

IXP200[©]

Access Control Software

Software Version 6.0

USER MANUAL

IMPORTANT NOTICE

In the event of any discrepancies in meaning between this, the original English version of the manual, and any other version of this manual, in whatever language, the information in this version shall take precedence.

IXP200 ACCESS CONTROL SYSTEM

SOFTWARE – VERSION 6.0*

USER MANUAL

LIST OF CONTENTS

WELCOME

WHAT'S NEW IN THIS RELEASE

SCOPE

NETWORK AND COMPUTER SECURITY

SECTION 1 - SYSTEM OVERVIEW

SECTION 2 - SOFTWARE INSTALLATION

SECTION 3 - SYSTEM CONFIGURATION

SECTION 4 - REPORTS

SECTION 5 - UTILITIES

SECTION 6 - MANUAL EDITING FACILITY

SECTION 7 - GLOSSARY OF TERMS

SECTION 8 - APPENDICES

Each Section of this manual includes a detailed List of Contents for that Section.

**Software or firmware changes may be made which do not require changes to this manual. This issue of this manual will remain valid for all future software updates until changes in the software require it to be updated.*

WELCOME

The IXP200 Series Software is a single- or multi-user access control System using the ImproX range of Hardware. It is designed for use with Windows 98 Second Edition, 2000, NT SP6a, or XP Professional.

The Software includes reporting and alarm monitoring capabilities.

This manual describes the installation and use of the IXP200 Application Software.

WHAT'S NEW IN THIS RELEASE (V6.0)

The release of Software version V6.0 provides the following new features :

- **Database Server.** This allows the IXP200 database to be installed on a separate Server PC.
- The system now supports the use of an **Editing Workstation**. This means that the IXP200 Software can now be installed on a second machine that serves as an Editing Workstation only. This machine has no connection to the system hardware (Controller, etc). A ProxMate or Registration Reader may be installed on the Editing Workstation for convenience. The Editing Station is used to edit the IXP200 Database, for example by adding or deleting Tagholders.
- **Image Editor.** The picture file imported for a Tagholder can be cropped, rotated, resized, etc from the Tagholder dialog.
- **Archive** will now create archive databases on the Database Server, which will be accessible for Web Reports.
- **Backup** can now be executed automatically when using a Database Server but must be manually restored when required.
- The **Web Server port** number can now be changed from the Software.
- The IXP200 Software is now deployed with Java JRE 1.4.2_13, which supports Daylight Savings changes that will be effective from March 2007 in the US, Canada, and elsewhere. **NOTE:** *The Windows Operating System must also include the appropriate patches for this to be effective.*

NETWORK AND COMPUTER SECURITY

CAUTION

The security of the network and the computers on which the software is installed remains the responsibility of the customer. If the computer on which the system is installed is compromised, or the network is compromised, then it may become possible to make unauthorized modifications to the configuration of the system, and physical security may be breached.

It is strongly recommended that the latest security updates are obtained and applied on a regular basis to all computers on which any component of the system is running.

Physical access to the computers running the system must also be controlled, to ensure that access by unauthorized persons does not occur.

SCOPE OF THIS MANUAL

This manual contains all the information necessary to correctly install and configure the IXP200 System Software. In addition, it describes how to use the Software together with the associated ImproX and 3rd party Hardware, and provides insight into the effects of the various options and how to select them.

Details of compatible Hardware are also provided.

RELATED PUBLICATIONS

The following related publications are produced by Impro Technologies :

ImproX Hardware Installation Manuals

An Installation Manual is supplied with each individual Hardware unit.

ImproX Hardware Product Specification Catalogues (PSCs)

A PSC includes more in-depth information than an Installation Manual. A PSC is available for each individual ImproX Hardware unit, on our web-site, at www.impro.net.

IXP200 System Hardware Installation Manual

This is supplied together with this manual on the IXP200 Software CD. It describes the installation of ImproX units to form a Hardware System compatible with the IXP200 Software.

ImproX Unit Installation Chart

This is supplied with the IXP200 Controller Unit. It is intended to be used to maintain a record of the physical location of every ImproX unit in the System.

Graphics Designer Software User Manual

The Graphics Designer Software User Manual IXP331-0-0-GB-XX is supplied together with this manual.

Card Designer Software User Manual

The Card Designer Software User Manual IXP333-0-0-GB-XX is supplied together with this manual.

IXP200

Software User Manual

SECTION 1

SYSTEM OVERVIEW

IMPRO TECHNOLOGIES (PTY) LTD - SOFTWARE LICENSE AGREEMENT

READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING THE PROGRAM DISKETTES OR CD-ROM, THE COMPUTER SOFTWARE THEREIN, AND THE ACCOMPANYING USER DOCUMENTATION (THE "PROGRAM"). THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM BETWEEN YOU AND IMPRO TECHNOLOGIES (PTY) LTD. (THE LICENSOR) AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES. BY OPENING THE PACKAGE CONTAINING THE PROGRAM, YOU AND YOUR COMPANY (COLLECTIVELY "YOU") ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE PACKAGE IN UNOPENED FORM, AND YOU WILL RECEIVE A REFUND OF YOUR MONEY.

1. LICENSE GRANT

Licensor hereby grants you, and you accept, a non exclusive license to use the Program CDROM and the computer Software contained therein object-code-only from (collectively referred to as the Software), and the accompanying User documentation, only as authorised in this License Agreement. The Software may be used only on a single computer owned, leased, or otherwise controlled by you; or in the event of the inoperability of that computer, on a backup computer selected by you. Concurrent use on two or more computers is not authorised without the advance written consent of Licensor and the payment of additional license fees. You agree that you will not assign sublicense, transfer, pledge, lease, rent, or share your rights under this License agreement.

2. LICENSOR RIGHTS

You acknowledge and agree that the Program consists of proprietary, unpublished products of Licensor, protected under Copyright Law and trade secret laws of general applicability. You further acknowledge and agree that all right, title, and interest in and to the Program are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this LICENSE Agreement.

3. LICENSE FEES

The License fees paid by you are paid in consideration of the licenses granted under this License Agreement.

4. TERM

This License Agreement is effective upon your opening of this package.

5. LIMITED WARRANTY

Licensor warrants, for your benefit alone, that the program diskettes in which the computer Software is embedded and the user's manual shall, for a period of 90 days from the date of commencement of this License Agreement (referred to as the warranty period), be free from defects in material and workmanship. Licensor further warrants, for our benefit alone, that during the Warranty Period the Program shall operate substantially in accordance with the functional specifications in the User's Manual. You agree that the foregoing constitutes your sole and exclusive remedy of breach by Licensor of any warranties made under this Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM, AND THE SOFTWARE CONTAINED THEREIN, ARE LICENSED "AS IS" AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. LIMITATION OF LIABILITY

Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims,

demands, or action arising out of or relating to this Agreement shall not exceed the License fee paid for the use of the Program. In no event shall Licensor be liable for any indirect, incidental, consequential, special or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages.

7. HIGH RISK ACTIVITIES

The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication Systems, air traffic control, direct life support machines, or weapons Systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Impro and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

TRADEMARKS

ImproX, ImproNet, IXP, and other names included therein are trademarks of Licensor. No right, license or interest in Licensor trademarks are generated hereunder, and you agree that no such right, license or interest shall be asserted by you with respect to such trademarks.

8. GOVERNING LAW

This License Agreement shall be construed and governed in accordance with the laws of Republic of South Africa.

9. COSTS OF LITIGATION

If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses.

10. SEVERABILITY

Should any item of the License Agreement be declared void or unenforceable to any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

11. NO WAIVER

The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

12. USE WITH 3RD PARTY EQUIPMENT

The use of this Software with a card printer (or any other 3rd party equipment) is undertaken at the client's own risk. Impro will not accept liability for any damage to such equipment caused by incompatibilities between Impro Technologies' Software and the said equipment.

READ THIS BEFORE OPENING THE ENVELOPE CONTAINING THE SOFTWARE

SECTION 1 - CONTENTS

GENERAL.....	2
ImproX Terminals	2
Types of Units	2
CONTROL AND INPUT/OUTPUT UNITS.....	2
125 KHZ TERMINALS, GROUP 1	3
125 KHZ REMOTE READERS FOR GROUP 1 TERMINALS	4
MULTI-MODE READERS.....	5
125 KHZ TERMINALS, GROUP 2	6
125 KHZ ANTENNA READERS FOR GROUP 2 TERMINALS	6
REGISTRATION INTERFACE AND READERS	7
MULTI-FUNCTION TERMINALS	8
WIEGAND READERS	9
OTHER READERS	9
SYSTEM INFORMATION.....	12
System Features.....	12
Compatible Registration Readers	13
Compatible Tag Types	13
Tag Levels	14
Modes.....	14
Power Control	14
Alarm Arming	14
Alarm Arming – Relay 2	15
Arming.....	15
When Armed	15
ACCESS CONTROL	16
Doors and Zones	17
Door Mode Patterns.....	17
Lift (elevator) Control.....	17
Access Groups	17
Addressing Scheme	17
Architecture – System PCs	18
Graphics Software	20

TABLES

Table 1 – Control and Input/Output Units	2
Table 2 –(125 kHz) Terminals, Group 1.....	3
Table 3 –125 kHz Remote Readers for Group 1 Terminals.....	4
Table 4 – Multi-mode (Mifare & FeliCa) Remote Readers: Group 1 & 3 Terminals	5
Table 5 – 125 kHz Terminals, Group 2	6
Table 6 – 125 kHz Antenna Readers for Group 2 Terminals.....	6
Table 7 – Registration Interface and Registration Readers	7
Table 8 – Group 3 – Multifunction Terminals	8
Table 9 – Wiegand Readers.....	9
Table 10 – Third-party Biometric Readers	9

SECTION 1 - SYSTEM OVERVIEW

GENERAL

The IXP200 Software is designed to work in conjunction with an Access Control System made up of Impro ImproX Hardware Terminals.

ImproX Terminals

The ImproX Terminals can be divided into two groups, each being used for different purposes, namely:




- Reader Terminals can be used as Access Readers for Doors and Lifts (elevators)
- The Input/Output Terminals can be used for Building Management and Lift (elevator) Control (e.g. I16 and O16 Units).
- The Reader Terminal group includes Readers that detect RF Tags. (e.g. PT, TA, etc.),
- Remote devices include Remote Readers (such as the ImproX MR, KHR), Antenna Readers, and Remote MIFARE Readers.

During the Configuration process each Terminal is assigned to control a specific Door, (including Lifts (elevators) or for Building Management.

Types of Units

All units included in Tables 1 - 8 may be used in an IXP200 System. The IXP200 System Software supports both 125 kHz and Mifare (13.56 MHz) Tags. Interface units support some types of third-party Biometric Readers (refer to Table 9), as well as Wiegand, Barcode, RF and IR devices.

CONTROL AND INPUT/OUTPUT UNITS

Table 1 – Control and Input/Output Units		
	IXP200 Controller (plus CDRom)	IXP200 LCD Keypad Controller (IXP920-1-0-GB-xx) and the associated Software.
	ImproX I16	ImproX 16-Channel Input Terminal.
	ImproX O16	ImproX 16-Channel Output Terminal.

125 KHZ TERMINALS, GROUP 1

Table 2 –(125 kHz) Terminals, Group 1		
Group 1 Terminals are : DT, ER, PT, TA and iTA .		
	ImproX PT	ImproX Portal Terminal. Can be used with any one of the Remote Readers listed in Table 3.
	ImproX TA	ImproX Time and Attendance Terminal. Can be used with any one of the Remote Readers listed in Table 3.
	ImproX ER	ImproX Extended Range Terminal. Has its own dedicated antenna - not for use with Remote Readers or Antenna Readers.
	ImproX iTA Industrial Time & Attendance Terminal	Industrialised version of ImproX TA. Can be used with any one of the Remote Readers listed in Table 3.

See next page

125 KHZ REMOTE READERS FOR GROUP 1 TERMINALS**Table 3 –125 kHz Remote Readers for Group 1 Terminals**



This table lists the Remote Readers and other ImproX units (acting as Remote Readers) designed for use with the ImproX, PT, TA or iTA .

Mifare Remote Readers for use with these Terminals are listed in Table 4.

	ImproX KHR	ImproX Harsh Environment Keypad Remote Reader.
	ImproX KR	ImproX ABS Keypad Remote Reader.
	ImproX MHR	ImproX Harsh Environment Micro Remote Reader.
	ImproX MR	ImproX Micro Remote Reader.
	ImproX TAR	ImproX Time and Attendance Remote Reader. This can be used with the ImproX PT or TA (but not with the ImproX TT).
	ImproX iTAR	Industrialized ImproX TAR This can be used with the ImproX PT or TA (but not with the ImproX TT).

NOTE : *The ImproX IR and RF units are treated as Remotes by the software.*

Table 3 –125 kHz Remote Readers for Group 1 Terminals

	ImproX IR	ImproX Infra-red Receiver
	ImproX RF	ImproX UHF Receiver


MULTI-MODE READERS**Table 4 – Multi-mode (Mifare & FeliCa) Remote Readers: Group 1 & 3 Terminals**

These Remote Readers can be used with the following Terminals:

- ImproX (MfT) Multi-function Terminal.
- ImproX (TRT) Twin Remote Terminal.
- ImproX (PT) Portal Terminal.
- ImproX (TA) Time Attendance Terminal.



	ImproX XFMm	Multi-mode 13.56 MHz Metal Remote
	ImproX XFMmk	Multi-mode 13.56 MHz Metal Keypad Remote
	ImproX XFMp	Multi-mode 13.56 MHz Plastic Remote

Table 4 – Multi-mode (Mifare & FeliCa) Remote Readers: Group 1 & 3 Terminals

	ImproX XFMpk	Multi-mode 13.56 MHz Plastic Keypad Remote
---	--------------	--

125 KHZ TERMINALS, GROUP 2**Table 5 – 125 kHz Terminals, Group 2**

Group 2 Terminals are : ImproX TT and TD (the TD is incorporated into the ImproX DBv).

	ImproX TT	ImproX Twin Antenna Terminal. This can be used with various Antenna Readers. (The TT does not support Remotes designed for use with the ImproX PT and TA Terminals)
	ImproX DBv	ImproX Vertical Drop Box.

125 KHZ ANTENNA READERS FOR GROUP 2 TERMINALS**Table 6 – 125 kHz Antenna Readers for Group 2 Terminals**

These Antenna Readers can be used with the ImproX TT, MfTor DBv.



	ImproX CA	Conduit Antenna Reader
	ImproX KA	Keypad Antenna Reader.

Table 6 – 125 kHz Antenna Readers for Group 2 Terminals

These Antenna Readers can be used with the ImproX TT, MfTor DBv.

	ImproX KHA	Harsh Environment Keypad Antenna Reader.
	ImproX KMA	Remote Mullion Keypad Antenna Reader.
	ImproX MA	Micro Antenna Reader.
	ImproX MHA	Metal Antenna Reader.
	ImproX MMA	Mullion Antenna Reader.

REGISTRATION INTERFACE AND READERS




Table 7 – Registration Interface and Registration Readers

The ImproX RS can be used with either the ImproX RRA (for 125 kHz Tags) or RRM (for Mifare or FeliCa Tags)

--	--	--

Table 7 – Registration Interface and Registration Readers

The ImproX RS can be used with either the ImproX RRA (for 125 kHz Tags) or RRM (for Mifare or FeliCa Tags)

	<p>ImproX RS, USB Registration Interface, Metal Housing</p>	<p>Provides two functions : USB to RS485 conversion; and Allows for the connection of an ImproX Mifare Remote Reader or 125 kHz Remote Reader for Tag Registration. (see also ImproX RRA, RRM).</p>
	<p>ImproX RRM, Registration Remote Reader, Mifare</p>	<p>Reads Mifare Tags. It is used with the ImproX RS.</p>
	<p>ImproX RRA, Registration Reader Antenna, 125 kHz</p>	<p>Reads 125 kHz Tags. It is used with the ImproX RS.</p>

MULTI-FUNCTION TERMINALS

Table 8 – Group 3 – Multifunction Terminals





	<p>ImproX MFT</p>	<p>ImproX Multifunction Terminal. Can be used with any one of the Antenna Readers listed in Table 6, or the Remote Readers listed in Table 3, as well as several biometric, magstripe, barcode remote readers.</p> <p>This unit is able to function normally independently of the system if communications with the system are interrupted.</p>
---	-------------------	---

Table 8 – Group 3 – Multifunction Terminals

	<p>ImproX TRT Twin Remote Terminal</p>	<p>Can be used with any of the following units –</p> <p><i>Multi-mode Remote Readers:</i> ImproX XFMp, XFMpk, XFMM, XFMMk</p> <p><i>Receivers:</i> ImproX RF, IR</p> <p><i>Wiegand Readers:</i> Impro & 3rd party</p>
---	--	--

WIEGAND READERS

Table 9 – Wiegand Readers

	<p>Impro Wiegand 26 (or 44) Non- keypad Metal Reader</p>	<p>26- (or 44-bit) Wiegand Reader for Harsh Environments, without keypad.</p> <p>This can be used with the ImproX PT or TA (but not with the ImproX TT).</p>
	<p>Impro Wiegand 26 (or 44) Keypad Metal Reader</p>	<p>26- (or 44-bit) Wiegand Reader for Harsh Environments, with keypad.</p> <p>This can be used with the ImproX PT or TA (but not with the ImproX TT).</p>

OTHER READERS

The System is designed to support several types of third-party manufactured Biometric Readers. These are listed in Table 10.

Table 10 – Third-party Biometric Readers

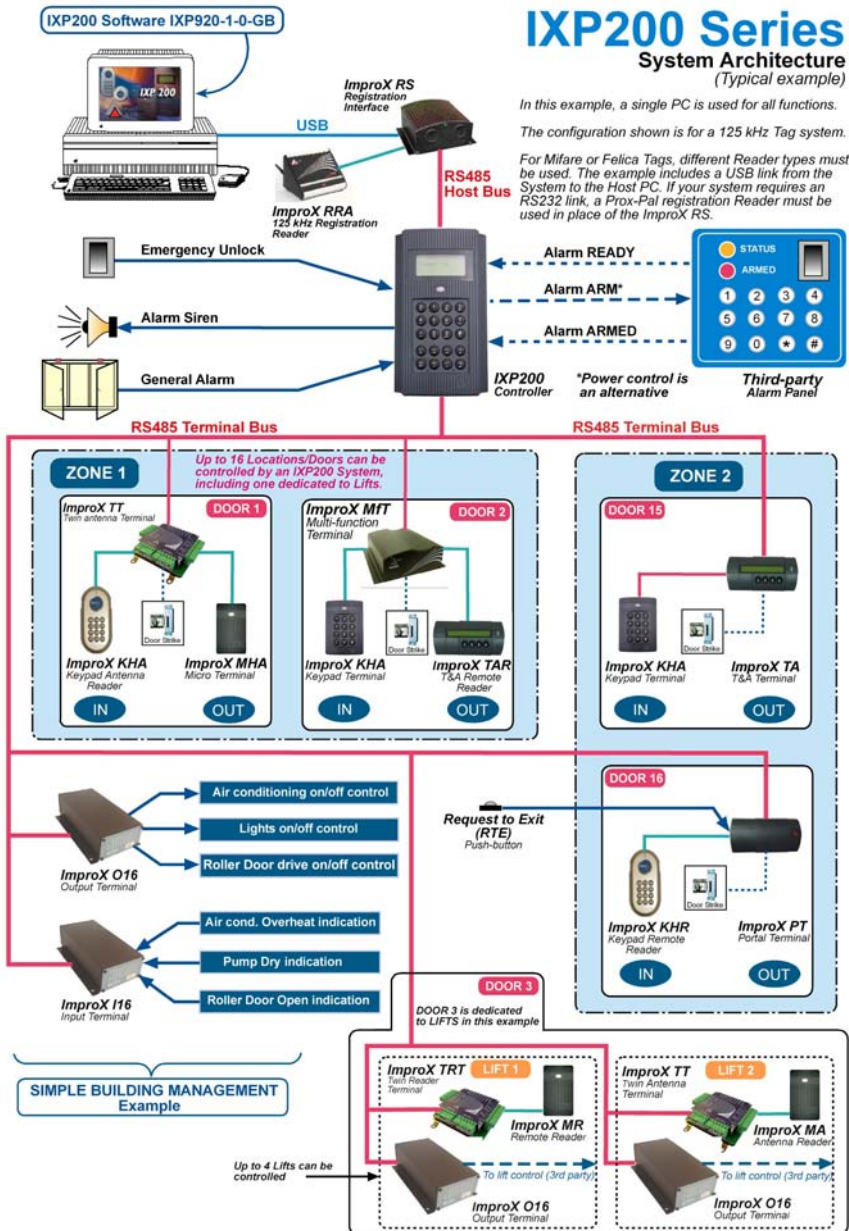
UNIT NAME	TYPE OF READER
Handkey CR	: Hand Registration Reader
Sagem MorphoAccess MA 200 Terminal	: Fingerprint Reader
Sagem MorphoAccess MA 300 Terminal	: Fingerprint Reader

An Impro Wiegand-44 Reader and an ImproX PT Terminal are required when using the Bioscript V-Flex or the Sagem MorphoAccess MA 300 Fingerprint Readers.

An ImproX DL is required when using the Sagem MorphoAccess MA 200 Terminal Fingerprint Reader.

NOTE : *For details of the installation and use of the various Biometric Readers, see the IXP System-compatible Biometric Reader Installation and User Manual.*

See next page



Block diagram of a typical IXP200 System

The system shown above includes only one PC, the Host. No Database Server PC or Editing Workstation PC is used in this example.

NOTES :

1. *Other units are currently being developed that may be used in an IXP200 System.*
2. *For details of the interconnection of the Hardware units, please refer to the IXP200 Hardware Installation Manual.*

SYSTEM INFORMATION

System Features

NOTE : *The figures quoted here indicate the maximum System capacity.*

Total number of Tags	:	2 000
Tags per Tagholder	:	4
Total number of buffered transactions per IXP200 Controller	:	8 000
Sites per System	:	1
Terminals per IXP200 Controller	:	40
Zones per IXP200 Controller	:	16
Tagholder Levels	:	4
Door Modes	:	9
Day Mode Patterns	:	26
Access Groups	:	64
Access Group Patterns	:	8
Standalone Capability	:	Off-line access control after initial configuration using PC; manual editing of some functions, including Tags.
Doors with Anti-passback	:	16
Emergency Unlock	:	All doors
Public Holidays	:	20
Messages	:	255
Message Length	:	64 characters
Time Triggered Actions	:	32
Input Event Triggered Actions	:	16
Digital Outputs for Lifts (elevators) / floors	:	4 x 16
Digital Inputs for Building Management Services	:	1 x 16
Digital Outputs for Building Management Services	:	1 x 16

Compatible Registration Readers

Tag registration in an IXP200 System can be done using one of several ImproX units as shown in the following table.

UNIT	TAG TYPES ACCEPTED BY THIS UNIT	TAGS TYPES <i>NOT</i> ACCEPTED BY THIS UNIT
IXP200 Controller	125 kHz Tags.	Mifare Tags, Infra-red Tags, UHF Tags, FeliCa Tags.
ImproX ProxPal	125 kHz Tags, Infra-red Tags.	Mifare Tags, UHF Tags, FeliCa Tags.
ImproX RS USB Registration Interface with an ImproX RRA Registration Reader Antenna	125 kHz Tags, Infra-red Tags	Mifare Tags, UHF Tags, FeliCa Tags.
ImproX RS USB Registration Interface with an ImproX RRM Remote Reader, Mifare	Mifare Tags, FeliCa Tags Infra-red Tags	125 kHz Tags, UHF Tags.

NOTES :

1. A Personal Access Code (**PAC**) is not a physical Tag, and is not read by any Reader. It acts as a Tag, but must be entered manually via the PC keyboard to register it.
2. Wiegand, ASCII, Barcode, Magstripe and **PAC** Tags must be registered manually via the PC keyboard.
3. The ImproX RS USB Registration Interface, together with either an ImproX RRA or RRM Reader, is one entity as far as the System Software Configuration is concerned. The combination is therefore often referred to as the USB "Registration Reader" in this manual.

Compatible Tag Types

Below is a list of the Tag types which are compatible with IXP200 Systems. The Software allocates a Level to the Tag, and this level can relax or restrict access requirements when the door is operating in certain modes.

The System provides read-only support for the following types of Tags :

- (a) Read-Only Tags (125 kHz Manchester format) – both Slim and Omega.
- (b) Writag 2048 (non-encrypted modes) (125 kHz Read/Write Tags).
- (c) Writag 128 (125 kHz Read/Write Tags).
- (d) ImproX RF 4-channel UHF Transmitter.
- (e) ImproX IR Infrared Transmitter.

- (f) Wiegand, ASCII, Barcode and Magstripe are also supported as logical Tag types. Some Terminals have interfaces to connect to input devices for these types.
- (g) Personal Access Code (**PAC**).
- (h) Mifare (13.96 MHz) Tags.
- (i) Felica (13.96 MHz) Tags.

NOTE : *The standard Impro 281 kHz and 125 kHz Tags are not compatible with this System. Contact your distributor for details.*

Tag Levels

Each Tag must be allocated one of the following levels in the IXP200 System :

- | | | |
|---------------|---|---|
| Visitor | – | for persons requiring temporary access. |
| Normal | – | typically used for employees. |
| Supervisor | – | can arm/disarm alarm System, acknowledge alarms, and has APB Over-ride. |
| Administrator | – | has Supervisor level access plus manual System configuration ability. Has access to doors in No Entry Mode. |

Modes

The System can operate in one of two modes, namely Power Control Mode or Alarm Arming Mode, depending on the hard-wiring of the IXP200 Controller in the System, as well as on the System Software configuration of the IXP200 Controller. (For System interconnection information, refer to the IXP200 Hardware Installation Manual).

Power Control

The Power Control Mode is available when Relay 2 on the IXP200 Controller is suitably connected. When the System is in this Mode the following apply :

- [1] When the first person enters an empty APB (Anti-Passback) Zone, the relay that controls the power switches on immediately.
- [2] The doors in the Zone must have APB selected, as the System counts the number of people inside the Zone who are leaving the Zone to determine when there are no Tagholders in the Zone. Once all the Tagholders have left the Zone, the System knows that power to appliances in the Zone should be switched off.
- [3] The relay (Relay 2) switches off 30 seconds after the last person leaves the APB Zone.

Alarm Arming

An Alarm System supplied by a third party can be linked to the IXP200 so that it can be armed or disarmed via one or more of the keypad Terminals in the IXP200 System. However the Alarm System can only be disarmed on its own Panel, using its own password, unless it has a simple toggle switch.

When Armed, designated doors are set to the Armed Mode as indicated by their Readers' status LED blinking Red.

In this Mode only the Administrator/Supervisor Tags can enter at these doors.

Alarm Arming – Relay 2

A third party Alarm System can be linked to the IXP200 so that it can be armed at any IXP200 Keypad Terminal designated for alarm arming.

The Alarm System can be automatically disarmed by presenting a Supervisor or Administrator Tag at an armed door.

NOTE : *Some Alarm Systems may additionally require a password to be entered on the associated Alarm System Panel.*

Arming

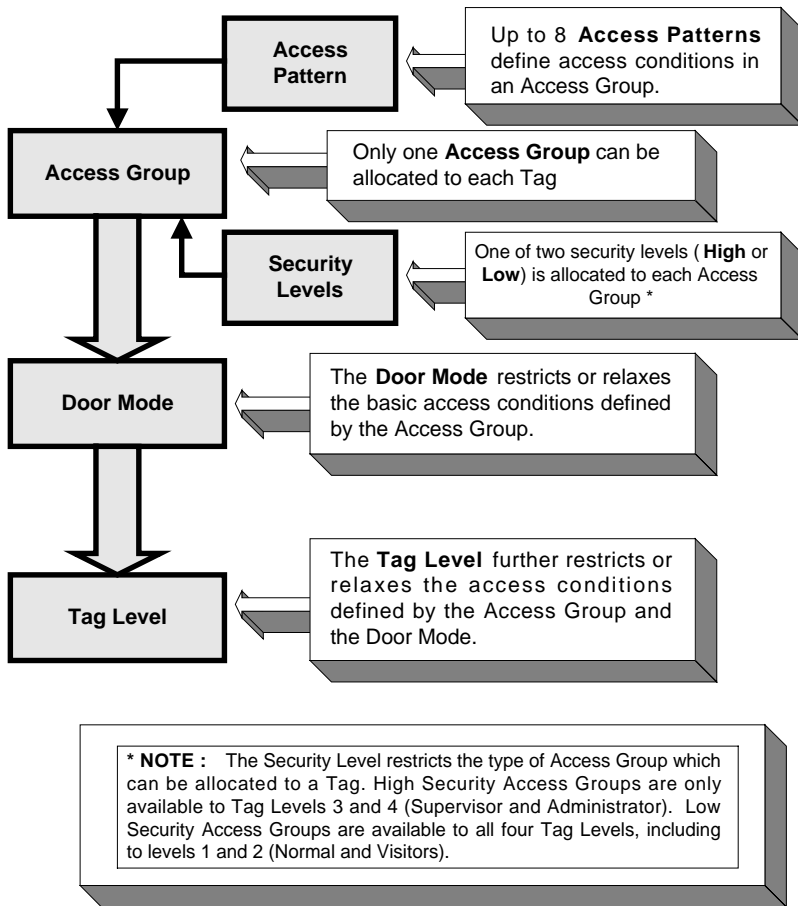
To arm the alarm System :

- [1] Present a Supervisor or Administrator Tag at the exit Readers.
- [2] Press # on the keypad within 10 seconds of presenting the Tag.
- [3] Exit within 30 seconds.
- [4] The System attempts to arm and will arm 30 seconds later if the Alarm Panel reports that it is armed.
- [5] The Reader's LED then indicates Armed Mode (blinking Red).
- [6] If the Alarm Panel is unable to arm at the first attempt, the System will automatically retry every minute.

When Armed

- [1] The Status LED of all armed door Readers indicates Armed Mode.
- [2] Only valid Administrator/Supervisor Tags can enter doors in Armed Mode. All other Tags are denied access, irrespective of the Access Group allocated to them.
- [3] Presenting a Supervisor or Administrator Tag at an armed door will automatically disarm the Alarm System, but the Alarm System may further require a password to be entered at its own panel to disarm it.

See next page



Allocation of Access Conditions to a Tag

ACCESS CONTROL

Access Control is effected by means of a Tag allocated to a person, which must be presented to the Readers at a door. The Tag identifies the person to the IXP200 Controller and access is then allowed according to certain rules as shown in the diagram Allocation of Access Conditions to a Tag.

Access is allowed according to the following rules :

- The Tag must have been allocated access (during System configuration) to the door for the time and day that it was presented, through an Access Group.

- (b) A Tag Level relaxation or restriction of the door access requirements may apply (only certain Tag levels may have access for this Door Mode).
- (c) A Door Mode relaxation or restriction may apply (The current Door Mode may impose other restrictions on the Tagholder, such as “Supervisor Unlock”).

Doors and Zones

Each door may have one or two Readers, namely, an Entry and/or Exit Reader. Two Readers are required to make a door function in Anti-Passback Mode. Doors may also be grouped together into one or more APB Zones (during System configuration).

Door Mode Patterns

A pattern consists of sequential time intervals or slots, covering a 24-hour period. There can be up to 8 Time Slots for each Pattern, each with a different Mode.

Lift (elevator) Control

The System can be used to control access to floors in a building via Lifts (elevators). When selecting the Lift option, a “door” represents a group of Lifts (elevators). A maximum of 4 Lifts (elevators) (Digital Output Terminals) and 16 Floors can be accommodated. Each Lift (elevator) must be provided with a Reader Terminal and associated Output Terminal (refer to the IXP200 Installation Manual for details).

For Lift (elevator) control, a Reader is installed inside a Lift (elevator) and is linked to a specific O16 Output Terminal that functions as a Lift (elevator) Control Unit. This means that access to specific floors can be assigned to the Tag. When the Tag is presented at the Lift (elevator) Readers only the buttons corresponding to those floors are enabled for selection. The duration of the enabled period can be set in the Configuration Software for the Lift (elevator) Control O16 Terminal.

Access Groups

Access to certain areas is given to Tags by means of Access Groups that define when access is allowed and the doors through which access is allowed. Each Tagholder Access Group can have up to eight Access Patterns. Each Tag must be allocated an Access Group.

Addressing Scheme

Each ImproX Terminal is factory programmed with a 4-byte unique address (called a Fixed Address). At the initial System start-up, the IXP200 Controller polls for these unique addresses and the IXP200 Software assigns a 2-byte Logical Address to each unit detected (this process is called “Auto-ID”).

The Logical Addressing as supported in the communications protocol is used to address all units. The Logical Addresses are stored in the individual units’ non-volatile memory, so that the process of assigning Logical Addresses is only required on the initial System start-up.

Architecture – System PCs

In an IXP200 System, the following PC configuration options can be used:

- Option 1

a single PC (called the Host) can be used for all control and storage functions. In this case, all system and database control are vested in this PC.

- Option 2

Two PCs (on the same network) can be used. The first, known as the Engine Workstation (a Host PC), would communicate with the system Controller, and would be used to monitor and control the IXP200 system. The second PC would be used for offline editing of the Database.

In this case the Host PC is known as the Engine Workstation, and the second PC as the Editing Workstation. Typically, the Host PC/Engine Workstation might be in a secure area, while the Editing Workstation could be at a desk where Tagholder administration, etc, is performed.

The Editing Workstation can be used in systems using V6.0, or higher versions, of the System Software. The Editing Workstation will not display live transactions or alarms, nor door status, and cannot perform any functions that require active connection to the Controller. Backup cannot be performed from the Editing Workstation. Tags and Access Groups can be added at the Editing Workstation, and Reports can be viewed from this PC.

- Option 3

Two separate PCs on the same network can be used, one for the IXP200 software (the Host PC), and the second (the Database Server PC) containing the System Database.

- Option 4

Two or three separate PCs can be used to provide a combination of Options 2 and 3.

Software

The System Software consists of a single application, IXP200, installed on to a PC (the Host PC) together with a database (Firebird). Both of these packages are included on the IXP200 Software CD. The database can be installed on a separate PC on the same network as the Host PC

The System Hardware is made up of a single IXP200 Controller, and up to 32 ImproX Terminals*¹ and 32 Remote Readers controlling 16 doors, and an optional ImproX O16 Output Terminal and ImproX I16 Terminal for building management. Additional O16 Terminals may be added for Lift (elevator) control, with 1 additional Reader per Lift (elevator), up to a maximum of 4 Lifts

(elevators) and 16 floors. A Tag can be given access to selected floors, or to all 16 floors.

NOTE*1: *This figure refers to single-address Terminals. Some Terminals have two addresses; if these types are used the total possible number of Terminals is reduced in proportion.*

The IXP200 Software communicates with the IXP200 Controller via an RS232 serial port or USB port. The IXP200 Controller may also act as a Reader for Tag registration, that is, to enter new Tags in the database, (except in Systems equipped with Multi-mode (i.e. Mifare/FeliCa) Readers).

Registration Readers

The ImproX RS Registration Interface provides USB to RS485 conversion, which permits the IXP200 Controller to be installed up to 1 km (0.62 miles) from the Host PC. ImproX IR Tags can be registered using the ImproX RS.

The ImproX RS must be used with an ImproX RRA (for 125 kHz Tags) or ImproX RRM (for Mifare or FeliCa Tags).

NOTES:

1. *An IXP200 System can continue to operate if the Host PC is disconnected from the IXP200 Controller, either deliberately or due to a fault. The IXP200 System then operates as a standalone System. Transaction data is recorded in the IXP200 Controller database.*
2. *When the Host PC is reconnected to the IXP200 Controller, the PC's database is automatically updated with the latest transactions from the IXP200 Controller's database. If changes are made on the Host PC's database while it is disconnected from the IXP200 Controller e.g. adding new Doors etc, a Full Upload (refer to Section 2) is then required to update the IXP200 Controller database with the updated configuration data from the System Database.*
3. *Updates to the System Database can also be made at the Editing Workstation (if used). Note that the Host PC **must** be online to the Controller for any changes to be propagated to the Controller.*
4. *The ImproX MFT Multifunction Terminal is able to validate Tags even when communications with the Controller are disrupted. It will continue to allow access to Tags that have previously been presented to it, but will deny access to other Tags. When comms is restored, transactions completed during the comms failure are uploaded to the Controller database.*

Graphics Software

The Graphics Software comprises two components, namely the Designer Module and the Runtime Module.

The Designer Module is a separate Module and allows the user to develop various plans, and is described in the Impro Graphics Designer Module manual.

The Runtime Module is integrated into the IXP200 Software and allows the Graphics Software to display plans derived using the Graphics Designer Software Module, and to permit the monitoring and control of various System Parameters by means of icons superimposed on the plans.

Refer to Section 3, Chapter 12 of this manual for further details of the use of the Graphics Runtime Module.

END OF SECTION

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_system-swm-en-12 Section 1.doc
------------------	----------	-----------	--

IXP200

Software User Manual

SECTION 2

SOFTWARE

INSTALLATION

SECTION 2 - CONTENTS

INTRODUCTION.....	6
DATE/TIME FORMATS	6
NETWORK AND COMPUTER SECURITY.....	6
IXP200 SYSTEM SOFTWARE INSTALLATION INSTRUCTIONS.....	7
Installation procedure when using a single (Host) PC.....	7
INSTALLATION PROCEDURE WHEN SEPARATE DATABASE SERVER PC IS USED ..	13
OPERATIONAL DIFFERENCES WHEN USING A HOST AND A SEPARATE SERVER ..	15
Backup.....	15
Restore	15
GETTING STARTED	15
Upgrading an Existing IXP200 Database	15
Communications (Controller to Host PC)	15
STARTING-UP THE IXP200 SYSTEM	16
Initial Operations	17
TROUBLESHOOTING	17
IB CONSOLE : DATABASE ADMINISTRATION UTILITY.....	17
Register - Server.....	17
CHANGING PASSWORD OR ADDING ANOTHER USER.....	18
Changing the Password	18
Adding Another User	19
REGISTER DATABASE (OPTIONAL)	19
INDEX	19

DIAGRAMS

Figure 1 : Installation introductory screen.....	9
--	---

SECTION 2 - SOFTWARE INSTALLATION

INTRODUCTION

This Section describes the installation procedure for the IXP200 System Software.

The IXP200 System Software is a single- or multi-user access control System using the ImproX range of hardware. It is designed for use with Windows 98 Second Edition*, 2000, NT SP6a, or XP Professional

NOTE : * *For limitations on the use of Windows 98, see **Operating System** later in this Section.*

This Software is supplied on the IXP200 System Software CDRom.

DATE/TIME FORMATS

All dates and times in the IXP200 System are entered and displayed in ISO Standard Format (Dates - yyyy-mm-dd, and Times hh:mm:ss).

NETWORK AND COMPUTER SECURITY

CAUTION

The security of the network and the computers on which the software is installed remains the responsibility of the customer. If the computer on which the system is installed is compromised, or the network is compromised, then it may become possible to make unauthorized modifications to the configuration of the system, and physical security may be breached.

It is strongly recommended that the latest security updates are obtained and applied on a regular basis to all computers on which any component of the system is running.

Physical access to the computers running the system must also be controlled, to ensure that access by unauthorized persons does not occur.

IXP200 SYSTEM SOFTWARE INSTALLATION INSTRUCTIONS

Installation procedure when using a single (Host) PC

General

If older versions of the Software exist on the drive, be sure to Uninstall these first, having first made a backup copy of the database file "proxette.fdb", "proxette.properties" and "graphics.properties".

Computer Hardware

An IXP200 System can use one, two or three PCs. These are:

The Host PC – this PC is always required. The System Software is installed on this PC.

A Server PC – the System Database can be installed on this second machine.

An Editing Workstation – this PC can be used to edit the System offline.

NOTE: *When an Editing Workstation is included, the Host PC is known as the Engine PC.*

The minimum requirements for any PC and peripheral devices used with the Software are as follows:

CPU	:	Pentium II 300 or faster processor.
Memory	:	Minimum 128 MB RAM (256 MB for Windows NT).
Peripherals	:	CDROM drive, or access to a network CDROM drive.
Communications	:	RS232 port.
Hard Drive	:	Minimum 200 MB of unused space.
Floppy Drive	:	3.5" high-density stiffy drive.
Pointing Device	:	Mouse or equivalent.
Printer	:	Laser or Inkjet printer.
Display	:	Super VGA with a minimum resolution of 800 x 600.

Disk Space Requirement per PC

200 MB of free disk space on the local drive is required to install the IXP200 System Software and the database.

Operating System

The IXP200 System Software requires one of the following operating Systems to be installed on each of the PCs involved:

Windows 98***, 2000 Professional, NT or XP Professional .

NOTE : *** *Windows 98 cannot be used in Systems using the USB Registration Reader.*

Software Location

The Software may be installed to a folder "IXP200" on any hard drive in the Local Host PC and the Editing Workstation (if used). The information in this section assumes that the Software is installed to C:\IXP200, which is a typical situation.

NOTE : *The Software must be installed on the Local Host PC, the PC that communicates with the Controller. It can also be installed on the hard drive of another PC in the same network as the Local Host where this second PC is used as an Editing Workstation. The Database Management System can also be installed on a separate Database Server PC in the network.*

NOTE : *If an older version of the Software exists on the drive, be sure to use Windows Add/Remove Programs to uninstall this older version before installing the new version.*

The database file "proxette.gdb" or "proxette.fdb" will not be removed by this process, and also will not be over-written when the new Software is installed.

Log-on Requirements

If you are using Windows NT or Windows 2000, you will need to log-on with Administrator privileges on the machine.

NOTE : *Before running setup files, quit all other applications.*

Database Type

IXP200 requires a Database Server to be installed :

- Versions prior to V4.0 of the IXP200 Software used **InterBase**.
- Version V4.0 and higher support the **Firebird** database Software. This database is supplied free of charge with the Software.
- Version V5.0 and higher use the **Jaybird** driver instead of the **InterClient** driver.

INTERBASE MUST BE REMOVED to allow version V4.0 or higher to be installed correctly. From V5.0 on, InterClient must also be removed.

To do this :

[1] First stop all InterBase-related applications and services. When no services are running, uninstall InterBase as described in the paragraphs which follow.

NOTE : *This is absolutely necessary as problems will be encountered if it is not done.*

The following general steps should be followed :

- [i] Stop InterServer (Start/Programs/InterBase InterClient /InterServer Configuration Utility). Go to the Advanced tab and click Stop.
- [ii] Stop InterBase Guardian if this is used. (Windows 98 users should see this

in the Task Bar, but other Windows users may have this running as a service).

- [iii] Stop InterBase Server (Start/Programs/InterBase/Server Manager).
- [iv] Uninstall InterBase 6.01 (Control Panel/Add/Remove Programs).
- [v] Uninstall InterClient (Control Panel/Add/Remove Programs).

NOTE: *This procedure may vary slightly and depends on the operating System used and the way the database was configured.*

- [2] Once InterBase has successfully been uninstalled, the new IXP200 Software can be installed as described below.

Installation Procedure – Single (Host) PC

NOTES:

1. Before running setup files, quit all other applications.
2. The installation procedure is described in several languages in the Installation Software. The required language can be chosen using the drop-down menu in the Installation introductory window.

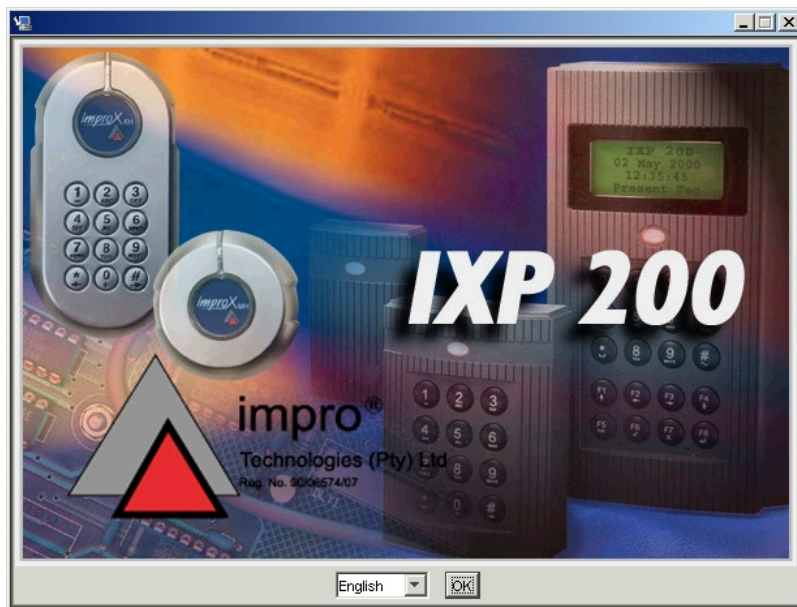


Figure 1 : Installation introductory screen

To install the IXP200 Software, proceed as follows :

- [1] If a previous version of IXP200 is installed, this must be uninstalled.
- [2] Run the **Setup.exe** file in the root folder on the CD to install IXP200 V6.0 and the associated applications.

- [3] Select the path to the Installation folder. By default, the files will be copied into the folder IXP200.
 - [4] From V4.0, the Database Management System has been changed from InterBase to Firebird. The Installer Software will automatically detect the presence of InterBase and will exit the setup process and ask the user to uninstall InterBase before restarting the Installer. Once restarted, the Installer will install Firebird if it has not previously been installed (See **Installation of Firebird**).
- NOTE :** *There is one condition here. If Firebird is already installed but the password for Firebird is not "masterkey" (the IXP200 default password), then the Installer will try to re-install Firebird and display a message to stop the Firebird or InterBase server. In this case, just click OK and ignore the message.*
- [5] Start icons will automatically be created for IXP200.
 - [6] Configuration information is stored in the "proxette.properties" file in the IXP200 folder. Defaults are supplied which should be sufficient for most installations.
 - [7] Any existing "proxette.properties" file is overwritten for V5.0 onwards to ensure that the correct driver settings are present. If the default settings had been changed in the existing installation, it may be necessary to browse to locate the existing database at logon and check the serial port and ProxPal Tag Reader/Registration Reader setting when starting IXP200.
 - [8] For a new installation where no prior database exists (file "proxette.fdb"), you will have been prompted during the installation for your locale (region). The correct database file type for that locale will then be automatically copied from the Empty Database folder to the Database folder. The encoding property in the "proxette.properties" file is automatically set to match the locale chosen. The "graphics.properties" file will have its settings synchronised with "proxette.properties" when logging on to IXP200. (See **Database Settings**).
 - [9] If a database already exists from a previous installation, refer to the **UpdateReadme** file for update instructions.

Java Runtime Environment Installation

The IXP200 Software Installation Wizard will automatically install the Java Runtime Environment (JRE) with comms extensions.

Installation of Firebird

This is triggered automatically during IXP200 installation, but can also be started manually if required.

Firebird (V1.5.2) is the version currently used. There is no need to reinstall the current version if you already have it.

If you have an older version of Firebird installed on the computer, then stop all Firebird-related applications and services and uninstall Firebird first.

Then :

- [1] To start a manual Firebird installation, run the Firebird Setup.exe file in the Firebird folder on the IXP200 CD.
- [2] When asked to select "Additional Tasks", the settings should all be checked by default. Always run Firebird as a service on an operating System which supports it. Windows 98 does not support services, so when using this operating System select Firebird as an application.
- [3] Jaybird, which is the JDBC driver for Firebird, is automatically installed with IXP200 Software. The current version is V1.5.
- [4] Reboot the computer when the Installation Wizard has completely terminated.
- [5] After rebooting, check in Start/Control Panel/Administrative Tools/Services that Firebird Server and Firebird Guardian Services are running.

Database Considerations

The default folder for the installed database to be used by IXP200 is IXP200\database and the default name is "proxette.fdb".

Different regions of the world use different encoding for their databases – these are listed below. From V3.4.2 on, the Software installs a database by default to match the locale chosen, but only if no existing "proxette.fdb" file is present. The installation creates the folder database/Empty Database which contains three folders, one for each of the different encodings that are now supported. These are :

- (a) Eastern Europe.
- (b) Western Europe.
- (c) Unicode. This is suitable for the Far East, but can also be used for other regions (except Eastern Europe), but does use more space on the drive.

Each folder contains an empty database suitable for the region concerned (all empty databases have the name "proxette.fdb").

NOTE : *These databases should never be edited directly, but retained as empty databases to be copied in case of recovery.*

In case a new empty database is required, select the database for the encoding required for your locale, and copy it to the IXP200\Database folder before starting IXP200 - all the databases have the same name "proxette.fdb". Ensure that the "proxette.properties" file has the correct entry for the encoding selected (see **Properties File** below).

Properties File

A file named "proxette.properties", located in the IXP200 folder, is used by the System to store initialization information, such as the location of the database, the serial port to be used, as well as Database settings, Serial Port settings and other settings. A default "properties" file is provided on installation. It should not be necessary to edit this file as selections made by the user in the Software are automatically recorded in the file. However, if necessary, this file can be edited, using a program such as WordPad or Notepad. Comment lines are preceded by a

"#" character.

The "graphics.properties" file also stores configuration information for the graphics module.

Database Settings

The database should have the setting 'Forced Writes' = true in Database properties.

It is not necessary to change the URL in the "properties" file to specify where "proxette.fdb" is located. When logging on to IXP200, the user can browse to locate the database. The database must be located on the same PC as the IXP200 Software. This location will then be stored in the "properties" file under the key

Proxette.database.Interbase.URL.0=C:\\\IXP200\\database\\proxette.fdb

The database encoding property also appears in the "proxette.properties" file. It is important to ensure that the encoding property matches the database selected. This is **essential** to ensure that the data in the database is interpreted correctly. This is done automatically for a new installation. An existing database is never overwritten, but the "properties" file is overwritten in V5.0 only of IXP200 to correct the driver settings.

e.g. Proxette.database.Interbase.encoding=ISO 8859_1

Use :

ISO 8859_1 for Western Europe (Latin 1).

WIN1250 for Eastern Europe (Latin 2).

UNICODE_FSS for the Far East (Unicode).

The encoding setting is case-sensitive and should be entered exactly as shown above. **Do not leave** any white spaces after the text.

NOTE : *The name "Interbase" in the above key will be retained even though the database used is now Firebird.*

The "graphics.properties" file has the same value for the database location and encoding as the "proxette.properties" file, and is synchronised with "proxette.properties" when logging on to IXP200.

Graphics.database.interbase.url=

jbdcl:firebird.sql\\:localhost/c\\:IXP200/database/proxette.fdb

Graphics.database.interbase.encoding=ISO8859_1

Error Setting : "proxette.log" file for Trouble Shooting

proxette.error.redirecttofile=true

By default, to ensure that error messages can be reviewed, the key "redirecttofile" is set true in order to log error messages to the "proxette.log" file. This file will be located in IXP200/log folder, named by date, e.g. "proxette20040914.log".

A new file is created each time IXP200 is executed. In case of execution errors, take a copy of this file to send to your dealer to assist in the analysis and resolution of errors.

Device Setting

This is usually set in the Controller Panel or Configuration/System Menu of IXP200 but can be set manually by editing the "proxette.properties" file as follows :

[1] Specify the serial port to which the IXP200 Controller or the ImproX ProxPal Terminal or the ImproX USB "Registration Reader" is connected as follows :

- i Proxette.coms.SerialPortID=COM1
- ii NOTE : Port 0 is COM1 and Port 1 is COM2.
- iii The baud rate and other settings may be left as default.

[2] Specify whether the ProxPal Tag Reader or USB "Registration Reader" is installed :

proxette.tagholder.tagReader.enabled=0

1=ProxPal or USB Registration Reader installed, 0=ProxPal or USB Registration Reader **not** installed

Leave all the other settings with their default values.

Multiple Databases

In some installations multiple databases may be required. For example, if one computer is used for several hardware installations (for example, several factory sites), then separate databases can be supported, one for each site, **but they must all have the same encoding.**

If your System requires multiple databases, each such database must be renamed appropriately (e.g. "IXP200Site1.fdb", "IXP200Site2.fdb", and so on, and held in a "site database" folder created by the user). When the PC is used at Site 1, the appropriate database must be selected at log-on, and so on.

INSTALLATION PROCEDURE WHEN SEPARATE DATABASE SERVER PC IS USED

NOTE: *When using separate PCs for the IXP200 application and for the Database, the PC where IXP200 is installed is known as the HOST, and the PC where the Database is installed is known as the SERVER.*

On the Host PC

- [1] If a previous version of IXP200 is installed, uninstall it.
- [2] Install IXP200 V6.0 to C:\IXP200, (or to the folder where IXP200 is to be installed, if different), and follow the sequence listed under Installation Procedure – Single (Host) PC.
- [3] Run UpgradeDatabase to upgrade an existing Database.
- [4] Firebird Server is not required to run on the Host anymore, and can be stopped.

On the Database Server PC

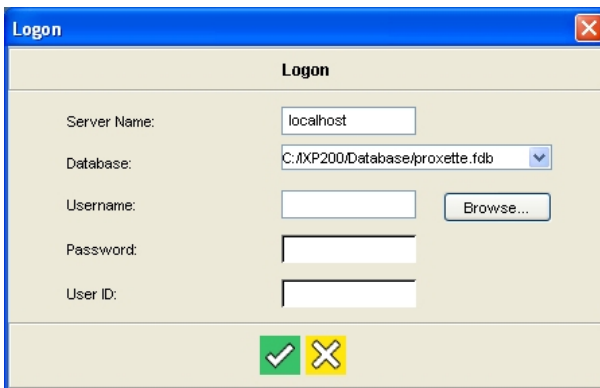
- [1] Install Firebird Server by running setup.exe from the Firebird folder on the IXP200 CD. Ensure that it runs automatically as a service, and that it has started.
- [2] Create a shared folder (called, for example, Access), and create a Database sub-folder inside it.
- [3] Assuming the folder Access is off the root directory, the path to the Database should be C:\Access\Database.

NOTE: *The shared folder must be accessible by the user at the Host PC.*

- [4] Copy the Database (proxette.fdb) from the Host to the Database folder on the Server. After this, it would be wise to rename the database file on the Host so as not to select it by mistake. IXP200 keeps a pick-list of previously selected databases in the Log-in dialog.
- [5] You would probably want to install IBConsole on the Server as well. This can be copied from the Host Tools folder.

On the Host PC

- [1] Start IXP200. The log-in screen will appear (see next illustration).



IXP200 Log-in screen

- [2] In the log-in screen, enter the actual name of the Server PC (as shown in Windows, System Properties > Network Identification); for example, this could be MyServer.
- [3] Enter the local path to the proxette.fdb database file (mapped network paths must not be used, and no browsing is permitted). A typical example of this path is C:\Access\Database\proxette.fdb (This is very important for the correct functioning of the Jaybird driver).
- [4] Enter the Username and Password, and log on.

- [5] If IXP200 does not run successfully, check all the previous steps, particularly the local path and the Server name.
- [6] Once the IXP200 software starts correctly, perform an AutoID in the normal way. There should be no change, as the hardware units are still connected to the Host PC.
- [7] Check that the software operates correctly. It should still allow/deny access at Doors, read Tags, store transactions, draw up and display Reports, and perform all of its normal functions.

OPERATIONAL DIFFERENCES WHEN USING A HOST AND A SEPARATE SERVER

When separate Host and Server PCs are used, there are some operational differences:

Backup

The Backup function can still be activated from the Host on the Server, but not the Restore function. The Backup function is modified so that it only creates a backup file of the type *.fbk if the database is installed on a separate Server.

Restore

The user can manually restore the *.fbk file at the Server using Firebird utilities. (In the normal case, where the database is installed on single Local Host PC, the Backup facility performs the Backup and Restore functions as usual).

- [1] To do backup from the Host at the Server, first map a network drive to the shared folder on the Server (for example, R: is mapped to //MyServer/Access).
- [2] In the Backup Dialog in IXP200, set the Backup path by browsing to the mapped drive and selecting the database folder, for example, R:\Database.
- [3] Click **Backup Now** to test this function. This should create a backup file *.fbk in the R:\Database folder, name according to the date it is created.

GETTING STARTED

Upgrading an Existing IXP200 Database

A utility called UpgradeDatabase is provided to upgrade the database automatically. This must be done whenever the Software is upgraded and before starting IXP200. Please refer to the file "UpgradeReadme.rtf" for detailed instructions.

Communications (Controller to Host PC)

There are three possible ways to connect the Host PC to the Controller :

Option 1 : Directly via Serial Port

- (a) Connect the RS232 Serial Port on the Host PC directly to the Controller's RS232 Port (Default option).
- (b) The distance between the Host PC and the Controller may not exceed 25 m (27.34 yd).
- (c) Tags are registered by reading at the Controller.

Option 2 : Serial Port to ProxPal to Controller

- (a) Connect the ProxPal to an RS232 Serial Port on the Host PC.
- (b) Connect the ProxPal to the Controller by RS485.
- (c) The Controller configuration must be manually changed to operate in RS485 mode - see Section 6 of this manual.
- (d) The distance between the Host PC and the Controller may exceed 25 m (27.34 yd).
- (e) Tags are registered at the ProxPal on the desktop.

Option 3 : USB Port to USB Registration Reader to Controller

- (a) Connect the ImproX RS USB Registration Interface, with its associated Reader, to a USB Port on the Host PC.
- (b) Connect the USB Registration Interface to the Controller by RS485.
- (c) A USB driver must be installed on the PC to redirect the USB Port to a COM Port - see NOTE below.
- (d) The Controller configuration must be manually changed to operate in RS485 mode - see Section 6 of this manual.
- (e) Tags are registered at the Registration Reader on the desktop.

NOTE : *When using the ImproX RS Registration Interface, a definite procedure must be followed to install the USB drivers. This procedure is described in the IXP200 "readme.rtf" file under the heading **INSTALLING THE USB DRIVER TO SUPPORT THE REGISTRATION READER (in place of the ProxPal)**. The COM port for USB communications is allocated as part of this procedure.*

STARTING-UP THE IXP200 SYSTEM

To run the Software, proceed as follows:

- [1] Click on the IXP200 icon displayed on your Desktop screen.
- [2] If the icon is not displayed on the Desktop proceed as follows:
 - [i] Click on Start.
 - [ii] Click on Programs.
 - [iii] Click on IXP200 and then the IXP200 icon.

Initial Operations

A Username and Password are required when logging onto the IXP200 System Software.

NOTE : *The password is case-sensitive.*

The default Username and Password for logging onto the System are:

Username	:	SYSDBA
Password	:	masterkey

When the IXP200 installation and configuration is complete, the Password must be changed to protect the security of the database. Refer to the "Change Password" paragraph for this procedure.

TROUBLESHOOTING

If the Logon Dialog box appears when running the Software, then the IXP200 and the JRE have been installed correctly.

If the logon operation fails, the most common problems are:

- (a) Password is in the wrong case. It should be "masterkey" (lower case).
- (b) The database server, Firebird Server, is not running. During installation it will have been automatically configured to start as a service (if supported) or as an application in the Windows Startup group. If Firebird Server is not running (check Services or look for the icon in the System tray for WIN98) Use Windows Explorer and go to the IXP200/Tools (or go to Control Panel, where it is installed as "Firebird 1.5 Server Manager") folder.
- (c) Execute Firebird Manager ("fbmgr.exe") and start the Firebird Server. If it cannot be run as a service, then ensure that Firebird Guardian is used. This will restart Firebird Server automatically if it stops running. If this fails then it could be that Firebird is not properly installed.
- (d) The PC does not have an IP address. This is necessary even if it is not on a network. Please refer to Appendix A.

IB CONSOLE : DATABASE ADMINISTRATION UTILITY

To run IBConsole :

- [1] Go to Start.
- [2] Then go to Programs.
- [3] Then go to Firebird.
- [4] Select IB_Console.
- [5] If IBConsole is not installed, copy it from the installation CD, namely \Firebird\IBConsole.exe, and place it in C:\Program Files\Firebird\bin. Create a short cut for this file and drag the shortcut into the Start/Programs/Firebird folder.

Register - Server

When using IBConsole for the first time, register the Server (PC) on which the Database is installed. This gives access to any Firebird Databases installed on the Server. To do this :

- [1] Select **Server / Register** from the menu to pop up the Register Server Dialog.
- [2] Select **Local Server** and then enter a description of the Server (e.g. Access Control PC).
- [3] Enter the User Name "SYSDBA" and Password "masterkey". "SYSDBA" is the Administrator User Name (that cannot be changed) and "masterkey" is the default Password that is valid for any new Firebird Database. In fact this is the Administrator password for the Server and gives access to all Firebird Databases registered on this Server.
- [4] The default password must be changed later (see "Changing the Password") to ensure the security of the Database. This is the most important password for the System, giving full access to all tables.
- [5] Click **OK** to save and exit.
- [6] An entry for the Server will now appear in the left-hand pane.

From this point on, when using IB_Console, select the Server and log-on using a valid User Name and Password.

CAUTION

A copy of the Administrator's User Name and Password must be given to the Manager of the Company / Owner of the System for safekeeping EVERY TIME THE PASSWORD IS CHANGED! If this password is lost there can be no access to the Database.

CHANGING PASSWORD OR ADDING ANOTHER USER

To carry out either of these operations, first :

- [1] Select the **Server icon** in the left-hand pane.
 - [2] Log on. Successful connection is shown by a green tick (check) mark next to the Server icon.
 - [3] Click the + sign next to the Server icon to expand the list of objects associated with the Server.
 - [4] Select Users and the list of users will be displayed in the right-hand pane.
- Then follow the appropriate sequence described below.

Changing the Password

To change the password :

- [1] Right-click an existing **User Name** displayed in the right-hand pane.
- [2] Select **Modify User** from the pop-up menu. The User Information Dialog will

now be displayed.

- [3] Change the password.
- [4] Confirm the change by entering the password again in the second box.
- [5] Click **Apply** to save the new password.
- [6] Click **Close** to exit.

Adding Another User

To add another User :

- [1] Right-click any **User Name** displayed in the right-hand pane.
- [2] Select **Add User** from the pop-up menu. The **User Information Dialog** is now displayed.
- [3] Enter a User Name and Password.
- [4] Confirm the new Password by entering it again.
- [5] Click **Apply** to save new User.
- [6] Click **Close** to exit.

NOTE : *IXP200 makes provision for another User to have limited access to the Database, to allocate Visitor Tags with low security access and to obtain reports. This User should have the User Name "OPERATOR" and Password "impro". Create this User if required, otherwise the only user would be the Administrator User. No other user has access to the tables.*

REGISTER DATABASE (OPTIONAL)

It is necessary to register the Database in order to do maintenance, such as a Sweep if the Database becomes corrupted.

Before connecting to a Database on IBConsole, it must be registered. To do this :

- [1] Select **Database / Register** from the menu to pop up the **Register Database and Connect Dialog**. The full path and file name of the Database file is required.
- [2] Click on the button to the right of the file name to locate and select it. An Alias name may be supplied.
- [3] The Administrator User Name and Password may now be entered.
- [4] Click on **OK** to save and exit.
- [5] The Database is now registered and opened (if the User Name and Password were supplied), indicated by a green tick (check) mark next to the Database icon.
- [6] To disconnect from the Database, first select the **Database** icon and then double-click, and then select **Disconnect** under Action in the right-hand pane.
- [7] Click the **X** in the right hand top corner of the main IBConsole window to Exit IB_Console.

INDEX

- Administrator, 8, 18, 19
- baud rate, 13
- Configuration, 8, 10, 13
- Controller, 13
- database, 7, 8, 9, 10, 11, 12, 13, 15, 17
- Database Management System, 10
- Database Server, 8
- Database Settings**, 10, 12
- default folder, 11
- Disk Space, 7
- Empty Database, 10, 11
- error messages, 12
- Firebird, 8, 10, 11, 12, 17, 18
- IBConsole, 17, 18, 19
- initialization information, 11
- Installation Folder, 10
- Installation Wizard, 10, 11
- Interbase, 12
- InterBase Guardian, 8
- InterBase Server, 9
- InterClient, 8, 9
- InterServer, 8
- IP address, 17
- locale, 10, 11
- minimum requirements, 7
- Multiple Databases, 13
- new installation, 10, 12
- operating system*, 9, 11
- Password, 17, 18, 19
- previous installation, 10
- proxette, 7, 8, 10, 11, 12, 13
- ProxPal, 10, 13
- serial port, 10, 11, 13
- setup files*, 8, 9
- uninstall, 8, 10
- Username, 17

END OF SECTION

USER'S NOTES

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	\\Custman\ IXP200\ English Manuals\ ixp200_sys-swm-en-12 Section 2.doc
------------------	----------	-----------	---

IXP200 Software User Manual

SECTION 3 CONFIGURATION PART A

[Chapters 1 to 5]

SECTION 3 PART A – SYSTEM CONFIGURATION

CONTENTS

CHAPTER 1 – INTRODUCTION	5
GENERAL	5
Manual Editing Facility	6
IXP200 Toolbar Icons.....	6
Typical Floor Plan and Block Diagram.....	7
Main Application Window	9
Auto ID, Database Connection and Communication Status Icons	9
Active Transaction Panel	10
Active Transaction Panel Fields and Buttons	11
Alarm Panel Fields and Buttons	12
Door Status Panel.....	13
Door Status Panel.....	13
Building Graphics Software.....	16
Graphics features	17
Addressing of Units.....	17
A Fixed Address.....	17
A Logical Address	17
Recording of Installation Information	17
IXP200 Software Start-up.....	18
New System – Logging on for the First Time	18
Auto Identification Unit Detection	19
Performing Auto-ID	19
SYSTEM STARTUP.....	20
SYSTEM CONFIGURATION PROCEDURE	20
IXP200 System Configuration Requirements.....	21
CHAPTER 2 - CONTROLLER CONFIGURATION	23
GENERAL.....	23
Port 1 - RS485.....	23
Port 2 - RS232/RS485	23
Port 3 - RS232.....	23
Digital Outputs	23
Power Control/Alarm Arming Modes.....	23
Power Control	24
Alarm Arming/Disarming	24
Digital Inputs	24
Controller Configuration	25
APB Lockout Delay.....	26
Mifare Readers	26
Controller Fields and Buttons.....	26
Configuring the Controller - Procedure	27
Daylight Saving	28
CHAPTER 3 – DOOR CONFIGURATION	31

GENERAL	31
DOORS, READERS AND DOOR MODE PATTERNS CONFIGURATION	31
Doors and Readers Panel Fields and Buttons	32
Door Tab Panel – Top Pane	32
Door Tab Panel – Middle Pane	32
Configuring Doors and Readers Procedures	33
Reader Setting Dialog	34
Entry and Exit Tabs	35
Entry and Exit Tabs – Middle Panel	37
DELETING AN EXISTING DOOR	39
LIFT (ELEVATOR) CONTROL	41
Door Tab Panel – Middle Pane	41
Configuring Lift (elevator) Readers - Procedure	42
Reader1 – 4 Tabs	43
Reader1 – 4 Configuration Procedure	44
Day Mode Setting	44
Day Mode Configuration Procedure	44
Day Mode Setting	45
DOOR MODE PATTERNS	46
Default Door Mode Pattern	46
Door Mode Pattern Tab	47
DOOR MODE COMPATIBILITY	52
Configuring Door Mode Patterns – Procedure	54
Deleting an Existing Door Mode Pattern	55
Deleting a Time Slot	56
CHAPTER 4 - INPUT/OUTPUT TERMINALS	57
GENERAL	57
NUMBER OF TERMINALS IN A SYSTEM	57
BUILDING MANAGEMENT	57
LIFT (ELEVATOR) CONTROL	57
I/O TERMINAL CONFIGURATION - PROCEDURE	57
Input/Output Terminals Panel Fields and Buttons	58
INPUT/OUTPUT TERMINAL CONFIGURATION	59
CONFIGURING AN OUTPUT TERMINAL - PROCEDURE	59
CONFIGURING AN INPUT TERMINAL - PROCEDURE	61
CHAPTER 5 – TIME/EVENT TRIGGERED ACTION CONFIGURATION	63
GENERAL	63
Action Types	63
Time Triggered Actions	64
Event Triggered Actions	64
Time/Event Panel Fields and Buttons	64
Time Triggered Actions Tab	65
Days of week	65
Select Action Type	65
CONFIGURING TIME TRIGGERED ACTIONS - PROCEDURE	65
Relay Action Configuration	67

Editing an Existing Time Triggered Action	67
Deleting a Time Triggered Action.....	67
EVENT TRIGGERED ACTION CONFIGURATION	68
Event Triggered Actions Tab	68
ACTION.....	69
EVENT TRIGGERED ACTION CONFIGURATION – PROCEDURE.....	69
Editing an Existing Event Triggered Action	71
Deleting an Existing Event Triggered Action	72
INDEX.....	72

CHAPTER 1 – INTRODUCTION

GENERAL

The IXP200 Software Suite has been designed with user-friendliness as a major design criterion.

The System must be configured using the IXP200 System PC software.

This section of the manual describes the configuration of the IXP200 System Software.

SAMPLE DATA

Many of the screens shown in this manual are based on a theoretical IXP200 System, a small System for a fictitious company called Excel Products. A floor plan for this installation is shown in Figure 1, and a typical block diagram of the System architecture is shown in Figure 2.

The Excel Products installation includes six Doors, four for access within the main building, one for access to the car park, and a sixth for control of a Lift (elevator). The System also performs Building Management functions, controlling a central air-conditioning plant, an emergency generator, oven heating and a roller door.

The last four characters of the ImproX unit Logical Addresses as allocated by the System are shown next to the units in Figure 1.

Four fictitious Tagholders are registered in this simple explanatory System. Their details are :

Tagholder's Name	Tag Number	Tag Level
William Newton	208038349100	Administrator
John Walton	208038343237	Normal
Clara Calisto	208038354551	Supervisor
James Nigel Haines	208038347205	Visitor

The System includes six Doors, and two Anti-Passback Zones. One ImproX O16 Terminal serves the Lift (elevator) (Door 2), and one ImproX O16 Terminal and one ImproX I16 Terminal provide Building Management services for the air-conditioning plant, roller door, the emergency generator and the ovens in the laboratory.

There are two departments, Administration and Laboratory.











Other details of the System are included as appropriate in the software configuration information.

Manual Editing Facility

















The current version of PC software and Controller firmware allow manual capture and editing of Tag data via the Controller keypad and LCD. This feature is described in Section 6 of this manual.

IXP200 Toolbar Icons

In the table below is a brief description of the shortcut Icons available to the user when configuring an IXP200 System.

	General System Setup.		Tagholders and Tags.
	Doors, Readers and Door Mode Patterns.		Holidays.
	Inputs and Outputs.		Web Reports.
	Time and Event Triggered Actions.		Help.
	Access Groups.		Open and close Active Transaction Panel.

Certain common functions are performed using buttons identified by icons. These buttons are shown below. In the text, the names shown are used to describe these buttons.

	Apply <i>or</i> OK		Cancel
	Add		Delete
	Edit		First
	Previous		Last
	Next		Print Card
	Building Graphics		Scale Floor Plan
	Next Tag		Previous Tag
	Show related Base Plan		Batch Print

Typical Floor Plan and Block Diagram

A Floor Plan and Block Diagram for a typical fictitious installation are shown on the next two pages.

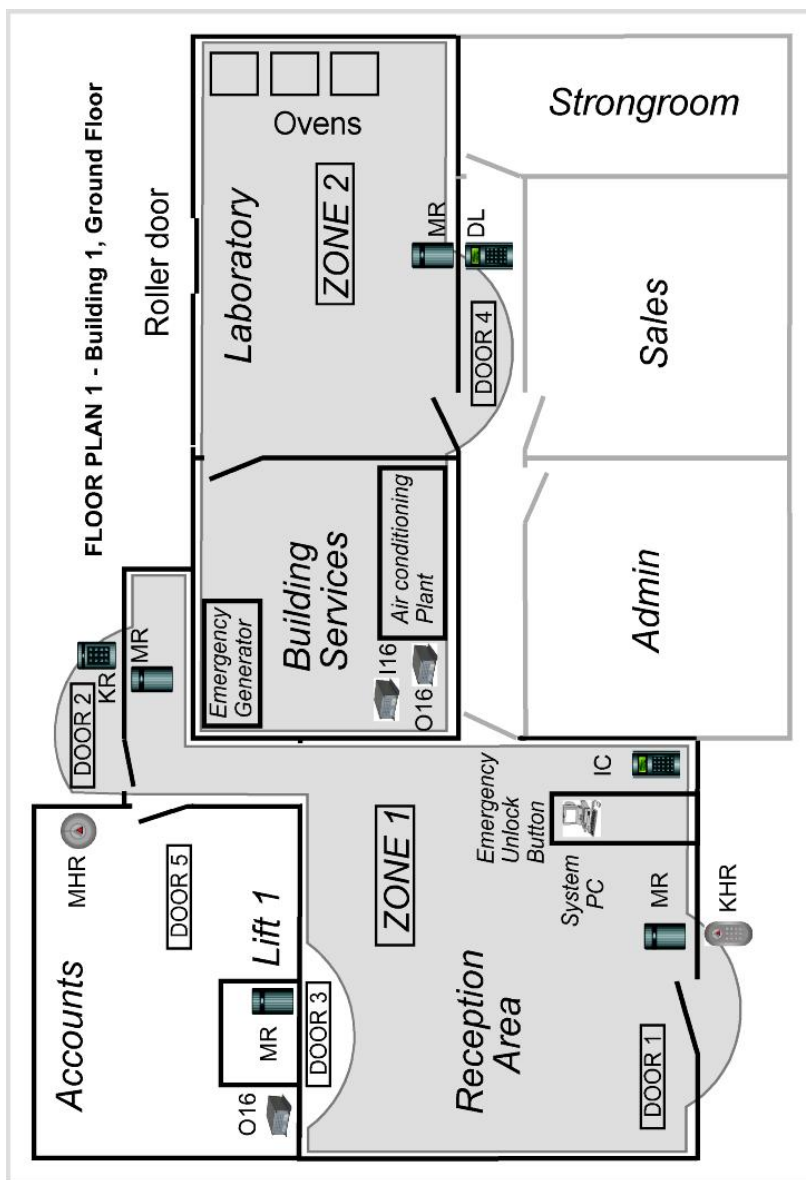


Figure 1 : Floor plan for Excel Products ground floor

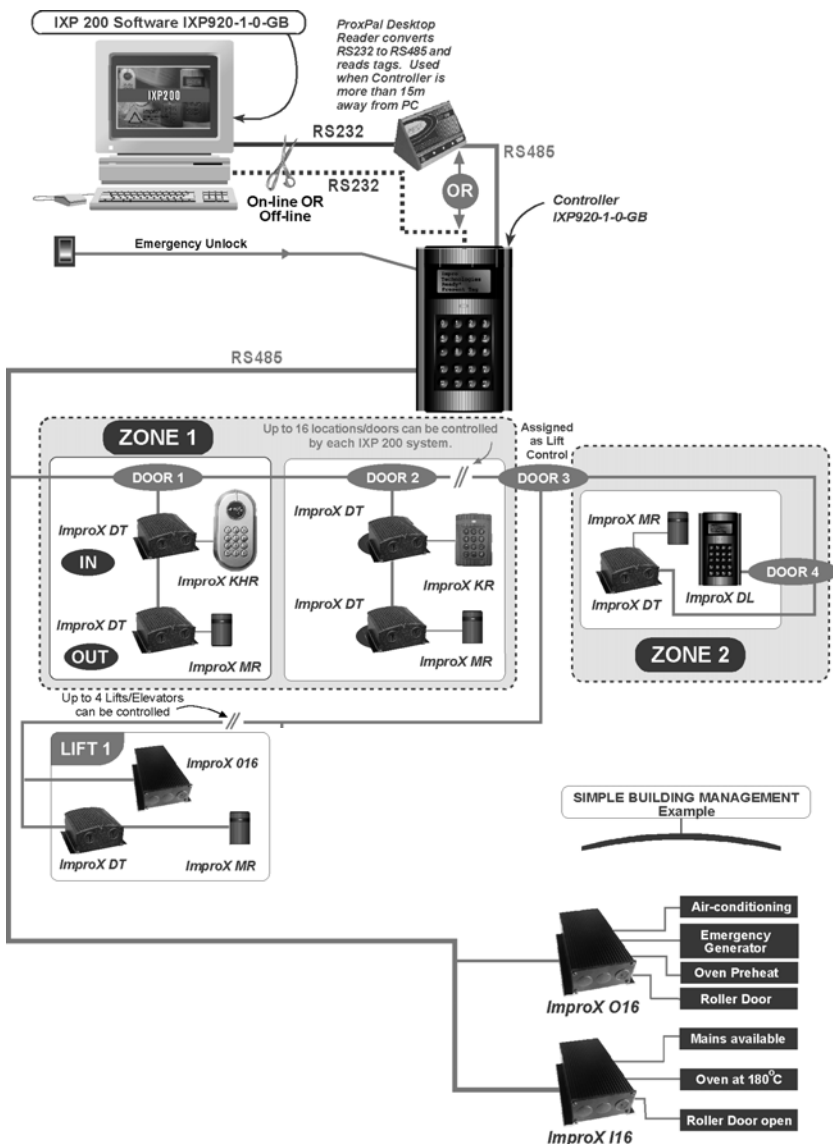



Figure 2: Block diagram of the Excel Products IXP200 System

NOTE : *A typical IXP200 System block diagram is included in Section 1 of this manual. That diagram shows some System features that are not used in the example shown in Figure 2.*

Main Application Window

The Main Application Window (see the illustration on the next page) has a menu and toolbar at the top and two panes below it. The upper pane displays an information panel for the menu item selected, and can also switch to the Graphics Runtime display panel. When an alarm transaction is received, the Graphics panel automatically switches to the front. A tool bar with buttons provides quick access to commonly used menu items.

The  button allows the user to toggle between Graphics and Configuration panels.

The lower pane displays current Transactions polled from the Controller. The centre bar dividing these panes may be moved by clicking the arrows on it, or by dragging it. The default position of the bar has been chosen so that none of the buttons or controls on the main panel is obscured.

The menu provides comprehensive access to all System configuration graphics and operating functions as well as reports and the card designer facility. Some menu items display a dialog box when selected, which must be closed before any other item can be selected.

There is a Status Bar at the bottom of the window to display messages to the user and two Status LED Indicators which display the current status of the Database Connection and Communication to the Units.

If an Auto-ID has been done in the current session, a third LED indicator is displayed on the Status Bar. This is an Auto-ID Indicator button; clicking on the button displays a logfile of the last Auto-ID process.

Auto ID, Database Connection and Communication Status Icons

Three LED Icons indicate the status of these parameters. When the System is not functioning correctly these Icons change color, indicating that a problem exists. The Icons are located at the bottom right hand corner of the Main Application Window.

See next page

Auto ID Status

Green	All Terminals were found and configured.
Amber	New Terminals were found but are not configured.
Red	Some Terminals are configured but were not found.

Database Connection Icon

Green	The System is connected to the Database.
Red	A loss of connection to database (e.g. network fault).

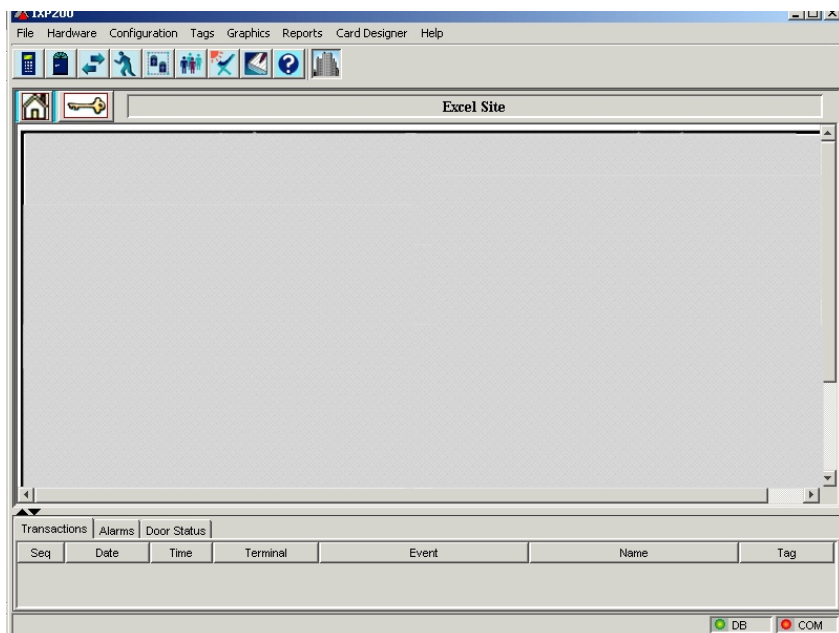
Communication Status

Green	Communication with the Controller is normal.
Amber	Terminal timeout (not responding) can be transient.
Red	Controller not responding.

Active Transaction Panel

The bottom pane of the Main Application Window (similar to that shown on the next page) is the Active Transaction Panel. This pane displays real time data. For example, as an employee or visitor presents a Tag, the access transaction data is then displayed in the various fields of the Active Transaction Panel.

See next page



Main Application Window

Active Transaction Panel Fields and Buttons

A brief description of the information that is displayed in the Active Transaction Panel's fields and the functions of the buttons is provided below.

Up/Down arrow icons	:	Used to open or close the pane. The mouse can be used to drag the pane to the appropriate size.
Seq	:	Displays the Transaction number as recorded by the Controller.
Date	:	Displays the date of the Transaction.
Time	:	Displays the entry/exit time of the Tagholder.
Terminal	:	Displays the identity of the door or Terminal where the transaction occurred.
Event	:	Displays the type of Event that was recorded.
Name	:	Displays the Tagholder's name.
Tag	:	Displays the Tagholder's Tag number.

Alarm Panel Fields and Buttons

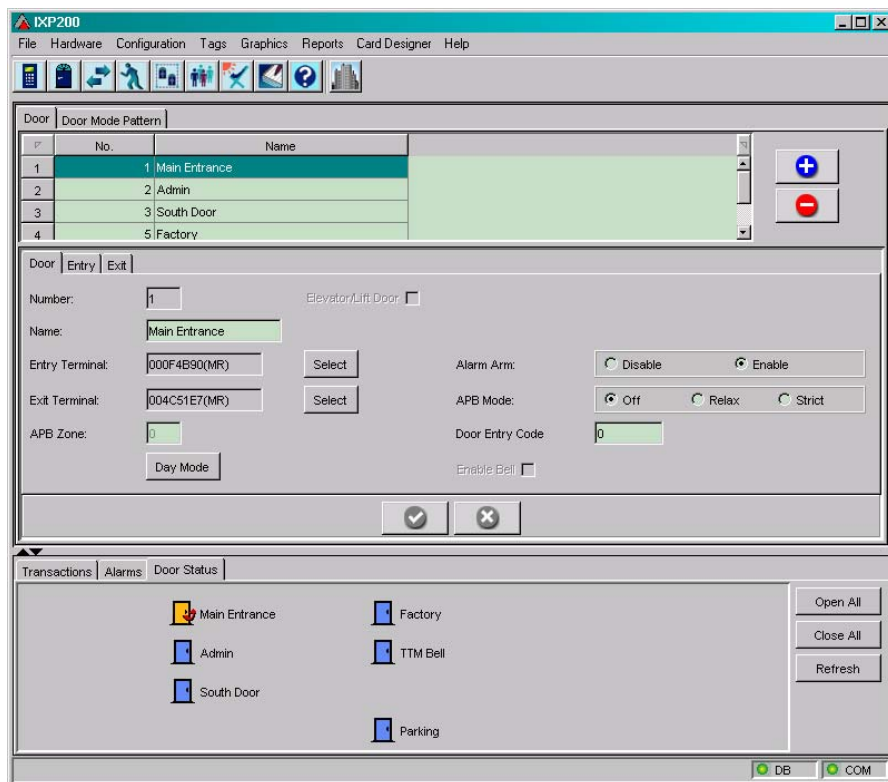
A brief description of the information that is displayed in the Alarm Panel's fields and the functions of the buttons is provided below.

Status	:	Indicates the current status of a displayed alarm (Acknowledged or Unacknowledged).
Seq	:	The transaction number as recorded by the Controller.
Date	:	The Date the alarm condition occurred.
Time	:	The Time that the alarm condition occurred.
Terminal	:	The Terminal at which the alarm condition occurred.
Event	:	The type of Event which caused the alarm to be triggered.
Operator	:	The Operator who acknowledged the alarm.
Tagholder	:	Tagholder number associated with the alarm, e.g. in the case of access made under duress.
Acknowledge All	:	This pushbutton acknowledges all currently displayed alarms.
Acknowledge	:	This pushbutton acknowledges the currently highlighted alarm.

See next page

Door Status Panel

This panel may be accessed by clicking the **Door Status** tab in the **Transaction View** panel in the lower part of the screen.



Door Status Panel

NOTE : *The proper functioning of this panel requires that door open sensors are installed on each door.*

This panel shows an icon for each door in the System. A label next to the icon indicates the name of the door. The current state of the door is reflected by the icon displayed. The state of the door can only be fully ascertained if a door open sensor has been installed on the door.

NOTE : *This panel will initially be blank for a new System after the doors have been configured. Click the Refresh button to display the door icons.*

There are four possible states or conditions, namely:

DOOR STATE	COMMENTS
Closed and locked	Normal condition while no access is made.
Closed and unlocked	During Open mode or Emergency Open mode.
Open	Normal condition during access, as detected by a door open sensor.
Open for longer than the specified limit	Abnormal condition, door remains continually open, as detected by a door open sensor.

The door state is obtained by polling the Controller at a specified polling frequency.

The icon state is refreshed when the Controller is polled and will remain fixed until the next poll.

The user may specify the **Polling Frequency** and the **Door Open Time Limit**. This **Door Open Time Limit** should not be confused with the **Door Open Duration** specified on the Reader Panel. The Door Open Duration can be set for an **individual** door and will generate an alarm if the door is left open longer than the duration specified.

The Door Open Time Limit for this panel is a parameter for the Door Status panel only and applies equally to all doors. If a door is left open longer than the time limit, the icon changes to a flashing image. No alarm transaction is generated.

Polling frequency : 5 seconds (Default). Minimum 1 second.

Monitored door open time limit : 300 seconds (Default).

Set these parameters from the Controller Panel using the Configuration/System Menu (see paragraphs under **Setting the Door Status Polling Parameters**).

Additional Functions

Several other functions are accessible from this panel.

Three buttons are provided :

BUTTON	FUNCTION
Open All	: Activates Emergency Mode at all doors, i.e. doors are unlocked.
Close All	: De-activates Emergency Mode at all doors, i.e. doors are locked, unless an Open mode is operating on the door

BUTTON	FUNCTION
Refresh	locked, unless an Open mode is operating on the door according to the current Door Mode Pattern assigned to it. : Detects new doors added or deleted and polls and displays current status.

Individual doors can be locked or unlocked by clicking on the appropriate door icon. A popup menu allows selection of the appropriate action. When an action is selected, the command is sent to the Controller and it is immediately polled for its new status. The door icons are refreshed according to the status.

The Graphics Panel still provides functions to open/close doors as before. The status of the door will be reflected in the Door Status Panel but may not be refreshed immediately. It will be refreshed when the Controller is next polled, in accordance with its polling frequency.

Door Unlocked – door colour : Yellow

Door Closed – door colour : Blue

Door Open – door colour : Green



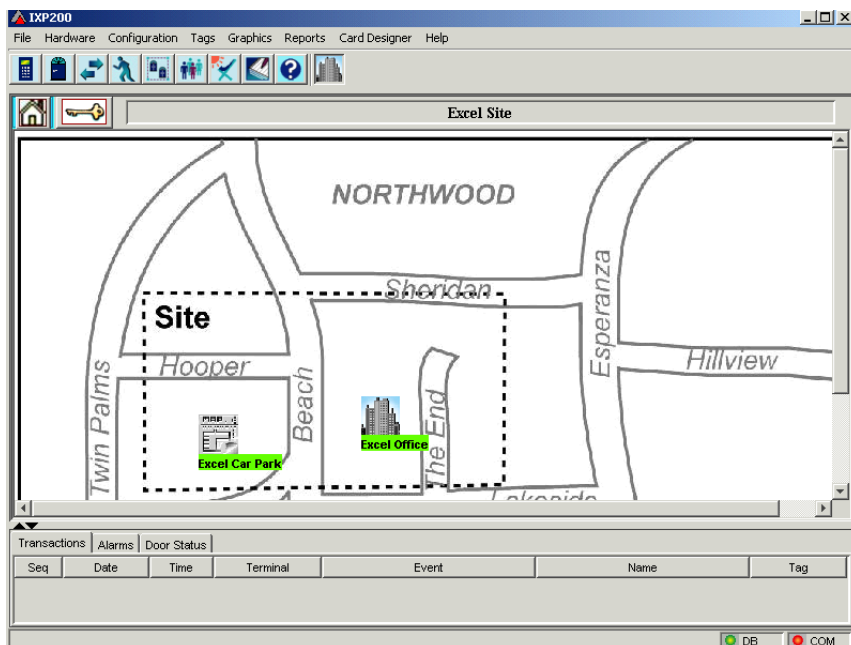
Door Status Icons

(See also the information under **Setting the Door Status Polling Parameters**).


See next page


Building Graphics Software

If the System uses the Building Graphics facility, a screen similar to that shown below will appear as the Main Application Window.



Main application window with Building Graphics

Use the  (Home) Icon to return to the Base Plan.

Use the  (Key) Icon to display the Base Plan in a small window at the left of the current panel, with an indicator pointing to the location of the current plan on the Base Plan.

The Graphics Software comprises two components, namely the Designer Module and the Runtime Module.

The Designer Module allows the user to develop various plans, and is described in the Impro Graphics Designer Module manual.

The Runtime Module allows the Graphics software to display plans derived using the Graphics Designer Software Module, and to permit the monitoring and control various System parameters by means of icons superimposed on the plans.

A software utility which permits the use of Graphics developed using the Graphics Designer Software Module (described in the Graphics User Manual IXP331-0-0-GB-XX) is incorporated into the IXP200 software.

Graphics features

The principal Graphics Runtime software features are :

- (a) Display of Base Plans and Floor Plans of the areas under access control.
- (b) Display, on these plans, of alarms generated within the System.
- (c) The ability to acknowledge alarms from the Plans.

The use of the Graphics Runtime Software is described in Section 3, Chapter 8 of this manual.

Addressing of Units

The ImproX units each have two types of addresses, namely :

A Fixed Address

This is a unique, unchanging address, which is allocated at the factory and stored in the memory of the unit during manufacture. This number appears on the printed label attached to the unit.

A Logical Address

This is assigned to a unit during the Auto-Identification (Auto-ID) process and is then used by the Host PC to address the Controller and the Terminals.

The first step in configuring a System is to establish the Logical Addresses and link these to the Fixed Addresses. This process is described in the following Auto-ID sub-section of this manual.

Recording of Installation Information

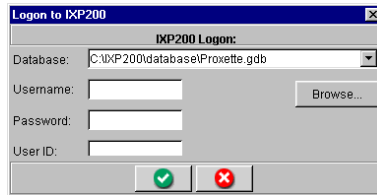
When ImproX units are physically installed, the Fixed Address associated with each unit must be recorded by the installation personnel. This is done using a label supplied with the unit, and an ImproX Unit Location Chart (provided with every ImproX IXP200 Controller). This label must be attached to the Chart, and a unique description of the unit's physical location must also be recorded on the Chart. Where applicable, record the unit as an Entry or Exit Reader.

If this procedure is followed it makes the Configuration of the units in software a simple matter by providing a record of all the information required.

IXP200 Software Start-up

Start the IXP200 software either from the IXP200 icon on the desktop or from the Programs menu / IXP200 folder.

On software start-up, the user is presented with a Log-on dialog to log-on to the database (see “IXP200 Log-on Window” on the next page).



IXP200 Log-on Dialog

Before logging on, first check the database location. The default pathname for the database is C:\IXP200\Database\Proxette.fdb. If this is not the correct location, click the Browse button and locate the Proxette.fdb database.

Enter the UserName 'SYSDBA' and the Password 'masterkey' and press Enter or click OK. This is the default administrator password and may be changed at a later stage after Configuration is complete.

The ID field in the Log-on dialog is for use by designated Operators (see **Adding Another User** in the Software Installation section (Section 2) of this manual). This field allows an Operator access to the database for Operator-designated functions.

Once the Administrator has logged on to the database, the System will attempt to open the serial port for communication with the ImproX IXP200 Controller. The first time that an attempt is made to log on to the System, the Controller I.D. will not yet be stored in the database. The user will therefore be asked if Auto-Identification (Auto-ID) is required.

New System – Logging on for the First Time

After logging on to a System for the first time, the dialog shown below will be displayed.



Auto-ID Request Dialog

- [1] Click on Yes to execute the Auto-ID.
- [2] Answer Yes to proceed immediately or No to display the Main Application Window.
- [3] Auto-ID can then be selected from the Hardware Menu.
- [4] If the serial port fails to open when the Main Application Window is displayed, select Configuration / System from the menu in that window, and then choose the correct serial port.

Auto Identification Unit Detection

The purpose of this process is to detect hardware units in the IXP200 System, to identify the type of each unit and to assign a Logical Address to each unit. This information is then stored in the database.

NOTE : *No configuration of the hardware can be done unless it is physically connected to the PC via the serial port. Data cannot be entered until the hardware units have been identified and assigned addresses using the Auto-ID function.*

Once assigned, the Logical Address is not changed during the next Auto-ID but preserved as recorded in the database. Auto-ID may therefore be repeated as often as required (e.g. when a new unit is added to the System) without corrupting the existing database.

Performing Auto-ID

- [1] Select Hardware / Auto-ID Units and wait until the cursor returns to a normal cursor. This may take a considerable time, increasing with the number of units in the System.
- [2] When the process is complete, a button will appear in the Status Bar, next to the Status LED indicators. The colour of the icon on the button indicates the result of the Auto-ID. (See paragraph **AutoID, Database Connection and Communication Status Icons** for details).

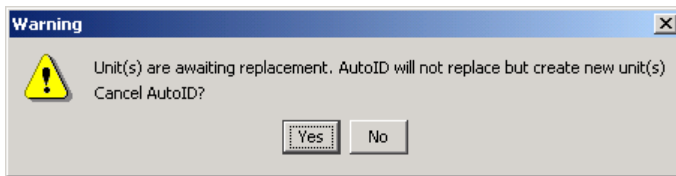
- [3] Click this button to display a log of the Auto-ID process. The first time Auto-ID is done, new units should have been found as indicated by an amber icon. These units have now been assigned logical addresses and are available as Terminals to assign to doors and for Building Management and lifts (elevators).

If Auto-ID fails it can be repeated until it succeeds. It may require more attempts if there are many units in the System.

If new units are added later, Auto-ID must be executed again to detect them and to assign Logical Addresses to them.

CAUTION : If a unit needs to be replaced or removed altogether, refer to the Section *Hardware: Replace Unit* for the correct procedure. This is most important to preserve data associated with the faulty unit.

NOTE : If a unit (or units) have been removed and are awaiting replacement, the following warning dialog will be displayed.



“Unit Awaiting Replacement” Warning

You can now proceed to Configuration of the System as detailed below.

SYSTEM STARTUP

At startup, the software automatically locates the System database. It then allows a user to log-on with a Log-on Name and Password. The target database URL (Universal Resource Locator) is read from the Proxette.properties file.

SYSTEM CONFIGURATION PROCEDURE

This section describes the Configuration of the System.

NOTE : *The terminology used in this Section assumes a working knowledge of Windows conventions on the part of the Reader.*

IXP200 System Configuration Requirements

The IXP200 Access Control System must be configured in the following order before the System can be used : Controller, Doors, Readers, Door Mode Patterns, I/O Terminals, Time/Event Triggered Actions, Access Groups, Tagholders and Tags.

In this section, the data to be captured for configuration of the System is presented. Diagrams of actual Graphical User Interface (GUI) screens and panels are presented, showing the type of data to be captured for each one. The GUI for this System is called the IXP200.

The configuration sequence is :

- [1] Configure the Controller.
- [2] Assign all unassigned Terminals to Doors, set up Door Mode Patterns as required and assign these to Doors and Zones.
- [3] Configure the Input/Output Terminals (optional).
- [4] Configure the Time/Event Actions (optional).
- [5] Configure Access Groups.
- [6] Configure Tagholders and Tags.
- [7] Configure Holidays.
- [8] Define Messages (optional).

Steps [1] to [6] must be completed for each new installation.

USER'S NOTES

USER'S NOTES

CHAPTER 2 - CONTROLLER CONFIGURATION

GENERAL

The Controller has three Serial Ports, two Digital Outputs (relay contacts) and four Digital Inputs.

Port 1 - RS485

This Port is the Terminal Bus using the RS485 Protocol. All the IXP200 Terminals, Readers and Digital Input/Output Terminals are connected to this Bus for communication with the Controller.

Port 2 - RS232/RS485

This Port is the PC Bus using the RS232 or RS485 Protocol (selectable manually in Controller Editing Facility – see Section 6 of this manual).

This bus connects the Controller directly to the PC when this is located close to the Controller. If the Controller is more than 25 m away from the PC then either an RS232/RS485 Converter (the ImproX ProxPal) or a USB/RS485 Converter (the ImproX RS Registration Interface) is required, and this port must be set to RS485 using the Controller manual editing functions.

Port 3 - RS232

This port could be used for a serial printer (for example) **but is not used in this version of the software.**

Digital Outputs

The Alarm Output is available when Relay 1 on the Controller is suitably connected (for these connections refer to the IXP200 System Installation Manual). This output can be connected, for example, to a siren that is triggered by alarms.

Power Control/Alarm Arming Modes

An IXP200 System can be used in either of two principal modes, namely the Power Control or Alarm Arming Mode. The IXP200 Controller must be hard-wired to suit the desired mode. The Mode selected depends on the connections to Relay 2 on the Controller (for these connections refer to the IXP200 System Installation Manual).

Power Control

If the System is operating in the **Power Control Mode**, then :

When the first person enters any APB (Anti-Passback) Zone Relay 2 on the IXP200 Controller switches on immediately.

The doors in the Zones must have APB selected, as the System maintains a count of the number of persons in each zone.

After the last person leaves an APB Zone and all zones are empty, the relay switches off after 30 seconds.

This arrangement means that Relay 2 in the Controller can be used to control the state of electrical equipment in the Zones to conserve power when no Tagholder is present.

Relay 1 is activated for a 1 second pulse when a Door Forced or Door Open Too Long event occurs at a door.

Alarm Arming/Disarming

The Alarm System can be armed or disarmed at a Reader which has Alarm Arming enabled. This is done by :

- [1] Presenting a valid Administrator/Supervisor Tag at the Reader.
- [2] Pressing the # key; the Tagholder has 10 seconds to press the # key to arm the Alarm System.

NOTE : *It is not necessary to press this key to disarm the System.*

Once the # key has been pressed to Arm the System, the IXP200 Readers will beep every second for 30 seconds before arming to allow users to exit the building.

When the System is Armed the door Reader's Status LED blinks Red.

Only valid Administrator/Supervisor Tags can disarm the System when entering the building. This is done automatically when the Tag is presented at a Reader on entering.


Digital Inputs

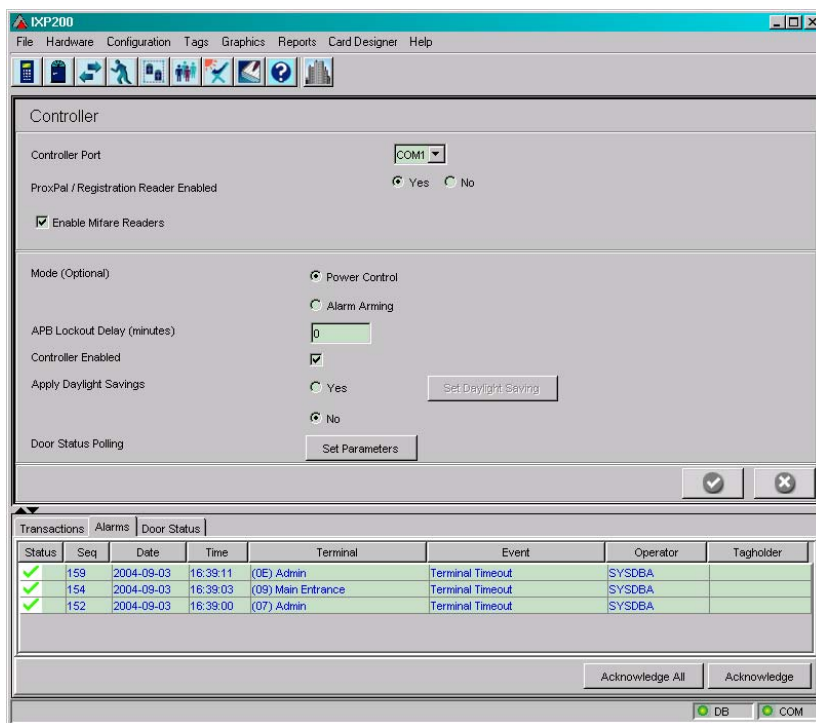
- | | |
|-----------|---|
| * Input 1 | This input indicates on the Controller LCD that the Alarm Panel is Ready. |
| * Input 2 | This input indicates on the Controller LCD that the Alarm Panel is Armed. |

- * Input 3 This input can be used as a General Alarm.
- * Input 4 This input indicates on the Controller LCD that the System is in the Emergency Unlock Mode.

NOTE : *The Controller is not approved for use as a burglar alarm.*

Controller Configuration

The first item to be configured is the Controller. To access the Controller Panel, click on the  Icon.



Controller Panel

This panel is used to configure the Controller. The "proxette.properties" file stores the settings for the serial port to be used for communication with the Controller. If the Controller is not detected on that serial port, use this panel to select an alternative port. Additional Controller functions can be set here as well as follows :

Mode :

- Power Control.
- Alarm Arming.

NOTE : *This selection must match the hardwiring of the IXP200 Controller Relay 2.*

APB Lockout Delay

This is the delay (in minutes) after a Tag has exited an APB Zone, before it will be allowed to enter the Zone again.

Mifare Readers

Ideally, for a System using Mifare Readers, Auto-ID should not be done until the Mifare Readers have been enabled during System Configuration (see **Controller Configuration**). Enabling the Mifare Readers disables ImproX PT or TA Terminals (which cannot read Mifare Tags) in the System, allowing up to 32 Mifare Readers to be assigned.

The Mifare Readers connect into the System through either ImproX PT or TA Terminals.

Controller Fields and Buttons

Below is a brief description of the information that is displayed in the Controller Panel's fields and the functions of the buttons :

Controller Port	:	The PC port to connect to the Controller or to a ProxPal Reader or ImproX USB "Registration Reader" (*NOTE 1).
ProxPal/Registration Reader Enabled	:	Yes must be selected here if an ImproX ProxPal Desktop Tag Reader or ImproX USB "Registration Reader" is installed. No must be selected if neither of these is installed (*NOTE 1).
Enable Mifare Readers	:	When selected, this enables Mifare Readers in the System.
Mode (Optional)	:	This selects Power Control or Alarm Arming Mode for Relay 2, if used.
APB Lockout Delay (minutes)	:	Restricts the same Tag from entering at the same point within a set period.
Site Communication Seed (0=no encryption)	:	As encryption is not implemented in this version, a zero (0) must be entered in this

	field.
Controller Enabled	: Toggles the Controller on or off; if off, the Controller is not polled by the PC.
Apply Daylight Savings	: This option, together with the Set Daylight Saving button, allows the Controller to implement daylight saving when off-line to the PC.
Apply	: This button saves new data to the System database and to the "Proxette.properties" file.
Cancel	: This button cancels the field selection and any newly typed-in data.

NOTE 1* : Refer to information under **Communications (Controller to Host PC)** in Section 2 of this manual for details of these connections.

Configuring the Controller - Procedure

To configure the Controller, proceed as follows :

- [1] Click the General System Setup icon on the toolbar or select from the Configuration dropdown menu. A Controller Panel similar to that shown previously will be displayed.
- [2] In the Controller Port field, select the required serial port (COM1 or COM2) to connect the PC to the Controller, either directly or through the ProxPal unit or ImproX RS.
- [3] In the ProxPal/Registration Reader Enabled field, select "Yes" to enable the ProxPal Desktop Tag Reader/ ImproX USB "Registration Reader" (if either of these units is installed in your System). These units are dedicated to Tag registration.
- [4] Enable or Disable Mifare Readers as required.
- [5] In the Mode field, select the Power Control or Alarm Arming Mode in accordance with the Controller wiring for your System.

NOTE : *Before selecting one of the radio buttons, the required option must be hard-wired (to Relay 2) before this function can be enabled. Details of this wiring are included in the IXP200 System Installation Manual.*

- [6] In the APB Lockout Delay field, select the cell and type in the amount of delay time required. This function prevents the same Tag from gaining access more than once at the same point of entry for that set period of time (e.g. 30 minutes). If no Lockout Delay is required, enter a zero (0).
- [7] The Site Communication Seed field is **not available** in this software version, but will be implemented at a later stage. At present a zero (0) must be entered in this field.

- [8] In the **Controller Enabled** field, the tick in this check box just verifies that the Auto-ID has detected the Controller. An unchecked box indicates that the Controller is not functioning correctly.
- [9] Click **Yes** or **No** for **Daylight Saving**.
- [10] Clicking **Yes**, enables the **Daylight Saving** button; click this and set the **Time Offset**, **Start Date** and **Time** and **End Date** and **Time** in the dialog displayed. Click **Apply** to save.
- [11] Click **Apply** to accept the new data into the System, or **Cancel** to reject any new data.

NOTE : *Changing to another panel before selecting Apply on the Controller Panel would result in the new data being rejected.*

Daylight Saving

The Daylight Saving feature allows the Controller to be set up for Daylight Saving (summer time).

Once it is set up it will operate the time switch-over even when the Controller is off-line, that is it will reset the time by the offset on the specified start date and time and switch it back again on the specified end date and time.

However, the PC time will still override the Controller time when it is on-line. The PC relies on the operating System (O/S) for the correct time and will upload it to the Controller every 5 minutes. The O/S generally knows the dates for which Daylight Saving applies, and switches over automatically. Of course if the Operating System time is incorrect, then it will make the Controller time incorrect too, as soon as it comes on-line.

NOTE : *Daylight Saving dates are set for a particular year and **must** be reset each year.*

To activate Daylight Saving, select **Apply Daylight Savings, Yes** on the Controller configuration screen.

The **Daylight Saving** dialog shown will be displayed.



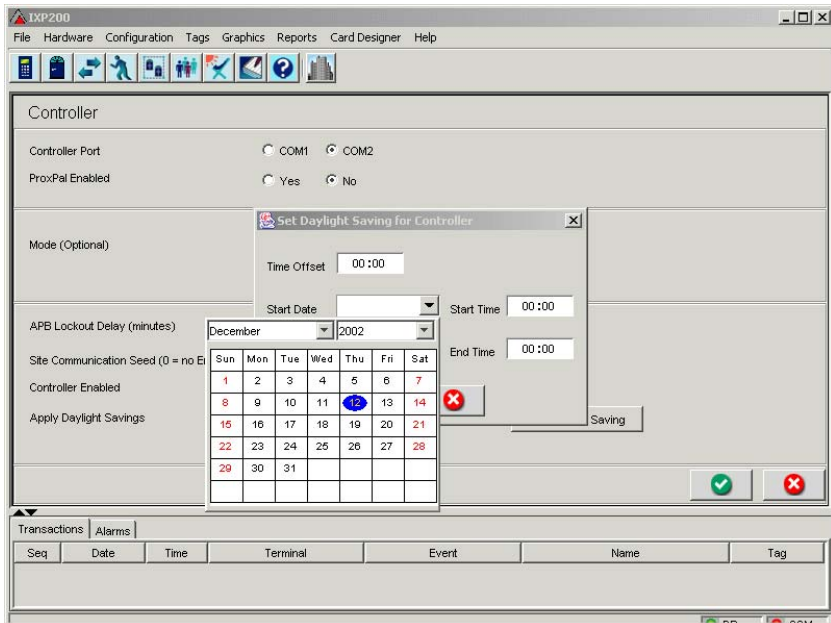
Daylight Saving dialog

To set the **Time Offset**, enter the hours and minutes in the Time Offset box.

To set the **Start Date**, select the Start Date drop-down menu from the Daylight Saving dialog, and choose the required date. Click on the chosen date to accept the setting.

To set the **Start Time**, type the required time into the Start Time box.

Set the **End Date** and **End Time** in a similar way.



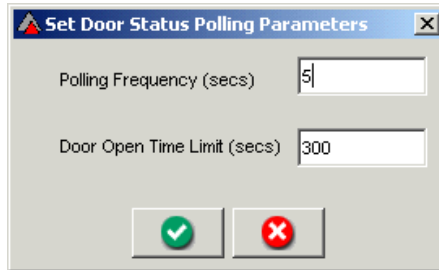
Daylight Saving – typical calendar

NOTE : To quit the calendar window without choosing a date press the escape button on the keyboard.

The start and expiry date can be deleted by highlighting the date and pressing the **Delete** button on the keyboard.

Setting the Door Status Polling Parameters

- Click the **Set Parameters** button, opposite the Door Status Polling label, to display the **Door Status Polling Parameters** dialog.



Door Status Polling Parameters dialog

- [2] Set the **Polling Frequency** in seconds. This determines how often the Controller will be polled and the panel display refreshed.
- [3] Set the **Door Open Time Limit** in seconds. This determines the period a door may remain open before the display icon should change to a flashing icon. This provides a visual alert to the operator.

Polling Frequency : 5 seconds (Default) (Minimum 1 second).

Monitored Door Open Time Limit : 300 seconds (Default).

THIS CONCLUDES THE CONFIGURATION OF THE CONTROLLER.

CHAPTER 3 – DOOR CONFIGURATION

GENERAL


The configuration of Doors involves the Configuration of :

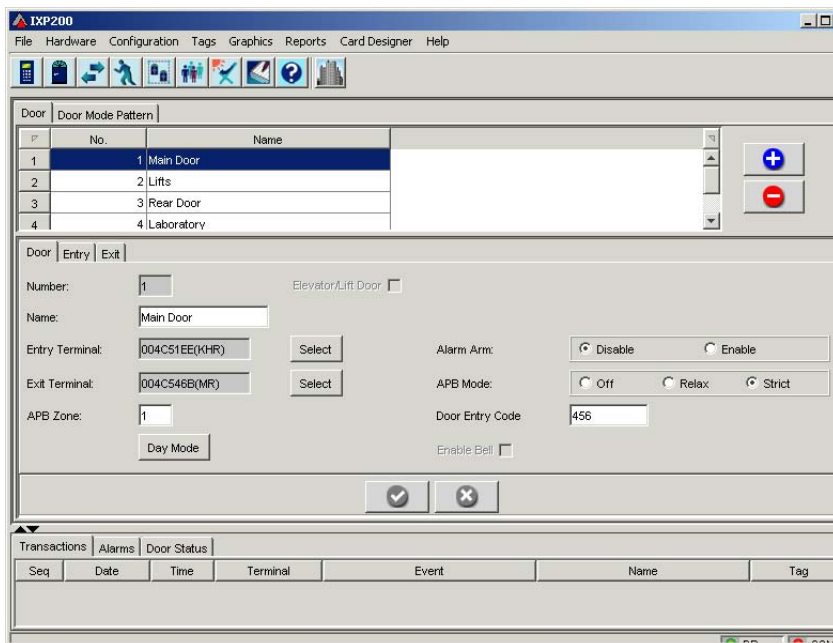
- (a) Readers.
- (b) Door Mode Patterns.
- (c) Day Modes.

Lift (elevator) Control is an optional aspect of Door Configuration.

DOORS, READERS AND DOOR MODE PATTERNS CONFIGURATION

The next item to be configured is the Doors. The purpose of this configuration is to define each Door and to assign Terminals to the Doors that they must control.

To access the **Door Panel**, click on the  Icon. (The Door Panel shown next includes previously configured Doors).



IXP200

File Hardware Configuration Tags Graphics Reports Card Designer Help

Door Door Mode Pattern

P	No.	Name
1	1	Main Door
2	2	Lifts
3	3	Rear Door
4	4	Laboratory

Door Entry Exit

Number: Elevator/Lift Door ☐

Name:

Entry Terminal: Alarm Arm: ☒ Disable ☐ Enable

Exit Terminal: APB Mode: ☐ Off ☐ Relax ☒ Strict

APB Zone: Door Entry Code:

Enable Bell ☐

Transactions Alarms Door Status

Seq	Date	Time	Terminal	Event	Name	Tag
-----	------	------	----------	-------	------	-----

Door and Readers Panel

Doors and Readers Panel Fields and Buttons

Below is a brief description of all the fields associated with the Door and Reader Panel, the information displayed in the fields and what the buttons' functions are :

Door Tab Panel – Top Pane

- No.** : Door number.
- Name** : The name given to the door.
- NOTE** : *This name must be taken from the Unit Location Chart.*
- Add** : Allows a new door to be configured.
- Delete** : This button removes the selected entry from the list.

Door Tab Panel – Middle Pane

- Number** : The new door number or that of the selected door in the top pane.
- Lift (elevator) Door** : When ticked (checked), defines this door as a lift (elevator)/lift (elevator) group.
- Name** : The name of the selected door in the top pane.
- Entry Terminal** : Entry Reader Terminal Fixed Address.
- Exit Terminal** : Exit Reader Terminal Fixed Address.
- Select** : Displays the Reader Setting Dialog.
- APB (Anti-Pass Back) Zone** : The Zone number for this APB door (0 means no APB).
- Day Mode** : Displays Day Mode Setting Dialog.
- Alarm Arm** : Enabled if door must be armed.
- APB Mode** : Off, Relaxed or Strict.
- Door Entry Code** : The Code required for access at this Door during Door Entry Code mode.
- Enable Bell** : The Door Configuration Panel now shows a check box to enable a bell. The bell is only available if the door is assigned a Reader which is a Twin Antenna Mullion Reader. This Reader has a bell pushbutton.
Tick (check) the check box to enable the bell to operate with relay 2. **Relay 1 will then operate with the door strike for both Readers.** If the box is not checked, then the relays operate as normal.
- Apply** : This button accepts the new door or edited data into the System.

Cancel : This button refreshes the data with the original data.

Configuring Doors and Readers Procedures

To configure Doors and Readers, first refer to the ImproX Unit Location Chart for the required data, and then proceed as follows :

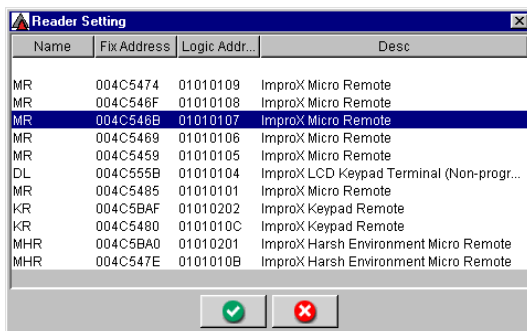
- [1] Click the Doors/Readers icon on the toolbar or select from the Configuration dropdown menu. The Doors and Readers Panel similar to that shown above is displayed. For a new site the list is empty.
- [2] This panel defaults to the **Door Tab Panel**, as shown above.
- [3] Click **Add (+)** in the top pane. The System allocates a number and the new entry area is highlighted under the **No.** and **Name** fields.
- [4] In the middle pane select the **Name** field, and type in the required description. The description should be appropriate and unique, ensure that the description is not confused with other descriptions.

NOTE : *The first thing to decide is whether the door is an actual Door or a Lift (elevator) Control point. If the latter, click the check box to select Lift (elevator) Door. Four Readers, one per lift (elevator), may then be assigned to the lift (elevator) control point, loosely referred to as a 'Lift (elevator) Door'.*

For normal Doors only two Readers (one for entry, one for exit) may be assigned.

- [5] The next step depends on whether a normal Door or a Lift Door is being configured :
 - (a) For normal Doors continue with this procedure (Step 6).
 - (b) For a Lift (elevator) Door continue with the procedures under **Lift (elevator) Control**.
- [6] In the **Entry Terminal** field, click **Select** in the middle pane. A **Reader Setting Dialog** similar to that shown below is displayed. Consult the Location Chart and then select the required Reader from the list. When accepted, this data is then displayed in the **Entry Terminal** field.
- [7] In the **Reader Setting Dialog**, click **Apply** to accept the Readers, or **Cancel** to reject the Reader.

NOTE : *To de-select a Reader click on the Blank line.*



Reader Setting Dialog

Reader Setting Dialog

- Name** : The type of hardware unit.
- Fixed Address** : The Fixed Address of the unit.
- Logical Address** : The assigned Logical Address of the unit.
- Description** : Describes the type of hardware i.e. ImproX Micro Remote.
- Apply** : This button accepts the Terminal selected from the list.
- Cancel** : This button cancels the selection and closes this panel.

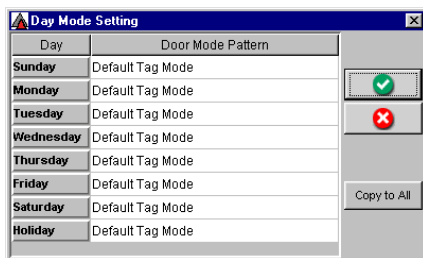
- [8] In the **Exit Terminal** field, click **Select** in the middle pane. A **Readers Setting Dialog** similar to that shown above will be displayed. Consult the Location Chart and then select the required Reader from the list. When accepted this data is then displayed in the **Exit Terminal** field.
- [9] In the **Reader Setting Dialog**, click **Apply** to accept the Reader, or **Cancel** to reject the Reader.
- [10] Enter a zone number only if the door is an APB door, otherwise leave this setting as zero.
- [11] In the **APB Zone** field, click in the cell and enter the zone number (between 1 and 16) that the selected door must be in. (If doors are grouped into a Zone, they must have the same Zone number).
- [12] In the **Alarm Arm** field, select this function. Click **Enable** to allow this door to enter the Alarm Arming mode when the System is armed. (This only applies if the Controller Mode is Alarm Arm). Click **Disable** if arming is not required.

- [13] In the **APB Mode** field, select this mode. If the user selects Relaxed or Strict and has not entered this door into a zone, when clicking **Apply** the user is then prompted to enter a Zone Number.
- [14] Door Entry Code mode. Enter a **Door Entry Code** for this Door if Door Entry Code Mode is to be used for the Door (this requires a keypad Terminal to be fitted at that Door). The valid range for a Door Entry Code is 1 – 65535.

Click **Apply** to accept the new data into the System, or **Cancel** to reject new data.

NOTES:

1. *Changing to another panel before clicking on the Door Mode Panel's **Apply** button, would result in the new entry being rejected.*
2. *The Door Mode Pattern for this door can be displayed by clicking **Day Mode**. The **Day Mode Setting Dialog** is shown below. (see the Day Mode Setting sub-section later in this document).*



Day Mode Setting Dialog

Entry and Exit Tabs

To configure Entry and Exit Readers, proceed as follows :

- [1] Select the required Door.
- [2] Click on the **Entry** tab. An Entry/Exit Panel similar to that shown on the next page will be displayed.
- [3] Enter all the required information for the Entry Reader.
- [4] Click on the **Exit** tab to define the operation of the Exit Reader.

See next page

Door | Door Mode Pattern

P	No.	Name
1	1	Main Door
2	2	Lifts
3	3	Rear Door
4	4	Laboratory

Door | Entry | Exit

Number: Elevator/Lift Door ☐

Name:

Entry Terminal:

Exit Terminal:

APB Zone:

Alarm Arm: ☒ Disable ☐ Enable

APB Mode: ☐ Off ☐ Relax ☒ Strict

Door Entry Code:

Transactions | Alarms

Seq	Date	Time	Terminal	Event	Name	Tag
17	2003-06-13	15:39:01	003 Main Door	Denied Unknown Tag In		XXXXXX

Door Tab Panels

See next page

Door Entry Panel

Reader Function: ☒ Access Control ☐ Time & Attendance

DOS Mode: ☐ Normally Open ☒ Normally Closed

RTE Mode: ☒ Normally Open ☐ Normally Closed

DOS Usage: Normal Strike Duration:(0.1s) 40

☐ Enable Offline Validation Open Duration:(s) 0

Message Display Terminal:

on Invalid Tag

LED Action: Flashing Red Duration: 20 (0.1s)

Buzzer Volume: Loud Duration: 20 (0.1s)

on Valid Tag

LED Action: Green Duration: 20 (0.1s)

Buzzer Volume: Loud Duration: 20 (0.1s)

Seq	Date	Time	Terminal	Event	Name	Tag
1	2006-07-04	12:57:06	(00)	Power Up		
0	2006-07-04	12:57:03	(00)	Tables Initialised		

Upload error: Terminals, Door Mode Patterns,

Door Entry Panel

Entry and Exit Tabs – Middle Panel

NOTE: *The layout of the Door Exit Tab is the same as the Door Entry Tab.*

Reader Function : Select **Time and Attendance** if transactions from this Reader must be exported for time and attendance purposes. The default setting is **Access Control Only**.

DOS (Door Open Sensing) Mode : The DOS Mode allows the selection of either Normally Open or Normally Closed contact; the choice depends on the type of sensing switches that are used. Details must be obtained from the Installer. A non- zero Open duration must be set to enable DOS.

RTE Mode	:	The RTE Mode allows the selection of either Normally Open or Normally Closed “Request to Enter/Exit” switch contacts; the choice depends on the type of sensing switches that are used. Details must be obtained from the Installer.
DOS Usage	:	Determines how DOS is used - Normal, Terminate Strike and Inhibit (see below).
Normal	:	Valid Tag presentation triggers the relay for the full strike duration.
Terminate Strike	:	Valid Tag presentation triggers the relay until the door is opened. The relay remains activated until the door closes, when it is de-activated or the strike duration expires.
Inhibit	:	Valid Tag presentation is denied unless the DOS contact is in the specified mode.
Strike Duration	:	The period of time the relay must be active on presentation of a valid Tag.
Open Duration	:	The period of time the door is allowed to remain open before an Event occurs. A non-zero value enables DOS.
Enable Offline Validation	:	This box is only enabled for the ImproX MFT Terminal. When checked, if the comms from the Controller fails, the MFT will continue to process Tags that have previously been successfully presented to that Terminal, giving those Tagholders access via the door concerned. The box is greyed-out for other Terminals.
Message Display (optional)	:	Terminal where message must be redirected, for Tag presented at this Terminal. This option is here to facilitate future System expansion. If this is a Terminal with an LCD display, select it to display messages locally.
On Valid/Invalid Tag		Select the LED and Buzzer Action that must occur on presentation of a valid Tag (or invalid Tag).
LED Action	:	The state of the LED when a Tag is presented.
Buzzer Volume	:	The buzzer volume when a Tag is presented.
Duration	:	The period of time the LED and Buzzer Volume are active during Tag presentation. Enter the

period of time (minimum 2 digits; e.g. 20 = 2 seconds) that the Action must be active.

Click **Apply** to accept the new data into the System, or **Cancel** to reject new data.

NOTE : *Changing to another panel before clicking on the Door Panel's Apply button, would result in the new entry being rejected.*

DELETING AN EXISTING DOOR

This operation must be done with the System on-line.

To Delete a Door, proceed as follows :

- [1] Click on the Door icon on the toolbar or select from the Configuration dropdown menu.
- [2] In the top pane, select the required name to be deleted in the Name field, and then click Delete to remove data from System.

See next page

NEXT – LIFT (ELEVATOR) CONTROL

LIFT (ELEVATOR) CONTROL

Any Door position may be allocated to the control of lifts (elevators). In the panel below, Door 2 has been allocated.

NOTE : *Only one of the sixteen System Doors may be configured for lifts (elevators).*

The screenshot shows the IXP200 software interface. The 'Door' tab is selected, displaying a table of doors:

No.	Name
5	Parking
6	kHR Door
7	Lifts

Below the table, the configuration for Door 7 is shown:

- Number: 7
- Name: Lifts
- Reader1: 004C51E4(KR) [Select]
- Reader2: 004C51E3(MR) [Select]
- APB Zone: 3
- Door Entry Code: 0
- Elevator/Lift Door: ☒
- Day Mode: [Button]

At the bottom, there are buttons for a checkmark and an X. The Transactions and Alarms tabs are also visible at the bottom.

Door Tab Panel when configured for Lift (elevator) Control

Door Tab Panel – Middle Pane

- Number** : The Door number.
- Lift (elevator) Door** : When ticked (checked), defines this Door as a Lift (elevator) Control Point.
- Name** : The name of the Door, selected in the top pane.
- Reader 1 - 4** : Lift (elevator) Reader Terminal Fixed Address.
- Select** : Displays the Reader Setting Dialog.

APB Zone	:	The APB zone number must be 0.
Door Entry Code		The code required for access by this Reader during Door Entry Code Mode.
Apply	:	This button accepts the new entry into the System.
Cancel		This button refreshes the data with the original data.

Configuring Lift (elevator) Readers - Procedure

To configure a Lift (elevator) Reader, proceed as follows :

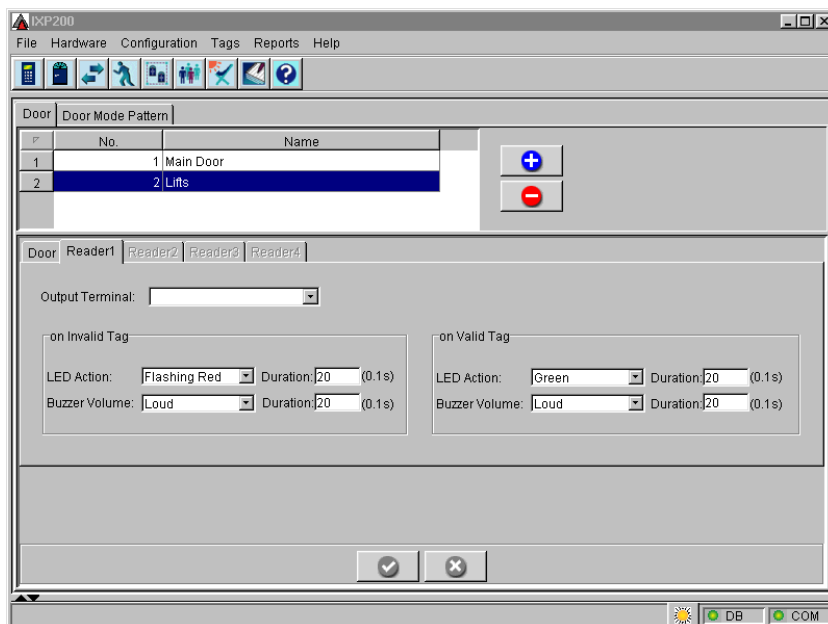
- [1] Add the Door allocated for Lift (elevator) Control.
- [2] In the Lift (elevator) Door field, click on the check box. A tick (check) will appear in the box and the Door Tab's Entry and Exit Tabs will change to Reader1 to Reader4 Tabs.

NOTE : *APB Mode is assumed to be **Off** for a lift (elevator) door (control point) as only one Reader is used per lift (elevator) (remember that APB Mode always requires two Readers at the access point concerned). The APB Zone must therefore also be 0.*

For each Reader to be configured, proceed as described below. This procedure is for Reader1; Reader2 - 4 configuration is similar.

- [1] Click **Select** (in the middle pane) associated with Reader1. A **Reader Setting Dialog** will be displayed as it was for the Door configuration.
- [2] Select the required Reader (as per the Unit Location Chart), located in the Lift (elevator).

See next page



Reader1 Tab Panel

- [3] Click Ok to accept the Reader1 data into the System, or Cancel to reject the data.
- [4] Click on the Reader1 tab. A Reader1 Panel similar to that shown below will be displayed.

Reader1 – 4 Tabs

Output Terminal : The Name and Logical Address of the Output Terminal associated with this Reader Terminal.

ON VALID/ INVALID TAG

- LED Action** : The state of the LED when a Tag is presented.
- Buzzer Volume** : The buzzer volume when a Tag is presented.
- Duration** : The period of time the LED and Buzzer Volume are active during Tag presentation.

Reader1 – 4 Configuration Procedure

- [1] In the Output Terminal field, it is necessary to link the Reader to an Output Terminal that can activate the lift (elevator) buttons.
- [2] Select the Terminal shown on the Unit Location Chart from the Output Terminal dropdown menu.

NOTE : *This menu will be blank until the output Terminals have themselves been configured. So on the first pass, leave this field blank, and save the Reader data by pressing Apply. Come back to this point and select the Output Terminal after it has been configured.*

- [3] After configuring Inputs and Outputs (see **INPUT/OUTPUT TERMINALS**), select this Terminal on the second pass
- [4] In the On Invalid Tag window. Select the LED and Buzzer Action that must occur on presentation of an invalid Tag and then click in the Duration fields to enter period of time (minimum 2 digits 20 = 2 seconds) the Action must be active.
- [5] In the On Valid Tag window. Select the LED and Buzzer Action that must occur on presentation of a valid Tag and then click in the Duration fields to enter period of time (minimum 2 digits 20 = 2 seconds) the Action must be active. Click Apply to accept the new data into the System, or click Cancel to reject new data. This is **essential**.

NOTE : *Changing to another panel before clicking on the lift (elevator) control Door Panel's Apply button, would result in the new entry being rejected.*

Day Mode Setting

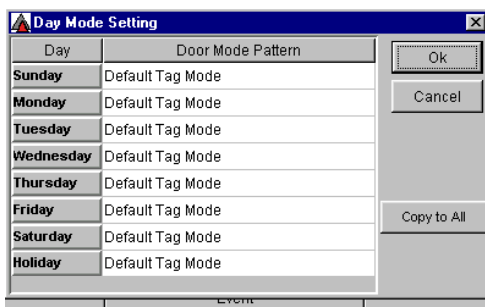
A default Door Mode Pattern is assigned for all 7 days of the week when a new door is configured.

If the user does not want to use the default pattern, new patterns may be defined using the Door Mode Pattern Tab. When any required new Door Mode Patterns have been configured (see “Configuring Door Mode Patterns – Procedure”) carry out the procedure described below.

Day Mode Configuration Procedure

To configure Day Modes, proceed as follows :

- [1] Click on the Door Tab and click the Day Mode button in the middle pane. The Day Mode Setting Dialog similar to that shown below is displayed.



Day Mode Setting Dialog

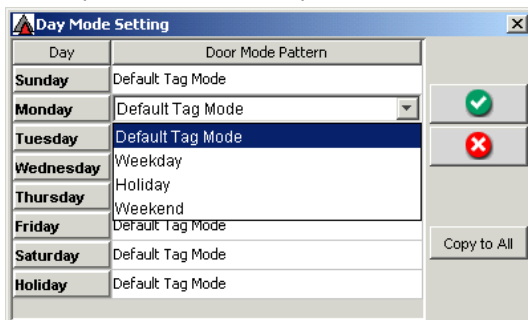
Day Mode Setting

- Day** : Days of the week, including a holiday.
- Door Mode Pattern** : Pattern associated with each day.
- Apply** : This button accepts the selected patterns for the days.
- Cancel** : This button cancels the selection and closes this panel.
- Copy to All** : This button copies the selected pattern to all the other days.

NOTE : If the same Pattern is required for each day of the week, click *Copy to All* ; this copies the pattern to all 7 days of the week.

To configure Day Mode Patterns, proceed as follows :

- [1] In the Day Mode Setting dialog, select the required day from the Day field, the Door Mode Pattern field is then highlighted, click on the highlighted area and select a pattern from the dropdown menu.



Day Mode drop-down menu

- [2] Click Ok to accept the Day Mode data into the System, or Cancel to reject data.

DOOR MODE PATTERNS

The mode of the doors does not in itself provide access to Tagholders (this is done by the Access Group), but can be used to further restrict access to Tags.

There are 26 possible composite patterns, which can be defined by the user. Each of the patterns operates for a full 24-hour period, consisting of up to 8 time slots.

For every door, one Door Mode Pattern is allocated to each day of the week plus holidays.

These patterns allow:

- (a) The operating mode (door status) for a door to be set differently for various periods in a day.
- (b) A PIN to be required at the door at selected times.
- (c) The requirement that dual Tags be presented for access.
- (d) With the above options, it is possible to further Restrict/Relax the access requirements for all Tags that use a door by using a Door Mode, even though the Tags have their own Access Group allocated.

Administrator and Supervisor Tags are not affected by the APB setting of the door.

The default Door Mode Pattern is shown below.

This pattern is always available in the System and is allocated by default when a new door is configured. If a different pattern is required, it must first be defined and then allocated.

Default Door Mode Pattern

Slot Number	:	1
Start Time Slot	:	00:00
End Time Slot	:	24:00
Door Mode	:	Tag
PIN required	:	No
Reason code required	:	No
Dual Tag required	:	No
Record Allowed Transactions	:	Yes
Alarm on Denied Transactions	:	No
LED	:	Red

Each Door Mode Pattern is made up as described below.

Door Mode Pattern Panel

Door Mode Pattern Tab

- No.** : Door mode Pattern number.
- Pattern Name** : The name given to the Door Mode pattern.
- Add (+)** : Allows a new pattern to be created.
- Delete (-)** : This button removes the selected entry from the list.
- Pattern Time Slot** : This pane provides details of each slot in the current Door Mode Pattern.

NOTES :

1. *The Start Time is allocated automatically to match the end time of the previous Time Slot (default is 00:00).*
2. *The required End Time for a new Slot must be typed in.*
3. *All other parameters are selected from combo boxes, which are available once the slot has been created.*

- No.** : Time Slot number allocated by the System [1–8 maximum].

- Start Time** : Starting time of the Time Slot in hours and minutes (hh : mm).
- End Time** : End time of the Time Slot in hours and minutes (hh : mm).
- Mode** : The Doors have 8 programmable modes. These are listed below in order of severity.
- (a) Open Now Mode.
 - (b) Open Mode.
 - (c) Door Entry Code Mode.
 - (d) Personal Access Code Mode.
 - (e) Tag Mode.
 - (f) Supervisor Unlock Mode.
 - (g) No Entry Mode.
 - (h) Locked Mode.
- (SEE THE **NOTES ON DOOR MODE OPTIONS** BOX BELOW FOR DETAILS).*
- + PIN** : Tagholder's PIN may be required with the Tag on entry or exit.
- + Reason** : Reason code may be required on entry or exit.
- + Dual Tag** : Two Tags may be required for access.
- Record** : Recording of allowed Transactions may be selected.
- Denied Alarm** : Invalid Tags can generate an alarm when presented at an armed door.
- LED** : The normal state of the Reader LED during this time slot.
- Apply** : This button accepts the new entry into the System.
- Cancel** : This button removes any new data from the fields and refreshes the original data.

See next page

NOTES ON DOOR MODE OPTIONS

THE DOOR MODE OPTIONS ARE DESCRIBED IN THESE NOTES.

There are 8 programmable Door Modes. Each of these can be modified to form other Modes by the selection of Mode options within the Door Mode Patterns. Notes on these 8 Modes are provided below.

Open Now Mode

The door unlocks immediately at the start of the time slot, and remains open until the end of the time slot. All Terminals in the same Zone as this Reader which are in Open Now Mode, will also be triggered.

Open Mode

The door remains unlocked until the start of the next Door Time Slot. This Mode is triggered by the first valid Tag presented to the Reader. All Terminals in the same Zone as this Reader which are in Open Mode will also be triggered.

Door Entry Code Mode

- This mode requires a keypad Reader at the door.
- When the door is in this Mode, the Door Entry Code for the door can be used for access.
- The Door Entry Code must be followed by the # key (Door Entry Codes can be 1 to 5 digits).
- No Tag is required, although a Tag can be used instead of the Door Entry Code as described in the Tag Mode paragraph.

NOTE : *Tag PIN, Dual Tag, Record and Denied Alarm settings are ignored for the Open, Open Now and Door Entry Code Modes.*

Personal Access Code Mode

- This mode requires a keypad Reader at the door.
- The Personal Access Code is effectively a type of Tag, and once entered, followed by a #, at the Reader, it is validated by the System as a Tag.
- Normal Tags are also valid during this mode.
- Neither Tag + PIN nor Tag + Reason apply during this mode.
- Dual Tag can be applied to this mode; the two Tags can either be two normal Tags, two PAC's or a normal Tag and a PAC.

Tag Mode

In this mode, all Tagholders with valid access are allowed when presenting a valid Tag.

Supervisor Unlock Mode

All doors can have this mode allocated to them. This ensures that normal Tagholders cannot enter until the supervisor has unlocked the door. The door then effectively reverts to Tag mode.

No Entry Mode

This Mode is similar to Locked Mode, except:

- Only Administrator Tagholders with valid access may enter.
- All Tagholders with valid access can exit.
- The RTE (exit) push button function allows any Tagholder still inside to Exit the controlled area.
- The RTE (enter) function is not operational therefore no person can gain access in this way.

WARNING

THIS LOCKED MODE CAN BE LIFE – THREATENING, IF THERE IS NO TELEPHONE IN THE AREA WHERE THE PERSON IS LOCKED IN, AS ONLY THE ADMINISTRATOR CAN OPEN THE DOOR BY CHANGING THE DOOR MODE PATTERN OF THE LOCKED DOOR VIA THE SOFTWARE.

Locked Mode

- No Tagholders, even Administrator Tagholders, can enter.
- The request to enter/exit (RTE) does not work for either Entry or Exit.
- All Tagholders still inside cannot Exit the controlled area.
- Any attempt to Enter or Exit the controlled area would result in a Transaction being recorded.

MODE OPTIONS

The Mode options which can be selected together with one of the 8 programmable Door Modes to form additional Modes are :

- +PIN Number
- +Reason
- +Dual Tag
- Record Transaction
- Denied Alarm
- LED

+ PIN Number (with Tag) Mode

- This System requires a PIN (allocated to the particular Tagholder) of up

to 5-digits to be entered, after the Tag has been presented, at applicable doors. If the PIN is less than 5 digits, # must be entered after the last digit.

- Configuring a particular door to require a PIN as well as presentation of a Tag enhances the security of the door in that area.
- If the allocated pattern of the door requires PIN entry, but the installed Reader does not have a keypad, the System would then allow access to Tagholders without requesting a PIN.
- When dual Tags are required, both Tagholders must enter their PINs.
- When a valid Tag is presented, the Tagholder's PIN entry must be completed within 20 seconds.
- A short beep can be heard from the buzzer indicating that a PIN is required.

+ Reason Mode

- In this mode, a 1- or 2- digit Reason Code must be entered via the Reader keypad after the Tag is presented at applicable doors.
- Configuring a particular door to require a Reason Code as well as presentation of a Tag provides a record of reasons for staff movements.

+ Dual Tag Mode

- Any two Tagholders with valid access must present their Tags consecutively to gain access.
- A 20 second period is allowed for the presentation of the second Tag.

Record Transaction Mode

- This initiates the recording of the Allowed Transaction i.e. Access Allowed in.
- All denied Transactions are recorded, irrespective of this setting.
- All Transactions must be downloaded on a regular basis. If the Controller buffer is full the oldest Transaction is deleted.
- A Transaction records the following data :
Date, Time, Door, Tag No., Unique Master No., Allowed or Denied code, and a user-configured Reason code (if any).

Denied Alarm Mode

- This only applies when the System is in Alarm mode and is Armed.
- The alarm relay is operated for 3 minutes, and an appropriate message is displayed on the Controller's LCD.
- A Transaction is recorded, identifying the Tagholder who was denied access. Only invalid Tags will generate an alarm.
- The Supervisor and Administrator Tagholders can acknowledge (clear) the alarm at the Controller.

LED Mode

This sets the specific color or mode that the Reader Status LED must display during this Door Mode. The User can set any type of format that is required.

SPECIAL MODES

In addition, there are 2 other special modes, Emergency Unlock and Alarm-armed. These are described below.

Emergency Unlock Mode

This mode is initiated from software, or from the Controller, and unlocks all doors. If a button connected to a Controller initiates this Action, the button must be placed in a glass-fronted box for emergency use only (see the IXP200 System Hardware Installation Manual for wiring details).

Alarm-armed

A third party Alarm System can be linked to the IXP200 so that it can be armed or disarmed at an IXP200 unit.

In addition it is possible to set doors controlled by the IXP200 System into an Armed Mode during the time that the Alarm System is armed. This Armed Mode overrides any existing Door Mode that is less restrictive than Supervisor Unlock Mode.

During Armed Mode, only valid Supervisor or Administrator level Tags may gain access to an armed door and enter the building. All other Tags are barred from access at an armed door. Furthermore the Supervisor and Administrator level Tags must also have been allocated access to the door in the usual manner via an Access Group.

A door that can be armed is one that is designated as such in the Door Configuration setup. Usually only external doors are so designated.

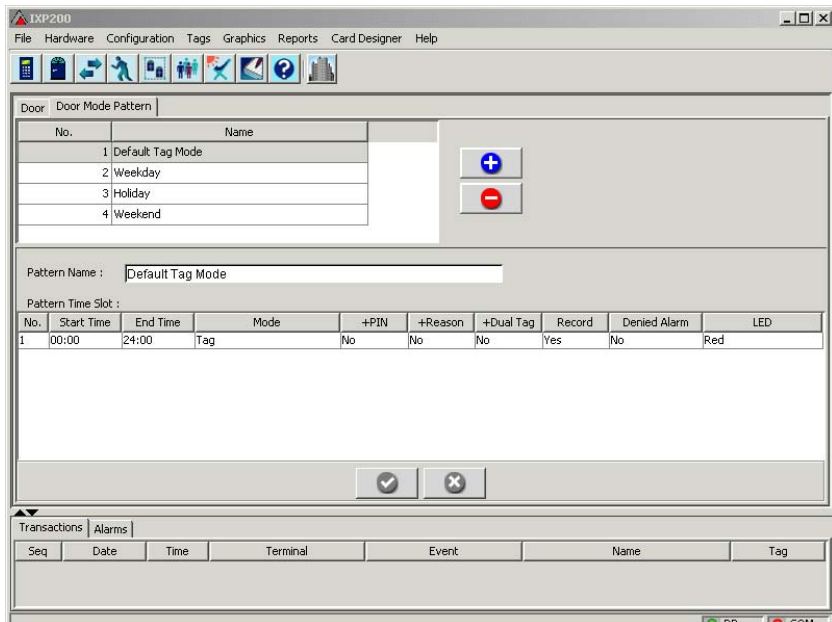
DOOR MODE COMPATIBILITY

Only certain Mode options are compatible with the various Door Modes.

The restrictions on the use of the 8 programmable Door Modes with the Mode options are shown in the table "**COMPATIBLE DOOR MODES AND OPTIONS**".

NOTE : *These restrictions are not apparent from the Door Mode Pattern setup information. For example (refer to the table), in Locked Mode, +PIN and/or +Reason and/or +Dual Tag may be specified during setup, but all of these settings will be ignored by the System as no Tag is accepted during this Mode.*

COMPATIBLE DOOR MODES AND OPTIONS				
	Mode options			
Door Mode	+PIN	+Reason	+Dual Tag	Comments
Tag Mode	Yes	Yes	Yes	
Supervisor Unlock Mode	Yes	Yes	Yes	
Locked Mode	Ignored	Ignored	Ignored	No Tag accepted
No Entry Mode	Yes	Yes	Yes	
Open Mode	Only with Tag	Only with Tag	Only with Tag	Opens on first valid Tag
Open Now Mode	Only with Tag	Only with Tag	Only with Tag	
Door Entry Code Mode	Only with Tag	Only with Tag	Only with Tag	
Personal Access Code Mode	Only with Tag	Only with Tag	Yes	System cannot be armed in PAC mode
Mode options - Comments				
+ Dual Tag	Not valid with APB Doors.			
Record	Recording of Allowed Transactions can be enabled/disabled for all Modes.			
Denied Alarm	Alarm created on denied unknown Tag presentation is only valid when : 1. Door is enabled for Alarm arming <i>and</i> 2. Controller is in Alarm Mode <i>and</i> 3. Set Alarm on Denied Transaction for Door Mode <i>and</i> 4. System is armed.			



Door Mode Pattern Panel (repeated for clarity)

Configuring Door Mode Patterns – Procedure

- [1] Click on the **Door Mode Pattern** tab. A **Door Mode Pattern Panel** similar to that shown above will be displayed. For a new site the list has only one entry, "Default Tag Mode", which cannot be edited or deleted. It is assigned by default to any new door, unless the user defines and selects a new pattern.
- [2] Click **Add (+)** in the top pane. The System allocates a new pattern number and highlights the new entry.
- [3] In the middle pane select the **Pattern Name** field, and type in the required description. The description should be appropriate and unique to ensure that it is not confused with other descriptions.
- [4] The **Start Time Field** defaults to midnight, and is therefore (00:00).
The Start Time field cannot be changed manually; it will change automatically to match the End Time of the previous Time Slot. The first field that can be changed manually is the End Time field to begin your own Door Pattern.
- [5] Click the **End Time** field, and edit the End Time settings to the pattern required.

Notes on End Time field

- (a) *This field defaults to 24:00, ensuring a full day period.*
- (b) *This field identifies the end of a particular mode for a door.*
- (c) *This time is set to a 1-minute resolution.*
- (d) *When altering the End time of a specific slot (1 of 8 possible settings), therefore:*
 - *A new next slot number is generated.*
 - *The End time of the slot is forced to be the Start time of the next.*
 - *The default parameters are loaded for the next slot (the slot being modified already has the default parameters).*

NOTE : *After every time change or selection from a combo box, press Enter to accept the entry in that cell.*

- [6] Click the **Mode** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [7] Click the **PIN** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [8] Click the **Reason** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [9] Click the **Dual Tag** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [10] Click the **Record** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [11] Click the **Denied Alarm** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [12] Click the **LED** field to select it. A dropdown menu will be displayed. Use the mouse to select the setting for the time slot.
- [13] Click **Apply** to accept the new data into the System, or **Cancel** to reject new data.

NOTE : *Changing to another screen before clicking on the Door Mode Patterns Apply button, would result in the new entry being rejected.*

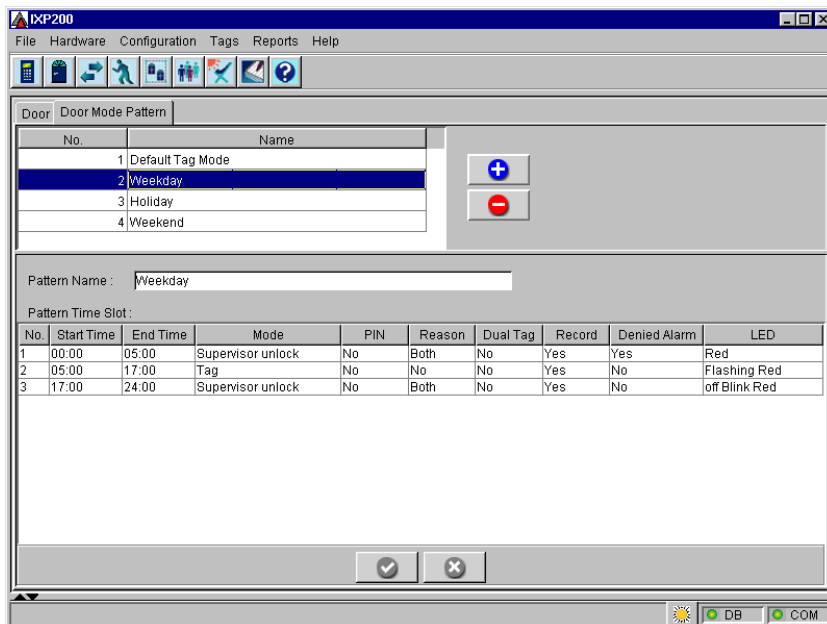
Deleting an Existing Door Mode Pattern

To Delete a Door Mode Pattern, proceed as follows :

- [1] Click on the Door icon on the toolbar or select from the **Configuration** dropdown menu.

- [2] Select the Door Pattern tab.
- [1] In the top pane, select the required name to be deleted in the Name field, and then click **Delete (-)** to remove data from System.

NOTE : *A pattern cannot be deleted while it is still allocated to any door.*



Example of Configured Door Mode Patterns Panel

After the Door Mode Patterns have been defined, they are available for setting the Day Mode of any Door (see **Day Mode Setting**).

Deleting a Time Slot

To delete a Time Slot, edit the end time of the previous slot to be the same as the end time of the slot to be deleted. It will then disappear. Click **Apply** to save.

THIS CONCLUDES THE CONFIGURATION OF THE DOORS.

CHAPTER 4 - INPUT/OUTPUT TERMINALS

GENERAL

This chapter describes the configuration of Input and Output Terminals.

The panel is used to allocate appropriate names to the Digital Input and Output Terminals and to configure these Terminals for use.

NUMBER OF TERMINALS IN A SYSTEM

A maximum of six Input/Output Terminals can be connected to this System, four to control Lifts (elevators) and two for Building Management.

BUILDING MANAGEMENT

The System can be configured as follows for Building Management :

- 1 x I16 Terminal.
- 1 x O16 Terminal.


LIFT (ELEVATOR) CONTROL

The System can be configured to use up to 4 x O16 Terminals for Lift (elevator) Control.

I/O TERMINAL CONFIGURATION - PROCEDURE

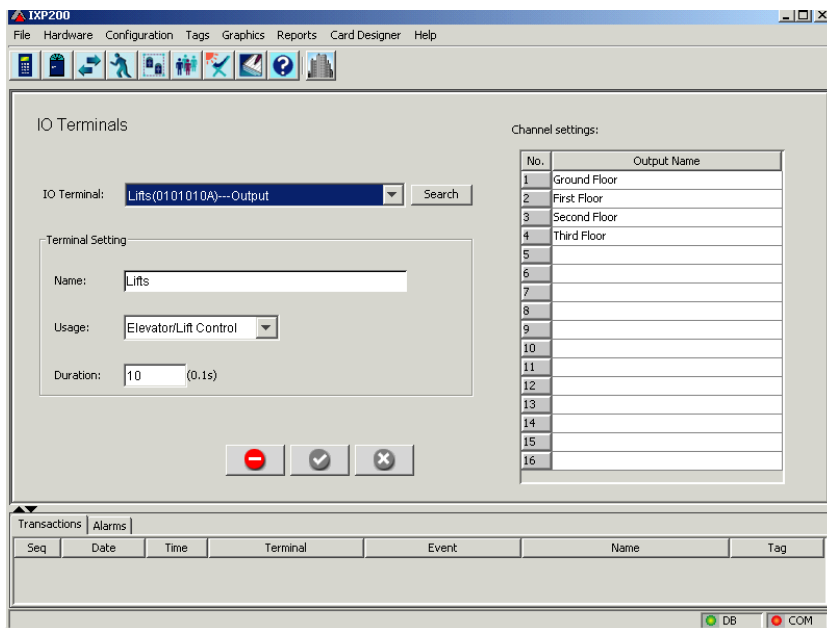
Each I16 Terminal monitors up to 16 digital input channels, and each O16 Terminal controls up to 16 relay outputs.

To configure the Input/Output Terminals, proceed as described below.

To access the Input/Output Terminals Panel, click on the  Icon.

- [1] If the System has detected any configured Input/Output Terminals the first item that is displayed when entering the menu, is the Terminal Name and its Logical Address.
- [2] Once the Terminals have been detected and named, each input/output line can then be allocated its own unique name.
- [3] Before the Terminals have been configured, the list of Terminals in the I/O Terminal dropdown box is blank.

- [4] Click Search to create a list of I/O Terminals. Referring to the ImproX Unit Location Chart for that Site, select and name each Terminal in turn.



Input / Output Terminals Panel – Lift (elevator) Control Example

Input/Output Terminals Panel Fields and Buttons

Below is a brief description of the information that is displayed in the Input/Output Panel's fields and what the buttons functions are:

IO Terminal : The Logical Address of the currently selected Input or Output Terminal. Click to show the dropdown list of the other detected Terminals.

NOTE : *Once a Terminal has been allocated a name in the Name field, this name will be displayed together with the Terminal's Logical Address in the IO Terminal field.*

Search : This button searches the Terminal Table for any Input or Output Terminal, and fills in the dropdown list of IO Terminals.

Terminal Setting

Name : The name of the Terminal.

End of Line (Input Terminal Only)	:	Enable or disable an End-of-Line resistor.
Usage (Output Terminal only)	:	Used for either Lift (elevator) Control or for Normal Output e.g. switch off lights as part of Building Management.
Duration	:	Duration for lift (elevator) button activation, in seconds.
Channel Setting	:	Named Input or Output channels.
Delete	:	Allows the I/O Device to be deleted.
Apply	:	This button accepts the new data into the System database.
Cancel	:	This button rejects this entry.

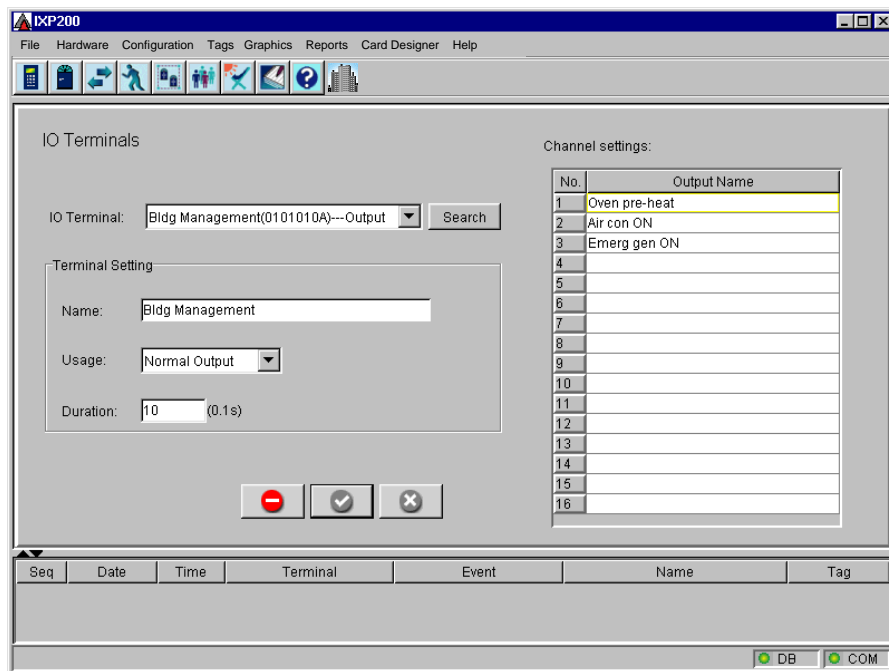
INPUT/OUTPUT TERMINAL CONFIGURATION

CONFIGURING AN OUTPUT TERMINAL - PROCEDURE

To configure an Output Terminal, proceed as follows :

- [1] Click on the **Inputs and Outputs** icon on the toolbar or select this from the **Configuration** dropdown menu. An **IO Terminal Panel** similar to that shown above is displayed. For a new site all fields are empty.
- [2] Click **Search** , the System then searches the Terminal Table in the PC for the Logical Addresses of the Input or Output Terminals, and then displays the Logical Addresses of the Terminals that were detected in the dropdown menu of the **IO Terminal** field.
- [3] In the **IO Terminal** field, click on the arrow button to display the combo box and select the Terminal to be configured. In this case, an Output Terminal is being configured.
- [4] In the **Terminal Setting** window, proceed as follows :
 - (a) Click in the **Name** field and type in an appropriate name for the Terminal (In this example, the name chosen is Lift (elevator) Control).
 - (b) In the **Usage** field, select the required option from the combo box to define the function of the Terminal.
 - (c) In the **Duration** field, select the cell and type in the period that the Tagholder has to make a selection (e.g. lift (elevator) buttons are active for 10 seconds).

See next page



Output Terminal configured for Building Management

- [1] In the **Channel Setting** window, select a cell and name the Output channels, as they have been physically connected e.g. if using the Lift (elevator) function (as in this example), enter the floor number or name of the floor (Marketing). Up to 16 Floors can be entered. (The example caters for four floors).
- [2] Click Apply to save the data or Cancel to reject it.

NOTES:

1. Where more than one Lift (elevator) Controller System is used, the lift (elevator) buttons must be connected to the output relays in exactly the same order in each lift (elevator). Each lift (elevator) can access the same 16 floors – not 4 x 16 floors.
2. The software automatically synchronises the output channels for multiple lift (elevator) Controllers.
3. Editing channels of one Output Terminal selected for Lift (elevator) Control changes the data in all the other Lift (elevator) Control units.

CONFIGURING AN INPUT TERMINAL - PROCEDURE

In the **IO Terminal** field, click on the arrow button to display the combo box, and select the Terminal to be configured. In this case, an Input Terminal is being configured.

[1] In the Terminal Setting window, proceed as follows :

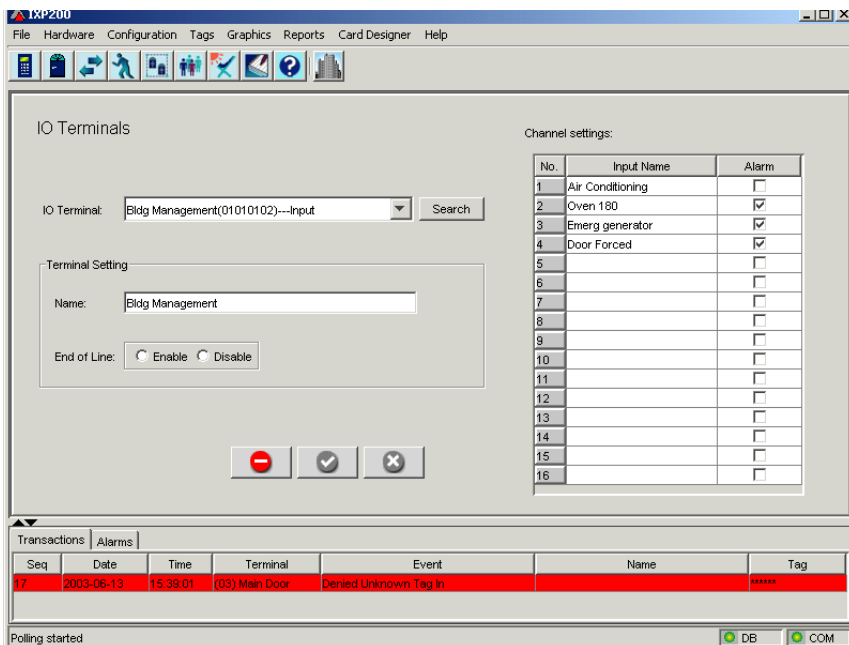
- (a) Click in the Name field and type in an appropriate name for the Terminal (In this example, the name chosen is Building Management).

NOTE : *This field is limited to 16 characters, and the name has therefore been abbreviated to "Building Manage".*

- (b) In the End of Line field, select the required radio button to enable or disable the Terminal resistor.

[2] In the **Channel Settings** window, select a cell and name each Input channel according to the function for which it has been physically connected.

[3] If required, the System will generate an alarm when the input channel condition. In this case, "Door Forced" will generate an Alarm.



Input Terminal Configuration Example

[4] Tick the box if an Input Channel must trigger an alarm when monitored for any specified state (see the Event Triggered Actions paragraph).

- [5] Leave the box unticked (unchecked) if no alarm should be triggered. The alarm setting does not inhibit Actions associated with monitored Inputs, only the triggering of Alarms.
- [6] Click Apply to accept the new data into the System, or Cancel to reject new data.

NOTE : *Changing to another panel before clicking on the I/O Terminal's Apply button, would result in the new entry being rejected. This must be done for each Terminal.*

This concludes the configuration of the Input/Output Terminals.

CHAPTER 5 – TIME/EVENT TRIGGERED ACTION CONFIGURATION

GENERAL

This chapter describes the configuration of Time and Event Triggered Actions.

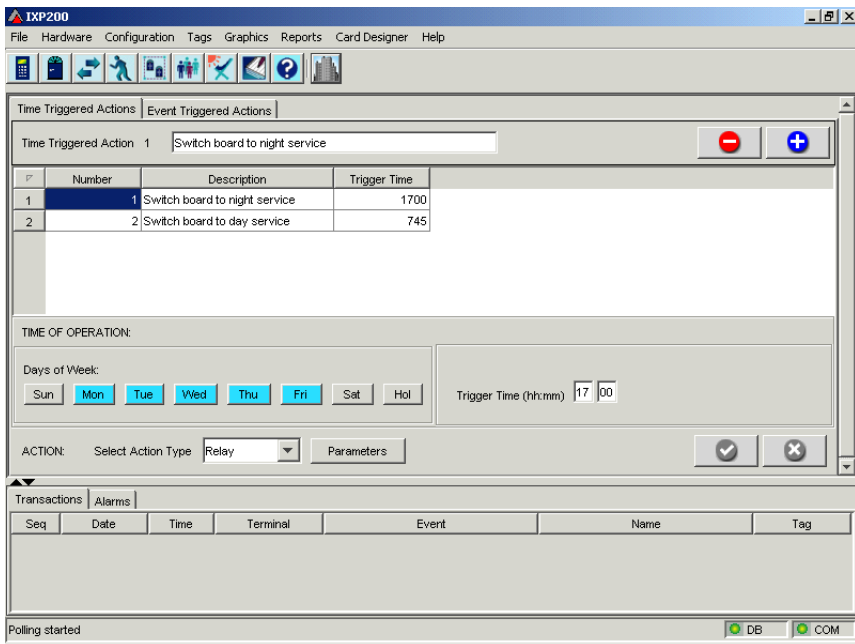
Action Types

There are two types of Actions available, namely **Relay** and **Message** :

- (a) **Relay** – Drives an Output Relay for a specified period of time or as determined by feedback from an Input.
 - Example 1 : Tea Time Siren sounds at 10 a.m. for 30 seconds.
 - Example 2 : Relay to open a roller shutter door operated at 7 a.m. for 2 minutes or until the limit switch Input indicates that the door is fully open.
- (b) **Message** - Sends a message to the IXP200 Controller's LCD. At a later stage in development the message will be able to be displayed on an electronic notice board.

NOTE : *Actions can only be configured if at least one Output unit has been detected and has been allocated to Normal use (as opposed to Lift (elevator) Control).*

See next page



Tab Panel

Time Triggered Actions

A Time Triggered Action will take place on specific days at a given time.

Event Triggered Actions

An Event Triggered Action will take place during a specified monitoring period on specific days, if a specified Input or Inputs switches to a specified state.

The I16 Terminal inputs are individually monitored to determine if an Event has occurred. Once the monitoring period has started, the System continuously polls the inputs for a change of state.

Time/Event Panel Fields and Buttons

Below is a brief description of the information that is displayed in all the Time Triggered Action Panel's fields and what the buttons' functions are.

The next item to be configured is the Time/Event Triggered Actions.

To access the Time/Event Triggered Actions Panel click on the  Icon.

Time Triggered Actions Tab

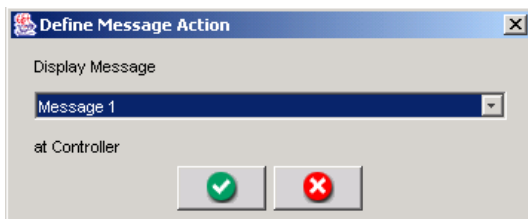
Time Triggered Action	: Description of the currently selected Action.
Delete (-)	: Allows the selected entry in the pane below to be removed.
Add (+)	: Allows a new entry to be created.
[Table or list of defined Time Triggered Actions]	
Number	: The Action number.
Description	: The Action Description.
Trigger Time	: The time at which the Action will be triggered.
Time of Operation (for the currently selected Action)	
Days of week	: (Mon, Tues etc) Days selected for the Action to be triggered.
Trigger Time (hh:mm)	: Time that an Action must be triggered, on the selected day.
Action	
Select Action Type	: The type of Action that will occur at the trigger time.
Parameters	: Displays a dialog box to further define the Action.
Apply	: Accepts the new data into the Systems database.
Cancel	: Cancels a new entry or refreshes an existing one.

CONFIGURING TIME TRIGGERED ACTIONS - PROCEDURE

To configure a Time Triggered Action, proceed as follows :

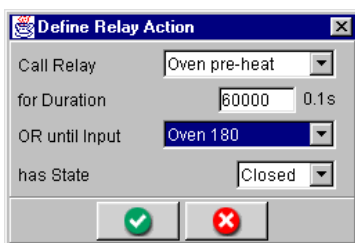
- [1] Click on the Actions icon on the toolbar or select from the Configuration dropdown menu. A Time Triggered Action Panel similar to that shown above is displayed. For a new site the list is empty.
- [2] Click **Add**; this clears the Time Triggered Action cell, click in the cell and type in the name for the new Time Action.
- [3] In the Time of Operation panel, proceed as follows :
 - (a) Click on the buttons in the Days of Week field to select the required days.

- (b) Click in the Trigger Time field cells to set the time (hh:mm) that the Action must be triggered.
- [4] In the Action field, click on the arrow button and select the required Action, namely Relay or Message.
- [5] Click Parameters. A dialog box appropriate to the Action selected will be displayed. Refer to either (a) or (b).
- (a) A **Define Message Action Dialog** similar to that shown below will be displayed. Click on the arrow icon and select the required message to be displayed from the dropdown list.

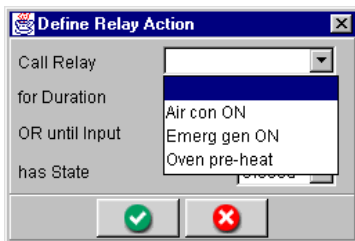


Define Message Action Dialog

A **Define Relay Action Dialog** similar to that shown below is displayed. Select the Relay to be triggered and enter the duration you want it to be active. If feedback from an Input is required, select the Input and the state, which should stop the Relay activation.



Define Relay Action Dialog – Oven Relay Selected



Define Relay Action Dialog

Relay Action Configuration

If a **Relay Action** is selected, the combo box will display all the relay outputs allocated under the related Output Terminal configuration, as shown above.

Call Relay	:	Displays the relay that must be triggered.
For Duration	:	Displays the period of time for the Relay Action.
Or until Input	:	Displays the input that supplies the feedback.
Has state	:	Stops the Relay activation when input has this state.
Apply	:	Accepts the entry.
Cancel	:	Cancels a new entry.

NOTE : *To set the relay drive time to an indefinite period, enter 65535 as the relay duration.*

- [1] Click **Apply** to accept the new Action parameters data into the System, or **Cancel** to reject data. This will close the **Action dialog** box.
- [2] In the **Time Triggered Actions Window**, click **Apply** to accept the new data into the System, or click **Cancel** to reject new data.

NOTE : *Failure to click Apply after adding a new Time Triggered Action or editing an existing one would result in the data being lost.*

Editing an Existing Time Triggered Action

To Edit a Time Triggered Action, proceed as follows :

- [1] Click on the **Action** icon on the toolbar or select from the Configuration dropdown menu.
- [2] Select the required **Time Triggered Action** from the list in the top pane.
- [3] Edit the Time and Action fields as required.
- [4] Click **Apply** to save the edited record.

Deleting a Time Triggered Action

To Delete a Time Triggered Action, proceed as follows :

- [1] Click on the **Action** icon on the toolbar or select from the Configuration dropdown menu.
- [2] In the top pane, select the required name to be deleted in the Description field, and then click Delete (-) to remove data from System.

Next – Event Triggered Actions

EVENT TRIGGERED ACTION CONFIGURATION

Event Triggered Action Tab Panel

Event Triggered Actions Tab

Event Triggered Action n : Shows currently selected Action n. Combo box navigates to the required Action record.

Name : Name of current Event Triggered Action.

Delete : Removes the currently selected entry.

New : Adds a new entry where Actions/Events can be configured.

PERIOD OF OPERATION

Days of Week – Mon, Tues, etc. : The days that an Event must be monitored.

Start Time : The time of day to start monitoring an Event.

Duration : The length of the monitoring period.

MONITORED INPUT(S) AND STATE

Select Input	:	Allows selection of an input to be monitored.
Select State	:	Allows selection of the state of the input that will trigger the Action.
Plus button	:	Chains new input with those already monitored for this Event.
Minus Button	:	Removes selected input from those monitored for this Event.
Channel No/Name/State	:	List of inputs being monitored for this Event any of which could trigger the Event
Input No.	:	Input Channel Number.
Input Name	:	Input Name.
State	:	Trigger state.

ACTION

Select Action Type	:	The type of Action that will occur when triggered by a monitored Event, namely Relay or Message.
Parameters	:	Displays a dialog box to further define the Action.
Apply	:	Accepts the new data into the Systems database.
Cancel	:	Cancels the new entry or refreshes an existing one.

EVENT TRIGGERED ACTION CONFIGURATION – PROCEDURE

To configure an Event Triggered Action, proceed as follows :

- [1] Click on the **Action** icon on the toolbar or select from the **Configuration** drop-down menu. The **Event Triggered Action Panel** similar to that shown above is displayed. For a new site the list is empty.
- [2] Click **New**; this clears the **Event Triggered Action** cell, click in the cell and type in the descriptive name for the new Event Action.
- [3] In the **Period of Operation** panel, proceed as follows :
 - (a) Click on the buttons in the **Days of Week** field to select the days when the Event must be monitored.
 - (b) Click in the **Start Time** field cells to set the time (hh:mm) to start monitoring the Event.
 - (c) Click in the **Duration** field cells (hh:mm) to set the period of time that the Event must be monitored.

[4] In the Monitored Inputs and State panel, proceed as follows :

- (a) Click on the arrow icon of the **Select Input** field, this displays a list of available inputs in the dropdown menu, select the required input.

NOTE : *More than one input can be chained and monitored for the same event, and any of the Events can trigger the Action.*

- (b) Click on the arrow icon of the **Select State** field, this displays state options in the dropdown menu, click on the required option to select the state.
- (c) Click + Icon to add the new Input selected above, to the list of monitored inputs below. Repeat this step if additional inputs must be monitored for this event.
- (d) Click the – Icon to remove any Input highlighted in the list below from the list of monitored inputs.

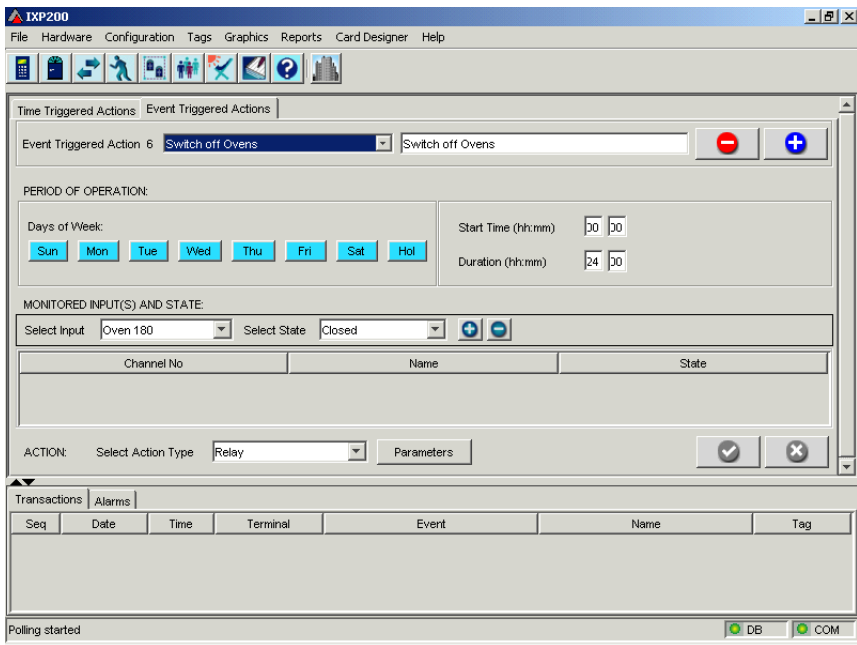
[5] In the **Action** field, click on the arrow button and select the required Action, namely **Relay** or **Message**.

[6] Click **Parameters**. A dialog box appropriate to the Action selected will be displayed (refer to Time Triggered Actions).

NOTE : *If **Relay** action is selected, the relay drive time can be set to an indefinite period by entering 65535 as the relay duration.*

[7] Click **Ok** to accept the new Action parameter data into the System, or **Cancel** to reject new data or refresh existing data. This will close the dialog box.

See next page



Sample Configured Event Triggered Action Panel

- [8] In the Event Triggered Action Window, click Apply to accept the new or edited data into the System, or Cancel to reject new data or refresh existing data.

NOTE : *Failure to click Apply after adding a new Event Triggered Action or editing an existing one would result in the data being lost.*

Editing an Existing Event Triggered Action

To Edit an Event Triggered Action, proceed as follows :

- [1] Click on the Action icon on the toolbar or select from the Configuration drop-down menu.
- [2] Choose the Event Triggered Actions tab.
- [3] Click in the Event Triggered Action combo box and select the required Event Triggered Action from the dropdown list.
- [4] Edit the days of week or time and duration as required.
- [5] Add or remove monitored inputs as required.
- [6] To change state of a monitored input, remove it first and add it again with the correct state.

- [7] Select the required Action and set its parameters.
- [8] Click Apply to save the edited record.

Deleting an Existing Event Triggered Action

To Delete an Event Triggered Action, proceed as follows :

- [1] Click on the Action icon on the toolbar or select from the **Configuration** drop-down menu.
- [2] Choose the Event Triggered Actions tab.
- [3] Click in the Event triggered Action combo and select the required Event Triggered Action from the dropdown list.
- [4] Click **Delete (-)** to remove it from System.

This concludes the configuration of the Time/Event triggered Actions.

INDEX

- + **Reason Mode**, 49
- Access**, 6, 21, 37, 46, 48, 49
- Actions, 6, 21, 61, 62, 63, 64, 65, 67, 68, 70, 71, 72
- Administrator, 18, 24, 46, 49
- Alarm, 23, 24, 25, 26, 27, 32, 34, 46, 48, 49, 55, 61
- Alarm Arming, 24, 34
- Anti-PassBack**, 32
- APB**, 24, 26, 27, 32, 34, 35, 42, 46
- Armed Mode, 49
- Auto Identification, 19
- Auto-ID, 17, 18, 19
- Buzzer**, 38, 43, 44
- buzzer volume, 38, 43
- Communication Status**, 9, 19
- COMMUNICATION STATUS, 10
- Controller, 6, 9, 10, 11, 17, 18, 21, 23, 24, 25, 26, 27, 28, 30, 34, 49, 60, 63
- CONTROLLER, 23
- Day Mode Patterns, 45
- Door Entry Code**, 32, 35, 42, 48, 49
- Door Entry Code Mode, 35
- Door Mode Pattern, 35, 44, 45, 46, 47, 54, 55
- DOS Mode, 37
- Editing, 6, 23, 60, 67, 71
- Emergency Unlock Mode**, 49
- end date, 28
- Event, 6, 11, 21, 38, 61, 63, 64, 65, 67, 68, 69, 71, 72
- EVENT, 63, 68
- Event Triggered Action, 64, 68, 69, 71, 72
- Fixed Address, 17, 32, 34, 41
- Graphics, 6, 9, 16, 17
- Graphics Designer, 16, 17
- icons, 6, 11, 12, 16
- Input, 21, 23, 24, 25, 57, 58, 59, 61, 62, 63, 64, 66, 67, 69, 70
- installation, 5, 7, 17, 21
- Invalid tags, 48
- LED Action**, 38, 43
- LED Mode**, 49
- LIFT (ELEVATOR), 41
- Locked Mode, 48, 49
- Logical Address, 17, 19, 34, 43, 57, 58

Log-on, 18, 20

menu, 9, 18, 19, 27, 29, 33, 39,
44, 45, 55, 57, 59, 65, 67, 69,
70, 71, 72

No Entry Mode, 48, 49

Output, 21, 23, 43, 44, 57, 58, 59,
60, 62, 63, 67

PAC, 49

Password, 18, 20

pathname, 18

PC, 5, 6, 17, 19, 23, 26, 27, 28, 59

PIN, 46, 48, 49, 55

Power Control, 23, 24, 26, 27

ProxPal, 23, 26, 27

Record Transaction Mode, 49

relay, 23, 24, 38, 49, 57, 67

RTE Mode, 38

serial port, 18, 19, 25, 26, 27

shortcut Icons, 6

site, 33, 54, 59, 65, 69

Special Modes, 49

start date, 28

Status Bar, 9, 19

Supervisor tag, 24

Supervisor Unlock Mode, 48, 49

system database, 20, 27, 59

Tag Mode, 48, 49, 54

time, 10, 11, 18, 19, 20, 27, 28,
29, 37, 38, 43, 44, 46, 47, 48,
49, 55, 56, 63, 64, 65, 66, 67,
68, 69, 71

Time and Attendance, 37

time slot, 49

Time Slot, 46, 47, 48, 49, 54, 56

Time Triggered Action, 64, 65, 67

Transactions, 9, 46, 48, 49

user, 5, 6, 9, 16, 18, 20, 35, 44,
46, 49, 54

Windows, 20

Zone, 24, 26, 32, 34, 35, 42, 49

USER'S NOTES

USER'S NOTES

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_System-swm-en-12 Section 3A .doc
------------------	----------	-----------	---

IXP200
Software User Manual
SECTION 3
CONFIGURATION
PART B
[Chapters 6 to 15]

SECTION 3 PART B –SYSTEM CONFIGURATION

CONTENTS

CHAPTER 6 – ACCESS GROUP CONFIGURATION	83
General	83
Access Groups Security Levels	83
Access Groups Panel Fields and Buttons.....	84
CONFIGURING AN ACCESS GROUP - PROCEDURE	85
Naming an Access Group - Procedure.....	85
Defining an Access Pattern.....	86
Access Pattern Dialog	86
Access Pattern - Day & Time Tab.....	86
Access Pattern – Door Tab	87
ACCESS PATTERN – FLOOR TAB	88
Adding More Access Patterns.....	89
Saving an Access Group	89
Editing an Existing Access Pattern.....	89
Deleting an Existing Access Pattern	89
Deleting an Access Group.....	90
CHAPTER 7 – TAG HOLDER CONFIGURATION.....	91
GENERAL	91
TAG LEVELS.....	91
Tag Level 1: - Visitor	91
Tag Level 2: - Normal	91
Tag Level 3: - Supervisor.....	91
Tag Level 4: - Administrator	92
TAGHOLDER	92
Tagholder Panel Fields and Buttons.....	93
TAG HOLDER CONFIGURATION - PROCEDURE	94
Adding a Tagholder.....	94
New Tagholder – General Tab	94
In the menu that appears in the photograph box, select Edit.....	96
Tagholder Details	97
New Tagholder – Details Tab	97
Department List.....	98
Adding a New Department	98
Editing a Department Name	98
Adding a Tagholder (Continuation) – Tag Data	99
New Tagholder – Tag Tab.....	100
Register the Tag.....	101
Registering UHF Tags	102
Registering Fingerprints as Tags.....	102

Registering Personal Access Codes (PACs) as Tags	102
Using Personal Access Codes with APB.....	103
Support for Devices using Wiegand Tag Codes	103
Tag Registration – Further Steps.....	104
New Tagholder – Operator Tab	106
Saving the Tagholder Record.....	106
Card Printing	106
Card Printing Procedure – Single Cards	106
Printing Directly onto Tags	108
Saving the Tagholder Record.....	108
Printing onto Adhesive Labels.....	108
Cards printed from some other PC.....	108
Printing Procedure – Batch Printing.....	108
Editing an Existing Tagholder	110
Deleting an Existing Tag	112
CHAPTER 8 – HOLIDAYS CONFIGURATION	113
General	113
Holiday Panel Fields and Buttons	114
Configuring Holidays - Procedure	114
New Holiday Dialog.....	115
Editing an Existing Holiday	116
Deleting an Existing Holiday	116
CHAPTER 9 – MESSAGES CONFIGURATION	117
General	117
Message Panel Fields and Buttons	117
Adding New Messages	118
Editing an Existing Message	119
Deleting an Existing Message	119
CHAPTER 10 – REASON CODES CONFIGURATION	121
General	121
Reason Codes Panel and Buttons.....	121
To Add a Reason Code.....	121
To Edit an Existing Reason Code	122
CHAPTER 11 – CARD DESIGN.....	123
INTRODUCTION.....	123
CARD DESIGNER	123
CHAPTER 12 – GRAPHICS	125
GRAPHICS SOFTWARE	125
Features	125
Using the Graphics Runtime Module.....	125
Selecting a Floor Plan	125
Alarms	126
Graphics Menu Options	127
Locate Tagholder Option	129
Display Change on Alarm Condition	130
Alarm Acknowledgement.....	130

Alarm Details.....	130
Controller Options Menu	130
Remote Reader Options Menu	132
CHAPTER 13 - OTHER SYSTEM OPERATIONS	137
General	137
Full Data Upload	137
Reset Anti-Passback (APB)	137
Emergency Open Doors	137
Emergency Open/Close Doors – Procedure	138
Replacing a Unit	138
Removing or Replacing a Terminal.....	139
Replacing a Controller.....	140
Clear Transaction Buffer.....	141
CHAPTER 14 – TRANSLATION	143
General	143
Translation – Localisation	143
Choosing a Locale for Translation	143
The Basics.....	143
Choose a Locale.....	144
Translating	145
Main Frame	146
Panels	146
Other	146
Calendar.....	146
Translate Web Reports.....	147
CHAPTER 15 – DATABASE BACKUP AND RESTORE	149
GENERAL	149
Why Backup?.....	149
File Extensions.....	149
BACKUPS	149
Scheduled Automatic Backup.....	149
Immediate Backup.....	151
CHAPTER 16 – ARCHIVE	153
GENERAL	153
CREATING AN ARCHIVE	153
INDEX	156

CHAPTER 6 – ACCESS GROUP CONFIGURATION

General

The purpose of an Access Group is to define a set of access conditions. Access is then given to Tags by allocating an Access Group to the Tag, that defines when access is allowed and the doors through that access is allowed. Tags with similar basic access requirements will be allocated the same Access Group.

An Access Group is made up of one or more Access Patterns, each specifying the days of the week and time of day during that access is allowed and also to that doors and lift (elevator) floors.

Each Tag is allowed one Access Group only (though the Group may have up to 8 Access Patterns).

The Tagholder only receives the “allowed” response when presenting his Tag if both the allocated Access Group and the current Door Mode have permission.

NOTE : *A Door Mode alone can never give access (except in the case of the Open mode), only the Access Group can define access. However a Door Mode can restrict or relax the access requirements. The Tag level can also further restrict or relax the Door Mode or access conditions.*

All groups conform to a single Anti-Pass Back (APB) lockout delay.

Access Groups Security Levels

Each Access Group that is entered into the System is allocated either High or Low security.

Tags with level 1 and 2 are restricted to Low security Access Groups. When an OPERATOR user logs on, he can only allocate Tags with level 1 and 2, and hence also only Low security Access Groups. An OPERATOR user may also not define an Access Group.

Only Tags with a Tag level of 3 (SUPERVISOR) and 4 (ADMINISTRATOR) are allocated to groups having a “High” security level setting. Therefore, “High security groups” would only be available to allocate to a Tag when the System Database Administrator (SYSDBA) user logs ON.

The next item to be configured is the Access Group. To gain entry to the Access Group panel, click on the  Icon.

Access Groups Panel Fields and Buttons

Below is a brief description of all the fields associated with the Access Groups Panel, the information displayed in the fields and what the buttons' functions are :

- Group Name** : Lists the existing Access Group names.
- Add** : Allows a new Access Group to be created.
- Delete** : Removes the selected Access Group from the list.
- Access Group** : Name of the currently selected Access Group (max 16 characters).
- Security Level** : Security Level of the currently selected Access Group.
- Access Patterns** : Lists the Access Patterns defined for the currently selected Access Group (maximum of 8 patterns per group).

The screenshot shows the IXP200 software interface. The 'Access Group' panel is active, displaying a list of groups: Admin, Lab Staff, and Supervisor. The 'Supervisor' group is selected. Below the list, the 'Access Group' field shows 'Supervisor'. The 'Security Level' is set to 'High'. The 'Access Patterns' table shows two patterns:

No.	Days	Start Time	Duration	Doors	Floors
1	Mon,Tue,Wed,Thu,Fri	00:00	24:00	4,3,2,1	Fir,Sec,Thi,Gro,
2	Sun,Sat,Hol	08:00	12:00	1,2	Fir,Sec,Thi,Gro,

At the bottom of the interface, there is a table with columns: Seq, Date, Time, Terminal, Event, Name, and Tag. The status bar at the bottom right shows 'DB' and 'COM' icons.

Configured Access Groups Panel

No.	:	Access Pattern number. The System allocates a number when a new entry is required.
Days	:	Days of the week when the Access Pattern is active.
Start Time	:	Starting time of the Access Pattern (hh:mm).
Duration	:	Duration of the Access Pattern from the Start Time.
Doors	:	Doors allowed for the Access Pattern.
Floors	:	Floors allowed for the Access Pattern.
Add	:	Allows a new Access Pattern to be created for the Access Group.
Delete	:	Removes the selected Access Pattern from the Access Group.
Apply	:	Accepts the new or edited Access Group entry into the System database.
Cancel	:	Cancels the new entry or refreshes the existing entry, only if the Apply button has not already been clicked.

CONFIGURING AN ACCESS GROUP - PROCEDURE

IMPORTANT NOTE :

There are four stages in the Access Group Configuration procedure :

Add a new Access Group name.

Add a new Access Pattern (Day and Time, Door and Floor).

Add more Access Patterns (optional).

Save the whole Group and its Patterns.

These stages are described below. Each stage must be completed to define an Access Group.

Naming an Access Group - Procedure

To name an Access Group, proceed as follows :

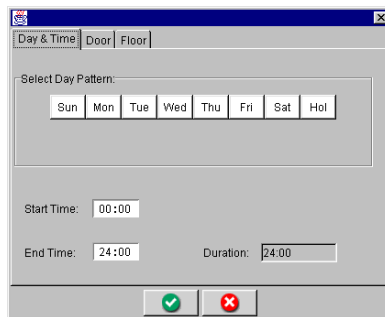
- [1] Click on the Access Groups icon on the toolbar or select from the Tags drop-down menu. The Access Groups panel similar to that shown on the previous page is displayed. For a new site the list is empty.
- [2] Click Add in the top pane. The System allocates a number and the new entry area is highlighted under Group Name.

- [3] In the middle pane select the Access Group field, and type in the required descriptive name. The name should be appropriate and unique to ensure that it is not confused with other Access Groups.
- [4] In the Security Level field use the mouse to select High or Low as required.

Defining an Access Pattern

To define a new Access Pattern, proceed as follows :

- [1] Click Add below the Access Patterns table. The Access Pattern – Day/Time Dialog similar to that shown below is displayed. This dialog defaults to its Date & Time tab.



Access Pattern - Day/Time Dialog

Access Pattern Dialog

This appears when clicking New or double-clicking on an existing Access Pattern. There are three tabs, namely: Day & Time, Door and Floor.

Access Pattern - Day & Time Tab

- Select Day Pattern** : Days of the week selected for this Access Pattern.
- Start Time** : Start time of this Access Pattern (hh : mm).
- End time** : End time of this Access Pattern (hh : mm).
- Duration** : Duration of this Access Pattern (automatically calculated).

- [2] In the Select Day Pattern field, click on the required weekday buttons to select the day pattern. The selected buttons change to light blue.
- [3] In the Start Time field, enter the time in hours (00 to 24) and minutes (00 to 59) to enable this time pattern.
- [4] In the End Time field, enter the time in hours (00 to 24) and minutes (00 to 59) to enable this time pattern.

NOTE : *The Duration field remains permanently gray. The System calculates the hours and minutes (00:00) as you enter the Start and End times.*

The dialog box titled 'Day & Time' has two tabs: 'Door' and 'Floor'. The 'Door' tab is selected. It contains a 'Select Day Pattern:' section with a row of seven buttons: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Mon', 'Tue', 'Wed', 'Thu', and 'Fri' buttons are highlighted in cyan. Below this is a 'Start Time:' field with the value '07:00'. To its right is an 'End Time:' field with the value '19:00'. Further right is a 'Duration:' field with the value '12:00'. At the bottom are two buttons: a green checkmark and a red 'X'.

Typical Access Pattern Day & Time Details

- [5] Click on the Door tab, the Access Pattern – Door Tab Dialog as shown below is displayed. In the No Access Doors field, all the doors of the building that have been entered are listed.
- [6] Select the required doors, and then click Add to transfer them to the Access Doors field.

The dialog box titled 'Access Pattern Setting' has two tabs: 'Day & Time' and 'Door'. The 'Door' tab is selected. It contains two list boxes: 'Access Doors:' on the left and 'No Access Doors:' on the right. The 'Access Doors:' list box contains the text 'Main Door', 'Rear Door', and 'Lifts'. The 'No Access Doors:' list box contains the text 'Laboratory'. Between the two list boxes are two buttons: a left-pointing arrow and a right-pointing arrow. At the bottom are two buttons: a green checkmark and a red 'X'.

Typical Access Pattern – Door Tab Dialog

Access Pattern – Door Tab

- Access Doors** : Displays the doors selected for access.
- No Access Doors** : Display the doors not selected for access.

Add : Moves the selected doors from the No Access list to the Allowed Access list.

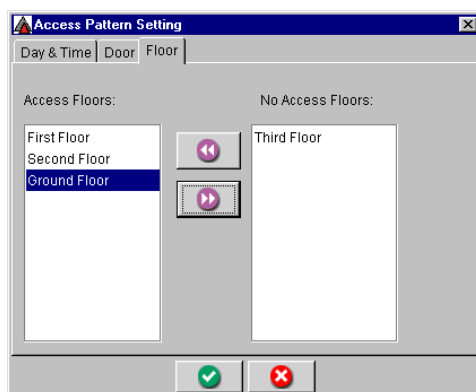
Remove : Moves the selected doors from the Allowed Access list to the No Access list.

[7] Click on the Floor tab, the Access Pattern – Floor Tab Dialog as shown below is displayed. In the No Access Floors field, all the floors of the building are listed.

[8] Select the required floors.

[9] Click Add to transfer the floors to the Access Floors field.

NOTE : *The Floor Tab is empty unless the System is using an O16 Terminal for lift (elevator) control and the Lift (elevator) Door has been selected for the Access Pattern.*



Typical Access Pattern - Floor Tab Dialog

ACCESS PATTERN – FLOOR TAB

NOTE : *If the Lift (elevator) Door has not been allocated for Door access, no floors appear in this list.*

Access Floors : Displays the floors selected for access.

No Access Floors : Displays the floors not selected for access.

Add : Moves the selected floors from the No Access list to the Allowed Access list.

Remove : Moves the selected floors from the Allowed Access list to the No Access list.

- [10] To remove a **Door/Floor** from the **Access Doors/Floors** Fields, first select the required Door or Floor, and then click Remove to transfer the selection back to the **No Access Doors/Floors** fields.
- [11] Click Ok to accept the new Access Pattern, or click **Cancel** to reject it or refresh an existing one. This returns the display to the **Access Group Panel**, where the new Access Pattern is displayed in the **Access Pattern** list.

Adding More Access Patterns

Add additional Access Patterns in the same manner, as required, up to a maximum of 8 Access Patterns per Access Group.

Saving an Access Group

Click Apply to accept the new Access Group into the System database, or on the **Cancel** to reject new data or refresh the existing Access Group data.

CAUTION

Failure to click Apply after adding a new Access Time Pattern or editing an existing one would result in the data being lost.

Editing an Existing Access Pattern

To Edit an Access Pattern, proceed as follows :

- [1] Click on the Access Groups icon on the toolbar or select from the Tags dropdown menu.
- [2] In the top pane, select the required Access Group from the list under Group Name. The Access Patterns for the selected Group now appear in the middle pane.
- [3] Using the mouse double click on required data to be edited, and then follow the appropriate procedures above.

Deleting an Existing Access Pattern

To Delete an Access Pattern, proceed as follows :

- [1] Click on the Access Groups icon on the toolbar or select from the Tags dropdown menu.
- [2] In the top pane, select the required Access Group from the list under Group Name. The Access Patterns for the selected Group now appear in the middle pane.

- [3] Select the Access Pattern to be deleted and then click Delete below the Access Pattern panel to remove it from the System.

Deleting an Access Group

To Delete an Access Group, proceed as follows :

- [1] Click on the **Access Groups** icon on the toolbar or select from the **Tags** dropdown menu.
- [2] In the top pane, select the required Access Group from the list under **Group Name**.
- [3] Click Delete in the top panel to remove it from the System. This may not be allowed if the group has been allocated to Tags because this would have the effect of deleting those Tags from the System as well. It is far better to redefine an Access Group than to delete it.

This concludes the configuration of the Access Groups.

CHAPTER 7 – TAG HOLDER CONFIGURATION

GENERAL

This chapter describes the configuration of Tags and Tagholders.

TAG LEVELS

Tags compatible with the IXP200 System are Impro Slim Tags, ImproX Read/Write Tags, ImproX Infra-red Tags and ImproX RF 4-Channel UHF Hand-held Tags, as well as Personal Access Codes (PACs).

NOTE : *A registered fingerprint can be used as a Tag if the System includes a Sagem MorphoAccess MA 200 Terminal finger print Reader, and is configured for this purpose. See “**Registering Fingerprints as Tags**” later in this Section for the procedure for the registration of a fingerprint.*

The user allocates a Level to the Tag, that can either relax or restrict access when the door is operating in certain modes. However the Tag Level cannot give access to any door, this is only done through an Access Group.

For example, if a door is in the Supervisor Unlock mode, then the Visitor and Normal level Tags would have access denied until a Supervisor level Tag has been presented at the door. This is so even if they have an Access Group that includes this door. The Tag Level works in conjunction with the Door Mode to further control access to the door. After the Supervisor level Tag has been presented, Tags that have Normal access to the door can be accepted.

Tag Level 1: - Visitor

The Visitor Tag Level has the following characteristics :

- (a) Expires at midnight.
- (b) Denied in Door Locked, No Entry, Supervisor and Armed mode.

Tag Level 2: - Normal

The Normal Tag Level has the following characteristics :

- Denied in Door Locked, No Entry, Supervisor and Armed mode.

Tag Level 3: - Supervisor

The Supervisor Tag Level has the following characteristics :

- (a) Can unlock a door in Supervisor mode.
- (b) Can acknowledge (switch off) alarms at Controller.
- (c) Has APB override (if allocated access to the door).

- (d) Can arm and disarm an associated alarm System.
- (e) Allowed in Door Armed mode (if allocated access to the door).
- (f) Denied in Door Locked and No Entry mode.


Tag Level 4: - Administrator

The Administrator Tag Level has the following characteristics :

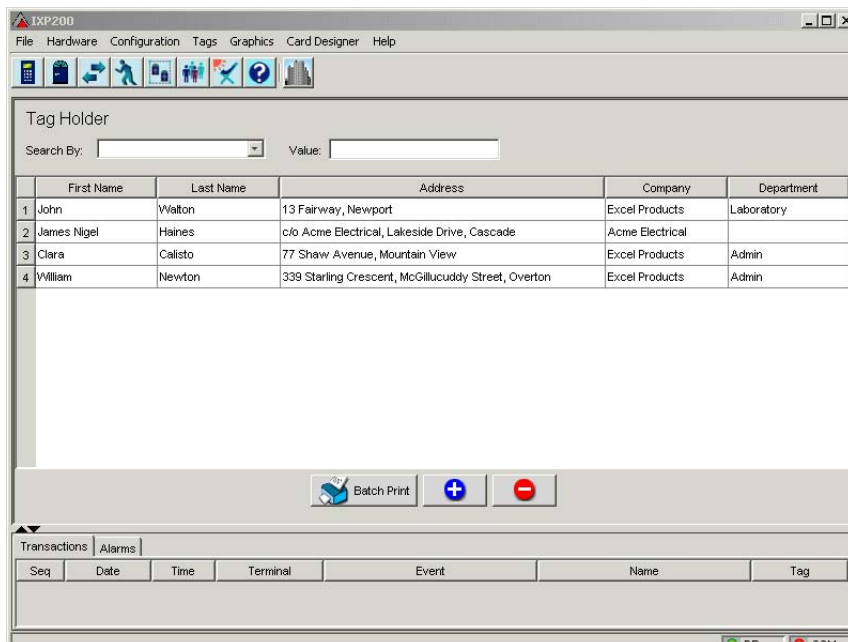
- (a) Can unlock a door in Supervisor mode.
- (b) Can acknowledge (switch off) alarms at Controller.
- (c) Has APB override (if allocated access to the door).
- (d) Can arm and disarm an associated alarm System.
- (e) Allowed in Door Armed mode (if allocated access to the door).
- (f) Has access to a door in No Entry mode (if allocated access to the door).
- (g) Denied in Door Locked mode.
- (h) Can manually edit Tag database at Controller (when supported by Firmware).

TAGHOLDER

A Tagholder is a person who was allocated a Tag to gain access to the Site. When the Tag is removed from a person, the person's Master record would remain in the PC's database to maintain the integrity of historical reports. However, the Tag would be removed from the Controller database and would not be allowed access when presented to any Reader. Up to three Tags can be allocated to the same Tagholder.

The next item to be configured is the Tagholders. To access the Tagholders Panel click on the  Icon.

See next page



Tagholder Panel

Tagholder Panel Fields and Buttons

Below is a brief description of all the fields associated with the Tagholder Panel, and the information displayed in the fields and what the button's functions are:

Search By : Allows searching by: first or last names, address, company and Tag.

Value : The name or address etc. being searched for.

[Tagholder List]

First Name : Tagholder first name is displayed in this field.

Last Name : Tagholder last name is displayed in this field.

Address : Address of Tagholder.

Company : Tagholder's company name.

Department : Tagholder's department name.

Add : Allows creation of a new Tagholder.

Delete : Removes a Tagholder from the System (not recommended).

Batch Print : Prints a batch of cards or labels.

TAG HOLDER CONFIGURATION - PROCEDURE

To configure Tagholder data, proceed as follows :

- [1] Click on the Tagholders icon on the toolbar or select from the Tags dropdown menu. A Tagholder Panel similar to that shown previously is displayed. For a new site the list is empty.
- [2] The panel displays data of all the Tagholders entered into the System database.

Adding a Tagholder

To add a new Tagholder, proceed as follows :

- [1] Click Add. The New Tagholder – General Tab panel similar to that shown below is displayed. This panel defaults to the General Tab.

New Tagholder – General Tab

New Tagholder – General Tab

- | | | |
|-------------------|---|--|
| First Name | : | Tagholder's first name (Optional). |
| Last Name | : | Tagholder's last name. |
| PIN | : | PIN code number (max 5 digits, Optional). |
| Company | : | Tagholder's company name (Optional). |
| Note | : | Comments about Tagholder (Optional). |
| Box above | : | Displays a photograph of the Tagholder (Optional). |

Camera Icon

Camera Icon : Browses folders to locate photographs.

Print Card : Print Card.

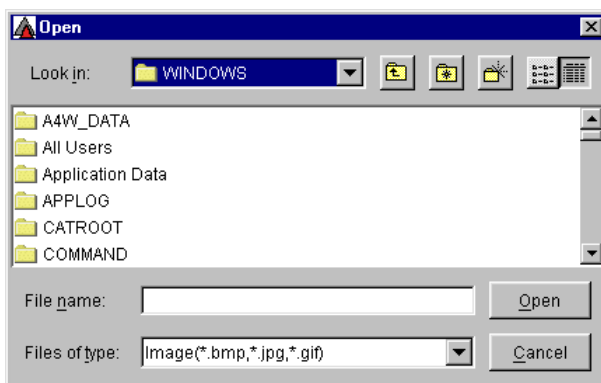
Apply : Save data and exit.

Cancel : Exit without saving changes.

- [2] Complete as many of the fields under the General tab as are required. The minimum information required for the System to accept the data is the Last Name Field.

NOTE : *If your company has photographs of its personnel, proceed as follows.*

- [1] Click on the **Camera** icon. A menu will be displayed over the photograph box.
- [2] Select the **Load from File** option from this menu.
- [3] A **File Open Dialog** similar to that shown below is displayed, and then locate the photograph folder. Select the required photo and click **Open**. The photo is then displayed in the box above the **Camera** icon.



File Open Dialog

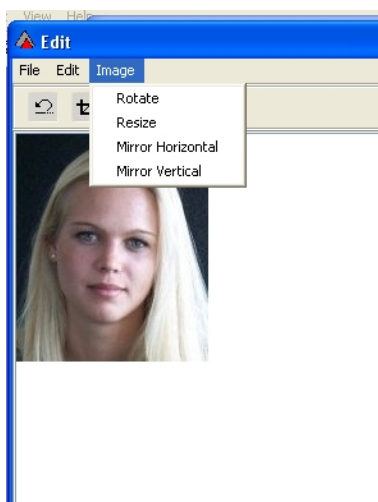
- [4] Photographs can be scaled and rotated. To do this, click on the picture or the **Camera** icon once a photograph has been imported into the Tagholder's screen.



Tagholder's photo edit options menu

In the menu that appears in the photograph box, select **Edit**.

A dialog will be displayed, with menu choices as shown in the next illustration.



Edit dialog

In the Edit dialog main menu bar:

The **File** option permits the translation of the screen text. The **Edit** option permits you to **Undo** any changes made before pressing **OK**. The **Image** option allows rotating and resizing of the image.

The Edit dialog sub-menu bar options enable you to **Crop** the photo, and to **Undo** changes.

Tagholder Details

Click on the **Details** tab. A **New Tagholder – Details Tab** similar to that shown below is displayed.

New Tagholder – Details Tab

New Tagholder – Details Tab

Id No.	:	Tagholder's personal Identity Number (Optional).
Department	:	Department selected for the Tagholder (Optional).
Department button	:	Allows selection of a department [Department Dialog].
Employee Number	:	Employee Number (Optional).
Tel	:	Tagholder's telephone number (Optional).
Date of Birth	:	Tagholder's birth date (Optional)
Address	:	Tagholder's home address (Optional).

Apply	:	Save and exit.
Cancel	:	Exit without saving changes.

Print Card button : Print Card.

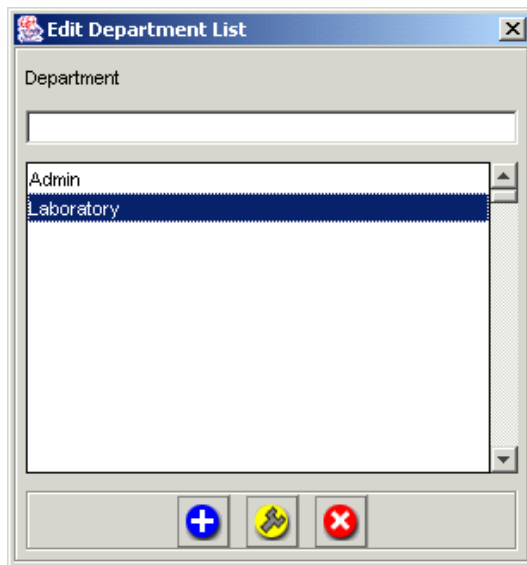
Complete as many of the fields under the **Details** tab as are required.

Department List

The **Department** field is optional and can be left blank. If a department is required, click the **Department** button to display the **Edit Department List dialog** shown below.

Adding a New Department

[1] To add a new Department, click **Add**.



Edit Department List dialog

[2] Type in a new department name.

[3] Click **Apply** to accept the changes, OR

[4] Click **Cancel** to reject them.

Editing a Department Name

[1] To edit a Department name, highlight the name by selecting it.

[2] Click the **Edit** Icon. Make the required changes, and then :

- [3] Click **Apply** to accept the changes, OR
- [4] Click **Cancel** to reject them.
- [5] Click the **Cancel** button or the cross in the top right corner to **Exit**.

IMPORTANT NOTE :

*At this stage, **if it is not** required that the Tag number appear on the card, the card may be printed using the following sequence :*

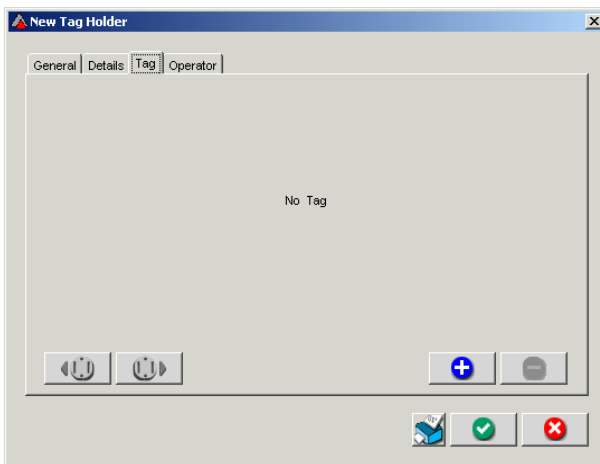
- (a) Print on a blank credit card Tag for a Tagholder before allocating the Tag to him, that is, before entering his Tag number into the System.
- (b) Read in the card number and allocate it to the Tagholder after printing it.

*This sequence is important as it avoids mismatching the Tag code with the Tagholder details. Secondly, it ensures better print quality as the cards are not handled before printing. The printing procedure is described below under the heading **Card Printing**.*

NOTE : *Printing on used credit card Tags is not recommended as dirt or grease on the Tags may result in poor quality printing.*

Adding a Tagholder (Continuation) – Tag Data

- [1] Click on the Tag tab. The New Tagholder – Tag Tab, with No Tag dialog similar to that shown below is displayed.
- [2] Click **Add** to add a new Tag. A blank Tag panel will be displayed.
- [3] Refer to the example shown with data entered.



New Tagholder – Tag Tab, with No Tag

Tag Holder: Tanya Johnson

General | Details | **Tag** | Operator

Tag: 1 ☐ Suspend ☐ Reset APB

Number:

Type: Start Date:

Level: Start Time:

Access Group: Expiry Date:

Usage: Expiry Time:

Message:

Navigation buttons: [Back] [Forward] [Home] [Search] [Add] [Remove] [Print] [OK] [Cancel]

New Tagholder – Tag Tab, with Tag

New Tagholder – Tag Tab

Number : Displays the unique Tag code number of the current Tag.

NOTE : *When using a fingerprint as a Tag, this number must be allocated by the user.*

Read Tag button : Allows the Tag code of a Tag presented to the Controller or Tag Reader to be read and displayed in the Number field.

Type : The type of the Tag.

Level : The level allocated to the Tag.

Suspend : Checked if all access for the Tag is suspended.

Reset APB : If checked will reset the APB status of the Tag in the Controller to neutral.

Start Date : Displays the date when the Tag will be active–yyyy mm dd. (blank = Indefinite).

Expiry Date : Displays the date when the Tag will expire–yyyy mm dd. (blank = Immediate).

Start Time : Displays the time of day on the Start Date when the Tag will be active (hh:mm 24 hour format).
If the Start Date is blank, the Start Time is ignored.

Expiry Time : Displays the time of day on the Expiry Date when the Tag will expire (hh:mm 24 hour format).

If the Expiry Date is blank, the Expiry Time is ignored.

Access Group	:	The Access Group allocated to the Tag.
Usage	:	Identifies Tag usage if issued with more than one (Optional).
Message	:	A pre-defined message associated with the Tag (Optional).
New Tag button (+)	:	Allows entry of a new Tag record.
Delete button (-)	:	Removes the Tag from the Tagholder.

Apply	:	Save and exit.
Cancel	:	Exit without saving changes.
Print Card button	:	Print Card.

NOTE : *Several types of registration devices can be used in an IXP200 System. These are :*

- *The IXP200 Controller.*
- *The ImproX ProxPal.*
- *The ImproX RS USB Registration Interface together with an appropriate Remote Registration Reader (this combination is often referred to in this manual as the ImproX USB "Registration Reader").*

- [1] Place the Tag at the registration device and then click **Read Tag**. The Tag's number is then displayed in the **Number** field, and the Type is displayed in the **Type** field.
- [2] The **Type** field is usually automatically read and displayed. Some Tag types cannot be read by any of the registration devices (see **Registering UHF Tags, Registering Finger Prints as Tags, Registering Personal Access Codes (PACs) as Codes** and **Support for Devices using Wiegand Tag Codes** later in this manual). For these Tags, select the Type manually from the dropdown list to correspond with the Tag used.

NOTE : *Additionally, neither the ProxPal nor the IXP200 Controller is able to read **Mifare Tags**, and Mifare Registration Readers are not able to read standard **125 kHz Tags**. In this case, however, the correct reader types must be included in the IXP200 System. The **Type** field cannot be used to resolve this situation.*

Register the Tag

The registration processes for Tag types that cannot be registered via any of the registration devices are described in the following paragraphs. Once a Tag is registered, proceed to the heading **Tag Registration – Further Steps**.

Registering UHF Tags

4-Channel UHF Tags (ImproX RF Tags) cannot be read directly as a UHF Tag type by any of the registration devices. However, each UHF Tag also has a Slim Tag code of the same value as the UHF Tag code.

- [1] To register such a Tag, read it in as a Slim Tag (using the registration device), change its **Type** to **RF** and save it.
- [2] If the Tag is also required to be read as a Slim Tag, read it in again and select its **Type** as **Slim Tag**. The Tagholder now effectively has two Tags, with the same Tag code, that are distinguished by their Type, for use at different Reader types.

Registering Fingerprints as Tags

- [1] Fingerprints cannot be read by any of the registration devices. A SAGEM MorphoAccess MA200* Automatic Fingerprint Recognition Terminal (*or similar device – refer to the IXP System-compatible Biometric Reader User and Installation Manual for further details) is required for this purpose. To register a fingerprint as a Tag, proceed as described in the above Manual.

Registering Personal Access Codes (PACs) as Tags

A Personal Access Code is effectively a Tag, and can be used instead of a Tag at doors that are set to the Personal Access Code Mode. A **PAC** is captured in the same way as any other Tag in the Tag Tab of the Tagholder dialog box.

Each **PAC** must be a number from 1 to 9 digits in length, and must be unique in that no other Tagholder can have the same **PAC**.

NOTE : *Each **PAC** must start with a non-zero numeral. A **PAC** with leading zero's will be disallowed by the System.*

A **PAC** can be used instead of a Tag at any door that has a keypad Reader and that is operating in Personal Access Code Mode.

NOTE : *A **PAC** is not to be confused with a **PIN**, that is not a Tag but a Personal Identification Number used by a Tagholder in conjunction with a Tag for extra security (for example, in Tag + PIN Mode).*

When first entered in the System the **PAC** number will be displayed, but once accepted will be displayed in the form ***** to maintain security. Only the **PAC** holder will then know the actual **PAC** number. The **PAC** will also be displayed as ***** in reports and in Transaction View.

To register a **PAC** as a Tag, proceed as follows :

- [1] From the keyboard, enter the **PAC** number in the **Tag Number** field.
- [2] Select the type as **Personal Access Code**.
- [3] Click **Apply** to accept the number. The number will now be displayed in the form * * * * *.

Using Personal Access Codes with APB

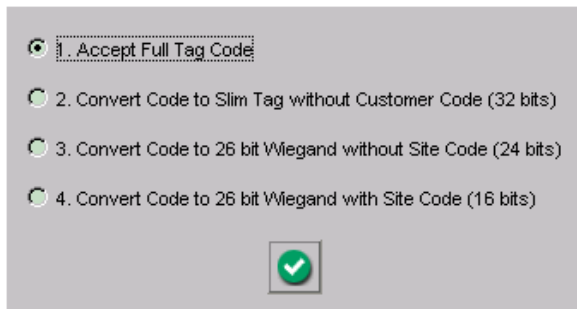
When a **PAC** is used to enter an APB Zone, the same **PAC** must be used to exit the zone, in the same way that the same physical Tag must be used to enter and exit an APB Zone.

Support for Devices using Wiegand Tag Codes

A normal Slim Tag may be used as a Wiegand Tag to interface with certain biometric devices, that require the Wiegand format. Also, certain types of Wiegand Tags may be used as Tags in the IXP200 System.

To register a new Tag in the IXP200 Database :

- [1] Read the Tag in the normal way at the registration device, or type in the Tag code if the registration device used cannot read this type of Tag.
- [2] Select the Tag type as ASCII/Barcode/Magstripe. A dialog will pop up to allow further conversion of the Tag code.
- [3] Select the appropriate conversion to truncate the Tag code, namely 32 bit, 26 bit or 16 bit.



Code Truncation selection dialog

- [4] Click the Apply button to save and close the dialog. Note that the Tag code value changes in the text box.
- [5] Continue and complete the other required fields and save the Tag by clicking Apply.

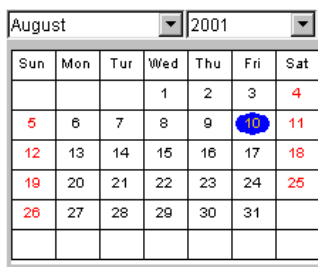
NOTE : *The same Tag may also be registered as a Slim Tag for the same*

person. The Tag will be read at normal ImproX Readers as a Slim Tag and at the Impro Wiegand26 Reader as a Wiegand Tag.

Tag Registration – Further Steps

For all types of Tags, continue as follows :

- [3] In the Level field, click on the arrow icon, and select one of the four levels from the dropdown list.
- [4] If the Tagholder's access is to be temporarily suspended, click on the Suspend box. A tick appears in the box.
- [5] To reset the APB status of the Tag in the Controller to neutral, click the Reset APB check box :
 - [i] Leave the check box unchecked for a new Tag.
 - [ii] Check this box, if necessary, to correct the APB status of an existing Tag that conflicts with the current status in the Controller.
- [6] The Start Date field can be left blank for indefinite validity. If a Start Date is required click on the arrow icon in the Start Date field. A Calendar Dialog similar to that shown below is displayed.



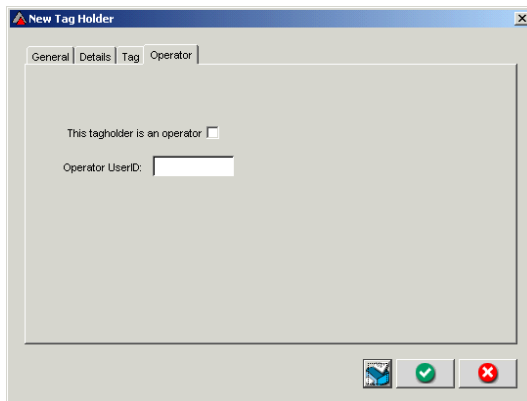
Typical Calendar Dialog

- (a) Click on the **Month** arrow icon; this displays a dropdown menu. Select the appropriate month.
- (b) Click on the **Year** arrow icon; this displays a dropdown menu. Select the appropriate year.
- (c) Click on the **Date** required in the grid. This closes the **Calendar Dialog**, and displays the data in the **Start Date** Field.

NOTE : *To quit the calendar window without choosing a date press the escape button on the keyboard.*

*The start and expiry date can be deleted by highlighting the date and pressing the **Delete** button on the keyboard.*

- [7] The Expiry Date field can be left blank for indefinite validity. If an Expiry Date is required, click on the arrow icon in the Expiry Date field. Select the date as described for the Start Date.
- [8] In the Access Group field, click on the arrow icon; and select an Access Group from the list available to this user and Tag level. (This is mandatory).
- NOTE :** *All Tags must have an Access Group. However, an Access Group with no access to any door can be defined and assigned to a Tag as a place-holder for a valid Access Group to be assigned at a later stage.*
- [9] The Usage field is used to identify employee Tags, if an employee has been issued with more than one. Click in the box and type in the required name e.g. Vehicle Tag. (Optional).
- [10] If a message should be associated with this Tag, click on the arrow icon in the Message field, and select from the list of pre-entered messages. This message will be displayed each time the Tag is presented to a Reader with a display.
- NOTE :** *If the Tagholder must operate the IXP200 and logon as a user, continue with step [11], otherwise skip to “Saving the Tagholder Record”.*
- [11] Click on the Operator tab. A New Tagholder – Operator Tab similar to that shown below will be displayed.



New Tagholder – Operator Tab

New Tagholder – Operator Tab

- Tagholder is an Operator** : Check the box if this Tagholder should be made an Operator for the System. The **Operator User ID** field is now available to enter the UserID for this Tagholder (an operator can log on to the System and allocate low security Tags).
- Operator User ID** : User ID (max 8 characters). Up to 8 characters can be entered.
- Delete button** : Removes the Tag from the Tagholder.

- Apply** : Save and exit.
- Cancel** : Exit without saving changes.
- Print Card button** : Print Card.

Saving the Tagholder Record

If card printing is not required for this Tagholder , click **Apply** to save all the data and close the **Tagholder Dialog** box. Otherwise proceed to “**Card Printing**” before saving and exiting.

Card Printing

At this stage, when all required information has been entered for the Tagholder, the Card may be printed.

If the Tag has been captured and allocated to the Tagholder, Barcodes may also be printed for numeric fields such as Tag Number, ID Number or Employee Number.

The following information describes the Impro Card Printing facility. At the end of this description, the text returns to the Tagholder Information Configuration procedure.

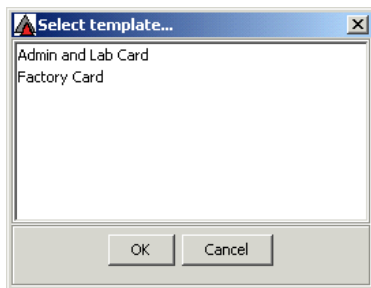
A card may be printed either :

- (a) before being captured (read in) to the System using a new, unused card Tag, OR
- (b) after allocation to a Tagholder. (a card or label can be printed with the Tag number on it). In this case it must be loaded as the first card in the printer to ensure that the Tagholder's details are printed onto the card just allocated to him/her.

Card Printing Procedure – Single Cards

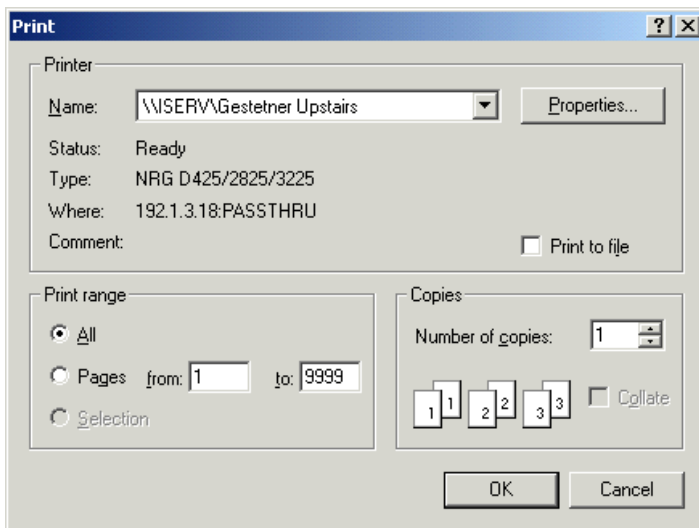
To print cards, follow this procedure :

- [1] Place one or more new cards in the printer as required (**only if the Tag code has not been read in yet**).
- [2] Print each card by clicking **Print Card** at the bottom of the Tagholder dialog.
- [3] The Select Template dialog shown below will be displayed, unless a default template has been set from the **Card Designer/Set Default Template** menu.



Select Template dialog

- [4] In the **Select template** dialog, highlight the required template, and click OK.
- [5] Once the desired template has been selected, select the required printer (a dialog similar to the one below will be displayed once the template is accepted).



Select printer dialog

- [6] Remove the card from the printer, and then read it in to the System and allocate it to the Tagholder as described previously under “**Register the Tag**”.

Printing Directly onto Tags

CAUTION : To print directly onto a Tag, a special printer is required. **DO NOT ATTEMPT TO PRINT DIRECTLY ONTO A TAG USING A NORMAL PRINTER AS DAMAGE TO THE CARD AND THE PRINTER MAY RESULT.**

Saving the Tagholder Record

Click **Apply** to accept the record for the new Tagholder, or click **Cancel** to reject the record or refresh data for an existing Tagholder. This returns to the **Tagholder Panel**, where the new Tagholder data is displayed.

Printing onto Adhesive Labels

To print onto adhesive labels, a standard commercial inkjet or laser printer can be used. Follow the printer manufacturer’s instructions, and the procedure given under **Printing Procedure – Batch Printing**.

Cards printed from some other PC

If the number of cards you need to print does not justify the purchase of a special printer, but you want to print directly onto Tags, your Impro Distributor may offer a printing service.

Printing Procedure – Batch Printing

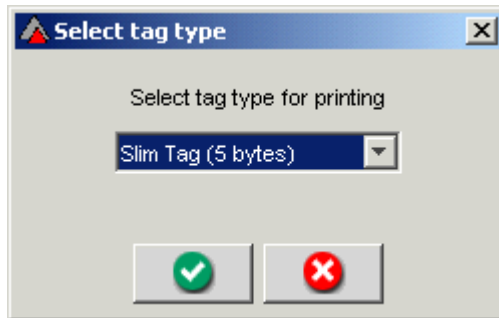
Batch printing can be used to print either adhesive labels for several cards, or a group of card Tags.

When Batch Printing is to be used for **labels**, a template for label printing must first be created in Card Designer.

To print a Batch of either labels or cards, proceed as follows :

- [1] In the Tagholder Panel, select the required Tagholders from the table, by either :
 - [i] Selecting the Tagholders one by one by holding down the Ctrl key and clicking the mouse on each Tagholder, or
 - [ii] Selecting a group of Tagholders (for example, Tagholders in a Department) by clicking on the first Tagholder, then pressing Shift and clicking the mouse on the last Tagholder in the group.
- [2] Then either :
 - [i] When printing to **labels**, load the label sheets into the printer.

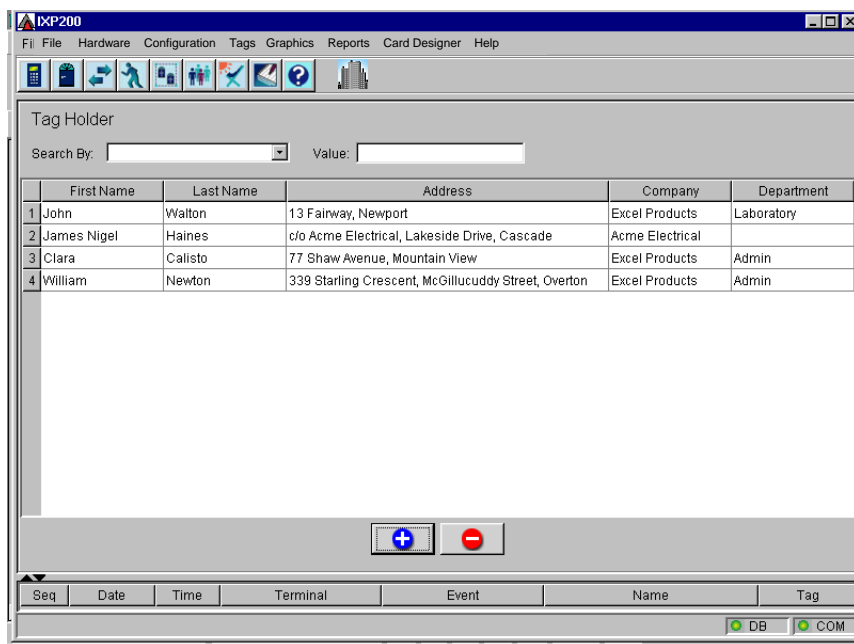
- [ii] When printing a **batch of card Tags** that **have** previously been allocated to Tagholders, load the cards into the card printer in **exactly the same order** as the Tagholder selection.
 - [iii] When printing a **batch of cards** that have **not** been previously allocated, allocate the Tags according to the printed information.
- [3] The **Batch Print** icon is at the bottom of the Tagholder Panel. Clicking on this icon when Tagholders have been selected will display the Select Tag Type dialog shown.



Select Tag type dialog

- [4] Select the Tag type for printing from the combo box.
- [5] Click **Apply** to print, or **Cancel** to abort.
- [6] If **Apply** is selected, the **Select Template dialog** shown previously under **Card Printing Procedure – Single Cards** will be displayed.
- [7] Proceed as per the instructions [4] and [5] that follow the **Select Template dialog** illustration.

See next page



Typical Tagholders Panel

Editing an Existing Tagholder

To Edit a Tagholder, proceed as follows :

- [1] Click on the **Tagholders** icon on the toolbar or select from the **Tags** dropdown menu.
- [2] Using the mouse double click on the required name to be edited and then select the appropriate procedures as described in "**Adding a Tagholder**" to complete the editing.
- [3] Search for the Tagholder/Tag required as described below.
- [4] Search options are provided to locate a Tagholder in a large table. Search by any of the items stored for the Tagholder. For example, search by Last Name and start typing the required name in the Value box. The selected row moves to locate the name matching the entry in the Value box, e.g. typing M then u then r etc., locates the first Tagholder with the last name starting with M, then Mur and so on. (This search facility is case sensitive).

NOTE : *This search requires the first (or any) line to be selected before starting.*

- [5] The alternative method of finding the record, if the Tag is available, is to search by Tag. A Read Tag button and a Find button appear next to the Value box.

- [6] Place the Tag on the Controller/tag Reader and click **Read Tag** . The Tag code appears in the Value box.
- [7] Click **Find** to locate the owner Tagholder. The Tagholder may have several Tags, so locate the Tag matching the Tag code in the Value box.

The screenshot shows a dialog box titled "Tag Holder: John Walton". It has four tabs: "General", "Details", "Tag", and "Operator". The "General" tab is selected. It contains the following fields:

- First Name: John
- Last Name: Walton
- Pin: (5 numbers)
- Company: Excel Products
- Note: (empty text area)

At the bottom of the dialog, there are four buttons: a left arrow, a right arrow, a printer icon, and a green checkmark button. There is also a red X button.

Tagholder General Tab for Editing

For existing Tagholders, the following additional buttons appear on the **Tagholder Dialog** :

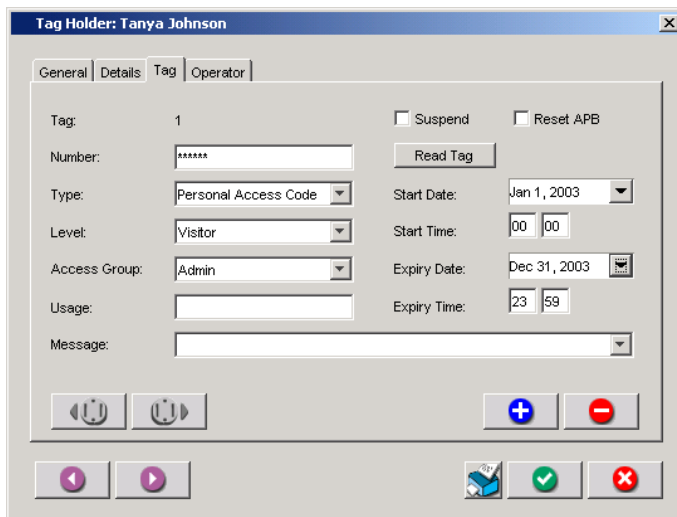
Next : Moves to the next Tagholder
Previous : Moves to the previous Tagholder

Also, on the Tag Tab, the following additional buttons appear :

Next Tag : Moves to the next Tag
Previous Tag : Moves to the previous Tag

(See the figure that follows)

See next page



Tagholder dialog showing “Next Tag” and “Previous Tag” icons

Deleting an Existing Tag

To Delete a Tag from a Tagholder, proceed as follows :

- [1] Click on the **Tagholders** icon on the toolbar or select from the **Tags** dropdown menu.
- [2] Select the required name to be deleted in the **Tagholders Panel**, and then double click on the selected name. The **Tagholder – General Tab** is displayed.
- [3] Click on the **Tag** tab. The **Tagholder – Tag Tab** is displayed with details of the Tag that is to be deleted.
- [4] Locate the correct Tag if there is more than one.
- [5] Click **Delete** to remove the Tag from System.
- [6] Click **Apply** to confirm deletion of the Tag, or click **Cancel** to restore the Tag.
- [7] Repeat for all Tags for this Tagholder, if required.


This concludes the configuration of Tags and Tagholders.

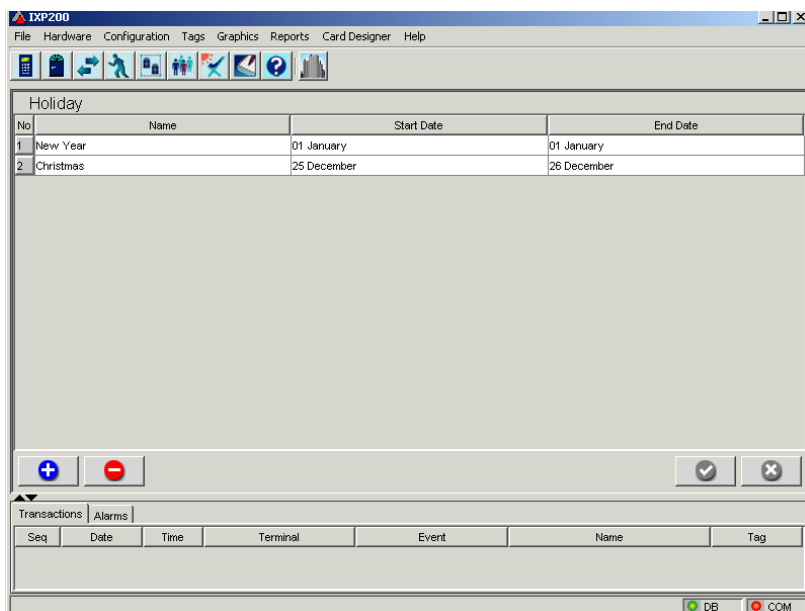
CHAPTER 8 – HOLIDAYS CONFIGURATION

General

- (a) This System allows for a maximum of 20 holiday dates to be entered by the user.
- (b) All holidays must have start and end dates.
- (c) Doors may operate in a specific mode during holidays.
- (d) After the holiday's end date is reached, the doors would then revert to their normal mode as defined by their day mode pattern.
- (e) This feature is designed for schools and institutions, where at the end of a period (term), the doors must automatically change to the special mode.
- (f) Furthermore access can also be specifically defined for holidays.

NOTE : *To allow same day holidays to be automatic year after year, the holiday has no year field.*

The next item to be configured is a Holiday. To access the Holiday Panel, click on the  Icon.



Holiday Panel

Holiday Panel Fields and Buttons

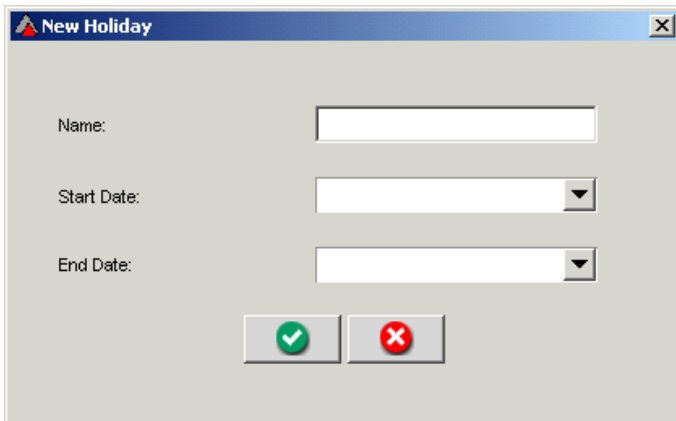
Below is a brief description of all the fields associated with the **Holiday Panel**, the information displayed in the fields and what the buttons functions are:

No.	:	Number allocated to the holiday.
Name	:	Displays the name of the holiday.
Start Date	:	Displays the commencement Date and Month.
End Date	:	Displays the expiry Date and Month.
Add	:	Allows a new holiday to be created.
Delete	:	Removes the selected holiday from the list.
Apply	:	Accepts the new holiday entries into the System database.
Cancel	:	This button removes any new or edited entries from the list if Apply has not been clicked.

Configuring Holidays - Procedure

To configure annual holidays, proceed as follows :

- [1] Click on the **Holiday** icon on the toolbar or select from the **Configuration** dropdown menu. A **Holiday Panel** similar to that shown above is displayed. For a new site the list is empty.
- [2] Click **Add** to add a new holiday. A **New Holiday Dialog** similar to that shown below is displayed.

The image shows a 'New Holiday' dialog box. It has a title bar with a small icon and the text 'New Holiday'. Inside the dialog, there are three labels: 'Name:', 'Start Date:', and 'End Date:'. Each label is followed by a text input field. The 'Start Date:' and 'End Date:' fields have dropdown arrows on their right side. At the bottom of the dialog, there are two buttons: one with a green checkmark and one with a red 'X'.

New Holiday Dialog

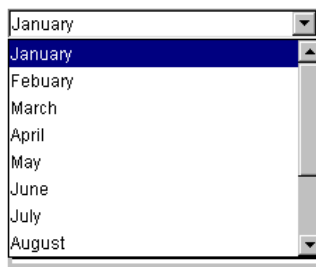
New Holiday Dialog

- Name** : Name of the new holiday.
- Start Date** : After the selection is made from the calendar, the month and date is displayed here.
- End Date** : After the selection is made from the calendar, the month and date is displayed here.
- Down Arrow Icon** : Displays the calendar.
- Apply button** : Accepts the new or edited holiday.
- Cancel button** : Rejects the data and closes the panel.

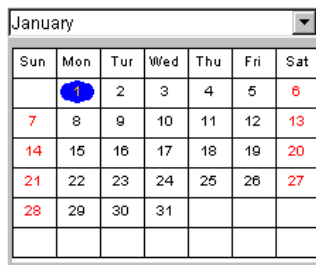
[1] In the **Name** field, type in the name of the holiday.

[2] For a single day holiday, proceed as follows :

- (a) In the **Start Date** field click on the arrow icon to view the calendar.
- (b) Select the **Month** dropdown menu by clicking on the arrow icon and then select the required **Month**, and then click on the required **Date** in the grid.



Month Dialog



Date Dialog

- (c) In the **End Date** field click on the arrow icon to view the calendar.

- (d) Select the **Month** dropdown menu by clicking on the arrow icon and then select the same **Month** as before, and then click on the same **Date** as before in the grid.
- [3] Click **Apply** to accept the new data or **Cancel** to reject data.
- [4] For a multiple day holiday, proceed with the above procedure, except in the **End Date** field select the last day of the holiday.
- [5] Click **Apply** to accept the new data into the System, or click **Cancel** to reject new data or refresh existing data.

NOTE : *Changing to another panel before clicking on the Holiday Panel's **Apply** button, would result in the all new entries being rejected.*

NOTE : *To quit the calendar window without choosing a date press the escape button on the keyboard.*

*The start and expiry date can be deleted by highlighting the date and pressing the **Delete** button on the keyboard.*

Editing an Existing Holiday

To Edit a Holiday, proceed as follows :

- [1] Click on the **Holiday** icon on the toolbar or select from the **Configuration** dropdown menu.
- [2] Double click on the holiday to be edited, and then select the appropriate procedures above to complete the editing.

Deleting an Existing Holiday

To Delete a Holiday, proceed as follows :

- [1] Click on the **Holiday** icon on the toolbar or select from the **Configuration** dropdown menu.
- [2] Select the required name to be deleted in the **Holiday Panel**, and then click **Delete** to remove the Holiday from the System.

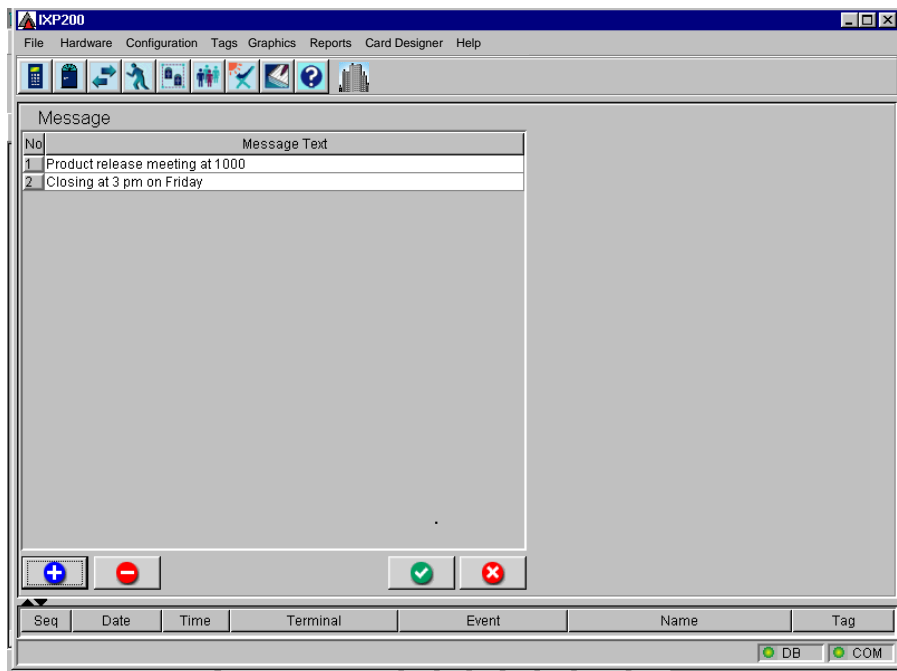
This concludes the configuration of Holidays.

CHAPTER 9 – MESSAGES CONFIGURATION

General

This panel allows the user to enter and store up to 255 Messages, each with a maximum of 64 characters. These Messages can be entered into and deleted from the System at any time.

A Message can be linked to a particular Tagholder to be displayed on the Terminal when his Tag is presented. Time or Event Triggered Actions can also initiate these Messages, that are displayed on the Controller LCD.



Message Panel

Message Panel Fields and Buttons

Below is a brief description of all the fields associated with the Message Panel, the information displayed in the fields and what the button's functions are:

No. : The System allocates a number when a new Message entered.

- Message Text** : Displays all the Messages that are stored in the Systems database.
- Add** : Allows you to add a new Message into the System.
- Delete** : This button removes the selected entry in the pane above.
- Apply** : This button accepts the new data into the System database.
- Cancel** : This button rejects any new or edited entries.

Adding New Messages

To add new Messages, proceed as follows :

- [1] Click on **Configuration** on the toolbar and select **Messages** from the dropdown menu. The **Messages Panel** similar to that shown above is displayed.
- [2] Click **Add** . The **New Message Dialog** similar to that shown below is displayed.



New Message Dialog

- Duration** : Duration of this message.
- Mode** : Displays the mode associated with the message.
- LCD Panel** : The text of the message as it will appear on the LCD display.
- Apply** : Accepts the new or edited message.
- Cancel** : This button rejects the new entry.

- [1] Click in the **Duration** Field, and entered period of time that the message must be displayed (i.e. 10s = 10 seconds).
- [2] In the **Mode** field, Normal is the default setting. The other options are not available with this version of Software.
- [3] In the **LCD Panel** field, click in the window and then type in the appropriate message to be displayed. Type spaces to fill a line and do not enter carriage returns.
- [4] Click **Apply** to accept the new data into the System, or click **Cancel** to reject new data.

NOTE : *Failure to click **Apply** in the **Message Panel** after adding a new Message or editing an existing one would result in the data being lost.*

Editing an Existing Message

To Edit a Message, proceed as follows :

- [1] Click on **Configuration** on the toolbar and select **Messages** from the dropdown menu.
- [2] In the **Message Text** pane, select the required message to be edited, and then double click on the highlighted message. An **Edit Message Dialog** similar to that shown above is displayed.
- [3] Edit the required fields and then follow the appropriate procedures above.

Deleting an Existing Message

To delete a message, proceed as follows :

- [1] Click on **Configuration** on the toolbar and then select **Messages** from the dropdown menu.
- [2] In the **Message Text** pane, select the required message to be deleted, and then click Delete to remove data from System.

NOTE : *To restore the original message click Cancel in the Message Panel, this only applies if the Apply has not already been clicked-on.*

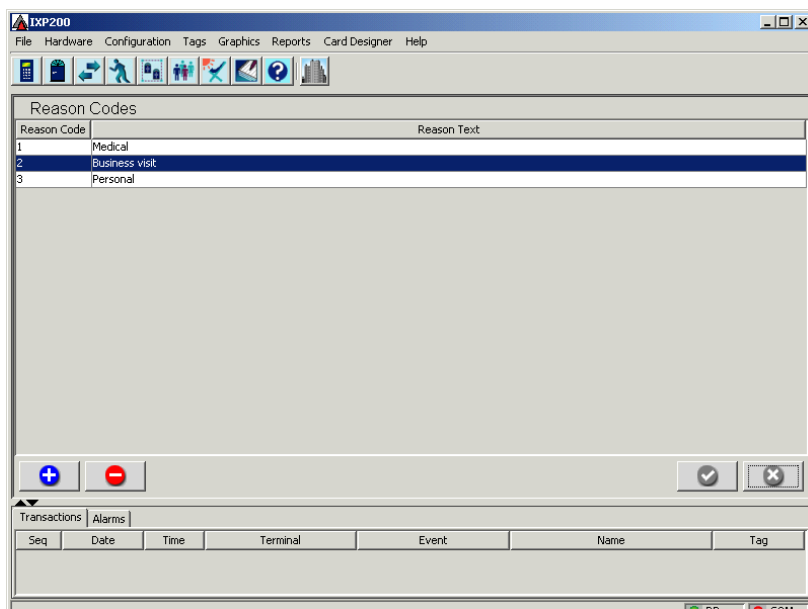
END OF CHAPTER

CHAPTER 10 – REASON CODES CONFIGURATION

General

This panel allows the user to enter and store up to 99 reason codes, each with a text description.

Reason Codes Panel and Buttons

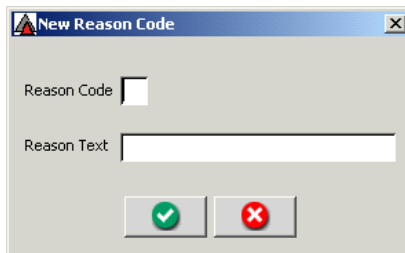


Reason Codes – typical Panel

To Add a Reason Code

- [1] Select **Reason Codes** from the **Configuration** Menu.
- [2] Click **New**.
- [3] The **New Reason Code dialog** shown on the next page will be displayed.
- [4] Enter the required code and its text description in the dialog.
- [5] Click **Apply** to accept the code and close the dialog, or **Cancel** to reject the code and close the dialog.

- [6] Add more Reason Codes as required.
- [7] Click **Apply** on the **Reason Codes** Panel to save all changes, or **Cancel** to reject them.



New Reason Code dialog

To Edit an Existing Reason Code

- [1] Double-click the row to be edited and change the text description in the **Edit Reason** dialog box displayed.



Edit Reason Dialog

- [2] Click on **Apply** on the **Edit Reason Dialog** to save any changes, or on **Cancel** to reject them.
- [3] Click **Apply** on the **Reason Codes Panel** to save all changes, or on **Cancel** to reject them.

END OF CHAPTER

CHAPTER 11 – CARD DESIGN

INTRODUCTION

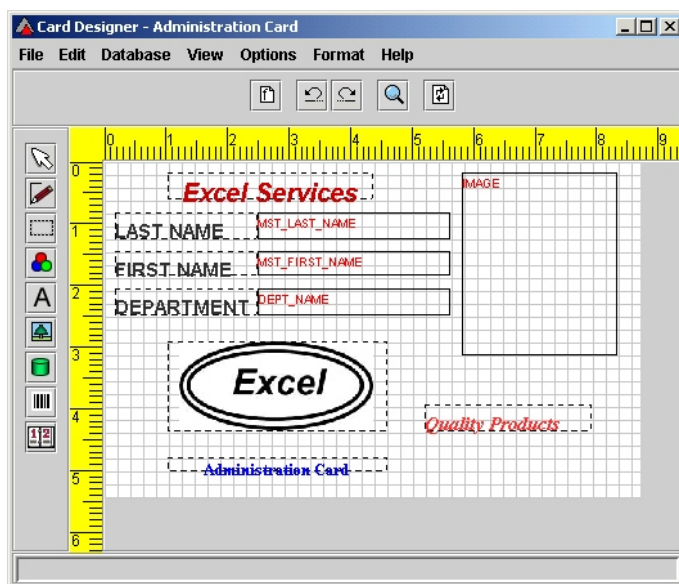
This Software permits the System user to design templates for the printing of data concerning a Tagholder onto the Tagholder's ISO credit card Tag, or on to adhesive labels.

Card printing may be either single-sided or double-sided.

The Software allows for the inclusion of custom text as well as Tagholder details from the System database, such as first and last names, department, and so on in card templates. It is also possible to include custom images, such as a company logo, as well as an image of the Tagholder from the database.

CARD DESIGNER

To access the Card Designer, click on **Card Designer** in the **Top Menu Bar**, then on **Card Designer**.



Typical Card Template Design

The use of the Card Designer is described in the Impro Card Designer User Manual, IXP333-0-0-GB-XX, that is supplied with your IXP200 Software – please refer to that manual.

A typical design for a card template is shown on the previous page for reference.

END OF CHAPTER

CHAPTER 12 – GRAPHICS

GRAPHICS SOFTWARE

The Graphics Software comprises two components, namely the Designer Module and the Runtime Module.

The Designer Module allows the user to develop various plans, and is described in the Impro Graphics Designer Module manual.

The Runtime Module allows the Graphics Software to display plans derived using the Graphics Designer Software Module, and to permit the monitoring and control of various System parameters by means of icons superimposed on the plans. The Runtime Module is integrated into the IXP200 Software.

Features



The principal Graphics Runtime Software features are :

- (a) Display of Base Plans and Floor Plans of the areas under access control.
- (b) Display, on these plans, of alarms generated within the System.
- (c) The ability to acknowledge alarms from the Plans.

Using the Graphics Runtime Module

Once suitable graphics have been developed using the Impro Graphics Designer, these Graphics are automatically accessed from the IXP200 System once the IXP200 Software is run.

The Graphics Base Plan will be displayed in the Main Application Window on startup. It will be immediately be replaced by the relevant Floor Plan whenever an alarm is received.

At any time it is possible to toggle between the Graphics display and any other configuration screen currently selected by clicking on the  Icon. Click the  (Home) icon to display the Base Plan if this is not already displayed.

Selecting a Floor Plan

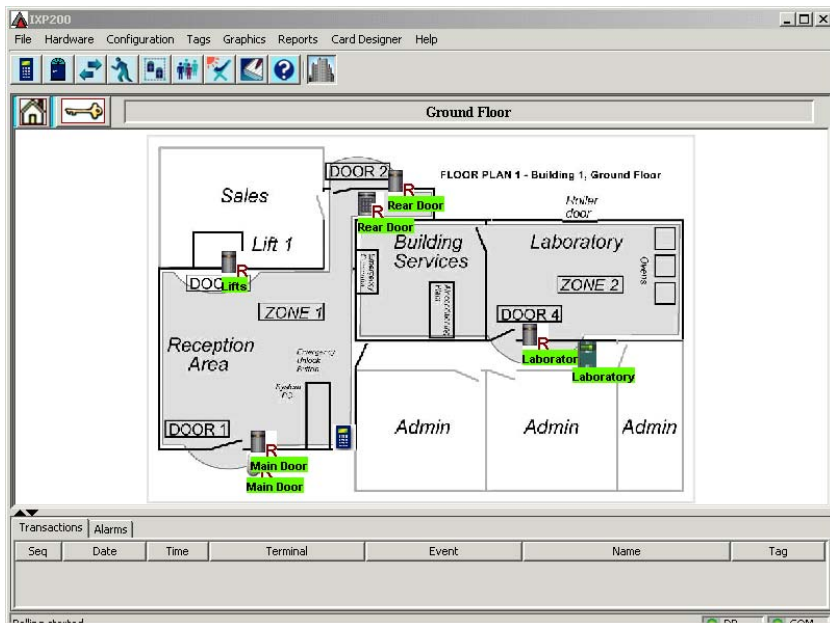
To select a Floor Plan :

- [1] Right-click on a **Building** icon. A “**Select floor...**” bar will be displayed.
- [2] Click on this bar. A **Select Floor Plan** dialog similar to that shown below will be displayed.
- [3] Select the required Floor and click **Apply**.

- [4] The selected Floor Plan will now be displayed in the Main Application Window.



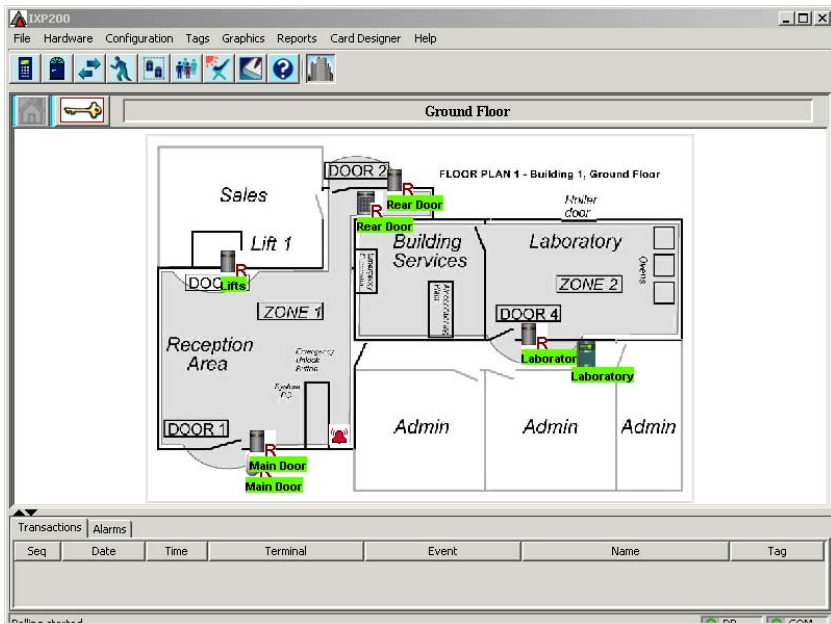
Select floor plan dialog



Typical Floor Plan display

Alarms

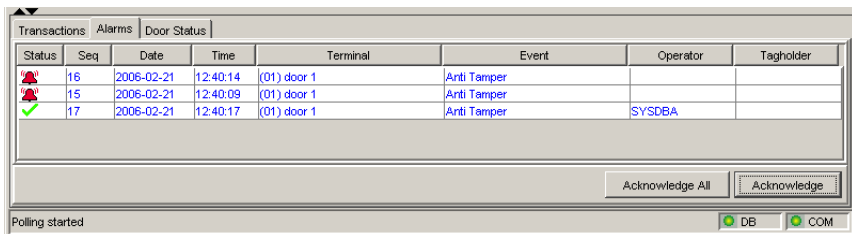
Alarms are indicated by a moving red bell icon, that replaces the icon for the Terminal at that the alarm occurred on the Floor Plan (see illustration on next page).



Typical Floor Plan showing unacknowledged Alarm at the Controller

All alarms are displayed at the bottom of the main screen, as shown in the next illustration.

The software displays unacknowledged alarms at the top of the list, and acknowledged alarms at the bottom.



Alarm display on Main Screen

Graphics Menu Options

The Graphics drop-down menu offers the following options :

View	⇒	Show Non-Readers Show Inputs Auto Resize Icon Text
Tools	⇒	Find Tagholder

The **View** option permits the user to choose whether to show **Non-Readers** and/or **Inputs**, as well as using **Auto Resize** to ensure that the Floor Plan is scaled to fit on the screen.

Selecting the **Icon Text** option displays the Icon Text dialog shown below.




Icon Text dialog

This dialog permits the user to choose globally whether to display Icon Text, and if so, whether it should be displayed above or below the icons. The Background colour can also be selected.

The **Default** button permits the user to select the settings chosen as the default setting. These will then be applied automatically every time the program is started.

See next page



The 'Locate tagholder' dialog box features a title bar with a red triangle icon and the text 'Locate tagholder'. It contains three input fields: 'First Name' with the value 'Clara', 'Last Name' with the value 'Calisto', and 'Department' with a dropdown menu set to 'ALL'. A 'Refine' button is located to the right of the 'Department' dropdown. Below these fields is a large text area displaying 'Clara Calisto'. At the bottom, there is a 'Find selected person' button and a yellow 'X' button.


Locate Tagholder dialog

Locate Tagholder Option

The **Tools** option in the **Graphics Menu** permits the operator to find a Tagholder; the System will indicate at that **Reader** a Tagholder last presented his/her Tag when this option is selected.

Select the Tagholder as follows :

- [1] In the **Locate Tagholder dialog**, enter the first and/or last names of the Tagholder. The **Locate Tagholder dialog** is shown above with details entered.
- [2] Click **Refine**. several Tagholder's names may appear in the main window as shown.
- [3] Highlight the required Tagholder's name.
- [4] Click **Find the Selected Person** to locate the Tagholder, or click **Close** to exit the dialog without searching.
- [5] A **Last transaction dialog** similar to that shown below will be displayed.



The 'Last transaction...' dialog box has a title bar with a red triangle icon and the text 'Last transaction...'. It displays the name 'Clara Calisto' at the top. Below this, there are four input fields: 'Date' with the value '2002-05-31', 'Time' with the value '16:15:27', 'Terminal' with the value 'Main Door', and 'Event' with the value 'Allowed In'. To the right of these fields is a box labeled 'No pic'. At the bottom center is a yellow 'X' button.

Last transaction dialog

Display Change on Alarm Condition

When an alarm condition occurs (e.g. if a unit is tampered with), the Graphics Software will change the display to show the Ground or Floor Plan of the area where the alarm occurred.

NOTE : *The display will only be shifted automatically to show an alarm in another area if the current alarm is acknowledged.*

Alarm Acknowledgement

An Alarm can be acknowledged on the display by right-clicking on the Alarm icon concerned, and selecting Acknowledge from the menu that appears.

Alternatively, highlight the alarm transaction in the alarm panel and click the Acknowledge button on the panel.

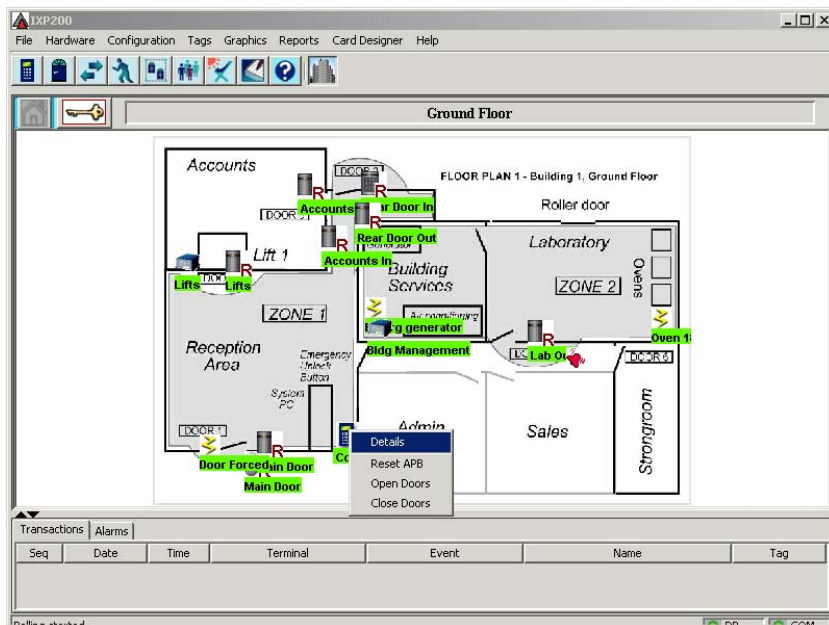
To acknowledge all outstanding alarm transactions in the database, click Acknowledge All.

Alarm Details

Details of an Alarm can be obtained by right-clicking on the **Alarm** icon in the Graphics Panel, and selecting **Details** from the menu that appears.

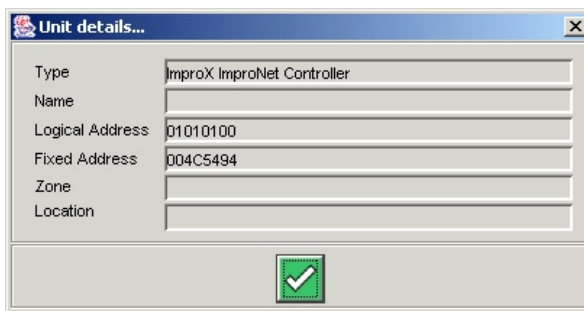
Controller Options Menu

- Right-clicking on the Controller icon will cause a menu to be displayed showing the options for that unit.
- A typical Options Menu for a Controller is shown in the diagram below.



Controller Options menu

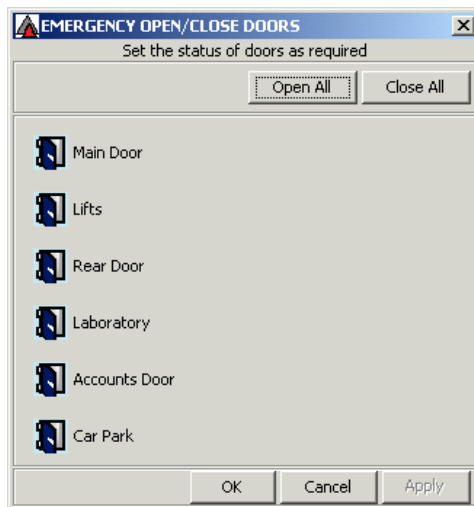
- Clicking on the Details option will display the Unit details dialog shown on the next page.



Controller details dialog

- Clicking on the **Reset APB** option will cause the System to set all the Anti-Passback Status of all Tagholders to Neutral. This option is for use, for example, after a building has been evacuated. It allows any Tagholder in or out of APB zones once only, no matter whether the Tagholder was in or out when **Reset APB** was selected.

- Clicking on the **Open Doors** option will cause the **Emergency Open/Close All Doors dialog** shown below to be displayed.



Emergency Open/Close All Doors dialog

In this dialog, proceed as follows :

- [1] To open all doors – click **Open All**; this immediately unlocks all the doors and leaves them open indefinitely.
- [2] To close all doors – click **Close All**; this immediately locks all the doors, the System will then revert back to the Door Pattern set for that period.
- [3] To open selected doors only, click on the appropriate **Door Icons**, to show an open icon. Click **Apply** to open or close the doors as indicated by the icons, or click **Cancel** to refresh the current door status as given by the Controller.
- [4] Click **OK** to close the window.

Remote Reader Options Menu

Right-clicking on a **Remote Reader** icon will cause a menu to be displayed showing the options for that unit.

The **Options Menu** for a Remote Reader provides the following options :

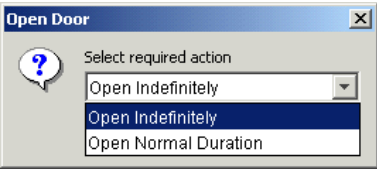
- (a) Details
- (b) Open Door
- (c) Close Door
- (d) Monitor Door

- [1] Clicking on the **Details** option will display the **Unit details dialog** shown below.

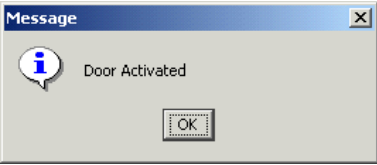
A dialog box titled "Unit details..." with a close button (X) in the top right corner. It contains several input fields: "Type" (filled with "ImproX ImproNet Controller"), "Name" (empty), "Logical Address" (filled with "01010100"), "Fixed Address" (filled with "004C5494"), "Zone" (empty), and "Location" (empty). At the bottom center, there is a green square button with a white checkmark.

Unit details dialog

- [2] Clicking on the **Open Door** option will cause the **Open Door dialog** shown below to be displayed.
- [3] Select the time period required from the drop-down menu.
- [4] Click **Apply** to accept this setting or **Cancel** to ignore the setting.

A dialog box titled "Open Door" with a close button (X) in the top right corner. It features a question mark icon in a speech bubble on the left. The text "Select required action" is above a drop-down menu. The menu is open, showing three options: "Open Indefinitely" (highlighted), "Open Indefinitely", and "Open Normal Duration".

Open Door drop-down menu

A message dialog box titled "Message" with a close button (X) in the top right corner. It features an information icon (i) in a speech bubble on the left. The text "Door Activated" is displayed. At the bottom right, there is an "OK" button.

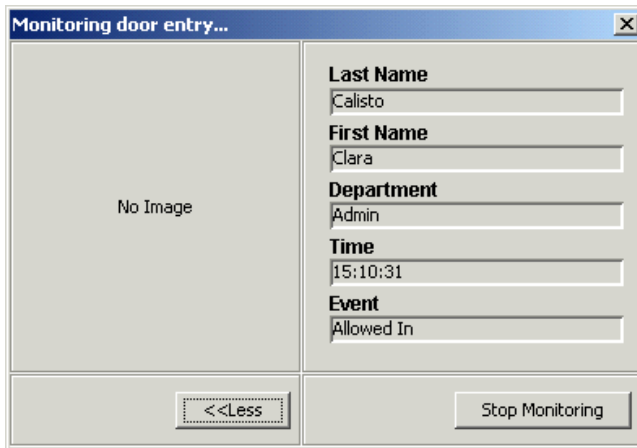
Door Activated dialog

Clicking on the **Monitor Door** option causes a dialog **Monitoring door entry dialog** such as that shown below to appear.

This dialog provides details of Tagholder movements at a door (including a photo if available), and the Time and Event.

Click **Stop Monitoring** to quit the **Monitor Door** mode.

See next page



Monitoring door entry dialog

This concludes the information on Graphics

USER'S NOTES

CHAPTER 13 - OTHER SYSTEM OPERATIONS

General

Several System configuration operations, that may need to be carried out from time to time, are described below.

Full Data Upload

If the Controller memory becomes corrupt, the Controller needs to be cleared of its current Configuration Tables, and then a **Full Upload** is required to update all configuration data to the Controller from the PC Database.

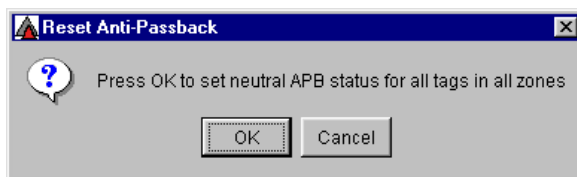
The clearing of the Configuration Tables has **no** effect on the Transaction Buffer.

To Upload data proceed as follows:

- [1] Click on **Configuration** on the toolbar.
- [2] Select **Start Full Upload** from the dropdown menu.
- [3] The System takes a while to clear and then uploads the configuration data.

Reset Anti-Passback (APB)

This function is used to Reset the Anti-Passback status of all Tagholders to neutral, e.g. if Tagholders have left the premises in an emergency, without presenting their Tags. Resetting the APB allows each Tagholder one entry, to reset their APB status.



Reset Anti-Passback Dialog

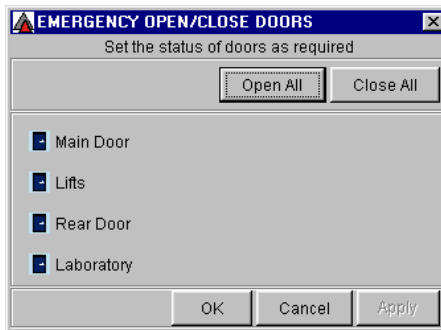
To Reset APB proceed as follows:

- [1] Click on **Hardware** on the toolbar.
- [2] Select **Reset Anti-Passback** from the dropdown menu.
- [3] The **Reset Anti-Passback Dialog** above is displayed to confirm if APB must be set to a neutral status.

Emergency Open Doors

This function is provided for emergencies where people are required to leave the building immediately, (e.g. if there is a fire in the building) without

presenting their Tags at the doors. The status of individual doors is displayed so that they can be closed or opened.



Emergency Open/Close Doors Dialog

Emergency Open/Close Doors – Procedure

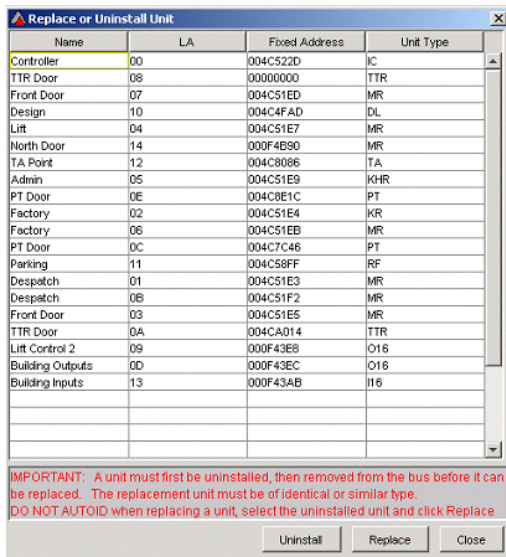
To select Emergency Open/Close Doors, proceed as follows :

- [1] Click on **Hardware** on the toolbar and select **Emergency Open Doors** from the dropdown menu. The **Emergency Open/Close Doors Dialog** similar to that shown above is displayed.
- [2] To open all doors – click **Open All**; this immediately unlocks all the doors and leaves them open indefinitely.
- [3] To close all doors – click **Close All**; this immediately locks all the doors, the System will then revert back to the Door Pattern set for that period.
- [4] To open selected doors only, click on the appropriate **Door Icons**, to show an open icon. Click **Apply** to open or close the doors as indicated by the icons, or click **Cancel** to refresh the current door status as given by the Controller.
- [5] Click **OK** to close the window.

Replacing a Unit

Do not physically remove any Terminal from the bus until it has been uninstalled in the Software. This is to ensure that the encryption seed, if used, is reset to zero. This will allow future communication with the Terminal if it is subsequently installed in another System. In addition, the Logical Address of the Terminal is cleared.

See next page



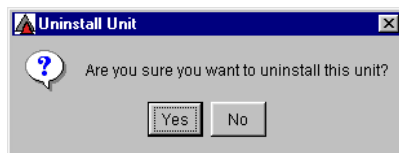
Typical Replace or Uninstall Unit Dialog

When this dialog is visible, all polling is halted.

Removing or Replacing a Terminal

First decide if the Terminal is to be permanently removed or whether it is to be replaced by another Terminal, In this example, a faulty Terminal is to be replaced. Proceed as follows :

- [1] Click on **Hardware** on the toolbar and select **Replace Unit** from the dropdown menu. The **Replace or Uninstall Unit Dialog** similar to that shown above is displayed.
- [2] Select the required Terminal from the list and click **Uninstall**.
- [3] Confirm by clicking **Yes** or exit by clicking **No**.



Uninstall Confirmation Dialog

- [4] Information message may advise that Uninstall failed. If the unit is faulty click **Yes** to uninstall anyway.

- [5] Click **Yes** when prompted to replace the Terminal. (If the Terminal was to be removed altogether, **No** would be clicked).
- [6] Disconnect the Terminal as instructed by the Information message.
- [7] Reconnect the replacement Terminal in the same position as the old one. It should be of a similar type, e.g. Reader replaces Reader type and IO Terminal replaces IO Terminal type.

NOTE : *Do **NOT** perform an Auto-ID before completing this procedure, as this would create a **new** unit ID instead of replacing an existing one. If required, the **Replace** or **Uninstall** Dialog may be closed at this point to continue at a later stage. In this case, when the dialog is re-opened, select the Terminal to be replaced (the Fixed Address should be 00000000), and continue from the next step.*

- [8] Click **Replace** and click **Yes** when prompted.
- [9] Select the **Terminal** type from the dropdown list and click **Apply**.
- [10] Enter the fixed address obtained from the label of the new Terminal and click **Apply** to install.
- [11] The new Terminal is now installed.
- [12] Click **Close** to exit the window.
- [13] Polling will restart automatically.

Replacing a Controller

To Replace a Controller, proceed as follows :

- [1] Select the Controller from the list and click the **Uninstall** .
- [2] Confirm by clicking **Yes** or exit by clicking **No**.
- [3] An Information message may advise that Uninstall failed. Click **Yes** to uninstall anyway as nothing further can be done.
- [4] Click **Yes** to reply to prompt that the Controller is to be replaced.

NOTE : *This step is **very important**.*

- [5] Click **Close** to exit the window.
- [6] An Information Message will appear, stating that no units have been identified for the site. Polling will not start.
- [7] Exit the program.
- [8] Disconnect the Controller.
- [9] Reconnect the replacement Controller in the same position as the old one. It should be of the same type, namely an ImproX Ixp200 Controller with the correct version of firmware.
- [10] Restart the program.
- [11] A **Database Hardware Check** message will appear stating that the Controller detected does not match the database.

- [12] Close the message and select **Replace Unit** from the **Hardware** menu.
- [13] Select the **Controller** from the list and click **Replace**.
- [14] Click **Yes** when asked if the Controller is connected to the bus.
- [15] Enter the fixed address from the label of the new Controller when prompted.
- [16] Click **OK** to install.
- [17] If no message appears, the new Controller has successfully been installed.
- [18] Click **Close** to exit the window and restart polling.

Clear Transaction Buffer

This function is accessed via the **Hardware Menu**. Selecting this function clears all transactions from the Controller memory, deleting the history of all transactions up to that time.

This function should generally only be used when the data is not valid, e.g. during the installation phase, or when a Controller has been replaced.

CAUTION : The use of the Clear Transaction Buffer function clears the Controller memory of all stored transactions. This data will be irretrievably lost !!!

THIS CONCLUDES THE CONFIGURATION OF THE IXP200 SYSTEM.

USER'S NOTES

USER'S NOTES

CHAPTER 14 – TRANSLATION

General

The text in the IXP200 application Software can be translated from English into another language by the user.

Translation – Localisation

This application is provided with English text. If localisation of the text is required, it may be dynamically translated making use of the Locale and Translate functions.

Translated text is stored in property resource files. Once translation is completed, these files should be distributed with the application.

Choosing a Locale for Translation

The following paragraphs provide a guide of how to go about translating the IXP200 Software. The basics are briefly described for first-time users, and very important information that can save a lot of time is included.

NOTE : *It is recommended that the user read this thoroughly before attempting translations.*

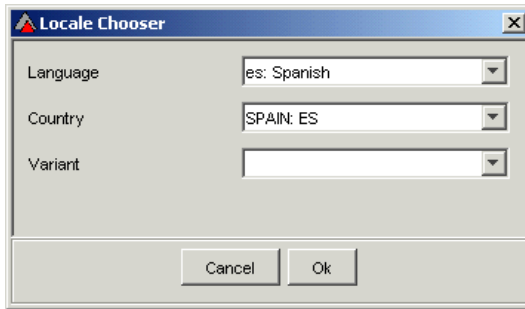
The Basics

The IXP200 Software can be translated into any language provided the computer supports that character set.

To begin translation :

- [1] Start the IXP200 program in either online or offline mode, with SYSDBA password.
- [2] From the **File** menu, select the **Choose Locale** option and make sure the language and country settings are correct.

See next page



Locale Chooser Panel

[3] A **Locale Chooser Panel** similar to that shown above is displayed.

Choose a Locale

It is very important that the correct Locale settings are chosen before beginning the translation. When the **Choose Locale** dialog first appears, it shows the default locale of the System. For instance, typical values may show that the language is French, and the country is France.

There is also a field called **Variant**, that is optional and by default is null. In most cases it is best to change the country field to None, and leave the variant field as none, thereby selecting “general” French. This means that the base French text can be defined that works for any System with a French setup, regardless of the country it is in.

If it then becomes necessary to change certain French text for a different country, the changes can be made at a later stage by simply modifying the base French text for the specific country without affecting the base French translation.

If this approach is not followed, then it may result in a lot more effort in the long run. e.g. if French/France is selected and translated, then translation to French/any other country would have to be done from scratch. If base French is defined, then only the changes for the specific country would need to be redone.

Furthermore, if it becomes necessary to have more than one **Variant** of a specific language/country combination, then the variant can be given. This is in the very rare case where the language in a certain country is spoken slightly differently in different parts. To enter a variant, type a 2-digit number in the variant field.

The best approach to adopt when choosing locales for translation is as follows:

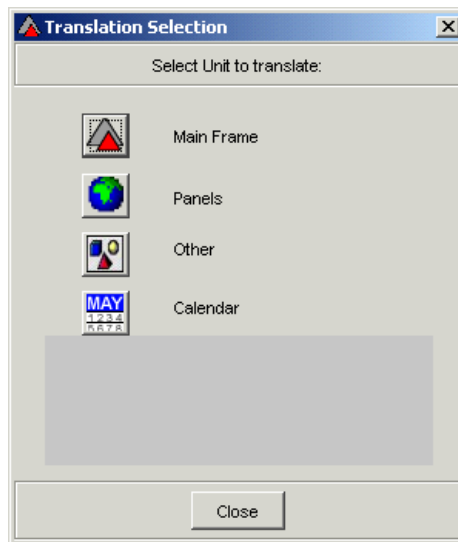
- [1] Translate the text in the base language (no country selected).
- [2] If modifications are required for a specific country, choose the language and country and translate text.
- [3] If a specific variant of that country is required, enter the variant code along with the language and country.

NOTE : *The application must be closed and restarted between steps [1], [2] & [3].*

It is recommended that the user follows all 3 steps in the correct order, to save time in the long term because future modifications for any country or variant of that language would only require slight changes, rather than re-entering all the base language text for every change.

Translating

Once the correct locale is chosen, from the **File** menu, select the **Translate** option. A **Translation Selection Dialog** similar to that shown below will be displayed.



Translation Selection Dialog

The categories for translation are split up into various components, namely Main Frame, Panels, Other, and Calendar.

Main Frame

This term refers to text that appears in the Main Application Window, including the Menus.

Panels

This option gives access to the panels used by each of the toolbar buttons.

- [1] Click **Panels** and the icon will appear in the toolbar.
- [2] Close the **Translation Selection Dialog** and click the **Toolbar** button to display the required Panel. This will give the context while translating.
- [3] Now click the **World** icon in the toolbar to display the **Translate Text Dialog** corresponding to the currently displayed panel.

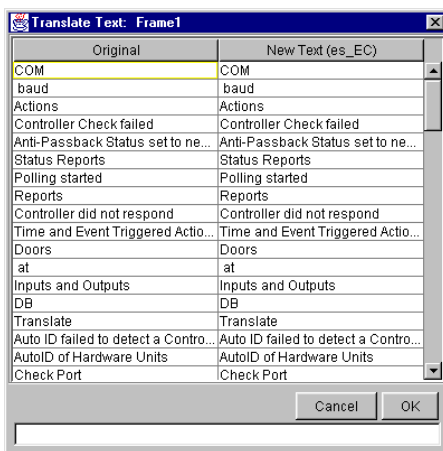
Other

This category includes text and messages that appear in message boxes and dialogs throughout the Software.

Calendar

This option allows translation of calendar text.

For **Main Frame** and **Other** categories, select a category to translate by clicking on the relevant icon. A **Translate Text Dialog** similar to that shown below is displayed.



Translate Text Dialog

The **Translate Text Dialog** shows the original text displayed in the left-hand column of the table. The translated text will appear in the right-hand column. Check the heading for the right hand column table, to ensure that the correct locale is displayed.

NOTE : *To sort a column in alphabetical order, double click the column header.*

To translate text :

- [1] Click in the relevant table cell in the right-hand column (or use arrow keys to navigate).
- [2] Type the desired translated text.
- [3] When all the changes have been made, press Enter to confirm the entries.
- [4] Click **Apply** to accept changes, or click **Cancel** to reject new changes.

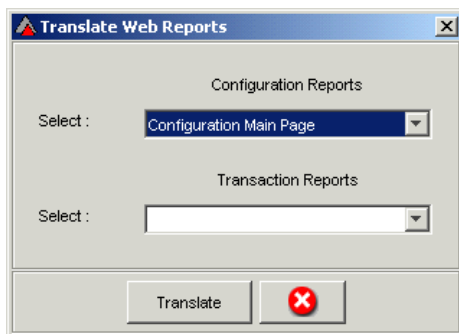
NOTE : DO NOT EDIT THE SAME CATEGORY TWICE IN A SESSION.

If changes need to be made, close the application and restart before making the changes. If you do edit more than once in a session, only the last translations entered are recorded permanently, and previous translation done in that session is overwritten with English text !

Translate Web Reports

- [1] To translate Web Reports, first **Choose Locale** as described in previous paragraphs.
- [2] Go to the **File** menu and select **Translate Web Reports**.
- [3] The **Translate Web Reports** dialog shown will be displayed.
- [4] Select the type of report required from either the **Configuration Reports** or the **Transaction Reports** combo box.

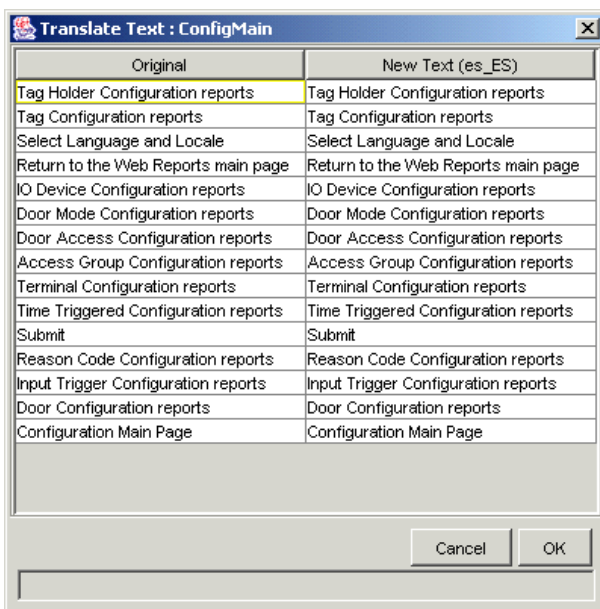
See next page



Translate Web Reports dialog

- [5] Click **Translate** to proceed with translation, or **Cancel** to abort.
- [6] If **Translate** is selected, the following dialog will be displayed.
- [7] Replace the English text in the right hand column with the equivalent translation.
- [8] Click **Apply** (i.e. **OK**) to Accept, or **Cancel** to escape without saving the changes.

NOTE : *Do not edit the same report twice in one session.*



Translate Main Configuration Page dialog

This concludes the System Configuration

CHAPTER 15 – DATABASE BACKUP AND RESTORE

GENERAL

The IXP200 Software provides the facility to backup and restore the database files.

Two types of backup are possible, namely an automatic scheduled backup or an immediate manually-selected backup.

Why Backup?

A Backup is a full copy of the database at a point in time. The purpose of the backup is for recovery if the current database should become corrupt and not able to be repaired.

It is a good practice to keep a set of up to date backups. The best way to do this is to schedule backups to be executed automatically.

File Extensions

NOTE: *All database files from V4.0 onwards have an fdb extension instead of a gdb extension. The extension is irrelevant for either the InterBase or the Firebird database management System. The reason for the change is to prevent the Microsoft Operating System from interfering and making a copy of the gdb file each time a change is made. This slows down the operation of the IXP200 Software too much. Backup is best left under the control of the System administrator.*

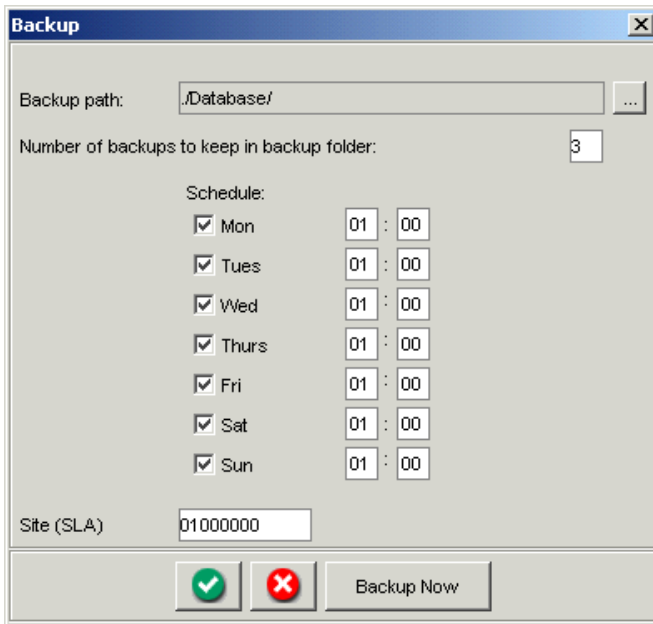
Backup files have the extension gbk that is necessary to identify the file as a backup. However the IXP200 backup process immediately restores the gbk file to a valid database file **so that it is ready for use**. If the current database file becomes corrupt, it can be deleted or renamed and the backup file can be renamed to the original filename, e.g. Proxette.fdb, so that it is immediately recognised by all the properties files.

The restored backup files are named for the date, the time, and the original database filename, e.g. 2003-10-01_140103Proxette.fdb.


BACKUPS

Scheduled Automatic Backup

- [1] Select **Backup** from the **File** Menu to schedule or execute a backup of the database. The Backup dialog shown will be displayed.

**Backup dialog**

- [2] By default the backup path is the IXP200\database folder but this can be changed.

- [3] To change the Backup path, click on the  Icon, and select the required path.

- [4] The number of backups to be retained must also be specified. Set the required number of backups to be retained by typing this number into the box provided (3 in this example) next to Number of backups to be kept in backup folder.

NOTE : *Backups made prior to this number of backups will be discarded by the System. The default is 3, meaning that only the latest 3 backups are retained, and the next backup will overwrite the oldest of these.*

- [5] Select the days of the week on that the backup operation is required by deleting the ticks from days on that backup is not required.
- [6] Set the time of day for each selected day at that backup is required by typing in the time in the boxes provided (in 24-hour clock format).
- [7] Leave the Site Logical Address (SLA) as the default 01000000.

- [8] Once the parameters have been selected, click **Apply** to save and close the dialog. Alternatively click **Cancel** to close and ignore changes to the parameters.
- [9] Automatic Backup can be scheduled to run at a specific time on one or more days of the week. The System defaults to a daily backup at 1 a.m. (01:00).
- [10] The backup will take place automatically at the scheduled times. A status message will be displayed in the Status Bar at the bottom of the main frame when backup is in progress.

Immediate Backup

- [1] Click on **Backup Now** to perform a backup independent of the preset scheduled times.
- [2] Observe the Status Bar in the main frame for messages.

IMPORTANT NOTE:

Please note that backup executes within IXP200 so the IXP200 application must be running at this time for the backup to execute.

The default backup folder is IXP200\database but another folder can be selected.

USER'S NOTES

USER'S NOTES

CHAPTER 16 – ARCHIVE

GENERAL

The IXP200 Software provides the facility to archive data in the database.

CREATING AN ARCHIVE

To create an Archive of the database, use the separate Archive utility in the IXP200 folder. A shortcut will have been created in the Programs menu. Log-on as the System Administrator when prompted.

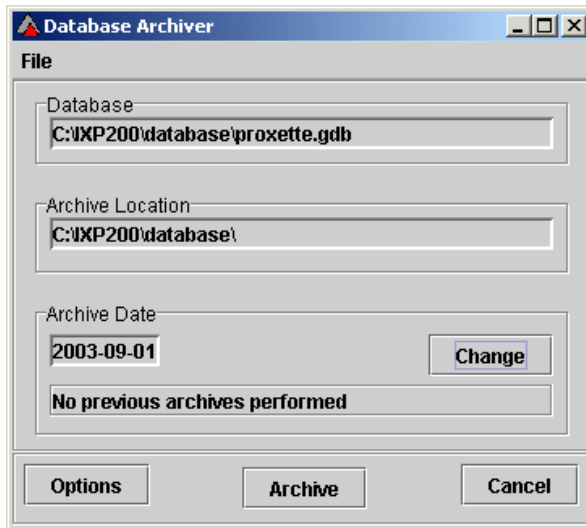
- [1] Close all other applications that may be accessing the database, e.g. IXP200, Graphics Designer, etc.
- [2] Click on the Archive short-cut. The Archive Password dialog shown will be displayed.



Archive Password dialog

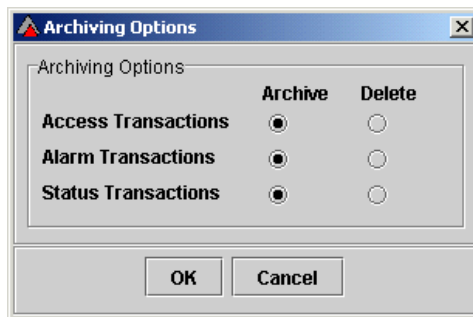
- [3] Enter the Administrator name and password, and click **OK**. The **Database Archiver Main Frame** will be displayed. This frame displays the current database name and the archive folder, that cannot be changed.

See next page



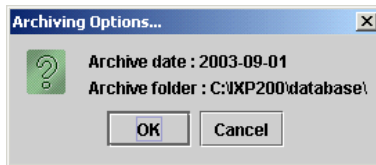
Database Archiver Main Frame

- [4] The date for the Archive must be selected by clicking on **Change** and selected the required date from the calendar displayed; the default is one month before the current date. All transactions prior to that date will be removed from the current database and written to the Archive database. If a previous archive exists, then it will contain data prior to its date and the new archive will contain data from the last archive up to the new date.
- [5] Click **Options** to see the **Archiving Options** dialog. The type of transaction to be archived may be specified. By default all types are archived.



Archiving Options dialog

- [6] Select the **Delete** option if transactions must be deleted from the current database and not written to the archive database, in other words if they are no longer required at all.
- [7] Click **OK** to save the changed options and close the **Archiving Options** dialog.
- [8] Alternatively, click **Cancel** to ignore changes and close the dialog.



Archiving Options..... dialog

- [9] Click **Archive** to start executing the archiving process. Close the application and check the log file on completion for any errors.

NOTES :

1. *The Archive files are named for the date only, with an fdb extension, e.g. 20030509.fdb.*
2. *A log file is created for each Archive, e.g. Archive 20030509.log. in the IXP200\log folder.*

END OF SECTION

INDEX

- Access Group, 83, 84, 85, 86, 89, 90, 91, 101, 105
- Access Pattern, 85, 86, 87, 88, 89, 90
- Adhesive Labels, 108
- Administrator, 83, 92
- alarm, 92, 124, 125, 129
- Anti-Passback, 130, 135
- APB, 83, 91, 92, 100, 102, 104, 130, 135
- APB Zone, 102
- BACKUP, 147
- Base Plan, 124
- calendar, 115, 144
- card printing, 99, 106
- card tag, 106
- Choose Locale**, 141, 142, 145
- communication, 136
- Configuration**, 85, 106, 114, 116, 118, 119, 120, 135, 145, 146
- credit card tag, 99, 122
- default, 107, 119, 127, 142, 145, 148, 149
- Department**, 93, 97, 98, 108
- Designer Module, 124
- Door Mode, 83, 91
- Emergency Open/Close Doors, 136
- Employee Number**, 97, 106
- end date, 113
- Event Triggered Actions, 117
- Expiry Date**, 100, 105
- field, 86, 87, 88, 93, 98, 100, 101, 102, 104, 105, 106, 113, 115, 116, 119, 142
- fingerprint*, 91, 100, 102
- fixed address, 138, 139
- Floor Plan, 124, 125, 126, 127, 129
- Graphics, 124, 126, 128, 129, 135
- Icon, 83, 92, 95, 98, 113, 115, 124, 127, 148
- LCD, 117, 118, 119
- lift (elevator)*, 83, 88
- Localisation, 141
- Logical Address, 136, 148
- Message**, 101, 105, 117, 118, 119, 138
- Normal Tag, 91
- Operator, 105, 106
- PAC, 102
- password, 141
- PC, 92, 108, 135, 145
- Personal Access Code, 102
- photograph, 94, 95
- PIN*, 94, 102
- Remote Reader, 131
- Runtime Module, 124
- Sagem*, 91
- Security Level**, 84, 86
- site, 85, 94, 114, 138
- slim tag, 102
- Start Date, 100, 104, 105, 114, 115
- Supervisor, 91, 92
- SUPERVISOR, 83
- Supervisor level tag, 91
- system database, 85, 89, 94, 114, 118, 122
- tag number*, 99, 106
- Tagholder, 83, 92, 93, 94, 97, 99, 100, 101, 102, 104, 105, 106, 108, 109, 110, 111, 112, 117, 122, 127, 128, 135
- templates, 122, 145
- Terminal, 88, 91, 102, 125, 136, 137, 138
- Transaction Buffer, 135, 139
- translation, 141, 142, 143, 144, 145, 146
- UHF Tag**, 102
- Visitor, 91
- Web Reports, 145, 146
- Zone, 102

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_sys-swm-en-12 Section 3B.doc
------------------	----------	-----------	--

IXP200 SOFTWARE USER MANUAL

SECTION 4

System

REPORTS

SECTION 4 – REPORTS

CONTENTS

REPORTS OVERVIEW.....	5
GENERAL.....	5
PASSWORD CONTROL OF REPORTS	5
ACCESSING AND USING THE REPORTS FACILITY.....	6
DEFINING PARAMETERS IN A REPORT PAGE.....	8
EXPORTING REPORTS TO EXCEL	9
REPORT DESCRIPTIONS	9
ADMINISTRATOR REPORTS.....	9
Archive Selector	9
Configuration Reports.....	10
DOOR AND ACCESS GROUP CONFIGURATION REPORTS.....	12
Common Report Screen Buttons.....	12
Access Group Configuration Report	13
Door Access Configuration Report	14
Door Configuration Report	15
Door Mode Configuration Report	16
Terminal Configuration Report	17
Reader Configuration Report.....	18
INPUTS AND TIME TRIGGERED CONFIGURATION REPORTS	19
IO Device Configuration Report.....	19
Input Triggered Action Configuration Reports	20
Time Triggered Configuration Report.....	21
Tag Configuration Report.....	22
Tagholder Configuration Reports	23
TRANSACTION REPORTS.....	24
Common Report Screen Buttons.....	24
Access Report	24
Alarm Report	30
Status Report.....	31
PERSON INFORMATION REPORTS	32
Hours Worked in APB Report	32
Person Access Pattern Report	33
Person Report.....	34
Zone Occupancy Report.....	36
Hours worked in APB Zone Time Sheet Report	37
Department Time Sheet Report.....	39
GENERAL SYSTEM REPORTS	41
Holiday Report	41

Reason Code Report.....43

INDEX.....44

REPORTS OVERVIEW

GENERAL

The IXP200 Software includes the facility to display and/or print copies of various Reports. These reports are presented as web pages. These reports fall into four categories, namely Administrator Reports, Transaction Reports, Person Information Reports and General System Reports.

Administrator Reports cover Archives and System Configuration. The Configuration information is only accessible to the database Administrator using the correct log-on name and password.

Transaction Reports are available to any User, and cover access, alarm and Terminal transactions.

Person Information Reports are available to any User, and cover access patterns and zone and APB occupancy for individual Tagholders.

General System Reports are available to any User, and provide Holiday and Reason Code status information.

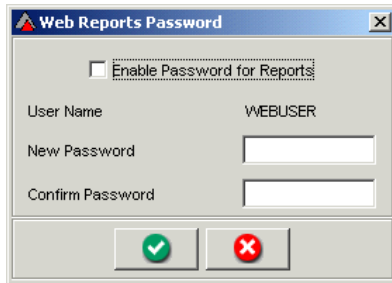
This section of this manual contains information about the type of Reports that the user can access. The selection of reports is performed using a Web Browser.

PASSWORD CONTROL OF REPORTS

The Administrator may enforce password control of reports. One global password can be defined which gives access to all Reports except the Configuration Reports, which are always accessible only with the Administrator password. By default, passwords are disabled.

To define and enable or disable the global password, select **Web Reports Password** from the IXP200 **File** menu. The Web Reports Password dialog will be displayed (see the next illustration).

See next page



Web Reports Password dialog

If a new global password is required :

- [1] Enter the password.
- [2] Enter the password again to confirm it.
- [3] To enable the password, ensure that the box is checked.
- [4] To disable the password, ensure that the box is unchecked.
- [5] Click **Apply** to save and exit, or **Cancel** to exit without saving.


ACCESSING AND USING THE REPORTS FACILITY

NOTES :

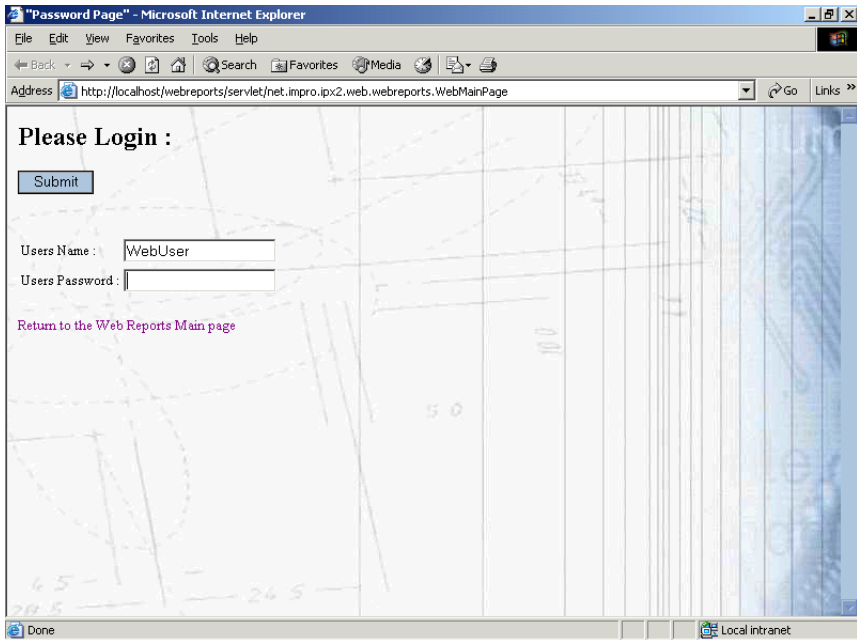
1. *The IXP200 Software must be running in order to access Web Reports.*
2. *The Web Reports can be accessed from any machine (PC) on the same LAN as the IXP200 Host PC.*

The Web Reports facility can be accessed in several ways as follows :

Method 1 – Using the Speed Button in the Toolbar

- [1] Start the IXP200 program.
- [2] A shortcut to the Web Reports is provided by the  icon.
- [3] A log-on dialog (see next graphic) will be displayed if Web Reports password is enabled.

See next page



Web Reports Log-on dialog

- [4] The **Web Reports for IXP200** screen shown will be displayed.

Method 2 – Using the Menu

- [1] Select Reports from the Main Top Menu.
- [2] Select Web Reports.
- [3] Start the IXP200 program.
- [4] A log-on dialog will be displayed if Web Reports password is enabled.
- [5] The Web Reports for IXP200 screen shown will be displayed.

Method 3 – Using the Browser (e.g. InterNet Explorer or Netscape)

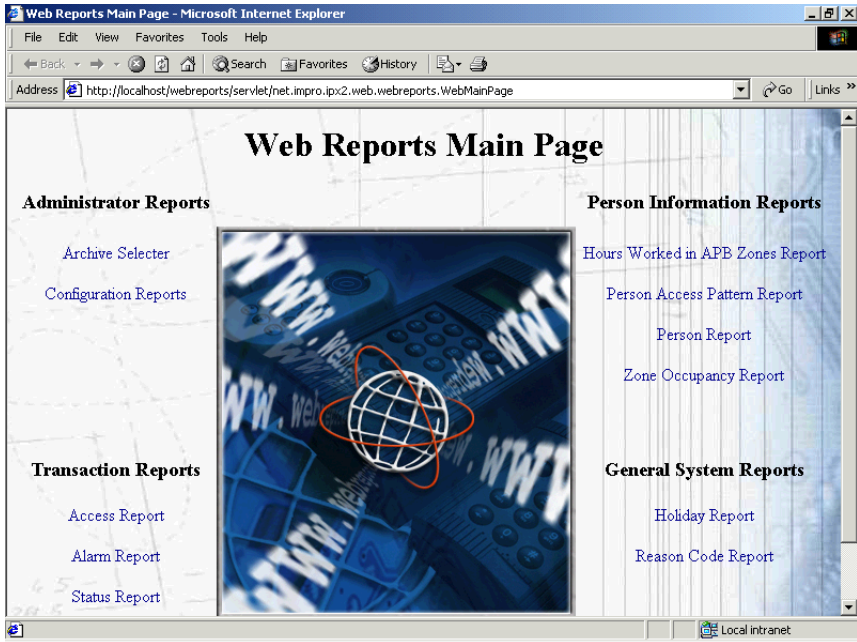
- [1] Start the IXP200 program.
- [2] If you are viewing the Reports on any other PC on the same LAN as the Host PC, start the Web Browser and type the following URL : <http://machinename/index.html>, where "machinename" is the name of the Host PC (the PC running the IXP200 application). Click Go.

NOTE : *If you are viewing the Reports on the Host PC, start the Web Browser*

and type the address <http://localhost/index.html> and click **Go**.

[3] A log-on dialog will be displayed if Web Reports password is enabled.

[4] The Web Reports for IXP200 screen shown will be displayed.



Web Reports for IXP200 Main Page

DEFINING PARAMETERS IN A REPORT PAGE

- [1] Once a Report page has been accessed, it is generally necessary to define the required parameters. Typically, this means :
- [2] Select the item of interest by clicking on its title or making a selection from a combo box as required.
- [3] Define the time period for the report by typing in the required dates.
- [4] Click **Submit** to display the required information.
- [5] Once the report is displayed, some report columns can be sorted by clicking on the required column heading. To determine which columns can be sorted, move the cursor across the column headings. The columns which can be sorted will be indicated by a hand icon.

EXPORTING REPORTS TO EXCEL

A Report may be exported to CSV (Comma Separated Values) format and then opened by Excel. This is easily done as follows :

- (a) Click the button "Export Report (CSV)" once the required report screen is displayed.
- (b) Supply a filename and path when prompted, to save the report to a CSV file.

REPORT DESCRIPTIONS

The reports which can be generated by the System are described below, with details provided (where necessary) about navigating through each type of report.

ADMINISTRATOR REPORTS

Administrator Reports cover Archives and System Configuration. The Configuration information is only accessible to the database Administrator using the correct log-on name and password.

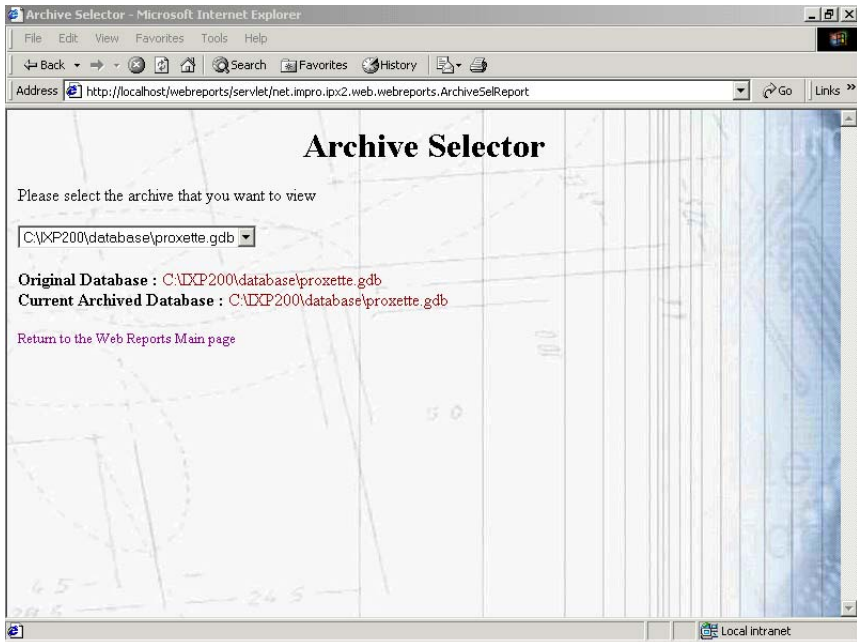
Archive Selector

The Archive Selector allows you to view archived databases.

To access this :

- [1] Click on **Archive Selector** in the Main Page.
- [2] Select the database you wish to view using the combo box. (Archives are named for the date only, with an fdb extension, e.g. 20030626.fdb).
- [3] Reports will then be processed based on the selected archive database.
- [4] Switch back to the current database when you have finished viewing reports on the archived database.

See next page



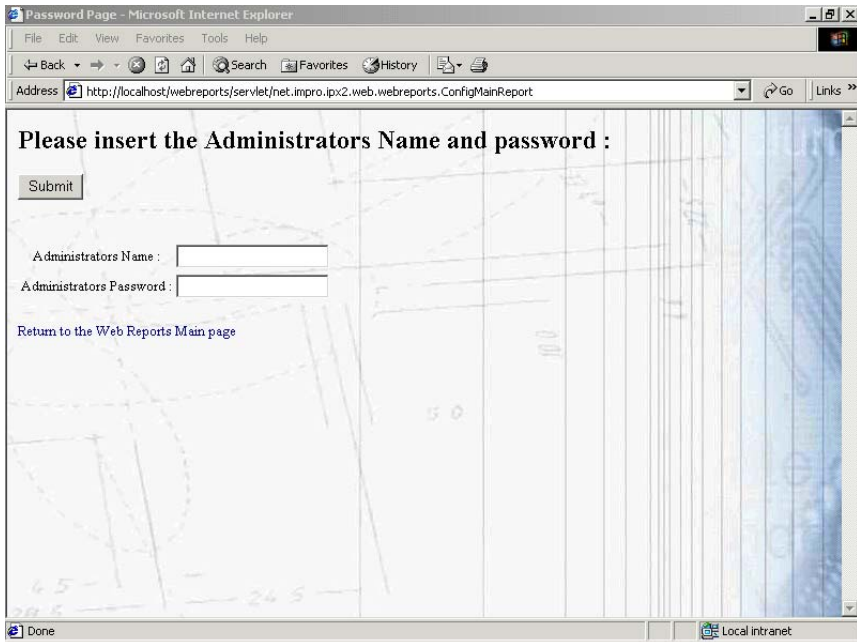
Archive Selector page

Configuration Reports

To access Configuration Reports :

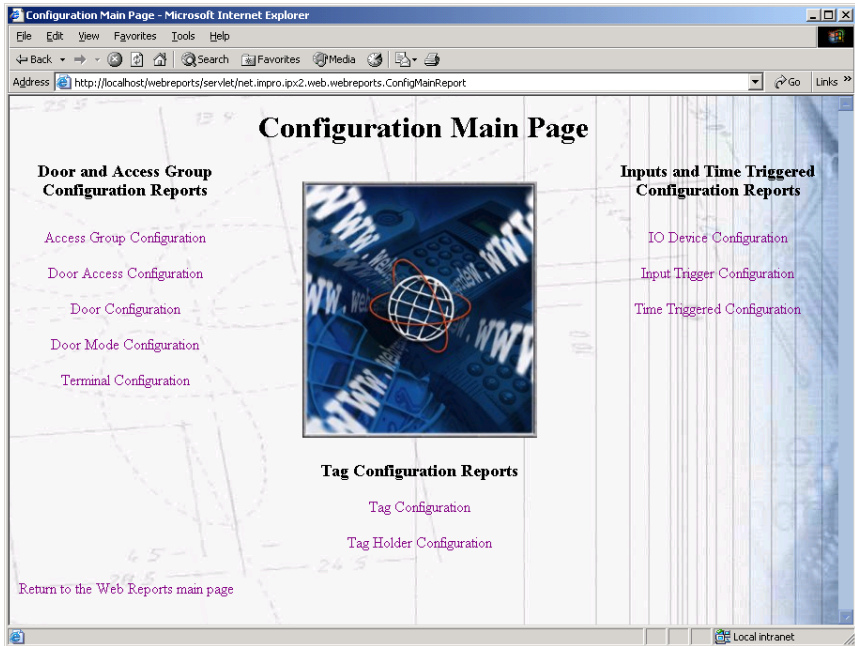
- [1] Click on **Configuration Reports**.
- [2] The **Password Page** shown will be displayed.
- [3] Enter the Administrator Password.
- [4] Click on **Submit**.
- [5] The **Configuration Main Page** shown will be displayed. This page lists the various types of Configuration Report available.

The Configuration Reports are described in the following paragraphs.



Password Page

See next page



Configuration Main Page [Part]

Configuration Reports are divided into Door and Access Group Configuration Reports, Input and Time Triggered Configuration Reports and Tag Configuration Reports.

DOOR AND ACCESS GROUP CONFIGURATION REPORTS

Door and Access Group Configuration Reports include :

- Access Group Configuration Reports,
- Door Access Configuration Reports.
- Door Configuration Reports.
- Door Mode Configuration Reports.
- Terminal Configuration Reports.

Common Report Screen Buttons

Each Report screen in this group includes two common buttons. The operation of these buttons is as follows :

- Click on **Submit** to update the displayed Report information.

- Click on **Export Report (CSV)** to export the displayed Report in CSV (Comma Separated Value) format for MS Excel and similar programs.

Access Group Configuration Report

No.	Name	Pat No.	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol	Start Time	Duration	Access Door	Access Floor
1	Admin	1		*	*	*	*	*			08:00	12:00 hrs	1, 2, 6,	1, 2, 3, 4,
2	Lab Staff	1		*	*	*	*	*			07:00	12:00 hrs	1, 2, 3, 4, 6,	
		2							*	*	08:00	04:00 hrs	3, 4, 6,	
3	Supervisor	1	*	*	*	*	*	*	*	*	00:00	24:00 hrs	1, 2, 3, 4, 5, 6,	2, 3, 4, 1,

Access Group Configuration Report

This report shows the Access Groups defined for the System with the time and place for which access is allowed for each group.

See next page

Door Access Configuration Report

Door Access Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

Door : **Car Park**
Amount of people allowed : 6

Door Names :	Name	Access Group	Pat No.	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol	Start Time	Duration
Accounts Door	John Walton	Admin	1		*	*	*	*	*			08:00	12:00
Car Park	James Nigel Haines	Admin	1		*	*	*	*	*			08:00	12:00
Laboratory	Clara Calisto	Supervisor	1	*	*	*	*	*	*	*	*	00:00	24:00
Lifts	William Newton	Supervisor	1	*	*	*	*	*	*	*	*	00:00	24:00
Main Door	Juliet Summerfield	Admin	1		*	*	*	*	*			08:00	12:00
Rear Door	Arturo Fettucini	Supervisor	1	*	*	*	*	*	*	*	*	00:00	24:00

[Return to the Configuration main page](#)

Door Access Configuration Report

Doors are listed on the left. Click a door to display a list of those people who are allowed access to the door, as well as details of the relevant access group.

See next page

Door Configuration Report

Door Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

Door No.	Door Name	APB	Zone	Armed	Door Pin	In Reader	Out Reader	Day	Mode
1	Main Door	Yes	1	No	456	01010103	01010107	Sunday	pac
								Monday	pac
								Tuesday	pac
								Wednesday	pac
								Thursday	pac
								Friday	pac
								Saturday	pac
								Holiday	pac
2	Lifts	No	---	No	0	01010109		Sunday	Weekend
								Monday	Weekday
								Tuesday	Weekday
								Wednesday	Weekday
								Thursday	Weekday
								Friday	Weekday
								Saturday	Weekend

Local intranet

Door Configuration Report

This report includes details of each door configuration, including the daily operating modes.

See next page

Door Mode Configuration Report

"Door Mode Configuration" - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://localhost/webreports/servlet/net.impro.ipx2.web.webreports.DoorModeConfigReport> Go Links

Door Mode Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

No.	Start Time	End Time	Mode	Pin	Reason	Dual Tag	Record	Alarm Denied	LED Mode
DMP Mode 1 : Default Tag Mode									
1	00:00	24:00	Tag	No	No	No	Yes	No	Red
DMP Mode 2 : Weekday									
1	00:00	05:00	Supervisor Unlock	No	Both	No	Yes	Yes	Red
2	05:00	17:00	Tag	No	No	No	Yes	No	Flashing Green
3	17:00	24:00	Supervisor Unlock	No	Both	No	Yes	No	Off, Blink Red
DMP Mode 3 : Holiday									
1	00:00	24:00	No Entry	No	No	No	Yes	Yes	Red, Blink Off
DMP Mode 4 : Weekend									
1	00:00	06:00	Supervisor Unlock	No	No	Entry	Yes	No	Off, Blink Red
2	06:00	17:00	Tag	No	No	No	Yes	No	Green
3	17:00	24:00	Supervisor Unlock	No	No	Entry	Yes	No	Off, Blink Red
DMP Mode 5 : pac									
1	00:00	24:00	Personal Access Code Mode	No	No	No	Yes	No	Green, Blink Off

Local intranet

Door Mode Configuration Report

This report provides details of all Door Modes which have been defined for the System.

See next page

Terminal Configuration Report

Terminal Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

Logical Address	Fixed Address	Enabled	Type	Type Description
01010101	004C5485	Yes	MR	ImproX Micro Remote
01010102	000F43B0	Yes	I16	ImproX 16 Channel Input Terminal
01010103	004C51EE	Yes	KHR	ImproX Harsh Environment Keypad Remote
01010104	004C555B	Yes	DL	ImproX LCD Keypad Terminal (Non-programmable)
01010105	004C5459	Yes	MR	ImproX Micro Remote
01010106	004C5469	No	MR	ImproX Micro Remote
01010107	004C546B	No	MR	ImproX Micro Remote
01010108	004C546F	Yes	MR	ImproX Micro Remote
01010109	004C5474	Yes	MR	ImproX Micro Remote
0101010A	004C5358	Yes	O16	ImproX 16 Channel Output Terminal
0101010B	004C5480	Yes	KR	ImproX Keypad Remote
0101010C	004C547E	Yes	MHR	ImproX Harsh Environment Micro Remote

[Return to the Configuration main page](#)

Done Local intranet

Terminal Configuration Report

This report provides a list of all Terminals identified by the Controller during Auto-ID. It shows the type and the addresses for each Terminal.

See next page

Reader Configuration Report

Reader Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

Door Names	Main Door		Rear Door		Laboratory		Accounts Door	
	In Reader	Out Reader	In Reader	Out Reader	In Reader	Out Reader	In Reader	Out Reader
Logical Address	01010103	01010107					01010101	01010108
Strike Duration (0.1s)	40	40					40	40
Open Duration (s)	0	0					0	0
Dos Input Type	Normal	Normal					Normal	Normal
Output Mode	None	None					None	None
Device Address	00000000	00000000					00000000	00000000
TA	False	False					False	False
Dos Mode	N/C	N/C					N/C	N/C
RTE Mode	N/O	N/O					N/O	N/O
On Allowed Tag								
Buzzer Volume	Soft	Loud					Loud	Loud
Buzzer Duration (0.1s)	7	7					20	20

Reader Configuration Report

This report provides a list of configuration information for each Reader in the System, including the indications given when an Allowed Tag or a Denied Tag is presented.

See next page

INPUTS AND TIME TRIGGERED CONFIGURATION REPORTS

IO Device Configuration Report

I/O Device Configuration :

[Return to the Configuration main page](#)

Devices Available

[Configured Input Devices](#)
[Configured Output Devices](#)

I/O Device Address	I/O Device Name	I/O Device Description
01010102	Bldg Management	ImproX 16 Channel Input Terminal
0101010A	Lifts	ImproX 16 Channel Output Terminal

Configured Output Devices

Device Name :	Lifts	Fixed Address :	004C5358
Logical Address :	0101010A	Unit Name :	016
Unit Description :	ImproX 16 Channel Output Terminal		

IO Device Configuration Report

This report lists configuration information for each Input and Output device in the System.

See next page

Input Triggered Action Configuration Reports

Input Triggered Action Configuration :

[Return to the Configuration main page](#)

No.	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol	Start Time	Duration	Trigger Inputs	Action Type
7	Activate door alarm	*	*	*	*	*	*	*	*	00:00	24:00	Door Forced (closed)	Relay
9	Switch on Emerg Gen		*	*	*	*	*	*		05:00	17:00	Emerg generator (closed)	Relay

[Return to the Configuration main page](#)

Done Local intranet

Input Triggered Action Configuration Report

This report provides a list of all monitored inputs, the time periods during which they are monitored, the trigger condition and the type of action that follows each trigger.

See next page

Time Triggered Configuration Report

Time Triggered Action Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

No.	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol	Trigger Time	Action Time
1	Switch board to night service		*	*	*	*	*			17:00	Relay
2	Switch board to day service		*	*	*	*	*			07:45	Relay

[Return to the Configuration main page](#)

Local intranet

Time Triggered Action Configuration Report

This report provides a list of Time Triggered Actions and the times at which they have been configured to occur.

See next page

Tag Configuration Report

Tag Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

Tag Code	Owner Name	Department	Level	Type	Start Date	Expiry Date	Suspended	Access Group
*****	Juliet Summerfield	Admin	Normal	Personal Access Code	Date N/A	Date N/A	No	Admin
208038343237	James Nigel Haines		Visitor	Slim Tag (5 bytes)	Date N/A	Date N/A	No	Admin
208038347205	John Walton	Laboratory	Normal	Slim Tag (5 bytes)	2001/12/10	2005/12/10	No	Admin
208038349100	William Newton	Admin	Administrator	Slim Tag (5 bytes)	2002/05/01	2005/12/31	No	Supervisor
208038350421	Arturo Fettucini	Admin	Administrator	Slim Tag (5 bytes)	2003/06/13	2008/06/30	No	Supervisor
208038354551	Clara Calisto	Admin	Supervisor	Slim Tag (5 bytes)	2001/12/10	2005/12/10	No	Supervisor

[Return to the Configuration main page](#)

Tag Configuration Report

This report provides a list of all Tags issued, together with the Access Group which has been assigned to each Tag.

Data can be sorted by clicking on the appropriate column heading.

See next page

Tagholder Configuration Reports

Tag Holder Configuration :

Submit Export Report (CSV)

[Return to the Configuration main page](#)

Emp No.	First Name	Last Name	Department	Company	Address	Tag Code	Tag Start	Tag Expiry
	Arturo	Fettucini	Admin	Excel Products	1332 West Arbuckle, Fairmont	208038330421	2003/06/13	2008/06/30
	Clara	Calisto	Admin	Excel Products	77 Shaw Avenue, Mountain View	208038334551	2001/12/10	2005/12/10
	James Nigel	Haines		Acme Electrical	c/o Acme Electrical, Lakeside Drive, Cascade	208038343237	Date N/A	Date N/A
	John	Walton	Laboratory	Excel Products	13 Fairway, Newport	208038347205	2001/12/10	2005/12/10
	Juliet	Summerfield	Admin	Excel Products	7 Kingsfield, West Fleetwood	*****	Date N/A	Date N/A
	William	Newton	Admin	Excel Products	339 Staring Crescent, McGilucuddy Street, Overton	208038349100	2002/05/01	2005/12/31

[Return to the Configuration main page](#)

Done Local intranet

Tagholder Configuration Report

This report lists the Tagholders and the Tag (or Tags) assigned to each of them.

Data can be sorted by clicking on the appropriate column heading.

See next page

TRANSACTION REPORTS

The various Transaction Reports are selected from the Web Reports Main Page by clicking on the title of the report required.

Common Report Screen Buttons

Each Report screen in this group includes two common buttons. The operation of these buttons is as follows :

- Click on **Submit** to update the displayed Report information.
- Click on **Export Report (CSV)** to export the displayed Report in CSV (Comma Separated Value) format for MS Excel and similar programs.

Access Report

Access Report

[Return to the Web Reports Main page](#)

Main Filters

Date from to

Daily Time from to (24 Hour Clock)

Person

Location :

Other Filters

☐ Department : ☐ Tag No. :

☐ Event Type : ☐ Reason Code :

Date Filter : 2003/07/17 to 2003/07/17

Time Filter : 00:00:00 to 23:59:59

Access Report with no filter selected

Access Reports can provide various details of access transactions within the System. The type of information required in an Access Report can be defined by selecting one or more types of filter. The filters permit selection of information in the categories described in the next few paragraphs.

There are two categories of filters, namely **Main Filters** and **Other Filters**.

The Main Filters (i.e. **Date/Time**, **Person** or **Location**) are those most commonly used.

The Other Filters can be used separately or Multiple filters can be used to generate more specific report information as described under **The Use of Multiple Filters**.

The screenshot shows a web browser window titled "Access Report - Microsoft Internet Explorer". The address bar shows "http://localhost/webreports/servlet/net.impro.ipx2.web.webreports.AccessReport". The form contains the following elements:

- Daily Time from**: 00:00:00 **to**: 23:59:59 (24 Hour Clock)
- Person**: Arturo Fettucini (dropdown menu)
- Location**: (empty dropdown menu)
- Other Filters**:
 - ☐ Department :
 - ☐ Event Type :
 - ☐ Tag No. :
 - ☐ Reason Code :
- Name Filter** : Arturo Fettucini
- Date Filter** : 2003/05/05 to 2003/07/17
- Time Filter** : 00:00:00 to 23:59:59

No.	Date	Time	Name	Department	Location	Event	Tag No.	Reason
61	2003/06/13	09:18:52	Arturo Fettucini	A dmin	Main Door	Allowed In	208038330421	
62	2003/06/13	09:44:17	Arturo Fettucini	A dmin	Main Door	APB Override In	208038330421	
63	2003/06/13	09:45:44	Arturo Fettucini	A dmin	Car Park	Allowed In	208038330421	
69	2003/06/13	09:49:30	Arturo Fettucini	A dmin	Main Door	APB Override In	208038330421	
72	2003/06/13	09:51:04	Arturo Fettucini	A dmin	Main Door	APB Override In	208038330421	
86	2003/06/13	10:36:17	Arturo Fettucini	A dmin	Main Door	APB Override In	208038330421	
22	2003/06/25	15:01:52	Arturo Fettucini	A dmin	Rear Door In	Allowed In	208038330421	

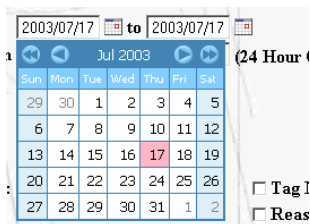
[Return to the Web Reports Main page](#)

Access Report with only Main Filters (Date and Person) selected

Date Filter

Selecting the Date Filter (Date from or Date to) will cause a drop-down calendar such as that shown next to be displayed.

See next page



Drop-down Calendar

The Date Filter default is the current date.

Select the month and year required, if necessary, by using the arrow icons. (The single arrows change the month, the double arrows change the year).

Lastly, select the day of the month required – this will close the calendar and transfer the selected date to the text box.

Time Filter

Using the Time Filter alone results in the Report including access information only for the time period defined, and on the current date.

The Time Filter default is 00:00:00 to 23:59:59.

See next page

Location Filter

NOTE : The term **Location** in this context means the same as **Door**.

Select any required **Location** from the drop down combo box. The report will reflect all transaction information for the default time period on the current date for that Location only.

If a report is required on all Locations, leave the **Location** field blank.

Click **Submit** to process the request.

Access Report - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://localhost/webreports/servlet/net.impro.ipx2.web.webreports.AccessReport> Go Links

Daily Time from 00:00:00 to 23:59:59 (24 Hour Clock)

Person

Location :

Other Filters

☐ Department : ☐ Tag No. : ☐ Reason Code :

☐ Event Type :

Date Filter : 2003/05/05 to 2003/07/17

Time Filter : 00:00:00 to 23:59:59

Location Filter : Main Door

No.	Date	Time	Name	Department	Location	Event	Tag No.	Reason
6	2003/06/11	14:34:45	John Walton	Laboratory	Main Door	Denied Tag Expired In	208038347205	
7	2003/06/11	14:34:52	Clara Calisto	Admin	Main Door	Denied Tag Expired In	208038354551	
8	2003/06/11	14:34:56	James Nigel Haines		Main Door	Allowed In	208038343237	
10	2003/06/11	14:35:10	Clara Calisto	Admin	Main Door	Denied Tag Expired In	208038354551	
11	2003/06/11	14:35:45	Clara Calisto	Admin	Main Door	Denied Tag Expired In	208038354551	
12	2003/06/11	14:35:47	James Nigel Haines		Main Door	Allowed In	208038343237	

Local intranet

Access Report – Location Filter activated

Person Filter

Select an individual Person from the drop-down combo box if required. A report will be generated including access information only for the Person selected, for the default time period on the current date.

To generate a Report on all Persons, leave the Person box blank.

Click **Submit** to process the request.

Department Filter

Check the Department check box, and select the Department required from the drop down list which appears. Using the Department filter alone generates a Report of access records for the Department selected only, for the default time period on the current date.

Tag No. Filter

Click the Tag No. check box, and type the required Tag Number into the text box which appears. Using the Tag No. Filter alone generates a Report of access records for the Tag No. selected only, for the default time period on the current date.

Event Type Filter

Click the **Event Type** check box, and select the required Event Type from the drop down list which appears. A Report will be generated for the event selected for the default time period on the current date.

If a report on all Event Types is required, leave the **Event Type** check box blank.

Reports can also be printed on **All Allowed Events** or **All Denied Events** by selecting these from the drop-down list.

Reason Filter

Click the **Reason** check box and select the required Reason from the drop-down list which appears. This generates a Report of access records for the Reason selected only, for the default time period on the current date.

If a report on all Reasons is required, leave the **Reason** check box blank.

The Use of Multiple Filters

Multiple Filters can be selected to more narrowly define the Access Report information displayed. An example is shown below where both Location and Person Filters have been selected.

NOTE : *Always click **Submit** again after defining a filter.*

See next page

Access Report - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <http://localhost/webreports/servlet/net.impro.ipx2.web.webreports.AccessReport> Go Links

Date from 2003/04/01 to 2003/07/17

Daily Time from 00:00:00 to 23:59:59 (24 Hour Clock)

Person Arturo Fettucini

Location : Main Door

Other Filters

☐ Department : ☐ Tag No. :
☐ Event Type : ☐ Reason Code :

Name Filter : Arturo Fettucini
Date Filter : 2003/04/01 to 2003/07/17
Time Filter : 00:00:00 to 23:59:59
Location Filter : Main Door

No.	Date	Time	Name	Department	Location	Event	Tag No.	Reason
61	2003/06/13	09:18:52	Arturo Fettucini	Admin	Main Door	Allowed In	208038350421	
62	2003/06/13	09:44:17	Arturo Fettucini	Admin	Main Door	APB Override In	208038350421	
69	2003/06/13	09:49:30	Arturo Fettucini	Admin	Main Door	APB Override In	208038350421	
72	2003/06/13	09:51:04	Arturo Fettucini	Admin	Main Door	APB Override In	208038350421	
86	2003/06/13	10:36:17	Arturo Fettucini	Admin	Main Door	APB Override In	208038350421	

[Return to the Web Reports Main page](#)

Local intranet

Access Report with Multiple Filtering

See next page

Alarm Report

Alarm Report

Submit Export Report (CSV)

[Return to the Web Reports Main page](#)

Date from 2003/06/02 to 2003/07/30

Daily Time from 00:00:00 to 23:59:59 (24 Hour Clock)

Date Filter : 2003/06/02 to 2003/07/30

Time Filter : 00:00:00 to 23:59:59

Date	Time	Source	Event	Tag Holder	Acknowledged?	Ack Date	Ack Time	Ack By
2003/06/06	14:31:27	(00)	Tables Initialised		Yes	2003/06/13	15:17:51	SYSDBA
2003/06/07	16:36:07	Lifts (09)	Anti Tamper		Yes	2003/06/13	15:17:51	SYSDBA
2003/06/13	09:46:26	Lab In (04)	Anti Tamper		Yes	2003/06/13	15:17:51	SYSDBA
2003/06/25	11:07:25	Lifts (09)	Anti Tamper		No	Date N/A	Time N/A	

[Return to the Web Reports Main page](#)

Local intranet

Typical Alarm Report

An Alarm Report displays the details of all alarms that were activated during the specified time period.

A sample Alarm Report is shown. The Date filter has been selected in this example. Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).

If no filter is selected, the date defaults to the current date, and the time period to 00:00 to 23:59:59.

See next page

Status Report

Status Report

Submit Export Report (CSV)

[Return to the Web Reports Main page](#)

Date from 2003/06/02 to 2003/07/31

Daily Time from 00:00:00 to 23:59:59 (24 Hour Clock)

Date Filter : 2003/06/02 to 2003/07/31

Time Filter : 00:00:00 to 23:59:59

Date	Time	Source	Source Terminal Address	Event	Operator
2003/06/06	14:31:30	Controller	01010100	Power Up	
2003/06/06	14:34:08	Controller	01010100	Power Up	
2003/06/10	11:45:43	Controller	01010100	Power Up	
2003/06/13	09:47:39	Controller	01010100	Power Up	
2003/06/13	09:52:08	Controller	01010100	Power Up	
2003/06/13	10:14:46	Controller	01010100	Power Up	
2003/06/13	10:22:21	Accounts Door	01010108	Power Up	
2003/06/13	10:22:22	Rear Door In	0101010B	Power Up	
2003/06/13	10:22:22	Car Park	0101010C	Power Up	
2003/06/13	10:22:22	Accounts Door	01010101	Power Up	

Typical Status Report

The Status Report provides a record of the Status Events at any of the System's Terminals and at the Controller (i.e. the System status) for the time period specified, for example Terminal Timeout, Power Up, etc.

Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).

If no Date or Time filter is selected, the date defaults to the current date, and the time period to 00:00 to 23:59:59.

See next page

PERSON INFORMATION REPORTS

Hours Worked in APB Report

Hours Worked in APB Zones Report

Submit Export Report (CSV)

[Return to the Web Reports Main page](#)

Select Person: Clara Calisto

Date from: 2003/06/01 to 2003/06/30

Summary Only: ☐

Hours at Work (LastOut-FirstIn) : 00:00:00

Hours Worked within APB Zones : 00:00:00 *** Error in processing! ***

Date Filter : 2003/06/01 to 2003/06/30

Name	Date	Time	Event	Terminal	Zone	Reason
Clara Calisto	2003/06/11	15:34:40	Allowed In	Main Door	1	
Clara Calisto	2003/06/13	09:14:40	APB Override In	Main Door	1	

[Return to the Web Reports Main page](#)

Hours Worked in APB Report Page

The Hours Worked in APB Zone Report provides a report of the hours that a specified Tagholder spent at work and the hours he/she spent within APB Zones. These details are provided for a period which may be selected by the viewer.

The required person must be selected from the **Person** combo-box.

Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).

A summary report may be selected by clicking on the Summary box.

See next page

Person Access Pattern Report

Person Access Pattern Report

Submit Export Report (CSV)

[Return to the Web Reports Main page](#)

Select Person : William Newton

Date from 2003/06/01 to 2003/06/30

Summary Only : ☐

Date Filter : 2003/06/01 to 2003/06/30

Date	Time In	Time Out	Hours	Errors
2003/06/11	14:42:48	16:12:26	01:29:38 (1.49)	
2003/06/12	16:08:21	16:09:00	00:00:39 (0.01)	
2003/06/13	09:16:09	09:16:09	00:00:00 (0.0)	*1 *0

Average Time In : 15:25:34 (2 Records)
 Average Time Out : 16:10:43 (2 Records)
 Average Hours at Work : 00:30:05 (3 Records)
 Total Hours at Work : 01:30:17 (1.50 Hours)

Person Access Pattern Report

This report details the Access Pattern of a specified Person for a specified period.

The required person must be selected from the **Person** combo-box.

Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).

See next page

Person Report

Person Report

Submit Export Report (CSV)

[Return to the Web Reports Main page](#)

Select Person: Juliet Summerfield

Date from 2003/06/01 to 2003/07/31

Personal Details	
Sequence Number :	5
First Name :	Juliet
Last Name :	Summerfield

Company Details	
Company :	Excel Products
Department :	Admin
Employee ID :	

Transaction Report :

Date Filter : 2003/06/01 to 2003/07/31

Sample Person Report

The Person Report provides information about a selected Tagholder, including his/her access transactions over a selected period.

The required person must be selected from the **Person** combo-box.

Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).

A sample report is shown in the two illustrations – the second shows the lower part of the report containing the transaction details.

See next page

"Person Report" - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media Print

Address <http://localhost/webreports/servlet/net.impro.ipx2.web.webreports.PersonReport> Go Links

Number :
First Name : James Nigel
Last Name : Haines

Company Details
Company : Acme Electrical
Department :
Employee ID :

Transaction Report :

Date Filter : 2003/06/02 to 2003/07/31

No.	Location	Event	Transaction Date	Transaction Time
8	Main Door	Allowed In	2003/06/11	14:34:56
12	Main Door	Allowed In	2003/06/11	14:35:47
17	Car Park	Allowed In	2003/06/11	14:47:05
19	Accounts Door	Denied Door Out	2003/06/11	14:47:31
22	Rear Door In	Denied Door In	2003/06/11	14:48:40
28	Lab Out	Denied Door Out	2003/06/11	15:31:07
32	Lab In	Denied Door In	2003/06/11	15:32:51
24	Main Door	Allowed In	2003/06/25	15:02:10
25	Accounts Door	Denied Door In	2003/06/25	15:02:49

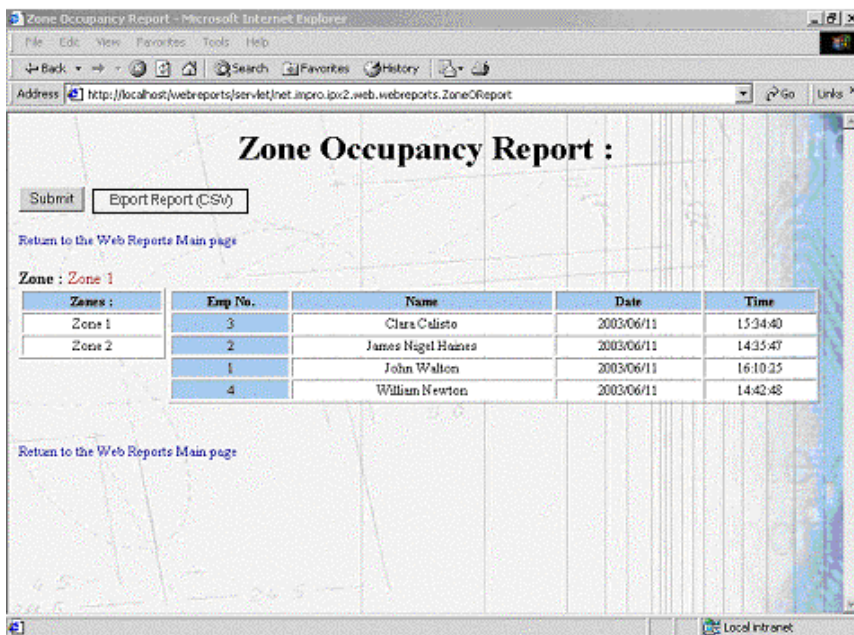
[Return to the Web Reports Main page](#)

Local intranet

Person Report : Transaction Report section

See next page

Zone Occupancy Report



Zone Occupancy Report

This Report provides information about the Tagholders in a specified Zone at the time the Report is generated, with the time of entry into the Zone.

See next page

Hours worked in APB Zone Time Sheet Report

Hours Worked in APB Zones Report

[Return to the Web Reports Main page](#)

Select Person:

Date from: **to:** [Summary Only](#)

Hours at Work (LastOut-FirstIn) : 00:27:53
Hours Worked within APB Zones : 00:13:26

Date Filter : 2006/02/01 to 2006/02/24

Name	Emp No	Date	Time	Event	Terminal	Zone	Reason
Tembo Maxwell		2006/02/22	14:43:01	Allowed In	A.dun	1	
		2006/02/22	14:51:27	Allowed Out	A.dun	1	
		2006/02/22	15:05:54	Allowed In	A.dun	1	
		2006/02/22	15:10:54	Allowed Out	A.dun	1	

[Return to the Web Reports Main page](#)

[Export Report \(CSV\)](#)

[Submit](#)

Hours worked in APB Zone Time Sheet Report

The Hours Worked in APB Zone Time Sheet Report provides a report of the hours that a specified Tagholder in all APB Zones between two dates.

The following selections must be made before clicking **Submit** :

- [1] The required date range must be selected. Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).
- [2] The required Person must be selected from the **Person** combo-box.

The report can be exported in CSV format.

See next page

Department Time Sheet Report

Department Timesheet Report

Address: <http://localhost/webreports/service/net.impro.ipx2.web.webreports.DepartmentAPReport>

Submit Export Report (CSV)

[Return to the Web Reports Main page](#)

Main Filters

Date from: 2006/02/01 to: 2006/02/24

Person:

Department: ☐ Hide Empty Departments

Location:

Company:

Date Filter: 2006/02/01 to 2006/02/24

Name	Company	Date	Time In	Time Out	Hours
Department : Design					
Sarah Barlow		2006/02/03	12:00:11	14:47:58	02:47:47 (2.79)
		2006/02/22	14:43:04	15:09:20	00:26:16 (0.43)
Total >>					03:14:03 (3.23 Hours)
Department : Marketing					
Tambo Maxwell		2006/02/03	12:00:07	14:47:56	02:47:49 (2.79)
		2006/02/22	14:43:01	15:10:54	00:27:53 (0.46)
Total >>					03:15:42 (3.26 Hours)

[Return to the Web Reports Main page](#)

Department time sheet report

The Department Time Sheet Report provides a report Tagholders, grouped by Department, showing the first and last transactions of each day, and the calculated time difference between them. The results are summarized as the total per Tagholder.

These details are provided for a one or more days, which may be selected by the viewer. The following selections must be made before clicking **Submit** :

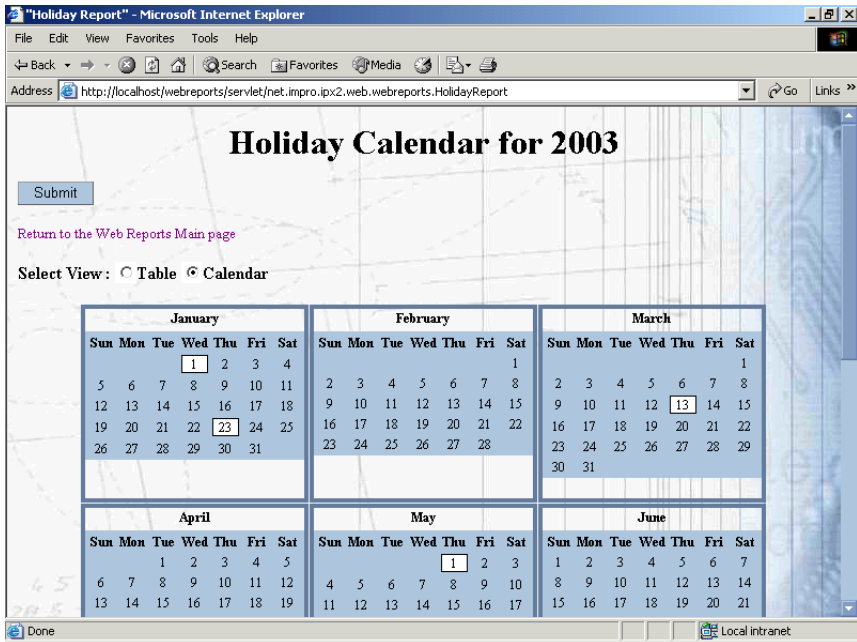
- [1] The required date range must be selected. Selecting the **Date from** or **Date to** option causes a drop-down calendar to be displayed (as described previously under **Access Reports**).
- [2] The report may be filtered by Person, Department and Zone.
- [3] Check the **Hide Empty Departments** box to exclude these from the selection list.

The report can be exported in CSV format.

See next page

GENERAL SYSTEM REPORTS

Holiday Report



Holiday Report – Calendar format

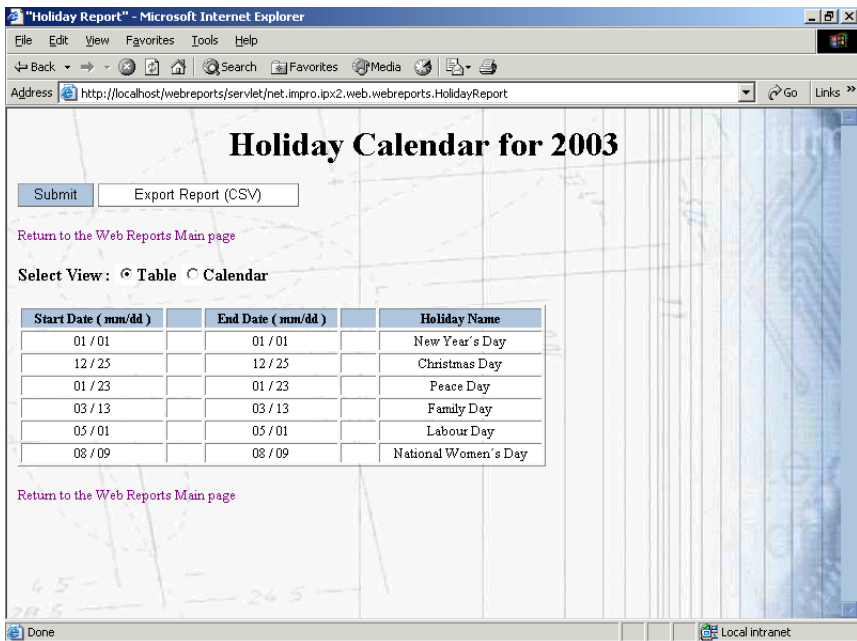
This Report shows the Holidays defined during the configuration process.

If the cursor is positioned over a holiday, a hand icon will be displayed together with the name of the holiday.

The default report format is in the form of a calendar as shown above. When Calendar format is selected, the CSV Export option is not available.

Select the **Table** button to change to table format (see next illustration). In this format the CSV Export is available.

See next page



The screenshot shows a Microsoft Internet Explorer window titled "Holiday Report" - Microsoft Internet Explorer. The address bar displays the URL: http://localhost/webreports/servlet/net.impro.ipx2.web.webreports.HolidayReport. The main content area features the title "Holiday Calendar for 2003" in a large, bold, black font. Below the title, there are two buttons: "Submit" and "Export Report (CSV)". A link "Return to the Web Reports Main page" is visible in purple text. Under the heading "Select View:", there are two radio buttons: "Table" (which is selected) and "Calendar". Below this, a table displays the holiday schedule for 2003. The table has three columns: "Start Date (mm/dd)", "End Date (mm/dd)", and "Holiday Name". The data rows are as follows:

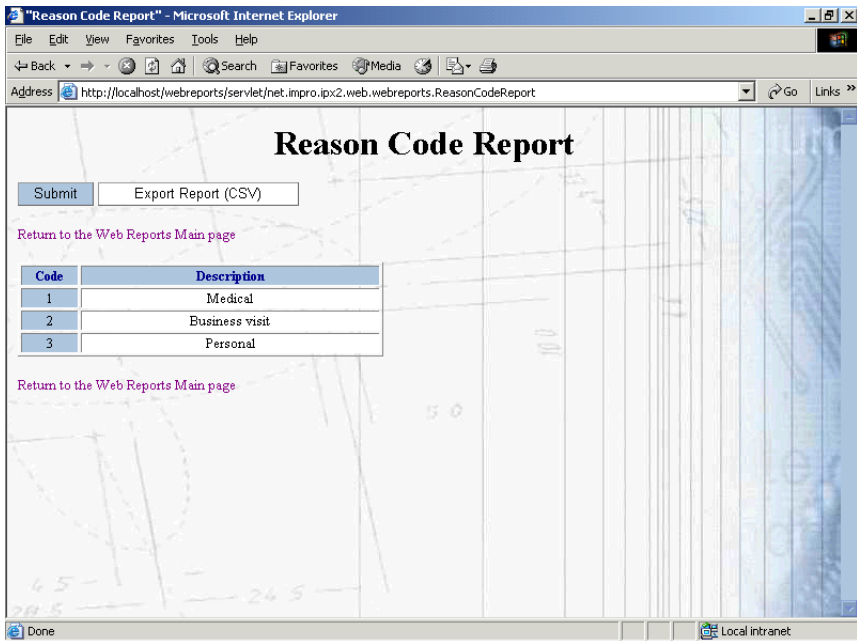
Start Date (mm/dd)	End Date (mm/dd)	Holiday Name
01 / 01	01 / 01	New Year's Day
12 / 25	12 / 25	Christmas Day
01 / 23	01 / 23	Peace Day
03 / 13	03 / 13	Family Day
05 / 01	05 / 01	Labour Day
08 / 09	08 / 09	National Women's Day

Below the table, another link "Return to the Web Reports Main page" is visible in purple text. The browser's status bar at the bottom shows "Done" and "Local intranet".

Holiday Report – Table format

See next page

Reason Code Report



Reason Code Report

This Report lists the System Reason Codes and their designated meanings.

See next page

INDEX

address, 8
Administrator, 5, 9, 10
column heading, 8, 22, 23
Configuration, 5, 9, 10, 12, 13, 14,
15, 16, 17, 19, 20, 21, 22, 23
databases, 9
global password, 5, 6
hand icon, 8
IXP200 application, 7
IXP200 program, 6, 7
LAN, 6, 7
name, 5, 7, 9
parameters, 8
Password, 5, 6, 10, 11
PC, 6, 7
Top Menu, 7
Web Browser, 5, 7
web pages, 5

USER'S NOTES

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_sys-swm-en-12 Section 4.doc
------------------	----------	-----------	---

SECTION 5
IXP200 Series
System
UTILITIES

IXP200 SOFTWARE USER MANUAL

SECTION 5 - UTILITIES

CONTENTS

INTRODUCTION	3
CHAPTER 1 – DATABASE UPGRADING.....	3
RUNNING SCRIPTS TO UPDATE AN EXISTING DATABASE	3
New Installation	3
Existing Installation	3
Automatic Upgrade.....	3
Manual Upgrade	4
CHAPTER 2 – FIRMWARE UPGRADE UTILITY.....	5
GENERAL.....	5
TOP MENU OPTIONS.....	5
FIRMWARE UPGRADING	6
Unit Type.....	7
Upgrade Type	7
Single unit.....	7
All units	7
All units (one at a time)	7
Other Information	7
Controller LA	7
Terminal LA	7
Force Upgrade	7
SYSTEM TOOLS	8
Ping Test	8
Comms Test.....	8
No. of cycles	9
Unit CLA	9
Reset.....	9
MISCELLANEOUS FACILITIES	9
Setting the Logical Address of the Controller or a Terminal	10
Set Default Message	10
Configure Controller Port 2.....	10
Clearing the Controller memory	10
CHAPTER 3 – CSV IMPORTER UTILITY.....	11
GENERAL.....	11
DEFINITIONS	12
REQUIRED CSV FORMAT	13
PROGRAM OPERATION.....	14
INDEX.....	15

SECTION 5 – UTILITIES

INTRODUCTION

The IXP System provides software utilities to assist with tasks which may be carried out occasionally, for example when upgrading from one software version to another.

These are described in this section.

CHAPTER 1 – DATABASE UPGRADING

RUNNING SCRIPTS TO UPDATE AN EXISTING DATABASE

New Installation

With each new release of IXP200, a set of empty Databases is included which is compatible with the new release. There is one Database per locale. These should be used for a new installation. No scripts are required to be run for a new installation. If there is no Database in the main Database folder after installation, it must be copied there from the chosen locale folder. Generally, from V3.4.2, the correct Database is automatically installed to match the locale chosen during installation.

Thus, for new site installations, where a NEW DATABASE IS USED, THERE IS NO NEED TO RUN ANY UPDATE SCRIPTS.

Existing Installation

However for customers with an existing Database containing user data that must be preserved, it may be necessary to run scripts on the Database to upgrade it to the new version. Upgrade scripts are included, as necessary, with each release of IXP200. The Scripts folder contains separate folders for each version, which contain the actual script files (*.sql). Thus, when upgrading IXP200, one will have to upgrade an existing Database by executing the scripts that are new for that release.

NOTE : *It will be necessary to run the scripts for each version of software after the existing version, up to and including the currently released version. It may also be necessary to add the Graphics images.*

Automatic Upgrade

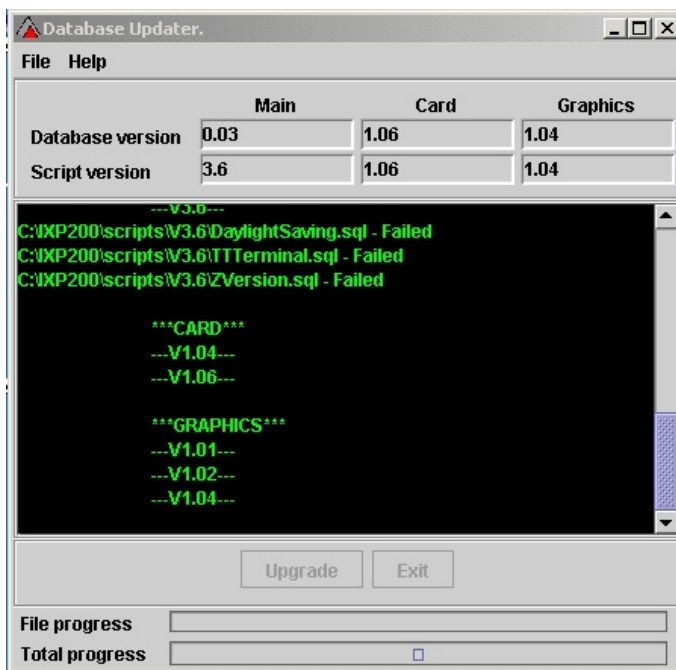
A utility has now been provided to upgrade the Database automatically. This utility is called UpgradeDatabase.exe and can be found in the install folder

(usually C:\IXP200) if a shortcut has not been installed on the **Programs Menu**.

To upgrade the Database automatically :

- [1] Double-click the icon and log on with the password for SYSDBA.
- [2] After running the program, please check the log folder. Two files are created, ScriptSummary and ScriptUpdater, for the date when executed.
- [3] Read through the ScriptSummary to check that all the script files have run successfully.
- [4] If not, then check the ScriptUpdater file. This file could assist your dealer in sorting out any errors reported.

The screen shown below is a typical Database updater dialog after updating the Database from V1.2 to V3.2.



Database Updater dialog

Manual Upgrade

Please refer to **RunningAScript.rtf** (Section 2 of this manual) for instructions on how to run a script file manually.

CHAPTER 2 – FIRMWARE UPGRADE UTILITY

GENERAL

The Firmware Upgrade utility provides several features :

- (a) Firmware Upgrade with units in the System.
- (b) System Tools.
- (c) Miscellaneous facilities including :
 - Setting the Logical Address of the Controller or a Terminal.
 - Setting a Default Message for display on the Controller LCD.
 - Configuring the Controller Port for RS232 or RS485 operation.
 - Clearing the Controller memory.

TOP MENU OPTIONS



Top Menu options

The Firmware Upgrade top menu options are as follows :

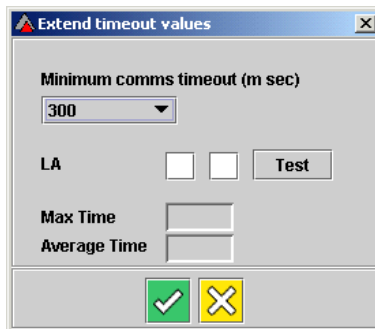
File – this offers the options **Choose Locale**, **Translate**, and **Exit**. For the use of **Choose Locale** and **Translate** see Section 3 Chapter 14.

Config – this offers the options **Port** and **Timeout**.

- **Port** permits the selection of PC port 1,2,3 or 4 as the communications port for the IXP200.
- **Timeout** permits the calculation of the minimum timeout period.

File Versions – this allows the display of current firmware versions of the upgrade files on disk.

Help – this provides access to **About** information.



Extend timeout values dialog

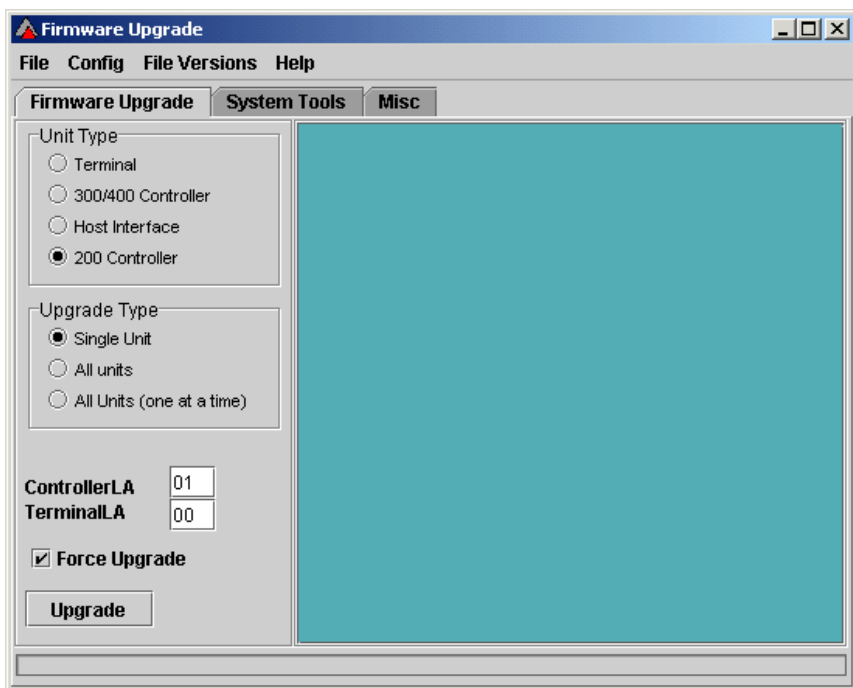
The communications timeout value determines the length of time the PC will wait for a response from Terminals before assuming there is a communications error.

In Systems where a different communications medium is being used, e.g. ethernet or radio modems.

The Minimum comms timeout time can be set using the combo box in this dialog. The default timeout is 300 milliseconds. This can be extended in 100 millisecond steps to a maximum of 3 000 milliseconds.

To test the communications time from the Controller or a Terminal to the PC, type the Logical Address of the Controller or Terminal into the boxes provided, and click **Test**. The Maximum Time and Average Time will be reported.

FIRMWARE UPGRADING



Firmware Upgrade

Unit Type

For IXP200 Systems, select either **Terminal** or **200 Controller** as appropriate. The other two options only apply to IXP300/400 Systems.

Upgrade Type

Single unit

Select **single unit** when only one unit needs to be upgraded.

All units

Select **all units** when all units need to be upgraded at the same time. This method is quicker than upgrading unit by unit, but carries the risk of a larger portion of the System being out of commission if there is a problem updating, whereas only a single unit would otherwise be affected. It is safer to use this method when installing a new System than when updating a functioning System.

All units (one at a time)

It is advisable to select **all units (one at a time)** when upgrading a System in use for the reasons stated in the previous paragraph.

Other Information

Controller LA

For IXP200 Systems, the Controller LA will always be 01.

Terminal LA

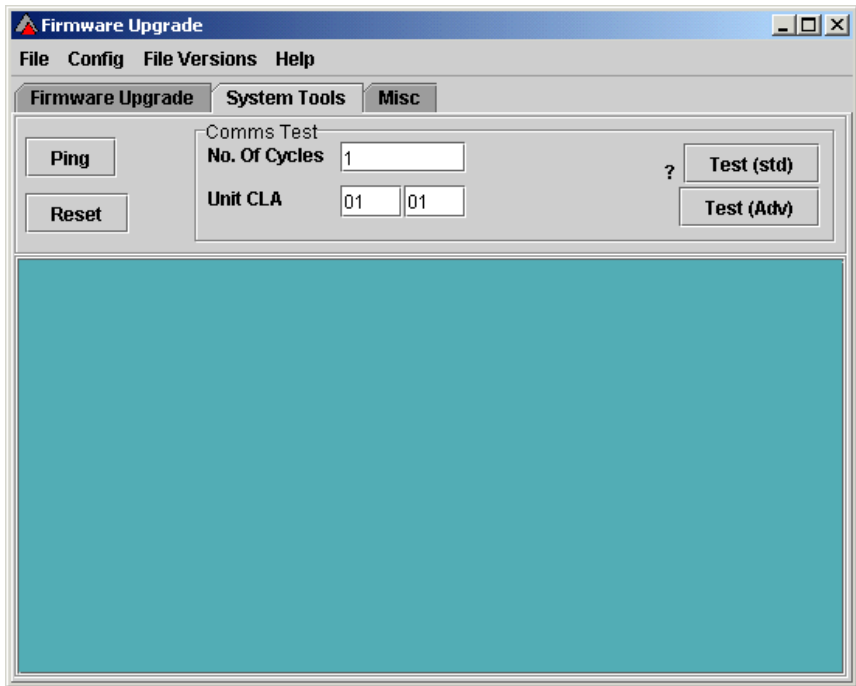
Type in the last two characters of the required Terminal's Logical Address.

Force Upgrade

This is necessary, for example, where the file version of the firmware is **not** newer than the currently installed firmware version.

See next page

SYSTEM TOOLS



System Tools

Ping Test

The **Ping Test** tests communications with all units in the System, and provides a report on each unit including the current firmware version installed.

It is normally used before performing a firmware upgrade to establish which units need to be upgraded.

Comms Test

The **Comms Test** is used to test communications with one unit at a time on the Controller and Terminal busses.

The options described in the following paragraphs are available for the Comms Test facility.

No. of cycles

The number of test cycles may be set as required. Up to 9 cycles may be selected. This facility is , typically used whenan intermittent communications fault is suspected.

Unit CLA

The CLA (Logical Address) of the required unit must be entered.

Test (std)

A **Standard Test** sends a group of messages to, and receives responses from, each Terminal, and reports a percentAge pass rate. A pass rate of less than 100% indicates a communications problem.

Test (adv)

An **Advanced Test** is used in Systems that include items such as RF modems or etherpads with longer response timeouts.

Reset

This performs a soft reset of the System, similar to a power-up reset.

MISCELLANEOUS FACILITIES

Firmware Upgrade

File Config File Versions Help

Firmware Upgrade System Tools Misc

Set Logical Address

☒ Controller ☒ Terminal

Fixed Address

Logical Address 01 01 OK

Clear Controller Memory

ControllerLA 01

☐ All Controllers OK

Set Default Message

ControllerLA 01 OK

Configure Controller Port 2

☒ RS232 ☐ RS485

ControllerLA OK

Miscellaneous Facilities dialog

Setting the Logical Address of the Controller or a Terminal

This could be done, for example, where a Terminal from another System is installed into the System, and has a previous LA which conflicts with another unit.

Set Default Message

The facility permits the user to set the default message which appears on the IXP200 Controller's and DL Terminals' LCDs.

In an IXP200 System, the Controller LA will always be 01.

To set the message, type the required message into the fields provided and click **OK**.

Configure Controller Port 2

This facility permits the selection of Controller Port 2 for either RS232 (default) or RS 485 format communications.

In an IXP200 System, Port 2 on the Controller is configured as follows :

- (a) RS232 when the Controller is connected directly to the PC.
- (b) RS485 when a ProxPal Reader or ImproX RS Registration Reader is connected between the Controller and the PC.

Clearing the Controller memory

The Controller's memory can be cleared using this facility.

CAUTION : This will also clear the Transaction Database.

CHAPTER 3 – CSV IMPORTER UTILITY

GENERAL

The CSV Import Utility enables the User to import a CSV (Comma Separated Value) file into a Database.

NOTE : *It is suggested that this Utility be used ONLY when first loading a new System and if the User has previous Database files such as may be created by Access, Dbase and similar.*

CAUTION : **Before executing the Import program, ensure that no other programs are loaded and running.**

CAUTION: **This procedure should only be used by competent Information Technology personnel. Before implementing any of the possible Import procedures, the User should be in contact with the service and maintenance personnel.**

This is not a utility that should be used more than once per table and should not be used on a mature Database unless some very specific, and advanced, procedures are followed. The Database consists of a very large number of Tables. These Tables are preloaded empty tables when the System is first installed. While the System is being configured, the Tables are updated with various data the User provides during configuration.

NOTE : *The Importer will usually be used after the software has been loaded and the site and Terminals configured. Then the CSV Importer enables the user to add the pertinent user data.*

For the above reasons the source CSV File must be carefully prepared and must conform to certain minimum requirements in order to be used by the utility.

Each Table has a specific name and format. The only tables suitable for importing data are the Department and Master tables.

The MASTER table comprises the following fields which store the details of each person :

MST_SQ (PK)	Integer	Not Null	(Master sequence number to identify this record)
MST_PIN	Integer	Null	(PIN number)
MST_FIRST_NAME	Varchar(20)	Null	
MST_LAST_NAME	Varchar(20)	Not Null	
MST_ID	Varchar(16)	Null	(ID number)
MST_ADDRESS	Varchar(65)	Null	
MST_DOB	Integer	Null	(Date of Birth 'yyyymmdd')

MASTER Table fields

MST_COMPANY	Varchar(20)	Null	(Company name)
DPT_NO (FK)	Smallint	Null	(Department number)*
*NOTE : <i>If a Department is entered in the MASTER record, it must exist in the Department table.</i>			
MST_EMP	Varchar(16)	Null	(Employee number or description)

MASTER Table fields (continued)

The **DEPARTMENT** table format comprises the following fields which store the details of each department :

DPT_NO	Smallint	Not Null
DPT_NAME	Varchar(20)	Not Null

DEPARTMENT Table fields

DEFINITIONS

Not Null means that the data must be provided. Null implies that the data is optional.

Integer is a whole number in the range -2 billion to +2 billion.

Smallint is a whole number in the range -32768 to +32767.

Varchar means a variable length character field, not greater than the maximum length specified in brackets. The data can be a mix of alphabetic and numeric characters. Trying to enter a value longer than the max length will cause an error.

PK means Primary Key. This is the sequential and unique number allocated to the record in the Database and serves as the primary means of maintaining sequence and access to that record. Trying to enter a record with a primary key which already exists in the table will cause an error. Hence the danger of importing Master records into a mature Database.

FK means Foreign Key and implies that this number is used in a different Table as the Primary Key.

MST_SQ is the primary key (PK) in the MASTER Table and is also used in the TAG Table as a foreign key (FK) to identify the Tag holder.

DPT_NO is the primary key (PK) in the DEPARTMENT Table and is also used in the MASTER Table as a foreign key (FK) to identify the department. Department number may be omitted from the MASTER record but if it is used it must be defined in the DEPARTMENT Table. Hence the Department table must be imported first.

REQUIRED CSV FORMAT

The **CSV** file is similar in concept to the Mail Merge system used by MS Word. It comprises a file that has a heading line which corresponds to the Database entry names, and then in sequence, the various entries. The file would normally be in Notepad or WordPad or similar Text form.

Do not use MSWord or Corel Word Perfect or similar word processing software as these programs include hidden characters which are used for text formatting. The file must be in pure Text (.txt) format, with commas separating the data fields, and each line ending with a normal Carriage Return (Enter Key).

Following the descriptions given of the Table Fields, or Database fields, the following examples illustrate the possible compilation of a CSV file.

The sequence of the record fields is not necessarily fixed but must be consistent throughout a file.

The name spelling is important and an incorrectly spelled name field will normally result in failure of the program to work as it cannot locate a required field.

Once the Table fields are defined in the first line of the record, the data in the data lines must follow the correct sequence. The use of the inverted commas on all fields except integer fields is important.

Example :

Department Records. File to be called 'DEPARTMENT.CSV'.

"DPT_NO","DPT_NAME"

26,"Marketing"

13,"Factory"

40,"Design"

DPT_NO	DPT_NAME		
40	Marketing		
13	Factory		
26	Design		

DEPARTMENT table - sample

Master Records. File to be called 'MASTER.CSV'.

"MST_SQ","MST_PIN","MST_FIRST_NAME","MST_LAST_NAME","MST_ID","MST_ADDRESS","MST_COMPANY","MST_EMP","DPT_NO"

1,17189,"CRAIG","NUGENT",8312175069087,"16 Pitlochry Rd","Impro Technologies","Technician",26
 2,56982,"PAUL","CHANU",7926857249837,"29 Westmead Park","Remez Security","Consultant",13
 3,98357,"JOHN","BARRETT", "16 Chearsley Rd","JoyLand/Stones","Driver",13
 5,01726,"TYRON","HOLMES",8039654006937,"32 Musgrave Rd","Edgecombe Estates"," ",40

MST_PIN	MST_FIRST_	MST_LAST_NAME	MST_ID	MST_ADDRESS	MST_COMPANY	MST_EMP
17189	CRAIG	NUGENT	8.3122E+12	16 Pitlochry Rd	Impro Tech	Technician
56982	PAUL	CHANU	7.9268E+12	29 Westmead Park	Remez Security	Consultant
98357	JOHN	BARRETT		16 Chelmsford Rd	Access Install	Technician
1726	TYRON	HOLMES	8.0397E+12	32 Musgrave Rd	TF Promotions	

MASTER table - sample

PROGRAM OPERATION

- [1] Start CSV Importer via IXP200 / CSV Importer.exe. The usual IXP200 logon sequence is applicable. The Database URL is obtained from proxette.properties, so this must point to the correct file.
- [2] After the logon the CSV Importer screen is displayed. It is very simple, with an Add (+) and Remove (-) button to add and remove CSV files and up and down buttons to order the sequence of the files.
- [3] Click the 'Add' button and browse through the folders to find the required CSV files.
- [4] Select the file to be imported and click 'Open'. This may need more than one iteration to select the files into the CSV Importer. Once selected, ensure that the Department.CSV file is first on the list, before Master.CSV.
- [5] To start the process, click the 'Start' button. When complete, a confirmation message will be displayed. Any errors will be recorded in a csvImport log file, named for the date, in the log folder located in the IXP200 folder.

INDEX

communications port, 5
Controller, 5, 6, 7, 8, 10
Controller Port, 5, 10
current firmware, 5, 8
database, 3, 4
Default Message, 5, 10
default timeout, 6
empty databases, 3
existing database, 3
fault, 9
Firmware Upgrade, 5, 6
firmware version, 7
installation, 3
locale, 3
log folder, 4
Logical Address, 5, 6, 7, 9, 10
main database, 3
new release, 3
new site, 3
new system, 7
password, 4
PC, 5, 6, 10
RS232, 5, 10
RS485, 5, 10
script, 3, 4
System Tools, 5, 8
Terminal, 5, 6, 7, 8, 10
Terminals, 6, 10
test communications, 8
timeout, 5, 6
upgrading, 3, 7
user data, 3

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_sys-swm-en-12 Section 5.doc
------------------	----------	-----------	---

IXP 200 Software User Manual

SECTION 6 MANUAL EDITING FACILITY

IXP200 Software User Manual

SECTION 6 – CONTROLLER MANUAL EDITING FACILITY

CONTENTS

INTRODUCTION	5
Entering the Menu	5
Transfer of Changes to the System PC Database	5
Active Keys	5
Menu navigation keys	5
Select keys	6
Editing keys	8
Alphanumeric Entry	8
MENUS	8
General	8
First Level Menus	9
EXAMPLE OF THE USE OF THE MANUAL EDITING FACILITY	10
Settings Menu Example	10
TAGHOLDERS' MENUS	12
Tagholders Menu	12
Delete Menu	13
Add/Edit Function	13
Add/Edit Menu	14
Suspend Menu	16
Name Menu	17
Level Menu	18
Access Group Menu	19
PIN Menu	20
Door Entry Code Menu	21
SYSTEM SETTINGS MENUS	22
Settings Menu	23
Emergency Unlock	23
Transactions Menu	24
Debug Mode Menu	27
Alarm Arm Relay Menu	28
Peripheral Port Menu	29
RTE Latch Menu	29
INDEX	31

INTRODUCTION

NOTE : *This information describes the options available in **Version 3.04** of the Controller firmware.*

It is possible to edit certain IXP200 system functions using the keypad and LCD on the system's Controller.

NOTE : *The PC software must be off-line to permit use of this editing facility.*

The Controller menu system allows the Administrator to Add, Delete or Edit Tag information as well as to change specific system settings.

Entering the Menu

To enter the menu, present an Administrator Tag at the Controller.

NOTE : *If the PC software is on-line then access to the menu is blocked until the software is exited. The menu is blocked for a further 20 seconds after exiting the software before it is available to enter.*

If no keypad activity is detected for 3 minutes then the Controller will automatically exit the menu.

Transfer of Changes to the System PC Database

All changes done in the menu are recorded as modification transactions so as to synchronise with the PC software database if necessary. This synchronisation is done automatically when the PC software connects to the Controller.

Active Keys





The active keys for each level in the menu tree are displayed on the bottom line of the IXP200 Controller's LCD when that level is accessed, and change depending where you are in the menu tree structure.

The following keys are used for this facility :





Menu navigation keys

The following are **Menu Navigation** keys. They allow you to move within the menu tree structure :

-  Scroll up
-  Scroll down
-  Enter
-  Escape

Select keys

The following keys are **Select** keys. They allow you to select characters in the current menu data field :

-  scroll left
-  scroll right

See next page













Controller Keypad Arrangement


See next page

Editing keys

The following keys are **Editing** keys. They allow you to enter and edit text within the current menu data field :

 to    	Alphanumeric entry, backspace.
 to  	Numeric entry, backspace.
	OK - This key accepts any new data.
	Cancel - This key cancels any new data and refreshes the existing data.

Alphanumeric Entry

- [1] Press the key that has the desired character. If the character that you want is not the first to be displayed, press the key again within 1 second before the blinking cursor appears, to display the next character.
- [2] If a character is missed then keep pressing the key until it appears again or press the  key to delete the character(s).
- [3] If the required new character is on the same key then wait 1 second until the blinking cursor appears, then select the desired character.
- [4] If the required new character is on a different key then that key can be selected immediately. The cursor will move to the next position automatically.

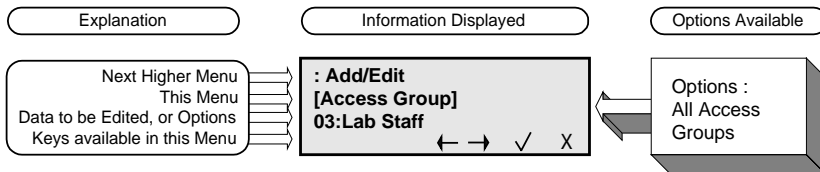
MENUS

General

The Manual Edit Facility is organised in a menu tree as shown in the following diagrams.

As you make selections in the menus, the Controller LCD information changes accordingly. The LCD will display information appropriate to the menu selected.

See next page

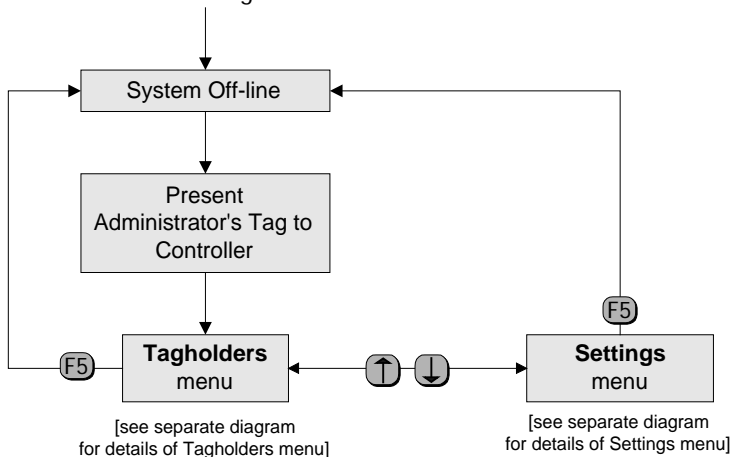


Explanation of Displayed Information

The LCD information will be formatted as shown on the previous page. The top line shows the name of the next higher menu, the second line shows the name of the menu selected, the third line the options available (in a few cases this will be information which can be edited instead of pre-set options). The last line shows the keys which can be used in the selected menu.

Each menu is described in detail in the paragraphs which follow.

Once the Controller Manual Editing menu has been entered, the next Add/Edit screen will be displayed. Detail of this screen and the first level menu options offered are shown in the diagram **First Level Menus**.



First level menus.vsd

First Level Menus

First Level Menus

The following first-level options are available in the Controller First Level Menus :

- Tagholders
- Settings

Once the PC has been off-line for more than 20 seconds, presenting an Administrator Tag to the Controller will cause the **Tagholders Menu** to be displayed.

If the Controller memory is initialised or there are no Tags in the database (i.e. when the Controller is received from the factory), press the Enter key to access the menu. This allows the installer to use the menu to choose the Comms Port Setting to be RS232 or RS485.

- [1] To toggle between the **Tagholders** menu and the **Settings** menu, use the Scroll up or Scroll down buttons.
- [2] To Escape from either of these menus, use the F5 key.

GENERAL POINTERS – FIRST LEVEL MENUS

- (a) The first menu to appear is the Tagholders menu.
- (b) The Settings menu can only be entered from the Tagholders menu.

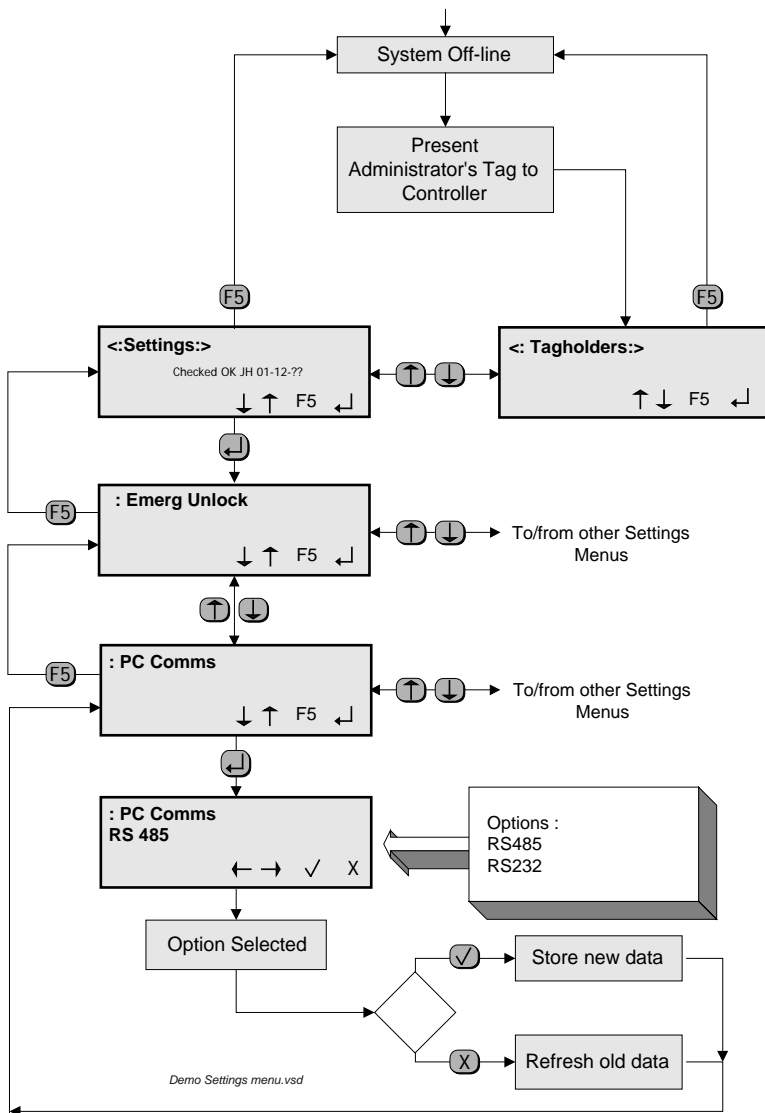
EXAMPLE OF THE USE OF THE MANUAL EDITING FACILITY

Settings Menu Example

To illustrate the use of the facility, an example of the use of a Settings menu, the PC Comms menu, is explained here. A flow chart showing the use of the PC Comms manual editing facility is included on the next page.

NOTE : *The methods described here can be used to navigate all the available menus and to select or modify data in those menus.*

- [1] Once the Controller is in Manual Edit Mode, the **Tagholders** menu will immediately be displayed.
- [2] Use the **Scroll up** key to toggle to the **Settings** menu.
- [3] Use the **Enter** key to enter the **Settings** menu.
- [4] Select the **PC Comms** menu using the **Scroll up** key.
- [5] Enter the **PC Comms** menu using the **Enter** key.
- [6] In the **PC Comms** menu, use the **Scroll left** and **Scroll right** keys to select the required option.
- [7] Use the **OK** key to accept the new option, or the **Cancel** key to reject it and to retain the original option.
- [8] This will return the system to the **PC Comms** menu.
- [9] From this point any other **Settings** sub-menus can be selected using the **Scroll up** and **Scroll down** keys, or you can return to the **Settings** menu by pressing **F5**.



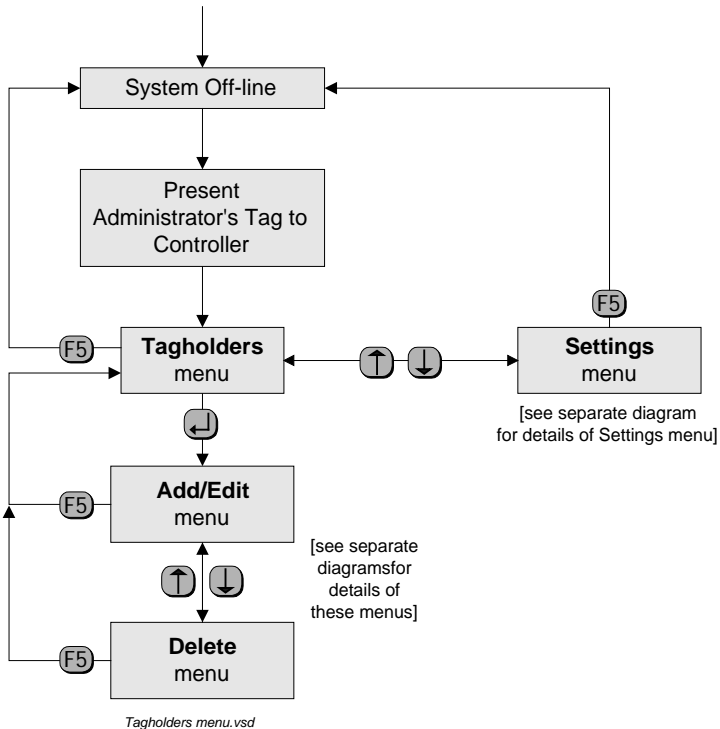
Entering and modifying the PC Comms Menu

TAGHOLDERS' MENUS

There are several menus available for changing data relating to Tagholders.

Tagholders Menu

The Tagholders menu offers the functions shown in the diagram **Tagholders Menu Options**. The link to the Settings Menu is also shown.

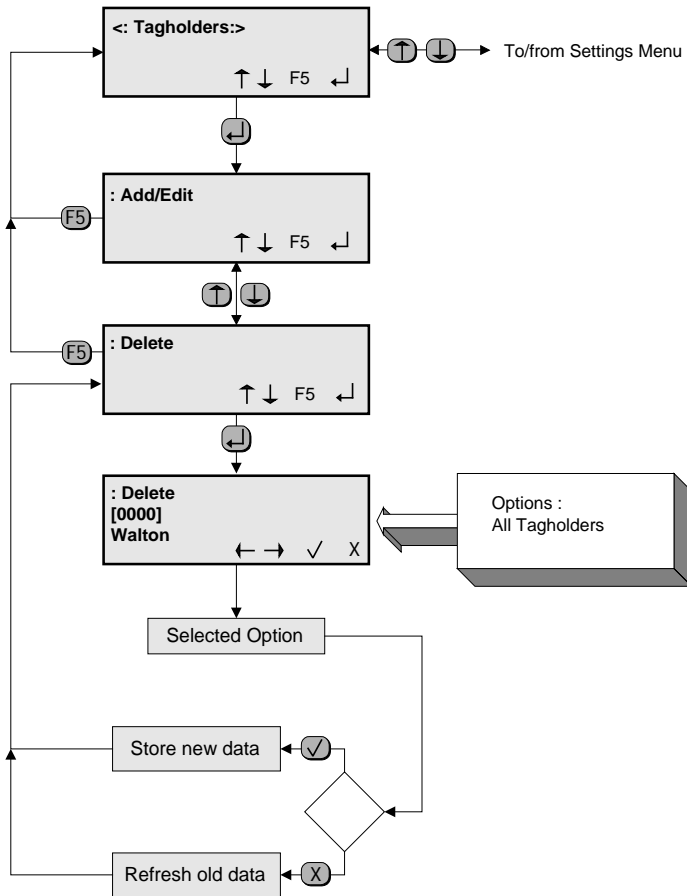


Tagholders Menu Options

See next page

Delete Menu

The Delete Menu is accessed from the Add/Delete Menu as shown above. This menu enables the Administrator to delete any Tag in the system as required. The Delete Menu is shown below.

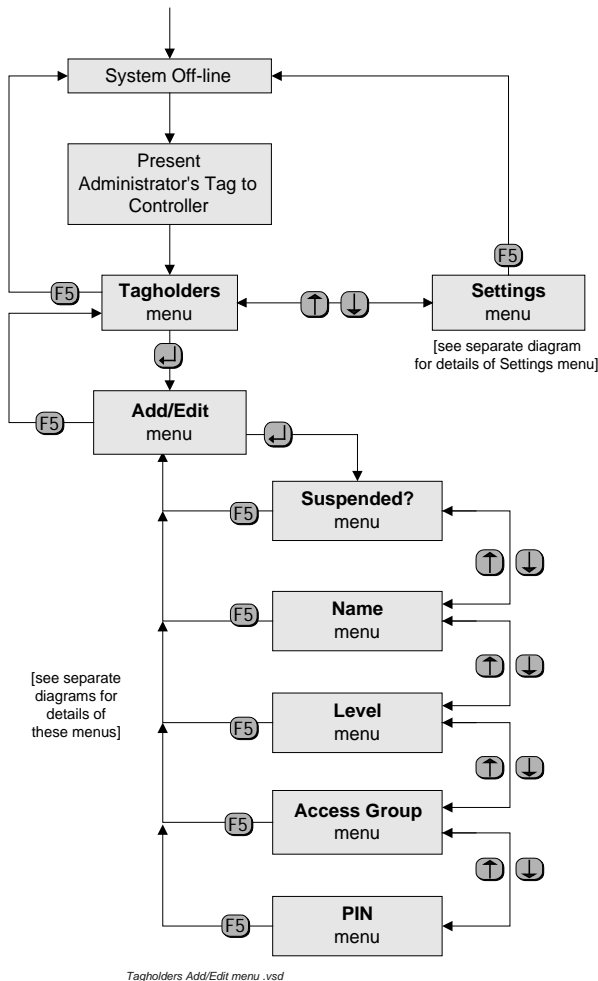


Delete menu.vsd

Delete Menu

Add/Edit Function

This function allows the addition or editing of Tag information. Access Groups can only be configured using the PC software. They can then be allocated to Tags using the menu.



Add/Edit Sub-menus

Add/Edit Menu

This menu has several sub-menus as shown in the diagram **Add/Edit Menus** above.

The sub-menus permit the Administrator to :

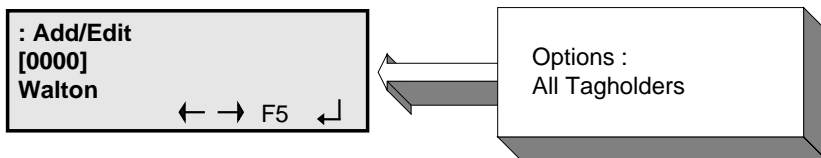
- Select a Tagholder, by either presenting a Tag or scrolling for a Tag using the keys. If the Tag presented is not in the database, then the LCD will indicate that it is a new Tag, and then the user can configure the Tagholder's name, etc.

- (b) If the Tag is in the database, then it will be located for editing.
 - (c) Suspend access permission for the selected Tagholder.
 - (a) Change the name of the selected Tagholder.
- Change the Access Group of the selected Tagholder.
- (b) Change the access Level of the selected Tagholder.
 - (c) Change the PIN of the selected Tagholder.

The Add/Edit Menu is entered via the **Tagholders Menu** as shown in the **Add/Edit Sub-menus** diagram above. The various sub-menus are described below.

Selecting a Tagholder

In each case the required Tagholder is selected in the **Add/Edit** menu. The subsequent menus permit the modification of various Tag-related information.



Add/Edit Screen

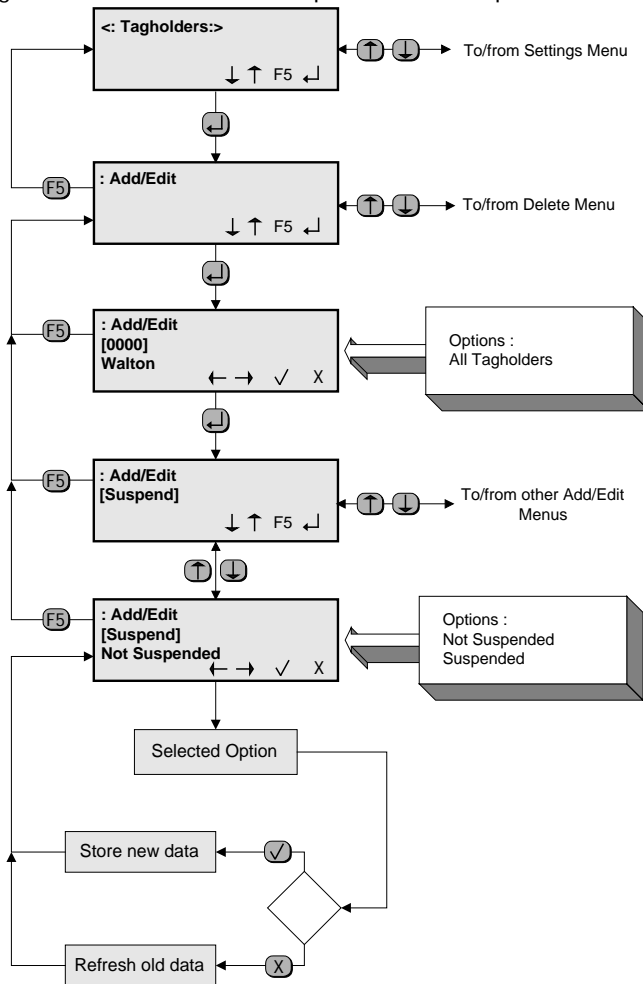
This screen appears when accessing any of the Tagholder sub-menus. It allows :

- (a) The selection of any Tagholder by name.
- (b) Entry of a new Tagholders' name after presenting a new Tag to the Controller.

See next page

Suspend Menu

This menu permits the Administrator to suspend access permission for the selected Tagholder and to re-instate this permission as required.

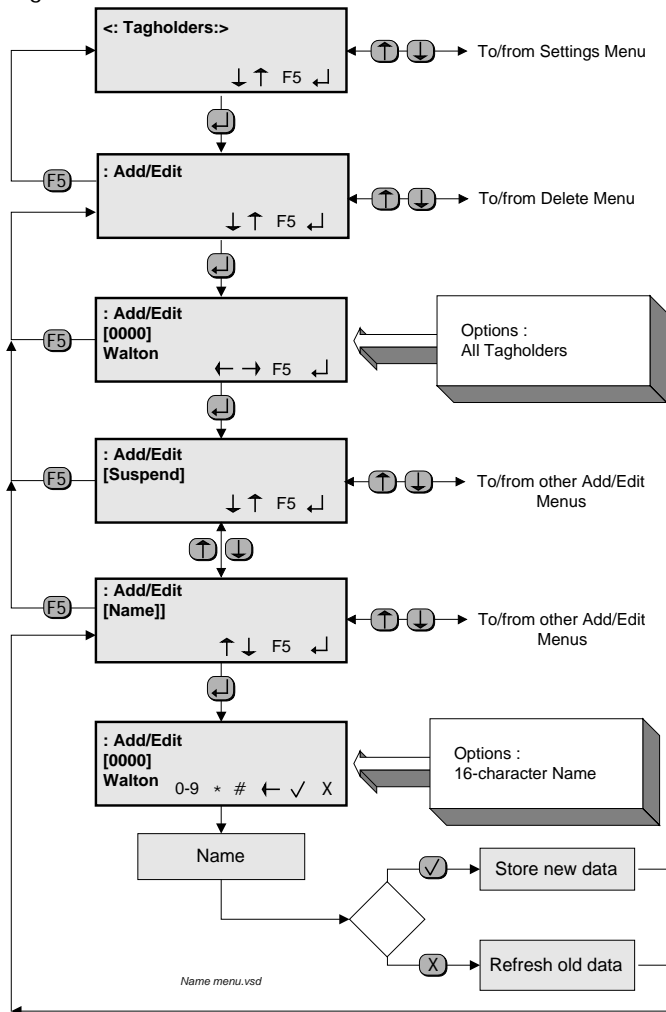


Add/Edit Access Group details.vsd

Suspend Menu

Name Menu

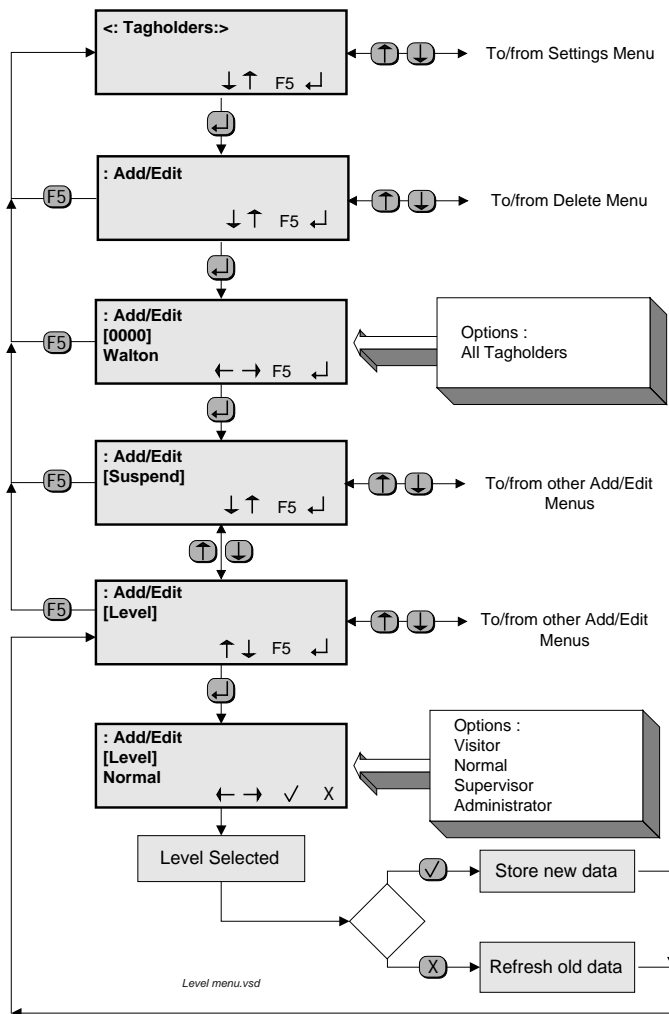
This menu permits the addition of a new Tagholder name or the editing of an existing Tagholder name.



Name Menu

Level Menu

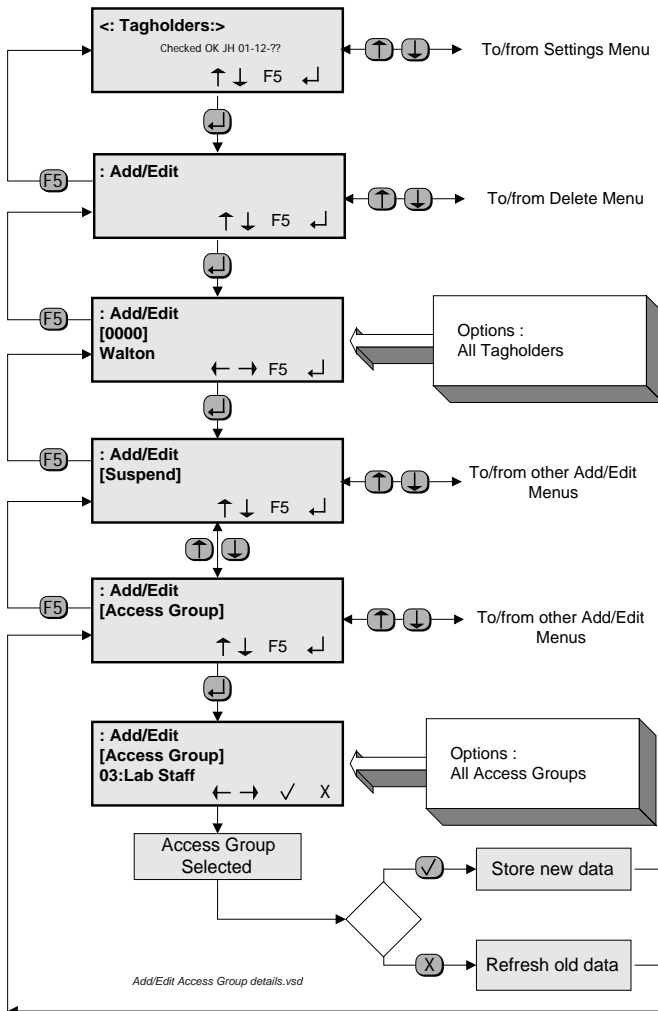
This menu permits the selection of a Tag Level for the selected Tagholder.



Level Menu

Access Group Menu

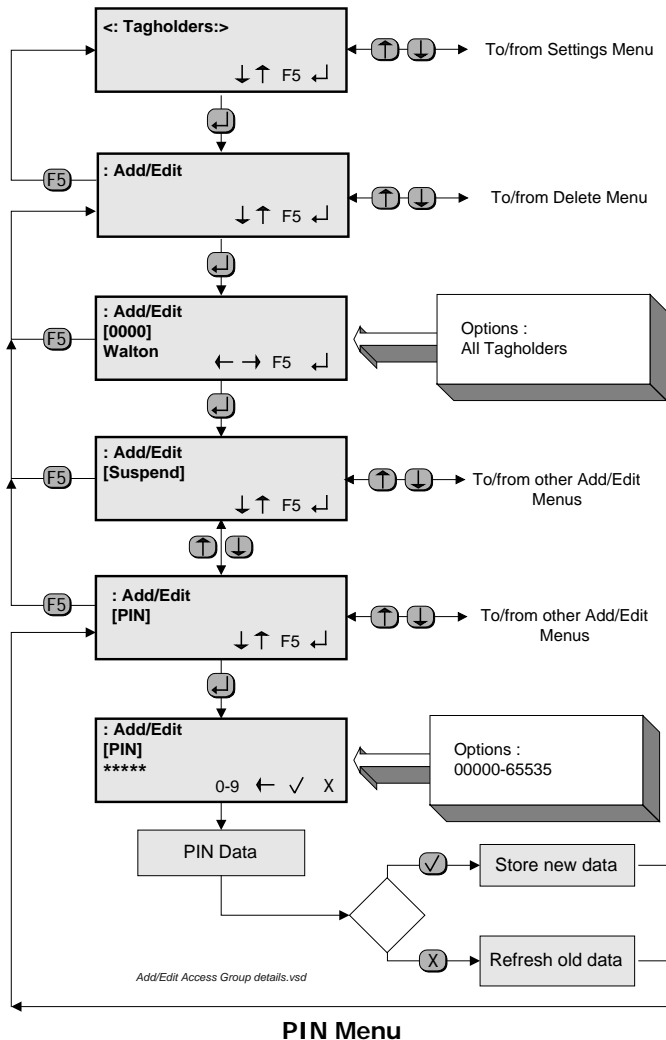
This menu permits any available Access Group to be allocated to the selected Tagholder.



Access Group Menu

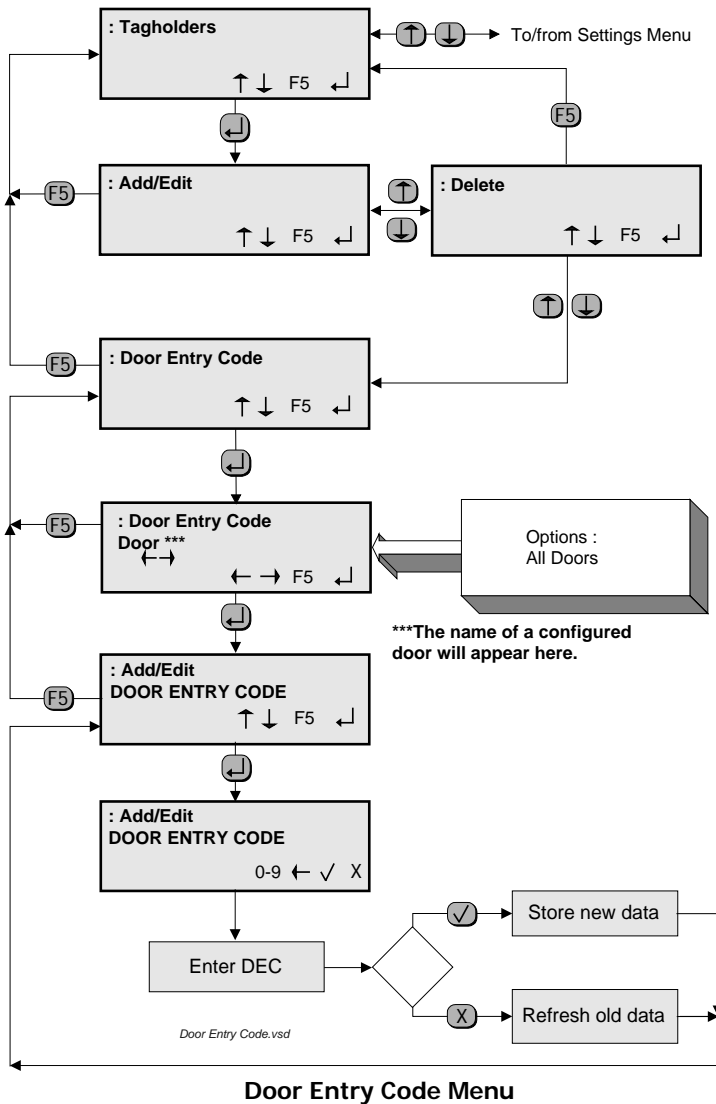
PIN Menu

This menu permits the allocation of a PIN number to the selected Tagholder, or the modification of an existing PIN number.



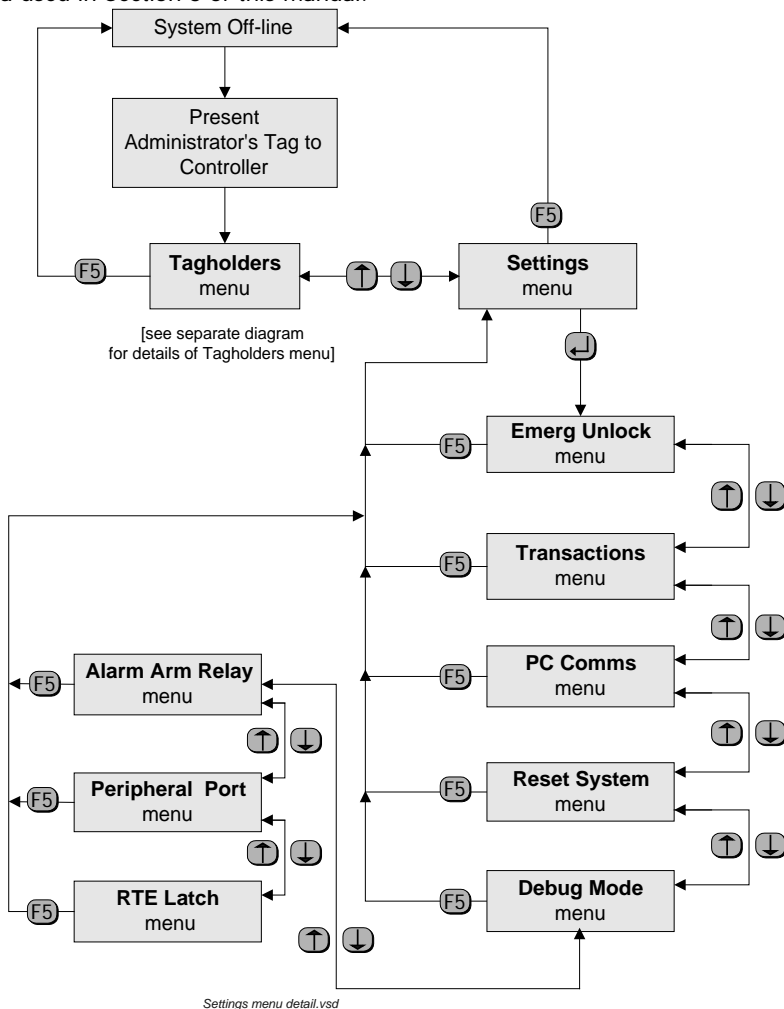
Door Entry Code Menu

This menu permits the manual entry or editing of Door Entry Codes.



SYSTEM SETTINGS MENUS

All of the menus which are related to system settings are entered via the **Settings** menu. The data presented here is related, where appropriate, to the data used in Section 3 of this manual.



Settings Menu Options

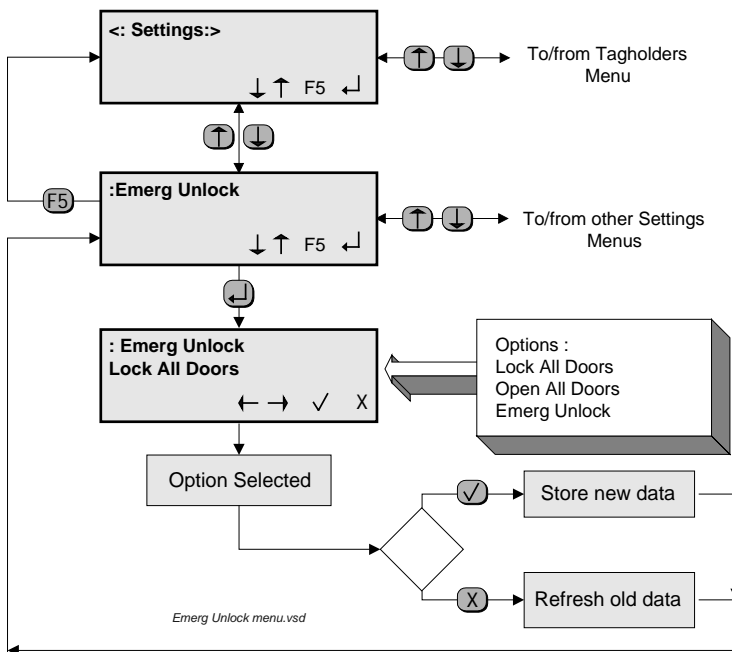
Settings Menu

The **Settings** Menu offers the options shown in the **Settings Menu Options** flow chart shown above.

Emergency Unlock

The **Emerg Unlock** menu allows the Administrator to select one of three options.

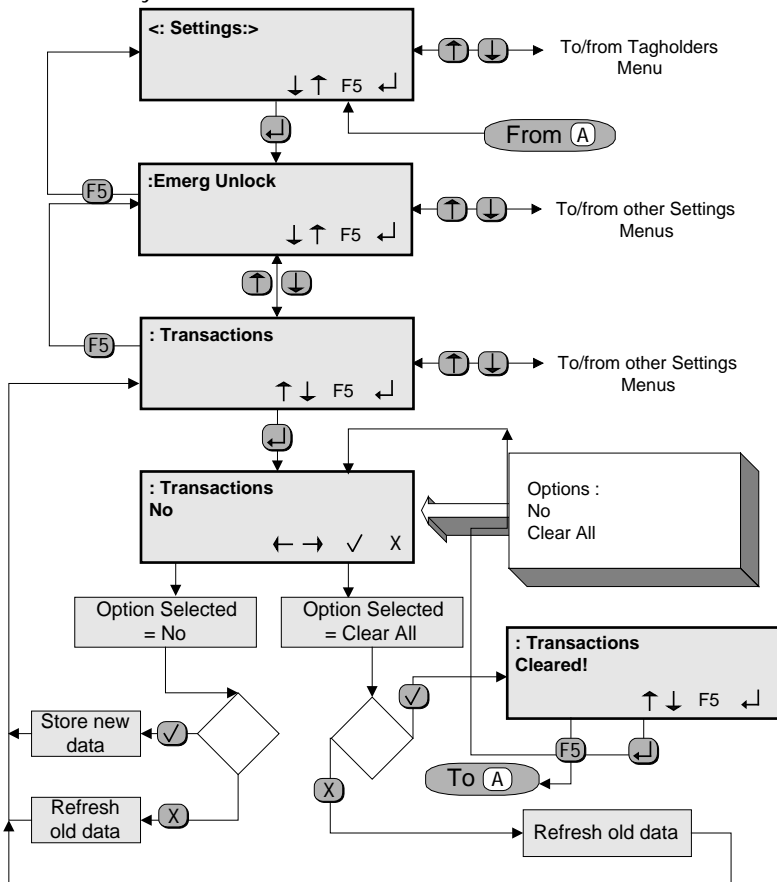
- Lock All Doors.** This is the default condition, in which doors can be opened by valid Tags in the normal way depending on Access Group, Door Mode and Level.
- Open All Doors.** This option opens all doors in the system for the time period allocated to each door.
- Emerg Unlock.** This option opens all doors and leaves them unlocked until Lock All Doors is selected.



Emergency Unlock

Transactions Menu

This menu enables the Administrator to clear all current transactions from the Controller memory.

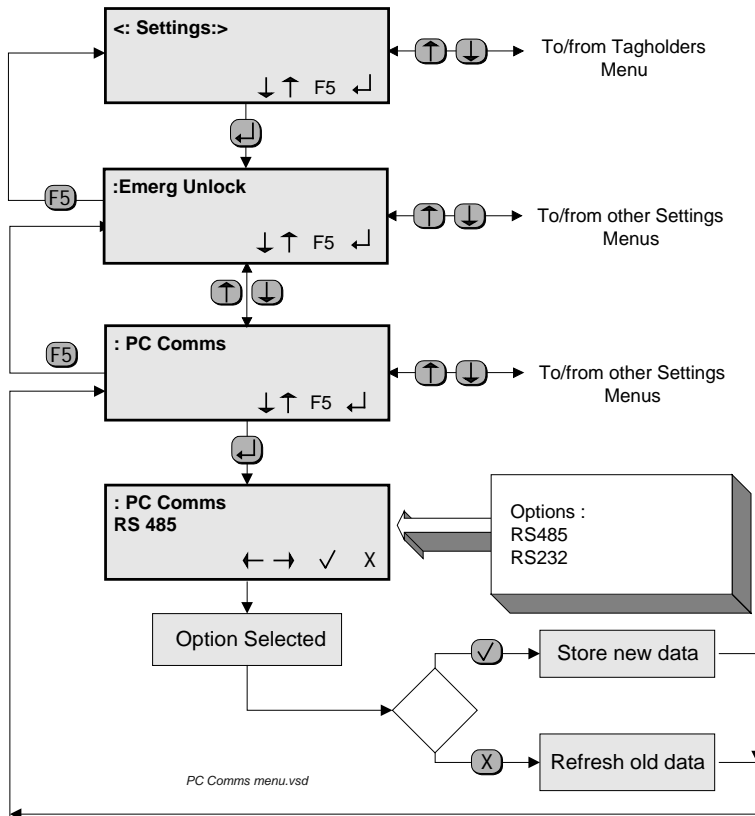


Transaction menu.vsd

Transactions Menu

PC Comms Menu

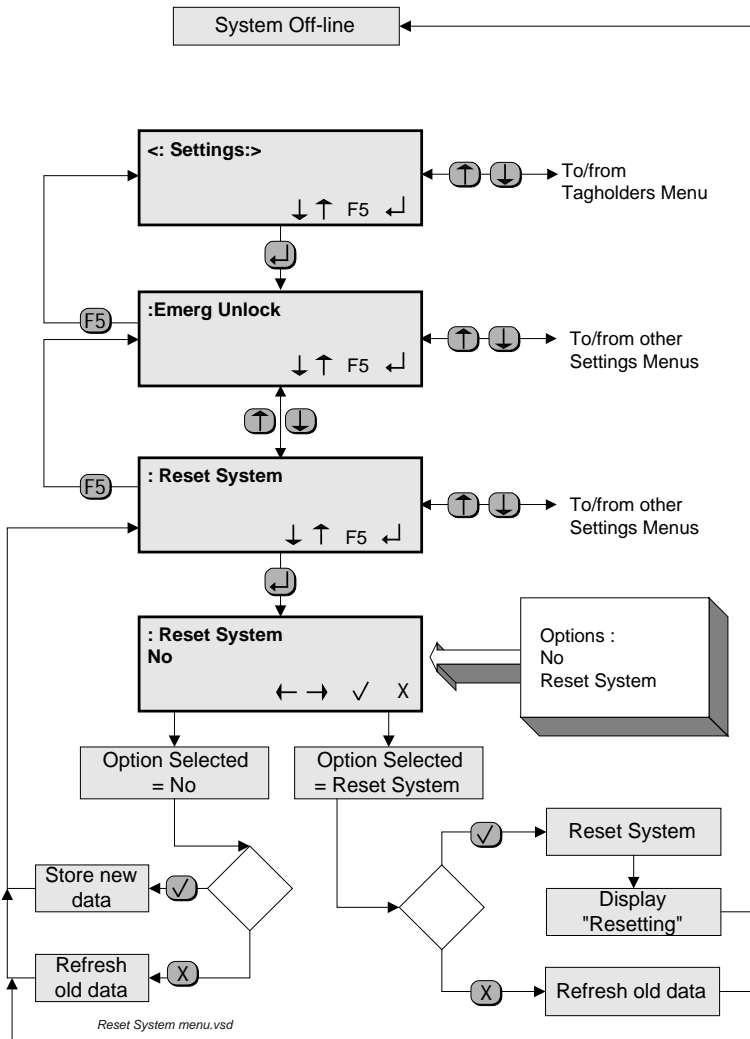
The PC Comms menu permits the selection of RS232 or RS485 communications on the Host Bus between the Controller and the PC.



PC Comms Menu

Reset System Menu

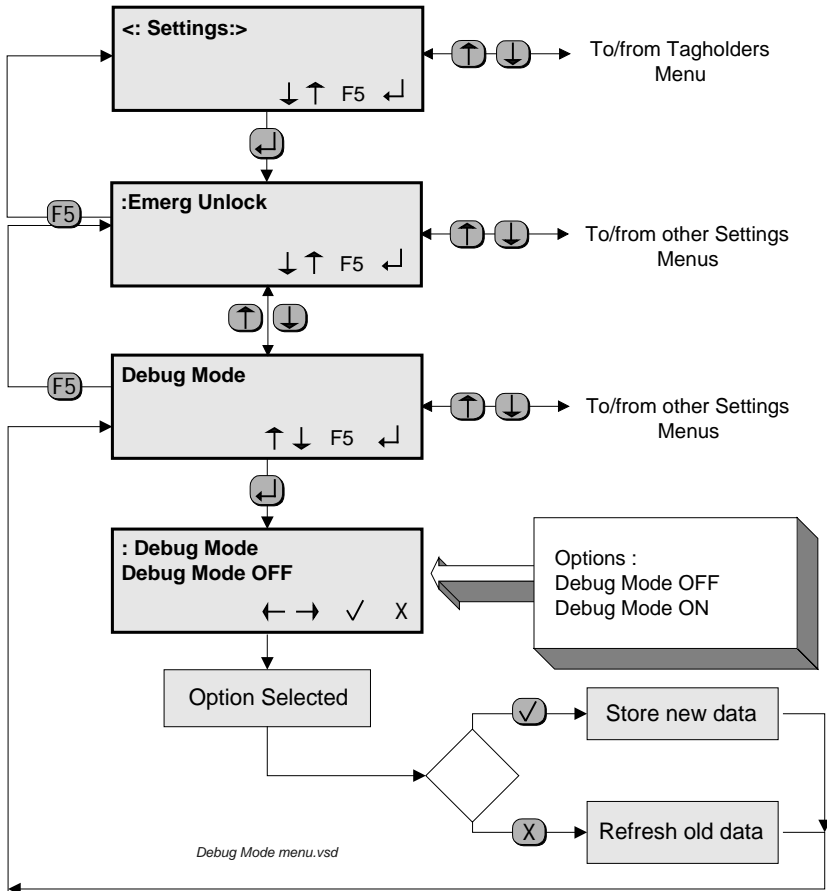
This menu permits resetting of the system.



Reset System Menu

Debug Mode Menu

This menu permits the selection of the Debug Mode. In this mode information is provided on the LCD concerning system conditions associated with a Tag when it is presented, “Denied Time In”. This facility is intended for use by installers.

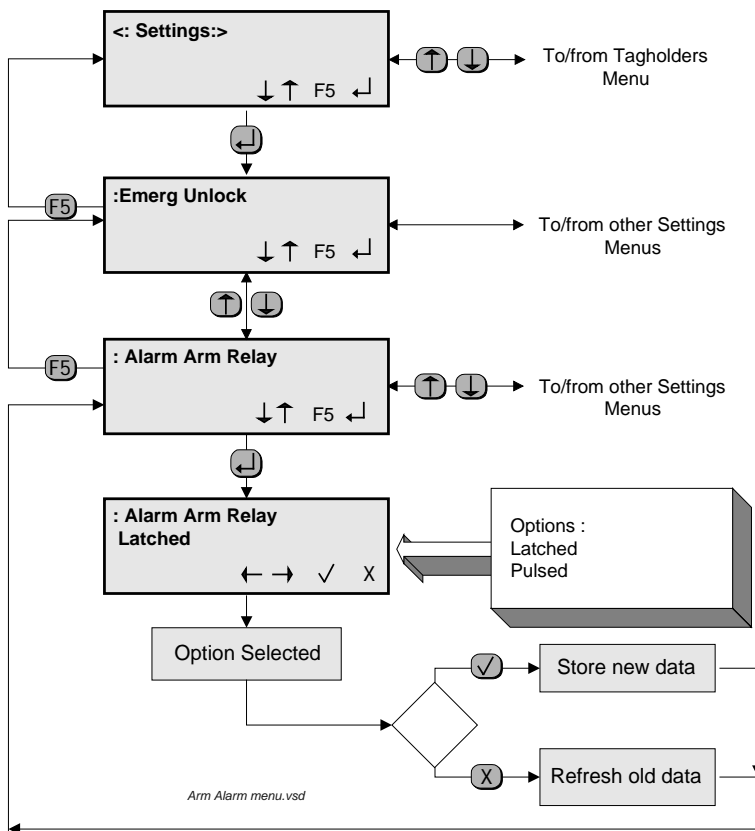


Debug Mode Menu

Alarm Arm Relay Menu

This choice is governed by the requirements of the third party alarm system. The menu permits the choice of :

- Latched operation of the alarm arm relay (relay #2) in the Controller. When activated, the relay will remain operated until the alarm system is disarmed.
- Pulsed operation of the relay. When activated the relay operates for a period of approximately 1 second, and then releases.



Alarm Arm Menu

Peripheral Port Menu

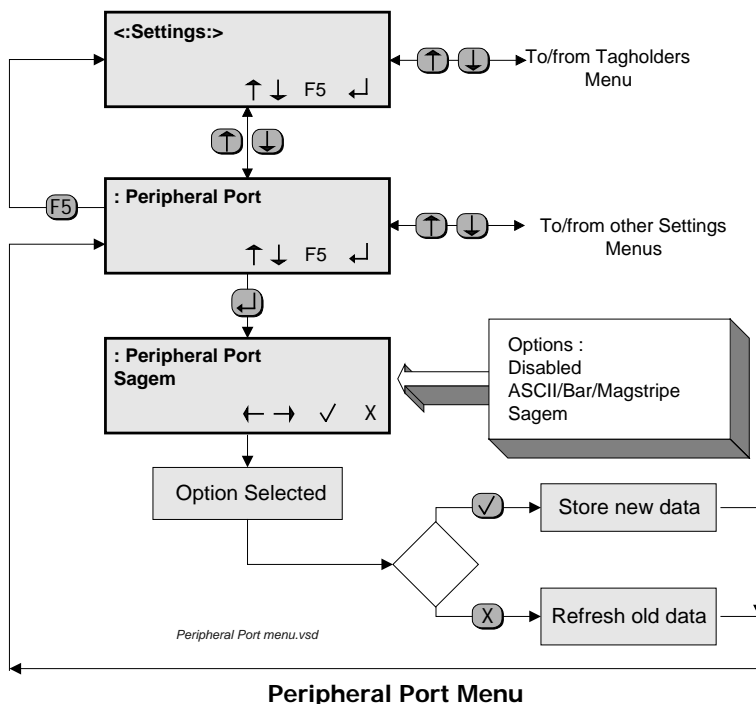
This choice is determined by the type of peripheral device which is connected to the Peripheral Port of an ImproX DL Terminal. The menu permits the choice of :

- (a) Disabling the Port.
- (b) Communication with an ASCII-based device such as a bar-code or magnetic stripe Reader.
- (c) Communication with a Sagem Fingerprint Reader.

The peripheral unit should be set to the following communications format :

Baudrate	: 9600 baud
Data bits	: 8 bits
Parity	: None
Stop Bits	: 1 bit

The Menu flowchart is shown on the next page.

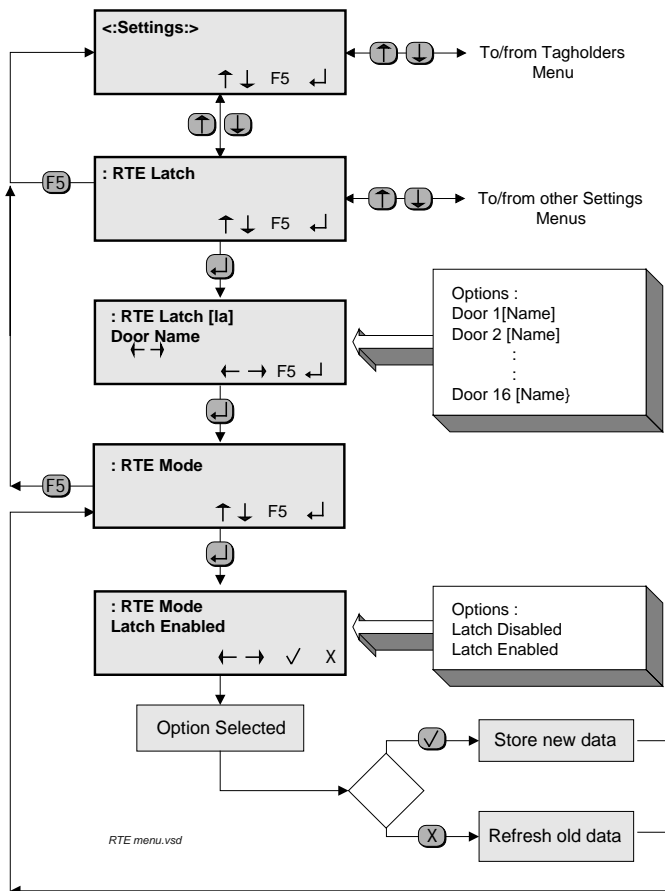


RTE Latch Menu

When the RTE Latch is enabled the latch is not activated, but the Door Open Timer will be enabled to suppress unwanted Door Forced transactions occurring

when the RTE pushbutton is used to open the door.

When RTE Latch is enabled RTE access transactions will also be suppressed by the Controller.



RTE Latch Menu

Details of the use of the Sagem Fingerprint Readers are included in the IXP System-compatible Biometric Reader manual. Interconnections are also shown in the that manual.

INDEX

- access*, 5, 10, 15, 16, 30
- Access Group, 15, 19, 23
- Add/Edit, 9, 13, 14, 15
- Administrator, 5, 10, 13, 14, 16, 23, 24
- alarm system, 28
- Alphanumeric entry, 8
- blinking cursor, 8
- Comms Port Setting, 10
- communications, 25, 29
- Controller*, 5, 7, 8, 9, 10, 15, 24, 25, 28, 30
- Database, 5
- delete any tag, 13
- Door Entry Codes, 21
- Door Forced, 29
- Door Open Timer, 29
- Editing keys, 8
- Emerg Unlock**, 23
- Escape, 6, 10
- existing data, 8
- F5, 10
- fingerprint, 29, 31
- flow chart, 10, 23
- Host Bus, 25
- IXP200, 3, 5, 31
- LCD, 5, 8, 9, 14, 27
- Lock All Doors**, 23
- Manual Edit Mode, 10
- Manual Editing menu, 9
- Menu navigation keys, 5
- menu system, 5
- menu tree, 5, 8
- new data, 8
- Numeric entry, 8
- off-line, 5, 10
- Open All Doors**, 23
- PC software*, 5, 13
- peripheral device, 29
- PIN, 15, 20
- resetting, 26
- RS232, 10, 25
- RS485, 10, 25
- Sagem, 29, 31
- Select keys, 6
- sub-menus, 10, 14, 15
- tag-related information, 15
- use by installers, 27

USER'S NOTES

USER'S NOTES

USER'S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ ImproNet Access\ English Manuals\ IXP200_system-swm-en-12 Section 6.doc
------------------	----------	-----------	---

IXP200
Software User Manual

SECTION 7
GLOSSARY OF TERMS

SECTION 7 - GLOSSARY OF TERMS

This section contains a Glossary of Terms applicable to IXP200 Systems. Items in bold in the right-hand column are listed elsewhere in the left-hand column as entries in this Glossary.

TERM	EXPLANATION
Access Pattern	: A description which defines a particular time and place where access is to be allowed. Eight Access Patterns may be defined for each Access Group .
Access Point	: (see Door) This may be a conventional door with 1 or 2 Readers, or a lift (elevator) control point with 1 to 4 readers (1 per lift (elevator)).
Action	: An observable, electro-mechanical or recordable system output triggered by an Event.
Antenna Reader	: Remote Reader consisting of an enclosed antenna only.
Anti-Passback	: Anti-Passback (APB) is intended to prevent a Tag-holder entering a Zone and, without physically exiting the Zone, passing the Tag to a person outside the Zone and thus allowing that person to gain entry to that Zone illegally. Three levels of APB are available : None, Strict and Relaxed.
Anti-Passback - Override	: The presentation of a Supervisor or an Administrator level Tag overrides any APB setting.
Anti-Passback - Relaxed	: No double entry allowed but double exit allowed.
Anti-Passback - Strict	: No double entry or exit allowed.
APB	: (See Anti-Passback).
APB Lockout Time	: This is the period of time for which a valid Tag-holder is not allowed to re-enter a Zone after he/she has exited it. This prevents a Tag-holder entering a Zone, then presenting his Tag to the "Out"

TERM	EXPLANATION
	Reader Terminal and, without physically exiting the Zone, passing it to a person outside the Zone and thus allowing that person to gain entry to that Zone illegally.
Auto-ID process	: A process whereby the ImproX hardware installed at a Site is detected, identified and assigned Logical Addresses .
Controller	: A unit which is a Master of the Terminals connected to it. The Controller, operating on Events generated by Terminals, determines the resultant Actions taken by the Terminals. A Controller acts as an interface between the system Host PC(s) and the system Terminals. It performs control functions such as the real-time control of access to the system, and maintains databases for system activities.
Database Server	: A server which contains the database for a system.
Default Tag Mode	: The Mode assigned to a new door if no other mode is specified.
Detected Unit	: Hardware unit detected on the bus.
Door	: An access point controlled by 1 or 2 Reader Terminals, one for entry and one for exit (see Access Point).
Door Entry Code	: Global code for a particular door. Valid when door is in Door Entry Code mode
Door Mode	: Qualifies the access allocated to a Tag. A mode is specific to a particular door Open, Tag, Supervisor Unlock, Door Entry Code, Personal Access Code, No Entry and Locked are the main modes, which can be selected for a door (see Door Mode Pattern). In addition PIN code , Reason code or Dual Tag may be required. Armed mode can be set when the Controller is armed.

TERM	EXPLANATION
Door Mode Pattern	: Defines a set of consecutive Time Slots for a day (24 hrs). Each Time Slot defines a mode which determines the operation of the door during that period. A door is assigned a Door Mode Pattern for each day of the week and holidays.
Dual Tag Access	: The Operator can select whether one or two Tags are required for entry or exit, that is two persons must be present to open a door.
Engine Workstation	: The PC on which the IXP200 software is installed, and which communicates with the IXP200 Controller.
Editing Workstation	: A separate PC (additional to the Engine Workstation) on which the IXP200 software is installed, but which is not connected to the system hardware, and therefore does not communicate with the IXP200 Controller. This PC is only used for editing the database.
Event	: An occurrence that is recognised by the system as a trigger for a system Action .
Event Triggered Action	: An externally initiated occurrence that triggers an Action in the system.
Fixed Address	: A unique address allocated to each ImproX unit during manufacture.
Host Bus	: A communications bus, which interconnects the ImproX Controller and the Host PC via either RS485 or RS232.
Host PC	: A Host is defined as a PC that communicates with the ImproX Units via the IXP200 Controller. (See also Local Host PC). In IXP200 Systems, a single Host can perform all functions, or a Host can be used with a separate Server PC .

TERM	EXPLANATION
IP (address)	: Internet Protocol (address)
Keypad	: A set of pushbutton keys mounted in the cover of a Terminal, which permit the entry of data into the system.
Lift (elevator) Reader	: A reader is installed in a lift (elevator) and operates in conjunction with ImproX O16 Output Terminal to activate lift (elevator) floor buttons. When a Tag is presented to the reader those buttons allocated to the Tag become active for a limited period.
Location	: (See Door).
Logical Address	: A unique address allocated to each unit in a system by the IXP200 Software .
Master	: A person's unique record in the Database .
Non-reader	: A unit that does not have the ability to read Tags . This includes Input and Output Terminals , which are used for Lift (Elevator) Control and Building Management.
Personal Access Code	: A number assigned as a Tag , of type Personal Access Code , to one Master record. Used as a Tag, when the door is in Personal Access Code mode. This number must be a unique value in the database and may not exceed 9 digits.
PIN	: Personal Identification Number , associated with one Master record. A PIN may be required, according to the system configuration, in addition to Tag presentation for greater access security. A PIN is always used in conjunction with a Tag , for example, when the door is in Tag+PIN mode. This number is not a unique value in the database.
Read/Write Tags	: A Tag from which data may be read, and to which data may be written.
Reader	: A device that reads Tag data and makes this data available to the Controller via the

TERM	EXPLANATION
	Terminal bus. In the IXP200 system the term “reader” refers to the combination of a Remote Reader (or equivalent) and a Door Terminal or Portal Terminal.
Reason Code	: A code describing a reason for requesting access (usually an exit) at a given Terminal .
Relaxed Anti-Passback	: See Anti-Passback – Relaxed .
Relaxed Exit Conditions	: If this condition is selected, a valid Tag-holder will be able to exit after his Access Pattern has elapsed.
Remote Reader	: A unit that has the ability to read Tags but cannot communicate directly with a Controller. A Remote Reader must be connected to a suitable ImproX Terminal (typically the ImproX DT or PT units) in order to be able to communicate with the associated system Controller. Some Remote Readers have keypads. All Remote Readers include an antenna and associated electronics. Some devices, such as the ImproX Infrared Receiver and the ImproX RF UHF Receiver are connected into a system in the same way as Remote Readers.
Server PC	: A separate PC, connected to the same network as the Host PC, which can be used to store the database.
Site	: A Site consists of one Host PC, optionally with a Database Server, and associated ImproX units. An Editing Workstation PC is optional.
Site SLA	: (See Site and SLA).
SLA	: (See Super Logical Address).
Slave	: A hardware unit (Terminal) under the control of another hardware unit (Controller).

TERM	EXPLANATION
Strict Anti-Passback	: See Anti-Passback – Strict .
Super Logical Address	: The Logical Address format which totally defines the unique address of a unit in a system. This has the form "01010101". Site-Host-Controller-Terminal (i.e. 2 digits each).
System	: An IXP200 Access installation containing one Site.
Tag	: A user's proximity access card.
Tagholder	: A person to whom one or more system Tags have been allocated.
Access Group	: Grouped Access Patterns which may be assigned to a Tag , and named as a group for easy selection. Each Access Group has up to eight Access Patterns .
Tag Level	: One of four levels which qualify Tag access and allow additional functions.
Terminal	: A Slave device which communicates with a Controller via an RS485 bus, and operates according to pre-defined modes. For example, a unit which captures access data (from Tags and/or a keypad) or which controls access points (such as doors). A type of unit which interfaces directly to an IXP200 Controller via an RS485 Terminal Bus. Terminals may be readers or non-readers, but never remote readers.
Terminal Bus	: An RS485 Bus which interconnects a Controller with the associated ImproX Terminals.
Terminal Name	: Each Terminal must be named by the Operator when configuring the system. The name used must be identical to the name used on the ImproX Unit Location Chart for the system, as well as any interconnection diagram used.
Time Triggered Action	: An internally initiated time-dependent occurrence that triggers an Action in the

TERM	EXPLANATION
	system.
Unassigned Unit	: An ImproX hardware unit with a Fixed Address and a Logical Address . The Operator must assign the unit to an Access Control Point.
Unit Location Chart	: Impro-supplied chart for use during installation of the hardware.
Valid Tagholder	: A person who has been assigned a Tag and an Access Group.
Zone	: A physically bounded area containing one or more Doors , for the purposes of anti-passback management.

ABBREVIATIONS

ABBREVIATION	MEANING
APB	: Anti-passback.
GUI	: Graphic User Interface.
IP	: Internet Protocol.
IR	: Infra-red.
OEM	: Original Equipment Manufacturer.
RF	: Radio frequency.
SLA	: Super-Logical Address.
UHF	: Ultra-High Frequency.

USER'S NOTES

USER'S NOTES

USER’S NOTES

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_sys-swm-en-12 Section 7.doc
------------------	----------	-----------	---

IXP200

Software User Manual

SECTION 8

APPENDICES

IXP200 Software User Manual

SECTION 8

APPENDICES

APPENDIX 1 - BASIC WINDOWS INFORMATION FOR THE USER.....	3
Graphic User Interface.....	3
IP ADDRESS	4
VIRTUAL NETWORK ADAPTER	4
Computer which has a Modem Card installed as well as a Network Card	4
For Computers which have a network card but no server	4
Assigning automatic private IP addresses for a simple network	5
For computers which have no network card installed	5
IP Configuration	6
Win 2000 – Setting up a Loop-back Adapter.....	6
APPENDIX 2 – ENGLISH TERMINOLOGY.....	18
REGIONAL DIFFERENCES IN ENGLISH TERMINOLOGY	18

APPENDIX 1 - BASIC WINDOWS INFORMATION FOR THE USER



Conventions used in MicroSoft Windows can be puzzling to any new user and especially so when applied to a large database system such as the IXP200 Access Control Software.

This introduction is not intended to teach the Reader how Windows works, but rather to introduce the concepts as they apply to the Access System and thereby help to ensure proper use of the System.

Graphic User Interface

The first concept to grasp is that of the GUI (pronounced 'goeey'), the Graphical User Interface. This is illustrated above. The arrow (representing the 'mouse') rests on a graphic representation marked 'Shortcut to Engine'. Such a graphic is also called an 'icon' because the graphic is 'live'. In other words, the graphic enables the computer to do something – to carry out a command. The classical definition of an icon is, "A small symbolic picture of a physical object that represents a particular option and can be selected to exercise that option."

In Windows, almost all commands are exercised through icons as this is the quickest way of selecting a task and activating it. The operator does not have to type nor remember obscure details, or the procedure which make these programs work.

IP ADDRESS

The IP (Internet Protocol) address is crucial to the operation of the database and the System as a whole. The IP address is the address of the Server, which in the case of IXP200 is the Host PC.

The System needs an address for each unit in order to operate correctly, and therefore the IP address is essential.

VIRTUAL NETWORK ADAPTER

As the small IXP200 is a small Access Control System which is not network-based, it is necessary to setup a Virtual Private Network so that an IP address can be acquired.

The Windows help files have the following instructions:

Computer which has a Modem Card installed as well as a Network Card

To set up a Dial-Up Networking connection to your corporate network

- [1] Double-click **My Computer**, double-click **Dial-Up Networking**, and then click **Make New Connection**. If it is your first Dial-Up Networking connection, you will be prompted automatically.
- [2] In **Select a Device**, click **Microsoft VPN Adapter**, and then click **Next**.
- [3] In **Host name or IP Address**, type the name or IP address of the virtual private networking server for the network to which you want to connect.
- [4] For example, type:

pptpserver.mycompany.com

or

172.16.48.1
- [5] Click **Next**, and then click **Finish**.

For Computers which have a network card but no server

(Such as on a peer-to-peer network using Windows as the network system).

Assigning automatic private IP addresses for a simple network

With Windows 98 Second Edition, Microsoft TCP/IP provides a new mechanism for IP addressing, called automatic private IP addressing. If you have a small network, without a server, you can assign a unique IP address to your network adapter using the "LINKLOCAL network" IP address space. LINKLOCAL network addresses always begin with 169.254 and have the following format:

169.254.X.X

LINKLOCAL network addresses are used only for private, internal address and are not valid for host computers that are visible on the Internet.

After the network adapter is assigned a LINKLOCAL network IP address, computers can communicate, using the TCP/IP protocol, with any other computer on the network that uses the same addressing.

For computers which have no network card installed

The procedure is similar to the previous example.

A Windows 98 Second Edition computer that is configured for automatic private IP addressing can assign itself a private IP address if either of the following applies:

- (a) If the computer is not configured as a laptop, it can assign itself an automatic IP address at startup if the computer does not have a valid DHCP lease and no DHCP server is found on the network. DHCP refers to a PC that functions as the server for a network.
- (b) If the computer is configured as a laptop, it can assign itself an automatic IP address if no DHCP server is found on the network, regardless of whether it has a DHCP lease or not.

NOTES :

1. *Automatic IP addressing allows the IP address to be configured automatically. This method decreases administration time and allows the reuse of IP addresses. It is recommended for all sizes of networks that do not have a direct Internet connection or the DHCP service available.*
2. *Static IP addressing allows you to manually enter a permanent IP address. Using this method is not recommended except as a last resort.*
3. *If a DHCP service is later found, the computer stops using the automatic IP address and uses the IP address assigned by the DHCP service. A DHCP IP address will not override a static (permanent manually entered – see above) IP address. The new, valid DHCP address will have to be manually entered.*

4. *If a computer is moved from a local area network (LAN) with a DHCP service to a LAN without a DHCP service, you can use the IP configuration utility (WINIPCFG) to release the assigned DHCP address. You can then have the computer automatically assign a private IP address.*

IP Configuration

To use the IP configuration (WINIPCFG) utility

- [1] Click **Start**, and then click **Run**.
- [2] In the **Open** box, type:

winipcfg
- [3] Click **More Info**.
- [4] To see the addresses of the DNS servers the computer is configured to use, click the ellipsis (...) button to the right of **DNS Servers**.
- [5] To see address information for your network adapter(s), select an adapter from the list in **Ethernet Adapter Information**.

NOTES :

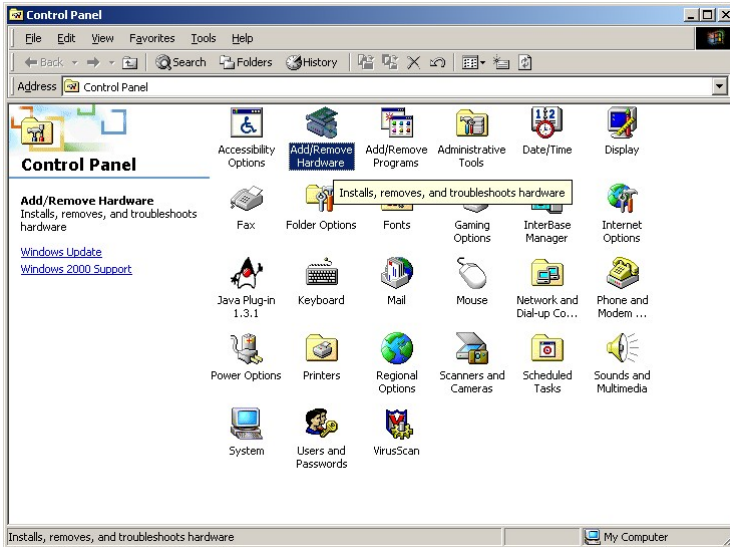
1. *The IP Configuration utility allows users or administrators to see the current IP address and other useful information about your network configuration.*
2. *You can reset one or more IP addresses. The **Release** or **Renew** buttons respectively release or renew one IP address. If you want to release or renew all IP addresses click **Release All** or **Renew All**.*
3. *When one of these buttons is clicked, a new IP address is obtained from either the DHCP service or from the computer assigning itself an automatic private IP address.*
4. *For information about assigning a simple IP address, see **Related Topics**.*

Win 2000 – Setting up a Loop-back Adapter

These pages illustrate the procedures in setting up a loopback adapter in Windows 2000.

The procedure is fairly self-explanatory. Where necessary comments are added to clarify a selection or alternative.

- [1] Select **Start** and **Control Panel**.



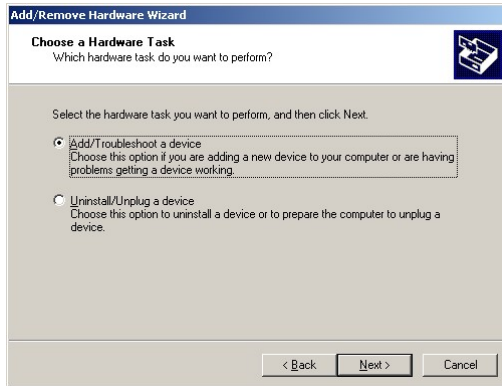
Control Panel

- [2] Select **Add/Remove Hardware**. The **Add/Remove Hardware Wizard** will be displayed.



Add/Remove Hardware Wizard

- [3] Click **Next**. The **Choose a Hardware Task** Screen will be displayed.
- [4] Select **Add/Troubleshoot** and click **Next**.



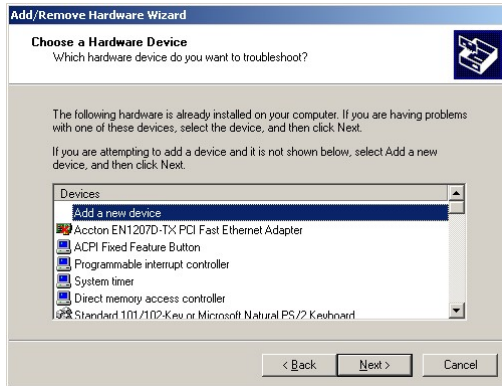
Choose a Hardware Task Screen

- [5] The System will search the Hardware list (**New Hardware Detection Screen** displayed).



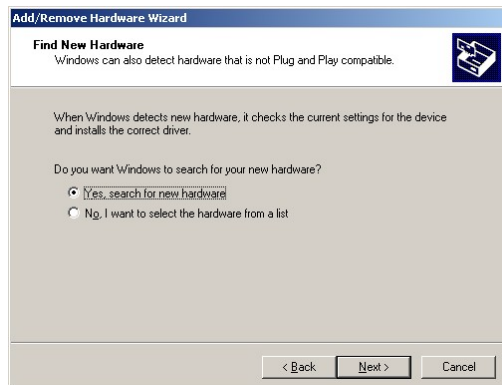
New Hardware Detection Screen

- [6] On the **Choose a Hardware Device Screen** which is then displayed, click **Add a new device** and then click **Next**.



Choose a Hardware Device Screen

[7] The **Find New Hardware Screen** will be displayed.

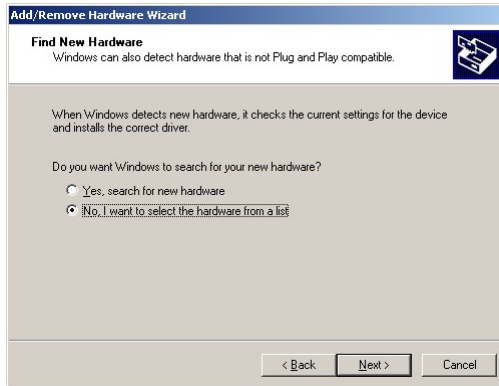


Find New Hardware Screen

[8] Select **No, I want to select the hardware from a list**.

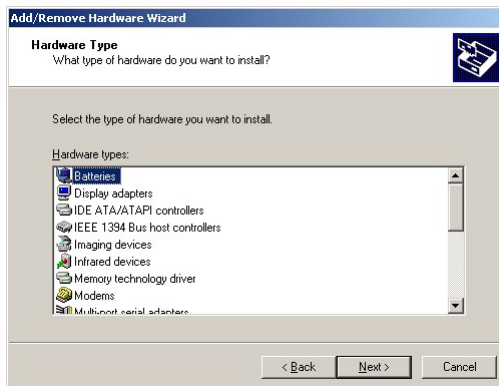
[9] The reason for this selection is that the loopback adapter is a system program and not a physical device and therefore the actions required have to be specifically chosen.

[10] Click **Next** to display the list.



Find New Hardware Screen

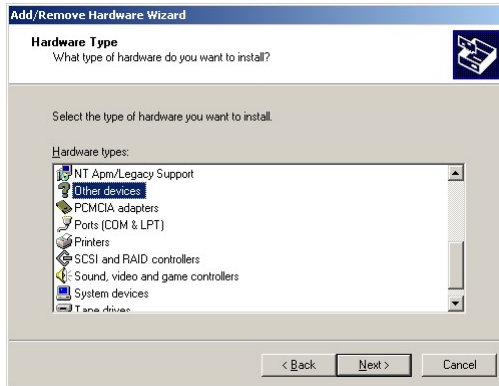
[11] The **Hardware Type** Screen will be displayed.



Hardware Type Screen

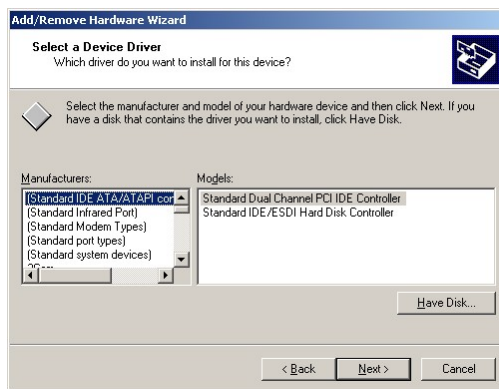
[12] Scroll down to find **Other Devices**.

See next page



Add/Remove Hardware screen

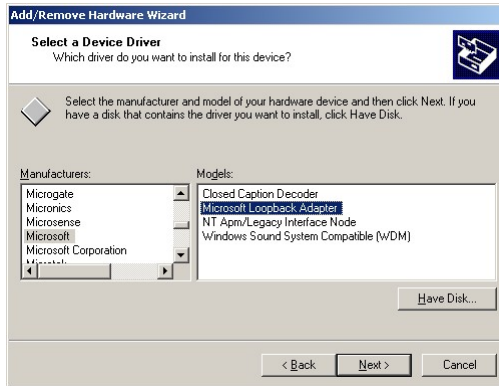
[13] Select **Other Devices**.



Select a Device Driver Dialog

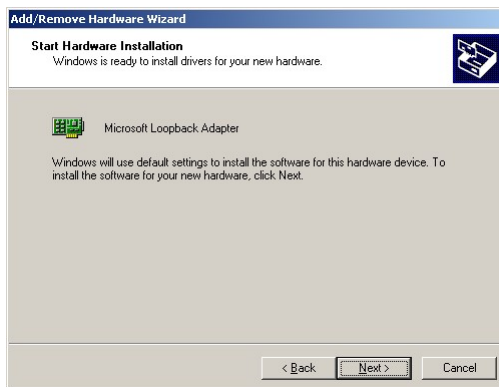
[14] Scroll down to find **Microsoft** from the **Select a Device Driver Screen** and then click on **Microsoft**.

See next page



Select a Device Driver Screen

[15] In the **Models Screen** select **Microsoft Loopback Adapter** and click **Next**.



Models Screen

[16] The System Settings will display the **Start Hardware Installation Screen** to install the driver programs.

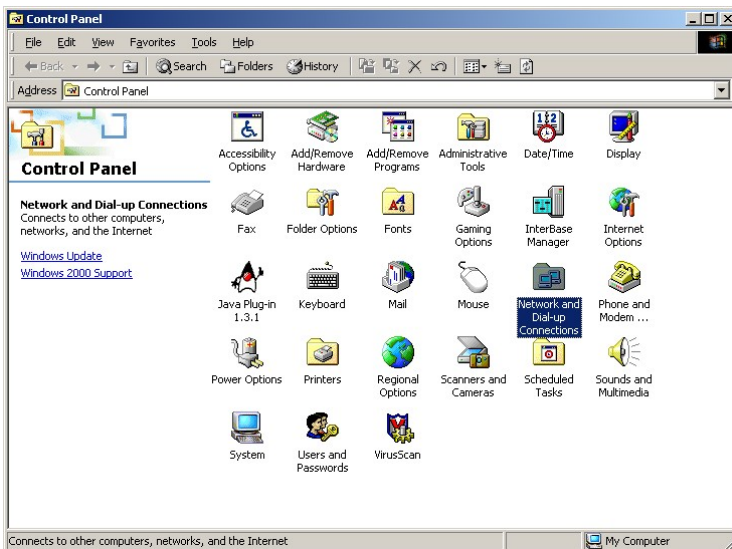
[17] Click **Next**.



Completing the Add/Remove Hardware Wizard Screen

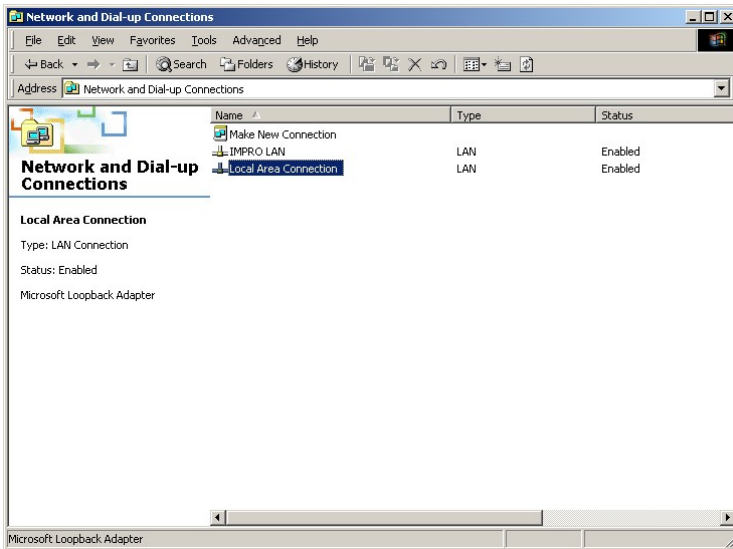
[18] The Drivers are loaded and the system displays the **Completing the Add/Remove Hardware Wizard Screen**.

[19] Click **Finish** to display the **Control Panel Screen**.



Control Panel Screen

Select **Network and Dial-up Connections**.

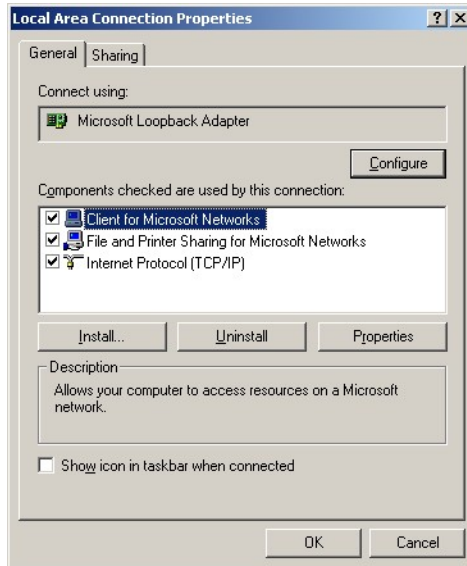


Network and Dial-up Connections Screen

[20] Select **Local Area Connection**.

[21] The next task is to choose the connection properties, protocols and addresses.

See next page



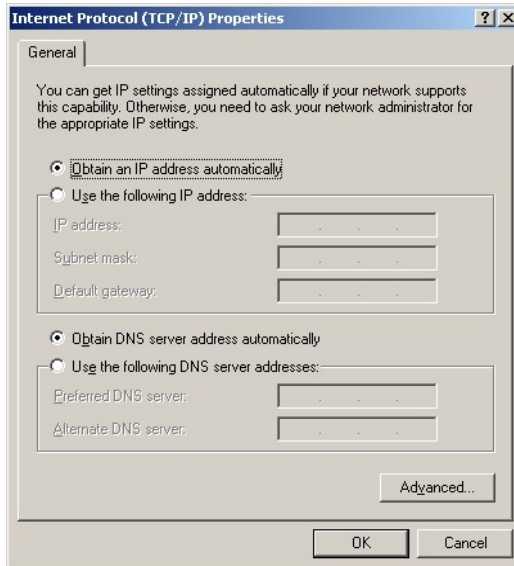
Local Areas Connections Screen

[22] Select **Internet Protocol (TCP/IP)**.

[23] TCP/IP (Transfer Control Protocol/Internet Protocol) is the data exchange system that the IXP200 Access Control System uses.

[24] Click **Install**.

See next page

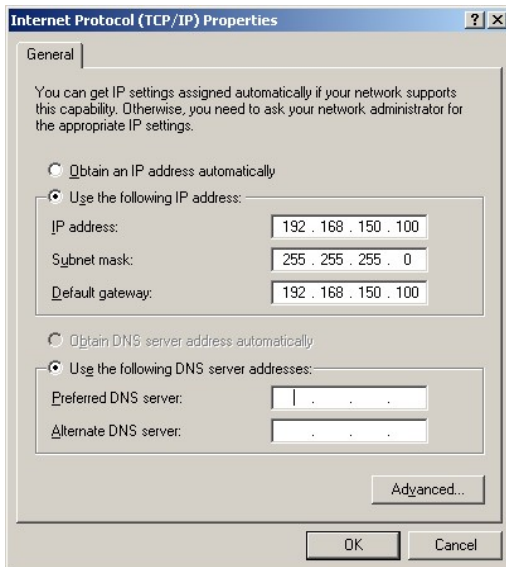


Internet Protocol (TCP/IP) Properties Screen

[25] In order to work an IP address needs to be entered.

[26] Select **Use the following address**.

See next page



Enter addresses on Internet Protocol (TCP/IP) Properties Screen

[27] The display waits for the user to enter the addresses required.

[28] Enter the addresses as displayed above:

IP Address	192 168 150 100
Subnet Mask	255 255 255 0
Default Gateway	192 168 150 100

[29] After typing in the addresses click **OK**.

The display will return to the settings screen. Close the screen to return to the Desktop and then Reboot to activate the loopback adapter.

See next page

APPENDIX 2 – ENGLISH TERMINOLOGY

REGIONAL DIFFERENCES IN ENGLISH TERMINOLOGY

The table below gives the US English equivalents of terms that may appear in UK English in this manual.

UK ENGLISH	US ENGLISH
Lift	: Elevator
Ground floor	: First floor
First floor	: Second floor
Reception	: Lobby
Car park	: Parking lot
Surname	: Last name
Tick	: Check

INDEX

Access System, 3

Adapter, 4, 6, 12

address, 4, 5, 6, 16

administration time, 5

administrators, 6

commands, 4

computer, 3, 5, 6

Control Panel, 6, 13

Conventions, 3

DHCP, 5, 6

Dial-Up Networking, 4

graphic, 3

graphic representation, 3

Graphical User Interface, 3

GUI, 3

Host PC, 4

icon, 3

Internet Protocol, 4, 15, 16, 17

IP, 4, 5, 6, 15, 16, 17

IP address, 4, 5, 6

LAN, 6

laptop, 5

LINKLOCAL, 5

local area network, 6

loopback adapter, 6, 9, 17

Modem Card, 4

network adapter, 5, 6

network-based, 4

peer to peer network, 4

server, 4, 5

Server, 4

system program, 9

TCP/IP, 5

UK English, 18

US English, 18

users, 6

Virtual Private Network, 4

VPN, 4

Windows, 3, 4, 5, 6

WINIPCFG, 6

USER'S NOTES

USER'S NOTES

APPLICABILITY OF THIS MANUAL

The last two digits of the standard Impro stock code indicate the issue status of the item concerned. This manual is applicable to the IXP200 Series Software, Version 6.0 onwards. The next issue of this section of the manual will determine the final software issue to which this manual issue is applicable.

*Please advise us of any errors or omissions in this manual
to enable us to improve our service to you.*

Thank you for choosing *Impro* products to implement your access control system.

Impro Technologies design and manufacture a wide range of technically advanced, high quality, reliable Access Control and Asset Identification and Management Systems. Please contact your distributor to find out more about our products, or advise us of your needs for specialized products not yet in our extensive and continually expanding range.

Patents and registrations for ImproX designs are pending (world-wide). Registration of the trademarks 'IXP200' & 'ImproX' is pending (world-wide).

IXP308-0-0-GB-11	Issue 12	June 2007	k:\Custman\ IXP200\ English Manuals\ IXP200_sys-swm-en-12 Section 8.doc
------------------	----------	-----------	---