

Access Group Programming

Access Groups contain a series of options which are used to decide which access control actions are allowed at a particular Door. Access Groups are allocated to Doors to Control Door access.

There are 3 default Access Groups programmed as default and available for use in the system. These Access Groups will cover most common Door programming requirements. **The procedure to reset Access Group Programming to the factory default is explained in more detail at the end of this chapter.**

Access Group Defaults

	AG001	AG002	AG003
Name	ENTRY Door	EXIT Door	INTERNAL Door
TimeZone			
Alternate Group			
ENTRY OPTIONS			
Entry Mode	PIN or Card	Card & PIN	PIN or Card
Entry Passback Option	None	None	None
Entry Button		Yes	
Deadlock Entry Button			
Auto Area Off	Yes		Yes
Dual User Requirement			
EXIT OPTIONS			
Exit Mode	Card & PIN	PIN or Card	PIN or Card
Exit Passback Option	None	None	None
Exit Button	Yes		
Deadlock Exit Button			
Auto Area Off		Yes	Yes
Dual User Requirement			
GENERAL OPTIONS			
Isolate on Entry			
De-isolate on Exit			
No Entry if wrong Area			
No Exit if wrong Area			
Two Zones Mode			

**Access Group to
alter: AG001**

This screen allows the Installer to select an Access Group for programming. Pressing the ON Key allows the programmer to search for a specific Access Group by pressing the digit key which corresponds to the first letter in the name of the Access Group.

**Find Acc. Grp ^
PIN Access**

e.g. Having pressed the ON Key, press the "6" Digit Key to display the name of an Access Group starting with P, Q or R.

**A. Grp. 001 Name
PIN Access**

This screen allows an optional Access Group name to be entered up to 16 characters long. It is recommended that Access Group names be programmed to simplify programming of other options where Access Groups are allocated.

**AG001 T.Zone ->
WEEKDAY**

This screen allows an optional TimeZone to be "attached" to this Access Group. When a TimeZone is "attached", the Access Group is only valid when the TimeZone is valid. When the TimeZone is invalid, the operation of this Access Group is also considered invalid and the Alternate Group, if programmed below, will be used instead, provided it too is in a valid TimeZone.

**AG001 TimeZone
TZ001**

To select a TimeZone press the right arrow key to scroll through all the available TimeZones alphabetically. Press the OFF key if you wish no TimeZone control of this Access Group. (The ON key may be used to change modes to allow a TimeZone to be selected by number, if desired).

**AG001 Alt. Grp->
CARD USER**

This screen allows the Installer to specify the name of an Alternate Access Group to be used in place of the primary Access Group whenever the "attached" TimeZone is invalid. If no Access Group is specified and when the TimeZone is invalid, all options for the Access Group are considered invalid and Doors assigned this Access Group will cease to operate.

**AG001 Entry ->
mode Pin or Card**

This screen determines the type of access mode to gain entry to the Door. The right arrow is used to cycle through all the choices:

Mode

PIN Only

Operation

Only a PIN code will allow entry through this Door.

Card Only

Only a Card will allow entry through this Door.

PIN or Card

A PIN code OR a Card will allow entry through this Door.

Card & PIN

A Card followed by a PIN code must be used to allow entry through this Door.

Anti Passback**AG001 Entry ->
Passback: None**

This screen determines whether Anti-passback is to be applied on entering. See explanation at the end of this document and "Anti-Passback and Wrong Area Processing" in the "Applications Programming section of this manual for details.

Mode

None

Operation

No anti-passback

Soft

Anti-passback rules are applied but access is still granted if violated, with a message recorded to review.

Hard

Anti-passback rules are applied and access is denied if violated, with a message recorded to review.

Spare

Spare for future developments - do not use.

**AG001 Entry BLAD
Options-> nnnn**

This screen sets basic **entry access options** for this Access Group:

B	Button facility	If set to "Y", the entry Button, if present, is operational for Doors with this Access Group.
L	Dead Lock	If set to "Y", the entry button, if present, will not operate on Doors with this Access Group if you are <i>leaving</i> an Area that is currently ON.
A	Auto Area OFF	This option enables the operation of granting access through a Door assigned this Access Group to automatically turn Off the Inside Area of that Door first, provided that a valid Inside Area is defined within its Door programming options. This prevents authorised users being granted access through a Door and walking into an armed Area, thus activating alarms. If an Entry Button has been installed, access through the Door will not be granted whilst the Inside Area is armed, the Area must be turned Off before access will be granted.
D	Dual User	If set to "Y", a Dual code is required to enter a Door with this Access Group. (Those Users with a User Type which has the Override Dual User flag set to "Y" will be exempt from this requirement).

**AG001 Exit
Mode: PIN Only**

This screen determines the operation of a Door when a User is **leaving** via the Door. These options apply to Doors with Card Readers positioned on the inside of the Door and for which "Inside" positioning of the Card Reader is properly reflected in their Reader Module programming. The right arrow key is used to cycle through all available options:

Mode	Operation
PIN Only	Only a PIN code will allow exit through this Door.
Card Only	Only a Card will allow exit through this Door.
PIN or Card	A PIN code OR a Card will allow exit through this Door.
Card & PIN	A Card followed by a PIN code must be used to allow exit through this Door.

**AG001 Exit
Passback: None**

This screen determines whether anti-passback is to be applied on exit. *See explanation at the end of this document and "Anti-Passback and Wrong Area Processing" in the "Applications Programming section of this manual for details.*

Mode	Operation
None	No anti-passback
Soft	Anti-passback rules are applied, but access is still granted if violated and a message recorded to review.
Hard	Anti-passback rules are applied and access is denied if violated with a message recorded to review.
Spare	Spare for future development - do not use.

**AG001 Exit BLAD
Options-> nnnn**

This screen sets basic exit access options for this Access Group:

- | | | |
|----------|------------------------|--|
| B | Button facility | If set to "Y", the exit Button, if present, is operational for Doors with this Access Group. |
| L | Dead Lock | If set to "Y", the exit button, if present, will not operate on Doors with this Access Group if you are <i>leaving</i> an Area that is currently ON. |
| A | Auto Area OFF | <p>This option enables the operation of exiting through a Door assigned this Access Group to automatically turn Off the Outside Area of that Door first, provided that a valid Outside Area is defined within its Door programming options.</p> <p>This prevents authorised users leaving via a Door which leads into an armed Area, thus activating alarms.</p> <p>If an Exit Button has been installed, departure through the Door will not be granted whilst the Outside Area is armed, the Area must be turned Off before departure will be granted.</p> |
| D | Dual User | If set to "Y", a Dual code is required to exit via a Door with this Access Group. |

**AG001 IDEXT
Options-> nnnnn**

This screen sets special access options for this Access Group:

- | | | |
|----------|---------------------------|---|
| I | Isolate on Entry | If set to "Y", the pre-defined Zone Input allocated to the User will be automatically Isolated when the User presents their Card at the "outside" Reader of a Door which has been allocated this Access Group. This is explained in more detail below. |
| D | De-Isolate on Exit | If set to "Y", the pre-defined Zone Input allocated to the User will be automatically De-isolated when the User presents their Card at the "inside" Reader of a Door which has been allocated this Access Group. This is explained in more detail below. |
| E | No Entry if Wrong | <p>If set to "Y" and the "outside" Area for the associated Door is non-zero, entry will only be granted through a Door with this Access Group if the User's current location is equal to the defined outside Area.</p> <p>(This function operates independently of Anti-passback rules).</p> <p><i>See explanation at the end of this document and "Anti-Passback and Wrong Area Processing" in the "Applications Programming section of this manual for details.</i></p> |
| X | No Exit if Wrong | <p>If set to "Y" and the "inside" Area for the associated Door is non-zero, exit will only be granted through a Door with this Access Group if the User's current location is equal to the defined inside Area.</p> <p>(This function operates independently of Anti-passback rules).</p> <p><i>See explanation at the end of this document and "Anti-Passback and Wrong Area Processing" in the "Applications Programming section of this manual for details.</i></p> |
| T | Two Zones Mode | If set to "Y", Reader Isolation options are enhanced allowing for two zones per User instead of one. |

Reader Isolate Options

The Reader Isolate and De-isolate options allow one or two specific zones to be isolated when a Card is presented at a Reader on the “outside” of a Door and to automatically de-isolate the zone(s) when a Card is presented at a Reader on the “inside” of a Door.

This option allows a system to simulate a very large number of Areas which only contain one or two zones. This is a useful feature in applications requiring hundreds or thousands of simple Areas such as storage locker applications.

For this feature to function correctly, the Menu Group assigned to the User Type, which in turn is assigned to the User, must have the “I” Isolate on Exit flag set to “Y”.

Operation

When a Card is presented at a Reader on the outside of a Door and the Card is allowed to un-lock the Door, the Control Module checks the Isolate option (see above) for the Access Group currently valid for that Door. If the Isolate option is set to “Y”, a specific zone will be isolated automatically depending on the User who presented the Card. If the “T” option is set, two Zones will be isolated. See the following table for Zone allocations.

When a Card is presented at a Reader on the inside of a Door and the Card is allowed to unlock the Door, the Control Module checks the De-isolate option (see above) for the Access Group currently valid for that Door. If the De-isolate option is set to “Y”, a specific zone will be de-isolated automatically depending on the User who presented the Card. If the “T” option is set, two Zones will be de-isolated. See the following table for Zone allocations.

If this “T” option is set to “n”, the Reader isolate option will provide one Zone per User. Whether one Zone or two Zones are isolated depends on the setting of this “Two Zones Mode” option.

The Zone(s) that are actually isolated is not programmable but follows the table below:

User Presenting Card	Zone Isolated (“T” option not set)	Zone Isolated (“T” option set)
U00001 to U00032	None	None
U00033 to U00048	B01:Z01 to B01:Z16	B01:Z01 to B01:Z32
U00049 to U00064	B01:Z17 to B01:Z32	B02:Z01 to B02:Z32
U00065 to U00080	B02:Z01 to B02:Z16	B03:Z01 to B03:Z32
U00081 to U00096	B02:Z17 to B02:Z32	B04:Z01 to B04:Z32
etc	etc	etc

32 Zone “B” Type Expanders must be used and the Zones run in sequence up to the maximum number of Users or Expanders. Furthermore, this function can only be performed via a Card Reader.

The Reader to be used for isolating Zones may or may not be associated with a real Door. The Reader can be set up outside an imaginary Door, for the sake of example, D001 and an Access Group with the “I” option set allocated to the Door. The lock Auxiliary can control a lamp or buzzer so that when a Card is swiped, indication is given to the User that the Card was accepted and their storage locker can now be accessed. Similarly the Reader to be used for de-isolating zones may be associated with D001 or another Door. The Reader can be set up inside the Door and an Access Group with the “D” option set allocated to the Door. The lock Auxiliary can control a lamp or buzzer so that when a Card is swiped, indication is given to the User that the Card was accepted and their storage locker is now secure.

All the usual TimeZone options apply allowing certain Users access at certain times. All isolate/de-isolate operations are saved to review. If the Process Group allows, the actual isolate/de-isolate can be reported for some/all Users.

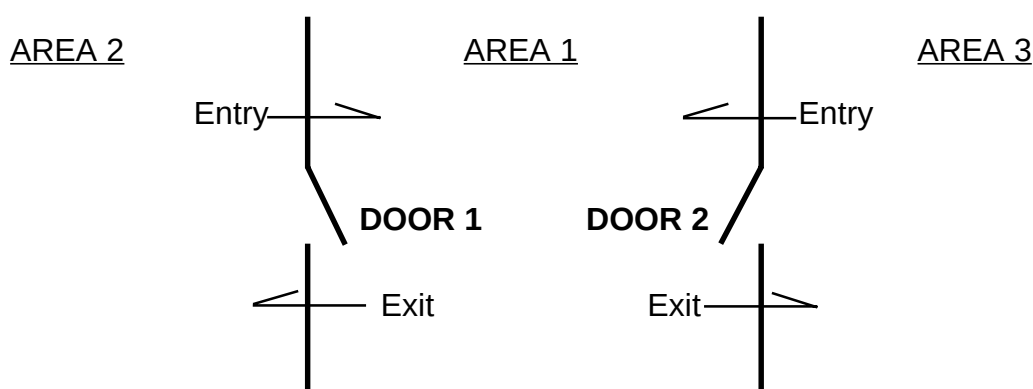
Wrong Area and Anti-Passback options in Access Groups

“Wrong Area” options operate independently of Anti-passback rules, however Hard anti-passback must be set when Wrong Area options are enabled. If the no (E)ntry on wrong area option is set to yes and the “outside” area for the associated door is non-zero, then entry will only be granted if the User’s current location is equal to the defined “outside” area.

Conversely, if the no E(X)it on wrong area option is set to yes and the “inside” area for the associated door is non-zero, then exit will only be granted if the User’s current location is equal to the defined “inside” area.

The Wrong area option may be considered as the HARDEST form of Anti-passback available. The comparison between Wrong aArea and Hard Anti-Passback may be made as follows.

Wrong Area will only allow access through a door if you are located within the associated area of that side of the door you are trying to gain access through. This means that if you present your card at an Entry Reader, your location must be in the OUTSIDE area associated to that specific Door. If you present your card at an Exit Reader, your location must be in the INSIDE area associated to that specific Door.



Hard Anti-Passback processing. Refer to the diagram above.

Hard Anti-Passback will only allow access through a specific door if you are considered on the correct side of it. If you are outside the door, you may go in, and if you are inside the door, you may go out. This still requires allocation of Inside and Outside areas to the door, but the Anti-Passback rules are on a per door basis.

What this means is if I go through Door #1 into Area 1 from Area #2, I am now inside Area #1. If there is another door that allows access into Area #1, Door #2, I may exit Area #1 via Door #2 which has an outside area of Area #3. Because I am now outside Area #1 (the inside area of both doors) I can now access either Door #1 or Door #2 to gain access legally to Area #1. Once inside Area #1 if I try to gain access into Area #1 while I am inside (because I passed back my card to someone else), access will be denied ANTI-PASSBACK. The same will occur if I am outside either door (in Area #2 or Area #3) and I try to exit. To summarize Anti-Passback; It only ensures I am on the correct side of the door, and that I have not exited illegally or given my card to another person.

Wrong Area processing. Refer to the diagram above.

Wrong area however will only let me through the specific door I entered or exited. If we take the above example again but now also have the “No Entry if Wrong Area” & “No Exit if Wrong Area” flags set in conjunction with Hard Anti-Passback, we get the following result. If I go through Door #1 into Area #1 from Area #2, I am now inside Area #1. If there is another door that allows access into Area #1, Door #2, I may exit Area #1 via Door #2 which has an outside area of Area #3. Because I am now outside Area #1 (the inside area of both doors) but inside Area #3, I cannot go back into Area #1 via Door #1. This is because I am in Area #3 and the access group options state “DO NOT ALLOW ENTRY if the area I am currently in, is NOT the AREA associated to that side of the door I am try to gain entry from”. In this case Area #2. To summarize Wrong Area, it controls specifically the direction and which door I may go through at all times.

Programming Notes.

Both "Anti-Passback" and "Wrong Area" require that the inside and/or the outside area of the door be set to a non zero value. The area selected will depend on the direction and level of restriction required.

It is suggested that when Anti-Passback is used, all doors that exit the premises entirely should have their outside area all programmed the same, or all set to None. In addition, it is suggested that a Calculated Auxiliary is programmed to perform an Amnesty function to operate on a daily basis once the premises is empty (automatically when the security area is turned on). This is to prevent Users locking themselves out or, or in, specific areas if they enter or exit illegally.

In the case of Wrong Area, it is suggested that all doors that exit the premises should have their outside area programmed the same. However, the Amnesty function should not be used, as this will render the location of every user as None, causing them to be locked out of all doors (because they are no longer in any area).

The User Types "Override Anti-Passback" flag can be set to allow particular User Types to enter or exit a door regardless of Anti-Passback or Wrong Area settings.

The easiest way to map out and implement both Anti-Passback or Wrong Area is to get a floor plan of the premises and mark out each door to be controlled and then assign areas to both sides of the doors. This will then produce common areas between doors, and the specific details required to complete the programming.

Refer to "Anti-Passback and Wrong Area Processing" in the Applications Programming section of the manual for more details and step-by-step programming procedures.

Access Group Defaulting

Two options are available to default Access Group Programming to factory settings. These are explained below:

**Access Group to
alter: AG001**

At the first Access Group Programming screen press HELP, "9".

**A.Grp. Default ->
Don't Default**

This screen is then displayed. Available defaulting options are viewed by pressing the right Arrow Key. To make a selection, press the OK Key.

Don't Default

Selecting this option will abort the procedure.

Clear All

Selecting this option will reset the first three Access Groups as follows:

AG001	ENTRY DOOR
AG002	EXIT DOOR
AG003	INTERNAL DOOR

In addition, this option will delete all other Access Groups, if present.

Standard

Selecting this option will reset the first three Access Groups as follows:

AG001	ENTRY DOOR
AG002	EXIT DOOR
AG003	INTERNAL DOOR

This option will make no alterations to any other Access Groups, if present.

**Push '9' key to
Confirm Default**

The confirmation screen is displayed. Press the "9" Key to confirm your selection.

**Default
Done**

The default procedure is confirmed.