

- **Increased security and powerful control of users is a feature of CS Technologies access control**
- **Hard, Soft, Global, Timed antipassback**
- **Auto-forgive, muster reports**

## Introduction

“Antipassback” is the name given to a number of features of access control systems, all designed in some way or another to stop users ‘passing back’ their credential to another person attempting to gain access. Examples of use of antipassback might be in a carpark, where an owner wishes to stop people letting their friends park in the carpark as well, or in a hazardous location where it is desired to know who is on site at any time in the event of an emergency.

Antipassback increases security because it reduces the chance of people passing their credential around. CS Technologies access control systems support a variety of methods of implementing antipassback and this document describes the different types of antipassback and how they are used with CS Technologies systems.

## Antipassback concepts

With any antipassback system the concept of reader “disposition” is introduced. This simply means being able to identify whether a particular reader is an ‘entry’, ‘exit’, ‘internal’ or ‘don’t care’ reader. When readers are designated as entry or exit the system becomes able to record whether a user is inside or outside at any time by simply noting the last place their credential was used. If the last time it was used was at an ‘exit’ reader then the system knows that they are outside; if the last time it was used was at an ‘entry’ reader then the system knows that they are inside.

### “Hard” antipassback

In the classic use of antipassback the system uses the individual status of each user to determine whether they are allowed to use a particular reader. Because readers are designated as entry/exit/don’t care then the system knows whether users are inside or outside. Hard antipassback stops them from using their card to enter the premises if they are already inside, or exiting if they are already outside.

Thus with hard antipassback implemented, users are unable to ‘pass back’ their credential to let their friend gain entry because once they have entered the system knows that they are inside and won’t let them re-enter unless they first exit.

Hard antipassback maintains a high level of security but can cause inconvenience as users who forget to use their card to enter or exit (by following someone else in for example) will have their status confused in the system – it will think that they are outside when they are actually inside, and so won’t let them leave.

### “Soft” antipassback

With soft antipassback the system records the status of each user, thus knowing whether they are inside or outside at any stage, but doesn’t “enforce” the status. Thus if they are inside and attempt to re-enter the system will grant them access. This increases convenience; the system still knows whether users are inside or outside based on their last reader used but may be less accurate because it hasn’t enforced that users must enter before exiting and vice versa. It also therefore reduces security; the system knows where a person is but doesn’t stop them from entering twice. This type of system is often used with time and attendance applications.

### Forgiving a user

Users can have three possible states with an antipassback system – inside, outside or unknown. “Forgiving” a user simply means setting their antipassback status back to ‘unknown’ so that the next time they attempt to enter or exit they will be granted access.

## Tailgating

Tailgating refers to a user following another user through a door or boomgate without presenting a credential. They follow closely enough that they can get through the door or gate before it closes. Only the first user is recorded as being inside or outside.

## Passback violation

A passback violation simply refers to a user attempting to gain access when their antipassback status is incorrect i.e. they are attempting to enter when the system records that they are already inside, or exit when the system records that they are already outside.

## Timed antipassback

Timed antipassback refers to a system where users are automatically forgiven after a certain period of time. For example, they might enter a carpark and then the system records that they are inside for the next 30 minutes which stops them from allowing their card to be used to let their friend into the carpark. After 30 minutes their antipassback status is set to 'unknown' again to allow them to re-enter. This eliminates the need for an exit reader which can reduce costs in some cases.

## Global antipassback

Within each controller in the network the antipassback status of each user is recorded and tracked. Global antipassback takes that information and retransmits it to all the other perimeter controllers in the network so that no matter where a user is their antipassback status is recorded.

## Muster report

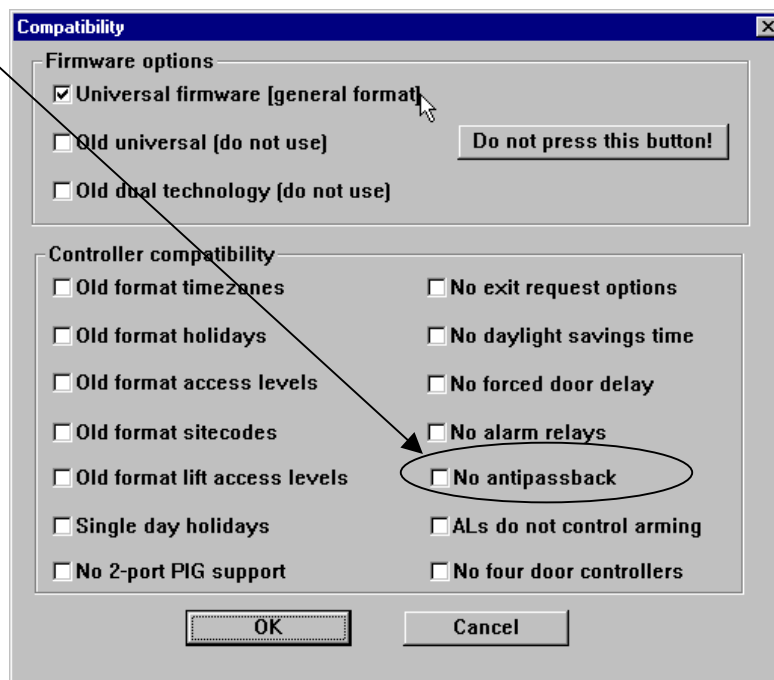
A muster report is simply a report of users where their antipassback status is recorded. Muster reports are often used in situations where it is required to know who is inside at any time in the event of an emergency. The muster report becomes an 'evacuation list'.

## Setting up the system for antipassback

Antipassback with the CS Technologies access control system works with Door firmware and with either PC3 or Advent software. Advent offers a much greater degree of power and functionality than PC3. To set up a system for antipassback the following steps must be taken.

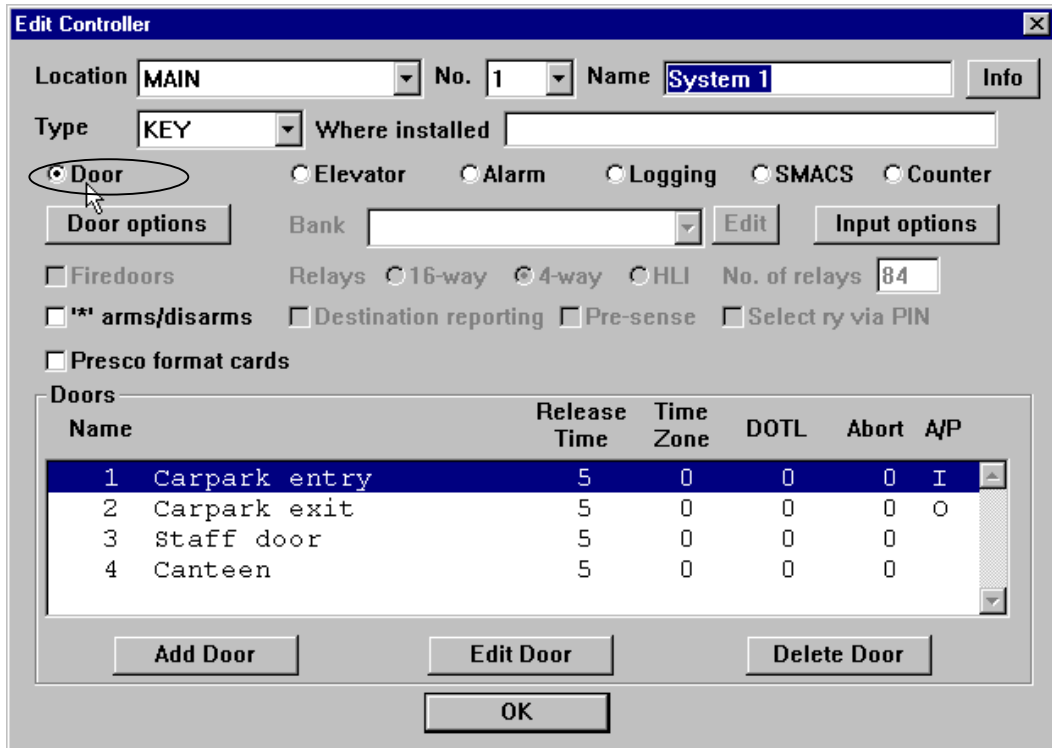
### 1. Ensure that antipassback is enabled under Technician/Compatibility

Early versions of firmware did not support antipassback so there is an option available to disable it. Ensure that this is not ticked.



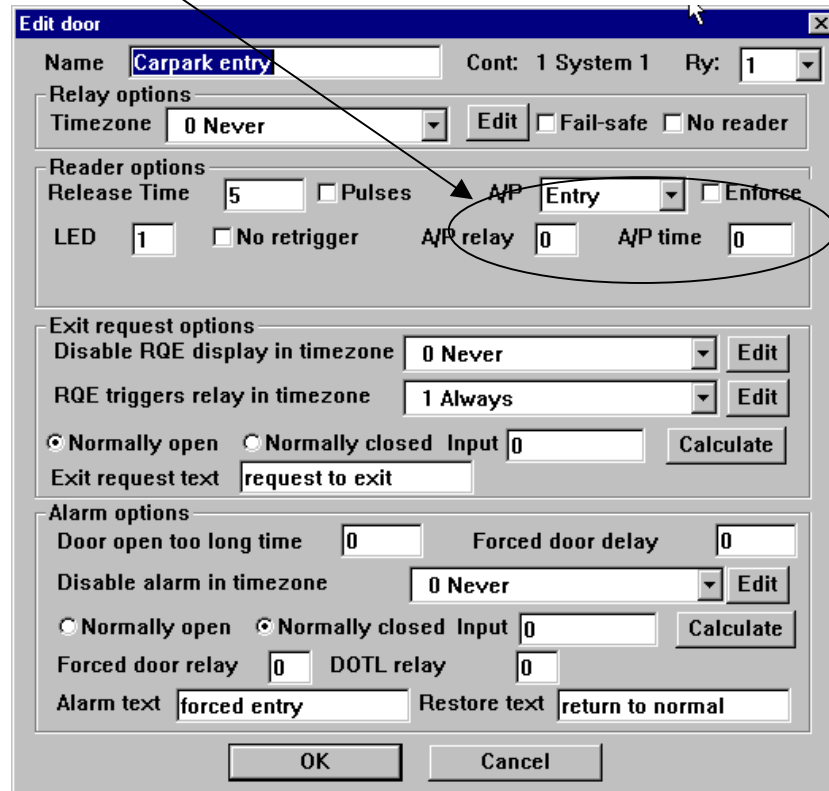
**2. When defining controllers, antipassback works with Door firmware**

Under Hardware/Controllers select the firmware type as 'door' and ensure that the firmware is actually door firmware.



**3. Set the door antipassback options for each door**

Under Hardware/Controllers/Edit controller/Edit door there are fields available which allow you to define various antipassback options for the door.



Fields to be completed include:  
 A/P – select Entry, Exit or Don't care

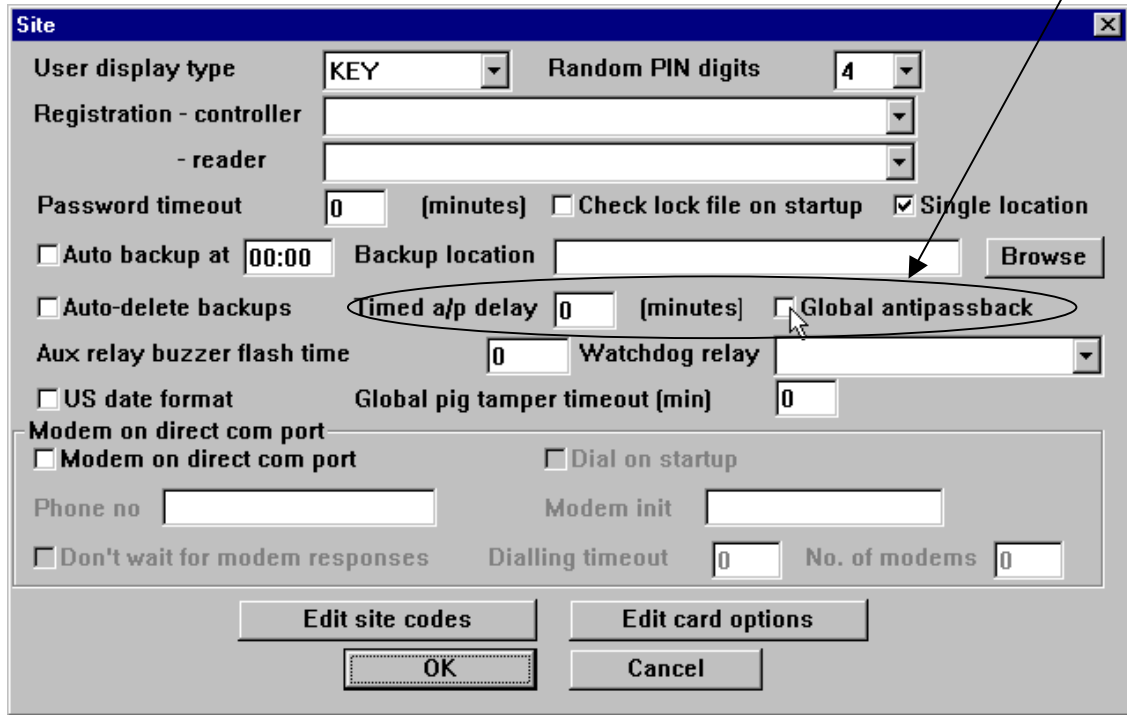
Enforce – tick this box to ‘enforce’ hard antipassback

A/P relay – this can be any of the on-board relays (1-4) which will pulse whenever an antipassback violation on that controller occurs.

A/P time – sets the pulse time of the antipassback relay

#### 4. Set global options

Under Technician/Site set the timed antipassback delay and whether you want global antipassback to apply.

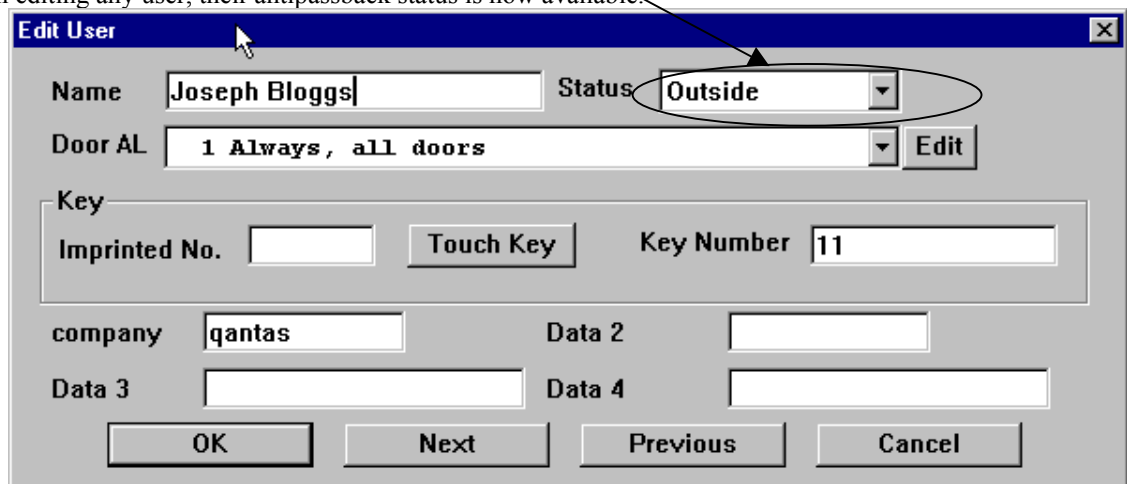


### Using antipassback

When antipassback is turned on there are several features available.

### Users

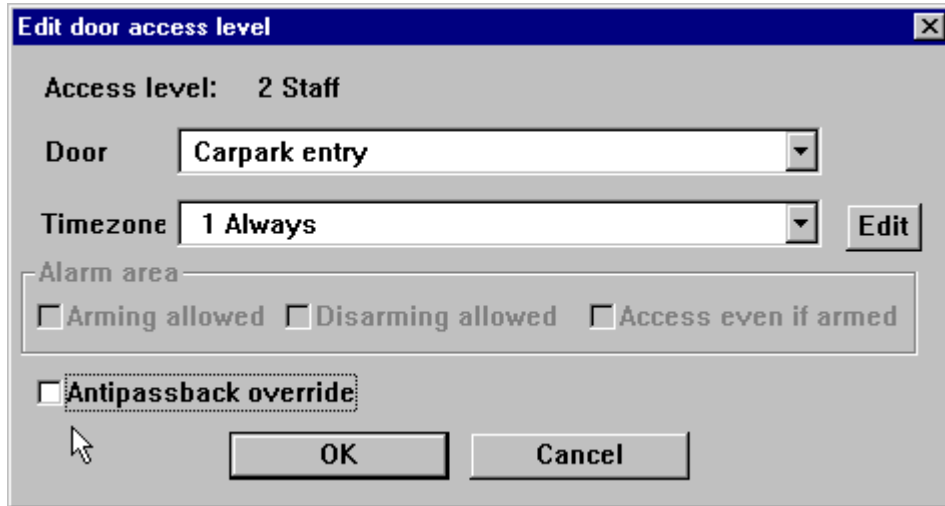
When editing any user, their antipassback status is now available.



It is possible from this window to change the antipassback status to Inside, Outside or Unknown. This field shows the current antipassback status of that user. Note that the status won't change while this window is open. Thus it is possible to view the antipassback status and also change it (forgive) for any individual user.

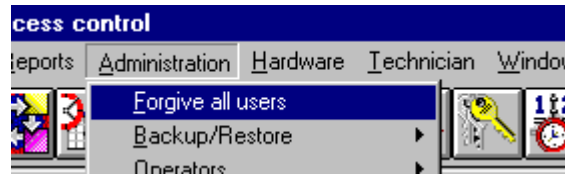
### Access levels

With R2 door firmware it is possible to define any access level as having antipassback applied to it or not. Access levels are defined under Setup/Access levels/Door access levels. Whenever editing a door on a controller to which antipassback applies the option ‘antipassback override’ appears. Tick this box to enable users with that access level to override the antipassback. Note that access level 1 always overrides antipassback.



### Forgive all users

Under Administration a menu selection ‘forgive all users’ will be visible.



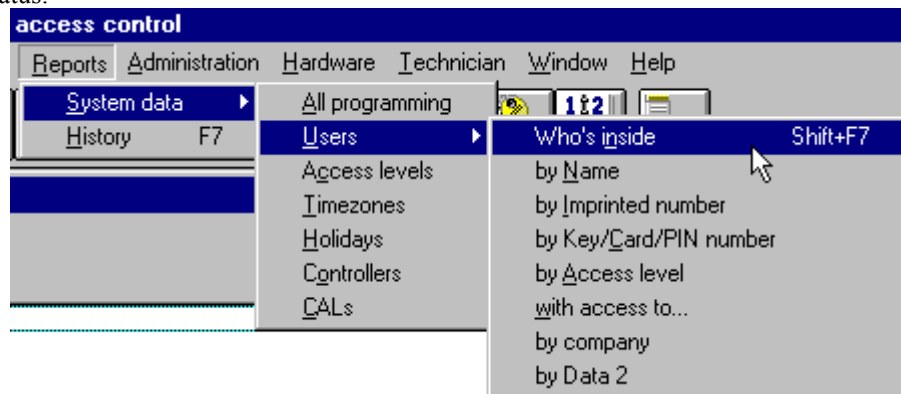
Selecting this menu will reset the antipassback status of all users to ‘unknown’. Note that this can take some time as it involves a full load of all users to the relevant controllers.

### Midnight forgive

Under Technician/Features a checkbox is available for ‘midnight forgive’. If this box is ticked then at 12:05am each day the antipassback status of all users will be reset to ‘unknown’.

### Muster report

Under Reports/System Data/Users/Who’s inside a quick report can be generated of users showing their current antipassback status.



When this report is selected all users are displayed grouped by their antipassback status. This report can also be generated very quickly by pressing the Shift+F7 keyboard combination.

An example muster report is listed below.

## User List

Total users in database = 2

<b>User Name</b>	<b>Imp. No.</b>	<b>Key Number</b>	<b>Door AL</b>	<b>STATUS</b>	<b>Company</b>
<b><u>Status: INSIDE</u></b>					
Joseph Bloggs	11	123456	1	INSIDE	Bricklayers
<b><u>Status: OUTSIDE</u></b>					
Charles Smith	1	654321	1	OUTSIDE	Tilers

Copyright © 2002 CS Technologies (A division of Trycup Pty Ltd ACN 003 341 982)

The above information is intended for information only and is believed to be correct at time of printing. CS Technologies accepts no responsibility for any damage as a result of the use or misuse of this information. E. & O. E.

\\BRUCE\BRUCE D\My Documents\CS Technologies\Brochures\Technical notes\Tech note re antipassback.doc