4 Door Controller Basic Setup & Programming for Access Control   AN100

These Programming Sequence guides set out the Door Data Menu Options and the relevant Challenger Installer Menu Options and User Menu Options in a recommended sequence to assist with the programming of Intelligent Doors (17 to 64) in a Challenger System.

Basic Setup & Programming for Access Control Functions.

1. **Set the DGP Address of the Intelligent Controller.**

Using DIPSwitches 1 to 4 on the Intelligent Controller, program the DGP Address.
(MUST be between DGP 1 and DGP 12)

2. **Set the Address/es of Arming Stations and/or Single Wiegand Interfaces connected to the 4 Door Controller LAN. (J22)**

Using DIPSwitches 1 to 4 on the units, program the RAS Addresses according to the table.

	FUNCTION			
	Access or IN	Access or IN	Access or OUT	Access or OUT
1st Door	1	5	9	13
2nd Door	2	6	10	14
3rd Door	3	7	11	15
4th Door	4	8	12	16

3. **Poll the 4 Door Controller DGP & Specify the DGP Type.**

INSTALLER MENU OPTION 4: -DGPs.

Program the DGP Address to be polled, and set the DGP Type as Type 1: Door Controller.

4. **Make a note of the Challenger Panel's relevant System Option settings.**

INSTALLER MENU OPTION 7: -System Options.

Note the setting of the "Input Tamper Monitoring" setting (YES or NO).
Note the value entered (if any) of the "Alarm Prefix Length". (None or 1 to 4).

These settings may need to be programmed into the Door Data Menu later.

5. **Program any Timezones required for Access Control functions.**

i) To specify when Egress is available on a door.
ii) To specify when Lock over-ride is active on a door
iii) To specify when a User may access a particular door. (Used in "Door Groups")

INSTALLER MENU OPTION 13: -Timezones.

Program the Timezones required and note the details for use in the Door Data Menu later. Only Timezones 1 to 24 can be used in the Door Data Menu.
(See Challenger Version 8 Programming Guide for details of programming Timezones)

6. **Determine which area/s (if any) will inhibit**
i) Egress on a door
ii) Access through a door
if the area/s are secure (armed or on)

INSTALLER MENU OPTION 2: -Area Database.

Obtain & note the details (number & name) of the area/s relevant to these access control inhibit functions.

Version 8 FOUR DOOR CONTROLLER PROGRAMMING SEQUENCE

7.   **Access the Door Data Menu.**

INSTALLER MENU OPTION 28: -Remote Controllers.

Access to the Door Data Menu for programming the details of individual Controllers & Doors is via Installer Menu Option 28. Select the Remote Number to Program. The "Remote Number" is the DGP Address or the unit.

8.   **Select the "Controller Options" to program the Controller details and details relevant to all doors on the controller.**

DOOR DATA MENU

Select Menu Option 1: -Controller Options.

9.   **Program the "Controller Options" required.**

DOOR DATA MENU OPTION 1: -Controller Options

Relay Controllers
(4 On-board relays are already provided for activating the 4 locks)

If 8 Way relay cards / 16 Way Open Coll. cards are fitted for extra relays. Specify the number or Relay Controllers (See Hardware Options for relay functions available)

Site Code A

If card readers are being used (card, key insert, bar code, etc.), the Site (or Facility) Code must be entered here.

Card Offset A

If the card ID numbers are to be Offset so that the resulting Challenger User number is different to the Card ID, program a suitable Offset Value here, and take note of it for use when programming the Users later.

Site Code / Card Offset B

A second Site Code and associated Offset can be programmed if required.

Alarm Code Prefix Length

If using PIN Code readers on the Controller for Access/ Alarm Control, enter the same value here as noted from the Challenger System Options.

Poll RAS

Enter the Number/s of the Arming Stations (RASs) to be polled according to the Addressing of the units in Step 2.

List RASs with LCDs

If any of the Arming Stations on the Controller LAN are LCD types, list their address here.

List RASs with Egress Input enabled

If any of the Arming Stations on the Controller LAN require Egress to be wired to the RAS, list their address here. (It is preferable to wire Egress to the Controller)

Input Tamper Monitoring

If 4 State monitoring is required on 4 Door Controller inputs, set this option to YES. (Should ideally be the same setting as noted in the Challenger System Options)

If the default timer settings are unsuitable, they may be altered.

Card to PIN time (Default = 8 secs)

Relevant when Card & PIN required for access.

Dual Custody time (Default = 8 secs)

Relevant when two User cards/codes required for access

Mode Time (Default = 5 secs)

Only relevant if alarm control required. Time between 1st & 3rd badge to arm/disarm if this method selected.

Lock Release time (Default = 3 secs)
(Re-lock time)

Time before door re-locks after Door Contact is re-sealed.

AN100

10.	**Access the Door Option Menu to program details of <u>individual doors.</u>**	<u>DOOR DATA MENU</u> Select Menu Option 2: -Door Options.
11.	**Select the "Door Number" of the door you wish to program.**	Select one of the four door numbers associated with the DGP Address of the Controller you are programming.
12.	**Select and program the "Access Options"**	<u>DOOR OPTIONS MENU OPTION 1: -Access Options</u>
	Access Time (Default = 5 secs)	Time that lock relay activates to unlock the door.
	Extended Access Time	Overrides Access Time when user has "Long Access".
	Shunting Option	Select the type of input shunting required (if any)
	Shunt Time	Program the time that input/s are to be shunted.
	Extended Shunt Time	Overrides the Shunt Time when user has "Long Access"
	Shunt Warning Time	Program the time before the shunt time expires, that the "Warning Relay" may be activated. (See Hardware opt)
	Low Security Timezone	If "Card & PIN"selected, specifies a Timezone when Card OR PIN will access the door.
	In Reader / Out Reader Card & PIN	Specify if "Card & PIN" is required to access the IN and/ or OUT reader/s.
	In Reader / Out Reader Inhibit PIN	Prevent PIN being used during "Low SecurityTimezone"
	AntiPassback Option In Reader / Out Reader Region Anti-Passback Time	Refer to "Programming for Anti-Passback".
	In Reader / Out Reader Dual Custody	Specify if Dual Custody is required to access the IN and/ or OUT reader/s.
13.	**If the Egress function is used, program the "Egress Options".** **(If Egress not used this option can be ignored)**	<u>DOOR OPTIONS MENU OPTION 2: -Egress Options</u>
	Egress Timezone	Specify a Timezone during which Egress will be available at this door. Timezone 0 = Always available.
	In Egress / Out Egress Disabled if Secure	Specify if IN Egress or OUT Egress is to be disabled when area/s assigned are Secure (armed or on) (See Hardware Options for area assignment)
	Egress Mode	Select the mode of Egress control required
	Egress Reporting	Specify if Egress function is to be reported to Printer/ Computer.

Version 8 FOUR DOOR CONTROLLER PROGRAMMING SEQUENCE

14. **Select & Program the "Reader Options".** DOOR OPTIONS MENU OPTION 4: -Reader Options

Card Format
(Not applicable to Tecom Magnetic Cards)

Specify the Card Format for any reader with Wiegand output.   Tecom ASC for Tecom Indala Proximity. Wiegand 26 Bit (ID=16, FC=8) for Wiegand Swipe Card and Key Insert.

Input Holds Door Unlocked

Select if door to be held unlocked until after door is closed. (If lock mechanism will prevent door closing)

Over-ride Timezone

Timezone when door will be held unlocked and shunted.

Over-ride After Entry

Select if start of Over-ride Timezone is to be delayed until a valid door access function is performed by a user.

Report Door Open

Select if report to be sent to Printer/Computer whenever door is unsealed and re-sealed.

Report Forced Door

Select if report to be sent to Printer/Computer whenever door is forced. (Unsealed without valid door function)

Report DOTL

Select if report to be sent to Printer/Computer whenever door is in DOTL state. (Open after Shunt time expires)

Reader LED Options

Select LED condition for Lock status or Area Status. (If Area status, see Hardware options for area allocation)

15. **Select and Program the "Hardware Options".**
Only system numbers associated with the
DGP Address of the Controller may be used.
Options marked #, have a default setting. See table at
rear of manual for the default input & relay numbers.

DOOR OPTIONS MENU Option 5:-Hardware Options

Lock Relay Number #

The Controller relay number that will activate the lock.

Input Number #

The input number that the Door Contact is wired to.

Forced Relay Number

The Controller relay that will indicate "Forced Door"

Shunt Input Number/s #

The Input number/s to be shunted when door is accessed.

Warning Relay Number

The Controller relay that will indicate shunt time ending.

DOTL Input Number #

The input used to report DOTL to The Challenger Panel

DOTL Relay Number

The Controller relay that will indicate "DOTL" state.

Egress Input Number #

The input number that the Egress button is wired to.

Interlock Input Number/s

Inputs on the Controller that door is interlocked with.

Area/s Assigned to Door
(It is recommended that only ONE AREA be assigned to a door)

Area/s assigned to the Door that may be utilized for: "Egress Disabled if Secure", "Access Denied if Secure", and Reader LED if indicating Area status.

Fault Relay Number

Controller Relay that will indicate lock or reader fault.

AN100

16. **When each Controller and each individual Door has been set up, the "Door Group/s" can be programmed.**

Door Groups are assigned to Users to specify which door/s may be accessed and when each door may be accessed.

USER MENU Option 20: -Door Groups

Program the Door Group/s to ensure that Users can be assigned a Group that will list all of the Doors that they are allowed to access.

Each Door in a Door Group is either assigned a Timezone or Disabled.
The timezone specifies when access is allowed.
Timezone 0 may be used to specify access always allowed

(See Challenger Version 8 User Guide for more details)

17. **Program the Users who are to be allowed access control functions.**

Create Users or modify existing User Records to ensure that Users have the appropriate access control facilities.

Select a User Number.

Assign an Alarm Group if required.

Assign a suitable Door Group to the User.

Floor Group not applicable

Set any User Flags required (If enabled)

Program the User Name (Users 1 to 200 only)

Program a PIN Code if required.
(Users 1 to 1000 only)

USER MENU Option 14: -Program Users

The User number must be the same as the Card ID number if Cards/Keys etc. are used.
(Allowing for the "Card Offset" if programmed)

If PIN codes only are used the User number is not critical.

Not necessary if User is only allowed access control functions and not Alarm Control functions.

Users must be assigned a Door Group which includes any doors at which they are to perform access control functions.

User Flag may be set to allow "Long Access".

A 16 character User name may be programmed.

A 4 to 10 digit PIN code may be entered.

(See Challenger Version 8 User Guide for more details)

18. **Program the "Input Database" to specify how Inputs on the 4 Door Controller will be treated by the Challenger System.**

The Input Database must be programmed to determine the type of alarm or function that will be generated when the 4 Door Controller inputs generate conditions such as "Forced Door", "DOTL", "Input Fault/Tamper", "Input Unsealed", etc.

INSTALLER MENU OPTION 1: -Input Database.

Program the Input Database for every input used on the 4 Door Controller.
i.e. All inputs that have devices connected to them and all inputs specified as "DOTL" inputs.

(See Challenger Version 8 Programming Guide for more details on programming inputs)

4 Door Controller
Programming for Alarm Control   AN100a

Programming to Add Alarm Control Functions.

1. **Follow the Programming Sequence for "Basic Setup & Programming for Access Control functions"**

Before Alarm Control functions can be added on Readers connected to 4 Door Controllers, the basic programming must be followed.

Follow the Basic Setup procedure, and select the access control functions required.

2. **Program any "Timezones" required for Alarm Control functions.**

i)   To specify when an Alarm Group is valid.

(Alarm Groups are assigned to Doors and Users to specify the Area/s and Alarm Control functions allowed.)

INSTALLER MENU OPTION 13: -Timezones.

Program the Timezones required and note the details for use in the Alarm Group Programming. Only Timezones 1 to 24 can be in Alarm Groups assigned to Doors. (See Challenger Version 8 Programming Guide for details of programming Timezones)

3. **Program any "Alarm Groups" required for Doors and Users. (Or select appropriate Alarm Groups from the default Groups available)**

An Alarm Group defines the Area/s, and Alarm Control functions (Arm, Disarm, Reset, etc), available to the User or Door to which it is assigned.
(An Alarm Group also defines the User Menu Options available, but these are not relevant in Alarm Groups assigned to Doors)

INSTALLER MENU OPTION 5: -Alarm Groups.

Program or choose appropriate Alarm Groups, as required, to provide the Area/s and level of control allowed and any Timezone restriction required.

(See The Challenger Version 8 Programming Guide for more details on programming Alarm Groups)

4. **Access the Door Data Menu.**

Access to the Door Data Menu for programming the details of individual Controllers & Doors is via INSTALLER MENU OPTION 28: -Remote Controllers. Select the Remote Number to Program. The "Remote Number" is the DGP Address or the unit.

5. **Access the Door Option Menu to program Alarm Control details of <u>individual doors.</u>**

DOOR DATA MENU

Select Menu Option 2: -Door Options.

6. **Select the "Door Number" of the door you wish to program to have Alarm Control facilities.**

Select one of the four door numbers associated with the DGP Address of the Controller you are programming.

Version 8 FOUR DOOR CONTROLLER ALARM CONTROL PROGRAMMING

7. **Select and program the "Alarm Control" functions for each Door.**

<u>DOOR OPTIONS MENU OPTION 3: -Alarm Control</u>

Alarm Group

Assign an Alarm Group that specifies the Alarm System Control facilities relevant to the door.

Method of Alarm Control

Choose the method of Alarm Control required from options specifying the number of card badges and the use of card plus buttons.

IN Access Denied If Area Secure

Select if Access at the IN Reader is to be denied when the Area/s assigned to the Door in the "Hardware Options" are secure.

OUT Access Denied If Area Secure

Select if Access at the OUT Reader is to be denied when the Area/s assigned to the Door in the "Hardware Options" are secure.

8. **Program the Users who are to be allowed Alarm Control functions.**

<u>USER MENU Option 14: -Program Users</u>

Create Users or modify existing User Records to ensure that Users have the appropriate alarm control facilities.

Select a User Number.

<u>The User number must be the same as the Card ID number if Cards/Keys etc. are used.</u>
(Allowing for the "Card Offset" if programmed)

If PIN codes only are used the User number is not critical.

Assign an Alarm Group.

<u>Users must be assigned an Alarm Group</u> that specifies the Alarm System Control facilities relevant to the User. Alarm Control functions available will be determined by a comparison of the User's Alarm Group and the Alarm Group of the Door Reader at which the User performs the function.

Assign a suitable Door Group to the User.

<u>Users must be assigned a Door Group</u> which includes any doors at which they are to perform access control and/or alarm control functions.

Floor Group not applicable

Set any User Flags required (If enabled)

User Flag may be set to allow "Long Access".

Program the User Name (Users 1 to 200 only)

A 16 character User name may be programmed.

Program a PIN Code if required.
(Users 1 to 1000 only)

A 4 to 10 digit PIN code may be entered.

(See Challenger Version 8 User Guide for more details)

4 Door Controller Programming for Anti-Passback AN100b

Programming to Add Anti-Passback Facilities.

1.   **Follow the Programming Sequence for "Basic Setup & Programming for Access Control functions"**

Before Anti-passback functions can be added on Readers connected to 4 Door Controllers, the basic programming must be followed.

Follow the Basic Setup procedure, and select the access control functions required.

In Step 2. Pay particular attention to the Addressing of the Arming Stations and/or Single Wiegand Interfaces connected to the 4 Door Controller LAN. (J22)
The Address chosen for each reader will determine whether the Reader will be an "IN" or "OUT" reader.
i.e. Where readers are installed on both sides of the same door, one must be addressed as the IN reader and one as the OUT reader.

Addressing Readers to be used for Anti-Passback

	FUNCTION			
	Access or IN	Access or IN	Access or OUT	Access or OUT
1st Door	1	5	9	13
2nd Door	2	6	10	14
3rd Door	3	7	11	15
4th Door	4	8	12	16

2.   **Access the Door Data Menu.**

Access to the Door Data Menu for programming the details of individual Controllers & Doors is via
INSTALLER MENU OPTION 28: -Remote Controllers.
Select the Remote Number to Program.
The "Remote Number" is the DGP Address or the unit.

3.   **Access the Door Option Menu to program Anti-Passback facility details of individual doors.**

DOOR DATA MENU

Select Menu Option 2: -Door Options.

4.   **Select the "Door Number" of the door you wish to program to have Anti-Passback facilities.**

Select one of the four door numbers associated with the DGP Address of the Controller you are programming.

5.   **Select and program the "Access Options" relevant to Anti-Passback for the Door.**

DOOR OPTIONS MENU OPTION 1: -Access Options

Anti-Passback Option required.

Select the type of Anti-Passback required.
"Soft Anti-Passback" & "Hard Anti-Passback utilize the "Regions".
"Timed Anti-Passback" utilizes the "Anti-Passback Time"

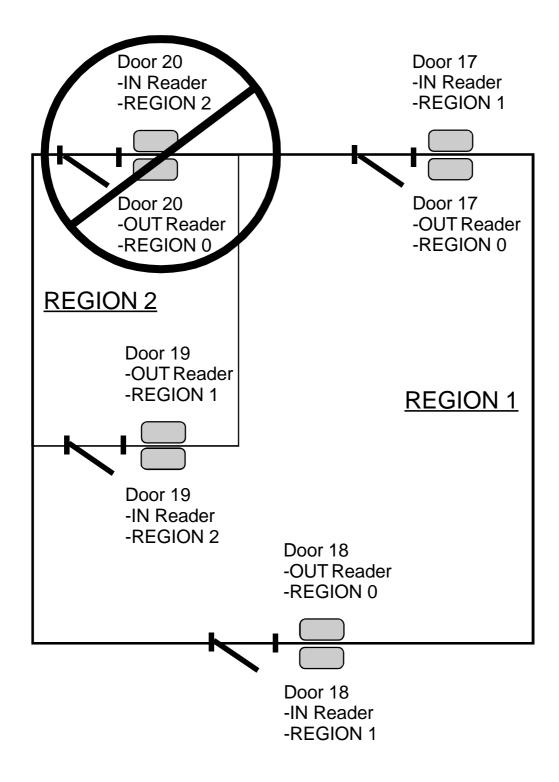IN Reader / OUT Reader Region number.

If Hard or Soft Anti-Passback selected, specify a region number for each reader type (IN & OUT) on the door.
A card/code cannot be used to enter the same region twice in succession.

Anti-Passback Time.

If Timed Anti-Passback selected, specify a period of time during which a card/code cannot be used at the reader twice in succession.

Example of Anti-Passback facility

Door 20
-IN Reader
-REGION 2

Door 17
-IN Reader
-REGION 1

Door 20
-OUT Reader
-REGION 0

Door 17
-OUT Reader
-REGION 0

REGION 2

Door 19
-OUT Reader
-REGION 1

REGION 1

Door 19
-IN Reader
-REGION 2

Door 18
-OUT Reader
-REGION 0

Door 18
-IN Reader
-REGION 1

REGION 0