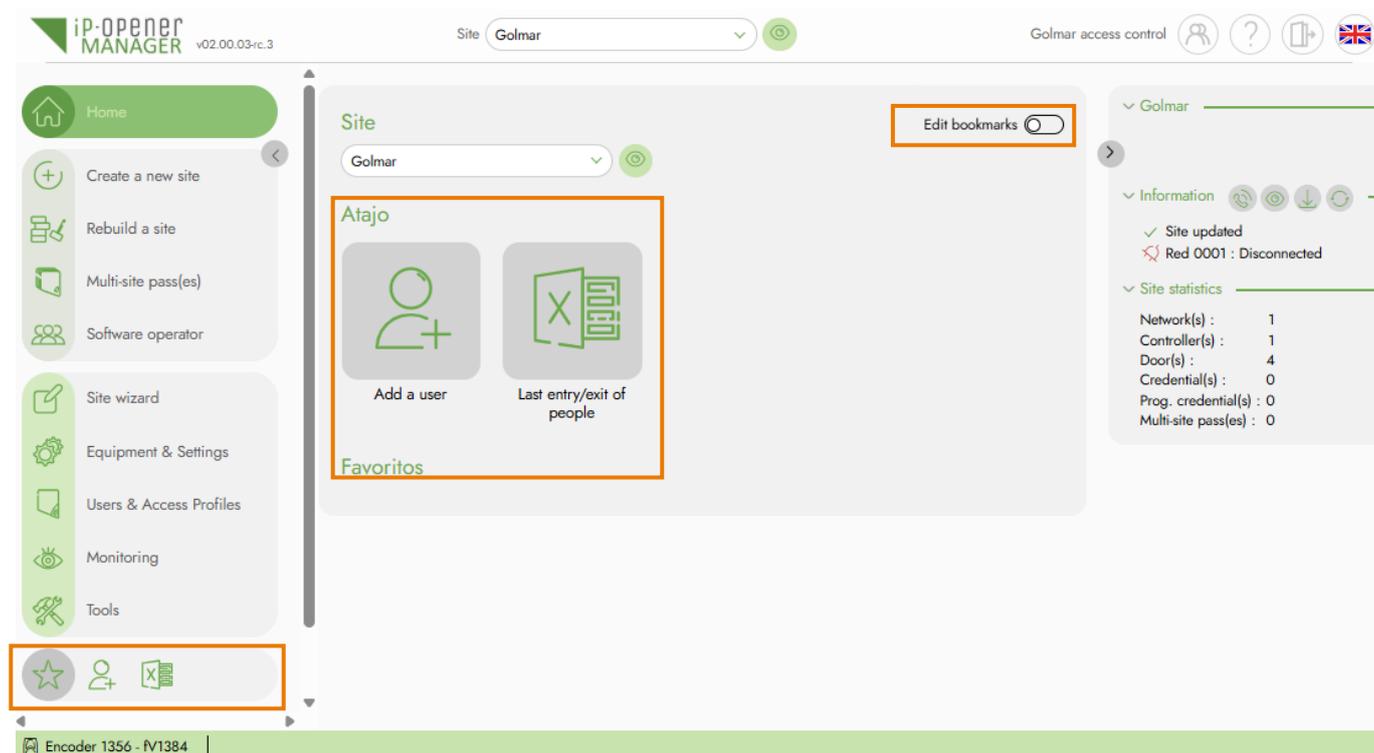
See below the available options when adding favorites (shortcuts):

Name	Favorites	Enter a name to identify the shortcuts.
Push buttons size	Large	Choose the size in which you want the icons to be displayed.
Allocated to users		Check to display favorites on the home page as well.
Displays on homepage	☑	
> Add and manage menus		Add shortcuts to certain functions (add a user, add an access profile or events).
> Assign external links		Add a shortcut to execute a link (web address, Windows program, ...).
> Assign doors and/or groups of doors		Generate commands for manual door activation.
> Assign exits and/or groups of exits		Generate commands for manual output activation.
> Assign input and/or input groups		Generate commands for manual input activation.
> Assign reports		Add shortcuts to generate and download reports.*

It is possible to generate and send reports by email on a recurring basis (if you are interested in this, please contact your administrator (installer)).

4 - Information and status of the selected installation
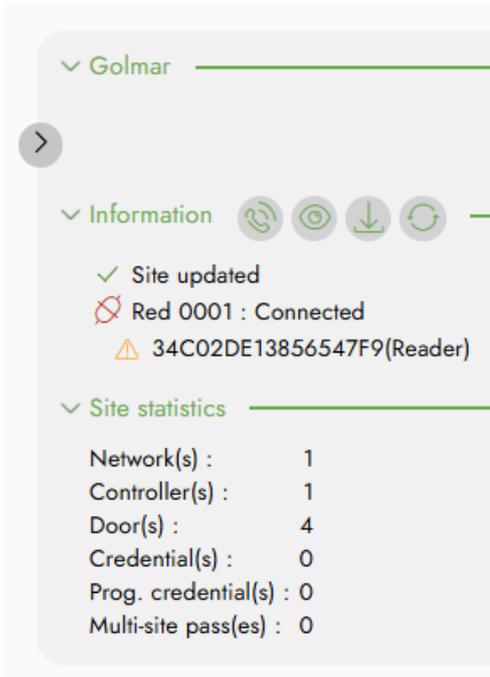
Pay special attention to ensure that the system
has communication with the server

5 - Language, user, and logout options.

4. ACCESS PROFILES AND TAGS

4.1 Manual registration

Select one of the access profiles created by your site administrator.For example, in this case "Access profile 0001" and click on "Add user".
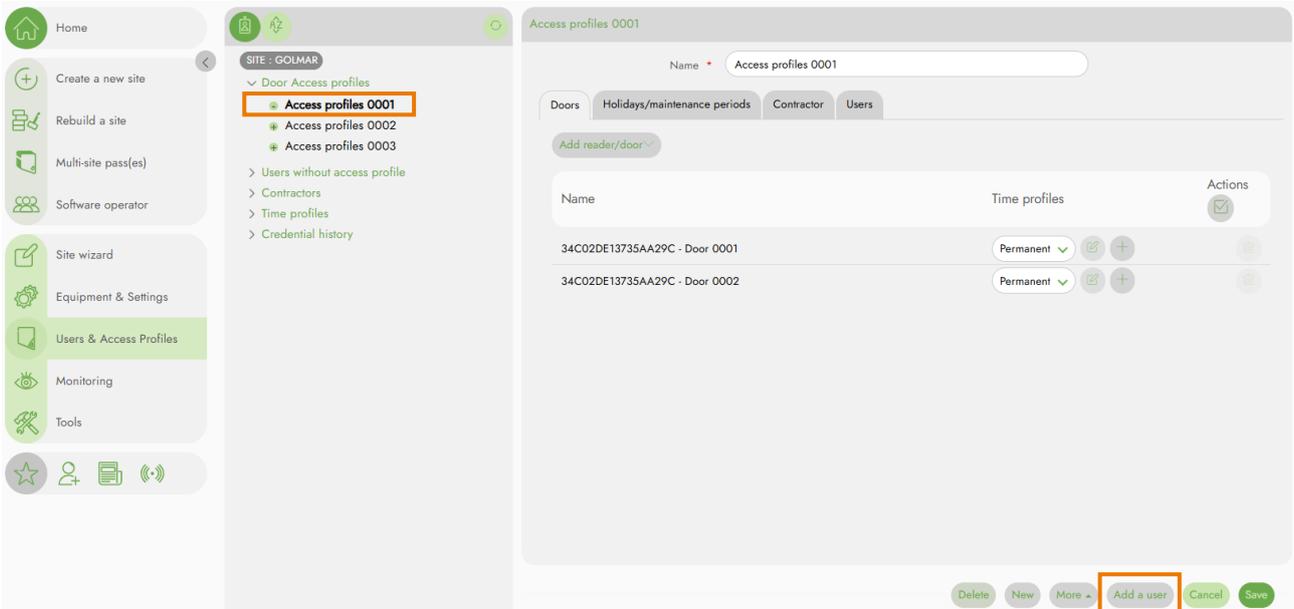
This will allow the user or users to be created to access the doors enabled in profile 0001 (door 01 and door 02).

This will allow the user or users to be created to access the doors enabled in profile 0001 (door 01 and door 02).

Fill in the personal data to identify the user to be registered.

Finally, add identification title(s) with which the user can validate their access.

Next, you can see the correspondence between the identification titles shown in the software and the Golmar references.

ID TITLE	REFERENCE	ID TITLE	REFERENCE
125KHz keyfob	PROKEY ID, TAGKEY ID	MIFARE Classic® keyfob	ISOPROX, KEYPROX SE
MIFARE Plus® keyfob	CARDDOOR MF+, TAGDOOR MF+	Telecontrol 1356-2/4 buttons	GM-WEIPOP
125kHz remote control - 2/4	-	MIFARE Classic® remote control	GM-WEIPOP MF
Telecontrol 1356 - 2 buttons	-	Access code	-
Vehicle number plate	-	Third-party credential (hexadecimal)	-
Third-party credential (decimal)	-	QR Code	-

With proximity credentials, it will be possible to register the credential by typing the number printed on the credential or by bringing the card or key fob close to the GM-USBIPOP encoder.

If you bring the card or key fob close to the GM-USBIPOP encoder, the serial number will be registered.
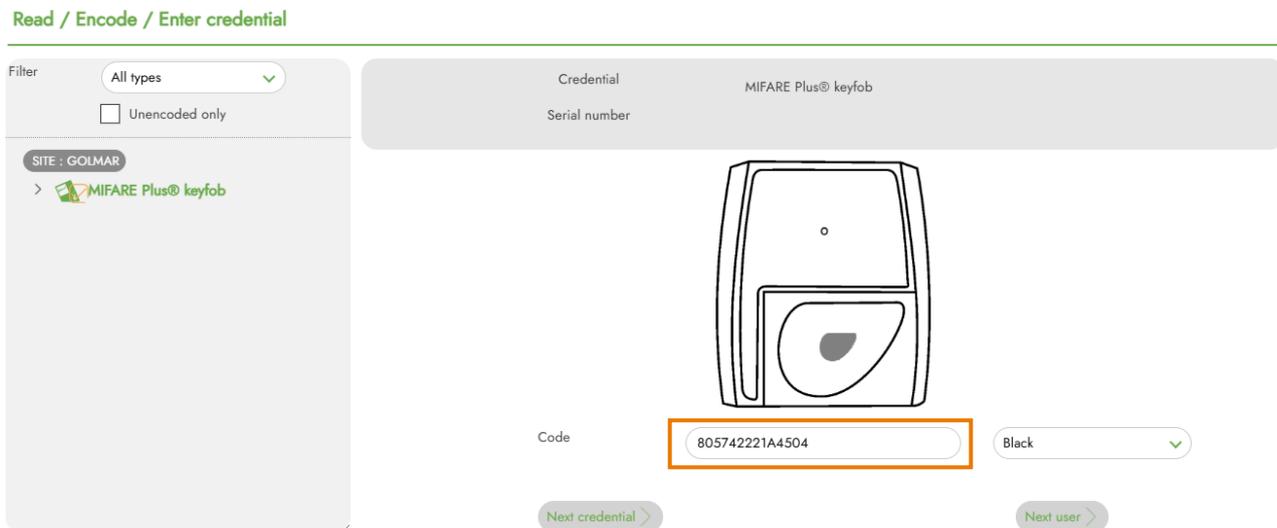
To use the programmer, it must be connected to a USB port on the computer and detected by iP-Opener Manager (requires the tool (plugin) to be installed, which can be installed from the browser status bar).
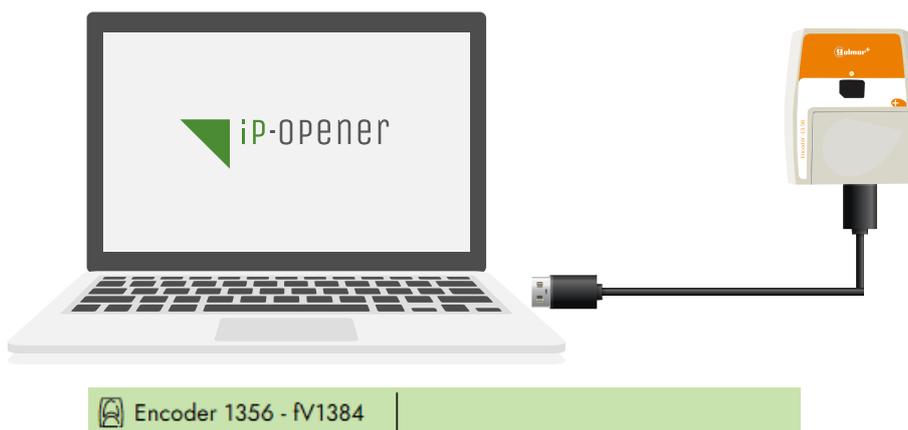
For PIN credentials (access code), it will be possible to set the access code or select "Automatic assignment" so that the software assigns a code to the user.
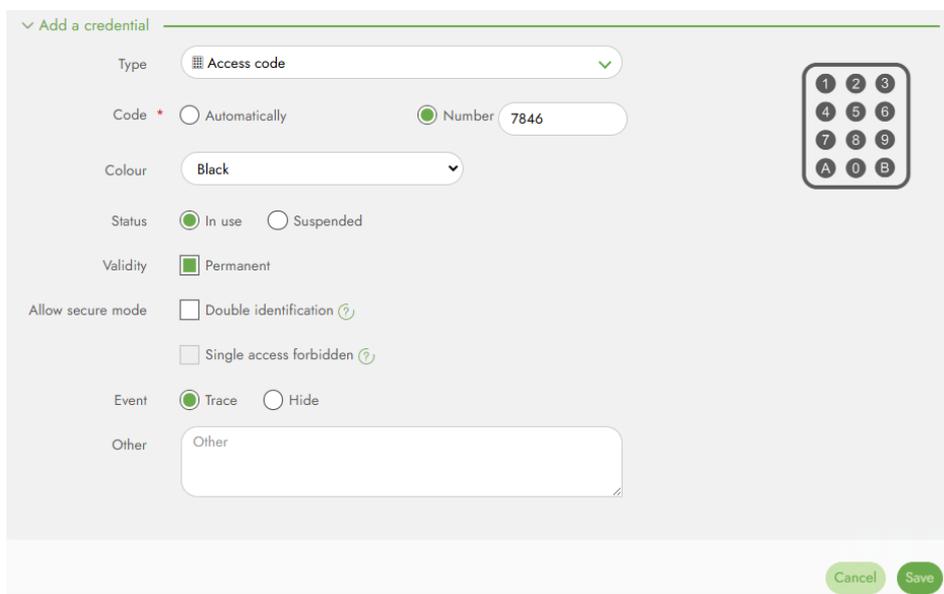
4.2 Create a new access profile

The creation of access profiles makes it easier to subsequently create users.

When generating the profiles, we indicate which doors are valid for access. In this way, later you will only need to associate the access profile with the users. If it is necessary to create a new access profile, proceed as follows:

1. Click on "Door access profiles" and then "Add an access profile":
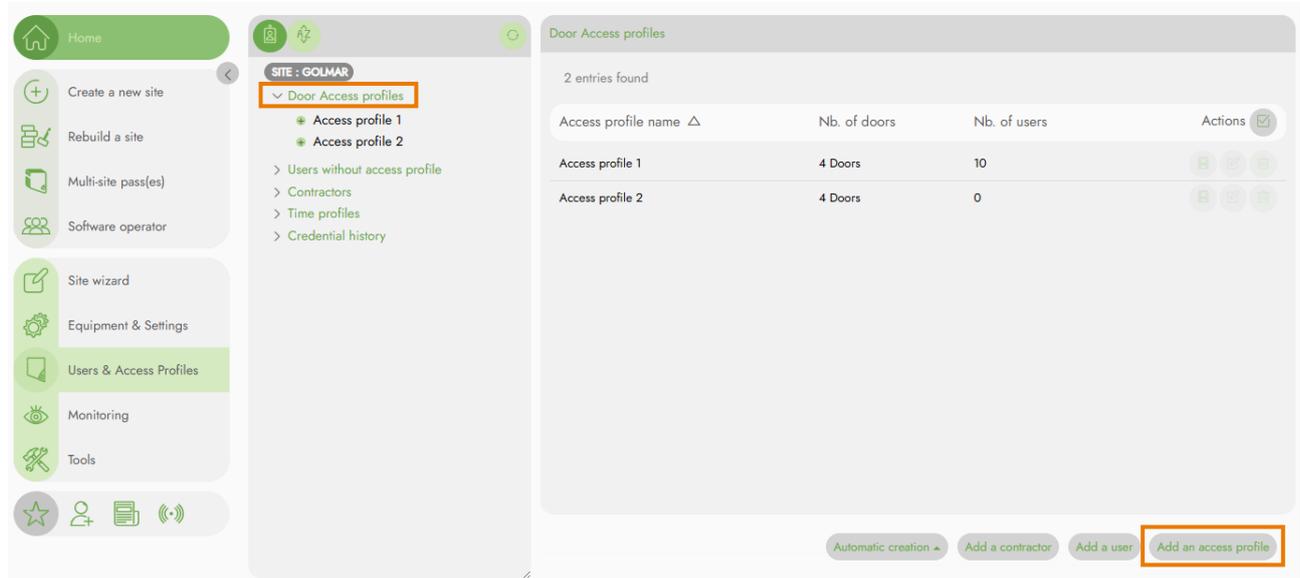
2. Select the doors that users of the profile will be able to use.
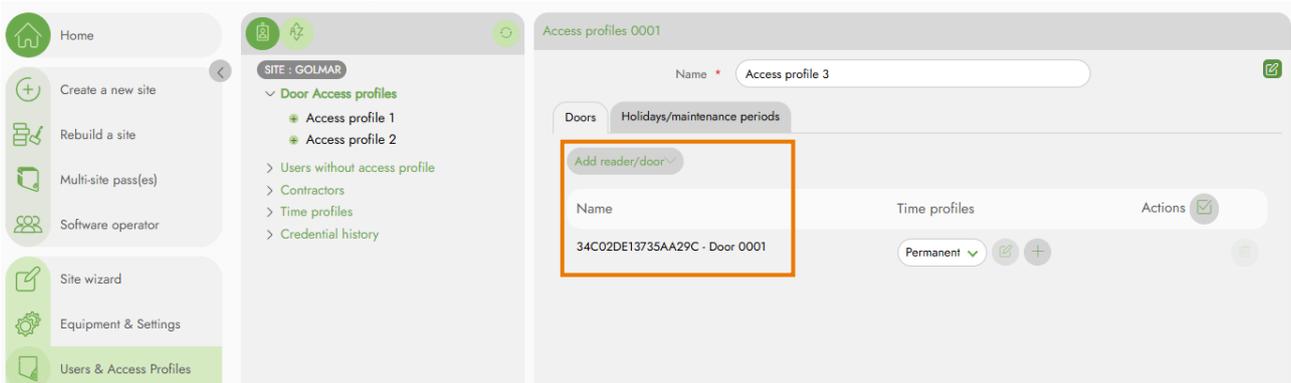
3. It is now possible to start creating users who will be able to access the selected door(s).
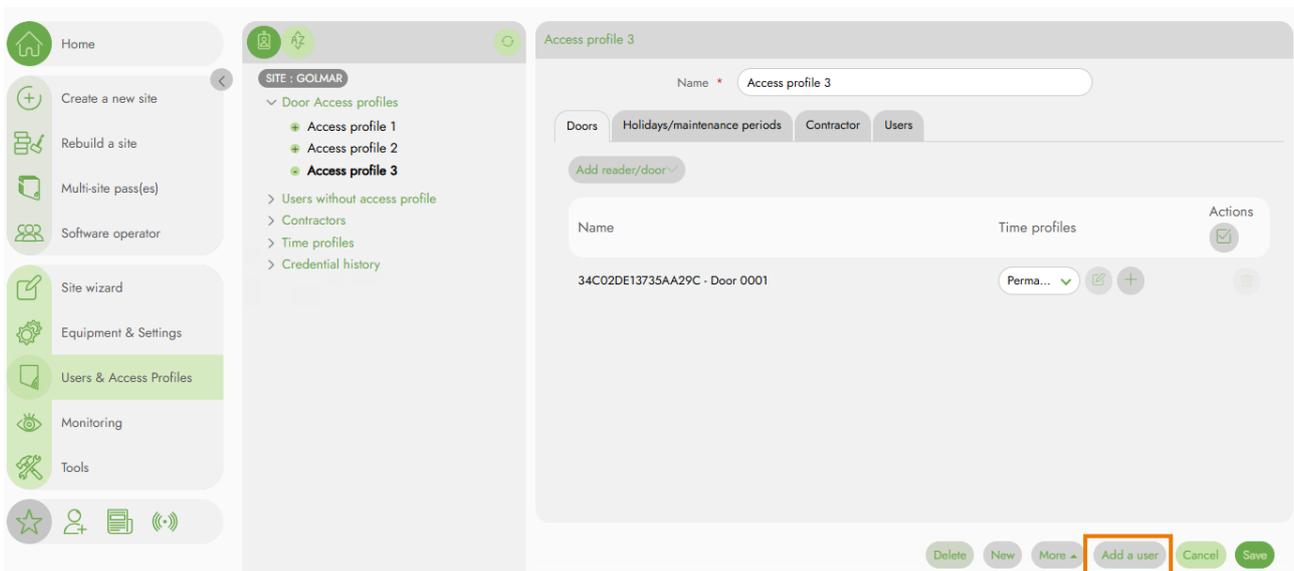
4.3 Automatic registration

In those installations where there are a large number of users to register, it is possible to generate users automatically. To do this, select an access profile and click on the "More" option and then "Automatic person creation".
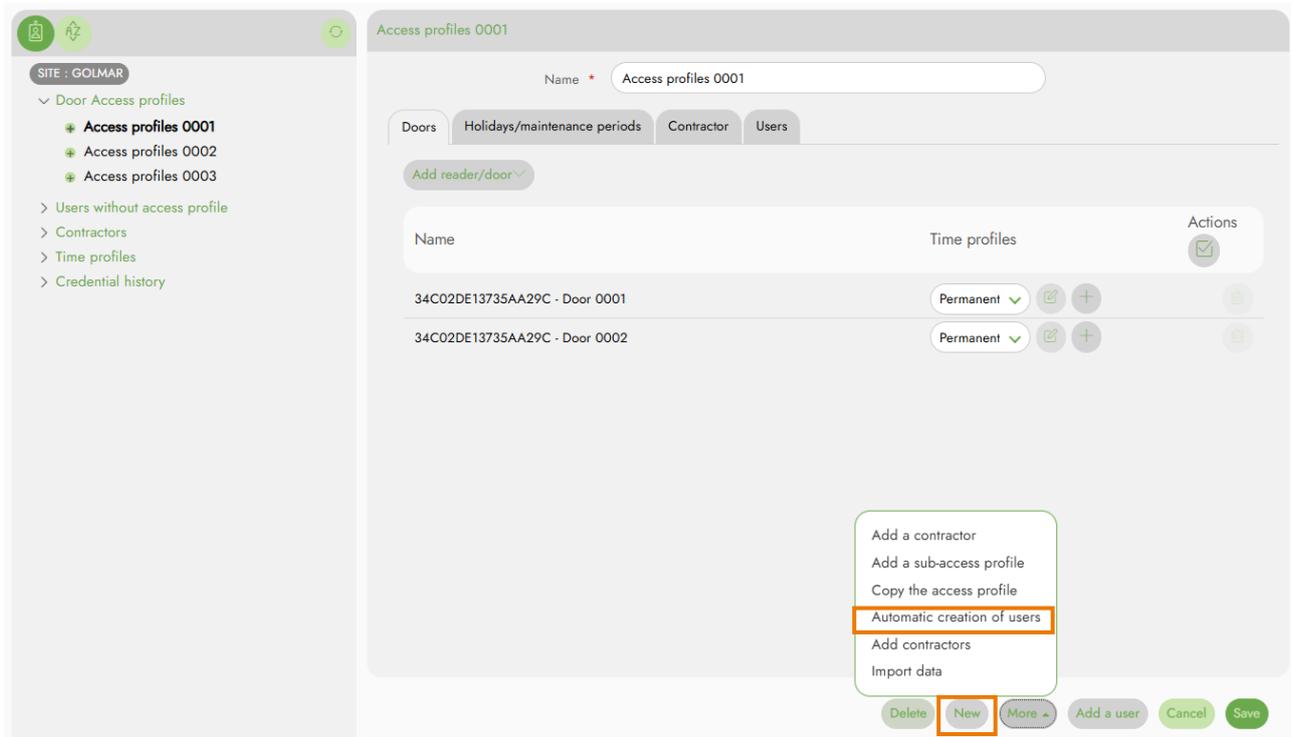
In the pop-up window, you can set the criteria for automatic generation.
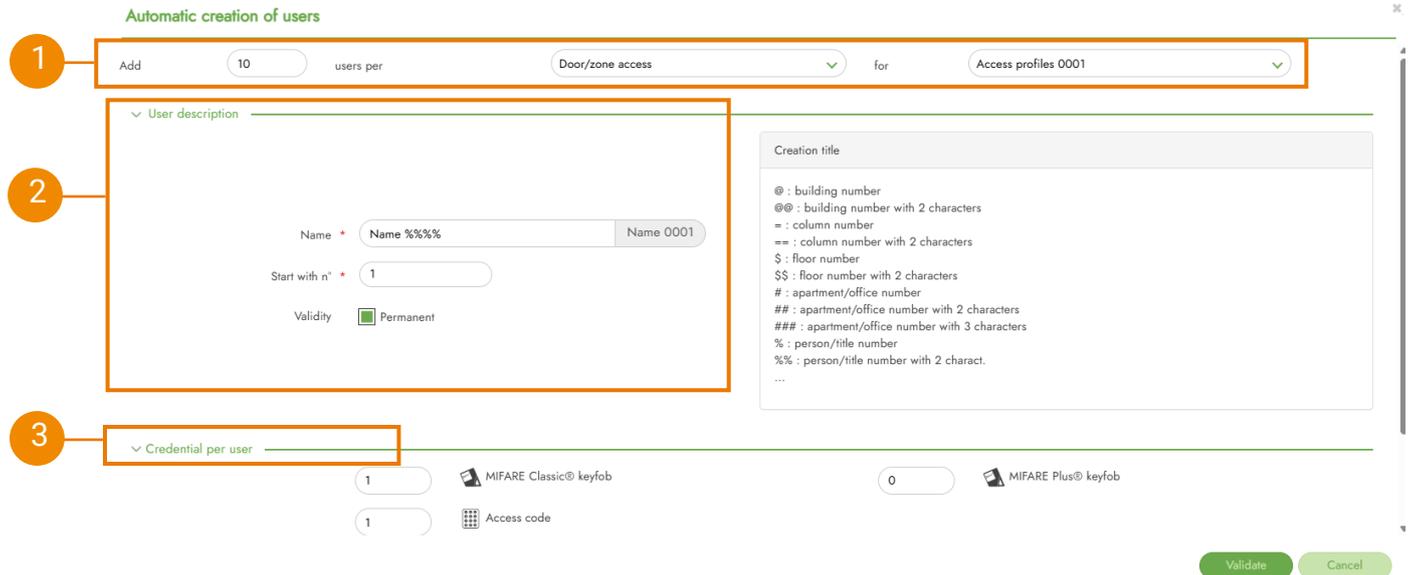
1. Indicate the number of users to generate and the access profile to assign to them.

2. Specify a surname (name) depending on the characters (see creation legend) that accompany it; it will be completed in one way or another. Set which value the creation should start with and whether the users will have permanent (indefinite) access. For example, in the configuration shown, it will be named "User" and will start with "0001". If "Resident %%" is indicated, it would be named "Resident" and would start with "01".

3. Define which credentials they will have and how many. Once all of the above has been set, click "accept".

4.4 Bulk registration

Another way to create users is to register them in bulk by importing them from an Excel file. To do this, follow the steps indicated below.

1. Click on "Automatic creation" and then "Import data":
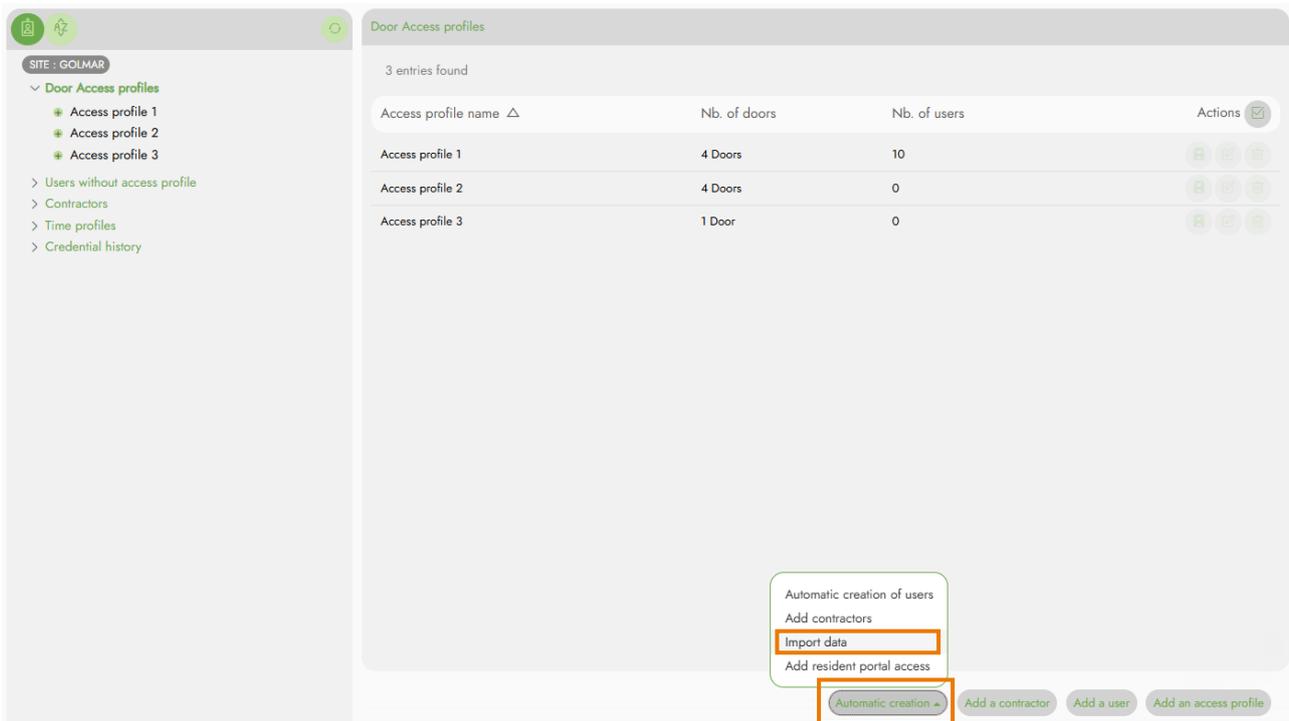
2. Download the file to be completed by clicking on "Get the file to complete".
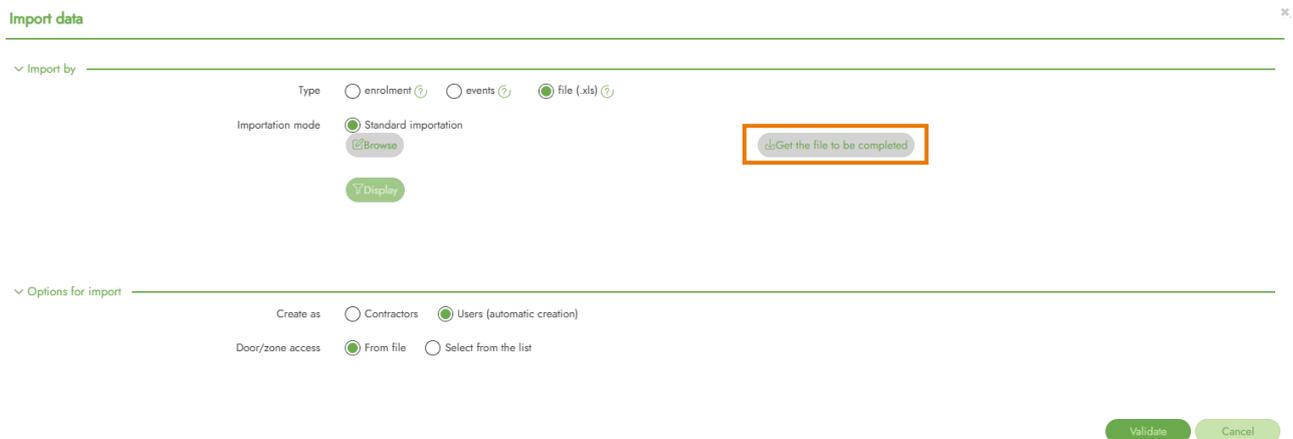
3. The first row will be completed as an example.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Code	Credential type	Lastname	Firstname	Number	Address	Postal code	City	Telephone	Email	others	Door access	Lift access
2	ABCD0001	Proximity token 1356 (202)	LastName1	Name1	num001	Lg 44 Market Street	2001	Sydney	+61 4 0000 0001	email1@domain1.com	test	Access profile 0001	Floor access profile 0001
3													
4													
5													
6													
7													
8													
9													
10													

4. Fill in at least the columns marked in yellow: "Code", "Credential type", "Surname", "Number" and "Door access".

Code	Credential type	Lastname	Firstname	Number	Address	Postal code	City	Telephone	Email	others	Door access	Lift access
2436	Access code (211)	John		num001							Access profile 0001	
7591	Access code (211)	Sarah		num002							Access profile 0002	
3768	Access code (211)	Harry		num003							Access profile 0001	
1405	Access code (211)	Emily		num004							Access profile 0001	
80555B626C3704	Mifare+ SE SL1 (212)	Thomas		num005							Access profile 0001	
F09F1084	Proximity token 1356 (202)	Jessica		num006							Access profile 0002	
80555B62694A04	Mifare+ SE SL1 (212)	Jack		num007							Access profile 0002	
3524	Access code (211)	William		num008							Access profile 0002	
55567	Access code (211)	Sophia		num009							Access profile 0002	

For proximity credentials, it is possible to type them in or import the user and then encode the cards/key fobs using the encoder.

5. Once the file is completed, import it by clicking "Automatic creation" and then "Import data".

This time click "Browse", select the completed file and click "Validate".
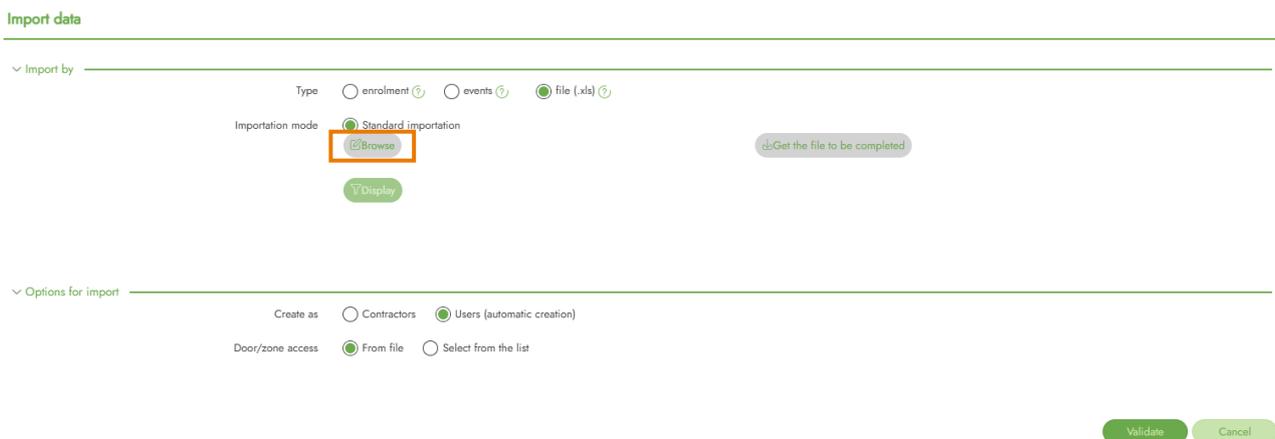
6. The users will be imported.
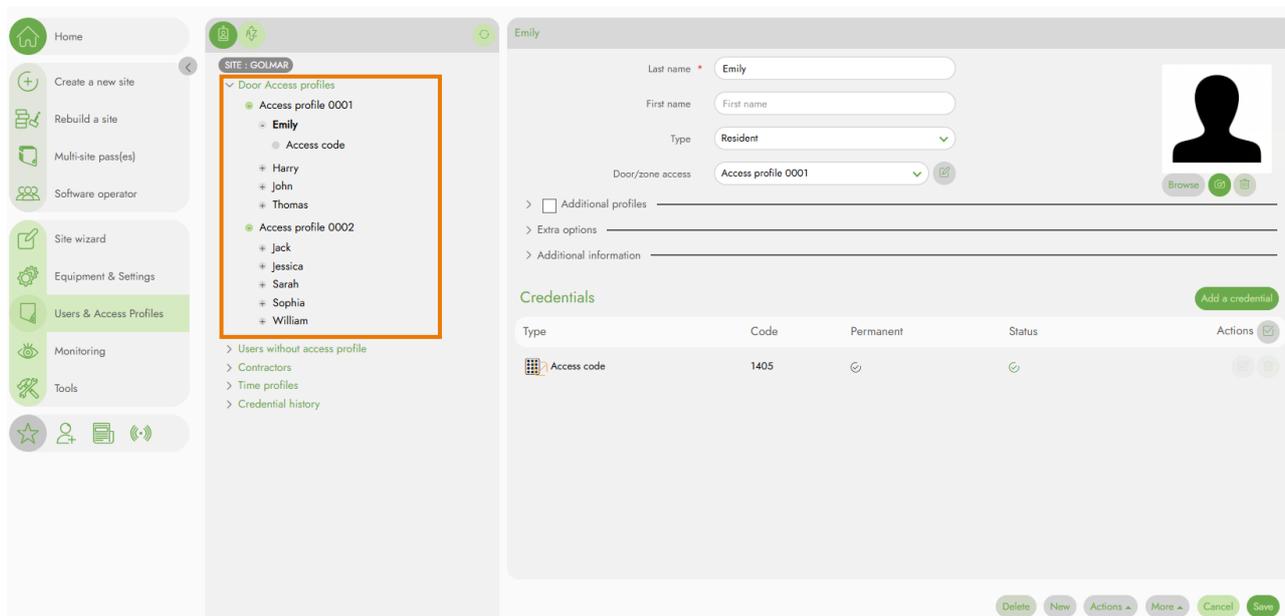
4.5 Additional information

Users without access profile, if users have been generated and not assigned to an access profile, they will appear in "Users without access profile". This generally applies to specific functions such as "Visitor management" and "Facility reservation management".

Contractors, it is not recommended to work with this feature.
Function intended to register users from service companies (cleaning, building maintenance, etc.) and not just a single person. The credentials work and are registered in the same way, only they are displayed differently. They simply appear separately in the "ICT" tab of the access profile.

Credential history, allows you to check the credential history: which user they belong to, when they were generated and deleted. Note that in reports it is possible to download reports related to credentials such as: "user list" or "unused credentials" which can help to have better management and control of users.

5. TIME PROFILES

5.1 Key time profiles

If it is necessary to limit access by time, a "Key time profile" must be created; below is an explanation of how to create and configure a key time profile.

Go to "Time profiles" in the "Users & Access Profiles" menu.
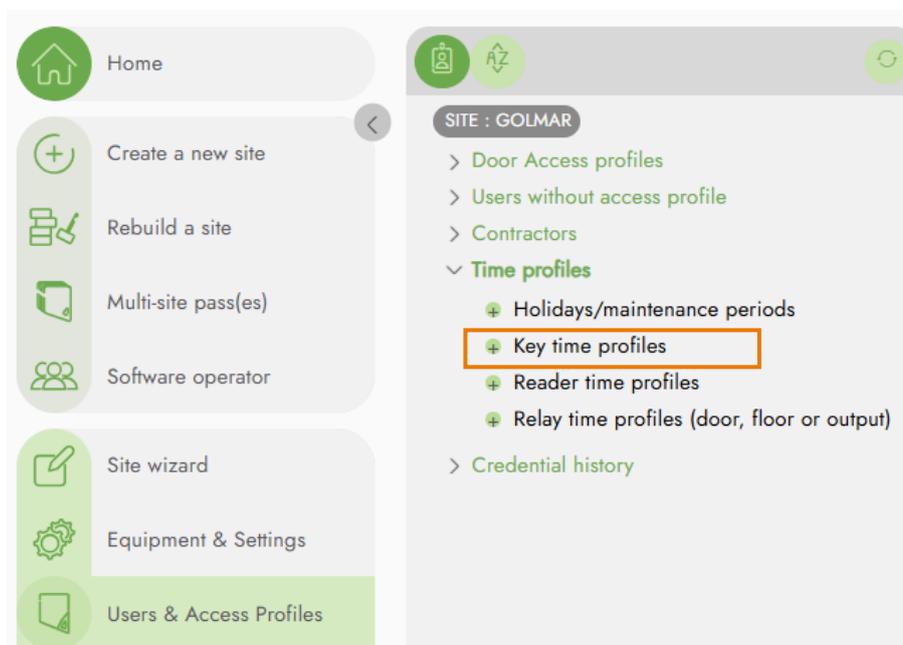
Click on the "add an access schedule" option

1. Enter a name to identify the schedule you have created.

2. Choose whether you want the authorized schedule (green) or unauthorized schedule (red) to be shown by default.

3. If you are going to set an authorized time range, select the green color code and check or select the daily and hourly boxes to authorize. If, on the other hand, you are going to set an unauthorized range, select the red color code.

In the example, access from 9:00 a.m. to 11:30 a.m. has been authorized and identified as gardener.

If you want to be more specific and define the schedule in smaller intervals, do the following:
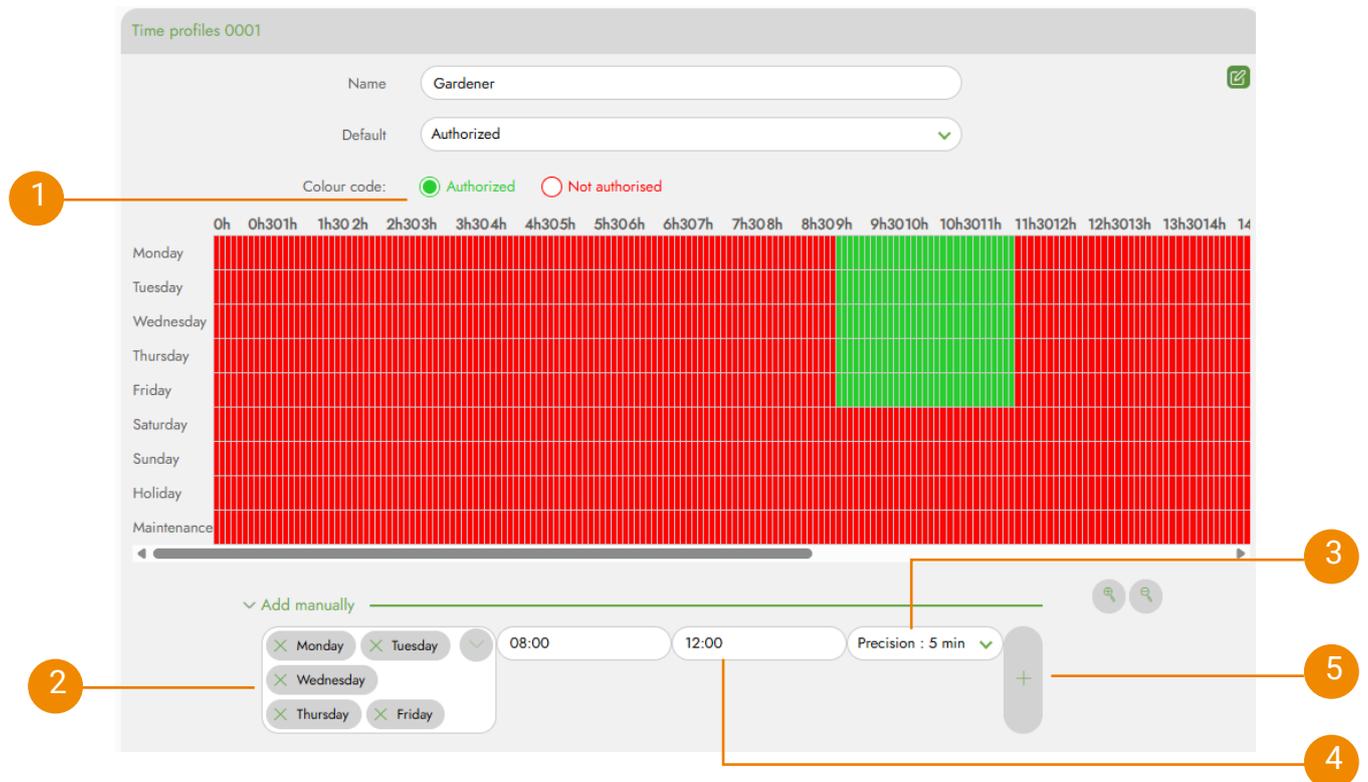
1. Select the code corresponding to what you want to define: green (authorized), red (not authorized).

2. Manually add the days that the schedule will affect.

3. Indicate the precision with which you want to set the range (5, 10, 15 or 30 minutes).

4. Set the start and end time.

5. Click the "+" symbol to insert it into the quadrant.

Once the schedule is completed, it must be assigned to an access profile. Below is an example:

In the installation, two access profiles have been created: "Gardener access profile" and "Owners access profile". In the gardener profile, this user only has access to door 1 and during a schedule, the one previously defined as "Gardener Schedule".
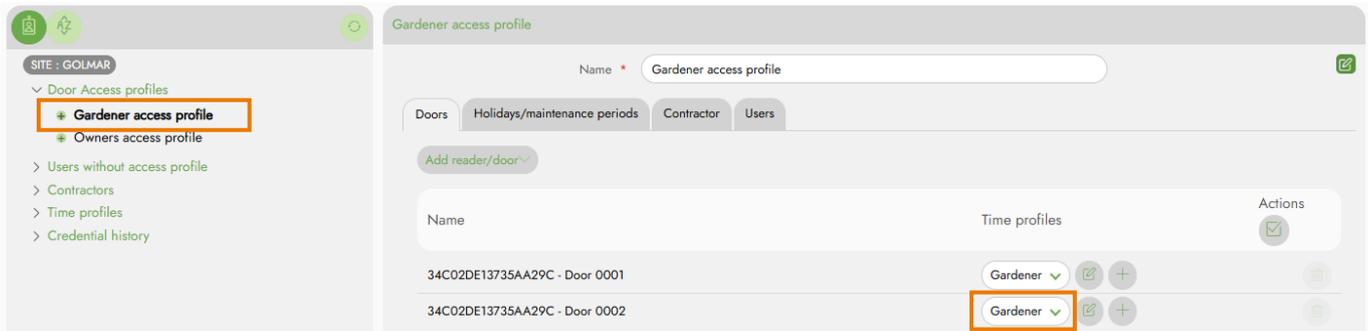
Whereas the owners profile can use both doors of the facility at all times (at any time).
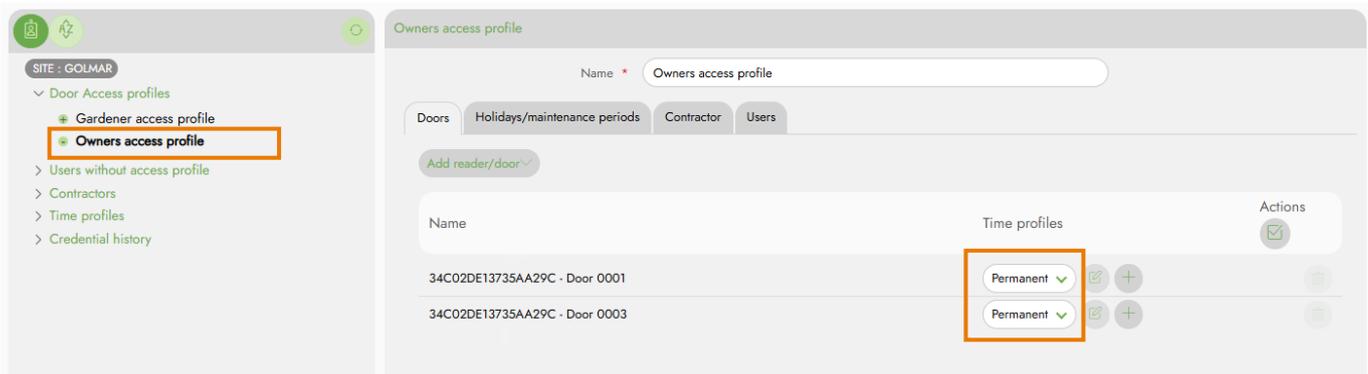
5.2 Holidays

In the previous schedule, the "holiday" has been set as unauthorized. To inform the system which days should be treated as holidays, go to the menu Schedules\Holiday/Working Periods.

Click on the "add a period" option
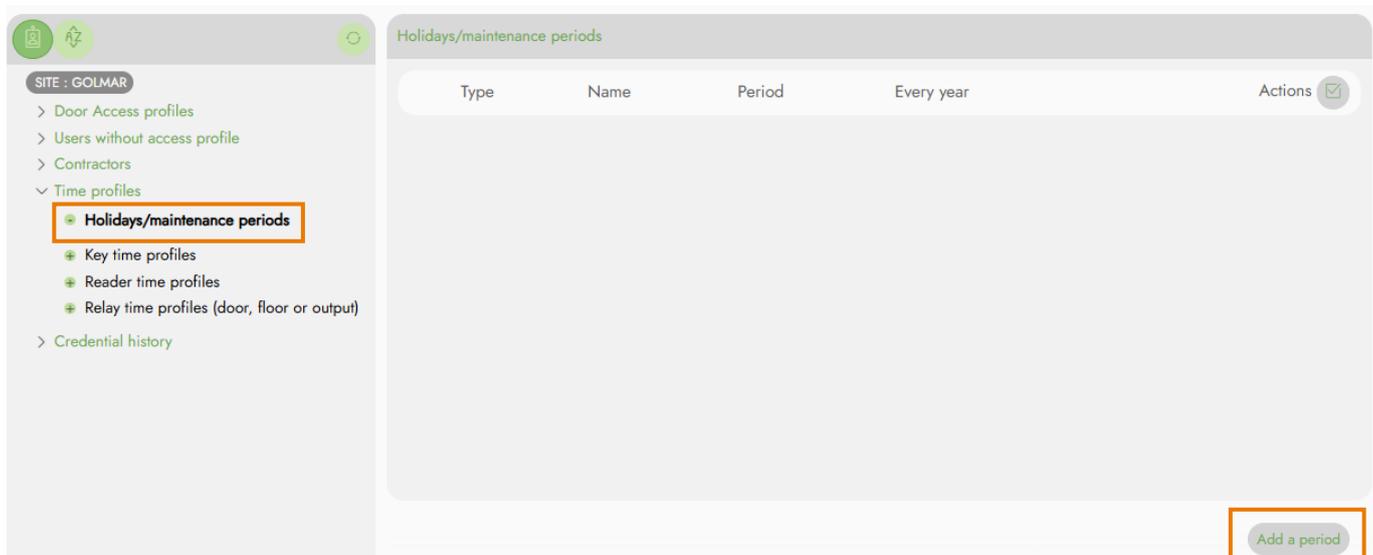
Name the holiday so you can identify it and select the date of the holiday. If it is an annual holiday, select repeat every year.

Period 0001	
Name *	25th december
Type	Holiday
Begin	2026-12-25 00:00:00
End	2026-12-25 23:59:00
	☑ Repeat every year

Finally, go to the user profile to which you want to assign the holiday schedule. Select the "Holiday/Working Periods" tab and click on the "Add a period" option, add the holiday or holidays created.

SITE : GOLMAR

∨ Door Access profiles
   ⊕ **Gardener access profile**
   ⊕ Owners access profile
> Users without access profile
> Contractors
> Time profiles
> Credential history

Gardener access profile

Name *   Gardener access profile

Doors   **Holidays/maintenance periods**   Contractor   Users

Period   ♟ **25th december**

Add a period ∨

Delete   New   More ▲   Add a user   Cancel   Save

6. MONITORING

6.1 Monitoring

You can monitor in real time what is happening in the facility. To do this, go to the monitoring section.

Events

Display   Download   Archives   Global settings   Settings

> Filters

Result limited to   30   Export   Purge   New tab

Date / Hour	Event	Element	Information		Identifier	Priority
2026-03-06 10:31:59	Access by single credential	Controller n°1 - Door 0002 Reader 0002 Access profiles 0001	👤User name 0005		E98A5EE0	5
2026-03-06 10:31:53	Access by single credential	Controller n°1 - Door 0001 Reader 0001 Access profiles 0001	👤User name 0001		805742221A4504	5
2026-03-06 10:31:47	Access by single credential	Controller n°1 - Door 0001 Reader 0001 Access profiles 0001	👤User name 0008		4252	5
2026-03-06 10:31:39	Access by single credential	Controller n°1 - Door 0001 Reader 0001 Access profiles 0001	👤User name 0007		2131	5
2026-03-06 10:31:31	Access by single credential	Controller n°1 - Door 0003 Reader 0003 Access profiles 0001	👤User name 0006		E99A2A10	5
2026-03-06 10:31:24	Access by single credential	Controller n°1 - Door 0002 Reader 0002 Access profiles 0001	👤User name 0004		E98353E0	5

In monitoring, everything with a priority level of 5 or higher will be displayed. You can display non-visible events as follows:

Select the "Settings" tab, check the event you want to activate or check the "surname" box to activate the group of events to be activated, then set the priority level to "5 normal" or higher and complete the process by clicking "save".
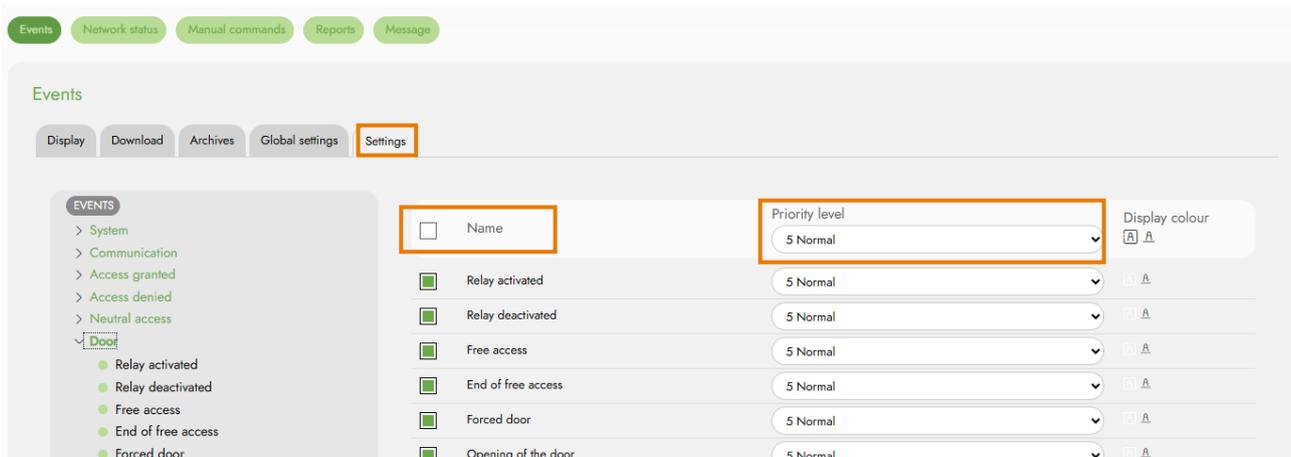
In the "View" tab it will be possible to customize the monitoring events.

1. Filters, allows you to define which events should appear in the monitoring. These can be filtered by different factors: date, event, controller, ...
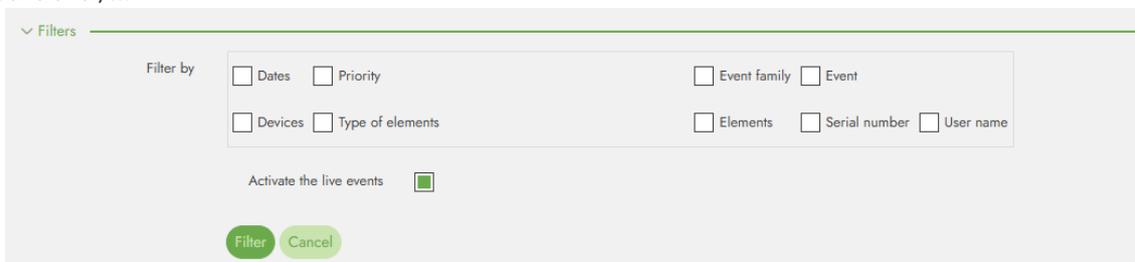
2. Result limited to, is used to set how many event lines will be kept on the monitoring screen.

3. Export, allows you to download the events on the monitoring screen as an Excel file.

4. Empty, allows you to delete events.
It is possible to delete all events and keep the most recent ones (by default the last 30 days) or delete specific events (by selecting them using the filters).
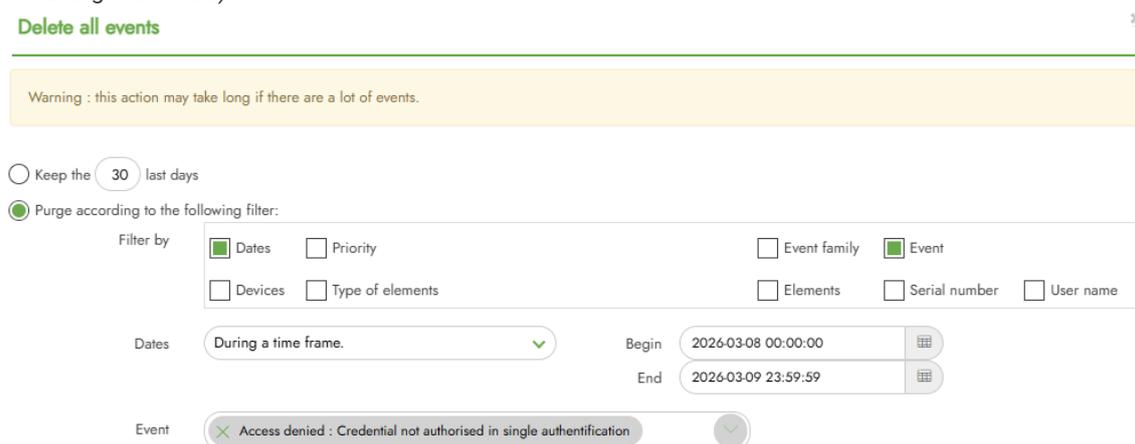
5.   New tab, opens the monitoring screen in a new tab (window).

This function is recommended for using two screens, one to continue managing the facility and the other to continue monitoring it.

6.   Columns, allows you to choose what information should or should not appear in the monitoring columns.

"Downloads" tab, this option is intended to be used only in cases where communication between the controller and the cloud has been lost, as it allows you to import the controller's information to the cloud.

Each controller stores up to 20,000 events. When the network connection is restored and the controller reconnects to the server, it is possible to retrieve from the controller the events that were not transferred to the cloud during the period when there was no connection, by clicking "download".

6.2 Reports

From the "Reporting" tab in monitoring, it will be possible to download (predefined) reports.

Name	Description	Selection	Actions
Credentials to be renewed	List of credentials expired or expiring in less a defined period.	Period	
Certificates to renew	List of expiring certificates		
Unused credentials	List of credentials without "Authorized access", in the last X days	Time limit	
Visit	List of visits	Period, Status	
List of users.	List of users and their credentials	Access profiles, User group, Architecture	
Access permissions to doors	List of authorised doors per access (with time profiles)	Door access profiles	
Access permission to floors	List of authorised floors per access (with time profiles)	Floor access profiles	
Operator form	User information, list of credentials and their access permissions.	User name	
Event export	List of the site events	Event	

For example, to download an "events" report, simply click on the icon [XI]. Before generating the report, the software may ask you to define certain information, such as the date.

Create report

Filter bydate   2026-03-09

Export   Cancel
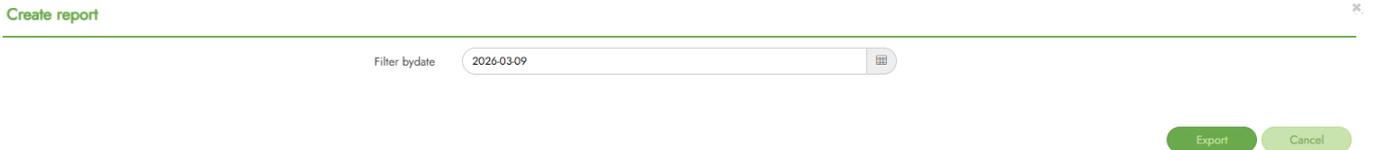
The software will download the file in Excel format (.xml).

List of people who entered the site on 2026-03-04

First in	Last out	Inner presence time	Last name	First name
2026-03-04 16:50:27	2026-03-04 16:50:27	00:00:00	User 3	
2026-03-04 16:49:58	2026-03-04 16:49:58	00:00:00	User 4	
2026-03-04 16:49:51	2026-03-04 16:49:51	00:00:00	User 5	
2026-03-04 16:49:55	2026-03-04 16:49:55	00:00:00	User 6	
2026-03-04 16:50:04	2026-03-04 16:50:08	00:00:04	User 1	
2026-03-04 16:48:04	2026-03-04 16:50:15	00:02:11	User 2	

6.3 Manual controls

If required, the administrator can remotely activate the relay of the doors or system elements, allowing access or activation of the element manually.

NOTES

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

.................................**END USER MANAGEMENT**...

....

NOTES

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

NOTES

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

END USER MANAGEMENT...

....

NOTES

golmar

we take care of your home