



iP-OPENER

CONFIGURATION



INSTALLATION MANUAL

www.golmar.es
golmar@golmar.es

iP-OPENER CONFIGURATION REV.0126 | ENGLISH

TABLE OF CONTENTS

1. INTRODUCTION.....	3
2. ACCOUNT CREATION	3
3. IP-OPENER HOME PAGE.....	4
4. START-UP.....	6
4.1 Site	6
4.2 Functions	6
4.3 Networks and controllers	7
4.4 Doors.....	9
4.5 Access Profiles.....	9
4.6 Cards (credentials).....	10
4.7 Read/Encode	10
5. USER AND ACCESS REGISTRATION	11
5.1 Manual Registration	11
5.2 Automatic Registration	13
6. TIME PROFILES	14
6.1 Types of time profiles	14
6.2 Key time profiles.....	14
6.3 Holidays	16
7. OTHERS	17
7.1 Backup	17
7.2 Supervision	18
7.3 Reports.....	19

1. INTRODUCTION

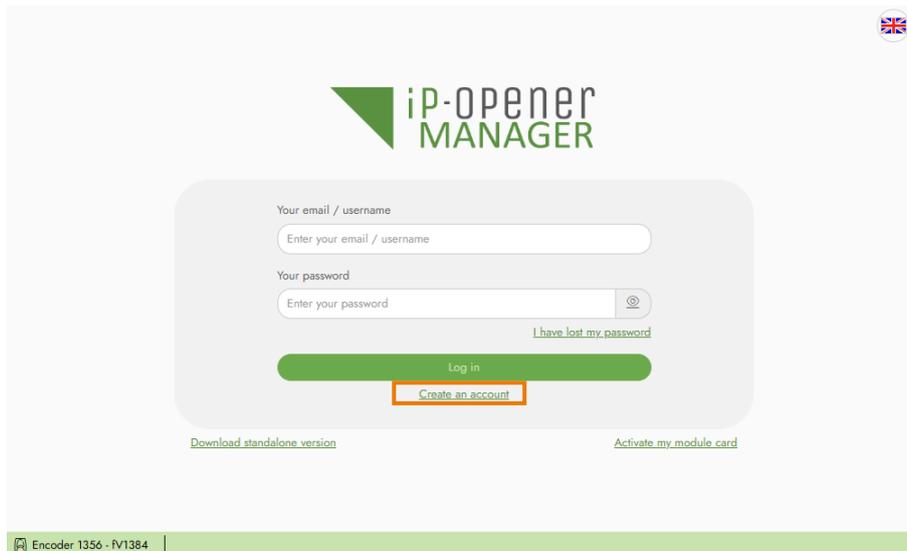
This manual gathers all the relevant information needed to start up an iP Opener system.

2. ACCOUNT CREATION

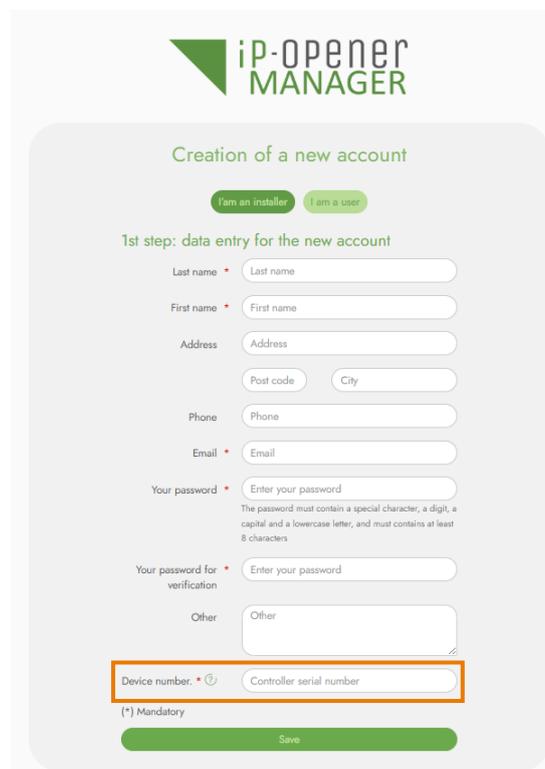
To begin the start-up process, a management account is required.

The installer can choose to create an account for that specific site or have a single installer account that includes all installations performed. In this second case, the installer could later grant permissions to users of the different installations (maintenance staff, concierge, ...) so they can access the settings either fully or partially.

To do this, go to www.ip-opener.com and select the "Create an account" option:



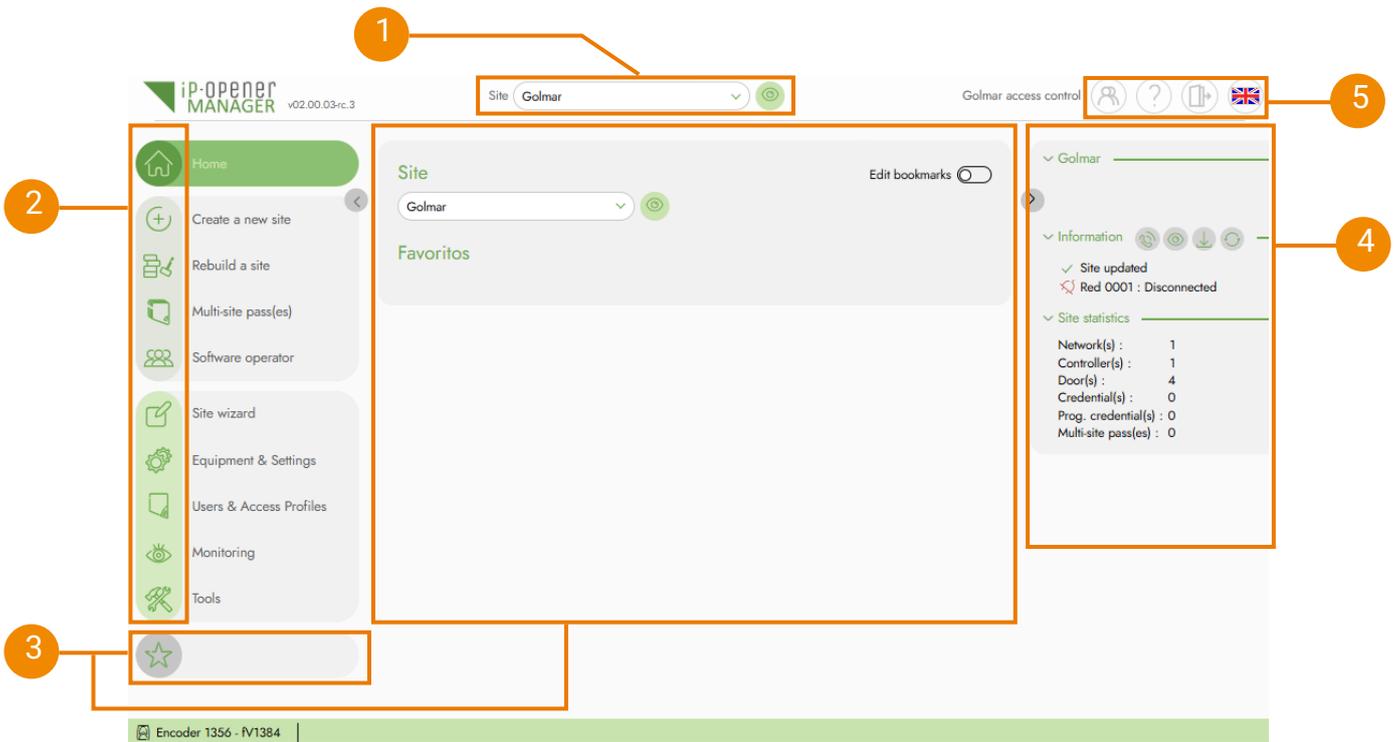
Next, fill in the fields in the following window (those marked with * are mandatory). 'In the "Login" field you must enter the ID of a controller (34C01DEXXXXXXXXXXX).'



'Once registered, you will receive an email at the provided address confirming your registration was successful.' After completing these steps, log in on the main access page (www.ip-opener.com).

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.

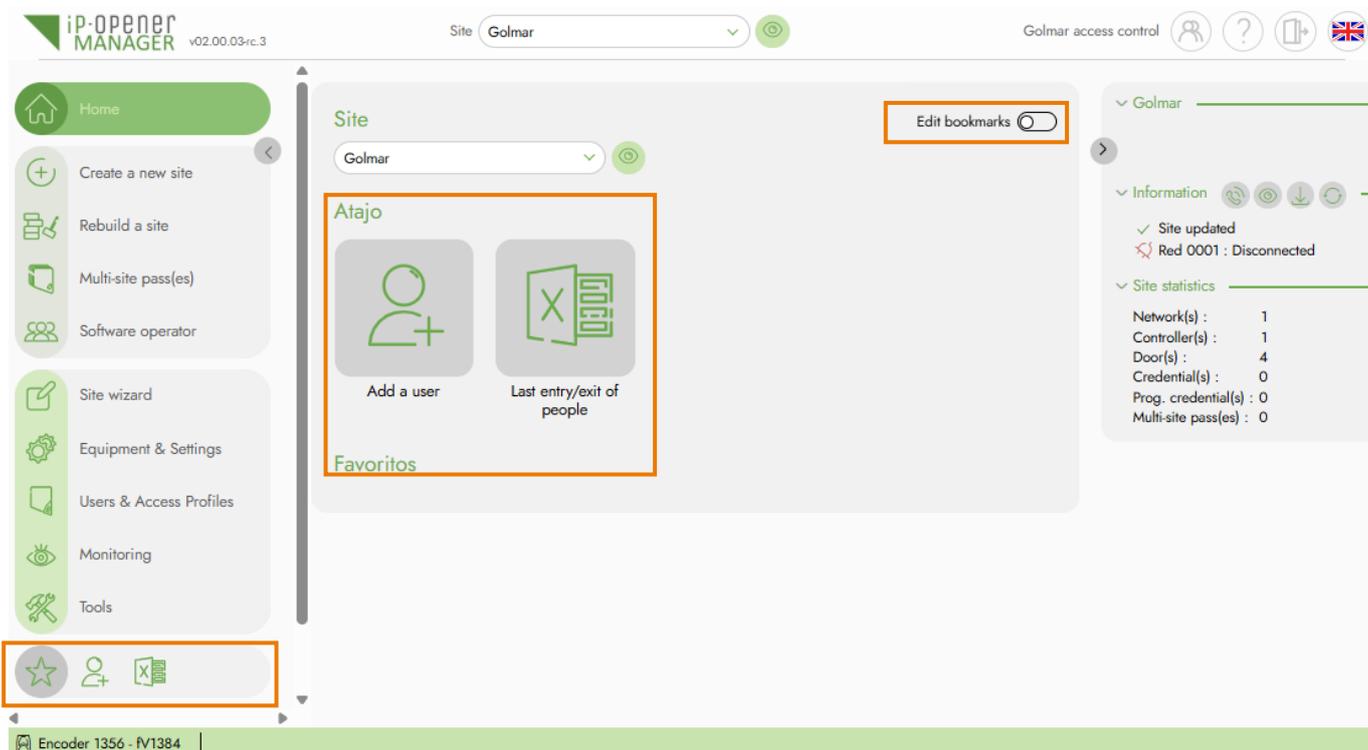


2 - Side menu.

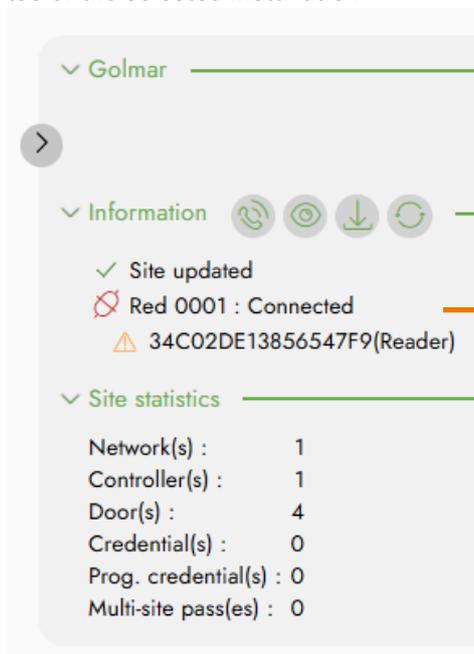
-  Home page.
-  Create new installation (site).
-  Rebuild a site (function for standalone installations).
-  Pass creation, a single card or credential allows access to different installations of the account.
-  Software access. Grant permissions to other users for full or partial use of the software.
-  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.



4 - Information and status of the selected installation



Pay special attention to ensuring that the network is connected and there are no pending FW updates.

5 - Language, user, and logout options.

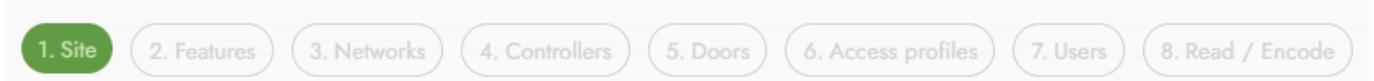


4. START-UP

To start up, click on the option "Create a new site" ,{



At this point, a wizard will start that will guide you through several stages until system configuration is complete:



*The configuration stages may vary depending on which functions were selected in step "2. "Functions" of the wizard.

4.1 Site

Define data that will allow you to later identify the installation (location, name, ...).

If you are not in the default time zone (UTC +01:00), select your region's time zone, then proceed through the wizard by clicking "next".

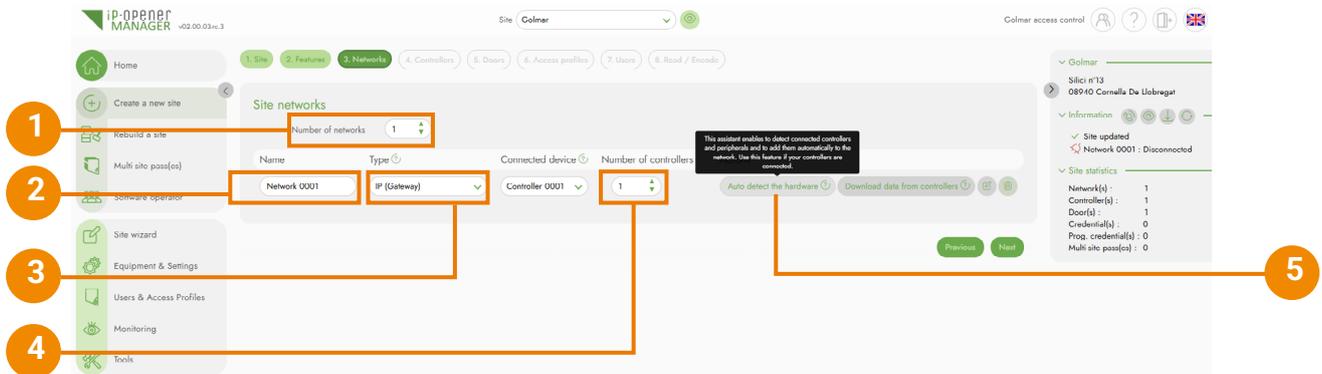
4.2 Functions

This manual outlines the steps to start up a configuration without additional functions, where the door relay contacts will be used. Therefore, it is not necessary to select any function; click "next":

If the installation requires more advanced configurations or includes additional elements, refer to the [iP Opener user manual](#).

4.3 Networks and controllers

1. 'Specify how many networks are needed.'
2. 'Assign a name to the network to be created that you can identify.'
3. 'Select the network topology.'
4. 'Indicate how many controllers are connected in your installation.'
5. 'Once all of the above is defined, click "Detect".'



NOTE: More than one network will be required when devices to be linked are located in different installations (do not share the same internet connection). In such cases, increase the number of networks and repeat this procedure for each one. This option allows management of companies with multiple locations.

Device search

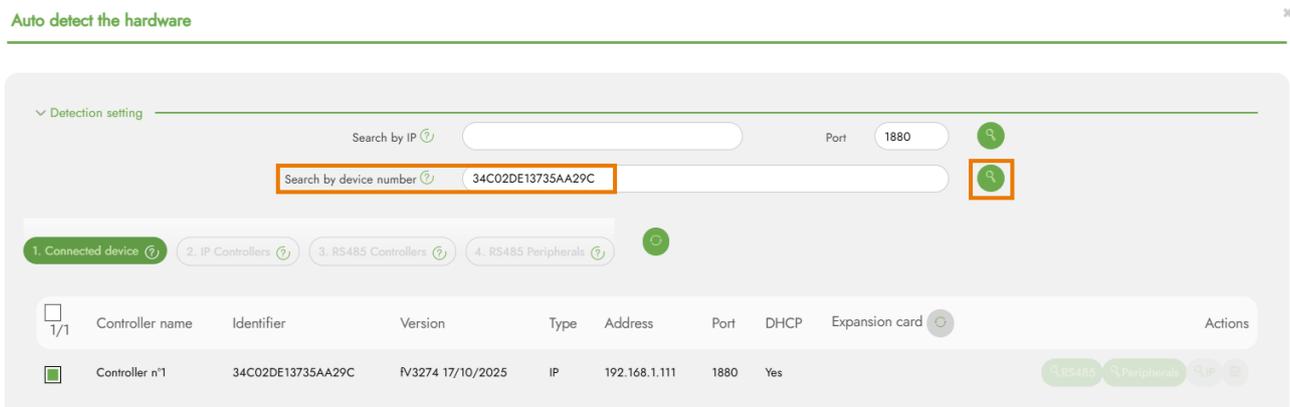
The device search consists of four phases:

- Phase 1: searching for an initial controller.
- Phase 2: searching for other controllers on the network.
- Phase 3, search for controllers connected via RS485.
- Phase 4, search for connected RS485 peripherals.

Once the required devices have been detected and added in any of the phases, you can complete the process by pressing **Close** and continue with the wizard'

Phase 1

Enter a controller ID in "Login Search" and press so that iP-Opener Manager can proceed with detection.

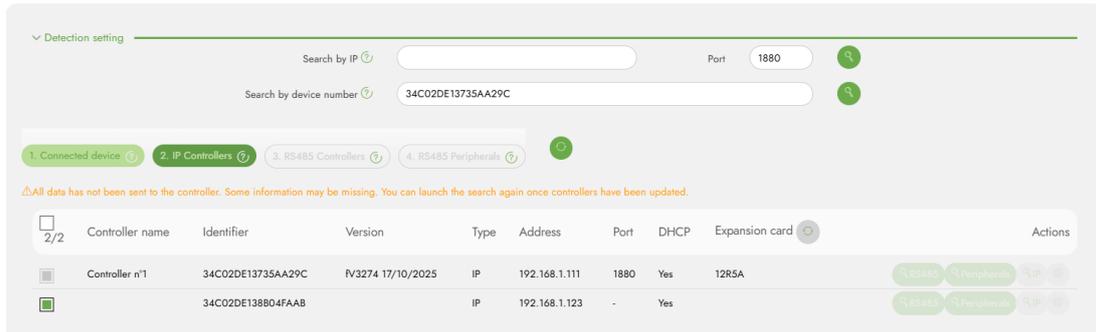


Select the detected controller and press **Next** to add it to the installation.

Phase 2

In phase 2 of device search, you will detect other IP controllers that are on the same network.

Auto detect the hardware



Phase 3

You will find controllers to add if the chosen connection topology is either "RS485" or "UTP + RS485".

Phase 4

In this final phase you will detect any connected "RS485 Peripherals" (output expander module GM-IPOP-10S-RS485 or input expander module GM-IPOP-10E-RS485).

Configuration of connected devices

1. Enter a name to identify each controller. Example: controller no.1.
2. Registered controller ID.
3. Controller model.
 - Central B2F/IP V2: For controllers with a 2SAFE bus and TCP/IP communication.
 - Central Wiegand /IP V2: For controllers with Wiegand protocol and TCP/IP communication.
4. Expander attached to controller. If an expander is attached to the controller, specify its model type:
 - 12 relays 5A. Reference GM-IPOP-EXP12S.
 - 12 analog inputs. 'Reference GM-IPOP-EXP12E.'
 - '4 Wiegand Doors.' 'Reference GM-IPOP-EXP4PW.'
 - '2 Doors (b2f).' 'Reference GM-IPOP-EXP2P.'
5. 'Doors.' 'Number of doors on the controller:'
 - 'GM-IPOP-1P.' '1 Door.'
 - 'GM-IPOP-4P.' '4 Doors.'
6. 'If there is any RS485 module connected and it was not added during device search, indicate its quantity in the "ES Cards" field and complete the details for the module to be added.'
7. Indicator tick for the controller that connects with the server.



4.4 Doors

Once the controller(s) have been added to the network, we can manage each of their doors.

1. Site 2. Features 3. Networks 4. Controllers 5. Doors 6. Access profiles 7. Users 8. Read / Encode

+ Door group

Doors of 34C02DE13735AA29C

Door name	Position	Door release time	Time profiles	Actions
34C02DE13735AA29C - Door C	1	5 sec	None	[edit] [add] [delete]
34C02DE13735AA29C - Door C	2	5 sec	None	[edit] [add] [delete]
34C02DE13735AA29C - Door C	3	5 sec	None	[edit] [add] [delete]
34C02DE13735AA29C - Door C	4	5 sec	None	[edit] [add] [delete]

By pressing you can adjust door settings such as: opening duration, relay operation mode (normal or reverse), set which reader will activate that door, ...

34C02DE13735AA29C - Door 0001

Name * 34C02DE13735AA29C - Door 0001

Position Num 1 Controller 34C02DE13735AA29C

Door release time 5 sec

Time profiles None

Reverse relay

Status Secured

> Reader

> Free access management

4.5 Access Profiles

Creating access profiles makes it easier to create users later on. When creating profiles, we specify which doors are valid for access. In this way, later on users only need to be assigned an access profile.

1. Site 2. Features 3. Networks 4. Controllers 5. Doors 6. Access profiles 7. Users 8. Read / Encode

Creation of door access profiles

Nb. of door access profiles 3

Name	Doors	Actions
Access profiles 0001	<input checked="" type="checkbox"/> 34C02DE13735AA29C - Door 0001 <input checked="" type="checkbox"/> 34C02DE13735AA29C - Door 0002	[edit] [delete]
Access profiles 0002	<input checked="" type="checkbox"/> 34C02DE13735AA29C - Door 0001 <input checked="" type="checkbox"/> 34C02DE13735AA29C - Door 0003	[edit] [delete]
Access profiles 0003	<input checked="" type="checkbox"/> 34C02DE13735AA29C - Door 0001 <input checked="" type="checkbox"/> 34C02DE13735AA29C - Door 0004	[edit] [delete]

Previous Next

For example, in the screenshot all profiles can access "door 01," which could be a general access door common to all users; meanwhile each profile's second door is specific. These could be for example for access to floor 2, floor 3 and floor 4.

Therefore in this way users with:

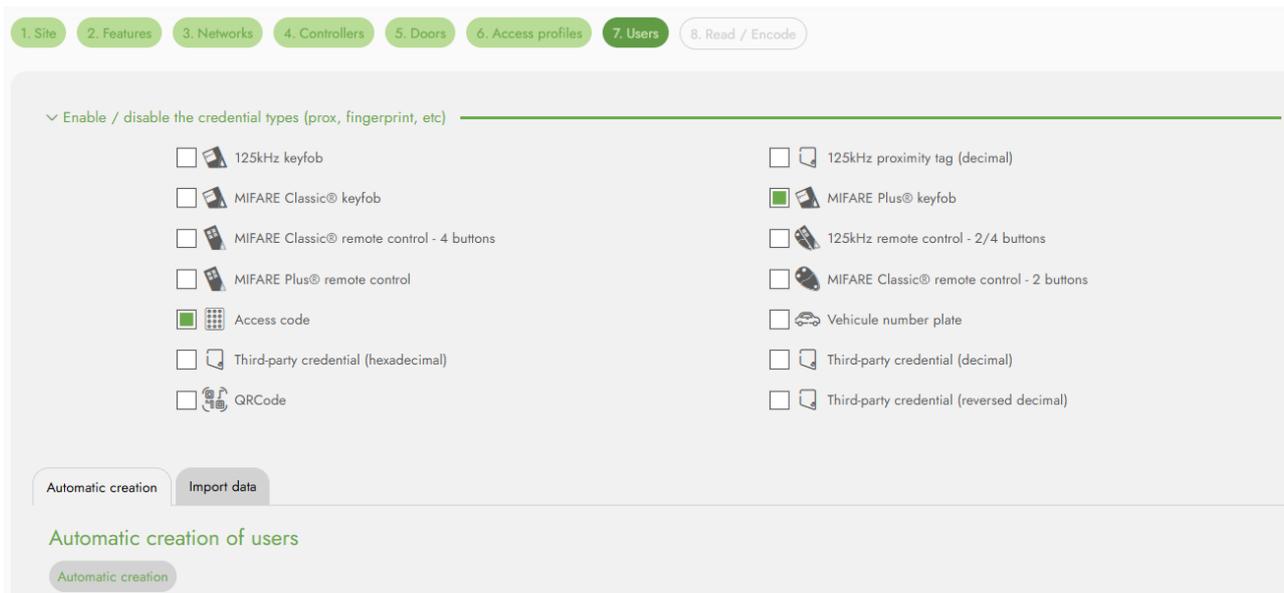
"Access profile 0001" would have access to both the common door and floor 2.

"Access profile 0002" would have access to the common door and floor 3.

"Access profile 0003" would have access to the common door and floor 4.

4.6 Cards (credentials)

Select the identifications that will be used in the installation:



Below, 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	-
Vehicule number plate	-	Third-party credential (hexadecimal)	-
Third-party credential (decimal)	-	QR Code	-

At this step, the wizard allows you to create users in bulk or by importing from a file. However, it is recommended to register and manage users from the "Access profiles and cards" menu, as it offers more complete and structured control.

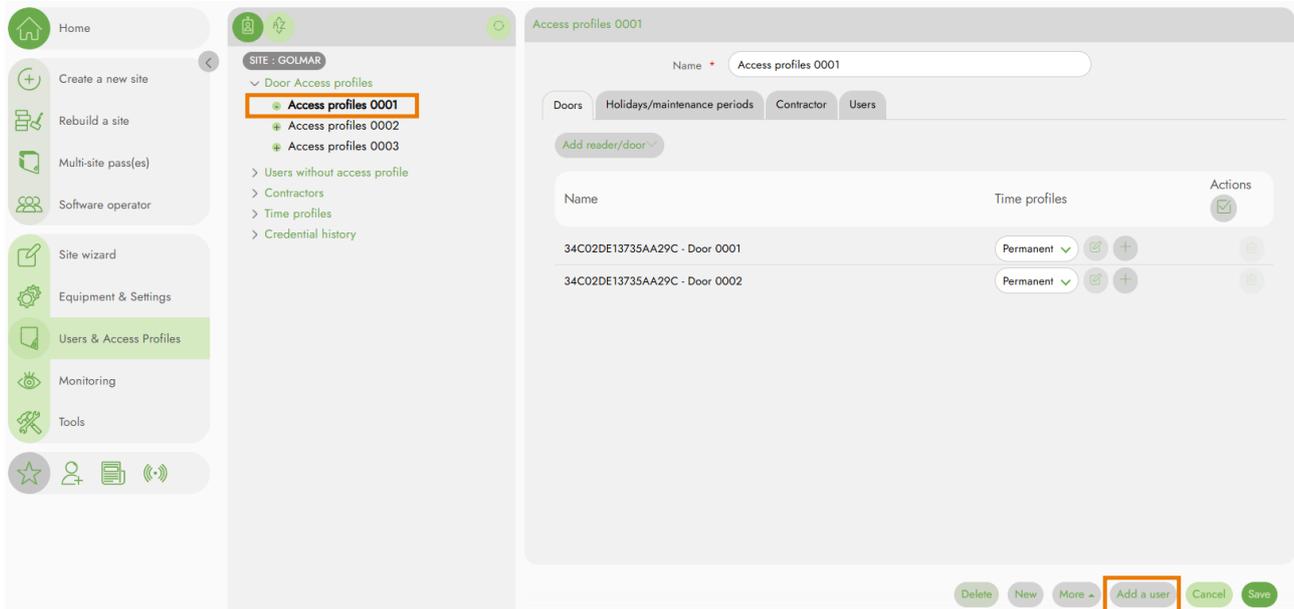
4.7 Read/Encode

It is recommended to skip this step and carry out user registration and management from the "access profiles and cards" menu.

5. USER AND ACCESS REGISTRATION

5.1 Manual Registration

Select one of the access profiles created with the wizard. For example, "Access profile 0001" and click "Add person."



This will allow the user(s) to be created next 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.

The screenshot shows the 'User name 0001' registration form. The form has the following fields: 'Last name *' with the value 'User name 0001', 'First name' with the value 'First name', 'Type' with the value 'Resident', and 'Door/zone access' with the value 'Access profiles 0001'. On the right side, there is a profile picture placeholder with a 'Browse' button and a camera icon. At the bottom right, there are 'Cancel' and 'Save' buttons.

Finally, add identification title(s) with which the user will be able to validate their access. The access identification options shown in the dropdown are those previously set in the "site" tab of the wizard.

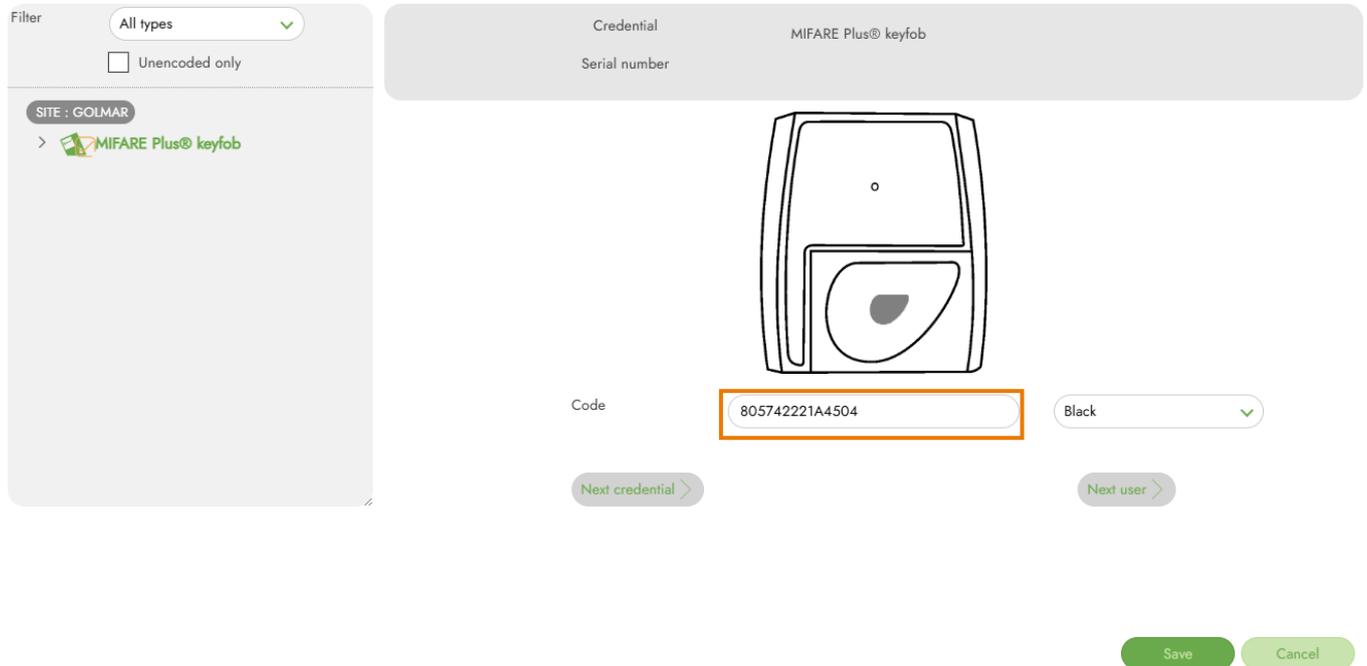
The screenshot shows the 'Credentials' form. The form has the following fields: 'Type' with the value 'MIFARE Plus® keyfob', 'Code' with the value 'Code', 'Colour' with the value 'Black', 'Status' with the value 'In use', 'Validity' with the value 'Permanent', 'Event' with the value 'Trace', and 'Other' with the value 'Other'. On the right side, there is an image of a keyfob. At the bottom right, there are 'Cancel' and 'Save' buttons.

If during commissioning any necessary identification was not selected, go to "Material and config." And then go to "Filter identification title types" to activate new identifications so they become selectable.

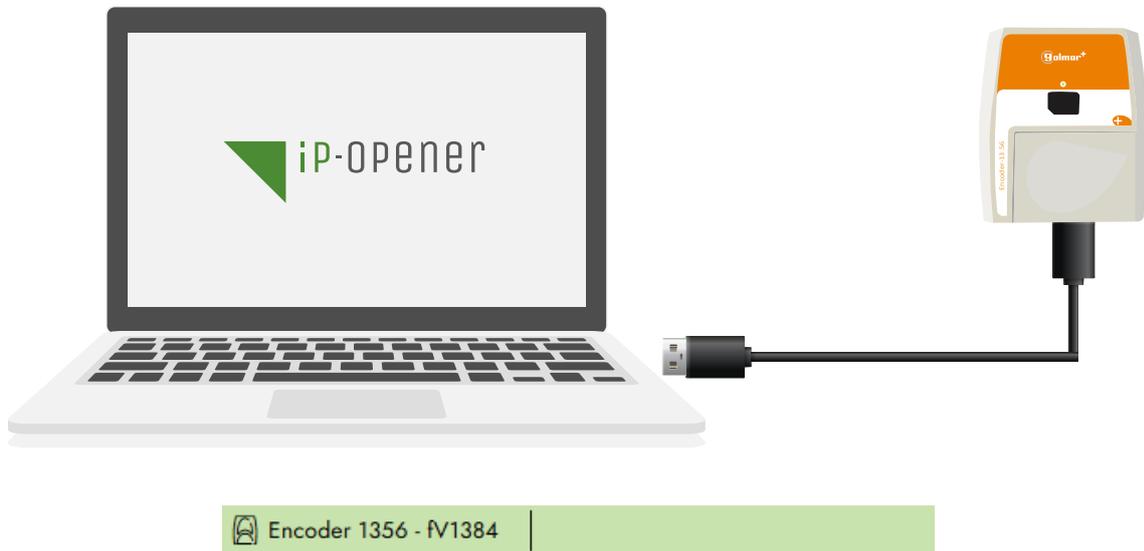
With proximity credentials, it will be possible to register the credential by typing the number printed on the credential or by bringing the card or key fob close to the GM-USBIPOP encoder.

If you bring the card or key fob close to the GM-USBIPOP encoder, the serial number will be registered.

Read / Encode / Enter credential



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.

▼ Add a credential

Type:

Code: Automatically Number

Colour:

Status: In use Suspended

Validity: Permanent

Allow secure mode: Double identification Single access forbidden

Event: Trace Hide

Other:

5.2 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".

SITE : GOLMAR

▼ Door Access profiles

- Access profiles 0001
- Access profiles 0002
- Access profiles 0003

> Users without access profile

> Contractors

> Time profiles

> Credential history

Access profiles 0001

Name: Access profiles 0001

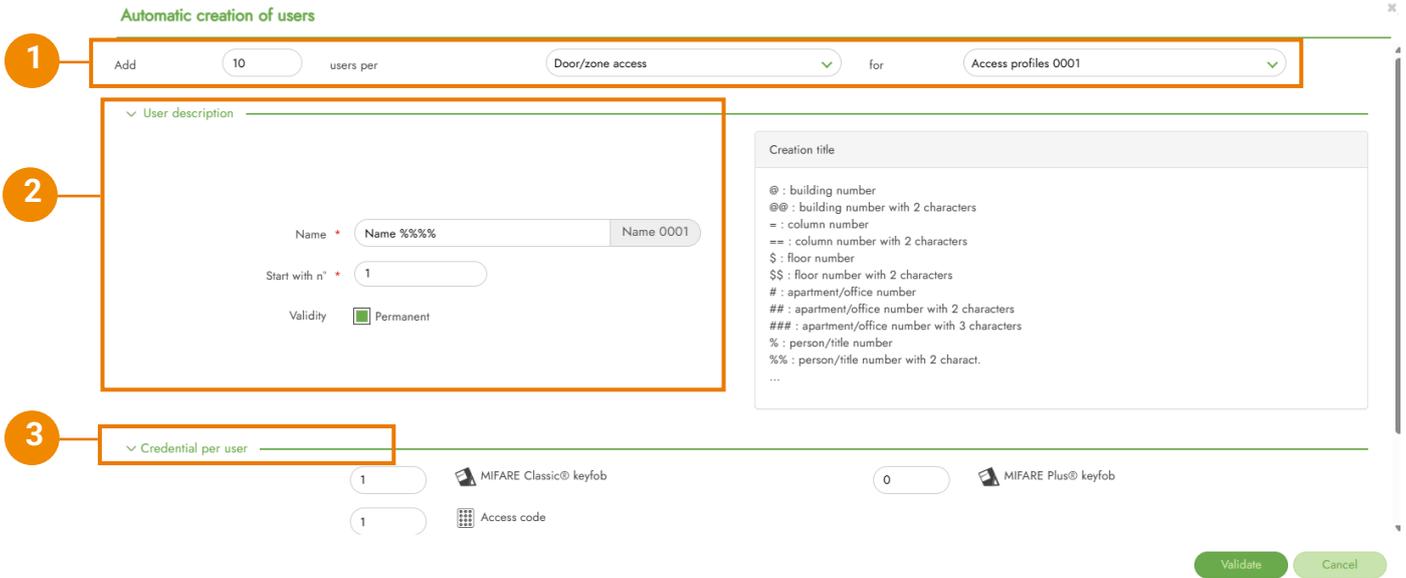
Doors | Holidays/maintenance periods | Contractor | Users

Add reader/door

Name	Time profiles	Actions
34C02DE13735AA29C - Door 0001	Permanent	<input checked="" type="checkbox"/> +
34C02DE13735AA29C - Door 0002	Permanent	<input checked="" type="checkbox"/> +

Add a contractor
 Add a sub-access profile
 Copy the access profile
Automatic creation of users
 Add contractors
 Import data

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".

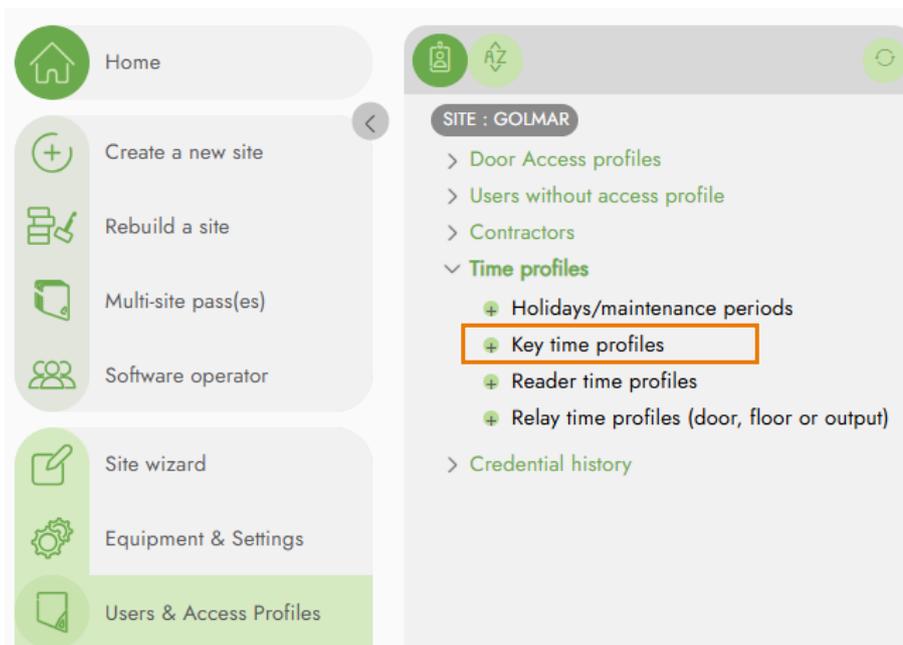
6. TIME PROFILES

6.1 Types of time profiles

There are different types of time profiles: key time profiles, reader time profiles, and relay time profiles.

6.2 Key time profiles

Below is a detailed explanation of how to generate a "key time profile." To do this, go to the "access profiles and cards" menu and then to the section time profiles\key time profiles.



Click on the "add an access time profile" option

1. Enter a name to identify the time profile you have created.
2. Choose whether you want the authorized time profile (green) or unauthorized time profile (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.

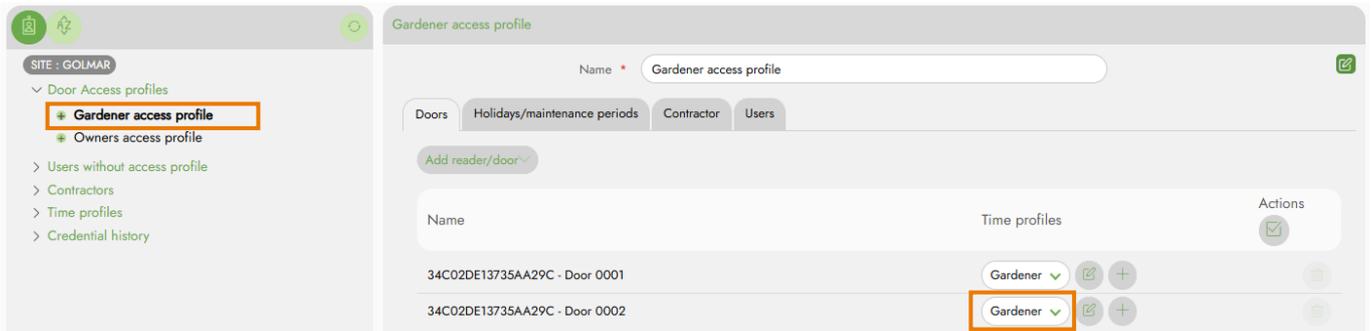
In the example, access from 9:00 a.m. to 11:30 a.m. has been authorized and identified as gardener.

If you want to be more specific and define the time profile in smaller intervals, do the following:

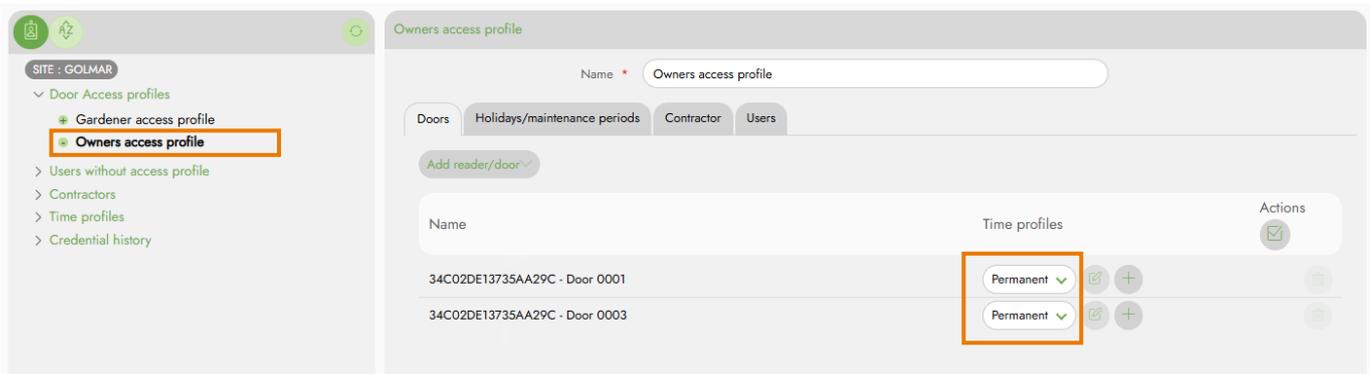
1. Select the code corresponding to what you want to define: green (authorized), red (not authorized).
2. Manually add the days that the time profile will affect.
3. Indicate the precision with which you want to set the range (5, 10, 15 or 30 minutes).
4. Set the start and end time.
5. Click the "+" symbol to insert it into the quadrant.

Once the time profile 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 time profile, the one previously defined as "Gardener".

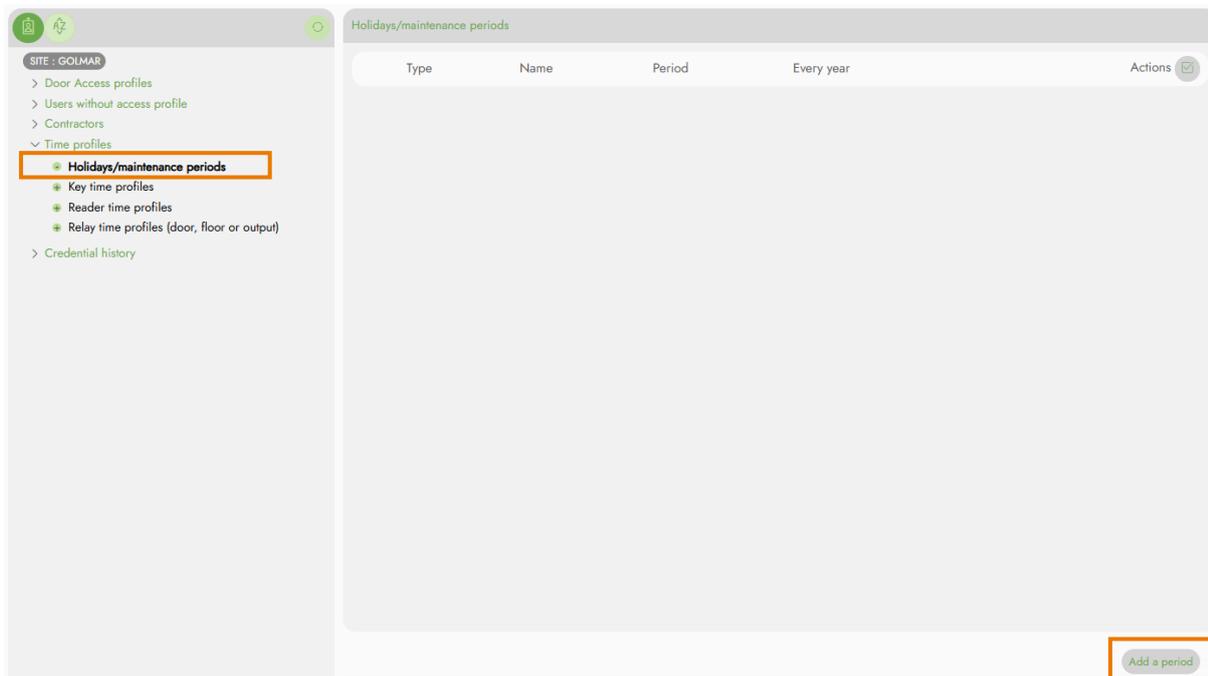


Whereas the owners profile can use both doors of the facility at all times (at any time).



6.3 Holidays

In the previous time profile, the "holiday" has been set as unauthorized. To inform the system which days should be treated as holidays, go to the menu Time profiles\Holidays/maintenance periods and 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.

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

7. OTHERS

7.1 Backup

It is recommended to perform a Back Up after completing the configuration. The configuration is stored in the cloud; a Back Up would allow you to return to a previous configuration point.

To perform a Back Up, go to the side menu "Tools." Select the "Import/Export" tab, click on "Add site for export," select the site (installation), and finally click "Back Up." This will download a ".db" backup file.

If at any time you wish to return to this configuration point, simply select the option "import one or more sites," select the ".db file," and click "Restore."

7.2 Supervision

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

The screenshot shows the i-OPENER MANAGER v02.00.03-r.3 interface. The site is set to 'Golmar'. The 'Events' section is active, showing a list of events. The table below represents the data shown in the screenshot:

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".

The screenshot shows the 'Settings' tab for Events. The 'Door' category is expanded, and the 'Name' checkbox is checked. The 'Priority level' is set to '5 Normal'. The 'Display colour' is also visible.

EVENTS	Name	Priority level	Display colour
<input type="checkbox"/>	Name	5 Normal	[A] [A]
<input checked="" type="checkbox"/>	Relay activated	5 Normal	[A] [A]
<input checked="" type="checkbox"/>	Relay deactivated	5 Normal	[A] [A]
<input checked="" type="checkbox"/>	Free access	5 Normal	[A] [A]
<input checked="" type="checkbox"/>	End of free access	5 Normal	[A] [A]
<input checked="" type="checkbox"/>	Forced door	5 Normal	[A] [A]
<input checked="" type="checkbox"/>	Opening of the door	5 Normal	[A] [A]

7.3 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 . Before generating the report, the software will ask us if we want to filter by date range.

Generar un informe ✕

Filtrar por fecha

Exportar Cancelar

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	



we take care of your home

Golmar Communication Systems S.A.
C/ Silici 13. Polígono Industrial Famadas
08940 - Cornellà de Llobregat - Spain
golmar@golmar.es - (+34) 93 480 06 96

www.golmar.es



Golmar se reserva el derecho a cualquier modificación sin previo aviso.
Golmar reserves the right to make any modifications without prior notice.
Golmar se réserve le droit de toute modification sans préavis.