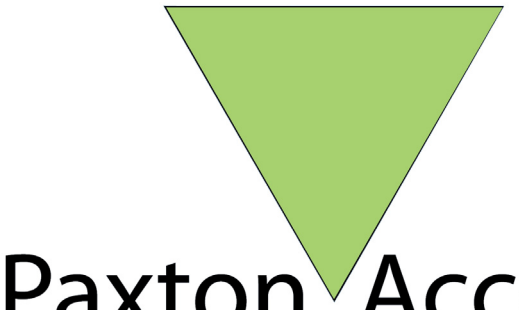
Net2 Installation Manual

Version 3



Paxton Access

Contents

Chapter 1 Introduction

This manual

Overview

This manual

This manual is designed for anybody installing and/or commissioning a Net2 access control system. The manual should be read in full before installation is attempted. As with any system of this nature, if the correct procedures are not followed, problems can occur requiring time consuming fault finding and diagnosis. This manual is designed to guide you through the installation of the Net2 system without problems.

Section	Function
Overview	An introduction to the system
What is required	A complete list of the parts required for an access control system
About…	In depth information about the system components to help specify the system and buy the correct components
Prepare yourself	ACU and cable schedules
Wiring	Wiring schematics
Commissioning	Guide to commissioning the system hardware and software
Fault-finding	Guide to fault-finding the system
Appendix	Useful information that is referred to throughout the document
Specifications	Full system specification

Figure 1.1
Table showing the layout of this manual

It is recommended that you study the **Contents** and understand the structure of this manual before reading.

Overview – System

The Net2 system is a revolutionary system with hardware and software developed simultaneously to meet the requirements of a modern day access control system. The hardware uses the latest in microchip technology allowing unprecedented levels of speed, resilience and value. The software is based on the latest Windows interfaces and is developed to enable powerful functionality whilst maintaining ease of use.

An access control system is an investment. The Net2 system ensures the future proofing of that investment in several ways:

- Latest micro-controller technology offering solid, capable hardware platform
- Hardware and software fully year 2000 compliant
- Use of FLASH memory allowing easy upgrades
- Software can be extended in functionality with 'Modules'
- System can be extended with no redundancy of equipment

The system is capable of controlling up to 200 doors and 10,000 users with the standard plus software. For systems larger than this please contact Paxton Access Ltd.

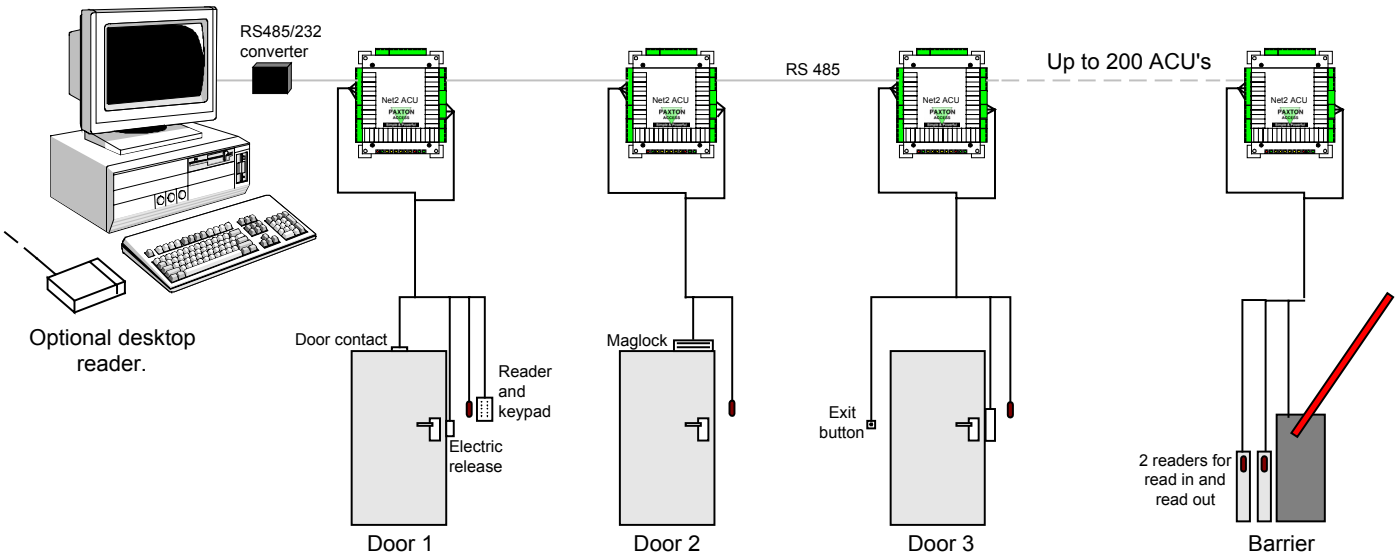


Figure 1.2
Net2 system schematic

Net2 V3 supports the use of multiple comports, allowing for star configuration networks from the PC. Control units are automatically detected.

Overview – Net2 hardware

Ease of wiring

Clearly labelled terminals on every access control unit remove the need for continual referencing to wiring diagrams. Clear colour coding of reader cables leads to fewer mistakes.

Diagnostic LEDs

An array of LEDs on the control unit indicate the status of key system features. This will aid commissioning and quick diagnosis of any problems should they occur.

FLASH Memory

FLASH memory in the access control units allows the downloading of new firmware to the control units from the PC over the network. This means that as new features are added to Net2, systems in the field can be upgraded to allow the use of the latest software features without any changes to the hardware.

Open architecture

Relay outputs and digital and analogue inputs allow integration with the hardware of other systems.

Latest technology

State of the art electronic components create a solid hardware platform, which is both high performance and compact.

Scaleable architecture

The system will be scaleable. The smallest system will be expandable to the largest system using the same hardware building blocks with no redundancy of hardware as the system expands.

Communications

Very high speed and resilient communications offer real time alarm reporting and the capability for very large systems.

Distributed intelligence

The Net2 single door control units provide fully distributed intelligence down to individual doors. This gives greater system resilience and makes support and problem diagnosis easier. Also, event information can be retained when the system is running off-line (2,300 events per control unit/door).

Multi-technology

The same control unit will support magstripe, keypads and proximity, mixed on a single site if required.

Overview – Net2 software

Open architecture

Microsoft Access database allows easy linking of data to other software systems.

Ease of use

Easy to learn user interface working in Microsoft Windows 98/2000/NT/XP environments. The user interface looks and feels like the latest Microsoft Windows explorer and Outlook programs so office PC users will be able to navigate the system intuitively.

Ease of commissioning

Auto detection and numbering of access control units. No DIP switches to set or binary numbering to worry about - switch on the software and go!

Modular

The software has the capacity for features to be added as and when they are required. The modular structure enables the user interface to be as powerful as required whilst remaining simple.

Chapter 2 What is required?

Essential

Optional

What is required?

Essential

Description
PC
Net2 software
Net2 access control units (ACUs)
Enclosures for ACUs
(If not fitted inside PSUs)
Readers/keypads
Reader and network cable
Cable for lock supply and inputs
Power supplies
User cards/tokens
Electric release/lock
RS485/232 communications interface

Optional

Description
RS485 repeater
Door contacts
Desktop reader
Door loops
Break glass
Exit buttons
Batteries for power supplies

For a full list of system components supplied by Paxton Access Ltd, refer to *Appendix (vi).*

Chapter 3 About…

Net2 access control unit

Readers/keypads

Power supplies

Inputs and outputs

User tokens

Desktop reader

Network

PC

Net2 access control unit – hardware features

- 16Bit Micro-controller running at 14.7MHz
- 128K FLASH Memory with over 100 years data retention
- 1 x 128K static RAM chips
- On board rechargeable 3.6V battery – approximately 1 weeks data retention
- On board real time clock with year 2000 compliant software
- Quiescent current of ACU at 12Vdc is between 50 and 350mA depending on what is functioning on the board
- RS485 Coms chip with full duplex communication at 115K BAUD
- Terminal blocks rated at >100 uses with rising clamp connectors
- On-board static protection:

Coms chip	Mosorb protected – clamped to 15V above ground (Will dissipate 1500W)
Inputs	Diode protected
12V dc input	Mosorb protected – clamped to 27V above ground Capacitor smoothed – capacitor can supply board for 0.25 seconds

Figure 3.1
Table showing board protection

- Outputs:

2 x clean contact relays	24V, 5Amps
1 x FET output	Variable voltage, 1Amp

Figure 3.2
Table showing outputs

Net2 access control unit – diagnostic LEDs

The diagnostic LEDs are designed to make fault-finding and commissioning easier.

Note:
All of the inputs work on the same logic. If the circuit is closed, the LED is on.

Label	On means…	Off means…
12V	12V okay	12V not okay
5V	5V okay	5V not okay
OK	This is the heartbeat of the system and should pulse regularly. This shows that the processor is functioning.	
PSU	Mains present	Mains not present OR mains monitoring not connected
Tamper	No tamper	Tamper OR tamper switch not connected
Contact	Door is closed	Door is open OR door contact not connected
Exit	Button pressed	Button not pressed OR exit button not connected
Relay 2	Coil energised. Com and N.O. terminals are connected.	Coil not energised. Com and N.C. terminals are connected.
Door relay 1	Coil energised. A fail closed lock will be open. A fail open release will be locked.	Coil not energised. A fail closed lock will be locked. A fail open release will be open.
Tx	The ACU is transmitting a network message	The ACU is not transmitting a network message
Rx	The ACU is receiving a network message	The ACU is not receiving a network message

Figure 3.3
Table showing functions of diagnostic LEDs

Net2 access control unit – enclosure options

The Net2 ACU is available in the following formats:

- No enclosure – The control unit PCB is provided with plastic adhesive posts for mounting into an enclosure.
- Mounted in Net2 plastic housing – a smart enclosure for the ACU
- Mounted in Net2 2A PSU in steel cabinet – a good quality power supply and enclosure.

Part number	Description
489-334	Net2 1 door access control unit
385-527	Net2 1 door ACU in plastic housing
571-692	Net2 housing for ACU black plastic
411-381	Net2 1 door ACU with 2A PSU in steel cabinet
857-693	Net2 2A PSU in steel cabinet

Figure 3.4
Table showing enclosure options

Readers and keypads – compatibility

Figure 3.5 shows the products manufactured by Paxton Access Ltd that are suitable for use with the Net2 ACU. Two readers AND two keypads can be wired to the same control unit to give card plus PIN or card plus code access control on both sides of an access point.

Part number	Description
600-628BL	TOUCHLOCK keypad black
600-628BR	TOUCHLOCK keypad brass
600-628SC	TOUCHLOCK keypad satin chrome
584-374	TOUCHLOCK keypad stainless steel
409-711BL	CARDLOCK reader black
409-711BR	CARDLOCK reader brass
409-711SC	CARDLOCK reader satin chrome
266-898	CARDLOCK reader black plastic external
355-098	PROXIMITY reader

Figure 3.5
Table showing compatible readers/keypads

OEM readers and keypads

Currently no other keypads are supported by the Net2 ACU. Magstripe and proximity readers with clock and data or 26-bit Wiegand outputs are compatible. Figure 3.6 shows the connection details to the control unit. If in doubt, consult the Paxton Access technical helpline.

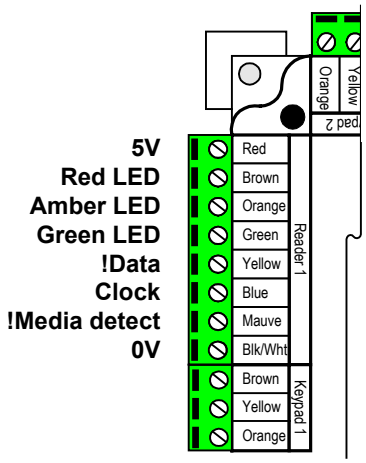


Figure 3.6
Diagram showing reader inputs

Readers and keypads – cable details

Paxton readers/keypads require Common Reference CR9540 cable. Figure 3.7 shows the reader cable supplied by Paxton Access Ltd.

Part number	Description
166-010	Reader cable 10 core CR9540 10m roll
166-025	Reader cable 10 core CR9540 25m roll
166-100	Reader cable 10 core CR9540 100m roll
166-500	Reader cable 10 core CR9540 500m roll

Figure 3.7
Table showing reader cables

The specifications of CR9540 are shown in figure 3.8.

CR9540		
	Cores	10
	Screened	Overall screened
	AWG	24
	Outside diameter	6.197mm
	Capacitance between conductors	98.4 pF/m
	Construction	7x32

Figure 3.8
Table showing reader cable specification

The type of reader/keypad will effect the maximum distance to the Net2 ACU. Figure 3.9 shows this relationship. All distances are assuming that CR9540 cable is used AND that the readers/keypads are wired as shown in this document. Using CR9540 ensures that the cable extensions match the reader tail.

Reader/keypad	Maximum distance from ACU
TOUCHLOCK keypad	30 metres
TOUCHLOCK keypad stainless steel	30 metres
CARDLOCK reader	100 metres
PROXIMITY reader	50 metres

Figure 3.9
Table showing maximum cable extensions for readers/keypads

The cable screen must be connected to the 0V (Blk/Wht) terminal at each ACU.

The minimum voltages that readers/keypads will operate with are shown in the table.

Reader type	Minimum voltage
PROXIMITY reader	4.5V
PROXIMITY reader (new style)	12V
CARDLOCK reader	4.5V
TOUCHLOCK keypad	4.5V
TOUCHLOCK keypad stainless steel	4.5V
OEM reader	Consult manufacturer's literature

Figure 3.10
Table showing minimum voltages for readers/keypads

Power supplies – Paxton supplied

Paxton Access Ltd offer two power supply solutions.

Part number	Description
339-424	12Vdc boxed backup power supply 1A
857-693	Net2 2A PSU in white steel cabinet
339-425	12V 1.2AH battery for 1A boxed PSU
862-719	12V 7AH battery for 2A boxed PSU

Figure 3.11
Table showing power supplies available from Paxton Access Ltd

12Vdc boxed backup power supply 1A

Standard 1 Amp 12V dc power supply unit with a 205mm X 230mm X 80mm enclosure (not enough room for the Net2 ACU). Hinge lid with a tamper switch. Takes 2 X 1.2AH batteries.

2A 12V d.c. boxed power supply with mains monitoring

This unit is now available, part number **857-693**. It includes many features including mounting posts for the Net2 ACU and mains monitoring.

Power supplies – choosing guide

When choosing a power supply for the Net2 system there are several considerations.

Current rating

The rating of the power supply must be suited to the load. The quiescent current of the various system components is shown in Figure 3.12.

Description	Load
Net2 ACU (not including readers etc.)	<350mA
PROXIMITY reader	60mA approx.
CARDLOCK reader	55mA approx.
TOUCHLOCK keypad stainless steel	35mA approx.
TOUCHLOCK keypad membrane	35mA approx.
Electric release/other	Consult manufacturer's literature
Battery charge	Consult manufacturer's literature

Figure 3.12
Table showing loads

The minimum power supply rating is equal to the sum of all loads plus 10% (safety factor).

Battery backup

The time that the Net2 system will continue to operate when the mains supply fails is dependent on the current consumption of the system and the battery backup in the power supplies. The relationship is shown in figure 3.13.

Figure 3.13
Relationship between current consumption and battery backup time

$$\text{Backup time (hours)} = \frac{\text{Amp hour of backup batteries (Amp hours)}}{\text{Current consumption of system (Amps)}}$$

Power supplies vary in the features they offer relating to battery backup. A few considerations are:

- **Deep discharge** – When a backup battery is drained too much it can reach a state whereby it cannot be recharged. This is deep discharge. Some power supplies have the ability to prevent this happening.
- **Recharge limit** – Some power supplies limit the current consumption of a battery whilst it is recharging. If a power supply does not do this then the system may not be immediately operational when mains power is resumed, i.e. the power will be consumed by the battery recharge.
- **Battery capacity** – the size of the enclosure will limit the amount/size of the backup batteries.

PSU ripple

Not all dc power supplies are smooth. The ripple is the amount that the voltage fluctuates. The ripple of a supply can be measured by setting a multimeter to measure ac voltage. If the ac voltage across the power terminals is greater than 2V, then it is not suitable for use with Net2.

PSU ripple should be measured under full load conditions.

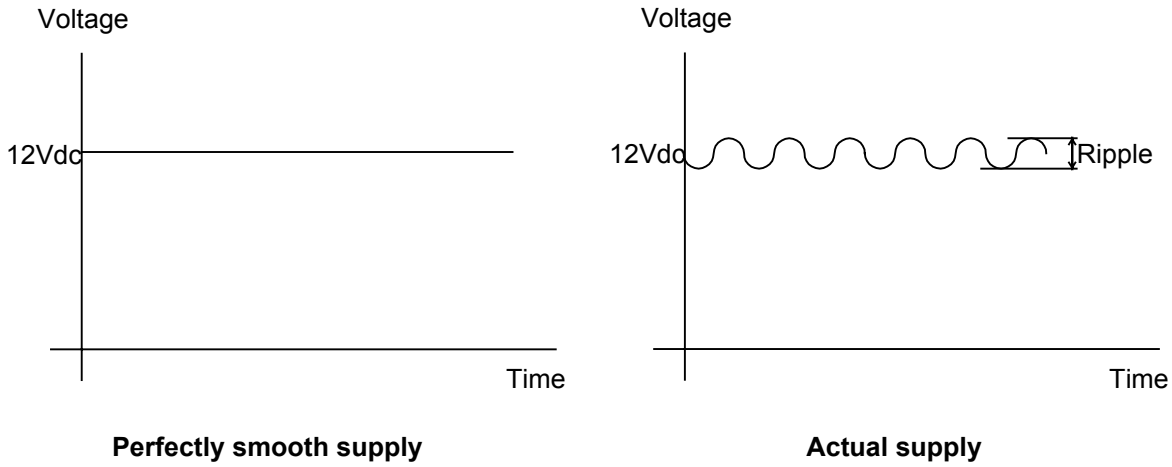


Figure 3.14
PSU ripple

Size of enclosure

If the ACU is to be mounted in the power supply enclosure then there must be sufficient space. An enclosure of 350x350mm or larger is recommended.

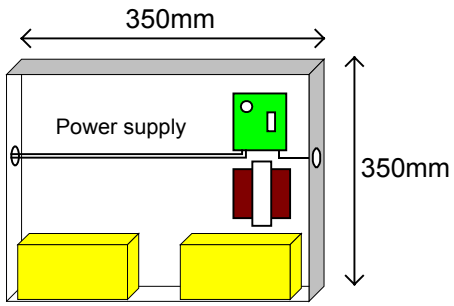


Figure 3.15
Recommended size of PSU enclosure

Alarms

The Net2 system has the capacity to report PSU tampering and mains failure. If the monitoring of these features is required then the chosen power supply must have tamper and mains fail clean contact outputs.

Inputs

Exit button

Any push to make button can be used. The button should be physically robust to suit the volume of traffic through the access point and the environmental conditions. An exit button is not required if exit is by using a handle or an out reader.

Door contact

To enable door monitoring, door contacts must be used. The door contact circuit must be closed when the door is shut. Two states of alarm can be generated with door monitoring, door forced open and door left open.

Autolock means that when a door closes, the locking mechanism automatically locks even if the door open time has not expired. This feature can help to reduce tailgating. If autolocking is required then a door contact must be fitted.

Power supply tamper

This input is for a power supply tamper switch. This will allow tampering to appear as an alarm event at the PC. The Net2 plastic enclosure also has a tamper switch fitted. Where there is a separate PSU and enclosure, the tamper switches can be wired in series.

PSU

This input is for mains monitoring. This requires the power supply to have a mains fail relay output. The ACU will report a mains fail alarm if this input changes state.

Outputs

Relay 1 - lock

The lock is controlled by door relay 1. Relay operation is described in *Appendix (i)*. The relay contacts are voltage free and are rated 5Amps at 12V ac or dc. Having relay contacts means that this output is very versatile and can operate virtually any electrical equipment including fail open and fail closed locks, electric gates, electric barriers, lifts…

There are two main types of locking devices - fail open and fail closed. Refer to *Appendix (iii)* for more information.

When using the same power supply for the ACU and electric release, diode suppression must be fitted. A standard 1N4001 diode is fitted as shown in *Wiring – inputs and outputs*.

Relay 2 – toggle/doorbell

Relay 2 can be configured to toggle in the software (See ins-113). It can be toggled by either reader 1 or by reader 2. If the relay has NOT been set to toggle then the doorbell of a TOUCHLOCK keypad fitted to the system will operate it. The output is rated 5Amps at 12V ac or dc. Relay contacts can operate virtually any electrical equipment including buzzers, lights etc…

General purpose output - alarm

This is the alarm output and is a FET, open drain that is capable of supplying 1Amp at 12-24Vdc. The FET acts as a switch to 0V.

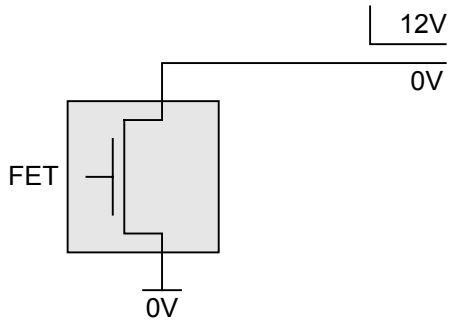


Figure 3.16
General purpose FET output

User tokens – choice

Users of the Net2 access control system will be required to carry a user token. Paxton manufacture a number of token formats.

Magstripe card

Credit card sized plastic card with a standard high coercivity (hi-co) magnetic stripe for use with magstripe card readers.

Proximity token

Tokens are about credit card size but are thicker. They can be used from inside wallets or handbags. Adhesive plastic stickers can be applied for photo ID and the slot in the tokens makes them ideal for use with low cost badge clips.

Proximity keyfob

Keyfobs are for applications where convenience is important. They are made of hard plastic and will fit onto a keyring. They can be attached to car/house keys for reduced losses, hence reducing the cost of replacing fobs.

Proximity ISO card

ISO cards are the same size as standard bank or credit cards. They can be used with standard card printers for photo ID. They also have a magnetic stripe that can be encoded for use with other systems such as vending.

User tokens – photo ID

There are several photo ID options with varying degrees of cost for both magstripe and proximity.

Magstripe

Magstripe ID cards can be produced in one of three ways.

1. The photo ID card is supplied encoded and has insets for a passport photo and some text. This is laminated with a standard office laminator.
2. A specialist bureau produce photo ID cards with corporate artwork. Paxton Access Ltd can encode these cards if required.
3. For large sites, an on-site photo imaging and card printing system can be purchased. Paxton Access Ltd can supply encoded blank magstripe cards if required.

Proximity

Proximity ID devices can be produced in any of the following ways.

1. The PROXIMITY token photo ID pouch overlay has inserts for a passport photo and some text. This is laminated in a standard office laminator and applied onto the face of the token with the adhesive backing.
2. The PROXIMITY token plain overlay can be printed with graphics using the desktop card printers used with on site photo imaging systems. They are applied to the token using the adhesive backing.
3. PROXIMITY ISO cards have the same dimensions as standard magstripe cards. This allows them to be printed using either a specialist bureau service or on site photo imaging systems. ISO cards are always supplied with a blank white face for printing.

   There is a small area on the bottom right hand of ISO cards which may cause printing irregularities and should be avoided when designing card artwork. Refer to *Appendix (vi)* for details.

User tokens – encoding

The Net2 system accepts many different encoding formats.

Paxton Net2 tokens

Magstripe and proximity tokens can be supplied encoded with an 8 digit number. This number will be unique to that particular token and the tokens will be labelled with the same number. To enrol a token the Net2 system will require this printed number to be entered either by typing it in or using a desktop reader.

CARDLOCK and PROXIMITY tokens

Magstripe and proximity tokens can also be supplied with an encoded number containing a site code and user code. These are the same tokens that are used with the CARDLOCK, PROXIMITY and NETWORK systems. The Net2 system can utilise the same user tokens as an existing Paxton system if required. Alternatively, the Net2 system can be used in conjunction with Paxton stand alone systems. These tokens do not have their number printed on them and so enrolling requires a desktop reader.

Third party user tokens

At present only proximity tokens manufactured by Paxton Access are compatible with the Net2 system. Third party magstripe cards can be used however. This is useful if the Net2 system is to be installed on a site where a magstripe card system (time and attendance, cashless vending, member's card…) is already in use. Figure 3.17 shows how Net2 interprets various formats of encoded numbers. If the number on the magstripe card is not known then a desktop reader will be required for entering the token number.

Encoded number	Net2 reads as…	Comments
1234	00001234	Where there are less than 4 digits encoded on a card, zeros are added to make up an 8 digit number.
123456789	12345678	Where more than 8 digits are encoded on a card, the first 8 are read.
123=456=789	12345678	Where digits are interrupted by field separators, the field separators are ignored and the first 8 digits are read.
123456789=6543	23456789	Where 8 or more digits precede a field separator, the 8 digits before the field separator are read. (This is how ABA and bank cards would be read)
Note: = denotes field separator		

Figure 3.17
Table showing interpretation of various encoding formats

Access control magstripe cards have a high coercivity (hi-co) magnetic strip. Some magstripe cards are low coercivity (lo-co). Bankers cards for example are lo-co. These cards are not recommended for access control. They are not as resilient to corruption as hi-co cards and wear at a much quicker rate giving a much shorter card life. Lo-co cards can be recognised by their brown magnetic strip; hi-co cards have a black magnetic strip.

User tokens – part numbers

Part number	Description
695-573	Net2 magstripe cards box of 10
693-112	Net2 proximity tokens box of 10
695-644	Net2 proximity keyfobs box of 10
692-448	Net2 proximity ISO cards box of 10

Figure 3.18
Table showing user token part numbers

Where the tokens are for use in conjunction with CARDLOCK or PROXIMITY stand alone systems, see the Paxton Access trade brochure for token part numbers.

Desktop reader

When a card is presented to the desktop reader, if it is known to the system the user record will be displayed, if it has not been previously entered on the system a blank record is displayed with the new card number displayed in the card number field.

A desktop reader is designed to be at the PC and used to administer the Net2 system. Alternatively, standard magstripe or proximity readers can be used but will have to be mounted appropriately. The desktop reader can read all Paxton magstripe and proximity tokens and is mounted on a metal plate designed to sit next to the PC.

Part number	Description
409-711BL	CARDLOCK reader black
409-711BR	CARDLOCK reader brass
409-711SC	CARDLOCK reader satin chrome
355-098	PROXIMITY reader
376-001	Desktop reader prox and magstripe

Figure 3.19
Table showing desktop reader options

The desktop reader can be wired to a spare reader terminal of any control unit on the system. BEWARE – the maximum cable distance from reader to control unit is as shown in figure 3.9. If there is not an ACU with a spare reader terminal within the required range of the PC, a dedicated ACU will be required.

Where Net2 tokens are being used the encoded number is supplied with the device, allowing the token number to be typed in manually or by swiping through the desktop reader.

Network – architecture

Daisy chain

The Net2 system communicates using an RS485 data line. Communication is full duplex at 115K BAUD giving up to 1,000 messages per second.

Because communication is duplex, all four cores of the network cable are used. The cable consists of two individually screened twisted pairs – white & green and red & black. One pair is used for transmitting, the other receiving.

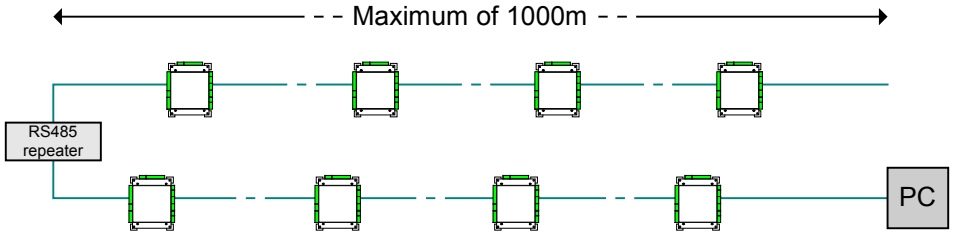


Figure 3.20
Daisy chain network with RS485 repeaters

The data line must be wired in 'daisy chain' formation with one control unit after the other. If the data line is over 1,000m a RS485 repeater (part number 477-836) should be used.

The PC can be located at the most convenient point along the network. This may be at the end of the network OR in between control units.

Termination resistors

At each end of the data line a termination resistor is required for each of the twisted pairs.

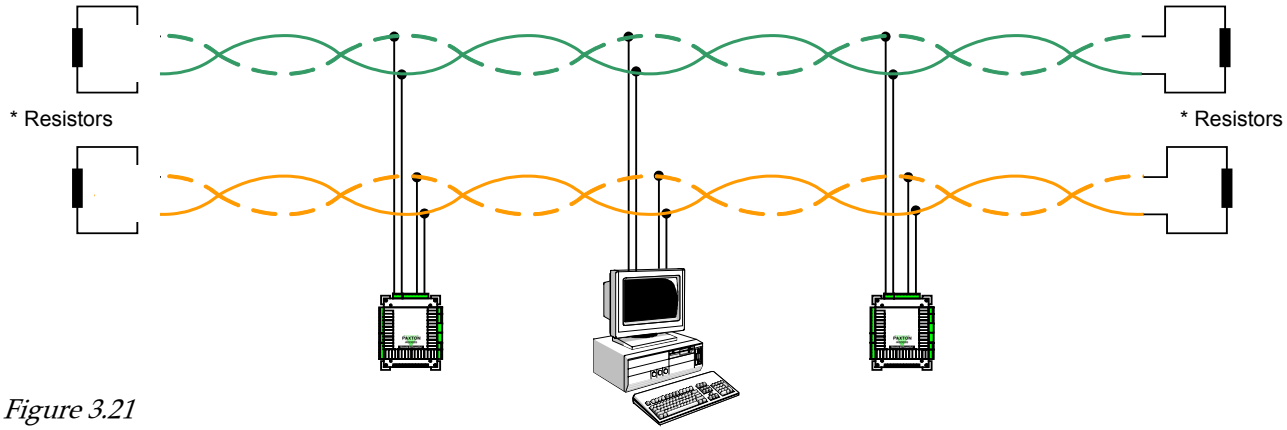


Figure 3.21
Termination resistors

* 120 Ohm resistors - supplied in the fitting kit

IMPORTANT NOTE:

The latest R485/232 converters do not contain termination resistors. If the converter is wired at the end of the network two 120 Ohm resistors must be wired between terminals 1 and 2, and 3 and 4.

Older RS485/232 converters may contain termination resistors. This type can be identified by two internal jumpers. If this type of converter is wired at the end of the network then these are left in place. Otherwise these jumpers have to be removed (JP1 and JP2 from converter PCB).

Network – data line cable

If unscreened cable is used, the unused cores should be connected into the screen terminal connection.

The recommended network cable is either CAT5 (Screened or unscreened) or CR8723.

Part number	Description
120-305	CAT5 data cable 305m boxed reel

CR8723		
	Cores	4
	Screened	Individually screened pairs
	AWG	22
	Outside diameter	4.267mm
	Capacitance between conductors	114.8 pF/m
	Construction	7x32

Figure 3.22
Table showing network cable specification

Network – RS485/232 interface

As the network protocol is standard RS485, a standard RS485/232 communications converter can be used. The converter will have to be capable of 115,200 BAUD and full duplex. Paxton Access Ltd manufacture a suitable interface.

Figure 3.23
Table showing RS485/232 interface

Part number	Description
289-641	Net2 RS485/232 kit incl converter with PSU and PC lead

IMPORTANT NOTE:

The latest R485/232 converters do not contain termination resistors. If the converter is wired at the end of the network two 120 Ohm resistors must be wired between terminals 1 and 2, and 3 and 4.

Older RS485/232 converters may contain termination resistors. This type can be identified by two internal jumpers. If this type of converter is wired at the end of the network then these are left in place. Otherwise these jumpers have to be removed (JP1 and JP2 from converter PCB).

Network – RS485 repeater

The RS485 network can span 1,000m (1km) from one end to the other. If the network is to exceed this length, repeaters will be required every additional 1,000m, see figure 3.20.

Figure 3.24
Table showing RS485 repeater

Part number	Description
477-836	Net2 RS485 high speed repeater

PC

Requirements

The Net2 system does not require a dedicated PC, other applications can be run alongside the Net2 user interface. Due to distributed intelligence, the Net2 system does not require the PC to be on for the system to be running. Each ACU has a capacity of 2,300 events, if the PC is off and this number of events is exceeded then the most recent events will overwrite the oldest events.

The minimum specification for a PC running a Net2 system are - Pentium 800Mhz processor, 128 Mbytes RAM, hard disk with 1 Gbyte free space, 800x600, 256 colour monitor, a free UART 16550 serial port, mouse, keyboard and a CD ROM drive. For best performance, increase the speed of the processor, the memory to at least 256Mb and hard disk size for systems over 50 doors or 1,000 users. The operating system should be Microsoft Windows 98, Windows NT with SP6, Windows 200 or Windows XP. Access to the Internet will enable easy system updates.

System backup

All system settings and user details are stored in an Access 7 database (Net2System.mdb). If this database is corrupted or deleted, the system will have to be reconfigured and all user records will be lost. For this reason it is essential that a backup copy of this file is made on a regular basis.

The Net2 software creates backup files automatically. A separate copy of the Net2System.mdb database is made every day the software is used. The backup file for a day has the date included in the file name (Net2System YYYYMMDD.mdb). The backup file is created either:

1. When the application is closed down

OR

2. At the automatic backup time as set in Options\Backup

If a backup file has already been created for that day, the file will be over written with the most current version of the database.

The retention period dictates the number of days that the backup files are kept for.

Note: Backup files should be saved on a different drive to the Net2System.mdb file.

Event backup

10,000 events are stored in NetSystem.mdb. These are the events that are displayed in the event screen. In addition, 12 months worth of events are stored in Net2Events.mdb.

Events are automatically archived to the backup folder. The archived event files are split into individual years (i.e. Net2 Events 1999.mdb and Net2 Events 2000.mdb).

Chapter 4 Prepare yourself

ACU schedule

This form, or a copy, is to be filled out when commissioning the system.

ACU serial number – Each ACU has a unique serial number. This is displayed on the front of the ACU.

Door Name – i.e. 'Main entrance'

Operating mode – Options are: inactive, card only, card plus PIN, card plus code, desktop reader, PIN only, code only. For an explanation of the difference between code and PIN, refer to *Appendix (iv).*

Operating mode	Description	Access gained by…
Inactive	There is no reader or keypad connected	
Card only	There is a PROXIMITY or CARDLOCK reader connected at this reader position	…presenting a user token
Card plus PIN	There is a reader and a keypad connected at this reader position	…presenting a user token and entering a PIN number
Card plus code	There is a reader and a keypad connected to this reader position	…presenting a user token and entering a code
Desktop reader	There is a PROXIMITY, CARDLOCK or desktop reader connected at this reader position	
PIN only	There is a TOUCHLOCK keypad connected at this reader position	…entering a PIN number
Code only	There is a TOUCHLOCK keypad connected at this reader position	…entering a code

Figure 4.1
Table showing operating modes

Commissioned – Every ACU should be tested as a part of the commissioning process.

ACU schedule

ACU serial number	Door name	Operating mode		Commissioned
		Reader 1	Reader 2	

ACU schedule

ACU serial number	Door name	Operating mode		Commissioned
		Reader 1	Reader 2	

Cable schedule

The cable schedule sheet is filled in when laying the cable and wiring the system.

Cable number – All cables are numbered. Cable numbers can be written on masking tape or proprietary numbering systems can be used.

Purpose – i.e. reader cable.

From, To – i.e. from ACU12345678 to Junction box 5

Cable type – i.e. 10 core screened

Cable schedule				
Cable number	**Purpose**	**From**	**To**	**Cable type**

Cable schedule

Cable number	Purpose	From	To	Cable type

Cable schedule

Cable number	Purpose	From	To	Cable type

Chapter 5 Fitting

CARDLOCK and PROXIMITY readers

TOUCHLOCK keypads

CARDLOCK and PROXIMITY readers

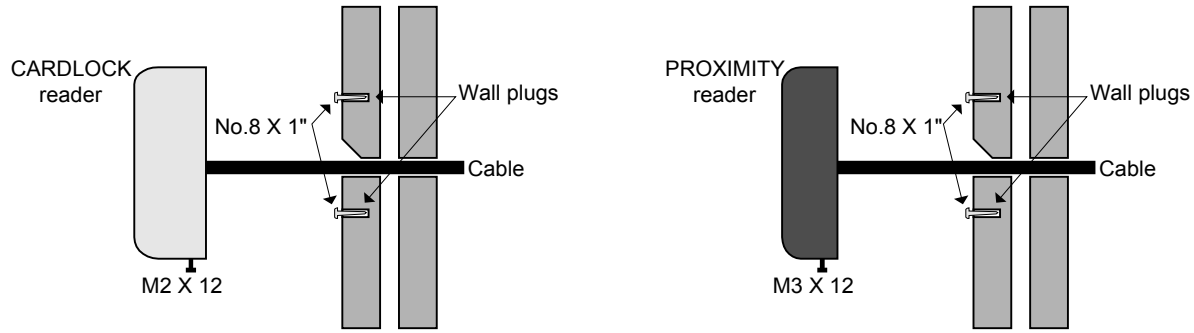


Figure 5.1
Fitting CARDLOCK and PROXIMITY readers

1. Using the template provided with the reader, drill holes for the two fixing screws and the cable.
2. Extend the top of the cable hole to allow the reader to slide down during fitting.
3. Insert the raw plugs and screw in the No.8 X 1" screws until a gap of approximately 2mm remains between the screw head and the face of the wall. Try the reader on the screws and adjust as required.
4. Once a good fit has been achieved, thread the cable through the wall and locate the reader. Lock it into place with the locking screw at the bottom of the reader. If being installed into a vandal risk area, a tamper resistant security screw can be used.

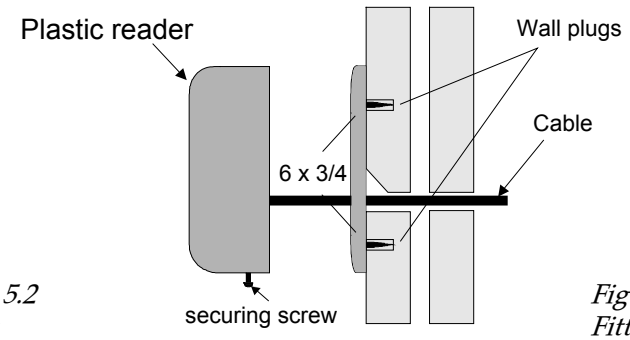


Figure 5.2 Fitting CARDLOCK

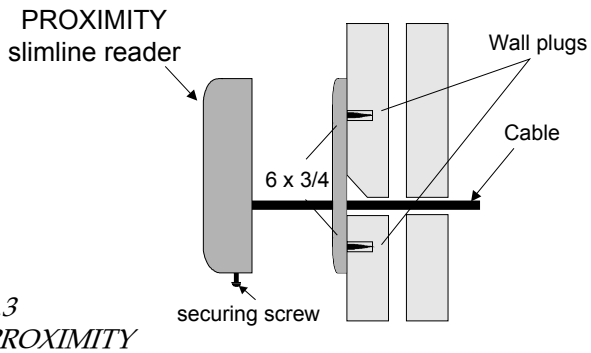


Figure 5.3 Fitting PROXIMITY slimline reader

1. Using the base plate as a template, mark and drill holes for the cable and the four screws.
2. Tap the four small raw plugs into the wall. Fix the base plate securely with the screws provided.
3. Feed the reader cable through the back plate and hang the reader at an angle over the back plate. Then slot the reader into the groove at the top of the base plate and press the reader into place.
4. Screw in the securing screw at the base of the reader.

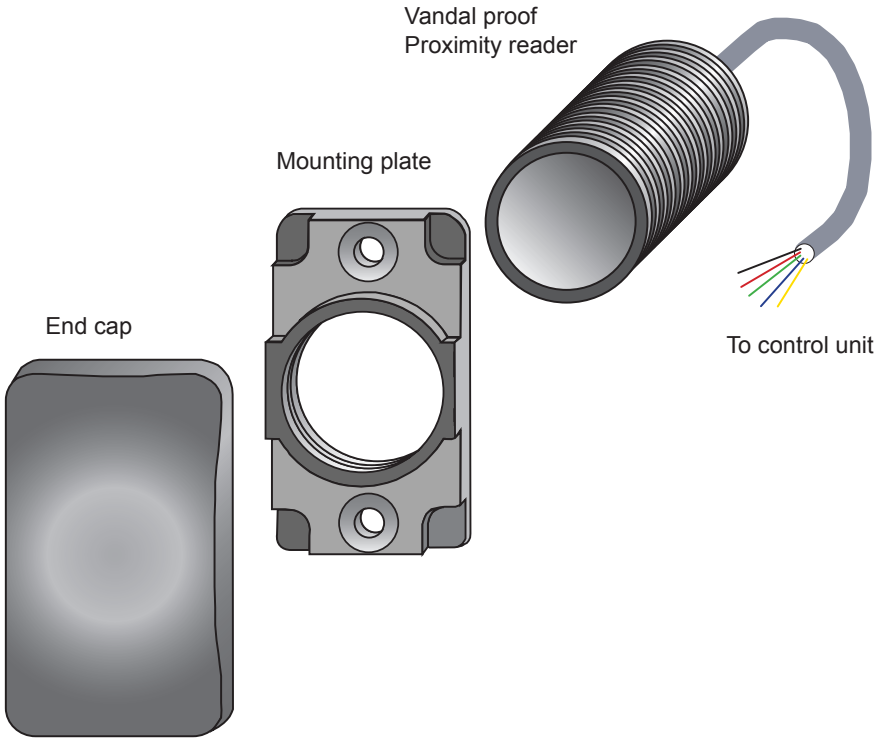


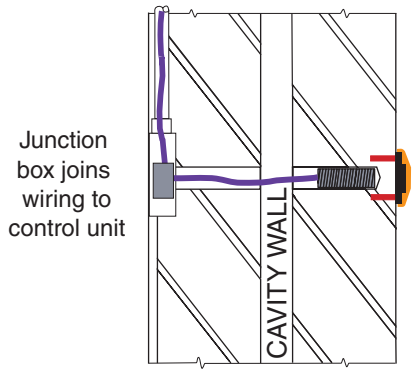
Figure 5.4 Main Components of the PROXIMITY vandal proof reader.

This can be mounted in a variety of different ways to solve all constraints that the installation may have. Its diameter means that only a single 20mm diameter hole has to be drilled, causing minimal installation debris and saving time.

The diagrams below show how the reader can be mounted in the most common types of installations.

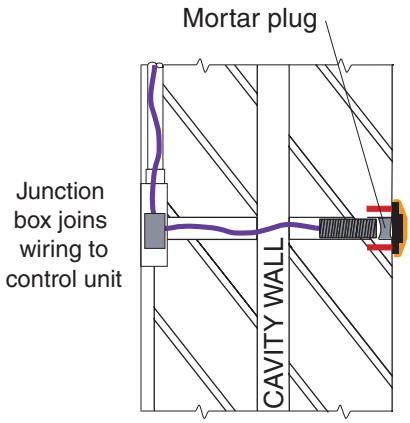
Where the reader is buried in the fabric of the wall it is as vandal proof as the structure.

Figure 5.5



Vandal proof PROXIMITY reader surface mounted from inside wall in a blind hole 20mm short of surface. The plastic end cap is placed over the location of the reader.

Figure 5.6

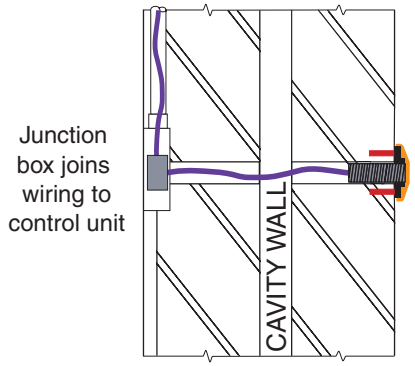


Vandal proof PROXIMITY reader mounted from inside wall, with mortar plug and plastic end cap placed over exposed end of reader.

In fig 5.5 the reader is mounted from the inside wall (Blind hole) and the mounting plate is used for a fixing marker.

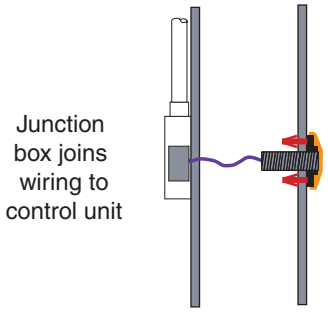
In fig 5.6 the reader is also mounted from the inside and the mounting plate is used for a fixing marker.

Figure 5.7



Vandal proof PROXIMITY reader surface mounted onto wall using mounting plate. The threaded reader body is screwed to the plastic end cap which is fixed to the wall.

Figure 5.8



Vandal proof PROXIMITY reader surface mounted onto a hollow wall. using the mounting plate. The plastic end cap is placed over the mounting plate.

In fig 5.7 the reader is surfaced mounted using the mounting plate.

In fig 5.8 the reader is surface mounted on a hollow wall using a mounting plate.

Fitting the vandal proof reader using the end cap

1. Using the back plate as a template, mark and drill holes for the PROXIMITY vandal proof reader and the two screws.
2. Tap the two small raw plugs into the wall.
3. Feed the reader cable through the back plate and then screw the back plate onto the reader. (about 4 or 5 complete turns)
4. Secure the back plate onto the wall with the 2 (6 x ¾) screws provided.
5. Secure one side of the end cap onto the back plate and then snap the end cap onto the back plate.

TOUCHLOCK keypads

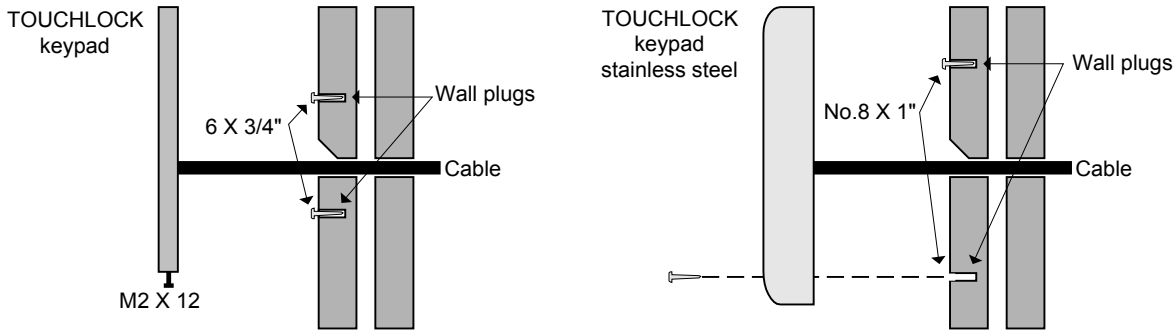


Figure 5.9
Fitting TOUCHLOCK keypads

1. Using the template provided with the keypad, drill holes for the two screws and the cable.
2. Extend the top of the cable hole to allow the keypad to slide down during fitting.
3. Insert the raw plugs and screw in the 6 X ¾" (only the top No.8 X 1" for the stainless steel keypad). Leave a gap of approximately 2mm between the screw head and the face of the wall. Try the keypad on the screws and adjust as required.
4. Once a good fit has been achieved, thread the cable through the wall and locate the keypad. Lock it into place with the locking screw at the bottom. If being installed into a vandal risk area, a tamper resistant security screw can be used.

Plastic ACU enclosure

1. Mount the housing backplate against the wall and secure using the raw plugs and No8 X 1 screws provided in the fitting kit.

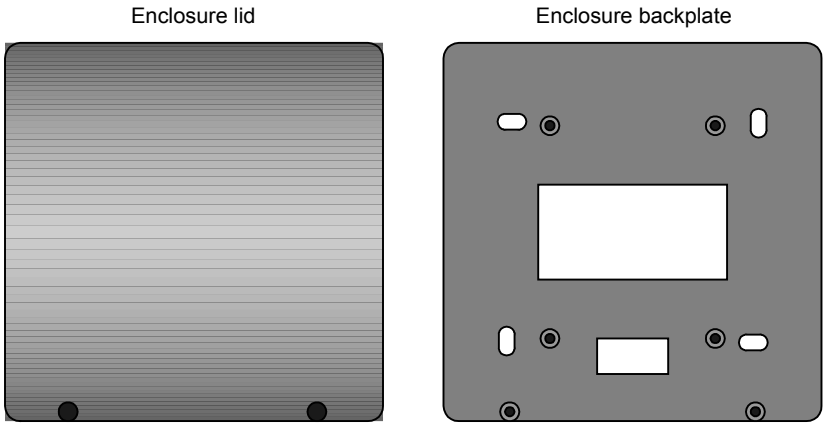


Figure 5.10
Fitting the plastic enclosure

2. The ACU can be secured into the housing using the No6 X 12 screws provided in the fitting kit.
3. The lid can be fixed in place using the remaining 2 No6 X 12 screws.
4. Cut-outs and loops for cable ties are provided.

Chapter 6 Wiring

This section covers wiring. Please read the About… section before attempting installation.

CARDLOCK readers

CARDLOCK and PROXIMITY readers are supplied with 5m of cable. The colours of the cable cores correspond to the labelling on the Net2 ACU. If the cable distance is to be extended then the cores that carry power to the reader must be doubled up as shown.

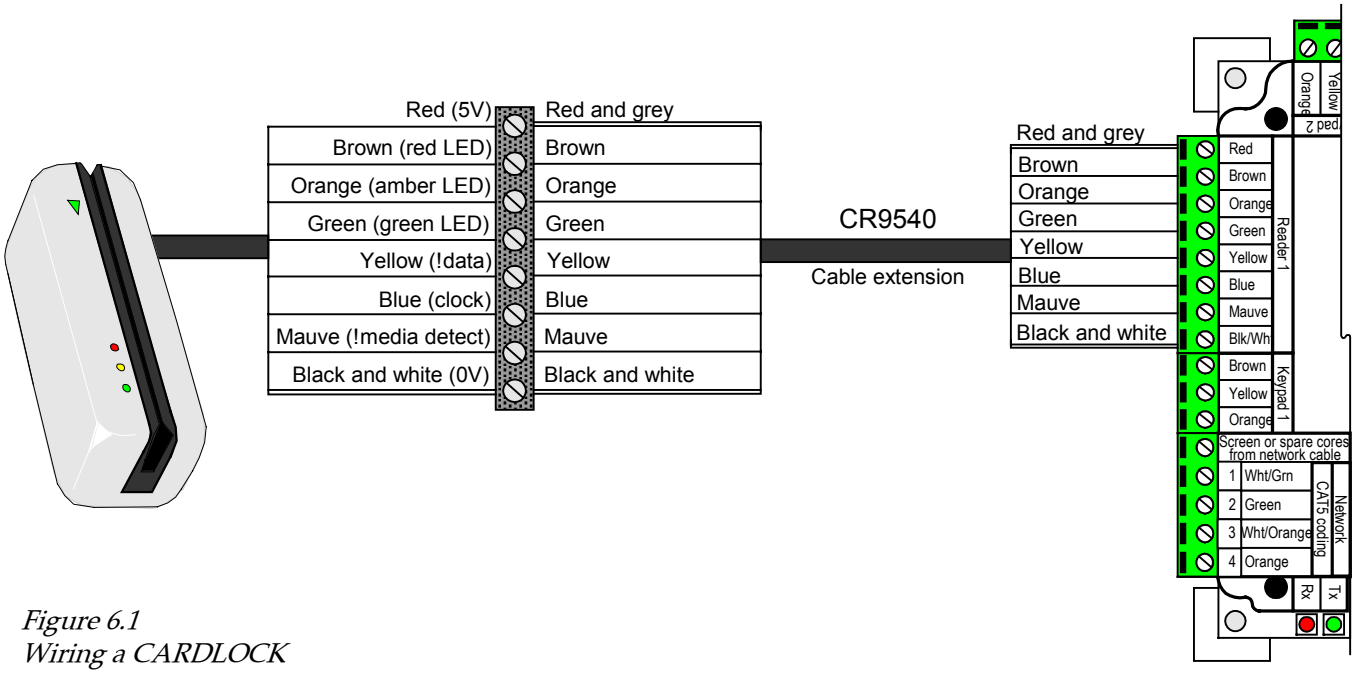


Figure 6.1
Wiring a CARDLOCK reader cable extension

PROXIMITY readers

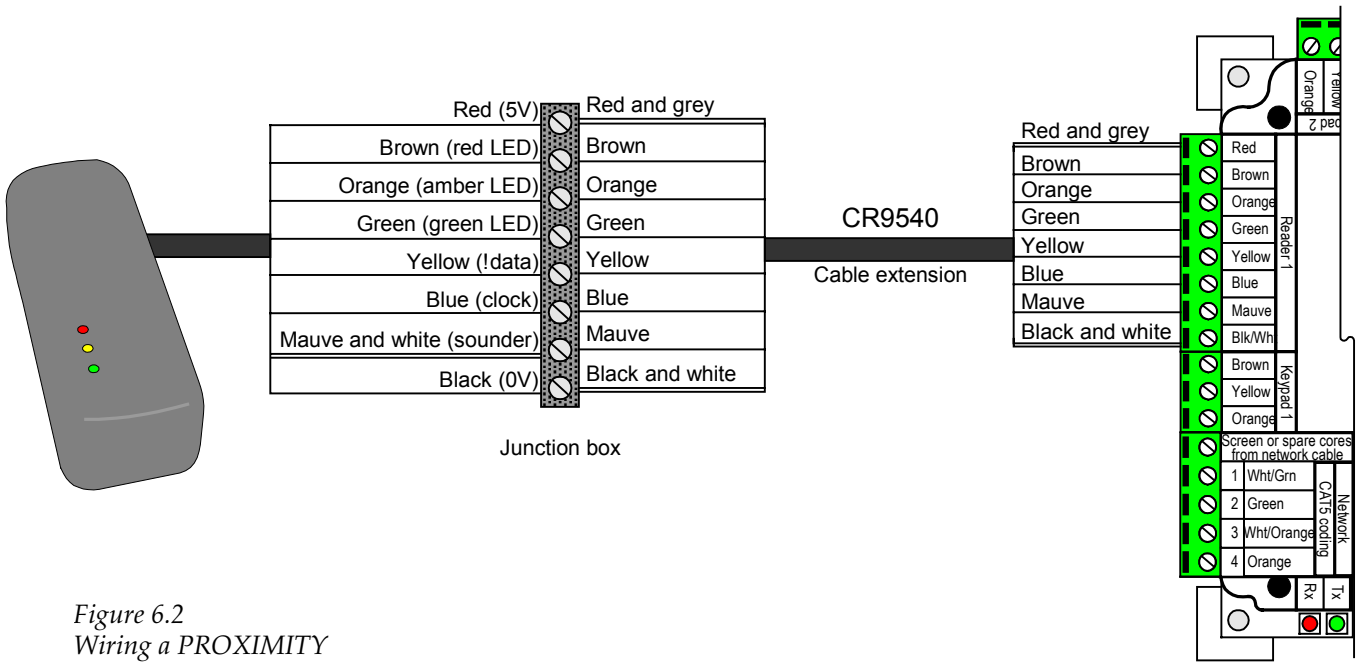


Figure 6.2
Wiring a PROXIMITY reader cable extension

The cable screen must be connected to 0V (Blk/Wht terminal) when wiring all readers or keypads.

PROXIMITY slimline readers

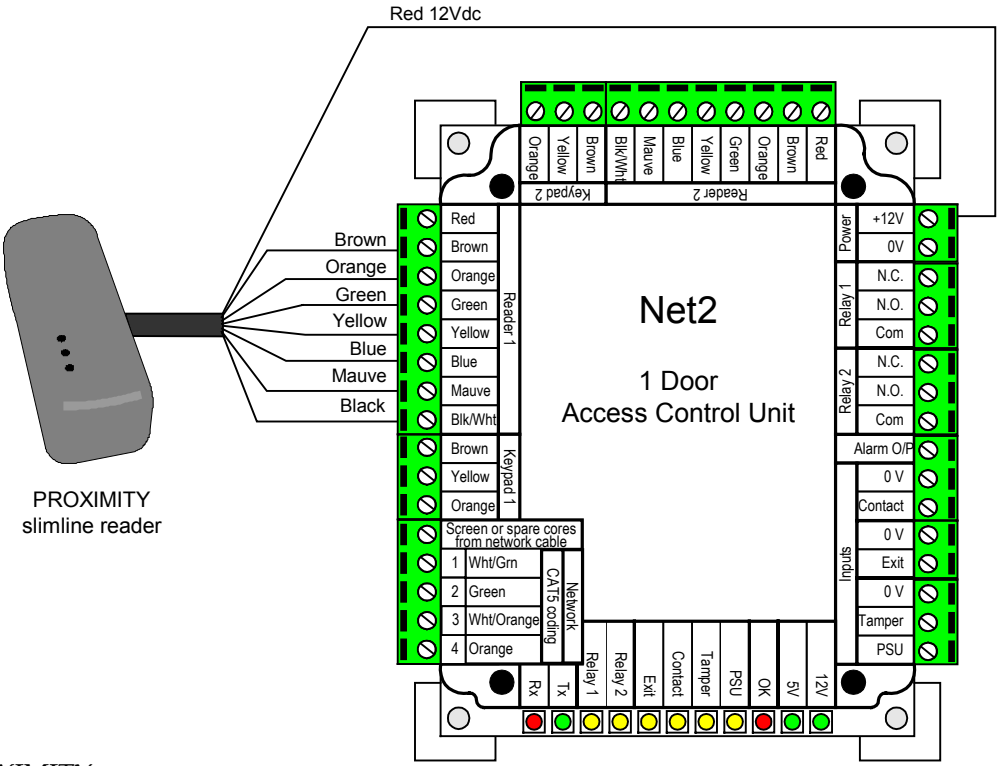


Figure 6.3
Wiring a PROXIMITY Slimline reader to Net2

Vandal proof readers

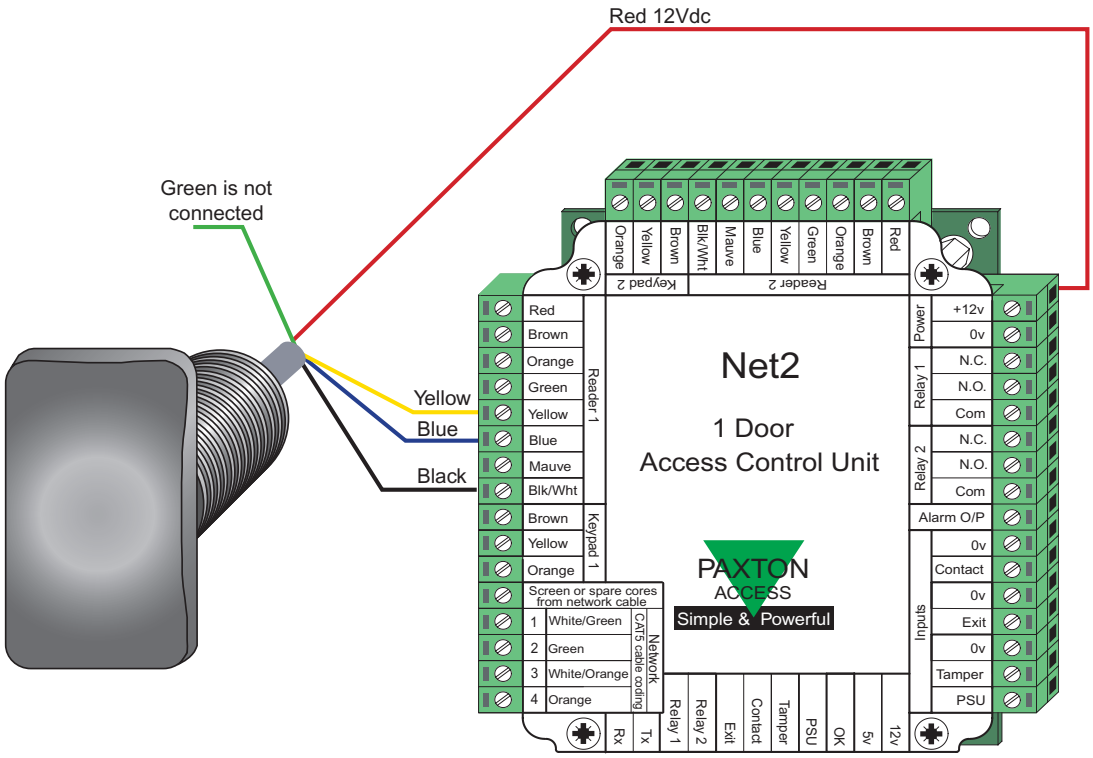


Figure 6.4
Wiring a PROXIMITY vandal proof reader to Net2

TOUCHLOCK keypads

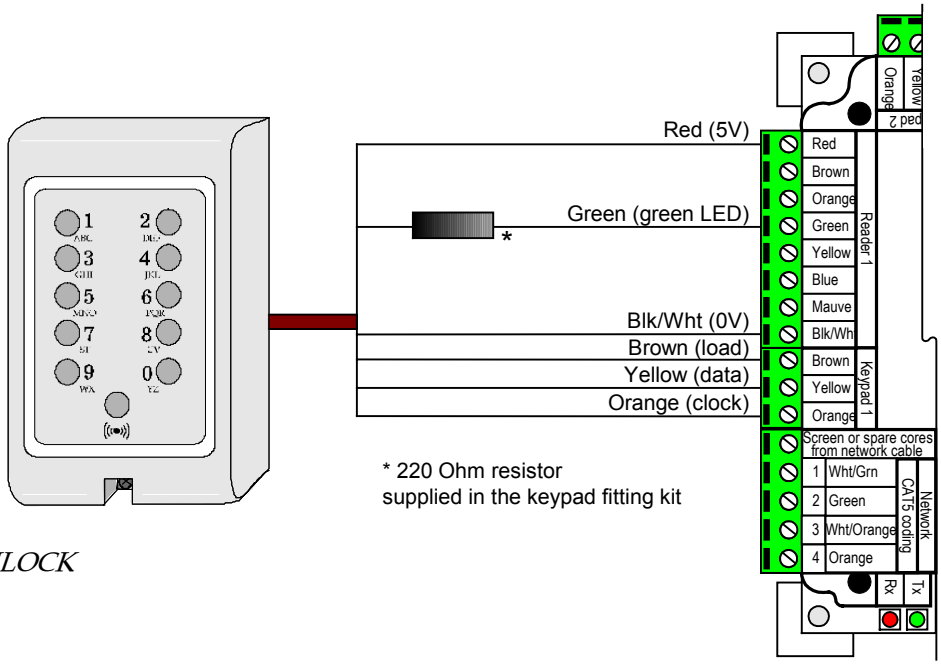


Figure 6.5
Wiring a TOUCHLOCK keypad to Net2

To save space on the board, a keypad wired to the Net2 ACU shares power and LED terminals with the reader.

If using a membrane keypad with the Net2 system the cable should not be extended over 5m.

Power supply

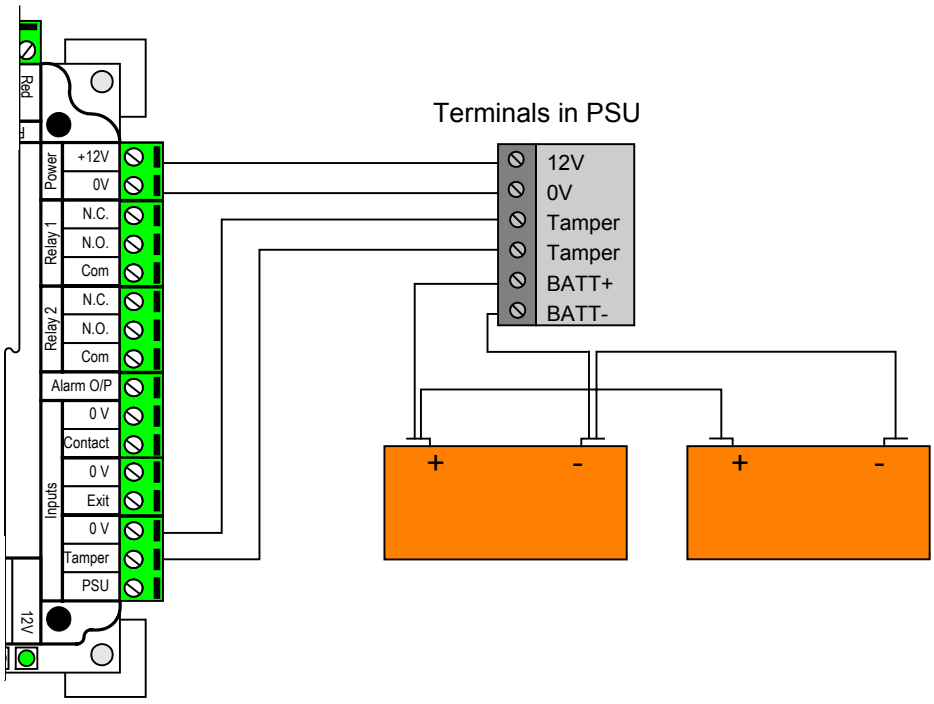


Figure 6.6
Wiring a power supply

Inputs and outputs - inputs

Exit button

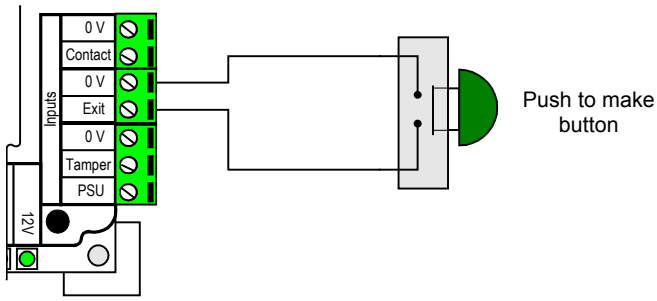


Figure 6.7
Wiring an exit button

Door contact

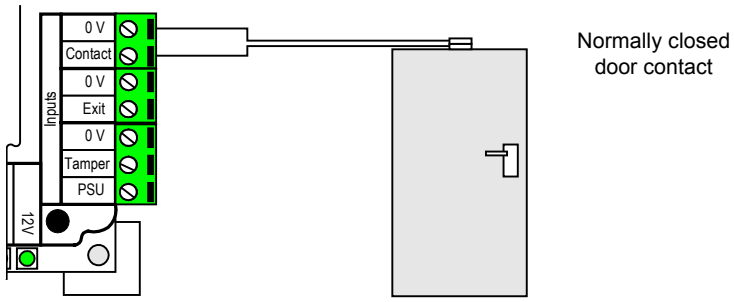


Figure 6.8
Wiring a door contact

Power supply tamper

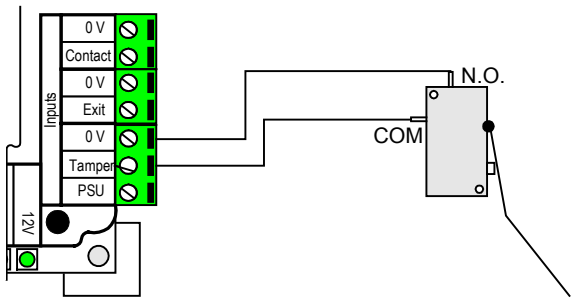


Figure 6.9
Wiring a power supply tamper switch

PSU – mains monitoring

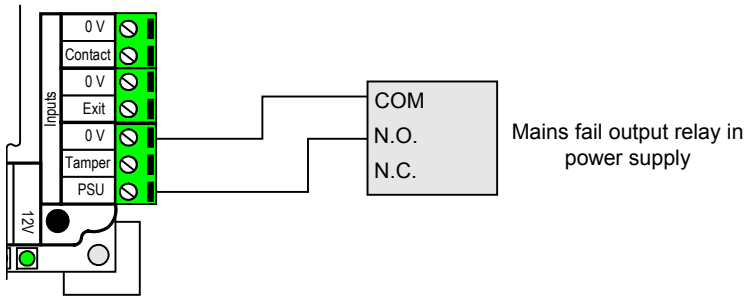


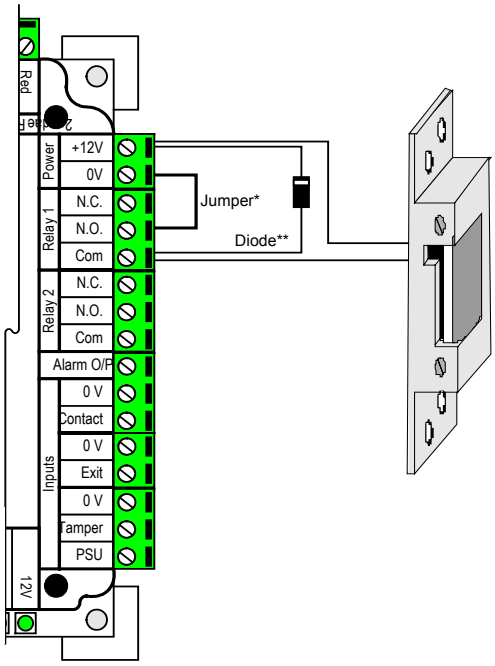
Figure 6.10
Wiring mains monitoring

Inputs and outputs - outputs

Relay 1 - lock

Wiring schematic illustrates wiring for the two main types of 12Vdc electric release mechanism. Other electrical devices can be switched using the voltage free relay contacts.

Fail closed



Fail open

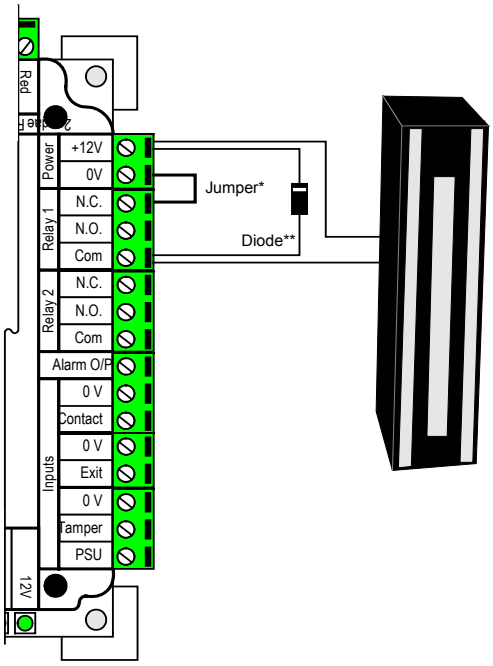


Figure 6.11
Wiring a lock

* The jumper is very important. Without it the lock will not work.

** Diode is supplied in the fitting kit. Reference: 1N4001 (only suitable for locks up to 1A). Diode must be fitted with correct orientation as shown in figure 6.11.

Other electrical devices can be switched using the voltage free relay contacts.

If an ac lock is used then a transient absorber must be fitted across the lock.

Relay 2 – sounder

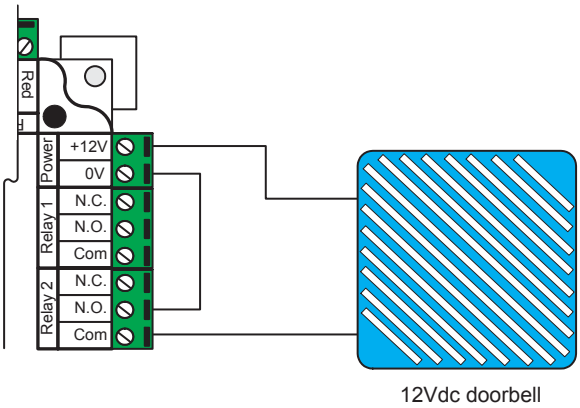


Figure 6.12
Wiring a sounder

If an ac device is used then a transient absorber must be fitted across the device.

General purpose output – alarm sounder

This is an open drain output and is capable of switching 1Amp at 12-24Vdc. The load of this output must be taken into consideration when selecting a suitably rated power supply, refer to *About…/Power supplies/Choosing guide.*

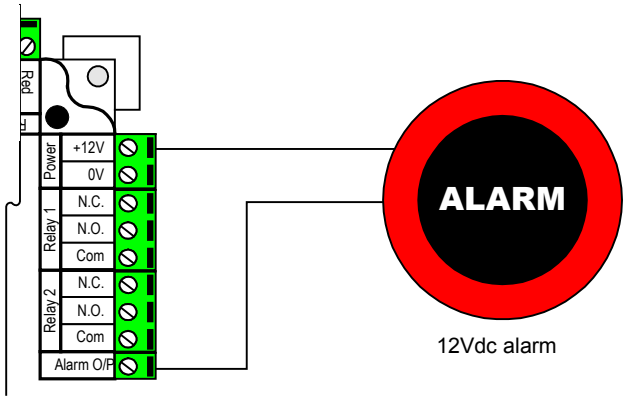


Figure 6.13
Wiring an alarm sounder

Wiring into a fire alarm

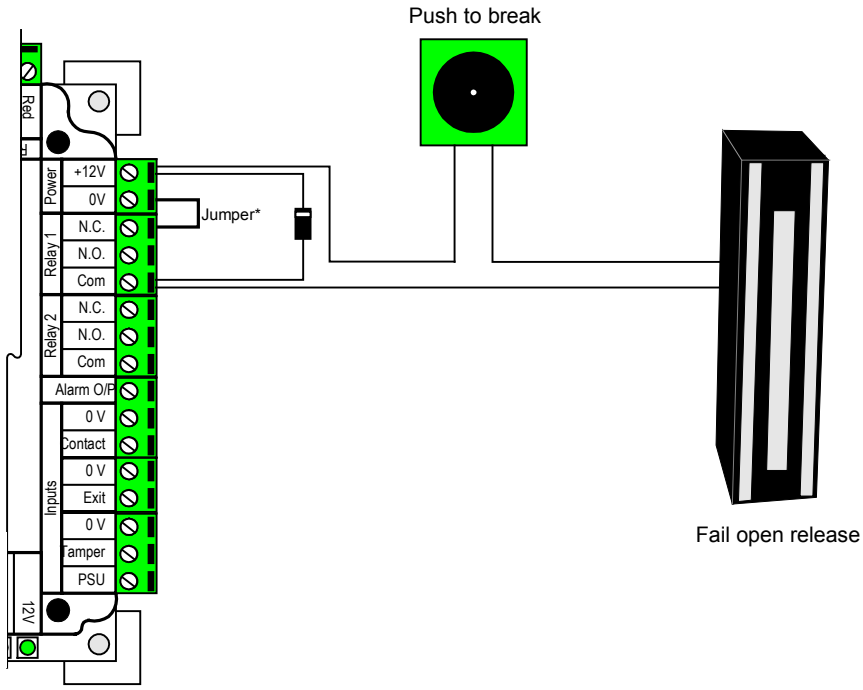


Figure 6.14
Wiring into a break glass local to the door

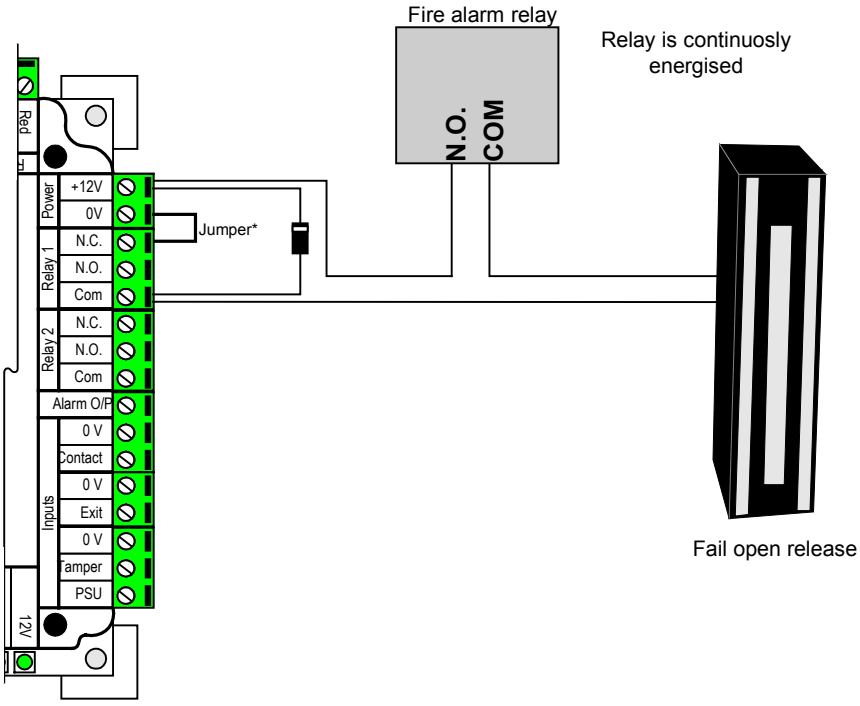


Figure 6.15
Wiring into a fire alarm system relay

* The jumper is very important. Without it the lock will not work.

Software controlled fire doors

Fire doors can also be configured through the Net2 software. A fire alarm relay, whose contacts will open in the event of a fire alarm, can be wired into any unused input of any control unit. For instance, to wire it into the Tamper input, it should be connected between 0V and the Tamper input. Under the doors configuration for the ACU with the fire alarm relay connected to it, on the Fire doors tab, you can specify which input is to be used as the fire alarm input (Tamper in this case) and which doors should open. It is also possible to specify that a roll call report for a certain area group should be generated if a fire alarm should occur.

Important note: This feature requires the Net Server to be running, and the network to be functional. If the server is not running for any reason, this feature will not operate as expected. Consequently, break-glasses should be fitted, in conjunction with fail open releases, to all fire doors, to ensure a reliable egress method in the event of an alarm.

Data line cable

Apart from at the ends of the data line, there will be an incoming and outgoing cable at each ACU. The ACU has a connection label showing CAT5 connection colour coding. CR8723 cable has 2 individually screened twisted pairs. White/Green and Red/Black. If CR8723 cable is used, it should be connected 1-White, 2-Green, 3-Red and 4-Black.

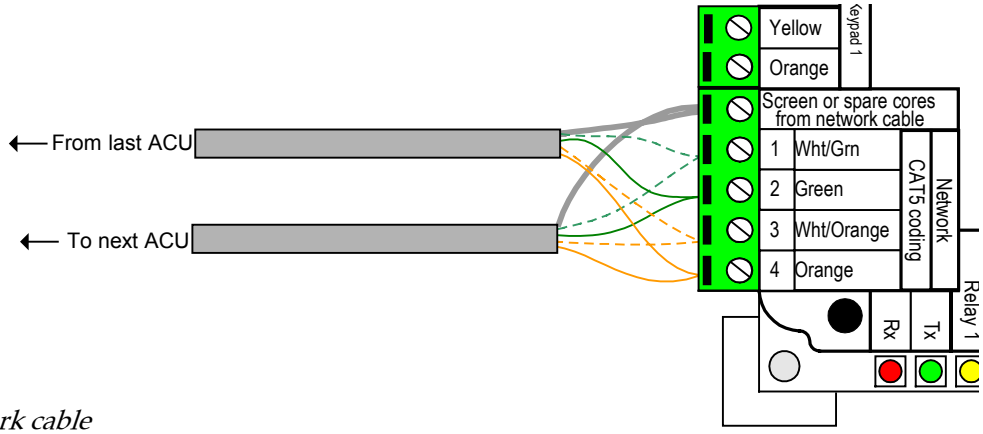


Figure 6.16
Wiring the network cable

All screens need to be wired into the Screen terminal. If unscreened cable is used, all unused cores should be wired into the Screen terminal.

120 Ohm termination resistors are required at either end of the data line. These are supplied in the fitting kit.

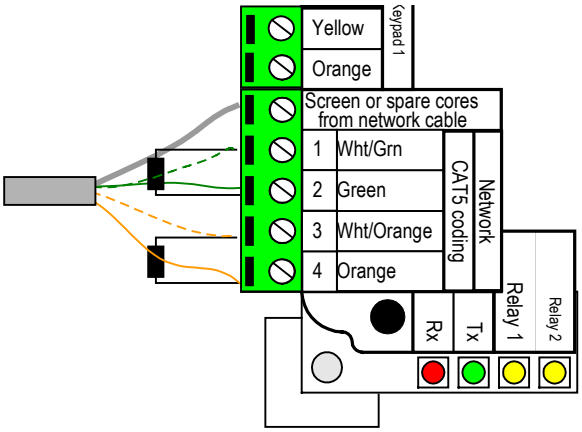


Figure 6.17
Wiring the termination resistors

RS485/232 communications converter

The PC with the RS485/232 interface can be positioned at the most convenient point along the network. The wiring is the same as at the ACUs.

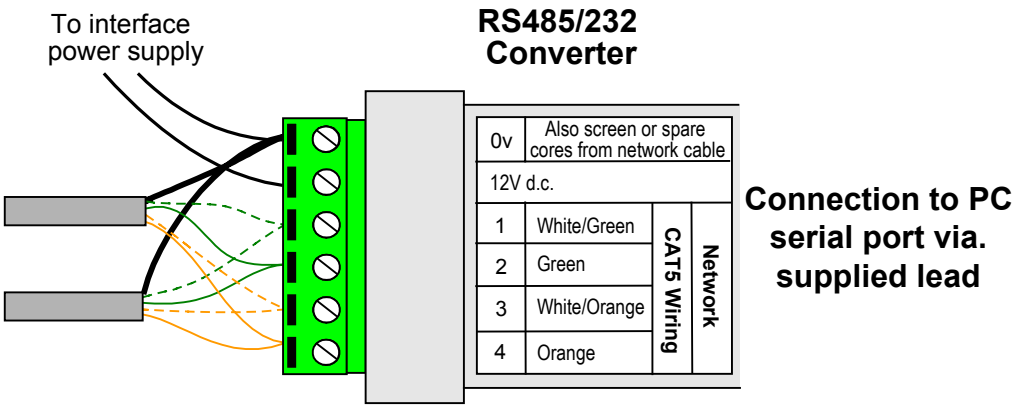


Figure 6.18
Wiring the RS485/232 communications converter

IMPORTANT NOTE:

The latest R485/232 converters do not contain termination resistors. If the converter is wired at the end of the network two 120 Ohm resistors must be wired between terminals 1 and 2, and 3 and 4.

Older RS485/232 converters may contain termination resistors. This type can be identified by two internal jumpers. If this type of converter is wired at the end of the network then these are left in place. Otherwise these jumpers have to be removed (JP1 and JP2 from converter PCB).

RS485 repeater

The RS485 repeater allows the data line to be extended beyond 1 Km and should be installed within this limit. It is recommended that only one repeater be used per data line.

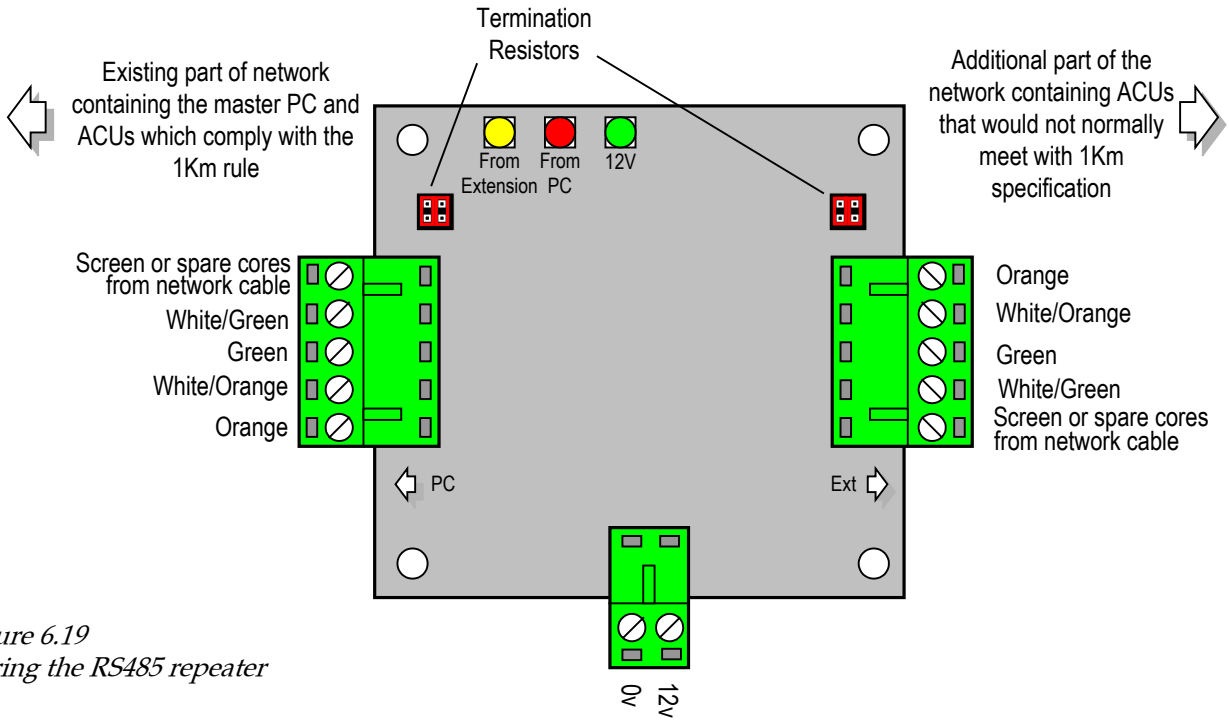


Figure 6.19
Wiring the RS485 repeater

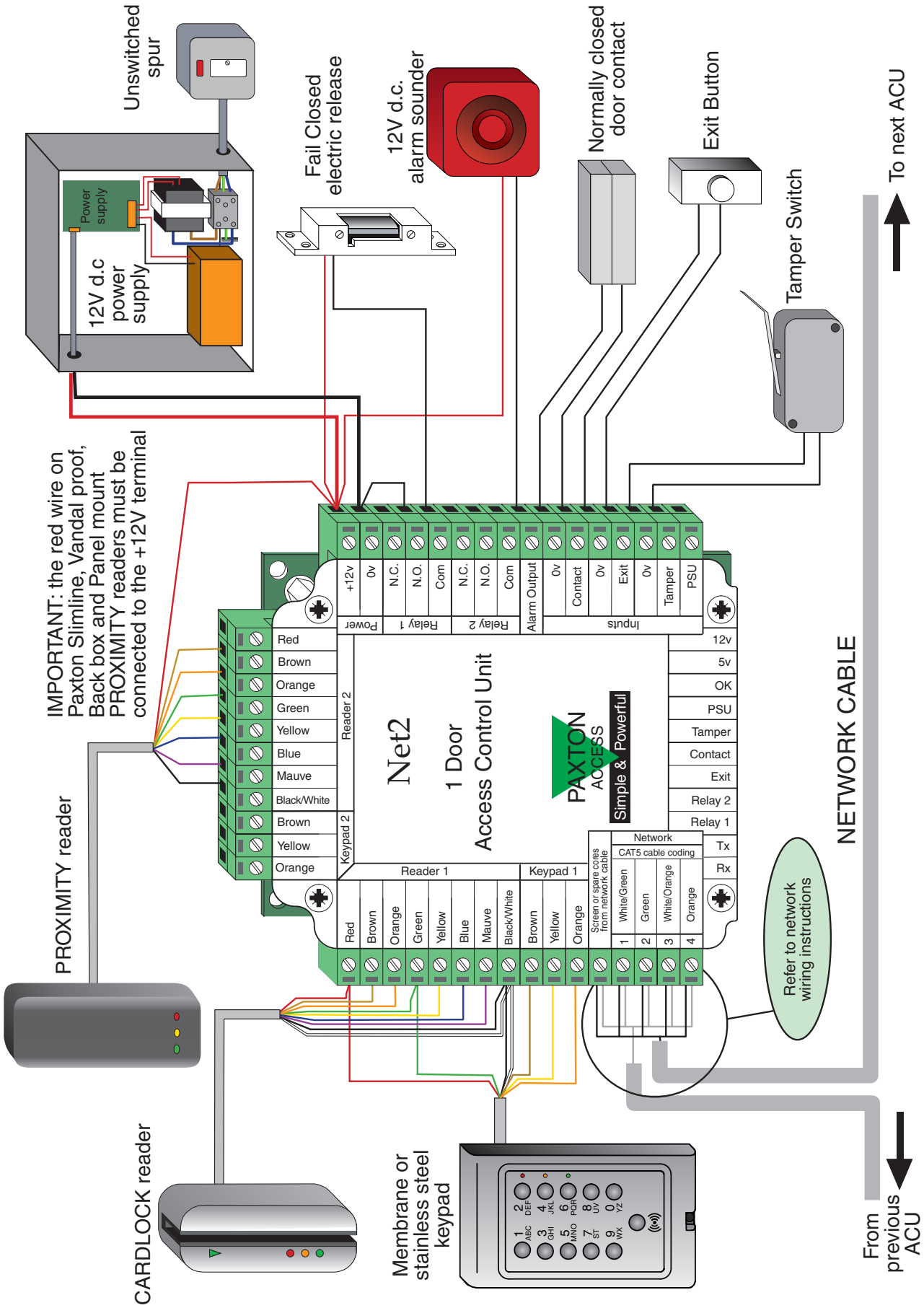


Figure 6.20
Wiring summary

Chapter 7 Commissioning

Hardware

Software

Hardware – network

Before power is applied to the system, the network must be checked. Check all network connections. Before testing, remove the network terminals from every ACU.

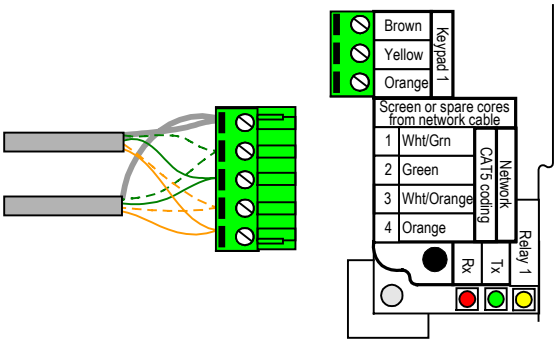


Figure 7.1 Remove network connections

Data cable

The resistance between each pair must be measured. This ensures that the termination resistors are connected and the cable is continuous.

1. Using a Multimeter, measure the resistance between terminals 1 and 2 of the network connection.. A resistance of between 50 and 70 Ohms is normal.
2. Repeat step 1 for terminals 3 and 4.

If the measured resistance is not within the recommended range then connections and cable should be checked throughout until the fault is found.

Screen shorts

1. At one end of the network check the resistance between the screen and terminal 1 of the network connection. The resistance should be high. This means that the screen is not shorted with this core along its length.
2. Repeat step 1 for terminals 2, 3 and 4.

If the measured resistance is low then the cable and connections should be checked.

Screen continuity

To ensure resilient communications, the network cable is screened. It is essential to the reliability of the system that the screens are continuous. To check this:

1. At one end of the network, connect the screen to terminal 1.
2. At the other end of the network, use a multimeter to check that the resistance between screen and terminal 1 is low (Less than 10 Ohms).

If the screens are not continuous then the cable and connections should be checked.

Once the network has passed the tests, the network terminals must be replaced in the ACU.

Hardware – the Access Control Unit (ACU)

Once all wiring has been completed and the system is ready to go, each ACU will require commissioning.

Turning on the power

If an ACU has a backup battery power supply, the mains should be connected first. Once mains power is being supplied to the ACU, the batteries can be connected. This will prevent damage to batteries caused by a sudden surge of current. If power to the ACU is being switched off, batteries should be disconnected before the mains is switched off.

ACU test

The diagnostic LEDs allow the functionality of each ACU to be tested quickly and accurately.

Check that the…	If not…
12V and 5V LED's are on.	Power supply problem, refer to *Fault-finding/system problems*.
OK LED is pulsing regularly?	Processor problem, refer to *Fault-finding/system problems*.
Exit LED is on when the exit button is pressed.	Input problem, refer to *Fault-finding/system problems*.
Contact LED is on when the door is closed.	Input problem, refer to *Fault-finding/system problems*.
Tamper LED is on when the circuit is closed.	Input problem, refer to *Fault-finding/system problems*.
PSU LED is on when the circuit is closed.	Input problem, refer to *Fault-finding/system problems*.
Present or swipe a user token through all readers connected to the ACU. The red LED should flash to indicate an invalid card.	Reader problem, refer to *Fault-finding/system problems*.
The Door relay 1 LED comes on when the exit button is pressed. If there is no exit button then jumper the exit button terminals with a piece of wire.	Output problem, refer to *Fault-finding/system problems*.

Figure 7.2
ACU commissioning test

Every ACU should be tested in this way before installing or running the software.

Software – installing the program

IMPORTANT NOTE

The Net2 software requires Internet Explorer 4 or greater. If this is not already installed on the PC then it is available on the Net2 CD. To install, simply run D: \IE6.0\ie6setup.exe (Where D is the drive letter of the CD Rom drive)

1. Load the CD into the drive.
2. The setup application can be automatically run (if autorun is enabled), otherwise setup can be run using Add/Remove Programs or by browsing to the CD drive and running Setup.EXE.
3. You will be warned that other applications should be closed down before installing the Net2 software. If there are any other programs running then press **Cancel** and close them before running setup. If there are no other programs open then press **Next** and proceed with installation. You will need to accept the license agreement before being able to proceed to the Registration Information. The CD key is supplied with the CD.
4. Enter the details of the registered owner of the Net2 software. All fields must be filled in to proceed.

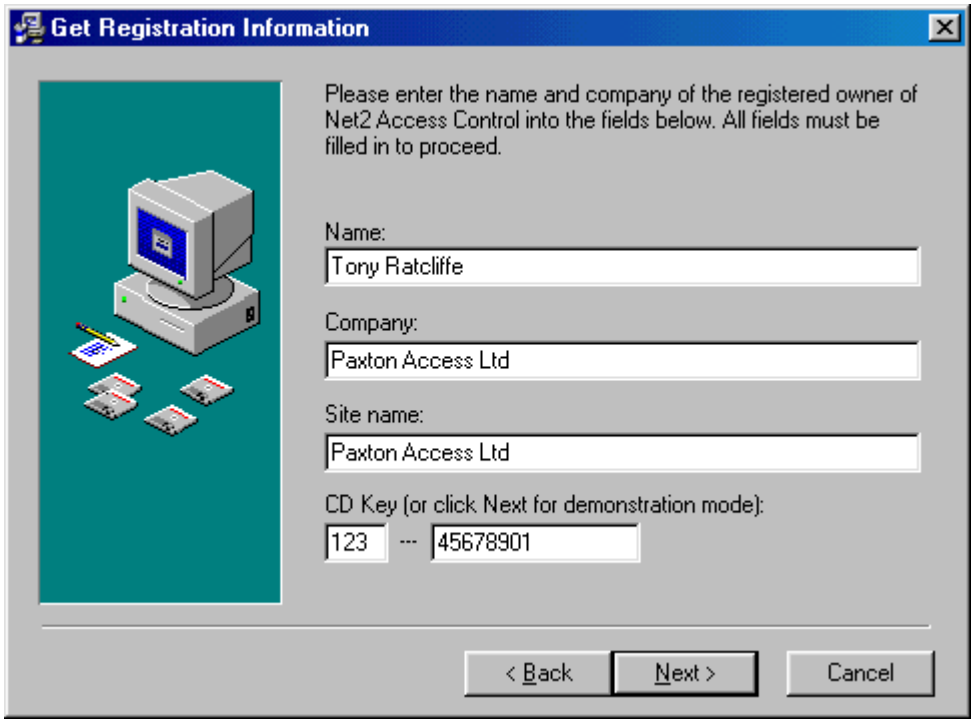


Figure 7.3 Get Registration Information

If the software is to be installed in demonstration mode (with a sample database with which to demonstrate the functionality of the software) then do not enter anything. Press **Next** to continue with the installation.

5. The Net2 software consists of the application (the program itself) and the database (where events, user details, system information etc. is held). Enter the desired locations for the application and the database. The default location for the application is **C:\Program Files\Paxton Access** and this would ordinarily be correct.

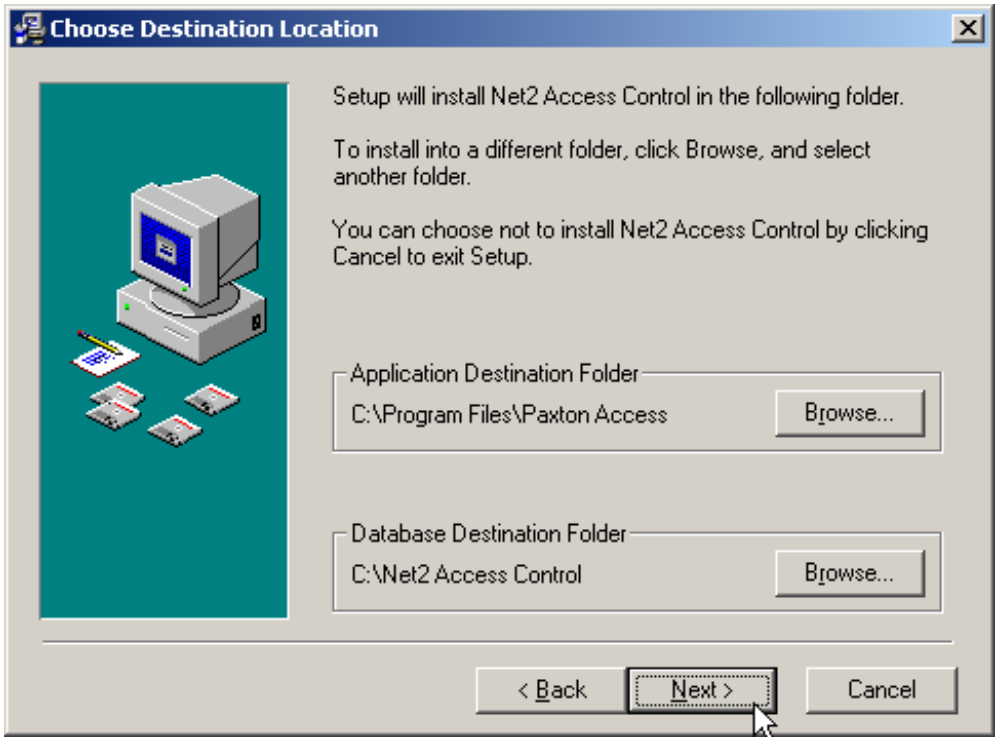


Figure 7.4
Choose Destination Location

The default location for the database is **C:\Net2 Access Control**

6. In Net2 V2, it was necessary to enter which comport should be used. Net2 V3 supports multiple comports, and features the auto detection of Net2 control units. No comport selection is required.

7. Next you must choose the options that you want to install. Only select **Advanced** if you want to set up the advanced options. These include **Areas**, **Anti-passback**, **Roll Call** and **Cameras**. Anti-passback and Roll Call require areas to also be enabled.

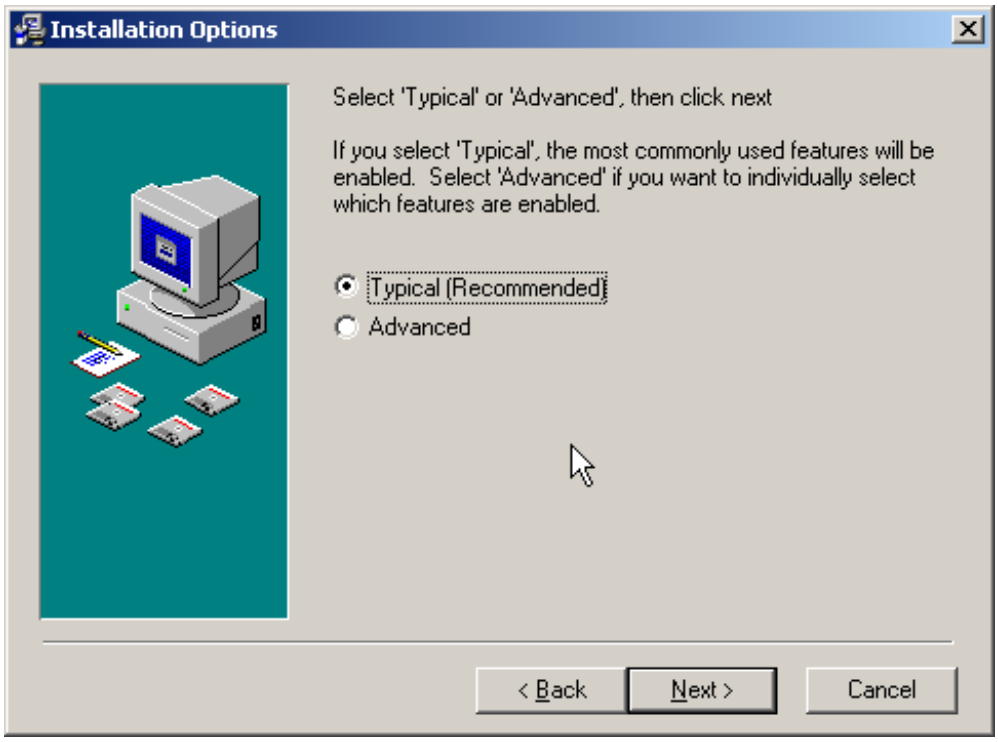


Figure 7.5
Choose Install Options

8. Select **Yes** or **No** to backup files being kept. Keeping backup files will allow you to undo the installation. Press **Next** to continue.

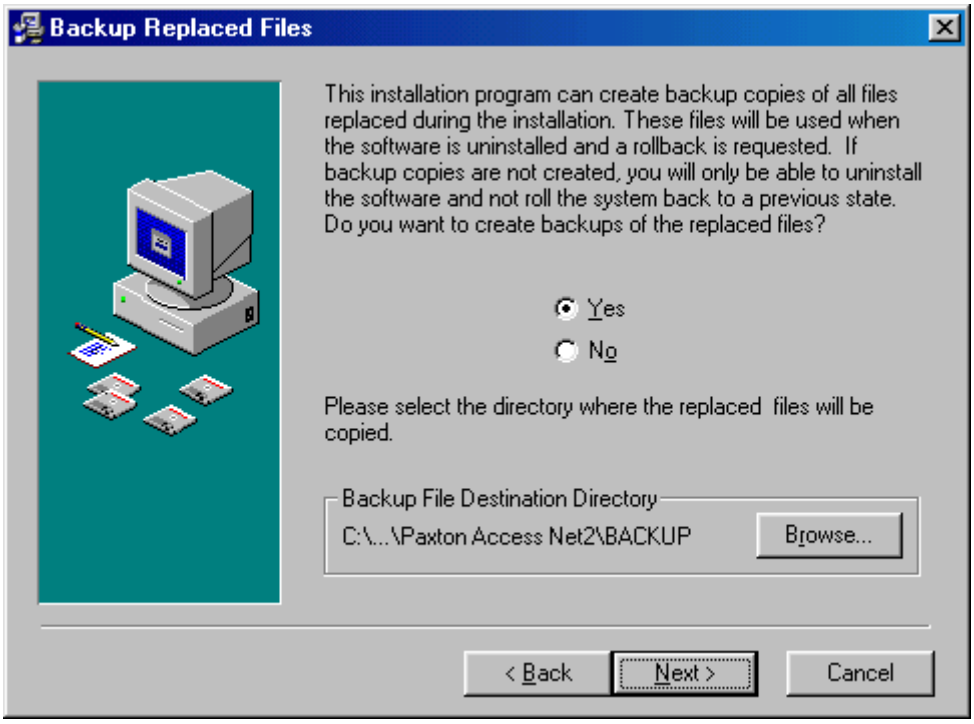


Figure 7.6
Backup Replaced Files

9. Enter the location for the shortcut in the start menu. The default location is Net2 Access Control in Programs.

10.

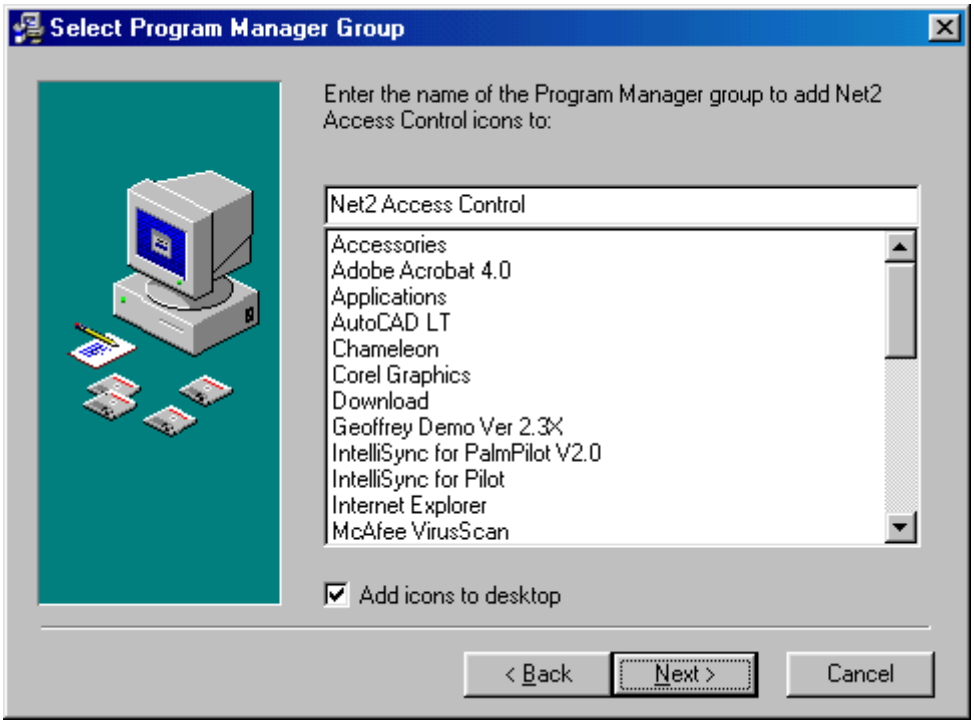


Figure 7.7
Select Program Group

Select whether the Net2 shortcuts should be added to the desktop. Press **Next** to continue.

11. Press **Next** to start installing the application files. Installation should take no more than a minute.

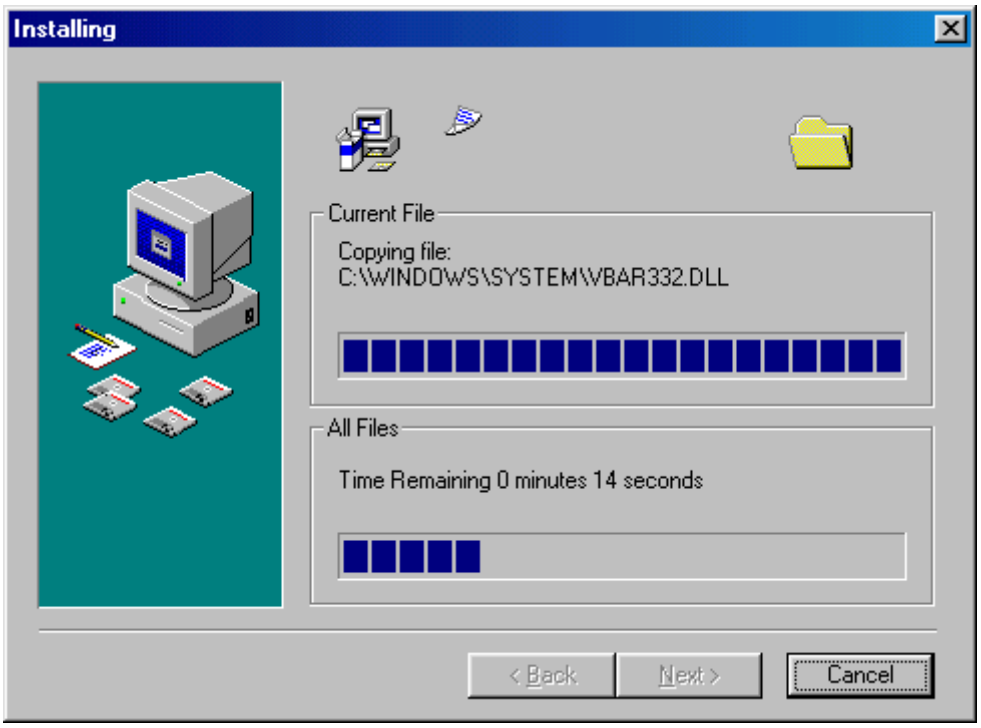


Figure 7.8
Installing

12. Once the application files have been copied, press **Finish** to exit.

If problems occur, please refer to *Fault-finding/system problems.*

Software – installing the database

1. Run the Net2 program by double clicking on the Net2 Access Control shortcut. The Net2 Server will start-up automatically, creating a new database if necessary, and detecting any control units which are connected. It will open all available comports, and once it has finished interrogating the network, will close down any which do not connect to Net2 control units.

> ***If you have run the Net2 Access Control application before and wish to 'start from fresh' then delete the system database (Net2system.mdb). The default location for this is C:\Net2 Access Control.***
>
> ***Warning: All system settings are held in the database.***

2. The default operator is **System engineer** with the password '**net2**' (Warning – the password is case sensitive).
3. Once into the software select **Operators\System Engineer.** Enter a new password and confirm.

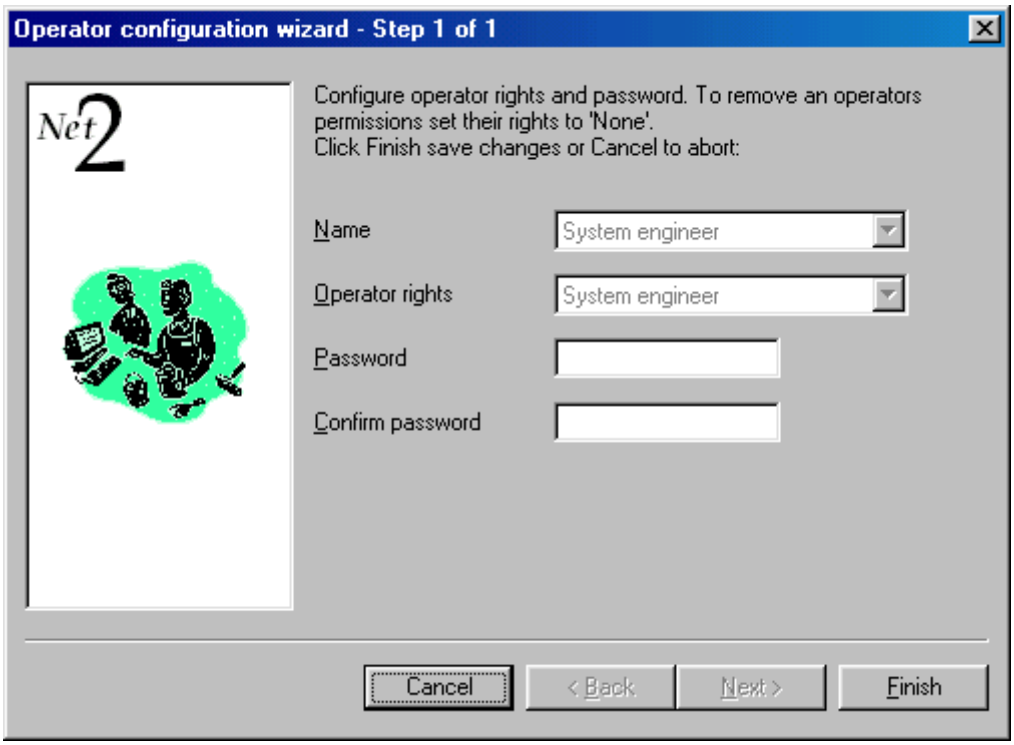


Figure 7.9
Operator Configuration Wizard

> ***This password will completely restrict access to the program. Make a note of the password:***

This password must now be used to gain access to the Net2 Access Control application. Press **Finish** to save changes and exit the wizard.

5. The Net2 Server will automatically upgrade the firmware of ACU's as necessary. Under normal circumstances this will only occur if the installation is new, or following a software upgrade.

Software – configuring the doors

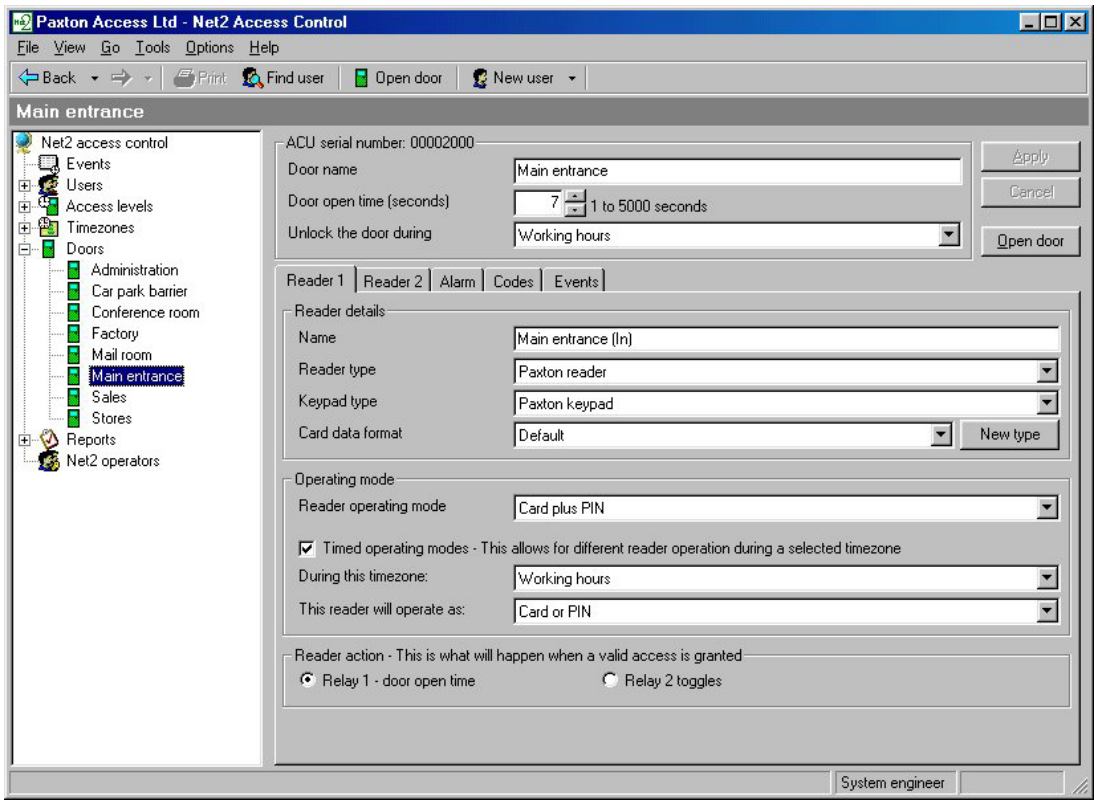


Figure 7.10
Configuring the doors - Reader1

The settings for each control unit are configured in this screen. The ACU serial number is shown in the top left corner of the main display. The lower section of the main display has tabs that allow access to the different settings (Reader1, Reader2, Alarm, Codes and Events). Sections are accessed by clicking on the relevant tab.

Door name

When the system is first powered up, the control unit name will be the same as the serial number. A descriptive name should be given to a control unit. This name will appear in the list of doors.

Door open time

The door open time is the amount of time that the output relay is switched for (the amount of time that the locking mechanism is released). The default setting is 7 seconds. This can be modified within the range 1 to 5000 seconds.

Unlock the door during

This feature allows the user to select a timezone in which the locking mechanism is released. If the working hours timezone is selected, the door will be open during working hours. An example of where this may be useful is where a receptionist is present to greet visitors during office hours. The main door can be left open so that anybody can walk in. Out of working hours the door is automatically locked and a valid user card is required to gain access.

A door can be held open during any timezone. For more information on timezones refer to *About... \ Timezones*.

Apply

When any changes are made to the door settings the Apply button must be pressed to commit the changes to the database.

Open door

The open door feature will release the locking mechanism for the door open time.

Doors\[Door name]\Reader 1

The Reader 1 tab shows the settings corresponding to Reader 1 and Keypad 1 connected to that control unit.

Name

The default name for reader 1 is [Door name] (IN). The default name for reader 2 is [Door name] (OUT).

The reader names set here will appear in reports and be used to set access levels.

Reader type

This should be set to the relevant type of reader.

Setting	Description
None	If no reader is connected.
Paxton reader	If a CARDLOCK or PROXIMITY reader is connected.
Clock and data	If a non – Paxton clock and data reader is connected
Wiegand	If a Wiegand reader is connected.

Keypad

This should be set to the relevant type of keypad.

Setting	Description
None	If no reader is connected.
Paxton keypad	If a TOUCHLOCK keypad is connected.

Card data format

Every card enrolled on a Net2 system must have a unique number. The card data format option allows Net2 to use cards and tokens with a variety of encoding formats.

The default setting is for the Net2 encoded cards and tokens (random 8 digit number).

Setting	Description
Default	This is for Net2 encoded cards and tokens (random 8 digit number).
Paxton cards	This is for CARDLOCK and PROXIMITY cards and tokens (encrypted number).
Bank cards	This allows Net2 to use bank cards.

Refer to *About… \Options \Card data formats* in the User reference manual for more detailed information.

Reader operating mode

The correct operating mode should be selected from the drop down menu.

Setting	Description
Inactive	There is no reader or keypad connected (or they are inactive for some other reason).
Card only	Access is granted by swiping a valid user card.
Card plus PIN	Access is granted by swiping a valid user card AND entering the relevant PIN.
Card plus code	Access is granted by swiping a valid user card AND entering a valid code.
Desktop reader	A desktop reader is connected. This reader is to be used to add users to the system.
PIN only	Access is granted by entering a valid PIN.
Code only	Access is granted by entering a valid code.
Card or PIN	Access is granted by swiping a valid card OR entering a valid PIN.
Card or code	Access is granted by swiping a valid card OR entering a valid code.
Card, PIN or code	Access is granted by swiping a valid card OR entering a valid PIN OR entering a valid code.

For information on the difference between PIN and code, refer to *Appendix \Difference between code and PIN*.

The list of operating modes displayed in the drop down menu is dependent on the reader type and keypad type settings. For example, if a keypad is configured without a reader, only Inactive, Code only and PIN only will be displayed in the drop down menu.

Timed operating modes

This feature allows a different operating mode within a timezone. For example, card plus PIN may be required outside working hours and card only within working hours.

To configure this, select the required timezone from the drop down menu. Select the required operating mode from the other drop down menu.

Reader action

This is the action that will happen when access is granted.

Setting	Description
Relay 1 – door open time	Access granted will open relay 1 for door open time. This can be used for temporarily releasing electric locking mechanisms.
Relay 2 toggles	Access granted will toggle relay 2. For example, a valid card will open relay 2. The relay will remain open until another valid card is presented. This can be used for switching an alarm system on and off, opening shutter doors etc.

Doors\[Door name]\Reader 2

The Reader 2 tab shows the settings corresponding to Reader 2 and Keypad 2 connected to that control unit.

The default name for reader 2 is [Door name] (OUT). This can be changed.

All settings are set as shown for reader 1. Readers 1 and 2 are configured separately and can have completely different settings.

Doors\[Door name]\Alarm

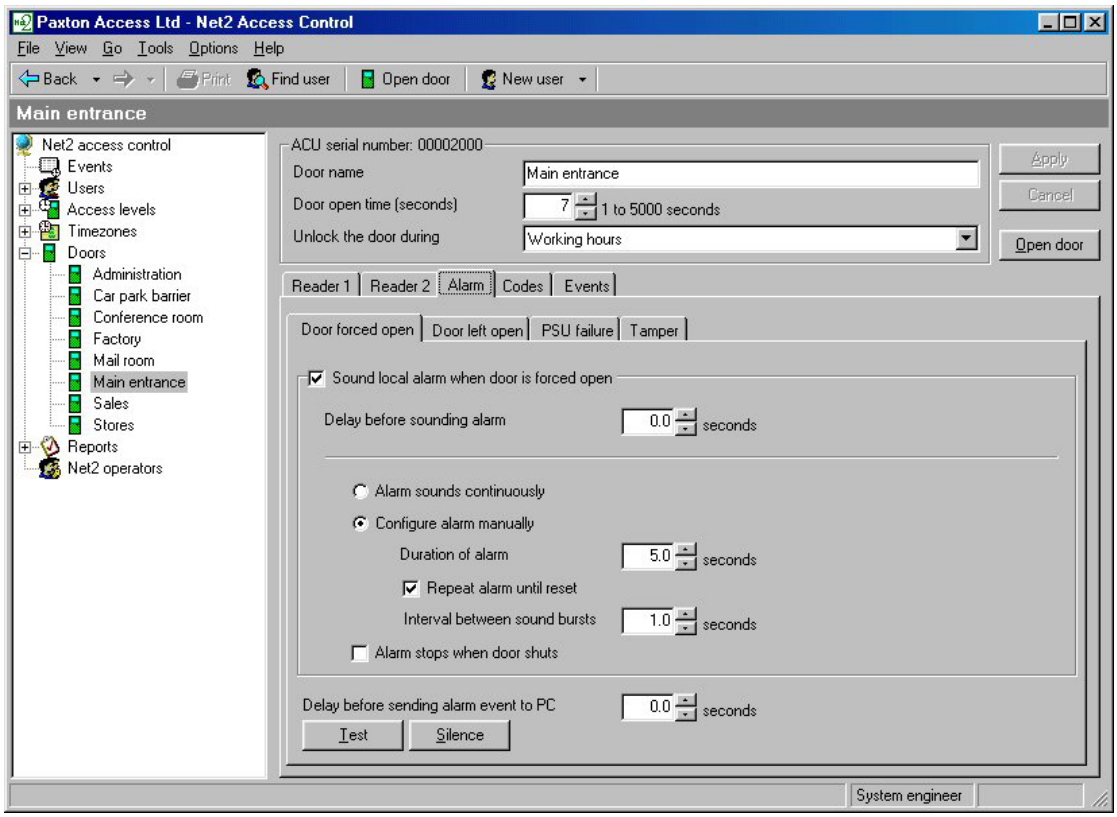


Figure 7.11
Configuring the doors - Alarms

There are 4 types of alarm that can be configured for each ACU.

Type of alarm	Description	Requires…
Door forced open	The door is opened without the permission of the access control system.	Door contact
Door left open	The door is opened with the permission of the access control system but is not closed within the specified time.	Door contact
PSU failure	The mains supply to the control unit PSU fails. If battery backup is fitted then the system will continue to operate.	Mains fail output on power supply
Tamper	The control unit enclosure has been opened.	Tamper switch on control unit enclosure

Each type of alarm has its own tab and is configured in the same way. The settings for each type of alarm can be different.

Local alarm

On every control unit there is an alarm output. This can be connected to a bell, sounder, light etc. The local output can be turned on or off for each type of alarm.

If the local alarm is activated then a delay can be imposed before the alarm is activated. It can also be configured in a particular way to distinguish between different alarm events. The alarm can be set to sound continuously or can be configured manually.

Testing the local alarm

The local alarm can be tested by activating it and silencing it from the PC.

Alarm reporting at the PC

All alarm events are reported at the PC. A delay can be imposed before an alarm event is sent.

Doors\[Door name]\Codes

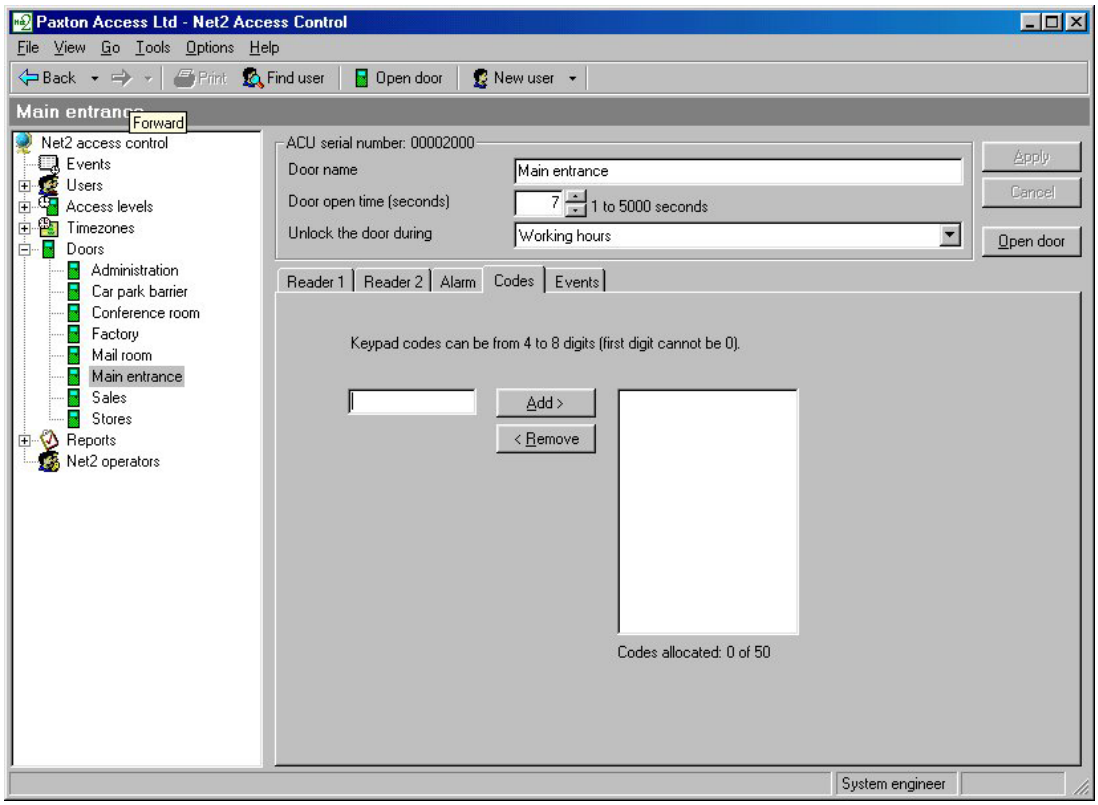


Figure 7.12 Configuring the doors - Codes

Note: The Codes tab only appears if a keypad is configured on the control unit.

Codes can be simply added and deleted. Codes added in this screen will only be valid for the individual door.

Up to 50 codes can be valid at any one time. Codes can be between 4 and 8 digits long.

Commissioning checks

The system is now configured. Ensure that:

- A user token given access privileges at the PC **does** open the doors that it is supposed to.
- Events are being reported back to the PC.
- All locking hardware is functioning correctly, i.e. the doors open when they should do.
- Alarm events such as door forced open are reported back to the PC from every door.

The system can now be handed over to the end user. Please refer to the Net2 system user manual (228-177) for full details of operating the system.

Chapter 8 Fault-finding

Fault diagnosis

Establish at first hand that the problem is genuine. Many problems are reported that are caused by user error i.e. tokens not presented properly or a programming error at the PC.

Once the problem is verified, it may be necessary to do a full system check to establish which aspect of the system is not functioning correctly. If the exact nature of the problem is already known then skip to the relevant section in this chapter.

Communications test

Whilst the Net2 access control program is running walk round and confirm that the Rx and Tx LEDs are flickering regularly on each control unit. The system is polling several times per second. The Rx LED flashing indicates that the ACU is receiving network messages from the PC and the Tx LED flashing indicates that the ACU is transmitting network messages back to the PC. If the LEDs are flashing as described then communications are functioning.

If the Rx and Tx LEDs are not flashing on any or all of the ACUs then there is a communication problem, refer to *Fault-finding/System problems*.

ACU test

The diagnostic LEDs allow the functionality of each ACU to be tested quickly and accurately.

Check that the…	If not…
12V and 5V LEDs are on.	Power supply problem, refer to *Fault-finding/system problems*.
OK LED is pulsing regularly? (See OK LED status at the end of this section for more details)	Processor problem, refer to *Fault-finding/system problems*.
Exit LED is on when the exit button is pressed.	Input problem, refer to *Fault-finding/system problems*.
Contact LED is on when the door is closed.	Input problem, refer to *Fault-finding/system problems*.
Tamper LED is on when the circuit is closed.	Input problem, refer to *Fault-finding/system problems*.
PSU LED is on when the circuit is closed.	Input problem, refer to *Fault-finding/system problems*.
Present or swipe a user token through all readers connected to the ACU. The red or green LED should flash to acknowledge a valid or invalid card.	Reader problem, refer to *Fault-finding/system problems*.
Enter a valid PIN number or code to any keypads connected to the ACU and check that the green LED flashes.	Keypad problem, refer to *Fault-finding/system problems*.
The Door relay 1 LED comes on when the exit button is pressed. If there is no exit button then jumper the exit button terminals with a piece of wire.	Output problem, refer to *Fault-finding/system problems*.
If used, the other outputs Relay 2 and Gen O/P must function as required.	Output problem, refer to *Fault-finding/system problems*.

Figure 8.1
ACU fault diagnostic test

OK LED Status

The OK LED has different flash modes to indicate different system status.

A **single short flash**, once a second, means that the ACU is functioning properly, and that it is in communication with the Net2 Server.

A **double short flash**, once a second, means that the ACU is functioning properly, but that it is currently off-line.

Rapid continuous flashing means that there is a real time clock failure. The ACU will allow access to users with 24/7 access rights.

The LED blinking **1 second on, 1 second off** means that the ACU has a real time clock failure, but it has been 'told' the time by the Net2 Server. It will continue to run normally as long as it does not loose it's power, unless the Net2 Server is running to set it's time again. An ACU with a real time clock failure should be replaced.

System problems – power supply

- **12Vdc supply** – Set a multimeter to dc range and measure the supply across the power terminals of the ACU. If this is not between 10 and 15V then there is a problem with the power supply.
- **Power supply ripple** – Set a multimeter to ac range and measure the supply across the power terminals. This measures the ripple of the supply. If a voltage above 2V is measured then there is a problem with the power supply.
- **5Vdc supply** – The ACU has an on board regulator.

If the 12V LED is on and the 5V LED is off, the power to the ACU must be switched off immediately, or damage to the board may result. A typical cause of this would be an incorrectly fitted or faulty reader.

To confirm that the regulator is functioning correctly, set a multimeter to dc range and measure the voltage across the Red and Blk/Wht terminals of each reader. A voltage between 4.8 and 5.2V indicates that the regulator is working.

If problems persist then contact the Paxton access technical helpline.

System problems – processor

- **Power** – Turn the power to the ACU off and then on. When the power is re-applied, the processor should be working and the OK LED should be pulsing regularly.

If problems persist then contact the Paxton access technical helpline.

System problems – inputs

- **Power** – Turn the power to the ACU off and then on.
- **ACU test** – Disconnect the input and place a jumper between the 2 input terminals and check whether the relevant diagnostic LED comes on. If the LED comes on then the ACU is working. If the ACU is working then the problem lies with the input itself, e.g. test the door contact for continuity and short circuit conditions.

If problems persist then contact the Paxton access technical helpline.

System problems – reader/keypad

- **Power** – Turn the power to the ACU off and then on.
- **Connections** – Check wiring and integrity of reader/keypad terminal connections.
- **Cable** – Check that the correct cable is used and that the maximum cable distance has not been exceeded.

Reader/keypad	Maximum distance from ACU
TOUCHLOCK keypad	5 metres
TOUCHLOCK keypad stainless steel	50 metres
CARDLOCK reader	100 metres
PROXIMITY reader	80 metres

Figure 8.2
Table showing maximum cable extensions for readers/keypads

- **Screen** - The screen must be continuous and connected to 0V.
- **Supply voltage** – Using a multimeter, confirm that the reader has sufficient voltage. Voltage should be measured at the reader/keypad across the Red and Blk/Wht terminals.

Reader type	Minimum voltage
PROXIMITY reader	4.5V
CARDLOCK reader	4.5V
TOUCHLOCK keypad	4.5V
TOUCHLOCK keypad stainless steel	4.5V
OEM reader	Consult manufacturers literature

Figure 8.3
Table showing minimum voltages for readers/keypads

- **User token** – Check that the user token used for testing the reader is operational. It can be tested on other 'known good' readers.

If problems persist then contact the Paxton access technical helpline.

System problems – outputs

- **Power** – Turn the power to the ACU off and then on.
- **ACU test** – Disconnect the output (i.e. lock) trigger the output and check whether the relevant diagnostic LED comes on. If the LED comes on then the ACU is working. If the ACU is working then the problem lies with the output device itself, consult device manufacturer.
- **Output device test** – The operation of the output device can be tested by applying power directly to it.

If problems persist then contact the Paxton access technical helpline.

System problems – communications

If some ACUs are communicating but not all

- **Finding the problem** – A full network test is documented in the *Commissioning/Hardware* section of this document. This should be completed before progressing with this section.
- **Power** – Turn the power to the ACUs off and then on.
- **Connections** – Check wiring and integrity of network terminal connections at the problem ACUs.
- **Cable** – Check that the correct cable is used and that the maximum cable distance has not been exceeded, refer to *About…/Readers and keypads/Cable details*.

If problems persist then contact the Paxton access technical helpline.

If all ACUs are not communicating

- **Finding the problem** – A full network test is documented in the *Commissioning/hardware* section of this document. This should be completed before progressing with this section.
- **Power** – Turn the power to the ACUs off and then on.
- **Interface** – Ensure that the interface has power. Check that all connections are as they should be.

- **Connections** – Check wiring and integrity of network terminal connections.
- **Cable** – Check that the correct cable is used and that the maximum cable distance has not been exceeded, refer to *About…/Readers and keypads/Cable details*.
- **Termination resistors** – Check that the 120 Ohm termination resistors are in place, 2 at each end of the network.
- **PC** – Please refer to *System problems/PC*.

If problems persist then contact the Paxton access technical helpline.

If there are inconsistencies between the database and control unit information

- Reinstate – Press the **Reinstate** button as shown in figure 8.4, select the controllers to reinstate. This will reset all selected ACUs and download the relevant database information to them.

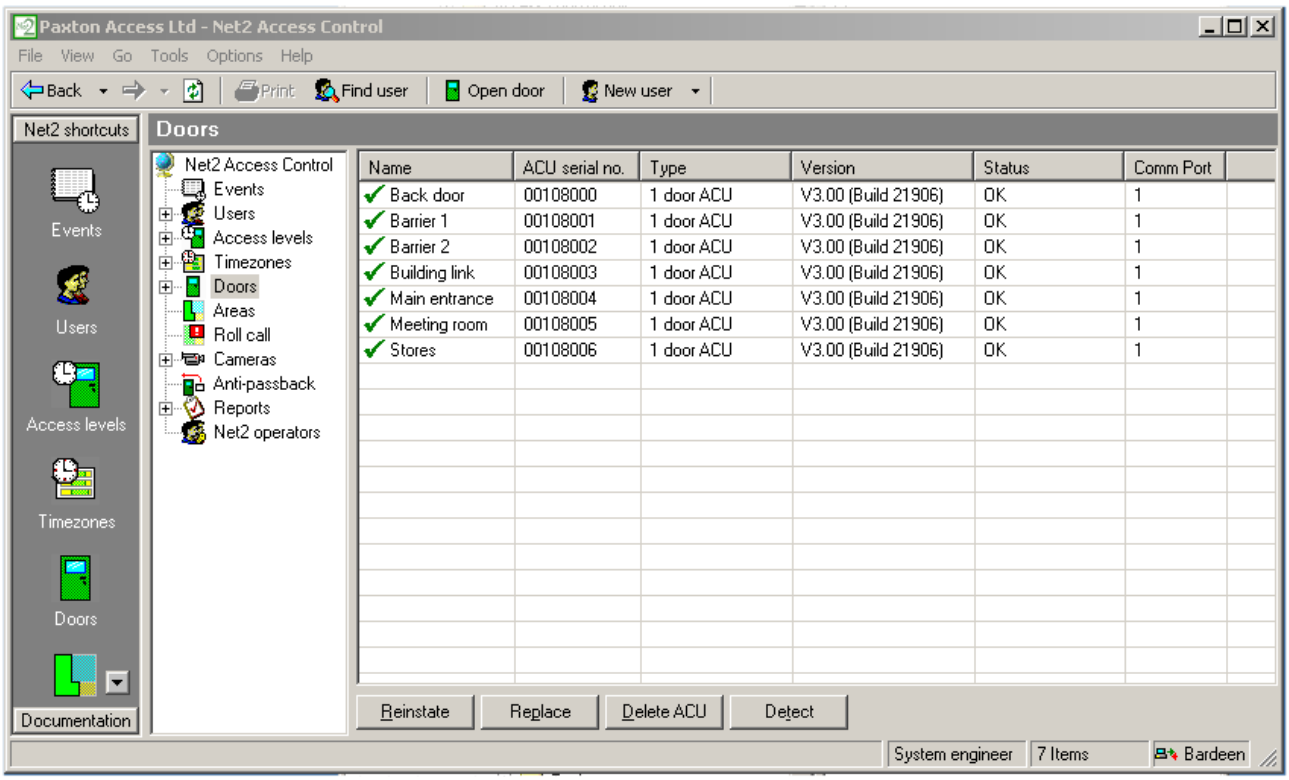


Figure 8.4
Reinstate ACUs

System problems – PC

If the system is not communicating

- **Comport** - Ensure that the RS485/232 interface is connected to the correct comport.
- **PC requirements** - Ensure that the PC meets the minimum requirements, refer to *About…/PC/Requirements*.
- **Comport test** - Ensure that the comport is functioning. This can be tested by completing the following:
  1) If HyperTerminal is not already installed then install it*.
  2) Open Windows explorer and open folder C:\Program files\Accessories\Hyper terminal. Run Hypertrm.exe.
  3) Enter paxton as the name of the connection and press OK.
  4) Next to 'Connect using' choose the relevant comport from the drop down list and press OK.

5) Enter the following settings:

Bits per second	115,200
Data bits	8
Parity	None
Stop bits	1
Flow control mode	None

6) On this computer serial port we must create a link between pins 2 and 3.

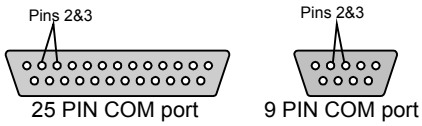


Figure 8.5
25 and 9 pin comports

7) If the serial port is functioning correctly, then, whilst the link is in place, any text entered will appear on the screen. When the links are broken, no text will appear on the screen.

* To install Hyper Terminal, the Windows installation disk (as supplied with the PC) is required. Go into the control panel (Located in settings on the start menu) and select Add/Remove Programs. Select the 'Windows Setup' tab at the top of the screen. Double click on communications and check Hyper Terminal installation if it is not already checked. Press OK. Press Apply. The Windows disk will be requested and the software can be installed.

If problems persist then contact the Paxton Access technical helpline.

If the Net2 program will not install

- **PC requirements** - Ensure that the PC meets the minimum requirements, refer to *About…/PC/Requirements*.

If problems persist then contact the Paxton access technical helpline.

Paxton Access technical help

Paxton Access offer a telephone technical help service. This is designed to assist installers at site installing or maintaining products manufactured by Paxton Access. Also technical questions concerning specifying etc. can be answered.

The person calling must have working knowledge of the system and will be expected to have read this manual and followed its guidelines and system problem checks.

The person calling must also have some PC knowledge. They must at least understand installing programs and using Windows explorer.

To be eligible for technical help the site must be registered. The registration form is included in with the Net2 software. For a copy of the registration form refer to Appendix (x).

To administer the registration of sites and the distribution of software, a technical support ID number is required to qualify for technical help. This technical support number is very easily generated from the software (in the **Help** drop down menu at the top of the screen).

The technical support ID number will only be valid if the software has been registered.

The Paxton Access technical helpline is available Mon-Fri 8.30am-5.30pm.

+44 (0) 870 6080886

The web site address for Paxton Access is www.paxton-access.co.uk

Chapter 9 Appendix

(i) Operation of a relay explained

(ii) Fail open and fail closed locks explained

(iii) Difference between code and PIN explained

(iv) Glossary of terms

(v) ISO card unprintable area

(vi) Net2 part numbers and product descriptions

(vii) Extending a Net2 system

(viii) Replacing a control unit

(ix) Site registration form

Appendix (i) Operation of a relay explained

The Net2 ACU contains two relays. These are very versatile and can be used to switch electrical devices. A relay consists of a coil and a switch and has output terminals common (COM), normally open (N.O.) and normally closed (N.C.).

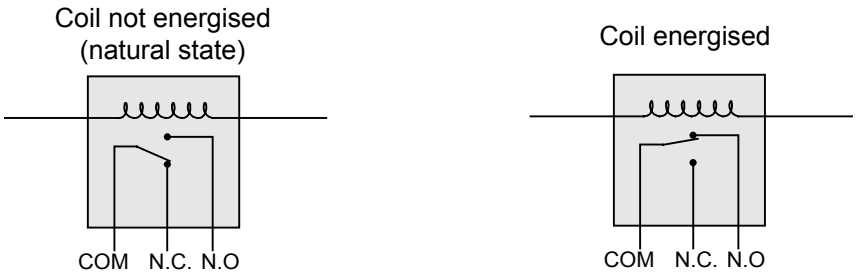


Figure 9.1
Operation of a relay

In the de-energised state, common and normally closed are connected. When the coil is energised, the switch moves and common and normally open are connected. As soon as the coil is de-energised the switch springs back to the normally closed position.

The output terminals COM, N.O. and N.C. are voltage free. This means that they can be included as part of a circuit to switch power to OR from an electrical device.

Appendix (ii) Fail open and fail closed locks explained

Fail open (fail safe)

Fail open devices require power to lock, i.e. if there is no power to the device it is unlocked. An example of a fail open device is a magnetic lock (maglock).

A fail open locking device is a requirement for fire doors. This is because it is not reliant on electrical power to unlock.

It is advisable to have a battery backup for systems using fail open devices. Otherwise a mains power failure would lead to doors unlocking for the period of the mains failure.

Fail open devices are inefficient in terms of power consumption when compared to fail closed devices. This is because they are powered for the majority of the time, i.e. when the door is locked.

Fail closed (fail secure)

Fail closed devices require power to unlock, i.e. if there is no power to the device it is locked. Most standard electric releases are fail closed.

If battery backup is not fitted, mains loss would result in doors being locked for the period of the power failure.

Fail closed devices are more efficient that fail open devices. This is because they are only powered when the door is unlocked.

Appendix (iii) Difference between code and PIN explained

PIN stands for Personal Identification Number. This is a number that is specific to an individual user. A user code can be common to many users.

Example of code only: A keypad has two codes to control the access of 1,000 users through an access point. 300 users use one code and 700 use the other.

Codes are very quick to setup; thousands of users can be given access to an area if the code is disclosed. Access privileges can be adjusted for groups of users, where the users are grouped together by a common code.

Example of PIN only: A keypad controls the access of eight users through a door. Each of the eight users has their own PIN, which they use to gain access.

Using PINs mean that access rights can be changed for every individual without affecting other users. PINs also allow users to be identified by the system for reporting purposes. However, more numbers valid on a keypad will increase the chances of guessing a correct number. This means that a non-authorised person can gain access by randomly pressing keys on the keypad. To reduce these risks to an acceptable level it is necessary to increase the number of digits in the PIN.

Example of card plus code: A proximity reader and a keypad are used to control access through a door. A user is required to present their proximity card to the reader and enter a valid code.

This involves two elements of security – possession and knowledge. The possession of the card is required AND a valid code has to be known. If the card is lost it cannot be used on its own. If the code is discovered it cannot be used without a valid card.

Example of card plus PIN: A magnetic stripe reader and a keypad are used to control the access through a door. A user is required to swipe their card and enter their PIN number. Only the combination of that user card AND that user PIN number is acceptable.

This involves both possession and knowledge but increases security even further. If a user card is lost it can only be used to gain access when used with the specific PIN number. For security reasons bank cash machines use a card plus PIN system.

Appendix (iv) Glossary

General access control terms	
Access control system	An access control system comprises input for identification (e.g. a keypad or reader), intelligent electronics for decision making and outputs for operating access point hardware and the access point hardware itself (e.g. locks, barriers).
Access Control Unit (ACU)	A general term to describe a range of devices which have the control electronics and intelligence to make the decision to allow access at one or several points. It will have connectors or cables ready to link to readers, keypads, locks, etc.
Bench test	The wiring and configuration of a system at the installers premises before installation. This is a recommended procedure before installing any system for the first time. The time spent in becoming familiar with the equipment will invariably be recouped several times over on site.
Coercivity	Coercivity relates to the resilience of the encoding of a magnetic stripe card. Hi coercivity encoded magstripe cards are more resilient to data corruption than Lo coercivity cards.
Common Reference (CR)	CR refers to the cable reference numbers commonly used to identify cable of a specific type.
Distributed intelligence	In a networked access control system access control units are linked and communicate with each other or a PC used to control the system. Distributed intelligence means that the access control units hold user information and system settings locally. This enables the ACUs to carry on functioning if communications links are severed.
Door open time	An electric locking device has power supplied/denied to release and allow access when a valid token is presented. The time period that the electric release is energised/de-energised is referred to as the door open time.
Event recording	Access Control Units may be provided with memory to record events. Events recorded should include the access point details, date, time and user ID for each occasion when access is granted. Many other events may be recorded depending on the system e.g. details of access denied and alarm events. Where events are recorded the access control unit will be capable of sending the information to a printer or computer.
Magstripe	Magnetic stripe reading technology – cards with a number encoded on a magnetic stripe are swiped through a slot on a reader.
Network system	A system where access control units are linked together by data cable for the exchange of information between units. The purpose of this is to provide easier configuration and better management information for larger and more complex applications. All access points on the system can be set up from a single point. The access control units on network systems record events. Most systems allow for a computer to be connected to the network to allow control and reporting to be carried out from a dedicated program.
Photo ID	Where a photograph of the user is printed or attached to their user token allowing them to be identified.
Proximity	The proximity device is held close to the reader and sends a unique number by radio signal to the reader.

Tailgating	A term used to describe an individual gaining access through an access point by following through after an authorised user.
User token	This is a generic term for the devices that users of an access control system use to identify themselves and gain entry through access points. User tokens may be magstripe cards, proximity keyfobs, smart cards, etc.
Paxton Access terminology	
Proximity ISO card	ISO cards are the same size as standard bank or credit cards. They can be used with standard card printers for photo ID. They also have a magnetic stripe that can be encoded for use with other systems such as vending.
Proximity keyfob	Keyfobs are for applications where convenience is important. They are made of hard plastic and will fit onto a keyring. They can be attached to car/house keys for reduced losses, hence reducing the cost of replacing fobs.
Proximity token	Tokens are about credit card size but are thicker. They can be used from inside wallets or handbags. Adhesive plastic stickers can be applied for photo ID and the slot in the tokens makes them ideal for use with low cost badge clips.

Appendix (v) ISO card unprintable area

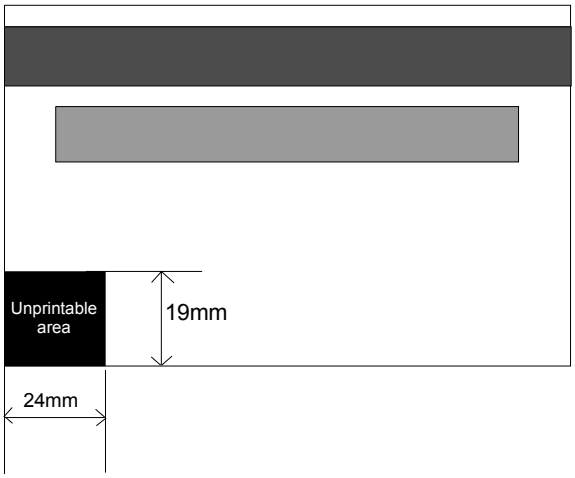


Figure 9.2
ISO card unprintable area

ISO cards are suitable for use with an ID card printer, subject to observance of the non-useable area on the card. The area is defined in figure 9.2 and is viewed from the magstripe side of the card. It is advised that there may be surface distortion here, which although within the specification of ISO 7810, may give poor results if printed upon. This restriction applies to both sides of the card.

Appendix (vi) Net2 part numbers and product descriptions

Part number	Description
	Hardware
489-334	Net2 1 door access control unit
385-527	Net2 1 door ACU in plastic housing
411-381	Net2 1 door ACU with 2A PSU in steel cabinet
857-693	Net2 2amp PSU in steel cabinet with mounting posts
571-692	Net2 housing for ACU black plastic
339-424	1 amp power supply unit
339-425	12V 1.2AH battery for 1A boxed PSU
862-719	12V 7AH battery for 2A boxed PSU
289-641	Net2 RS485/232 kit incl converter, PSU and PC lead
477-836	Net2 RS485 high speed repeater
	User tokens
693-112	Net2 proximity tokens pack of 10
695-644	Net2 proximity keyfobs box of 10
692-448	Net2 proximity ISO cards box of 10
695-573	Net2 magstripe cards box of 10
	Software
936-001	Net2 standard software 50 doors, 2000 users
945-065	Net2 standard plus software 200 doors, 10,000 users
	Readers/keypads
409-711SC	CARDLOCK reader satin chrome
355-098	PROXIMITY reader
600-628SC	TOUCHLOCK keypad satin chrome
485-374	TOUCHLOCK keypad stainless steel
376-001	Desktop reader prox and magstripe
	Cable
166-025	Reader cable 10 core CR9540 25m roll
166-100	Reader cable 10 core CR9540 100m roll
189-100	Data cable 2 pair CR8723 100m roll
189-500	Data cable 2 pair CR8723 100m roll

Appendix (vii) Extending a Net2 system

The correct procedure for extending a Net2 system is as follows:

1. Close the Net2 software application.
2. Wire the additional ACUs .
3. Open the Net2 software application and detect the new ACUs by pressing the **Detect** button in Doors.
4. Press **Apply** to commit the ACUs to the database.
5. Configure the new ACUs in the usual way.
6. As default no user will have access to the additional doors. Make the required adjustments to access levels and individuals user records (where access levels are not used).
7. To confirm that the system is working as it should, perform the following checks:
   - A user token given access privileges at the PC does open the doors that it is supposed to.
   - Events are being reported back to the PC.
   - All locking hardware is functioning correctly, i.e. the doors open when they should do.
   - Alarm events such as door forced open are reported back to the PC from every door.

Appendix (viii) Replacing a control unit

If a Net2 control unit is faulty then it may need replacing with a new unit. The 'Replace control unit wizard' administers downloading the relevant settings and user information to the new control unit.

1. Close the Net2 software application.
2. Physically remove the old control unit from the network and wire the new unit in its place (for full wiring details refer to *Wiring*).
3. Open the Net2 software application and detect the new ACU by pressing the **Detect** button in hardware as shown in figure 9.3. Ensure that the new ACU has been detected before proceeding.
4. Start the replace control unit wizard by pressing **Replace** in hardware as shown in figure 9.3.
5. Press **Next** to continue.

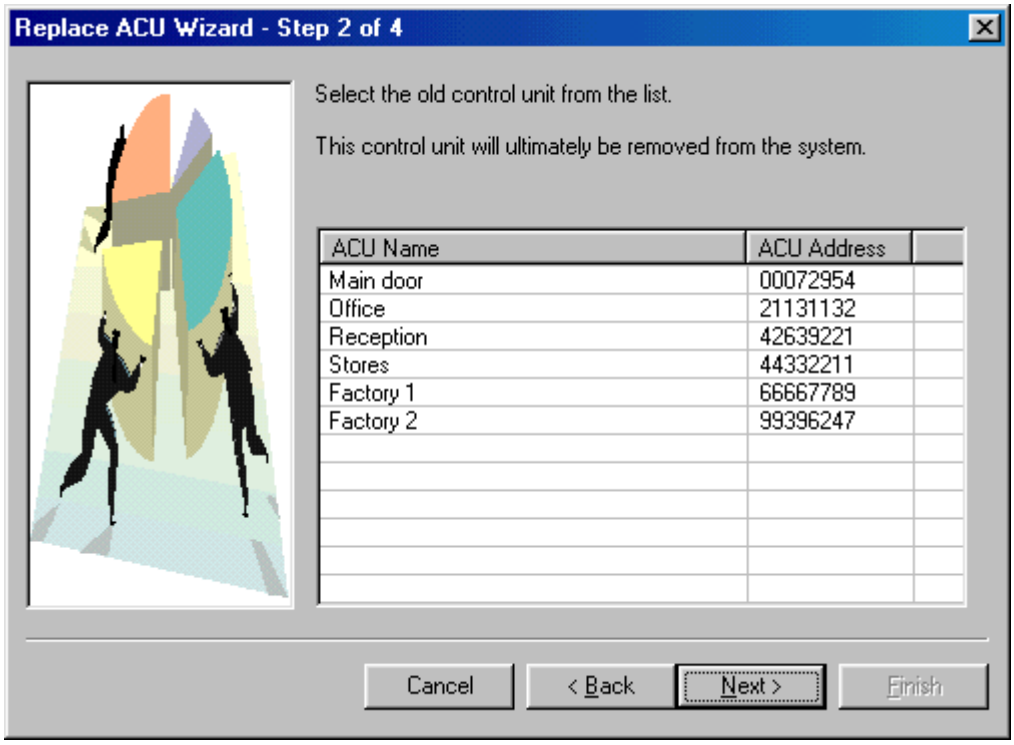


Figure 9.4
Replace a control unit wizard

6. Select the control unit to be replaced from the list as shown in figure 9.4. Press **Next** to continue.
7. Select the new control unit from the list and press **Next** to continue.
8. If the details displayed are correct then press **Finish** to complete the replacement.

Appendix (ix) Site registration form

You must register your software to receive technical support

Registering couldn't be simpler. Simply complete this form and fax it to us.

This form is available in pdf format on the CD-ROM (Net2 V1.03\Literature\Registration.pdf) should you need to print out another copy.

Installation company

Contact
Company
Address

Post code
Tel Fax
Email

Site information

Contact
Site name
Address

Post code
Tel Fax
Email

Installation details

CD-KEY ☐☐☐ ☐☐☐☐☐☐☐☐

Number of doors installed on site ☐☐☐

Date commissioned ☐☐ ☐☐ ☐☐

Fax number: +44 (0) 1273 483753

Chapter 10 Specifications

Net2 software for 200 doors	
Maximum number of users	10,000
Maximum number of doors	200
Net2 software for 50 doors	
Maximum number of users	10,000
Maximum number of doors	50
Net2 software for 20 doors	
Maximum number of users	10,000
Maximum number of doors	20
Reading technologies supported	All Paxton Access readers: PROXIMITY, CARDLOCK magnetic stripe, TOUCHLOCK keypads
Individual access rights by access point	All users, all access points
Individual time zones	All users
Access levels	Up to 250
Time zones	Up to 64
Read in and read out	Yes
Card plus PIN (Personal identification number)	Yes
PIN only entry	Yes
Number of system operators	unlimited
System operator privileges	4 levels
System operator log on to software	Individual password protection
Desk top reader	Provides fast access to user records
Advance entry of Bank Holidays	Yes
Door held / wedged open alarm	Reported to software and output for local sounder at door
Door forced alarm	Reported to software and output for local sounder at door
Instant reports	Screen reports on recent events
Printed reports from entire access event history	Yes
Database format	Microsoft Access 97
Data available to other programs	Yes - including Word, Excel, Access, etc
Timed backup of event log	Manual backup required
Fail open (fail safe) locks	Yes
Door open time	1 to 5,000 seconds
Operates gates, barriers, turnstiles, etc	Yes - all equipment that can be switched by clean relays
Network Details	
Communications with other control units	RS485 full duplex 115,200 BAUD
Maximum number of control units per data line	200
Full distributed intelligence	Yes
Off line memory in access control units	2,300 events
Access control unit user card capacity	10,000 Paxton Access proximity devices or magstripe cards
Access control unit user card capacity	10,000 bank / credit magstripe cards
Details of supported readers	
Magnetic stripe readers	CARDLOCK
Reader life	>1,000,000 swipes
Proximity readers	PROXIMITY
Reader life	Unlimited token reads
Keypads	TOUCHLOCK membrane or TOUCHLOCK stainless steel
Keypad life (key presses)	>100,000 membrane or > 1,000,000 for stainless steel
Water resistance	All readers IPX7 (submersible) except membrane keypad IPX5
Finishes of CARDLOCK and TOUCHLOCK	Black, brass or satin chrome
Finish of PROXIMITY	Black
Finish of TOUCHLOCK stainless steel	Stainless steel and satin chrome
Minimum PC minimum specification: Pentium PIII/800 processor, 128 Mbytes RAM, UDMA hard disk with 1Gbyte free space, 800 x 600, 256 colour monitor (SVGA), a free UART 16550 serial port, mouse, keyboard and a CD ROM drive 4 x or better.	

Network communications	
Network communications cable	CAT5 (Screened or unscreened) or Belden® 8723*
Maximum length of communications bus	1,000m
Access Control Unit	
Number of doors per control unit	1
Memory in the event of complete power failure	All system settings and user details are retained for 7 days
Backup batteries ensure operation of	Entire system except PC - control of access continues
Connections in the access control unit for each of the doors	
Readers	1 or 2 (in, in/out)
Keypads	1 or 2 (in, in/out)
Analogue / digital inputs	4 (default uses: exit button, door contact, PSU monitor, tamper)
5 amp relay outputs (NC, and NO)	2 (default use: lock relay and door bell relay)
1 amp FET controlled output	1 (sinks up to 1A at 12Vdc, default use: local door alarm)
Reader to access control unit distances	
TOUCHLOCK keypad *	30m
TOUCHLOCK keypad stainless steel *	30m
CARDLOCK reader *	100m
PROXIMITY reader*	50m
Access control unit power requirement details	
Required supply voltage	9V to 15V dc
Maximum current for access control unit	350mA at 12Vdc (allow extra for FET output)
Maximum current for Paxton Access magstripe readers	65mA
Maximum current for Paxton Access proximity readers	70mA
Maximum current for Paxton Access keypads	45mA
Maximum current for other keypads and readers	See reader manufacturer's literature
Maximum current for locks	See lock manufacturer's literature
Access control unit dimensions	
Board size	102 x 116 x 30mm high
Recommended minimum space for board in other manufacturer's enclosures	200 x 170mm high
Board weight	190g
NETWORK RS485 / 232 communications converter	
Size	80 x 50 x 20mm
Communications protocols	RS232 to PC, RS485 to access control units
Maximum serial cable distance to PC	7m
Low voltage power supply	250mA 12V dc
Desktop reader details	
Type of reader	The reader type used at the doors on site may be used or:
Paxton Access dual technology desktop reader	Reads magstripe cards and Paxton Access proximity devices
Size of Paxton Access dual technology desktop reader	160 x 90 x 30 mm
Maximum distance to access control unit	As for other reader distances noted above
Black plastic housing	
Size	175 x 170 x 40mm
Features	Tamper switch, cable tie loops, cable entry knock outs
PSU enclosure size	
Details to be confirmed	

* All reader and data cables should be segregated from mains power cables to avoid interference. IEE Regulations and normal good practice should be observed. Belden cables or exact electrical equivalents must be used.