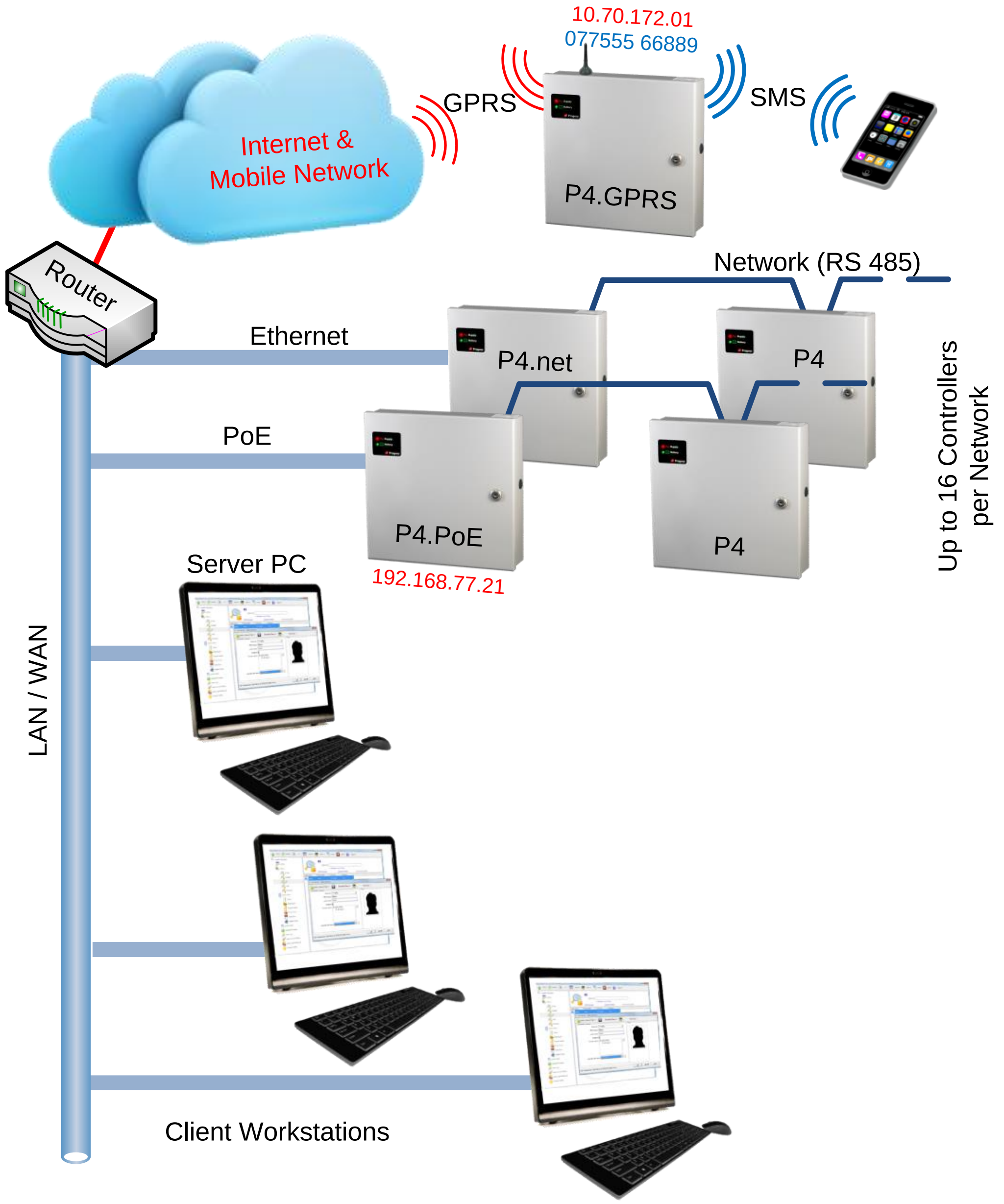
P4 Controller Manual

Now Including Biometric Support



Product Codes	Description
4001-5A	Single Door P4 Controller with 12V 5 A Charger PSU
4001D-5A	Two Door P4 Controller with 12V 5 A Charger PSU
4006-5A	Single Door P4 Controller with 12V 5 A Charger PSU + GPRS Interface
4006D-5A	Two Door P4 Controller with 12V 5 A Charger PSU + GPRS Interface
4003	Single Door P4 Controller with 12V 1 A PSU + Ethernet Interface & POE Splitter
4003-17	Single Door P4 Controller with 12V 1.7 A PSU + Ethernet Interface & POE Splitter

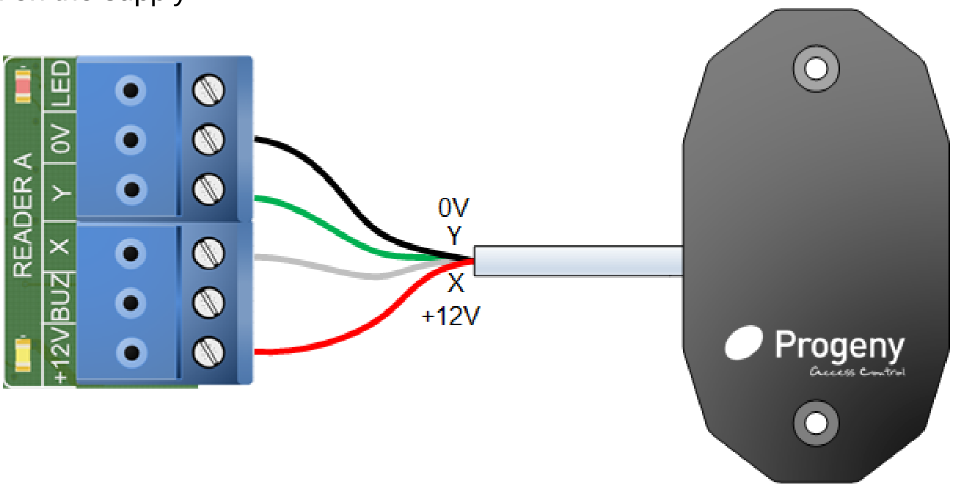
Table of Contents

Quick Start Procedure

To quickly set up and test your controller follow this procedure. The examples given are for a P4 Controller connected to P4 Readers and using P4 Cards. You may need to adapt the settings for the readers you are using.

Wiring

1. Connect the reader to the controller
2. Connect the mains supply to the controller
3. Switch on the supply



Programming

Once all the connections are made, the following procedure will allow you to test a Card.

1. Press * & # on the keyboard at the same time to unlock the keyboard
2. Use the Discover Card (see User menu 02) Enter: * 6 5 4 3 2 1 * 0 2
3. Now present the required cards or fobs to the reader one after then next.
4. Press the # key to finish.

Testing

Now test by presenting the card you enabled to the reader: The reader LED will turn green and the lock relay will open for 3 seconds.

Note: if you are using a reader other than P4 you may need to set correct card technology (see Engineer menu 04 and 05)

Other Quick Starts

Other quick tests you can try are:

Request to Exit

Temporarily short the RQE input to 0V. This simulates a Request to exit button Push and will operate the lock output for 3 seconds

Access Code

1. Unlock the keyboard by pressing * & # keys at the same time
2. Enter * 6 5 4 3 2 1 * 0 1
3. Enter 7 8 9 0 #

An access code of 7890 has now been programmed. Enter 7 8 9 0 at the keyboard and the lock will release for 3 seconds.

Introduction

This manual covers the Progeny P4 range of access controllers. These work with Doors Enterprise management software. For best results we recommend using V8.00 or later.

The POE controllers are only available as single door. All controllers feature interfaces for:

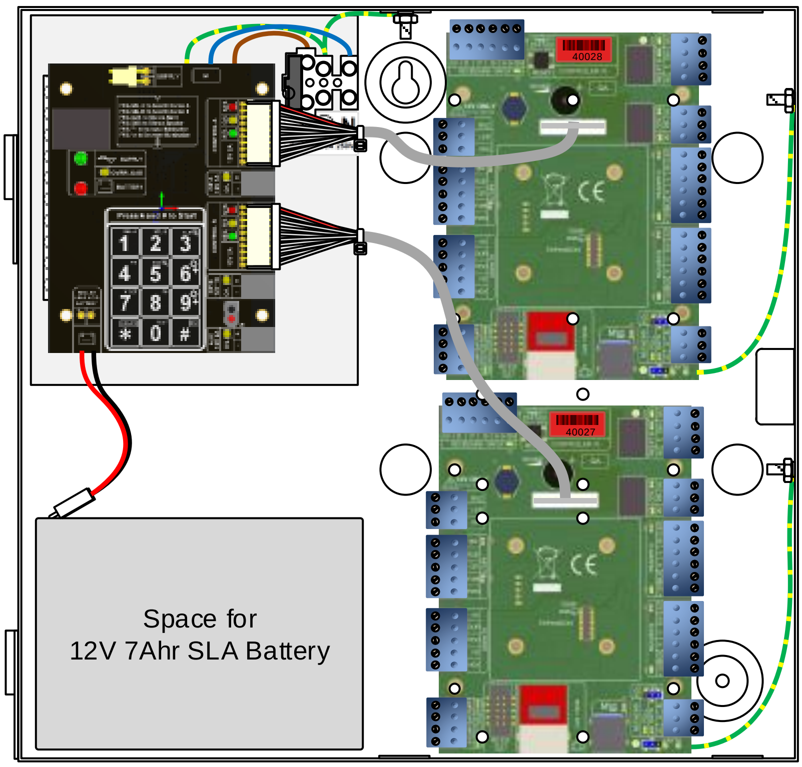
- Lock Drive (Electronic & Relay switched)
- Two Readers
- Keyboard, Request to Exit
- Door Monitor
- Interlock
- RS 485 network
- Engineer Programming Keyboard

IP Addressable

The IP settings such as IP Address, Gateway Address and Subnet Mask can be programmed from the front panel of each P4.net controller. (See Engineer functions 80 to 84).

Online or Stand Alone

The P4 access control system is designed to be an online system centrally programmed via the Doors Enterprise software. However, the controllers can also be programmed to operate stand-alone via the on-board keyboard. This gives flexibility when installing a system to confirm correct operation without the need for a PC.

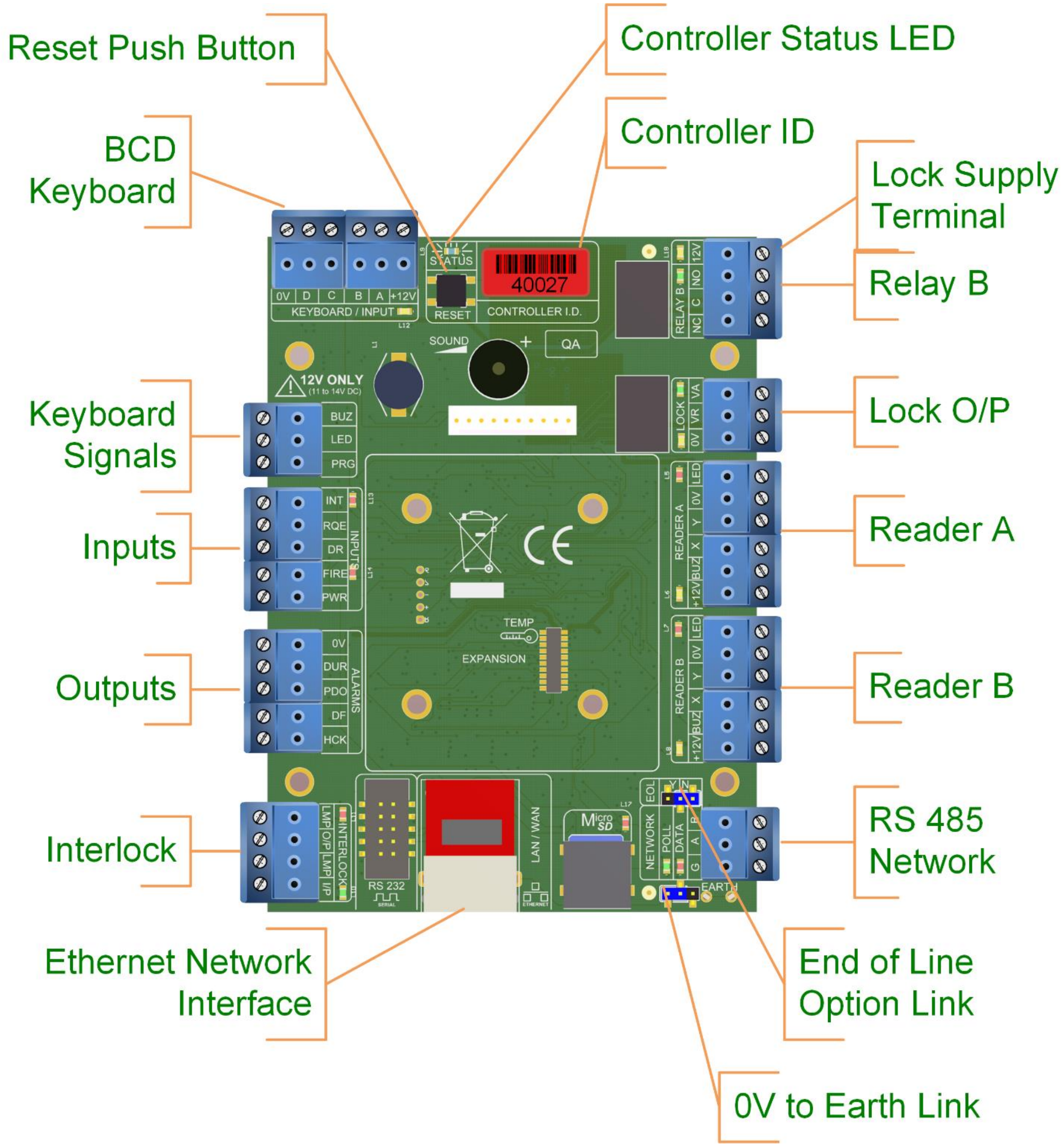


Time & Date

Each controller has a real time clock and non-volatile event memory to allow for the system to continue operation even when isolated from the PC or remainder of the network.

Communication

The P4 Controllers can connect via a USB Adaptor or via the P4.Net controllers using the LAN or WAN to distribute information to multiple sites or remote parts of the system.



Indicators

Status LED's can be found on the front panel of the controller and repeated at the keyboard and card readers. These indicators have the following meanings.

Keypad Status LED	Meaning
Off	Normal
On	Lock released
Flashing	Programming Mode

READER "A" & "B" LED's	Meaning
Off	Normal
On	Lock released
2 Flashes	Anti-pass back
3 Flashes	Card not registered
4 Flashes	Invalid card
5 Flashes	Card out of valid period
6 Flashes	Access Level Time Zone
7 Flashes	Reader Error

Sound

Sound is used to give the user additional feedback on the status of the controller and progress during programming.

Sound	Meaning
Continuous Two Tone, High Volume	PDO Alarm
Four Notes “Low – High – Low – High”	Programming Mode
Two Notes “Low – High”	Confirm Programming Change
Two Notes “High – Low “	Programming Error
Single Short Note “High”	Keyboard Key Push
3 long Beeps	Card not Registered (No Card Pack)
4 short Beeps	Card Registered but not enabled.
Tic Tic Tic	Memory Programming in progress

Note: The sounds from the keyboard controller can be annoying if located in earshot. To mute the on-board sounder, press **#** & **5** together. However, the sounder will re-activate when the * key is pressed. Note that this will not mute the PDO alarm sound.

Alarms

PDO

The “Prolonged Door Open” (PDO) or “Door Failed to Close” alarm acts as a reminder that a door is a security door and should not be wedged or held open for too long. If the door sensor has been connected then each time the door is detected opening the PDO timer starts. If this timer reaches a pre-set value before the door closes, a two-tone PDO alarm will be heard from the keyboard and the PDO output will activate. At the controller keyboard press keys # and 3 simultaneously to mute the current two tone sound from the controller.

PDO alarm cancels automatically when the door is closed. The PDO alarm is not active if the door is open due to Toggle mode.

Door Forced

The operation of the door forced alarm depends on the ability of the controller knowing when the door has been opened legitimately or not. In order to do this, both the door sensor input and the “request to exit” (RQE) inputs must be wired. Thus if the door is detected as opening without the lock being released then a Door Forced alarm will go active. This is a latching alarm.

Duress

A duress alarm can be raised by entering a modified access code. When the duress feature is turned on and the last digit of the access code is incremented, the duress alarm output is latched on. For example, if your access code is “1 2 3 4” then if you enter “1 2 3 5” the door will be released as normal but also the duress alarm output will go active and latch. If the duress feature is turned off, then “1 2 3 5” would not open the door. See “ENGINEERING MENU” later in this manual. This is a latching alarm.

Hacker

Persons trying to gain access by trying successive codes can be detected and an alarm raised via the Hacker output. The controller will count the number of consecutive errors and when this predetermined value is reached the alarm is generated. The factory set default hacker count is 0 (Off). This is a latching alarm.

Cancelling Latched Alarms

Door forced, Duress and Hacker alarms are all latching. They may be cancelled by:

1. Presenting a valid card
2. Entering the valid user password
3. Valid access code at the keyboard.

Programming

The P4 controller is capable of being programmed “Stand-Alone” from the on board or externally connected keyboard or “On-Line” from Doors Enterprise software running on a central PC.

Programming is achieved by entering a password at the keyboard followed by a menu selection code. There are two Programming Menus, one for the USER and one for the ENGINEER. Each menu has a separate six-digit password. Depending on the menu option selected, configuration data can then be entered at the keyboard.

Unlocking the Keyboard

To unlock the keyboard for programming press * and # together. The keypad will not accept any input until it is unlocked.

One Door Version

The single door version contains only one controller and therefore the indicators for Door B are not needed. These indicators are included in case the unit is ever upgraded to two doors. Before programming make sure that the ‘SELECTED’ indicator for Control A is illuminated. If not, press **[#]** and **[1]** keys <u>together.</u> The controller will beep and the ‘Control ‘A’ selected’ LED will illuminate.

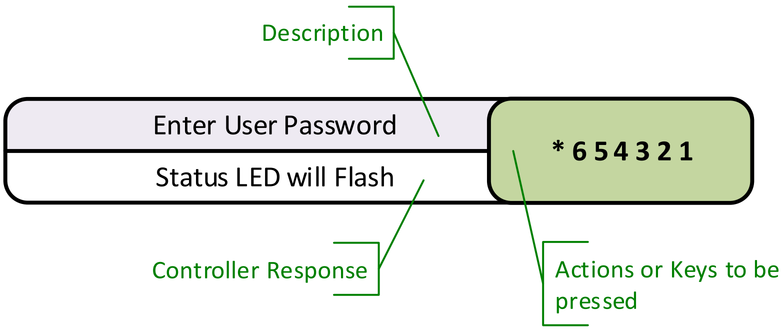
Two Door Version

The “two door” version simply contains two access controllers in one enclosure. Both controllers can be programmed from the front panel keyboard but first the user needs to choose which controller to program.

To select control panel A (or door 1) press the **[#]** and **[1]** key <u>together</u>. The controller will beep and the ‘Control ‘A’ selected’ LED will illuminate.

To select control panel B (or door 2) press the **[#]** and **[2]** key <u>together</u>. The controller will beep and the ‘Control ‘B’ selected’ LED will illuminate.

Programming Flow Diagrams



User Menu

The User Menu is accessed by entering * followed by the User Password. The default for this is 654321.

User Menu #	Description	Default Value
* 00	User Password	6 5 4 3 2 1
* 01	Access Code	None
* 02	Discover Presented Cards	-
* 03	Forget Presented Cards	-
* 04	Add Card by Number	-
* 05	Remove Card by number	-
* 10	Add Bio Administrator Rights	-
* 11	Remove Bio Administrator Rights	-
* 14	Add / Update Template (Enrol)	-
* 15	Delete Bio Template	-
* 16	Edit Bio Slot to ID Table	-
* 22	Copy Templates	-

User Password

Passwords are the means by which the systems operator gains access to the programming functions. This is a 6-digit number and can be changed by using the following procedure.

Changing the user password

This example shows the password changed to 234567.

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select “User Password” menu	* 0 0
Enter the new Password	2 3 4 5 6 7
Enter the new Password again	2 3 4 5 6 7
Complete & Exit Programming Mode Status LED will stop Flashing	#

Default Value:

- 654321

The factory default can be restored by a “Full Reset” or by connecting the PWR input to 0V for 4 seconds.

Related Engineer Menus:

- 00 “Engineer Password”

Progeny
Access Control

Access Code

Programming the Access Code

User Function 01

The P4 controller has a single access code that can be programmed. The access code can be any number of digits from 1 to 8. The access code is only active when the keyboard is in “Normal Keyboard Mode”.

See Engineer Function 20 for more details

If more than one access code is needed see “Virtual Card” modes for the keyboard.

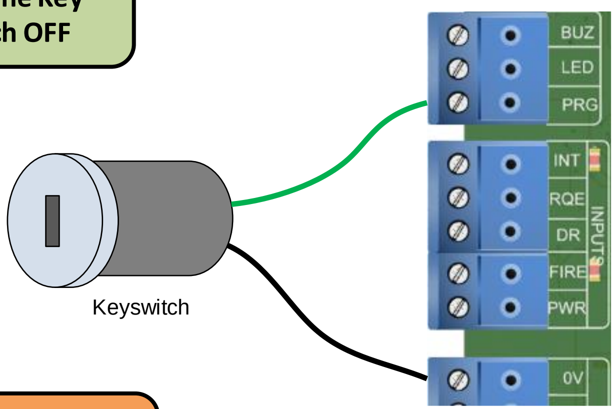
Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Single Access Code	* 0 1
Enter the required Access Code	1 2 3 4
Complete & Exit Programming Mode Status LED will stop Flashing	#

Start After 4 seconds Status LED will Flash	Turn The Key Switch ON
Enter the required Access Code	4 5 6 7 8 9
Complete Status LED will stop Flashing	Turn The Key Switch OFF

Key Switch Programming

Key switch programming makes changing the access code very simple and quick.

The P4 controller has an input labelled “PRG”. This can be wired to a simple key switch (Normally Open Contacts). When the key switch is turned the controller will take the next key sequence as the new access code.



Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Clear Access Code” menu	* 9 8
Complete & Exit Programming Mode Status LED will stop Flashing	#

Removing the Access Code

Engineer’ function 98 will erase the access code.

Cards & Fobs

Adding Cards by Presentation (Discover)

User function 02

Make sure you have the correct reader technology selected for the readers that are connected before using this function.

All cards presented to the reader will be remembered and given access.

Related User Menus:

- 03 “Forget Cards”
- 04 “Add Card”
- 05 “Disable Card”

Related Engineer Menus:

- 04 “Reader A Technology”
- 05 “Reader B Technology”
- 20 “Keyboard Mode”
- 11 “Random Search
- 20 “Keyboard Mode”
- 31 to 36 “Feedback Volume Control”

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Discover Card Menu	* 0 2
Present Cards one after another	**Present Card**
Complete & Exit Programming Mode Status LED will stop Flashing	#

Removing Cards by Presentation (Forget)

User function 03

This is the reverse of the Discovery Mode. The cards presented to the reader will be removed from memory and will report as “Unknown Card” if access is attempted.

If you simply need to disable a card use menu function 5.

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Forget Card Menu	* 0 3
Present Cards one after another	**Present Card**
Complete & Exit Programming Mode Status LED will stop Flashing	#

Adding Cards by Number

Adding or enabling credentials by entering the Card ID can be useful when the credentials themselves are not available or if a large number of credentials need to be added.

Single Card:

Note that some cards have a serial number printed on them. This should be used with the cross-reference list, provided with cards, to determine the actual card number.

This example will enable a single card numbered 80230001.

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select "Add Card ID" Menu	* 0 4
Enter Card ID	8 0 2 3 0 0 0 1
Complete & Exit Programming Mode Status LED will stop Flashing	#

Block of Cards

The quickest way to enable a whole group of cards is to use the block add method shown in this flow diagram.

This example will enable 50 cards, Site code 8023 from card 0001 to 0050.

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select "Add Card ID" Menu	* 0 4
Enter Card ID	8 0 2 3 0 0 0 1
Enter *as a separator	*
Enter Quantity (1 to 9999)	50
Complete & Exit Programming Mode Status LED will stop Flashing	#

Related User Menus:

- 02 "Discover Cards"
- 03 "Forget Cards"
- 05 "Remove Card"

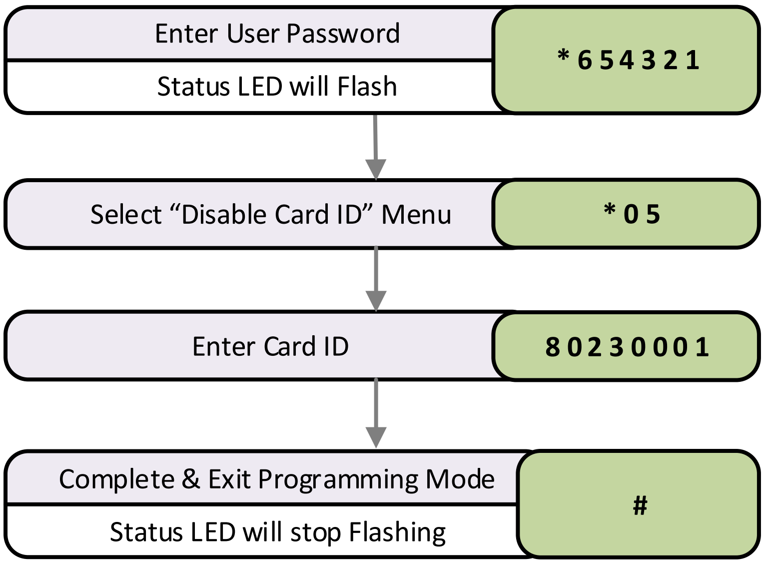
Related Engineer Menus:

- 04 "Reader A Technology"
- 05 "Reader B Technology"
- 11 "Random Search
- 20 "Keyboard Mode"
- 31 to 36 "Feedback Volume Control"

Disabling Cards by Number

Single card

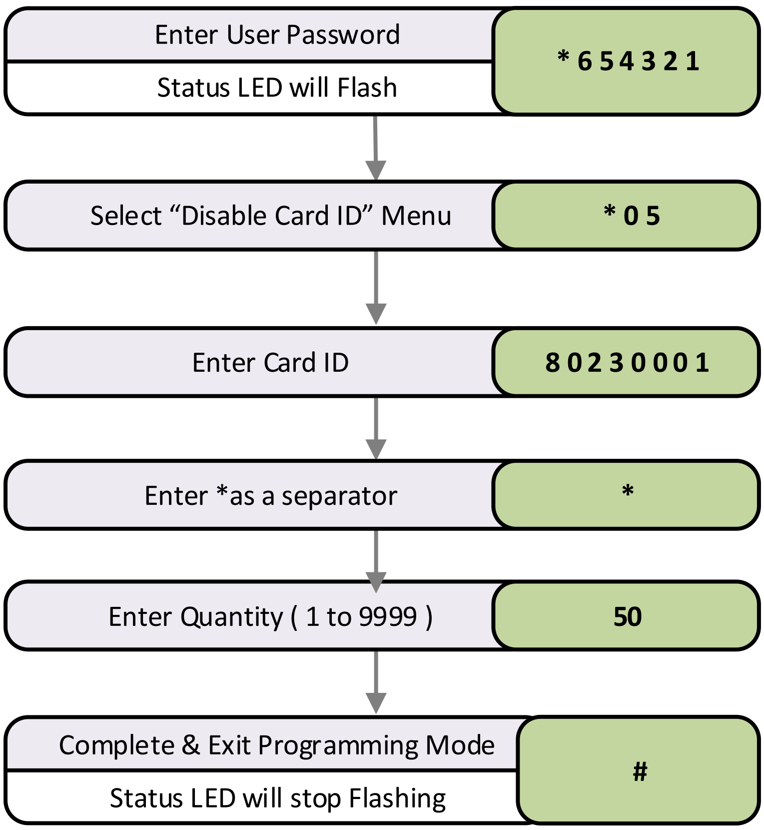
If a card is reported lost or stolen, the card can be disabled to remove the security risk without affecting any other card users.



Block of cards

The quickest way to disable a whole group of cards is to use the "Block Disable" method shown in this flow diagram.

This example will disable 50 cards, Site code 8023 from card 0001 to 0050.



Related User Menus:

- 02 "Discover Cards"
- 03 "Forget Cards"
- 04 "Add Card"

Related Engineer Menus:

- 04 "Reader A Technology"
- 05 "Reader B Technology"
- 20 "Keyboard Mode"
- 11 "Random Search"
- 20 "Keyboard Mode"
- 31 to 36 "Feedback Volume Control"

Add Administrator Rights to Card ID

User function 10

To allow a particular card holder to manage biometric enrolment using the "Gesture" method with mirror cards.

Related User Menus:

- 11 "Remove Bio Admin"
- 15 "Delete Bio Template"

Related Engineer Menus:

- 21 "List Templates"
- 22 "Copy Templates"
- 23 "Delete Templates"
- 59, 79 "Multi Factor Control"

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select "Add Bio Admin Right"	* 1 0
Enter the ID of the user or Present a card with this ID	80230001
Complete & Exit Programming Mode Status LED will stop Flashing	#

Remove Administrator Rights to Card ID

User function 11

This function removes the permission to manage Biometric Enrolment.

Related User Menus:

- 10 "Add Bio Admin"
- 15 "Delete Bio Template"

Related Engineer Menus:

- 21 "List Templates"
- 22 "Copy Templates"
- 23 "Delete Templates"
- 59, 79 "Multi Factor Control"

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select "Remove Bio Admin Right"	* 1 1
Enter the ID of the user or Present a card with this ID	80230001
Complete & Exit Programming Mode Status LED will stop Flashing	#

Start Biometric Template Enrol / Re-Enrol

User function 14

This function starts the Biometric Enrolment process at the door. It requires a Slot number to be specified.

Uses templates are stored in “slots” numbered 0 to 999 for the right hand and 1000 to 1999 for the left hand.

Each user is allowed two slots one for the right hand the other for the left. If Slot number “456” is selected for a user’s right hand then the slot for the left, is simply +1000; in this case “1456”.

Related User Menus:

- 10 “Add Bio Admin”
- 11 “Remove Bio Admin”
- 15 “Delete Bio Template”
- 16 “Edit Template ID”

Related Engineer Menus:

- 21 “List Templates”
- 22 “Copy Templates”
- 23 “Delete Templates”
- 59, 79 “Multi Factor Control”

Enter User Password Status LED will Flash	*** 6 5 4 3 2 1**
Select “Start Biometric Enrol”	*** 1 4**
Enter the biometric slot number	**902**
Complete & Exit Programming Mode Biometric Sensor will Light Blue	**#**
Present the Subject Finger Short Beep and Strobe flash	(Sample 1)
Present the Subject Finger Short Beep and Strobe flash	(Sample 2)
Present the Subject Finger Confirm Tone and Strobe flash	(Sample 3)

Progeny
Access Control

Del Biometric Template

User function 15

Access control for Biometric transactions is simply controlled by the alias ID of the template. However, it may still be required to remove the template of a user from the system.

For standalone operation this can be done from a connected keypad.

The slot number of the template to be deleted are required for this operation.

Related User Menus:

- 10 “Add Bio Admin”
- 11 “Remove Bio Admin”
- 14 “Start Bio Enrol”
- 16 “Edit Template ID”

Related Engineer Menus:

- 21 “List Templates”
- 22 “Copy Templates”
- 23 “Delete Templates”
- 59, 79 “Multi Factor Control”

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select “Delete Biometric Template”	* 1 5
Enter Slot Number	902
Complete & Exit Programming Mode Status LED will stop Flashing	#

Edit ID of Bio Template

User function 16

Each biometric template has an Alias ID. By default, this is the same as the slot number. So slot number 902 will have an alias ID of “00000902”. This can be modified to any 8-digit number.

This can be helpful for those systems using both card and biometric readers. Users can have the same ID if they use a card as when they use biometric authentication.

The ID number and the slot number are required for this operation.

Related User Menus:

- 10 “Add Bio Admin”
- 11 “Remove Bio Admin”
- 14 “Start Bio Enrol”
- 15 “Delete Bio Template”

Related Engineer Menus:

- 21 “List Templates”
- 22 “Copy Templates”
- 23 “Delete Templates”
- 59, 79 “Multi Factor Control”

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select “Edit Biometric ID”	* 1 6
Enter New ID	8 0 2 3 0 0 0 1
Enter *as a separator	*
Enter Bio Slot Number (0 to 1999)	902
Complete & Exit Programming Mode Status LED will stop Flashing	#

Progeny
Access Control

Copy Single Template

User function 22

Biometric templates can be copied from reader to controller or from controller to reader.

Once initiated the reader will change from Blue to Red for a few seconds during the data transfer.

Related User Menus:

- 10 “Add Bio Admin”
- 11 “Remove Bio Admin”
- 14 “Start Bio Enrol”
- 15 “Delete Bio Template”
- 16 “Edit Template ID”

Related Engineer Menus:

- 21 “List Templates”
- 22 “Copy Templates”
- 23 “Delete Templates”
- 59, 79 “Multi Factor Control”

Enter User Password Status LED will Flash	* 6 5 4 3 2 1
Select “Copy Biometric Template”	* 2 2
Select Direction: • 1 = Controller to Reader A • 2 = Controller to Reader B • 3 = Controller to Reader A & B • 51 = Reader A to Controller • 52 = Reader B to Controller	1
Enter *as a separator	*
Enter Bio Slot Number (0 to 1999)	902
Complete & Exit Programming Mode Status LED will stop Flashing	#

Progeny
Access Control

Engineer Menu

Engineer Menu #	Description	Range	Default Value
*** 00**	Password	000000 to 999999	1 2 3 4 5 6
*** 01**	Delay to Lock Release	0 to 99 Sec	0
*** 02**	Lock Release Duration	0 to 99 Sec	3
*** 03**	PDO Time	0 to 99 Sec	0 = Off
*** 04**	Reader A technology	0 to 99	0 (P4 4 Wire)
*** 05**	Reader B technology	0 to 99	0 (P4 4 Wire)
*** 06**	Duress	1= On, 0 =Off	0 = Off
*** 07**	Relay “B” mode	0 to 12	0 (follow relay A)
*** 08**	Timer for “B” relay	0 to 99 Sec	3
*** 09**	Penalty Time	0 to 99 Sec	0
*** 10**	Hacker Count	0 to 99	0
*** 11**	Random Search Rate	0 to 99	0 (Off)
*** 12**	Unlock Time Zone	0 to 64 (250)	65
*** 14**	Lock Drive Mode	0 to 4	0 (Relay Only)
*** 15**	Auto Relock on Door Close	1= On, 0 =Off	0 (Off)
*** 16**	Clear Event Log	749162	-
*** 17**	Clear Card Data	749162	-
*** 18**	Network Security	0 to 1	0 (DE V7.01.x)
*** 19**	External keyboard * mode	0 to 1	0 = (Disabled)
*** 20**	Keyboard Mode	0 to 8	0 (Access Code)
*** 21**	List Bio Templates	0	-
*** 22**	Copy Bio Template	0, 1, 2, 51, 52, 53, 91, 92	-
*** 23**	Delete Bio Template	1, 2, 3, 4 ,5	-
*** 24**	Bio Slot to ID Entry	-	-
*** 25**	Reader A APB Configuration	0 to 3	0
*** 26**	Reader B APB Configuration	0 to 3	0
*** 27**	Relay B Time Zone	0 to 64 (250)	65
*** 28**	2nd Stage Delay	0	0
*** 29**	Network Transmit Delay	0 to 99	10
*** 30**	Controller Mode	3	3
*** 31**	Alarm Sound Volume Controller	0 to 15	15
*** 32**	Feedback Volume Controller	0 to 15	8
*** 33**	Alarm Volume Reader A	0 to 15	15
*** 34**	Feedback Volume Reader A	0 to 15	8
*** 35**	Alarm Volume Reader B	0 to 15	15
*** 36**	Feedback Volume Reader B	0 to 15	8
*** 40 to 54**	Custom Reader Template A	-	-
*** 56**	Prefix code for reader A	0000 to 9999	0000
*** 58**	Status Light Brightness Reader A	0 to 9	5
*** 59**	ID Factor Sequence A	-	-
*** 60 to 74**	Custom Reader Template B	-	-
*** 76**	Prefix code for reader B	0000 to 9999	0000
*** 78**	Status Light Brightness Reader B	0 to 9	5

*** 79**	ID Factor Sequence A	-	-
*** 80**	IP Address	0.0.0.0 to 255.255.255.255	0.0.0.0
*** 81**	Gateway IP address	0.0.0.0 to 255.255.255.255	0.0.0.0
*** 82**	Net mask (Host Bit Count)	0.0.0.0 to 255.255.255.254	255.255.255.0
*** 84**	Server IP Address	0.0.0.0 to 255.255.255.254	0.0.0.0
*** 97**	Factory Reset IP Settings	-	192.6.32.200
*** 98**	Clear Access Code	-	-
*** 99**	Reset User Password	-	654321

Lock Delay Time

Lock delay time is the amount of time before the locking device is released following a valid card or the triggering of the RQE input. This may be from 0 to 99 seconds.

Programming the Lock Delay Time

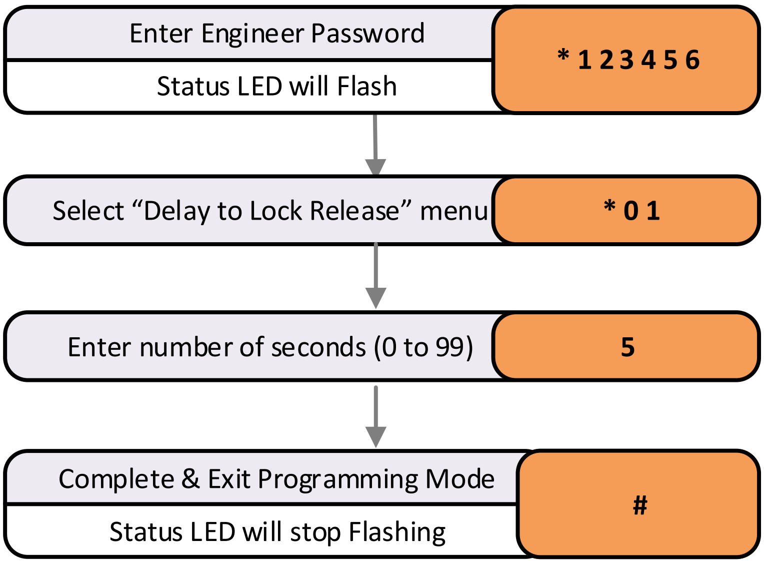
This example will change the “delay to lock release” to 5 seconds.

Default Value:

- 0 Seconds

Related Engineer Menus:

- 02 “Lock Release Time”



Lock Release Time

Lock time is the amount of time that the locking device is released following a valid card or the triggering of the RQE input. This may be from 0 to 99 seconds. If a door sensor is fitted then the auto relock feature means that the lock time will be cut short once the door closes again.

Programming the Lock Release Time

Default Value:

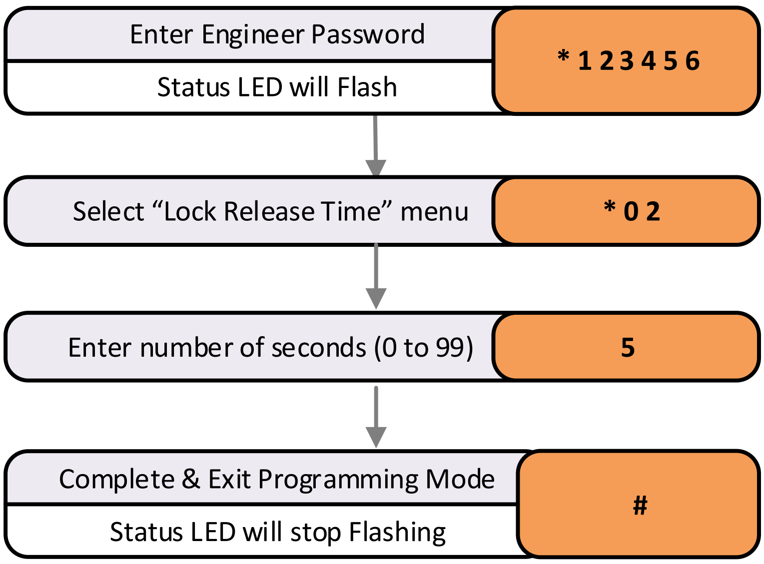
- 3 Seconds

Related Engineer Menus:

- 01 “Delay to Lock Release”
- 15 “Auto Relock on Door Close”

Toggle Mode

If the lock time is set to zero the lock output will be in “Toggle Mode”. In this mode: each time a valid card is presented or correct code is entered, the output relay will “Toggle” to the opposite state and stay that way.



Door Failed to Close Alarm (PDO)

Previously known as “PDO” alarm. There are connections on the control unit to allow the monitoring of the door open status. This value is the amount of time the door may be open before triggering an audible alarm from the control unit. This may be from 0 to 99 seconds. If this is set to zero, the PDO alarm is disabled.

Programming PDO Time

Pressing 7 and 8 together will mute the integral PDO alarm sounder. This does not affect the PDO alarm output. The PDO will however re sound on the next alarm occurrence. To disable the PDO sound and output permanently, program the PDO time to zero.

Enter Engineer Password Status LED will Flash	*** 1 2 3 4 5 6**
Select “Failed to Close Timer” menu	*** 0 3**
Enter number of seconds (1 to 99)	**15**
Complete & Exit Programming Mode Status LED will stop Flashing	**#**

Reader A & B Technology

The reader technology code allows different types of card readers and cards to be used. Each card reader input can have its own technology setting.

Code	Template	Notes
0	Crystal Reader	Native Bidirectional 4 wire Interface
1	ISO 15693	ISO 15693 (Tagit 64) (Firmware 4.30+)
2	Progeny Prox	Standard Progeny HID format for Prox & iCLASS
3	26 bit (8 + 14)	General 26 bit Max Card ID = 9999
4	26 bit (8 + 16)	Extended 26 bit Wiegand Max Card ID = 65535
5	MIFARE A	MIFARE CSN 8 + 16
6	MIFARE B	MIFARE CSN 16 + 16
7	Corporate 1000	Use Engineer 56 & 76 to set the ID for Reader A & B
8	Tech 8	Not Used by P4 Controllers
9	Progeny Magstripe	For use with Progeny Scrambled Magstripe Cards Only
10	Royal Mail	
11	8 Digit C & D	General clock & data
12	Lobby Entry	Uses the Most Significant 4 Digits as the Card ID
15	BSBELE (Hughs)	TECH 15 for P4 controllers

Programming Reader Technology A

Crystal readers

These are connected using the 4 wire method. Select Template 0.

Progeny iCLASS readers

Most commonly uses Template 2 “Progeny Prox”

Progeny HID Pox readers

Most commonly uses Template 2 “Progeny Prox”

- Enter Engineer Password / Status LED will Flash: * 1 2 3 4 5 6
- Select “Reader A Template” menu: * 0 4
- Enter code for required template: 11
- Complete & Exit Programming Mode / Status LED will stop Flashing: #

Programming Reader Technology B

Crystal readers

These are connected using the 4 wire method. Select Template 0.

Progeny iCLASS readers

Most commonly uses Template 2 “Progeny Prox”

Progeny HID Pox readers

Most commonly uses Template 2 “Progeny Prox”

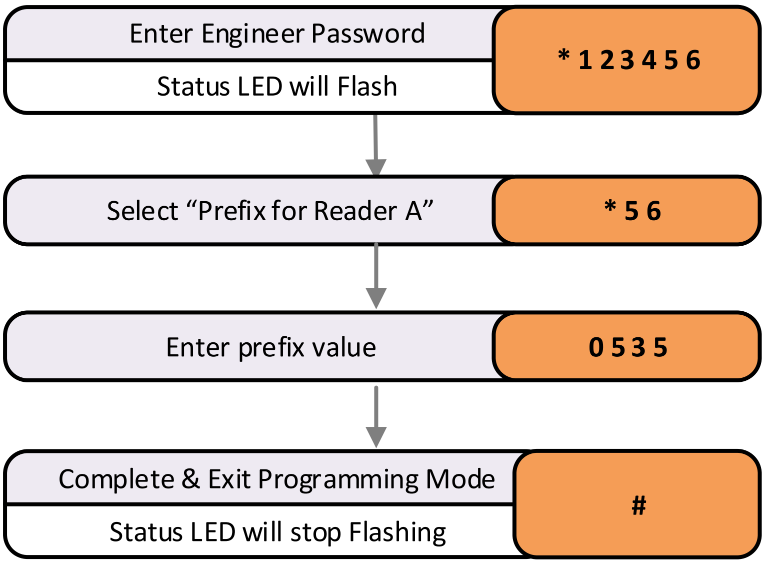
- Enter Engineer Password / Status LED will Flash: * 1 2 3 4 5 6
- Select “Reader B Template” menu: * 0 5
- Enter code for required template: 11
- Complete & Exit Programming Mode / Status LED will stop Flashing: #

Corporate ID

This function sets up the Corporate ID code for HID Corporate 1000 format cards. This works in conjunction with technology 7, which must be selected in order for this format to operate correctly.

Example 1:

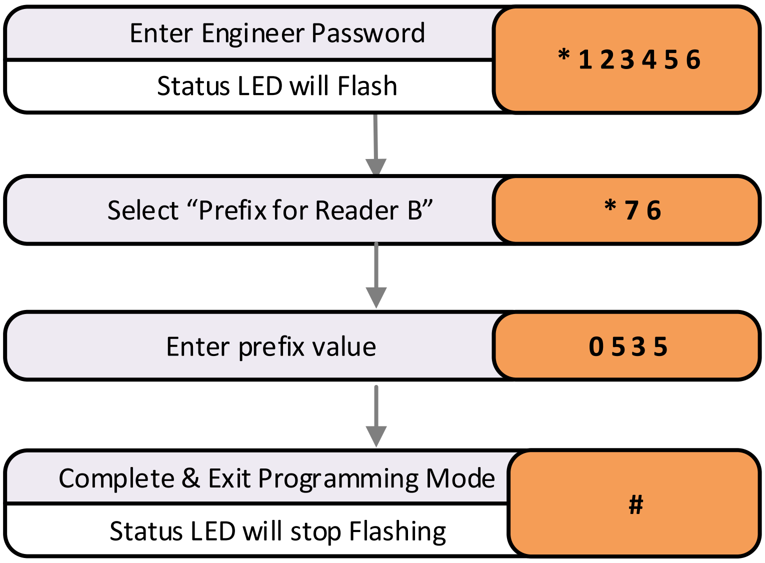
Sets up reader A to check the prefix 0535 for corporate 1000.



Example 2:

Sets up reader B to check the prefix 0535 for corporate 1000.

Without these values set, the card will report as "Unknown Card".



Duress Feature

If the duress feature is turned on, a duress alarm is generated when a modified access code is entered. To modify the access code to a “Duress Access Code” just increment the last digit of the “Normal Access Code. For example, if your access code is “1 2 3 4” then if you enter “1 2 3 5” the door will be released as normal but also the duress alarm output will go active and latch. If the last digit is 9 then rap around to 0.

A duress alarm can only be cancelled by entering the valid User / Engineer password or by presenting a valid card. While this feature is turned on each access code has a shadow thus doubling the number of valid access codes.

Programming Duress Feature

Range of Values:

- 0 = Off
- 1 = On

Default Value:

- 0 = Off

Related Engineer Menus:

- 01 Access Code

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Duress Feature” menu	* 0 6
Enter 1 to Enable or 0 to Disable	1
Complete & Exit Programming Mode Status LED will stop Flashing	#

Relay B Mode

Relay B can be configured to perform a number of different roles. By default, the relay simply mimics the lock relay and allows loads to be driven or provide voltage free contacts for other equipment such as Barriers, Turnstiles etc.

Code	Behaviour
0	Follow Lock Output
1	Future Use
2	Follow Door Forced
3	Follow Duress
4	Follow Hacker
5	Follow PDO
6	Follow Random Search
7	Follow Fire Input
8	Follow Intruder Input
9	PC Controlled
10	Follow Time Zone
11	Two Stage Lock Release
12	Turnstile Mode

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Relay B Mode” menu	* 0 7
Enter code for function required	1
Complete & Exit Programming Mode Status LED will stop Flashing	#

Programming the Relay B Mode

Relay B Timer

Lock time is the amount of time that the locking device is released. This may be from 0 to 99 seconds. If this value is set to zero, then each time the channel is triggered the relay will “Toggle” to the opposite state.

Programming the Relay B Timer

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Relay B Timer” menu	* 0 8
Enter number of seconds (0 to 99)	3
Complete & Exit Programming Mode Status LED will stop Flashing	#

Penalty Time

This feature can slow down persons who are trying to gain access by using successive codes. As soon as an incorrect code is detected at the keyboard this penalty time is invoked, preventing any further access attempts until the timer elapses.

Programming the Penalty Time

The factory set default penalty time is 0 seconds (Disabled).

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Hacker Count” menu	* 1 0
Enter maximum consecutive errors	3
Complete & Exit Programming Mode Status LED will stop Flashing	#

Hacker Output

Persons trying to gain access by trying successive codes can be detected and an alarm raised via the Hacker output. The controller will count consecutive errors and when this predetermined value is reached the alarm is generated. This alarm is latching and can only be reset by someone who knows the password. See "Resetting alarm" later in this manual.

TO CHANGE THE HACKER COUNT

The factory set default hacker count is 0 (Disabled)

Enter Engineers Password Status LED will Flash	*** 1 2 3 4 5 6**
Select "Hacker Count" menu	*** 1 0**
Enter maximum consecutive errors	**3**
Complete & Exit Programming Mode Status LED will stop Flashing	**#**

Random Search

It is sometimes necessary to carry out random searches on staff as they enter of leave a site that is sensitive or has high value items.

This feature signals when a random search should be done. This removes any possible "Collusion" or "Prejudice" to be levelled at the personnel carrying out the searches.

The Hacker Alarm output is used to signal the search.

Programming Random Search Feature

The value entered using this Engineer function sets the average rate that searches will be signalled.

- 0 = Off
- 1 = 1:1
- 99 = 1:99 1 in 99 accesses

Default Value:

- 0 = Off

Related Engineer Menus:

- 07 "Relay B Mode"

Enter Engineer Password Status LED will Flash	*** 1 2 3 4 5 6**
Select "Random Search Rate" menu	*** 1 1**
Enter the Rate required (1 in x)	**10**
Complete & Exit Programming Mode Status LED will stop Flashing	**#**

Lock Drive Mode

The lock drive from a P4 controller has the conventional Relay driven output that switches positive supply to the locking device. However, it also has a new electronic drive that switches the negative supply to the lock.

The electronic switch option has the advantage of needing less power and having no moving parts.

Note: in electronic modes the Lock LED will flash when the lock is released

Range of Values:

Mode 0 = Relay Only
Mode 1 = Electronic VR
Mode 2 = Electronic VA
Mode 3 = Protected Relay

Default Value:

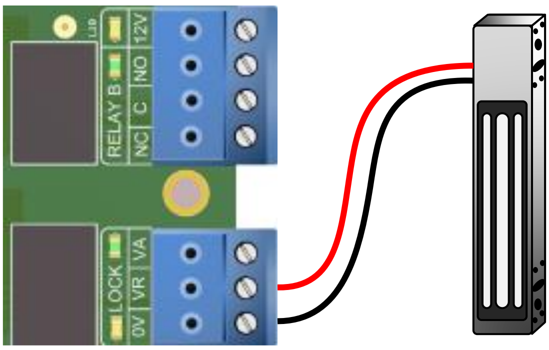
- 0 = Relay Only

Related Engineer Menus:

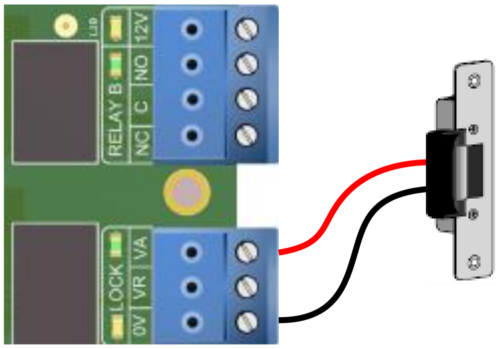
- 01 Delay to Lock Release
- 02 Lock Release time

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select "Lock Drive Mode" menu	* 1 4
Enter Code for desired mode	2
Complete & Exit Programming Mode Status LED will stop Flashing	#

Relay Modes 0 & 3

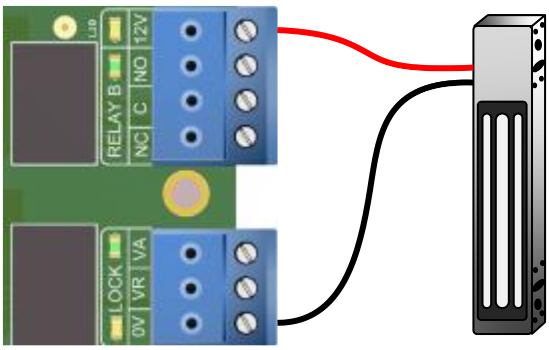


Fail Open

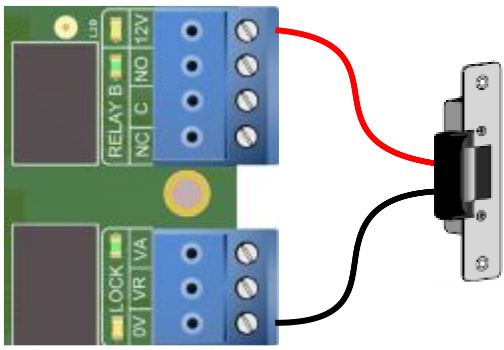


Fail Secure

Electronic Modes 1 & 2



Fail Open



Fail Secure

Auto Relock

This function is used to control the behaviour of the controller after the door sensor input detects that the door is opened and closed after a valid lock release. If enabled, the door will be automatically locked once the door is closed, effectively shortening the lock release time.

Programming Auto Relock Feature

This example flow diagram shows the "Auto Relock" feature being turned on.

Range of Values:

- 0 = Off
- 1 = On

Default Value:

- 0 = Off

Related Engineer Menus:

- 02 "Lock Release Time"

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select "Auto Relock" menu	* 1 5
Enter value (0 or 1)	1
Complete & Exit Programming Mode Status LED will stop Flashing	#

Clear Event Log

The P4 controller can store up to 8000 events in the event log. It can be useful in some cases to erase this data without affecting any other programming.

Engineer function 16 will clear the event log as long as the fixed verify code is entered as shown. The verify code prevents accidental use.

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select "Erase Logged Events" menu	* 1 6
Enter fixed verify code	7 4 9 1 6 2
Complete & Exit Programming Mode Status LED will stop Flashing	#

Progeny
Access Control

Clear Card Data

This function will erase all card pack data in the controller, and will reset the card pack count to zero.

N.B. Using this function will erase all card data from the controller.

Erase Card Data Function

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Clear Card Data” menu	* 1 7
Enter fixed verify code	7 4 9 1 6 2
Complete & Exit Programming Mode Status LED will stop Flashing	#

Network Security

This function selects the active protocol. The default value 0 selects Doors Enterprise 7.01.0xxx. When set to 1 it selects the more secure 7.02.xxxx. You must have Doors Enterprise V7.02 or higher installed to use this setting.

Network Security

Range of Values:

- 0 = V7.01.xxxx Legacy mode
- 1 = V7.02.xxxx or higher with improved security

Default Value:

- 0 = V7.01

Related Engineer Menus:

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Network Security” menu	* 1 8
Enter Security Level	1
Complete & Exit Programming Mode Status LED will stop Flashing	#

External Keyboard Star Key Mode

External keyboards are those connected to the Keyboard terminal block or Reader A or Reader B terminals. These keyboards can be used for programing in the same way that the engineer's keyboard is used. However, for additional security this can be stopped by disabling the "Star" key on those keyboards.

Values

0 = Disable

1 = Enable

Default Value

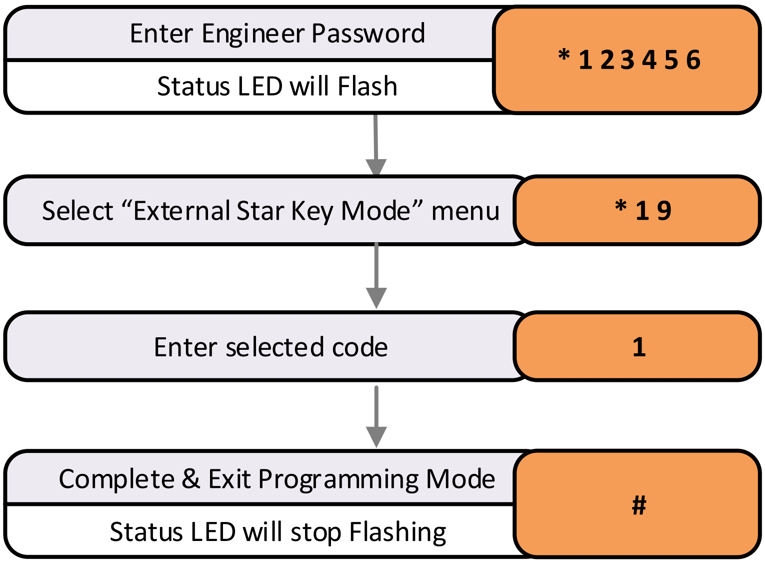
- 0 = Disabled

Related User Menus:

- 01 "Access Code"

Related Engineer Menus:

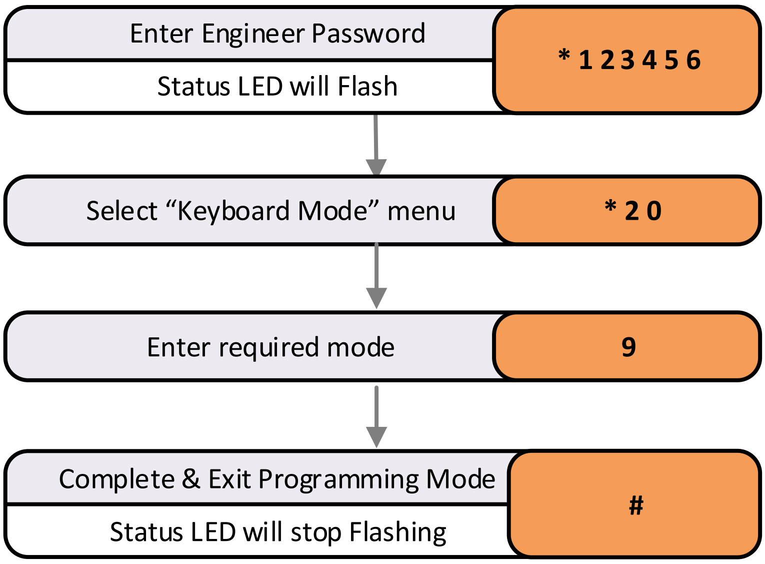
- 20 Keyboard Mode
- 98 Clear Access Code



Keyboard Mode

By default, the keyboards work as simple access code input. However, they can be used in number of different modes for access control.

Code	Behaviour
0	Normal Keyboard
4	Virtual Card (4 Digits)
5	Virtual Card (5 Digits)
6	Virtual Card (6 Digits)
7	Virtual Card (7 Digits)
8	Virtual Card (8 Digits)



Related User Menus:

- 01 "Access Code"

Related Engineer Menus:

- 19 External keyboard * mode
- 98 Clear Access Code

Reader A APB Configuration

This programming function will select the way in which a reader will affect and/or implement the anti-pass back feature.

Programming Reader A APB Configuration

APB Mode	Behaviour
0	No change to APB
1	Log Card In
2	Log Card Out
3	Enforce APB & Log Card In
4	Enforce APB & Log Card Out
5	Enforce APB In
6	Enforce APB Out

Enter Engineer Password Status LED will Flash	*** 1 2 3 4 5 6**
Select "Reader A APB" menu	*** 2 5**
Enter required mode	**1**
Complete & Exit Programming Mode Status LED will stop Flashing	**#**

Reader B APB Configuration

This programming function will select the way in which a reader will affect and/or implement the anti-pass back feature.

Programming Reader B APB Configuration

APB Mode	Behaviour
0	No change to APB
1	Log Card In
2	Log Card Out
3	Enforce APB & Log Card In
4	Enforce APB & Log Card Out
5	Enforce APB In
6	Enforce APB Out

Enter Engineer Password Status LED will Flash	*** 1 2 3 4 5 6**
Select "Reader B APB" menu	*** 2 6**
Enter required mode	**2**
Complete & Exit Programming Mode Status LED will stop Flashing	**#**

Two Stage Lock Release Interval

When relay B is set for “Two Stage Lock Release” (See Engineer 07) this function sets the interval between “Relay A (Lock Relay)” opening and “Relay B” operating. A two-digit number from 0 to 99 can be entered. This is multiplied by 10 milliseconds, thus a value of 25 would give a 250mS interval.

This can be useful when driving automatic door openers and locking the same door. Use Relay A to power the lock and relay B to trigger the opening device shortly after.

Programming the Two Stage Lock Release Interval

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Two Stage Interval” menu	* 2 8
Enter required time (x 10mS)	12
Complete & Exit Programming Mode Status LED will stop Flashing	#

Network Transmit Delay

The Network Transmit Delay is used to allow the controller to interface with USB to RS485 converters. The value entered will delay the controller from transmitting an RS485 network response for 1 ms x the value entered. 10 mS is the default.

Programming the Network Transmit Delay

Range of Values

0 to 99

Default Value

10

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Network Transmit Delay”	* 2 9
Enter value (1 to 99)	2
Complete & Exit Programming Mode Status LED will stop Flashing	#

Controller Mode

Mode 3 is the only currently valid and supported Mode. Do not change this. The current value is displayed on the blue Status LED. 3 flashes with a pause will be Mode 3.

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select "Controller Mode menu	* 3 0
Enter required Mode (1 to 4)	3
Complete & Exit Programming Mode Status LED will stop Flashing	#

Restoring Factory Settings

Reset Button

The reset button allows the engineer to perform a factory reset. This resets all parameters to the factory default values and removes all Cards, Access Levels, Time Zones, Calendars and the Access Code.

The reset button needs to be held for 4 seconds to start the reset sequence. All the LEDs on the PCB will go into lamp test mode during the reset sequence.

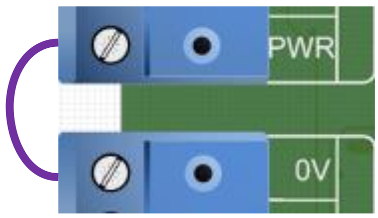
The Controller will now use the factory settings for all codes and timings. See defaults listed in the user and Engineer menu.

Note:

This will also remove all programmed cards and access codes. This procedure does not remove any IP address, Gateway or Subnet Mask values from the Ethernet port on the P4.net controller.

Password Reset

The "PassWord Reset" (PWR) input can be used to restore just the User & Engineer Password to factory defaults without affecting any other programming. Place a temporary link from PWR to 0V and hold it for 4 seconds. The Passwords will then be reset to:



- User: 654321
- Engineer: 123456

IP Address

NOTE: When programming IP parameters, unplug the Ethernet cable and the RS485 Network Terminal Block.

The IP address allows the Doors access control software to communicate with the P4.net controller and any P4 controllers connected to the (RS 485) P4 network. The IP address must be fixed and will be assigned by the network administrator.

Programming the IP Address

The number is usually represented in an "x.x.x.x" notation. When programming the IP address, use the * key to represent the decimal points. Each "x" will be a number from 0 to 255. A typical IP address would be 192.168.0.200, entered as 192*168*0*200.

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
↓	
Select "IP Address" menu	* 8 0
↓	
Enter value	192*168*0*56
↓	
Complete & Exit Programming Mode Status LED will stop Flashing	#

Gateway Address

The gateway or router address allows communication between LAN segments or subnets. The gateway address should be the IP address of the router connected to the same segment as the P4.net controller. The network manager should be able to supply this information.

Programming the Gateway Address

The gateway address is represented in an "x.x.x.x" notation as for the IP address. When programming, use the * key to represent the decimal points. Each "x" will be a number from 0 to 255. A typical IP address would be 192.168.0.1, entered as 192*168*0*1.

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
↓	
Select "Gateway Address" menu	* 8 1
↓	
Enter value	192*168*0*1
↓	
Complete & Exit Programming Mode Status LED will stop Flashing	#

Netmask

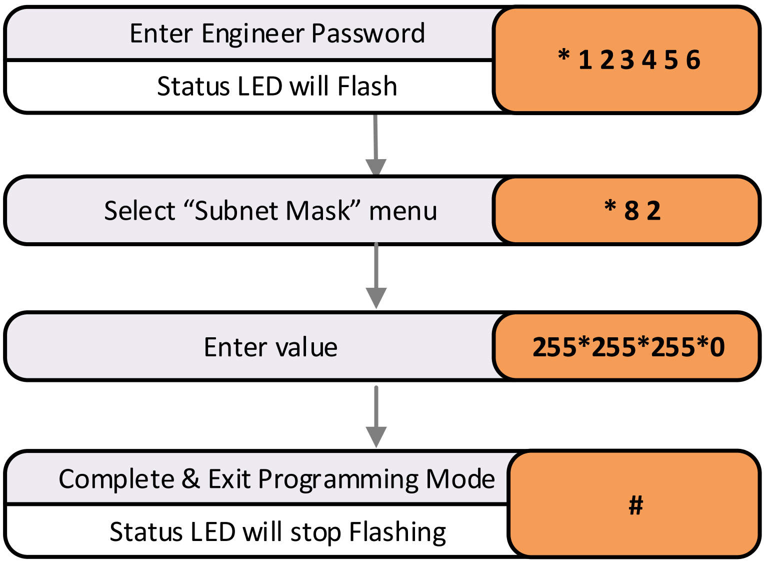
The IP address is a 32-bit binary number. The net mask divides the bits of the IP address into “Net” and “Host” parts. Normally the net mask is represented in the “x.x.x.x” notation, e.g. 255.255.255.0. The last number “0” represents the 8 zeros of the 32bit net mask.

The network manager should be able to supply the Subnet Mask required.

Programming the Netmask

Only certain values are valid for a Subnet Mask. The value being used or supplied by the network manager should be one of the following:

Class	Net-mask	Host Bits
C	255.255.255.254	1
C	255.255.255.252	2
C	255.255.255.248	3
C	255.255.255.240	4
C	255.255.255.224	5
C	255.255.255.192	6
C	255.255.255.128	7
C	255.255.255.0	8
B	255.255.254.0	9
B	255.255.252.0	10
B	255.255.248.0	11
B	255.255.240.0	12
B	255.255.224.0	13
B	255.255.192.0	14
B	255.255.128.0	15
B	255.255.0.0	16
A	255.254.0.0	17
A	255.252.0.0	18
A	255.248.0.0	19
A	255.240.0.0	20
A	255.224.0.0	21
A	255.192.0.0	22
A	255.128.0.0	23
A	255.0.0.0	24



Reader A Brightness Control

The Dark Crystal range have status light indication that can be made brighter or darker as the application demands. Mostly the default value is fine. However, in some un supervised locations it may attract the attention of vandals and it may be preferable to turn the brightness down to 0.

Values

- 0 = Off to 9 = 100%

Default Value

- 5 = Medium Bright

Related Engineer Menus:

- 78 Reader B Brightness
- 33 Reader A Volume
- 36 Reader B Volume

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select "Brightness Reader A"	* 5 8
Enter Value (0 = Off to 9 = 100%)	5
Complete & Exit Programming Mode Status LED will stop Flashing	#

Reader B Brightness Control

The Dark Crystal range have status light indication that can be made brighter or darker as the application demands. Mostly the default value is fine. However, in some un supervised locations it may attract the attention of vandals and it may be preferable to turn the brightness down to 0.

Values

- 0 = Off to 9 = 100%

Default Value

- 5 = Medium Bright

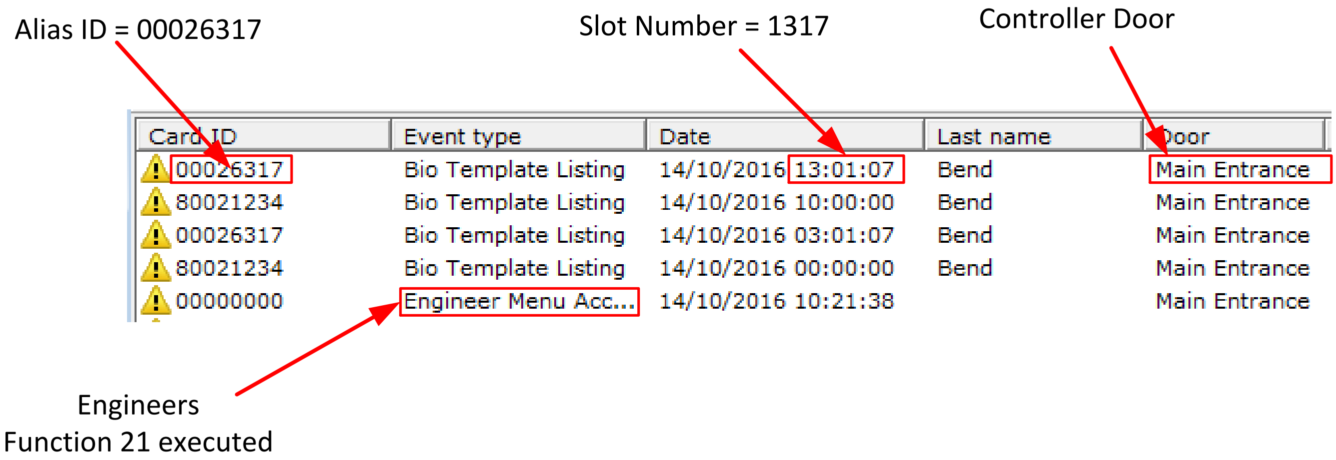
Related Engineer Menus:

- 58 Reader A Brightness
- 33 Reader A Volume
- 36 Reader B Volume

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select "Brightness Reader B"	* 7 8
Enter Value (0 = Off to 9 = 100%)	5
Complete & Exit Programming Mode Status LED will stop Flashing	#

List Templates

This is a diagnostic tool to read the template memory of the controller and report via the event log each template found. The results will only be seen in a live event viewer as shown below.



Card ID	Event type	Date	Last name	Door
00026317	Bio Template Listing	14/10/2016 13:01:07	Bend	Main Entrance
80021234	Bio Template Listing	14/10/2016 10:00:00	Bend	Main Entrance
00026317	Bio Template Listing	14/10/2016 03:01:07	Bend	Main Entrance
80021234	Bio Template Listing	14/10/2016 00:00:00	Bend	Main Entrance
00000000	Engineer Menu Acc...	14/10/2016 10:21:38		Main Entrance

Values

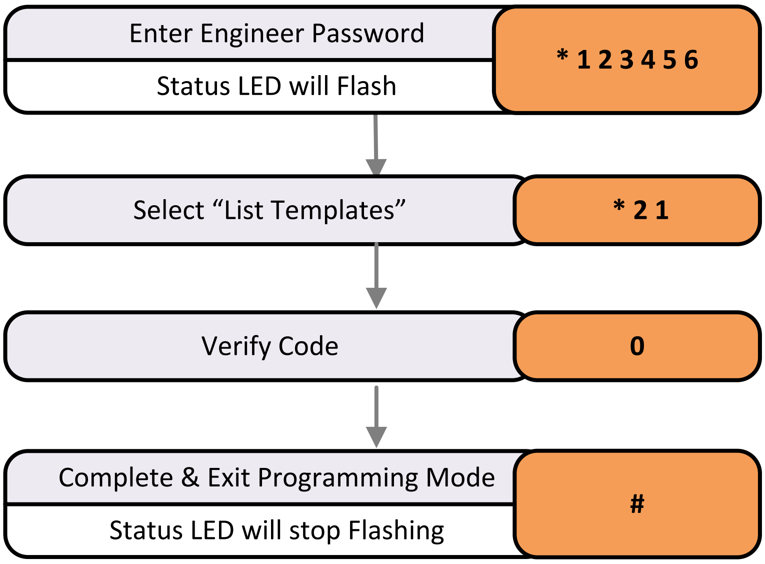
- 0 = Confirm

Related User Menus:

- 10 “Add Bio Admin”
- 11 “Remove Bio Admin”
- 14 “Start Bio Enrol”
- 16 “Edit Template ID”

Related Engineer Menus:

- 22 “Copy Templates”
- 23 “Delete Templates”



Copy Templates

It is possible to copy all the templates from a controller to a biometric reader and visa-versa.

Engineers function 22 starts this process running. It runs as a background process that can take a couple of hours to run. During this time, you may notice the biometric reader flash to red every few seconds.

To cancel the copy process, enter “0” as the direction.

Related User Menus:

- 10 “Add Bio Admin”
- 11 “Remove Bio Admin”
- 14 “Start Bio Enrol”
- 16 “Edit Template ID”

Related Engineer Menus:

- 21 “List Templates”
- 23 “Delete Templates”

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Copy Templates”	* 2 2
Select Copy Direction: 1 = Controller to Reader A 2 = Controller to Reader B 3 = Controller to Reader A & B 51 = Reader A to Controller 52 = Reader B to Controller 91 = Reader A to controller and Server 92 = Reader B to controller and Server 0 = Cancel Copy Process	2
Complete & Exit Programming Mode Status LED will stop Flashing	#

Delete Templates

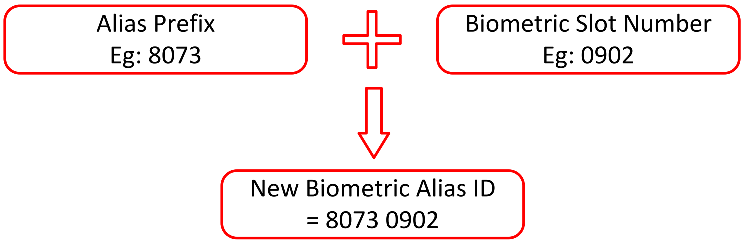
This function deletes all Biometric templates from a target device (Biometric Reader, or Controller).

Enter Engineer Password Status LED will Flash	* 1 2 3 4 5 6
Select “Delete Templates”	* 2 3
Target Device or Devices: 1 = Reader A 2 = Reader B 3 = Readers A & B 4 = Controller 5 = Controller, Reader A & B	1
Complete & Exit Programming Mode Status LED will stop Flashing	#

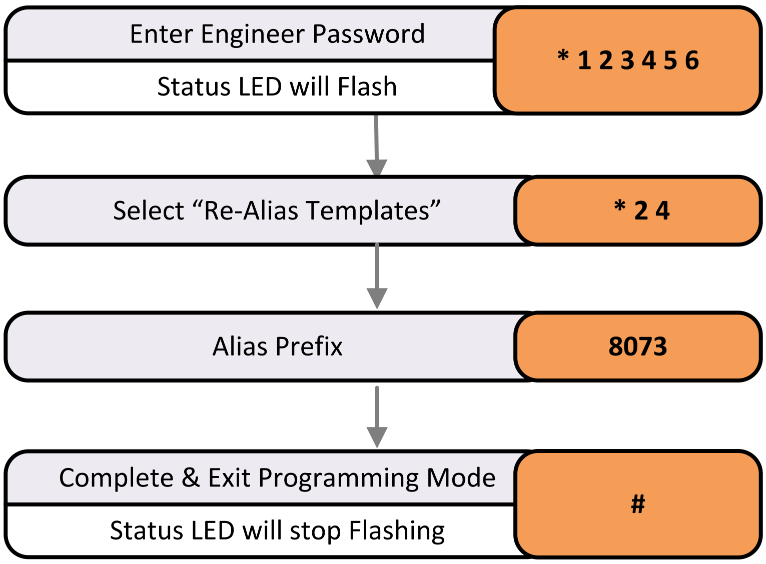
Re-Alias Template ID’s

The Biometric Alias ID is the Identification Number used for access control. When a finger is Identified or Verified, the Alias ID for that biometric slot is looked up and used for all access control decisions. When Enrolling online from Doors Enterprise or when using the Gesture Method these Aliases are already defined. However, if the stand alone keypad method is used to enrol then the default Alias ID is just the slot number.

This function allows the quick renumbering of the Biometric template alias ID’s. The function takes the Prefix and adds it to a 4-digit format of the slot number.



This is repeated for all the templates in the controller memory.



Sequential Multi Factor Authentication

This is a selection of authentication methods presented in a sequence. For example, to increase security on a door we could insist that all users to identify themselves using three factors. The three factors being:

1. An access code “Something you Know”
2. A valid card “Something you Have”
3. Biometric fingerprint “Something you Are”

The procedure would be one transaction and each has a Transaction ID.

Selecting Authentication Factors and Sequence

At Reader A or B (In or Out) there may be 1, 2, 3 or 4 authentication methods used via the same interface.

Giving separate control over Reader A & B allows for any combination of 1 to 4 factor in and/or out of a given door. Any unused factors in a sequence will be available as random access. For example, if we use 4 & 9 card verified by biometric then “access code” via the same keypad will be available if it is setup.

Engineers Functions:

- Engineers Function 59 ID Factors Reader A:
- Engineers Function 79 ID Factors Reader B:

Sequential Authentication function:

These functions accept up to 4 digits’ calculator style. Each digit represents an authentication Factor option from a Dark Crystal reader. The digit represents:

Authentication Digit	Method Required	Notes
0	Off	Any authentication method can be used in isolation
1	Access Code	Engineers 20 (1 = code), User 01 to Set Code
2	Virtual Card	Engineers 20 sets number of digits (4, 5, 6, 7 or 8)
3	PIN (4 Digit in card record)	Must be preceded by 2 or 4
4	Card / Fob	Physical Card ID
5	Not Used	For future use
6	Not Used	For future use
7	Not Used	For future use
8	Biometric Identification (1:N)	Any Valid Biometric ID
9	Biometric Verification (1:1)	Must be preceded by 2 or 4

Examples:

1 Factor:

Card Only just enter “4”. With a 4850 reader the biometric read is disabled.

1 Factor:

Biometric Only just enter “8”. With a 4850 reader the proximity read is disabled and the standby colour changes to pink.

2 Factor:

Valid Card followed by Code enter “4 1”. A valid card followed by the entry of the access code for that door will release the lock.

2 Factor:

Code followed by valid Card enter “1 4”

2 Factor:

Valid Card followed by valid Virtual Card enter “4 2”

2 Factor:

Valid Card followed by valid PIN enter “4 3”

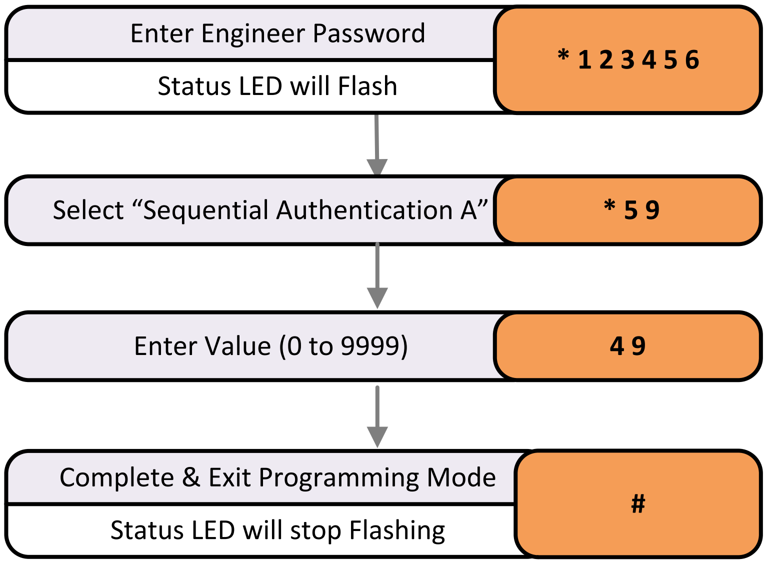
3 Factor:

Card followed by 4 Digit VC followed by Bio Verification enter “4 2 9”

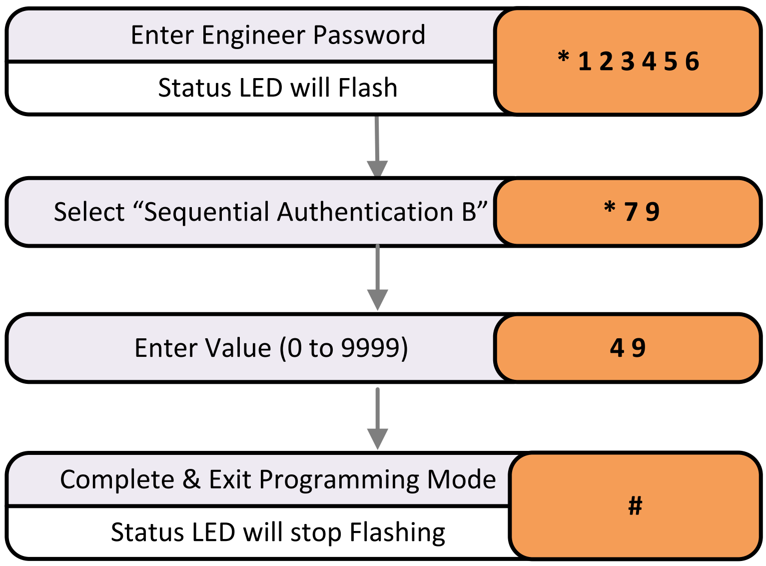
4 Factor:

Code followed by 6 Digit VC followed by Card followed by Bio Verify enter “1 2 4 9”

For Reader A



For Reader B



Engineer Password

The passwords are the means by which the commissioning engineer gains access to the programming functions. This is a 6-digit number and can be changed by using the following procedure.

Changing the Engineer Password

Default *123456

Enter Engineer Password Status LED will Flash	*123456
Select “Engineer Password” menu	*00
Enter the new Password	789789
Enter the new Password again	789789
Complete & Exit Programming Mode Status LED will stop Flashing	#

Reset User Password

It can be useful for the engineer to reset the user password. By entering the engineering menu and select function 99 the Users Password will be set to the new value.

Resetting the User Password

Enter Engineer Password Status LED will Flash	*123456
Select “Reset User Password” menu	*99
Enter the new User Password	234567
Enter the new User Password again	234567
Complete & Exit Programming Mode Status LED will stop Flashing	#

Progeny
Access Control

Installation

Safety Notes

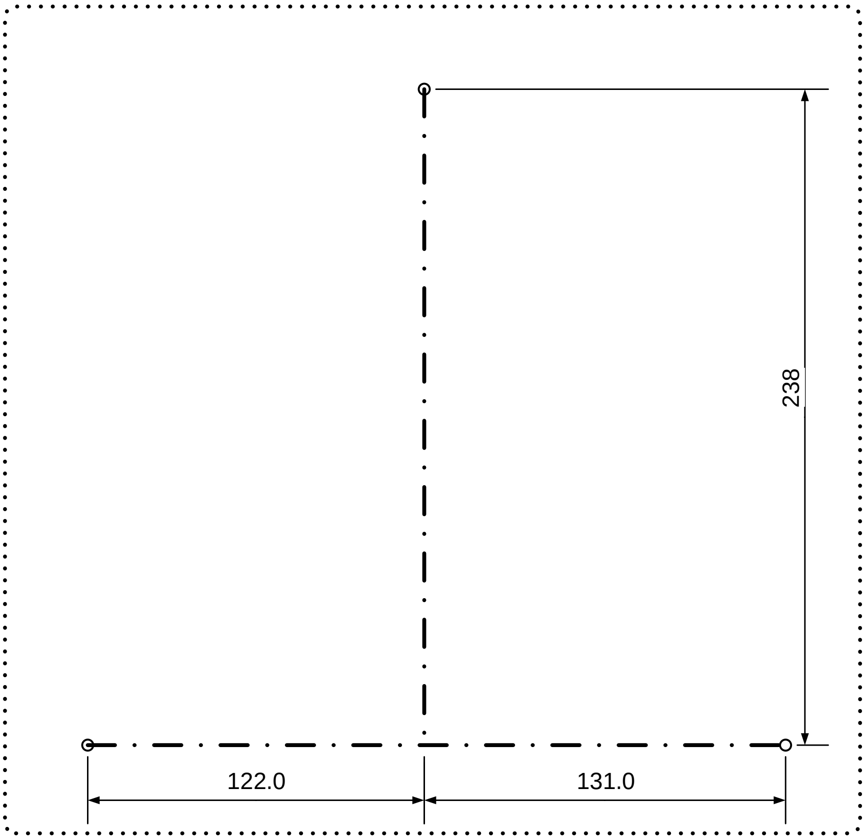
- Please read this manual carefully before attempting to install, program or operate the Progeny Access Control P4 equipment.
- This equipment must be installed in line with all relevant regulations and standards.
- Make sure that wiring is rated according to fuses and current limits of relevant power supplies.
- Apart from the mains supply, all connections to this unit must be SELV level. (Safety Extra Low Voltage as defined in BS EN 60950-1:2006)
- No users should access the inside of the control box. The control box contains hazardous voltages and access is limited to qualified personnel only. All user-programming for the controller is either done at one of the keyboards or at the PC.
- Every effort is made to ensure that this manual is complete and free from errors. However we reserve the right to make changes to these products and this manual without notice.
- No liability is accepted for loss damage or injury as a consequence of using these products or instructions.

Mounting

The optimum location for the controller depends on the application. As a general Guide:

- Always mount the control equipment on the secure side of the door.
- If the user needs to program the unit from the keyboard on the front panel, mount at head height in an accessible location with reasonable light.
- Mount as close as possible to the door(s) to be controlled (less than 100m).

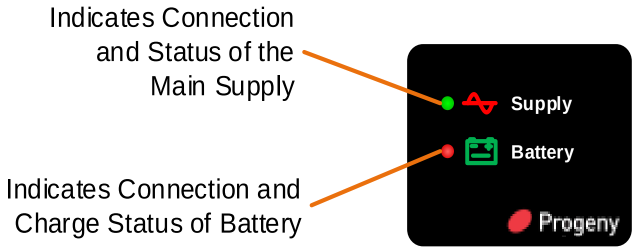
Drill & Plug the wall for three mounting screws to line up with the fixing dimples. Bring in mains supply and other cables that are to enter via the rear cable access holes. Screw the controller to the wall.



Mains Power

The P4 Controller should be connected to a 24 Hour 220V mains supply. A fused spur should be used for this purpose. The cable used to connect the mains supply should be 0.75 to 2mm^2. A fused terminal block is provided for mains; observe the polarity when making these connections.

WARNING: Extreme caution must be used when opening the controller housing. DO NOT touch any connections or components other than the reset button. Avoid touching any of the terminations with a metal object such as a wristwatch or jewellery.



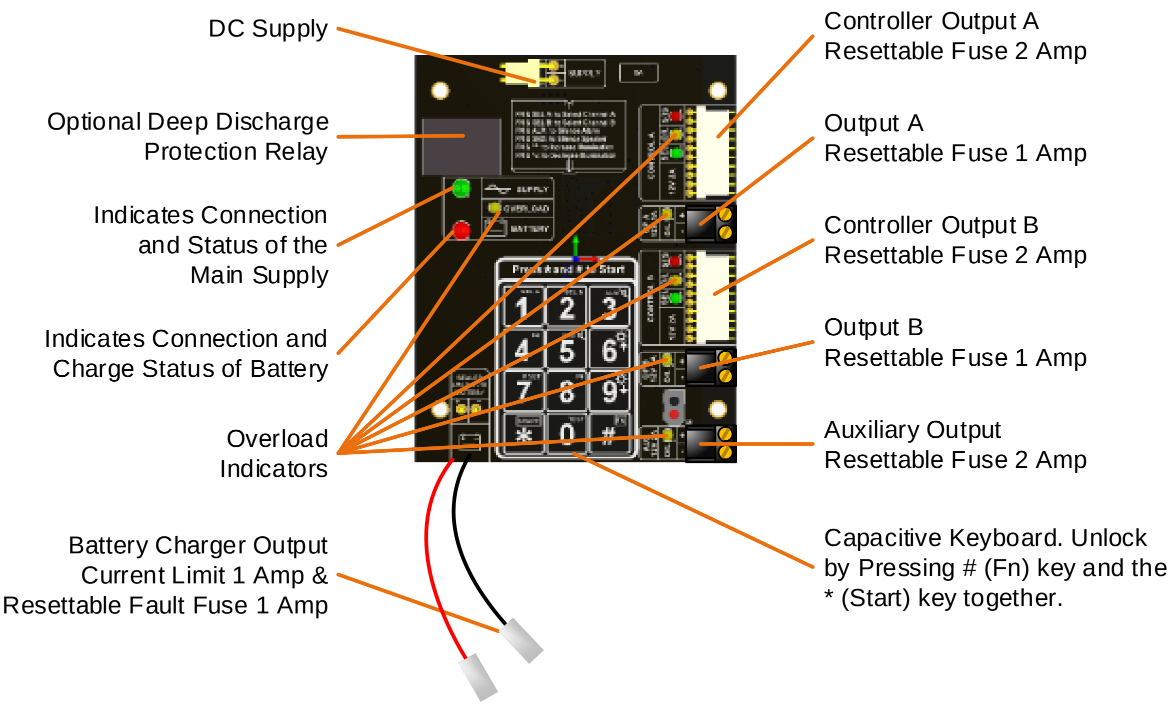
Front Panel Indicators

When designing an access control system, it is important to make sure that the power supply is not overloaded. The built in power supply of the P4 range of controllers is capable of providing power for most standard applications. However, there may be situations where additional power supplies are required. These notes are intended to help you determine when this is the case.

Power Supply Maximum Loads

To protect external wiring each output from the power supply has an individual current limit or resettable fuse. There are overload LED indicators next to each output port that will light if the overload protection is activated. The maximum loads on the PSU terminals are as follows:

Power Port	Connection Type	Overload Protected	Voltage
Battery Charger	Spade Terminal	1A	13.8V
Control A	Grey 10 Pin Cable	2A	13.8V
Control B	Grey 10 Pin Cable	2A	13.8V
OP A	Terminal Block	1A	13.8V
OP B	Terminal Block	1A	13.8V
Aux	Terminal Block	2A	13.8V



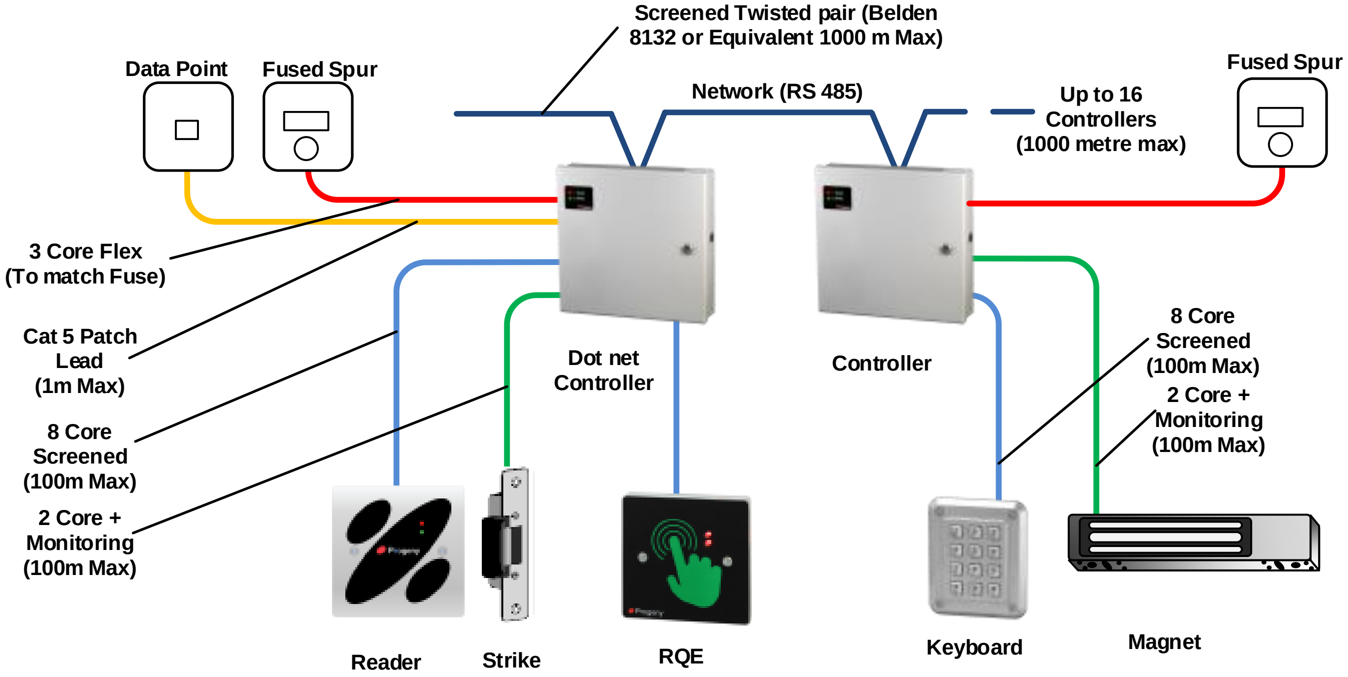
Budgeting

Note that the above table shows the current limit of each connection and does not show the total budget available**. Total available current at any one time is 5A**. When budgeting for the load it is the Peak current values of the devices that will be connected that should be used.

Cables

Pay close attention to the current rating of cables that are connected to this power supply and any fitted equipment. In particular the 2 Amp outputs, typical alarm cable is 7 strands of 0.2mm and is only rated at 1 Amp. Check with your supplier of the cable you are using.

P4 & P4.net Cabling Diagram



Battery

We recommend fitting a 12V 7Ah battery in the event of a mains failure. Batteries should be serviced at regular intervals (24 months is a respectable period).

Important Note:

If rechargeable batteries are to be fitted, then they must be of the correct type. The power supply is designed to charge sealed lead acid batteries. **Do not;** connect NiCad, Dry Cell batteries or any other chemistry of battery.

- Power up sequence should be: Mains first then Battery
- Power down sequence should be: Battery first then Mains

Connection Diagrams

Ethernet (IP Addressed) Connection

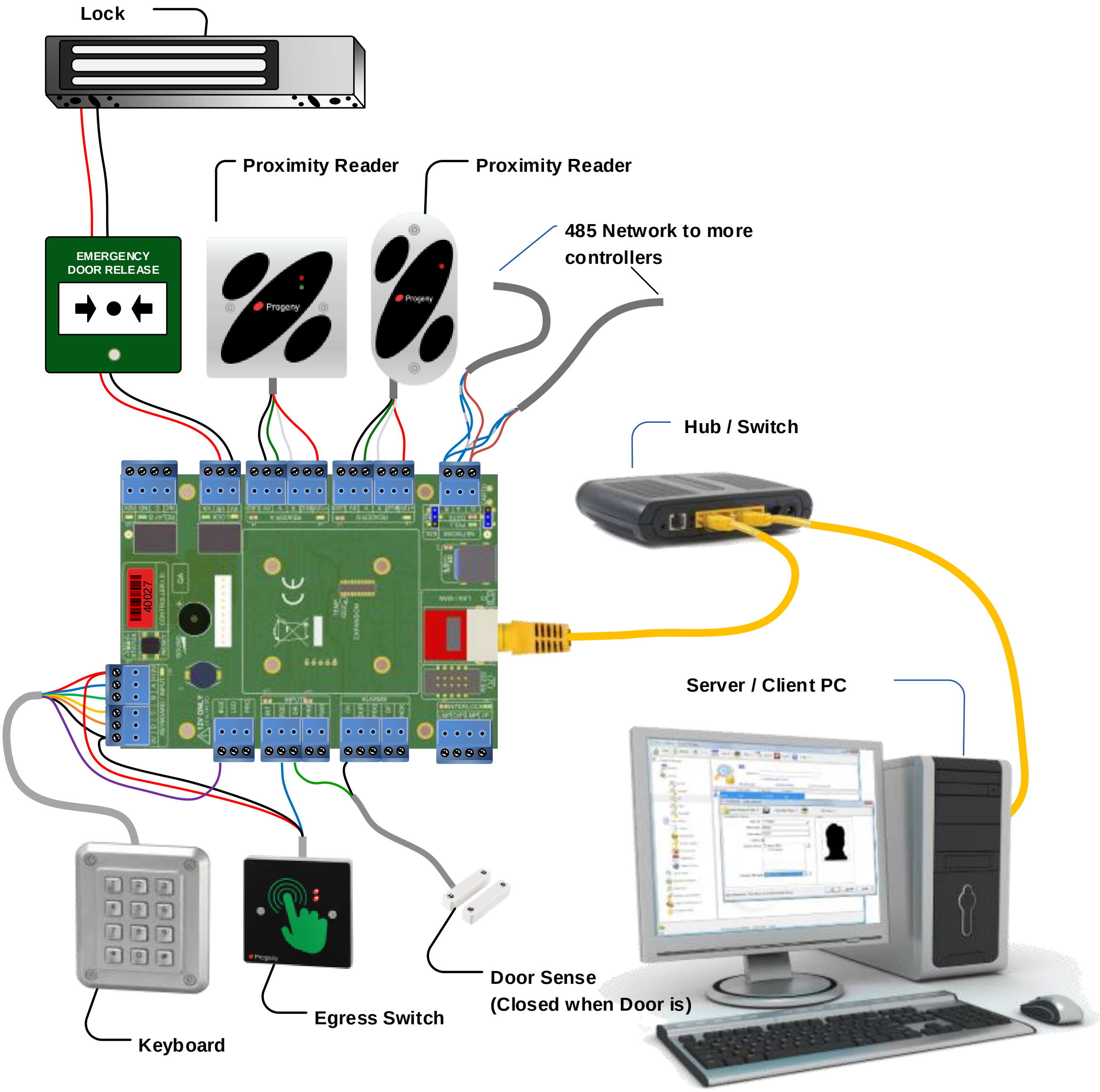


Figure 1

Lock & Relay B

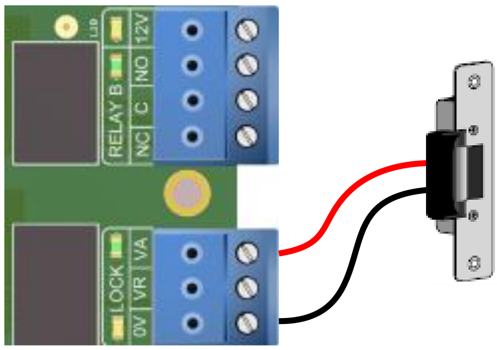
Locking devices fall into categories:

- "Fail Secure"
- "Fail Open"
- “Triggered Device”

The following diagrams show a typical connection of these two types of locking device.

Fail Secure

The “Fail Secure” locks require power to release the door. This diagram shows an electric strike, however these devices can be Fail Secure or Fail Open and some can be configured for either.

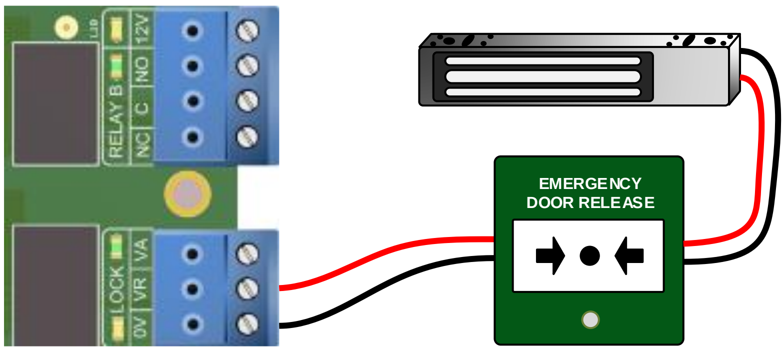


Fail Open

The “Fail Open” locks require power to hold the door locked.

Note: in this case if the door forms part of an emergency exit route, a means of overriding the device should be fitted.

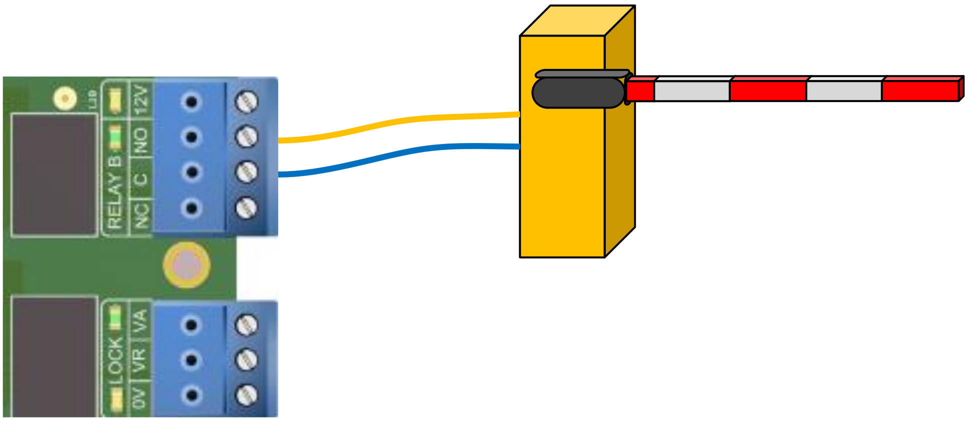
This diagram shows a green call point but it could equally be a “Fire Relay” controlled from a Fire Alarm system.



Triggered Device

Triggered devices usually require a normally open voltage free contact to trigger the device. This can be a Car Park Barrier or a powered Automatic Door Opener.

Relay B provides voltage free contacts and the default behaviour is to follow the lock relay. It can also be programmed to work in conjunction with the lock relay to give a two stage release or to work with a directional turnstile.



Progeny
Access Control

Lock Suppression

It is important to check that the locking device is suppressed. Any electromagnetic device will produce a Back E.M.F when power is removed. This can interfere with and even damage other electronic equipment. Most good locking devices will already have suppression fitted. If not, you should fit an appropriate suppression device across the coil.

In the case of solenoid operated locks, a flywheel diode will do. Connect the cathode to the positive and the anode to the negative terminal of the coil. The diode will need to be rated at the full operating current of the coil.

Do not use a diode for a mag-lock, as this will cause an excessive delay to the release of the door. An MOV or VDR is a far better choice. Polarity is not critical, but make sure the rated voltage is greater than the normal operating voltage of the lock.

A more detailed explanation of Back E.M.F. can be located at our website here: https://progeny.co.uk/back-emf-suppression

Lock Volt Drop

Figure 1 shows how the voltage at the locking device varies with cable length and core size.

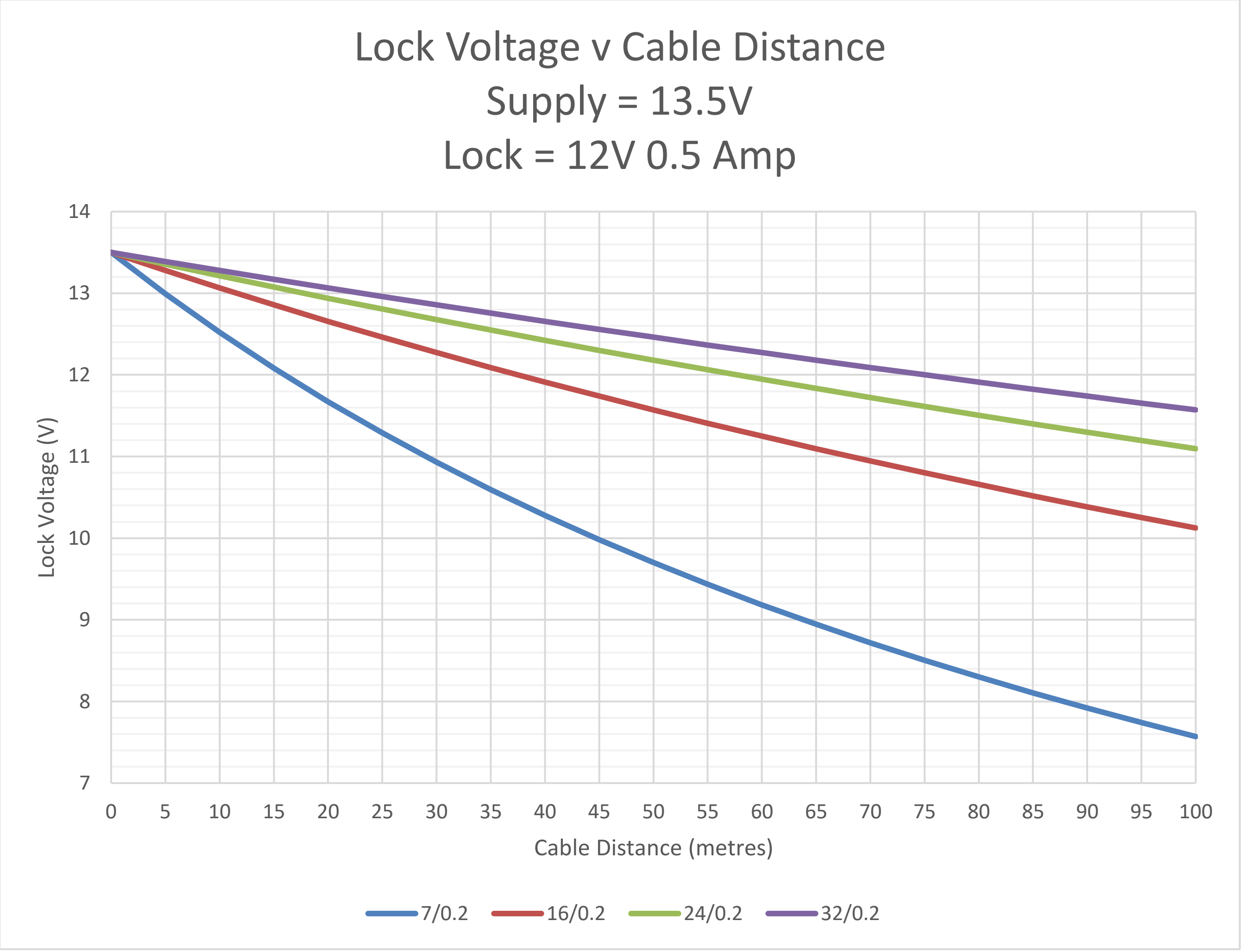
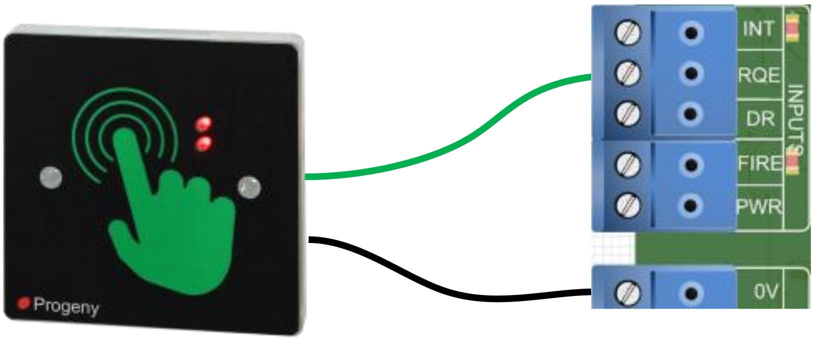


Figure 1

Inputs

Request to Exit (RQE)



The RQE “Request to Exit” input is used to trigger the lock release timer. The input accepts a normally open voltage free contact.

Generally, this input is used to provide egress where the locking device does not provide mechanical override. Door Magnets and Turnstiles are a couple of examples.

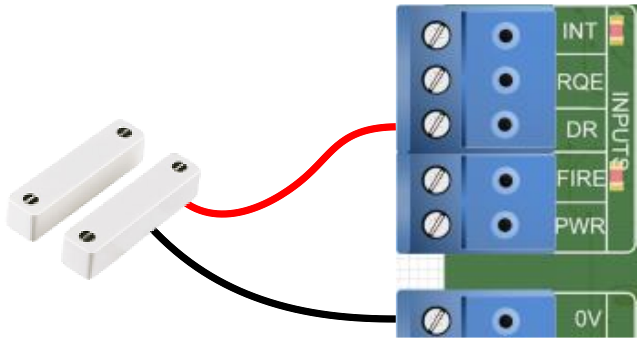
This input may also be used to provide a remote opening; from a receptionist’s desk or a video or intercom door entry system.

Door Sense (DR)

The Door Sense input is used to detect when the door is fully closed. The voltage free contact should be closed when the door is closed.

The use of door monitoring is optional but there are many features that make use of this input including:

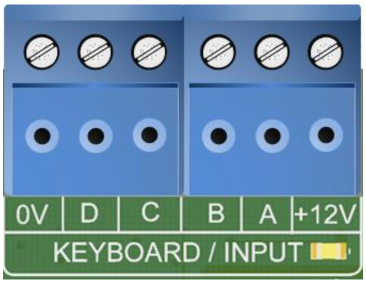
- Auto Relock
- Door Failed to Close Alarm (PDO)
- Door Forced Alarm
- Interlock



If the door is not being monitored, a wire link can be fitted between the “DR” input and the “0V” terminals.

Some door magnets have built in monitoring, this can be used for PDO and Door Forced monitoring but may not suitable if the system is to be used in reverse action interlock or auto relock applications.

Keyboard



The keyboard interface allows for code or pin to be used for access control and to allow remote programming of the standalone system. The interface uses a binary coded decimal (BCD) scheme to reduce the number of connections required. When a key is pressed, the A, B, C, & D terminals are pulled to 12V in a combination representing the key. It useful to note that the keys 1,2,4 & 8 pull A, B, C & D respectively.

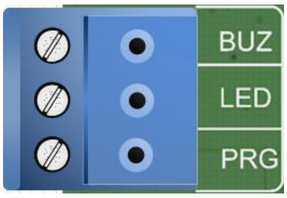
P4 Controller	2040	2011	2121
Controller	Spy Proof Keyboard	Scramble Keyboard	Vandal Resistant Keyboard
+12V	+12V	+12V (2)	+12V
A	A	A (6)	A
B	B	B (5)	B
C	C	C (4)	C
D	D	D (3)	D
0V	0V	0V (1)	0V
BUZ	BUZ	NC	BUZ
LED	LED	A (7)	NC
PDO	NC	NC	PDO
Earth Stud	Screen	Screen	Screen

Cable & Connections:

Always use a screened non-twisted cable for keyboard. More than one keyboard can be wired in parallel for Code in Code out applications. The screen of the cable should be connected to the earth stud of the controller. Keep the pigtail of the screen as short as possible once the cable has entered the enclosure. The inner cores can then make the rest of the journey to the terminal blocks.

Status Outputs

All the status outputs are open collector transistor driven. When active the transistor switches the terminal to 0V. Any externally connected devices should be connected between that terminal and the +12V available at the keyboard terminal block. Any inductive loads, such as relay coils or electromechanical buzzers should have suitable suppression fitted. A diode is usually sufficient for a relay coil. Connect the bar end (cathode) to the +ve.



Buzzer

This is provided for backward compatibility with earlier controllers. The sounds from this type of output are limited to long & short beeps and trill.

LED

This is a status LED drive for use with BCD interface keyboards.

STATUS LED	
LED state	**Meaning**
OFF	Standby
On	Lock released or Interlock from another door
Flashing	Programming Mode

Card Readers

Reader A, Reader B:

Only one reader may be connected to each input. Reader A & Reader B are separately identified in the event log. They can be used for

- “Card In” and “Card Out”
- Dual Height Readers
- Directional Turnstiles

Cable & Connections:

Always use screened, and ideally, none twisted cables for card readers. Don’t exceed the 100 m cable limitation. The screen of the cable should be connected to the earth stud of the controller. Keep the pigtail of the screen as short as possible once the cable has entered the enclosure. The inner cores can then make the rest of the journey to the terminal blocks.

P4 Controller	P4 4 Wire	Crystal Barcode	Progeny Magstripe	Progeny HID Prox	Progeny iCLASS
Template:	0: Crystal (Default)	11: Eight Digit Clock & Data	11: Eight Digit Clock & Data	2: Progeny Prox	2: Progeny Prox
+12V	+12V	Red (+12V)	Red (+12V)	Red (+12V)	Red (+12V)
BUZ		Blue (BUZ)	Yellow (BUZ)	Yellow (BUZ)	Yellow (BUZ)
X	X	White (DAT)	White (DAT)	White (D1)	White (D1)
Y	Y	Green (CLK)	Green (CLK)	Green (D0)	Green (D0)
0V	0V	Black (0V) & Brown (D)	Black (0V)	Black (0V)	Black (0V)
LED		Orange (LED)	Orange (LED)	Orange (LED)	Orange (LED)
Earth Stud	Screen	Screen	Screen	Screen	Screen

Networking

Networking the access control system allows the server PC to communicate with each door controller. The networks can be constructed in a number of ways called “Topology”.

Individual access control PCBs are addressed using a combination of the “Controller Address” and “Communication Channel”.

Doors Enterprise can communicate via:

- USB to RS485 Interface using a virtual com port
- Ethernet UDP/IP over a LAN or WAN
- GPRS UDP/IP over the mobile telephone network

Dot net to Every Controller

In this topology, each controller has its own Ethernet Port and its own IP address. The IP address must be a fixed IP address.

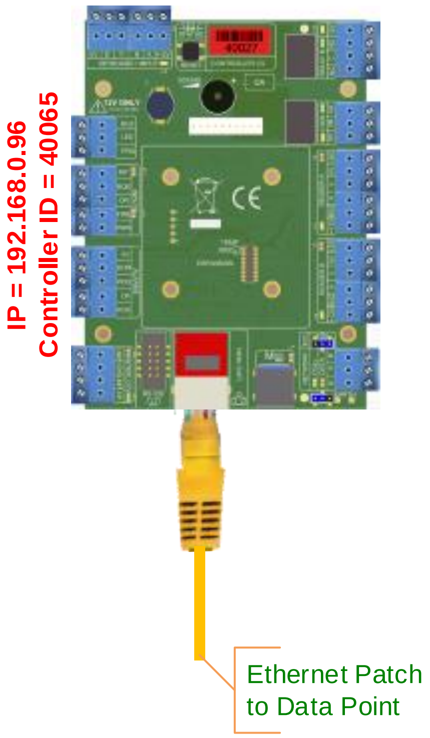
Pros

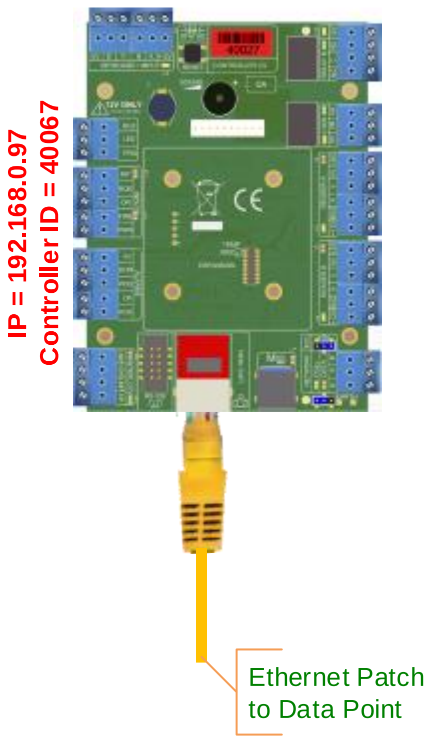
With this topology there is no need to connect strings of controllers together on the RS 485.

The Controller can be anywhere in the world as long as there is a LAN or WAN to connect to.

Cons

Equipment cost per door will be higher due to the additional Ethernet device servers. This may be offset with reduced installation time.





Dot net with RS485 Daisy chain

In this topology, each controller on the RS 485 shares the same IP address of the single dot net controller.

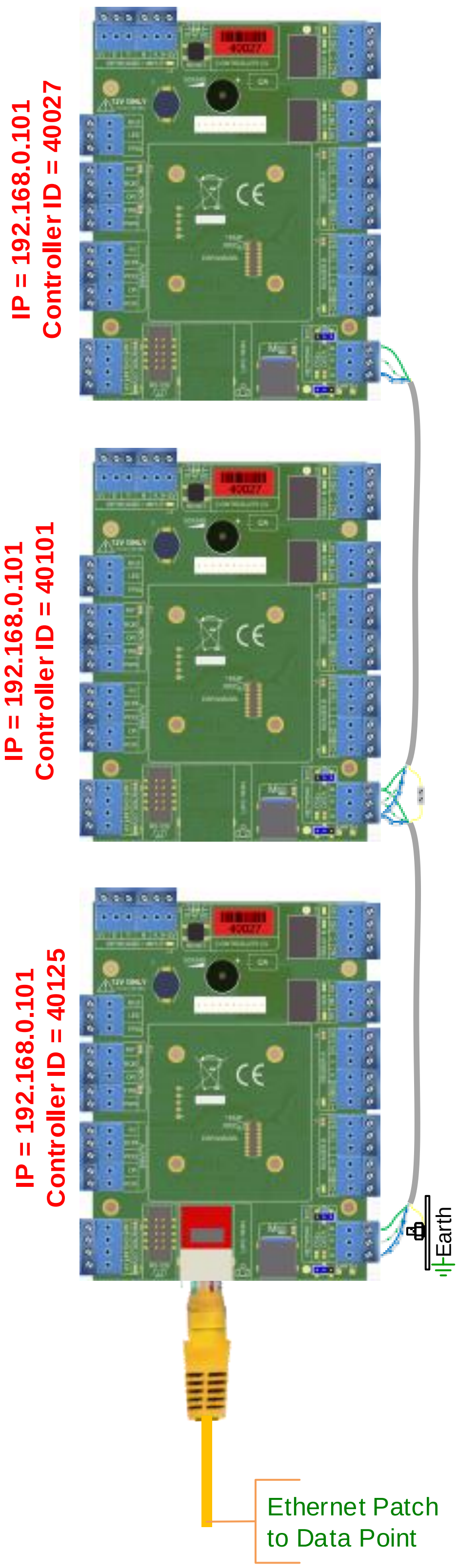
The Maximum number of controllers that can be connected this way is 16.

Pros

Reduced equipment cost.

Cons

Installation time.



Progeny Access Control

RS485 Network Connection

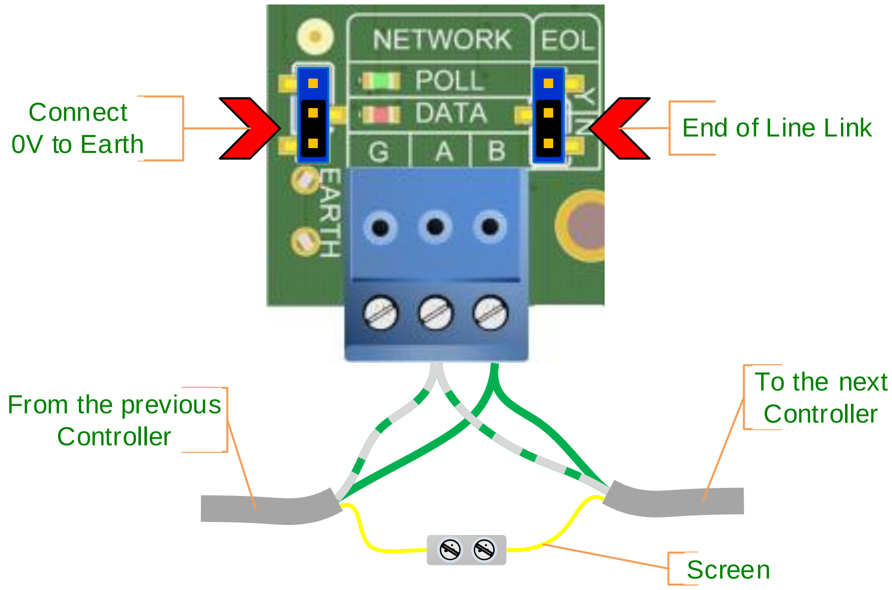
The network used to link the controllers back to a central point is “RS 485”. This allows half duplex communication and requires a cable with twisted pairs and an overall screen.

When pulling the cable into place, be careful to avoid Fluorescent lighting ballasts and large mains transformers, motors and switchgear.

There are two methods of connecting networks of controllers together. Both methods require the screen of each segment of cable to be connected to the next. It is also important to connect the screen of the network cable to earth at just one point.

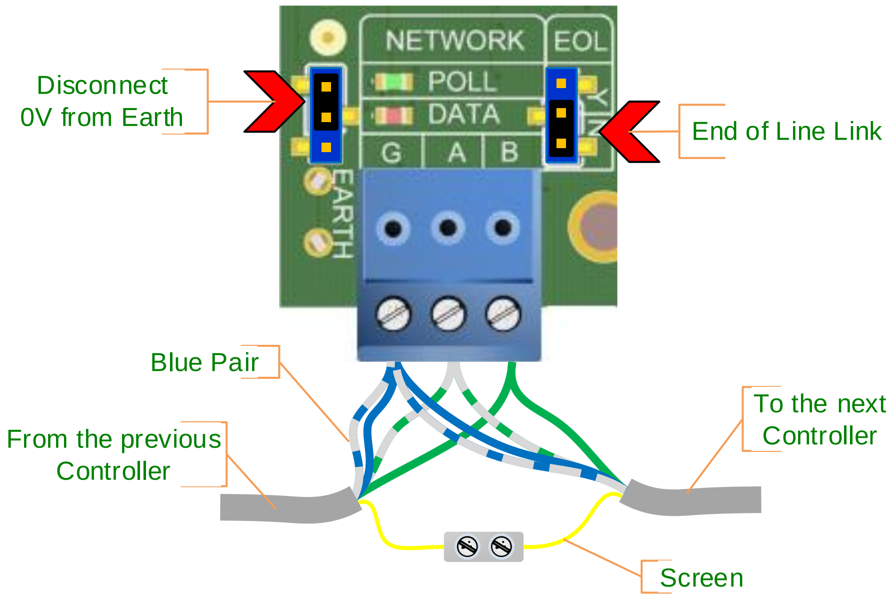
Connection Method A

This method uses the earth as a reference ground. This method is simple and works well in small systems where the controllers are located close together. However, if you have controllers that are a long distance apart or where there is significant noise on the earth, method B will be better.



Connection Method B

This method isolates the earth from the 0V and uses a spare pair of conductors to connect the 0V of each controller.



Alarms

This diagram shows the three main ways that alarm devices can be connected to the controller. All the alarm outputs are open collector transistors that switch to 0V when active. Any inductive loads, such as relay coils or electromechanical buzzers, should have suitable suppression fitted. A diode is sufficient for a relay coil. Connect the bar end (cathode) to the +ve.

The PDO alarm sounder is shown powered from the access control PSU. The extra load should be accounted for and care should be taken that the alarm device voltage rating is the same as that selected for the lock load.

The door forced alarm is shown connected to an external power supply. Note that the -ve of the external PSU is connected to the 0V of the access control unit.

The Hacker and Duress outputs are shown connected to a “Digital Communicator”. Check that communicator will accept the open collector as an input trigger. Note again that the 0V of the DC communicator is connected to 0V of the access control unit.

Relay B can also be made use of if voltage free contacts are required for any of the four alarm outputs. See Engineer programming menu 07.

Interlocking

Interlocking allows two or more doors to work together creating an airlock system. This works by each controller informing others of the door status. This is done using the interlock input and the interlock output.

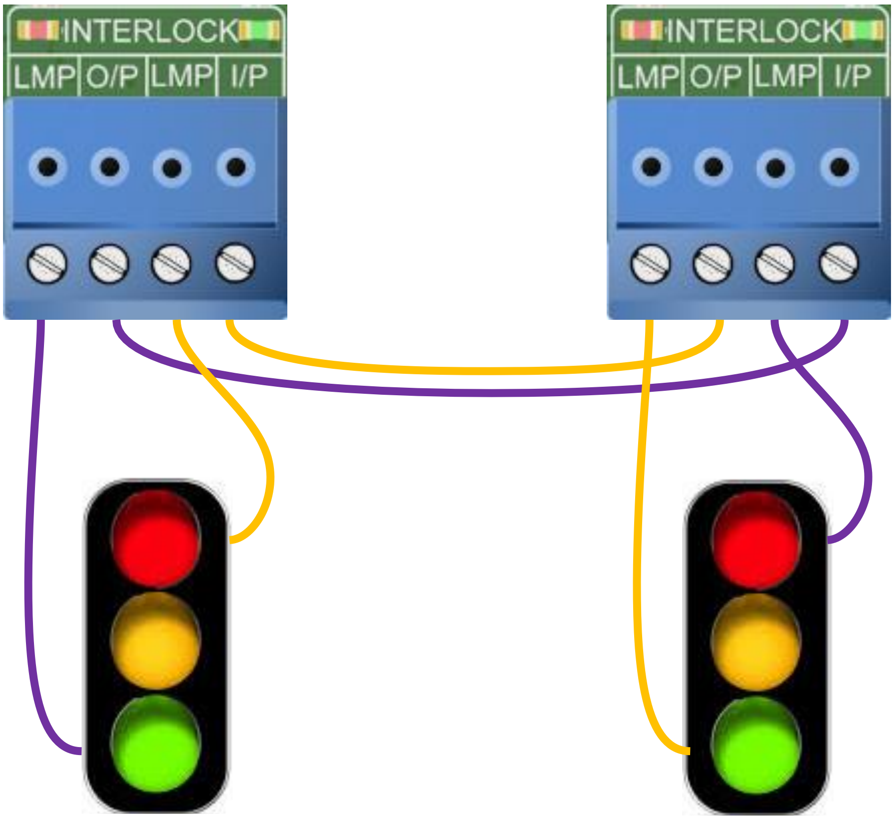
Interlock Output:

This output becomes active if either the Door sensor input is open or the lock output is active. In other words, the door is insecure.

Interlock Input:

This input prevents the controller from initiating an unlock sequence. This applies to all possible sources including RQE, Card Reader, Keyboard, Network command.

The lamp drives allow indication of interlocked status at the door.



Tip:

When commissioning remove the interlock connections and test each door’s operation first. Then connect the interlock and verify the interaction of the two doors. Three and four way interlocks can be constructed using the 2069 Interlock-Programming module. See the separate data sheet for more information.

Specification

Ethernet

Speed	10Base-T or 100 Base-T (Auto-Sensing)
Cable	Category 5 (90metres max)
Protocols	TCP/IP, UDP/IP, ARP, ICMP (PING)
Management	Via programming keyboard or DS Manager

Controller Memory

Event Memory	8000 time date stamped
Time Zones	up to 250
Time elements	up to 250
Calendars	up to 100
Cards	32,000 standard (128,000 option)
Custom Card Formats	Standard Wiegand & Clock/Data
Reader Technologies	Proximity, Wiegand, Barcode, Magstripe, Biometric. Crystal
Two Reader Inputs	“Card in” – “Card Out” or Dual Height
Reader supplies	12V @ 1.0 A current limited
Access codes	1 (1 to 8 digits)
Virtual Cards	up to 32,000 (4 to 8 digits)
Biometric Templates	1000 users (2 Templates per user)

Controller

Dimensions:	310mm, 330mm, 90mm
Keyboard Functions	PDO Mute, Sound Volume

Relay Outputs

Lock Output Relay	12V DC Applied & Removed
Relay B contact ratings	3.0 Amps at 30V DC
Lock Timer	1 to 99 seconds 0 = Toggle mode
Anti-Tailgate Feature	As standard

Network

RS 485 (2 wire)	Half Duplex

Interlock

Connections	In & Out with lamp drives

Inputs

Request to exit input	Normally Open Contact
Door sensor input	closed contact when door closed
Auxiliary	Fire, Intruder (Closed for standby, Open for Alarm)

Alarms

Door forced alarm output	100 mA switched to 0V
PDO alarm output	100 mA switched to 0V
Hacker alarm output	100 mA switched to 0V
Duress output	100 mA switched to 0V

Status

LED	Readers, keyboard
Buzzer	100mA

Programming

Stand Alone or Online

Power Supply

Supply	230 V AC 75 Watts
Battery Charger	Sealed Lead acid 12V 7Ahr

ADVANCED FEATURES

User Formats

For Clock & Data formats

When the controller reads a card, the number is loaded into a 32-digit buffer. If there are more than 32 digits, the surplus digits are ignored apart from being used to calculate and check the LRC.

Functions 40 to 54 store a two-digit number 1 to 32 representing the ordinal positions of digits the in buffer. If a particular digit needs to fixed to a set value. Storing a value 50 to 66 does this. 50 represents a digit 0, 51 a 1, 52 a 2 and so on. 60 to 66 represents hexadecimal A to F. Thus field separators can be represented (0Dh, "=").

Function 54 allows the numbers to reference from the beginning or the end of card information. If left justified the digits are counted from the start sentinel forward. If right justified, the digits are counted from the end sentinel backward.

The fifth digit of the site code and card number are both fixed to 0 by using “50”. The card is read from the start (*54 = 0). The fourth digit of the card number is taken from the ninth digit from the start of the card and so on.

Reader A	Reader B	Wiegand Description	Clock & Data Description
***40**	***60**	1= Wiegand, 2 = C&D, 3 = P4	1= Wiegand, 2 = C&D, 3 = P4
***41**	*61	Card Number Start (bit)	Site Code Digit 4
***42**	*62	Card Number length (bits)	Site Code Digit 3
***43**	*63	Site Code Start (bit)	Site Code Digit 2
***44**	*64	Site Code length (bits)	Site Code Digit 1
***45**	***65**	Total Bit Count (0 = no check)	Total Digit Count (0 = no check)
***46**	*66	Card Number Digits Use	Card Number Digit 4
***47**	*67	Site Code Digits Use	Card Number Digit 3
***48**	*68	Even Parity Length (bits) 0 = None	Card Number Digit 2
***49**	*69	Odd Parity Length (bits) 0 = None	Card Number Digit 1
***50**	*70	Prefix Code Start (bit)	Dist Code Digit 4
***51**	*71	Prefix Code length (bits)	Dist Code Digit 3
***52**	*72	Prefix Code Digits	Dist Code Digit 2
***53**	*73	Even Parity Start (0 = MSB)	Dist Code Digit 1
***54**	*74	Odd Parity Start (0 = LSB)	“Read from” 0 = Left, 1 = Right

Function												
Reader A	Reader B	**Wiegand Description**	**ISO 15693 (Tagit 64)**	**Progeny 27**	**26 Bit 8 + 14**	**26 Bit 8 + 16**	**MIFARE CSN 8 + 16**	**MIFARE CSN 16 + 16**	**Corporate 1000**	**No Change**	**P3 BSBELE (See Notes)**	**37 Bit GlobW**
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**15**	**16**
***40**	*60	1= Wiegand, 2 = C&D, 4 = BCD	1	1	1	1	1	1	1	0	4	1
***41**	*61	Card Number Start (bit)	49	14	10	10	17	17	15	0	1	24
***42**	*62	Card Number length (bits)	16	14	16	16	16	16	20	0	16	14
***43**	*63	Site Code Start (bit)	33	1	2	2	9	1	0	0	17	8
***44**	*64	Site Code length (bits)	16	13	8	8	8	16	0	0	16	14
***45**	*65	Total Bit Count (0 = no check)	64	27	26	26	32	32	35	0	36	37
***46**	*66	Card Number Digits Use	5	4	4	5	5	5	8	0	4	4
***47**	*67	Site Code Digits Use	3	4	4	3	3	3	0	0	4	4
***48**	*68	Even Parity Length (bits) 0 = None	0	0	12	12	0	0	0	0	0	0
***49**	*69	Odd Parity Length (bits) 0 = None	0	0	12	12	0	0	34	0	0	0
***50**	*70	Prefix Code Start (bit)	0	0	0	0	0	0	3	0	33	0
***51**	*71	Prefix Code length (bits)	0	0	0	0	0	0	12	0	4	0
***52**	*72	Prefix Code Digits	0	0	0	0	0	0	4	0	0	0
***53**	*73	Even Parity Start (0 = MSB)	0	0	0	0	0	0	0	0	0	0
***54**	*74	Odd Parity End (0 = LSB)	0	0	0	0	0	0	35	0	0	0
***56**	*76	Prefix Code 0000 to 9999	0	0	0	0	0	0	12 34	0	4	0

Notes:

- Tech 15 Requires firmware 4.33 and above
- Tech 16 Required firmware 4.54 and above

Progeny
Access Control

Function: Reader A	Function: Reader B	Clock & Data Description	P4	Magstripe	Royal Mail	8 Digit C & D	Lobby Entry	Pub Barcode	BAE	BLICK	1 ST	BTP	Manchester University
			0	9	10	11	12						
*40	*60	2 = C&D, 3 = P4	3	2	2	2	2	2	2	2	2	2	2
*41	*61	Site Code Digit 4	0	5	50	7	50	6	3	55	4	2	7
*42	*62	Site Code Digit 3	0	6	50	7	50	6	3	55	4	2	7
*43	*63	Site Code Digit 2	0	7	7	6	50	7	2	55	5	3	6
*44	*64	Site Code Digit 1	0	8	8	5	51	8	55	51	6	4	5
*45	*65	Digit Count (0 = no check)	0	0	0	0	16	0	0	0	0	0	0
*46	*66	Card Number Digit 4	0	1	1	4	1	9	12	4	7	7	4
*47	*67	Card Number Digit 3	0	2	2	3	2	10	11	3	8	8	3
*48	*68	Card Number Digit 2	0	3	3	2	3	11	10	2	9	9	2
*49	*69	Card Number Digit 1	0	4	4	1	4	12	9	1	10	10	1
*50	*70	Prefix Code Digit 4	0	50	50	50	50	50	50	50	50	50	12
*51	*71	Prefix Code Digit 3	0	50	50	50	50	50	50	50	50	50	11
*52	*72	Prefix Code Digit 2	0	50	50	50	50	50	50	50	50	50	10
*53	*73	Prefix Code Digit 1	0	50	50	50	50	50	50	50	50	50	9
*54	*74	"Read from" 0 = Left, 1 = Right	0	0	0	1	0	1	1	1	0	0	1
*56	*76	Prefix Code 0000 to 9999	0		0	0	0	0	0	0	0	0	1234

Custom Format

Interface Type

When sent from Doors 7.02 omits to send 40 & 45. So Eng 40 can be used to select the interface type:

1 = Wiegand

2 = Clock & Data

3 = P4

Engineer function 45 sets the number of bits to be expected (0 = No check).

Prefix Code

If the template in question requires a "Prefix Code" to be checked, the value entered here will be used to do that check. It can be any number from 0001 to 9999. All cards presented to this reader interface will be expected to have this prefix. If it does not, it will be reported as "Unknown" and no access granted. If the Prefix Code is set to 0000 then the check is not made.

The prefix code is not displayed on the software screen.

Document Number:	MAN0034	
Firmware Version Number:	PSU: 3.24 and later P4: 4.55 and later	
EMC & LV Certificate Number:	17851	
WEEE Certificate Number:	WEE/JG2915VS	