Configuring anti-passback

Anti-passback principles

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. If a user follows a colleague OUT of an area without presenting their own card, their error is discovered when they try to return to the area. As this user is still shown as being IN the area, the use of their card for the IN direction is barred.

To use anti-passback, areas must be set up first. For further details on how to set up areas and area groups refer to:- AN1023 - Configuring areas and area groups < http://paxton.info/978 >

Door contacts should be fitted to doors included in the anti-passback system to confirm that the door has actually been opened. If not, the users 'last known position' will not be changed.

Logical Anti-passback

Logical anti-passback is used on sites where strict access control is important. It requires both IN and OUT readers at each area boundary. The system must see a user card leave an area before allowing access in the opposite direction.

This is particularly suited to deter users from tailgating each other. If they do not read out of an area, they will not be allowed back in, no matter which door they try. Similarly, if a user tailgates another onto a site, the system can prevent that user from accessing other areas of the site, until they have fobbed into the site correctly.

An Administrator must Reset the users anti-passback permissions to allow access into the area.

Timed-Logical Anti-passback

This system is suited for a general office environment. As long as a user obeys the logical anti-passback rules, they may re-gain access to an area immediately. If, however, the user tailgates another user out of the area they will be allowed to re-enter after the specified time period from their previous valid access. This waiting period should inconvenience the user but will avoid them being trapped in an area.

This removes the need to reset the user's permissions but the Access Denied event is still recorded.

Timed Anti-passback

Timed anti-passback prevents a user card from entering the same area twice during a set time duration. This is useful where there is an exit button or free access turnstile and no OUT reader.

A swimming pool may only have access control into the area but no control on the exit. Setting up timed anti-passback with a duration of 15 minutes, would prevent a user being able to enter the area and hand their card immediately to a friend or colleague to also gain entry.

Configuring Anti-passback
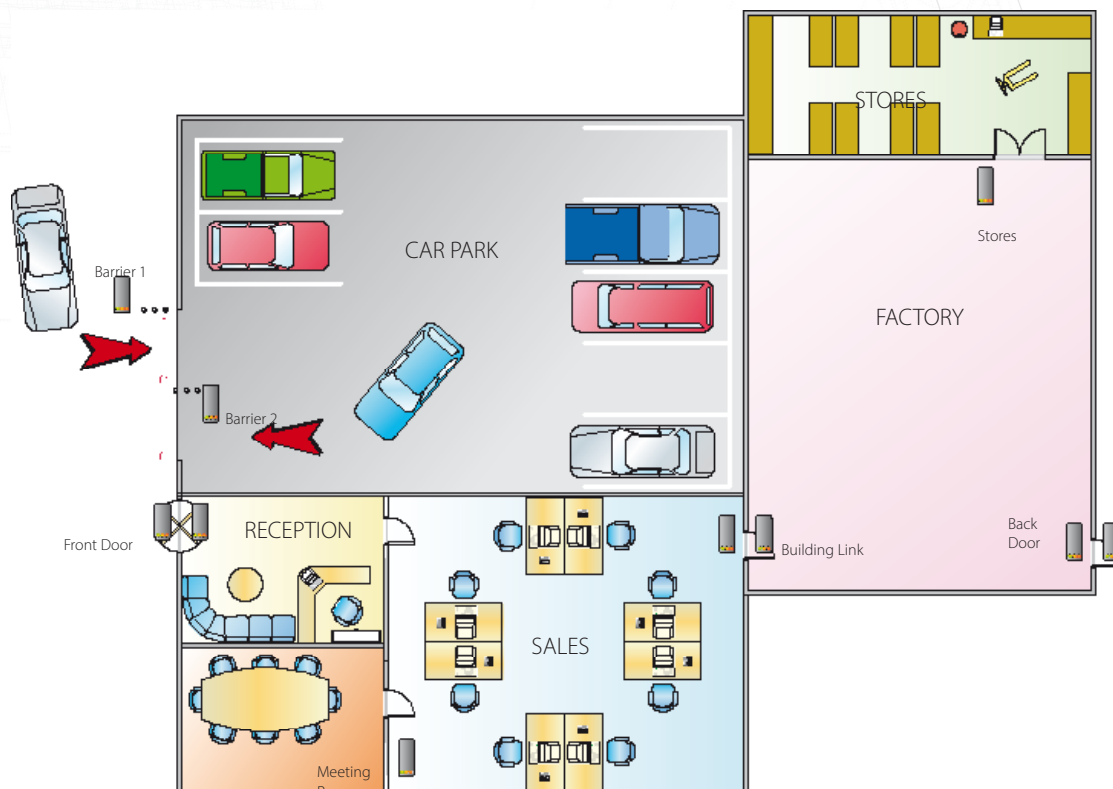
Anti-passback requires areas and area groups to track user cards around the site. In the above diagram, we see that several areas have more than one entry/exit door. (e.g. Factory) Anti-passback must be aware of this to ensure that it controls all the doors surrounding each area.

See also:- AN1023 - Configuring areas and area groups < http://paxton.info/978 >

We will look at some examples of anti-passback.

Car Park - We can set up anti-passback to ensure that once a card has been used at the IN barrier, it must then be read at the OUT barrier before being valid for entry again. This will deter users from handing their card to a friend after they have gained access to the car park.

In the above screenshot, we have a Car Park area with the two barrier ACU's controlling access to and from the Outside World. Ensure that the To and From direction for Reader 1 (In) is correct.
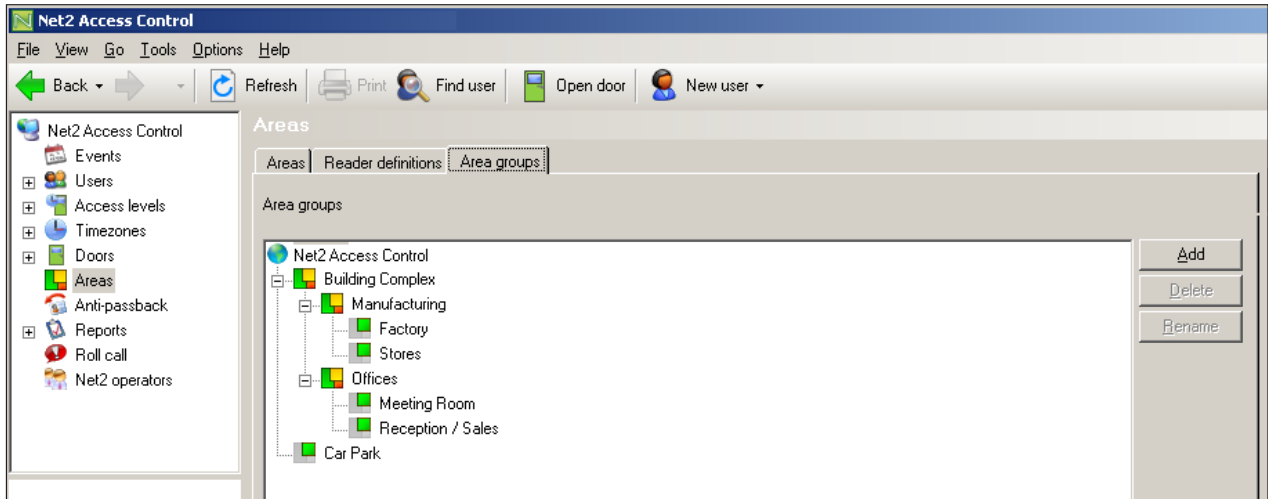
The area groups have been configured with the Car Park as a standalone area.

Click on the anti-passback icon. Select Car Park from the areas list and we can see the two readers that control this zone.

Selecting Logical anti-passback will ensure that this restriction is applied.
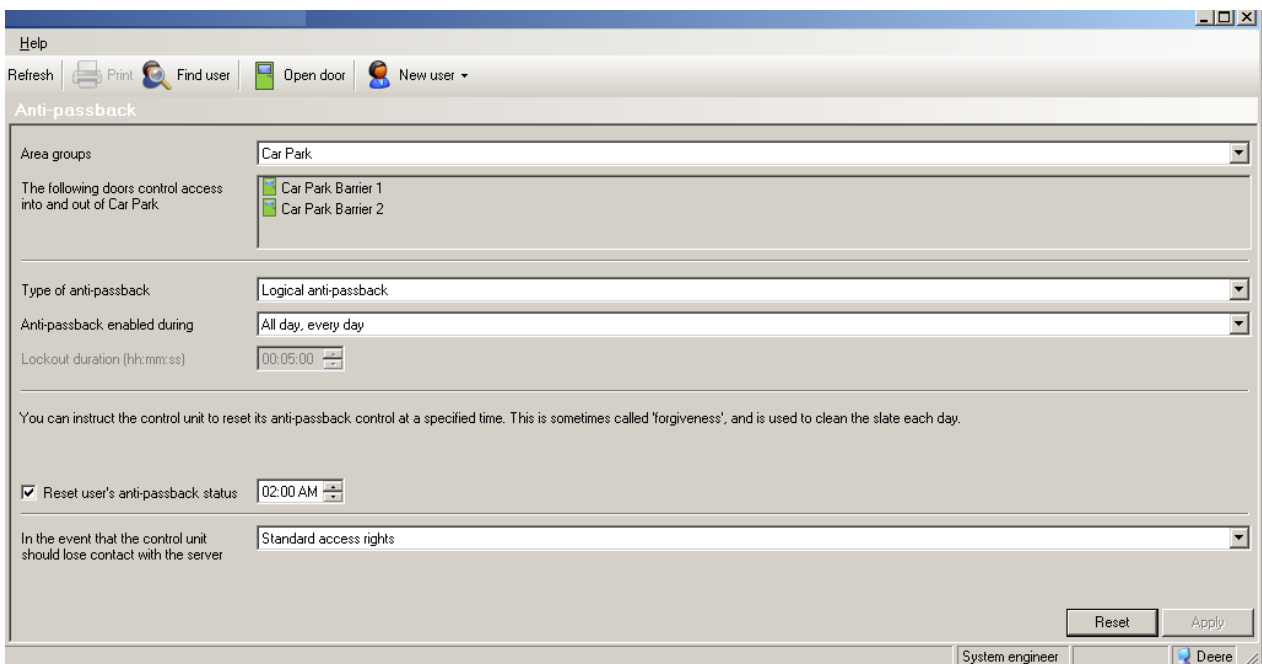
Anti-passback can be controlled by a time zone. This allows the system to be turned off when tight control is not required or desirable (e.g. out of hours).

The system can be configured to reset the anti-passback status at a specified time. This means that every user can start the next day with a clean slate.

There is also a manual Reset button that gives all the users a fresh start.

For anti-passback to work, the Net2 server must constantly update all ACU's. In the event of the server losing contact with the control units you can choose to either have the ACU's deny users access or allow them standard access rights.

Event data

Every anti-passback event will have the type of anti-passback used (Logical, Timed or Timed+Logical) included in the event record. If this information is missing, that door or user has not been included in the anti-passback system.

The first example (events are displayed from the bottom up) shows a user attempting to pass through a door twice in the same direction, possibly having tailgated a previous user, that has Logical control.

✖	18/01/2008 09:33:37 IT Visitor	Door 9 (Out)	Access denied - invalid token	Anti-passback (Logical)
➡	18/01/2008 09:30:00 IT Visitor	Door 9 (Out)	Access permitted - token only	Anti-passback (Logical)
➡	18/01/2008 09:29:54 IT Visitor	Door 9 (In)	Access permitted - token only	Anti-passback (Logical)

The second example shows a user card being denied access through a timed door with a 5 minute timeout. The repeated use of the card within the 5 minute period has been denied.

|				
➡	10/01/2008 07:52:28 IT Visitor	Door 15 (In)	Access permitted - token only	Anti-passback (Timed)
✖	10/01/2008 07:44:13 IT Visitor	Door 15 (In)	Access denied - invalid token	Anti-passback (Timed)
✖	10/01/2008 07:44:07 IT Visitor	Door 15 (In)	Access denied - invalid token	Anti-passback (Timed)
➡	10/01/2008 07:44:01 IT Visitor	Door 15 (In)	Access permitted - token only	Anti-passback (Timed)
➡	10/01/2008 07:35:46 IT Visitor	Door 15 (In)	Access permitted - token only	Anti-passback (Timed)

Global anti-passback restrictions
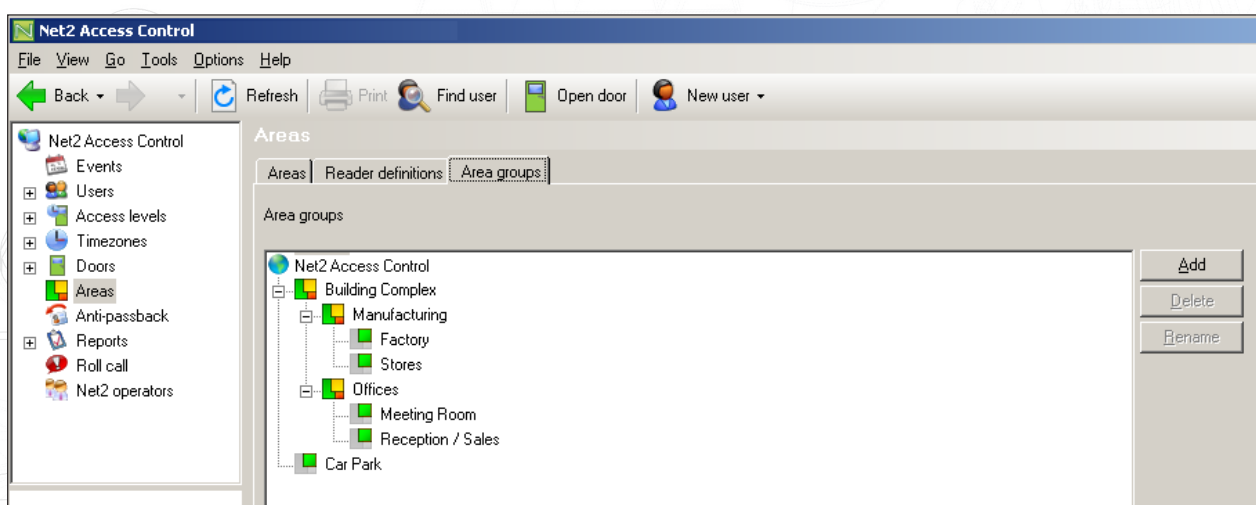
The same door must NOT be used to control two individual anti-passback boundaries.

The system will display all the possible door combinations that relate to the area or area group. This does not mean that it is valid to use them all at the same time.

In our example, we have set up anti-passback on the Building Complex. We cannot activate any of the other possible anti-passback zones that will use the same door as a boundary. One access event cannot update multiple anti-passback calculations.

 - i.e. You cannot use anti-passback on both the Manufacturing and Building Complex (Manufacturing + Offices) areas as the Back Door is required in both definitions. Leaving the Manufacturing area does not always mean that you are leaving the Building and so the Back Door operation would be unreliable.

The Car Park and Building Complex can each use anti-passback as no door is used in both definitions.
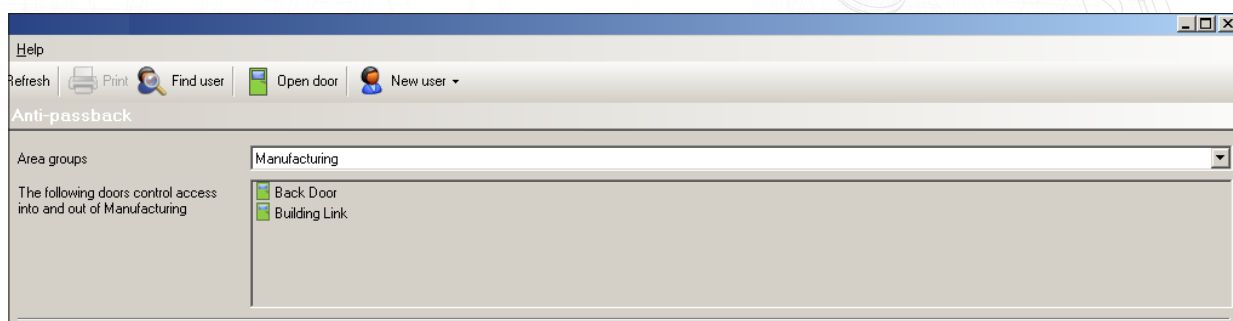
You may NOT create a group that contains individual Timed and Logical anti-passback areas.
You may NOT set up a Logical area with only a single reader and an EXIT button. (e.g. Stores)

In both cases, the user can return to an area without being tracked and will eventually produce a conflict within the anti-passback rules.

Try to determine the users exact requirements and only set up those zones that are necessary. Combining internal areas to produce sequential locking may be configurable (A to B then B to C) but may conflict with other anti-passback rules.

WARNING - These conflicts are difficult to predict and should not be offered as a reliable solution.

User permissions

By default, users must obey anti-passback rules. The Administrator has access to an anti-passback tab on the user record that allows the user to be deselected from the system. (e.g. Security Staff).

This allows them to tailgate an unauthorised intruder and not then become barred from other areas.

The users record also contains a Reset button. This clears their status should they become denied access by the anti-passback system. Their next valid access sets their location in the system.
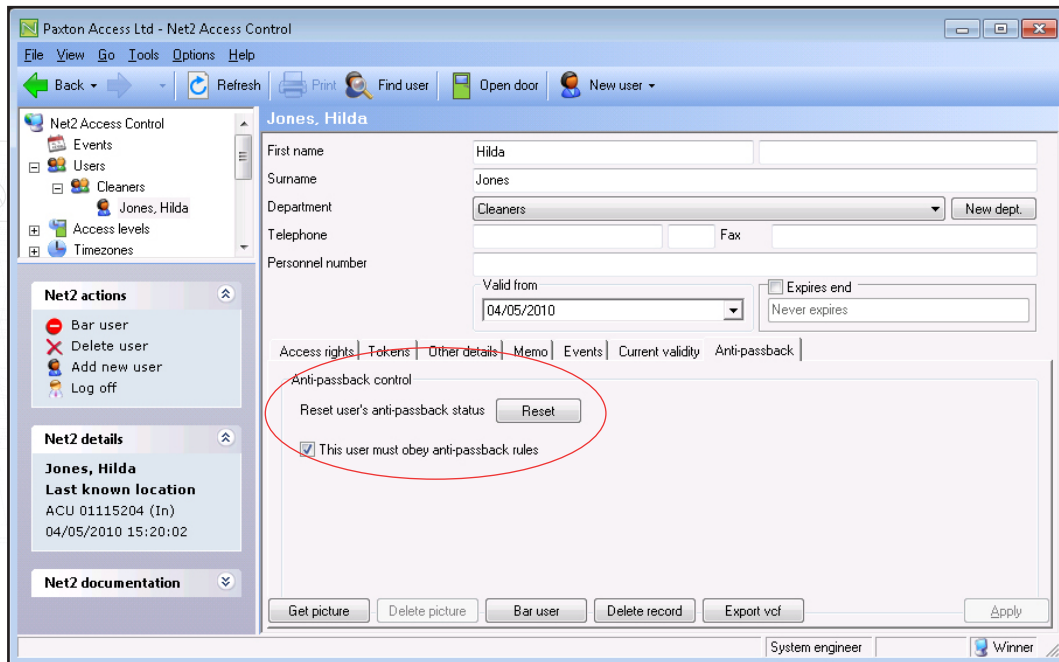
Important

Anti-passback requires the Net2 Server to be running. If you want to use anti-passback, it is recommended that the Net2 Server be installed on a dedicated machine.

If Net2 Fire Alarm integration is also configured, the Anti-passback system is reset when the Fire Alarm event is cleared and the doors relock. This allows users to be tracked again from scratch once they start using access control again.

The current specification for compatible PC hardware, network and operating systems is available on our website at the following link:-   http://paxton.info/720