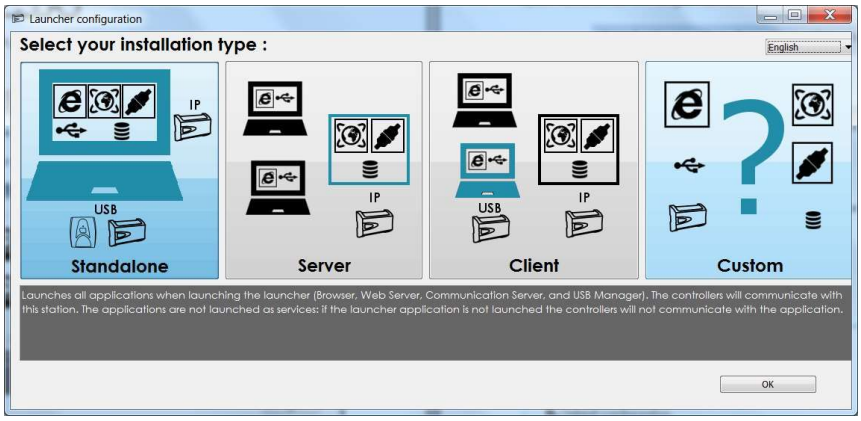
Configuration guide

First start

Run iPassan from the desktop icon.

When running iPassan for the first time it is necessary to choose the installation type –



Standalone

Choose this mode if the site will be set up on a laptop for example, and then left to run standalone i.e. without a PC or laptop permanently connected.

Note that in this mode all information from the site (events etc) can be interrogated at a later date when a PC or laptop is re-connected.

Server

Choose this mode if a PC will be permanently left connected to the site. The software will be permanently running.

Client

Choose this mode when the software will be permanently running on a Server PC (over a network) and this PC will be used only to connect to the site or to administer the site, for example to add keys.

Custom

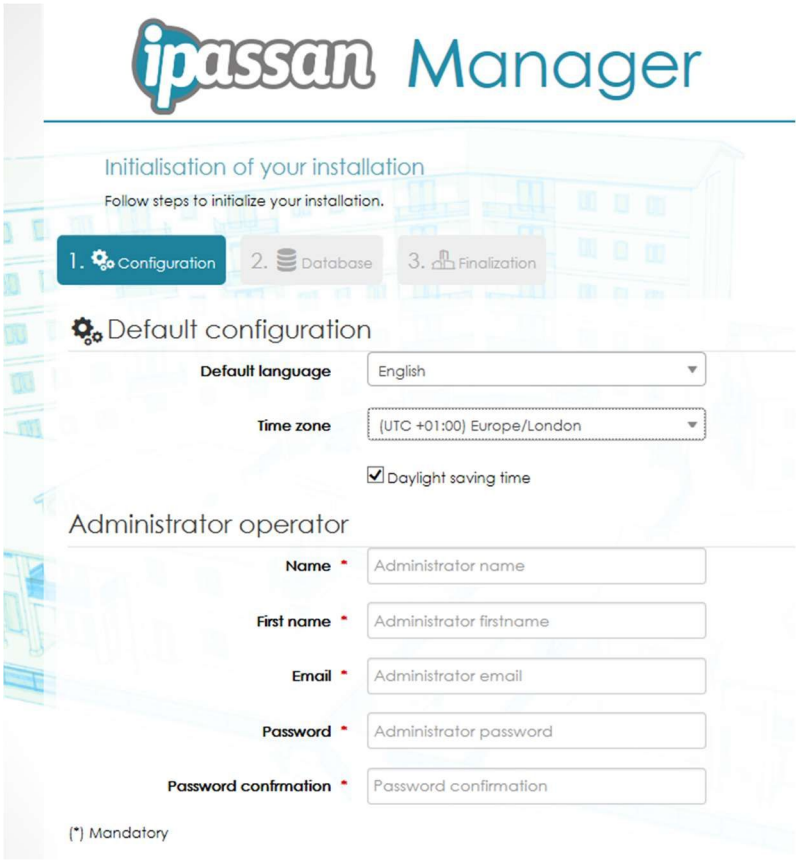
Choose this mode for complex installations i.e. multiple PCs across a network for example where the system database can be managed from one PC, and the communications from another PC.

Note that it is possible to change the installation type at a later date

Basic software setup

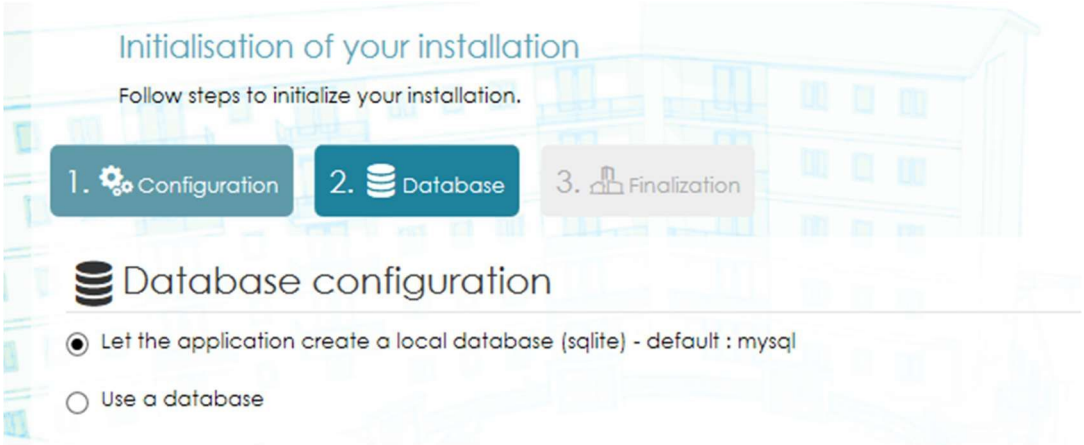
Configuration

Choose the **Default language** and select the **Time zone**, then enter the mandatory information and click **Next** –



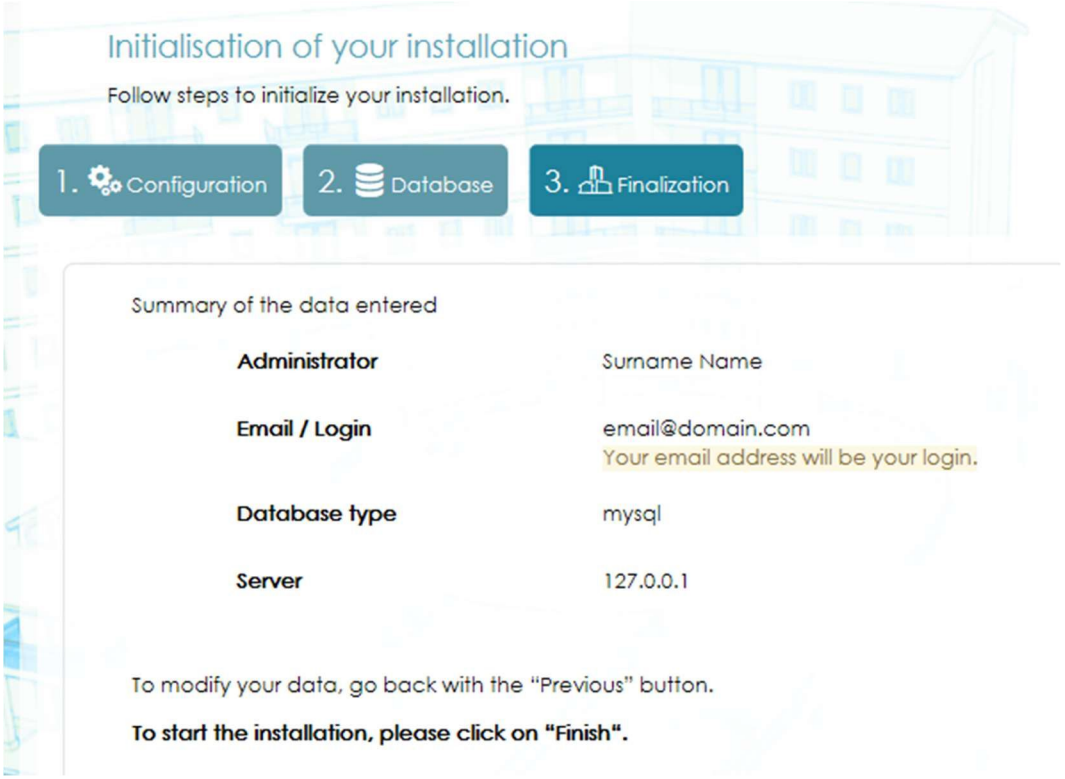
Database

It is recommended to use the default (mysql) database.

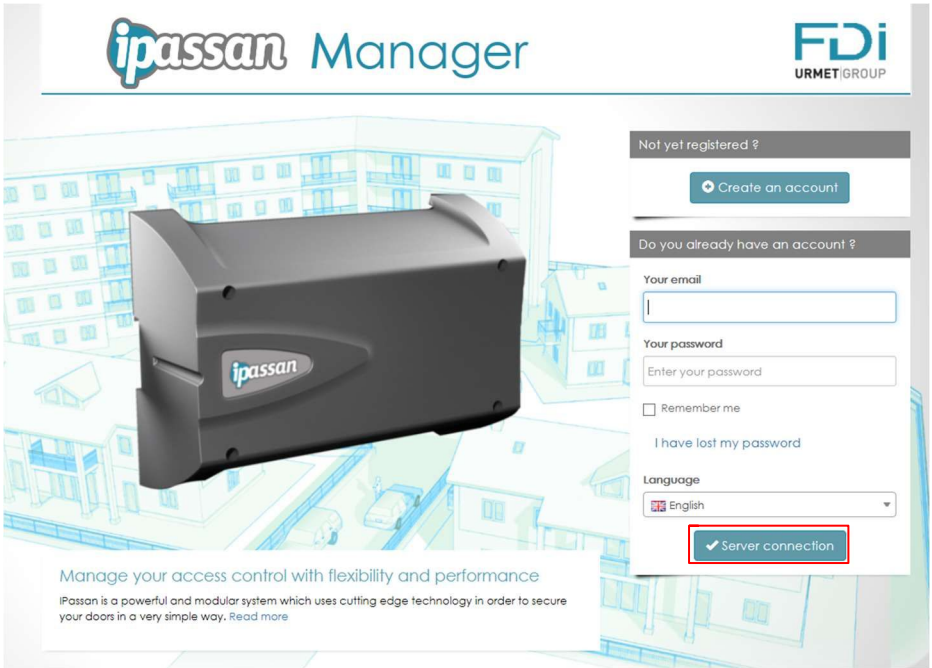


Finalization

Review the information and click **Finish**

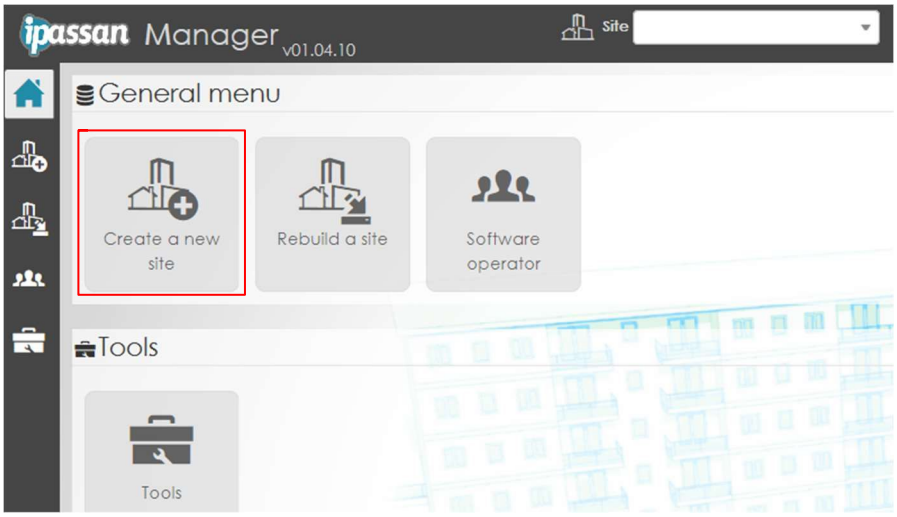


Enter the email address and password which you have previously set up and click **Server connection**



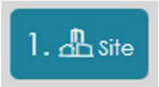
Creating a new site

Click **Create a new site**

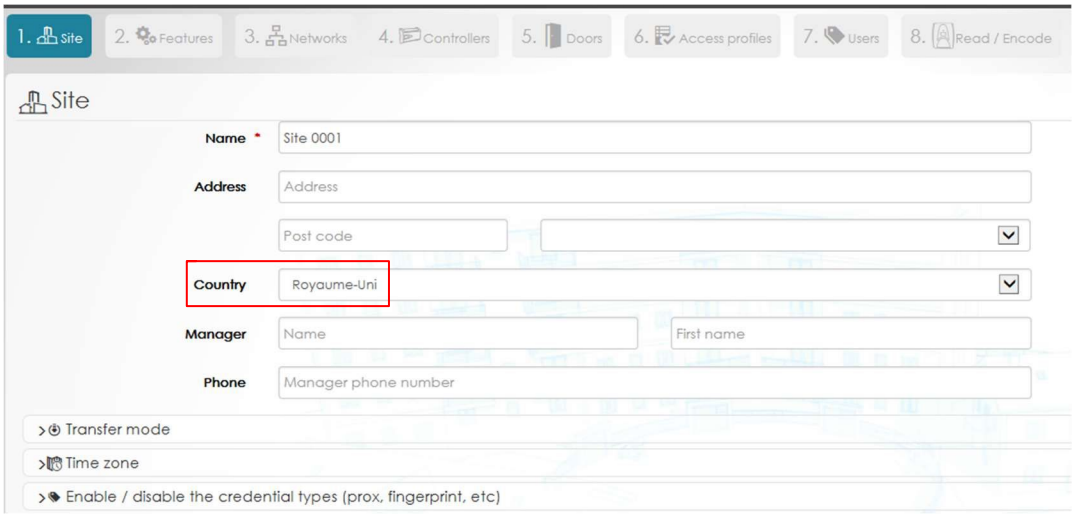


There are eight steps to creating the site, which can be seen in the bar along the top of the page -

Step 1



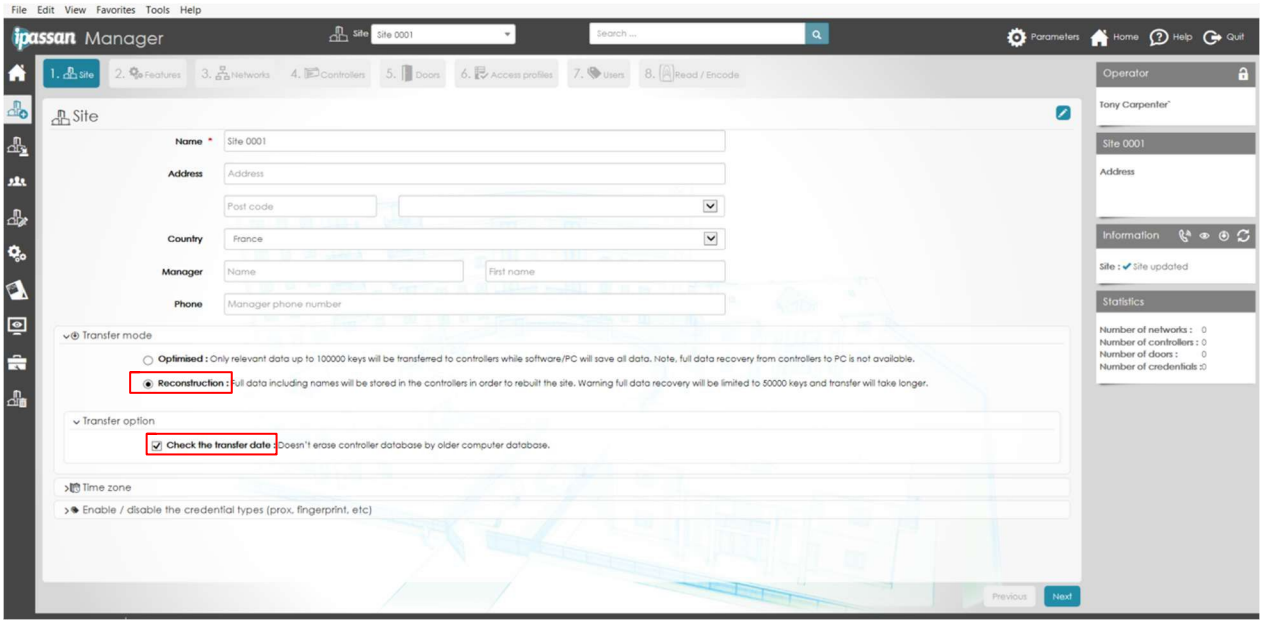
Complete the Site details form - select **Royaume-Uni** (United Kingdom) for the country.



Click the **Transfer mode** dropdown –

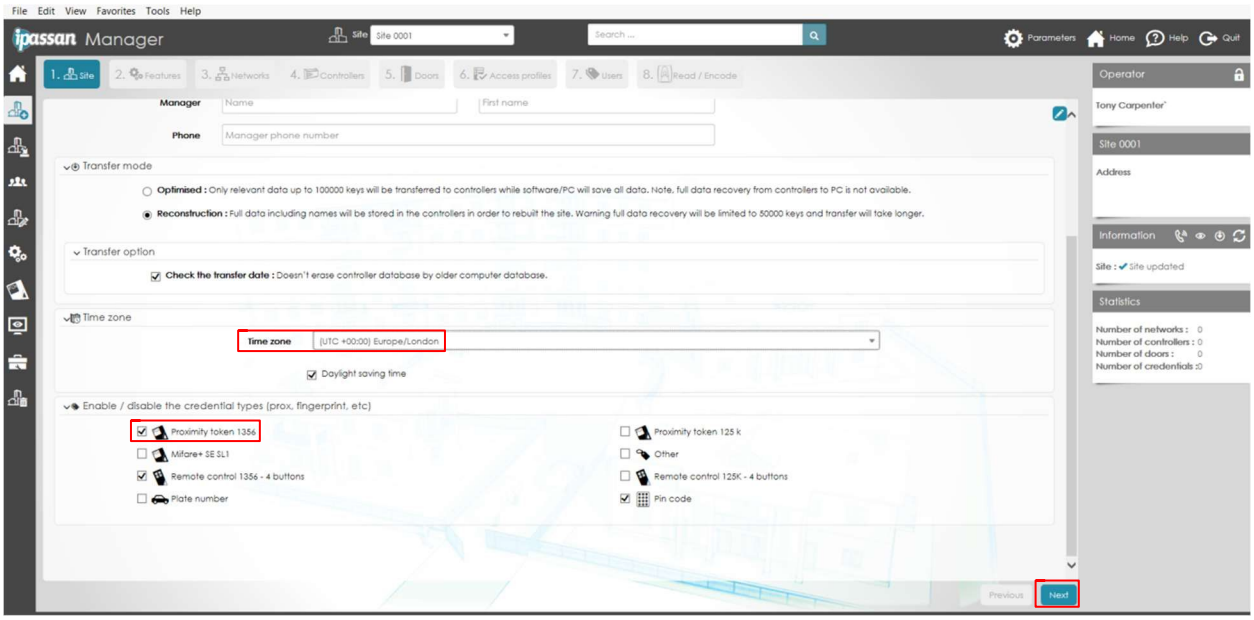
If the site will contain less than 50,000 keys then it is recommended to choose **Reconstruction**

Under **Transfer mode**, make sure that **Check the transfer date** is ticked. This prevents an older database on the PC from overwriting a later database in the controllers.



Choose **Europe/London** for the **Time zone**

Select the type of keys, remote controls, keypads etc which will be used and then click **Next**


File Edit View Favorites Tools Help
ipassan Manager
Site
Site 0001
Search ...
Parameters
Home
Help
Quit
1. Site
2. Features
3. Networks
4. Controllers
5. Doors
6. Access profiles
7. Users
8. Read / Encode
Manager
Name
First name
Phone
Manager phone number
Transfer mode
Optimised : Only relevant data up to 100000 keys will be transferred to controllers while software/PC will save all data. Note, full data recovery from controllers to PC is not available.
Reconstruction : Full data including names will be stored in the controllers in order to rebuilt the site. Warning full data recovery will be limited to 50000 keys and transfer will take longer.
Transfer option
Check the transfer date : Doesn't erase controller database by older computer database.
Time zone
Time zone
(UTC +00:00) Europe/London
Daylight saving time
Enable / disable the credential types (prox, fingerprint, etc)
Proximity token 1356
Mifare+ SE SL1
Remote control 1356 - 4 buttons
Plate number
Proximity token 125 k
Other
Remote control 125K - 4 buttons
Pin code
Previous
Next
Operator
Tony Carpenter
Site 0001
Address
Information
Site : Site updated
Statistics
Number of networks : 0
Number of controllers : 0
Number of doors : 0
Number of credentials :0

Step 2

The final look of the iPassan system for the end user can be customised. So if for example there are no counting zones or anti-passback zones, the **Use zones** option will not be ticked at the setup stage, and the end user will not see icons relating to zones.

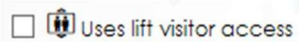
Site architecture is used in complex buildings where it will be necessary to sort users by building or by floor for example. If iPassan manages lift control then it is mandatory to tick this option. Otherwise it is recommended not to.

If door contacts are used for example to detect doors left open or doors forced, then tick this option.

Tick if you will be using counting zones or anti-passback zones.

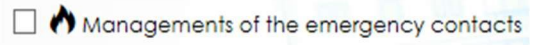
This option is used if it will be necessary to configure relationships between system events, for example a door forced open creates an output from an iPassan expansion card

Tick if you are using any of the following products - 1104/910 (10 Input Base Module) 1104/913 (10 Output Base Module) 1104/912 (12 Input Expansion Card) 1104/914 (12 Output Expansion Card)



If iPassan controls access to lifts tick this option. Note that when ticking this option, **Use site architecture** will automatically be ticked.

This feature allows the 4-button RF remotes to be customised for different users. It is not recommended to use this function.

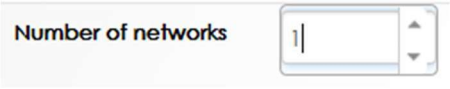


Tick this option if the fire alarm system will be interfaced to iPassan.

Tick this option if you will be using a site code.

Step 3

See Pages 3 & 4 of the **iPassan Installation Guide** for an explanation of the types of networks that can be implemented using iPassan.



Use the following examples to determine the number of networks in your installation –

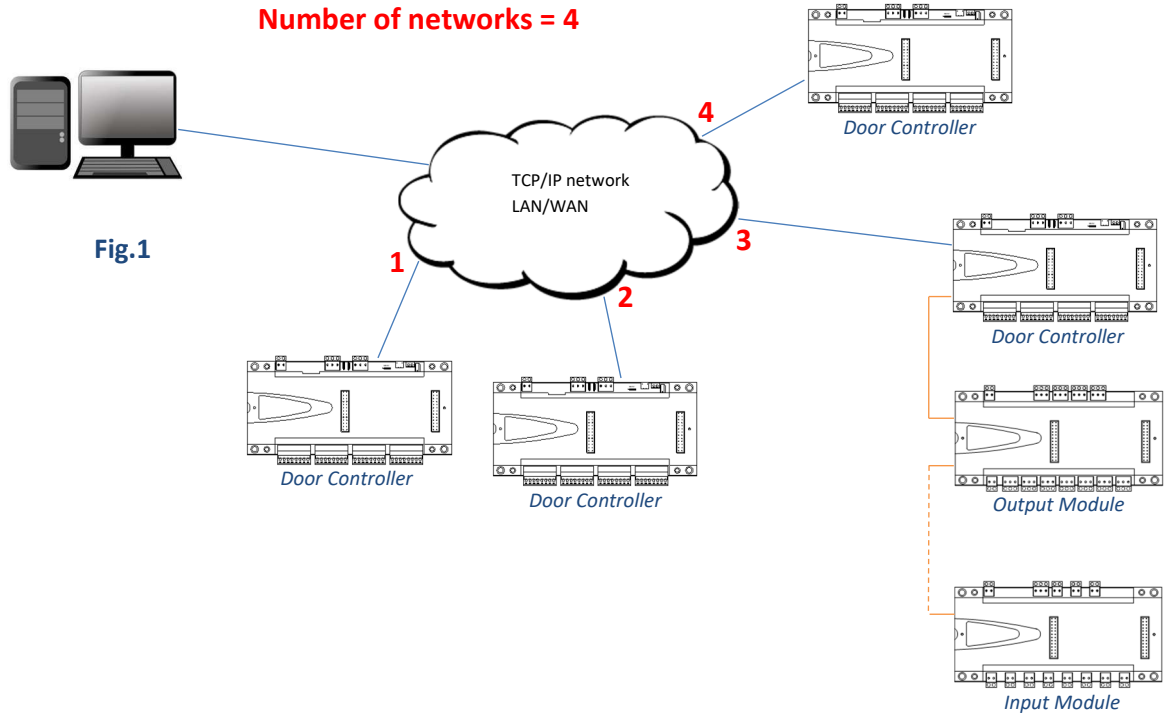


Fig.1

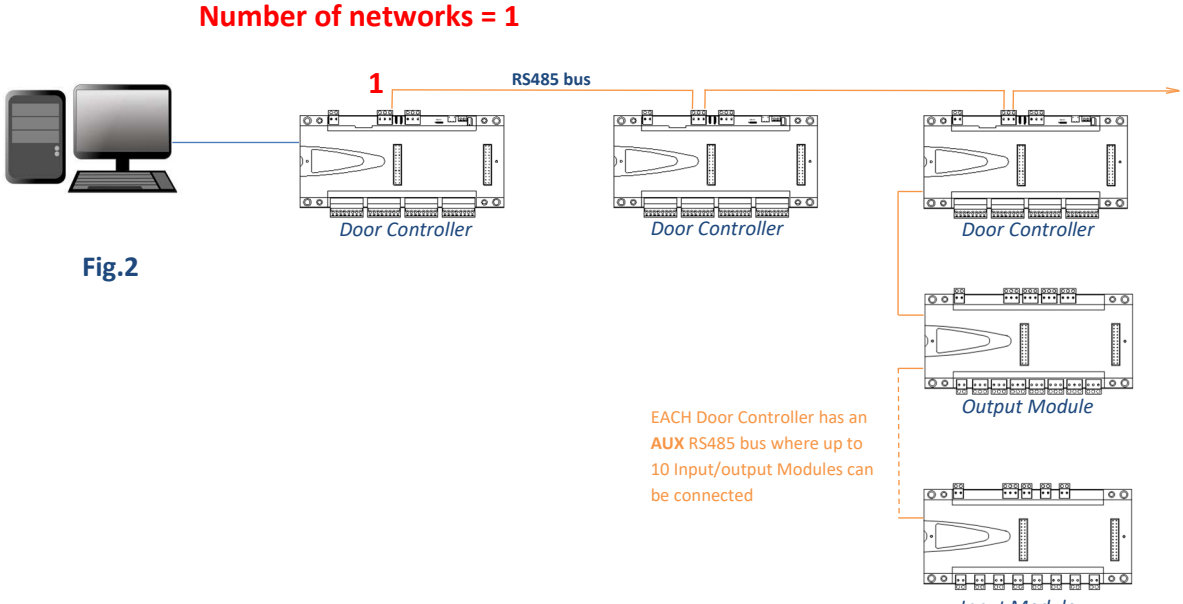


Fig.2

Number of networks = 4

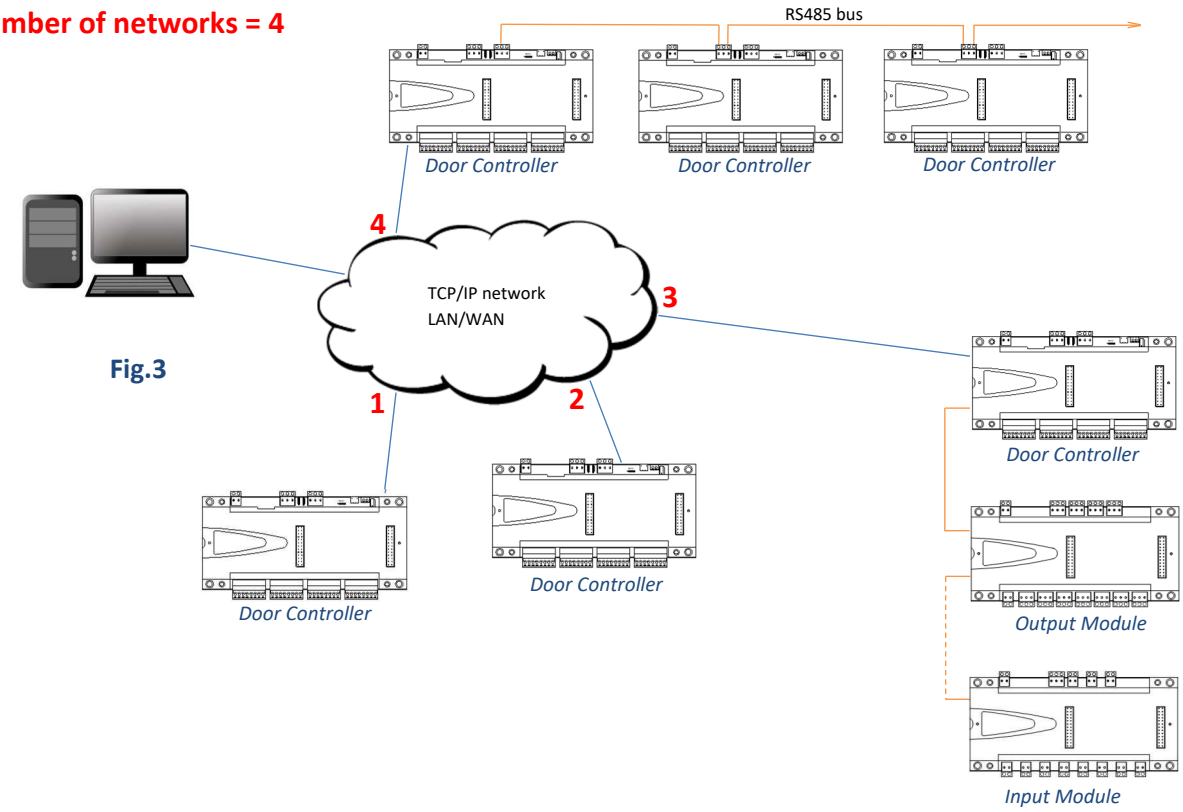
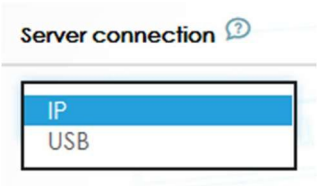
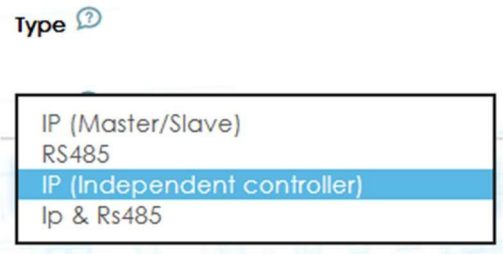


Fig.3

Give the network a name.



Specify the type of connection between the server (the PC where the iPassan software is running) and the network.



IP (Master/Slave) One controller communicates with the server (Fig.1)

IP (Independent controller) Each controller communicates with the server (Fig.1)

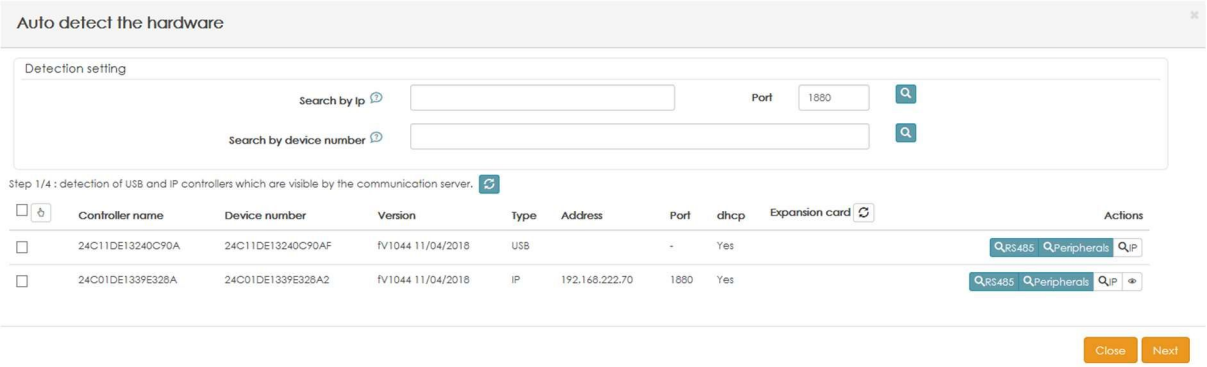
RS485 See Fig.2

IP & RS485 See Fig.3

Select the type of network.

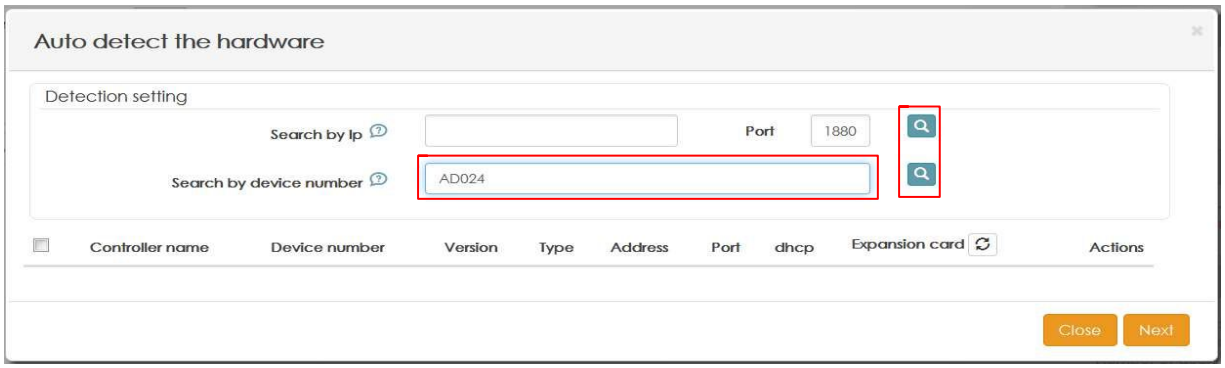
Choose the number of controllers. This is the total number of Door Controllers (not Input/output modules) in the installation. In Fig.3 the number of controllers would be six for example.

Clicking **Auto detect the hardware** will automatically detect the connected controllers and peripherals and add them to the network.



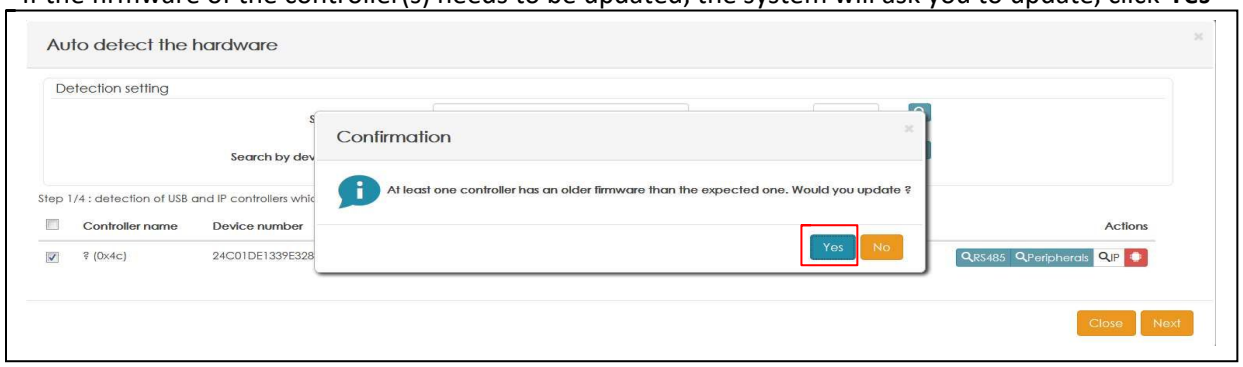
If the system does not find the controller(s), it is still possible to search via IP address (controller default: 192.168.1.250) or directly via device number (printed on the sticker on the side of the unit) – recommended.

Enter the device number next to **Search by device number** and click the  icon



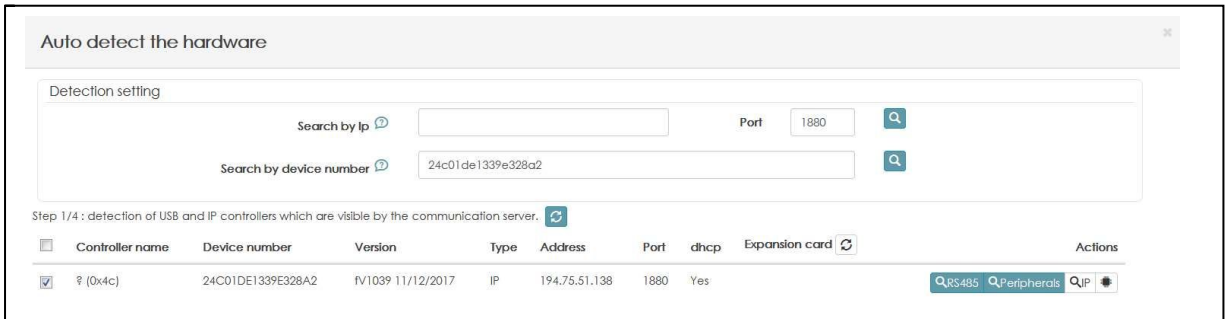
Once the controller(s) have been found they will be listed, tick the check box next to the required controller(s) and then click **Next.**

If the firmware of the controller(s) needs to be updated, the system will ask you to update, click **Yes**



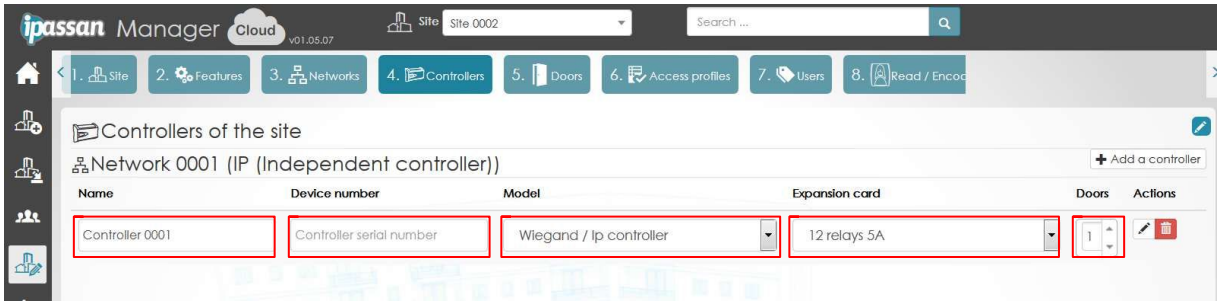
Tick the button for the firmware version, enter the device password (default 0000) and click OK

Once completed, the controller will automatically reboot itself, click **Close** to finish.



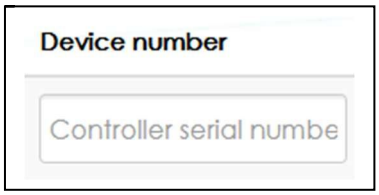
Step 4

Here you need to enter details of the controller and expansion cards (if fitted).

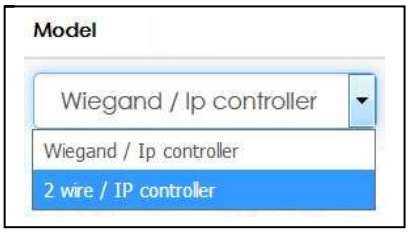


First enter a suitable **Name** for the controller so it can be identified easily on the network.

Then under **Device number** you should see the serial number of the controller that was discovered in the previous step.

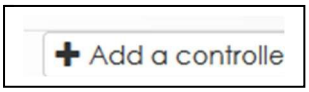


Next select the **Model** of the controller; this can be either Wiegand / Ip controller or 2 Wire / IP controller. This will normally be 2 Wire / IP controller.



Each controller is able to manage an expansion card (12 inputs or 12 outputs or extra doors). Select if an expansion card is connected to this controller.

Lastly enter the number of **Doors** that are connected to the controller.

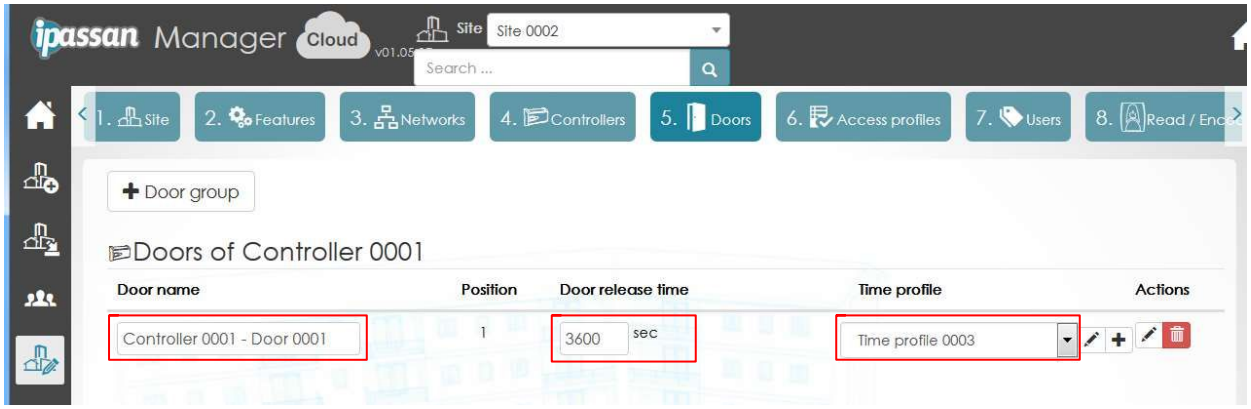
If you need to add another controller onto the network then click on 

and repeat the above until all controllers have been added to the system.

Then click 

Step 5

Here you can enter details of the door(s) on the system.



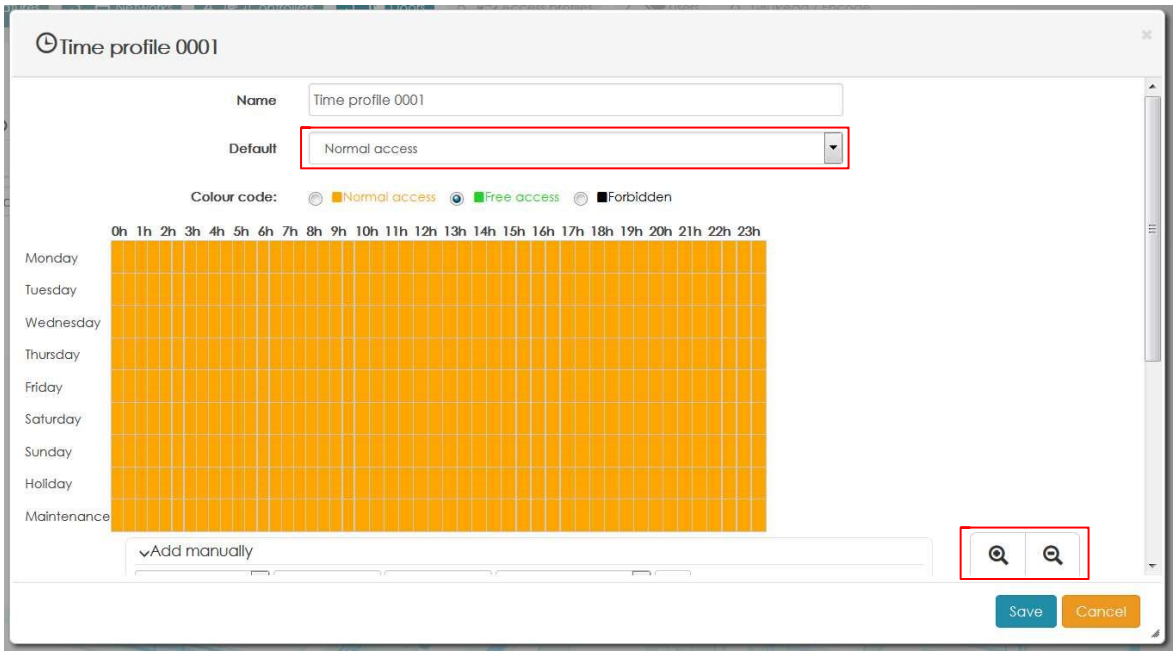
Here you can enter details of the door(s) on the system.

First under **Door name** enter a suitable name for the door so it can be identified easily on the network.

Then enter the **Door release time** (the default is 5 seconds) – the maximum time allowed is 3600 seconds (60 minutes).

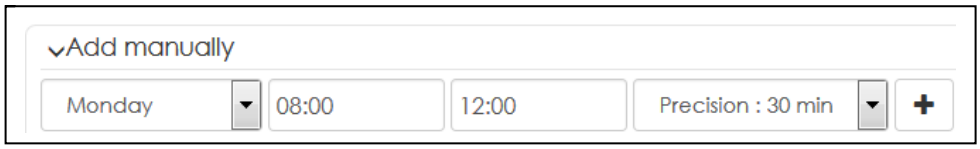
A door can have 3 types of operation:
- Free access, the door is unlocked.
- Forbidden, no access even if a valid key fob is presented to the reader.
- Normal, a valid key fob has to be presented to release the door.

To add a door time profile click on the  icon and the following window will open –

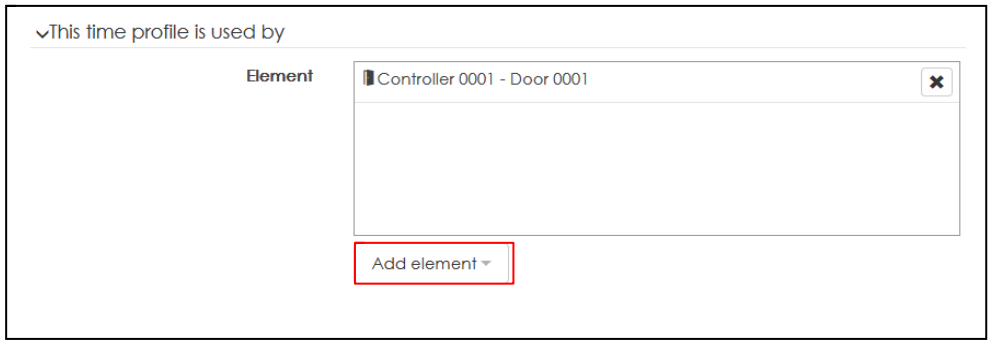


Name the profile, and then in **Default**, use the drop down arrow and select the type of operation for the profile - **Normal access**, **Free access** or **Forbidden** as required.

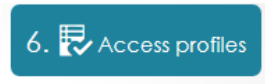
Using the  icons will enable a progressively more precise time to be selected for the graphical profile (range is 30, 15, 10 or 5 minute increments). In addition this information can be added manually by selecting the drop down arrow next to **Add manually**



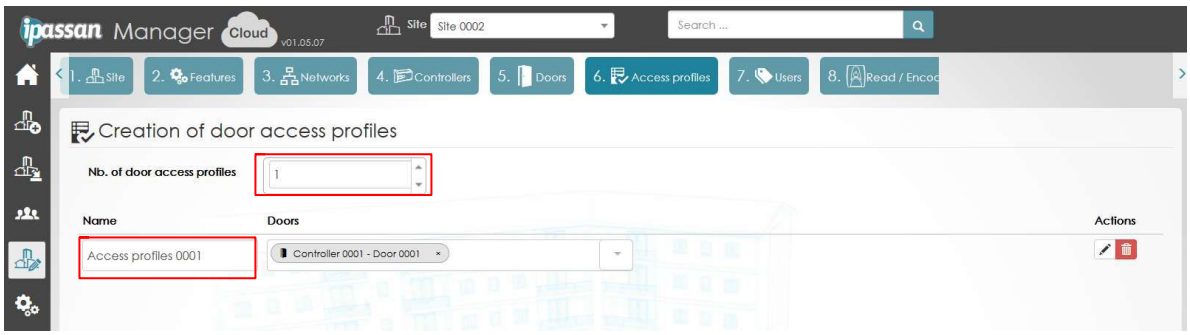
Scroll down and then you can select the controller on the system that will use this specific profile, click on **Add element** and then select as required. Click **Save**



Step 6

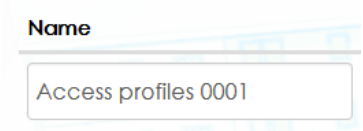


The system works with access profiles. An access profile is a list of authorised doors that a user can open or has access to.
It is possible to have either a permanent or temporary profile.
A temporary access profile is a list of authorised doors that a user could use from a beginning date to an end date.

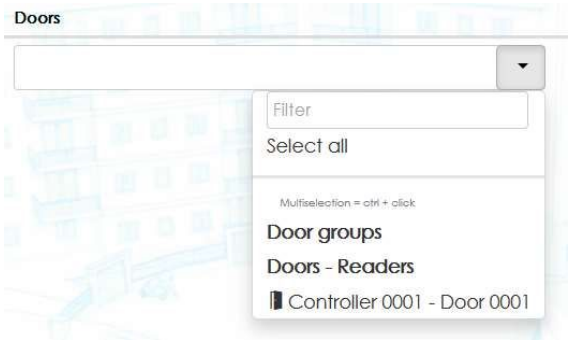


First select how many access profiles are required:

Then give each profile a suitable **Name**: *e.g. Ground Floor Doors.*

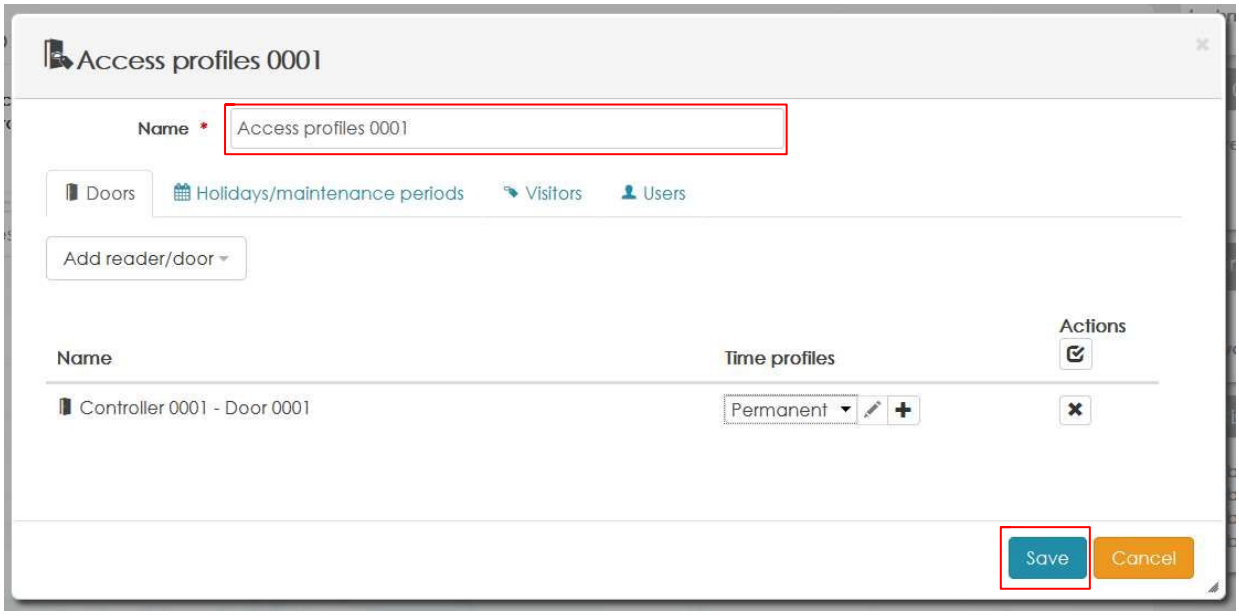


Next, click the drop down arrow and select the controllers and/or doors that will be within the profile:



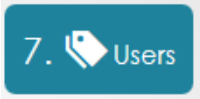
The doors will then be displayed under the access profile to which they belong.

Clicking on the  icon will bring up the following window.



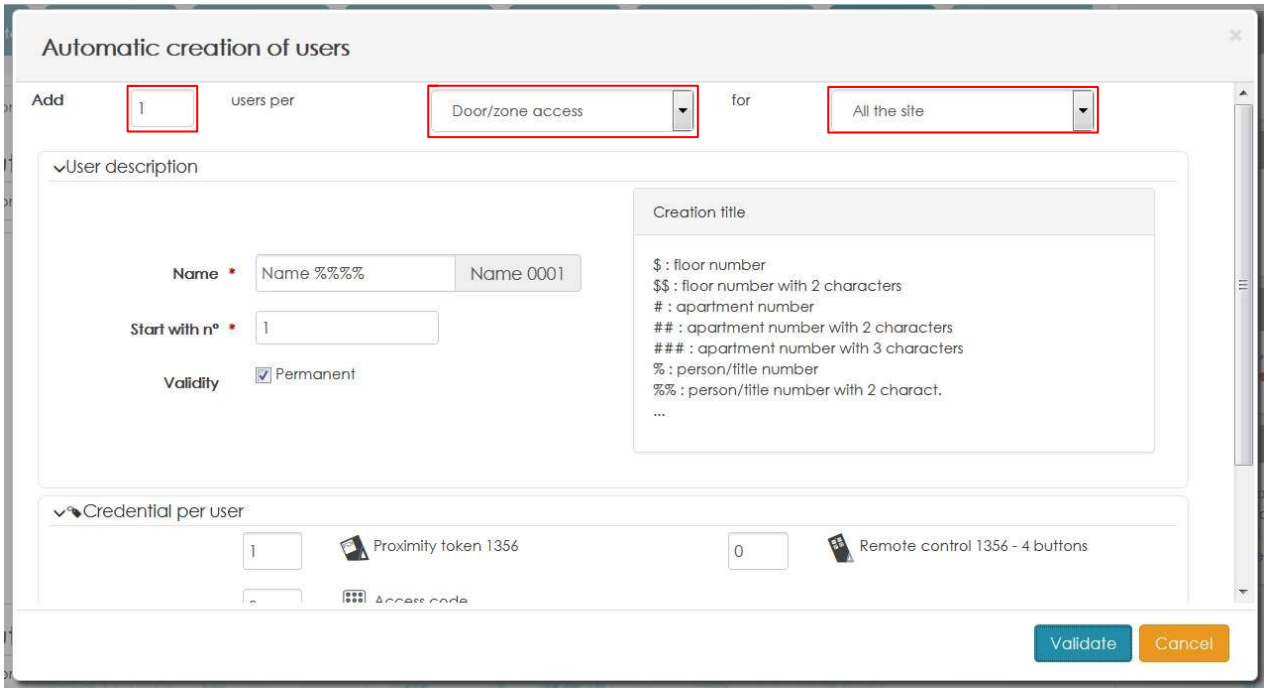
Give the profile a suitable name, then click **Save**

Step 7



The system can automatically create a number of users. Click on 

and the following window will open up:
(Note this automatic creation can be repeated for additional blocks of key fobs as required).

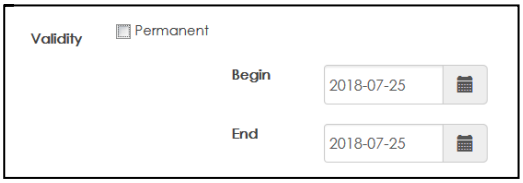


First, next to **Add** enter the number of users you wish to add, then next to **users per** leave the default Door/zone access selected, lastly next to **for** use the drop down arrow to select the access profile if required. Note the default setting will be All the site.

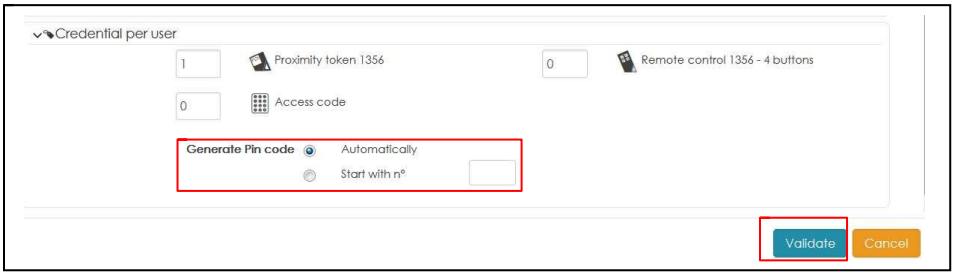
In the **User description** field enter a name for the user – this will be replicated for all users, and the user number will be added to it. So below you would have Name 0001, Name 0002, Name 0003 etc.

Then enter the **Start with no** of the user. This could be useful, if you have for example 20 users for parking only, then another 15 for gym access. The fobs could then run 1 -20, then 21 to 35.
Ensure the **Validity** box is ticked.

If you untick the **Validity** box, then you have the option to set a date window during which the key fob will operate. This can be useful if you need contractors to have access during renovation works, and then after the works have finished the key fobs will automatically expire.



Lastly, enter details of the type of credential that will be used. A credential is another name for the way in which the user is granted access.
A user can have unlimited credentials such as key fobs, access codes for keypads and remote controls.
Access codes for keypads can be automatically generated.
Next to **Generate Pin code** there are 2 buttons able to be selected – **Automatically** or **Start with no**. Select **Automatically** to have the system generate a random 4 keypad code for the user, select **Start with no** to have the system generate codes beginning from an entered number.

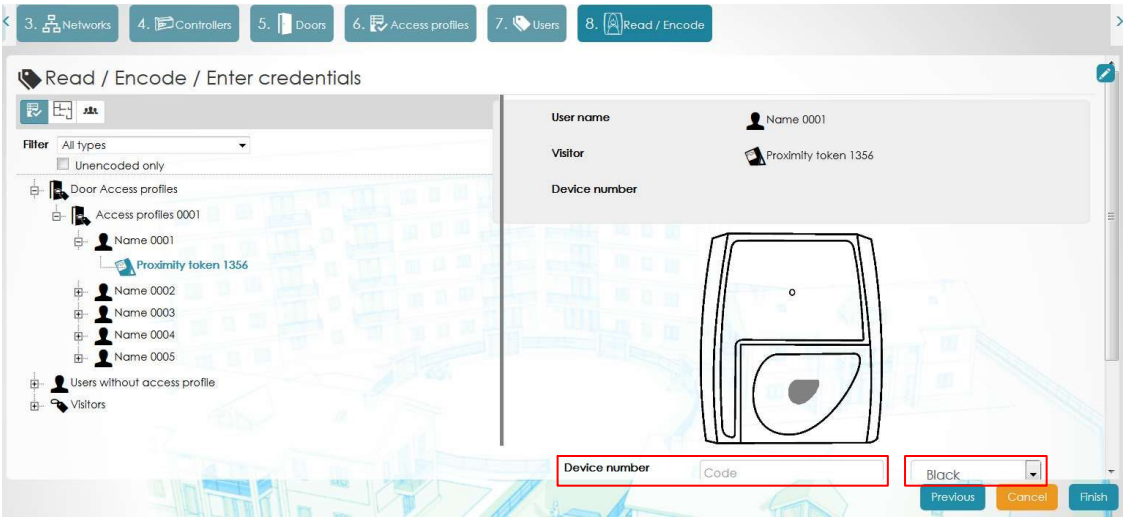


Finally, click **Validate** to save the information.

Step 8

The last step is to encode the key fobs.

There are two ways to do this.
- Manually enter the number printed on the key fob.
- Use a USB management reader/encoder (part number 1104/904) connected to the PC to read the number from the key fob.



On the left hand side of the screen you can select the user for whom you wish to add the key fob details. On the right hand side of the screen you will see the user details.

If no management reader/encoder is connected you can manually enter the key fob number in the **Device number** box, and then select the key colour (if required). When the key fob is programmed the system will automatically move to the next user. Scroll down to reveal two user options.

If the user has more than one key fob then selecting **Next credential** will enable you to program the next credential (key fob) for that user.
Selecting **Next user** will jump to the next user for programming of the next key fob.

Once all key fobs have been entered then click **Finish** to finish creation of the site.