

Software management of iPassan controllers
01.2025

ipassan



Summary

1. Common use of the software	8
1.1. Local mode	8
Prerequisite	8
IPassan downloading	8
Setup.exe	9
Create an admin account	10
1.2. Online mode	14
2. Site creation wizard	14
2.1. Site properties	14
2.2. Features	17
2.3. Networks	19
2.4. Architecture	21
2.5. Controllers	25
2.6. Doors	26
2.7. Intercom	27
2Voice integration with the interface	27
2Voice integrations with 2smart panels intercoms	29
Intercom settings	30
2.8. Lifts	31
Technologies supported by iPassan	31
Intercom integration	32
Programming	33
2.9. Zones	35
2.10. Access Profile	36
2.11. Users	37
2.12. Read / encode	38
3. Equipment and settings	39
3.1. Mail server setting	39
3.2. Multi-societies management	41
Function activation	41
Company creating	42
Assign societies to devices	42

Assign a company to access profiles & users	44
Software access.....	46
3.3. Networks	48
3.4. Controllers	49
3.5. Doors.....	50
3.6. Readers.....	51
Standard settings	52
RS485 readers.....	53
ANPR reader	54
Connected reader: Apério	58
Readers profile	60
3.7. Lifts.....	61
3.8. I/O (input and output) card	62
3.9. Input	64
Input adaptation settings	66
3.10. Exits.....	67
3.11. Anti-pass back (APB).....	68
Create a counting zone	69
3.12. Schedule and public holiday / work period	72
Access schedule	72
Door, exit or floor schedule	73
Reader schedule.....	74
Process schedule.....	76
Copying time profiles	77
Public holidays	78
3.13. Video integration.....	79
General	79
Synoptic.....	80
Choosing RTSP reading software	81
Settings.....	82
Advanced section configuration:	83
4. Intrusion	85
4.1. Dry contact intrusion	85

Zone settings	85
Zone intrusion settings	87
4.2. Elkron/Medea Intrusion	88
Prerequisite	88
Zone intrusion settings	89
4.3. Common intrusion parameters	90
Intrusion activation according to schedule	90
Intrusion settings for each zone	91
Reader profile for intrusion	92
Reader used for intrusion	93
User commissioning/decommissioning the alarm (with access profile)	94
Late departure	95
Intrusion tracking with events	96
Intrusion manual commands	98
5. Users and access profiles	100
5.1. Door access profile	100
5.2. Floor access profile	102
5.3. Users without access profile	103
User information	103
User's credential	105
6. Monitoring	107
6.1. Events	109
6.2. Network status	110
6.3. Manual commands	110
6.4. Reports	110
6.5. Zone	111
7. Booking management	112
7.1. Prerequisite	112
7.2. Adding bookable assets	114
Global settings	115
Advanced setting	116
Limitations period	118
Users	118

Mail sending.....	119
Actions.....	120
Instructions	121
7.3. booking management	122
8. Visitors management	123
8.1. Visits settings	123
General tab	124
Productivity tab	124
Email settings tab.....	125
Enable/disable the credential types (prox, fingerprint, etc...) tab.....	125
Default fields	125
Custom field.....	125
8.2. Create a visitor profile.....	126
8.3. Create a visit	126
Planning a visit.....	127
Create an instant visit	128
8.4. Visitors access management.....	129
Manual management of visit start/end.....	129
Automatic management of credentials	130
9. Advanced use of the software.....	131
9.1. Automatic modification tool.....	131
Controller information modification	131
Controller IP address change.....	132
Input modification.....	133
Output modifications	136
9.2. Automatic person/token creation tool.....	137
9.3. Emergency action.....	138
9.4. Reflexes	139
What is a reflex	139
Allow a user to create reflexes	139
How to configure a reflex	140
Reflex limit of IPassan manager.....	142
9.5. message.....	142

9.6 API commands143

10. Tools144

10.1. Firmware upgrade145

10.2. Logs146

10.3. Back-up / restore data146

10.4. Restore (site file import).....147

10.5. Automatic tasks148

10.6. Controller detection.....148

11. Software operators management.....149

11.1. Add an additional profile149

11.2. Add, modify an operator149

12. Integrations151

12.1. Automatic import/import file template151

12.2. Manual import.....154

12.3. Imports with automatic task155

12.4. Import with external commands156

1. Common use of the software

IPassan manager can be used whether in its online or local mode. The local mode requires downloading the .exe file on the IPassan website. While the online version only needs an account to log in.

1.1. Local mode

Prerequisite

The prerequisite configuration is:

- Quad-core processor > 3ghz (Intel Core i5 like)
- 8Go of Ram
- Operating system: Windows 11
- 10Go available on HDD or SSD
- Network interface card 100/1Go
- Internet connection to send mail and update the application if necessary

Java doesn't need to be installed anymore.

By default, the IPassan controller TCP/IP config is set to DHCP. It means that, when the controller starts, the system asks the DHCP server for an address. If nothing is entered the system will use the following parameters:

IP Address: 192.168.1.250

Mask: 255.255.255.0

gateway: no information provided

When the controller is correctly wired to the PC or with IP, but without DHCP server, the computer must be configured as follows:

IP Address: 192.168.1.1

Mask: 255.255.255.0

Gateway: no information provided

IPassan downloading



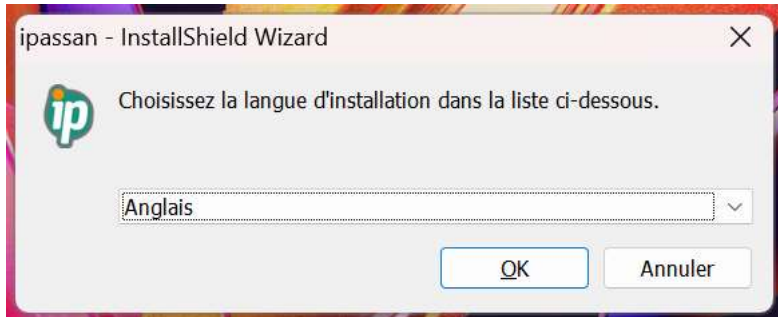
From the website <https://www.iPassan.com>, click the button « download the standalone version ».



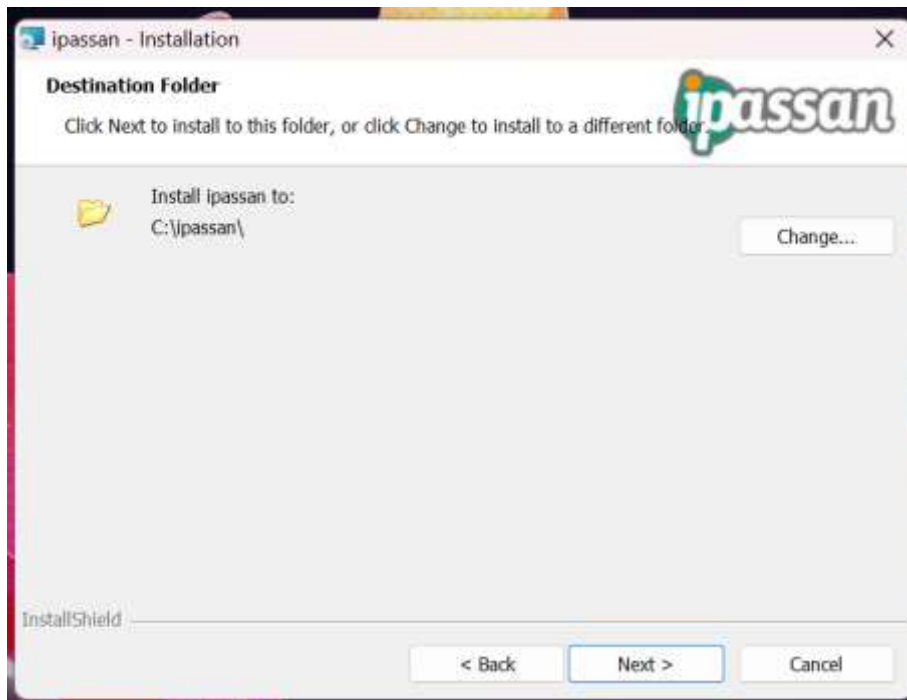
On the next screen, enter a valid controller number (it starts with 54Cxxxxxx).

Then, the downloading of IPassan Manager executable starts (the file weighs around 500MB). Click on it when it's finished to launch the setup.

Setup.exe

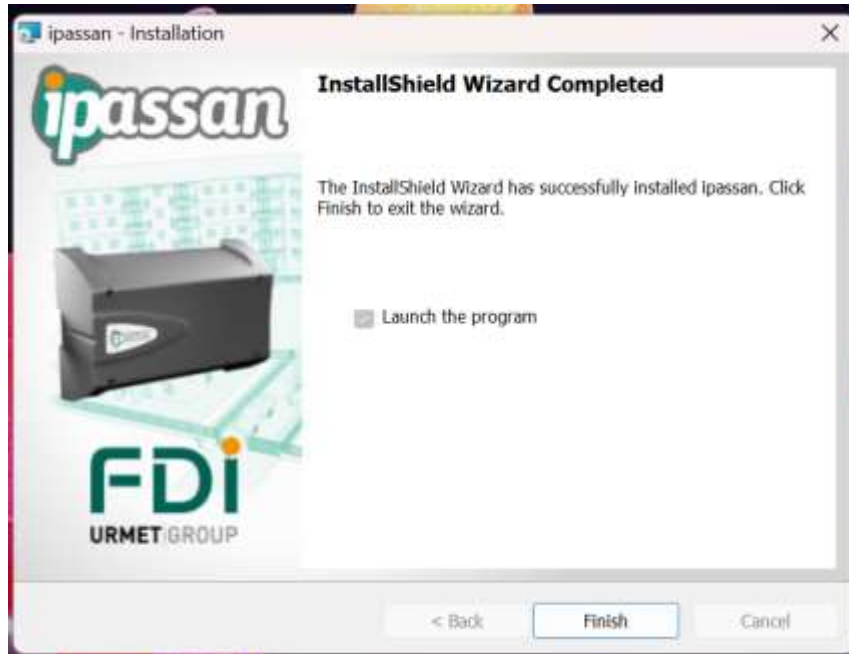


Launch the executable. Select the language and then click on "OK".



Click on « Next ».

Select the directory where to install the software and click on “next”. And choose “install” at the bottom of the next page.



By clicking on the “install button” the system will ask which internet browser you want to use to create your admin account. This browser will be used forever to launch IPassan manager, even in local mode.

Create an admin account



When the IPassan setup is done, the next step is to create an admin account. For the first launch of IPassan manager, the system asks which browser to use to run IPassan manager. Note that the program works with an internet browser even in local mode.

By clicking on the browser of your choice, you will be redirected to the following address <https://127.0.0.1:8443/iPassan/?login>. Note that “127.0.0.1” IP address is the loopback address. It’s used by the computer to refer to itself. It’s also known as a localhost.



If you haven't created an account yet, click on the "create an account" button. On the next view, enter your name, surname, phone number and password, and click the « Save » button.

Depending on whether you are an installer or a resident, you can click on the button at the top of the page. It changes the fields that can be filled underneath.

See the screenshot below if you click the "I'm an installer" button:

Creation of a new account

1st step: data entry for the new account

Last name *

First name *


Address

Phone


Email *

Your password *
The password must contain a special character, a digit, a capital and a lowercase letter, and must contains at least 8 characters

Your password for verification *

Device number. * 

(*) Mandatory



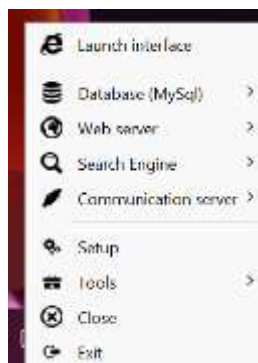
See the screenshot below if you click the “I’m a resident” button.

The screenshot shows the 'ipassan Manager' web interface. At the top, there's a header with the 'ipassan Manager' logo and the 'FDI urmet' logo. Below the header, there's a section titled 'Creation of a new account'. Under this section, there are two buttons: 'I'm an installer' and 'I'm a resident'. The 'I'm a resident' button is highlighted. Below these buttons, there's a section titled '1st step: data entry for the new account'. This section contains four input fields: 'Email', 'Your password', 'Your password for verification', and 'Resident code'. Each field has a red asterisk indicating it's mandatory. The 'Your password' field has a small text box below it stating: 'The password must contain a special character, a digit, a capital and a lowercase letter, and must contain at least 8 characters'. At the bottom right of the form, there is a green 'Save' button with a checkmark icon. A legend at the bottom left indicates that the red asterisk (*) denotes a mandatory field.

Once you clicked on the “save” button, please wait a few seconds while the system is processing the account create.

Congratulations, IPassan manager in local mode is installed on your computer! Now an icon appears on your desktop. Depending on the operating system this icon can be automatically named as “New Shortcut 1”. Feel free to rename it as you wish.

You can launch the software with the shortcut at the bottom right of the task bar.



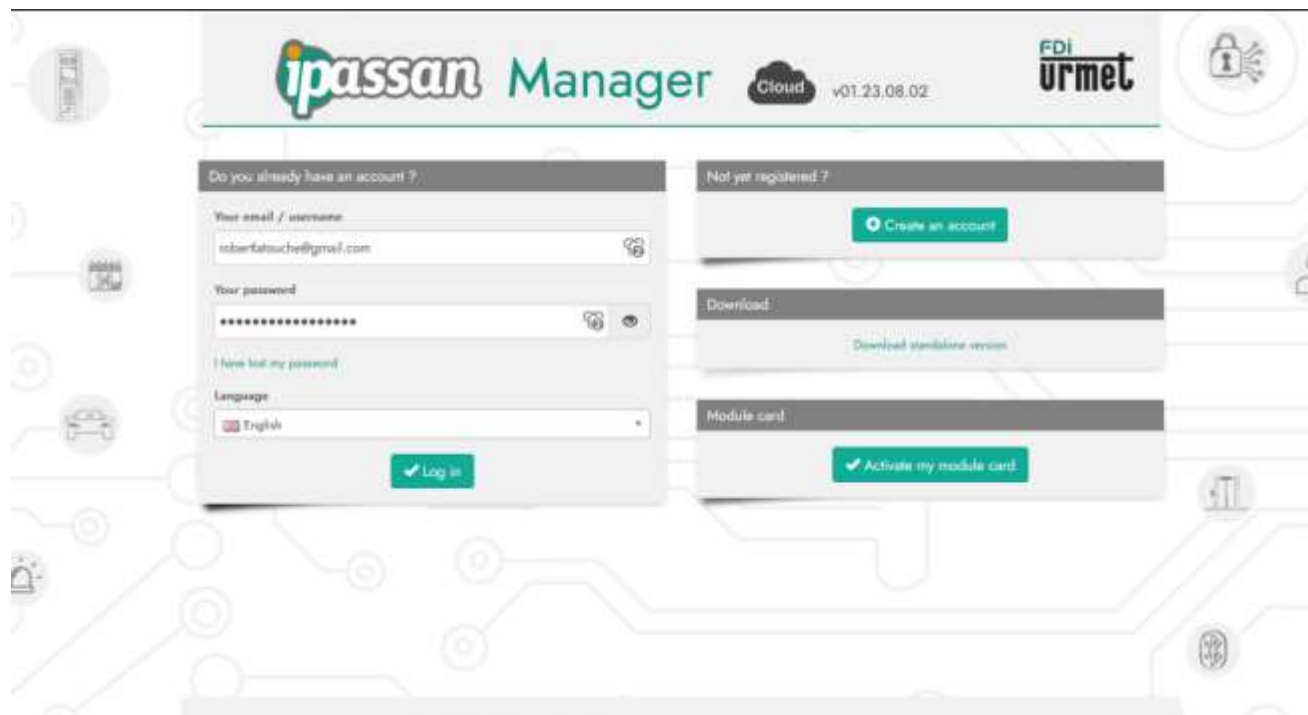
A left click on the icon develops the menu.

Select « launch interface » to open the software.

The software is compatible with Microsoft Edge, Mozilla or Chrome.

1.2. Online mode

You can access the IPassan manager with its online version. Enter the address <https://www.iPassan.com> on your web browser or search for "IPassan manager".



If you don't have an account yet, click on the "create an account" button at the top right of the page. Enter your login and password to connect to IPassan manager.

2. Site creation wizard

Click on the "Create a New Site" button on the main page. An assistant will guide you through the process of creating the site step by step.

2.1. Site properties

The first step is to define the site:

- Name, contact details of the person responsible, etc.
- Time zone
- Types of keys used
 - o Proximity key / remote control
 - o 13.56 MHz / 125 kHz

Transfer mode:

The software offers two modes for sending data to the controllers:

- **Optimized:** the server transfers only the data necessary for access control processing to the controllers. The controller does not know the name of the door or the user, as it does not need that information to allow or deny access to the door. This transfer mode is called "optimized" because it is faster. Unnecessary data are not transmitted over the communication buses.
- **Reconstruction:** the server transfers as much data as possible to the controllers. This includes usernames, door names, access profiles, schedule names, etc. This mode results in longer transfer times. In return, all information is available in the controllers in case of a reconstruction to the same or another server.

Note: The default option for the cloud server is "Optimized," as data backup is natively managed.

In local servers, the default option is "Reconstruction," which allows the site to be rebuilt on another PC in case of theft or destruction of data on the original server.

At any time, it is possible to switch from one mode to another. In this case, a complete transfer of the site's data is required.

Transfer options

Transfer option

- ☒ **Check the transfer date** : Doesn't erase controller database by older computer database.
- ☒ **Transfer data through UTF-8 encoding** : UTF8 allows to transfer any characters of any language. On the other hand, it needs more space in the controller memory. Some fields may be truncated in case of rebuild.
Without this option, encoding is ISO-8859-1

Check transfer dates: the server systematically records the last update dates and times in the controllers. When this box is checked, the server tests its own last updated date and that of each controller.

- If these dates do not match, it means the server has been updated after the controller. The system will then offer to force the controller to update.
- If the update date and time is later in one or more controllers than on the server, it may indicate that another PC/server was used on the site. The server will then offer to rebuild the site from the controllers to the server.

Transfer Data in UTF8: This option is necessary when intercoms need to display special characters (e.g., Norwegian alphabet).

Credentials: the software manages several types of credentials (physical and nonphysical)

Enable / disable the credential types (prox, fingerprint, etc)

<input type="checkbox"/> Proximity token 125k	<input type="checkbox"/> Token 125 k (decimal)
<input checked="" type="checkbox"/> Proximity token 1356	<input checked="" type="checkbox"/> Mifare+
<input type="checkbox"/> Remote control 1356 - 4 buttons	<input type="checkbox"/> Remote control 125K - 2/4 buttons
<input checked="" type="checkbox"/> Mifare+ remote control	<input type="checkbox"/> Remote control 1356 - 2 buttons
<input checked="" type="checkbox"/> Access code	<input type="checkbox"/> Plate number
<input type="checkbox"/> Other (hex)	<input type="checkbox"/> Other (decimal)
<input checked="" type="checkbox"/> Bluetooth	<input type="checkbox"/> QRCode
<input type="checkbox"/> Other (reversed decimal)	

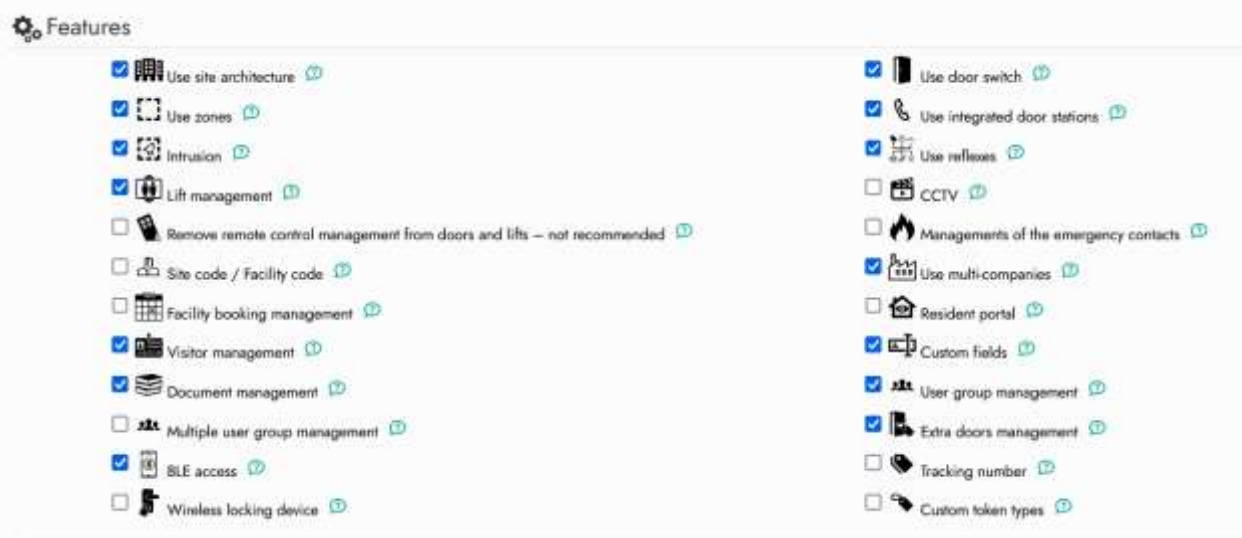
- **Mifare + Proximity token/remote control**: these are keys that operate on the frequency 13.56MHz. They are engraved with 14 characters.
- **Proximity token/remote control 1356**: These are token/remote controls operating on the 13.56 MHz frequency . They are engraved with 8-character hexadecimal.
- **Token 125K** : older technology for keys and remote controls. The keys usually start with 00xxxxxx, and the remotes are engraved in decimal with 8 digits starting with 9.
- **Keypad code** : 3 to 8 digits.
- **Plate number** : IPassan integrates with license plate recognition systems. In this case, the integration is considered "smart" because the camera or OCR (Optical Character Recognition) software communicates the license plate number to the IPassan controller in full text. This is not a Wiegand conversion.
- **Autre (decimal)**: useful when using readers and keys from a previous access control system. Tokens can be engraved in decimals.

- **QRCode** : The software can generate QR codes, which can be used in visitor management, for example.

2.2. Features

In the second step, we select the features relevant to this building that we wish to configure using the IPassan software. The software is designed to be as user-friendly as possible while allowing advanced features to be managed.

Example: the user who does not manage counting zones or anti-pass back (APB) will not check the option at this stage. For the subsequent steps, IPassan will not prompt the user to enter the criteria related to this feature.



Custom token types : allows custom token types to be imported from the partner software.

Use site architecture (see the chapter about the Architecture Concept)

Use zones: allow you to manage the overall or group counting of a space. They also help manage backpass and zone presence. If the site doesn't use zones, don't check this box.

Intrusion: the software manages two types of intrusion: via dry contacts or via Elkron/Medea connected controllers. By defining zones and readers within them, credentials can disable or enable intrusion management for set zones. An IPassan controller can manage up to 1 Medea controller per network. Both devices must be wired on the same IP network.

Lift management : this option allows you to control up to 110 floors from a controller. Note that enabling elevator management automatically activates the use of architecture (see chapter "Architecture"). IPassan manages conventional elevators (via dry contacts) and manages smart elevators via TCP/IP communication. The lift manufacturer Kone, markets two systems: the COP (Car Operating Panel) and the DOP (Destination Operating Panel).

- In COP mode, the reader is in the elevator car and is made by FDI access. The iPassan controller communicates the authorized floors to the Kone controller via a TCP/IP connection whenever a valid token is presented.
- DOP mode, the reader is outside the elevator. The user presents his token, and then enters his destination floor. The Kone sign indicates which elevator car to use. In the DOP system, several users going to the same floor at the same time are directed to the same cabin. This is designed to transport more people in the same time slot, thus consuming less energy.

Remove remote control management from doors and lifts – not recommended : not recommended.

Site code/facility code: a site may have been previously set up on IPassan manager. With the entry of the site code, all the previously defined parameters are found in this new site.

Facility booking management: You can manage bookings for assets or equipment with the software. The manager or employee can book a room from a dedicated portal.

Visitor management: residents or managers can add a visitor (or manage their visit) with the resident portal on their own. Depending on the settings of the visitor profile, they have access to the right door or floor.

Document Management : IPassan Manager allows documents storing such as a driver's license, insurance certificate, etc.

Multiple user group management: this feature is useful, for example, in the sharing of a car park between several entities.

BLE access: Users can access buildings with their smartphones. They must first download the "Kapp" application. Their Bluetooth access must be entered into the software.

Wireless locking device: the software can manage up to 6 Assa-Abloy/Aperio wireless locks per iPassan controller. The locks are linked to radio hubs (AH30 Gen5 IUD) that are wired to the controllers via the RS485 bus.

Use door switch: The door contact is a native function of the controller. It can detect the following events: door open, door forced, door open for too long, etc. If these door contacts are not used in the field, do not check this option.

Use integrated door stations: allows you to integrate the management of a site's intercoms from iPassan manager. There is integration via interfaces or intelligent integration (without interface).

Use reflexes: A reflex connects processes to conditions. For example, a relay is activated when a door is forced.

CCTV: IPassan integrates CCTV via the RTSP protocol. This integration allows one or more cameras to be linked to specific doors, inputs, outputs, readers, etc. For each event, the software offers a new button representing a camera. By clicking on it, the operator can view the video associated with the event. For example, in case of a forced door at night, IPassan Manager will display the images from the camera linked to the door at the corresponding time.

Management of emergency contact: an emergency contact allows the unlocking of one or more doors if an entrance is active. Usually triggered by a fire alarm.

Use multi-companies: this feature allows the management of a site occupied by different companies, where each company can only see its own areas. Only site administrators have full visibility. For example, in an office building, common doors are used by all companies. Each software operator manages access to these common areas for their own employees, without seeing other users, doors, or access profiles specific to other companies.

Resident Portal: residents have access to a lighter version of the software. It is responsive (it adapts to all screen sizes). The user can book assets/equipment or manage his visitors.

Custom Fields: the software manages fields such as first and last name, email, etc., for users. When the admin needs additional fields, they have the option to create them and set the type, format, etc. Then, the admin can add it to the required form in iPassan manager.

User group management: The software offers a default sorting of keys and users by access profile. For apartment buildings/residences, the software also provides a view of buildings, floors, and apartments. In addition to these two sorting options, IPassan Manager allows the creation of user groups, such as a department in a company or a class in a school, etc.

Extra doors management: allows you to add access to only one user

Tracking Number: this feature allows you to assign an additional code to all keys in a building or site.

Custom token types: allows you to import custom token profiles from the "Partner" application

2.3. Networks

The software is multi-network. These networks can be of the TCP/IP, RS485, or mixed type.

What is an IP network? When the equipment is wired with an Ethernet cable (RJ45) or a USB cable (when a computer is physically connected to the controller or server). In the case of multiple controllers installed via TCP/IP, they are all connected to an Ethernet switch, which is in turn connected to the internet modem.

A TCP/IP network can support up to 64 controllers communicating with each other via IP. When a site includes more than 64 IP controllers, it is necessary to create multiple networks in IPassan Manager.

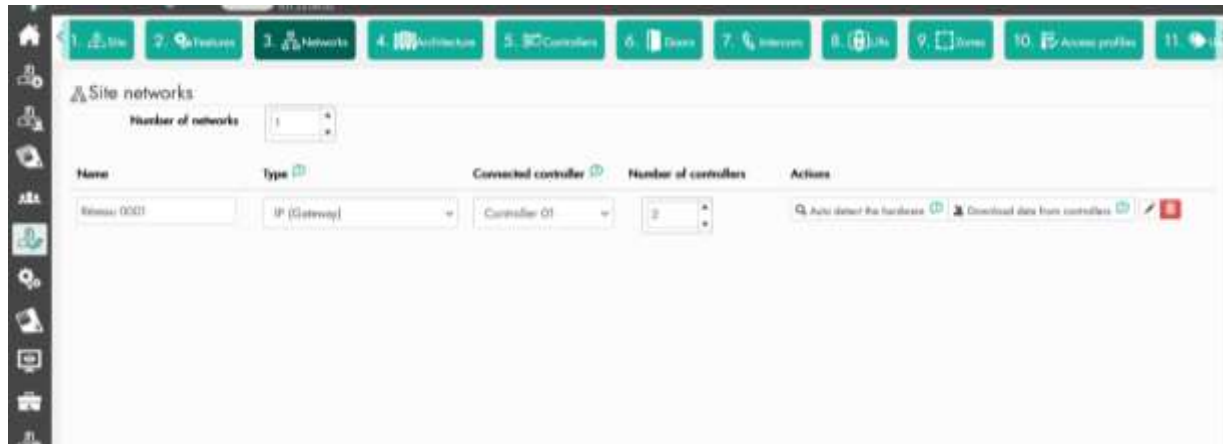
What is an RS485 network? When the equipment is wired using RS485. The first controller in the network must first be wired via RJ45 (TCP/IP) to have internet access.

An RS485 network allows communication between 32 controllers over 1 km. The first controller in the network can communicate with the server via TCP/IP or USB.

What is a mixed network? This refers to a network containing equipment wired both in RJ45 (TCP/IP) and RS485. From the communication server, it is possible to wire TCP/IP controllers first, followed by RS485 controllers, but not the other way around.

If a controller is connected via RS485 to the controller network, it cannot act as an IP gateway for other controllers.

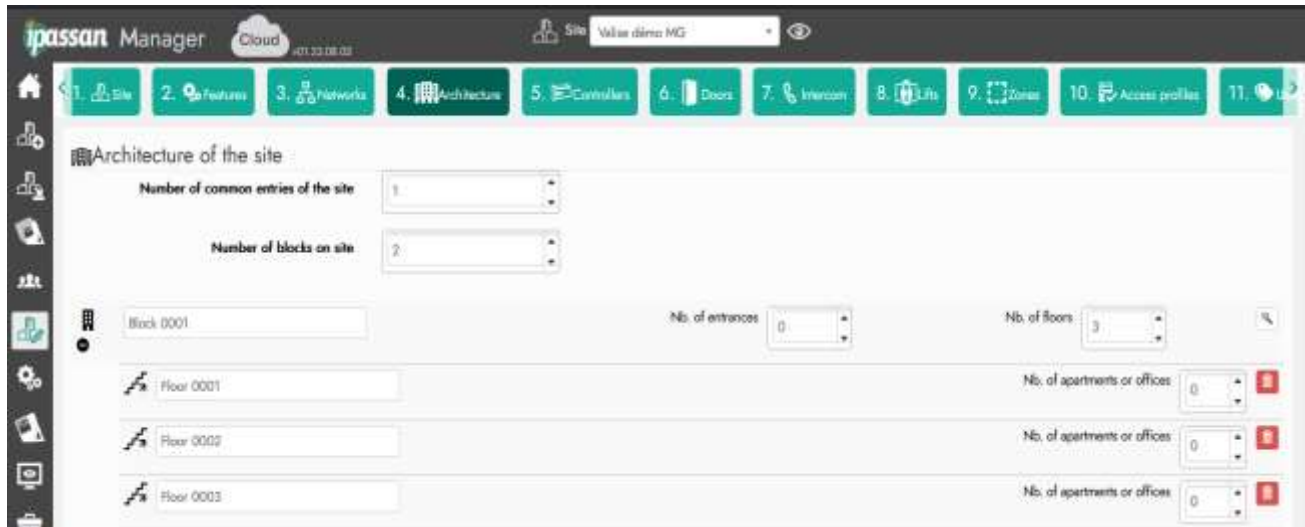
In other words, a mixed network is always TCP/IP on the server side, and optionally RS485 afterward. However, a mixed network can contain multiple RS485 branches (or multiple departures).



In IPassan Manager, enter the number of networks and the number of controllers per network, then click Next or use the “magnifying glass” button when the server is connected to the controllers. In this case, the server searches the network for the presence of controllers.

This option also offers the advantage of automatically retrieving the serial numbers of the controllers, their connected options, and the presence of input/output modules without any user intervention.

2.4. Architecture



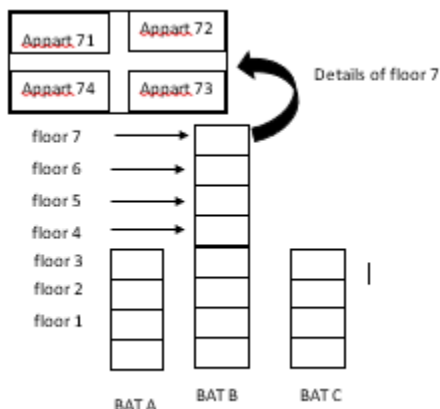
On IPassan, the architecture concept allows the creation of buildings, floors, apartments, and offices. It is then possible to sort equipment or users by geographical location (rather than just by access profile or group). This concept of architecture is optional when managing access control to doors but becomes mandatory for access to floors.

This explains why, when defining functions, selecting "Elevator" automatically selects "Architecture."

This concept simplifies site management significantly. The software operator can find their cards through buildings, floors, or offices, rather than in a long list of access profiles.

Additionally, it allows for automatic assignment of floor access to all elevators: for example, when an operator authorizes people to the floor, they can do so in the same action for all elevators serving that floor.

Use: both views (by architecture or by access profile) are functional at any time. An icon at the top of the tree view (left panel of the screen) allows switching between the two views.



Example of architecture definition in software and its impact on management:

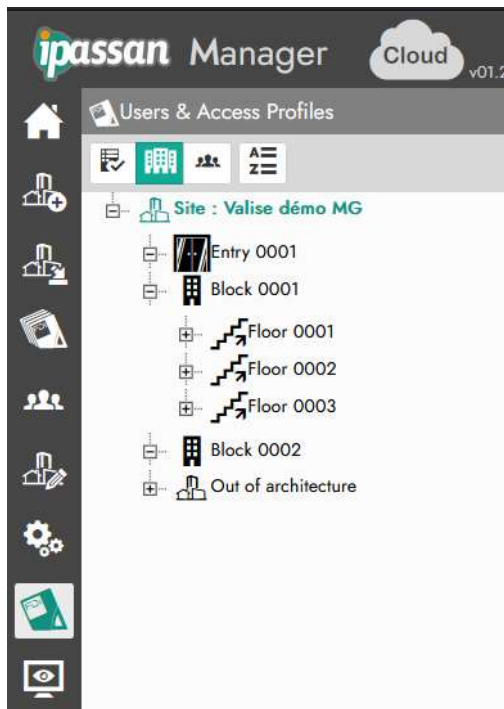
- A site consists of three buildings, one of which, Building B has 7 floors
- The 7th floor has 4 apartments, numbered 71 to 74

Classic view (category type classification)



In the usual management, users and their keys are sorted in the software by door or floor access profile.

View by architecture



In this view, users and their tokens are sorted by Building, Floor, and Office or Apartment.

Setting of the architecture concept

leading to the site. Internal building accesses are defined later in the creation tool. This concept of site entry is optional but helps the manager later by allowing the sorting of system doors into categories such as exterior, buildings, floors, etc.

Number of blocks on site

The number of buildings is required when elevators are managed within the software. In everyday use, when the software operator grants rights to a user for floor 4, the system authorizes all floor 4 levels of all elevators in the building with the same operation.

Then, you can enter the number of floors or the number of apartments/offices. Note that the concept of "office" is optional and can later be used to sort people and their keys.

Example an office building, 5 companies share a floor, but all have the same access to doors and floors. Without the office concept, users will all be classified under a profile like "Building A, Floor X." With the office concept, these users will be sorted into different categories in the people/keys window.

Note that a button with a magic wand icon (see above) allows you to easily create and name floors, apartments, and units. Clicking on it opens the following window:

- Enter the number of basements and above-ground floors. The software will automatically increase the numbers.
- Check the "Ground floor" box if the elevator also controls the ground floor. Otherwise, checking or unchecking the box does not matter.
- The "Front/Rear" option applies only to Kone integration if the elevators have both front and rear doors whose opening is controlled by key rights.
- Enter the number of apartments per floor and provide a common name, along with the number of digits for the floor and apartment numbers on each floor. For example, by entering "Apartment \$\$-###", the software will generate "Apartment 0001, 0002, ..., 0501, 0502," etc.

2.5. Controllers

In the next step, enter the number of controllers and the options they support on top or via the RS485 bus. Also, specify the number of doors and elevators managed by each controller.

Name	Identifier	Model	Expansion card	Doors	Intercoms	Lifts	Expanders	GTW	Actions
Corridor 01	24C02DE138091C3DC	2 wire / IP controller V2	2 doors (2 wire reader)	4	1	1	1		
Certe ES 0001	217230794F1B41C	10 wire SA	None						
Controller 0000	Controller serial number	2 wire / IP controller	None	0	0	0	0		

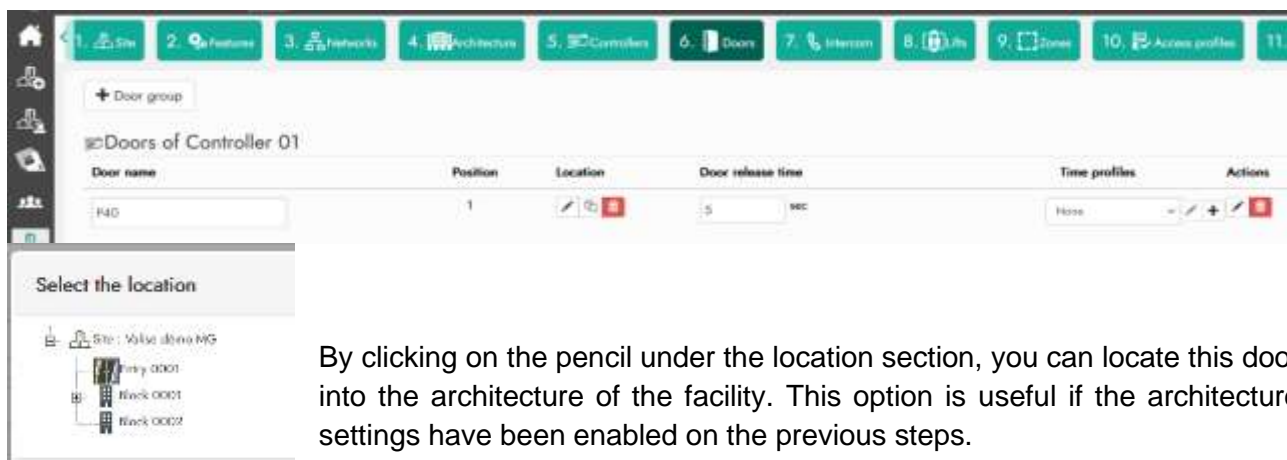
In the window above, fill in the fields as follows:

- **Name of the controller:** 32 characters, this is a free text designating the controller or its location.
- **The controller identifier** is the one written on the controller's label (ex 54C01AA000B00C000).
Note that this identifier is broken down as follows: 54C01 or 54C02 or 54C12 or 54C12 depending on the version of the controller and its protocol.
AA000B00 is the end of the MAC address. The beginning (00 0E) is common to all the controllers, so the MAC address of this controller is 00 0E AF 00 0B 00 C000.
- **Option:** a controller supports an optional card mounted on top of the housing. This card can provide one of the following options: 4 additional readers, 12 inputs, or 12 outputs.
- **Doors:** enter how many doors are managed by the controller (the maximum number of doors per devices are 6)
- **Expanders:** each controller manages up to 10 RS485 input/output cards.
- **GTW (gateway):** if the controller is connected to the cloud, it will show a green tick.

2.6. Doors

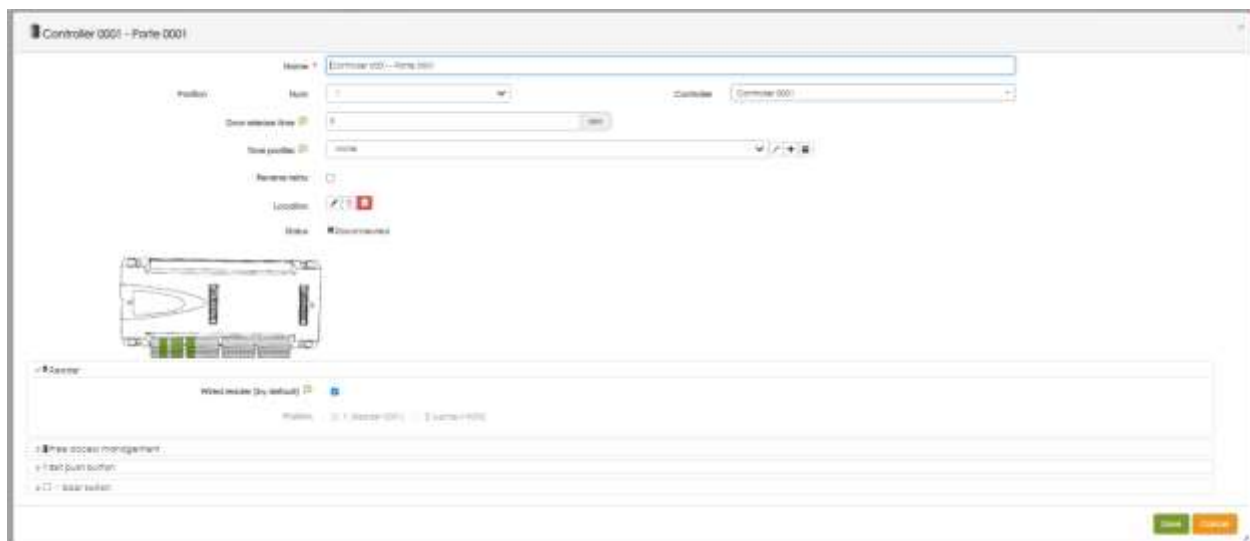
In the following screenshot, you can modify the doors settings.

- **Change the name** of each door.
- **Adjust the door release time** if needed (default is 5 seconds).
- **Door release time (+ button on the left)** : optionally, add time slots to the door during which the door is:
 - Free access: the magnetic lock is not powered, and the door remains unlocked. (example: during office hours to let the postal service enter.
 - Forbidden: even a valid key cannot open it.
 - Normal: a valid key is required to open the door.



By clicking on the pencil under the location section, you can locate this door into the architecture of the facility. This option is useful if the architecture settings have been enabled on the previous steps.

The pencil on the right, you access advanced settings.



2.7. Intercom

This step allows street panels configuration. The only intercom system that can be integrated intelligently (using bus communication, no dry contacts) is the 2Voice system.

In the 2Voice system, street panels can be primary, capable of calling all the apartments in all columns, or secondary, able to call only the residents of a specific building.

Two integrations are available on iPassan:

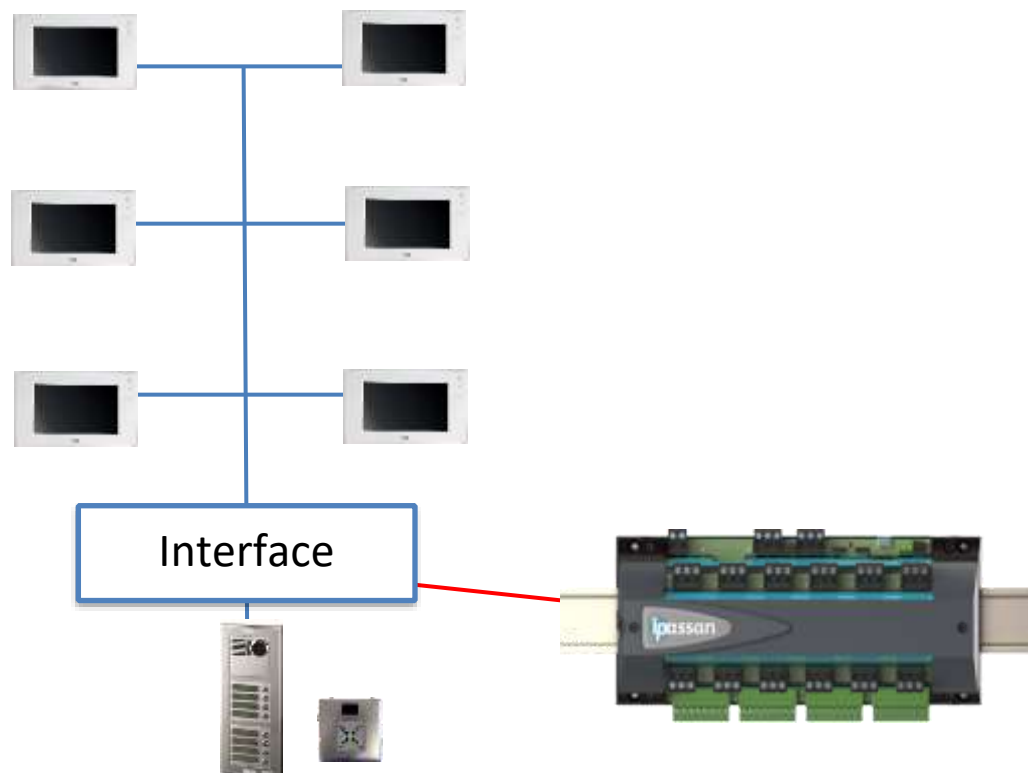
- **The first relies on 2Voice bus interfaces.** The street panels sold by Urmet Group (Italy) require FDI interfaces wired to the 2Voice bus, which listen for the messages. The interface acts as a "sniffer," allowing the central unit to interpret the signal sent by the street panel.
- **The second integration involves 2Voice Street Panels** made by FDI Matelec. In this case, they are fully managed by the central units and the iPassan Manager software, which means that names and combined codes are managed in the software just like keys.

2Voice integration with the interface

An interface can manage up to 4 street panels, which is also the limit for a central unit. However, a central unit can manage up to 4 interfaces.

This means that for the installation of 4 street panels, if they are wired to the central unit on the same bus, only one interface is needed. However, if the 4 street panels correspond to 4 separate columns across different central units, the site will need 4 interfaces.

As a reminder, the 2Voice interface should be considered as a sniffer; it listens to the messages on the 2Voice bus, and the central unit interprets them. The interface cannot send messages to the bus.



The benefits of this integration are multiple:

- **Event management:** the 2Voice intercom system does not natively manage events. By adding and managing these interfaces, events are stored in the controller. This allows tracking “when a call was made” and “who opened the door for the visitor”. This event management complies with regulations like Secure by Design in the UK.
- **Increased security:** by using the relay in the central unit instead of the relay on the street panel, which is more vulnerable to vandalism, security is enhanced. When the resident opens the door for the visitor, the central unit reads the message on the 2Voice bus and releases the correct door. The wiring is also simplified.
- **Added flexibility:** for each button on the handset and street panel, it is possible to control up to 4 doors or relays (e.g., for an air lock or lighting).
- **Elevator management:** through configuration in iPassan, the administrator can associate an apartment with a specific floor. This way, the central unit knows the characteristics of the apartment that requested the door opening (including the floor), and it can grant access to the correct level for the visitor. Example: an apartment on the 5th floor allows the opening of the lobby door. The elevator will only allow access to that floor for the visitor.

⇒ How does it work?

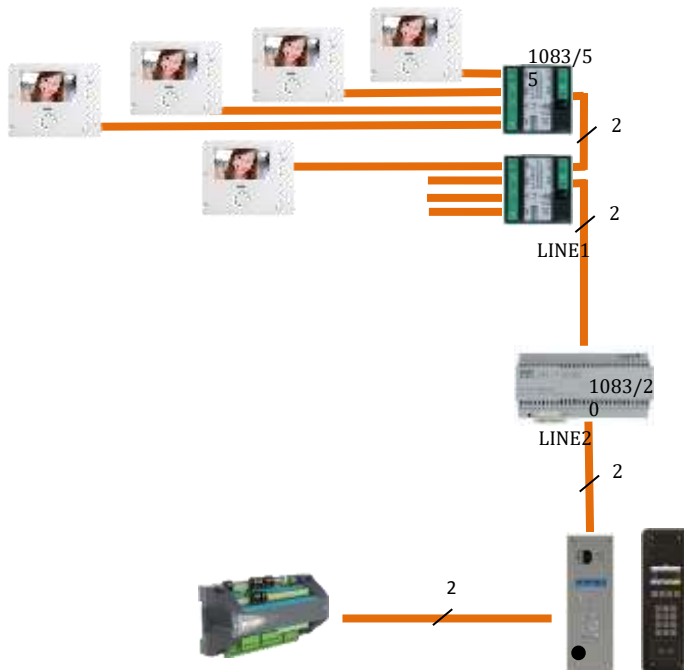
Street panels and apartments are created in iPassan Manager. The software configuration must correspond to the installed products and wiring.

When a visitor calls an apartment from the intercom, iPassan knows which combined code is being called and which apartment it corresponds to. The software events will therefore show:

- "Call to apartment 'Martin' in progress"
- "Door opening"
- Possibly "Door left open"
- End of communication
- "Door closed"

In addition, the iPassan controller manages the correct floor for the authorized elevators. The visitor enters the building, calls the elevator, enters inside, and can only press the authorized floor.

2Voice integrations with 2smart panels intercoms



The use of the 2Smart panel offers the following advantages:

- **Access control (door and elevator) and intercom management** from the same software
- **Management of events related to access control and intercom** in a single tool
- **Simplified wiring** since the lock is wired only once to the controller. No wiring on the street panel, which only requires one pair of wires for the 2Voice bus and another for the 2-Wire bus to the controller
- **Creation of an intelligent interface** between the intercom, elevator, and access control. This feature does not require special decoders.

The maximum number of 2Voice street panels is limited by the system itself:

- **16 main street panels**
- **2 secondary panels per column**

The main advantages of these 2Smart Street panels are:

- **Disability law compatibility**
 - Braille keyboard
 - Voice messages
 - Large screen, pictogram display
 - Hearing loop
- **Management of alphanumeric call codes up to 8 characters**

- Special codes allowed
For example, a call code could be B2-12.

⇒ How does it work?

As with the integration via the 2Voice interface, the on-screen configuration must match the installed equipment.

When a call is made from the street panel to an apartment, the controller knows which apartment is being called. It will authorize the correct door as well as the corresponding floor for the visitor.

The integration type (interface or 2Smart plate) should have been chosen previously. See below:
The second option is to choose whether the names of the apartments or the names of the keys in the software will be displayed on the intercom.

- In the first option, the manager does not modify the names of the residents on the intercom. They are displayed "Apartment 01", "Apartment 02", etc.
- In the second option, the name assigned to the keys is also displayed on the street plates. This option allows the manager to change "Dupont" to "Martin" while keeping the apartment name as "Apartment 01".

Intercom settings



In the site creation wizard, at the Intercom stage, select the type of street plate and its position in the building. The number is automatically generated by the software.

Type of intercoms:

- **Main:** can call all columns.
- **Secondary:** can only call the apartments in the column it is wired to.

Important: The screen settings must match the wiring of the following references:

- 1083/50 (Urmet 2Voice Column interface)
- 1083/75 (Urmet 2Voice door station interface)
- 1083/76 (2Voice interface for 16 plates)

For each intercom, select its position on the controller where it is wired.



2.8. Lifts

Technologies supported by iPassan

IPassan manages the integration of several elevators and can control up to 110 floors per controller. Most of the time, the integration of the elevator into the access control system is done using dry contacts. However, IPassan also offers two types of smart integration with the Kone brand. These two integrations, explained below, rely on TCP/IP communication between the access control system and the elevator.

The elevator functionality can be repurposed to manage lockers, mailboxes, or storage boxes. Indeed, for the same reader or keypad, the system manages up to 110 relays, which can be locker locks or alarm deactivation contacts.

- Traditional elevators

Access control readers are installed inside elevator cabins. The user calls the elevator, enters, presents their tokens, and presses the desired floor button. Typically, the buttons corresponding to their authorized floors light up after the token is presented.

For a resident, only their residential floor and underground parking floor buttons light up, whereas for a caretaker, access to all floors may be granted. The control panel provides dry contact for each floor and elevator. For example, in a building with 15 floors and two elevators, this would require 30 relays.

- Kone COP (Car operating panel)

The principle is the same as for traditional elevators, but here communication between access control and the elevator relies on TCP/IP.

The Kone Cop integration achieves this without additional hardware. The functionality requires an activation card, which must be entered into the controller.

This solution simplifies the wiring between the elevator and the controller. For example, in an installation using dry contacts, a building with 80 floors and 10 elevators would require 800 relays on the access control side and 800 inputs on the elevator side, all of which would need to be supplied, powered, and wired.

- Kone DOP (destination operating panel)

The residents' apartment floor is programmed into their access profile. When they enter the building with their key, the elevator is called and takes them to the corresponding floor.

This system is useful when a group of elevators serves the same floor. At each level, a terminal allows the user to select their floor, and the elevator directs them to the appropriate vehicle.

This system improves elevator efficiency by streamlining trips, transporting more people per hour while consuming less energy.

The Kone Dop integration with IPassan is software-to-software: the elevator configuration is done in Kone Access. The databases of IPassan Manager and Kone Access are linked.

Intercom integration

Elevator management in iPassan concerns both residents, who access authorized floors with their cards, and visitors, who are automatically granted access to the correct floor (when the resident gives permission via the intercom). By integrating the intercom, access control, and elevator systems, iPassan manages these three functions under one software. This integration can take various forms.

- Dry contact integration

Each floor has a dry contact activated when the resident allows a visitor at the door. This contact is connected to the iPassan software and linked to a specific floor. When activated, the controller grants the visitor access to the correct floor. iPassan can manage up to 4 elevators for the same floor contact, and the delay for the dry contacts can be adjusted.

Two types of delays are possible for these dry contacts:

- A delay in seconds for tokens-based access
- A delay in minutes (3 minutes by default) for visitors.

Indeed, the resident enters the elevator, presents his card, and selects his floor. The visitor, who is outside the building and has been authorized, enters the building's lobby, calls the elevator, which descends to the ground floor, enters, and presses the floor button.

- **Smart integration with the intercom.** In some cases, the integration becomes intelligent between the intercom, access control, and the elevator.

The first of the smart integrations concerns the Urmet 2Voice intercom system. By adding an interface to the 2Voice bus, iPassan knows which residence is being called and which one opened the door for the visitor. This is possible only because the apartments are entered into iPassan Manager with their intercom handsets codes and respective column numbers. This allows the controller to authorize the correct elevator(s) as well as the correct floor for the visitor.

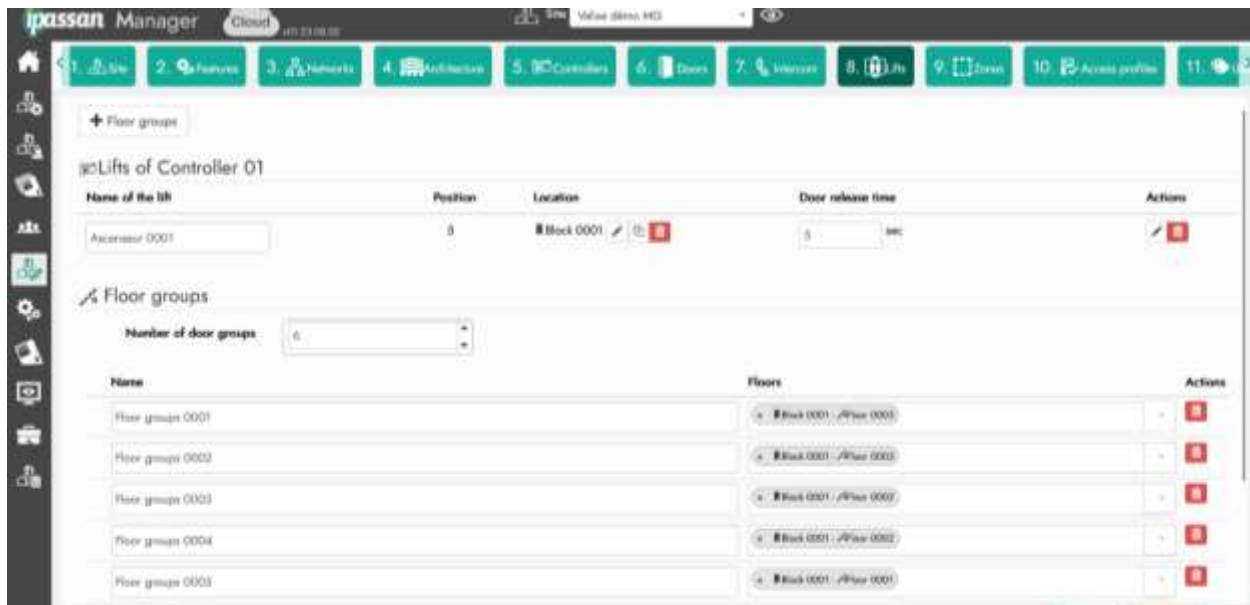
The second smart integration is achieved with 2Smart street panels. These products, manufactured by FDI Matelec, are controlled by iPassan controllers without specific configuration. The controller thus knows which residence is being called and has authorized the visitor. It can therefore activate the correct floor for the appropriate elevators.

Programming

Because elevators were added to the controllers in the previous steps, the software automatically performed the following operations:

- Assign these elevators to their respective buildings.
- Select an unused reader from the controller for each elevator.
- Assign the available relay outputs to the floors.

To manage these elevators, use the pencil icon under "Building" or the one under "Actions" to modify their settings (see second screenshot).



In the screenshot below, you can change or add the following settings:

The screenshot shows the configuration page for 'Ascenseur 0001'. The 'Name' field is set to 'Ascenseur 0001'. The 'Position / Room' is '0'. The 'Location' is 'Block 0001'. The 'Company' field is empty. Under the 'Reader' section, 'Wired reader (by default)' is checked. The 'Release time' is set to '5'. The 'Full safe life' checkbox is unchecked. The 'Time profiles' table has three rows:

Name	Delay	Time profile	Actions
Ascenseur 0001	Carte 0001 - Suite 0001	None	[Edit] [Delete]
Ascenseur 0002	Carte 0002 - Suite 0002	None	[Edit] [Delete]
Ascenseur 0003	Carte 0003 - Suite 0003	None	[Edit] [Delete]

- **Reader:** when an elevator cabin is equipped with two or more readers, they can be added here by unchecking 'default reader' and selecting the corresponding readers.
- **Release time:** this is the time between key presenting on the elevator reader and floor selecting. Visitors, who logically do not have a key, require sufficient time between the access authorization (granted by the host), and the entering of the desired floor.

That's why iPassan manager distinguishes two different activation delays: the first one in seconds for tenants and the second one in minutes for visitors.

It's possible to add an additional push button operated by the switchboard operator. This one transmits dry contact to an iPassan controller input. What grants the visitor the rights to select and access the required floor.

2.9.Zones

The system allows for the management of counting zones and/or anti-pass back. The following window appears when the "zone" feature has been checked in the previous step (see chapter 3.1).

A counting zone allows you to:

- Know in real time the number of people, cars, etc., in a zone
- Limit the number of people, cars, etc...
- Be able to display the zone where an access control user is located

Advanced options help to ensure the accuracy of the counting process:

- Passage confirmation: IPassan can use the door contact as passage confirmation. This could be an infrared barrier for a parking gate, or a contact provided by a turnstile in pedestrian access control.
- Anti-pass back: this can be linked to counting to ensure that user A does not lend their key to user B, thus bypassing the rules.

Note that anti-pass back can also be used without counting, depending on the scenario.

In the following window, enter the number of zone(s) and then, for each one, select the entry and exit readers for the zone. Check the Anti-pass back and count options if necessary.

Name	Entrances	Exits	Anti-pass Back	Counting	Intrusion	Actions
SATIMENT	R420 - Barten pousseur 0003 R420 - Barten pousseur 0001	R420 - Barten pousseur 0001	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

2.10. Access Profile

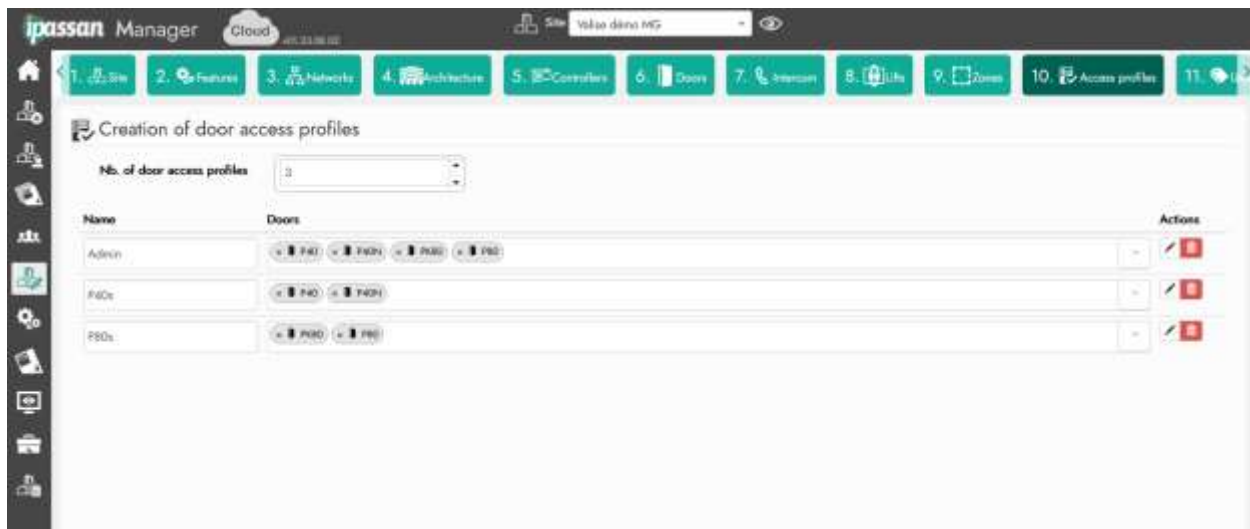
The software operates with access profiles. It contains a list of authorized doors.

Note: a system user has four different access profiles.

- A permanent door access profile
- A permanent floor access profile
- A temporary door access profile
- A temporary floor access profile

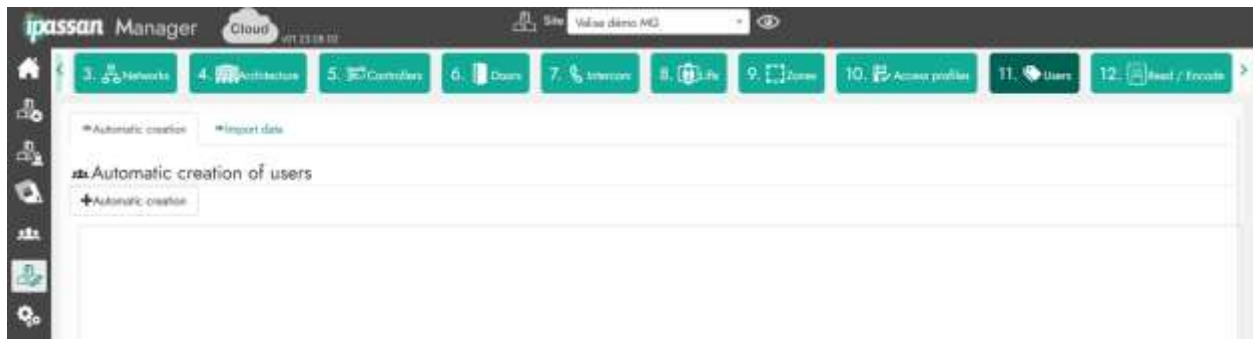
A temporary profile is therefore a list of additional doors or floors that a user can access within a given time interval (e.g., from 04/06 to 15/06, from 03:00 am to 6:00 pm).

When a user needs access to both an "office" area and a "workshop" area, an access profile must be created in the software that includes all the relevant doors.



2.11. Users

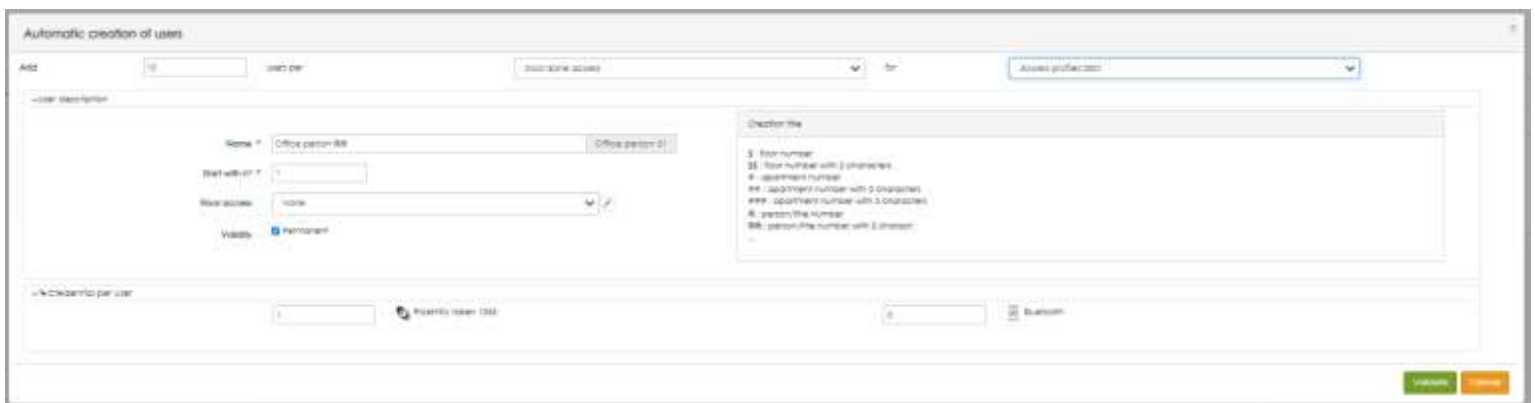
The users wizard allows you to automatically create individuals, their keys, keyboard codes, etc. From this same window, you can add multiple items: for example, 20 individuals using the same access profile plus 15 others using a different profile. These automatic additions apply to sites, door access profiles or floors, groups of people (e.g., Engineering, Sales, Administration, etc.), or architectural elements (e.g., buildings, floors, offices). Click on the "Automatic Creation" button in the following screenshot; the second screenshot shows the details of the tool.



In the following window, enter the number of individuals to create for each option (access, building, floor, etc.). Then select the appropriate profile, building, floor, etc.

In the "Person Information" field, enter a name and refer to the legend for managing automatic increments.

The following example shows how to create 10 individuals, each with 1 token and a keyboard code, using the "Access profile 001" access profile and named: Office Profile Person 01 / Office Profile Person 02 / ... 03 / ... 04 / etc.



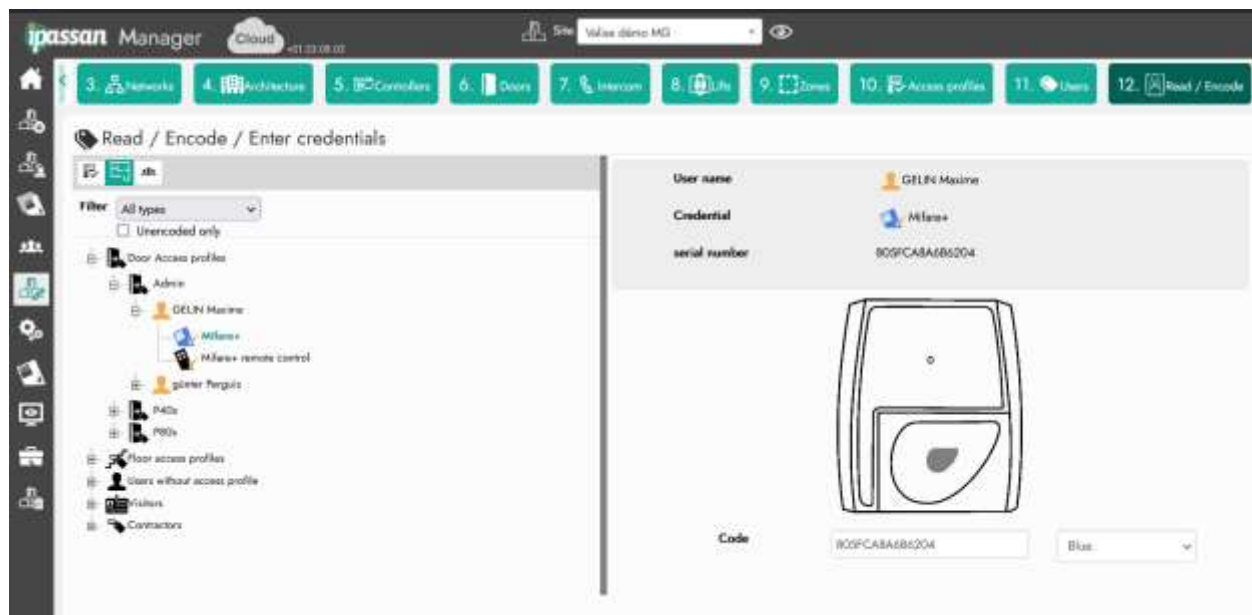
2.12. Read / encode

At the final step, the wizard suggests reading the cards serial numbers using the desktop reader and associating them with the automatically created individuals.

In the left frame, you find all the entered people. You can order them by access profile, apartment or by group. You can select them manually to add them to a credential.

The right frame indicates the selected person whose key will be encoded. The left frame allows you to switch directly to another profile, group, person, etc.

With each token scan, the software automatically moves to the next one. Thus, no action is required between each key presentation to the encoder.



3. Equipment and settings



All system & site settings are editable. By clicking on the gear icon « Equipment and settings ».

See the screenshot below.

After clicking on the "equipment and settings" gear icon and then on "Site: xxxxxx" in the tree structure, we gain access to the main site settings.

This menu includes all the information entered during the site's creation. For more details on the fields present here, refer to **Chapter 2: Site Creation Wizard**.

3.1. Mail server setting

The software can send emails either via scheduled tasks or processes. To do this, it's necessary to configure the email account on the server.

- > Time zone
- > Enable / disable the credential types (prox, fingerprint, etc)
- > Keypad codes setting
- > BLE access
- > Emails settings

From the « equipment and setting » menu click on the site in question.

Below all the coordinate fields on the site, and among all the available options, click the "email settings" button.

The window below appears:

An e-mail account must have been created. The computer supporting IPassan manager must have access to this server. Click on the + button to the right of the “SMTP” field.

Then enter the required fields and test the mail sending by entering an address and clicking on Test.

3.2. Multi-societies management

IPassan Manager offers multi-company management. For a single site, several software operators can view and manage their own doors, access profiles or users, without seeing what belongs to other operators. Only site administrators or operators with multi-company rights see the whole.

This management applies, for example, to an office building where floors are used by different companies, but all use common doors or elevators.

Company A's operators see their own doors and floors, as well as the shared doors. They only see their access profiles and users.

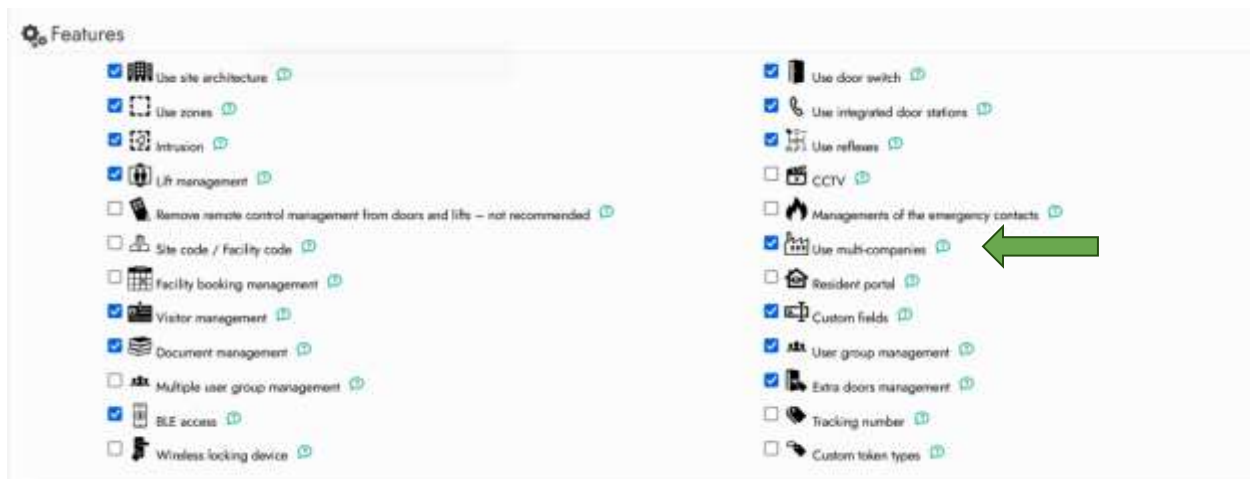
In event management, they only see authorized doors and/or users.

Multi-company management can be applied to other uses, such as residential condominiums: if the building is occupied by condominium owners on some levels and social housing on others. In this case, lessors and condominium managers are seen as two companies, and only see each other's access and common areas.

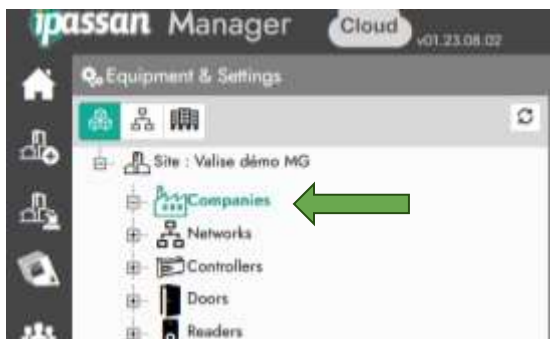
The Cloud version of IPassan facilitates multi-company management, since it's easy to separate the site into networks and connect each independent network to the IPassan.com server. In this case, there's no need to link these central networks together. IPassan.com is the link between them all.

Function activation

By default, the « multi society management » function is disabled. In site wizard / Features, check the “use multi-companies” box.



Company creating



In the “equipment and setting” tab, open the “Companies” node, then click on the “Add a company” button in the right-hand window.

Then enter a name and check “address identical to site” if this company is based at the address already defined for the site or uncheck to enter an address of its own.

Assign societies to devices

Each equipment or site parameter can be linked to one or more companies. For example, a common door can be assigned to several companies, whereas a machine room or office door can only be used by another company.

Company selection applies to the following parameters:

- Controllers
- Readers / doors
- Elevators / floors
- Input / output cards
- Counting / anti-pass back zones
- Access Profile
- Schedules
- Reflexes

Example of a controller:

Controller 0002

Save Cancel Activate third party module More +New Delete

Name * Controller 0002

Identifier Controller serial number

Model 2 wire / IP controller

Expansion card None

Companies ?

Example of a door:

visitor door

Save Cancel +New Delete

Name * visitor door

Position Num 1 Controller Controller 01

Companies x FDI access x AGS x Urmet

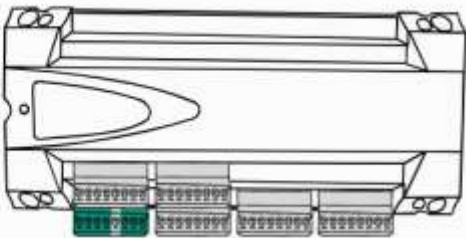
Door release time 5 sec

Time profiles None

Reverse relay

Location

Status X Disconnected



The Previous “Visitor door” is visible and usable by operators of the three selected companies.

These operators can control the door via manual commands, selecting it to create access profiles or view events. At the bottom of this window, you can see a drawing of the controller and the port affiliated to this reader/door.

Assign a company to access profiles & users

The system can manage 1000 access profiles in total. For each profile, one or more companies can be selected. For example, an “Entrance Hall” access profile can be assigned to several companies, while the “office FDI” profile can only be assigned to operators of the “FDI” company.

Example

The screenshot shows the 'Access profiles 0001' configuration window. At the top, there are 'Save' and 'Cancel' buttons. The 'Name' field is set to 'Entrance hall'. Below this, there is a 'Visitor access profile' checkbox which is currently unchecked. The 'Companies' section shows three selected companies: 'FDI access', 'AGS', and 'Urmet', each with a small icon and a close button. Below the companies, there are three tabs: 'Doors', 'Zones', and 'Holidays/maintenance periods'. The 'Doors' tab is active, showing an 'Add reader/door' button. At the bottom, there is a table with columns for 'Name', 'Time profiles', and 'Actions'.

Example of a user:

The screenshot displays a user management interface for 'User name 0001'. At the top, there are 'Save' and 'Cancel' buttons. The form includes the following fields:

- Last name ***: User name 0001
- First name**: First name
- Type**: Resident (dropdown menu)
- Door/zone access**: None (dropdown menu with edit icon)
- Floor access**: None (dropdown menu with edit icon)
- Location**: (field with edit and delete icons)
- Companies**: FDI access (field with add and remove icons)
- auto ***: thermique (dropdown menu)
- User group**: (field with add and remove icons)

On the right side, there is a profile picture placeholder with a 'Browse' button and a 'Save' icon.

“Username 0001” will only be visible and usable by “FDI Access” operators.

Software administrators automatically inherit all rights.

When the multi-company operator profile is created, it is possible to create the operators.

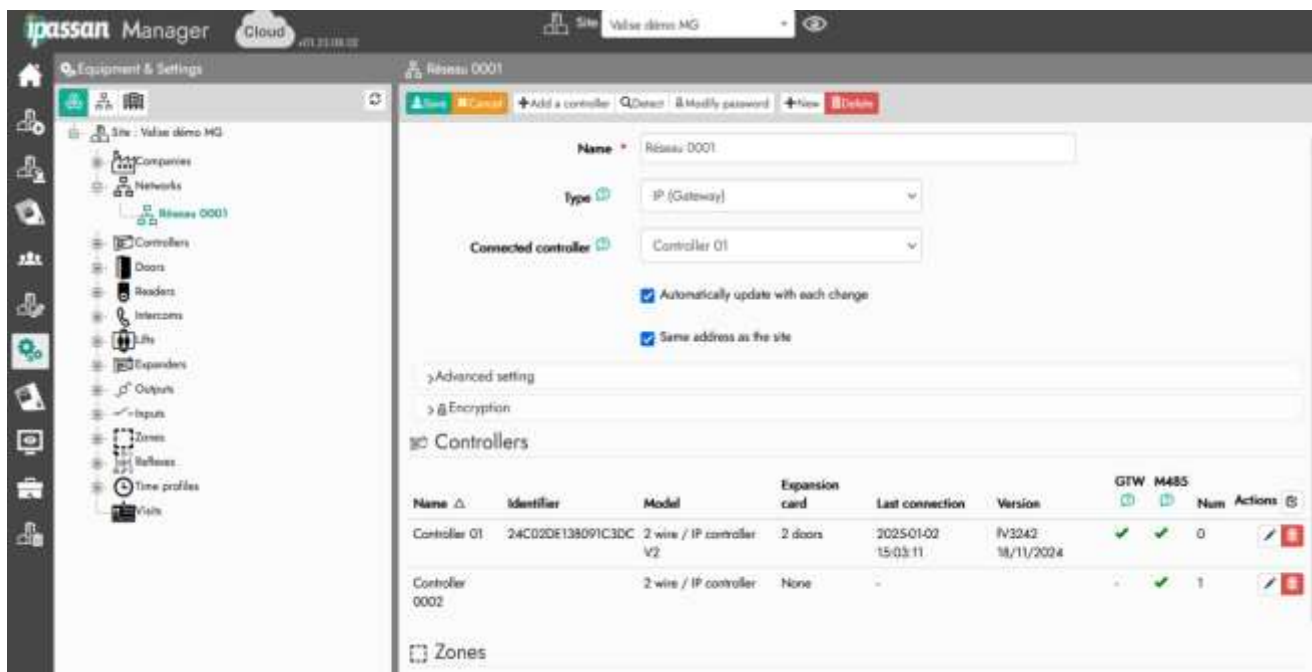
Under the profile, click on “+Add an operator”. This window appears:

3.3. Networks

A network includes up to 64 central units able to communicate with each other. Beyond 64 central units, it is necessary to create another network.

If an organization has sites in different geographical locations, then additional networks must be created. For example, a company with offices in Paris & Lyon plus a production site corresponds to 3 networks in the software.

Then, in day-to-day management, the software operator adds keys to the site without having to manage transfers to one or more networks specifically.



A network is defined as follows:

Connection: this is the dialogue between the server and the first controller. It can be TCP/IP or USB. In the case of USB, the other controllers are linked together in TCP/IP via ethernet cable.

Type: Ip local means that each controller in the network question the server directly. This is the default choice for installation on an internal network. "IP Distant" is referring to a network managed via the Internet. In this case, one controller in the network acts as a gateway for the others.

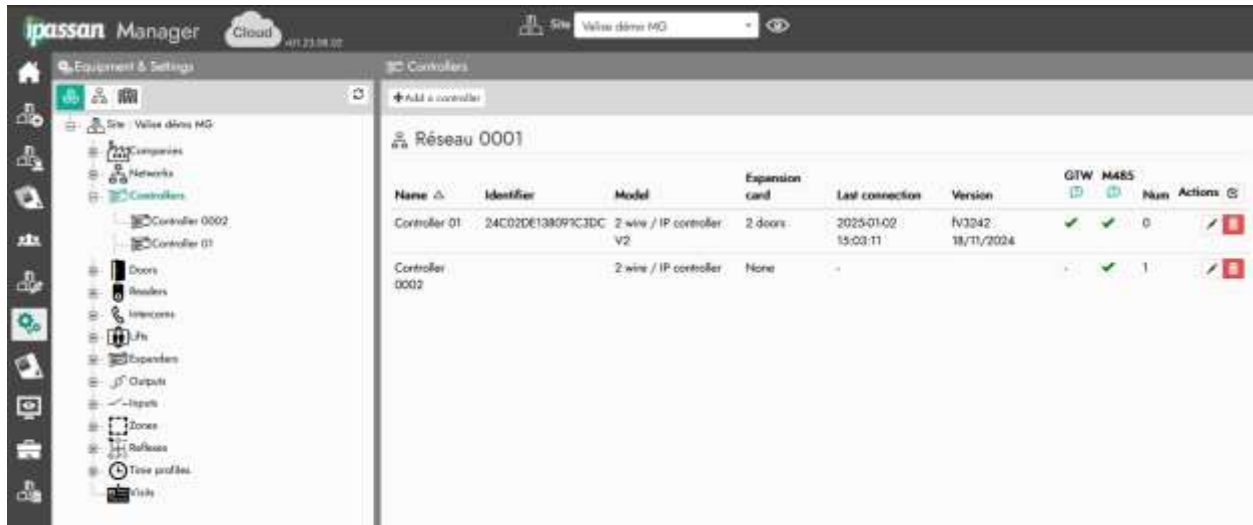
UDP port: controllers use UDP to communicate with each other. This port can be modified when network equipment already uses this port.

This may be the case when the same physical network supports two IPassan controller networks.

3.4. Controllers

The controllers group the intelligence of the access control. It runs the door by freeing the lock if the presented card is entered in the IPassan software.

To see the controllers on the site, click on the gear icon “equipment and settings” on the left. All the devices appear under the “controller” node. By selecting one of them in the treeview (left frame), details open on the right. A controller is defined as follows:



Field	Description
Name	With 32 characters
ID	Id of the controller, written on the label sticked to the cover
Model of the controller	Can't be modified
Options	4 Wiegand doors / 12 outputs / 12 inputs option
Leds	Disable LED lighting
Server communications	Disable server / control panel communications. This option is useful when the control panel is not yet or no longer in service. The server does not try to communicate with it.
TCP/IP configuration	<ul style="list-style-type: none"> - DHCP or fixed IP - If fixed IP, address, mask and gateway - DNS (domain name server), manual or automatic. This information must be entered when the control panel is managed on IPassan.com, for example.
Advanced configuration	The controller can restart daily at a specified time of the day.

3.5. Doors

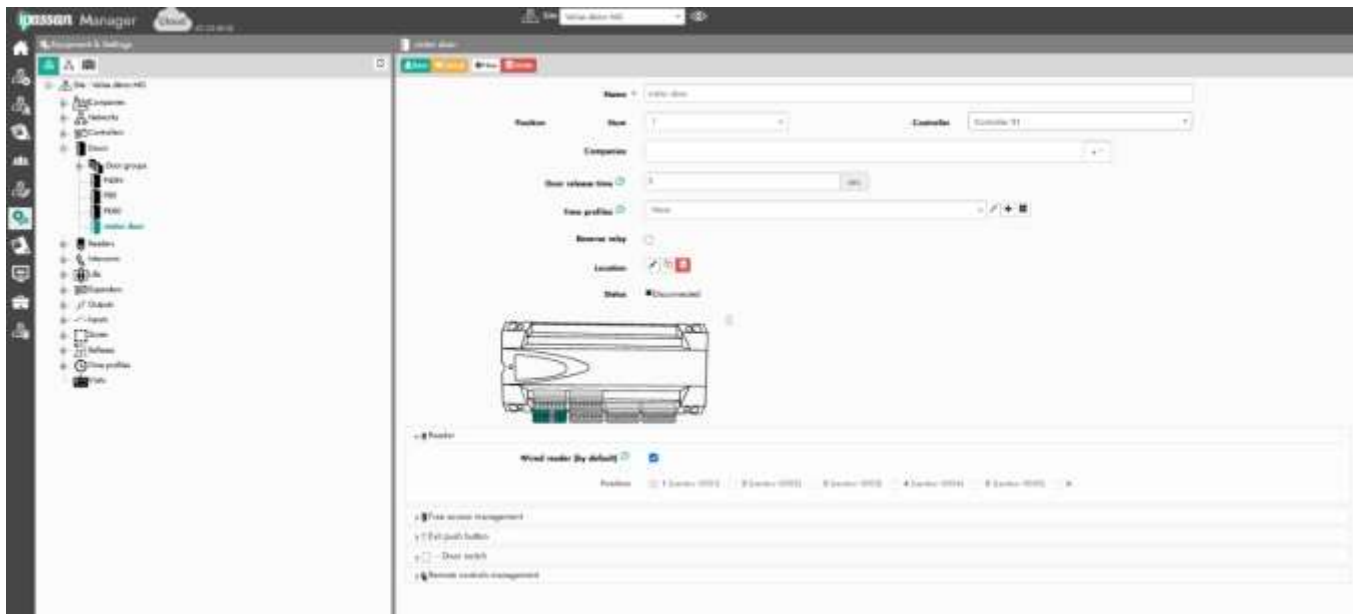
From a hardware point of view, the door is:

- An entry for a Wiegand reader
- An entry for the exit button
- An entry for the door contact
- A relay to control the electric lock

In the software, the following settings can be personalized:

Field	Description
Name	With 32 characters
Position of the controller	Useful function when a reader is linked to a controller but needs to be managed by another one. In this case, schedules, Wiegand configuration or safety related information are also supported by this second controller.
Type	This optional field is available when the function "secure connected locks" is checked on the "site properties". This field specifies if the door is configured as "wired" (standard configuration), or with "secure connected locks". If this second option is selected, a new field is added to the door configuration form.
Schedule profile	A schedule with free access time slots (the door is freed), forbidden time slots (even a valid key doesn't open the door), and regular time slots (a valid key is needed to open the door)
Reader	By default, door 1 is associated with reader 1, door 2 with reader 2. You can link two readers (maximum 6 devices) to one door. This is intended to dedicate one reader to entry and another one for exit. You can link several doors to one reader. For example, from one reader, user A opens the pedestrian door and user B opens the barrier.
Push button	By default, the push button works 24/7. You can apply a schedule and restrict its operation at specific times of the day. For example, to forbid exit through a door after given time. See chapter 4.11.1 to create a schedule with push button. An advanced mode can operate on the link between the exit push button and the door. By default, the input "Push button 1" runs door 1, "push button 2" runs door 2. However, you can link two push buttons to one door.
Door contact	Door contact is a native function within the controller. It can be of various types : all-or-nothing, impedance (the end of line resistance value needs to be specified), or distant contact (if electronic locks are used).

Also check « trigger the security events » if you want to manage « forced door » or « door opened too long » events. In this case, specify the time in seconds after which the door is open too long.



3.6. Readers

The internal or external readers produced by the company FDI can communicate with the IPassan system through wired or connected methods.

- **2Smart readers** (FDI proprietary 2-wire bus with a range of up to 100m)
- **FDI or competitor Wiegand readers** (universal 8-wire bus with a range of up to 100m)
- **RS485 reader:** FDI proprietary 4-wire bus with a range of up to 1000m
IPassan can integrate external readers, such as Dahua license plate recognition cameras or Assa Abloy connected handles.
- With a logical IP cable (e.g., for Dahua license plate recognition camera)
- Through industry gateways that are connected and integrated into the IPassan system (e.g., for electronic handles & locks)

Regardless of the reader or wiring choice, the reader limit per control panel is capped at 6 devices. Example: adding an ANPR (license plate recognition) reader takes the place of a reader on the control panel.

Standard settings

With IPassan manager, the readers are configurable as follows:

field	Description
Nom	With 32 characters
Controller position	Useful function when a reader is linked to a controller but needs to be managed by another one. In this case, schedules, Wiegand configuration or safety related information are also supported by this second controller.
Wiegand configuration	<p>By default, only one credential (key, keypad code, fingerprint....) is enough to have authorized access to a door. With IPassan manager, you can add time condition:</p> <ul style="list-style-type: none"> - Double authentication: during worktime, a key is sufficient to open the door. When the office is closed, you need a key + a pin code. - Time in seconds: between key reading and pin code entry (10 seconds by default) - Dry contact: To enter a car park, you need a key or remote control and a vehicle detected on a magnetic loop. - Door contact: to open door B, you need to open door A first. Thanks to this mode, you can create an entry vestibule. - Manager presence: you can enter only if the manager has already swiped the key at the entrance reader. For example, a production employee can enter the factory only if the Production manager is in the zone.
Configuration Wiegand	<p>Wiegand configuration: by default, the controller adapt to the received protocol. The basic managed protocols are Wiegand 26, 30, 32, 34 bits in hexadecimal</p> <p>You can also choose 34 bits decimal for braille keypads.</p>

Example of configurable fields in the reader menu.

RS485 readers

The 2-wire or Wiegand readers are designed for a maximum distance of 100m. Beyond this, RS485 readers can be used, which can operate up to 1000m with a local 12V power supply.

Important: RS485 readers cannot be added to traditional readers. Each RS485 reader replaces a standard reader. Therefore, the maximum number of readers per controller remains 6.

In the reader configuration, change the default reader type to RS485, then enter the reader's identifier (label on the back) or click the magnifying glass to find the reader on the controller's auxiliary bus.

ANPR reader

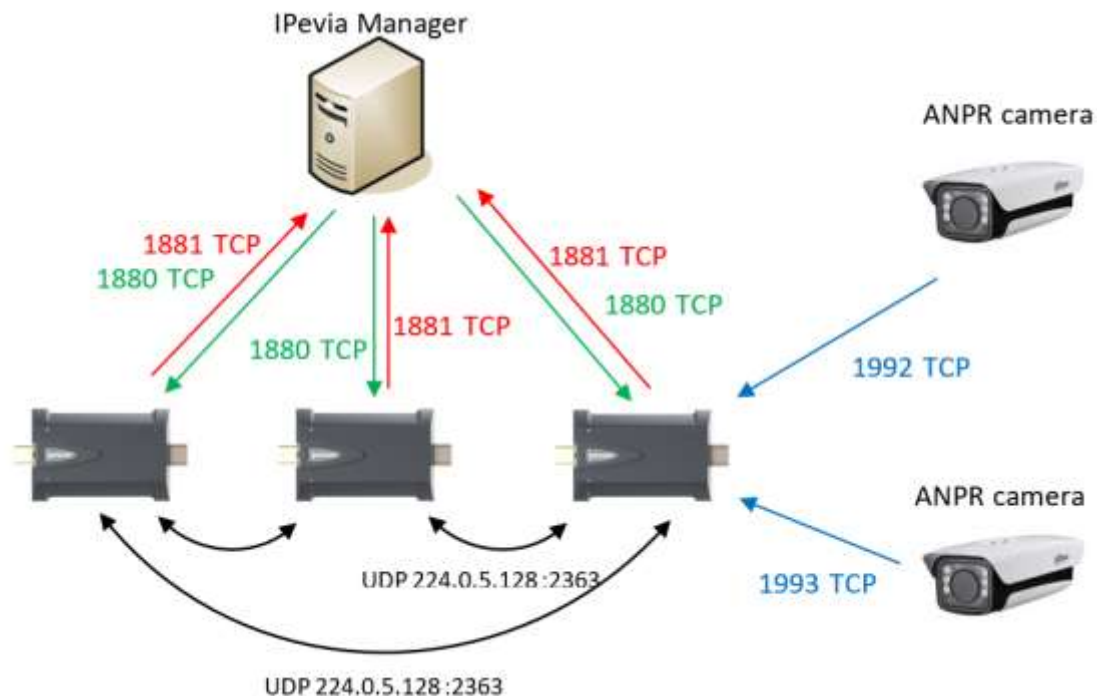
IPassan allows up to 4 license plate recognition (ANPR) cameras to be connected per central unit. These cameras communicate via IP with the central unit and transmit the license plate number in full letters. For example, the plate AG-891-CX programmed in the software will be authorized, not a Wiegand equivalent. Events will also display the plates in clear text, whether the cars are authorized or denied.

Prerequisites: The intelligent integration of ANPR (Automatic Number Plate Recognition) requires an activation card for each central unit managing cameras.

There are two types of ANPR camera integration available in the "reader" menu:

- **Automatic:** As soon as a plate is read, the ANPR system transmits the number to the central unit, which handles it like a token.
- **With Trigger:** When a sensor connected to an input detects a vehicle, the central unit requests the ANPR system to provide the read number.

These integrated cameras (Dahua and OCR Innova software) must communicate with the central unit via TCP. See the diagram below.



After the activation card has been validated for the central unit, you can choose the ANPR type in the reader settings.

Automatic type ANPR

Lecteur 0005

Warning: This reader is not linked to a door

Name * Lecteur 0005

Position Num 6 Controller Controller 01

Companies

Type Anpr

ANPR setting

Type * automatic ANPR

Mode * Socket communication

Ip address of the camera * 192.168.1.1 Port * 1992

Start characters * #1 End characters * \$

Select "automatic" in the ANPR settings tab and enter the IP address and port used by the camera.

To define the communication between the controller and the ANPR used, select the corresponding integrated protocol for the hardware in the "mode" menu.

Mode * Socket communication

camera * Socket communication
Communication by http/json (dahua)

- Socket communication (link between two programs): intended for Dahua cameras with Australian firmware (ITC237) and the OCR Innova software in scenario 4.
- Communication by HTTP/JSON (Dahua): intended for Dahua cameras available in 2022 (non-Australian firmware) such as ITC 437, ITC 415, ITC 237, ITC 215.

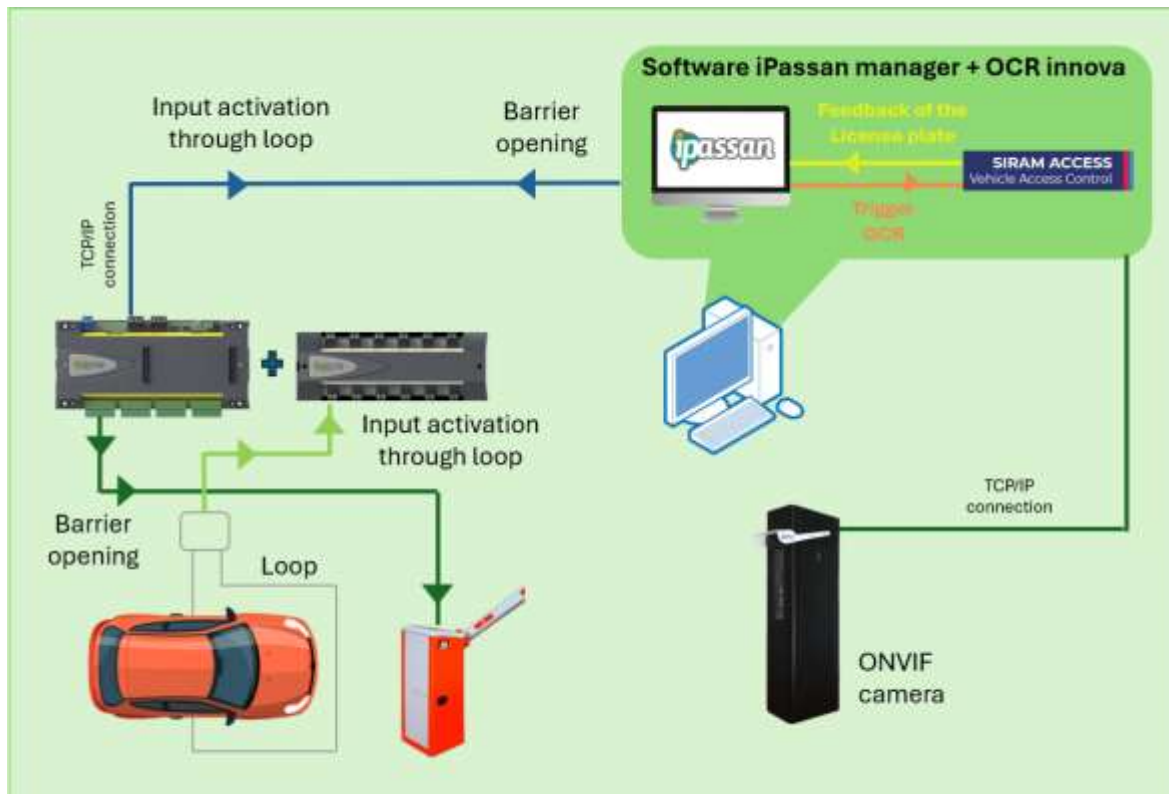
NOTE: the start and end characters are the default characters defined in the communication.

ANPR on trigger

This option is linked to innova OCR (optical character recognition) devices.

More information on : www.innovagroupbcn.com

This integration is based on TCP/IP communication.



When the input connected to the vehicle detector is activated, the controller then requests the OCR (optical character recognition) to transmit the license plate number of this detected vehicle. If the number is recognized, the barrier opens.

Lecteur 0006

Warning: This reader is not linked to a door.

Name * Lecteur 0006

Position Num 6 Controller Controller 01

Companies

Type Anpr

ANPR setting

Type * ANPR External trigger

Ip address of the camera * 192.168.1.1 Port * 1992

row number *

Selected input * Controller 01 - Entrée 0001

Timeout * 5000 ms

For this configuration, the following must be specified:

- The IP address of the computer where the OCR (optical character recognition) Innova is installed.
- The channel number.
- The input used by the vehicle detector.
- Adjustment to the maximum communication delay.

The input used must be configured as an all-or-nothing type (NO normally opened or NC normally closed).

If there are 4 cameras on site, each OCR Innova software will use its respective communication port. By default :

- Channel 1 will use port **22601**.
- Channel 2 will use port **22602**.
- Channel 3 will use port **22603**.
- Channel 4 will use port **22604**.



The camera must also be configured

Connected reader: Apério

The integration of connected locks is available by enabling the option in the site's features (see chapter 2.1).

This integration is based on the use of the "RS485 aux" bus to connect "Apério hubs" linked to "Apério readers and locks": see the diagram below.

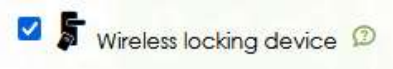


Each IPassan controller can manage up to 6 connected locks through 6 hubs (usual capacity regardless of the door/reader technology).

It is possible to combine "standard" readers and connected devices on the same controller within the same limits.

The smart lock is set up in 5 steps (from A to E):

A- In the site features (see chapter 3.1), check the option :



B- In the "controller" configuration page :

- Select the RS485 Apério bus only compatible with the devices in the range

- Activate the module referenced FD-050-106 (1 per controller using connected readers)



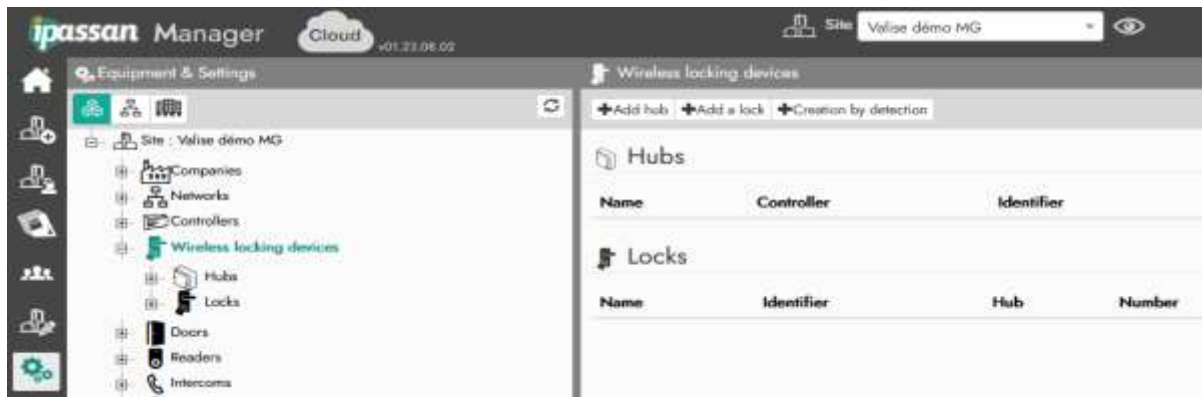
The "RS485 type" is either standard or Aperio.

Modules = N° of the activation card

C- Use the Aperio software to pair hubs and locks (see Aperio user manual for more information)

locks (see Aperio user manual for more information)

D- Open the « electronic secure lock» integration menu to configure those devices.



There are two modes: automatic (D-1) or manual (D-2) :

D-1- Select « Creation by detection » when hubs and locks are connected to IPassan controller RS485 bus.

Each connected device will appear in the table of detected hardware.

Check each line corresponding to the devices that need to be set. It will save all the required data required for the global setup of the material (step D2).

D-2- Select a hub » or « add a lock ». Then fulfill the required fields to finish the setup.



Now that configuration is complete, these connected locks and readers can be used like any other one in the site. You can see access profiles or new events linked to the connected locks.

Readers profile

The behavior of the readers is defined by the controller. By default, it's set as shown below:

Reader profile 0001

Save Cancel

Name * Reader profile 0001

List of behaviours + Add a custom behavior

Name	Color 1	Color 2	Blinking	Duration	Buzzer
Normal behavior	Blue	Blue	Fix single-color		
Access granted	Green	Green	Fix single-color	Event	Long bip
Access denied	Red	Red	Quick single color	Secondes 3 s.	3 short bips
Wait for double identification	Orange	Orange	Fix single-color	Event	Off
Door open for too long	Orange	Orange	Slow single color	Event	Continus bip
Forced door	Orange	Orange	Slow single color	Event	Continus bip
Forced door / free access	Green	Green	Fix single-color	Event	Off
Reader tamper	Red	Red	Slow single color	Event	Off
Double swipes	Green	Green	Quick single color	Secondes 3 s.	3 short bips
Intrusion: zone is in service	Red	Blue	Slow bi-color	Event	Off
Intrusion: zone is in alarm	Orange	Red	Slow bi-color	Event	Continus bip
Intrusion: zone status change	Orange	Blue	Slow bi-color	Event	Long bip

∨ This profile is linked to

Element

Select

However, parameters can be modified to create a personalized reader profile. You can apply them to a specific controller by choosing it below the tab named "this profile is linked to".

3.7. Lifts

An elevator in IPassan is defined as follows:

- A 32-character name
- A position on the controller and the name of the control panel
- Location: To use the elevator functionality in IPassan, it is necessary to create at least the building and floors in the Architecture step during site creation (chapter 2.5).
- Reader: The default setting is 1 reader per elevator car, but you can add a second by unchecking 'default reader' and selecting readers.
- Activation timer: there are two different timers, one in seconds for token users. They present their token to the reader in the cabin, then press the button on their floor.

For visitors, the system manages a time delay in minutes. Usually, the visitor calls from the intercom handset, the switchboard receives the call and authorizes the visitor to open the door via his intercom.

By means of an additional button, the switchboard supplies a dry contact to an IPassan input, authorizing the visitor to use the elevator to reach the right floor only.

In IPassan Manager, check "Intercom", enter the time in minutes and the system input used for each floor.

Floor / output: Because the building has been selected above, the software proposes the correct floor list.

Select the relay associated with each floor.

Schedule: A schedule contains time slots during which the floor is :

- **Non-secure or free access:** the floor button can be selected without a key.
- **Forbidden:** even a valid key cannot access this floor.
- **Normal:** a valid key is required to access the floor.

Intercom: When visitors must be authorized to enter the elevators via intercom system, iPassan uses inputs to retrieve the dry contacts of these intercoms.

Select the input corresponding to each floor.

The screenshot displays the 'Access 0001' configuration window. It features several input fields: 'Name' (Access 0001), 'Position / Name' (1), 'Location' (Block 0001), and 'Controller' (Controller 01). Below these are sections for 'Reader' configuration, including a 'Read reader (by default)' section with a 'Position' dropdown, a 'Release time' field, and a 'Full only ON' checkbox. There is also an 'Interval' field and a 'Please release time from handset' field. At the bottom, a table lists three entries for 'Card 0001', 'Card 0002', and 'Card 0003', each with a 'Name', 'Entry', 'Time profile', and 'Actions' column.

3.8. I/O (input and output) card

Each controller manages up to 10 input/output cards. These cards have a unique identifier which must be entered into the software during commissioning.

A card is defined in the software as follows:

- A32-character name
- A unique identifier of type 517xxxx
- An option: either a 12-input or 12-output card.

For example, reference FD-125-021 is a 10-input RS485 card with a 12-output option.

The screenshot shows the iPassan Manager software interface. The sidebar on the left contains a tree view with the following structure:

- Site: Value d'Info HQ
 - Companies
 - Networks
 - Controllers
 - Doors
 - Readers
 - Intercoms
 - Alarms
 - Expanders
 - Card ES-0001
 - Expander 0001
 - Outputs
 - Inputs
 - Accessories
 - Time profiles
 - Events

The main configuration area for 'Expander 0001' contains the following fields:

- Name: Expander 0001
- Identifier: Expander serial number
- Model: 10 zone inputs (with and management)
- Expansion card: None
- Controller: Controller-01
- Companies: (empty field)
- Location: (empty field)
- Activation of links: ☒

Below the configuration fields, there are two tables:

Outputs

Name	Num	Used by	Door release time (s)	Output inverted	Location

Inputs

Name	Num	Used by	Type	Location
Expander 0001 - input 0001	1	-	2 state input (on / off)	
Expander 0001 - input 0002	2	-	2 state input (on / off)	
Expander 0001 - input 0003	3	-	2 state input (on / off)	
Expander 0001 - input 0004	4	-	2 state input (on / off)	

Details of the inputs and/or outputs managed by this card are displayed at the bottom of the window.

3.9. Input

From a hardware point of view, IPassan 's inputs are either a 12-input option on the controller, or a remote card on the RS485 bus.



A controller whose “RS485Aux” bus is configured to communicate with the Aperio system cannot communicate with RS485 fdi inputs/outputs or readers.

An input is defined as follows:

- A name with 32 characters
- An input type:
 - **All or nothing:** where the input is whether an active or inactive kind. The input can be set up such as normally opened or normally closed (NO/NC)
 - **Impedance (EOL):** via end-of-line resistors, the input differentiates between open-circuits (wire break/sabotage), short circuit (sabotage), inactive input and active input. Select the resistance values R1 (series) and R2 (parallel).
 - **Decimal input:** depending on the received signal, the controller attributes a decimal value. Depending on this value, you can set thresholds to trigger reflexes for example.

Note that an impedance input is always of type NC (normally closed).

Example of “all-or-nothing” input:

Example of impedance input. The values of resistance must be entered into the software:

Expander 0001 - Input 0001

Name: Expander 0001 - Input 0001

Device: Expander 0001 Num: 1

Companies: [Empty field]

Use this input as: EOL management input

End of line resistor1: Default (4.7 kΩ)

End of line resistor2: Default (10 kΩ)

Input status: ☐ Normally open ☒ Normally closed

Location: [Edit icon] [Reset icon] [Red square icon]

> Options

Save Cancel

Example of a decimal input:

Expander 0001 - Input 0001

Name: Expander 0001 - Input 0001

Device: Expander 0001 Num: 1

Companies: [Empty field]

Use this input as: Decimal input

Location: [Edit icon] [Reset icon] [Red square icon]

Threshold setup

Threshold	Value	Range
Threshold 1	3047	(0 to 4095)
Threshold 2	4095	(0 to 4095)
Threshold 3	4095	(0 to 4095)

> Options

Save Cancel

Input adaptation settings

The screenshot shows a configuration window titled 'Options'. It contains the following settings:

- Anti-bounce back value:** A text input field with the value '80' and a unit dropdown set to 'ms'.
- Delay under threshold 1:** A time selector with 'Hours', 'Minutes', and 'Seconds' fields, all set to '0'.
- Delay between thresholds 1 & 2:** A time selector with 'Hours', 'Minutes', and 'Seconds' fields, all set to '0'.
- Delay between thresholds 2 & 3:** A time selector with 'Hours', 'Minutes', and 'Seconds' fields, all set to '0'.
- Delay above threshold 3:** A time selector with 'Hours', 'Minutes', and 'Seconds' fields, all set to '0'.
- Differential validating the threshold move:** A text input field with the value '0'.

Individual input settings allow you to adjust the behavior of the input as close as possible to the signal, or to set a switchover delay before the state of the input changes in the controller.

Anti-bounce value consists of fine filtering the signal and ignoring interference. If set at 80m/s, the controller will ignore any signal if it occurs less than 80m/s after the last signal.

“Differential validating the threshold move” is the minimum value required to switch to another status (total range is 0 to 4095)

To monitor the input, the controller can watch impedance or TOR (active/inactive) selection.

According to the value of 2 resistances (R1 & R2), there are 4 different states for each input

- Short-circuit
- No detection
- Detection
- Disconnected

The transfer of this status information to the controller can be delayed in the input card by adding a “status hold timer”. This adds the function of integrating the signal, improving your operation:

Adding a 30 s delay to an input connected to a limit switch ensures that the position is reached, the movement completed...

3.10. Exits

IPassan outputs are either a 12-output option inserted on the controller, or the same option inserted on a 10-input RS485 bus card. An output is defined as follows:

Field	Description
Name	32 characters name
Time profiles	<p>If required, you can add a timetable to an input. A schedule contains time slots during which the output is :</p> <ul style="list-style-type: none"> - Forced stuck: the output remains active, whatever commands it may receive (process, reflex, elevator control). - Forced idle: the output remains idle regardless of commands - Normal: an action (e.g. reflex or presentation of token to elevator reader) is required to activate the output.
operation	<ul style="list-style-type: none"> - Monostable corresponds to activation for the programmed time. - Maintained corresponds to activation until the next deactivation condition.
Release time	Enter the duration in seconds for which the output will be activated (case of activation / independent of forcing).
Output inverted	<p>Select the relay status in the event of a power failure. For example, we'd like the output to be closed at rest, but open in the event of a power failure.</p> <p>We therefore wire NO contact, but define the output as inverted.</p>

3.11. Anti-pass back (APB)

IPassan offers the possibility of managing counting or anti-pass back. A counting zone is defined by entry and exit gates/readers. The system knows how many people or vehicles are in the zone and can block entry when a threshold is reached.

This feature is useful for parking lots but can also be used to limit the number of people in an area (swimming pool, common room).

An additional IPassan option allows you to count by apartment, group of people or company.

Examples of when APB is relevant: **in a commercial parking lot**, several companies use the same parking lot, but each only has a predefined number of spaces. Company A's employees all have tokens, but only a certain number can park at the same time. For counting to be effective, anti-pass back is often associated with counting. APB prevents a user from entering a zone until he or she has left it.

In the “equipment and settings” tab (on the left frame), select “zone” in the treeview”. Select or create a zone. At the bottom of this window, select the “anti-pass back” check box to access the other settings.

The screenshot shows the IPassan software interface for configuring a zone. The window is titled "Zone" and has a sidebar with "Equipment and settings" selected. The main area contains the following sections:

- Name:** A text field with the value "example".
- Company:** A dropdown menu.
- Entrances:** A list of readers with the value "1.1932 - Station process 0003". Below it is an "Add reader/door" button.
- Exits:** A list of readers with the value "1.1932 - Station process 0003". Below it is an "Add reader/door" button.
- Anti-pass Back:** A section with several checkboxes:
 - ☐ Anti-pass time (Cancellation time): 00:00
 - ☐ Authorize the entrance to the zone in case of communication fault
 - ☒ Anti-pass Back
 - ☐ Anti-pass time (Cancellation time): 10
 - ☒ Anti on entry only
 - ☒ Authorized allowed pass after the end of validity
- Counting:** A section with a dropdown menu for "Type of counting" set to "Global". Below it is an "Interdiction threshold" section with three thresholds:
 - Alarm:** 20
 - Warning:** 10
 - Info:** 5

As you can see in the screenshot above, IPassan offers three types of anti-pass back

- **Anti pass time (cancellation time):** the APB is cancelled after a programmed delay
- **APB on entry only:** in this case : users are always authorized to exit.
- **Authorized allowed even after the end of validity (or Soft Apb):** users can exit the zone even after the validity period has expired. The only condition to be authorized to exit is to be present in the zone.

This option is useful for visitors leaving the parking lot after their visit has ended.

Create a counting zone

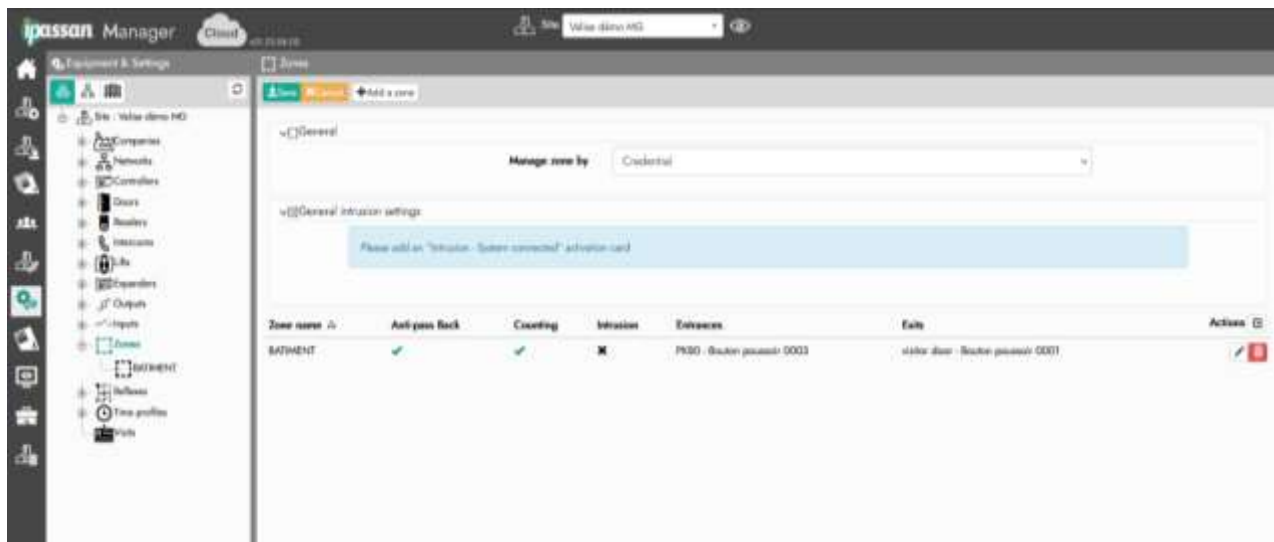
IPassan manages zones in which you can activate global counting or counting by apartment, company or group. The APB option can be added.

The “ZONE” checkbox must be enabled in the site properties (see chapter 2.2).

IPassan allows you to count by credential (key, fingerprint, license plate) or by user.

- With the first option, a user entering a zone with a license plate must leave by using the same credential.
- With the second option, the user can enter a zone with a license plate and exit with a card, because the license plate reading would not have worked.

In the next screen, select the desired option on the list next to “manage zone by”.



Click on the “add a zone” button.

A zone is defined as follows:

- **One or more entry readers** entered in the “entrances” section.
- **One or more exit readers** entered in the “exits section”
- **Entry or exit pushbuttons.** The system then counts only the number of people in the zone, without knowing the identity of those present. They must be entered in the “entrances” or “exits” sections. These push-button inputs can be linked to infrared sensors or turnstiles, for example. So, we know how many cars/users are present in the zone.
- **List of access profiles** managed by the zone.
- **Maintenance personnel or janitors**, for example, are not subject to APB and counting.
- Three programmable thresholds
 - The first two thresholds can be used to control actions (relay activation, sending a message on screen or by e-mail).
 - The third threshold, known as the alarm threshold, blocks any new entry to the zone.

Advanced settings

- **Reset the zone everyday:** at a set time, the zone is cleared by software.
- **“Authorize the entrance to the zone in case of communication lost”:** if the in-between controller connection is lost, the access control authorizes to enter the zone. This option is made to avoid people getting stuck in the zone.
- **Counting by apartments, companies, etc...**
 - 1) Architecture creating: the « architecture » function must have been checked in the site properties (see chapter 2.5 for more information).

- 2) Create the apartments, users and titles in the software.

Type	Code	Permanent	Status
Mifare+	803FCAB866204	✓	✓
Mifare+ remote control	8061330A5D7004	✓	✓

- 3) Select the counting zone by apartments in the zone settings.

By default, the number of parking spaces is identical for all apartments, but it is possible to customize them by unchecking "Setup the same threshold for all elements".

A new window then appears, where you can enter the authorized threshold for each apartment, company, group of people, etc.

Name	Threshold

Beforehand, apartments must have been entered in the software. See the chapter 2.5 architecture for more information.

3.12. Schedule and public holiday / work period

IPassan offers different types of schedules:

- **Key access schedule:** a key operates only at authorized times.
- **Door, exit or floor schedule:** the door or floor is freely accessible, locked or requires a key to be controlled according to time slots.
- **Reader schedule:** depending on the time of day, a valid key is sufficient, or another condition must be met. For example, a pin code must be entered, an alarm contact must be deactivated, etc.
- **Process schedule:** processes used in reflexes operate according to time slots.
- **Intercom schedule:** names displayed on 2Smart panels are only displayed at programmed times.

A time profile includes 7 days of the week plus one public holiday and one workday. This means that a person can have different access depending on the current period (normal, holiday, work).

In the example below (capture chapter 4.11.1), considering that the user uses the office profile at one door and that it is a Thursday,

- He is authorized from 8am to 5:30pm in normal period
- He is authorized from 8:00 a.m. to 12:30 p.m. during public holidays
- It has no access during work periods

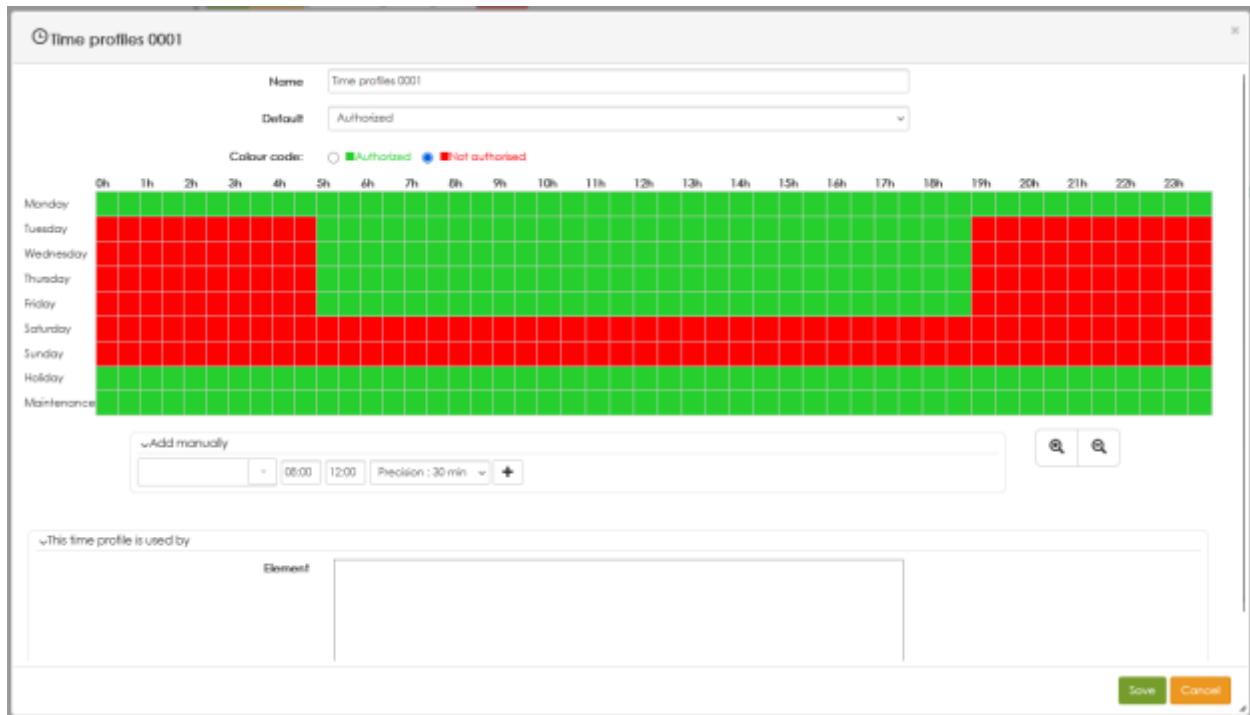
Public holidays and work periods are declared in chapter 3.13.6 and then applied to access profiles, doors, exits, floors or processes.

IPassan manages up to 200 schedules (all combined)

Access schedule

Access schedules(or time profiles) are used in door or floor access profiles. There are two ways to create access time profiles :

- Click “equipment and settings” on the left frame. Select a door on the tree view. Click the “+” at the right of the field “time profile”.
- Click “users & access profiles” on the left frame and click on the + below the “time profiles” column.



For the same access profile, doors or floors can use different time profiles. For example, users have 24/7 access to one door, 08:00-20:00 to another and 08:00-17:00 to a third.

In the following view, keys are authorized during green periods.

Note: by clicking on the + or - buttons, you can enlarge the area and select 5-minute slots.

Door, exit or floor schedule

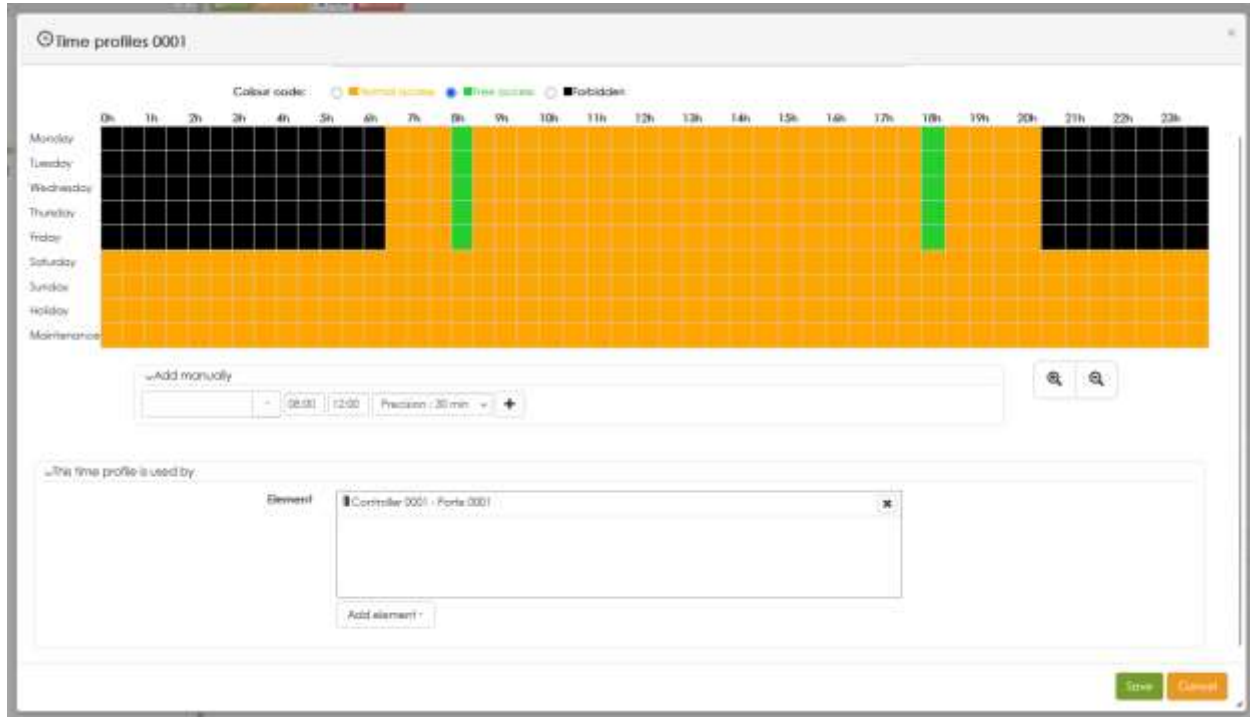
“Relay” schedules have three states:

- Stuck (free access): the door, exit or floor is activated regardless of token or reflex operation.
- At rest (access denied): even a valid key cannot open the door or exit.
- Normal (normal access): doors, floors or exits are activated according to programmed access or reflexes.

In the example below, the doors and floors selected in the lower frame are

- Forbidden (relay at rest) at times shown in black (8:30 p.m. to 6:30 a.m. on weekdays)
- Free access (relay stuck) between 8 a.m. and 8.30 a.m., then 6 p.m. and 6.30 p.m.

- Secured (normal access), but accessible with a valid key during orange periods

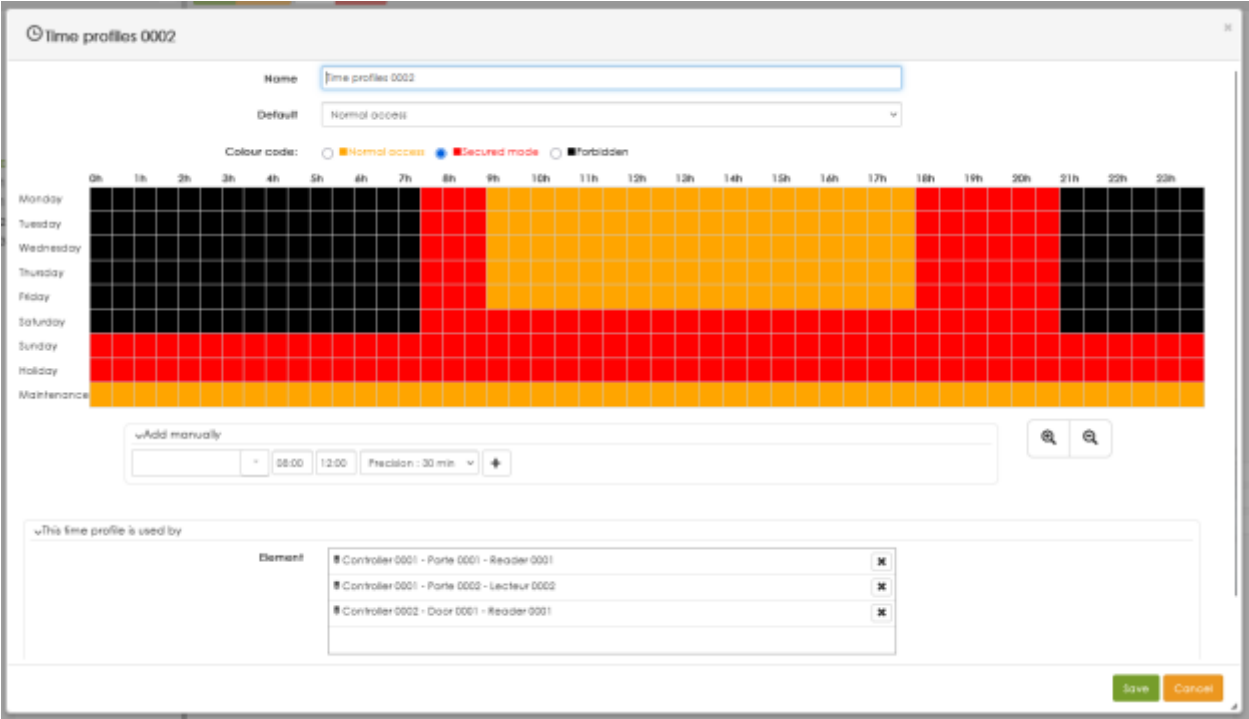


Reader schedule

A door can be managed by several readers. For example, an office entrance has an entry and an exit reader. In this case, the behavior of these devices can be differentiated with a key + code to enter, but just a key to exit.

In the following example, the building's entry readers function as follows:

- No access possible at night from 9 pm to 7:30 am, Monday to Saturday inclusive.
- Secure access (key + pin code)
 - Monday to Friday, 7.30 a.m. to 9 a.m. and 6 p.m. to 9 p.m.
 - Saturday from 7:30am to 9pm
 - All Sunday
 - All public holidays
- Key access Monday to Friday, 9am to



Process schedule

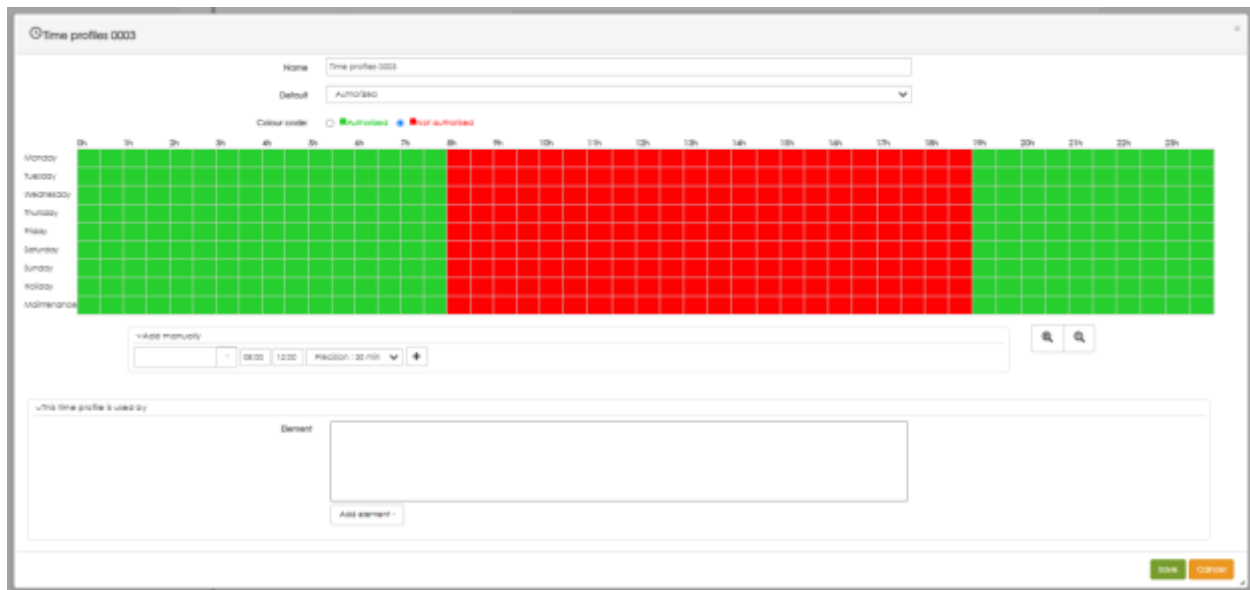
IPassan manages reflexes. It is the sum of 1 or more conditions which, when “true”, trigger one or more processes.

- An example of a condition is a forced door.
- A process could be sending an e-mail or activating a relay.

IPassan lets you manage schedules for these processes. For example, for a “forced door” event, the same people may not be notified during the day or night.

To schedule a reflex, select it on the “equipment and settings” menu. In the field “time profiles” select an already defined one. By clicking on the “+” button on the right, you can create a new time profile.

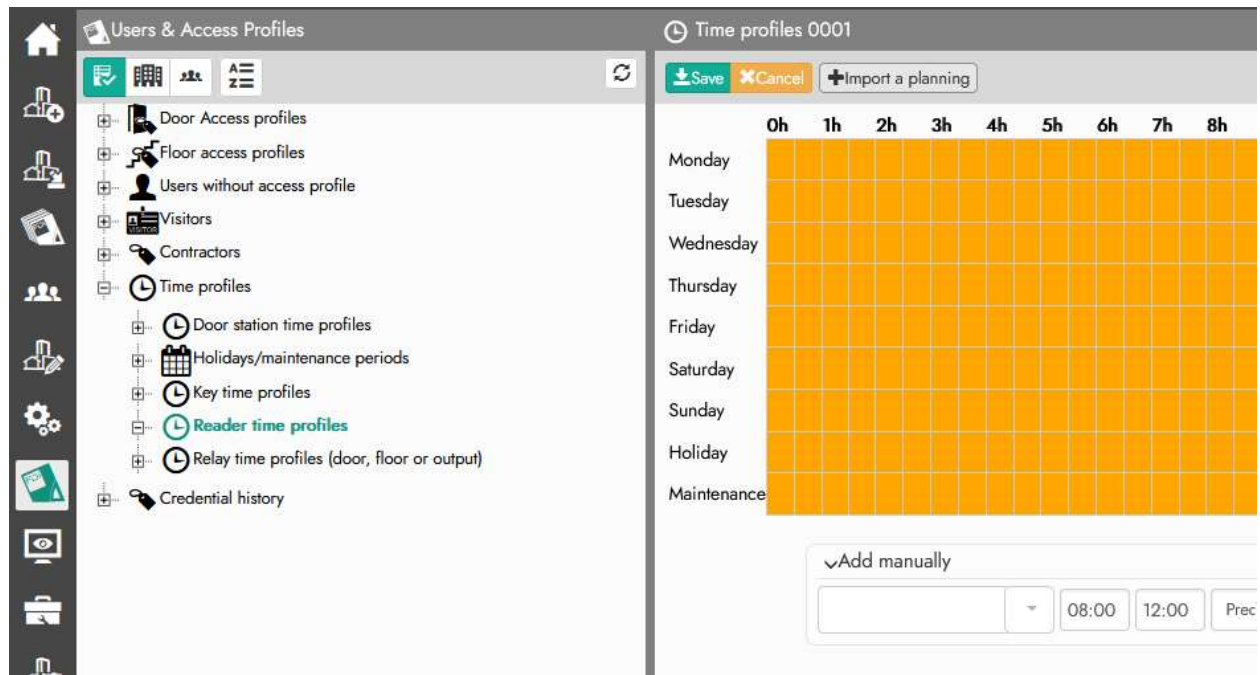
In the following example, a process will only operate at night.



Copying time profiles

IPassan Manager controls several time profiles. However, it can be useful to use a schedule for doors and use this same slot for processes or keys.

For that, it's necessary to create a new schedule and to import the time slot in the original profile. When the new schedule is created, click on the "import a planning" button.



The following window appears :

Select the schedule to duplicate. For each option, indicate the new behavior.

Note: some schedules can have two different statuses (authorized or refused) for a key or three different states for a reader (refused, access with key or key + code). Click "OK" to confirm the change.

Public holidays

Holidays or work periods automatically modify the conduct of doors, floors, access profiles, etc.... according to predefined dates.

The modification can be secured. For example, a floor is free on Thursday mornings from 8am to 12pm but is secured when Thursday is a public holiday. Conversely, the door is free on Sundays and on public holidays.

One way to create a public holiday period is to click on the access profile button on the left frame. Then select the access profile and the "holiday/maintenance periods" tab. Select the "add a period" button".

The following example shows a public holiday period starting on December 22 at 5pm and ending on Friday January 2 at 7am. This holiday period is tracked by doors, access profiles, floors, exits or processes.

A “Repeat every year” checkbox makes it easy to manage fixed dates.

Important: if a day is both a holiday and a workday, priority is given to the “work” behavior.

3.13. Video integration

IPassan Manager lets you integrate video surveillance via RTSP (real time streaming protocol).

All NVRs (video recorders) supporting this protocol can be integrated into IPassan, provided you know the corresponding RTSP Live and playback links.

General

By integrating video surveillance with access control, a link is created between a camera and a door, for example.

So, if a door is forced open, the software operator visualizes the event on screen and clicks on the video button to see the record of the break-in.

How does it work?

In the software, a camera is linked to a door, a reader, an entrance or exit, etc.... So when an event concerns this element, an icon showing a camera is available on the event line.

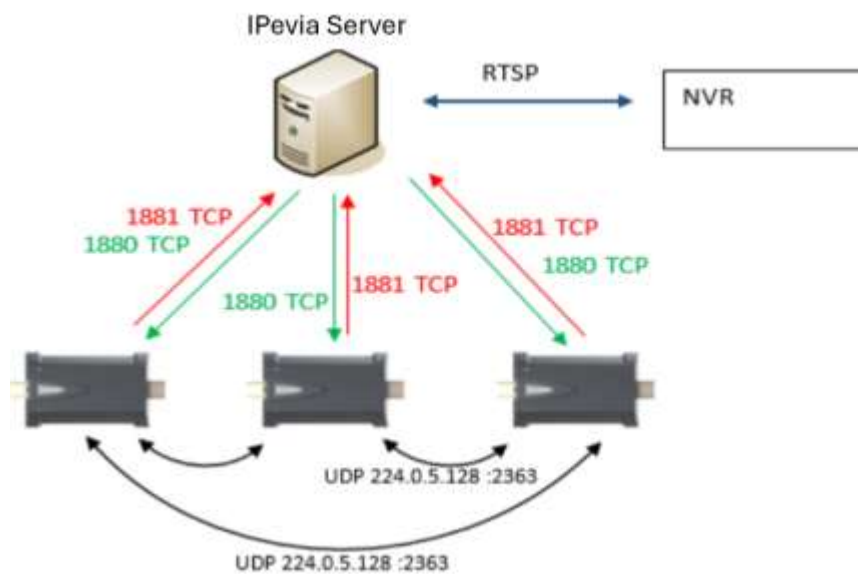
This integration works for both live and replay.

To access the video servers of the CCTV, you need to check this function on the site configuration. Go to site wizard and select the “function tab”. To get more information about this, see the “2.2 features” chapter.

Synoptic

The controllers are not directly involved in this integration; they save the events and transmit them to the server, but it is the server that maintains the link between the cameras and the entrances, doors and readers.

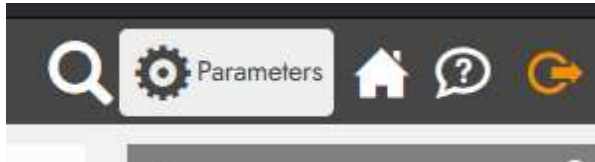
So it's the IPassan server that communicates with the NVRs.



Choosing RTSP reading software

IPassan manager controls the link with video servers. However, it does not display the RTSP stream directly. You need to select an external player (VLC, for example).

Select the application setting button at the top right. If this one doesn't appear, it means that the CCTV function hasn't been selected on the site configuration. See chapter 2.2 for more information



Then it displays the following window.

A screenshot of a web application window titled 'Parameters of the application.'. Inside the window, there is a section titled 'Video stream' with a folder icon. Below this, there are three input fields: 'Stream type' (a dropdown menu showing 'VLC'), 'Link to the software' (a text input field), and 'Backup folder' (a text input field with a folder icon). To the right of the 'Link to the software' field is a green 'Test' button. Below the 'Backup folder' field is a green 'Download VLC' button. At the bottom right of the window are two buttons: a green 'Valider' button and an orange 'Annuler' button.

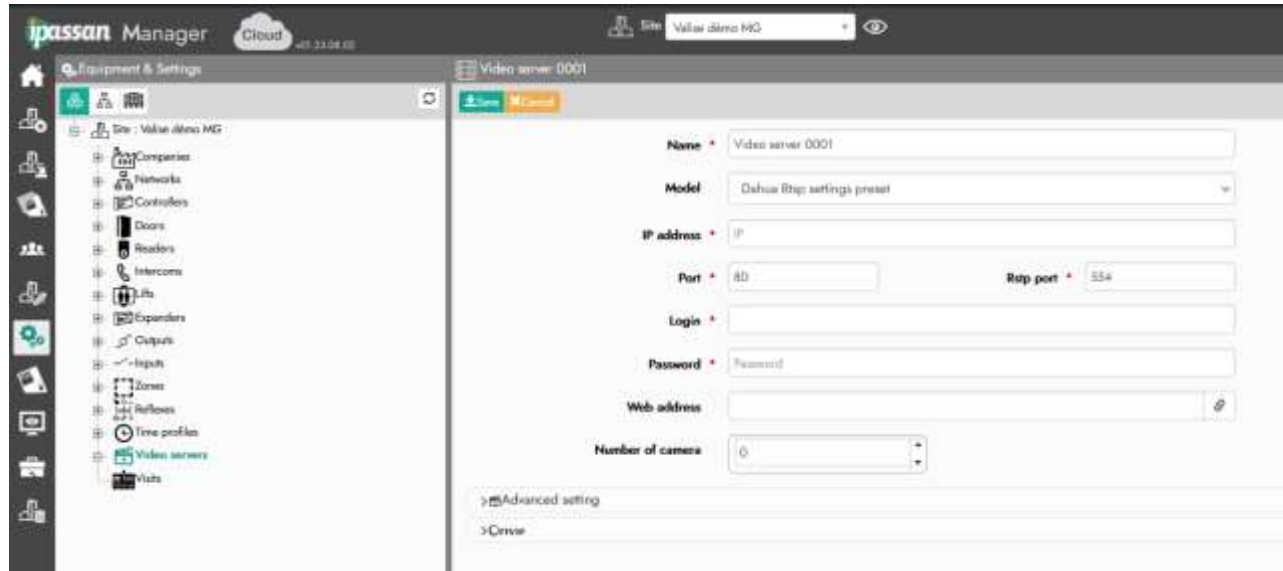
Enter the path to the chosen application.

Note: VLC is a free program that can read RTSP streams. It can be chosen to play videos from NVRs.

Enter the path to the player and the directory where the videos will be saved.

Settings

Note that IPassan Manager can detect ONVIF devices on the network (a standard protocol for communication between IP surveillance devices). The software would detect if the NVRs used on-site are ONVIF for their communication with third-party equipment, and not only for camera integration.



Go to the “equipment & settings” menu and choose “video server” on the left tree view. Click on the “add a video server” button at the top of the page.

- Enter a name for the server, its IP address, and RTSP/web communication ports.
- Choose the right model within the list
- Enter the login and password, then click Save.
- Note that the RTSP protocol is opened and shared by many recorder brands. However, each brand uses its own syntax. Example of RTSP link for Urmet live: `rtsp://[username]:[password]@[ipaddress]:[rtspport]/ch[camnum]/0` IPassan offers three presets: Urmet, Dahua and HIK. To integrate another brand, the appropriate informations must be manually entered as shown below.

Advanced section configuration:

If the NVR is not one of the models for which a preset is available, enter the RTSP strings for live and replay, then specify the date/time format used by the NVR. Two fields allow you to enter the number of seconds before the event and the number of seconds after the event.

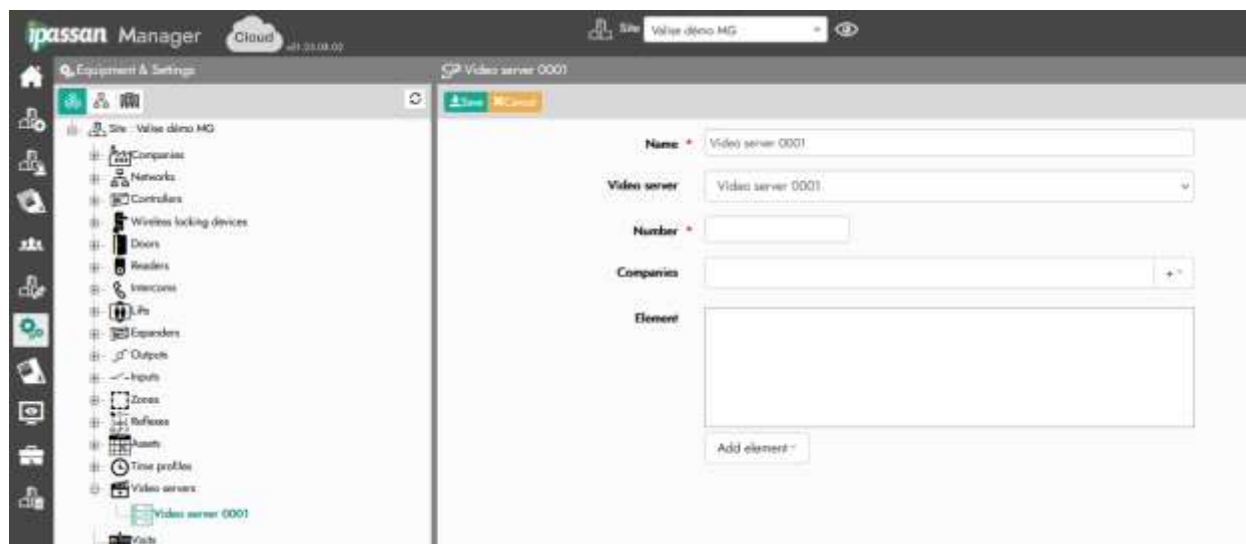


Note that these two times (before and after the event) only concern the preview in IPassan Manager. It is possible to view more cameras or a broader period on the NVR.

As shown below, for each camera, select the doors, readers, push buttons, inputs or outputs involved. In the supervision view, for each event concerning these elements (entry, reader, etc.), a button displaying a camera will be clickable.

Note that a camera can be linked to multiple elements, and an element such as a door can be linked to multiple cameras. For example, a camera monitors both the entrance and exit of a parking lot (two readers), or conversely, two cameras monitor the same visitor door but from two different angles.

To link the camera to an equipment, select the video server in “equipment and settings” and click the “add a camera” button at the top of the window. Then in the element section, select the door, reader, etc... that needs to be linked to this camera.



4. Intrusion

IPassan controllers incorporate intrusion functionality.

Two intrusion concepts are available:

- "Unconnected" intrusion with dry contacts
- "Connected" intrusion with Elcron/Medea controllers

Connected intrusion requires an activation card, while dry contact intrusion does not. By default, the selected intrusion mode is "dry contact".

It should be noted that it is not possible to combine the two intrusion concepts.

4.1. Dry contact intrusion

Zone settings

Intrusion settings can be accessed in the site zone settings.

Select « Dry contacts within the list of the integration type.

Commissioning by :

- **Double/triple swipe:** arming of the area is available only by people with the right to arm/disarm the intrusion into this area.
- **Commissioning when the zone is empty:** only applies to areas that also manage counting

Decommissioning by :

- **First swipe authorized (without alarm rights):** disarmament of the area possible by any person having access to the area.
- **First swipe authorized:** the alarm is decommissioned only if the user has the right to do so.

- **Double / Triple swipe:** Disarmament of the area is possible only by people with the right to arm/disarm intrusion into this area.
- **Zone presence decommissioning:** If this box is checked, the alarm will be disarmed as soon as the zone has at least one person.

Late departure: this feature allows you to postpone an alarm commissioning.

▼

☒ Late departure

Activated by

Single swipe ▼

Time before application of the
"Late departure" reader
behaviour

10

min

Delayed start time

30

min

Activated by: the behavior that will postpone the alarm commissioning. It can be a single/double or triple swipe.

Time before application of the “late departure” reader behavior: the period before the normal time of commissioning that a user can use the late departure function. For example, if 10 minutes is entered in this field, and the alarm is normally triggered at 10pm, the user will be able to use “late departure” from 09:50pm.

Delayed start time: the period during which the triggering of the alarm will be delayed.

Zone intrusion settings

To apply intrusion to a zone, check the “intrusion (dry contact)” box. Then you can access to numerous configurable fields.

▼ ☒ Intrusion (Dry contact)

Commissioning output: None

Out of Service: None

Report zone in alarm: None

Zone status report: None

Time profiles: None

☒ Enable time-dependent commissioning

☒ Enable time-controlled shutdown

Options

☐ Commissioning via an input

☒ Late departure is applied to this zone

Doors concerned

Add reader/door

For each zone you must define:

- 2 outputs to commission, decommission the zone.
- 2 inputs to know the intrusion status of the zone (commissioned or decommissioned)
- 1 optional input to control the intrusion commissioning via external command (see chapter 5.3 manual commands).

You can apply a time profile to the alarm commissioning/decommissioning.

4.2. Elkron/Medea Intrusion

Prerequisite

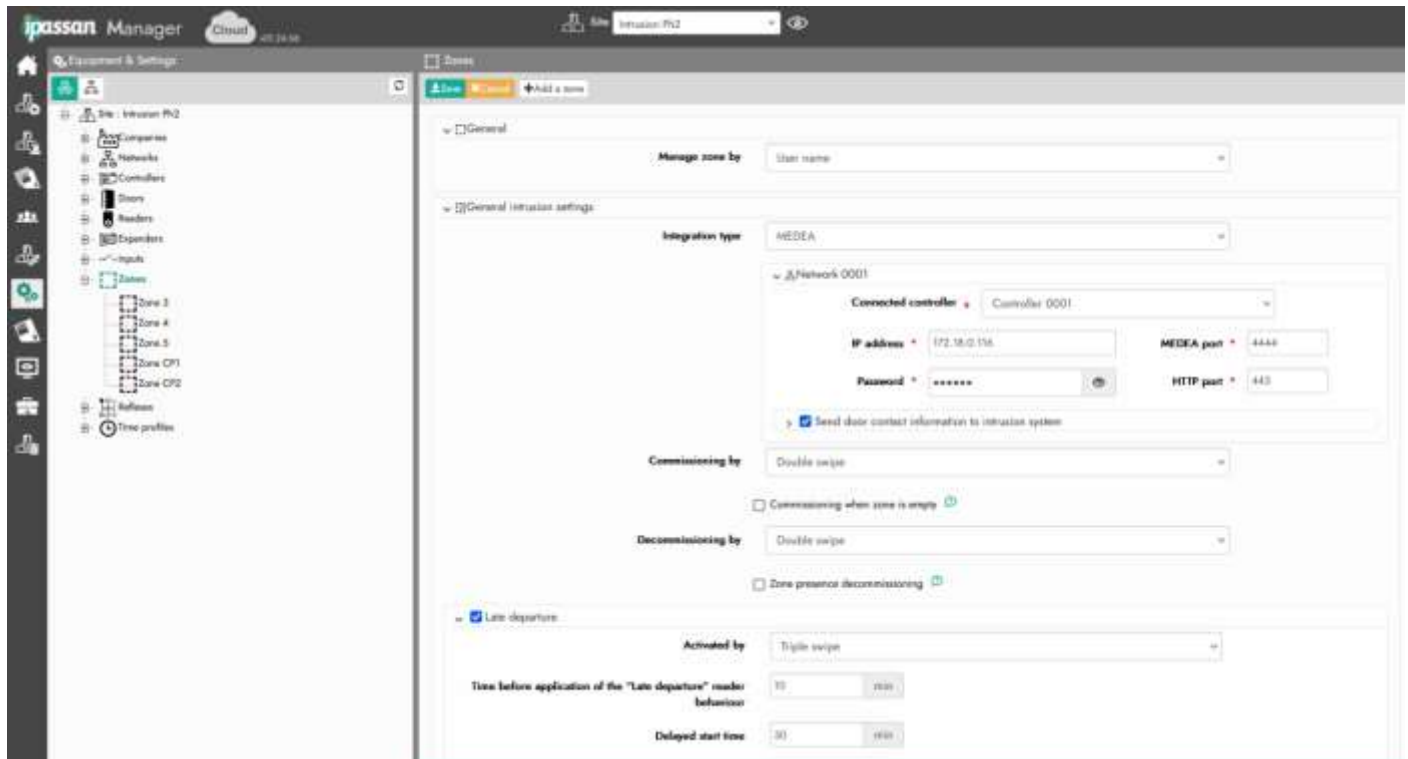
To set up the intrusion, check the « intrusion » function in the site creation wizard (see chapter 2.2).

Verify the following compatibility factors:

- **Access control software** : version > 1.23.06
- **V2 controllers (with a serial number x4Cx2DExxxxxyyyy)** firmware version >= fV3230.
- **Activation card of the intrusion function:** that you need to enter in the software. Select a controller in the “equipment and settings” menu. Then select the “activate a module” button at the top of the window.
- **Multi technologies Reader** version >=3071

Zone intrusion settings

Intrusion management is defined by sectors in the Medea controller. It is also associated with zones in the access control software. To manage the main settings of the intrusion, select **"Equipment and settings"** in the left frame, then click on the line **"zone"**.



Under the **"General intrusion settings"** tab, select the **IPassan controller connected to the Medea system**. If there are multiple devices on this site/network, then multiple devices will appear in this list. Enter the **IP address** and password of the Elkrone/Medea controller.

In the last fields, specify the modes of commissioning/decommissioning of the zones.

Commissioning by:

- Double/triple swipe: arming of the area is available only by people with the right to arm/disarm the intrusion into this area.
- **Commissioning when the zone is empty**: only applies to areas that also manage counting

Decommissioning by:

- **First swipe authorized (without alarm rights)**: disarmament of the area possible by any person having access to the area.
- **First swipe authorized**: the alarm is decommissioned only if the user has the right to do so.
- **Double / Triple swipe**: Disarmament of the area is possible only by people with the right to arm/disarm intrusion into this area.

- **Zone presence decommissioning:** If this box is checked, the alarm will be disarmed as soon as the zone has at least one person.

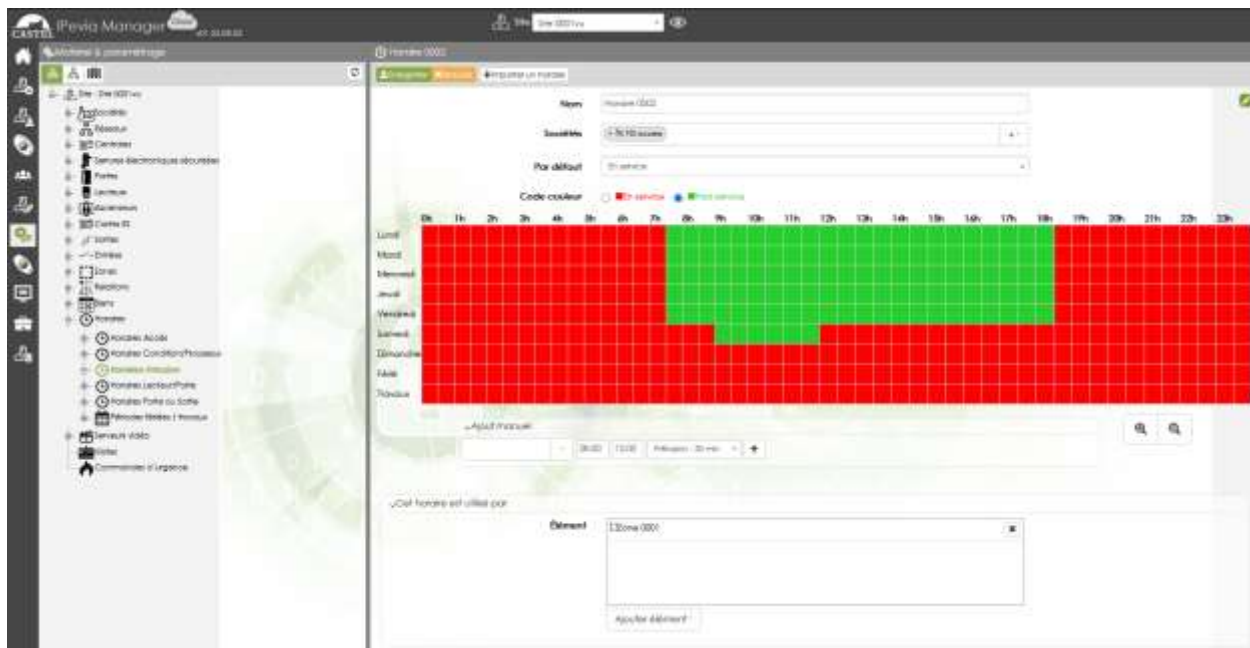
4.3. Common intrusion parameters

Even if connected or unconnected intrusion are different, many settings are the same.

Intrusion activation according to schedule

From the IPassan manager software, it is possible to commission/decommission a zone according to specified schedules.

In the "Equipment and settings" menu, under the heading "Time Profiles", select "Intrusion Time profiles". Click on the "add intrusion schedule" button at the top of the page if one has not already been created.



Select "in use" or "out of order" to arm/disarm the alarm during time slots.

In the example above, the intrusion will be decommissioned from 7:30 a.m. to 6 p.m. during the week. On Saturday, it will only be commissioned from 8:30 a.m. to 11:30 a.m.

Once the intrusion schedule has been established, select the zone to which it applies under the "this time profile is used by" tab. An intrusion schedule can be applied to multiple zones.

Intrusion settings for each zone

For each zone, an additional tab "Medea intrusion" is available. Check the box on the left side of this tab to access its settings.

The screenshot displays the 'Zone 3' configuration page in the Medea interface. The 'Intrusion (Medea)' tab is active. Key settings include:

- Sector number:** 3
- Time profiles:** None
- Options:**
 - ☒ Enable time-dependent commissioning
 - ☒ Enable time-controlled shutdown
 - ☒ Commissioning via an input
 - ☒ Late departure is applied to this zone
- Doors concerned:** (Empty list box)

Sector number: IPassan manages zones with doors or readers associated with them. In the Medea interface, the zones are called "sectors". These sectors can include one or more sensors. It should be noted that a Medea controller manages up to 16 sectors. Sectors are set up in the Elkron/Medea controller software.

In the zone settings (in IPassan software), associate the zone to the corresponding sector. Thus, if one or several readers are provided for this area, their actuation can control the arming/disarming of the intrusion.

Enable time-dependent commissioning/enable time-controlled shutdown: If these settings are checked, then specific schedules will arm/disarm the intrusion of that area. It is possible to apply already defined periods or to create new ones by clicking on the "+" to the right of the field.

Reader profile for intrusion



See chapter 3.6 (readers) for more information about the reader profile.

Select and create a reader profile. Apply it to the corresponding devices.

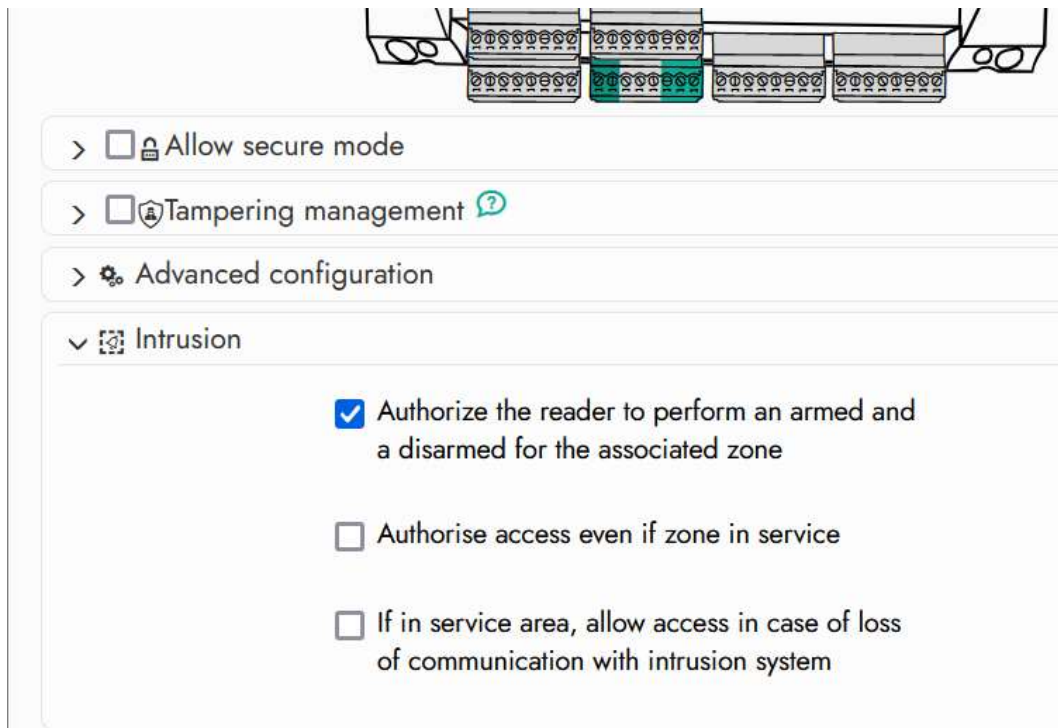
In its settings, you can define the behavior of the reader LEDs when:

Name	Color 1	Color 2	Blinking	Duration	Buzzer
Normal behavior	Blue	Blue	Fix single color		
Access granted	Green	Green	Fix single color	Event	Long bip
Access denied	Red	Red	Quick single color	Seconds 3 s	3 short bips
Wait for double identification	Orange	Orange	Fix single color	Event	Off
Door open for too long	Orange	Orange	Slow single color	Event	Continuous bip
Forced door	Orange	Orange	Slow single color	Event	Continuous bip
Forced door / free access	Green	Green	Fix single color	Event	Off
Reader tamper	Red	Red	Slow single color	Event	Off
Double swipes	Green	Green	Quick single color	Seconds 3 s	3 short bips
Intrusion: zone is in service	Red	Blue	Slow bicolor	Event	Off
Intrusion: zone is in alarm	Orange	Red	Slow bicolor	Event	Continuous bip
Intrusion: zone status change	Orange	Blue	Slow bicolor	Event	Long bip
Intrusion: late departure	Orange	Green	Slow bicolor	Event	3 short bips

- **"Intrusion: zone is in service"**: behavior of the LEDs when the intrusion is armed.
- **"Intrusion: zone is in alarm"**: behavior of the LEDs when the intrusion is disarmed.
- **"Intrusion: zone status change"**: behavior of the LEDs when the intrusion of an area changes from armed to disarmed or vice versa.

Reader used for intrusion

The previous settings have added lines under the heading "readers" in the "Equipment and settings" menu. To configure intrusion management by a reader, choose a device with the prefix "intrusion zone".



If a reader needs to be associated with intrusion does not have the "intrusion zone" prefix, then it has not been set as an input reader. To do this, go back to the intrusion settings for each zone.

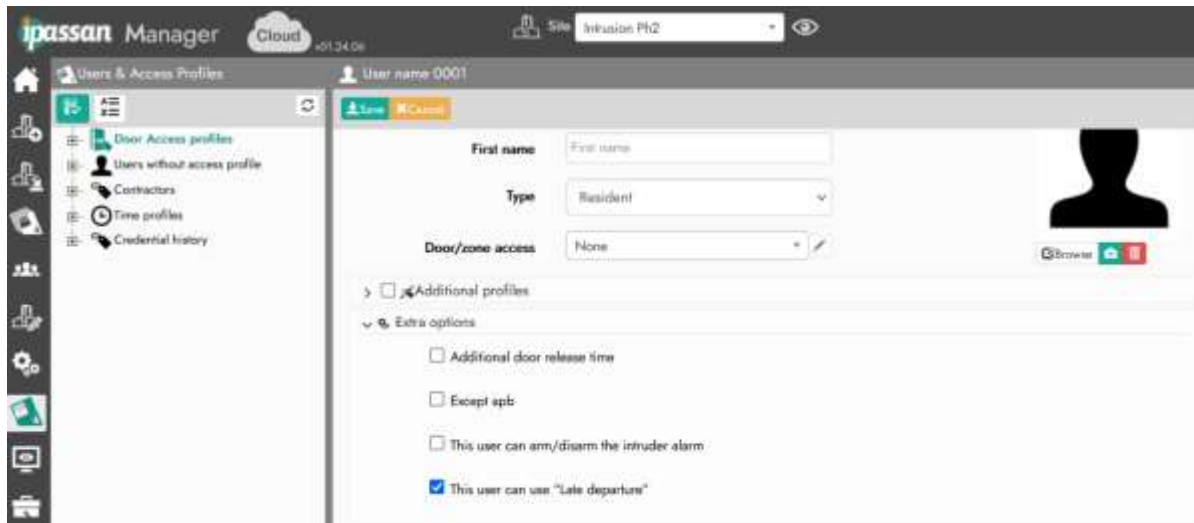
Once you have selected the right reader, click on the "intrusion" tab to deploy its settings.

1. **Allow the reader to perform an MES and MHS for the associated area:** the reader can be used to turn the intrusion on/off with an authorized token.
2. **Allow access even in an area in use:** access can be authorized even if the intrusion is armed.
3. **If the area is in use, allow access in the event of loss of communication with the intrusion system:** when the IPassan control panel loses its communication with the Medea control panel, allow the door to be opened to valid tokens.

User commissioning/decommissioning the alarm (with access profile)

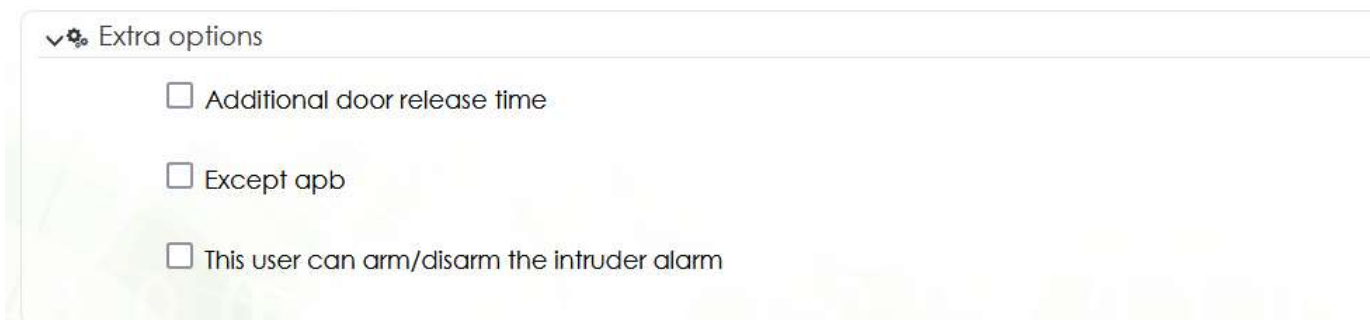
To commission/decommission the intrusion of an area, the user must have:

- **Access rights to the relevant areas** in their access profile (see Chapter 5 to set up an access profile).
- **A validated specific right:** under the "Extra options" tab of their user form, tick the box "this user can arm/disarm the intruder alarm"



You can allow a user to arm/disarm the intrusion, without conceding this right to his entire access profile, and therefore to other users of the site.

To do this, access a user's form in the "User and access profiles" menu. Select a person from the tree on the left.



Under the "specific settings" tab, check **"this user can arm/disarm the intrusion alarm"**.

Late departure

The « late departure » function allows authorized users to postpone alarm commissioning compared to the one planned (with an intrusion time profile). To access this option and its settings, tick the box « Late departure » in the “zone” settings.

▼

☒ Late departure

Activated by

Single swipe ▼

Time before application of the
"Late departure" reader
behaviour

10

min

Delayed start time

30

min

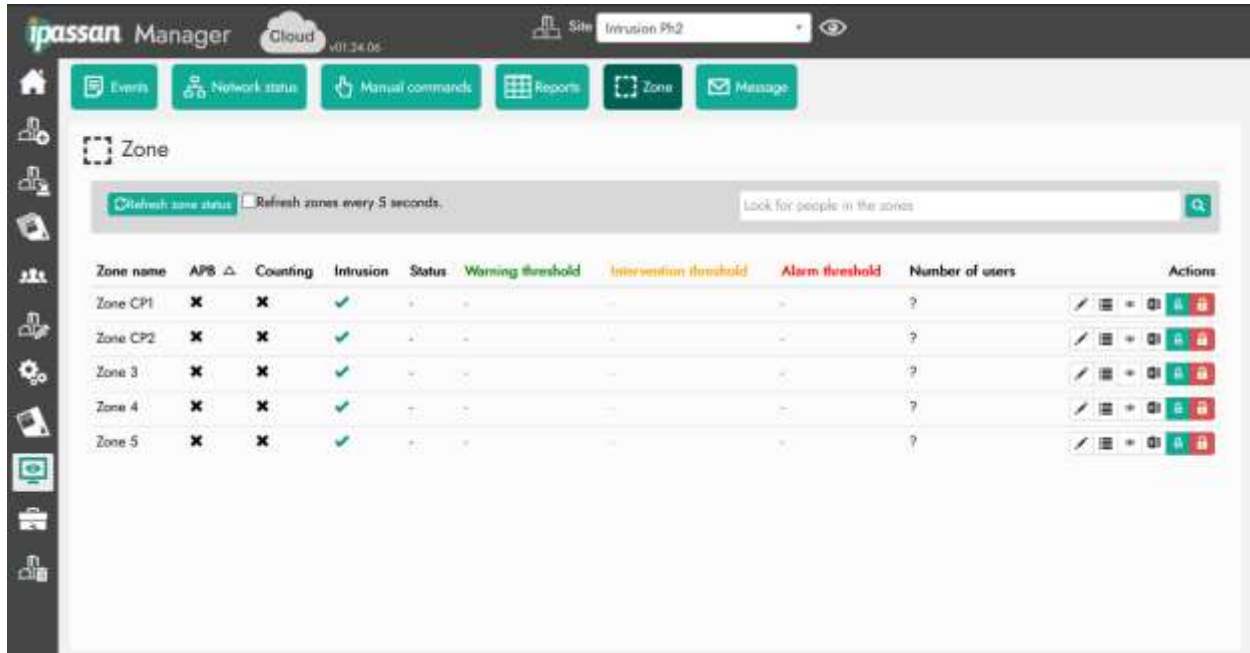
Click on "**Equipment and settings**" in the left frame, then select the zones row. Check the "late check-out" box to access the additional settings.

- **Activated by:** the behavior that will postpone the alarm commissioning. It can be a single/double or triple swipe.
- **Time before application of the “late departure” reader behavior:** the period before the normal time of commissioning that a user can use the late departure function. For example, if 10 minutes is entered in this field, and the alarm is normally triggered at 10pm, the user will be able to use “late departure” from 09:50pm.
- **Delayed start time:** the period during which the triggering of the alarm will be delayed.

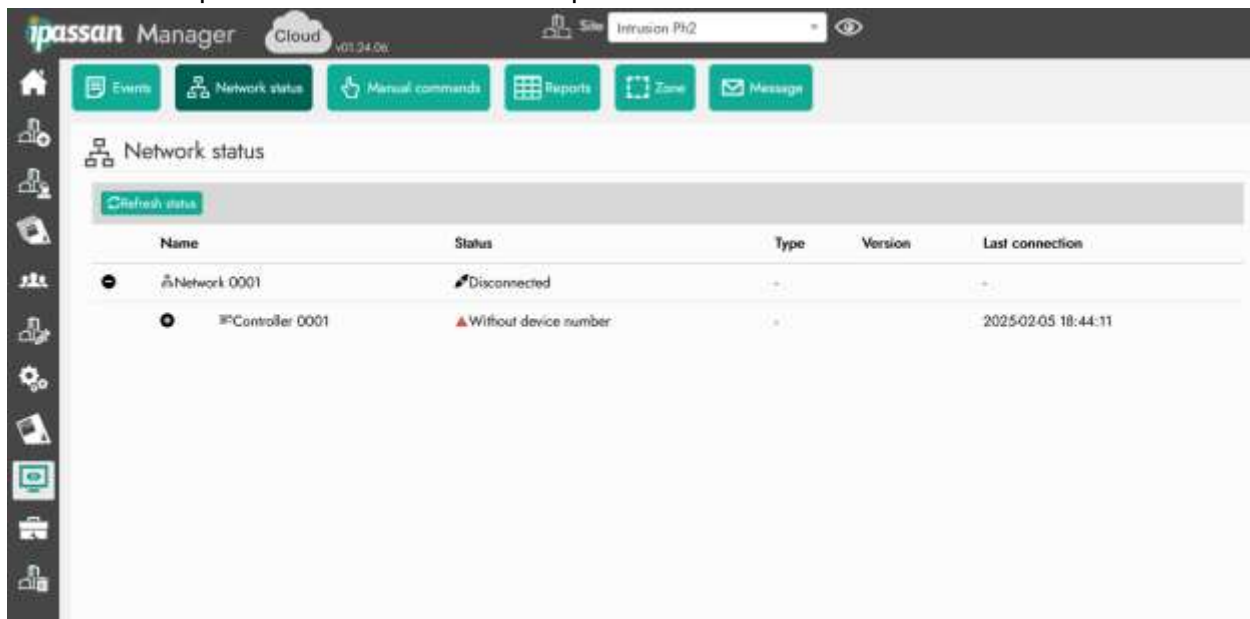
Intrusion tracking with events

Three menus are used to monitor the intrusion on a site:

1. **"Monitoring/Zone"** the status of the zones managing the intrusion is displayed as well as the validity of its connection.



2. **"Monitoring/network status"** means the connection of the Elkron/Medea intrusion control panel to the IPassan control panel.



3. **"Monitoring/event"** the event log shows when an area is in "armed" or "disarmed" status.

ipassan Manager Cloud v01.34.06 Site: Intrusion Ph2

Events Network status Manual commands Reports Zone Message

Events

Display Download Archives Global settings Settings

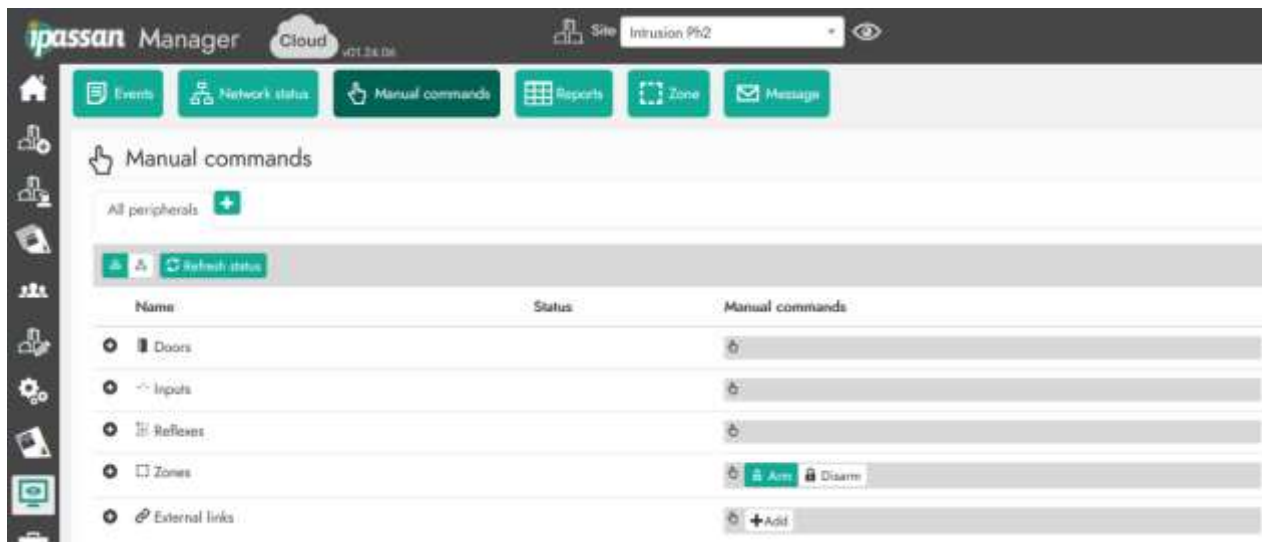
Filters

Result limited to 200 [Refresh] [Purge] [New tab]

Date / Hour	Event	Element	Information	Identifier	Priority
2025-01-13 17:37:17	Access by single credential	Controller 0001 - Door 0002	Resident 12	805FCA92117A04	5
2025-01-13 17:37:17	Armed request via credential	Zone CP2 Reader 0002	Resident 12	-	3
2025-01-13 17:37:16	Relay activated	Controller 0001 - Door 0002	-	-	2

Intrusion manual commands

From the menu « **Monitoring/Manual commands** » the manager can have a look at each zone status (commissioned/decommissioned). He can affect the zone status by arming or disarming the alarm by clicking on a button.

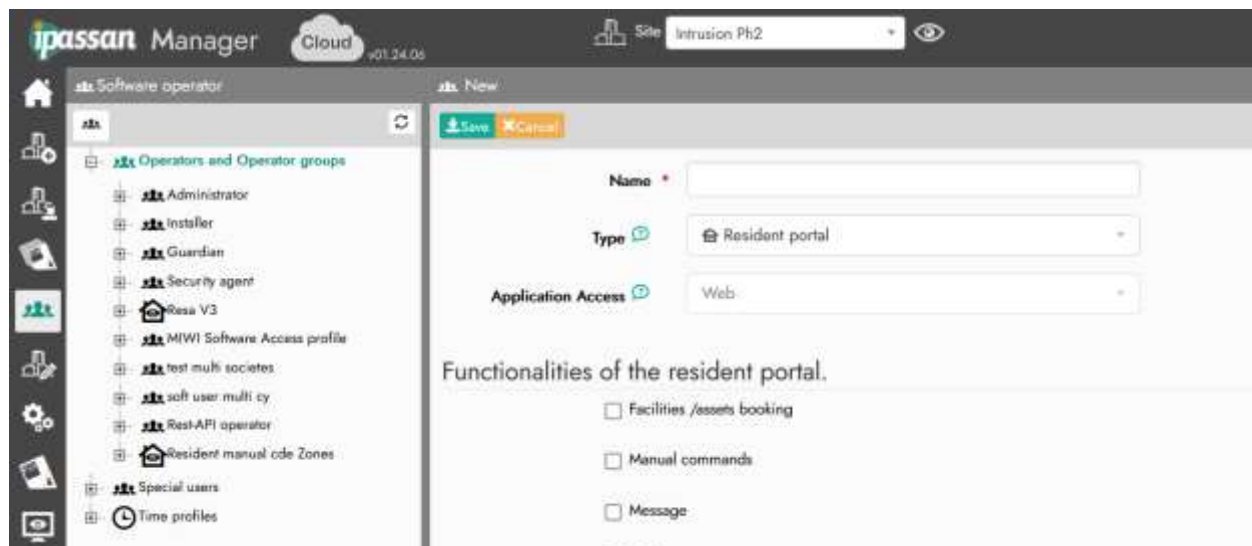


The site manager can delegate the alarm commissioning/decommissioning to a « simple user »:

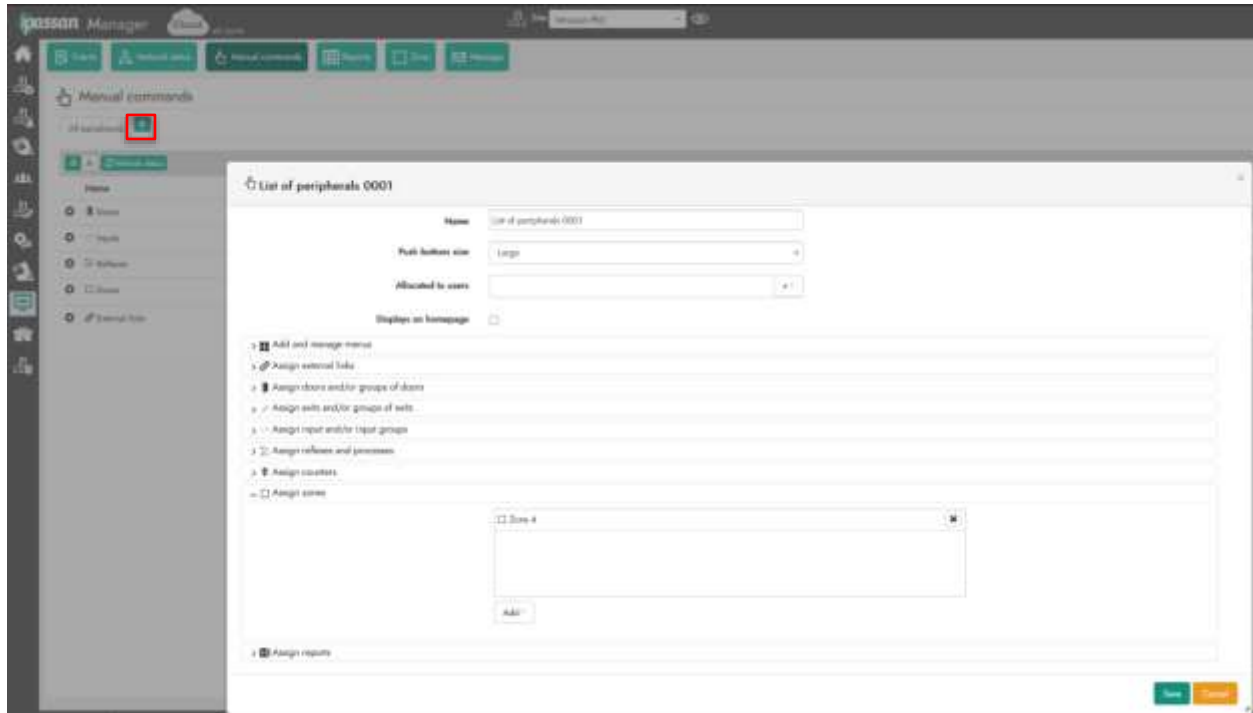
- **By accessing the resident portal:** select "software operator" in the left-hand banner, then click on the "add user group" button at the top.

In the "type" field, choose "employee portal". Among the "Employee portal features", check the box "manual commands". Then save this new user group.

Then, when you create a new user, select the previously created employee portal from the list in the "user group" field.



Via a **personalized manual control page**: from the "monitoring" menu and then "manual commands", click on the "+" button at the top of the page. The following page opens:



The "available to users" field allows you to enter the people who will be able to use the manual controls.

The "assign zones" tab allows you to determine which zones they will be able to fly.



When logging in with their account, the user will be able to arm/disarm the zone(s) from the manual commands.

5. Users and access profiles

All floor/door access profile management are accessible via the token shaped button on the left frame. With this menu, you can also manage users, contractors assets and time profile.



5.1. Door access profile

The door access profile is a list of authorized doors with specific time schedules. These profiles apply to individuals and their keys.

The software manages two door access profiles per user as well as two floor access profiles. Each time, there is a permanent profile plus a temporary profile limited by a start and end date/time.

An access profile contains the following tabs:

- **Door:** list of authorized doors
- **Zones:** list of doors considered as zone entrances
- **Public holidays/works:** list of public holidays or works that this access profile will follow
- **TIC (common identification title):** this refers to a token, keypad code, etc., not assigned to anyone. It can be an access code provided to different people or visitor tokens
- **People:** list of people using this access profile

“Doors” tab: we can see the doors entered for this access profile as well as their respective time profiles.

“Zones” tab : counting and/or anti-pass back zones were created during the setup (see chapter 2.9). For each zone, it is possible to select access profiles and thus the users subject to the rules of these zones.

For example, if you create a "Management" access profile, you can exclude it from counting. Even when a zone is full, users included in the "Management" profile can still enter. Users subject to anti-pass back and counting rules appear in the lower section.

“Holidays/maintenance periods” tab: allows to apply holiday or work period to a specific access profile. Select the period concerned on the list at the bottom or create a new one if necessary.

“Contractor” tab: this tab is used to enter a credential used by an external person. For example, a subcontractor or a craftsman.

“Users” tab : it groups the users using this access profile. You can import them by clicking on the “more” button and selecting “import data”. It is possible to import people from another access profile : select the “+ assign other users” and select those concerned in the list.

You can also export users from one access profile to another by checking the box next to the “action” title on the right. Then you can check the users with boxes on their left.

Then select move users at the top of the users list.

<div> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div>				
	Name △	First name	Type	Nb. of cr
<input checked="" type="checkbox"/>	Manager		✓ Employee	0
<input checked="" type="checkbox"/>	Name 0001		✓ Employee	1
<input checked="" type="checkbox"/>	Name 0002		✓ Employee	1
<input type="checkbox"/>	Name 0003		✓ Employee	1
<input type="checkbox"/>	Name 0004		✓ Employee	1

Then it displays the following window :

Move users

> ☐ 24/7 access

> ☐ Additional profiles

> ☐ User group

> ☐ Architecture

Save

Cancel

- 24/7 access: assign a new permanent access profile (door and/or floor) to this selection
- Additional profiles: assign a new temporary access profile (door and/or floor) to this selection
- User group: link this selection to a group of people (e.g., BE, administrative, sales, etc.)
- Architecture: link this selection to an architectural concept (a building, a floor, an office, etc.)

“Assets” tab: IPassan integrates asset management, letting people book a room or equipment. You can link an asset to an access profile.

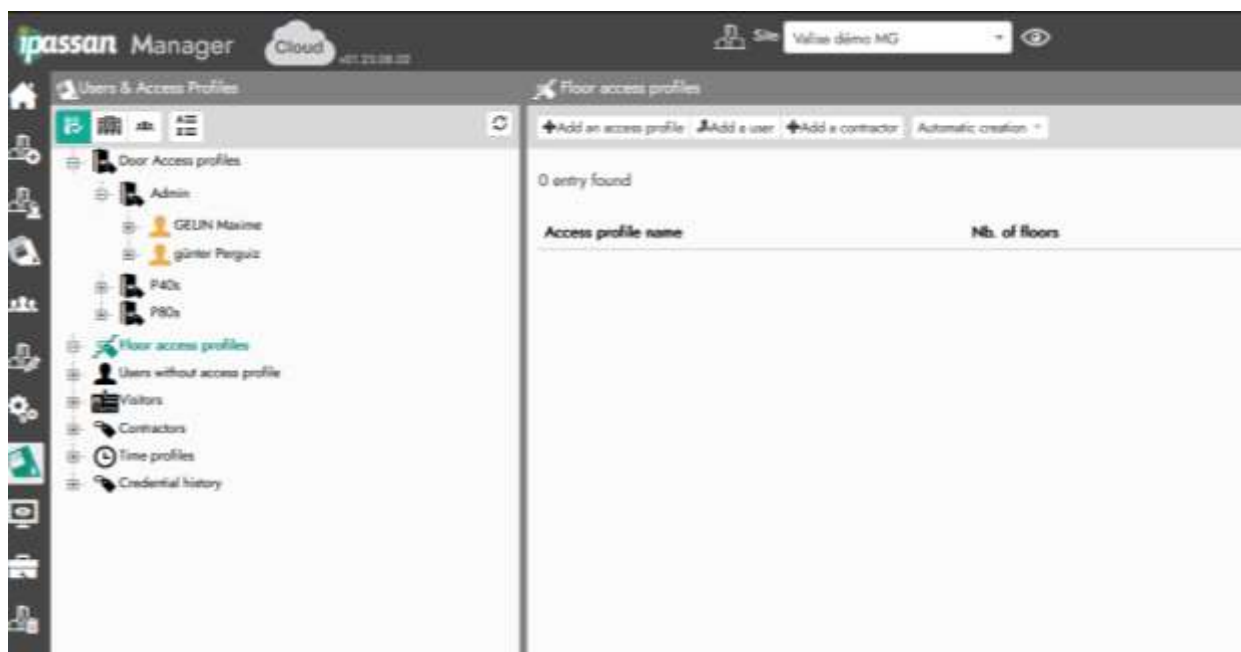
5.2. Floor access profile

The floor access profile is a list of buildings/floors authorized at specific times. These profiles apply to people and their KEYS and influence the lift behavior. If a floor is forbidden at a specific time, the lifts will never reach this level.

An access profile contains the following tabs:

- **Floor:** list of authorized floors
- **Holidays / Maintenance periods:** list of holidays or work periods that this access profile will follow
- **Assets:** you can apply a specific asset to a floor access profile. During the floor access time profile, the user can whether access the asset or it can be forbidden.

The tab “Holidays/Work” is identical to those detailed in the chapter 4.1 “door access profile”.



5.3. Users without access profile

Under the “users and access profiles” section, there is a specific menu that lists the users without an assigned access profile.



It is possible to assign multiple identification credentials (IC) to an access control user. An IC refers to a token, fingerprint, license plate, keypad code, etc.

User information

By clicking on the “add a user” button at the top of the window, you can create a new person and assign him one or several IC.

User name 0001

Save Cancel

Last name * User name 0001

First name First name

Type Resident

Door/zone access None

Floor access None

Location

Companies

auto * thermique

User group

> Additional profiles

> Extra options

> Additional information

> Visits

> Extra doors

Credentials

+ Add a credential

A person (or a user) in the access control system is defined as follows:

field	description
Name	first/last name or additional information (employee ID, email, address, etc...)
Door/zone access	Door/zone access profile the user is authorized to with his credential(s). This one is permanent
Floor access	Floor access profile the user is authorized to with his credential(s). This one is permanent.
Location	When the architecture option is checked (see chapter "2.2 features") it can be more convenient to locate a person within a site and assign him the required access profile.
Additional profiles (tab)	Allows you to define one temporary door/zone access profile and one floor access profile. They are limited by start/end of validity dates and time.
Extra options (tab)	<p>Additional door release time: if checked, the defined time here is added to the time set for each door/floor access profile.</p> <p>Except APB (anti-pass back) : if checked, the user will not be affected by the APB options.</p> <p>This user can arm/disarm the intruder alarm: linked with the intrusion option, if checked the user can arm/disarm the alarm.</p>
Additional information (tab)	To enter other identity information such as an email, a registration number, an address....
Visits (tab)	To see the visits entered on the software that concerns this user
Assets (tab)	A list of assets this user will be able to book
Extra Doors (tab)	To add a specific door in addition to the door access profile entered. This door can be linked to another access profile not entered for this user. It's useful to create a specific access control for a user, no matter the access profile settings.

User's credential

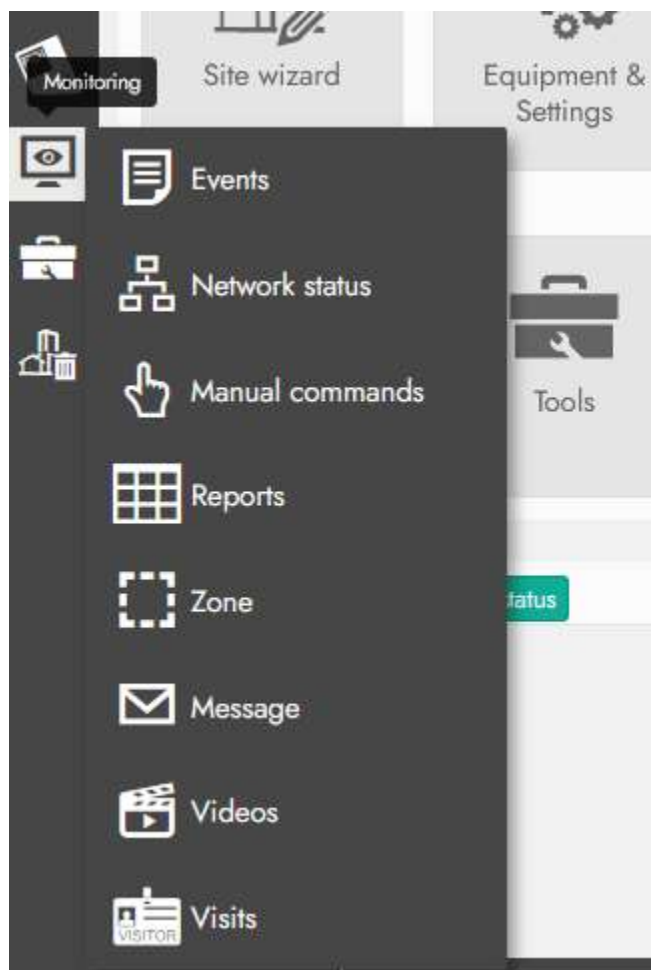
Each user has an unlimited number of identification credentials. Options can be set for each credential (token or Bluetooth access). To add a new credential, click on the “create a credential” button at the bottom right of the window.

It opens the window below

Field	Description
Type	It can be : Mifare+, Mifare+ remote control, Proximity token 1356, access code, Bluetooth.
Code	<p>If Proximity token 1356/ mifare+/ mifare+ remote control/ is set in the previous field, enter Hexa code written on the key.</p> <p>If access code is entered in the previous field, you can choose to automatically assign a code, or define one next to the “number” checkbox.</p> <p>If bluetooth is set in the previous field, enter the mobile and email information of the user.</p>
Status	<p>In use: the token gives access as normal</p> <p>Suspended: when the token is lost. If you uncheck this box, the user will regain its access rights</p>
Validity	If “permanent” is unchecked, you can enter validity dates for this credential
Event	<p>Trace: this credential will appear in the event monitoring when used.</p> <p>Hide: it will not appear in the event log when used.</p>
Others...	To add comments/additional information to this credential

6. Monitoring

The monitoring menu, accessible from the left frame, allows you to display/monitor everything that happens within the site.



When you click on the monitoring icon, you can browse between all the different tools by clicking on the top buttons:



Here are the available tools:

- **Events:** view the history of the controller with all events (unknown token, denied access, authorized access, etc.).
- **Network status:** view the status of central units and input/output cards (connected yes/no, software version).
- **Manual commands:** control doors, floors, exits from customizable dashboards.
- **Report:** generates Excel exports on tokens, people, events, etc.
- **Zone:** display the list of people present in each zone.
- **Message:** display only events for which specific display has been programmed. Generally, these are alert-type events such as "Forced door," etc.
- **Videos:** to see the cctv live
- **Facilities / assets booking** displays a planning view of the assets booking.
- **Visits:** displays of all the visits planned. You can schedule a visit or create an instant one.

6.1. Events

IPassan controllers manage up to 20000 events that are sent to the servers in real-time, when the server/controller communication is up and running.

The event function gives access to other options

- **Display:** each event type has a priority rate from 1 to 9. The display can be configured to show only the most important ones. For example, the "Forced door" event has a priority level of 8, while "Door open" has priority level of 2. For instance, with a priority level set to 5, the event "Door open" will not appear. The priority level of each event is set in the "settings" tab.
It is also possible to filter the display by event type, by element (door, floor, etc.), or by event (for example, only denied access).
- **Download:** each controller manages up to 20,000 events. When communication with the server is initialized, only the latest events are retrieved. The "Download" option allows searching for these missing events in the controller. The filters described above also apply when downloading from the central units.
- **Archives:** to load archives to the software. It can be an excel file.
Because the event limit for each controller is 20.000, this option allows you to save more than 20.000 events in the software.
- **Global settings:** this tab allows you to define for which priority levels events are stored in the controllers and for which other levels they are displayed on the screen.
- **Settings:** to choose the priority level of the event (cover opening) as well as the color displayed by the reader.

6.2. Network status

A window shows the status of the controllers (connected / disconnected), their software versions, and the input/output cards connected to each controller.

6.3. Manual commands

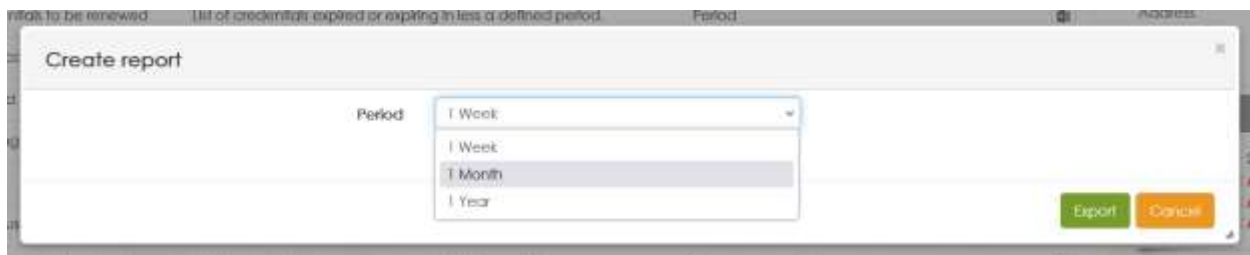
This menu allows controlling doors, exits, or floors from the software. These commands can be either impulse or permanent. For example, it is possible to open a door for a visitor or disable the security of a floor until it is re-secured from the software.

6.4. Reports

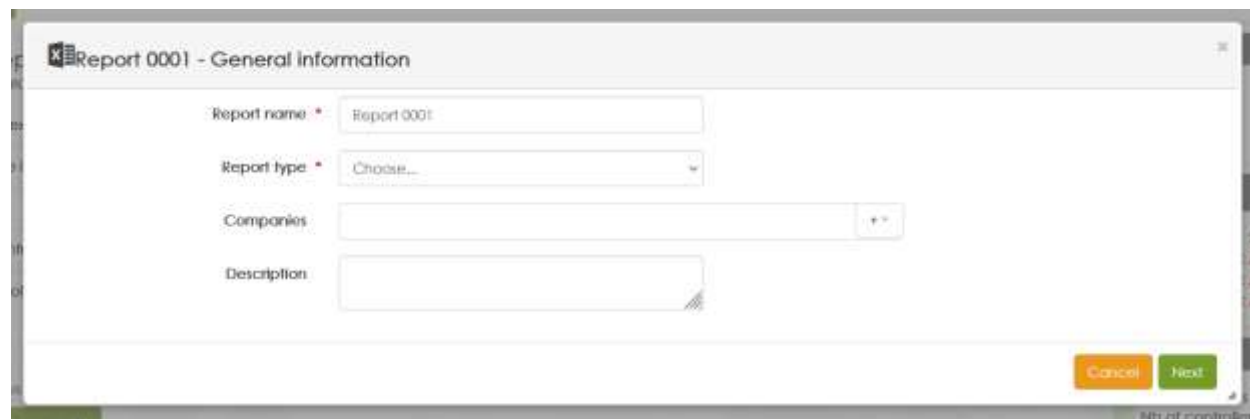
The software allows generating reports on events, users, doors, floors, etc... A report is an excel sheet and can be triggered manually, automatically or by an event. Fourteen reports are predefined when the software is installed.

Select the report within the list and click on the excel logo on the right.

Then enter the period focused by this export. It can be 1 week, 1 month or 1 year. To download it in excel type, click on the “export” button.



You can also create custom reports taking account of specific criteria. Click the “create a report” button at the bottom of the page. The following window opens:



- **Report name:** assign a name to the excel export file
- **Report type:** to choose the relevant information that will appear on your export. Such as events, usernames, zones or visits. This choice will change the fields to fill in the next step.
- **Companies:** you can choose to show only the criteria depending on the company. By clicking the “+” button, you will see a list of all the companies within the site.
- **Description:** to add few comments about this file

By clicking on the “next” button, you access more export settings. The appearing fields are defined by the choice made in the “report type” field.

Example if event is entered in the report type :

Example if username is entered in the report type:

6.5. Zone

When the zone management is enabled (see chapter 2.8), the “zone” tab provides a direct view of the users in each zone

- Zone configuration (pencil)
- Zone details (feature available only for counting by company, profile, person)
- List of attendees (eye) with an option to export this list manually
- zone reset (circular arrow)

7. Booking management

IPassan Manager allows you to manage bookings of assets (a meeting room, a coworking space, parking spots for visitors, equipment, etc...).

When booking a room for one or more people, these users automatically inherit access rights to the doors and floors leading to the items concerned (meeting room, equipment, etc.).

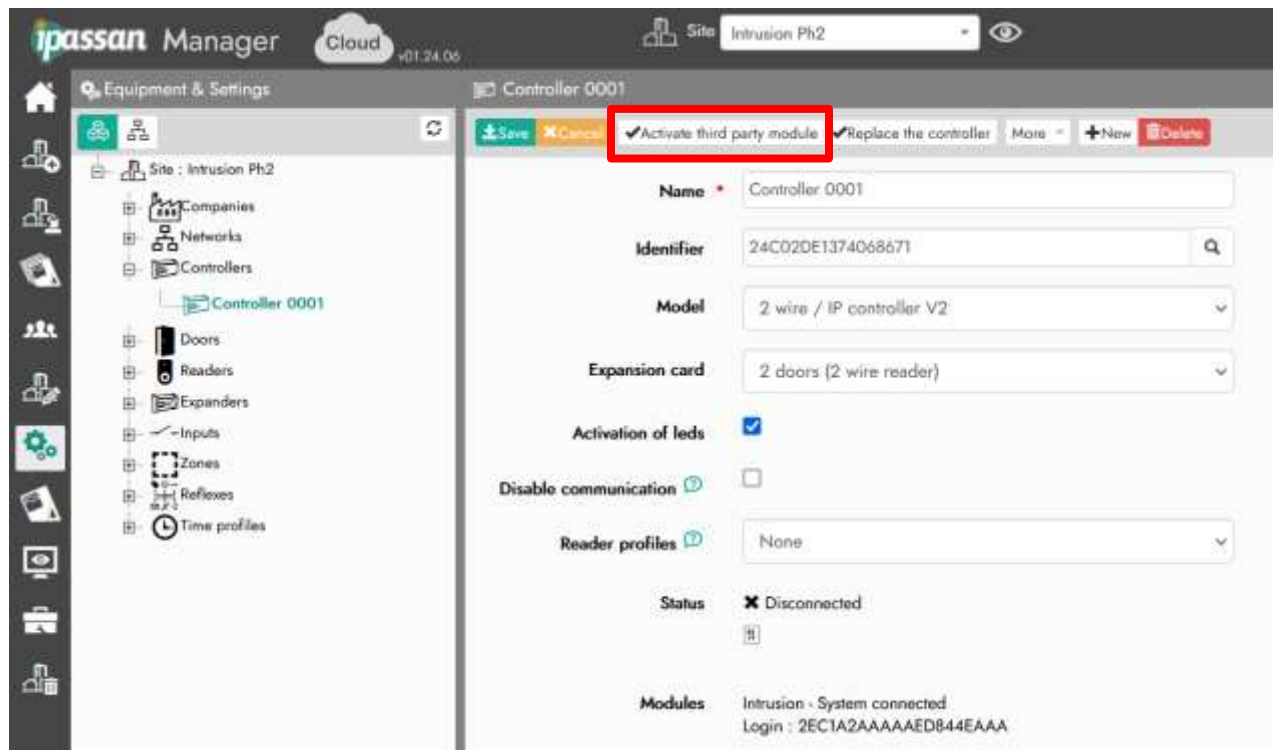
The reservation functionality requires an add-on license. It is accessible through software activation. See the following steps:

7.1. Prerequisite

1- The reservation function must have been activated in the site properties (see chapter 2.2: features)

2- The license must be activated

In IPassan, licenses are linked to controllers. Select a controller available in the "equipment and settings" menu and choose one in the tree view on the left. Then click on the "activate third party module" button (see screenshot below).



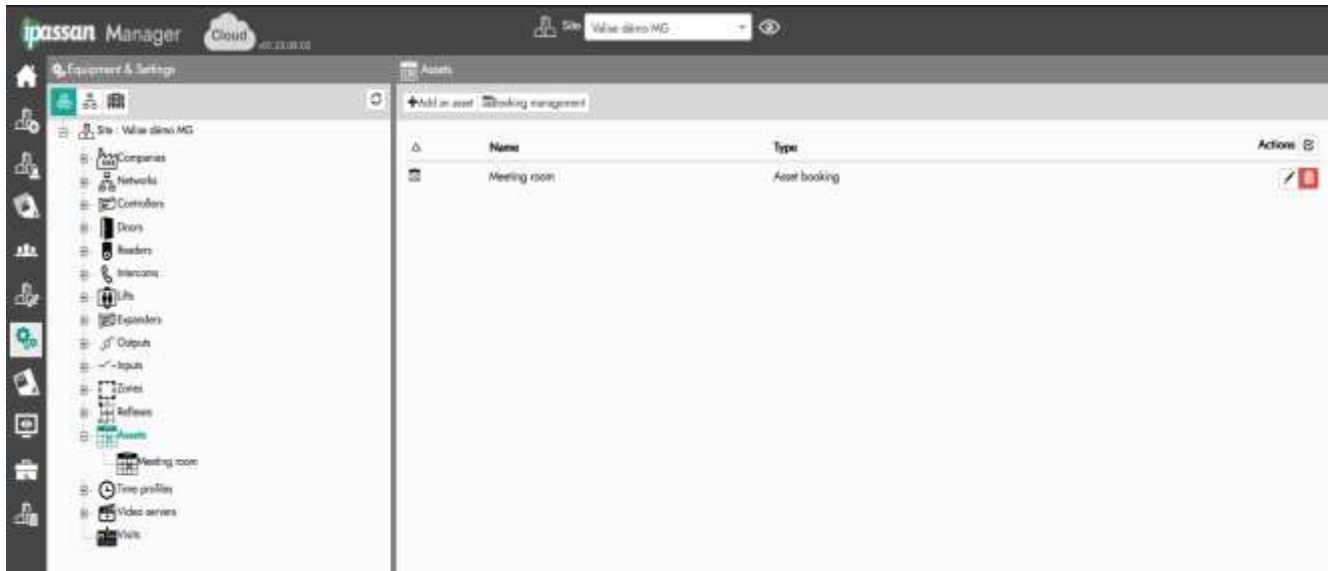
Then choose one of the two options. Enter the information on the following window:

To test the function activation, see the controller overview. A new field with the card number of the booking function must appear at the bottom of the window.

7.2. Adding bookable assets

From the equipment and settings menu, select “assets” in the tree view on the left.

Click on the “add an asset” button to add a room or an equipment.



Global settings

The screenshot shows the 'Asset 0001' configuration window. It contains the following fields and options:

- Name:** A text field containing 'Asset 0001' with a calendar icon and a 'Name' label.
- Type:** A dropdown menu set to 'Asset booking'.
- Display:** A dropdown menu set to 'Planning view'.
- Asset access behavior:** A dropdown menu set to 'Access with credential'.
- Manage Persons visited:** A section with three checkboxes: 'Include persons' (checked), 'Include groups of persons' (unchecked), and 'Include companies' (unchecked).
- Door/zone access:** A dropdown menu set to 'Admin'.
- Floor access:** A dropdown menu set to 'None'.
- Zone:** A dropdown menu set to 'None'.
- Additional access period:** Two time input fields: 'Before scheduled time' and 'After scheduled time', each with a numeric input and a 'min' label.
- Time profiles:** A dropdown menu set to 'None' with a '+' icon.
- Location:** A field with a location pin icon and a red 'X' icon.

Name: enter the name of the asset (meeting room, vacuum cleaner...)

Type: the software offers three different types of bookings. They differ on who can use the bookable asset

- **Asset booking:** the software manager or residents themselves reserve meeting rooms or equipment for users registered in the site's management system. Once the reservation is confirmed, authorized users inherit access rights to doors and floors leading to the room.
- **Visitors can spot booking:** in this mode, managers or residents reserve spaces or equipment for guests, such as a visitor parking spot where a resident must reserve a space for their visitor.
- **Mixed booking:** combines the two modes above.

Display type: define the asset booking is displayed in a weekly or schedule view. For the second option, the assets will be shown in an overview planning of all the assets within the site.

Asset access behavior: to define how the door access profile will authorize or not the door opening:

- **Access with credential:** the door remained closed, but all authorized users inherit access right to this door during the booked time slot. The best option for doors with magnetic locks.
- **Free access:** depending on the door's selected settings (equipment and settings/doors), it remains unlocked for the entire booking period or can be opened with a push button.
- **Free access after a planner comes in:** if the planner accesses the asset, it door remains open.
- **Access with credential after a planner comes in:** if the planner enters the door of the asset, other users will be able to access it with their credential

Manage person visited: if the planner is part of a company or a group, you can choose to delegate access rights to the affiliated people. Example, the planner works for Company A, with this option, you can give access to the asset to every person of Company A.

Door/zone access & floor access: the asset can have specific access/floor profile that allows users to access it during defined time profiles. enter the access profile concerned.

Zone: if the door belongs to a specific zone.

Before scheduled time: the asset can be bookable or accessible during time slots. With this setting you can choose to make it bookable xx mins before the start of the booking.

Time profiles: the asset can be bookable only some days or during time slots. This must have been defined in equipment and settings/time profile/+ button/add an access time profile

Advanced setting

Advanced setting

Time slot ⓘ
30 min

Max booking time ⓘ
0
min

Allow only one booking per time slot
☒

Max number of people ⓘ
1

Max number of user per booking ⓘ
1

Max number of applicants per time slot ⓘ

Authorise recurring booking
☐

Assets linked ⓘ
+

Time slot: it's the minimum time of booking. The booking time is multiple of these criteria. (Example: if the time slot is set as 5 mins, the global time of the slot can be 5 min, 10 or 15minutes).

Max booking time: in minutes, this is the maximum time the equipment or asset can be reserved. When this field is 0, it is unlimited.

Allow only one booking per time slot: the definition of 'maximum number of people in total' and 'maximum number per booking' (next settings) can authorize several simultaneous bookings (swimming pool, car park, etc.) but this possibility can be inhibited by ticking this box and thus making the property exclusive.

NB: This limitation to a single reservation per slot is forced if the 'management of applicants' includes groups or companies. It also implies the cancellation of the following settings

Max number of people: this is the maximum number of people allowed for a booking. The software manages the number of people included for the booking, as well as the maximum capacity. For example, if a catering area accepts 30 PAX it cannot accept a booking with 35 people included. But two people can book this area if each of their groups is composed of 15 people (if the previous option "allow only one booking per slot" is unchecked).

Max number of users per booking: IPassan manager can restrict the number of people per booking. This prevents the privatization of the asset for one organizer. If the asset gauge is 30 PAX, you can restrict 10 people per booking to let it be available for more than one booking.

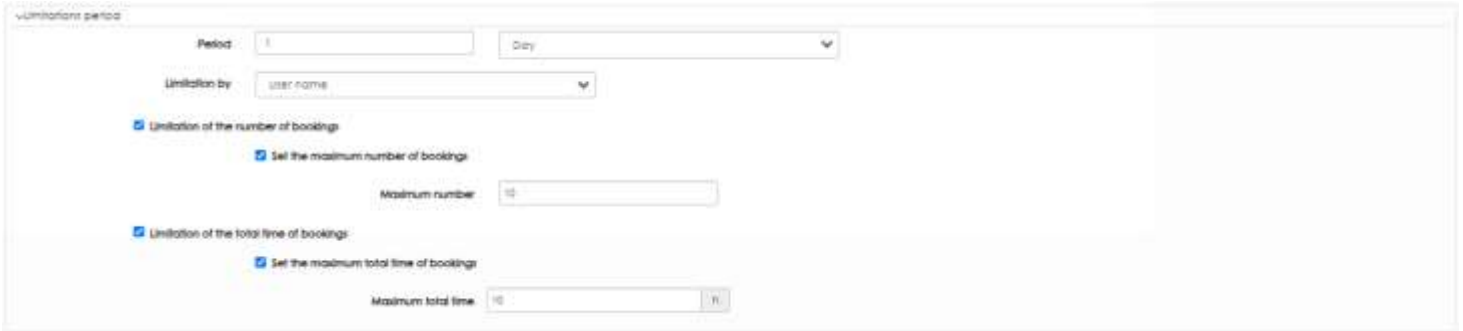
Max number of applicants per time slot: the software can limit the max number of applicants within time slots. It prevents attempts to privatize the asset by duplicating applications.

Authorize recurring bookings: by checking this box, it allows the booking of the asset periodically. For example, an employee can book the room each Monday every week, each first Monday of the month.

Asset linked: for organizational reasons and building design, it is possible to link several assets of the same type and if they are using the same method. It aims to make it easier to manage the whole facility.

Example: if you access a gymnasium by a hall, you can link the hall and the gymnasium. The same if for example, there are changing rooms next to it : booking the gymnasium will also book the changing room.

Limitations period



As well as being determined by time slots, access to the defined assets can be restricted by periods.

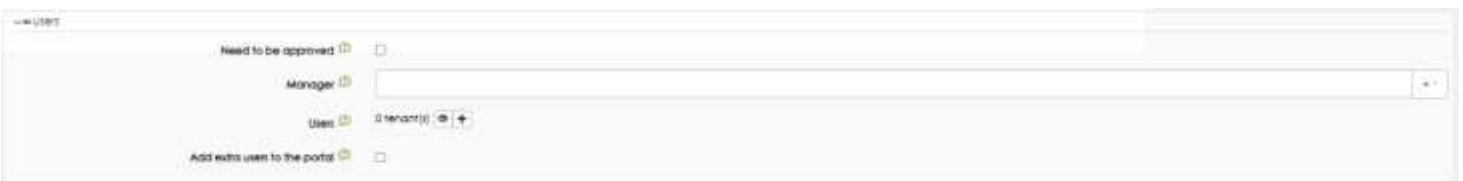
Period: the period can be defined as a number of day(s)/week(s)/month(s) or year(s): you will also need to specify the first calendar day (for weeks, define the first day taken into account).

Limitation by: choose if this period apply to person, person group or company. For example, you can set a period for company A and not Company B.

Limitation of the number of bookings and set the maximum number of bookings: during the defined period, you can limit the number of bookings (max 1.000 bookings per period). It is useful for a tennis court, for example : the club members will be able to book it twice a week.

Limitation of the total time of bookings and set the maximum total time of bookings: allow limiting the duration of the booking. Example: the quantity of tennis lesson booking by club members is 4hours.

Users



Need to be approved: if checked, the software will send a request to the manager. He can accept or refuse the booking. If this box is unchecked, the booking will be automatically accepted.

Manager: the people in charge of validating or not bookings.

Users: enter the people who can book the asset.

Add extra users to the portal: an applicant can add a user to his booking, even if he's not in the user list (see the previous setting).

Mail sending



Sending management emails: this is the setting for email to managers and applicants. The one which will be sent to the manager for acceptance or refusal of bookings. And the validation/refusal email to the applicant.

When the “sending management email” box is ticked, the software automatically sends e-mails to residents to inform them of the progress of the reservation: request completed, request approved or refused, etc.

Footer of the email: you can customize the footer of emails sent to users to reinforce communication about the booked asset, to make it easier for the recipient to understand, etc.... To do this, you can choose from 4 selections available in the ‘email footer’ field:

- None: only information relating to the reservation will be displayed
- Site: the applied settings will be those set in “equipment and settings”, selecting the site at the top of the tree view and the “email settings” tab.
- Company: the settings will be those associated with the companies configured in the “equipment and settings menu” and click the “email settings” tab after selecting a company.
- Custom: it opens an editing tab in this window.

Actions

This tab trigger process is configured in the reflex menu, they can be activated automatically or by badging.

Double tagging:

- End of access authorization
 - If the operating mode of the asset includes an 'organizer' and this box is ticked, double tagging an 'organizer' will cause the advanced end of the reservation:
 - if the chosen mode was free access by token or power cut to the lock, it will lock again.
 - If the chosen access mode was by token, the authorized tokens are no longer authorized.

Without this double sign-in, token rights and/or door behavior are modified as expected at the end of the reservation slot.

- Trigger a process: when an organizer double swipes his token, the IPassan central unit can trigger a process. This process must have been previously planned. It may involve activating a relay to switch off the lighting, air conditioning, etc.

Double swipes and launch a process: when a host arrives (when they are first logged in), the controller can trigger a process (relay activation, for example) by swapping its token twice in front of the reader. This process must have been created previously.

Start of the time slot: at the start of the slot, the controller initiates a process (lighting relay activation, for example). This process must have been created previously.

End of time slot: at the end of the slot, the controller initiates a process (for example to activate an alarm).

X minutes before the time: depending on the time programmed, the controller starts a process (heating relay activation, for example). This process must have been created previously. If "skip

if another booking is ongoing” is checked, the process will not be triggered if another booking occurs just before this one.

X minutes before the end time: depending on the time programmed, the controller starts a process (e.g. activating a dimming relay). This process must have been created previously.

X minutes after the end time: depending on the time programmed, the controller starts a process which must have been created previously. If “skip if another booking is ongoing” is checked, the process will not be triggered if another booking is made just after this one.

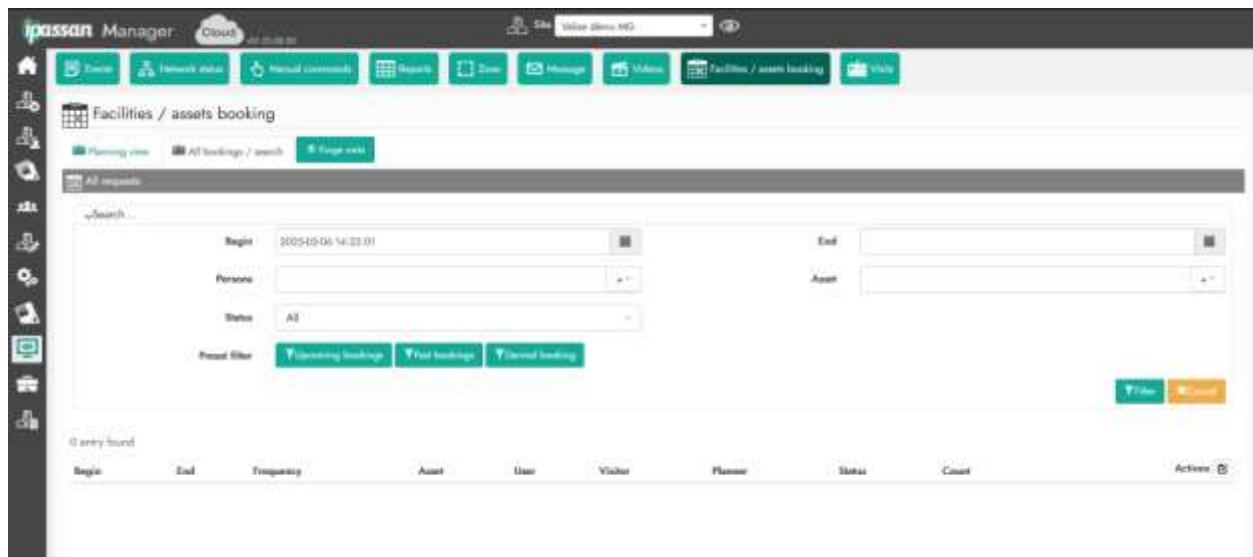
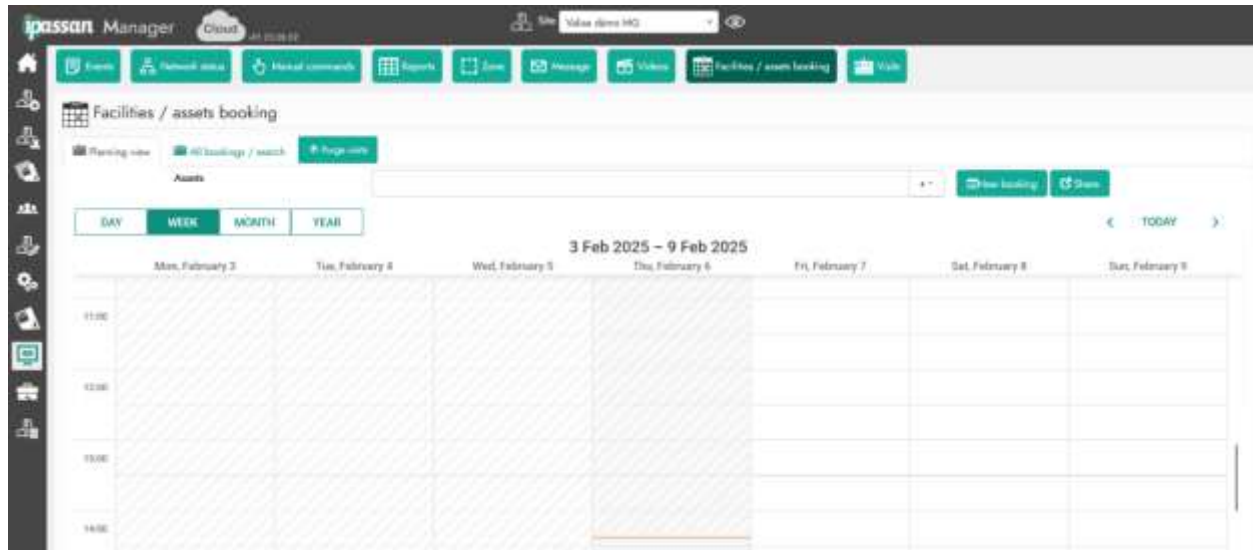
Instructions

This free field is used to provide instructions to the organizers. For example:

- No noise, no alcohol
- Leave the room clean
- The remote control for the video projector must be put away in a specific place

7.3. booking management

On the software manager side, via the 'Monitoring / facility assets booking' menu, all booking management appears depending on the type of display: "planning view" or "all booking/search".



These two presentations offer the same functions.

You can create a new booking by clicking on the button on the right of the "assets" list.

General tab

Activation of the visitor credentials: access permissions for cards and access codes can be managed automatically or manually.

- Automatically on scheduled times and dates: the access title is valid for the designated doors and within the specified visiting hours automatically.
- Manually managed by the software operators: the credential becomes valid when an operator (e.g., receptionist) enters the start of the visit into the IPassan Manager software. The access title is deactivated when the operator indicates the end of the visit in the software.

Management of the visited users in the resident portal: through their IPassan employee accounts and based on choices configured by the administrator, users can book meeting rooms (see chapter 7.3.1.1) or add visitors. Depending on the administrator's configuration, the residents may only be able to schedule visits for themselves, or they may be allowed to add visitors for other residents.

Max duration for visits: maximum time a visit can last.

Max period for recursive visits: users can create a recurrent visit. You can choose to add a minimum period between two recursive visits. For example 3 weeks, one month, 3 months or 1 year.

Productivity tab

Add button for direct printing : in the visit overview, the receptionist can access a button that prints the visitor his qr code

Access profile filtering: if “all visitor access” is selected, when the receptionist checks for the visit occurring (monitoring/visits/all visits), every created visitor will appear on the field “visitor”. If the other option is selected, the receptionist will only see the visitors entered for “in progress” visits.

Default visitor profile: if you want the access right of the visitor to match those of the visited person.

- First element: first access profile of the full list is selected. It can be convenient to name one access which starts with an A. With this option, the software will automatically choose this access profile. It's useful if every visitor follows the same path or need the same door access.
- Visitor profile is the same as the visited person: visitor will inherit the same access right that the person he visits.
- Visitor profile linked to the visited profile: it opens a new customizable field to link a specific visitor profile to the person visited.

Automatically generate visitor names: the software can name the visitors by itself.

Email settings tab

Allows you to apply a defined theme. You have three options:

- **None:** no footer will appear on the email to the visitor
- **Site:** the footer will be the same as the one defined in the site email settings (equipment and settings/select the site/email settings tab)
- **Company:** the footer will be the same as the one defined in the company email settings (equipment and settings/compagnies/select the company/email settings tab)

Enable/disable the credential types (prox, fingerprint, etc...) tab



This tab allows you to choose which kind of credential can be used for visitors. It can be real credential (token, plate, QRcode...) or virtual (Bluetooth, access code...)

Default fields

The checked fields in the list will appear on the visitor form to create a new visit.

Custom field

The visitor entry form can be customized with the addition of custom fields. To do so, first add a custom field.

Click the “tools”  menu on the left frame and select “customize”. Create the required custom field. “Then on equipment and settings” , select “visit” in the tree view and check the field to add to the form at the bottom of the window, below the “custom fields” tab. For example, this created field named “output”.

Once the customized field is created, you will find it under the “custom fields” tab. Tick the linked checkbox to make it appear on the visitor entry form.



Custom fields

☐ Output

8.2. Create a visitor profile

The door and floor access profiles managed in the software are not automatically usable for visitor management. To make them selectable when creating a visit, the "Visitor profile" box must be checked. See section 4 "users and access profiles".

8.3. Create a visit

To access ongoing visits or create new ones, click on "monitoring" then "Visit." The following window will appear:

Begin	End	Frequency	Access profile	Visit purpose	Person visited	Visitor	Status	Actions
2025-03-07 14:30:00	2025-03-07 14:45:00	-	Visitor access		Engler Erwan	Heider Barbara	📅	🗑️
2025-03-06 14:30:00	2025-03-06 15:30:00	-	Visitor access		Erwan Engler	Gunter Alan	📅	🗑️

Under the "Visit" title, there are two tabs:

- **Dashboard:** Only ongoing or upcoming visits are displayed (see screenshot above).
- **All Visits:** Allows filtering visits and displaying them based on specific criteria (see screenshot below).

Planning a visit

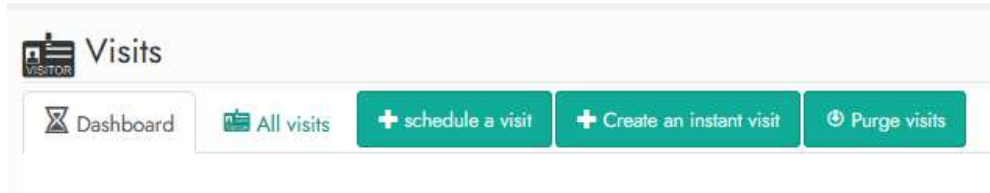
The IPassan software allows you to schedule a visit in advance. In the following window, enter the name of the person or people being visited. Select the access profile for the visitor. Only profiles that are marked as selectable for visitors will be offered here.

Reminder: to make an access profile selectable, check the "visitor profile" box in the access profile form.

Enter the frequency of the visit: it can be either one-time or periodic with start and end dates. The screenshot below shows an example of a periodic visit.

Create an instant visit

At the top of the visit menu, click on the “create an instant visit” button. This option is a simplified version of visit scheduling, as it proposes the start of the visit for the current time.



Then this window is displayed:

You can repeat this visit. By clicking on the “recurring visit” check box, the software will show other options, such as days and hours to repeat this visit.

Enter the required information and click “OK”.

8.4. Visitors access management

In regards of the parameters configured in the menu « Equipment and settings » / « visits », the credentials activate and deactivate automatically with an operator action.

Manual management of visit start/end

When the activation of access credentials is set to manual in the Equipment & settings / Visitors menu (see below), token and key codes will only work after operator intervention.

General

Activation of the visitor credentials

Manual, managed by the software operators

The start of the visit and therefore the activation of the token or code is done in the Monitoring / Visits / Dashboard window by clicking on the "Play" triangle.

The end of the visit and therefore the deactivation of access cards is done in the Monitoring / Visits / Dashboard window by clicking on the "End" square as shown below.

begin	end	frequency	Access profiles	Visit purpose	Person visited	Visitor	Status	Actions
2025-01-14 14:00:00	2025-01-14 16:00:00	-	Prof (Faculté 001)		Manager	Duchêne		
2025-01-14 15:00:00	2025-01-14 16:00:00	-	Prof (Faculté 001)		Manager	Vergués		
2025-01-25 15:00:00	2025-01-25 16:15:00	-	Prof (Faculté 001)		Manager	Jigien		

Automatic management of credentials

When the credential activation option is set to "automatic" in **equipment and settings / Visits**, the tokens and access codes are automatically valid on the date and time of the visit.

General

Activation of the visitor credentials

Automatic, on scheduled times and dates

9. Advanced use of the software

9.1. Automatic modification tool

Different renaming and/or configuration tools have been provided to simplify the installer work. These tools are used on control panels, inputs, outputs, doors, and allow the same modification to be applied to multiple elements in a single operation.

For example, these tools can be used to rename multiple outputs as "Output 1, Output 2, etc." with an increment or to configure end-of-line resistances for impedance inputs in a single operation.

Controller information modification

In the "Network" or "Controller" view, click the "Actions" button (1) on the right, then check the control panels you want to modify in the first column (2). Finally, click the "Network" button (3).

	Name	Identifier	Model	Expansion card	Last connection	Version	GTW	M485	Num	Actions
<input type="checkbox"/>	Controller 01	24C02DE138091C3DC	2 wire / IP controller V2	2 doors	2025-01-02 15:03:11	IV3242 18/11/2024	✓	✓	0	[Edit] [Delete]
<input type="checkbox"/>	Controller 0002		2 wire / IP controller	None	-		-	✓	1	[Edit] [Delete]

Multiple edition

Creation file:

\$: Number
\$\$: number with 2 digits

Selection:

☐ Name: Controller 0001 First number: 1

☐ Companies: [Dropdown]

☐ Activation of leds: ☒

☐ Disable communication: ☐

☐ Reboot the controller every day at: ☐

[Save] [Cancel]

The following window appears:

It allows you to modify:

- the names of the control panels with automatic increment management.
- Enable or disable the status LEDs (reader, door, server communication, etc.).

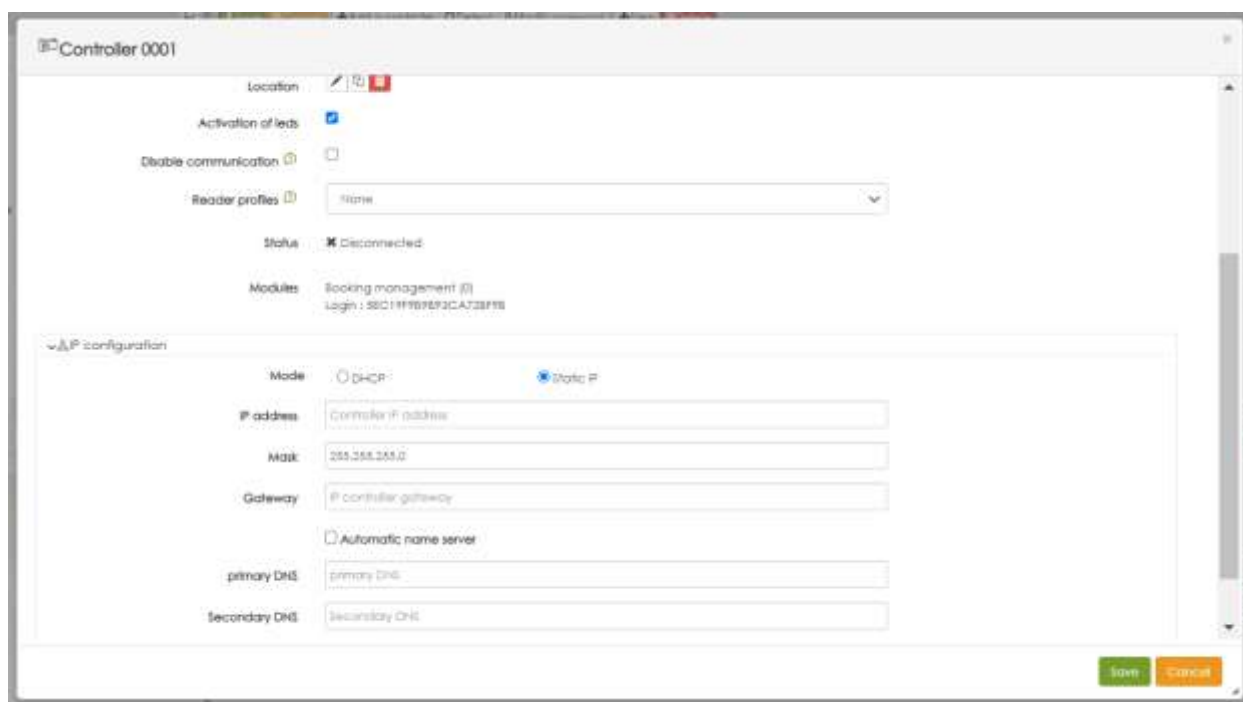
- Schedule an automatic restart.

Controller IP address change

In the "Network" or "Control Panels" view, click the "Actions" button (1) on the right, then check the control panels you want to modify in the first column (2). Finally, click the "pencil" button (3) on the right of the controller.



	Name	Identifier	Model	Expansion card	Last connection	Version	GTW	M485	Num	Actions
<input type="checkbox"/>	Controller 01	24C02DE138091C3DC	2 wire / IP controller V2	2 doors	2025-01-02 15:03:11	V3242 18/11/2024	✓	✓	0	[Pencil] [Erase]
<input type="checkbox"/>	Controller 0002		2 wire / IP controller	None	-		-	✓	1	[Pencil] [Erase]



Controller 0001

Location: [Edit] [Erase]

Activation of leds: ☒

Disable communication: ☐

Reader profiles: [Name] [Dropdown]

Status: ☒ Disconnected

Modules: Locking management (I)
Login: 58C1FFB7E92CA728F7B

IP configuration

Mode: ☐ DHCP ☒ Static IP

IP address: [Controller IP address]

Mask: 255.255.255.0

Gateway: IP controller gateway

☐ Automatic name server

primary DNS: [primary DNS]

Secondary DNS: [secondary DNS]

[Save] [Cancel]

The software displays the following window:

Check the "static IP" box. Then enter the desired information in the fields. In this example, the first selected controller in the list will be assigned the IP address 255.255.255.0 and the second controller will get 255.255.255.1.

Input modification

From the input view, click on Action (1), then select the inputs to modify (2), and click on the pencil icon (3). The check boxes on the left of the field allow you to modify only certain fields.

Expander 0001

1

Name	Num	Used by	Type	Location	Actions
<input type="checkbox"/> Expander 0001 - Input 0001	1	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0002	2	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0003	3	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0004	4	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0005	5	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0006	6	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0007	7	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0008	8	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0009	9	-	2 state input (on / off)		
<input type="checkbox"/> Expander 0001 - Input 0010	10	-	2 state input (on / off)		

2

3

The following window appears for all the selected inputs, it is possible to modify the name by managing an automatic increment and to choose the input type as either "normally open" (NO) or "Normally closed". Example for a switch:

- In NO mode, the switch won't conduct electricity until it is activated,
- In NC mode, the switch will conduct electricity until it is pressed.

Multiple edition

Creation file

1 - number
15 - number with 2 digits

Selection

Name: input 1111 Input 0001

Compartment

Use this input as: 2 state input (on / off)

Input status: ☐ Normally open ☐ Normally closed

Options

With automatic back value: 10

activation time: 0 0 0 0 0 0

deactivation time: 0 0 0 0 0 0

Save Cancel

Use input this input as:

- **2 state input (on/off):** the signal can only have two possible states, such as on/off or open/closed, or 0/1. There are settings to prevent bounce back (see information below)

Anti-bounce back value (in ms): this setting is particularly useful for push buttons. Even if they are simple to use, sometimes they are subject to bounce: they don't switch from opened to closed directly. For a very short time (milliseconds), it will switch several times between opened and closed. So the controller will understand each state change as a button push.

To prevent this phenomenon, you can set a value (in ms), so the controller will not take account of the push button status change. This value needs to be sufficiently high to prevent the controller from understanding one solicitation as two. Also, it must be sufficiently low to understand two actions when needed.

Activation & deactivation time: you can choose to apply this anti-bounce back only after a certain time. While the previous data is entered in milliseconds, you can choose to apply an anti-bounce back after hours, minutes or seconds.

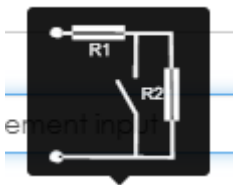
- **EOL management input:** an End-of-Line Resistor (EOLR) helps monitor wiring by detecting open or short circuits. It allows the controller to identify four states based on the resistances (Ω) and the switch. If the resistance exceeds a set value, the controller detects the input and can trigger a reflex for example.

End of line resistor1 ?

Default (4.7 k Ω)

End of line resistor2 ?

Default (10 k Ω)



You enter line resistor values for R1 and R2. Depending on the current resistance (Ω) and the switch, you can create four conditions:

Short circuit: the switch is closed, and the circuit bypasses the two resistors because $\Omega >$ to R1 and R2.

Standby (or not detection): the switch is closed and Ω is only $>$ to R1 value.

Active (or detection): the switch is closed and $\Omega >$ to R1 & R2.

Open circuit (or unplugged): when the circuit is open and the electric current overpasses R1 or R2 values.

With the settings above, you can for example, define that the controller would detect a short circuit, only if it happened x time after the first one (anti bounce back value). If two short circuits happen in less time than this setting, the controller will only detect one short circuit.

Anti-bounce back value

80

ms

"Short circuit" time

Hours: 0 Minutes: 3 Seconds: 0

"No detection" time

Hours: 0 Minutes: 0 Seconds: 0

"Detection" time

Hours: 0 Minutes: 0 Seconds: 0

"Unplugged" time

Hours: 0 Minutes: 0 Seconds: 0

Differential validating the threshold move

You can use the slide bar to define that the controller will detect a short circuit only if it lasts more than X seconds, X minutes or X hours.

The field “differential validating the threshold move” needs to be entered when other values than 4.7kΩ and 10kΩ.

- **Decimal input:** offers the possibility to manage 3 customized thresholds from decimal value within 0 to 4095, so the controller can detect 4 different statuses based on these thresholds. It is useful to manage door reflex for example

Note that threshold 1 value < threshold 2 value < threshold 3 value.

To simplify, the Decimal type is an EOL kind of input type. Instead using the preset thresholds you can use customized ones. Analogic values measured in the input by the controller will be converted to a digital value between 0 to 4095.

Like the other input type, you can define anti-bounce back settings, to prevent the controller interpreting and consider state-change disturbances

Output modifications

From the output view, click on **Action**, then select the outputs to modify, and click on the pencil icon.

Some output can be assigned to a company.

The time delay consists of the period in which the controller will send a command. If set to 5 seconds, the controller via the output will send the message for 5 seconds.

Multiple edition

Creation file:

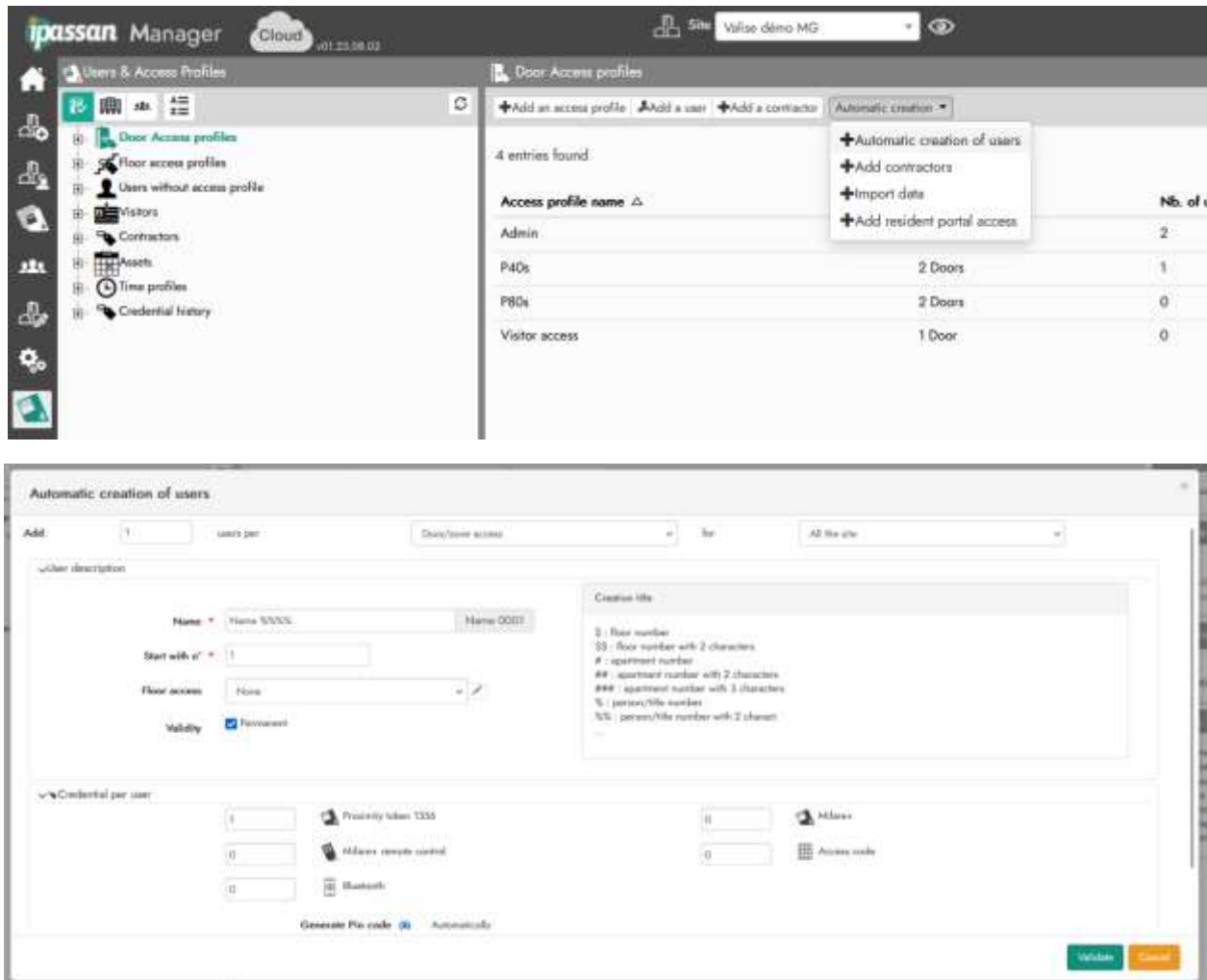
\$: Number
\$\$: number with 2 digits

Selection	Name	Companies	Time profiles	Operation	Release time	Output inverted
<input checked="" type="checkbox"/>	Output \$\$\$		None	<input checked="" type="radio"/> Monostable pulse <input type="radio"/> Bistable: trigger to open, trigger to close	5 sec	<input type="checkbox"/>
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						

Save Cancel

9.2. Automatic person/token creation tool

It is possible, in IPassan Manager, to automatically create users and their keys. This feature allows for the creation of x cards. This tool is available by clicking on “users and access profiles” on the left frame. Then under the “automatic creation” list, select “automatic creation of users”.



You can choose to create x users per **door, zone access/ floor access/ user group/ block/ floor/ apartment** for **all the site/a specific access profile**.

With specific characters (see the creation title section next to for more information) you can automatically create names.

You can also apply a schedule in which they will be valid (if “permanent” is unchecked).

Finally you can add one or more proximity token/Bluetooth access for each user.

9.3. Emergency action

The "Emergency Command" feature allows doors or a group of doors to be released if an input is active. For example, this setup enables the wiring of a fire alarm to an input on the IPassan controller. When this contact is active, it releases the electric strikes or magnetic locks, keeping the doors open.

Prerequisites:

- This function controls a group of doors or all doors in the network, so it's necessary to create one or more door groups that will be controlled by these contacts.
- Only electric strikes with break contacts or magnetic locks, which are powered continuously, are compatible with this mode. Fail-safe locks are not designed for continuous power and are unsuitable for this option.
- The input used for this function must be configured as NO (normally open), NC (normally closed), TOR (on/off), or impedance.

To access emergency action settings, click on the "equipment and settings" button on the left frame. Select the "+add an emergency action".



9.4. Reflexes

What is a reflex

A reflex is therefore a link between a condition and a process.

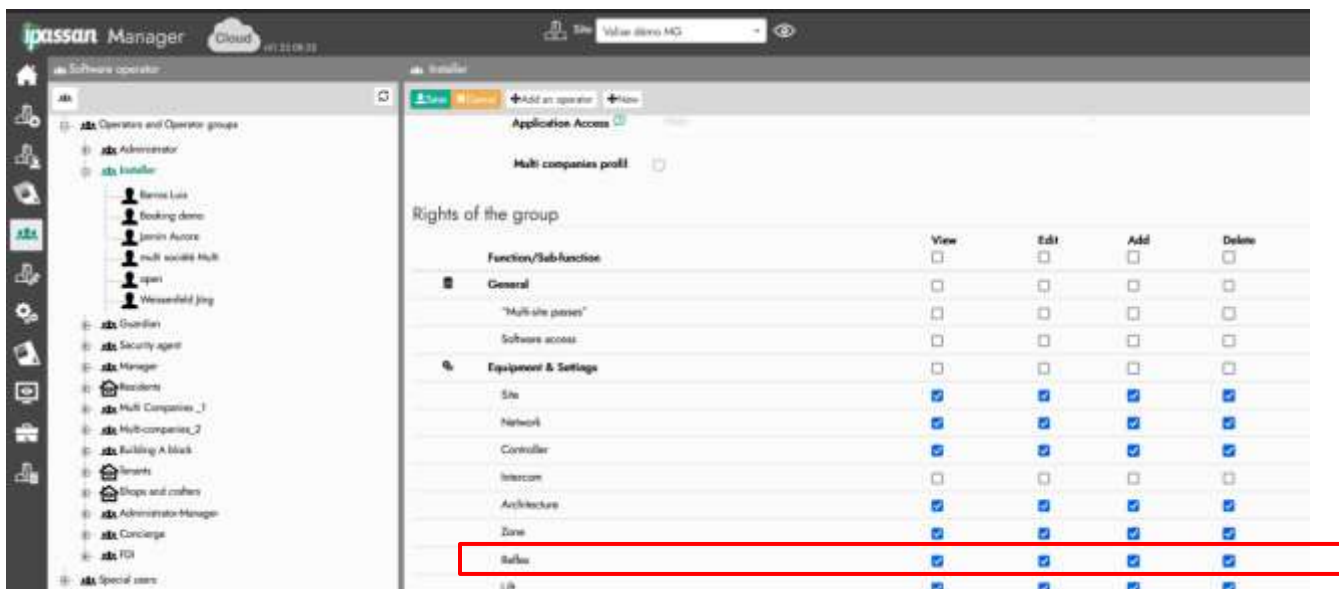
- The condition is the state of one or more inputs, doors, events, etc.
- A process is a sum of actions (control a relay, unlock a floor or door, send a message to the software...).

Reflexes are useful in IPassan Manager to manage anything that is not predefined. Examples of functions achievable via reflexes:

- Force a relay as soon as a door is forced (principle of an intrusion alarm) & release the relay when a specific key is presented to a specific reader.
- Activate a relay to disable an alarm, for example, when a key from a specific profile is presented to certain readers.
- Display a message in the software when a "suspended" key is presented to a site reader.
- Etc...

Allow a user to create reflexes

You can delegate reflex creating to other users of the software. Click the "software operator" button on the left frame. Then choose the group of people you want to let create or manage reflexes. Then tick the checkboxes next to "reflexes".



It is useful to let the installer set up all the site access control. He will be able to create conditions and processes to automate some actions.

How to configure a reflex

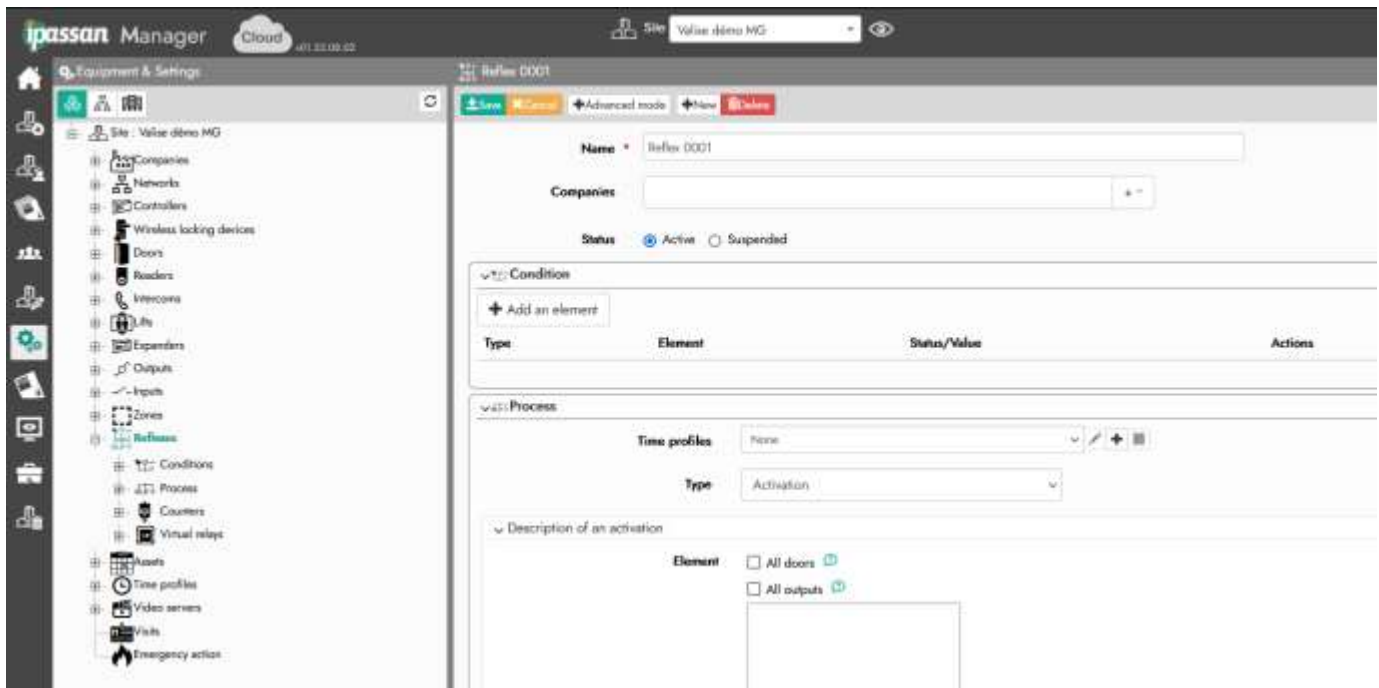
To configure a reflex in IPassan, ensure that the reflex functionality is selected in the site's features. (see chapter 2.2). To access reflex settings, go to "equipment and settings" and choose "reflexes" on the tree view.

The software offers two methods for managing reflexes:

- **Simple Method:** in this method, the user selects all elements from the same view:
 - o **One condition** (from 5 possible events or states)
 - o **One process** (from 5 available actions) The software then automatically creates the condition, process, and reflex together.
- **Advanced Method:** in this method, the user must first define at least one condition and at least one process. Once defined, these conditions and processes can be reused in other reflexes, offering more flexibility and control over the configuration.

Example of a simple reflex:

After clicking on the "add an element" button under the "condition tab", choose the type of



condition you want to use. See the screenshot above to see all the options. This choice modifies the option you can select under "element" or "status/value" tab.

Condition

+ Add an element

Type

--Choose--

--Choose--

Event

User name

Input

Counter

Condition

Virtual relay

Door

Output

Time profiles

Zone TOKEN_IMPORT_MAXLIMIT - Error during import: - limit reached (00 lines max)

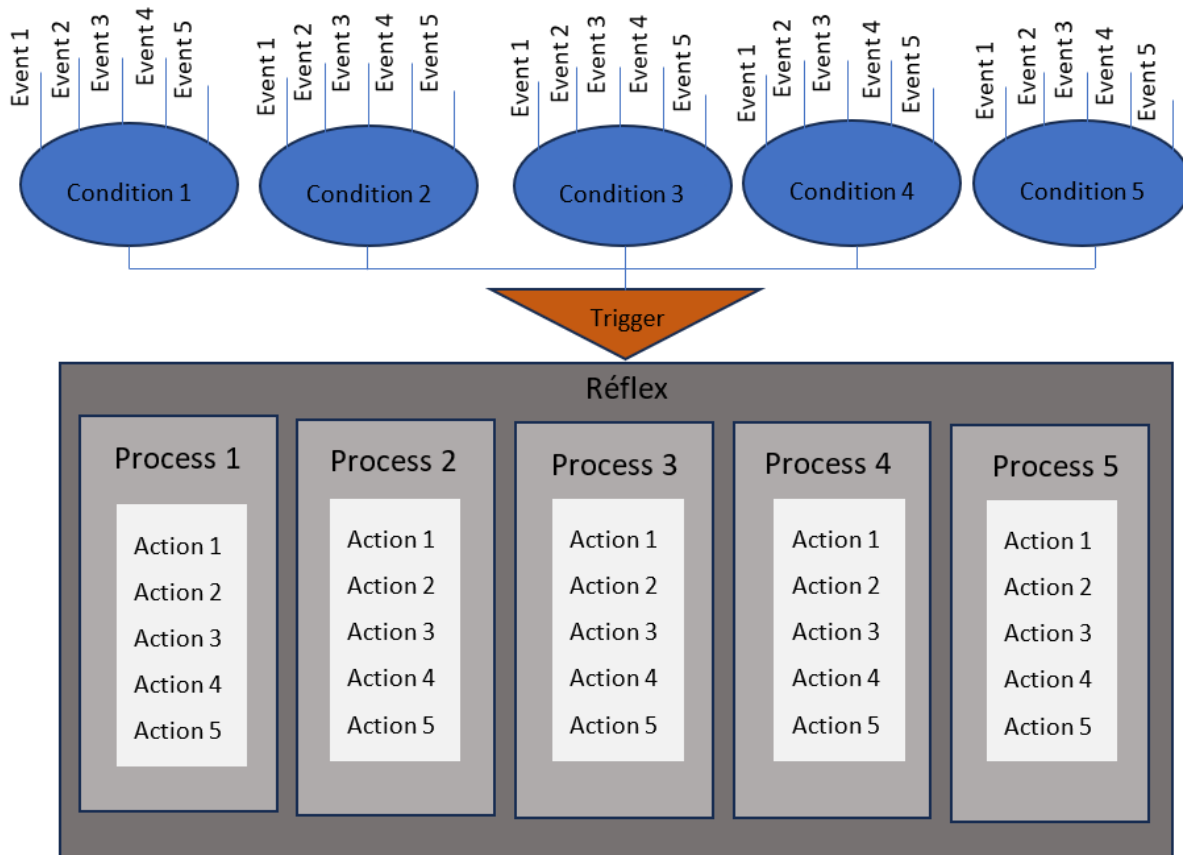
Element	Status/Value	Actions
---------	--------------	---------

The process is the consequence of the condition above. There are several types of processes, such as an activation of a door, an output or the sending of a message. This choice affects the last fields.

Reflex limit of IPassan manager

Limits of IPassan (see the diagram for additional information):

- A condition includes up to 5 events or states with "AND" or "OR" logic.
- A reflex can be triggered by up to 5 conditions with "AND" or "OR" logic.
- A process includes up to 5 actions.
- A reflex can launch up to 5 processes.



9.5. message

The "**Message**" feature, accessible from the "**Monitoring**" tab, displays alert messages that have been programmed via **reflexes**. This menu shows: the **alert message**, the **date and time** of the event, the **person** who acknowledged (or ignored) the alert, the option to **add a comment** to the event

This tool helps monitor and manage alerts in real-time, allowing operators to track the status of events and take appropriate actions.

9.6 API commands

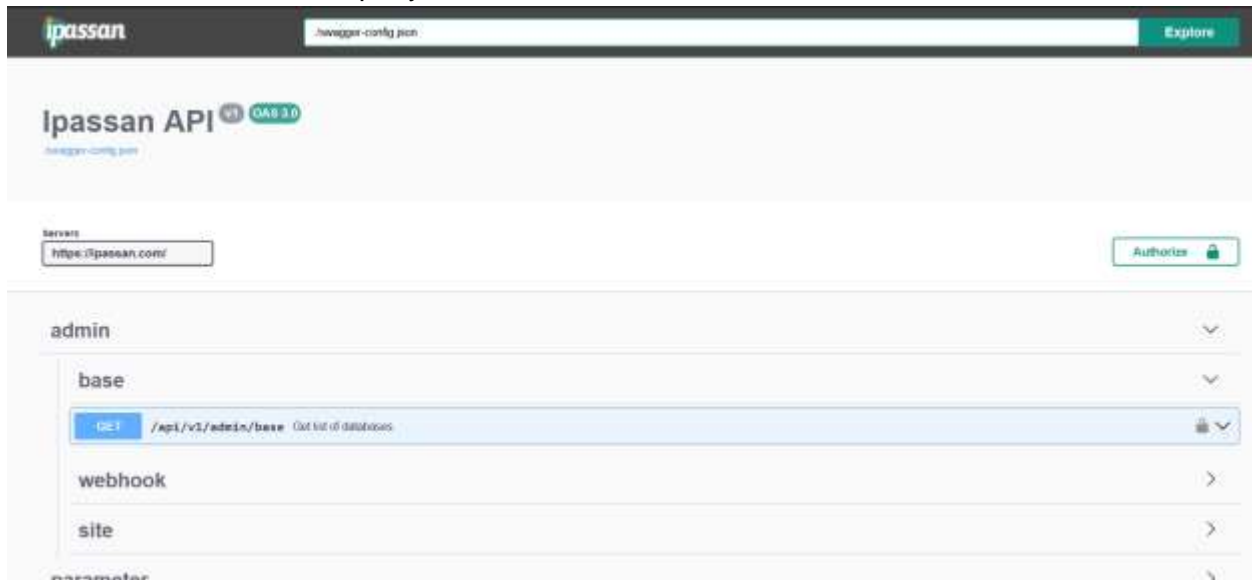
It is possible to send commands via API to iPassan controllers. However, before doing so, the operator must first be authorized to access these commands.

This section is intended for integrator clients who wish to control an iPassan installation from their own solution.

In the left-hand menu, click on “**Software Access**”, then select “**Special Users**” in the tree structure. Choose an existing profile or create a new one.

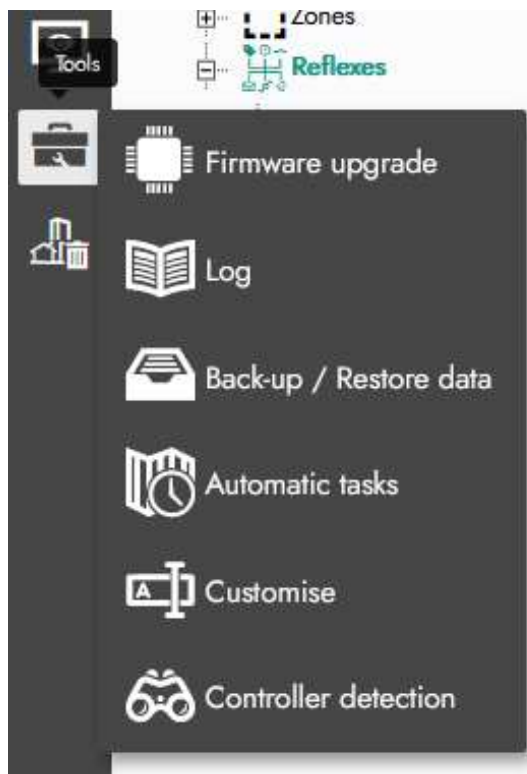
To access the various commands, follow this link: <https://ipassan.com/swagger>

For any additional information regarding commands managed by the iPassan API, please do not hesitate to contact our company, FDI Matelec.



10. Tools

Different tools, accessible by clicking on the toolbox in the left toolbar, are provided in the software and allow the following:



- **Firmware Update:** Updates the firmware of various hardware devices such as controllers and entry/exit cards. This ensures that the devices are running the latest version for optimal performance and security.

- **Log:** View real-time information regarding the site, including events such as access logs, alarms, and system activities. This tool helps monitor and track system performance.

- **Backup/Restore:** Allows importing and exporting sites (e.g., transferring a site from one PC to another). This feature is useful for data migration or creating backup copies of your site configurations.

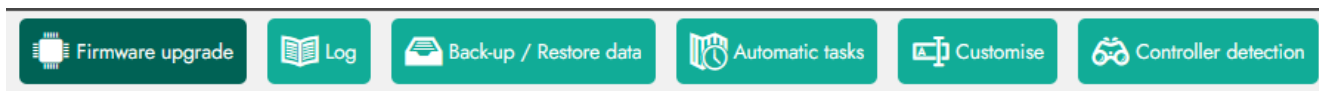
- **Automatic Tasks:** Enables you to force updates on controllers, retrieve events, and trigger email reports. This is ideal for automating routine tasks and ensuring timely updates.

- **Customise:** Create custom fields and insert them into forms, such as visit creation forms. It also allows importing data based on specific criteria for greater flexibility and integration.

- **Controller Detection:** Automatically detects devices on the network, including their parameters. This tool helps identify and configure new devices for

easy integration into the system.

To navigate between the different tools, you can also select them from the top buttons. These provide quick access to various functions and features, allowing you to efficiently switch between tasks without having to go through menus.



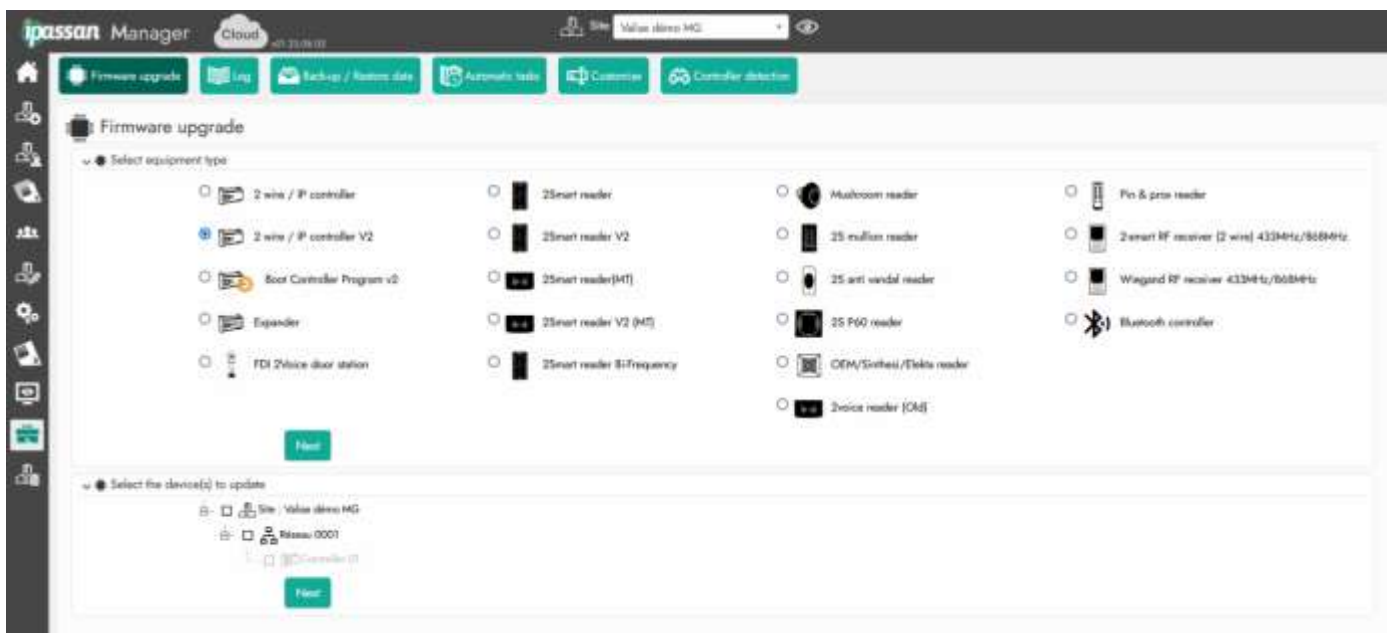
10.1. Firmware upgrade



In the **Tools** menu, click on **"Firmware Update"**. The hardware update process is done in two steps:

- **Select the Type of Hardware:** choose the type of hardware you wish to update.
- **Apply the Update to the Selected Hardware:** after selecting the hardware, apply the firmware update to the chosen device by following the on-screen instructions.

This process allows you to update the firmware for various hardware components within the system, ensuring they run the latest version for improved performance and security.



Then, select the firmware version and click on the « Update the firmware » button:

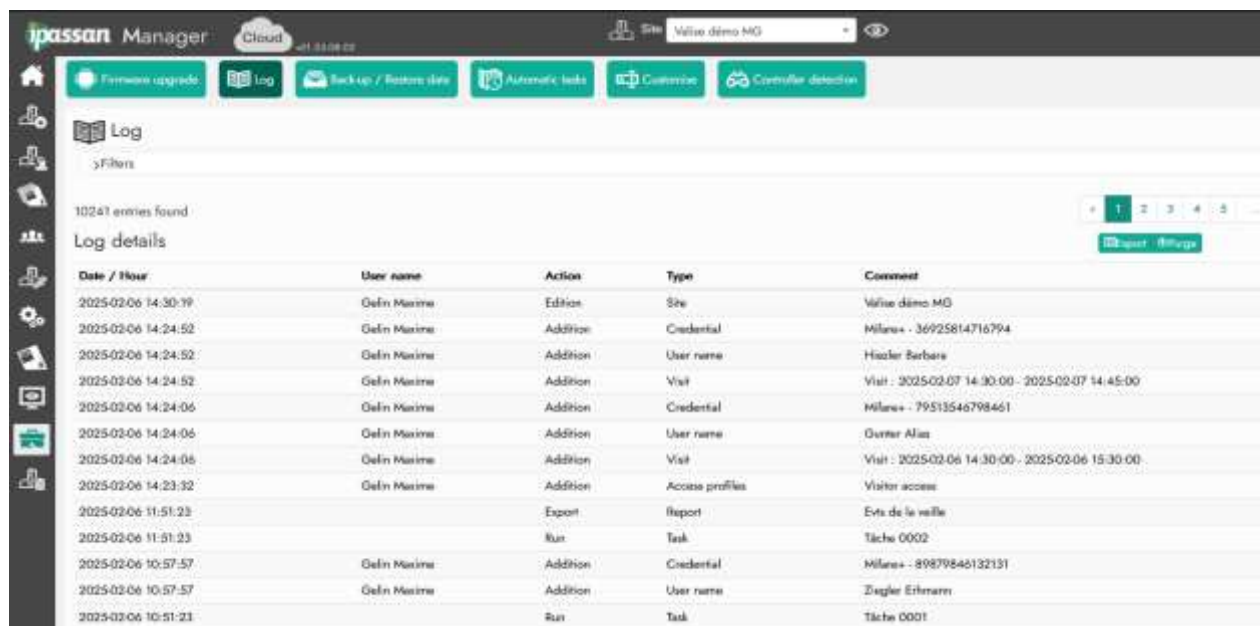
If the firmware download isn't specified in the software (and the server), a menu allows you to add it. At the bottom of the window, under the firmware list, click on "add a software" and specify a name for it. It's possible to add a description. Click on the « browse » button to add the firmware file from the pc directory.

Once the firmware is loaded, the page refreshes by itself. Then it's possible to send the file to the controllers.

10.2. Logs



In the Tools menu, a log tracks the actions of each operator. You can filter these logs by user, dates, sites and other criteria.



Date / Hour	User name	Action	Type	Comment
2025-02-06 14:30:39	Gelin Maxime	Edition	Site	Valise demo MG
2025-02-06 14:24:52	Gelin Maxime	Addition	Credential	Milano+ - 36925814716794
2025-02-06 14:24:52	Gelin Maxime	Addition	User name	Hacker Barbara
2025-02-06 14:24:52	Gelin Maxime	Addition	Visit	Visit : 2025-02-07 14:30:00 - 2025-02-07 14:45:00
2025-02-06 14:24:06	Gelin Maxime	Addition	Credential	Milano+ - 79513546798461
2025-02-06 14:24:06	Gelin Maxime	Addition	User name	Owner Alias
2025-02-06 14:24:06	Gelin Maxime	Addition	Visit	Visit : 2025-02-06 14:30:00 - 2025-02-06 15:30:00
2025-02-06 14:23:32	Gelin Maxime	Addition	Access profiles	Visitor access
2025-02-06 11:51:23		Export	Report	Evs de la veille
2025-02-06 11:51:23		Run	Task	Tâche 0002
2025-02-06 10:57:57	Gelin Maxime	Addition	Credential	Milano+ - 89879846132131
2025-02-06 10:57:57	Gelin Maxime	Addition	User name	Ziegler Erhard
2025-02-06 10:51:23		Run	Task	Tâche 0001

10.3. Back-up / restore data



When transferring a site from one server to another (e.g., from **iPassan.com** to a local server, or from the installer's PC to the final client's database), the software allows the creation of backup files

that can be directly imported onto the other server.

A backup file can include multiple sites. During restoration, a dialog box lets you select which sites to import.

Steps to Export Sites:

- In the **Tools** menu, navigate to the **Backup/Restore data** tab.
- Click the **Add a site to back-up** button.
- Use the **Ctrl** key to select multiple sites if needed.
- On the right side, click **back-up** to generate the file.
- Depending on your browser, a window will prompt you to save the file to your PC.

Note: Exporting a site from a database does **not** delete it from the original database.

10.4. Restore (site file import)

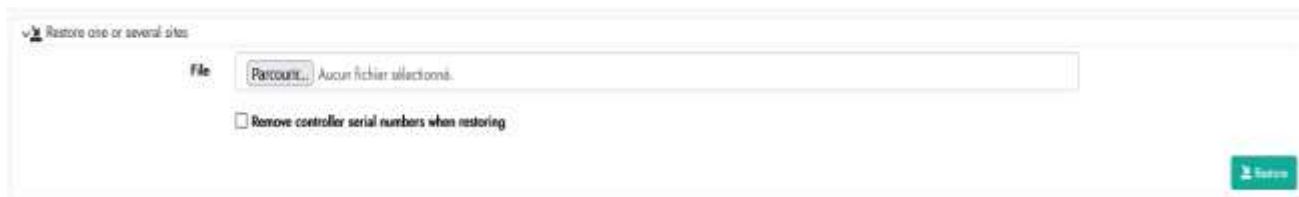


This menu allows you to retrieve a site from another machine (or the Web) onto the server.

Click on **Tools**, then select the **Backup/restore data** button.

In the "**restore one or several sites**" option, click on **Browse**. This opens the Windows file browser.

Select the backup file, then click on **Restore**. The following window appears:

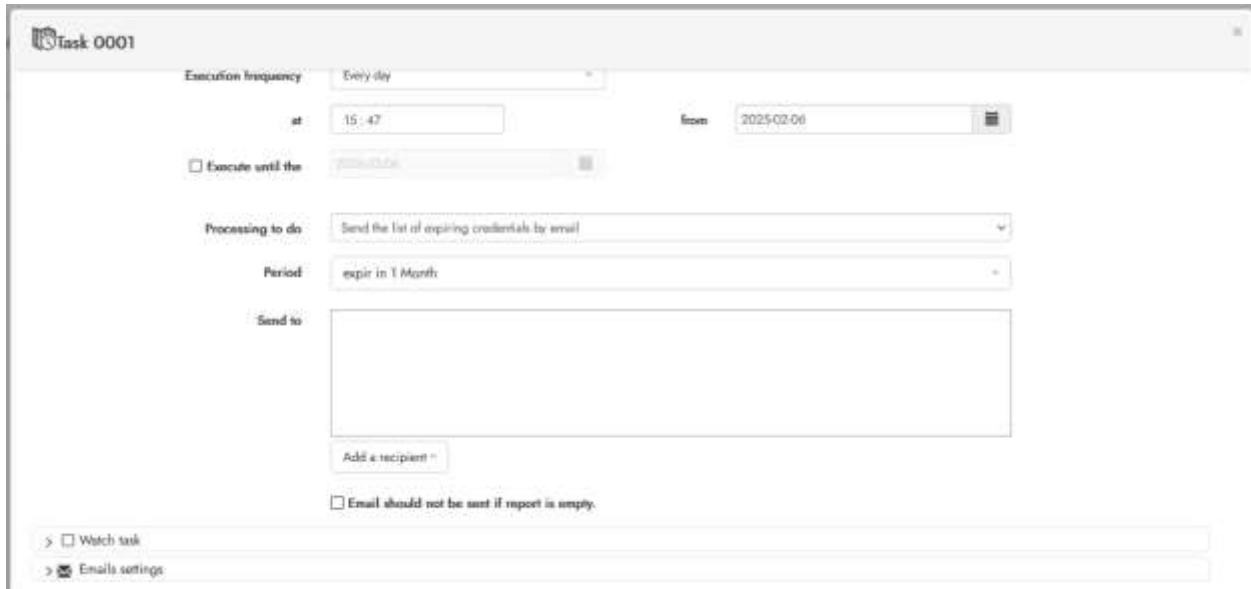


Click on **Restore** to start the import process. A final message will confirm: "**The import was successful**".

10.5. Automatic tasks

In IPassan Manager, it is possible to create scheduled tasks. These are actions that the controller will automatically perform at specified dates/times.

A scheduled task can involve an action on the controllers, a database backup, or sending a report via email.



Note: It is possible to avoid sending a report if it is empty by checking the option at the bottom of the window (under the "email settings" tab)

The task can be monitored, so one or more recipients will receive an email informing them of the successful completion of the task, but without receiving the report itself.

10.6. Controller detection



This tool allows the detection of new controllers on the network, if they have not already been integrated. Unlike the "**Supervision**" menu and "**Network Status**", which display all controllers on the network, including those that have already been integrated into

the site.

11. Software operators management

The software allows the creation of operator profiles that are limited to specific sites and/or software functionalities.

For example:

- An **Administrator** has full rights across all sites: they have access to all features and the ability to create other operators.
- An operator with the **Installer** profile can perform any action on the sites they are authorized to access.

Name	Type	Multi companies profile	Nb. of users	Actions
Administrator	Default	<input type="checkbox"/>	0	
Administrator Manager	Customization	<input type="checkbox"/>	1	
Building A block	Customization	<input type="checkbox"/>	0	
Colocage	Customization	<input type="checkbox"/>	0	
FDI	Customization	<input checked="" type="checkbox"/>	0	
Guardian	Default	<input type="checkbox"/>	0	
Installer	Default	<input type="checkbox"/>	0	

Existing profiles, except for Administrator, can be modified. It is also possible to create as many profiles as needed. There is no limit to the number of operators per profile.

11.1. Add an additional profile

When no existing profile meets the requirements, it is possible to create additional ones. Click on **"Operators and operator groups"** at the base of the tree structure. Then click on the **"Add an operator"** button. Define the operator's name as well as his privileges.

For example:

- **"Manage Reflexes"** in **"Modify"** status means the operator will have rights to make changes to the already configured reflexes.
- If **"Add"** is checked, the operator will be able to create new reflexes.

11.2. Add, modify an operator

An operator is defined by:

- **Name, surname, email, and password**
- **Membership to an operator profile (group)**
- Optional data such as employee number, address, etc.
- A list of authorized sites. The rights are the same for each site.

New
Save Cancel

Group of operators
Administrator

Last name *
Last name

First name
First name

Password *
Password

The password must contain a special character, a digit, a capital and a lowercase letter, and must contain at least 8 characters

Password confirmation *
Password confirmation

☐ Ask to change the password next login.

Email *
Email

Registration number
Registration number

Address
Address

Post code
City

Phone
Phone

Others...
Others...

Device number ⓘ
UID of the credential

12. Integrations

IPassan Manager offers several data integration options. The easiest method is importing Excel files, which can be automated.

The second option is to create read-only access to the database. A developer can then retrieve, for example, information related to supervision (such as integration with time management systems).

Alternatively, this database access can be set to read/write.

12.1. Automatic import/import file template

It is necessary to define the column mapping for the file to be imported. Then, you can choose to either import one or more files into the software manually or create an automatic task that imports the data every hour, day, etc.

A final option allows you to trigger the task on demand via a URL.



In **Tools / Customize**, click on **Add a Custom Import**.

First, define the fields for **"Custom Import Configuration"** as well as the **"Import Options"**:

- Enter a name for this file import model.
- Select the file type:
 - **Xls**
 - **Csv** (default separator is ";")
 - **XML**
- **"Create as"**: this option allows you to choose whether the added tokens will be categorized under **"Access Profile"** or **"Common Identification Title"**.
- **"Door/Zone Access"**: this option automatically assigns an existing access profile from the software. This will always be the same. Alternatively, you can retrieve the door access profile from the Excel file. In this case, the user is added to the specified profile. If the profile doesn't exist, it will be automatically created, but without a door selection.
- **"Identification Title Type"**: this option allows you to select the type of identification title to import.
 - o Choose **"from the file"** if this information is provided in the Excel sheet.
 - o The **"select from the list"** option is useful if the Excel sheet doesn't contain the title type or if it indicates a type with no meaning for IPassan Manager. This option forces the identification type.

Alternatively, you can specify the identification type in the Excel file, but in that case, they have to be correctly mentioned (e.g., Mifare+ token, Keypad Code, 4-button Remote, Hexadecimal Other, etc.).

In the **"Import Data"** section at the bottom of the page, you can import a file using the **Browse** button. This allows you to:

1. Skip the first **x** lines.
2. Define which column in the Excel file contains the data to be imported.

Import data

Download a file for the setting *

Browse
import file.xlsx

Number of lines ignored

Action option on the drop-down list :
U : update TI (Update)
A : add TI (Add)
D : delete TI (Delete)

Save

Cancel

Note: columns can be excluded from import.

12.2. Manual import



Click on the icon « Passes » in the left-hand menu.



In the next window, under the “import by” section, select “file (.xls)”. Then use the “Browse” button to select a custom import and also the type of file to import.

Import data

Import by

Type

☐ environment
 ☐ events
 ☒ file (.xls)

Importation mode

☒ Standard importation
 ☐ Bulk importation

Browse

Get the file to be completed

Options for import

Create as

☐ Contractor
 ☒ Users (automatic creation)

Door/zone access

☒ From file
 ☐ Select from the list

Floor access

☒ From file
 ☐ Select from the list

Companies

+

Bluetooth

Antigua & Barbuda

12.3. Imports with automatic task

IPassan Manager also allows the automatic import of these file types. Third-party software can regularly place a file in a designated directory, and IPassan Manager will then import it.

Once the file is processed by IPassan Manager, it is moved from the designated directory to **/Backup**.

If multiple files are placed in the directory, they will all be processed.

In **“Tools” / “Automatic Tasks”**, click on **“Create a Task”**.

Task 0001

Name: Task 0001

Execution frequency: Every month

From: 2025-01-20 14:42:50

☐ Execute until the: 2024-01-20

Processing to do: Archiving of site data

Archive the latest: Month and earlier

> Archiving option

> ☒ Purge after archiving

Backup type: Mail

Add a recipient

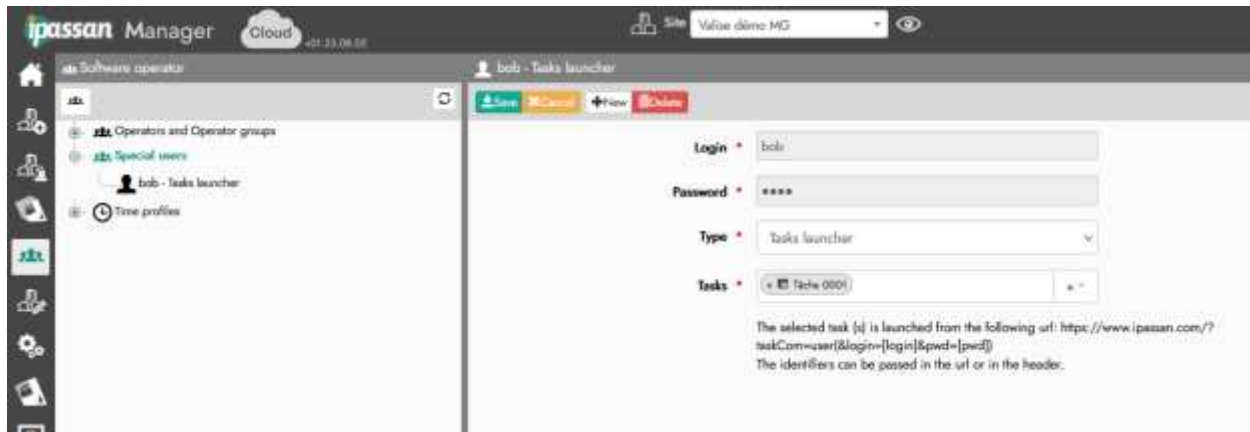
> ☐ Watch task

> ☐ Emails settings

- Enter a **name** for the task and **select the frequency** (e.g., hourly, daily, weekly, etc.).
- Choose the **action to perform** on the list next to the “processing to do” field (e.g., importing people via file in this example). Depending on the selected option it may affect the next fields or add others).
- **Specify the directory** where the files to be imported are stored.
- Select the **import type** (default in IPassan Manager / custom).
- If it's a custom import, choose the predefined template. Click **Save** at the bottom right.

12.4. Import with external commands

Once the scheduled tasks are configured, they can be triggered on the server via a URL. The first step is to create a software user who is authorized to launch the task. Click on “Software Access” in the left-hand menu. Then, in the tree structure, select “Special Users”.



- Enter a login and then a password.
- Select the “**Task Launcher**” option in the “**Type**” field.
- Choose the task by clicking on the “+”.
- Don't forget to **save**.

The following text appears and shows the syntax to follow in order to trigger the task via a web browser:

Note: to run this task from another computer, simply replace **127.0.0.1** with the IP address of the IPassan server, as shown in the example below:

[https://127.0.0.1/IPassan /?taskCom=user&login=lanceur&pwd=0000](https://127.0.0.1/IPassan/?taskCom=user&login=lanceur&pwd=0000)