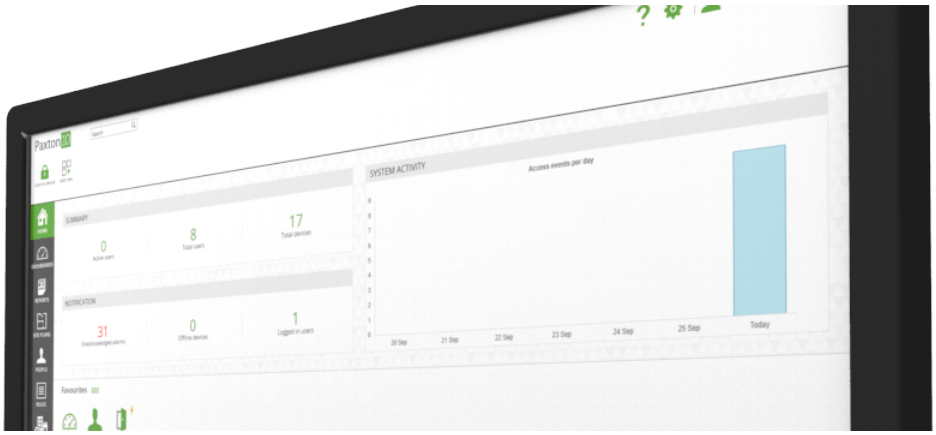


Configuring anti-passback

Overview

The main purpose of an anti-passback system is to prevent a card holder from passing their card back to a second person to gain entry into the same controlled area; for example, a Car Park. It also improves the accuracy of roll call, 'Last known position' reports and deters tailgating.

For anti-passback to be effective, entrance and exit should be monitored and controlled and ideally door contacts should be fitted.

Anti-passback rules in Paxton10 can be found in the '**Rules**' section of the software.

Types of anti-passback

Paxton10 provides two types of anti-passback:

Traditional

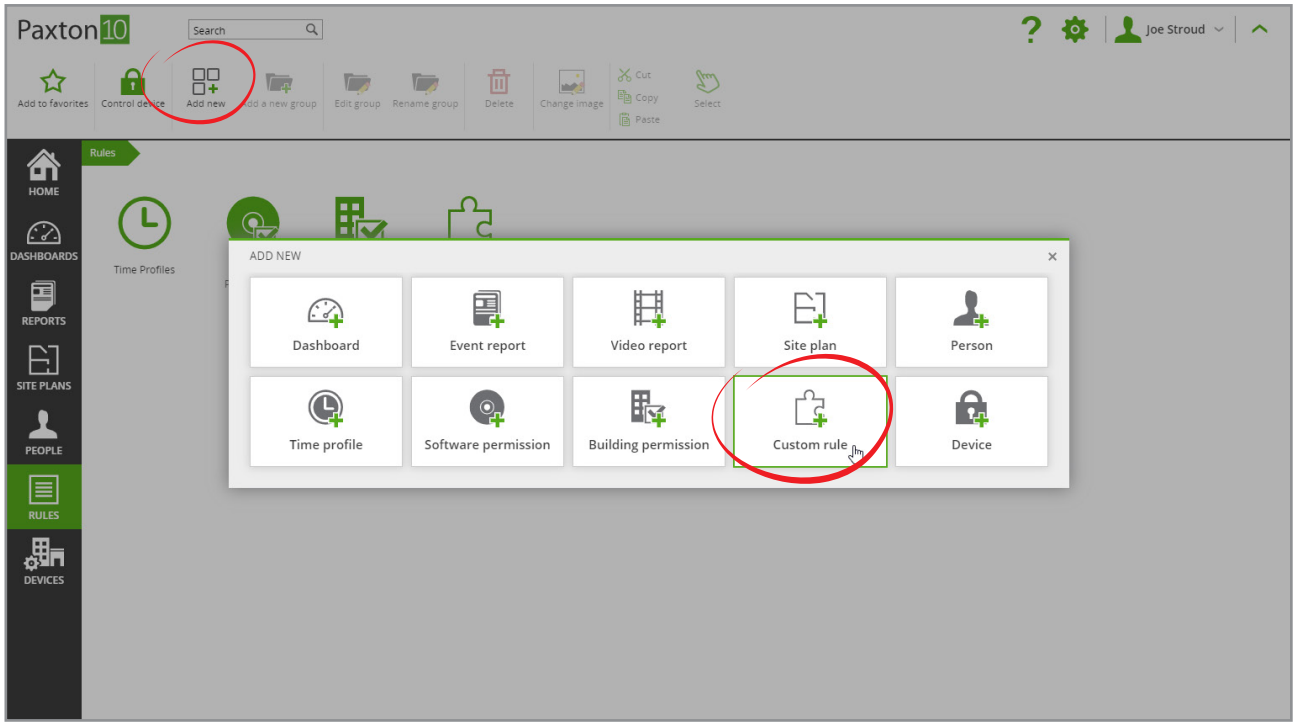
Traditional, also known as Logical anti-passback, is used on sites where strict access control is important. It requires both Entry and Exit readers at each boundary. The system must see a user leave an area before allowing access in the opposite direction.

Timed

Timed anti-passback restricts a user's access for a specified time after their initial entry to the area. This can be used where Exit readers are not installed or enforced.

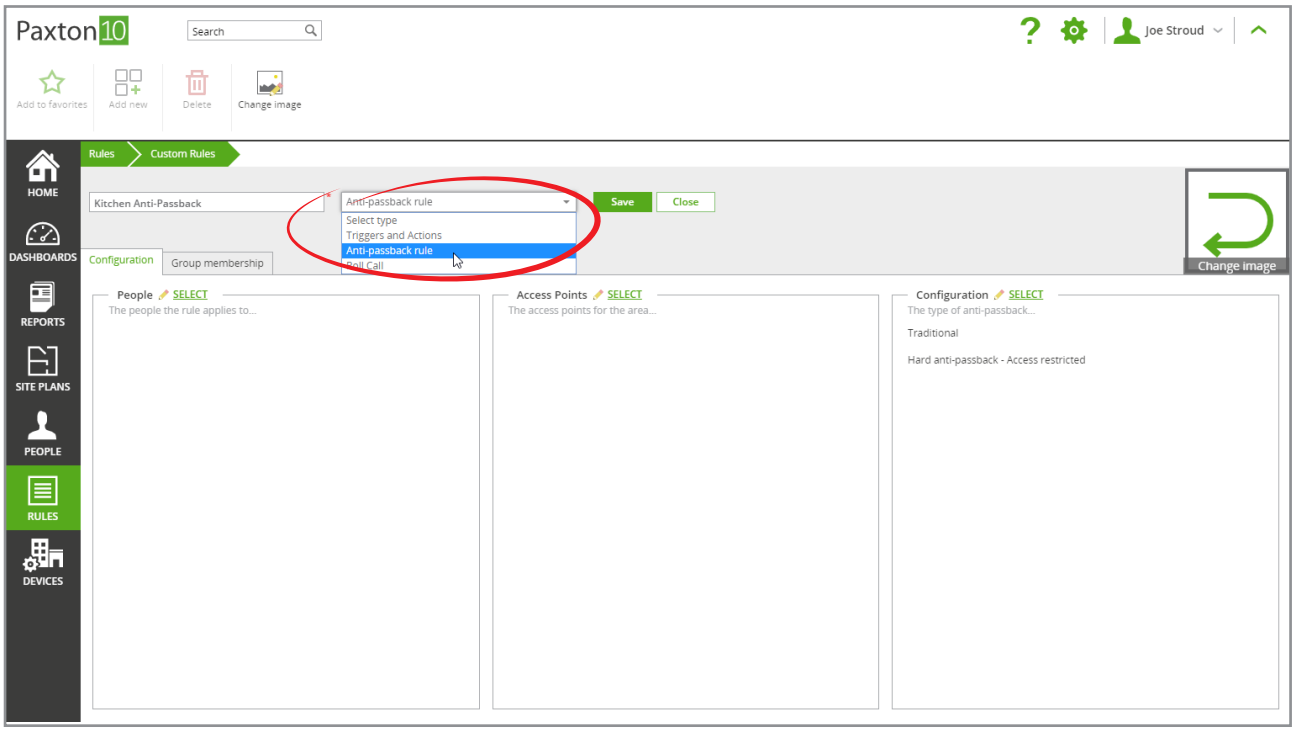
Create an anti-passback rule

1. From the ribbon, select '**Add new**'
2. Select '**Custom rule**'



3. Give the rule a name

4. Select '**Anti-Passback**' as the rule type



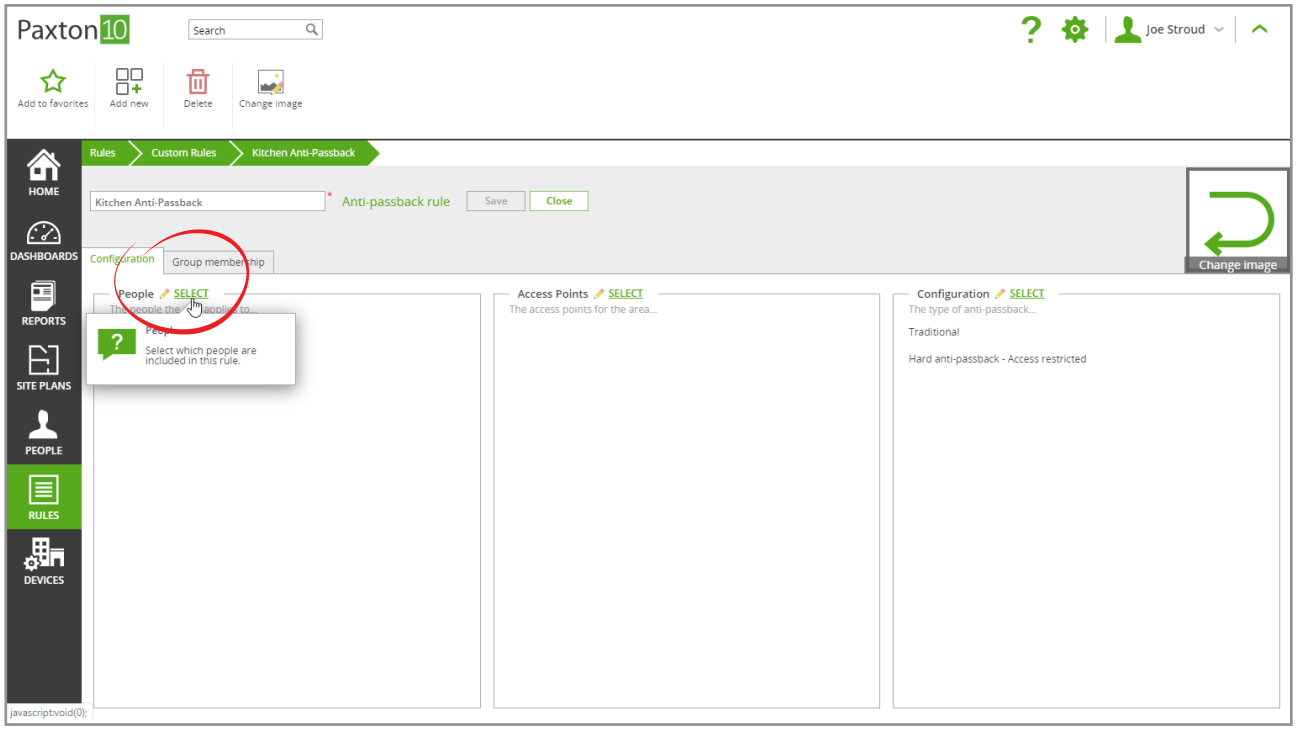
5. Click '**Save**'

Add people to the rule

The anti-passback rule can be applied to everyone, or a selection of users.

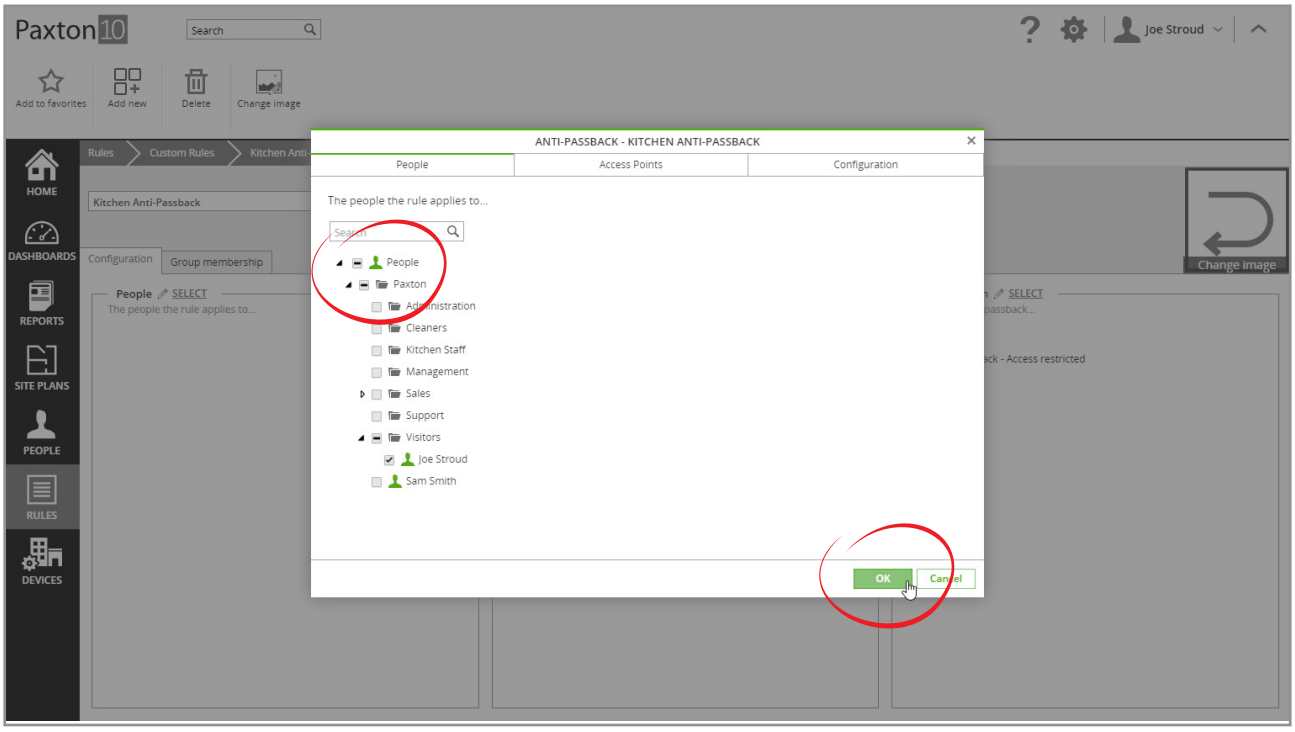
While viewing an anti-passback rule:

1. Click '**Select**' next to the '**People**' box



2. Check the box next to '**People**' if everyone is required to abide by the rule, or select individuals and groups if not everyone is required to abide

3. Click '**OK**'

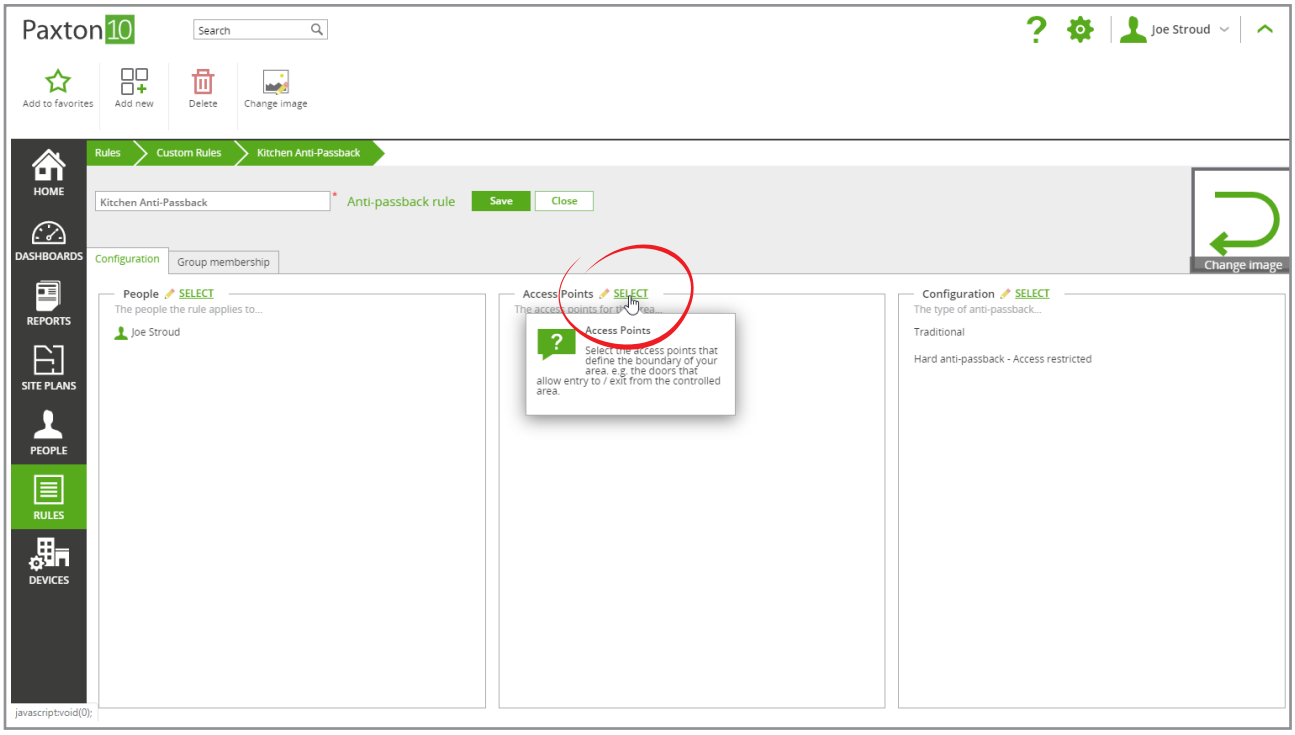


Define the anti-passback area

For the anti-passback rule to be effective, the access points that define the area must be selected.

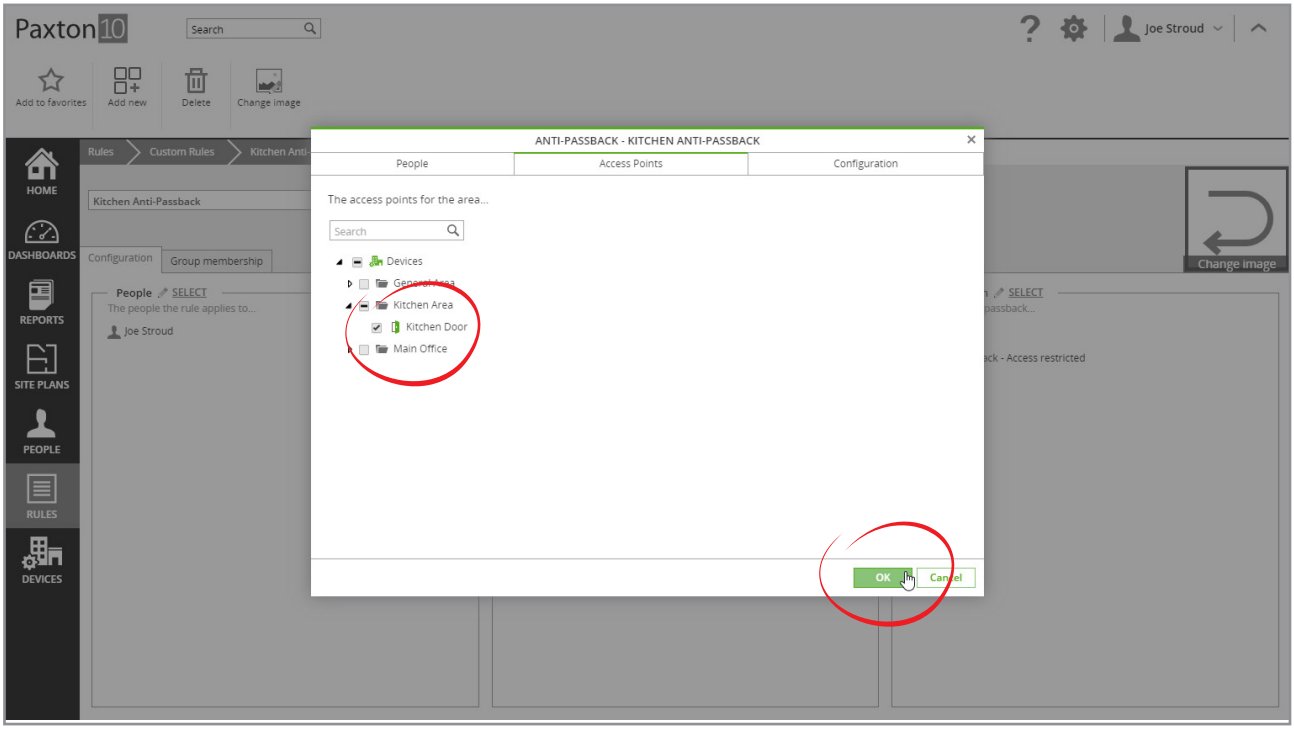
While viewing an anti-passback rule:

1. Click '**Select**' next to the '**Access Points**' box



2. Check the box next to the access points that allow entry to, or exit from, the area that you wish to enforce

3. Click '**OK**'

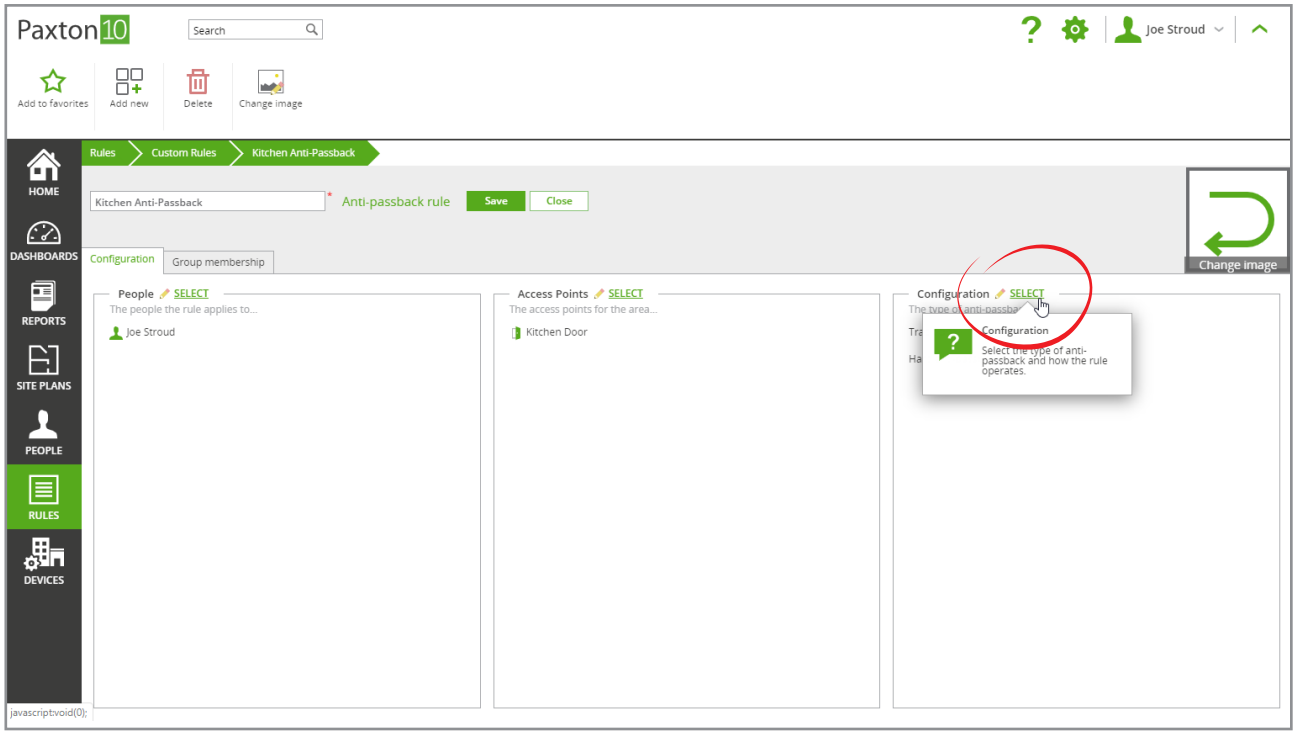


Configure the rule

How the rule is enforced will depend on the type of anti-passback and restriction level.

While viewing an anti-passback rule:

1. Click '**Select**' next to the '**Configuration**' box.



2. Select the type of anti-passback: Traditional or Timed (See description on page 1)

For Traditional:

Select '**Forgiveness**' to reset everyone's in/out status at a chosen time every day, allowing people who do not exit properly to still gain access the next day.

For Timed:

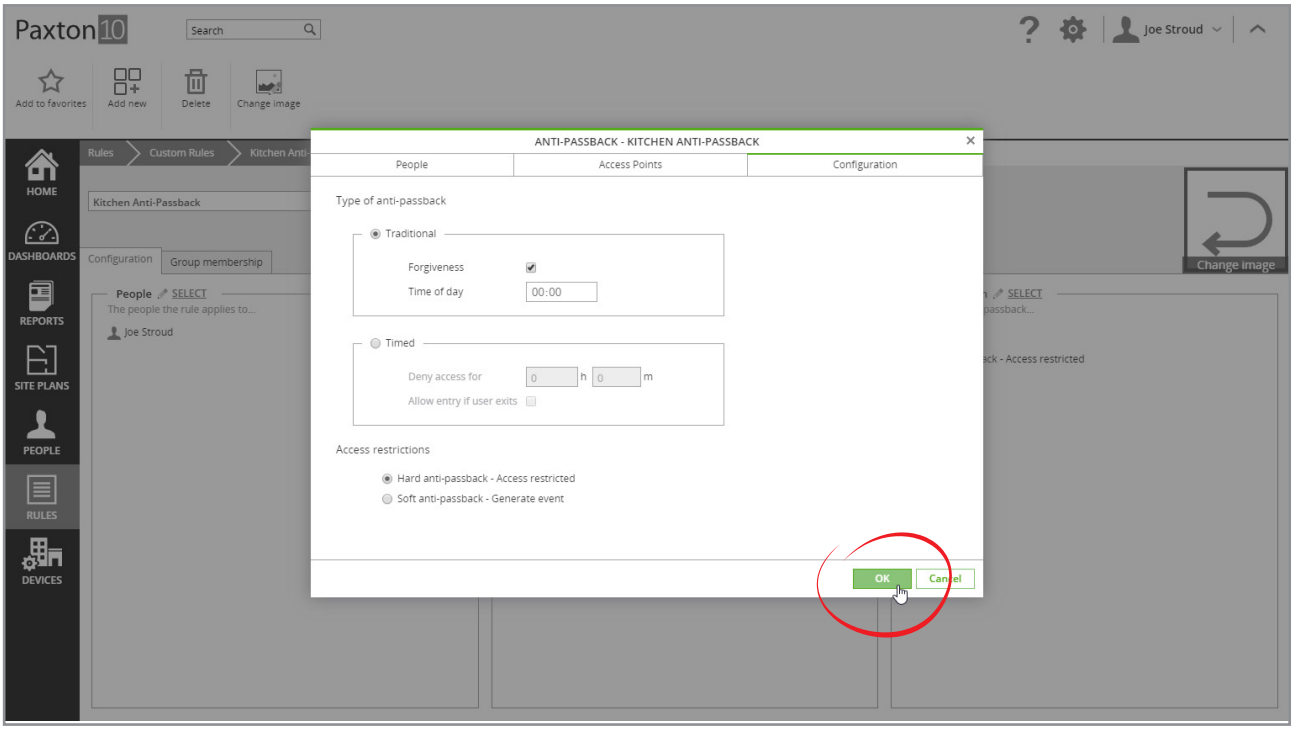
Entry how long each user should be denied access for after their initial access, and select '**Allow entry if user exits**' to allow users to re-enter before the specified time if they had exited using an Exit reader.

3. Select the access restriction required:

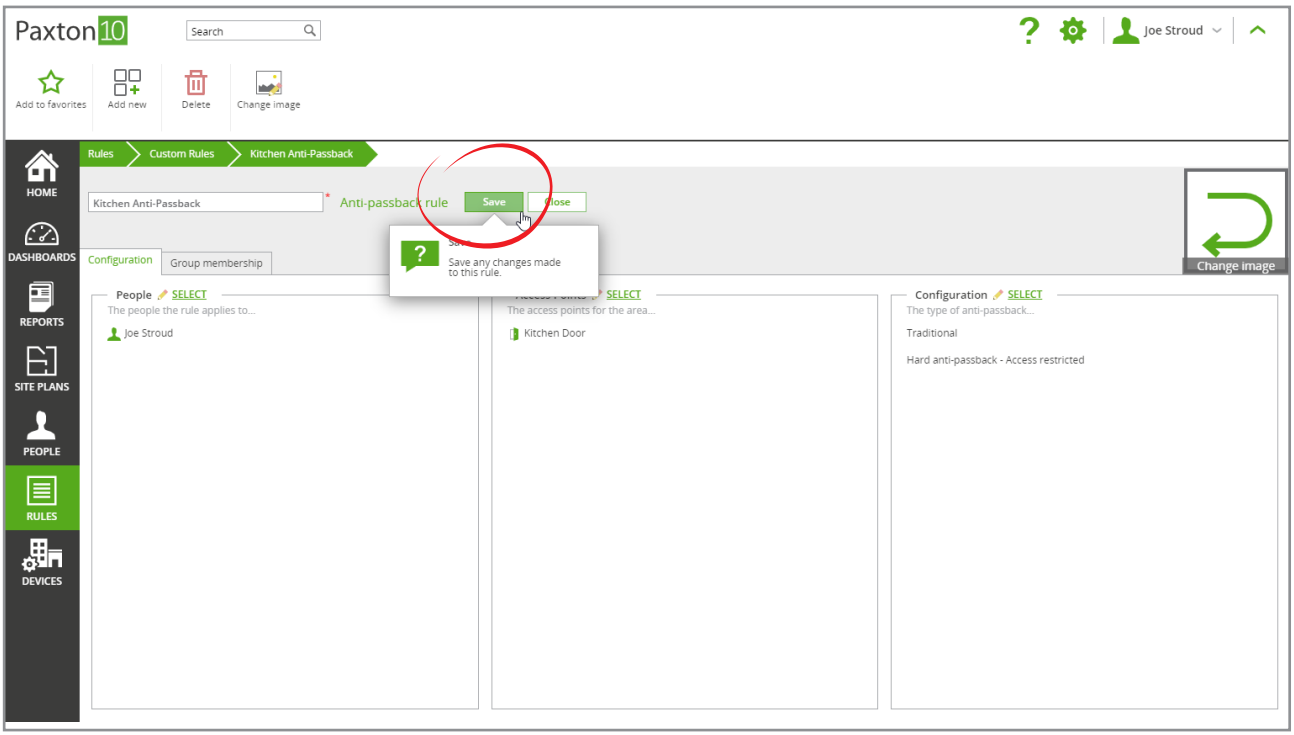
Hard anti-passback will restrict a user's access upon breaking the rule, not allowing them into the area while generating an '**access denied**' event.

Soft anti-passback will allow a user access when breaking a rule but will record the behaviour as an information event.

4. Click '**OK**'



5. Click '**Save**' to apply this rule to your system



Example – Car park

Use case

To prevent employees from passing their token back to friends and family to use the office car park.

Pre-condition

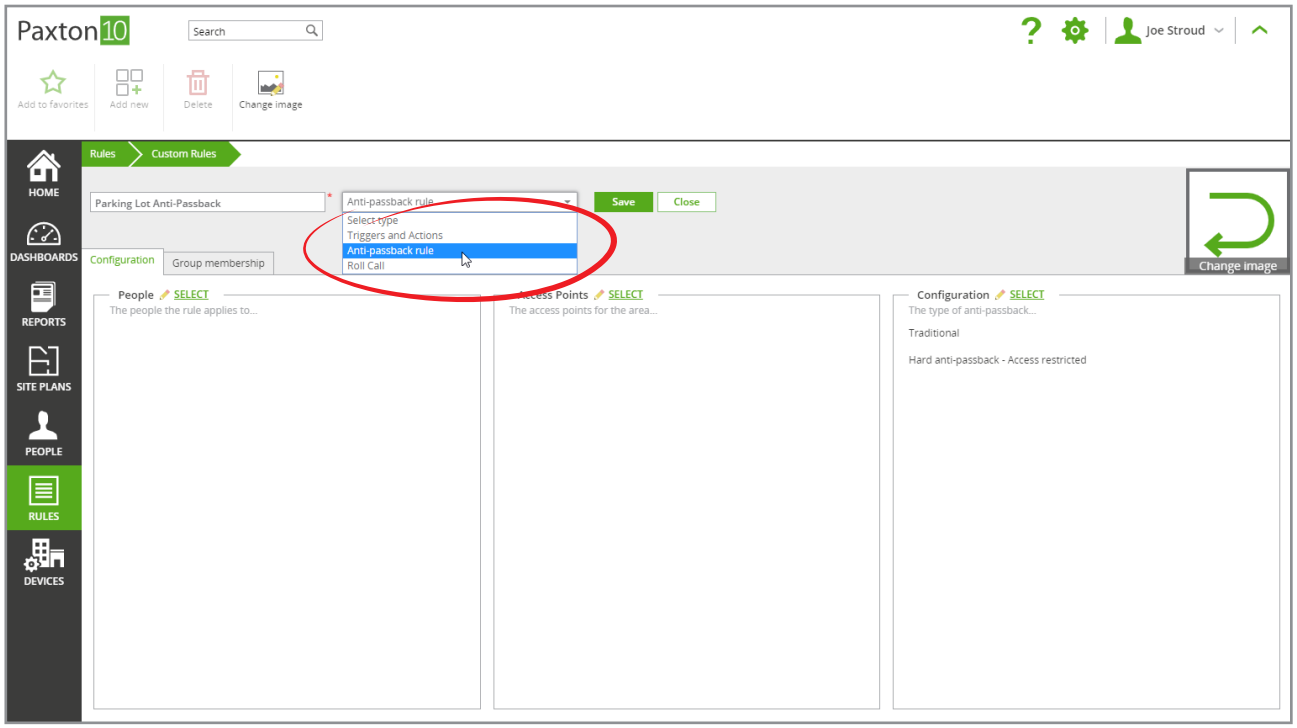
The car park entrance is accessed through an access controlled barrier, with free exit barriers on the exits.

Step 1 – Create a new rule

1. Click '**Add new**' from the menu, ten select '**Custom rule**'

2. Enter a name – Car Park anti-passback in this case

3. Select '**Anti-passback rule**' from the dropdown

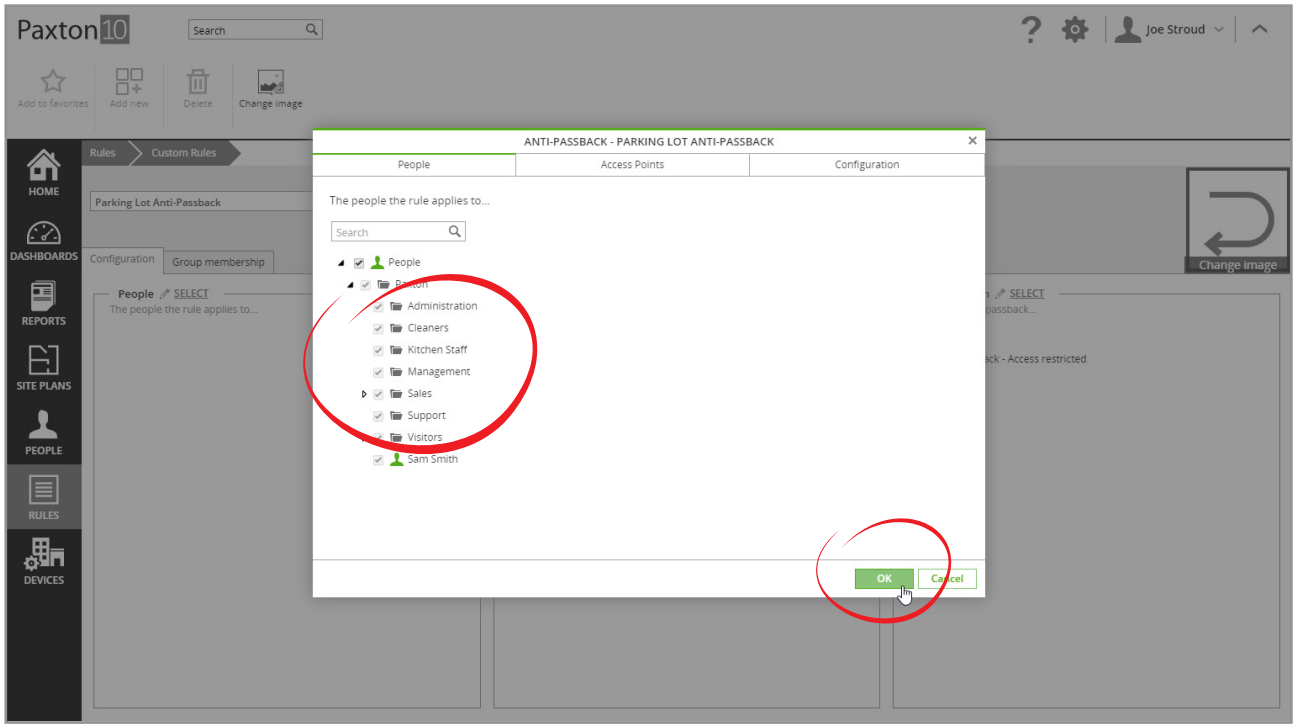


Step 2 – Select People

1. Click '**Select**' by the '**People**' box

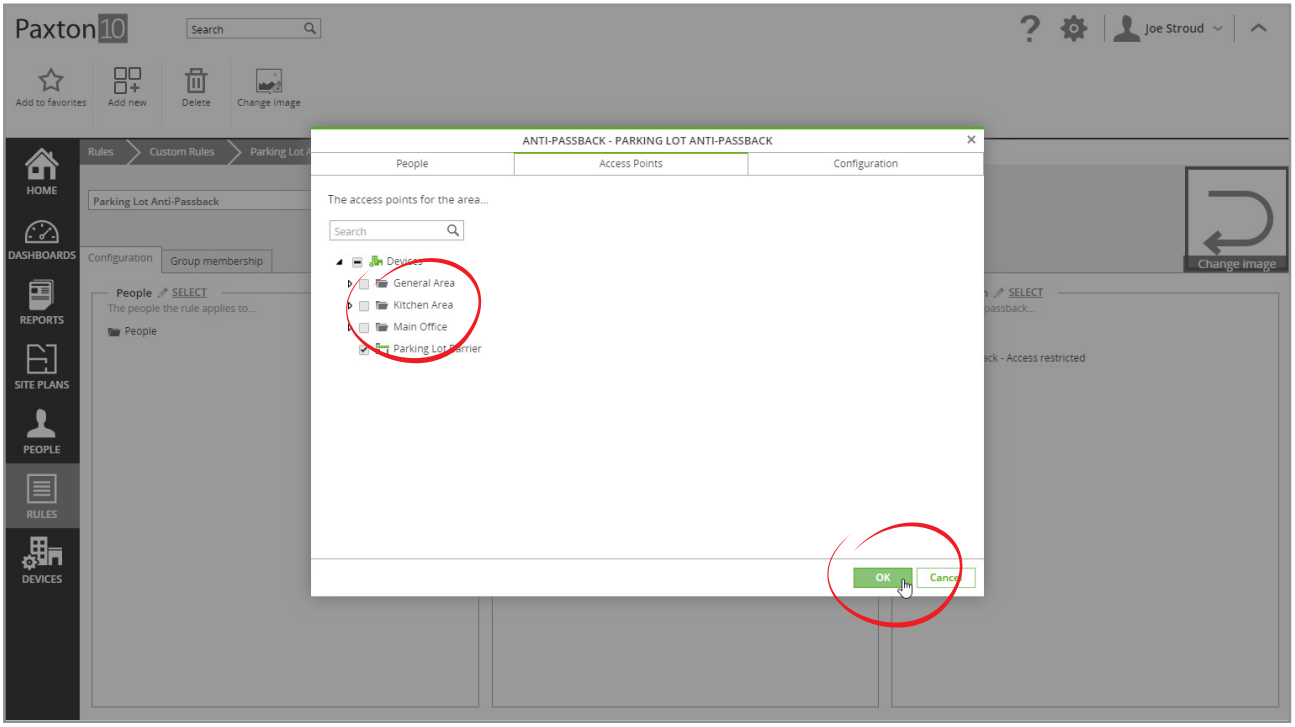
2. Select the '**Employees**' People group

3. Click '**OK**'



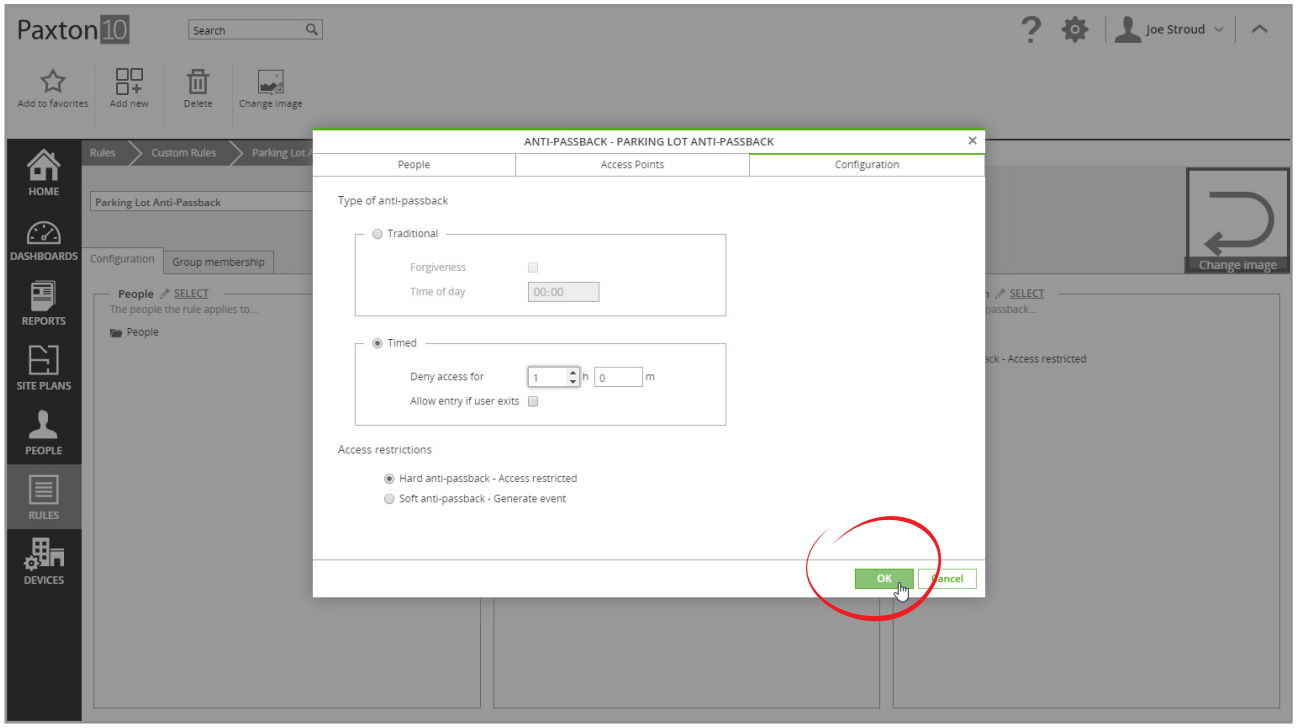
Step 3 – Define the area

1. Click '**Select**' by the '**Access Points**' box
2. Select '**Car Park Barrier**'
3. Click '**OK**'



Step 4 – Configure the anti-passback

1. Click '**Select**' by the Configuration box
2. Select '**Timed**' anti-passback
3. Enter 1 hour (01h 00m) to deny access for
4. Ensure '**Allow entry if user exits**' is unchecked (since exit readers are not installed this option is not relevant)
5. Select '**Hard anti-passback**'
6. Click '**OK**'



Click '**Save**'

The rule is now complete – Employees will be unable to use their token to access the car park for 1 hour after their initial access, preventing them from allowing access to the people behind them.

Example – busy office

Use case

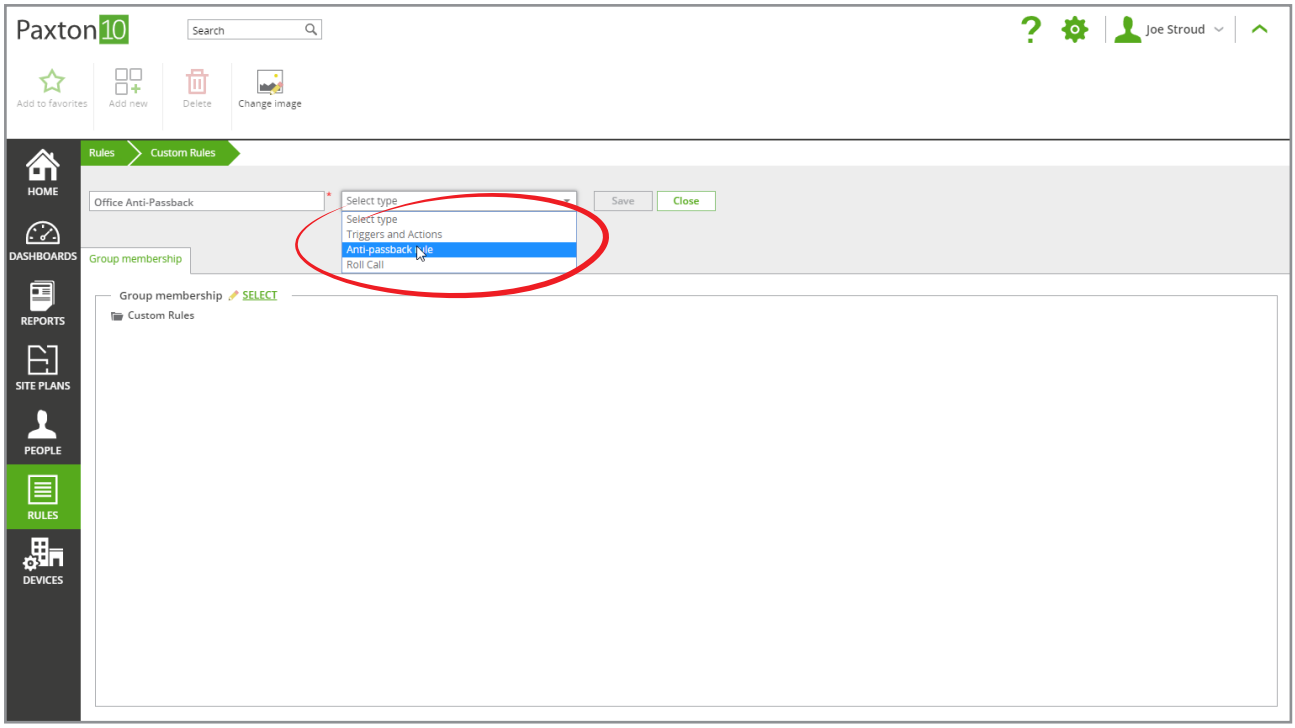
An office wants to monitor which employees are on premises at any given time. Since the office is accessed via a single turnstile, congestion can be a problem and it is not ideal to restrict a user access, instead any violations should be recorded and followed up at a later stage. Since the office closes each night it can be assumed the building will be empty, allowing employee status to be reset at the end of each day.

Pre-condition

The office contains a single turnstile at the entrance with Entry and Exit readers, and a back door allowing Exit only, containing Exit readers.

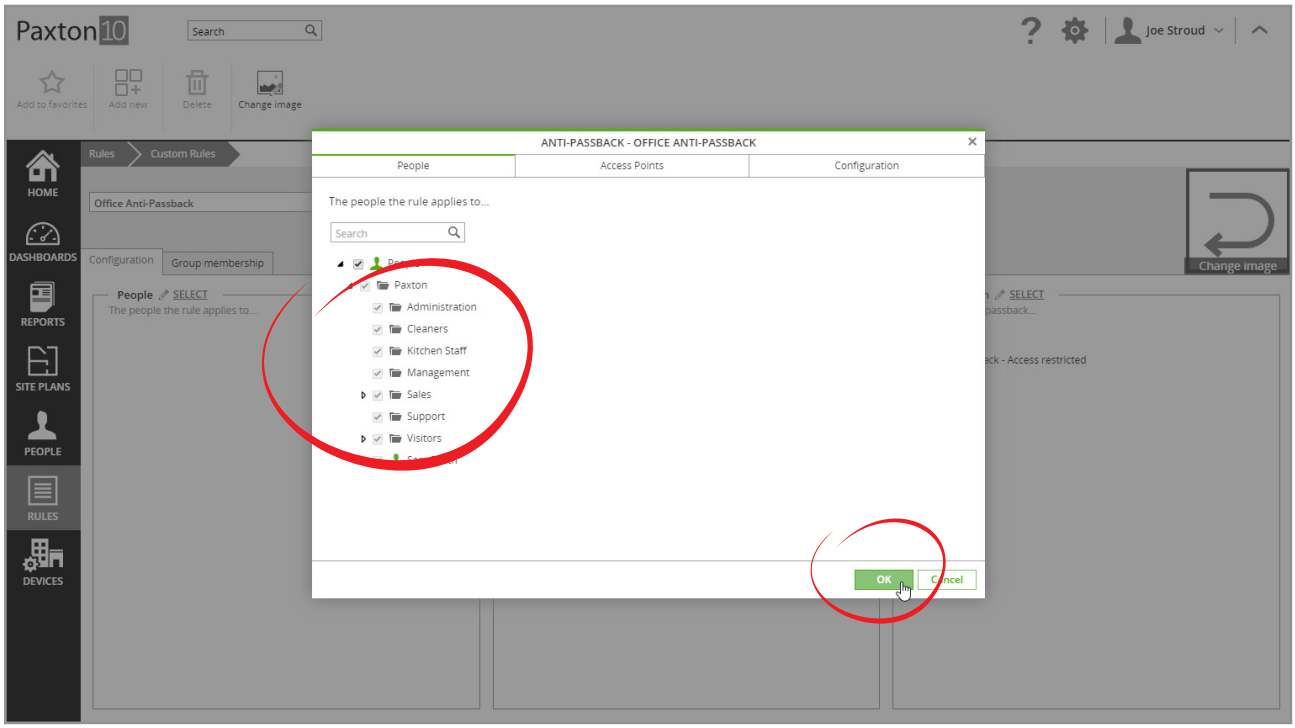
Step 1 – Create a new rule

1. Click '**Add new**' from the menu, ten select '**Custom rule**'
2. Enter a name – Office anti-passback in this case
3. Select '**Anti-passback rule**' from the dropdown



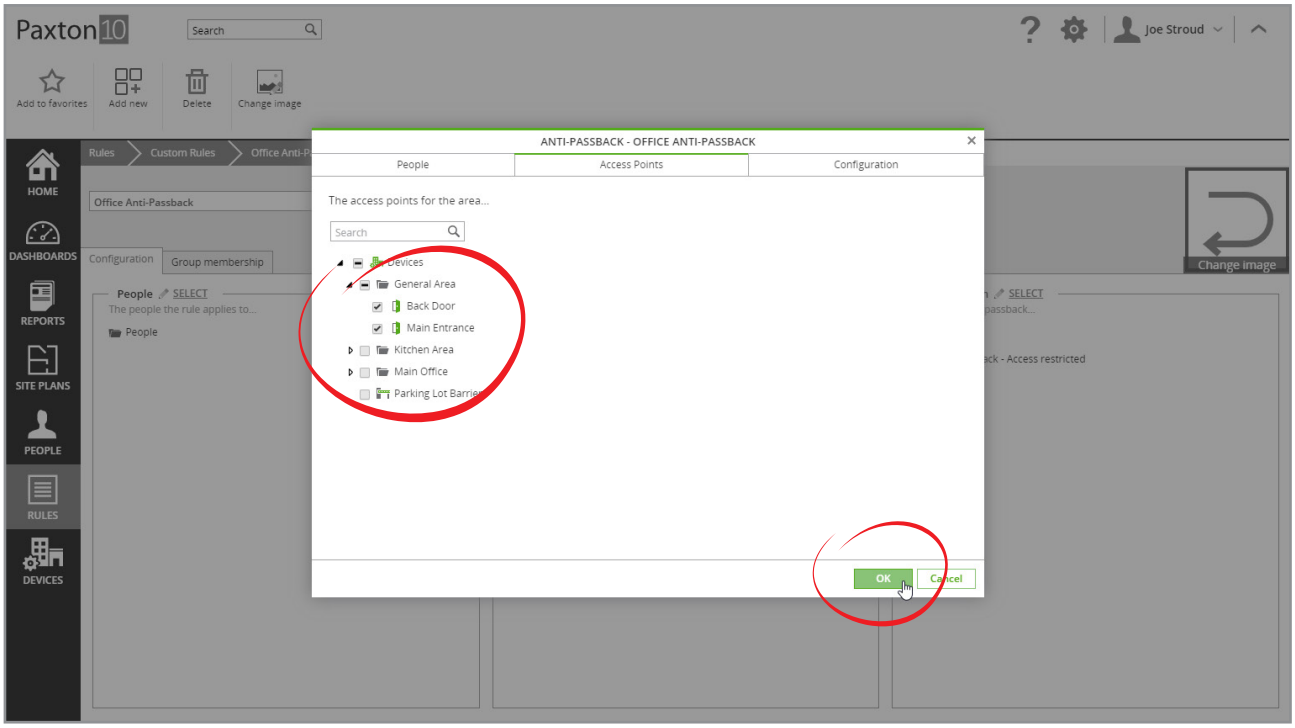
Step 2- Select People

1. Click '**Select**' by the People box
2. Select '**People**' (Everyone must abide by this rule)
3. Click '**OK**'



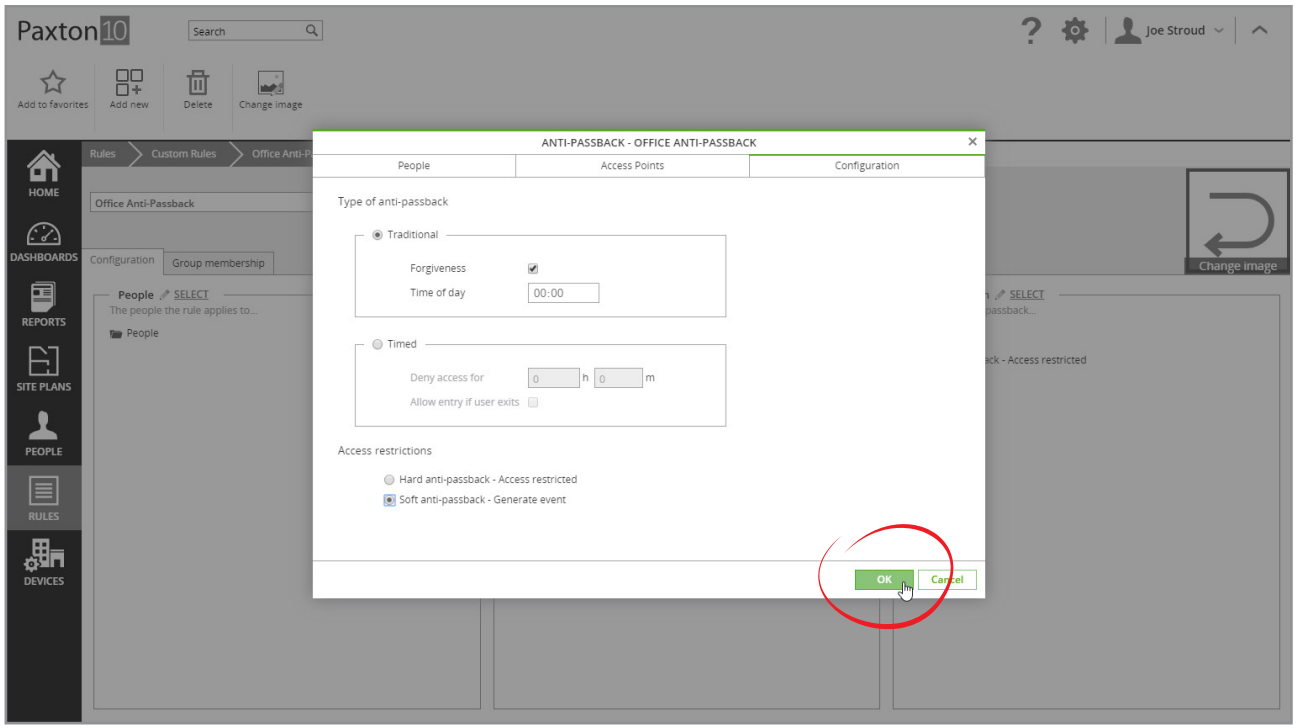
Step 3 – Define the area

1. Click '**Select**' by the '**Access Points**' box
2. Select '**Main entrance**' and '**Back door**'
3. Click '**OK**'



Step 4 – Configure the anti-passback

1. Click '**Select**' by the Configuration box
2. Select '**Traditional**' anti-passback
3. Select '**Forgiveness**'
4. Enter 00:00 for forgiveness to occur
5. Select '**Soft anti-passback**'
6. Click '**OK**'



Click '**Save**'

The rule is now complete – An information event will be raised if anyone passes their token back to allow an unauthorised person into the office or attempt to re-enter if they didn't exit as required. If a person forgets to exit using an exit reader at the end of the day, they are forgiven (reset at midnight) and allowed access the next day without infringement.

Frequently asked questions

Do I need door contacts fitted to use anti-passback?

Although door contacts are not strictly required, they will enhance the accuracy of anti-passback.

What happens when someone breaks the anti-passback rule?

When configured as '**Hard**' restriction, breaking the rule will result in the user not being granted access, and a relevant 'access denied' event will be raised to inform the system administrator.

When configured as '**Soft**' restriction, the user will be granted access according to their permissions, but an 'access granted – anti-passback rule breached' event will be generated to inform the system administrator.

How to I make a reader an Entry or Exit reader?

When assigning a reader to an access point, on the '**Installation**' tab within the device there is the option to select either '**Entry reader**' or '**Exit reader**' for each. Select Entry reader for the readers located on the outside of your controller area, which would allow entry into the area, and select Exit reader for the readers installed within the area, allowing exit from the area.

How do I define an area?

In Paxton10, it is not required to define the areas prior to making the rule. Within the rule, select the access points that allow access to the area. Whether these access points allow entry or exit to the area is configured in the device as a reader setting (Entry or Exit reader).

What if a user doesn't have permissions to a door in the anti-passback rule?

Software permissions are not affected by anti-passback. If a user does not have permission to go through an access point, including them in an anti-passback rule will not provide them with access.

Can a user always exit an anti-passback area?

Only Entry to an area applies the anti-passback restrictions; providing the user has the relevant permission, exit is always allowed.

Can I set up an anti-passback area within an existing anti-passback area? (Nested anti-passback)
Yes, however the order that areas are accessed cannot be restricted. Providing both areas use their own access points, an area can exist within an area, but it is not possible to enforce the order that the areas must be accessed in.

Can a single access point be used in multiple rules?

It is possible for areas to have a common access point if the direction remains consistent. (The access point must either allow entry into both areas, or exit from both areas).

E.g. '**Fire exit 1**' can be used in Office 1 and Office 2 as an Exit, however 'Office divider door' which joins Office 1 and Office 2 cannot be used, since this would require a single reader to be '**Entry**' for one area while being '**Exit**' for another.

Can I stop a user from accessing internal devices until they've entered the area? (Regional anti-passback)

No. Anti-passback in Paxton10 only restricts access to the access points defined in the rule. The functionality of other devices on the system is not affected.

© Paxton Ltd 1.0.0