

AX200 & i-BOX

Installation & User Guide



Axxess Identification Ltd

27-28 Shrivenham Hundred Business Park,
Watchfield, Swindon, Wiltshire SN6 8TZ
United Kingdom

Tel: +44 (0)1793 784002

Fax: +44 (0)1793 784005

Email: info@axxessid.com

Installation & User Guide

Microsoft® is a registered trademark of Microsoft Corporation.
Windows™ is a registered trademark of Microsoft Corporation.

Document Title: AX200 & I-BOX Installation & User Guide v13.07.07

This document contains proprietary information of Axxess Identification Ltd. Unauthorised reproduction of any portion of this manual without the written authorisation of Axxess Identification Ltd is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. Axxess assumes no responsibility for incorrect information this manual may contain.

©2007 by Axxess Identification Ltd
27-28 Shrivenham Hundred Business Park, Watchfield, Swindon SN6 8TZ United Kingdom

Telephone +44 (0)1793 784002
Fax +44 (0)1793 784005

Email info@axxessid.com
Web www.axxessid.com

Installation & User Guide

License Agreement

NOTICE TO USER: THIS SOFTWARE PACKAGE IS A CONTRACT. BY INSTALLING THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Use of the Software. You may install and use the software only for the purpose intended.
2. Copyright. You may not duplicate or copy the software or documentation, except that you may make one backup copy of the software. All copies must bear copyright notices contained in the original copy.
3. Limited Warranty. Axxess Identification warrants that the software will perform substantially in accordance with the printed documentation when correctly installed on a properly configured computer for which it is intended. Axxess Identification warrants the compact disc upon which this product is recorded to be free from defects in materials and workmanship under normal use for a period of five years from the date of purchase. During the warranty period Axxess Identification will replace compact discs, which prove to be defective.
4. Axxess Identification does not warrant and cannot warrant the performance or results you obtain by using the software or documentation. In no event will Axxess Identification be liable to you for any consequential, incidental or special damages. For further warranty information, please contact Axxess Identification.

Installation & User Guide

Contents

.....	1
AX200 Installation	8
AX200 Software Setup	8
TCP/IP Configuration (Fixed IP Address)	10
IP Definitions Applicable to the AX200	11
AX200 & i-BOX Connections	12
9 Way i-BOX I/O Connection	12
Sounder /Beacon for i-BOX (IC-ASB)	13
AX200 Expander Board Connections	14
Break glass Wiring AX200.....	15
Break glass wiring AX50/AX100	16
.....	17
.....	18
AX200 Software	19
Operating Systems.....	19
Software Installation	19
Starting the AX200 Software	22
Language Selection	23
Password Reminder.....	23
Windows™ Classic or Graphic Style (XP) Screen.....	23
Backup & Restore	24
Email Backup Settings	25
Standard Query Language (SQL).....	26
Database Integrity Check.....	27
Communication between the AX200 Software and Controller	27
Plug & Play Devices.....	28
Controller Status & Control	29
High Security Mode (HSM).....	29
Door Unlock Mode	30
Date and Time	30
On & Offline Operation.....	30
Force Download & Clear Controller	31
Performance Analyzer.....	31
Transaction Screen.....	32
Who's In/Out List.....	33
Display Filters	34
Photo Display.....	34
Email	34
Save on Exit	36
Test Wizard	36
Cardholder	41
Main Settings	41
Card Number	41
Imprint Number.....	42
Employment.....	42
Department.....	42
Access Group	42
Card Type.....	42
Card Status.....	42
Pin Code.....	42
Time Zone	42

Installation & User Guide

Photo.....	44
Photo ID	44
Add a Photo.....	45
Capture Picture from Camera.....	45
Import Picture from File.....	46
Templates.....	46
Add New Card Wizard.....	46
Card Replacement Wizard	47
Card Diagnostics.....	48
Search	49
Card 0 Function	50
Print Current Card Details	50
Database Fields per Cardholder.....	50
Main Settings Tab.....	50
Other Info.....	51
Employer	52
Mode Settings.....	53
High Security (Hi Sec).....	54
Extended Door Open Time (Ext'd Door)	54
Set High Security Mode (Set Hi Sec).....	54
Set Latch	54
Time Zone	54
Personal Info.....	54
Vehicle info	55
Access Point Configuration.....	56
Access Point Settings.....	56
Access Identity.....	56
Access Point Name.....	56
Door Comments.....	57
Door Release Time	58
Start-up Mode Settings	58
Door Contact Settings.....	58
PIN Settings.....	59
Device Parameters.....	60
Device Group.....	60
Device Type.....	60
Hardware Version	60
Firmware Version.....	61
Batch Number.....	61
Serial Number in Batch	61
Database Stamp	61
Access Groups.....	61
Creating a new access group	62
Device Manager	62
Automatic IP Setup	63
Device Status Indication.....	65
Device Settings.....	67
Fire alarm	68
Test Connection.....	68
System Settings	69
Site Info	69
Test Wizard.....	70
E-Mail Facilities.....	71

Installation & User Guide

E-Mail Unknown Format to Axxess ID	71
DB Maintenance	72
Compact Database	72
Backup Settings.....	73
Database Restore.....	73
Export Cardholders	73
Import Cardholders	73
Export Photo ID Templates	73
Import Photo ID Templates	73
Firmware Settings.....	73
Rollback.....	74
Hidden Functions	74
General Settings	76
Maximum PIN Number 1~6.....	76
Number of Lines in Screen.....	76
Transaction Screen Pause.....	76
COM Port Timeout.....	76
COM Port Retry Times.....	76
Link Alive Retry Times	77
Function Settings	77
COM Port Settings.....	77
Multiple/Single Card Format.....	78
Default Access Level.....	79
Default Time Zone	79
Default.....	79
Third Party File	79
Format & Statistics.....	79
Card Type Information.....	80
Facility Code.....	80
Card Matching.....	81
Card Format Analyzer & Format Configuration	81
Security Settings.....	81
Adding a New User	82
Adding a New Authorisation Group.....	82
Report.....	83
Cardholder Brief.....	84
Cardholder Details	85
Log File.....	85
Dossier	85
Work Spell	86
Operators.....	86
Environmental.....	86
System Summary.....	86
Quick View.....	86
Printing	87
Format Types.....	87
Destination.....	87
i - BOX.....	88
Environment.....	89
i- BOX Parameters	90
Sensor Settings.....	90
Alarms	91
i- BOX Settings	92

Installation & User Guide

PDU (Power Distribution Unit)	93
Details	94
Sensor	97
Hardware Connection Details	97
Sensor Settings	97
Isolate	98
PIR	99
Dust Particle Sensor	100
Dust Particle Sensor	101
Mains Present Sensor.....	102
DTU (Data Transfer Unit).....	103
Connecting the DTU.....	103
DTU	105
Add a New Door using a DTU	105
Adding Card Formats using a DTU.....	106
DTU Step by Step	106
DTU Operation.....	107
DTU LED Indicators	107
Clear DTU.....	108
Removing the AX200 Program.....	108
Anti-Virus.....	109
Readers.....	111
Fingerprint Reader	111
Connection Details.....	111
Proximity Readers.....	115
How to connect the reader to the host.....	115
Software Configuration.....	115
AXM Readers.....	117
Output Type.....	117
Connection Details.....	117
Proximity Request to Exit	118
Technical Details.....	118

Installation & User Guide

AX200 Installation

This Installation Guide details the initial setup and steps to get the AX200 software operational. For further information and additional features please refer to the AX200 software manual.

Complete software installation and TCP/IP configuration must be performed whilst logged into Windows with full Windows Administration rights.

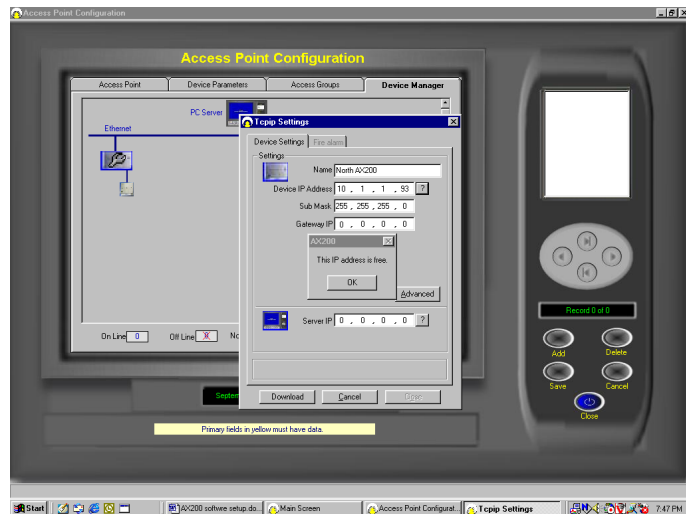
AX200 Software Setup

1. Install the AX200 software. Insert the CD, if auto run is disabled then click Start and select Run. Enter d:\setup.exe in the text box and click OK. (Note substitute the CD-ROM drive letter in place of d) Follow the on screen instructions to complete the installation.
2. Ensure that the PC is connected to the network and the AX200's are connected to the network but powered off.
3. Ensure that the PC has a [fixed IP address](#).
4. Start the AX200 software and enter the user name and password to login. The default user name is "1" and the default password is "1". Allow the software to initialise.
5. Power up the first AX200 and the AX100(s) connected to this controller.
6. Click on the Access point button located near the bottom left on the screen.
7. Click on the last Tab Sheet labelled as Device Manager.
8. Wait for approximately 10 seconds and the device manager will seek all of the AX200's connected to the network that are powered on. New AX200's will be displayed in red; previously configured AX200's will be displayed grey. (AX200's previously configured but not online will be displayed as Grey with a red cross) Double click on the Red AX200.



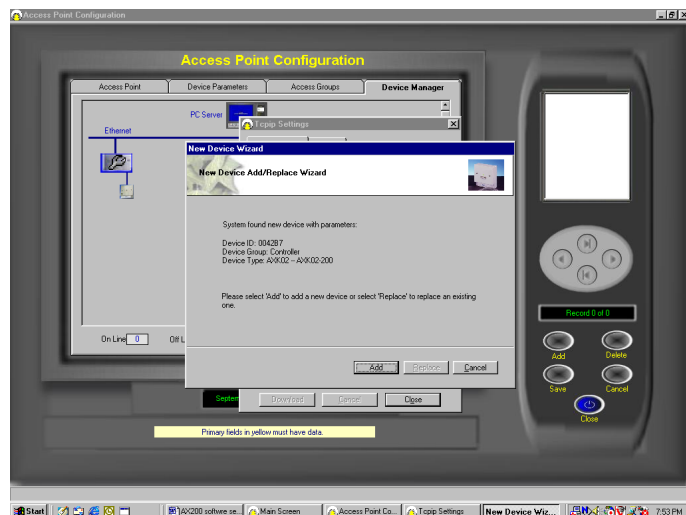
Installation & User Guide

- Click on the ? at the end of the Server IP address. The Server IP address will fill in. On local area networks (LAN) the Device IP address and the Server IP address will match for the first 3 numbers (Segment address) and the last number will be unique to the AX200.



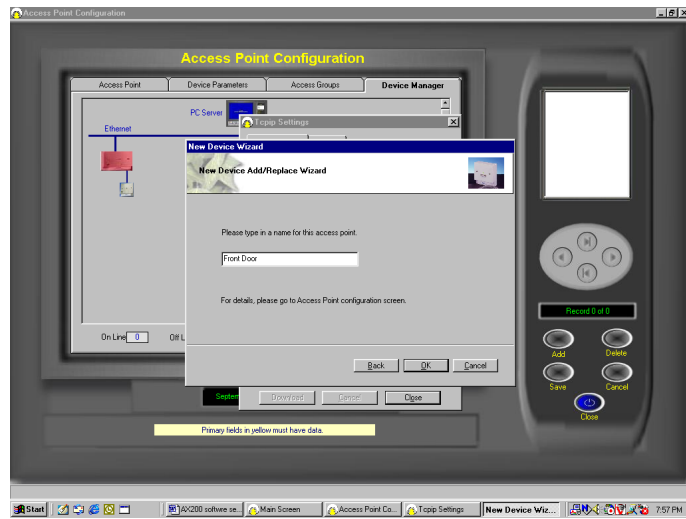
- Enter a name for the AX200 and an IP address for the device. To ensure that this IP address is not already assigned click on the ? next to the device IP address. Do not use an IP address that is already assigned as this will cause the system not to operate correctly. Enter the subnet mask and if advised by the network administration manager, enter the gateway IP address for this device.

- Click on the download button and confirm by clicking yes. After approximately 5 seconds the AX100 add wizard will appear.



Installation & User Guide

12. Click Add. Select the type of reader (with or without PIN) then click next. Enter a suitable name for the door location being added. Then click OK. After a brief period of time the add wizard will be completed. Access point specific settings such as lock times, IN/Out configuration may be set under Access point / Access point. When a new AX100 is added the access point screen will be displayed. Note if two AX100's are connected to the AX200 after 15 seconds the Add wizard will appear again for Device two to be added.



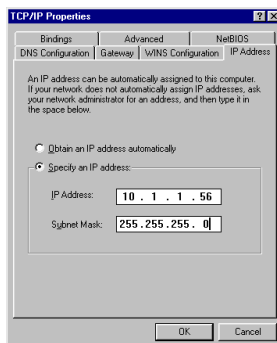
13. Close the TCP/IP settings screen and close the device manager screen or access point screen.
14. From the main screen click on the cardholder button and add a card(s) When the cardholder screen is exited the information will be downloaded to the relevant controllers and the door will lock.
15. Power up the next AX200 to be added and repeat steps 6 – 13 until all controllers are configured.

TCP/IP Configuration (Fixed IP Address)

Refer to this section if the PC does not have a fixed IP address or for additional IP address information.

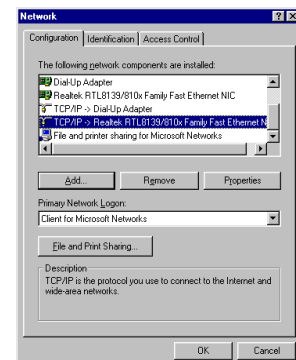
To specify a fixed IP address

Click the Windows Start button then select setting and select control panel. Double Click on the Network icon. In the components box scroll down to TCP/IP Network card name and click on it. (On Windows XP the control panel may be displayed directly from the Windows Start button) Click on Properties Button.



Select the IP Address Tab

Ensure that the system is set to specify an IP Address and that a valid IP address is in the IP address box. (Note – most organisations allow fixed IP address ranges, and a suitable IP number is normally obtained from the network administration manager) Enter a valid subnet mask



Installation & User Guide

address. Typically this is set to 255.255.255.0

Click OK or Apply.

Click OK to exit the network setup and close the system control panel window. If prompted to reboot or to insert the Windows installation disk please follow the on-screen prompts.

IP Definitions Applicable to the AX200

IP Address

An IP address is a unique identifier for each controller, PC or other Ethernet device. The IP address range is from 0 to 255, where 0 is null, 1 to 254 are valid numbers and 255 is a broadcast number. (Example – 10.1.1.25) Note – Consult with the Network Administrator before using any IP address to avoid duplicate numbers

Subnet Mask

This is the mask or range of address that the device is allowed to talk to, typically the broadcast number is used (Example 255.255.255.0 in this example permission is granted to talk to all devices on the network)

LAN

Local Area Network refers to structured Ethernet cabling within a local area such as a single building.

WAN

Wide Area Network, refers to a group of LAN's connected together such as a group of buildings.

VPN

Virtual Private Network, refers to a separate IP numbering system applied on WAN's that allows different equipment in various locations to communicate as a LAN

Gateway

The Gateway is the device used to channel IP traffic between LAN's over a WAN.

IP Port number

The IP port number is the number assigned for the communications over TCP to that specific IP address. The AX200 uses Port numbers 4848 for the controller and 1818 for the AX200 software.

Firewall

A firewall may comprise of a physical device or software on a PC and it is designed to stop malicious attacks by computer hackers or virus. **Note** Firewalls may also stop communication between the AX200 and the software unless the specified IP port numbers are listed in both the TCP and UDP protocol safe list on the firewall.

LAN Configuration

When working on a local area network (LAN) all devices that are configured to operate with fixed IP address such as the AX200 controller, will require the same segment address. So if the Server (PC) IP address is 10.1.1.15 then the AX200 will require an IP address with the same segment such as 10.1.1.52. When building a private network (if there is not already one there) it is

Installation & User Guide

recommended that the segment address is 10.1.1.x Use the subnet mask as 255.255.255.0 and the gateway IP address should be 0.0.0.0

WAN Configuration

When working on a wide area network (WAN) all devices that are configured to operate with fixed IP address such as the AX200 controller, will probably have a different segment address. So if the Server (PC) IP address is 10.1.1.15 then the AX200 will require an IP address with the appropriate segment such as 10.1.2.52. Use the subnet mask as 255.255.255.0 and the gateway IP address must be configured (Please consult the Network Administrator for all IP Settings)

VPN Configuration

Generally configure Virtual Private networks as per the LAN Configuration setup. (Please consult the Network Administrator for all IP Settings)

Example IP Address Table

Device Name	Location	IP Address	Gateway Address	Subnet Mask Address
File & Printer Server	London	10.1.1.10	10.1.1.1	255.255.255.0
Sales PC	London	DHCP	DHCP	DHCP
AX200 PC	London	10.1.1.35	10.1.1.1	255.255.255.0
AX200 Controller	London	10.1.1.36	0.0.0.0	255.255.255.0
AX200 Controller	London	10.1.1.37	0.0.0.0	255.255.255.0
File & Printer Server	New York	10.1.2.10	10.1.2.1	255.255.255.0
Sales PC	New York	DHCP	DHCP	DHCP
AX200 Controller	New York	10.1.2.55	10.1.2.1	255.255.255.0
AX200 Controller	New York	10.1.2.56	10.1.2.1	255.255.255.0

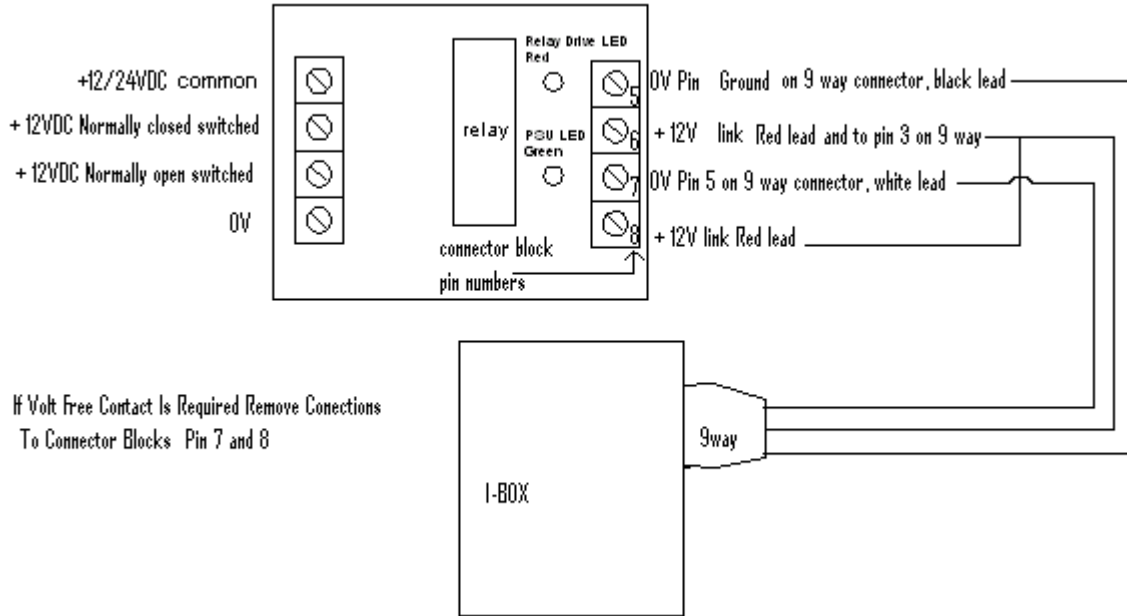
AX200 & i-BOX Connections

9 Way i-BOX I/O Connection

Table below describes the 9 way connector on the i-BOX and states the functionality of each pin.

9 WAY D	DESCRIPTION	NOTES	COLOUR
1	Not connected		
2	Breakglass 2	(switched) + 12v (pin 3)	Blue
3	+ 12v D.C		Red
4	Relay 2	Output goes low when active	Purple
5	*	Ground	White
6	Fire Input	(switched) + 12v (pin 3)	Orange
7	Breakglass 1	(switched) + 12v (pin 3)	Green
8	Relay 3	Output goes low when active	Yellow
9	Relay 1	Output goes low when active	Black

Installation & User Guide



Sounder /Beacon for i-BOX (IC-ASB)

The sounder /Beacon for the i-BOX connects directly to the i-BOX and will sound the alarm and flash the strobe for a pre-programmed period of time when an alarm condition occurs on the i-BOX.

Connect the 9 way D connector to the i-BOX.

To configure the duration select the environment button in the software.

Click on the I-box in the tree menu.

Adjust the alarm sounder period time to the desired length of time and click Save.

Installation & User Guide

i-BOX

IBOX Identity:	<input type="text" value="1342181656"/>	Batch-Serial no:	<input type="text" value="1"/> <input type="text" value="280"/>
IBOX Name:	<input type="text" value="200 -3"/>		
Firmware Version:	<input type="text" value="1.8"/>	Hardware Version:	<input type="text" value="2"/>
Application Version:	<input type="text" value="1"/>		
Host Online Timeout:	<input type="text" value="20"/> sec	Handshake Period:	<input type="text" value="5"/> sec
Force time update:	<input type="text" value="300"/> sec	Shunt Delay:	<input type="text" value="15"/> sec
Alarm Strobe Period:	<input type="text" value="0"/> sec	Alarm Sounder Period:	<input type="text" value="10"/> sec
Transaction Reporting			
Minimum Timeout:	<input type="text" value="5"/> sec	Maximum Timeout:	<input type="text" value="80"/> sec
Accumulation Period:	<input type="text" value="10"/> sec		

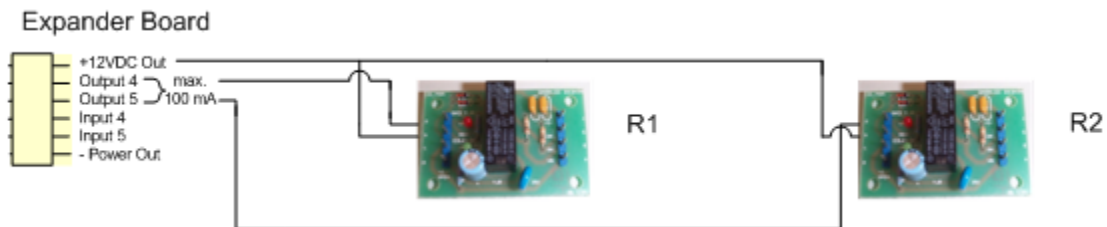
Settings

IP Address:	<input type="text" value="192.168.16.100"/>	MAC Address:	<input type="text" value="0090C2CDB827"/>
Submask:	<input type="text" value="255.255.255.0"/>	Gateway:	<input type="text" value="0.0.0.0"/>
AX100(1):	<input type="text" value="24001083"/>	AX100(2):	<input type="text" value="2400100F"/>

AX200 Expander Board Connections

Expander Board connections are located at the top-right corner of the AX200 board. Output 4 (associated with door 1) & output 5 (associated with door 2) are activated once the “**Door forced/held open alarm**” is triggered on the appropriate controller and will stay active until the alarm is cleared either by using a *valid card* or by using the *clear alarm button* on the main screen.

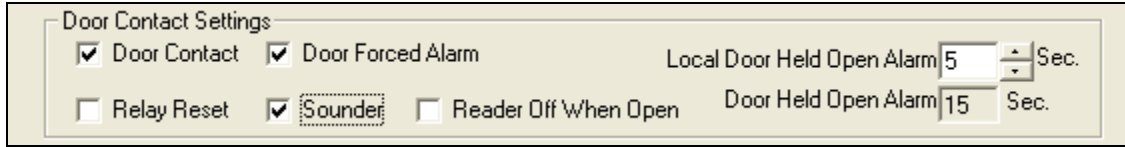
Note: the alarm is cleared only when the “**Door forced/held open alarm cleared**” transaction appears on the main screen.



Expander Board	R1	R2
12 VDC Out	PIN 6	PIN 6
Output 4	PIN 5	-
Output 5	-	PIN 5

Installation & User Guide

Door forced / held open alarm settings can be accessed through Main Screen • Access Point • (Enable) Door Contact.

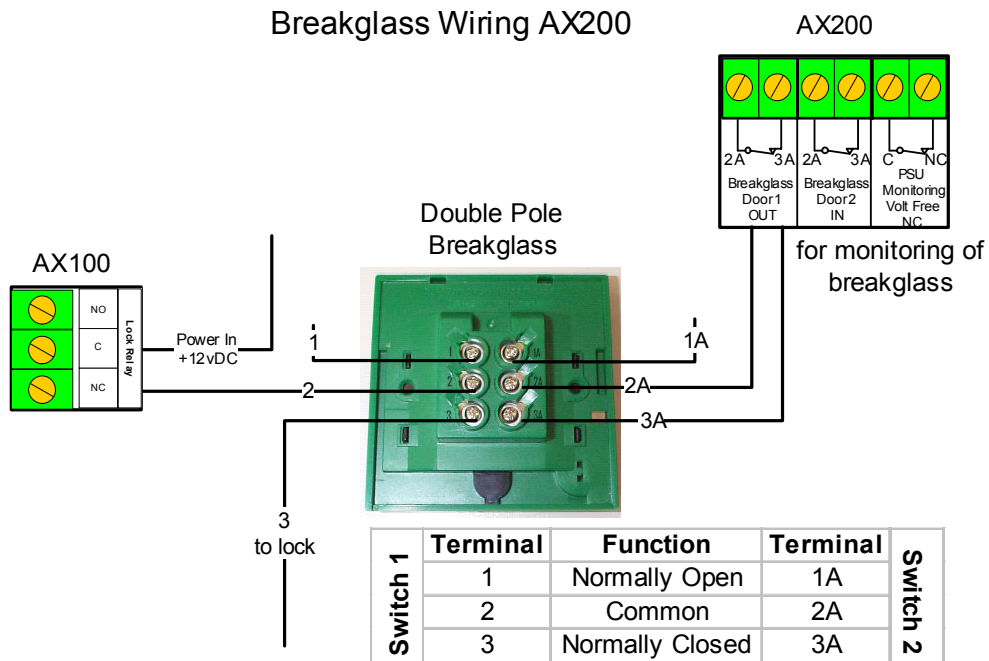


For more information about these settings please refer to Access Point Configuration • Access Point Settings on this manual.

Note: Relay No.3 generates a 1 second pulse through the **Access Granted** connection block, located at the top of AX200 board. The connection is normally closed and the pulse is generated once the access is granted through either door.

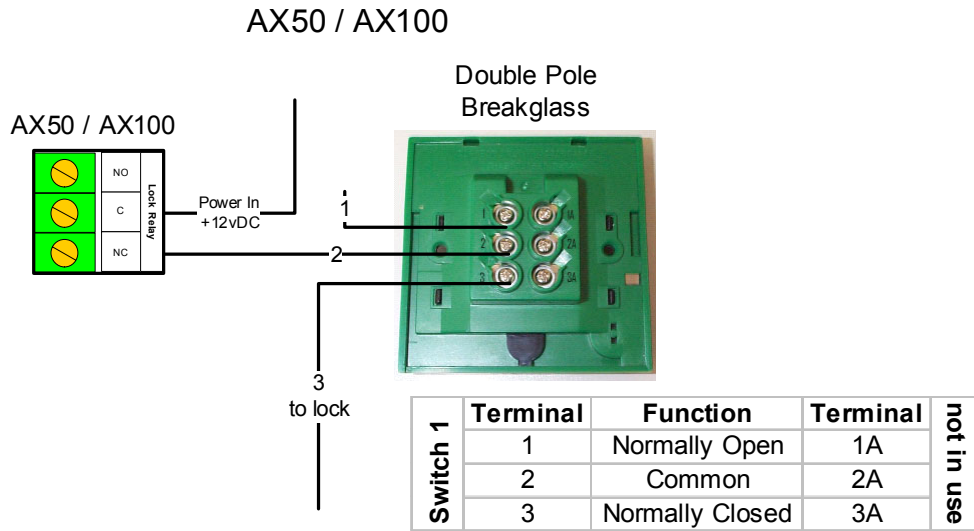
Diagrams on the following pages illustrate the connections between the AX200 components. Please note that if you are installing a brand new unit, the *Fire Alarm, Break glass & PSU Monitoring* links will not be activated until the first time they are used.

Break glass Wiring AX200

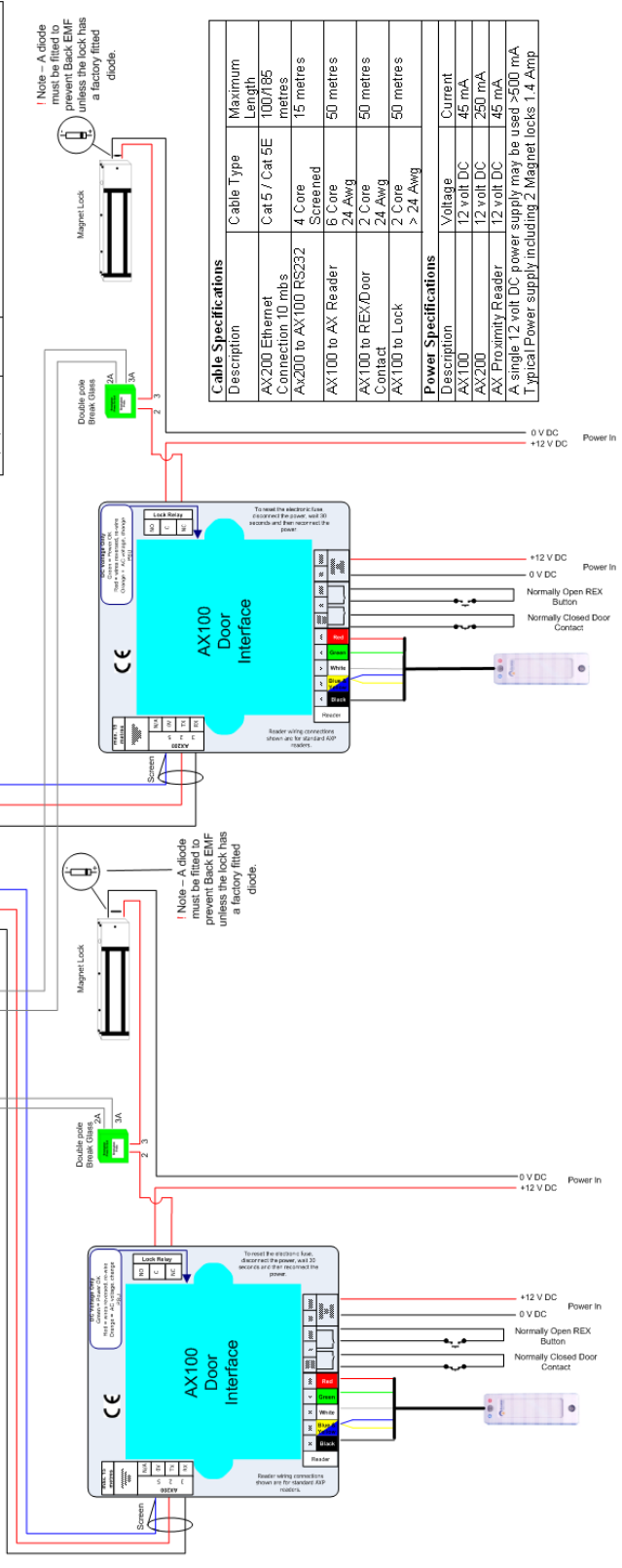
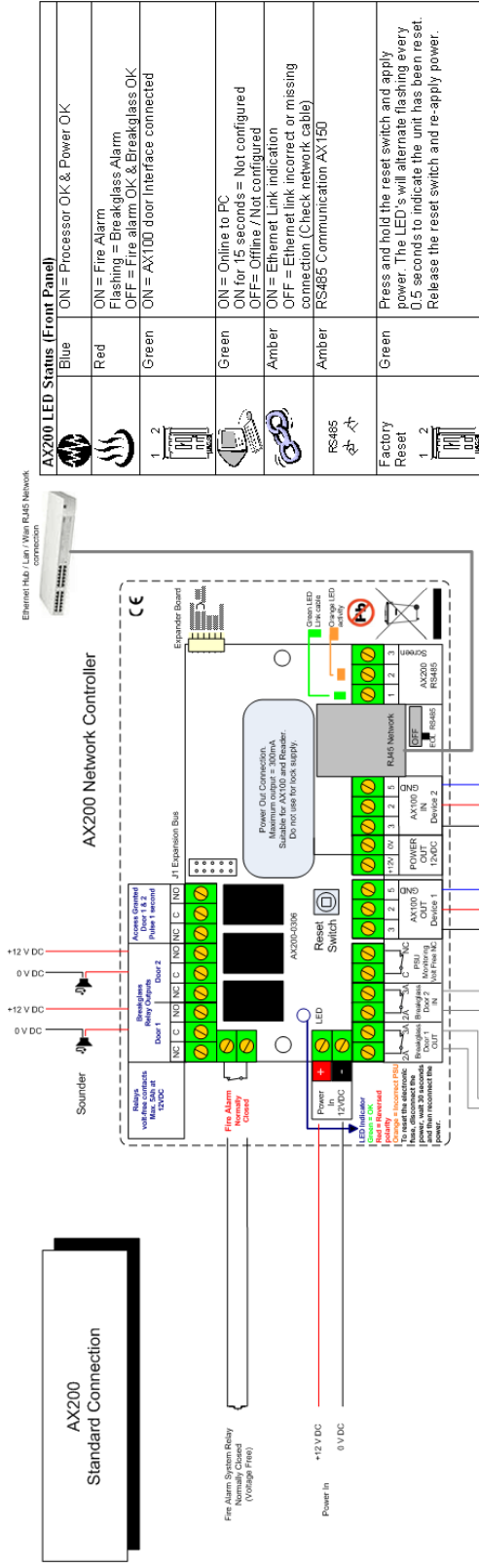


Installation & User Guide

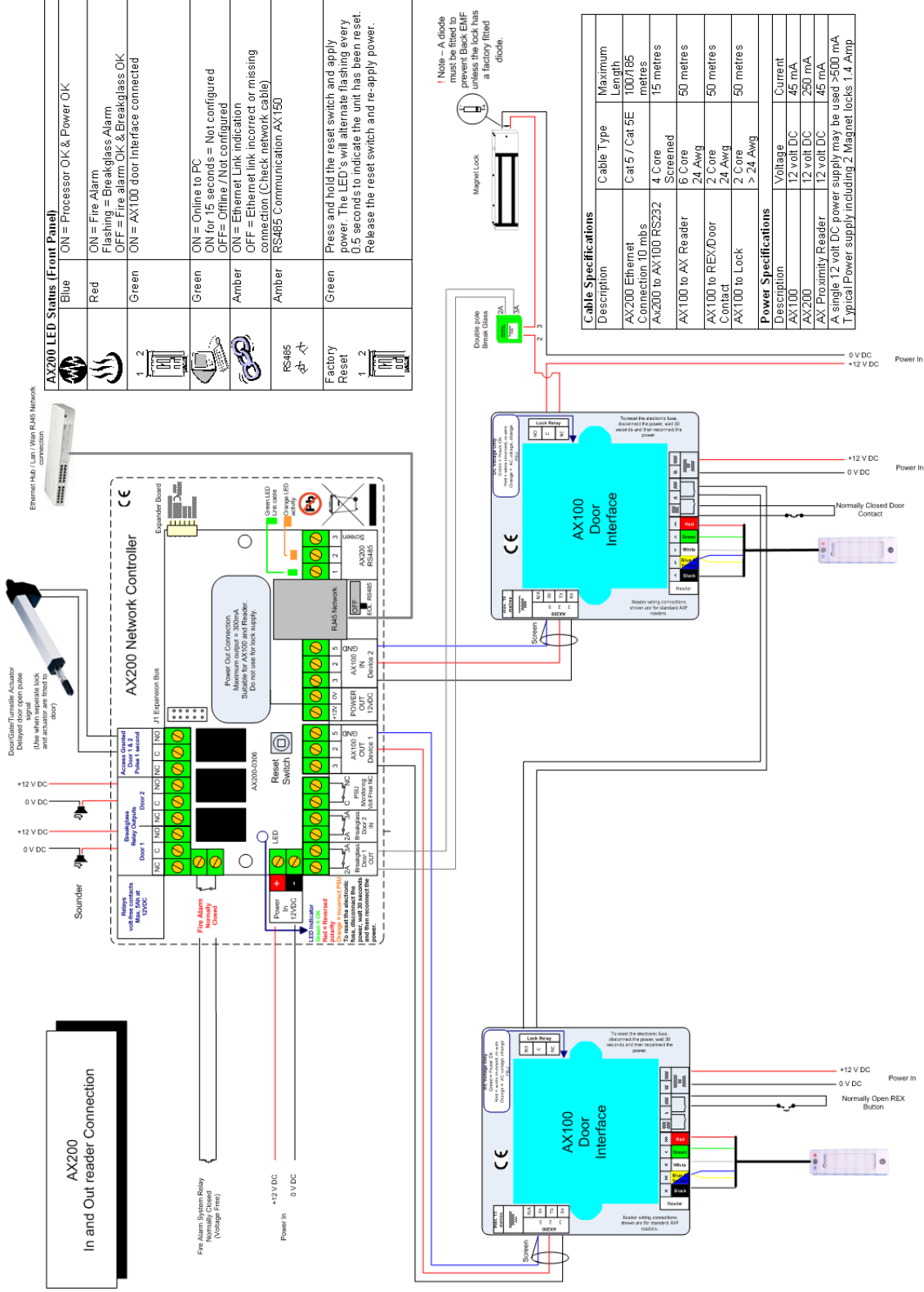
Break glass wiring AX50/AX100



Installation & User Guide



Installation & User Guide



Installation & User Guide

AX200 Software

The AX200 software is where all the programming data and cardholder information is entered.

It consists of the following:

- Cardholder
- Access Point
- System Settings
- Format & Statistics
- Security
- Reports
- Environment


The PC is where all the system configuration and data management is stored. The optional data transfer unit (DTU) enables the data that has been entered at the PC to be downloaded to the controller without the need of a physical PC connection.

The AX200 system supports a wide variety of card technologies, including proximity, magnetic stripe (AX Series), Wiegand and Wiegand compatible card types.

Operating Systems

The AX series supports a wide range of operating systems and can run on Windows NT Workstation, NT Server, 2000 Professional and Advanced, ME, XP and Vista without the need for different CD's or drivers. A number of checks are implemented within the software to ensure that the correct files for the operating system are present. The installation process automatically detects the operating system and installs the correct files and drivers.

If you are using windows Vista please note:

- The recommended screen resolution for running the AX200 software on Windows Vista is 1024×768.
- If you receive a message at the start-up saying that the "*User does not have write access to the database*", right click on the AX200 icon and select "Run as Administrator". After doing so, this icon  might appear in front of the AX200 icon.

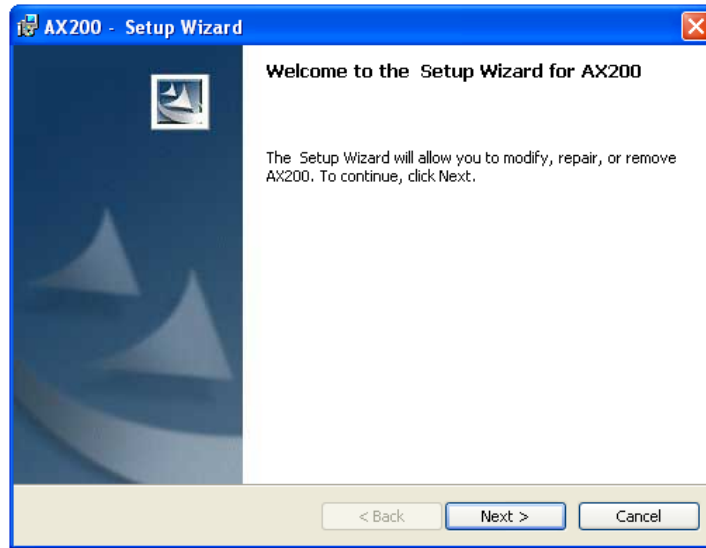


Software Installation

Put the AX200 CD in your CD drive. If the CD doesn't run automatically, click on the **Start** button and select **Run**. Type in **x:\setup.exe** on the command line (replace **x** with the letter of your CD-ROM drive).

Click **Next** > to continue with the AX200 Setup Wizard.

Installation & User Guide

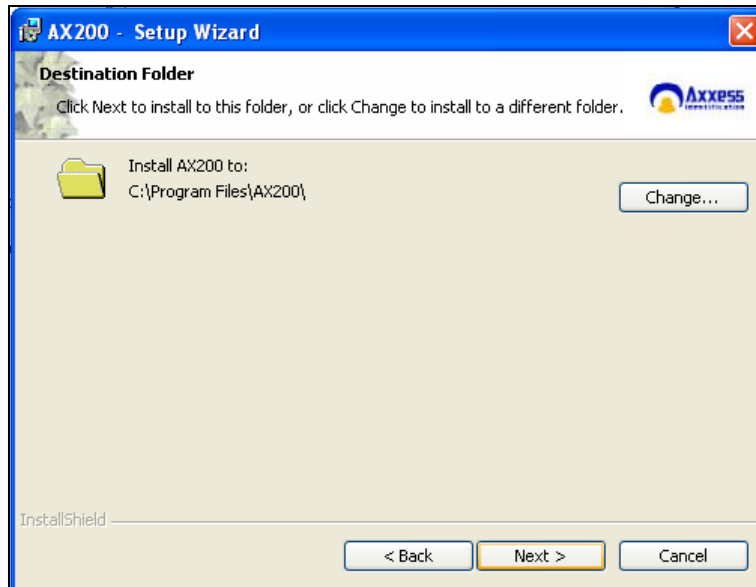


Please read the License Agreement, to accept the terms select **I accept...** then click on **Next >**.

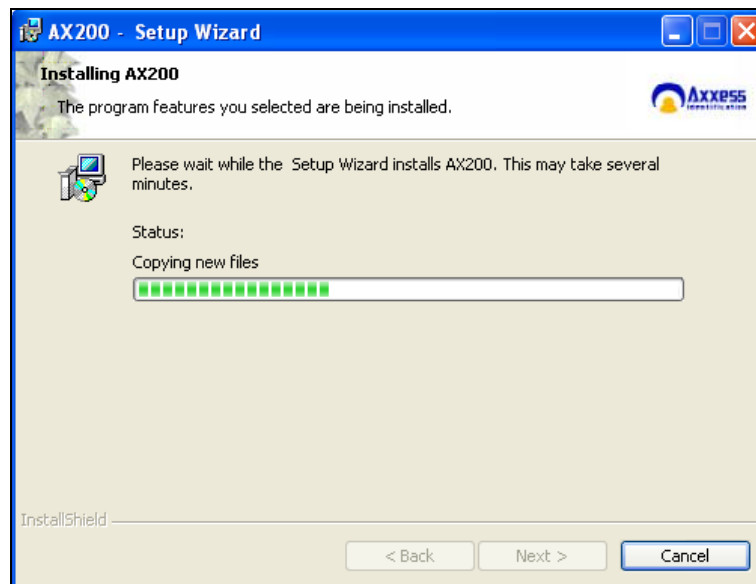


The default directory where program files are installed is **C:\Program Files\AX200** If required, click on **Change** to choose a different folder. Click on **Next >** to accept the default, or when you've entered a different destination folder.

Installation & User Guide

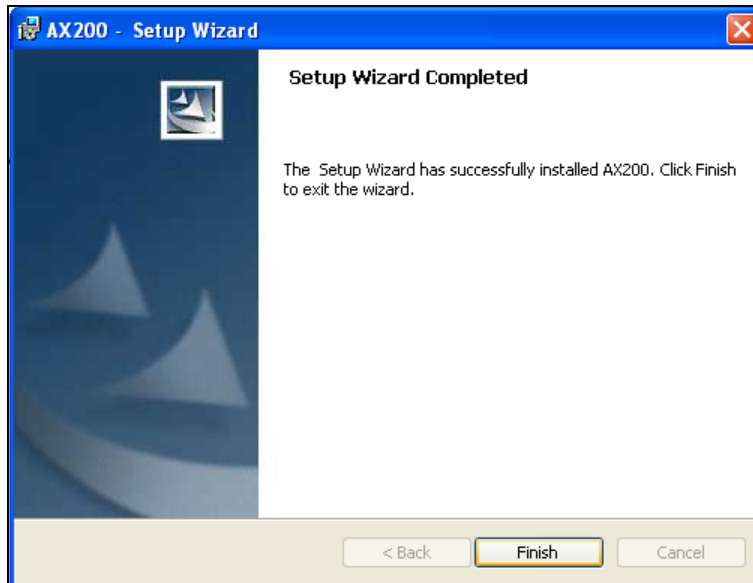


The AX200 program files will now be installed.



The AX200 installation is now complete. Select **Finish** to exit the setup wizard.

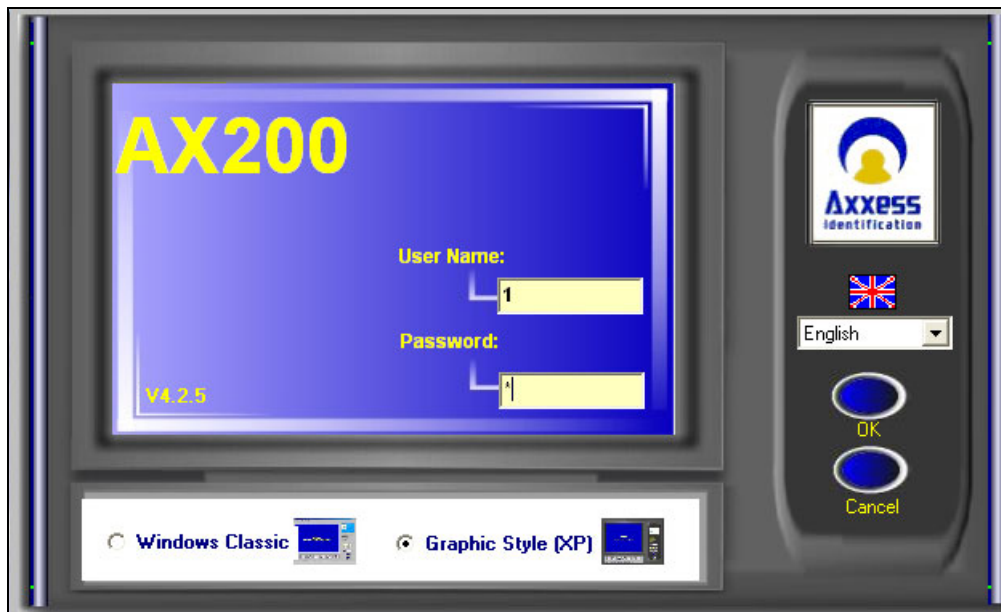
Installation & User Guide



Some operating systems also require Microsoft Data Access Components to support SQL. This is automatically installed if required. Please follow the on-screen instructions.

Starting the AX200 Software

Connect your AX200 controller to the PC using the communication cable supplied. Go to **Start • All Programs**, left click on **AX200 Access Control System** and it will launch the AX200 software, alternatively double click the AX200 logo from the Windows desktop.



Installation & User Guide

The AX200's default user name is **1** and the default password is **1**. The user names and passwords are not case sensitive. Enter the default user name and password and select **OK**.

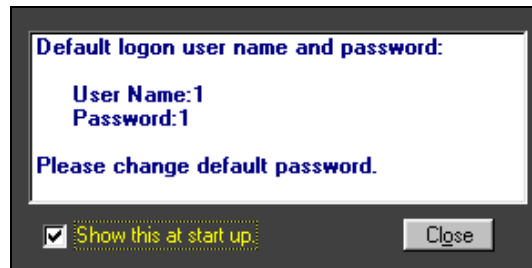
Language Selection

Installation and operation of the software can be selected in different languages. Changing the language can be done from the login screen as well as within the program on the main screen, without the need to restart the software or the computer.



Password Reminder

A password reminder box displaying the factory default reminds the user to change the default password. This reminder box disappears automatically when the default password has been changed.

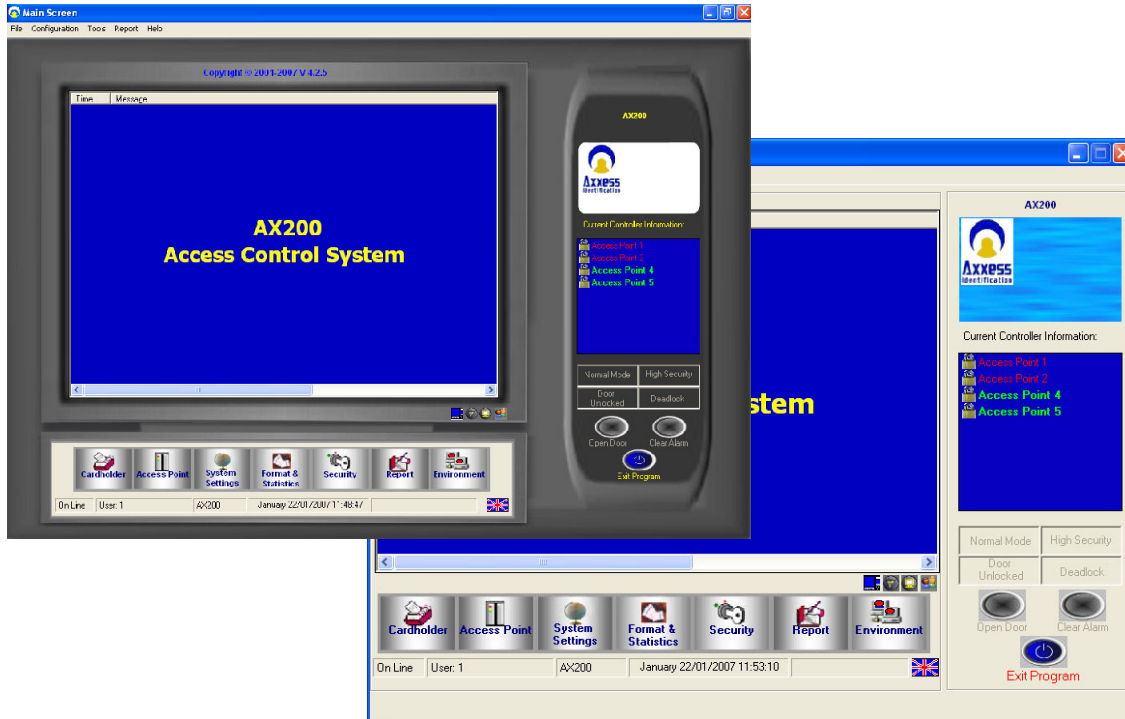


Windows™ Classic or Graphic Style (XP) Screen

Users can select the type of interface on the main login screen. Windows™ Classic is most suitable for older PC and laptops with only 64MB of RAM and 800 x 600 video resolution. Graphic Style (XP) has been optimised for the Windows™ XP operating system. The graphical user interface makes it easy to use and operate. The specification of the PC is automatically checked and will only allow installation or selection of the user interface if sufficient resources are available.



Installation & User Guide



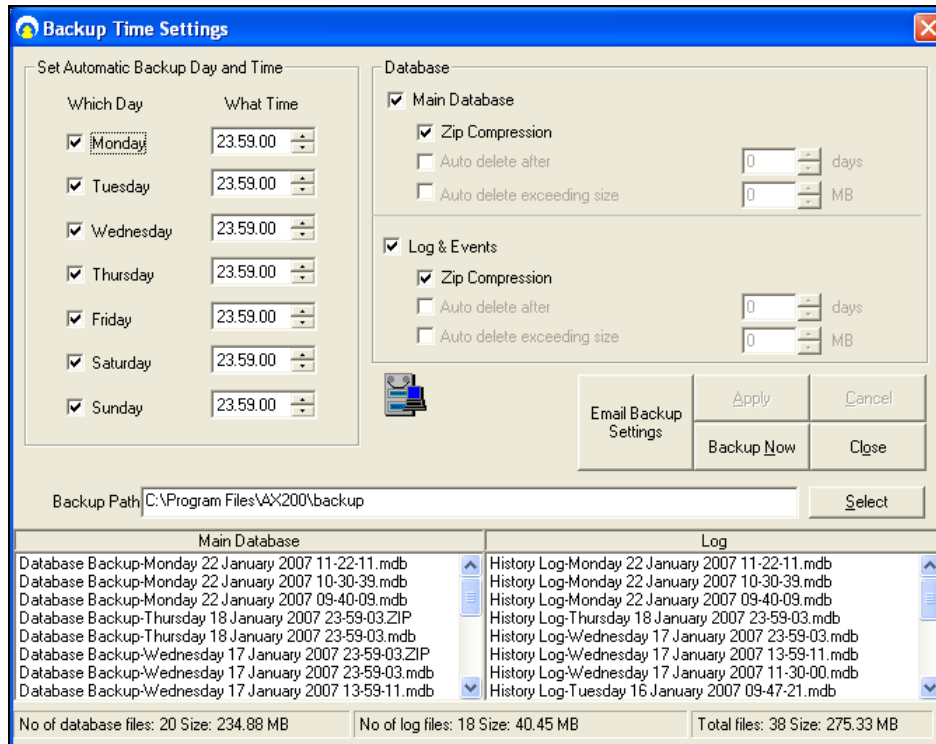
Backup & Restore

The AX software has a built-in backup utility. Backups can be done automatically at preset times and days, or manually with network backup support. Backups from older software versions are automatically converted avoiding the need for multiple steps to restore the software.

A backup can be restored in one single step. Automatic backups are numbered using the date and time the backup took place. If you wish to delete older backups, highlight the appropriate file by clicking on it and press delete, confirmation of this action is requested. It is useful to create a complete system backup as soon as all the system settings have been entered. Create a backup as normal, go to restore, highlight the newly created file and right click with the mouse and select rename – rename the file e.g. *Master settings*. This backup will allow you to restore the system back to its original programmed settings, if required. To restore an existing database go to the File menu • Database Restore.

When exiting the software, if any data has changed, the application will automatically perform the database backup. There is no need to close the program or cardholder screen for the automatic backup to execute. Partial backups can also be selected for database or history files only.

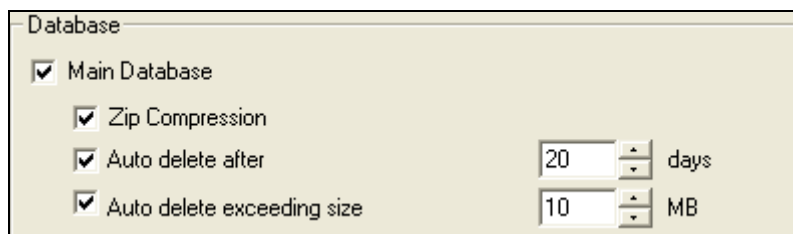
Installation & User Guide



Backup time settings window can be reached through the File menu. The default day and time for automatic backup is displayed on the left side of the window. By default, the application will take a backup of your database at 23:59:00 every night.

Settings on the right hand side give you more options on how to manage your backup files. Normally the backup process saves both, the **Main Database** and **Log & Events**; however you can exclude either of them from the backup process simply by removing the tick in the check box.

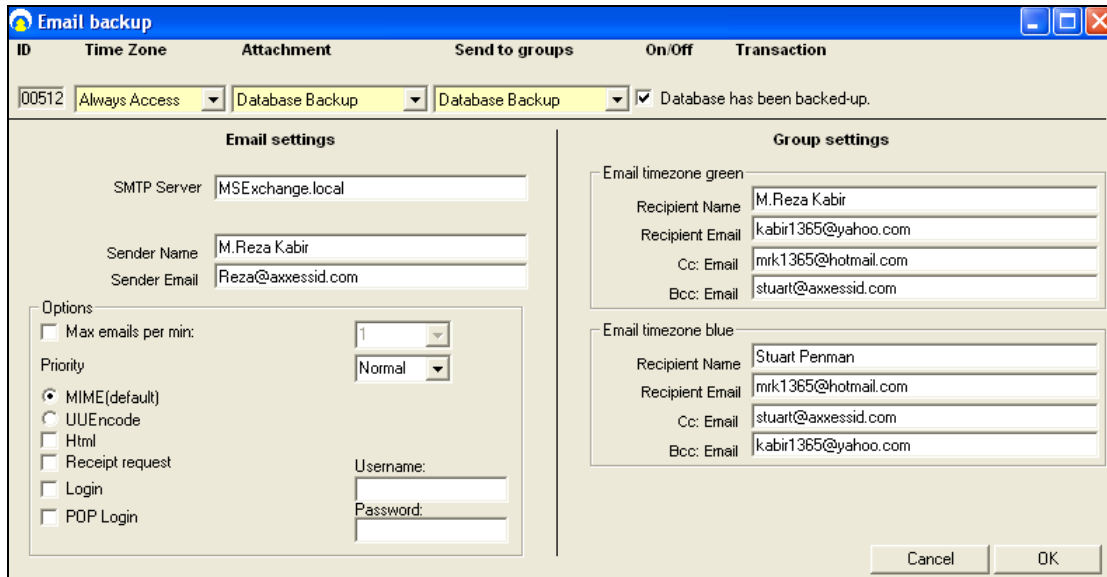
You can also set the application to automatically delete the backup files after a specific number of days or once they exceed a certain size (in MB).



Once the **Zip Compression** is enabled, the software will automatically compress the backup file into a zip file. Since the .mdb file cannot get through the fire wall, zip compression is very helpful when you wish to email the backup settings.

Email Backup Settings

Installation & User Guide



Email settings could be sent to a specific group of people via Email. You need to specify the time period during which you would like the email to be sent out (Time Zone), the information you want to include (Attachments) and the name of the recipients (Groups).

Enter the name and email address of the sender on the left. If you're using a local server enter the name of your local SNMP server for email.

Group settings on the right include the name and email address of the people who will receive the email. These settings are divided into two blocks. The people on the top section will only receive the email if the backup has taken place during a green time zone and the people in the bottom section will receive the email if the database has been backed up during a blue time zone (exception monitoring).

A number of optional settings are also included in this screen. You can set priorities for your emails and choose the maximum email messages sent in a minute. There are also a number of different options for email format. MIME is the default.

MIME (default): *Multipurpose Internet Mail Extensions (MIME)* is an Internet Standard that extends the format of e-mail to support text in character sets other than US-ASCII, non-text attachments, multi-part message bodies, and header information in non-ASCII character sets

UU Encode: UUencoding is a form of binary to text encoding that originated in the Unix program uuencode, for encoding binary data for transmission over the UUCP mail system. The name "UUencoding" is derived from "*Unix-to-Unix encoding*".

Standard Query Language (SQL)

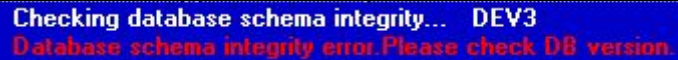
The database structure is based on Microsoft SQL. This ensures stability and a high data throughput with easy interfacing to other applications. The database handles up to 65,525 cardholder records with over 60 fields per cardholder. Card numbering is up to 10 digits allowing support for a wide variety of formats e.g. existing cards or multi-purpose cards (vending machines etc.)

Installation & User Guide

Database Integrity Check

A main failure or system crash with an open database normally requires running a separate application to repair the data. All data in the AX200 database is automatically checked on start up and repaired if necessary.

At the start-up, the software automatically checks the database version. If the database is too old and not supported by the new version of software the following transaction will appear on the screen asking you to check the version of the database.

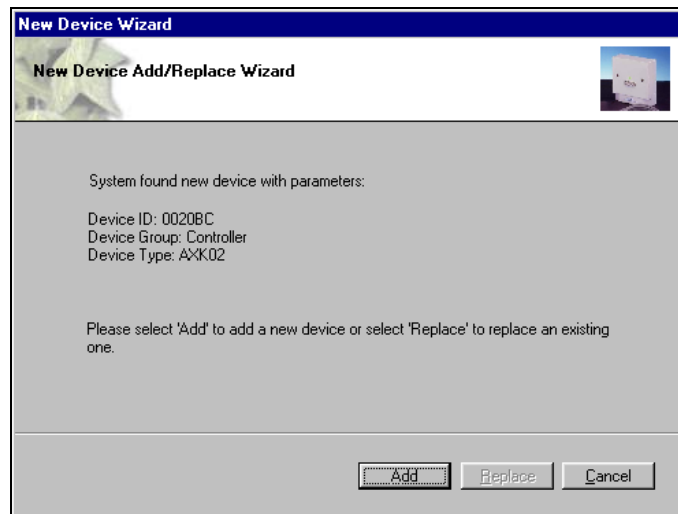
A screenshot of a blue error message box with white text. The text reads: "Checking database schema integrity... DEV3 Database schema integrity error. Please check DB version."

Checking database schema integrity... DEV3
Database schema integrity error. Please check DB version.

You can view the version of your database in the *Performance Analyzer* screen; under *Tools • Enable Optional Software*. This problem usually occurs when you manually copy a new database over the old database in the AX200 folder. **That's why we strongly recommend that you use the restore function only!**

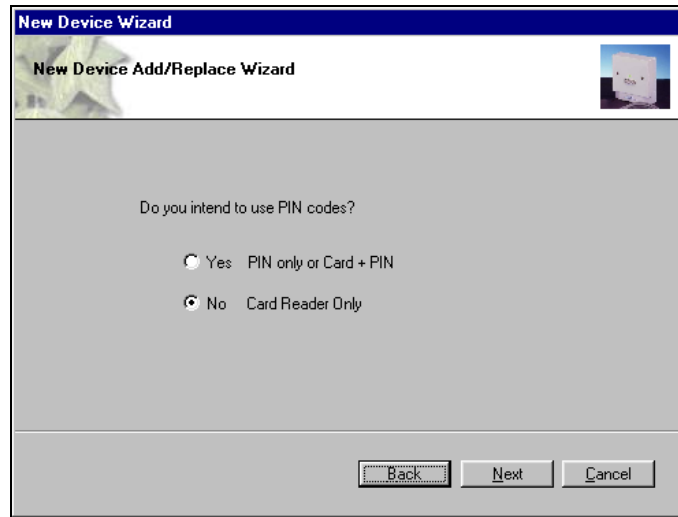
Communication between the AX200 Software and Controller

A benefit of the AX200 software is its plug and play ability to detect new devices when they are installed. The New Device Wizard will automatically detect the controller and its unique device ID. Follow the on-screen prompt by selecting **Add**.



The following screen will ask whether you are using PIN codes only, a card reader and a PIN code or a card reader only. Please select the appropriate radio button for your installation, followed by **Next**.

Installation & User Guide

A screenshot of a software window titled "New Device Wizard" with a subtitle "New Device Add/Replace Wizard". The window contains a question: "Do you intend to use PIN codes?". Below the question are two radio button options: "Yes PIN only or Card + PIN" (which is unselected) and "No Card Reader Only" (which is selected). At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

New Device Wizard

New Device Add/Replace Wizard

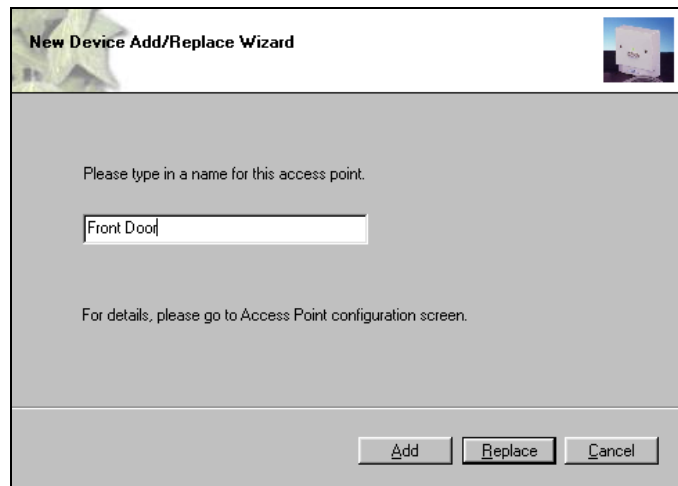
Do you intend to use PIN codes?

Yes PIN only or Card + PIN

No Card Reader Only

Back Next Cancel

Provide a name for the access point i.e. the location and select **OK**.

A screenshot of a software window titled "New Device Add/Replace Wizard" with a subtitle "New Device Add/Replace Wizard". The window contains the instruction: "Please type in a name for this access point." Below this is a text input field containing the text "Front Door". Below the input field is the instruction: "For details, please go to Access Point configuration screen." At the bottom of the window are three buttons: "Add", "Replace", and "Cancel".

New Device Add/Replace Wizard

Please type in a name for this access point.

Front Door

For details, please go to Access Point configuration screen.

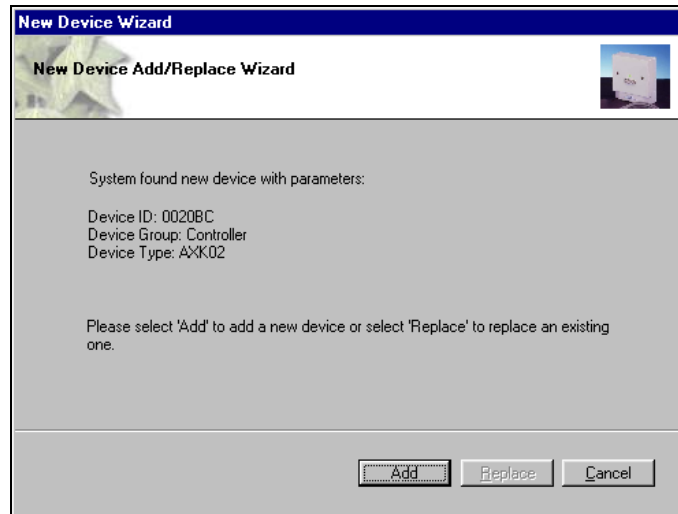
Add Replace Cancel

Plug & Play Devices

The PC communication port is automatically setup and new devices connected will be automatically detected and can be added (or replaced) using the new device wizard, which allows setting up a new controller in seconds. When enabled under system settings, Plug & Play is active at all times and does not require a restart of the application or computer. This allows addition of new controllers on the fly. AX readers are also entirely Plug & Play being automatically identified with the relevant information displayed under access points. COM ports 1 to 16 and TCP/IP (TCP/IP AX200 only) addresses can also be set up manually if required. Error correction, speed, bit length, parity etc are all automatically set up for the optimum performance of the system. Once the controllers are in the system, the new device wizard also allows auto-replace. This feature allows replacement of controller data with the press of a single button.

All the Plug & Play devices have a unique identity number so no jumpers or switches have to be set on either controllers or readers.

Installation & User Guide



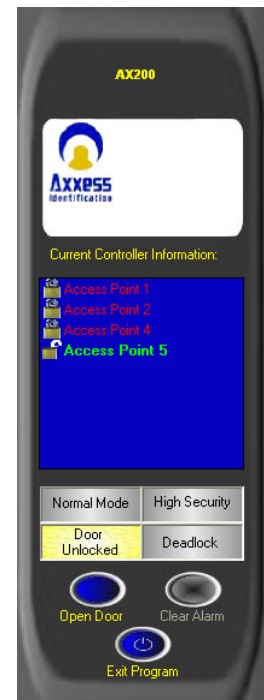
Controller Status & Control

Devices connected are highlighted and display the door status in real-time on the main screen. Doors can be controlled directly from the main screen. Commands can only be given to controllers online and functionality is greyed out if the controller is not available online to avoid any uncertainty.

Door open	Opens the door for a set time e.g. 5 seconds
Normal mode	Standard mode
Door unlocked	Door permanently unlocked
High security mode	Only cardholders with high security mode valid will have access
Deadlock	Locks door for all cardholders, request to exit is still active. <i>Please exercise care when using the feature.</i>
Clear alarm	Door reset, door forced, door held open alarm

High Security Mode (HSM)

This feature allows individual doors to be enabled where standard cards no longer have access. Only cardholders with the high security mode set (HSM) have access whilst this feature is enabled. The HSM feature can be switched on by using a card which has the “set high security” enabled, four times consecutively at the reader. To change back to the normal mode use a card with the HSM feature four times consecutively.



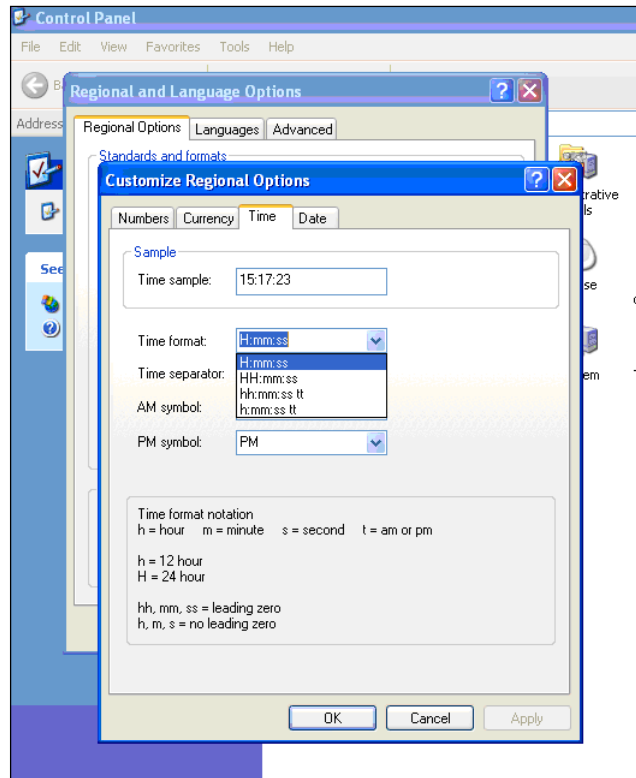
Installation & User Guide

Door Unlock Mode

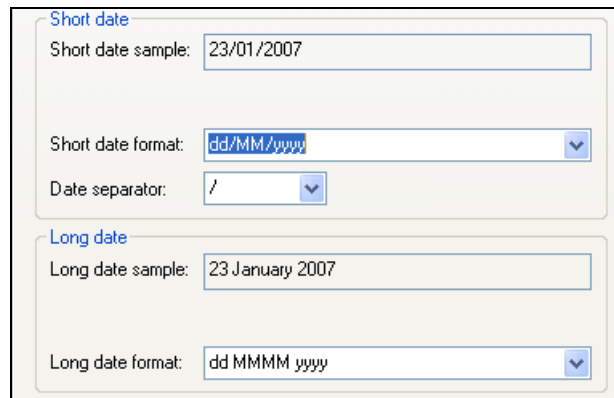
This feature can be activated from the PC or cards with the “set unlock” feature enabled. Using a card with this feature twice consecutively at the reader will permanently unlock the door. To return to the normal mode, use the card again twice consecutively. Typical applications include reception doors during normal office hours or for goods inward deliveries.

Date and Time

The date and time formats are obtained by default from the operating system and therefore no user intervention is required. The 12 hour time format is NOT supported by this application. If you are using the 12h time format you need to go to *Control Panel • Regional and Language Options • Regional Options • Customize...* • *Time* and choose the 24 hour (H) time format. You also need to make sure that your PC is set to UK time format which is (dd/MM/yyyy).



You can change the date settings in the same window under the Date tab.



On & Offline Operation

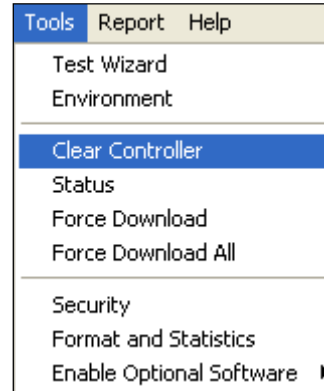
The AX software enables the use of on and offline controllers from within the same software simultaneously. The AX100 controller can also be updated using a portable data transfer unit (DTU). This allows the use of remote doors or doors not requiring online information to be used at the same time as doors with real-time online information. This reduces costs substantially with full control from a single software package.

Installation & User Guide

Force Download & Clear Controller

Clear controller deletes the database that has been stored in the controller. Once the controller is cleared, the door becomes permanently unlocked. At this time if a card is presented to the reader, a transaction will appear on the screen saying “Door is unlocked” followed by the cardholder’s name, card number and the door’s name. To clear a controller highlight the appropriate access point on the current controller list (on the right) and select *Clear Controller* from the *Tools* menu.

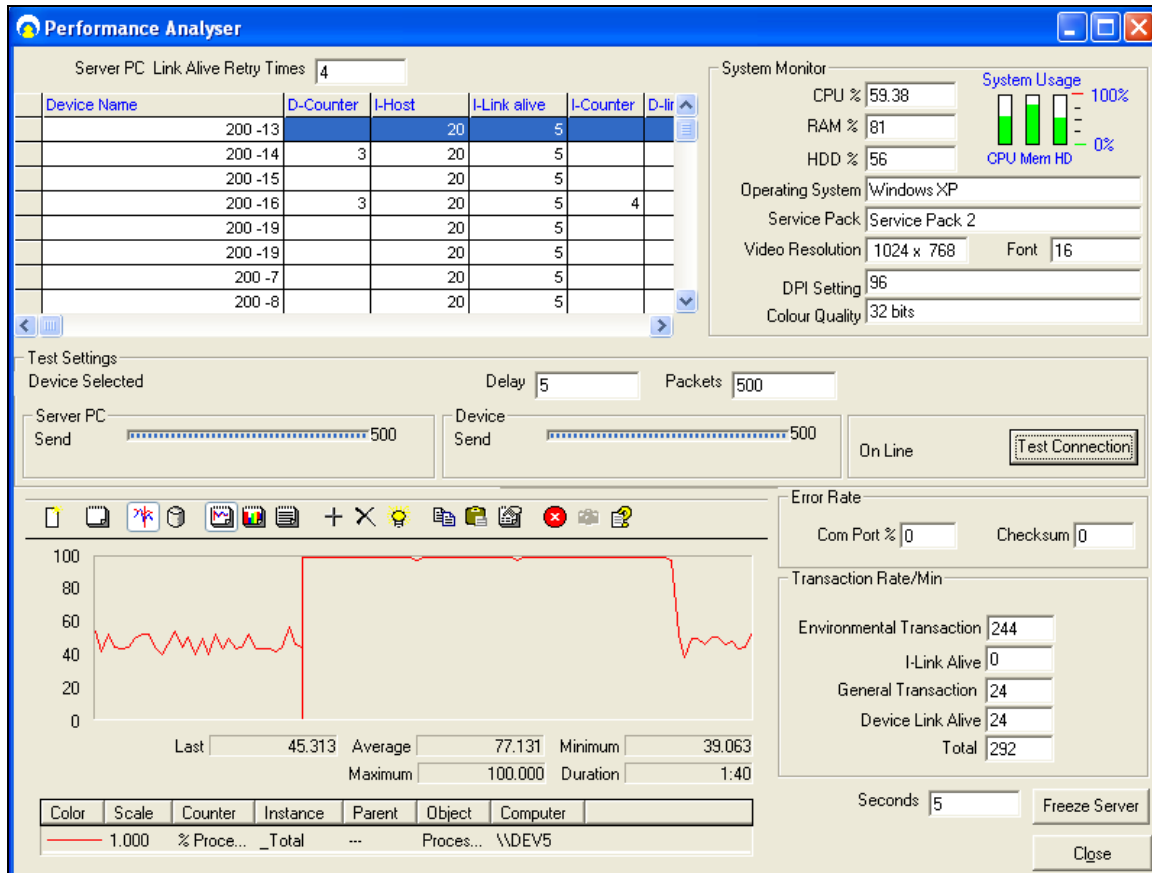
If for whatever reason the automatic download doesn’t take place, you can always select individual controllers and click on the **Force Download** on the tools menu or choose **Force Download All** instead and have the database downloaded on all the controllers. You can find out which controller(s) needs a download by double clicking on the *Download Required* icon at the bottom of the main screen.



Performance Analyzer

One of the optional features in AX200 software. Performance analyzer is a collection of the features that demonstrate the performance of the system. These features are scattered in the software and can be found in different parts of the application. Performance analyzer could be accessed through *Tools • Enable Optional Software*.

Installation & User Guide





The list on the top shows all the units that have been configured on your PC at some point. This can also be found in *Access Point • Device Manager*. You can also test the connection between the online units and the PC by pressing the Test Connection button.

The graph on the bottom, demonstrates the performance of different elements of your system such as the CPU, hard disk and To add a new graph click on the “+” button and select the appropriate object from the menu.

Transaction Screen

All system transactions are displayed on the main screen with time and date stamp. A detailed description is given for each transaction e.g. No access, invalid PIN code.

For diagnostic and security purposes, the transaction screen can be cleared, by clicking on the blue button  under the window. The transaction pause button  will temporarily freeze the screen without losing any data. Transactions will continue to be registered in the log file. The stop button will block the new transactions; however they are still stored in the log file.



The date and time column can be shortened or extended by clicking on the column header. If a large number of transactions are logged, the date field can be hidden to extend the length of the

Installation & User Guide

field. All system transactions are colour-coded, valid entries are displayed in green, access denied transactions etc in red and system messages in yellow.

The number of transactions kept in memory for quick overview on the main screen can be set under “System Settings”. The larger the number, the more memory will be required. Transactions are always stored and can be viewed or printed under “Reports”.

Time	Message
11:59:58 AM	User: 1 Start Application Computer Name:AXXESSID
12:10:55 PM	Invalid card. Access denied. Unknown 290 Car Park North
12:10:55 PM	Reader is present. Car Park North
12:12:18 PM	Invalid card. Access denied. Unknown 289 Car Park North
12:13:11 PM	Invalid card. Access denied. Unknown 4699 Car Park North
12:17:16 PM	Start automatic download... Car Park North
12:17:19 PM	Automatic download finished. Car Park North
12:17:26 PM	Access granted. Priscilla Tims 290 Car Park North
12:17:42 PM	Access granted. William Rees 289 Car Park North
12:17:52 PM	Access granted. Clare Renald 291 Car Park North
12:18:01 PM	Access granted. Peter Simons 4699 Car Park North
12:18:08 PM	Invalid card. Access denied. Unknown 124 Car Park North

Who's In/Out List




In order to use the who's in/out list, you need to have at least one reader configured as **In Reader** and one reader configured as **Out Reader** on your PC. To do this, go to the *Access Point* screen. Select the appropriate reader from the list on the right. Change the settings to *In* or *Out Reader* and click Save. Once you've done this the in/out list becomes active. If someone opens the door with a valid card his/her name will appear on the who's in list, along with the card number, department name, time of entrance and the last door which he/she passed through. This list could be printed by clicking on the printer icon.


In	Time in	Department	Card No.	Last Door
Andre Shevche...	02/09/2007 09:11:09*	Accounts	47143	
Arnold Schwar...	02/09/2007 09:11:09*	Operations	4000	
Albert Einstein	02/09/2007 09:11:09*	Accounts	88210	
Harrison Ford	09/02/2007 15:17:29	Technical	272208	Access Point 4

Search Surname In 21

The number of people inside the building is displayed on the bottom. You also have the ability to search people by their surname.

It is also possible to book people in/out manually if necessary. Click on  icons for Manual Book In/Out. Select the appropriate people and the appropriate doors from the lists and press Book In/Out.



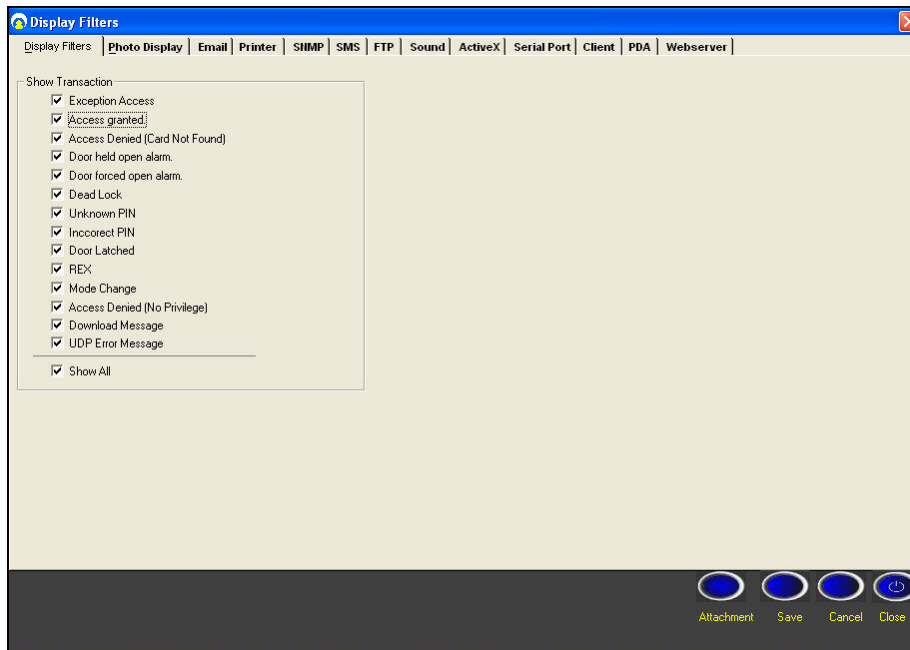
Clicking on  would open the who's out list which basically shows the list of the people who are not in the building. When a person presents his card to the out reader his name will be removed from the in list and appear on the out list.

The total number of hours that an individual or a group of people have spent in the building can be calculated in *Reports • Work spell*.

Installation & User Guide

Note: in order to program the software to print out the who's in list when the fire alarm goes off go to *Display Filters • Printer • Setup* and enable the **Auto print on fire alarm**.

Display Filters



This screen includes 13 different tabs, however only 4 of them are included in the AX200 software. The other 9 features are only available in the AX500 software.

The Display Filters tab contains a list of 14 different types of transactions that appear on the main screen. Please note that these are not individual messages. Each one is a type of transaction which may include several messages that are similar to each other. For instance; “Access granted” type includes access granted with card, PIN & card + PIN. If you don't wish to see any of these transaction types just remove the tick from the check box.

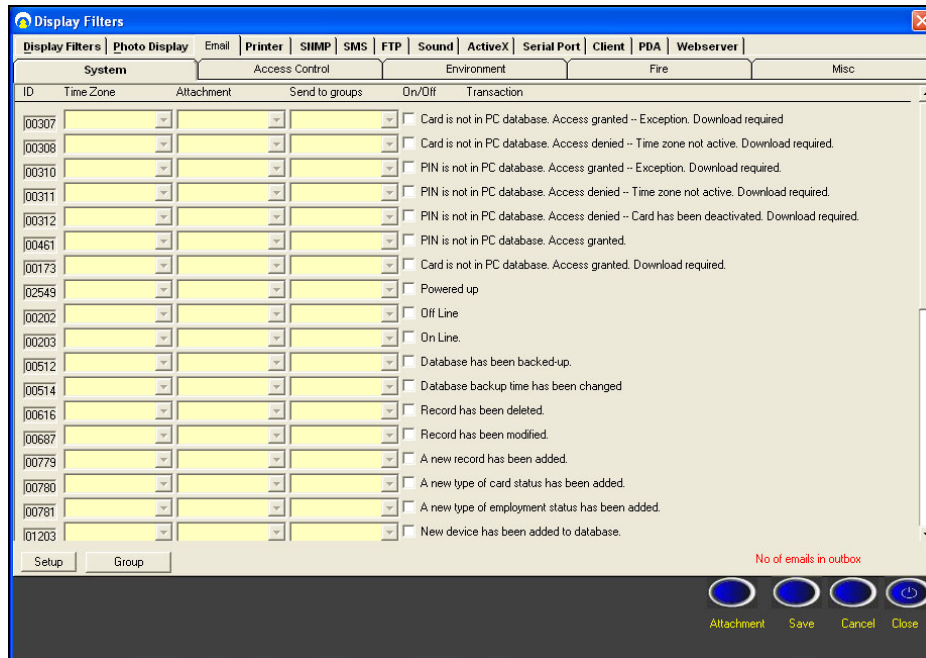
Photo Display

You can decide whether or not you would like the cardholder's photo to be displayed on the main screen once a valid card is presented at a particular door. If you decide not to display the cardholder's photo, company's logo will be displayed instead along with the card number, cardholder's name, department and the name of the access point.

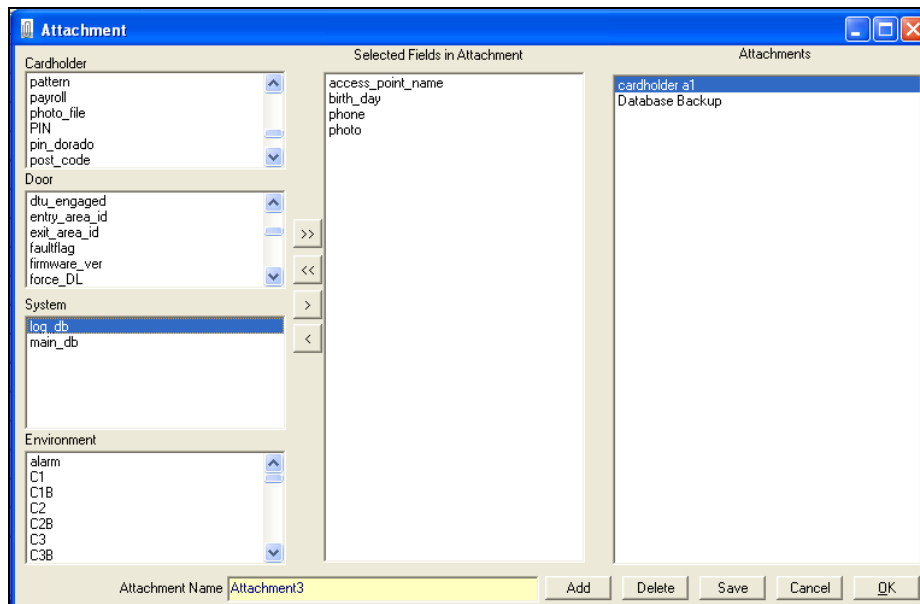
Email

The AX200 application could be programmed to create an email message to be sent to a single or a group of users once a particular transaction appears on the main screen.

Installation & User Guide



Select the appropriate transaction simply by ticking the check box next to it. From the time zone column select the time zone during which you would like the email to be sent out. Selecting “Always Access” would send the email at any time. The attachment menu gives you the ability to specify what information you would like to be included in the email. To add a new attachment click on the **Attachment** button on the bottom of the screen.

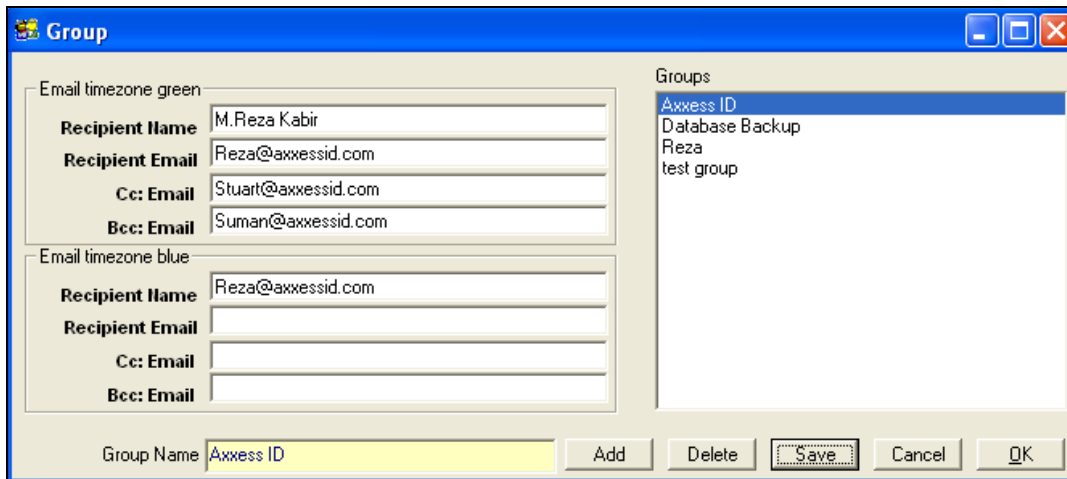


To create a new attachment press “Add” and enter an appropriate name. from the four lists on the left hand side select the information that you would like to appear in the email and move them over to the middle list by clicking on the > button. Once you’ve completed the selection of your

Installation & User Guide

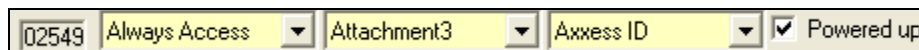
fields click Save & OK and go back to the email tab. Now you can select the attachment that you just made from the drop-down list.

The next drop-down list includes the person or the group of users whom the email will be sent to. To add a new group click **Group** on the bottom of the screen.



To create a new group click on “Add” and enter an appropriate name. Enter the name and the email address of the recipient. When you’re finished click Save & OK.

You have not completed the email configuration. For instance in this case, if the **“Powered up”** transaction appears on the screen during the time zone **“Always Access”**, an email message containing the information included in **“Attachment 3”** will be created and sent to the people listed in the **“Axxess ID”** group.



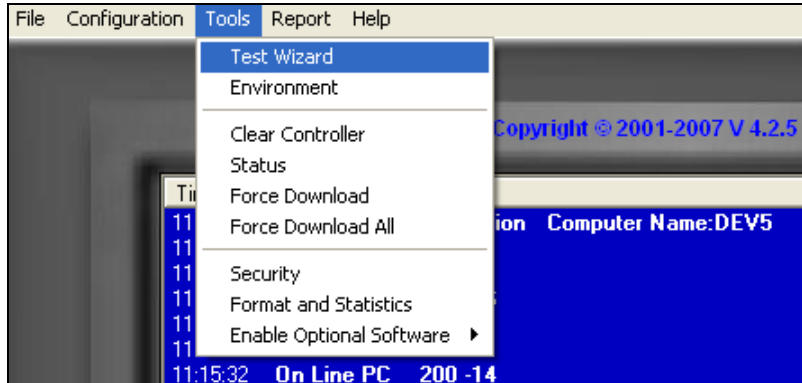
Save on Exit

Preferences selected are automatically saved. Under General Settings, a factory default button restores all the important system settings. If any system or card changes have been made, the system will automatically backup the data when exiting the program.

Test Wizard

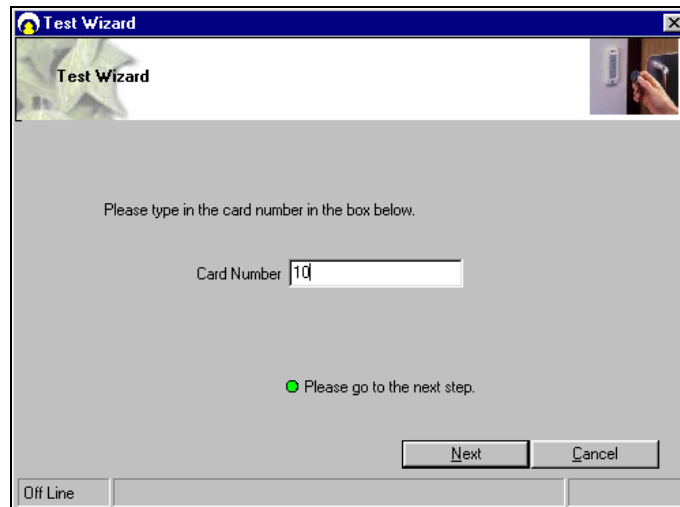
The test wizard can be selected from the Tools drop-down list on the top menu bar.

Installation & User Guide



The test wizard will guide you through automatic setup of the card formats and a complete hardware and software test.

On the Test Wizard screen type in the card number of one of the cards which you would like to test and select **Next**.



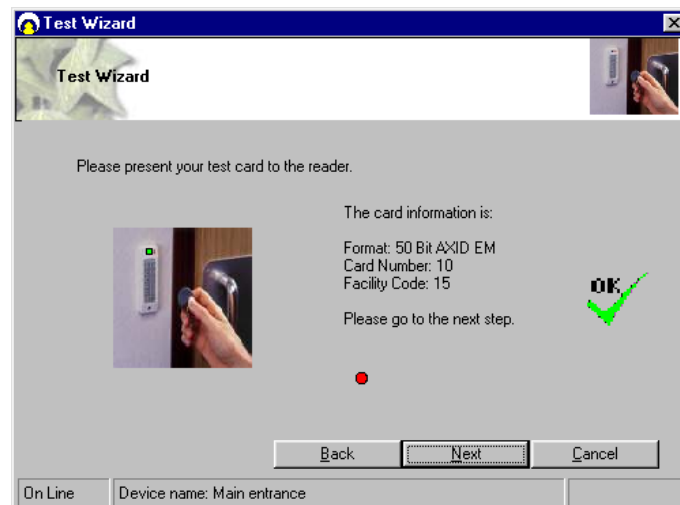
Ensure your AX200 controller is still connected to the PC – the Test Wizard will now check and communicate with the controller. If the controller is communicating correctly a green acceptance tick is displayed.

The Test Wizard now requests that a card is swiped or presented to the reader.

Installation & User Guide

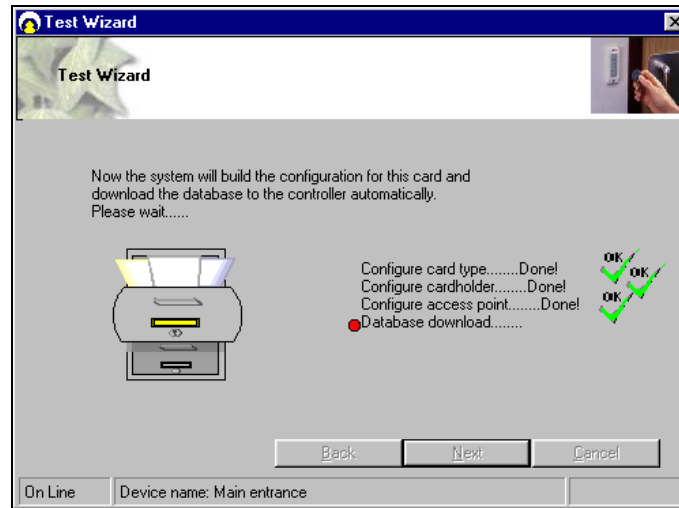


The Test Wizard will now check and verify the card format, facility code and card number. Select **Next** to continue.

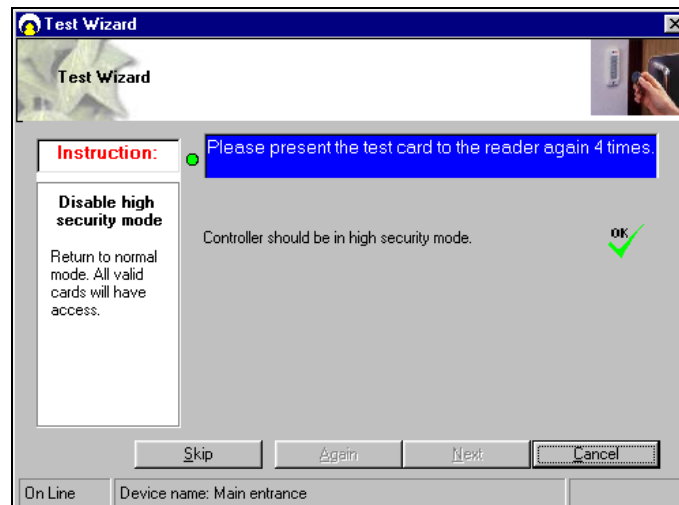


The Test Wizard will now configure the card format, cardholder, and access point and download the data to the controller. Select **Next** to continue.

Installation & User Guide



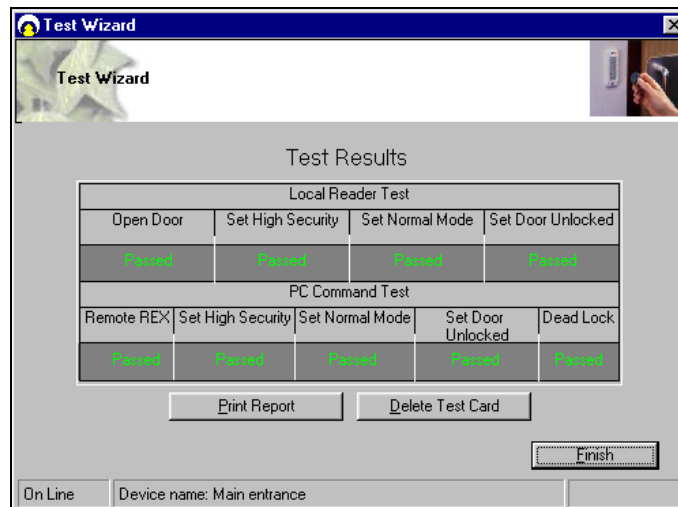
Now the Test Wizard will complete a number of hardware tests – please follow the on-screen prompts.



- Unlock Door – presenting your card to the reader once will unlock the door, the controller LED should stay on green for 5 seconds
- High Security Mode – presenting your card to the reader 4 times will test the high security mode, the controller LED will flash 4 times red every 5 seconds
- Normal Mode – presenting your card to the reader again 4 times will put the system back to normal mode, the controller LED flashes green every 5 seconds
- Door Latched Open – presenting your card to the reader twice will latch the door open, the controller LED will flash green twice every 5 seconds
- Door Locked – presenting your card to the reader twice again will lock the door, the controller LED flashes green every 5 seconds.

Installation & User Guide

Select **Next** to continue.



Once completed, additional cardholders can be added by selecting the cardholder icon or through the cardholder configuration screen. Optional features can be set through the access point configuration.

Installation & User Guide

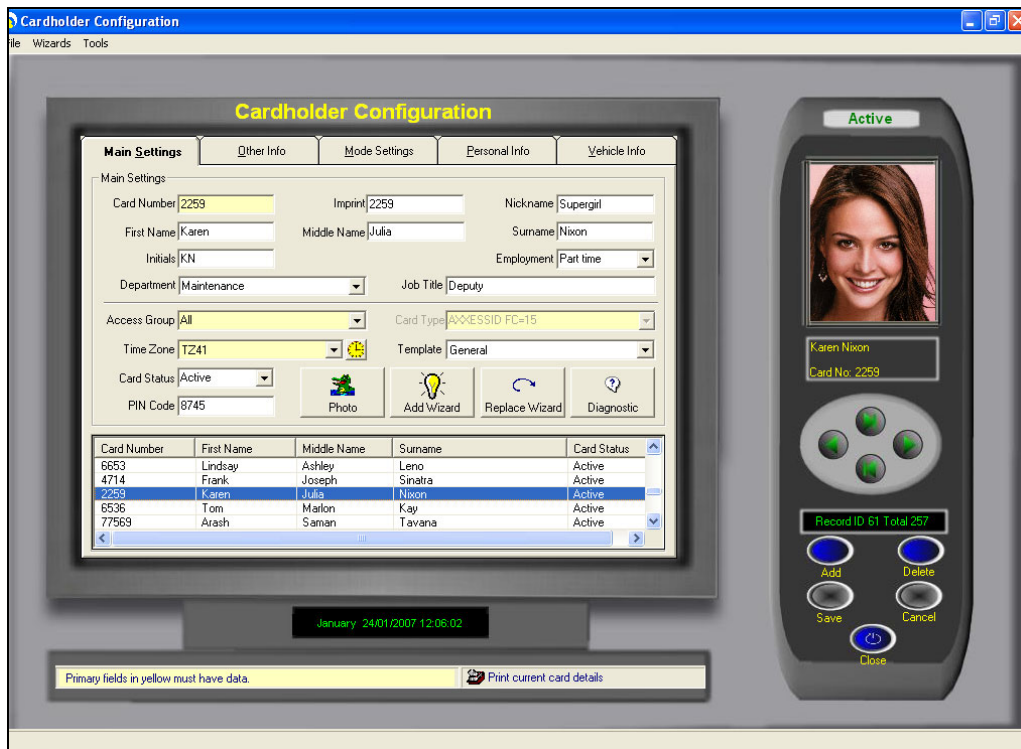
Cardholder

Cardholder configuration consists of five elements

- Main Settings
- Other Info
- Mode Settings
- Personal Info
- Vehicle Info

Adding new cardholders can be done from the main settings screen. The other tabs are for extra features and additional database fields.

Main Settings



Card Number

Unique card number – maximum 10 digit number. This number excludes the facility and site code number which is defined in card type.

If you change the card number to 0 (= no card), data can be left on the database in case the person requires a card again or, if all the data is entered first and cards are issued at a later stage. This feature is specifically useful for frequent visitors and contractors.

Installation & User Guide

Imprint Number

If the number on the card is not the 'true' number in the card, then this printed number can be entered here. Alternatively this field can be used for other data e.g. membership numbers etc.

Employment

To indicate the type of cardholder, fields can be selected from the drop-down box or entered manually. When entered manually it will ask for confirmation when you save the record and can be selected the next time from the drop-down box.

Department

Select a department from the pop-up window, departments can be added or deleted as required.

Access Group

An access group is a collection of doors. When a group is selected, the cardholder will have access to the doors assigned in the access group. Two groups are fixed and cannot be deleted – **All** and **None**. The group All automatically includes all the doors including those added by the device wizard. If the group None is selected, the cardholder will not have access to any of the doors.

Card Type

The card type is by default greyed out. If under *System Settings, General Settings the Multiple Card Format* is enabled, then this field can be used if you require cards from other system to work as well.

A card type is the name given to the card format and facility code combined. It is recommended that you use the card format wizard if you wish to add new card types.

Card Status

This field overrides all settings, if the card is set to: Destroyed, Inactive, Lost, Stolen or Suspended. The card will not have access unless set to Active.

It is recommended that you use this field if a card is for instance stolen instead of deleting the whole cardholder record. By using this method, you can always see at a later stage why the card was inactive.

Pin Code

1 to 6 numbers – the default setting is 4.

This field is required if PIN Settings (found on the Access Point screen) is enabled and a keypad or reader with keypad is used. If a reader with PIN is selected, the card is presented to the reader first followed by entry of the PIN code.

Time Zone

An important part of the AX200 software; this feature allows you to determine exactly when a card holder is allowed to have access through a particular door. To open the time zone window click

on the  icon.


This page contains a time table which includes eight columns representing seven days of the week plus an extra column for holidays.

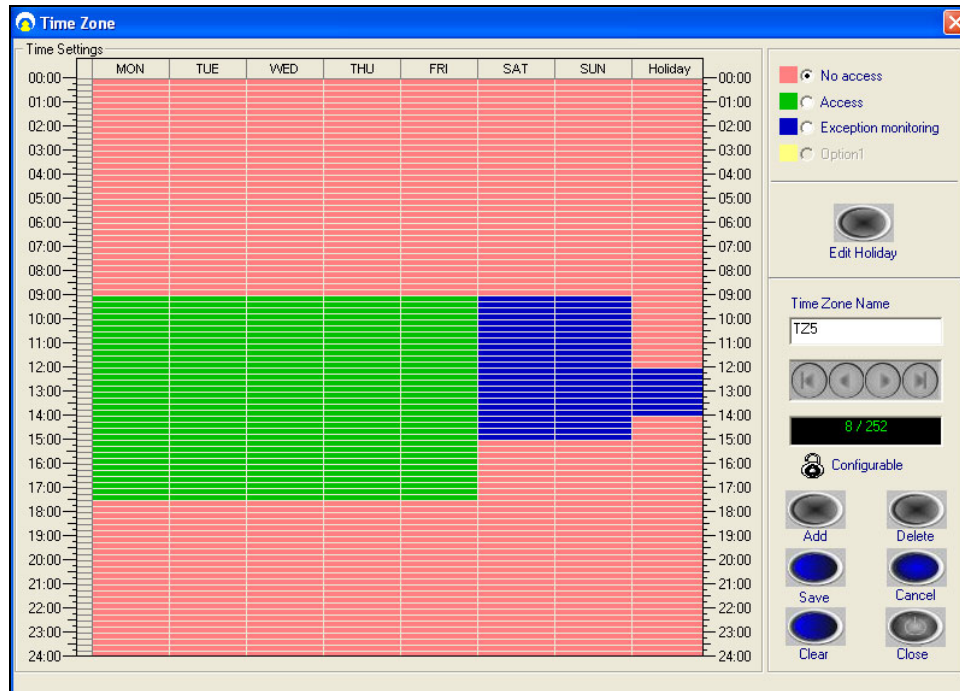
To create a new time zone press add and enter an appropriate name for the time zone. You can program up to 256 different time zones. Any record after the 256th time zone will not be

Installation & User Guide

downloaded onto the controller. Every day of the week has been divided into the periods of 15 minutes. Red zone is when the card holder will not gain access through the door. If the cardholder presents his/her card during this period the message on the screen will say that the time zone is not active and therefore access will be denied. To grant access to a cardholder during a specific period of time, click on the start time, hold the left click down and drag the mouse to the end time. The selected period will be displayed in green. Alternatively you can give exception access to the cardholder by selecting the “Exception Monitoring” and follow the same procedure. In this case the selected area is displayed in blue. So when the cardholder presents his/her card to the reader the transaction on the main screen will be of “Access granted – Exception” type.

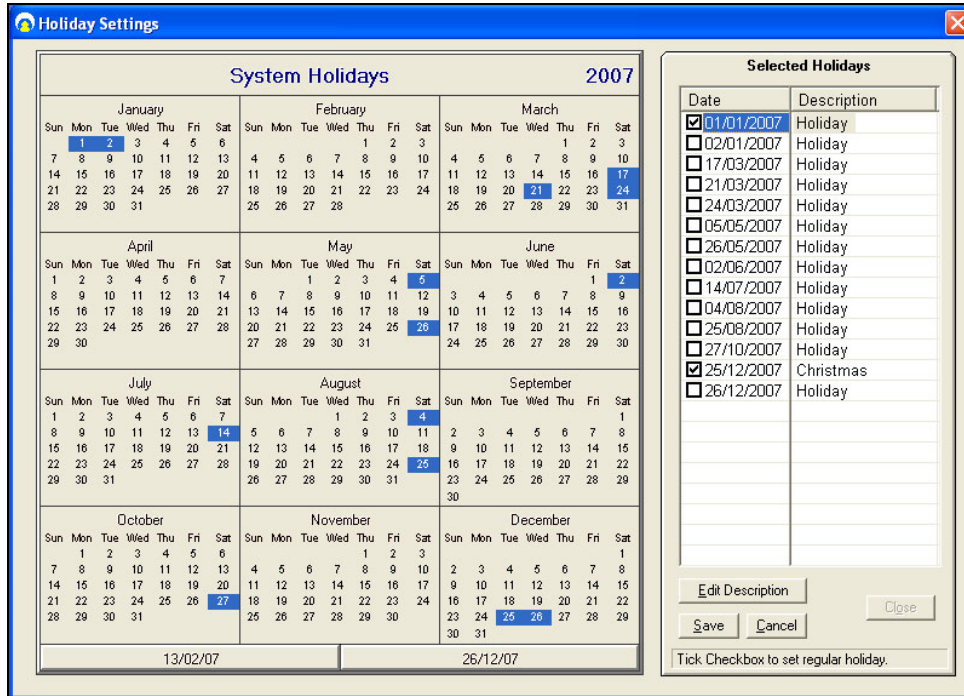
Access granted – Exception <Cardholder’s Name> <Card No.> <Door’s Name>

Once you’ve finished programming your time zone press *Save*. Use the  button to scroll through the existing time zones. The first 9 records including No Access, Always Access, Always Exception and TZ1 • TZ6 are the defaults and included in the blank database.



Access on holidays could be programmed separately. To change the holiday settings press “Edit Holiday”. Mark the holidays in the calendar simply by clicking on them. Once you’ve highlighted a date, it is added to the selected holidays list on the right. If you need to take a day off the list click on it once more. Some holidays are not fixed and move every year. Tick the check box next to the regular holidays (like Christmas) so you won’t have to program them again next year. You can enter a brief description for each holiday by pressing the “Edit Description” button. Click save and close the screen when you’re finished.

Installation & User Guide



Photo

A digital photo can be added in the following formats – JPEG, GIF and BMP. To add a cardholder photograph, click on the Photo button and select the file using the browser. If the controller is used on-line then every time a cardholder presents a card, the transaction including the photo will show on the Main Screen.

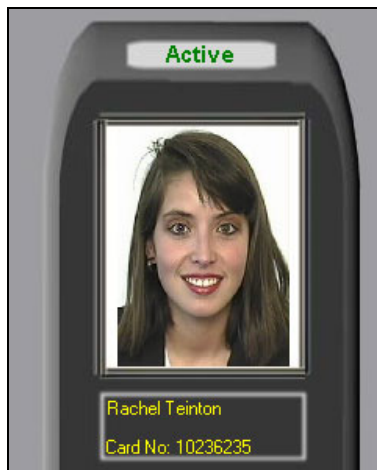


Photo ID

Installation & User Guide

To access the Photo ID window click on the “*Photo*” button under the “*Main Settings*” tab in the *Cardholder* screen.

Photo ID window is where you can add a picture or change the template on your card.



Add a Photo

There are two ways of adding a new photo to your card. You can either import a photo from a file or use a camera.

Capture Picture from Camera

If there is a camera connected to your PC you can have live picture on your screen. Just click on the **Start** button in the **Picture Creator** section on the right hand side. A new window will be opened where you can capture an image from the live picture. The captured picture will then appear in the picture creator window. After selecting the appropriate part of the picture click “Accept”. Your picture will now be printed on the card.

Installation & User Guide



Import Picture from File

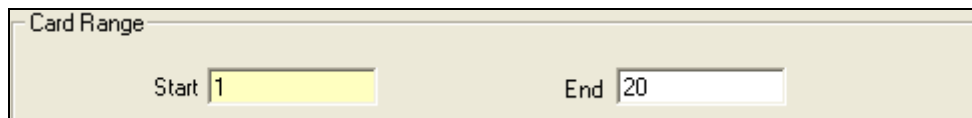
You can also import a photo from a jpg, gif or a bmp file on your PC. Just click on the import button, select the file on your hard disc then click open.

Templates

To create a new template click **Add**. By default the company's logo would be displayed instead of the cardholder's photo unless you import a picture either from a camera or a file on your PC. The text fields displayed on the right hand side could be moved simply by clicking and dragging. Click **Save** once you're finished. To edit an existing template press the **Edit** button.

Add New Card Wizard

It is a simple way to add a single or a block of cards at once. Start field definitely needs to be filled in. the value in the start field will be the first card number. If you're planning to add a block of cards you need to fill in the End field as well. The number in the second field will be the last card number.



Any other information entered in the other sections will be applied to all new cards. If the high security and door unlocked feature are selected then these will be for all the doors in the access group.

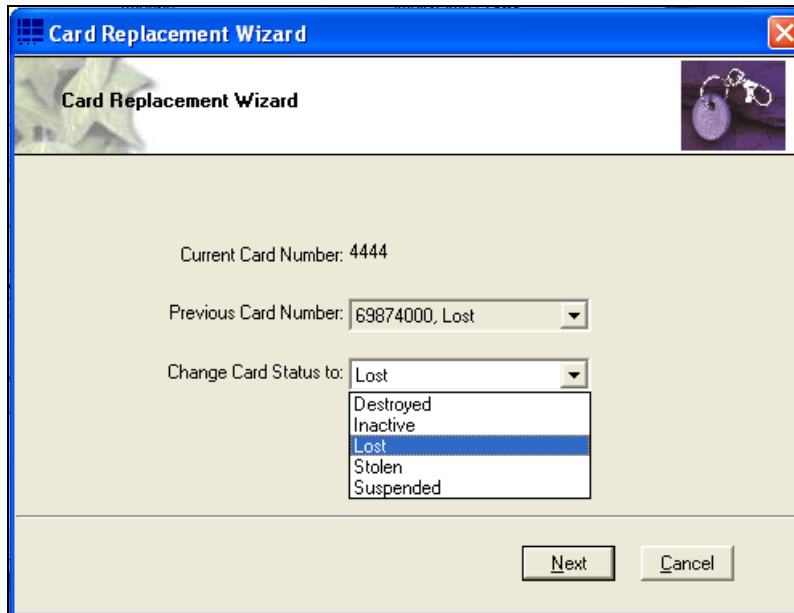
Individual settings per door can also be made using Mode Settings.

Installation & User Guide

First Name	<input type="text" value="Mike"/>	<input checked="" type="checkbox"/> High security card
Surname	<input type="text" value="Mckay"/>	<input checked="" type="checkbox"/> Allow to set door unlocked
PIN Number	<input type="text" value="2546"/>	<input checked="" type="checkbox"/> Allow to set high security mode
Department	<input type="text" value="Technical"/>	<input checked="" type="checkbox"/> Extended door open time
Card Status	<input type="text" value="Active"/>	Issue Date <input type="text" value="02/01/2007"/>
Card Settings		
Access Group	<input type="text" value="All"/>	
Time Zone	<input type="text" value="Always Access"/>	

Card Replacement Wizard

Card replacement wizard will substitute the current card with a new one. You can specify which card status you want the current card to change to.



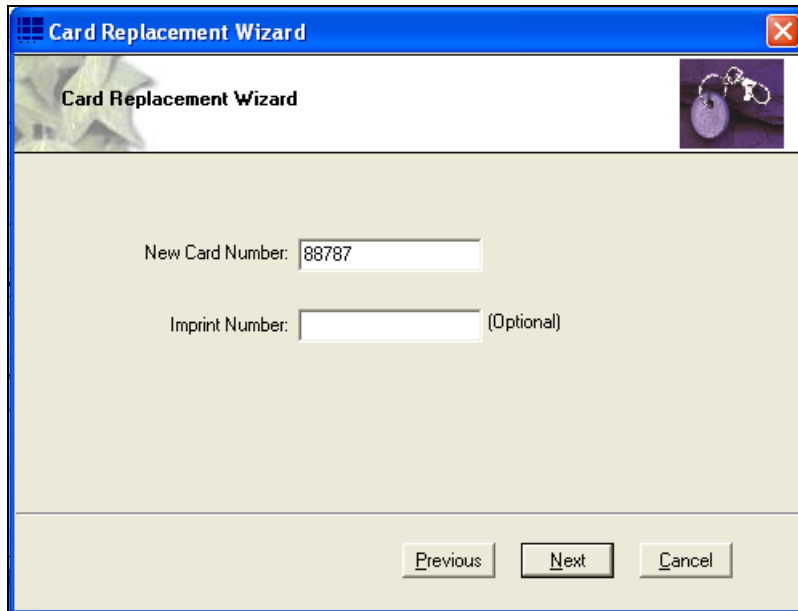
The screenshot shows a dialog box titled "Card Replacement Wizard" with a close button in the top right corner. The main area contains the following fields:

- Current Card Number: 4444
- Previous Card Number:
- Change Card Status to: (with a dropdown menu open showing options: Destroyed, Inactive, Lost, Stolen, Suspended)

At the bottom right, there are two buttons: "Next" and "Cancel".

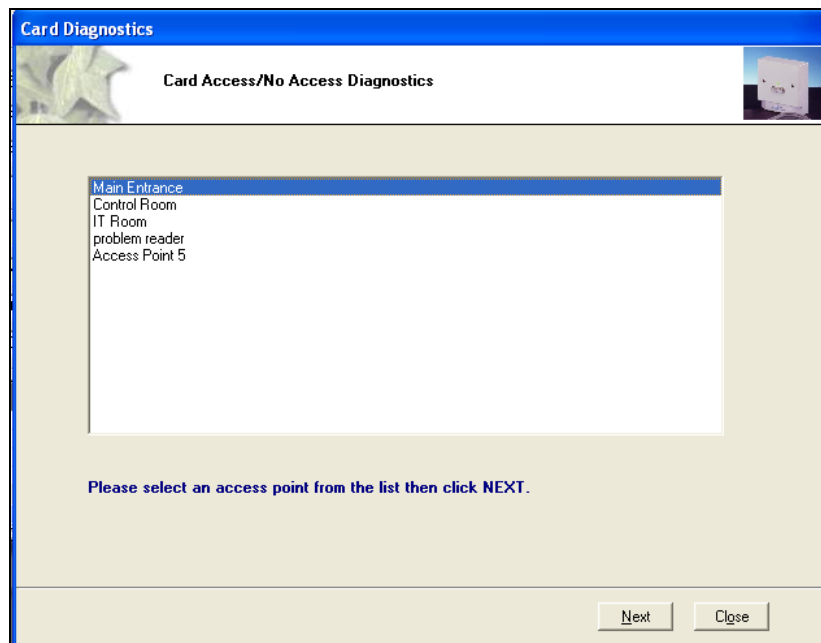
After clicking **Next** the current card will be deactivated. All you have to do now is to enter a new card number.

Installation & User Guide



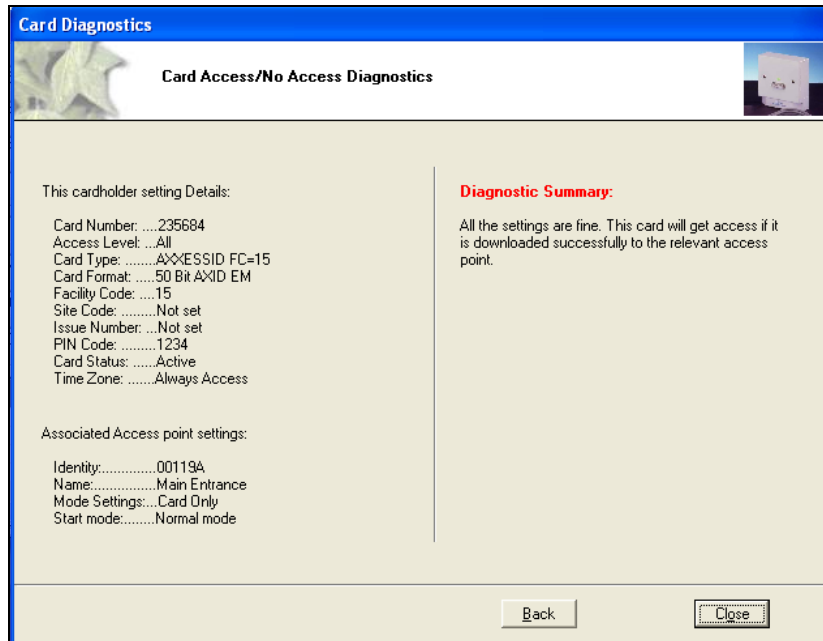
Card Diagnostics

Card diagnostics gives you a summary of the current cardholder setting details. If a card does not have access to a door, then the diagnostic button is a quick and easy way to see why.



After selecting the appropriate door click **Next**.

Installation & User Guide

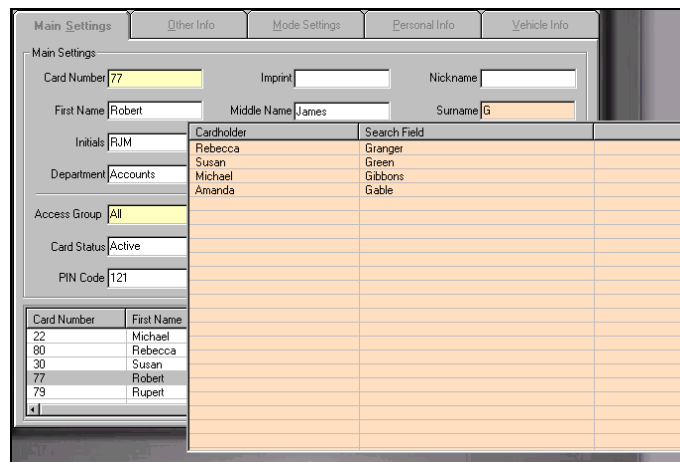


The information on the left is a brief summary of cardholder setting details and the associated access point settings which can also be found under cardholder *Configuration • Main Settings & Access Point Configuration • Access Point*.

Diagnostic summary on the right explains whether or not the current card holder will get access through the selected door.

Search

Searches can be performed on the cardholder record by clicking with the mouse on the field label. The mouse pointer changes to a magnifying glass on field labels which are searchable.



You can specify certain criteria when performing a search for example on the card number field

>5 will produce a result of all cards greater than 5

Installation & User Guide

<5 will produce a result of all cards less than 5
 1-5 will produce a range of cards from 1 to 5

From the search list you can either select the required record or press Escape key (Esc.) to exit.

The search facility also allows partial searches e.g. by clicking on the surname field label you can enter the first letter (or more) of the surname and the results will automatically be displayed on screen. By clicking in the search list will display the appropriate cardholder record.

Card 0 Function

Cardholder details remain on the system without deleting the information. This feature is especially useful for frequent visitors or contractors. Simply change the card number to 0 when the person leaves, upon their return simply change the card number from 0 to the actual card number issued.



Print Current Card Details

On the cardholder screen, there is a printer icon, which allows the user to print the current cardholder record without going to the report menu. This feature is especially useful if the cardholder has to sign for the card issued to them and a hard copy is kept.



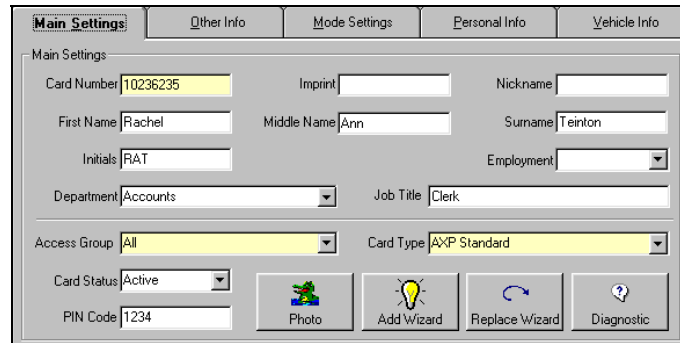
Database Fields per Cardholder

A card number and access group are the minimum fields required to activate a card. All the other database fields are optional and are grouped over a number of easy to navigate tabs.

Main Settings Tab

Installation & User Guide

Card number	up to 10 digits
Imprint number	20 characters – usually the number printed on the card
First name	30 characters maximum
Middle name	30 characters maximum
Last name	30 characters maximum
Nickname	30 characters maximum
Initials	10 characters maximum
Employment type	e.g. contractor, visitor, part-time - unlimited number of characters
Department	50 characters e.g. Administration, Sales
Job title	20 characters maximum
Access group	50 characters - which doors the cardholder has access
Card type	each card can be a different format or facility code, allowing use of a variety of existing cards within the same technology
Card status	active, lost, stolen, suspended, destroyed, inactive
PIN code	from 1 to 6 digits (individual per user)
Photo	graphic file e.g. BMP, JPEG, GIF

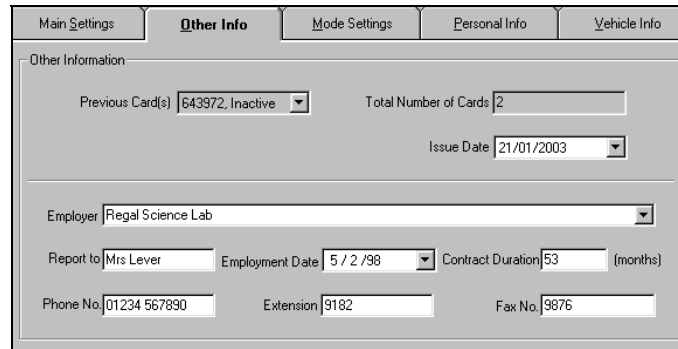


Other Info

Includes a few more details about the cardholder and the employer.

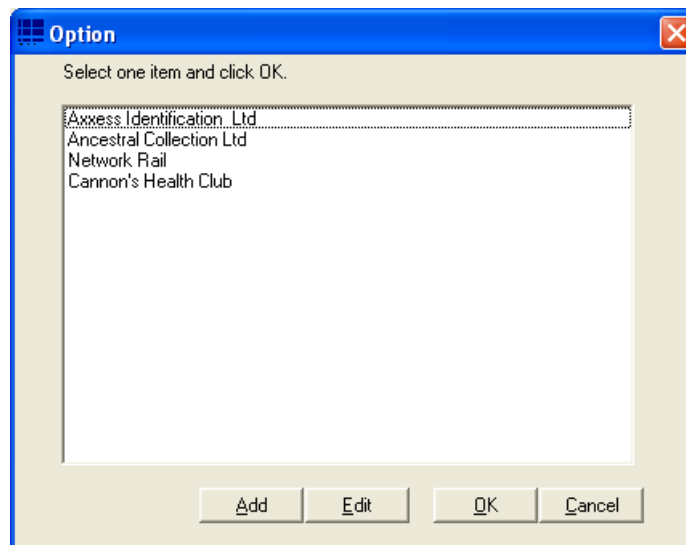
Previous card(s) lost	previously issued card numbers and reasons for cancellation e.g. lost
Total number of cards	total number of cards issued to this person
Issue date	records the date the card is entered onto the system
Employer contractors	multi-company support for shared entrances etc or site
Report to	manager's name
Employment date	use drop down calendar or type in date
Contract duration	enter number of months
Phone number	30 characters maximum
Extension number	50 characters maximum
Fax number	30 characters maximum

Installation & User Guide



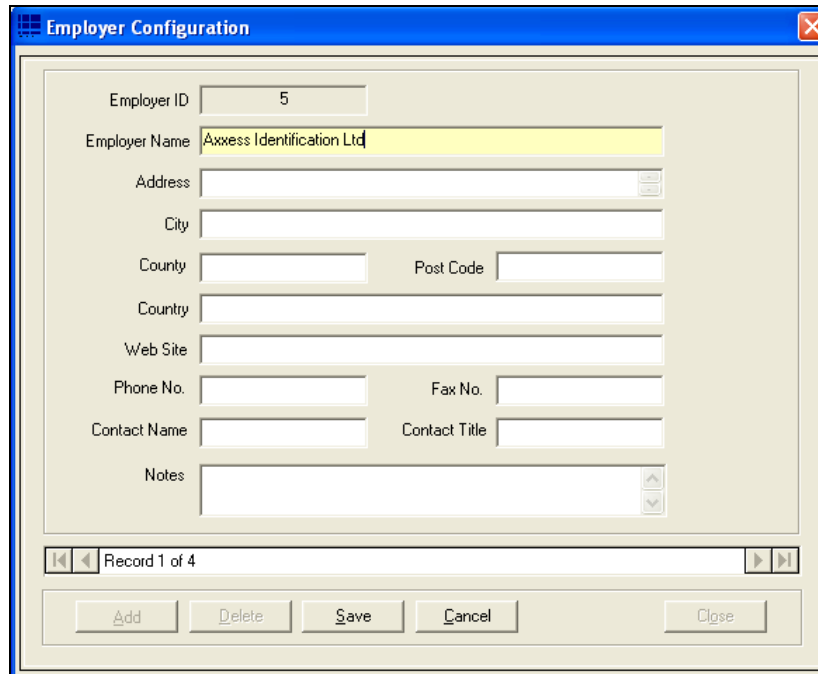
Employer

To add a new employer click on the drop down menu. Once the employer list has been opened click **Add**.



You must enter an **Employer Name** in the Employer Configuration window. Once you're finished click **save** and exit. You can edit an existing employer by clicking on the **Edit** button.

Installation & User Guide



The Employer Configuration window contains the following fields:

- Employer ID: 5
- Employer Name: Axxess Identification Ltd
- Address: [Empty]
- City: [Empty]
- County: [Empty] Post Code: [Empty]
- Country: [Empty]
- Web Site: [Empty]
- Phone No.: [Empty] Fax No.: [Empty]
- Contact Name: [Empty] Contact Title: [Empty]
- Notes: [Empty]

Navigation: Record 1 of 4. Buttons: Add, Delete, Save, Cancel, Close.

Mode Settings

Individual setting per door and per user for High Security and Latch function

- authorised to set Latch function
- authorised to set High Security mode
- access granted in High Security mode
- extended door open time on valid card use

Mode settings tab is an important section of cardholder configuration. It allows you to programme a card to have a specific effect when presented to each reader. The access point column includes the list of all the readers configured on your PC.

Mode Settings						
Access Point	Hi Sec	Ext'd Door	Set Hi Sec	Set Latch	Time Zone	
Main Entrance	Yes	No	Yes	No	Always Access	
▶ Control Room	No	Yes	No	Yes	Always Access	Always Access
IT Room	Yes	No	Yes	No	Always Access	

Dropdown menu options: Always Access, No Access, Always Access, Always Exception, TZ9, TZ8, TZ7, TZ6, TZ5.

Installation & User Guide

High Security (Hi Sec)

If a door is set on high security mode, you need to have a high security card to unlock it. Mode settings section is the place to create a high security card. By default no card has the permission to open a high security door. However you can grant this permission simply by changing the text **NO** to **Yes** (by clicking on it) under the Hi Sec column.

Extended Door Open Time (Ext'd Door)

Activates the Extended Door Release Time function. To change the Ext'd door release time please refer to *Access Point configuration • Access Point*.

Set High Security Mode (Set Hi Sec)

There are two ways to set a door on high security mode. You can use the High Security button located on the right hand side of the main screen under the list of controllers or you can use a card. Once the "Set Hi Sec" is activated; if you present your card to the appropriate reader, 4 times within eight seconds, the reader will automatically go on the high security mode. To restore the normal mode repeat the same procedure. Activating "set high security" mode also activates the "high security" option.

Set Latch

Once the set latch is activated; if you present the card to the appropriate reader twice within four seconds, the door will be unlocked and it will remain open until it is put back to normal mode, either by using the same card twice or by pressing the normal mode button on the main screen.

Time Zone

Allows you to choose a different time zone for every door.

Personal Info

Includes additional information about the cardholder such as: date of birth, address, e-mail and ...

Date of birth	use drop down calendar or type in date
Age	automatically calculated using the date of birth field
Sex	male, female, other
Address	maximum 101 characters over 28 lines
City	text field maximum 30 characters
County	text field maximum 30 characters
Country	text field maximum 20 characters
Postcode	text field maximum 20 characters

Installation & User Guide

Home phone	text field maximum 30 characters
Mobile	text field maximum 30 characters
Email address	text field maximum 50 characters
Home page	text field maximum 50 characters
National Insurance No	text field maximum 20 characters
Payroll	text field maximum 20 characters
Notes	text field maximum 255 characters

Personal Information

Date of Birth Age Sex

Address

City County

Country Post Code

Home Phone Mobile

Email Address Home page

National Insurance No. Notes

Payroll

Vehicle info

Contains information about the person's vehicle. You can choose your car make and model from the appropriate list. Press **Add** (in the car make/model list) if you need to add a new car or press Edit if you need to change the details of an existing model.



First Car

Car make	select from drop down list
Car model	select from drop down list
Car colour	select from drop down list, pre-defined with car shown in selected colour
Registration number	text field 30 characters maximum
Parking space	text field 50 characters maximum

Second Car



Car make	select from drop down list
Car model	select from drop down list
Car colour	select from drop down list, pre-defined with car shown in selected colour
Registration number	text field 30 characters maximum
Parking space	text field 50 characters maximum

Installation & User Guide

Main Settings	Other Info	Mode Settings	Personal Info	Vehicle Info
Vehicle Information				
First Car				
Car Make	Ford		Car Colour	Green
Car Model	Probe		Registration No.	G54654
Parking Space	P3			
Second Car				
Car Make	Peugeot		Car Colour	Black
Car Model	405		Registration No.	KJY5431
Parking Space	12M			

Access Point Configuration

Access Point Settings

Access Point Settings		
Access Point ID	2	
Access Identity	001009	
Access Point Name	Access Point 1	
Comments		
<input checked="" type="radio"/> Normal	<input type="radio"/> In Reader	<input type="radio"/> Out Reader
<input checked="" type="checkbox"/> Door Schedule	 Time Settings	<input type="checkbox"/> CCTV 

Access Identity

Every device has a unique “**Access Identity**” and is given a distinctive “**Access Point ID**” when connected to the PC. Each controller has a serial number and this is used to communicate with the PC. If the identity has been entered manually during a system setup or where controllers are connected using a DTU, then the replace function should be used when the controllers are operational.

Access Point Name

Access Point Name is specified by the user and could be changed at any time. The extended length of the field allows up to 50 characters e.g. Building 1 Section West Door 28 Admin. The first 20 characters are displayed on the current controller information.

Installation & User Guide

Door Comments

This memo field can store additional details regarding the location or any other use e.g. temporarily out of use due to building work

Every reader can be programmed as **Normal**, **In Reader** and **Out Reader**.

If a reader is set to operate as an **In Reader**, the card number and the person's name would appear on the "who's in list" when the card is presented to it.

If a reader is programmed to be an **Out Reader**, the card number and the person's name would be removed from the "who's in list" and appear on the "who's out list" when the card is presented to the reader.

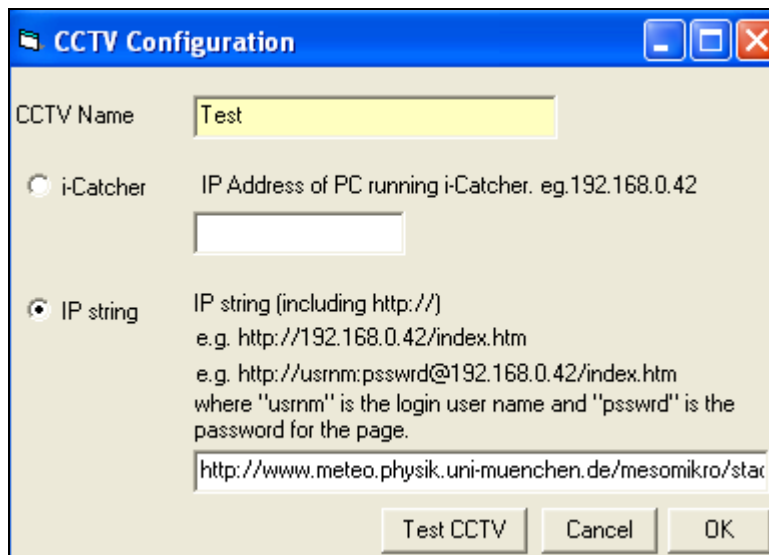
If a reader is set on **Normal** mode, access will be granted to the person holding a valid card. However it doesn't affect the *who's in/out* list. In other words it doesn't influence the count of the people inside the building.

Time settings button becomes active by ticking the **Door schedule** box and clicking on the **save** button.

You can schedule a door to be open during a specific period of time by clicking on the "**Time Settings**" button. The door can be programmed simply by clicking and dragging the mouse. The green zone is the time period during which the door will be unlocked.

Note: Please note that the door status selected in the main screen overrides the door schedule. This means that once the door has been unlocked by using the controller buttons on the main screen, it will remain open even though it has been scheduled to be closed.

CCTV: opens the CCTV configuration window. You will then have to either enter the IP address of the PC running the *I-Catcher* software or enter address of the web page containing the camera.



Installation & User Guide

Door Release Time

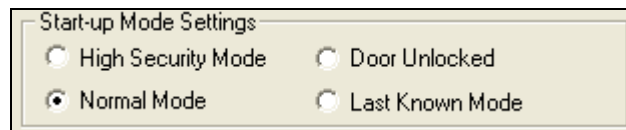


Standard door release time is the amount of time it takes for the door to be locked again, after being opened by a valid card. (Range: 1•255s)

If the “**Extended** door open time” option has been activated in the *mode settings* of a card; then the door will remain open for the amount of time entered in the **Extended** field. (Range: 1•255s). It allows individual cardholders to have the door open for a longer period of time e.g. disabled or elderly people.

Request to Exit This time can be individually set and is often set longer when the REX is used at the reception allowing visitors a slightly longer entry time. When the REX Button is used, the reader fitted outside can be set to sound twice to indicate the door has been released for visitors. This feature is particularly useful when used with magnet locks since their operation is totally silent.

Start-up Mode Settings



The start-up mode settings enable you to determine how the door operates in case of total power failure, including exhaustion of the battery back-up. All the data is stored permanently in the controller for up to 100 years without the need for any power and upon power-up will continue to operate without the need for a database download.

High security mode	Only cardholders with the high security mode enabled will have access.
Normal mode	Returns to normal mode from whatever the status was prior to power failure.
Door unlocked	The door unlocks permanently until a valid card with the unlock feature is used twice, or the door is changed to normal mode from the PC.
Last known mode	This will return to the status the door was set to prior to power failure.

Group(s) contain this point displays the list of the *access groups* which the current access point is assigned to.

Door Contact Settings

Installation & User Guide

Door Contact Settings			
<input checked="" type="checkbox"/> Door Contact	<input checked="" type="checkbox"/> Door Forced Alarm	Local Door Held Open Alarm	5 Sec.
<input checked="" type="checkbox"/> Relay Reset	<input checked="" type="checkbox"/> Sounder	<input checked="" type="checkbox"/> Reader Off When Open	Door Held Open Alarm 15 Sec.

Door contact settings are enabled by ticking the **Door Contact** box. Door Contact

Door Forced Alarm: generates an alarm immediately after the door has been opened by using force. The alarm is cleared automatically as soon as the door has been closed. However the **sounder** remains active until you select the appropriate reader from the menu on the right hand side of the main screen and press “Clear Alarm”, or present a valid card.

Relay Reset: De-activates the relay timer instantly when the door is opened. By choosing this option only one person gets access after presenting a valid card and the possibility of tailgating is reduced.

Reader off When Open: the reader will be disabled (not the REX) if the door contact is open. This feature can be used for alarm systems e.g. the alarm is on so the door cannot be opened, Parking application - there is no car on the presence loop, so the barrier cannot be activated by a pedestrian or for air locks, one of the two doors is open so the second remains closed.

Door Held Open Alarm: the length of time after the relay expires the door is allowed to be open before an alarm is generated.

Local door held open: This is a local alarm activating the sounder in the reader but does not send an alarm to the PC (if online). This feature is normally used in conjunction with door held open alarm and warns people local to the door to close the door or a full alarm will be raised. This feature is particularly useful with online systems where security guards are called out a number of times whilst people are talking in the doorway.

PIN Settings

PIN Settings			
<input checked="" type="radio"/> Card Only	<input type="checkbox"/> High Security Mode Activates Card + PIN		
<input type="radio"/> PIN Only	<input type="radio"/> Card + PIN	PIN Timeout	5 Sec.

Card Only: PIN pad is deactivated when the Card Only mode is selected. Access is granted only when a valid card is presented.

PIN Only: A Personal Identification Number (PIN) only is required to open the door. This can be an individual number per user or a number for a group of users. The system supports 2,000 PIN only or 2,000 card and PIN users. In this mode, if different PIN lengths are used per person, less than the maximum PIN length set under “general settings” the number requires # to complete the entry. If the maximum length is set to four then only four digits have to be entered.

Card + PIN: First a valid card must be presented to the reader followed by the individual PIN of the cardholder. In this mode the controller will know from the card what the PIN length will be and no # will be required

Installation & User Guide

PIN Timeout: Indicates in seconds, the time required to enter the PIN number before clearing the buffer or sending the data as invalid or incomplete. A longer time might be required for elderly, disabled or specific locations i.e. car parks.

High Security activates PIN: The system normally operates in card only mode and changes to card + PIN when a High Security card is used four times at the reader. This is normally used at the end of the day to increase security after normal office hours.

Device Parameters

Device name & Identity are displayed on the top left of the screen. Device name could be specified in the *Access Point Settings* section under the *Access Point* tab. Do not attempt to change the Identity manually; it may no longer be recognized by the application.

Every device is given a specific name when connected to the PC. **Device Name** could be changed in the *Device Manager* tab.



Device Group

This specifies the type of device connected.

Device Type

Within the device group the type of unit

Hardware Version

Hardware revision number

Installation & User Guide

Firmware Version

Firmware revision number in AX100 PCB

Batch Number

Production identity number

Serial Number in Batch

Serial number to be used with batch number

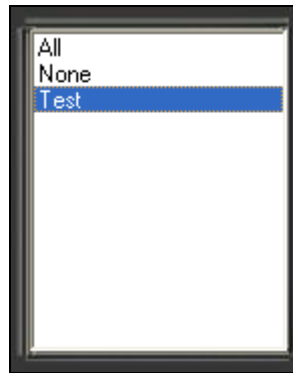
Database Stamp

This number is automatically generated and ensures the correct data is automatically downloaded. If another PC is connected, this number is different and a forced download is required since the data held on the PC and the AX100 controller are different.

Access Groups

Access groups give you the possibility to gain access through more than one door by using a single card. Once the access group is assigned to a card (in the card holder section) you can open all the doors listed in the access group.

The menu on the right hand side of the screen contains all the access groups created in the software. All & None are the defaults. The first group in the list is automatically highlighted when you open the Access groups tab.



Access group tab contains two separate lists: **Controller(s) available & Selected Controller(s) in Group**. The first list contains all the access points that have not yet been assigned to the highlighted access group. Therefore if group “All” was highlighted the “Controller(s) available” list would be blank. The access group ‘All’ gives access automatically to all AX200 controllers including new ones added at a later date and cannot be deleted or altered.

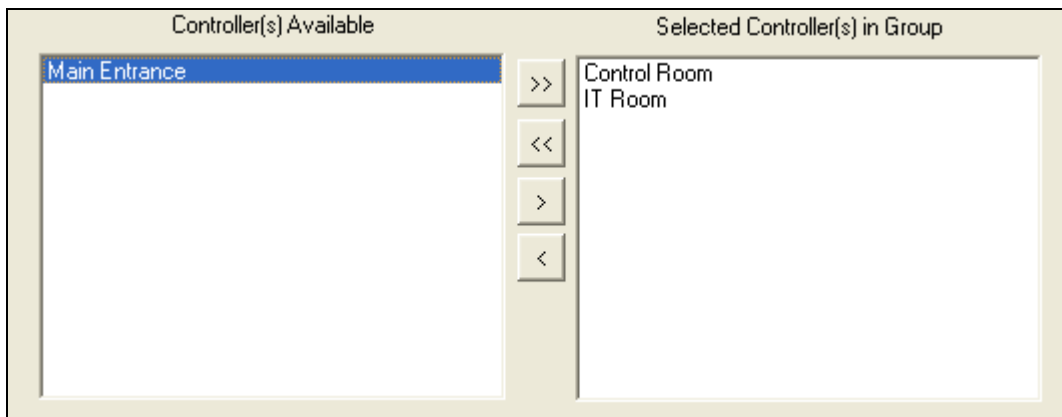
The **Fixed** sign in the Group Configuration section means you cannot change any information displayed on the screen.

Installation & User Guide

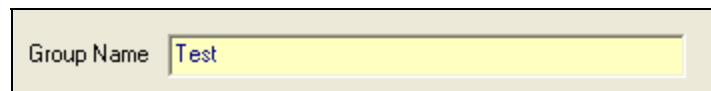


Creating a new access group

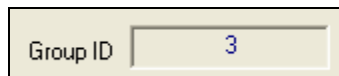
Making a new access group is very easy and quick. All you have to do is to click on the “Add” button and transfer the appropriate doors from the “Controller(s) available” list over to “Controllers in group” list. In order to move an access point across; you can either double click on it or highlight it and press the > button. Clicking on the >> button would transfer all the access points at once.



When finished, type in a name for your group and click “Save”.



After saving, the software will automatically give your group and ID number.



Device Manager

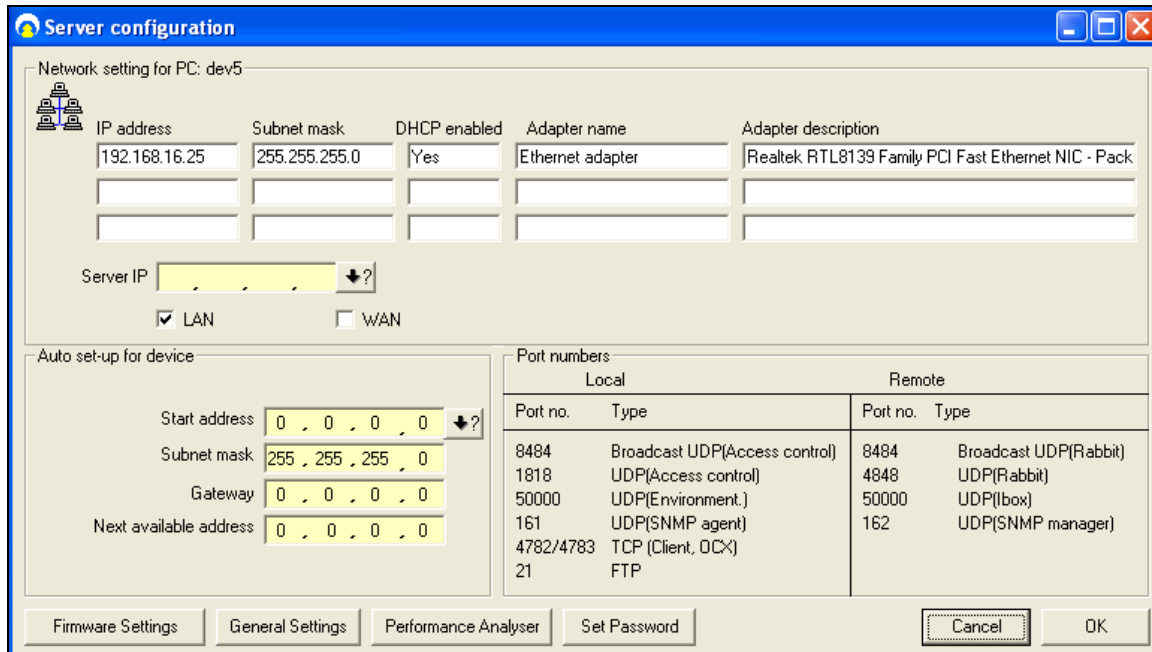
Device manager displays all the devices that are or have been connected to the local network at some point.

The PC server icon on the top opens the **Server IP Configuration** window where you can configure the network settings of your PC. If the icon becomes red it means there is something wrong with the network settings of the PC. This usually happens when the IP address of the server is incorrect.

Installation & User Guide



So if the PC server icon is red open the server configuration window by double clicking on the icon.

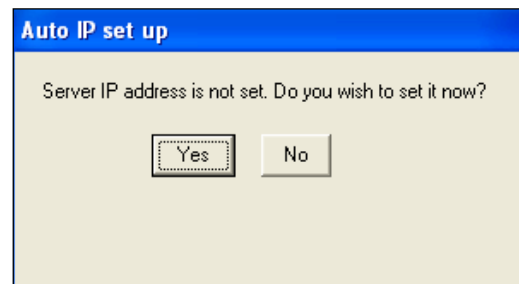


If the **Server IP** field is blank or contains a number which is different from the IP address of your PC click on the •? Button. The software will automatically obtain the correct IP address of your PC. When you're done click OK. The PC server icon should now be blue.



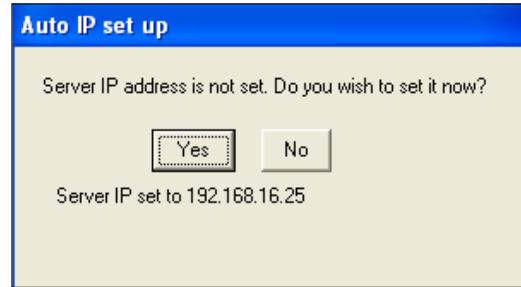
Automatic IP Setup

The IP address of the server stored in the database is automatically checked against the IP address of the PC every time the application is restarted. If the IP address has not been set, the software will notify the user by displaying a message box asking if they want to obtain the correct IP address.



Installation & User Guide

After pressing **Yes**, the correct IP address is automatically detected and displayed. This IP address will be recorded in the database as the server IP.

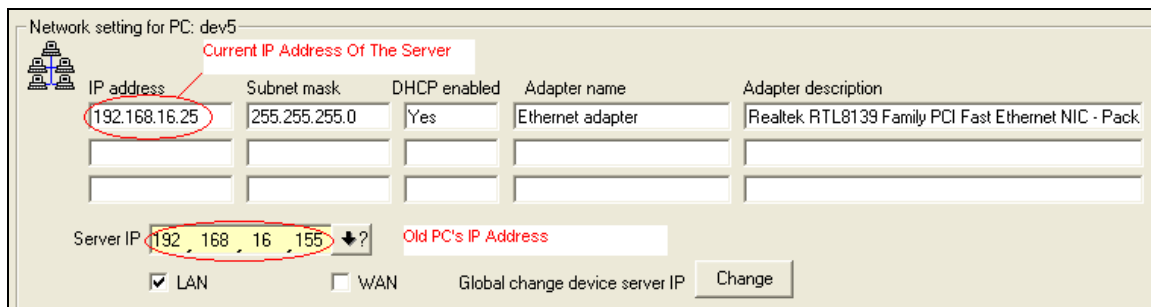


If the IP address of the PC does not match with what's been recorded in the database, the software will warn the user at the startup by displaying the following transaction.

10:59:13 Server IP is incorrect Please go to device manager to correct it

To get to the *Server IP Configuration* click on *Access Point* on the main screen; under the *Device Manager* tab click on **server IP** icon at the top. In this screen you can obtain the correct IP address by pressing the ↓? Button. This usually happens when the database is moved to a different PC.

If the database has been restored on another PC the server IP address in the database will not match the IP address of the new PC. If you press the Change button in the server IP configuration **the software will automatically download the IP address of the new PC onto all the devices connected to the local area network**. In other words all the devices on the network are now configured to communicate with the new server (current PC).



If however the IP address of the server is changed while the DHCP is not running; you will have 2 options available: 1) you can download the current server IP onto all the devices connected to LAN, by pressing **Global change device server IP**; or 2) you can change the current IP address of the PC, back to the last recorded IP address in the database, by pressing **Set PC IP address to last stored**. Once the PC is set the old IP address you will be able to communicate with all the devices that had previously been configured on your PC.

Installation & User Guide

Network setting for PC: dev5

IP address	Subnet mask	DHCP enabled	Adapter name	Adapter description
192.168.16.199	255.255.255.0	No	Ethernet adapter	Realtek RTL8139 Family PCI Fast Ethernet NIC - Pack

Server IP: 192, 168, 16, 25

LAN WAN Global change device server IP Set PC IP address to last stored

Current IP Address Of The Server (points to 192.168.16.199)

Server IP As Stored In The Database (points to 192, 168, 16, 25)

Device Status Indication

If a device has been disconnected from the network it goes **off-line** and is displayed with a red cross on it.



If a device icon is red it means the controller is connected to the network but is not programmed to communicate with your PC.

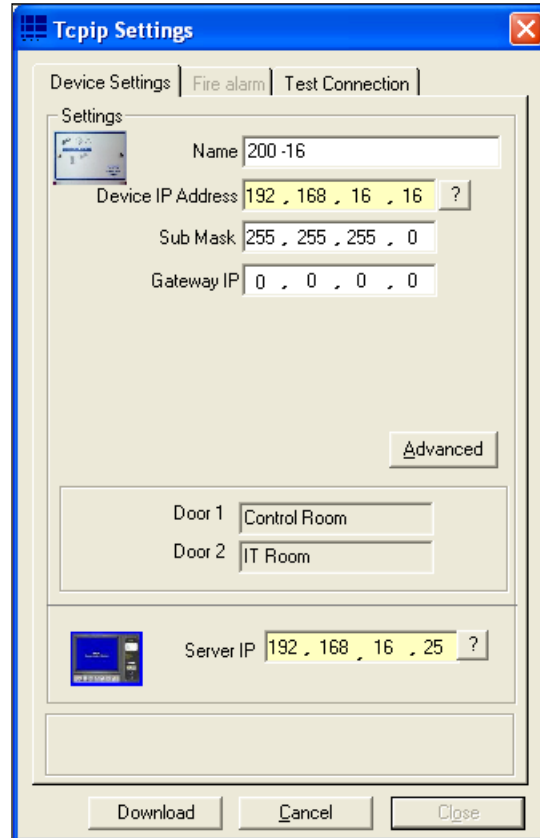


In order to configure a device on your PC open the **Tcpip Settings** window by double clicking on the device icon.

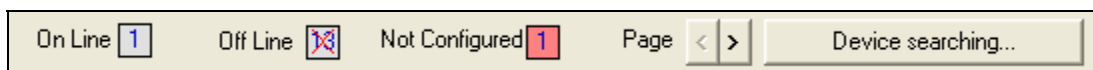
Installation & User Guide

In the Tcpiip settings window, under the Device settings tab; click on “?” in front of the Server IP field (on the bottom) to obtain the server PC IP address.

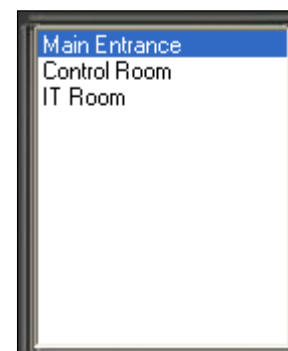
The device IP address is made up of 4 numbers separated by “,” and is located in the top half of the screen. The first three numbers of the device IP address must match the first three numbers of the Server IP address. However the fourth number could be anything between 1 and 254. After entering the device IP, click on the question mark to make sure the IP you’ve entered is free. If the message says the IP address is in use, change the last number of the IP address and try again. Choosing a duplicate IP address could cause conflicts in the network. When you’re finished click download.



The numbers of Online, Offline & Not Configured units are displayed on the bottom of the window. You can use the **Device Searching** button to refresh the screen.



The menu on the right shows the list of all the configured access points. Double clicking on any of them will open the Tcpiip settings window of the unit which the access point is connected to.



Double clicking on any of the units in the device manager screen will open the Tcpiip Settings Window.

Installation & User Guide

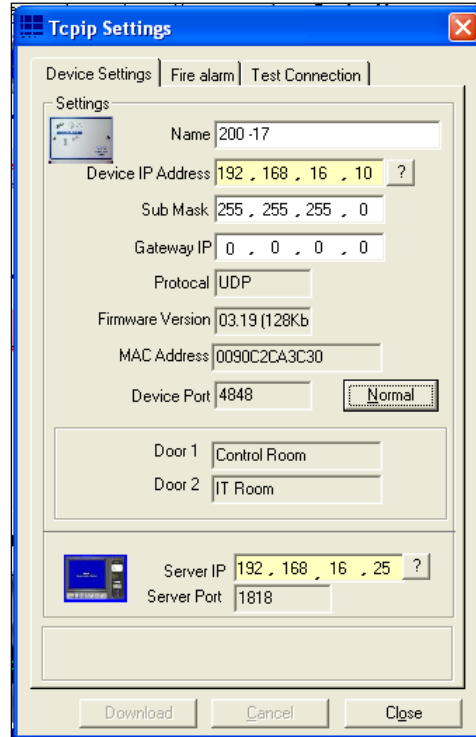
Device Settings

Device settings tab mainly provides you with the network settings of the selected unit. Every unit is given a unique name by the application when connected to the network. You can change this name at any time. To avoid any possible conflicts in the network make sure you don't choose a duplicate name.

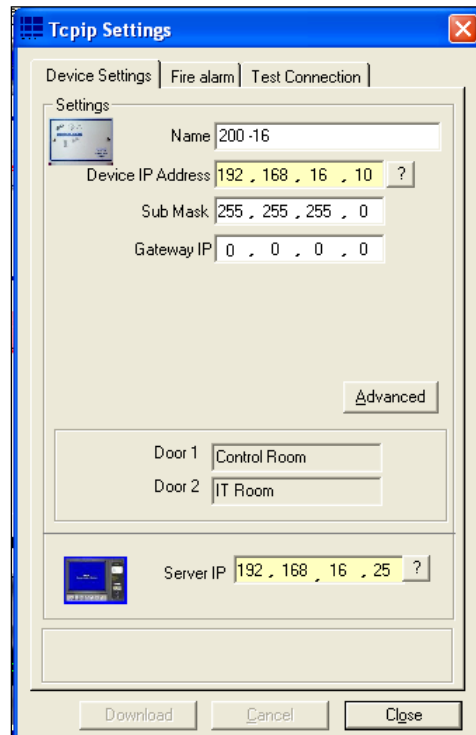
The IP address of the server is displayed at the bottom of the page. The correct IP could easily be obtained by clicking on the ? Button.

The **Device IP Address** however should be entered manually. The first three numbers are identical with the first three numbers of the **Server IP**. The fourth number could be anything from 1 to 254. The question mark is to make sure that the device IP address is not in use.

The name of the doors connected to the controller is shown in the middle of the screen. To change them you need to go back to the *Access Point* tab.



Clicking on the **Advanced** button provides you with more information about the current device such as the firmware version or the MAC address.

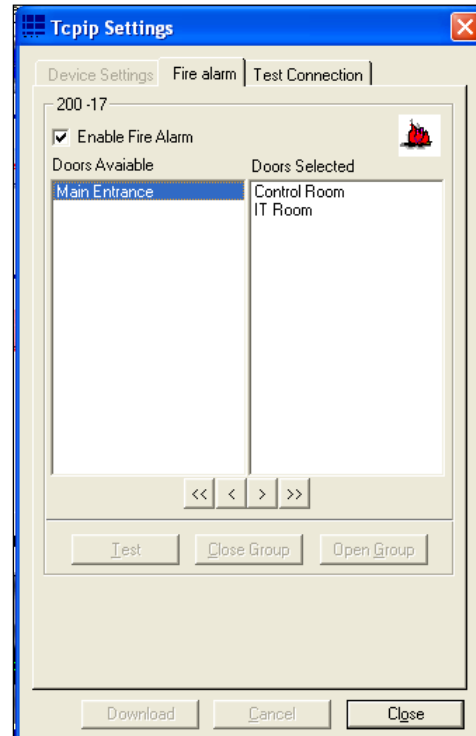


Installation & User Guide

Fire alarm

This section gives you the ability to unlock all the doors in your building simultaneously by using only one controller. The way it works is that, if the fire alarm is triggered on the current controller all the access points listed in the doors selected list will be opened at once. To enable the settings tick the **Enable Fire Alarm** box.

Doors available list contains all the access point configured on your PC. By default the **Doors selected** list contains only the reader(s) that are connected to the current controller and you cannot remove them. You can add more doors to your list by double clicking on them or using the buttons below the list. Press the download button once you're finished.



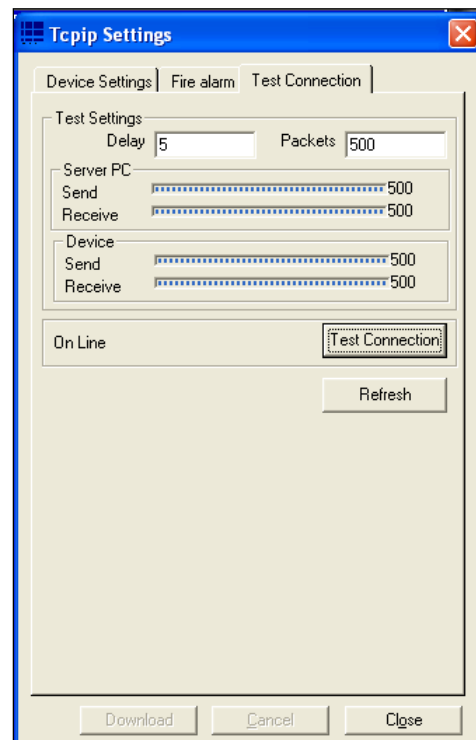
Test Connection

Test communication checks the communication between the PC and the device through transmitting messages from one to the other. The number of these messages is given in the **Packets** field.

When you press the **Test Connection** button the PC will start sending 500 (default) packets to the device and the device responds by sending 500 packets back to the PC.

You can control the speed of the process by specifying the delay between 2 packets. The number in the delay field is in milliseconds.

The connection is considered to be in a good condition, provided that no more than 15% of the sent packets are lost.



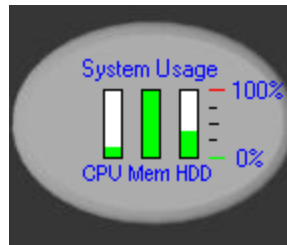
Installation & User Guide

System Settings

A continuous check is carried out on the PC's system resources. These graph bars are located under the system settings menu and indicate the performance of the system. Often systems grow bit by bit and no care is given to memory, hard disk space or CPU usage. This can result in very slow operation or, in the case of lack of hard disk space, a computer crash.

Real-time indicators are:

- CPU usage** The CPU usage displays how hard the processor is working. If this is continuously on 100% the system will be slow and would improve substantially if the processor is upgraded. During backups etc. this indicator will go to 100% which is quite normal since these tasks are processor intensive.
- Memory** This displays the amount of RAM in use by the computer in total. Often other applications running in the background occupy a lot of memory leaving less than expected for the access control application. A continuous 100% bar shows that adding memory will improve performance substantially.
- HDD Usage** This should never come to close to 90%. Clean up unwanted and very old files on the computer to free up disk space. If there is not sufficient hard disk space available, the computer will become very slow and eventually will stop operating. Refer to your Windows manual for further details.



Site Info

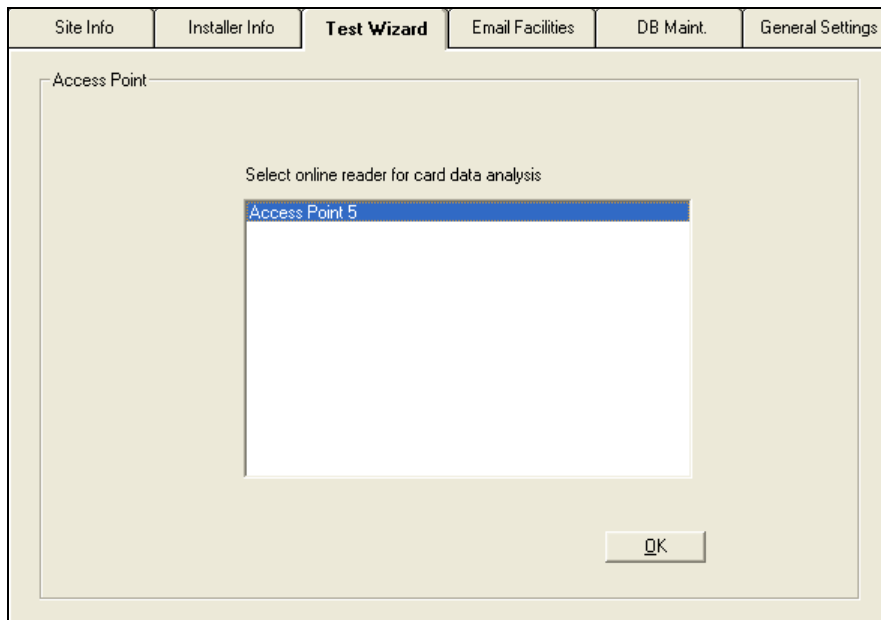
The site info tab under "general settings" contains 11 data fields including contact name, address, telephone and system reference numbers. This information is automatically included in various reports and email functions e.g. card re-ordering and System Settings report.

Installation & User Guide



Test Wizard

The test wizard provides an easy and effective way to setup the AX200 system. Together with hardware and software tests, the test wizard enables you to setup the appropriate card format. The card used for testing will have access to all doors with high security and latched (door unlocked) functions enabled. At the end of the wizard, the test report can be printed to a default printer and the test card can be deleted if required.



Select the appropriate door from the list and press OK. The list contains only the doors that are online and communicating to your PC.

Installation & User Guide

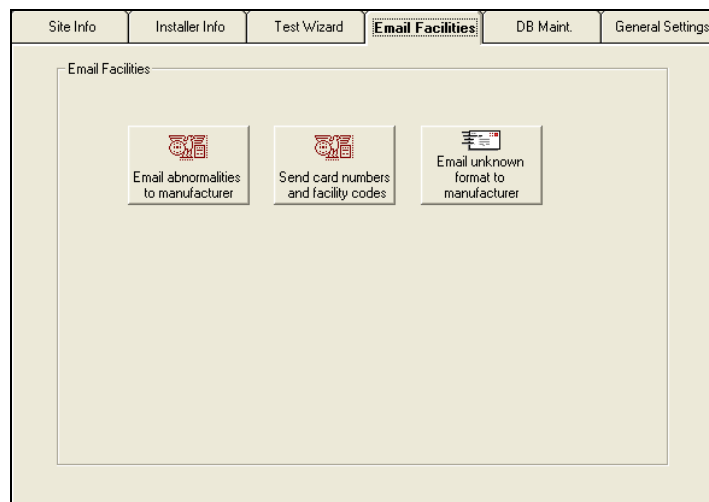
Test wizard is also accessible under Tools menu on the main screen.

E-Mail Facilities

When additional cards need to be re-ordered, it is often difficult to know the type of card, facility code etc. which can result in delays of card supply or the supply of incorrect cards for the system. The send card numbers and facility code, emails all the relevant data to the installer. This feature requires an internet connection.

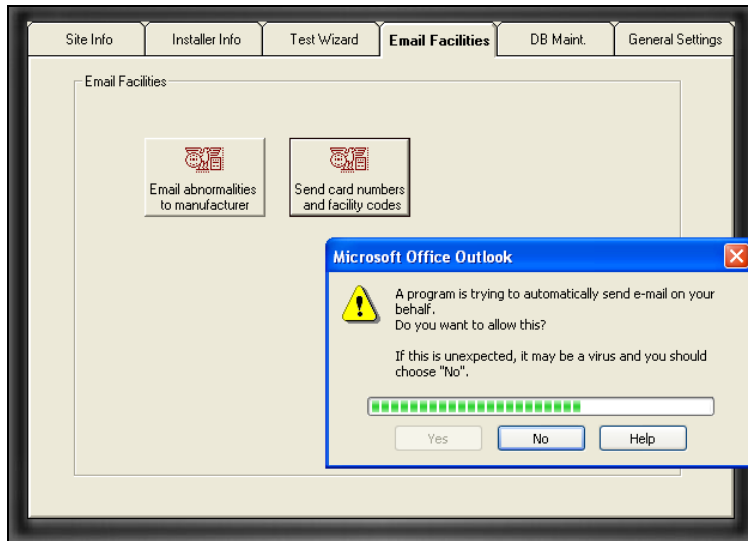
E-Mail Unknown Format to Axxess ID

If existing cards are used which are not known to the AX200, the data collected under Format and Statistics – Card Matching can be e-mailed from here. This avoids the need to send cards in the post for verification. New formats created can then be e-mailed back.



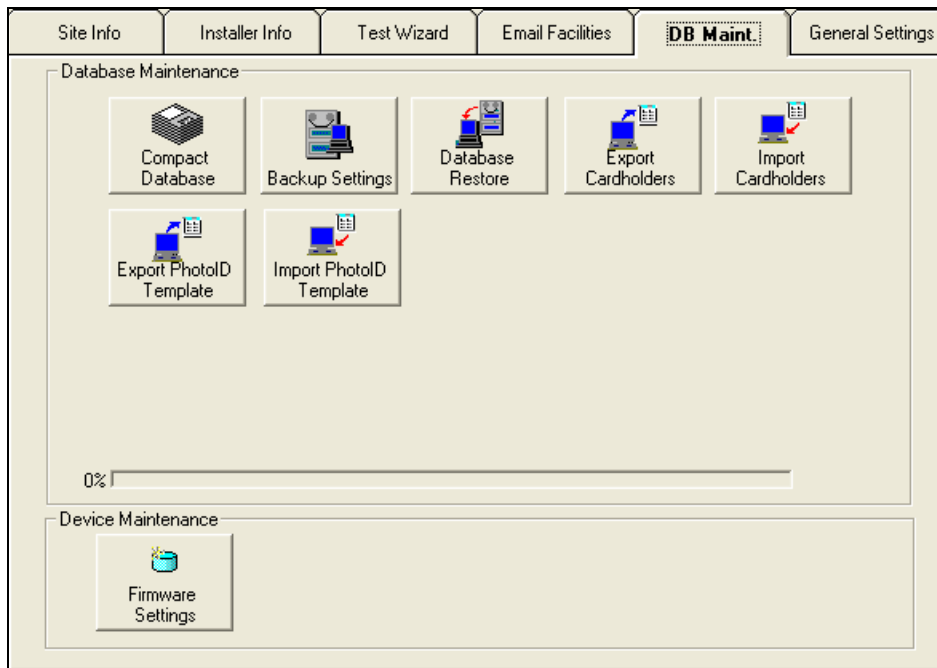
When you press one of these buttons, the program will try to send the relevant information to the manufacturer (*support@axxessid.com*) on your behalf. The application will use *Microsoft Office Outlook* to transmit e-mail messages.

Installation & User Guide



DB Maintenance

Database maintenance is normally done by the AX200 automatically. If data is corrupted because of an unexpected shutdown of the PC this is repaired automatically when the software is restarted. All erase functions require an override password and are normally never used. After each backup, files are automatically deleted.



Compact Database

Installation & User Guide

The database can become slow if a large number of additions and deletions of records occur. The compact database function reorganises the database which reduces the database size and improves the speed. Compacting the database is recommended every three months or every 500 cardholder changes.

Backup Settings

It is strongly recommended to backup the system frequently. This can be done manually or automatically at preset times and days. The backup path is by default to the same hard disk as the AX200 software (*C:\Program Files\AX200\backup*). It is recommended to backup to tape in case of hard disk failure.

Log and event files can be deleted after a specified amount of time (Backup settings), to prevent the hard disk becoming full. Using the report module, backup events can be viewed and printed.

Database Restore

In the unlikely event that a database corruption cannot be repaired, (automatically on start-up), this feature allows you to restore a backup database. Cardholders or system changes made since the last backup will be lost.

Export Cardholders

Cardholder details can be exported in standard .CSV files for use in other software programs. You will need *Microsoft Excel* to open that file.

Import Cardholders

Contact factory for details.

All of the above features are also accessible under the *File* menu in the main screen.

Export Photo ID Templates

Exports all the photo ID templates in a mdb file. You will need *Microsoft Access* to open that file.

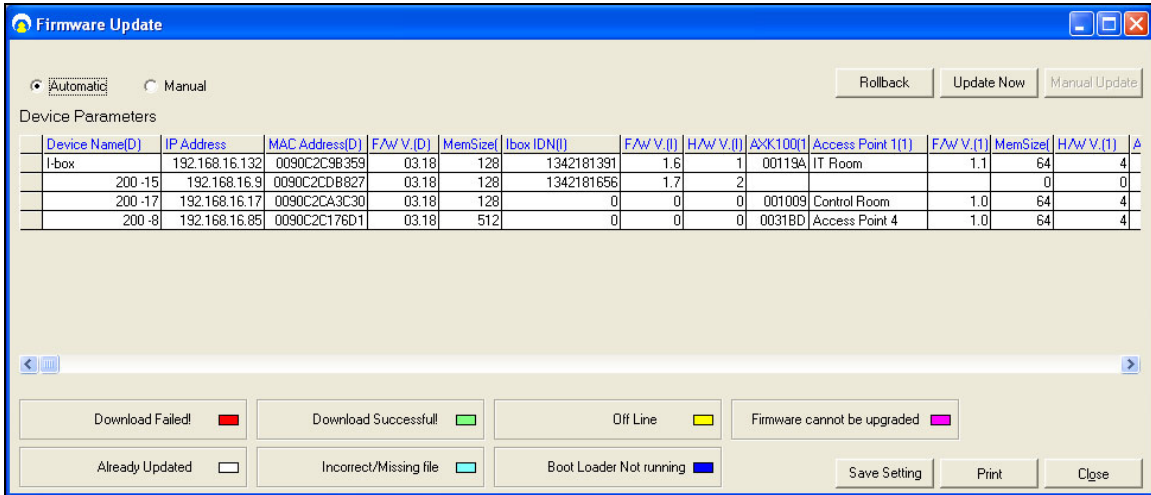
Import Photo ID Templates

Contact factory for details.

Firmware Settings

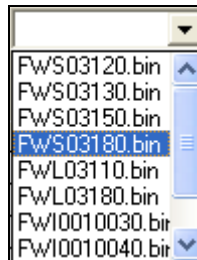
Firmware update window contains a list of all the devices on the network and the relevant information about the network settings and the firmware on each unit.

Installation & User Guide



Firmware update functions both manually and automatically. If the automatic option is selected all the units on the network will be upgraded to the latest version of firmware on 11:00 PM at night. Both rabbit FW and I-box FW will be automatically upgraded. If a device already has the latest version of firmware, it will not be affected.

If the manual option is selected, a drop-down menu will appear on the screen where you can download the appropriate firmware on individual units. The menu contains every version of firmware on your PC. You have to upgrade the rabbit firmware and the I-box firmware separately.



If the download is successful, the cell containing the device name will become green. Other colours are explained on the bottom of the screen.

Device Name(D)	IP Address	MAC Address(D)	F/W V.(D)	MemSize(I)	Ibox IDN(I)
I-box	192.168.16.132	0090C2C9B359	03.15	128	1342181391

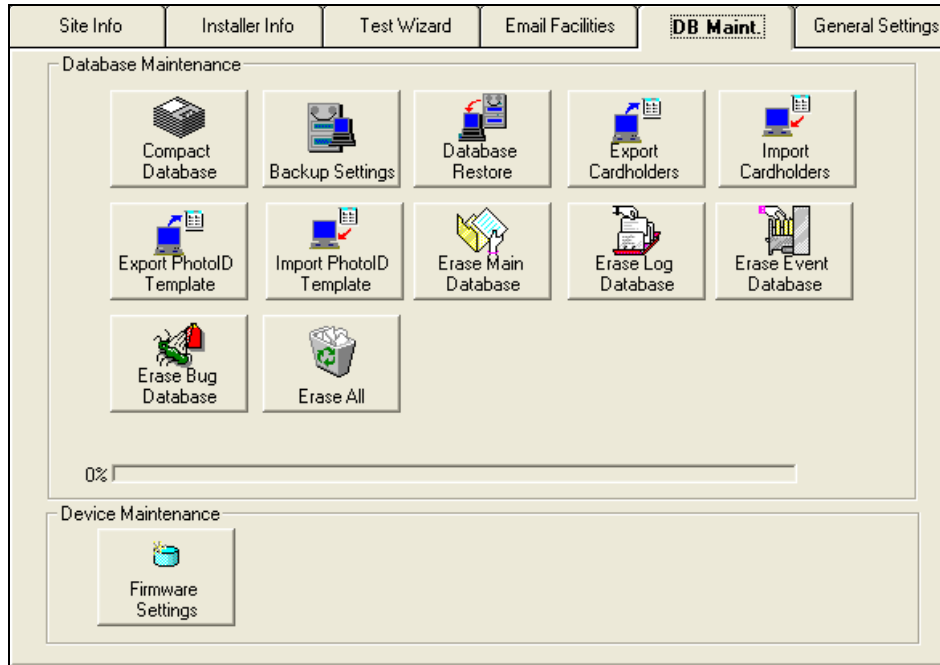
Rollback

Rollback button is an automatic function. When you press the rollback button the software will downgrade both the rabbit firmware and the I-box firmware by one version on every unit connected to the local network.

Hidden Functions

Installation & User Guide

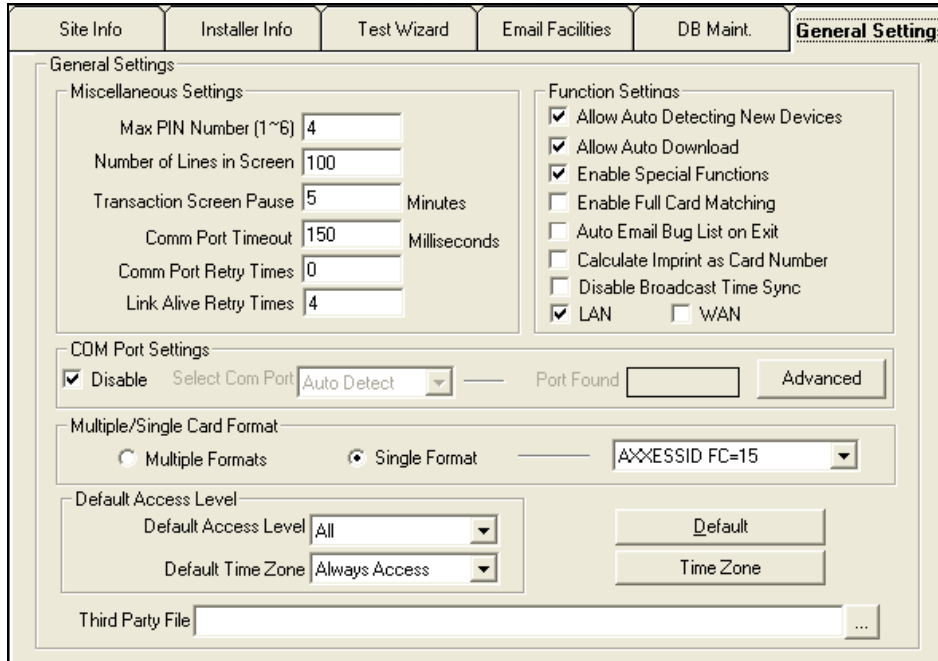
Hidden functions are only displayed when the *Special Functions* in the *General Settings* tab are enabled. These features are for engineering purposes only. That's why by default these functions are disabled.



These functions include: *Erase Main Database*, *Erase Log Database*, *Erase Event Database*, *Erase Bug Database* and *Erase All*. *Erase All* includes all the other erase functions and will replace your current database with a default (blank) one. You need to enter 1234 as the override password to use any of the above mentioned functions.

Installation & User Guide

General Settings



Maximum PIN Number 1~6

This option sets the maximum number of digits required when using a PIN code. If a PIN only is being used and the PIN code is less than the number of digits set under this setting, the # key is required to complete the action.

Number of Lines in Screen

This is the number of transactions kept in active memory, allowing the user to see them instantly on the main screen. A larger number will use more memory and can affect the speed of the software.

Transaction Screen Pause

When the main screen is full with transactions, yellow buttons appear allowing you to temporarily stop incoming transactions. Transactions will still be stored on the hard disk for viewing at a later stage through the report module. After the set time, the system will automatically resume. The default setting is 5 minutes.

COM Port Timeout

This is one of the special functions which is hidden until the *Special Functions* are enabled in the software. If a device which is communicating through the COM port doesn't get a response in a certain amount of time, the communication will stop. The recommended time is 150 milliseconds.

COM Port Retry Times

This is the number of times that the software will try to reconnect to the device after the COM port timeout. The default value is 0.

Installation & User Guide

Link Alive Retry Times

The AX200 and the I-box units send a link alive message to the PC every 5 seconds to confirm that the communication is stable. If the PC doesn't receive this message it assumes that the unit has gone off-line. This option specifies the number times that the PC will attempt to get a link alive message before the "PC Off-line" transaction appears on the main screen.

Function Settings

Allow Auto Detecting New Devices

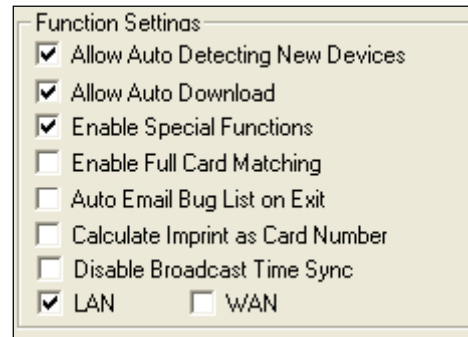
Auto detect can be switched off if required.

Allow Auto Download

System and cardholder data is automatically downloaded to the controller when you close and go back to the main screen. When switched off, a red icon will appear on the bottom of the main screen; if a



download is required. In this case downloads have to be done manually using the Utilities, Download menu.



Enable Special Functions

This feature is mostly used for engineering purposes. It enables the hidden features embedded in different parts of the software. The default setting is off.

Enable Full Card Matching

This feature allows the use of facility code, site code, card number and issue number. Site code and issue number are occasionally used by some card manufacturers. The default setting is off.

Auto Email Bug List on Exit

Uses the default e-mail facility on your PC to email the Bug list to the manufacturer (Support@Axxessid.com) when you attempt to quit the software. The default setting is off.

Calculate Imprint as Card Number

Calculates the imprint as reverse mifare and works out the correct card number.

Disable Broadcast Time Sync

Disables the broadcast of the time synchronization. This feature is used for older firmwares.

LAN/WAN

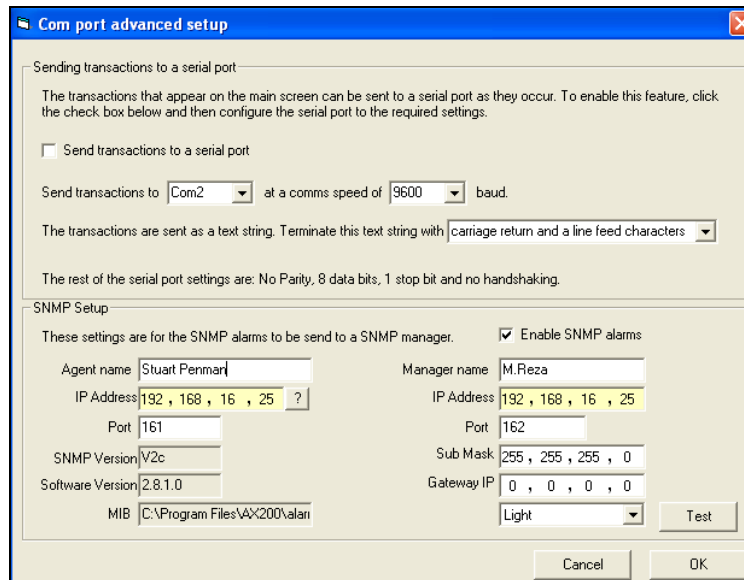
You can select between the Local Area Network and the Wide Area Network. This option is also available in the Device Manager • Server Configuration.

COM Port Settings

Installation & User Guide

Select COM Port

The AX200 software on start-up will automatically scan COM ports 1 to 4, and if found, display the port found. Consequent start-up of the AX200 software will look at the port found address only. By selecting auto-detect, the software will scan all ports and find the appropriate COM port. Manually ports 1 to 16 can be selected if required. Baud rate and parity settings are automatically configured. The default setting is “Disable”.



Com port advanced setup

Sending transactions to a serial port

The transactions that appear on the main screen can be sent to a serial port as they occur. To enable this feature, click the check box below and then configure the serial port to the required settings.

Send transactions to a serial port

Send transactions to **Com2** at a comms speed of **9600** baud.

The transactions are sent as a text string. Terminate this text string with **carriage return and a line feed characters**

The rest of the serial port settings are: No Parity, 8 data bits, 1 stop bit and no handshaking.

SNMP Setup

These settings are for the SNMP alarms to be send to a SNMP manager. Enable SNMP alarms

Agent name **Stuart Penmar** Manager name **M.Reza**

IP Address **192, 168, 16, 25** IP Address **192, 168, 16, 25**

Port **161** Port **162**

SNMP Version **V2c** Sub Mask **255, 255, 255, 0**

Software Version **2.8.1.0** Gateway IP **0, 0, 0, 0**

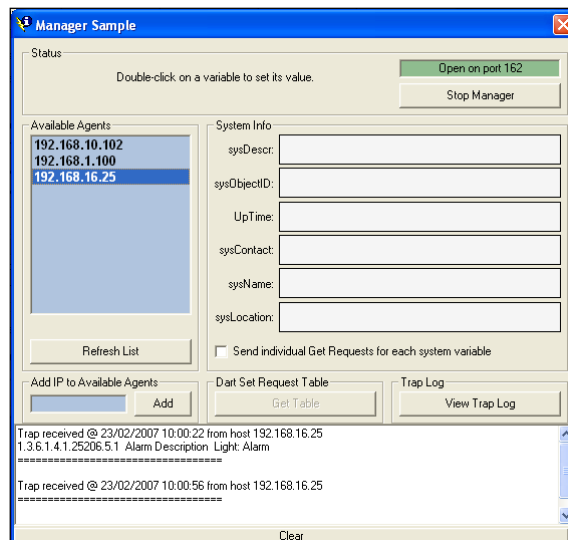
MIB **C:\Program Files\AX200\valar** **Light** **Test**

Cancel **OK**

Clicking on the advanced button will open the Com Port Advanced Setup screen where you will be able to generate SNMP messages to be sent to a SNMP manager when an alarm goes off. To activate the SNMP settings tick the check box next to the “Enable SNMP alarms”. Enter manager’s specifications including Manager’s name & the IP address on the right hand side. Agent’s information will be entered on the left. So when an alarm is generated an SNMP message is automatically sent to the manager. This message will contain the I-box ID number and IP address, Sensor ID, Alarm description, time and date. You can generate a sample SNMP message by clicking on the Test button.

In order to access the SNMP Manager Screen go to the main screen, click on the Tools menu on the top. Then go to *Enable Optional Software • SNMP Manager*. Click on “Start Manager” button on the top; the application will automatically search for the available agents on the network and list their IP addresses on the left. Click on the appropriate IP address. Once the alarm is generated the SNMP message will appear in the in the space on the bottom.

Multiple/Single Card Format



Manager Sample

Status: Double-click on a variable to set its value. **Open on port 162** **Stop Manager**

Available Agents

- 192.168.10.102
- 192.168.1.100
- 192.168.16.25

Refresh List

System Info

sysDescr:

sysObjectID:

UpTime:

sysContact:

sysName:

sysLocation:

Send individual Get Requests for each system variable

Add IP to Available Agents **Add** **Get Table** **View Trap Log**

Trap received @ 23/02/2007 10:00:22 from host 192.168.16.25
1.3.6.1.4.1.25206.5.1 Alarm Description: Light: Alarm

Trap received @ 23/02/2007 10:00:56 from host 192.168.16.25

Clear

Installation & User Guide

Multiple Formats – The AX200 software allows that each cardholder has a unique format. If selected, then a card type (this includes format and facility code) should be selected for each cardholder.

Single Format – Normally cards are of the same format and facility code. If cards of the same technology/manufacturer are used from other systems then multiple formats can be used. Single format is the default setting.

Default Access Level

This is the access level which by default is displayed in the Cardholder screen.

Default Time Zone

When adding a new card in the cardholder screen the default time zone is Always Access. You can choose a different time zone from the list to be the default or you can create a new time zone by clicking on the time zone button.

Default


Selecting this will set all the software settings back to factory default.

Third Party File

Allows you to lunch another software package like the *i-Catcher* for the CCTV.

Format & Statistics



Card Type Information	Card Matching	Card Format Analyser	Format Configuration
Card Type Information			
Card Type Name	AXXESSID FC=15		
Card Format	50 Bit AXID EM	Facility Code	15
Comments	<input type="text"/>		
 Fixed			
Total Number of Cardholders in the database 257			
This Format		Whole DB	
Total Active Cards	257	Total Destroyed Cards	0
Total Lost Cards	0	Total Inactive Cards	0
Total Stolen Cards	0	Total records of Card	0
Total Suspended Cards	0		

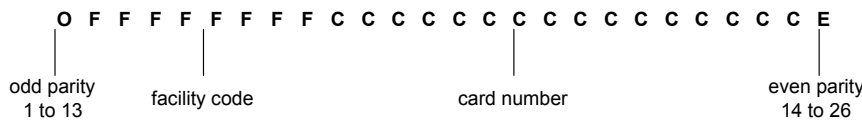
Installation & User Guide

Card Type Information

The AX200 supports up to 4,000 different card formats and facility codes. The format and facility code combined is called a card type.

Format is the number of bits programmed in a card and the location of parity checks.

E.g. 26 bits



The first and last bit check that the data received is correct.

- 8 x F indicates facility code
- 16 x C indicates card number location

The card type information tab under Formats and Statistics gives a total system overview of the number of cards and records in the system.

Details are provided per card format/facility code on:

- Total Cardholders in the database
- Total active cards
- Total lost cards
- Total stolen cards
- Total suspended cards
- Total destroyed cards
- Total inactive cards
- Total records of card 0 (cardholder details with no card issued)

Total Number of Cardholders in the database <input style="width: 50px;" type="text" value="257"/>			
	This Format	Whole DB	
Total Active Cards	<input style="width: 40px;" type="text" value="257"/>	<input style="width: 40px;" type="text" value="257"/>	Total Destroyed Cards
Total Lost Cards	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Total Inactive Cards
Total Stolen Cards	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Total records of Card 0
Total Suspended Cards	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>

Facility Code

Is a number allocated to a specific customer to avoid that card 1 would have access also on another system which uses card 1. A 26 bit format is not recommended since it allows only 256 different facility codes worldwide.

Installation & User Guide

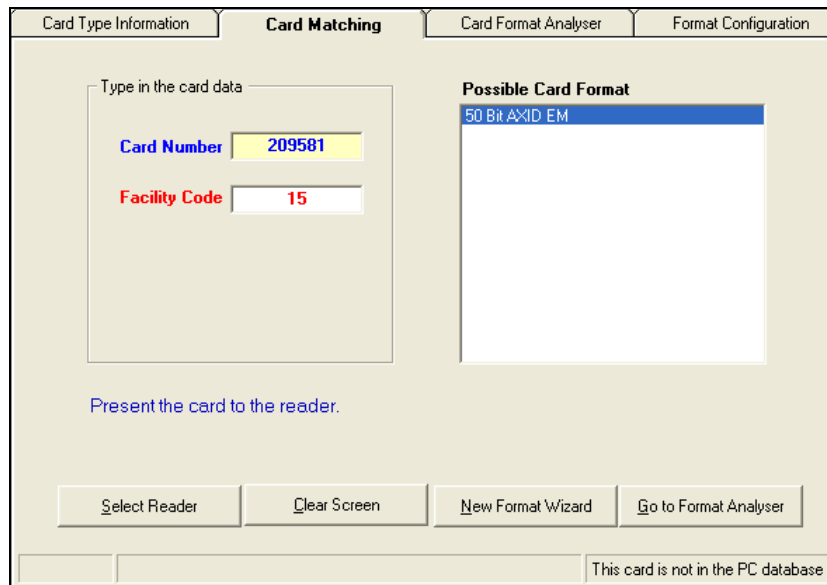
Most card manufacturers have their own specific format, providing a higher security than the 'open standard', which is not as secure.

The default facility code is 50 bit card format, providing the highest level of card number security.

Card Matching

The AX200 supports a number of well known formats. Enter the card number and if known, the facility code. Present the card to the reader (systems should be online). If known, it will display the possible format. Ensure that multiple cards from the same batch are used to verify the card format. You can then use the New Format wizard to add this to the AX200.

The card matching feature automatically identifies known formats and displays the card number and facility code. The Card format wizard allows the simple addition and quick addition of new facility codes or card formats by presenting the card to the reader. Unknown Card formats can be added using the optional Card Analyser Program or by contacting the factory.

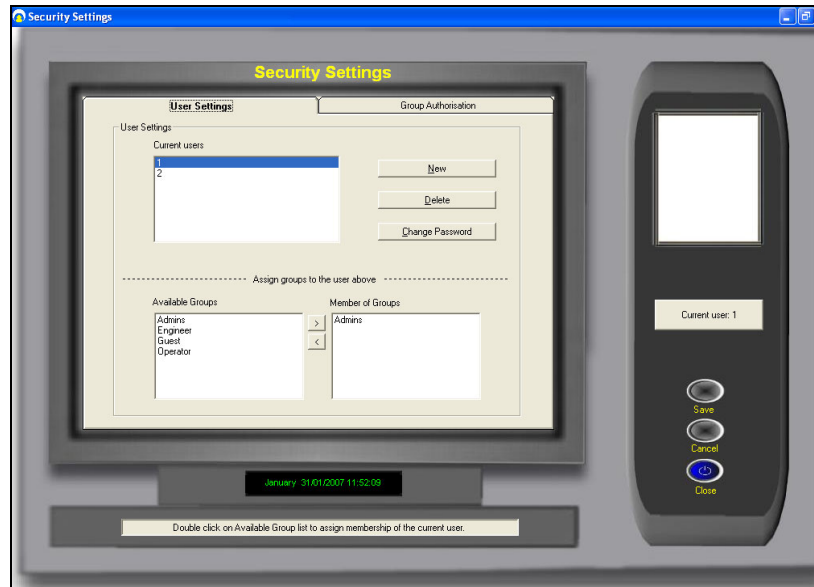


Card Format Analyzer & Format Configuration

These features are hidden and for engineering uses only. For more information please contact your manufacturer.

Security Settings

Installation & User Guide



Individual passwords can be issued to different users with different rights to view and edit. Passwords are not case sensitive. The default user 1 cannot be deleted however the password can be changed.

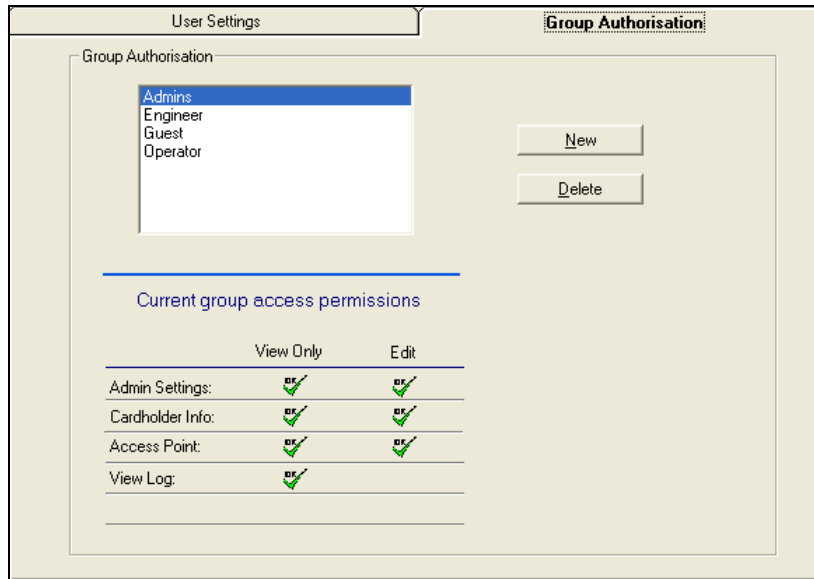
Adding a New User

To add a new user, select **New**, enter the **user name**, **password** and confirm the user **password**. You are asked to select an existing group authorisation or alternatively you can setup a new group by selecting the Group Authorisation tab. To assign a group to a user, select a group from the Available Groups list. You can double click on the group or use > button to move it across to the other list. Click save when you're finished.




Adding a New Authorisation Group


Installation & User Guide



Select the **Group Authorisation** tab, select **New**, type in the new **Group Name**.

Double click on the current group access permission symbols to enable or disable the permissions.

 Access enabled

 Access disabled

Select **save**.

Report

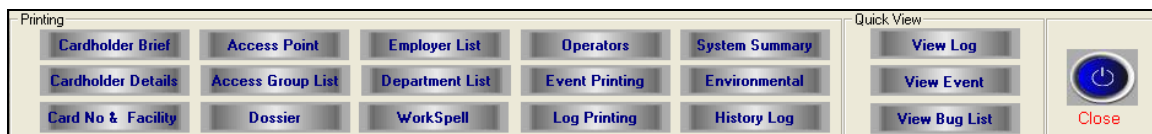
The AX series has a built in report generator which allows full or filtered information to be viewed on screen or printed. Colour printers are supported and give the benefit of alarm messages printed in red. Reports can also easily be e-mailed or exported in a large number of different formats.

Formats supported are:

Lotus mail
Microsoft Mail
Microsoft Excel
Microsoft Access

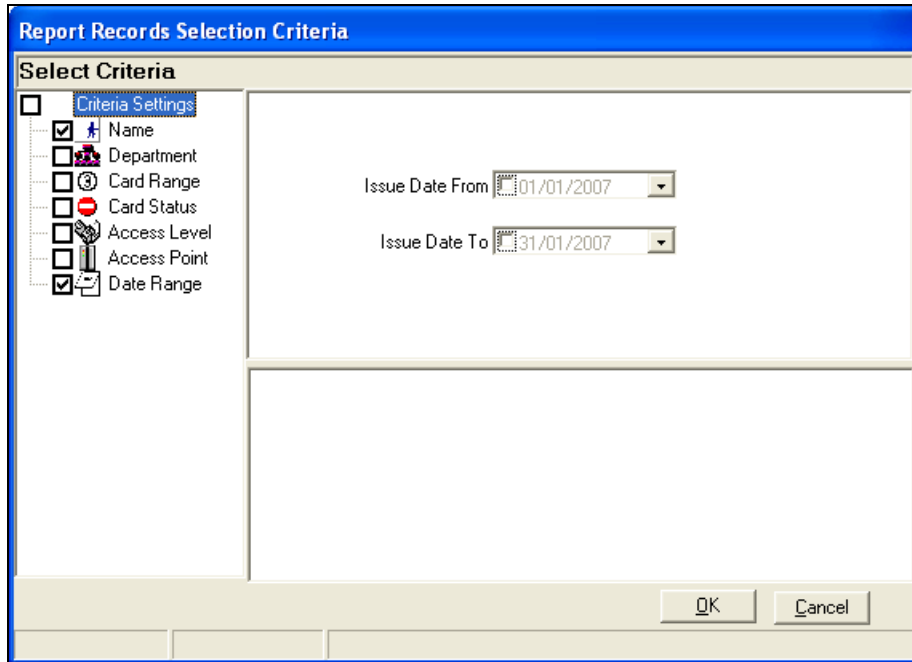
Microsoft Word
Text files
CSV files
ODBC

ASCII file
Comma delimited file
Standard reports
Rich Text Format



Installation & User Guide

Powerful reports are easily obtained entering selection criteria. The report will only include the information obtained up to the last backup.



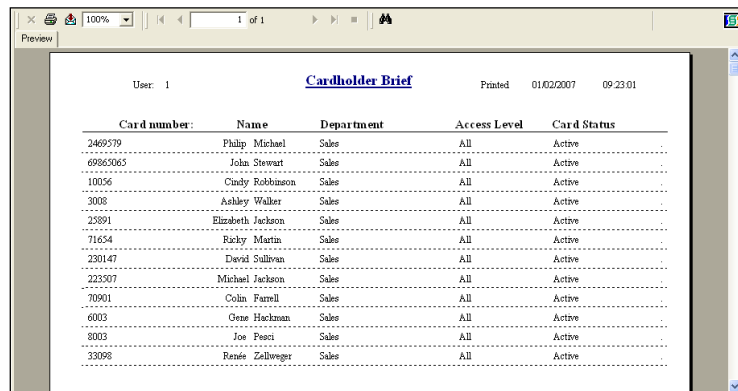
Brief Cardholder Summary
 Detailed Cardholder Summary
 Card Number & Facility Code
 Access Points
 Access Group List
 Dossier Report

Employer Details
 Department List
 WorkSpell
 Operators
 Event Printing
 Log Printing

System Summary
 Environmental
 View Log
 History Log
 View Events
 View Bug List

Cardholder Brief

Gives a brief account of the information about the cardholder including: *Card Number, Name, Department, Access Level & Card Status.*

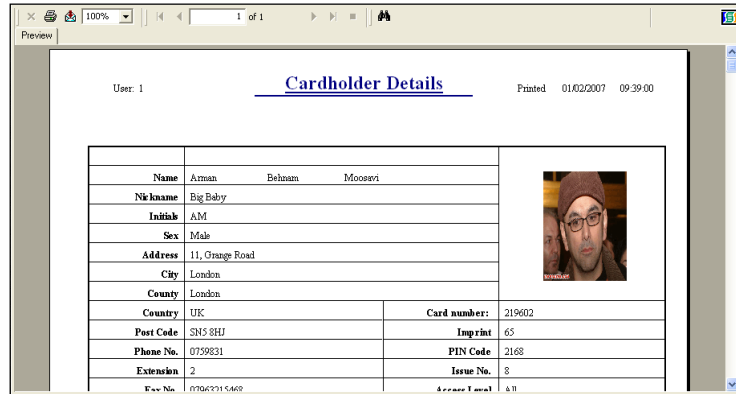


Card number:	Name	Department	Access Level	Card Status
2469379	Philip Michael	Sales	All	Active
69863065	John Stewart	Sales	All	Active
10036	Cindy Robinson	Sales	All	Active
3008	Ashley Walker	Sales	All	Active
23991	Elizabeth Jackson	Sales	All	Active
71654	Ricky Martin	Sales	All	Active
230147	David Sullivan	Sales	All	Active
223507	Michael Jackson	Sales	All	Active
70901	Colin Farrell	Sales	All	Active
6003	Greg Hackman	Sales	All	Active
3003	Joe Pesci	Sales	All	Active
33098	Rende Zaldwegger	Sales	All	Active

Installation & User Guide

Cardholder Details

Displays all the information in the cardholder screen in details along with the picture of the card holder.



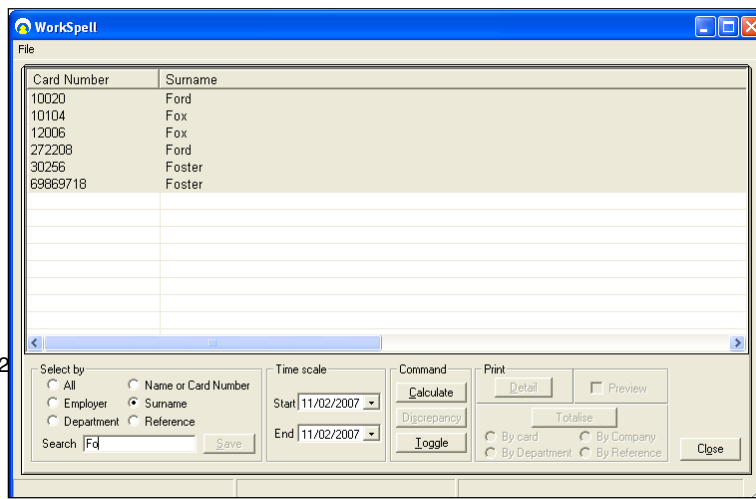
Log File

All the system transactions from the online controllers are stored, including all operator actions. Cardholder, system changes and operator commands are all stored in the log file with date, time and the type of transaction. eg 12:00 05/12/2002 card 52 added. The log file can be viewed or printed using selection criteria e.g. from / to date, cardholder, department Etc.

LogID	UserID	Date/Time	Object	Action	Type
572	1	01/02/2007 10:24:15	Arman Moosavi	Access granted.	Transact
571	1	01/02/2007 10:24:11	Access Point 3	On Line	Transact
570	1	01/02/2007 10:24:04	Arman Moosavi	Access granted.	Transact
569	1	01/02/2007 10:23:59	Access Point 3	Reader is present.	Transact
568	1	01/02/2007 10:23:59	Arman Moosavi	Access granted.	Transact
567	1	01/02/2007 10:23:56	Controller. Acce...	Automatic download finished.	Download
566	1	01/02/2007 10:23:49	Controller. Acce...	Start automatic download.	Download
565	1	01/02/2007 10:23:36	Access Point 3	On Line	Transact
564	1	01/02/2007 10:23:13	Arman Moosavi	Invalid card. Access denied.	Transact
563	1	01/02/2007 10:23:10	Arman Moosavi	Invalid card. Access denied.	Transact
562	1	01/02/2007 10:23:00	Arman Moosavi	Invalid card. Access denied.	Transact
561	1	01/02/2007 10:22:58	Arman Moosavi	Invalid card. Access denied.	Transact
560	1	01/02/2007 10:22:28	Arman Moosavi	Access granted.	Transact
559	1	01/02/2007 10:22:26	Arman Moosavi	Invalid card. Access denied.	Transact
558	1	01/02/2007 10:21:33	Controller. Acce...	Automatic download finished.	Download
557	1	01/02/2007 10:21:21	Controller. Acce...	Start automatic download.	Download
556	1	01/02/2007 10:21:20	Controller. Acce...	Automatic download finished.	Download
555	1	01/02/2007 10:21:07	Controller. Acce...	Start automatic download.	Download
554	1	01/02/2007 10:21:02	Cardholder. Arm...	Card No: 228396. Record has been modified.	DB Modi
553	1	01/02/2007 10:20:33	Unknown	Invalid card. Access denied.	Transact
552	1	01/02/2007 10:20:28	Unknown	Invalid card. Access denied.	Transact
551	1	01/02/2007 10:20:24	Unknown	Invalid card. Access denied.	Transact
550	1	01/02/2007 10:20:22	Unknown	Invalid card. Access denied.	Transact
549	1	01/02/2007 10:20:17	Access Point 3	Reader is present.	Transact
548	1	01/02/2007 10:20:17	Unknown	Invalid card. Access denied.	Transact
547	1	01/02/2007 10:20:17	Access Point 3	Off Line	Transact

Dossier

Gives a brief description of the people working in the same department. This information includes name, department, job title, employer and contact details along with photo display for each person.



Installation & User Guide

Work Spell

An exclusive feature in the AX200 application gives you the possibility to calculate the total number of hours which an individual or a group of cardholders have spent inside the building. You can search a cardholder by their name or card number and workout the number of hours they have spent in the building, during a specific period of time. Alternatively you can carry out this calculation for the people working in the same department or under the same employment. Select the appropriate criteria from the options on the left. Type the correct name in the search field. Select the correct record from the list and press save. Now specify the correct time period and press calculate. The result will appear on the list providing the cardholder's name, card number, start time, end time, duration, employer, department and

Card No.	First Name	Surname	Start Time	End Time	Duration
69860535	Robert	Jones	12/02/2007 16:38:01	12/02/2007 19:38:23	03:00:22

If you're running the report for more than one person or a cardholder who's been booked in & out more than once; you can sum up the total number of hours they have been present by pressing **Totalise**. You will have the option of totalising by card, company, department or by reference. This list can be printed out or exported in a number of different formats. **Discrepancy** tells you when the cardholder has been booked in/out.

Operators

Presents a list of the users allowed to use the application. To add a new user, go to *Security • User Settings*.

Environmental

You can run detailed reports on the i-Box activities. These reports can be filtered by i-Box name & ID, Location, Sensor Type, Name & ID, Transaction type and Time range.

System Summary

System summary prints out the Site Information, Installer Information, System Settings, List of Card Types, Access Point and the list of Operators.

Quick View

This feature enables immediate retrieval of the last events for quick viewing. The event and log files are cleared after each backup however can be viewed using history event or history log.



Installation & User Guide

Printing

This will provide a selection of reports, all the data is sorted on the screen. To print, select the print icon or select the envelope icon to export the data from the report.

Reports can be exported to a number of spreadsheet and word processor formats as well as ODBC and common data interchange formats. This makes the distribution of information easier. The export process requires you to specify a format and a destination. The format determines the file type and the destination determines where the file is located.

Format Types

- Character-separated values
- Comma-separated values (CSV)
- Crystal Reports (RPT)
- Crystal Reports 7 (RPT)
- Data Interchange Format (DIF)
- Microsoft® Excel
- Lotus® 1-2-3
- ODBC
- Paginated Text
- Record style (columns of values)
- Report Definition
- Rich Text Format
- Tab-separated text
- Tab-separated values
- Text
- Word for Windows

In addition to the standard export format types installed on your PC, you may find additional export format types are available to you. These are determined by the DLL files on your PC.

Note: - When you export a report to a file format other than Crystal Reports format (RPT), you may lose some or all of the formatting that appears in your report. However, the program attempts to preserve as much formatting as the export format allows.

Note: Transaction date and times are issued by the PC. Events are not stored in the AX200.

Destination

The destination determines the export location of your report.

- Application
- Disk File
- Microsoft® Exchange folder
- Lotus® Domino
- Microsoft Mail™ (MAPI)

Installation & User Guide

All operation commands/database or system changes are stored and can be previewed in Reports.

i - BOX

A new product introduced along with the AX200 software; i-BOX provides both access control security and environmental monitoring. Each i-BOX includes a built in temperature, humidity, light and voltage sensor with 14 ports for plug and play connections of additional smart sensors, together with 2 access control ports.



When presenting a card to a reader connected to the i-BOX, the transaction will be recorded, providing a date and time stamp. Detailed reports of all the transactions can be filtered by single or a group of doors, employee name, company or department, individual date or date range. These reports can be printed or exported into a database or spreadsheet for analysis. Just go to *Reports • Environment* and select the appropriate criteria.

In addition to the Light/Voltage & Temperature/Humidity sensors placed inside the i-BOX during manufacturing; there are 16 different types of plug & play smart sensors which can be plug into one of the 14 ports on the back of the i-BOX. Each sensor can be programmed to take readings as frequent as 1 every second. Maximum and minimum values could be set for every sensor and once the reading exceeds the limits an alarm transaction will be generated and displayed on the main screen, providing the time, date, type of the alarm, i-BOX and the sensor's name. Accurate reports of all the readings taken by all the sensors could be obtained in *Reports • Environment*. These reports can be filtered by a single or a group of locations, sensor's type, name & ID and i-box Name & ID.

The following table contains the list of all the plug & play smart sensors supplied by Axxess Identification.

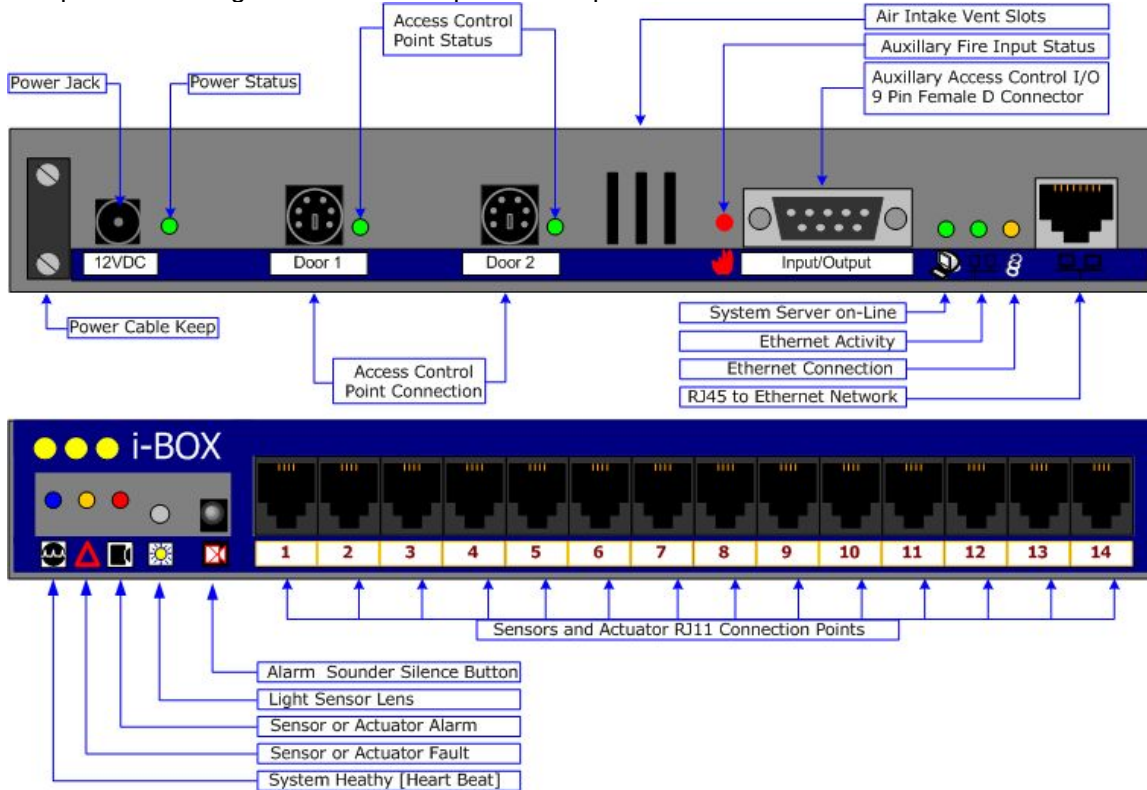
Door Panel Position Sensor	Detects the position of side panels and doors
Vibration / Shock Sensor	Detects Vibrations from intrusion attempts
Temperature Sensor	Standard temperature sensor range -20C to +80C
Temperature & Humidity Sensor	High accuracy temperature, condensation and humidity sensor
Temperature & Door Contact Sensor	Combined standard temperature and door position sensor
Mains Present Monitoring Sensor	Monitors the availability of mains power
Hot Spot Temperature Sensor	Early warning temperature sensing of equipment
High Level & Door Contact Sensor	Combined light level and door position sensor
Flood Sensor	Flood sensor with 5 meters of water sensing cable
Smoke & Temperature Detector	Combined optical smoke and temperature detector
Intrusion / Movement PIR	Detection of people for intrusion or presence
Sounder / Beacon Module	Combined sounder and beacon for audio and visual warning
Fan Fail Sensor	Fixed temperature alarm for temperature and fan fail sensor
Inputs / Output Module	Two general purpose inputs and 1 relay output module
General Input Module	Two volt-free general purpose input module

Installation & User Guide

Dust Particle Sensor

Monitors the concentration of dust particles in the air flow

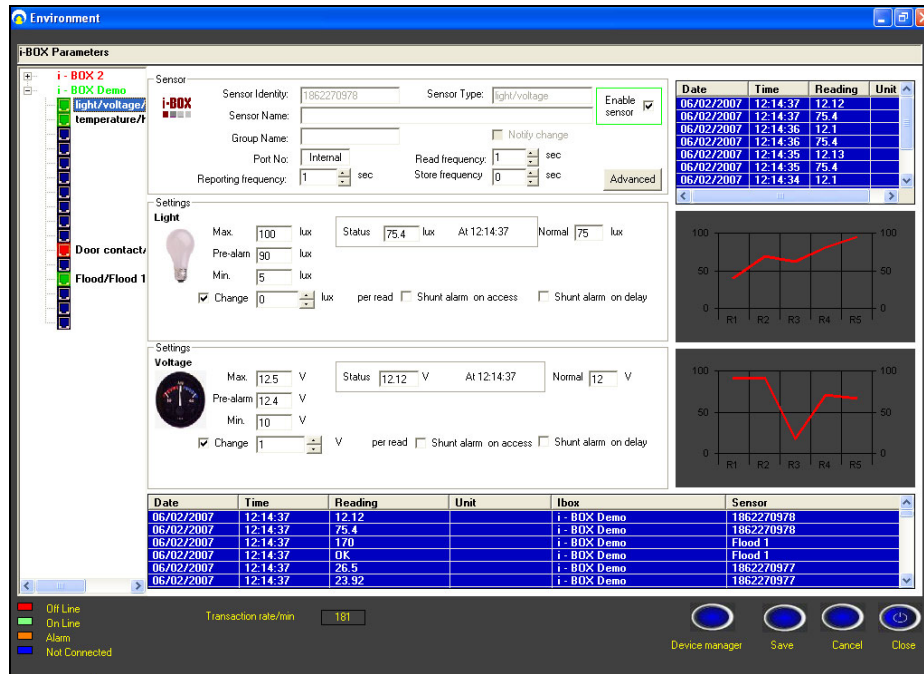
The picture below gives a brief description of the ports and LEDs on the i-BOX.



Environment

An essential part of the AX200 software which is exclusive to the i-BOX. Environment screen contains settings and configurations for the i-BOX activities.

Installation & User Guide



i-BOX Parameters

The diagram on the left shows all the i-box units configured on your PC. On-line units are displayed in green. Clicking on + will display all the sensors connected to that i-box. Other than the first two sensors which are already in the i-box, there are 14 empty ports for smart sensors to be plugged in. Once a new sensor is plugged in, a new device wizard will be opened and you can easily configure your sensor. Once a sensor is highlighted on the diagram, all the sensor settings will be displayed on the screen.

The blue list on the bottom of the screen displays all the readings taken by all the online sensors.

Sensor Settings

Sensor

i-BOX

Sensor Identity: Sensor Type: Enable sensor

Sensor Name:

Group Name: Notify change

Port No: Read frequency: sec

Reporting frequency: sec Store frequency: sec Advanced

Sensor's specifications are displayed on the top of the page. **Sensor Identity** and **Sensor Type** are automatically detected by the application once the sensor is connected to the i-box. These values cannot be changed.

Note: the Serial Number of the sensor is not shown on this page however it is displayed on the new device wizard once you plug in the sensor for the first time.

Installation & User Guide

Sensor Name is specified by the user and can be changed at any time.

Port No displays the number of the port which the sensor is connected to (1•14). In the case of a built-in sensor like Temperature/ Humidity, it shows *Internal*.

To **enable a sensor** tick the check box and click the save button on the bottom of the page. Once the sensor is enabled it will start taking readings.

Read frequency specifies how often you want the sensor to take a reading. This number is in seconds and could be in the range of 1 • 255.

Date	Time	Reading	Unit
06/02/2007	12:14:37	12.12	
06/02/2007	12:14:37	75.4	
06/02/2007	12:14:36	12.1	
06/02/2007	12:14:36	75.4	
06/02/2007	12:14:35	12.13	
06/02/2007	12:14:35	75.4	
06/02/2007	12:14:34	12.1	

Reporting frequency tells you how often the reading is displayed on the screen. The blue list on the right hand side shows all the readings taken by the current sensor.


Store frequency is how often the reading is stored in the i-box. This option is only applicable for certain types of sensor.

Advanced settings include more information on sensor’s name and identity, hardware and the firmware version. It also includes the calibration settings for the sensor. Do not attempt to change these settings if you’re not sure as this will affect the performance of the sensor.

Alarms

Settings

Light



Max. 100 lux

Pre-alarm 90 lux

Min. 5 lux

Change 0 lux per read

Status 111.51 lux At 09:32:40

Normal lux

Shunt alarm on access

Shunt alarm on delay

Any sensor could be given a maximum and minimum reading value. Once the current reading exceeds those limits, it will generate an alarm. In the case of High/Low limit alarms the Max/Min fields will become amber. In the case of the pre-alarm they become yellow. Simultaneously, an alarm transaction will appear on the main screen providing the sensor’s type, alarm description, i-BOX name and sensor ID. An “Alarm cleared” transaction will follow once the current reading falls back within the limits.

```

09:41:29 light : pre-alarm . i-BOX : 200 -16 Sensor : 1862270978
09:41:52 light : high limit alarm . i-BOX : 200 -16 Sensor : 1862270978
09:42:53 light : high limit alarm cleared . i-BOX : 200 -16 Sensor : 1862270978
```

You can also program a sensor to generate an alarm once the reading changes considerably. Once you’ve ticked the check box you can specify the magnitude of this change in the “**Change**” field.

Shunt alarm on access

Installation & User Guide

When a door is opened there might be a dramatic change in the sensor readings (especially temperature and light sensors), which may result in generating a false alarm. By enabling this feature the application will ignore the alarm generated by that sensor once the door has been opened.

Shunt alarm on delay

In the same way, when the door is closed the reading will go back to its original status quickly which may cause in generating an alarm. To avoid this; once you have activated this feature, you can specify the **shunt delay time** in the i-BOX settings. To view these settings just click on the i-box name. As the result, when the door is closed, any generated alarm would be ignored until the delay time is over.

i- BOX Settings

More information on the i-box such as i-BOX identity, firmware version or the serial number could be obtained by clicking on the i-box name (on the diagram on the left).

Host Online Timeout

Is the number of seconds after which the I-box assumes that the PC is offline when it does not receive a response for the link-alive. So during this time if the I-box does not receive any response for link alive the software will report "*PC off line*"!

Force time Update

Specifies the amount of time before the clock on I-box is synchronized with the PCs clock!

Alarm Strobe Period

Indicates how long the strobe light will flash once the alarm goes off. (Triggered by Pin 9 on the 9 way connector on the i-BOX [Ref. page 12])

Handshake Period

Determines the period of the initial interaction when two units on the network start communicating with each other.

Shunt Delay

The period of time during which any alarms generated by the sensors connected to this i-box would be ignored after the door is closed. (Shunt alarm on delay needs to be enabled)

Alarm Sounder Period

The amount of time that the sounder is activated when the alarm is generated. (Triggered by Pin 4 on the 9 way connector on the i-BOX [Ref. page 12])

Minimum & Maximum Timeout

Installation & User Guide

The default maximum value is 5 seconds. This means, when the I-box sends a transaction to the PC it will wait for a response from the PC. If it does not receive any response it will wait for 5 seconds before sending another message. This number is doubled with every try, until it reaches 80 seconds (Minimum Timeout).

Accumulation Period

Number of seconds that the transactions will be accumulated in the transaction queue in the I-box before they are sent (applicable in case of block transaction: max 15 transactions can be in a block). If it is set to 2 sec then all the transactions accumulated during 2 sec will be sent. It's the delay period of block transaction but if the queue is already filled with 15 transactions it is sent anyway.

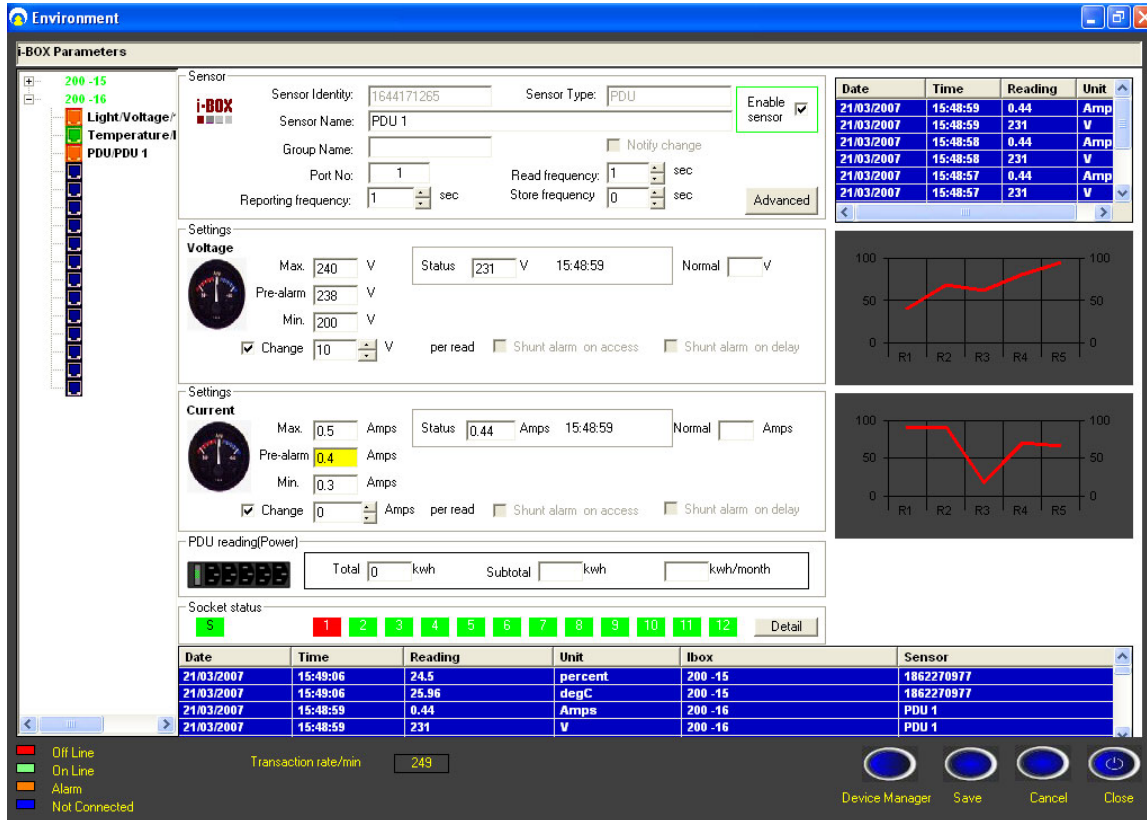
i-BOX					
IBOX Identity:	1342181391	Batch-Serial no:	1	15	
IBOX Name:	200-16				
Firmware Version:	1.6	Hardware Version:	1		
Application Version:	1	Location:	location 1		
Host Online Timeout:	20	sec	Handshake Period:	5	sec
Force time update:	300	sec	Shunt Delay:	15	sec
Alarm Strobe Period:	0	sec	Alarm Sounder Period:	0	sec
Transaction Reporting					
Minimum Timeout:	5	sec	Maximum Timeout:	80	sec
Accumulation Period:	10	sec			
Advance					
Settings					
IP Address:	192.168.16.16	MAC Address:	0090C2C9B359		
Submask:	255.255.255.0	Gateway:	0.0.0.0		
AX100(1):	2400119A	AX100(2):			

The bottom part of the page contains some information about the network settings on the i-box such as the IP address, MAC Address and... it also displays the access identity of the readers connected to the access control ports on the back of the i-box.

PDU (Power Distribution Unit)

The Power Distribution Units (PDU) are part of the family of plug & play sensors manufactured by Axxess Identification; representing a streamlined and more efficient use of power delivery into the rack environment.

Installation & User Guide



High and low limits could be defined for both voltage and current. Once the reading exceeds these limits it will trigger an alarm and the appropriate transaction will appear on the main screen, providing the sensor's type, alarm description, i-BOX name and sensor ID.

Details

The status of the sockets is displayed on the left hand side. Each status has a unique colour. Colour green means that the socket is switched on and colour red indicates that the socket is switched off. If there is a fuse failure in any of the sockets, it will be displayed in amber and the appropriate transaction will appear in the main screen. There is a space in front of every socket to enter a brief description of the equipment connected to that particular socket.

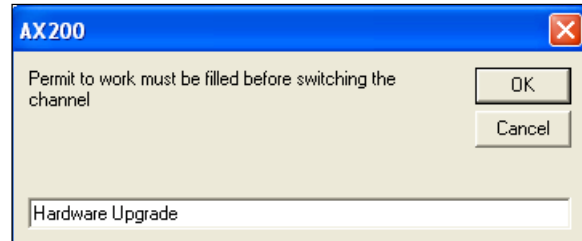
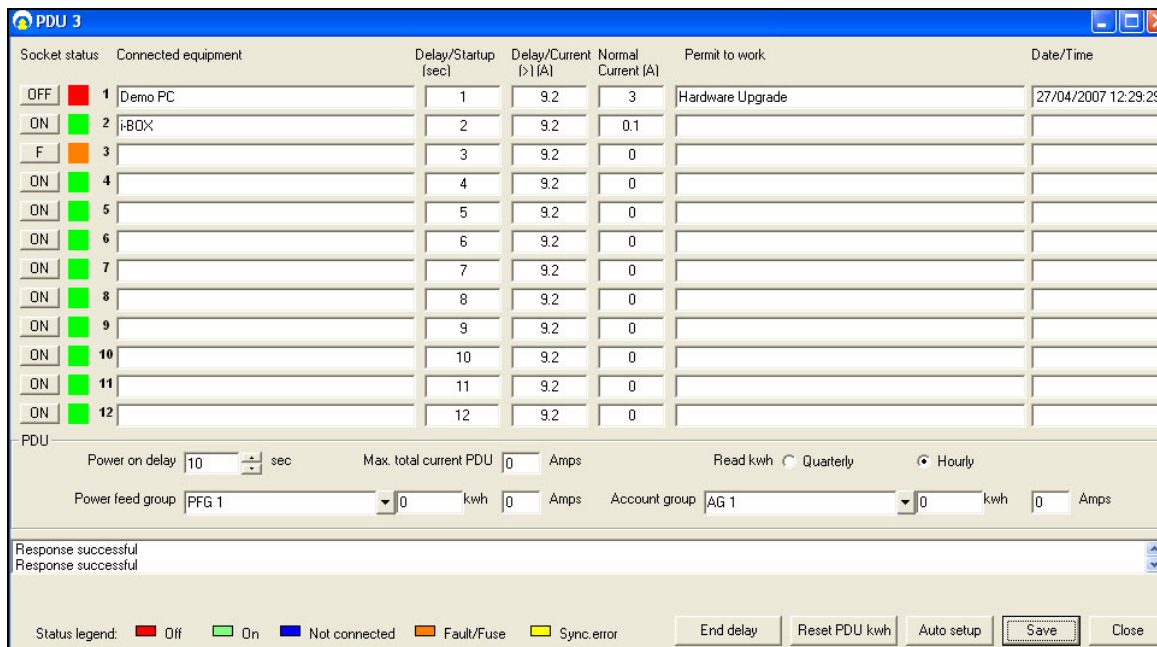
The **Delay Start-up** column includes the number of seconds before a socket is activated when the PDU is switched on. If the input value is zero, the socket will not be switched on. (Range: 0s • 255s)

The **Delay/Current** column indicates the upper limit of the current in the unit before a particular socket is switched on. For example if the input value for a particular socket is 5, it will not be switched on until the current in the unit has dropped down to 5 amps or less. If there is a mismatch between the database and the PDU settings, these fields become yellow. All you need to do is to press the save button to synchronize the database.

Installation & User Guide

Normal Current: shows the normal amount of current consumed by each device. This value is determined by the user and is merely for user's information and has no effect on the operation of the PDU.

Permit to work & Date/Time: the last two columns are for entering a brief explanation in case of a socket being switched of by the user. To switch off a socket remotely click on the ON/OFF buttons on the left hand side. Once you click on the ON/OFF button a separate window will be opened asking you to enter the "Permit to work".

Socket status	Connected equipment	Delay/Startup (sec)	Delay/Current (>1[A])	Normal Current (A)	Permit to work	Date/Time
OFF	1 Demo PC	1	9.2	3	Hardware Upgrade	27/04/2007 12:29:29
ON	2 i-BOX	2	9.2	0.1		
F	3	3	9.2	0		
ON	4	4	9.2	0		
ON	5	5	9.2	0		
ON	6	6	9.2	0		
ON	7	7	9.2	0		
ON	8	8	9.2	0		
ON	9	9	9.2	0		
ON	10	10	9.2	0		
ON	11	11	9.2	0		
ON	12	12	9.2	0		

PDU

Power on delay sec Max. total current PDU Amps Read kwh Quarterly Hourly

Power feed group kwh Amps Account group kwh Amps

Response successful
Response successful

Status legend: ■ Off ■ On ■ Not connected ■ Fault/Fuse ■ Sync.error

Power on delay is the amount of time before any of the PDU sockets becomes activated. Please note that once the unit is switched on, this delay time is applied before the delay time set for individual sockets. For instance if the overall delay is 10 seconds and the delay time for the first socket is 1 second; once the unit is switched on it will take the first socket 11 seconds to be activated. To set the overall delay enter the appropriate number of seconds in the field, and press save.

Power feed group

The units connected to the same power line could be classified into a separate feed group. To create a new feed group enter an appropriate name inside the *Power feed group* field and press save. When you add the next PDU, you can select the feed group that you have just created and the new unit will be assigned to that group.

There is also a way to categorize the units that are being fed through different power lines. In this case you need to create an Account group which can contain the units that are not connected to the same power line.

Installation & User Guide

Pressing the **End delay** button will terminate any delay time and all the sockets in the unit will be switched on. **Reset Power** button will bring the value of total power back to zero.

Voltage, current and the power readings are displayed on the LCD screen on the PDU. If you press button No.4 you'll be able to view the *Serial Number*. Button No. 5 will display the channel status for all the sockets. The status of each channel is reported in the following way:

- 0** Switched Off
- 1** Switched On
- F** Fuse Fault
- *** Mains present on the output but the relay is off.

Button No.6 displays the Hardware and the Firmware version inside the unit. In order to reset the PDU to its default settings press and hold buttons 1, 3, 4 and 6. After resetting the unit, the time interval between the sockets being switched on (in the start-up sequence) increases to 3 seconds.

States to be indicated on PDU relay LED:

1. **Normal:** *Power switched on, power sensed* – **LED on solid**
2. **Fault Feedback:** *Power switched off, power sensed* – **0.5 sec on/off flash for 3 seconds, off 2 seconds**
3. **Fuse Fault:** *Power switched on, power not sensed* – **80 ms seconds on/off flash**
4. **Socket Off:** *Power switched off, power not sensed* – **LED off.**

Installation & User Guide

redetec® Sensor

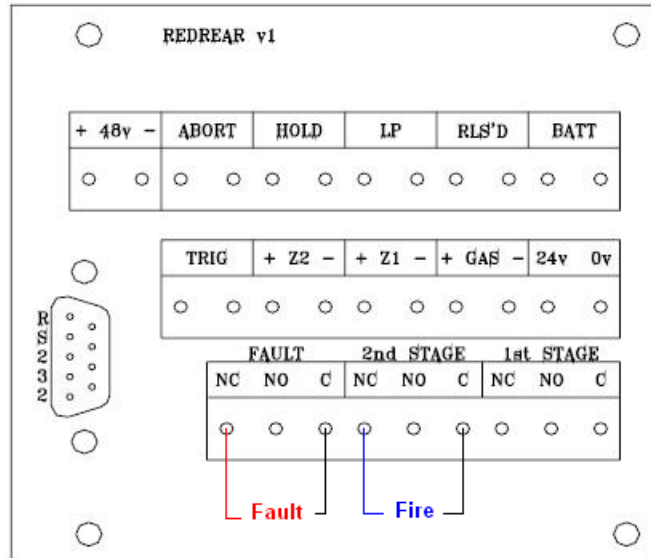
Redetec sensors are Input/output modules specifically designed to be used with Redetec units to provide the ultimate cabinet protection. Redetec is a self-contained automatic fire extinguishing unit, which can be used in many industry sectors.

Like all the other plug & play smart sensors, redetect sensor is connected to the I-box using a standard sensor cable only. The unit takes 2 inputs, **Faults & Fire**. The output signal is the **Isolate** command which puts the extinguishing circuit in complete isolation. This disables the extinguishing section for maintenance purposes.

Hardware Connection Details

Fault and fire inputs are taken from one of the external connector blocks located at the rear of the Redetec unit. Both of these connections are normally closed. The opposite diagram illustrates the external connections between the rear connecting block and the Redetec sensor.

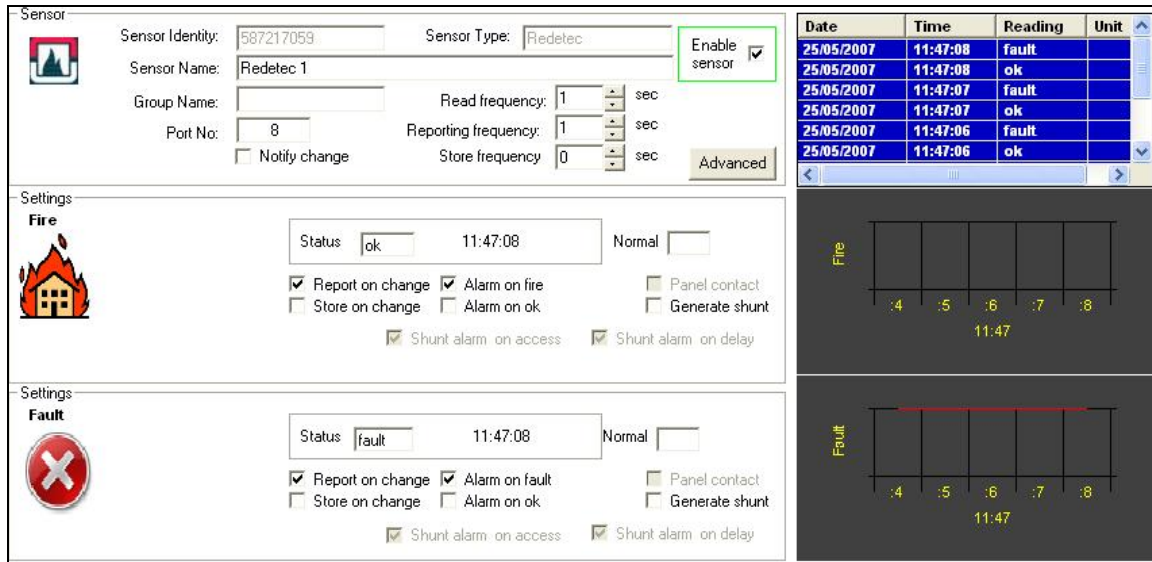
The output relay on the sensor should be connected to the key switch located in front of the Redetec unit. There are six wires connected to the key switch 5 of which are connected to the main processor card located at the front. These connections are in 2 separate rows. Looking from the top, from the 3 wires that are closer to the main processor card, the bottom 2 (Black & Blue) are the ones that need to be connected to the output relay on the Redetec sensor. Please note that there are 2 blue wires connected to the key switch; one of which is connected to the relay card on the side. *The connection should be made between the blue wire going to the main processor card and the out put relay on the sensor.*



Sensor Settings

Once you've plugged the sensor into the I-box a new device wizard will appear and the sensor will automatically be added to the database. To view the sensor settings go to the environment screen, click on the appropriate I-box and select the Redetec sensor.

Installation & User Guide



Date	Time	Reading	Unit
25/05/2007	11:47:08	fault	
25/05/2007	11:47:08	ok	
25/05/2007	11:47:07	fault	
25/05/2007	11:47:07	ok	
25/05/2007	11:47:06	fault	
25/05/2007	11:47:06	ok	

Sensor’s specifications are displayed at the top of the screen. You could specify how frequent you would like the sensor to take readings and how often you’d like the readings to be reported. All the reported and unreported data will be stored in the log file and can be accessed via the report section.

If the Alarm on Fault/Fire is ticked, once there is a fire or fault in the unit, an alarm transaction will be generated and displayed on the main screen. This message will include the I-box and the sensor’s name + type and the time of the alarm. The AX200 software now has the ability to send these alarm messages along with all the necessary information via email.

12:18:06 Fault: fault alarm i-BOX : 200 -10 Sensor : Redetec 3

Isolate

In order to switch on the isolate, click on the advanced button. The output settings are located on the bottom of the screen. The software will ask you to enter a brief explanation called “permit to work” before switching on the isolate. The software reports the isolate state by showing a flashing icon below the controller buttons on the main screen.



Please note that the Isolate is considered an alarm condition so as long as the unit is in isolate the sensor’s symbol in the environment screen will remain amber, even if all the other alarms have been cleared!

Once you switch on the isolate the isolate light on the Redetec unit comes on. Please note that the isolate command from the software overrides the position of the keys switch.

Installation & User Guide

Note: if the Redetec sensor goes off line for any reason, it will lose control over the Redetec unit. This means if the unit has been isolated by the sensor, it will come out of isolate once the sensor is disconnected. *Therefore we strongly recommend using the key switch for isolation before starting any maintenance work.*

PIR

PIR sensors have been designed to detect movements in an adjustable range of 5 to 15 meters.

PIR sensor is connected directly into one of the free ports on the back of the i-BOX using the standard sensor cable only. Once the sensor is connected to the i-BOX a New Device Wizard will appear on the screen. Follow the on-screen prompts to add the new sensor to the database. To access the settings for the PIR sensors go to the environment section, select the appropriate i-BOX from the tree menu on the left hand side and select the PIR sensor.

Once the sensor has been programmed to trigger the alarm on movement, an alarm transaction will appear on the main screen when the movement is detected. This transaction will include the I-box name, sensor type and the type of the alarm.



15:11:41 PIR:movement alarm i-BOX : 200-3 Sensor : PIR 1

All the readings from the PIR sensor could be accessed through the *Reports* section.

Sensor

Sensor Identity: 1610616928 Sensor Type: PIR Enable sensor

Sensor Name: PIR 1

Group Name: Read frequency: 1 sec

Port No: 8 Reporting frequency: 1 sec

Notify change Store frequency: 0 sec Advanced

Settings

PIR

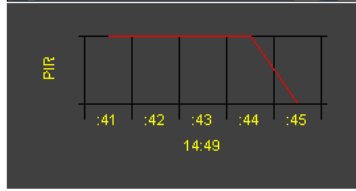
Status: Alarm 14:49:45 Normal

Report on change Alarm on ok Panel contact

Store on change Alarm on movement Generate shunt

Shunt alarm on access Shunt alarm on delay

Date	Time	Reading	Unit
16/07/2007	14:49:45	Alarm	
16/07/2007	14:49:44	OK	
16/07/2007	14:49:43	OK	
16/07/2007	14:49:42	OK	
16/07/2007	14:49:41	OK	
16/07/2007	14:49:40	OK	



The three LEDs on the PIR sensor are colour coded as follows:

- PIR Detection: Green/Blue Flash**
- Microwave Detection = Orange**
- Alarm = Red**
- No Movement = Blue (Steady on with short flash)**
- No Communication = Blue (Fast Flash)**

Note: To avoid any potential false alarms:

- ✓ Make sure the sensor is not under direct sunlight.
- ✓ Do not mount detectors near heaters.
- ✓ Open windows may induce false alarms caused by draughts and moving objects.

Installation & User Guide

INSTALLATION

- Remove case lid by unscrewing fixing screw **B1**, and remove the PCB.
(Do not touch Pyro sensor **D4**.)
 - Choose suitable wall fixing holes. **B1**
 - Mark wall for fixing positions (Do not route wires near mains cabling, avoid vibrating surfaces, and only use solid wall).
 - Drill fixing holes.
 - Fix case to wall. **B2**
 - Replace PCB (Do not touch Pyro sensor **D4**).
 - Rotate microwave adjustment to select the required range and if required adjust the PIR range as illustrated in **A2**.
 - Refit lid to case and fasten.
- Final Steps**
- Apply power and wait 2 to 3 minutes for the detector to stabilise
 - Replace cover and walk test the detector to verify the sensitivity and check that alarms are indicated at the control panel.
 - The three LEDs are colour coded as follows:
PIR detection = Green
Microwave detection = Orange
Alarm = Red
 - If LEDs are to be disabled remove the test link header. **D2**
It is recommended that the LEDs are disabled after installation to prevent potential intruders from walk testing the system.

POTENTIAL FALSE ALARM HAZARDS

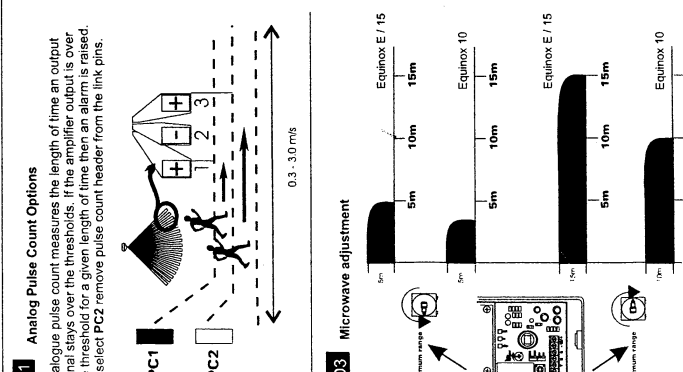
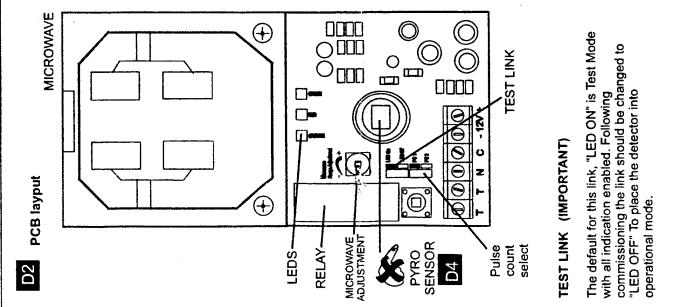
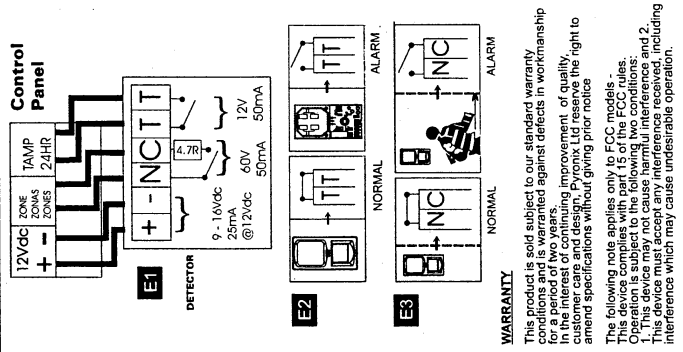
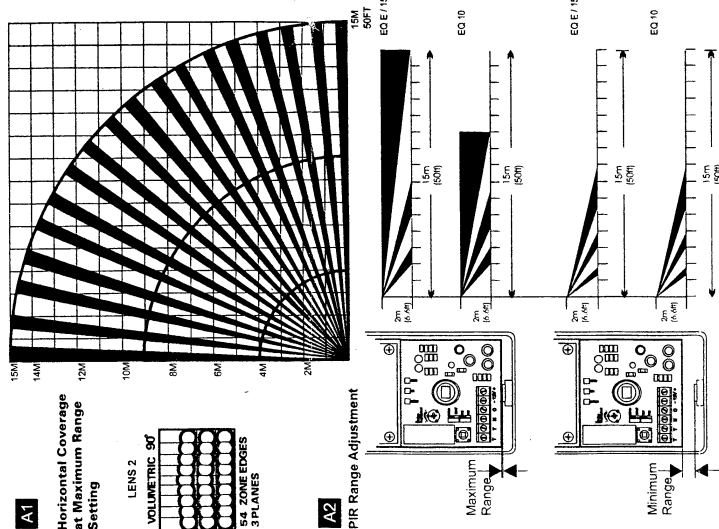
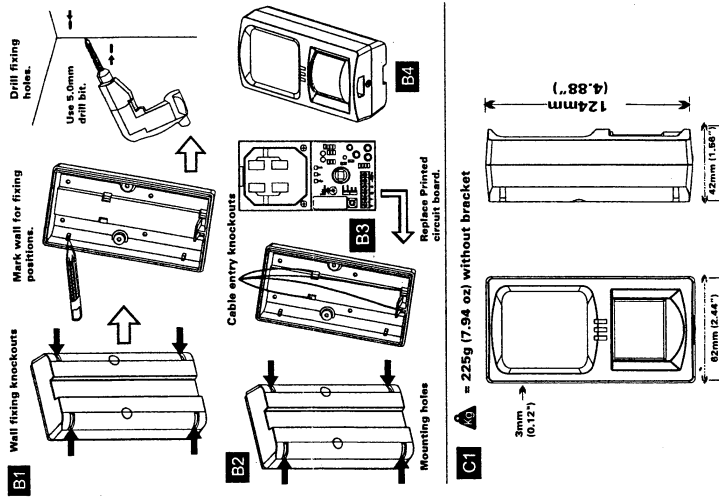
- Direct sun light on detector may cause a PIR to activate.
- False Alarms may be caused by pets and animals.
- Do not mount detectors near heaters.
- Open windows may induce false alarms caused by draughts and moving objects.

DIAGRAMS

- A1** Horizontal coverage pattern
 - A2** PIR range adjustment
 - B1** Wall fixing knockouts
 - B2** Mounting holes
 - B3** Cable entry knockouts
 - B4** Case lid screw fitting
 - C1** Measurements and weight
 - D1** Analog pulse count options
 - D2** PCB Layout
 - D3** Microwave range adjustment
 - D4** Pyro sensor
 - E1** Wiring to control panel
 - E2** Tamper operation
 - E3** Relay contacts
- Normal = No movement
Alarm = Cover open

SPECIFICATIONS (QUICK REFERENCE)

Model:	Equinox 10 - 15 and E
Colour:	White
Casing:	3mm ABS, 0.4 mm HDPE in lens area
Detection method:	PIR = Dual element Pyroelectric sensor FET oscillator with 16m patch antennas
Detection Zones:	Lens 2, 54 zone edges
Detection speed:	0.3 - 3m/s
Operating Voltage:	9 to 16 volts DC (12V nominal)
Quiescent Current:	25 mA at 12V
Alarm Current:	Alarm LEDs enabled = 45mA at 12V Alarm LEDs Disabled = 15mA at 12V
Relay Output:	100V, 75mA maximum, normally closed voltage free at 2.7 Ohm, series resistor.
Mounting Height:	1.8 to 2.4m (6 to 8 ft)
Tamper Switch:	Normally closed voltage free contacts
Storage Temp:	-40°C to 60°C, 14" to 140" F
Operating Temp:	-30°C to 60°C, 14" to 140" F
Emissions:	EN55022 class B
Immunity:	To new European standard EN50130-4



Installation & User Guide

Dust Particle Sensor

Dust sensor has been designed to detect the level of dust particles in the air. The air is sucked in through the air inlet on the side and released through the outlet on the top. Once the air comes in contact with the sensor the level of dust particles is measured and reported through the software.

Please note that the dust sensor must be fitted sideways and the air inlet and outlet should not be blocked.



Dust sensor is directly connected to the i-BOX through one of the 14 ports on the back using a standard sensor cable. Once the sensor is detected by the i-BOX, a new device wizard will appear on the screen. Follow the on-screen prompts to add the sensor to the database.

Dust sensor settings could be accessed in the environment section. On the main screen click on the environment button. Select the appropriate i-BOX from the menu on the left and click on the dust particle sensor.

You may use the default settings by pressing the **Auto Setup** button at the bottom of the screen; or you can use alternative settings due to different environmental conditions. **Read frequency** indicates how often the sensor measures the level of particles in the air; **Reporting frequency** shows how often the reading is reported & **Store frequency** indicates how often the reading is stored in the log file. The status reading could be in the range of 1000 to 8500. If you wish to lower this figure go to the calibration settings by clicking on the **advanced** button. The status reading is directly affected by the value of C2. That means by decreasing the value of C2, you could lower the range of status reading.

By enabling the **Change** function the software will notify you if there is a sudden change in the level of dust particles in the air. Define the minimum and maximum limits and press save. Depending on the environmental conditions the normal reading varies in the range of 1500 to 2500.

Sensor

i-BOX

Sensor Identity: 1610617048 Sensor Type: Dust particle Enable sensor

Sensor Name: Dust particle 1

Group Name:

Port No: 12 Read frequency: 5 sec

 Reporting frequency: 60 sec

Notify change Store frequency: 0 sec

Settings

dust particle


Max: 8000 Status: 1534 10:04:13 Normal

Pre-alarm: 6000

Min: 1000

Change 2000 per read Shunt alarm on access Shunt alarm on delay

Date	Time	Reading	Unit
09/08/2007	10:04:13	1534	
09/08/2007	10:04:13	1534	

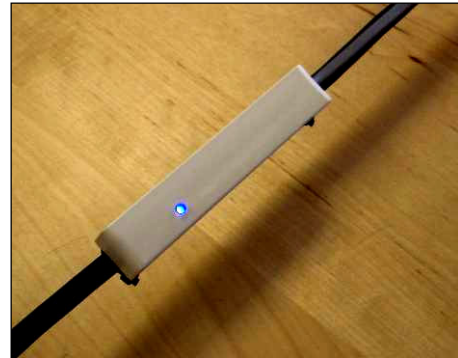


If the level of particles in the air exceeds the defined limits, the software will notify the user by going into the alarm mode. Instantly an alarm transaction will appear on the main screen stating the date & time and the type of the alarm. All the alarms and routine readings can be observed in the **Reports** section.

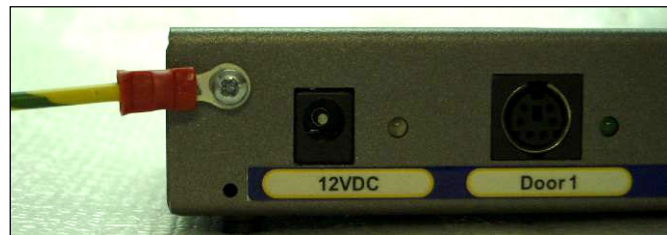
Installation & User Guide

Mains Present Sensor

Mains Present sensor is directly connected to the i-BOX through one of the 14 ports on the back using a standard sensor cable. Once the sensor has been detected by the i-BOX, a new device wizard will appear on the screen. Follow the on-screen prompts to add the sensor to the database. Use the cable ties on the sensor to strap the sensor onto the mains cable.



Please note: in order for the mains present sensor to work reliably, the **i-BOX must be earthed**. Every mains present sensor is supplied with an earth cable & plug. Connect the earth cable to the i-BOX as demonstrated in the picture and plug the other end into the electrical socket.



Settings for the Mains Present sensor could be accessed in the environment section. In the main screen click on the environment button. Select the appropriate i-BOX from the menu on the left and click on the mains present sensor.

The default settings are displayed in the screen-shot below. You may use alternative settings if you wish. Remember you have to press “Save” for the new settings to take effect. If at any time you wish to restore the default settings press the *Auto Setup* button located at the bottom of the screen.

Sensor

Sensor Identity: 1677725704 Sensor Type: Mains Present Enable sensor

Sensor Name: Mains Present 3


Group Name: Read frequency: 1 sec

Port No: 5 Reporting frequency: 60 sec

Notify change Store frequency: 0 sec

Settings

Mains present

 Status: Present 11:42:13 AM Normal

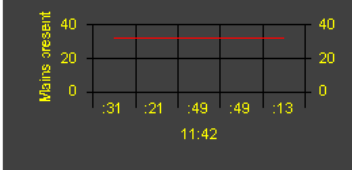
Report on change Alarm on present Panel contact

Store on change Alarm on off Generate shunt

Shunt alarm on access Shunt alarm on delay

Gain: 32 0 63 0

Date	Time	Reading	Unit
8/20/2007	11:42:13 ...	32	
8/20/2007	11:42:13 ...	Present	
8/20/2007	11:41:49 ...	32	
8/20/2007	11:41:49 ...	Present	
8/20/2007	11:41:49 ...	32	
8/20/2007	11:41:49 ...	Present	



Read frequency indicates how often the sensor checks the presence of mains in the cable; **Reporting frequency** shows how often the reading is reported & **Store frequency** indicates how often the reading is stored in the log file. The **Gain** value ($0 < Gain < 63$) determines the level of sensitivity of the sensor. You may need to change this value depending on the thickness of the insulation on the mains cable. As this value increases the sensor becomes more sensitive. In order to tune the sensor you need to change the value of Gain and try to find the point where the sensor starts to detect the mains. Try to find the point where you're getting Off/Present readings

Installation & User Guide

from the sensor, then add one to whatever the value of Gain is at that moment. For example if the sensor starts detecting the mains at Gain = 33, then the suitable sensitivity would be Gain = 34. If **“Alarm on off”** is ticked in the sensor’s settings; once the mains in the cable is lost; an alarm transaction will appear on the main screen stating the date & time and the type of the alarm. All the alarms and routine readings can be observed in the **Reports** section.

8/20/2007 3:05:28 PM Mains present off alarm i-BOX : 200 -1 Sensor : Mains Present 3

DTU (Data Transfer Unit)

Originally introduced as an AX100 component, the data transfer unit is available as an option, to transfer database changes from the PC to the controller without the need for a direct PC connection.

After the initial programming, the AX100 controller can be disconnected from the PC and the controller will perform all access control functions autonomously. The controller can open and close doors without computer intervention.

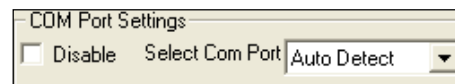
The PC is where all the system configuration and data management is stored. The optional data transfer unit (DTU) enables the data that has been entered at the PC to be downloaded to the controller without the need of a physical PC connection.

One data transfer unit can be used for up to 255 controllers, or a total of 16,000 cardholders distributed over multiple controllers in a single download. E.g. 10 controllers each with 1,600 cardholders can be downloaded in one go, without the need to go backwards and forwards between the PC and controller. Similarly 255 controllers each with 60 cardholders can be downloaded to each controller without returning to the PC. Only valid cardholders are downloaded to the controller.

The Data Transfer Unit is fully *plug and play* at the controller and PC. The AX200 PC software allows multiple DTU’s to be used.

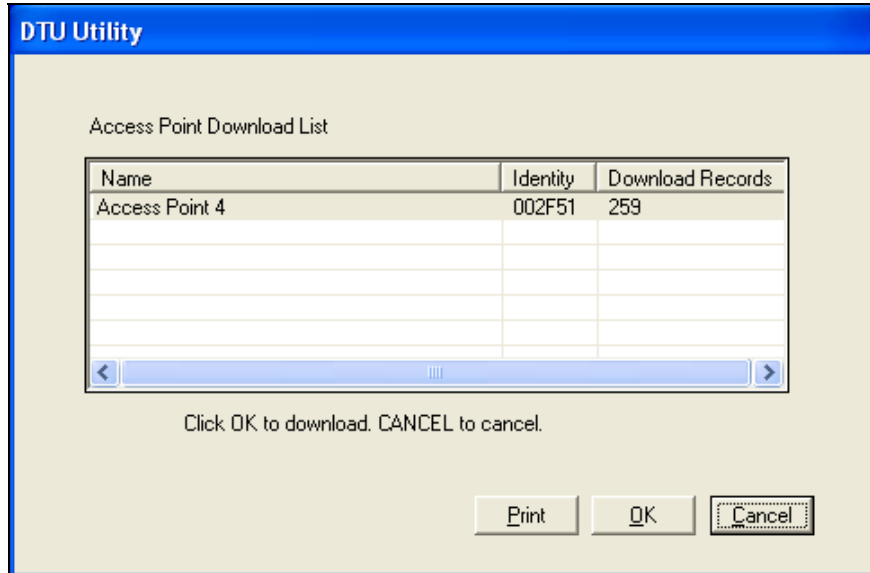
Connecting the DTU

Make sure the COM port settings are enabled in *System Settings • General Settings*. Connect the power supply to the communication cable at the 15 way connector. Plug in the 9 way connector to the serial port of the PC. Start the AX200 software. Connect the DTU to the RJ45 connector, follow the on-screen instructions of the install wizard.



After configuring the DTU, the following window will appear on the screen. This window contains the list of the doors that require download.

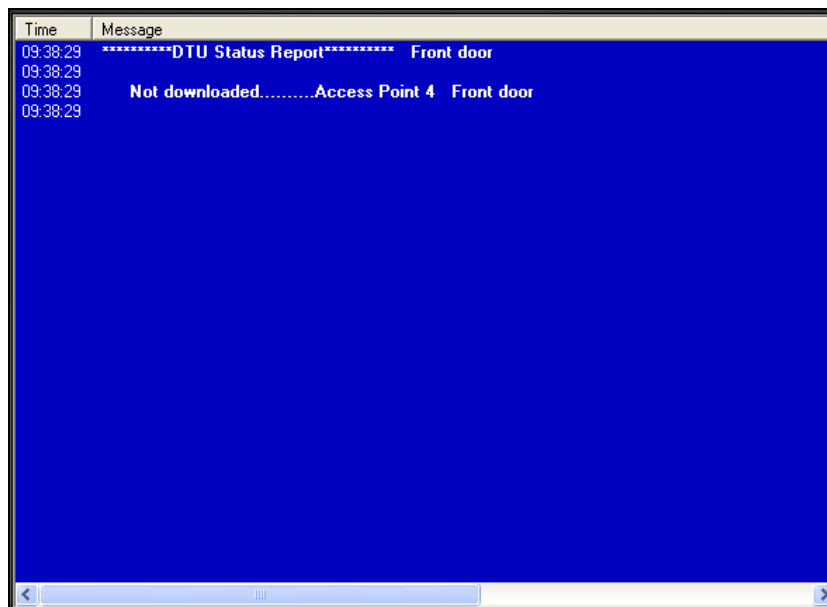
Installation & User Guide



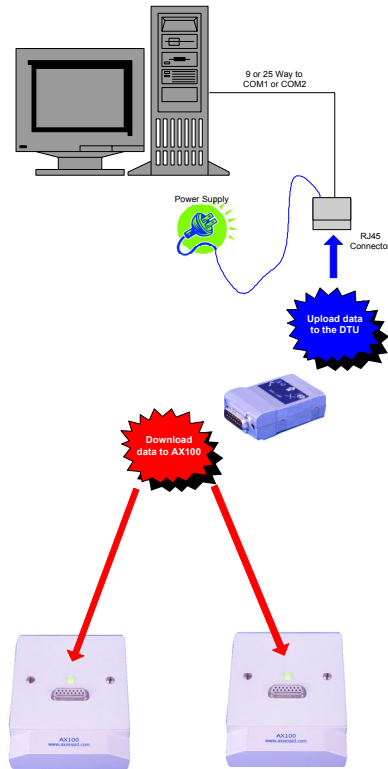
By pressing OK, database changes are automatically downloaded into the DTU. A list of controllers requiring a download can be printed using the reporting function.

Once the data has been downloaded into the DTU, disconnect and plug the unit into the AX100 controller directly (no cable or power supply is required). The data is now automatically transferred into the controller. Once downloaded the LED will go to green (completed) or if flashing green then it is completed but other downloads to controllers are still in the DTU. Complete downloads to all the controllers until the LED is permanent green. Once complete, go back to the PC plug in the DTU. This will confirm all the downloads and remove them from the pending list.

 Download Req'd Any outstanding downloads can be viewed by clicking on the green icon.



Installation & User Guide



DTU

The DTU is fully automatic without any buttons or other complicated things to do. Connect the DTU to the PC and once the information is loaded walk to each door and insert the DTU in the 15 way connector. The DTU will automatically know which information has to be downloaded. If the controller is unknown it will automatically collect all the data and report this back to the PC when connected. If a door is forgotten the download required icon remains visible on the main screen and by double clicking this, a list is shown with outstanding controllers. The list with outstanding controllers can also be printed off as a reminder which doors require a download. When a cardholder is added to the database, downloads are only required to those doors the cardholder requires access.



Add a New Door using a DTU

Installation & User Guide

New doors can be added by simply plugging the DTU into the controller and returning back to the PC. This will automatically start the new device wizard, which allows you to add the new controller. *There is no need to pre-program the controller at the PC first; all settings are handled by the DTU.* Note: - the DTU must be in the current controller list however it does not need to be active for this function to work.

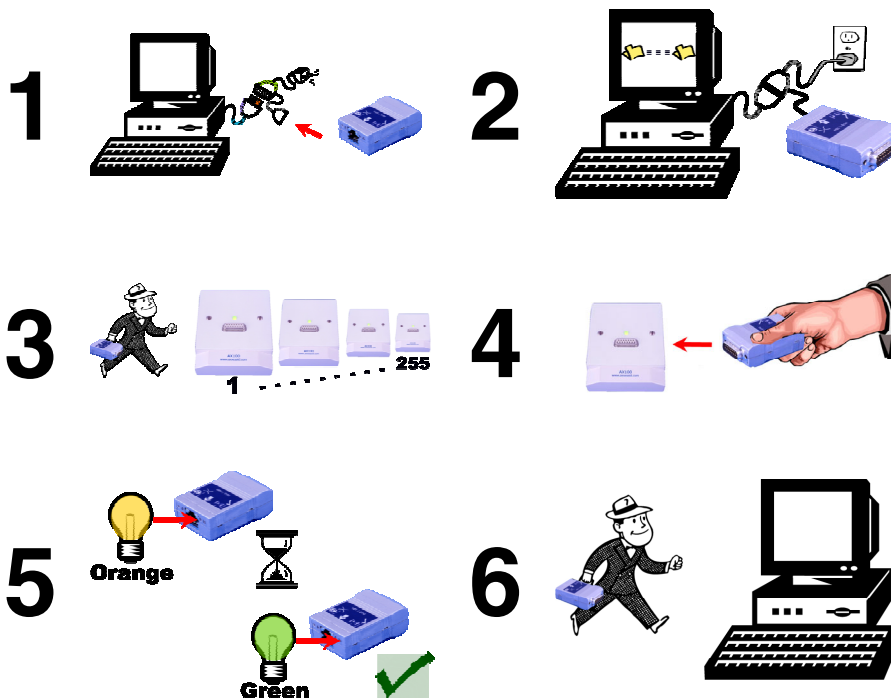
Adding Card Formats using a DTU

A single transaction can also be brought back to the PC by inserting the DTU into the controller and whilst inserted, use a card at the reader. When you return to the PC the transaction will show on the transaction screen. If it is an unknown card type, it will automatically start the card format wizard allowing the addition of the card type to the database (subject to technology type).

The DTU does not contain any batteries, which might need replacing. It is powered directly from the controller and at the PC by the plug-in power supply which connects to the RJ45 connector plug.

Data is permanently stored in the DTU without the need for batteries; this means the DTU can easily be sent in the post to update for instance remote sites. On and offline controllers can be combined within one system.

DTU Step by Step



Installation & User Guide



DTU Operation

1. Start the AX200 software on the PC.
2. Connect the DTU to the serial port on the PC.
3. The auto detect hardware device wizard will start within 10 seconds.
4. Follow the on-screen prompts to add the DTU into the software.
5. Remove the DTU from the PC and plug into a controller.
6. Wait 10 seconds
7. Remove the DTU from the controller and plug it back into the PC.
8. The auto detect hardware device wizard will start within 10 seconds.
9. Follow the on-screen prompts to add the controller.
10. Click on the cardholder button and add new cards as required.
11. Upon exiting the cardholder screen, the new cards will automatically be downloaded to the DTU.
12. Click OK and wait for the on-screen message for the download to be completed.
13. Remove the DTU from the PC and plug it into the controller.
14. When the cards have been transferred from the DTU to the controller, the LED on the DTU will turn green.
15. Remove the DTU from the controller and plug it into the PC.
16. The software will report that the download has been completed successfully.

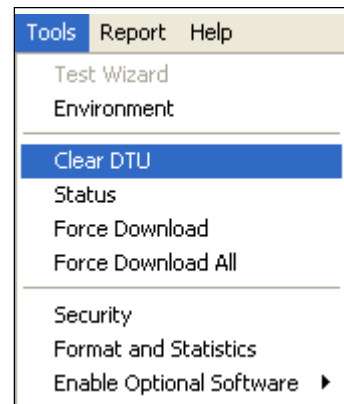
DTU LED Indicators

Blue		DTU Power OK
Blue/Red	Flashing	No Communication
Red	Flashing	Wait
	Constant	Error
Orange		Data download in progress
Green	Flashing	Data downloaded to this controller – data to be downloaded to others
	Constant	Data downloaded and complete

Installation & User Guide

Clear DTU

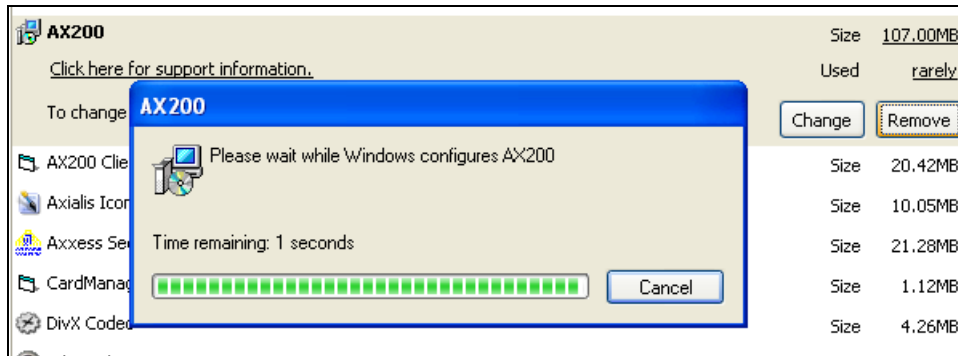
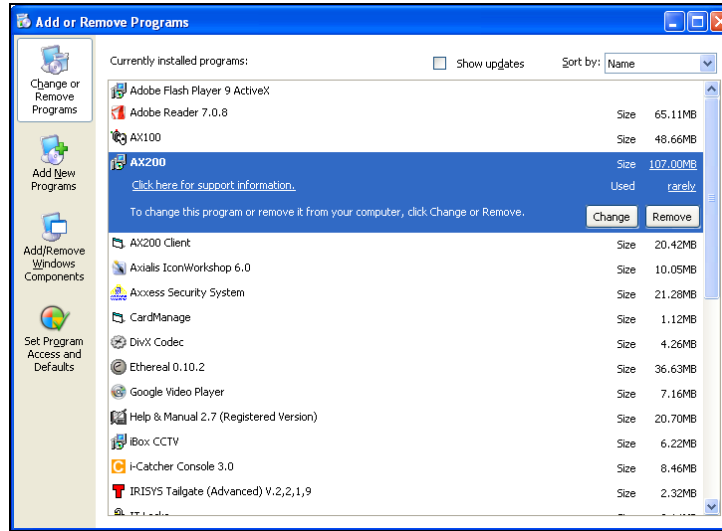
This command can be found on the main screen toolbar. If the DTU has been used for testing purposes with other controllers not belonging to the customers' site, then the DTU will inform you that there is a new device, until you clear the DTU. Just highlight the DTU in the current controllers list on the main screen. Now click on tools on the toolbar and select *Clear DTU*.



Removing the AX200 Program

To remove the AX200 program from your PC, click on the Windows **Start** button, select **Control Panel**, double-click Add/Remove Programs, select **AX200** from the list, select **Remove...**

Installation & User Guide



The AX200 has now been removed from your PC.

Anti-Virus

Sometimes the activities carried out by the AX200 software can be disrupted either by the firewall or the antivirus software which is protecting your PC. This section is intended to provide you with the solutions to some of the problems caused by the most popular antivirus packages.

McAfee®

If you are trying to configure an SMTP server for e-mail in the AX2000 software, when you do a test send, you may encounter an error the instant the AX200 connects to the sever; "**Email aborted due to a timeout or other issue**". When you click on ok the server disconnects and does not send the email!

The issue is caused by *McAfee Virus scan Enterprise version 8 or higher*.

By default the SMTP port in the AX200 is port 25. The antivirus blocks all mass mail processes on port 25.

Installation & User Guide

In order to change the antivirus settings, perform the following steps (On the PC that the AX200 is running):

- I. Select virus scan console from the system tray.
- II. Select access protection
- III. Select the Rule "*Prevent mass mail worms from sending email Port 25*" and click edit.
- IV. Add axid.exe (in lower case) to the excluded process's - note if this is not enabled then enable it, if more than one process is in the list each process is separated with a comma.
- V. Restart the PC

E-mails should now go out correctly.

Installation & User Guide

Readers

Fingerprint Reader

The Verid + fingerprint verification units are standalone devices, designed to provide access control system with instant improved security, or to act as a means of identity verification in a wide range of different applications.

The Verid + fingerprint verification units are available as 3 variants: 1. Verid +, 2.Verid + PIN and 3.Verid + PROX.

When used in an access control system, Verid + is installed between the existing PIN device and door controller, and confirms the identity of the person.

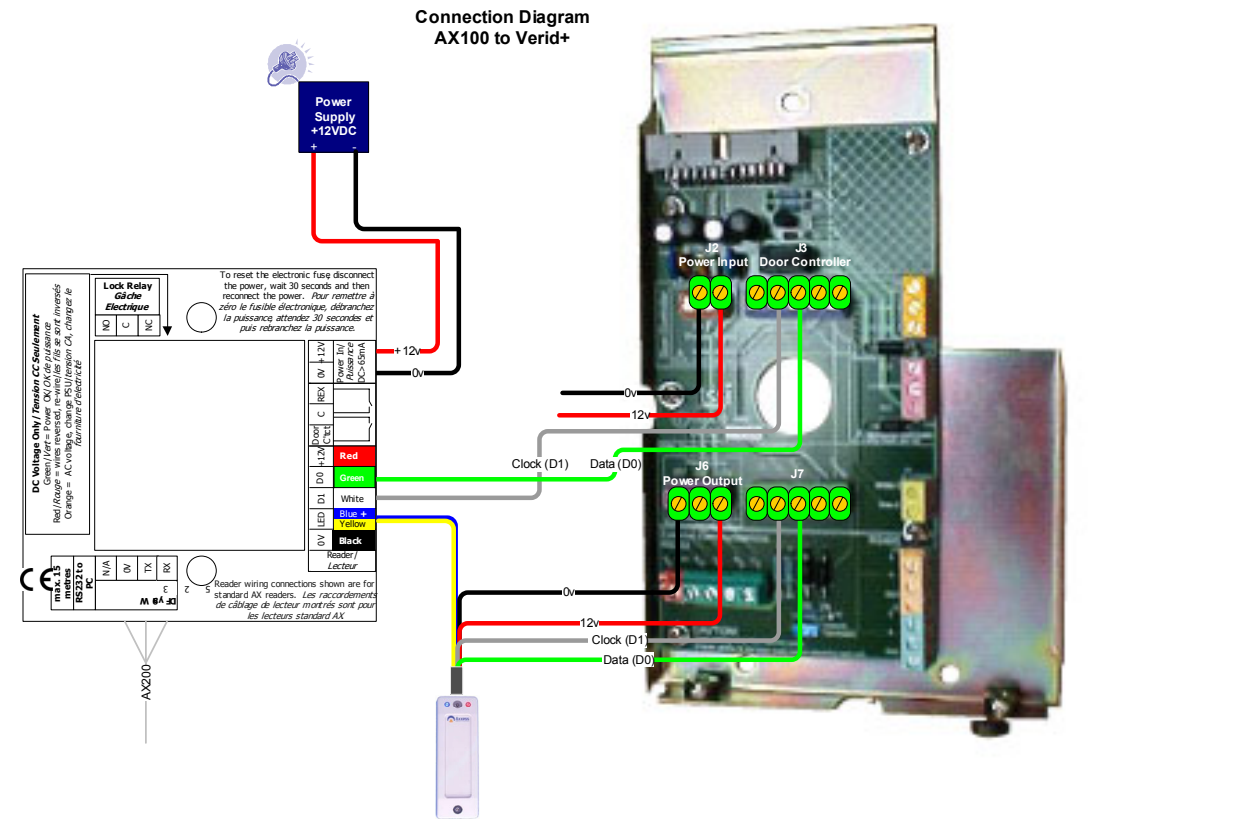
Connection Details

12V input power must be connected to J2 terminal block located on the rear plate of the fingerprint reader. Data0 (D0) & Clock (D1) connections on J3 terminal block are wired into Data0 (D0) & Data1 (D1) connections on the AX100 Controller respectively.

The Power for AXP Proximity reader is taken from J6 block and D0 & D1 wires are connected to J7 terminal block. The required connections to and from Verid+ are listed in the table below.



Installation & User Guide



J2	0V	Power Input	Power Supply Input: 0V
J2	12V	Power Input	Power Supply Input: 12V
J3	Clock(D1)	Door Controller	Output to door controller Clock or Wiegand 1
J3	Data (D0)	Door Controller	Output to door controller Data or Wiegand 0
J6	0V	PIN Power Output	Output to external device 0V
J6	12V	PIN Power Output	Output to external device 12V
J7	Clock(D1)	PIN Device	Input from PIN-Clock or Wiegand 1
J7	Data (D0)	PIN Device	Input from PIN-Data or Wiegand 0

Configuring Verid+

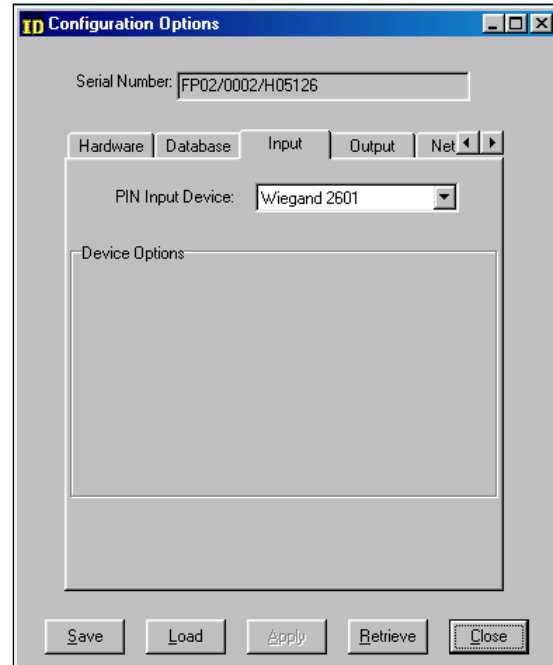
Verid+ has been designed to support PIN entry from a variety of devices – track 2 card readers, proximity readers, and keypad with Wiegand or track 2 outputs water mark and Wiegand readers. All new Verid+ units are delivered to accept input from Wiegand input device. Verid+ will need to be configured to expect the appropriate PIN input device. The appropriate data format for the finger print reader in order to be compatible with the AX200 system is **Wiegand 2601**. Therefore the reader connected to Verid+ unit needs to be programmed to have Wiegand 2601 output. To do this you need to present the appropriate configuration card within 10 seconds of reader start-

Installation & User Guide

up. Note that the card number should be smaller than 65535 otherwise the card number that appears on the screen would not be correct.

To program Verid+ to expect Wiegand 2601 format you need to use Verid + software (Win 95, 98) provided with the unit. Use the provided cable to connect the unit to the serial port on the back of the PC. Then open the software and click on **Connect** in the **Connection menu**. To enter the Configuration mode open the **Mode menu**. The required password is "**Config**". Once in the configuration mode go to **Configuration Options** and make sure that the input and output formats (under Input & Output tabs) are Wiegand 2601. You will have more option available to you in the Supervisor mode (password: SysManager)

Remember that these configurations must be done on a blank database (you can erase the database while you're in the configuration mode. Just go to the database menu).

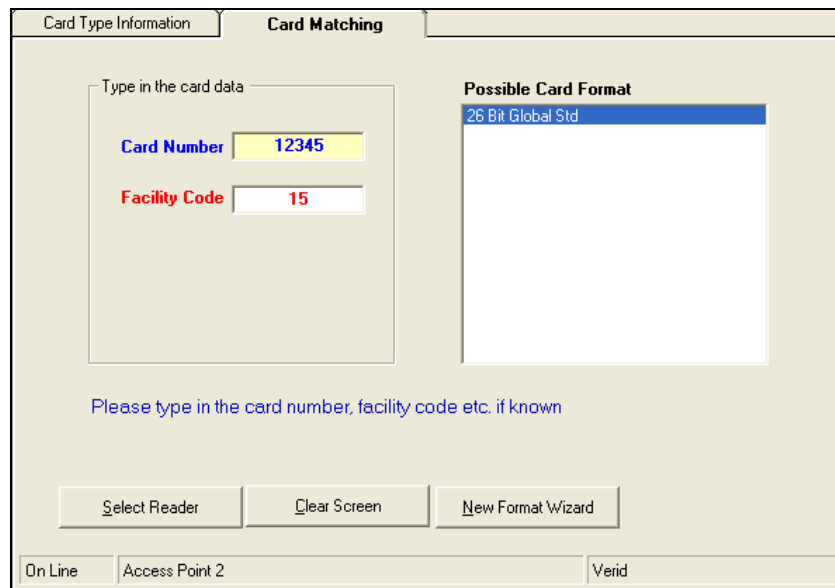


Programming a New User

To program a new user make sure that the database in the reader is empty. When you power up the unit it will automatically enter the **Super User** mode. When "Add a new User" is displayed press enter. Select super user if you're about to enter the first record. Then Select Global Settings. The unit will scan your fingerprint 3 times and create a record known as a template. You will have the option of adding a second template for your user. When "Enter PIN is displayed" *swipe your card or enter a PIN number* and press Enter. If "invalid PIN" is shown on the screen while swiping a card, either the card has not been swiped correctly or Verid+ has not understood the card format or data signals. RE-swipe the card a couple of times. Then check the wiring and the configuration settings. *You can always go back to the super user mode by holding the cancel button while swiping a valid card or entering a valid PIN.*

Once you've programmed the first user successfully, you can use your valid PIN to unlock the door through the AX200 system. To set up a cardholder in the AX200 software you need to choose the correct card format through the **Format and Statistics** section. In the Format and statistics go to card matching and swipe your valid card. After the fingerprint verification the correct card format will appear on the screen.

Installation & User Guide

The screenshot shows a software window titled "Card Matching" with two tabs: "Card Type Information" and "Card Matching". The "Card Matching" tab is active. On the left, under "Type in the card data", there are two input fields: "Card Number" with the value "12345" and "Facility Code" with the value "15". On the right, under "Possible Card Format", there is a list box containing "26 Bit Global Std". Below the input fields, a blue text prompt reads "Please type in the card number, facility code etc. if known". At the bottom, there are three buttons: "Select Reader", "Clear Screen", and "New Format Wizard". At the very bottom of the window, there are three small buttons: "On Line", "Access Point 2", and "Verid".

You need to add this format through the New Format Wizard.

Getting Started Quickly

1. Do the connections according to the table provided in the first page.
2. Install the Verid software provided with the unit and connect the unit to the serial port on the back of the PC.
3. Enter the configuration mode (password: Config)
4. Make sure that the database is empty. (If the database is empty the unit will automatically enter the super user mode at the start up.) If the database is not empty you can erase it in the database menu.
5. Under Options • Configuration Options • Input, select Wiegand 2601 from the drop-down menu. Make sure the out-put is the same.
6. Before exiting the software go to Mode • Start Verification.
7. Once the unit has been programmed to accept Wiegand 2601 format. Power up the unit and add your first user.
8. In the AX200 software add the correct format through "format & statistics" (26bit Global Std)
9. Setup a cardholder with the correct card number & card format.

Installation & User Guide

Honeywell Proximity Readers

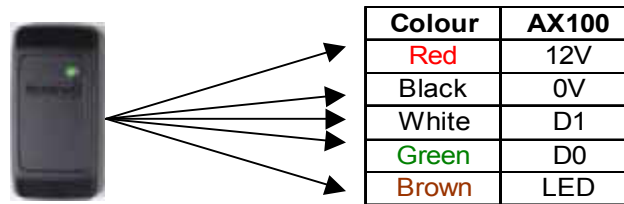
Honeywell proximity readers have been designed to be installed for use with access control systems. The following instructions outline the connections between the reader and the AX200 access control system as well as the software configurations that need to be carried out in order to make the system ready to operate.



How to connect the reader to the host

The reader is supplied with an 18-inch pigtail, having a 6-conductor cable. To connect the reader to the AX200 system, perform the following steps:

1. If there is a connector on the end of the cable (used during manufacture for testing purposes), cut it off. Prepare the reader cable by cutting the cable jacket back 1.25 inches and strip the wires 0.5 inch.
2. The reader is connected directly to the AX100 controller. The table below shows the connections on the AX100 controller and the corresponding wires on the Honeywell proximity reader.



When using a separate power supply for the reader, power supply and the AX100 must have a common ground.

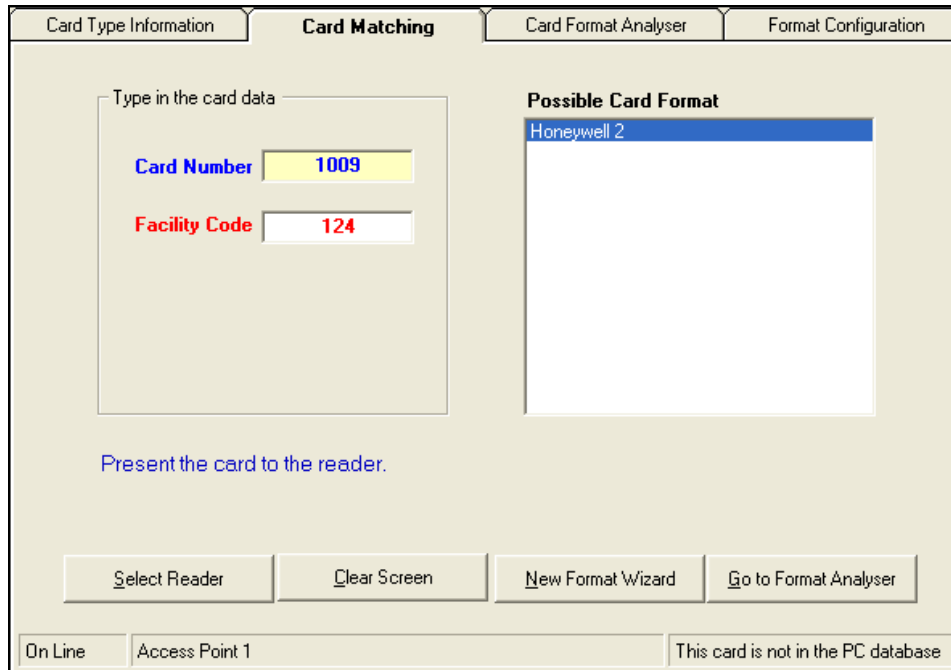
3. Do not connect the Tamper (purple) lead to the AX100.
4. Trim and cover all conductors that are not used.

Software Configuration

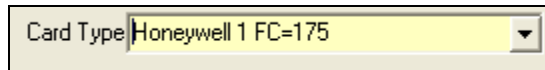
Once the reader & the AX100 controller have been connected to the AX200 unit you should be able to see it on the controllers menu on the right hand side of the main screen. In order to program a valid card with the ability to have access through a Honeywell proximity reader you need to choose the correct format.

1. On the main screen click on the Format & Statistics.
2. Under the Card Matching tab press "Select Reader"
3. Choose the appropriate reader from the list and present the card to the reader
4. The software will automatically display the card number, Facility Code and the possible card formats.

Installation & User Guide



5. The most common card formats associated with Honeywell proximity readers are Honeywell 1 & 2 which are included in the default database.
6. If the format displayed on the screen is correct, press New Format Wizard.
7. Follow the on-screen prompts to add the new card format.
8. Once the correct card format is added, go to the cardholder screen and add your new card and choose the correct card type.



9. To be able to see other card formats in the card type menu you need to enable “*Multiple Card Formats*” under *System Settings • General Settings*.

Installation & User Guide

AXM Readers

The AXM magstripe readers provide high performance and reliability for high security access control. AXM readers are completely weatherproof and suitable for in-door and out-door applications.



Output Type

- Wiegand 50 bit (Type 5)

Other output formats available for most OEM applications

Magstripe cards supplied by Axxess Identification are encoded in order to work with 7×7 format. In this type of encoding the first 7 digits are used to calculate the card number and the rest makes up the facility code. For example if the card has a 10 digit number; using the 7 ×7 format, the first 7 digit will form the card number and the last 3 digits will form the facility code. If the number of digits is less than 7 then the facility code will be zero.

7	×	7
0000FFF		CCCCCCC

All the standard cards supplied by Axxess ID are recognized by the AX200 software and ready to be programmed. If you have not purchased your card from Axxess Identification, you may have to use the card matching function and activate the appropriate card format in order to make the card valid. Card matching feature is available in the Format & Statistics section. For more information please refer to the Format & Statistic section on this manual.

Connection Details

The following table explains the connections between the AXM reader and the AX100 controller:

Colour	AX100		Reader
Black	0V		Black 0VDC Signal Gnd
Yellow	Buzzer		Yellow Buzzer Control
Orange	LED		Orange Green/Yellow LED
White	D1		White Data (Weigand 1)
Green	D0		Green Clock (Weigand 0)
Red	12V		Red VDC Supply (5-18)

- ❖ Yellow and Orange wires are both connected to the LED socket on the AX100 controller.
- ❖ You may disconnect the yellow lead if you wish to disable the buzzer.
- ❖ DO NOT connect the purple wire as it is only used for programming.
- ❖ Blue wire is for card present indication. (DO NOT connect)

Installation & User Guide

Proximity Request to Exit

The Proximity REX detects the hand within the range of approximately 5cm. Once the hand has been detected, the relay goes off and closes the connection between the relay board and the request to exit terminal on the AX100 controller. The Proximity REX acts exactly like the REX Button and once the request to exit has been granted, the appropriate transaction appears on the main screen stating the time and the name of the access point. Please note that this product is based on infrared technology; therefore other infrared light sources may affect the performance of this detector.



8:58:48 REX button access granted. Access Point 1

Technical Details

- ❖ Power Requirement: 10-14 VDC (15mA Quiescent. 35mA Operated)
- ❖ Changeover relay contacts rated 30VDC Max. 1A non-inductive.

The diagram below shows the connections between the proximity REX and the AX100 controller.

AX100	Proximity REX
C	COM
REX	NO

