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 >

If the system is Reset, the next valid access for a user sets their current location in the system.

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.