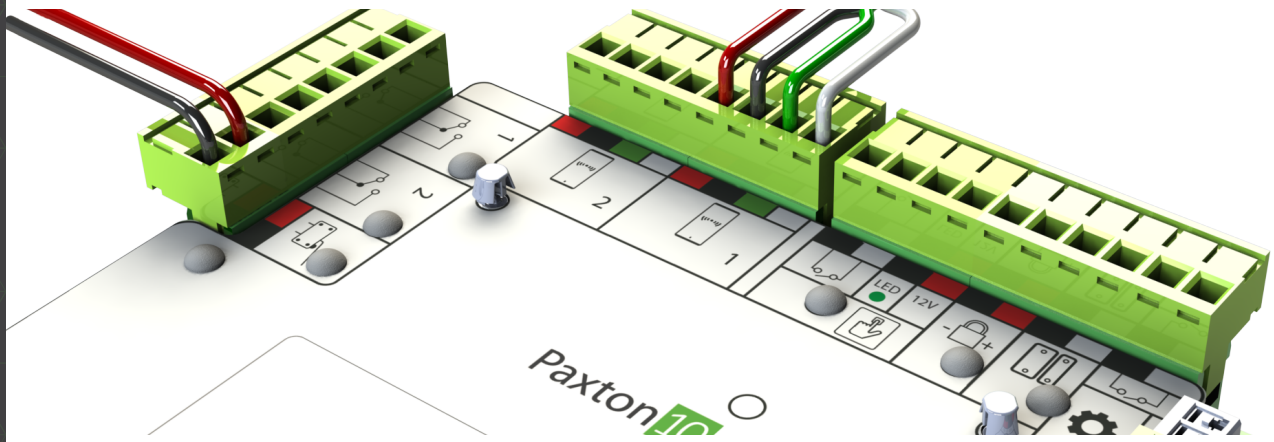


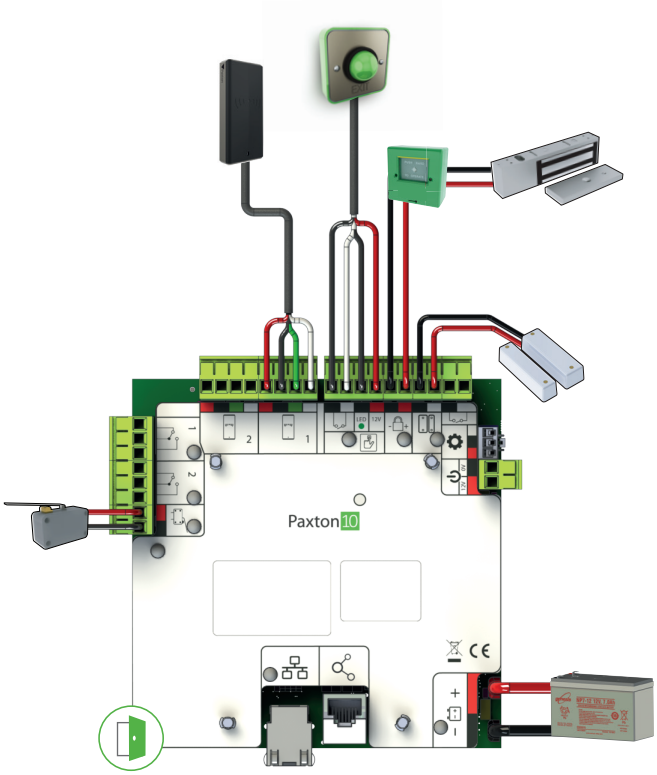
How to add an access point to Paxton10

Overview

Securing access points with Paxton10 allows control and monitoring of who, when, and where in the site users are gaining access, providing the option to restrict access based on the person, access point, and date and time of day.

The Paxton10 controllers are the brains of the system. Each controller is responsible for allowing or restricting user access, and has the built in peripherals for securing a single access point.

Hardware setup

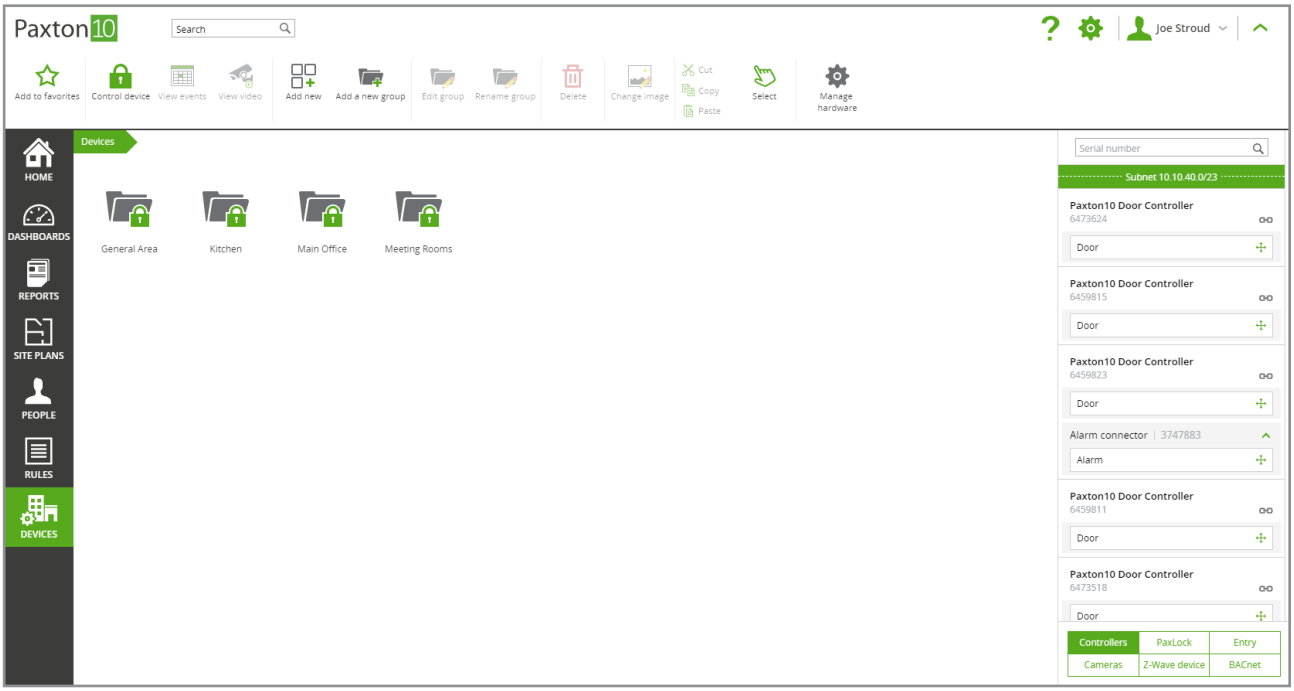


Adding a controller to the system

1. Navigate to the '**Devices**' section. The Device Panel (right-hand side of the screen) will show all unmapped* Paxton10 controllers

*unmapped controllers are those not currently associated with a Paxton10 device. Once bound and mapped to a device, the controller will appear in the '**Hardware Management**' window.

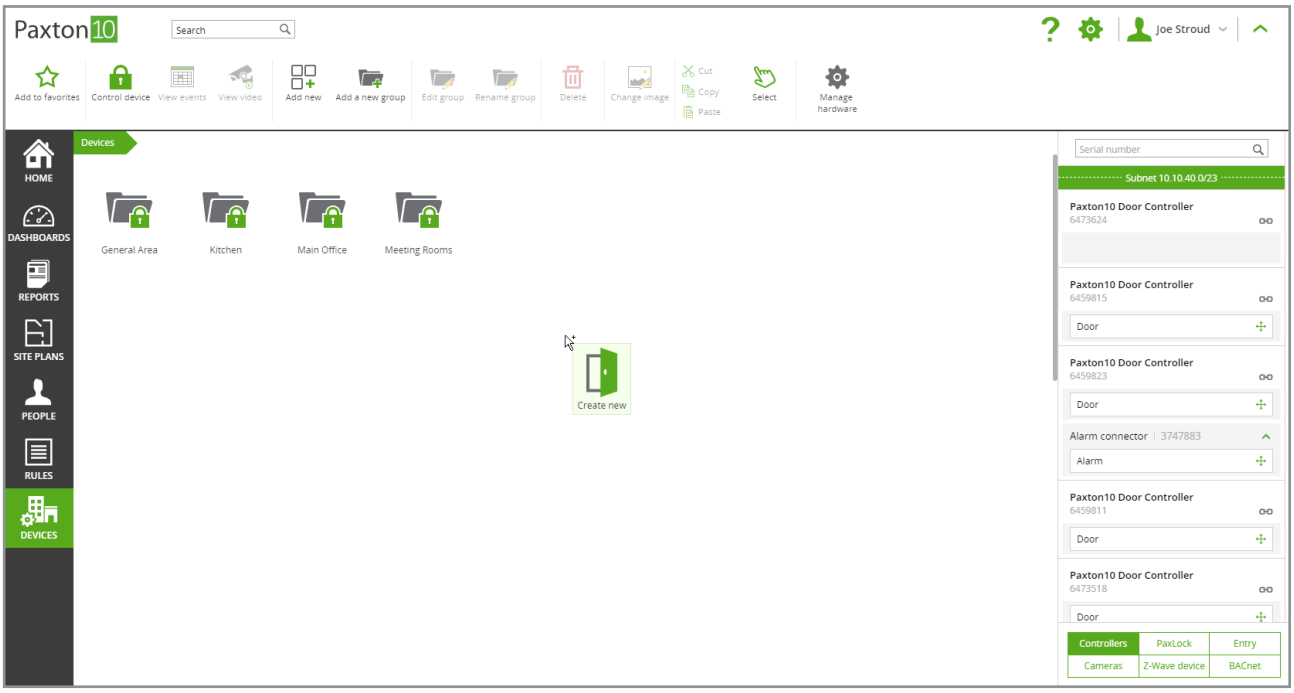
2. If your controller is connected to the same network as your Paxton10 server, the controller will automatically be detected and listed in the Device Panel. If the controller isn't listed / is installed on a different subnet or network, please go to APN-0058 (Using Multi-Site to create a Paxton10 system across separate sites (or subnets)) to see how to add your controller.



3. Drag a component (e.g. Door) from the controller and either drop it onto an empty space to create a new device in Paxton10, or drop it onto an existing device to map the component to the device.

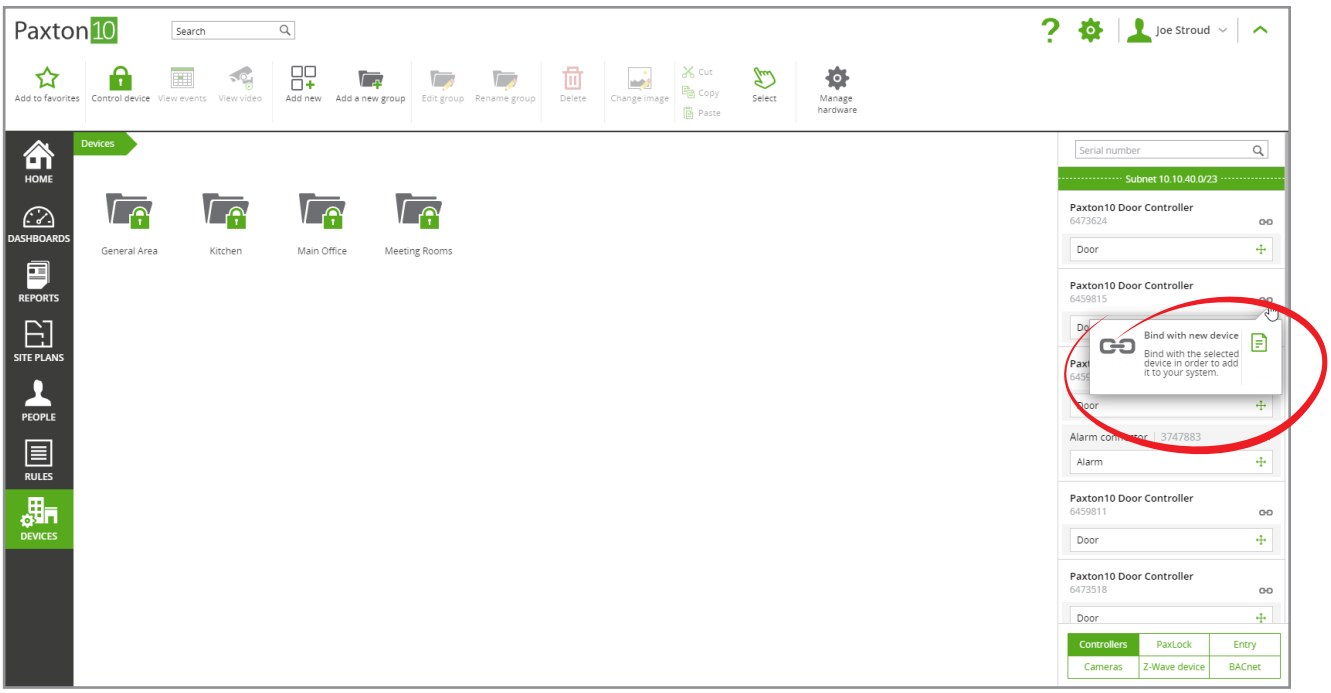
4. In the '**New Site**' window, either enter the IPv4 address of the controller, or enter its serial number and activation code*, then click '**Add**'. The controller, and any others on the same network, will now be listed in the device panel

*serial number and activation code method of detection requires that both the server and the controller have an internet connection.



Once a component from the Paxton10 controller is mapped to a device in Paxton10, the controller is then bound to that Paxton10 system, and can't be detected or controlled by any other system.

If it is not appropriate to create and map to devices at this stage, clicking the green 'link' icon next to each controller in the right-hand side of the screen will also bind the controller to the system, preventing any other systems from taking ownership.



Configuring an access point

Upon dragging a '**Door**' component from the device panel, a pop-up will show with some basic configuration. For many installations this is all that is required, and the access point will now be up and running. If a different setup or advanced settings are required, locate the newly created access point in the '**Devices**' section and click on it.

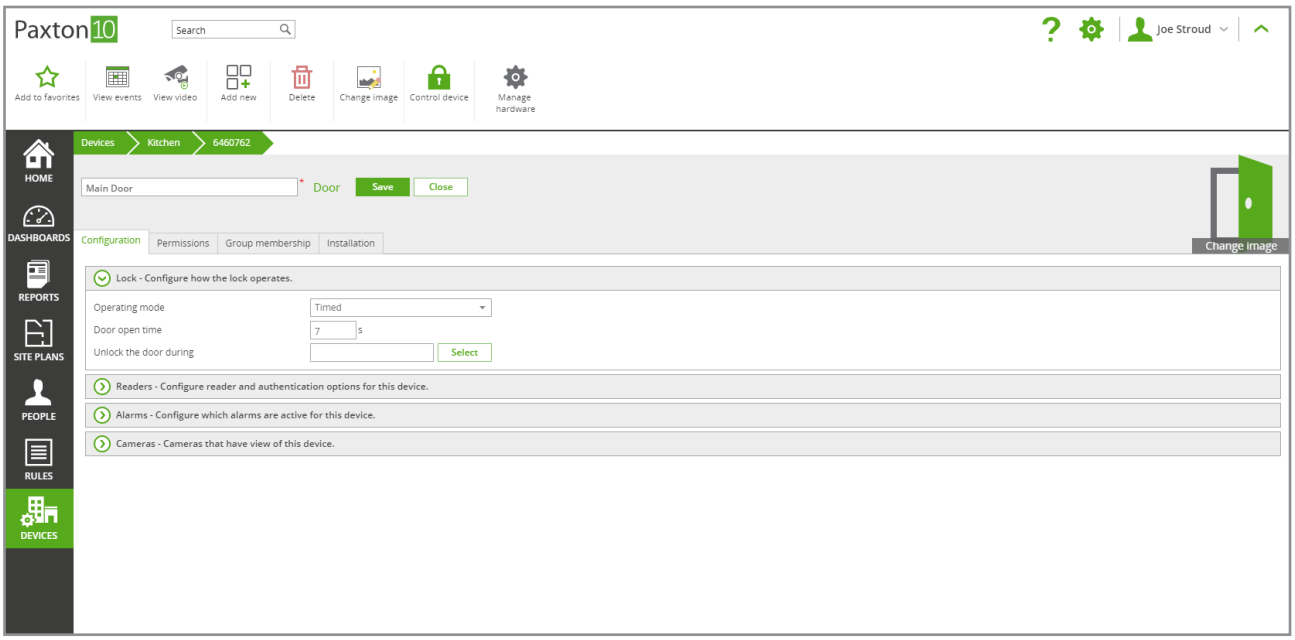
Configuration

Lock

1. Select the operating mode of the door – Toggle (present token to unlock, present again to lock) or Timed (present token to unlock for a number of seconds)

2. Define the door open time (if using timed mode)

3. Select a time profile that the door will stay unlocked during



Readers

The reader settings apply to all readers mapped to this access point. Not all settings apply to every type of reader.

1. Check the box to enable audible feedback when presenting credentials.

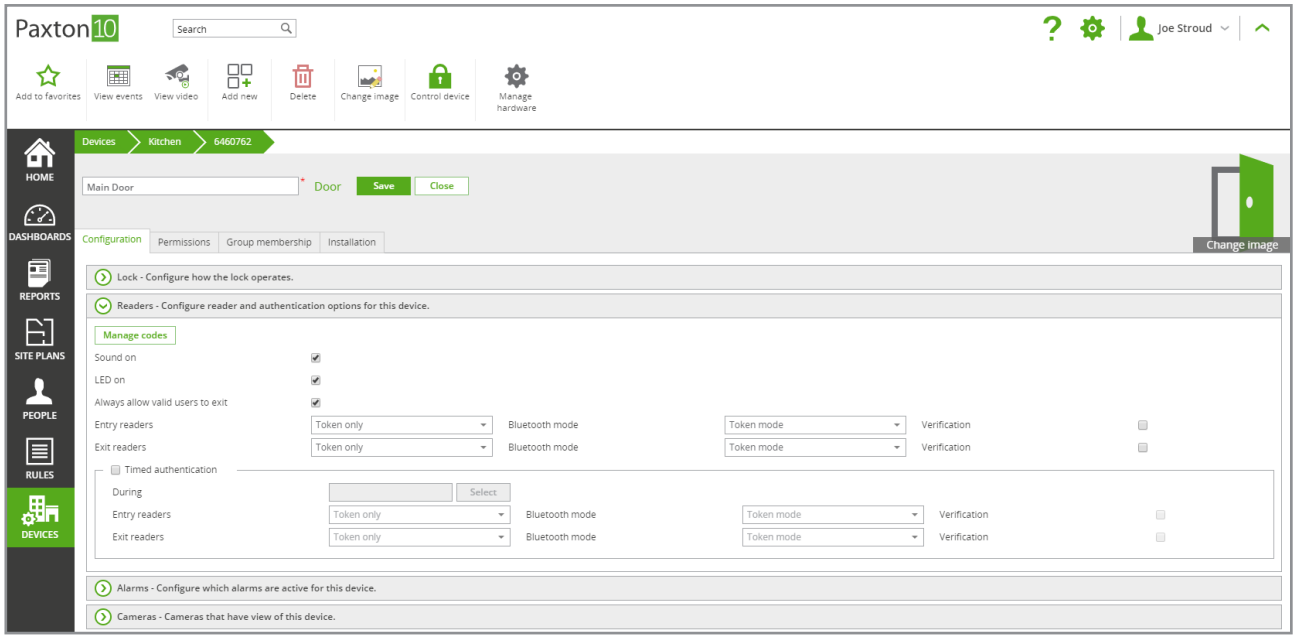
2. Check the box for the readers to always show a white LED, allowing the reader to be easily located in a dark environment.

3. Select whether to always allow users to exit (even if they are outside of their permissioned time profile).

4. If using keypad readers, configure the authentication required at each reader (Token, PIN, Code).

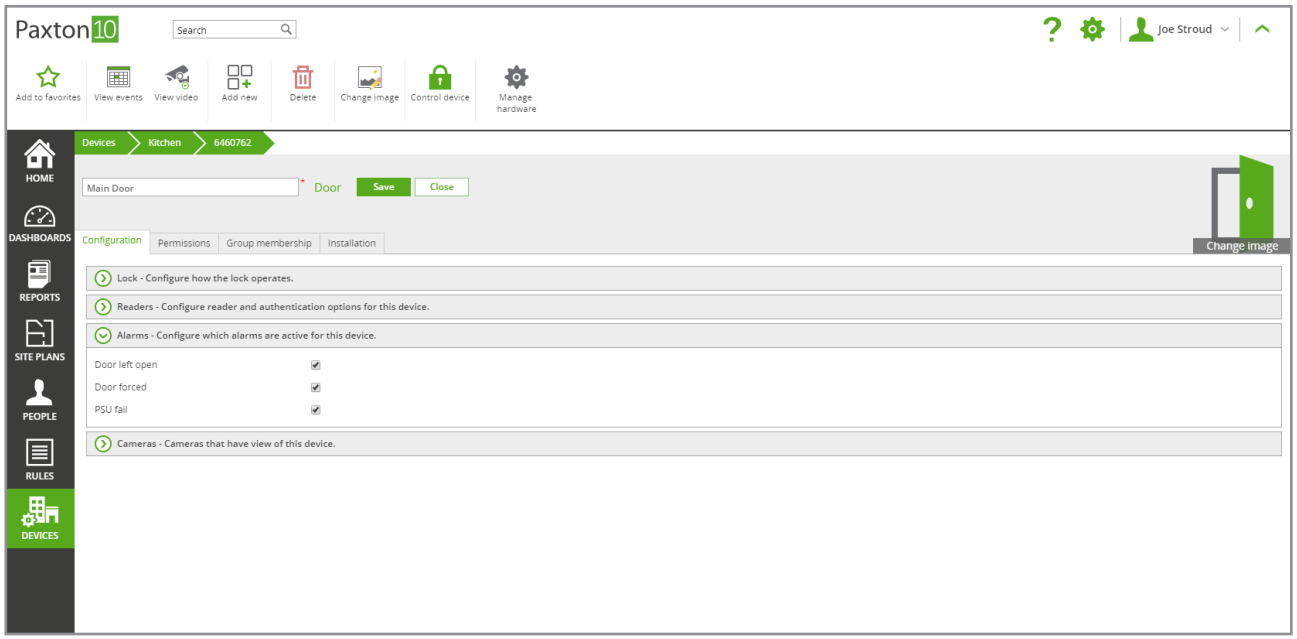
5. If using Smart credentials (Smartphones or Bluetooth fobs), select the Bluetooth read range.

6. If using Smartphones, tick 'Verification' to enforce users to unlock their device before access is granted.



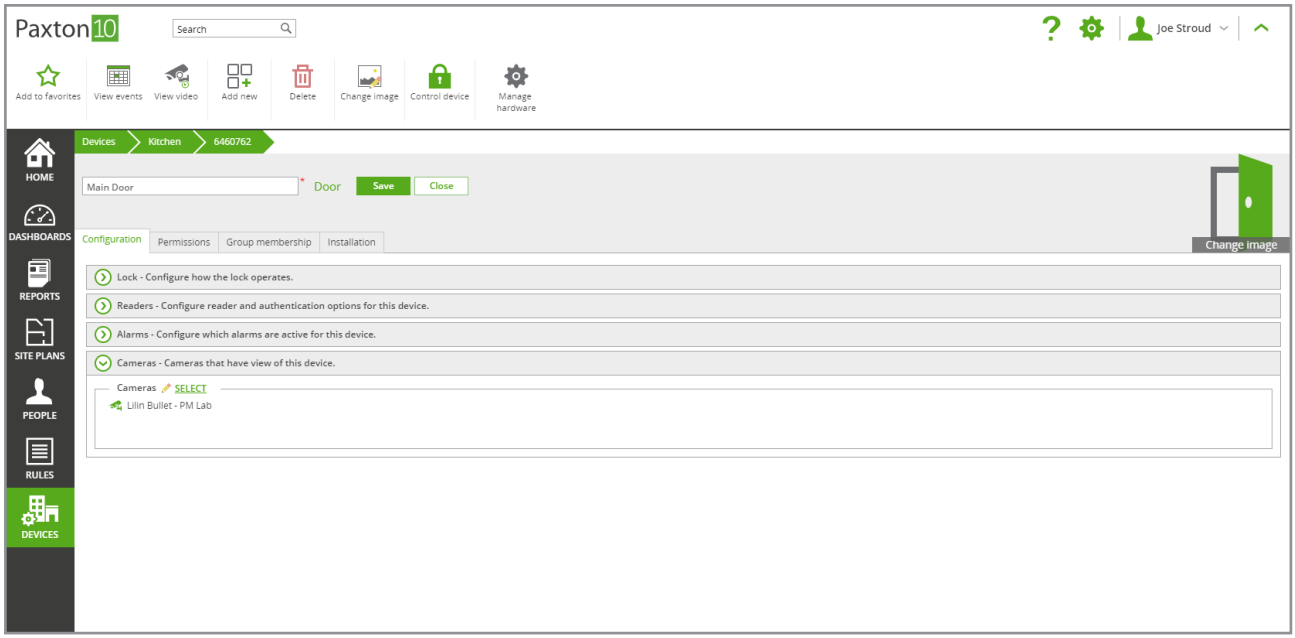
Alarms

Depending on the contacts fitted to the door, an alarm can be sounded to indicate/alert that the door has been forced, left open, or that the power supply has failed. Select all the alarms that should sound at the door.



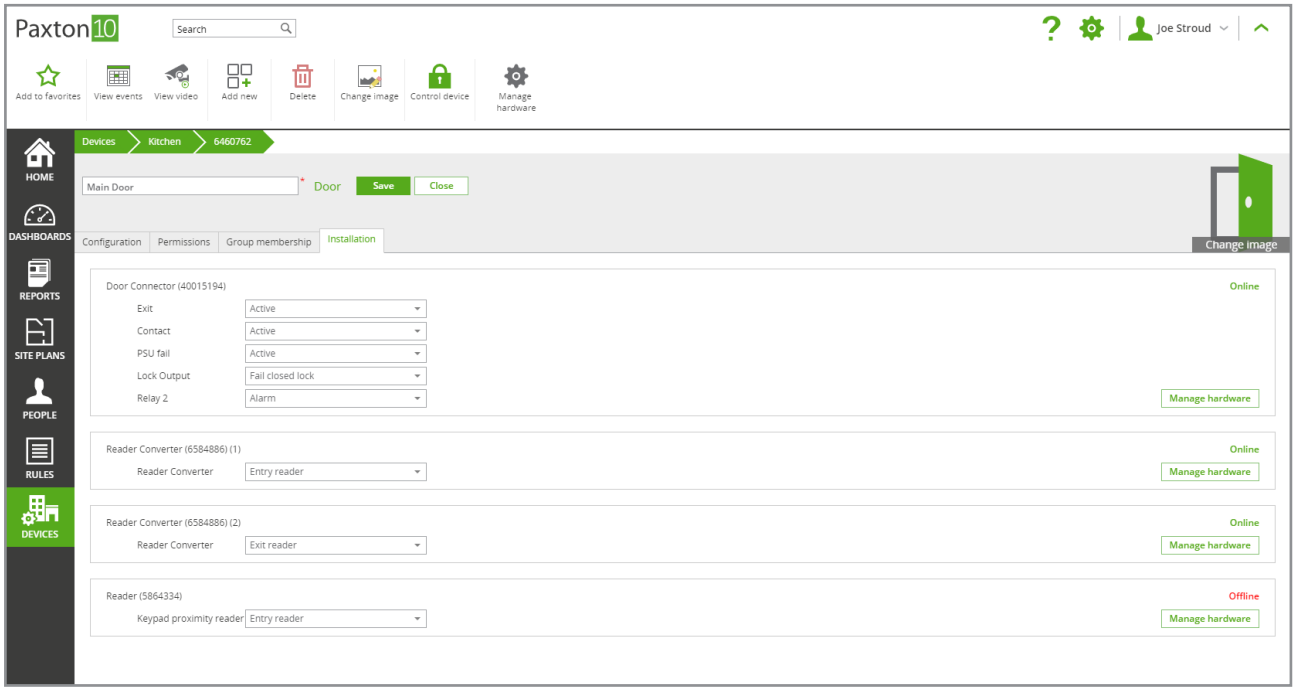
Cameras

These are the cameras that have view over the access point. Associate a camera with this access point to provide events with video and create video reports to monitor its use.



Defining peripheral functionality

When a controller is mapped to an access point, each peripheral is assigned a default role, such as Lock Output, or Entry / Exit reader. It is possible to reconfigure what each peripheral is in the device's '**Installation**' tab.



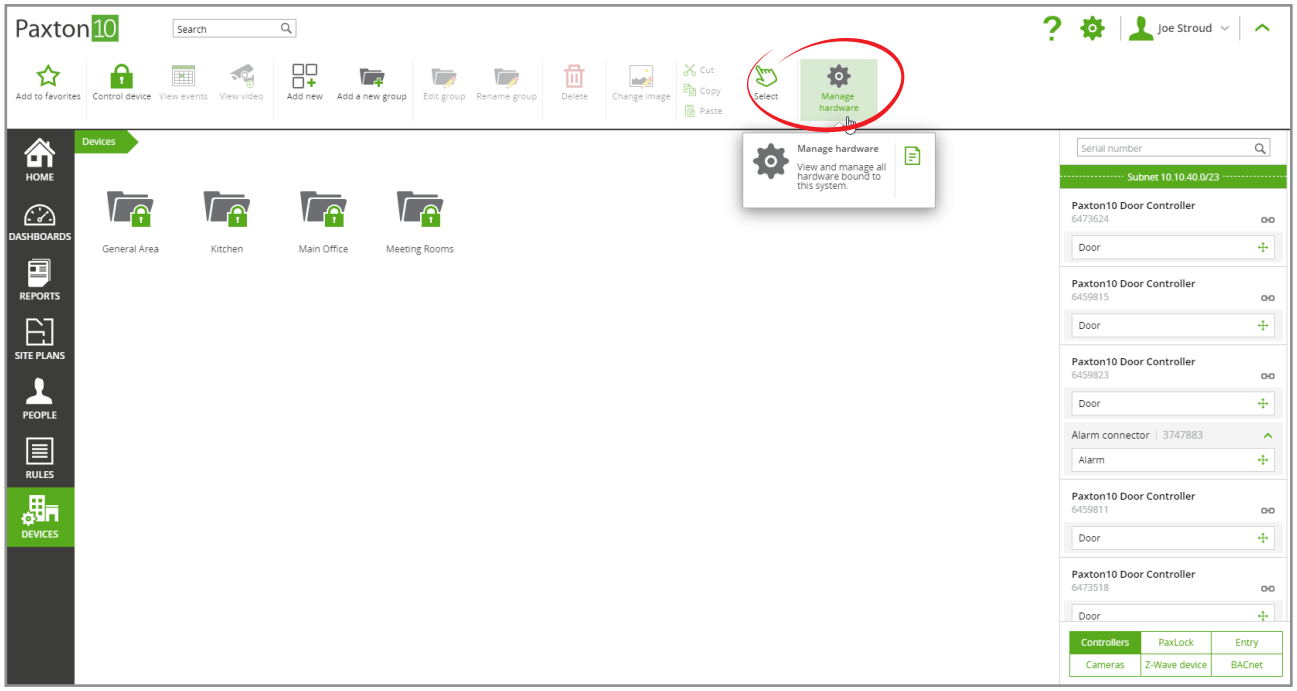
To remove a peripheral from the device (to use it on a different device), see Hardware Management.

Hardware management

Once a controller is bound to a system, the controller and its components will be displayed in the Hardware Management window. It is here that you can see the hardware details, online and offline status, battery charge, and device mapping.

1. Navigate to the '**Devices**' section

2. Click on '**Manage hardware**'



Frequently asked questions

What is the difference between timed and toggle operating mode?

Timed operating mode - the access point will unlock for a number of seconds when an authorized credential is presented, allowing a single person access.

Toggle operating mode - the access point will unlock on presentation of an authorized credential, unlike timed mode, the access point will remain unlocked until an authorized credential is presented a second time.

Can I control a turnstile with Paxton10?

Currently, turnstiles are not supported as a device in Paxton10, however, turnstile control can be achieved using Custom rules.

Why do I need to specify if a reader is entry/exit?

Reader direction is used in events so that you know if a user entered or exited an area. It is also required for anti-passback and roll call.

What is the difference between a PIN and a code?

A personal identification number (PIN) is unique to each user. Each user will have their own PIN, and their PIN will only give access at devices they have building permission for.

A code is set at each device and can be used by multiple users. A code cannot be used to identify a user, and therefore are not constrained by building permissions.

Does using a code operating mode affect anti-passback or roll call?

When using 'Code only' operating mode, the user is not known and therefore user position cannot be determined. For roll call reporting and anti-passback restriction, an operating mode that includes a user credential (Token or PIN) is required.

Why am I getting access denied?

Once setup, a user requires building permissions to the device for their credential to be valid. Within the device, navigate to the 'Permissions' tab, and select the building permissions that the device should be added to.

Alternately, if an intruder alarm is armed, this may also be preventing access.

Why is the reader is showing an amber LED?

An amber LED generally means that the device is in a Token + PIN or Token + code operating mode. When a valid token is presented, the reader will show amber to indicate that it is waiting for the additional PIN or code.