

Access Easy Controller™ Software User Manual

All rights reserved. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of BOSCH SECURITY SYSTEMS.

This manual is provided pursuant to a license agreement containing restrictions on their use. The manual contains valuable trade secrets and proprietary information of BOSCH SECURITY SYSTEMS and is protected by international copyright law. It may not be copied or distributed to third parties, or used in any manner not provided for in the said license agreement.

All software is provided "AS IS." The sole obligation of BOSCH SECURITY SYSTEMS shall be to make available all published modifications that correct program problems are published within one (1) year from the date of shipment.

The software is intended for use only with the hardware specified in this manual and in the absence of other software. Concurrent use with other software or with hardware not specified may cause the program to function improperly or not at all. BOSCH SECURITY SYSTEMS may not provide support for systems operating under such conditions.

All efforts have been made to ensure the accuracy of the contents of this manual.

The above notwithstanding, BOSCH SECURITY SYSTEMS assume no responsibility for any errors in this manual or their consequences.

The information on this document is subject to change without notice.

Access Easy Controller™ is a trademark of Bosch Security Systems

Other product and company names mentioned herein may be the trademarks of their respective owner.

Edition 1.0.1

Released: March 2006

Manual P/N (Stock Code) :

Copyright © 2006 by
Bosch Security Systems
38C Jalan Pemimpin
SINGAPORE 577180.
Tel : 65-6319 3450

Web site : <http://www.boschsecurity.com>

End-User License Agreement for Access Easy Controller™ software

BOSCH SECURITY SYSTEMS SOFTWARE PRODUCTS: -

- **Server Software:** Access Easy Controller™ Software,
Number of Client Access Licenses: 8

BOSCH SECURITY SYSTEMS HARDWARE PRODUCTS: Access Easy Controller™ and all input/output modules.

IMPORTANT - READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and BOSCH SECURITY SYSTEMS for the BOSCH SECURITY SYSTEMS SOFTWARE PRODUCT, which you acquired, and any of the HARDWARE PRODUCT(s) identified above.

The SOFTWARE PRODUCT includes computer software, the associate media, any printed materials, and any "online" or electronic documentation. By installing, copying or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, BOSCH SECURITY SYSTEMS or its resellers are unwilling to license the SOFTWARE PRODUCT to you. In such event, you may not use or copy the SOFTWARE PRODUCT, and you should promptly contact BOSCH SECURITY SYSTEMS or its distributors for instructions on return of the unused product for a refund.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as intellectual property laws and treaties.

The SOFTWARE PRODUCT is licensed, not sold.

1. **GRANT OF LICENSE.** The SOFTWARE PRODUCT refers to the Access Easy Controller™ Software that runs on the "Access Easy Controller™" that enables a computer or workstation running a Web Browser Software ("Third Party Software") to access or utilise the services provided by the Access Easy Controller™ Access control. This EULA grants to you the following rights to the SOFTWARE PRODUCT:

- **Use of the Server Software.** You may use one copy of the Server Software running on one Server, which may be connected at any point in time an unlimited number of workstations or computers operating on one or more networks. You must acquire a separate Client Application Software License to access or otherwise utilise the services of the Server by using the Third Party Software.

2. **DESCRIPTION OF OTHER RIGHTS AND LIMITATION**

- **Client Access Licenses.** This EULA grants you the number of Client Access Licenses for the SOFTWARE PRODUCT indicated at the top of this EULA. Each license permits one additional computer or workstation the right to access or utilise the services of the Server. The services of the Server are considered to have accessed or utilised when there is a direct or indirect connection between a computer or workstation and a Server.
- **Restriction** against copying or modifying the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is copyrighted by BOSCH SECURITY SYSTEMS or third parties. Except as expressly permitted in this agreement, you may not copy or otherwise reproduce the SOFTWARE PRODUCT. In no event does the limited copying or reproduction permitted under this agreement include the right to de-compile, reverse engineering, disassemble, modify or electronically transfer the SOFTWARE PRODUCT, or to translate the SOFTWARE PRODUCT into another computer language.
- **Separation of Components.** The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one Server.
- **Rental.** You may not rent or lease the SOFTWARE PRODUCT.
- **Termination.** Without prejudice to any other rights, BOSCH SECURITY SYSTEMS may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

3. **COPYRIGHT.** All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by BOSCH SECURITY SYSTEMS or its suppliers. The SOFTWARE PRODUCT is protected by the copyright laws and international treaty provisions. You may not copy printed materials accompanying the SOFTWARE PRODUCT.

LIMITED WARRANTY – BOSCH SECURITY SYSTEMS warrants that (a) Access Easy Controller™ Software and (b) Access Easy Controller™ Access Control Panels and all input/output modules manufactured only by BOSCH SECURITY SYSTEMS will perform adequately in accordance with the accompanying User's Manual; and will be free from defects in materials and workmanship under its intended normal use and service for a period of 1 year from date of purchase.

CUSTOMER REMEDIES – BOSCH SECURITY SYSTEMS'S entire liability and your exclusive remedy shall be, at BOSCH SECURITY SYSTEMS'S option, either (a) return of the price paid or (b) repair or replacement of the hardware or software that does not meet BOSCH SECURITY SYSTEMS'S limited warranty and which is returned to BOSCH SECURITY SYSTEMS with a copy of your purchase receipt. This limited warranty becomes void if failure of the hardware or software has resulted from abuse, accident or misapplication.

NO LIABILITY OR CONSEQUENTIAL DAMAGES – Under no circumstances shall BOSCH SECURITY SYSTEMS or its suppliers be liable for any other damages whatsoever (including, without limitation, damages for business interruption, loss of business profits or other pecuniary loss) arising out of the use of or inability to use this BOSCH SECURITY SYSTEMS product. BOSCH SECURITY SYSTEMS total liability under any provision of this agreement shall be limited to the amount actually paid by you for the product.

This Page Intentionally Left Blank

How to Use this Manual

This manual describes the operation and administration of the Access Easy Controller software. It is to be read in conjunction with the Hardware Manual.

Access Easy Controller provides the necessary operation of an Access Control system and it has its own Intrusion Detection system. It can store up to 20,048 Card IDs in the database and the transactions/events buffer can hold up to 20,048 records. New features such as short text messaging service (SMS) have been incorporated into it. Access Easy Controller is a product that can function independently.

Access Easy Controller Series features summary is included below for the users to refer to.

Access Easy Controller Functional Features		
Item	Description	Remarks
1	Door access control	√
2	Intrusion alarm/input monitoring	√
3	Output device control (on/off)	√
4	Time attendance clocking	√
5	Email messaging upon triggered conditions	√
6	SMS messaging upon triggered conditions	√
7	Support modem dial-in from remote PC	√
8	Immediately save database (parameters, activities & audit log) into compact flash	√
9	Integrate to Access Easy Master	√
10	Support normal anti-passback (2 zones) without priority control	-
11	Support priority anti-passback zone (254 zones) operation and only registered if door contact detect door being open by cardholder	√
12	Support door forced open alarm delay	√
13	Support door held open pre-warning	√
14	Support reader lockout after a pre-define invalid card event	√
15	Support elevator access control	√
16	Integrated door access reader with arm/disarm function (using same reader)	√
17	Special cardholder with extended duration for door strike and keypad	√
18	One time access	√
19	Dual card entry (2 man rule)	√
20	Card enrolment function for any card with unknown card format	√
21	Option to unlock door by schedule only after a valid access card is presented	√
22	Input monitoring (door contact, request-to-exit, alarm input points) support configurable 2 state non-supervise, 2 state supervise and 4 state supervise for all input points in the controller.	Configurable:- • 2 state non-supervise (no EOL) • 2 state supervise (6.8K EOL) • 4 state supervise (12K & 15K EOL)
23	Card database import and export function (in CSV format)	√
24	Real time activities and status update	√

25	Department field in the card assignment	30 alpha-numeric characters
26	Advance I/O (guard tour, feed through, Or, And, Xor, Nand, up/down counter and exit door)	√
27	Support interlock / mantrap operation using advance I/O configuration	√
28	Browser login encryption	128 bits SSL
Maximum Capacities		
1	Wiegand reader support	16
2	Input monitoring points	32
3	Relay outputs	32
4	Cardholder	20480
5	Transaction history	20479
6	Audit log	1023
7	Compact flash size	128MB
Supported Languages		
1	US English	√
2	UK English	√
3	Japanese	√
4	Spanish	√

Table of Contents

CHAPTER 1. INTRODUCTION TO ACCESS EASY CONTROLLER	1-1
CHAPTER 2. ACCESSING ACCESS EASY CONTROLLER	2-1
CONNECTING TO ACCESS EASY CONTROLLER	2-1
LOGGING ONTO ACCESS EASY CONTROLLER	2-2
<i>Logging onto Access Easy Controller</i>	<i>2-3</i>
<i>Logging off from Access Easy Controller.....</i>	<i>2-3</i>
UNDERSTANDING THE HOME PAGE MAIN MENU GROUPS	2-4
View Activity.....	2-5
Activity Report.....	2-5
Manual Control	2-5
Card Database	2-5
Card Access Admin.....	2-5
Panel Admin	2-6
Panel Maintenance.....	2-6
Logout.....	2-6
NAVIGATING THROUGH ACCESS EASY CONTROLLER PAGE	2-7
USAGE OF THE BUTTONS	2-9
CHAPTER 3. VIEW ACTIVITY	3-1
TO ACTIVATE VIEW ACTIVITY	3-3
TO GENERATE A PRINT PREVIEW OF THE REPORT	3-6
<i>To format report based on Card Number.....</i>	<i>3-6</i>
<i>To format report based on Name.....</i>	<i>3-7</i>
<i>To format report based on Department</i>	<i>3-8</i>
<i>To format report based on Location.....</i>	<i>3-8</i>
<i>To format report based on Date/Time</i>	<i>3-9</i>
PRINTING THE REPORT.....	3-10
CHAPTER 4. CARD ASSIGNMENT.....	4-1
TO ACTIVATE CARD ASSIGNMENT	4-2
<i>To view different sets of Card range.....</i>	<i>4-2</i>
ADDING/DELETING A RANGE OF CARD NUMBERS.....	4-3
<i>To add a Batch of Card Number.....</i>	<i>4-3</i>
<i>To delete a Batch of Card Number</i>	<i>4-4</i>
<i>To add a Batch of Card Number with same data entries.....</i>	<i>4-4</i>
<i>Using Automatically replace the existing card(s) with default/reference card information function.....</i>	<i>4-5</i>
Cards Enrolment Operation.....	4-6
Card Enrolment of Card with Unknown Wiegand Format.....	4-6
Card Enrolment Using Web Page	4-6
Card Enrolment Using Pre-Assigned Enrolment Card.....	4-9
System Messages	4-11
EDITING THE CARD PARAMETERS.....	4-12
To add or edit Card Number parameters	4-12
Card Details	4-12
Card Functionality	4-13
Dual Card Assignment.....	4-16
To select Card Functionality	4-16
To select and edit Card Validation Period	4-17
To Select and edit dual card assignment	4-17
Card Database Import and Export Function (In CSV Format).....	4-18
Exporting the Card Database	4-18
Importing the Card Database	4-23
THE SEARCH FUNCTION	4-24
<i>To find a particular Cardholder based on Card Number.....</i>	<i>4-24</i>
<i>To find a particular Cardholder based on Name</i>	<i>4-24</i>
<i>To search for Empty Slot.....</i>	<i>4-25</i>
TO GENERATE A PRINT PREVIEW OF THE REPORT	4-26
To generate a Card Assignment report	4-26
CHAPTER 5. SCHEDULES.....	5-1

TO ACTIVATE SCHEDULE	5-2
<i>To edit Schedule parameters</i>	<i>5-3</i>
SYSTEM BEHAVIOUR WHEN USING SCHEDULE	5-5
TO GENERATE A PRINT PREVIEW OF THE REPORT	5-6
<i>To generate a Schedule report.....</i>	<i>5-6</i>
CHAPTER 6. ACCESS GROUPS.....	6-1
TO ACTIVATE ACCESS GROUPS	6-2
<i>To configure/edit Access Group parameters</i>	<i>6-3</i>
TO GENERATE A PRINT PREVIEW OF THE REPORT	6-3
<i>To generate an Access Groups report</i>	<i>6-4</i>
CHAPTER 7. HOLIDAYS.....	7-1
TO ACTIVATE HOLIDAYS	7-2
<i>To edit Holidays parameters</i>	<i>7-3</i>
TO GENERATE A PRINT PREVIEW OF THE REPORT	7-5
<i>To generate a Holidays report.....</i>	<i>7-5</i>
CHAPTER 8. DOOR CONTROL.....	8-1
TO ACTIVATE DOOR CONTROL.....	8-2
<i>To control the Doors manually.....</i>	<i>8-3</i>
CHAPTER 9. INPUT CONTROL.....	9-1
TO ACTIVATE INPUT CONTROL.....	9-2
<i>To control (Arm/Disarm) an Input Point.....</i>	<i>9-4</i>
<i>To control (Arm/Disarm) the Alarm Zone</i>	<i>9-5</i>
CHAPTER 10. OUTPUT CONTROL.....	10-1
TO ACTIVATE OUTPUT CONTROL	10-2
<i>To control the Output Points</i>	<i>10-3</i>
CHAPTER 11. RESET APB.....	11-1
TO ACTIVATE RESET APB	11-2
<i>To reset APB based on Card Number wrt Reader / All Readers</i>	<i>11-2</i>
<i>To reset APB based on Name wrt Reader / All Readers.....</i>	<i>11-3</i>
<i>To reset APB by All Card numbers wrt Reader / All Readers</i>	<i>11-3</i>
TO GENERATE A PRINT PREVIEW OF THE REPORT	11-4
<i>To generate APB Zones Report</i>	<i>11-4</i>
CHAPTER 12. DATABASE BACKUP.....	12-1
TO ACTIVATE DATABASE BACKUP	12-2
<i>To define Daily Backup Schedule</i>	<i>12-2</i>
<i>To Backup System Database To PC</i>	<i>12-3</i>
<i>To Backup Activity, Audit log and/or Attendance Records to PC.....</i>	<i>12-5</i>
CHAPTER 13. PANEL SETUP	13-1
TO ACTIVATE PANEL SETUP	13-2
NETWORK SETTING	13-2
<i>To Configure LAN 1 Network Setting.....</i>	<i>13-3</i>
REMOTE PC ADDRESSES	13-4
<i>To edit Remote PC Addresses.....</i>	<i>13-4</i>
EMAIL SERVER SETUP INFORMATION	13-5
<i>To Configure the Email Server Setup Information</i>	<i>13-6</i>
DIAL IN IP SETUP INFORMATION	13-6
<i>To edit the Dial In IP Settings Information</i>	<i>13-7</i>
Access Easy Master Controller Settings.....	13-8
SMS Server Settings Information.....	13-8
To Configure Access easy controller as a SMS Server	13-9
To Configure Access easy controller as a SMS Client.....	13-10
INPUT POINT CONFIGURATION	13-12
<i>To activate Input Point Configuration.....</i>	<i>13-12</i>
<i>To select Input Point Configuration</i>	<i>13-13</i>

<i>Support Configurable 2 State Non-Supervised, 2 State Supervised and 4 State Supervised For All Input Points in The Panel</i>	13-14
SET DATE & TIME	13-14
<i>To activate Date & Time Setting</i>	13-15
<i>To set the Date & Time</i>	13-15
<i>To set the Time Synchronization</i>	13-16
Synchronizing date & time with a internet Time Server	13-16
Synchronizing date & time with an intranet Time Server	13-16
AUTO LOGOUT TIMER	13-17
<i>To activate Auto Logout Timer</i>	13-17
<i>To edit the Auto Logout Timer</i>	13-17
AUDIT LOG	13-18
<i>To View the User Log</i>	13-18
<i>To View System Log</i>	13-19
DEFAULT SETTINGS	13-21
<i>To activate Default Settings</i>	13-21
<i>To edit View Activity Setting</i>	13-22
<i>To edit Default Activity View Setting</i>	13-22
<i>To edit the User Definable Fields and Facility Code</i>	13-22
CARD FORMAT	13-23
<i>To activate Card Format</i>	13-23
<i>To configure Card Format</i>	13-24
COMPANY PROFILE	13-27
<i>To activate Company Profile</i>	13-27
<i>To edit Company Profile</i>	13-27
<i>To edit Department List</i>	13-28
EMAIL/SMS CONFIGURATION	13-29
<i>To activate the Email Configuration</i>	13-30
<i>Send To</i>	13-30
<i>To edit the Email Configuration (Send To)</i>	13-31
<i>To test the Email sent verification</i>	13-31
<i>Message field</i>	13-32
<i>To edit the Message field</i>	13-32
<i>Devices</i>	13-33
<i>To edit the Email Configuration (Devices)</i>	13-33
<i>Cardholders</i>	13-34
<i>To edit the Email Configuration (Cardholders)</i>	13-34
<i>Events</i>	13-35
<i>To edit the Email Configuration (Events)</i>	13-35
LATENESS REPORT	13-36
<i>To edit the Email Configuration (Lateness Report)</i>	13-36
SAMPLE EMAIL CONFIGURATION FOR LATENESS REPORT	13-38
<i>SMS Configuration</i>	13-40
<i>To activate the SMS Configuration</i>	13-40
<i>Send To</i>	13-41
<i>Message field</i>	13-41
<i>Devices</i>	13-41
<i>Cardholders</i>	13-42
<i>Events</i>	13-42
CHAPTER 14. INPUT SETUP	14-1
TO ACTIVATE THE INPUT SETUP	14-2
<i>Alarm Zone Description</i>	14-4
<i>To generate a Print Preview of the Input Point</i>	14-5
CHAPTER 15. OUTPUT SETUP	15-1
TO ACTIVATE THE OUTPUT SETUP	15-2
<i>Disable Activity From Output Point</i>	15-3
<i>To Generate a Print Preview of the Output Point</i>	15-4
CHAPTER 16. CARD READERS	16-1
<i>Reader Function</i>	16-2
Entry Reader	16-3
Exit Reader	16-3

Entry and Arm/Disarm Reader	16-4
Elevator Reader	16-5
<i>Reader Options</i>	16-7
Turn off the reader	16-7
Enable Keypad Only Operation	16-7
On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)	16-8
Keypad Timeout	16-8
Enable Reader Lockout	16-8
<i>Scheduling Options</i>	16-10
Unlock door (For Entry Reader, Entry and Arm/Disarm Reader)	16-10
Disable Elevator Reader (For Elevator Reader Only)	16-10
Schedules will not be used to unlock this door	16-10
Schedules will be used to unlock this door	16-10
Schedules and Holidays will be used to unlock this door	16-11
<i>Door Output Settings (For Entry Reader, Entry and Arm/Disarm Reader)</i>	16-13
Door Open Timer	16-13
Door Strike Timer	16-13
Door Strike	16-14
<i>Door Input Settings (For Entry Reader, Entry and Arm/Disarm Reader)</i>	16-15
Request-to-Exit Device	16-15
Door Contact	16-15
Door Forced Open Alarm delay duration	16-15
Schedules and holidays will be used to shunt door contact	16-16
Pre-alarm Warning before door held open alarm	16-16
<i>Floor Output Settings (For Elevator Reader Only)</i>	16-17
<i>PIN Code Settings</i>	16-19
PIN code not required	16-19
PIN code required at all times	16-19
PIN code required, except during schedule intervals	16-20
PIN code required, except during regular schedule intervals and holiday schedule intervals	16-20
PIN code only operation using Reader's PIN code	16-20
<i>Anti-Passback (APB) Settings</i>	16-22
APB deactivated	16-22
Activate Time Based APB	16-22
Activate Soft APB	16-23
Activate Full APB	16-23
<i>Dual Card Configuration</i>	16-26
Dual Card Mode disabled	16-26
After using 2 card to initiate the access, the system will switch back to single card access	16-26
Dual Card access at all time	16-27
<i>To generate a Print Preview of the Card Reader Report</i>	16-27

CHAPTER 17. ADVANCE I/O SETUP..... 17-1

Guard Tour	17-1
Feed Through	17-3
OR Logic	17-3
AND Logic	17-4
XOR Logic	17-5
NAND Logic	17-6
Interlock / Man Trap	17-6
Up-Down Counter	17-10
Exit Door	17-11
One Shot	17-13
<i>Ability to accept other types of Arm/Disarm Input Control</i>	17-14
Inter-connection	17-14
Output	17-14
Input	17-14
Schedule	17-14
Criteria	17-14
Always On/Off	17-24

CHAPTER 18. USERS..... 18-1

TO ACTIVATE USERS	18-2
<i>To edit User ID and Password</i>	18-3
<i>To select access right to Access Easy Controller menu items</i>	18-4

CHAPTER 19. UPDATE FLASH 19-1

TO ACTIVATE UPDATE FLASH	19-2
--------------------------------	------

<i>To Update Panel Software.....</i>	<i>19-3</i>
CHAPTER 20. REBOOT PANEL, SHUTDOWN PANEL.....	20-1
TO ACTIVATE REBOOT PANEL.....	20-1
TO SHUTDOWN PANEL	20-2
CHAPTER 21. DIAL IN USER	21-1
SETTING UP WINDOWS FOR DIAL-IN.....	21-1
SETTING UP MACINTOSH FOR DIAL-IN	21-9
APPENDIX A. INITIAL SETUP TO ACCESS EASY CONTROLLER.....	A-1
PROCEDURE TO SET THE IP ADDRESS OF COMPUTER	A-3
<i>For PC Users.....</i>	<i>A-3</i>
<i>For Macintosh Users.....</i>	<i>A-7</i>
SETTING TO BE MADE TO THE WEB BROWSER	A-9
<i>For PC User.....</i>	<i>A-9</i>
<i>For Macintosh Users.....</i>	<i>A-13</i>
SETTING THE ACCESS EASY CONTROLLER IP ADDRESS THROUGH ADDRESS RESOLUTION PROTOCOL (ARP).....	A-16
APPENDIX B. ACTIVITY TRANSACTIONS	B-1
ALARM ACTIVITY	B-1
RESTORE ACTIVITY	B-1
VALID ACTIVITY	B-2
TIME ATTENDANCE.....	B-2
APPENDIX C. EMAIL/SMS CONFIGURATION TABLE.....	C-1
APPENDIX D . SETTING UP A TIMESERVER (WINDOWS 2000 AND XP PROFESSIONAL).....	D-3
APPENDIX E. BLANK CONFIGURATION FORMS	E-1

This Page Intentionally Left Blank

CHAPTER 1

Introduction to Access Easy Controller™

Access Easy Controller is a revolutionary invention that takes advantage of the web technology age by changing the way an electronic access control system is implemented.

The conventional way of implementing a typical access control system requires installation of PC based application programs that are used to remote control and monitor a controller in the system. Furthermore, application programs that are designed for a specific operating system, has to be re-developed before it can run on another operating system, for example from Win 98 to Win NT/2000.

Access Easy Controller uniquely combines the features of a Web server and Access Control functionality's into one complete unit. Such powerful combination provides a highly cost-effective solution, which truly offers to user the simplicity and ease-of-use associated with the popular Web interface while incorporating a rich suite of sophisticated security features essential for small to medium-sized businesses.

The design of Access Easy Controller adopts the common desktop metaphor for all web based applications for consistency and ease of use. The same "look-and-feel" such as buttons and check boxes that you have experienced in other web based applications will be seen in Access Easy Controller.

This Page Intentionally Left Blank

CHAPTER 2

Accessing Access Easy Controller

In this chapter, you will learn the basic information of how to access the Access Easy Controller and logging onto the software.

In order to operate one or more Access Easy Controller from one or more computers, a standard web browser program such as *Internet Explorer, version 4.0 and above*, or *Netscape Navigator, version 4.0 and above* on each of the central monitoring computer is required.

Connecting to Access Easy Controller

Before the Access Easy Controller can be access, it must be configured properly and integrated to the existing computer network.

As this integration is fairly complex and requires knowledge on networking, it is the responsibility of the *System Installer* to working closely with your company's *Network Administrator* to do the initial set up.

However, for general knowledge, a description is presented in *Appendix A*.

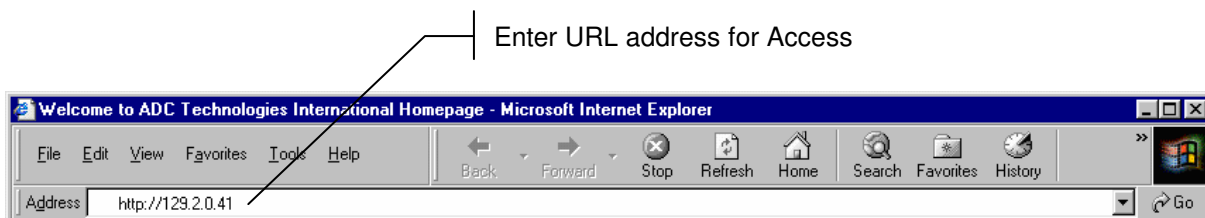
For users accessing the Access Easy Controller using their own computer, please read up on the section *Setting to be made to the Web Browser*.

Logging onto Access Easy Controller

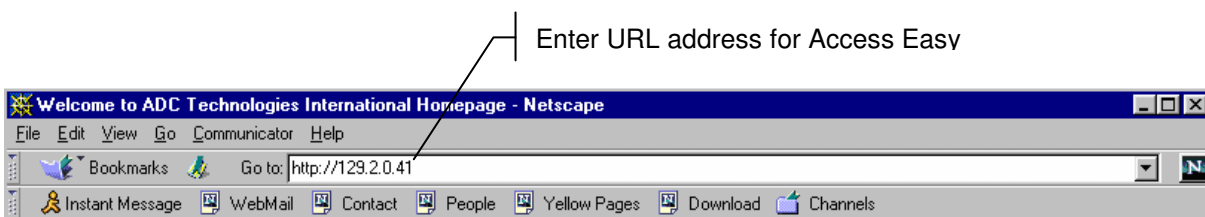
A working knowledge of Windows or Macintosh and the standard web browser program, either Internet Explorer or Netscape Navigator and the ability to manoeuvre with a mouse pointer is required to complete the appropriate screen.

To get connected to Access Easy Controller, run your web browser program and key in the Access Easy Controller's URL address followed by the **Enter** key.

The following screen-capture shows example of some typical web browser page with the default URL address for the Access Easy Controller. The outlook of the screen might differ from what is shown here, this is largely due to the software version in use.



This is a sample of how the screen would look like for user using *Internet Explorer*.



This is a sample of how the screen would look like for user using *Netscape Navigator*.

The *User Login* dialog box appears.

This *User Login* dialog box provides a security control that protects the Access Easy Controller from unauthorised access. It requires a user to enter his or her *User ID* followed by a *Password* before he or she is allowed access to Access Easy Controller. Up to two users are able to log onto the same Access Easy Controller concurrently using different computers.

NOTE: The *Password* is case-sensitive and can be changed.

When the Access Easy Controller is first installed, there is only one assigned *User ID* and *Password*. This default User ID is called the *Super-user* and is usually assigned to the *System Administrator*. For obvious reason, this user has the full access rights to all features of the Access Easy Controller, including the Access Easy Controller Utility programs, and the access rights cannot be disabled. However, the *User ID* and *Password* can be changed.

The default User ID = **user1** and Password = **8088**

NOTE: Once the system is commissioned and handed-over, change the default User ID and Password as soon as possible to prevent unauthorised access.

Logging onto Access Easy Controller

1. Enter your assigned *User ID* in the *User ID* edit box.
2. Enter your assigned *Password*.
3. Click on the **Login** button.

If you do not know your User ID and Password, contact your System Administrator to obtain them. User IDs and Passwords are only configured by the Access Easy Controller System Administrator.

Logging off from Access Easy Controller

After you finish your session with Access Easy Controller or need to be away from the computer, it is recommended to log off from the Access Easy Controller.

To log off, click on the **Logout** link, Click on the appropriate button to proceed.

ALWAYS BACKUP THE DATABASE AND LOG OFF BEFORE LEAVING THE COMPUTER!

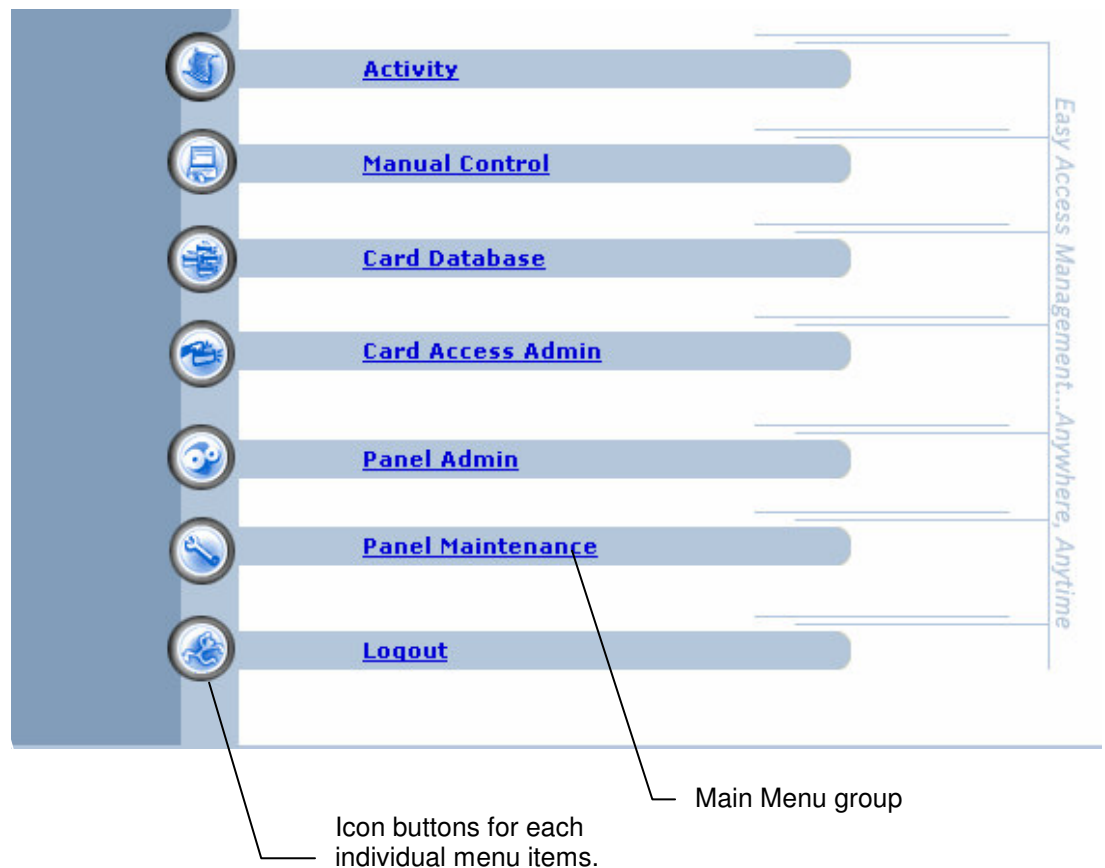
Understanding the Home Page Main Menu Groups

The *Home Page* gives an overview of the main functional features that the Access Easy Controller support and does not contain any parameters setting or data.

For the user convenience, the icon buttons, in line to the main menu group, is linked to the page of the first menu item in the group.

Once in the menu item page, the *Home* page icon button is added to the bottom of the list after the Logout button. This is good for security reason. Should a user is suddenly disrupted while in a middle of setting the Access Easy Controller parameters, for example to answer a phone call, he or she can click the *Home* button to exit the setting without having to click a few times on the *Back* button. This will prevent prying-eyes from looking at the setting.

The screen-capture shown below shows the *Home* page.



Details of the various menu items will be covered in the next following chapters. However, a brief description of each item will be presented here.

View Activity

The **View Activity** menu-item show transactions generated due to access control, system control, and alarm conditions. The transactions are categorised into the following: Alarm, Valid, Restore and Time Attendance. User can view only specific category or All Transactions. Besides showing the transactions, the Date and Time of the Access Easy Controller is indicated on the status bar of the web browser.

Activity Report

This menu-item allows user to generate print preview of the various types Activity Report.

Manual Control

This menu group relates more to manual (user intervention) control of system hardware and consists of the following menu items: **Door Control**, **Input Control**, **Output Control**, and **Reset APB**.

Card Database

Card Assignment set-up the card parameter such as Card Number, Cardholder's name, etc including the right to Arm/Disarm an Alarm Zone.

Access Groups allows user to categorise the Card Readers into different Access Group for Cardholder's access rights.

Card Access Admin

Schedules are used to set-up time intervals for use in access, system and hardware control.

Holidays are used to define and assign programmable holiday dates.

Card Readers are used to define the function of the Reader and its parameters, such as Door Settings, Hardware Setup...

Panel Admin

Users are to set-up the User ID and Password including access rights to the various menu items.

Panel Setup is for setting up of various miscellaneous parameters: -

- Network Settings
- Input Point Configuration
- Set Date & Time
- Auto Logout Timer
- Audit Log
- Default Settings
- Card Format
- Company Profile
- Email/SMS Configuration

Input Setup is used to set-up Alarm Monitoring Point to be armed / disarmed based on Schedule or via an assigned Reader. It also allows the definition of which Output Point(s) to trigger should an alarm is detected.

Output Setup is used to set up the triggering of Output Relay based on Schedules. This can be used to turn on lighting in an area after office hours, for example.

Advance I/O Setup is used to enable the rerouting of physical or logical information from one operation to another.

Database Backup is used to backup (write) all databases into the flash memory of the controller and further download to the hard disk of a PC. User can also define a time to which the Access Easy Controller will perform an automatic backup to the flash memory.

Panel Maintenance

Update Flash is a utility that is used when there is a program upgrade. It's usually carried out for firmware enhancement, new features, or bug fixing. It can also be used for database recovery.

Reboot Panel is used to reboot the Access Easy Controller. It's usually carried out before changes can take effect. Some examples are Access Easy Controller IP Address or during a firmware upgrade.

Shutdown Panel is used to shutdown the Access Easy Controller. It's usually carried out for hardware upgrades..

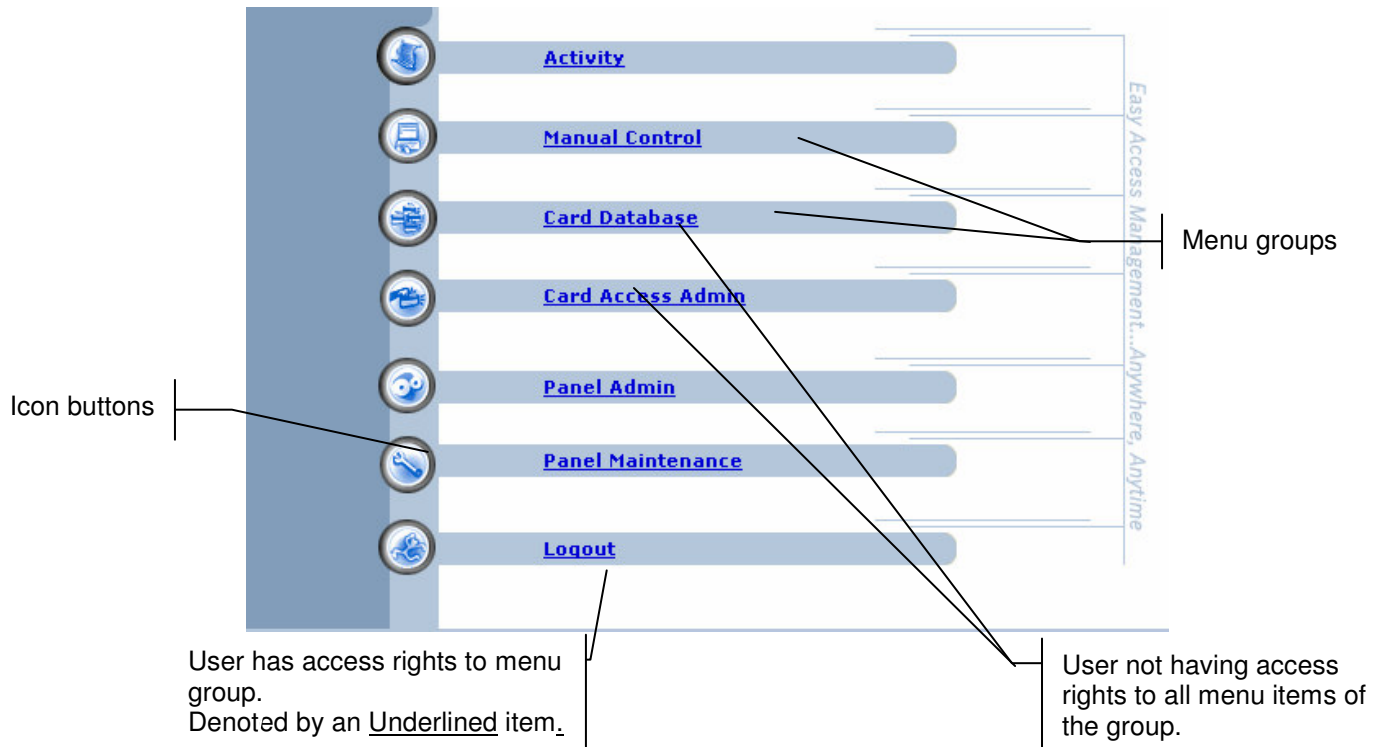
Logout

To log off from Access Easy Controller.

Navigating Through Access Easy Controller page

The following screen-capture shows some sample pages indicating how you can navigate through Access Easy Controller software.

Home Page



Clicking on an **Underlined** menu group would bring you to the first available access-right- menu item web page in the group.

Menu item page

Sub-menu item link.

Panel Admin

Panel Setup

Network Settings

Input Point Configuration

Set Date & Time

Auto Logout Timer

Audit Log

Default Settings

Card Format

Company Profile

Email/SMS Configuration

Email Server Settings

Dial In IP Settings

AEMC Settings

SMS Server Settings

Network Settings

Panel's IP Address: 129 . 2 . 1 . 73

Panel's IP Netmask: 255 . 255 . 0 . 0

Panel's Gateway: 129 . 2 . 0 . 254

Remote PC Address

#	IP Address	PC Name
1	129 . 2 . 0 . 157	remotehost1
2	129 . 2 . 0 . 189	remotehost2
3	129 . 2 . 0 . 43	remotehost3

Menu items are displayed on left pane for ease of operation. The menu groups are those in bright yellow background.

Current menu item page on right pane.

Usage of the buttons

The buttons that appeared at the bottom of each screen can be explained as follows:

Button	Description and Usage
	The save button saves the current settings to the (Dynamic RAM) DRAM and refreshes the current web page.
	The add button provides the following functions: - - It carries out the addition process during a batch card operation. - It also adds a selected parameter to a list window.
	The delete button provides the following functions: - - It deletes all configurable parameters and set it to default. - It also removes a selected parameter from the list window.
	The next button provides the following functions: - - It saves the setting made on the current screen and - It brings up the next screen.
	The list button provides a few function: - - It allows you to go back to the first web page of a menu item. - It can also be use in place of the cancel button to abort changes. However, condition applies that none of the other buttons namely, the next, prev or save is clicked prior to this. - In report generation, the list button is used to obtain a print preview of the report.
	The previous button has similar function as the next button, - It saves the setting made on the current screen and - It brings up the previous screen.
	The reset button provides the following functions: - - It is use to reset APB violation. - It is use to clear the field in the Holiday date setting.
	Abort changes and revert to previously saved settings.

This Page Intentionally Left Blank

CHAPTER 3

View Activity

Every activity transaction such as *Door Forced Opened*, *Door Held Opened*, etc. are captured by Access Easy Controller and displayed on the View Activity web page in real-time mode according to the transaction occurrence date and time. Access Easy Controller has the capability to store 20,479 activity transactions.

On the web page, user is given the option to view one of the following: -

- Alarm Transactions,
- Restore and Alarm Transactions,
- Valid and Alarm Transactions,
- Time Attendance, or
- All Transactions.

Please refer to *Appendix B Activity Transactions* for the transactions in the different groups.

Access Easy Controller can now support real time activities and status update.

Using Java Applet technique, all the activities and status on the manual control pages (Door, Input and Output) will be automatically updated in real time instead of waiting for 30 seconds to refresh.

The Door status will consist of Door Forced Open, Door Held Open, Open, Closed, Request-to-Exit, Door Contact Fault-Open and Door Contact Fault-Short.

The Input status will consist of Alarm, Alarm Restore, High, Low, Fault-Open and Fault-Short.

User can view the latest transactions on screen and make hardcopy of the history via a printer. The number of records to view on screen is configurable by the user up to a maximum of 70 records (see NOTE). Please refer to *Panel Setup, View Activity Setting* for detail on setting the number of transaction records to view on screen.

NOTE: The View Activity web page is dynamic and will expand beyond the “*Number of Transactions to view*” setting to always accommodate transactions, up to 70 records, starting from the first “not acknowledge” alarm transaction up to the latest transaction.

When any of the Alarm Activity transactions is transacted, an alerting audio tone is sent to the Central Monitoring Computer (CMC). Please ensure that the CMC’s audio system is in working order and the volume is set to a reasonable level.

To activate View Activity

There are various ways to activate the View Activity menu item. They are: -

1. From the home page, click on [View Activity](#) hyperlink or its icon button.
2. From any of the menu items page, click on [View Activity](#) hyperlink.
3. From any of the menu items page of the Manual Control Group.

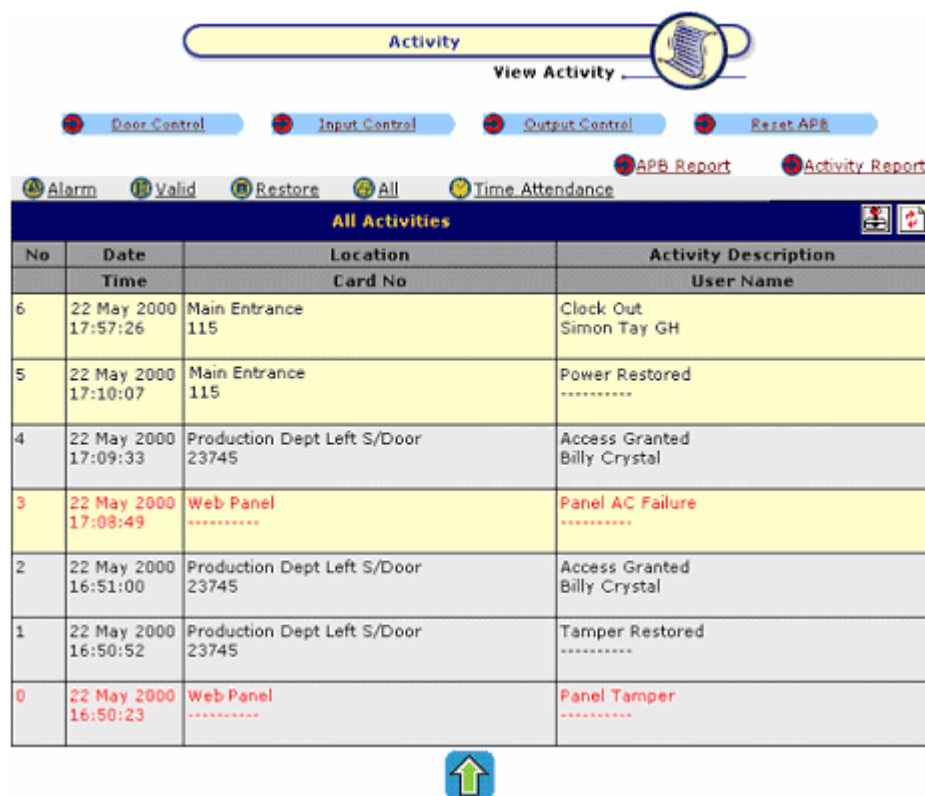
The following paragraphs provide some description of what you will see on the web page. For a detailed list on the different groups of activity transactions, please refer to *Appendix B Activity Transactions*.

 Alarm	To display only the Alarm transactions. Examples of Alarm transactions include Access Denied, Door Held Open, Panel Tamper, Duress, and others. For a detailed list on Alarm transaction, please refer to <i>Alarm Activity</i> in <i>Appendix B Activity Transactions</i> .
 Valid	To display only the Alarm and Valid transactions. Examples of Valid transactions include Access Granted, Turn On, Disarmed, Duration On, and others. For a detailed list on Valid transaction, please refer to <i>Valid Activity</i> in <i>Appendix B Activity Transactions</i> .
 Restore	To display only the Alarm and Restored transactions. Examples of Restored transactions include Door Closed, Tamper Restored, Alarm Restored and Power Restored.
 All	To display All the transactions.
 Time Attendance	To display only Time Clocking transactions. Examples of Time Attendance transactions include Clock In and Clock Out.
	To acknowledge Alarm transactions. This will also silent the audible tones on the CMC.
	To update the web page for the latest transactions.
 APB Report	To obtain a print preview of cardholder(s) who are in the specific APB Zone(s) at the time of the preview. Please refer to the Chapter on Reset APB for detail on print preview of the report.
 Activity Report	To obtain a print preview of the Activity report before printing.
 11:19:43 7 Sep 2000 Thu	Located on the left side of the status bar, it shows the current Access Easy Controller's Time and Date.

The features of activity transactions are as follows:-

- All new transactions have a yellow background.
- All Alarm transactions have red coloured text wording while other transactions have black coloured text wording.
- When the web page refreshes, either automatically or through user intervention, the yellow background is replaced with grey background except for Alarm transactions, which remains unless the  button is activated.

We will explain the web page through an example.



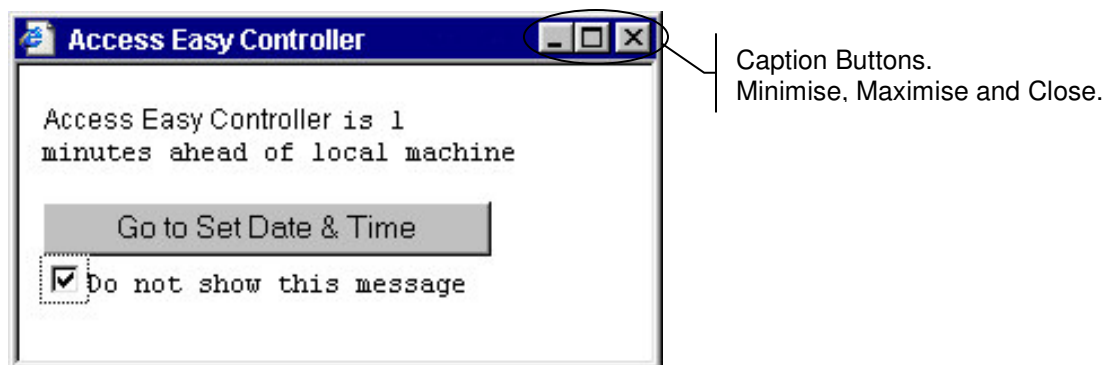
No	Date	Time	Location	Card No	Activity Description
6	22 May 2000	17:57:26	Main Entrance	115	Clock Out Simon Tay GH
5	22 May 2000	17:10:07	Main Entrance	115	Power Restored
4	22 May 2000	17:09:33	Production Dept Left S/Door	23745	Access Granted Billy Crystal
3	22 May 2000	17:08:49	Web Panel		Panel AC Failure
2	22 May 2000	16:51:00	Production Dept Left S/Door	23745	Access Granted Billy Crystal
1	22 May 2000	16:50:52	Production Dept Left S/Door	23745	Tamper Restored
0	22 May 2000	16:50:23	Web Panel		Panel Tamper

Reference to the screen-capture above shows All Activities and the listings in *Appendix B Activity Transactions*.

- No. 6. Shows a new "Clock Out - Time Attendance" transaction.
- No. 5. Shows a new "Restore" transaction (black text wording and yellow background).
- No. 4. Shows a "Valid" transaction.
- No. 3. Shows a "not acknowledge Alarm" transaction (red text wording and yellow background).
- No. 2. Shows a "Valid" transaction.
- No. 1. Shows a "Restore" transaction.
- No. 0. Shows an "acknowledged Alarm" transaction (red text wording and grey background).

In addition to those items mentioned earlier, the Access Easy Controller – Time Difference message box will also appear: -

- The time difference between the computer and the Controller is 1 minute or more, and
- The user was given the access rights (see Chapter on Users) to synchronise the date and time, and
- User is viewing the View Activity web page.



From the message box, you can click on the  button to change the Access Easy Controller's Date and Time.

If you do not wish to synchronise the Date and Time at the moment and find that the message box is obstructing your view, you can disable this message box for this session by checking the check box and closing it using the **Close** caption button. However, the message box will appear again on the next successful log on when the conditions are valid.

To generate a Print Preview of the report

1. Click on the  **Activity Report** link from the **View Activity** web page or **Activity Report** link from any other menu item page.



Activity

Activity Report

Selection Criteria for Activities

Activities:

Card Number:

Name:

Department:

Location:

From: Day Month Year To: Day Month Year

From: Hour Minute To: Hour Minute

This dialog screen allows user to select the types of activity report and also to customise the hardcopy report items based on the combination of *Card Number*, or *Name*, or *Department* with *Location*.

2. Select the Activity types from the list.
3. To generate a print preview of the report based on *All Card Number* and

All Location, just click on the  button.

To format report based on Card Number

1. Enter the exact *Card Number* in the Card Number field.
2. Click on the  button.
If the card number is not in the database, you will be prompted by an error message.
3. Select the appropriate *Readers* from the list. If you want to generate report for all readers, select *All Locations*.
4. Click on the  button for a print preview of the report.

To format report based on Name

1. Enter a character, a portion, or the full name and click on the  button.
If a match is found that satisfied the entry, a window will appear with the Names. For example, enter Thomas and click the  button resulted in:



The screenshot shows a software window titled "Activity Report" with a yellow header bar. Below the header is a section titled "Selection Criteria for Activities" with a dark blue background. The form contains the following fields and options:

- Activities:** A dropdown menu set to "All".
- Card Number:** A text input field containing "1".
- Name:** A text input field that is empty.
- Names Found:** A list box showing search results: "Datuk Thomas (1)", "King Thomas (3)", and "Sir Thomas (4)".
- Department:** A dropdown menu.
- Location:** A dropdown menu set to "All Locations".
- From:** Date and time selection fields. The date is set to 23 Aug 2005, and the time is 00:00.
- To:** Date and time selection fields. The date is set to 30 Aug 2005, and the time is 23:59.

At the bottom of the form, there are two buttons: a blue button with a clipboard icon (print preview) and a blue button with a red 'X' icon (cancel).

2. From the window, select the desired name.
The selected name appears in the *Name* field.
3. Select the appropriate *Location* from the list.
4. Click on the  button for a print preview of the report.

To format report based on Department

1. Enter the exact *Department code* in the Department field.
2. Select the appropriate *Location* from the list.



3. Click on the button for a print preview of the report.

To format report based on Location

1. Select the appropriate *Location* from the list.
2. Click on the  button for a print preview of the report.

A sample of the preview for report based on All Card Numbers and All Locations is shown below.

[Return To View Activity](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Alarm Activities Report

Tuesday, 13 Sep 2005 11:16:24

Card Number : All Card Numbers
Name : All Names
Department : All Departments
Location : All Locations
Start Date : 12 Sep 2005
End Date : 13 Sep 2005
Start Time : 00:00
End Time : 23:59
1-5120 of 20417

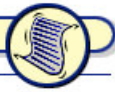


No	Date Time	Location Card No	Activity Description User Name
1	12 Sep 2005 17:34:02	Reader 10 (0) 30	Invalid Card Standard 26-bit Card Format
2	12 Sep 2005 17:34:05	Reader 11 (0) 31	Invalid Card Standard 26-bit Card Format
3	12 Sep 2005 17:34:08	Reader 12 (0) 32	Invalid Card Standard 26-bit Card Format
4	12 Sep 2005 17:34:11	Reader 9 (0) 1	Invalid Card Standard 26-bit Card Format

3. To view other cards activity, click on the  link.
4. To quit and return to *View Activity* screen, click on the [Return To Activity](#) link.
5. To generate a preview of other configuration, click on the [Return To Selection Criteria](#) link.

If you wish to obtain a hardcopy, please proceed to the section, *Printing the report*.

To format report based on Date/Time



Activity

Activity Report

Selection Criteria for Activities

Activities: Alarm ▼

Card Number: 

Name: 

Department: ▼

Location: Motion Detector 2 ▼

From: Day 13 ▼ Month Sep ▼ Year 2005 ▼

From: Hour 00 ▼ Minute 00 ▼

To: Day 13 ▼ Month Sep ▼ Year 2005 ▼

To: Hour 23 ▼ Minute 59 ▼

User can select the range of dates of the activities which he is searching for. This would cut down the time on scrolling through the list of activities if the user knows when the activities have taken place.

A sample of the preview for report for Alarm activities located in “Motion Detector 2” occurring on 13th Sept 2005 from 0000 hr to 2359 hr is shown below.

[Return To View Activity](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Alarm Activities Report

Tuesday, 15 Sept 2005 15:15:15

Card Number : All Card Numbers
 Name : All Names
 Department : All Departments
 Location : Motion Detector 2
 Start Date : 13 Sept 2005
 End Date : 13 Sept 2005
 Start Time : 00:00
 End Time : 23:59

1-3 of 3

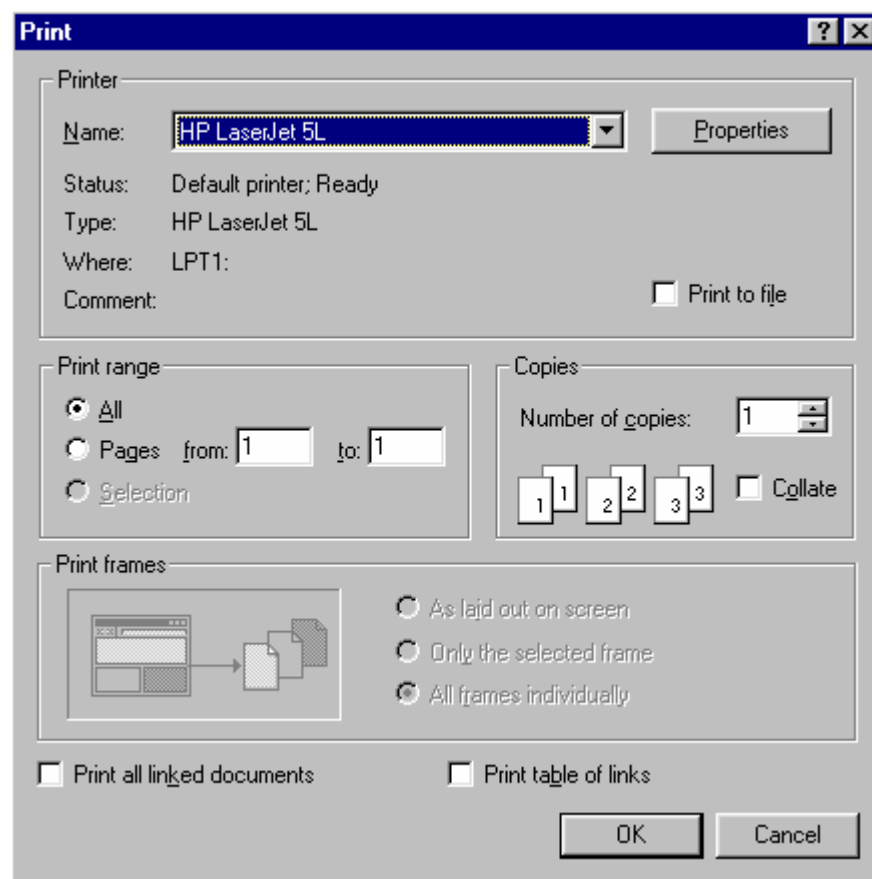
No	Date Time	Location Card No	Activity Description User Name
1	13 Sept 2005 10:13:55	Motion Detector 2 -----	Alarm -----
2	13 Sept 2005 10:15:58	Motion Detector 2 -----	Alarm -----
3	13 Sept 2005 16:11:11	Motion Detector 2 -----	Input Point Fault - Shorted -----

 BOSCH SECURITY SYSTEMS

Printing the report

During the preview, the report can be sent to printer for printing. The printing process is the same as any Windows 95/98/NT or Win 2000/XP software application printing. As such, it is very straightforward.

From the *Menu* bar, click on *File* and select *Print...*
The *Print* dialog box appears.



Make the appropriate selection and click on the **OK** button.

CHAPTER 4

Card Assignment

This chapter describes the features of the Card Assignment function and the set up procedure.

Card parameters are parameters that control the use of cards. It contains information such as which card reader a cardholder can access at specified *Schedule*. There will be some extra fields for user to configure additional card information like Department, Telephone...etc. *Card Assignment* consists of the following parameters: -

- **Card Details**
 - Card Number
 - Facility Code
 - Card Format
 - User Name
 - Department
 - User Field 1 and 2 (user definable field)
 - Access Groups A and B
- **Card Functionality**
 - Cardholder Arm/Disarm rights
 - Card Operations
 - Card + PIN Operations
 - User PIN
 - Card Validation Period
 - Dual Card Assignment

NOTE 1: Access Easy Controller supports a maximum capacity of 20,480 cardholders.

NOTE 2: As the Access Easy Controller is able to support different types of *Card Format*, whether 26-Bits, or other customised format, there will be overlapping of *Card Number* range. It is possible to assign same Card Number(s) but with different Facility Code. The Access Easy Controller will process the *Facility Code* (if any) together with the *Card Number*.

To activate Card Assignment

The *Card Assignment* can be activated only from the menu item page.

1. From any menu item page, click on Card Assignment hyperlink.

Card Database

Card Assignment

Search:

Option:

Batch Cards:

Empty Slot:

Select a CSV file:

Card ID Range:

ID	Card #	Name
1	1	John d'Baptist
2	2	Karen
3	3	Ivan
4	4	John
5	5	Eric
6	6	Jason
7	7	Yvonne
8	8	Ruth
9	9	Keline
10	10	Sean
11	11	Thomas
12	12	Daniel

To view different sets of Card range

To view different sets of card ID range, click on the pull down list and select the range that you want. For example, to view ID listings from No. 201 – 300, click on the pull down list and click the 201-300 range as shown below.

1-100

1-100

101-200

201-300

301-400

401-500

501-600

601-700

701-800

801-900

901-1000

1001-1100

NOTE : Access easy controller supports a maximum of **20,480** cardholders.

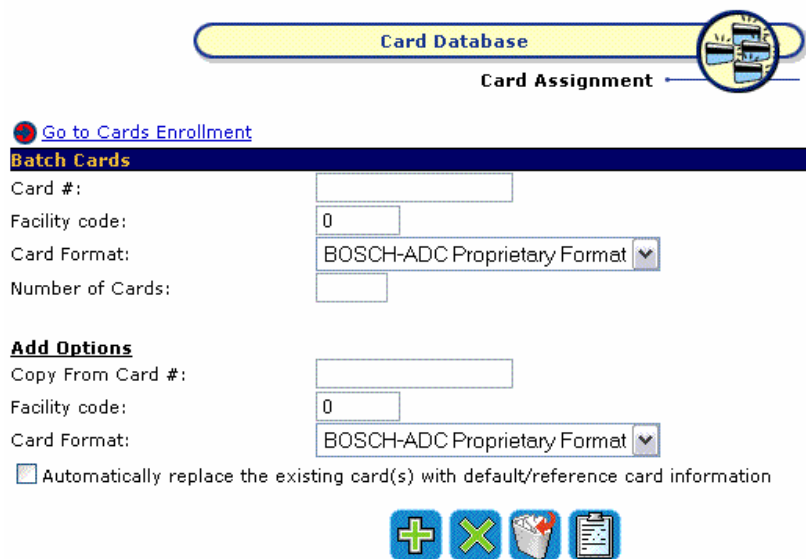
Adding/Deleting a range of Card Numbers

This feature allows user to add/delete a single card or a block of card numbers. The Access Easy Controller software will search the database and assigned the card numbers to empty slots when *adding* and will set all parameters within a card number to default during a card *deletion*.

NOTE: Please proceed to edit Card number information/parameters thereafter when adding card numbers.

To add a Batch of Card Number

1. Click on the  button for *Batch Cards*.



The screenshot shows the 'Card Database' window with a 'Card Assignment' button circled. Below it, the 'Batch Cards' section is active, displaying fields for Card #, Facility code, Card Format, and Number of Cards. The 'Add Options' section below it includes a 'Copy From Card #' field, Facility code, Card Format, and a checkbox for 'Automatically replace the existing card(s) with default/reference card information'. At the bottom, there are four icons: a green plus sign, a green X, a trash can, and a clipboard.

2. Enter the card number in the *Card #* field (the number specified here will be the starting number of the batch card operation and will be included).
3. The number in the Facility code is configured in *Panel Setup, Default Settings*, if the code is different from the default, then change it. Please refer to the section on Default Settings for detail. Enter 0 if the *Card Format* doesn't support *Facility Code*.
4. Select the appropriate *Card Format* from the list. The configuration of the *Card Format* is carried out under the *Panel Setup, Card Format*. Please refer to the section on Card Format for detail.
5. Enter the number(s) of card number to add in the *Number of Cards* field.
6. Click on the  button.

If there is no error during the card numbers addition, the **Cards added successfully** message would be shown. Please refer to the section on *System Messages* if other message is shown instead.



7. Click on the  button to return to the menu item first page.
8. Proceed to edit the newly added card number parameters.

To delete a Batch of Card Number

The procedures to *Delete* a range of card numbers is similar to *Adding* a

Batch of Card Numbers. Instead of clicking on the  button, click on the  button.

WARNING! Exercise care in the usage of this function, as it is not reversible. All information will be permanently erased from the database once it is carried out.

To add a Batch of Card Number with same data entries

This function allows addition of a range of card numbers with data entries copied from a reference card number (see NOTE below). All card number(s) added will be copied with the data / parameters of the reference card. However, the following parameters will not be copied, *Facility code*, *Card Format* and *Username* as all these parameters relates to the individual card and cardholder.

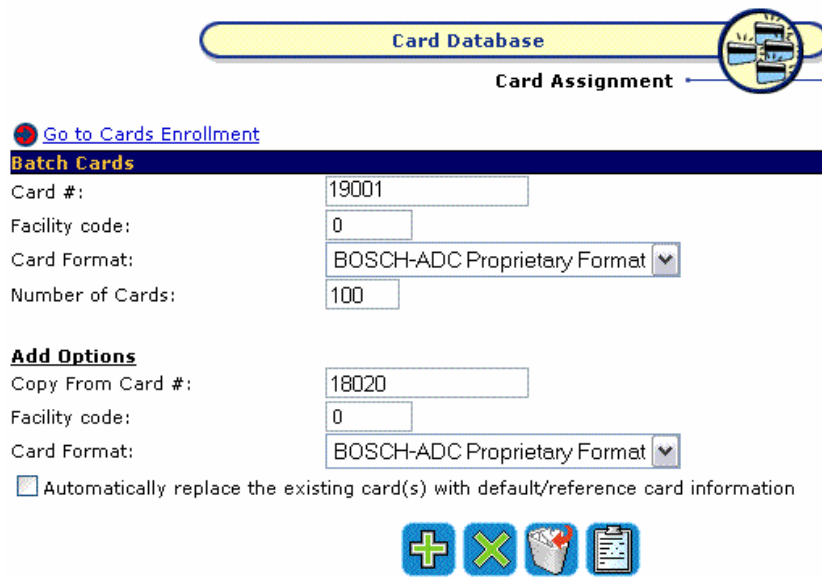
NOTE: In order for the process to be carried out, the reference card number entered must be **exact** in term of *Card Number*, *Facility Code* and *Card Format*. The Controller will prompt the user with an error message if a non-existence reference card number is specified.

This is very useful and time saving when assigning a batch of card number to a specified department staff, for example.

To assign the cards, with number ranging from 19001 to 19100, to staff in the Production department. This batch of card number has the *Facility Code* of 0 and is of *BOSCH-ADC Proprietary Card Format*. Using card number 18020 from Production department to be our reference for the new card range setting proceed as follows: -

NOTE: The Card Number 18020 is of *BOSCH-ADC Proprietary Card Format* with *Facility Code* of 0. It is used as a reference as we wanted to set similar parameters for the new card numbers such as Access Group(s), ...etc.

1. Click on the  button for *Batch Cards* and enter the relevant fields as shown.



[Go to Cards Enrollment](#)

Batch Cards

Card #: 19001

Facility code: 0

Card Format: BOSCH-ADC Proprietary Format

Number of Cards: 100

Add Options

Copy From Card #: 18020

Facility code: 0

Card Format: BOSCH-ADC Proprietary Format

☐ Automatically replace the existing card(s) with default/reference card information

2. Click on the  button to proceed.
A message will appear. Refer to the next section on *System Messages* to interpret the meaning of the message.
3. Proceed to edit the newly added card number parameters.

Using Automatically replace the existing card(s) with default/reference card information function

This function will overwrite all data within a card number when the software encounters existing card number (with same Card Format and Facility Code) during *Batch Cards* function. It allows recycling of card number allocation when employee resigns.

The function will be activated when a tick (✓) appears in the check box.

WARNING! Exercise care in the usage of this function, it is not reversible. All information on the existing card number in the database will be permanently overwritten once it is carried out.

Cards Enrolment Operation

This function is to facilitate selected card holders to have the right to use their card to activate a Reader to be in enrolment mode.

Card Enrolment of Card with Unknown Wiegand Format

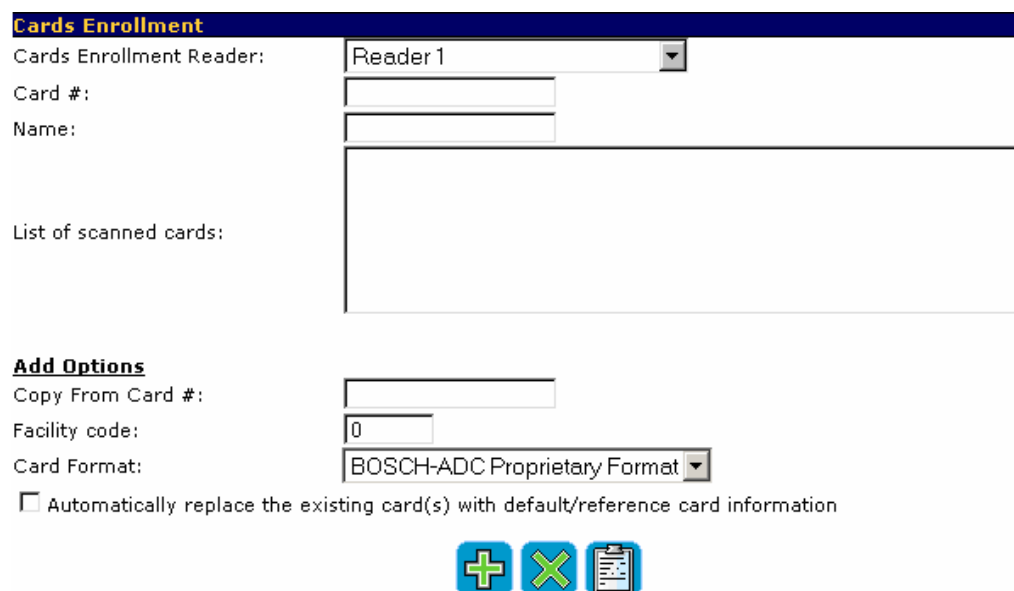
To use any unknown proprietary wiegand card format, administrator can activate a Reader, either by pre-assigned enrolment card or by web page, to be in enrolment mode and enrol any card into the card database (maximum bit length is 64). The sections below will guide the administrator on how to activate a Reader to be in enrolment mode, both by enrolment card and by web page.

Card Enrolment Using Web Page

If the administrator chooses to enrol a card of unknown proprietary wiegand card format using the web page, he should follow the steps below.

1. To go to the page as shown below, select *Card Assignment* from the Left Pane, followed by *Batch Cards*  at the top-right corner, and lastly select *Go to Cards Enrolment*  [Go to Cards Enrolment](#).

The screen as shown below will appear.



2. Select a Reader to be the enrolment Reader. In this example, we select Reader 1 to be the enrolment Reader.
3. Click on the  button to activate the selected Reader as the enrolment Reader.

- Present the card with unknown Wiegand Format to the enrolment Reader, which is Reader 1 in this example.

The card that has been presented to the enrolment Reader will appear in the box for *List of scanned cards*, as shown in the screen below.

Cards Enrollment	
Cards Enrollment Reader:	Reader 1
Card #:	
Name:	
	01 0x0000000002E3DE70 26
List of scanned cards:	
Add Options Copy From Card #: Facility code: 0 Card Format: BOSCH-ADC Proprietary Format ☐ Automatically replace the existing card(s) with default/reference card information	
  	

- The administrator can now assign any Card # and Name to the card. In the screen below, the Card # is assigned as 1208 and the Name of the cardholder as Julia Chua.

NOTE It is recommended that the administrator assigns a number to the card of unknown wiegand format beforehand and sticks a label on the card, so that it is easier to refer to the card number during the card enrolment process.

Cards Enrollment	
Cards Enrollment Reader:	Reader 1
Card #:	1208
Name:	Julia Chua
	01 0x0000000002E3DE70 26
List of scanned cards:	
Add Options Copy From Card #: Facility code: 0 Card Format: BOSCH-ADC Proprietary Format ☐ Automatically replace the existing card(s) with default/reference card information	
  	

- Highlight the card in the *List of scanned cards* that you are assigning the Card # and Name to, as shown in the screen below.

Cards Enrollment

Cards Enrollment Reader: Reader 1

Card #: 1208

Name: Julia Chua

01 0x00000000002E3DE70 26

List of scanned cards:

Add Options

Copy From Card #:

Facility code: 0

Card Format: BOSCH-ADC Proprietary Format

☐ Automatically replace the existing card(s) with default/reference card information



7. Click on the  button to add the card with the assigned Card # and Name to the database.

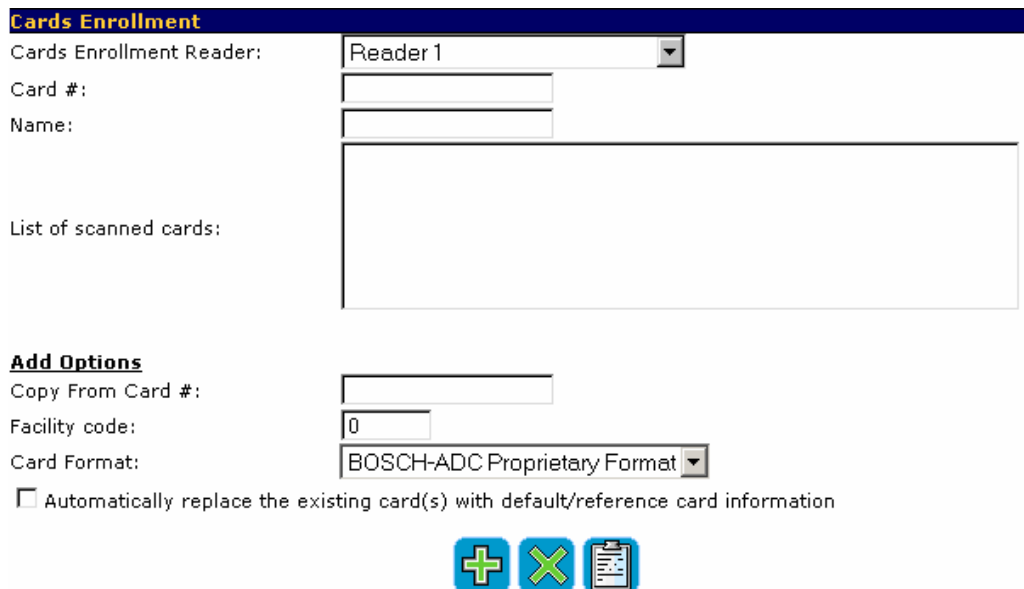
Card Enrolment Using Pre-Assigned Enrolment Card

A pre-assigned enrolment card is a user card that has been checked with the option Card Holder Can Enable Enrolment Operation. For the details on how to set a card to be a pre-assigned enrolment card, refer to the section *Card Holder Can Enable Enrolment Operation* above.

If the administrator chooses to enrol a card of unknown proprietary wiegand card format using pre-assigned enrolment card, he should follow the steps below.

1. To go to the page as shown below, select *Card Assignment* from the Left Pane, followed by *Batch Cards*  at the top-right corner, and lastly select *Go to Cards Enrolment*  [Go to Cards Enrolment](#).

The screen as shown below will appear.



Cards Enrollment

Cards Enrollment Reader: Reader 1

Card #:

Name:

List of scanned cards:

Add Options

Copy From Card #:

Facility code: 0

Card Format: BOSCH-ADC Proprietary Format

☐ Automatically replace the existing card(s) with default/reference card information

2. Present the pre-assigned enrolment card to a Reader. The Reader is now activated to be in enrolment mode. If the pre-assigned enrolment card also has access right to the Reader, press key <7> on the Keypad before presenting the pre-assigned enrolment card.
3. Present the card with unknown Wiegand Format to the enrolment Reader. If key <7> is pressed before presenting the pre-assigned enrolment card, the timing on *Keypad Timeout* will have to be observed. This means that when a pre-assigned enrolment card is presented to the Reader to activate the Reader as an enrolment Reader, the new card to be added to the panel has to be presented to the same Reader within the timing set in *Keypad Timeout*. Failure to do so will cause the Reader to return to normal mode. For the setting of timing on the Keypad Timeout, please refer to *Chapter 16 Card Readers, Keypad Timeout*.

The card that has been presented to the enrolment Reader will appear in the box for *List of scanned cards*, as shown in the screen below.

Cards Enrollment

Cards Enrollment Reader: Reader1

Card #:

Name:

01 0x00000000002E3DE70 26

List of scanned cards:

Add Options

Copy From Card #:

Facility code: 0

Card Format: BOSCH-ADC Proprietary Format

☐ Automatically replace the existing card(s) with default/reference card information

4. To add in the new card to the card database, refer to *Steps 5 ~ 7* in the section *Card Enrolment Using Web Page* above.

System Messages

The following are sample of the other messages displayed when carrying out the *Batch Card* function.

Card numbers already exist.

This message indicates that the card number, having the same Facility code and Card Format, already exist in the database and the *Overwrite* function was not activated.

Card database full. 3 cards starting from card number 20479 were not added.

This message appears when an attempt is made to add in more *Card number* when the card database is already full. It indicates the card number and number of card(s) not added, in this example, card number *20480*, *20481*, and *20482* was not added.

Card not found.

This message indicates that the Card number specified during a batch card deletion does not exist and the deletion could not proceed.

Cards deleted successfully.

This message indicates that all Card Numbers specified during a batch card deletion has been carried out successfully.

5 cards deleted.

This message indicates that only 5 Card Numbers out of the Number of Cards specified during a batch card deletion was carried out successfully. The remaining card numbers doesn't exist in the database.

3 cards added successfully.

This message indicates that only 3 Card Numbers out of the Number of Cards specified during a batch card addition was added successfully. The remaining card numbers already exist in the database and the *Overwrite* function was not activated.

Unable to perform add operation.

This message appears when the *Card Number* or the *Number of Card* field was not specified during the add operation.

Unable to perform delete operation.

This message appears when the *Card Number* or the *Number of Card* field was not specified during the delete operation.

Reference card not found.

This message shows that the user has made reference to a non-existence card number.

Editing the Card parameters

Before the Cardholder can use his/her card to gain access, the System Administrator must configure the card parameters into the Access Easy Controller Card Database.

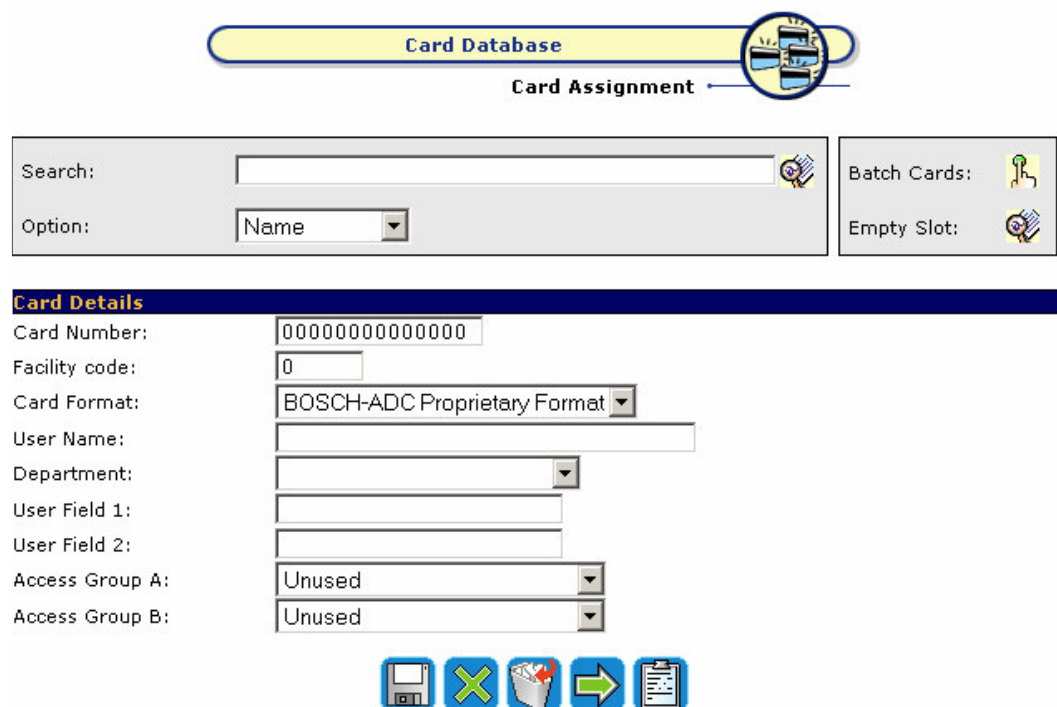
To add or edit Card Number parameters

Card Assignment is used frequently for new employee or employee who resigned from the company.

NOTE: If Card Numbers are added using the *Batch Cards* feature, the System Administrator only needs to edit part of the Card Details section. Please proceed straight to step 5.

Card Details

1. Click on either the numbering under the *ID, Card #*, the text in the *Name* title or empty slot icon  to add a new card or proceed with the editing.



Card Database

Card Assignment

Search:

Option:

Batch Cards: 

Empty Slot: 

Card Details

Card Number:

Facility code:

Card Format:

User Name:

Department:

User Field 1:

User Field 2:

Access Group A:

Access Group B:

2. Highlight the default Card Number and enter the new *Card number*.
3. The number in the Facility code is configured in *Panel Setup, Default Settings*, if the code is different from the default, then change it.

NOTE: The *Card Number* together with the *Card Format* and *Facility Code* is a unique field, so do not enter the duplicate information.

4. Select the appropriate *Card Format* from the list.

NOTE: The Card Format and its Description is configured in *Panel Setup, Card Format*. Please refer to the section for detail.

5. Enter the *Cardholder's (User) Name* in the *User Name* field.
6. Enter the *Department* code (limited to 4 characters).
7. Enter the appropriate detail in *User Field 1*
8. Enter the appropriate detail in *User Field 2*

NOTE: The *User Field 1* and *2* is defined under *Panel Setup, Default Settings*. Please refer to the section for detail.

9. Select the appropriate Access Grouping for *Access Group A* and/or *B* from the list. Leave the entry as *Unused* if there is only one or no assignment.



10. Click on the button to proceed with card functionality configuration.

Card Functionality

Card Functionality consists of the Arm/Disarm access rights, access behaviour and validation dates. Each card can be configured to behave differently. However, some settings would only be activated with the co-ordination of the *Card Readers* parameters such as Card + PIN mode.

Card #: 61240

Name: May

Card Functionality

☐ Card holder is able to Arm/Disarm Alarm Zone 1

☒ Card holder must abide by holiday schedules (to work in conjunction with Reader Options)

☒ Allow exit reader usage only in accordance with time schedules

☐ Card holder can enable enrollment operation

☐ Disable card from all access permanently

☐ Card holder with one time access only

☒ Card + PIN is required on keypad readers

Enter user PIN (1-7 digits):

Extended duration for door access: seconds

Access Status: ☒ Valid ☐ Expired

Card Validation Dates:

☐ Start Date Day: Month: Year:

☐ End Date Day: Month: Year:

Dual Card Assignment:

☐ Dual Card not assigned

☒ Dual Card presentation sequence Second Card

Dual Card Group ID:



Cardholder is able to Arm/Disarm

If this feature is checked, it implies that the cardholder is given the authority to arm/disarm a specific Alarm Zone or All Alarm Zone as defined in the field.

This functionality works in conjunction with the reader that is set to arm/disarm the alarm zone. Refer to *Chapter Card Reader, Entry and Arm/Disarm Reader* for details.

If this function is enabled on the cardholder, when he press '0' on the reader keypad and then present his card, the alarm zone will toggle from arm to disarm or vice versa. However if he just present his card to the reader without activating the arm/disarm function on the reader keypad, it will unlock the door depending on his access right.

Cardholder must abide by holiday schedules (to work in conjunction with Reader Options)

This mode must be checked if the cardholders' access rights are different during holidays. It is to work in conjunction with the *Reader Options, On holidays, follow holiday schedules*. If both are checked, the 4 sets of *Regular or Special Holiday* schedules (on the Access Group) are used to operate the access mode, e.g. Cardholder is allowed to access the controlled area during weekdays and during office hours. However, during holiday, cardholders are only allowed to access this area as defined by the Holiday schedule intervals.

If the *Reader Options* is not checked, cardholder's access rights to the reader will follow the Schedule intervals for weekdays.

Allow exit reader usage only in accordance with time schedules

This mode is valid only if there is an exit reader. When this mode is selected, the Reader will allow the cardholder to exit within his/her valid Schedule intervals. When it is not selected, the reader will allow the cardholder to exit the area at all times (no matter whether the valid time interval has expired or not).

Card holder can enable enrolment operation

This function is to facilitate selected card holders to have the right to use their card to activate a Reader to be in enrolment mode. Please refer to the above section *Card Enrolment Operation* for more details.

Disable card from all access permanently

When this mode is selected, user card will be denied access from the system immediately. This feature is useful to prevent illegal access to the system should the user lost/misplaced the card

Card holder with one time access only

This will enable the administrator to assign cardholder with only one time access to the system. This means that after the card holder has gained access, his access will become invalid immediately. To gain access again, he needs to request the administrator to reactivate the one time access

right again. This function will be useful in a remote station delivery application.

Ensure that the *Valid* radio button is selected for the *Access Status*. After the card has been used for one time access, the *Access Status* will expire immediately and the *Access Status* will be updated to *Expired* automatically.

Card + PIN is required on Keypad readers

This mode works only when the Card Reader's PIN mode is set. The cardholder is required to enter the PIN code, besides presenting his/her card, before access is granted. User could configure up to 7 digit for the PIN, if the user uses less than 7 digit as the pin, for example "5566". When using it on the reader, he should enter the PIN follows by the "E" for C3 readers and S-Series reader or "#" for HID compliant readers. For the above example, the user will need to enter "5566#" for his PIN.

Enter user PIN (1-7 digits)

This field is to be used for the Card + PIN mode (default PIN code 1234000).

Extended duration for door access

This function is to facilitate special card holders to have extended duration for Door Strike and Keypad Timeout. This feature will allow the cardholder to keep the door open for a longer time after a successful access grant before a Door Held Open alarm is activated. The Keypad Timeout duration is also extended by the selected time on top of the normal Keypad Timeout duration. An example of such an application is for the handicapped person who needs a longer time to access the door.

To select the extended time duration, select the time in seconds on the list box seconds beside the *Extended duration for door access*. The range is from 0 to 255 seconds.

Card Validation Dates

This feature defines the start and end date parameters.

Card Validation Dates

☒ Start Date	Day: 01	Month: Jul	Year: 2004
☒ End Date	Day: 31	Month: Dec	Year: 2004

The Start Date is the date from which the card is valid and End Date is the date from which the card is no longer valid. The card will not be able to access any door before the Start Date and after the End Date.

Cards having such parameter settings are normally issued to contractors or temporary staff who will only be allowed to access the controlled area for a known period of time.

The usage of this feature can be either one or the combination of both. You can define a card that only allow access after a specified future date but doesn't have an expiry date. In this case, you only select and set the *Start Date* but leave the *End Date* unchecked.

Alternatively, you can define a card that is valid with immediate effect but is valid only for 2 days, in this case you can leave the *Start Date* unchecked but checked and select the *End Date*.

NOTE User must check the respective box for Start Date or End Date in order for it to be effective.

Dual Card Assignment

This mode is useful if 2 cards are required to be presented in sequence to the Reader to unlock the door. This mode work in conjunction with *the Dual Card Configuration* in the *Chapter, Card Reader*. The First Card has to be presented first before the Second Card is presented, else the door will not unlock. A Don't Care Card can act as the first or second card. In this setup here, the user will need to define whether a card is a First Card, Second Card or Don't Care Card, and which group it belongs to. Cards from different groups cannot unlock the door.

Dual Card Assignment

☒ Dual Card not assigned
☐ Dual Card presentation sequence Don't Care
 Dual Card Group ID (1-255) 1

Select the radio button *Dual Card presentation sequence* to enable this mode. User will need to define whether a card is a First Card, Second Card or Don't Care Card from the list box First Card. User will also have to select the *Dual Card Group ID* from the list box 1. 2 cards from the same Dual Card Group ID must be presented to the Reader to unlock the door. All the possible card combinations that can be presented to the Reader is shown in the table below.

Possible card combination	
First card	Second Card
Don't Care	Don't Care
First Card	Don't Care
Don't Care	Second Card
First Card	Second Card

To select Card Functionality

1. To select the various **Card Functionality**, click on the corresponding check boxes to show a tick (✓) mark. To de-select the point, click on it again.
2. To assign the **Alarm Zone**, select the appropriate Alarm Zone from the list.
3. To edit **User PIN code**, highlight the default PIN code and enter the new *User PIN code*. See NOTE 1 and 2.

NOTE 1: User can enter from 1 to 7 digits for the *User PIN* code.

NOTE 2: For security reason, every character entered for the PIN code is represented by an asterisk (*). For *Macintosh* user, it is represented by a dot (.) instead.

To select and edit Card Validation Period

1. To enable the *Start Date*, click on the *Start Date* check box to show a tick (✓) mark. To de-select, click on it again.
2. Select the appropriate *Day* from the list.
3. Do likewise for the *Month* and *Year* field.
4. To enable the *End Date*, click on the *End Date* check box to show a tick (✓) mark. To de-select, click on it again.
5. Repeat steps 2 and 3 for *End Date*.

NOTE: Date setting will not be updated if the corresponding check box is not checked. It will revert to the previous setting.

To Select and edit dual card assignment

This is applicable to both *After using 2 card to initiate the access, the system will switch back to single card access and Dual Card access at all time.*

Dual Card Assignment:

☒ Dual Card not assigned
☐ Dual Card presentation sequence
 Dual Card Group ID (1-255):

First Card

First Card
 Second Card
 Don't Care

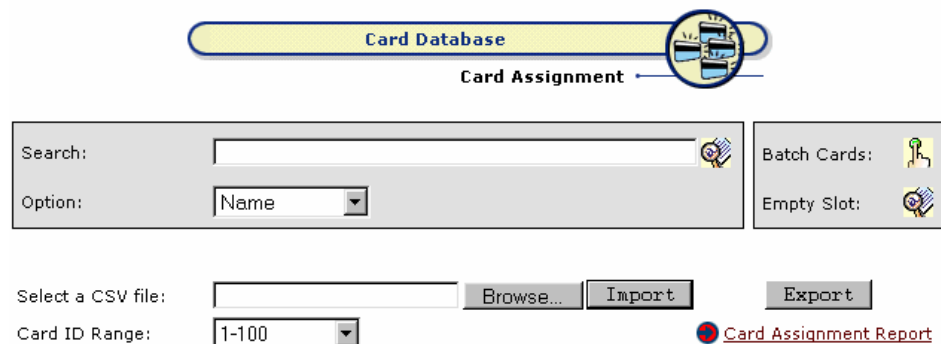
1. Go to *Card Assignment, Card Functionality, Dual Card Assignment*.
2. Select the *Dual Card presentation sequence* radio button and choose whether the card is a First Card or Second Card. If no sequence is required, select Don't Care.
3. Also select the Dual Card Group ID from the drop-down box.

Card Database Import and Export Function (In CSV Format)

This feature is to facilitate the administrator to have the flexibility of exporting and administering card database in a familiar CSV format before importing it back into the controller.

It is also used as a backup and restore utility.

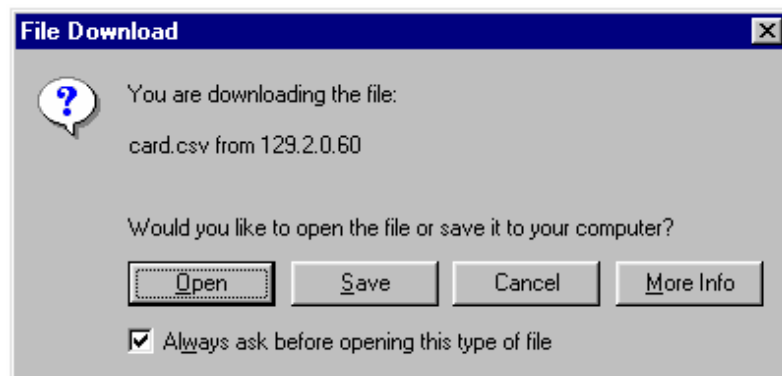
To go to the Card Database Import and Export page, select *Card Assignment*. A screen as shown below will appear.



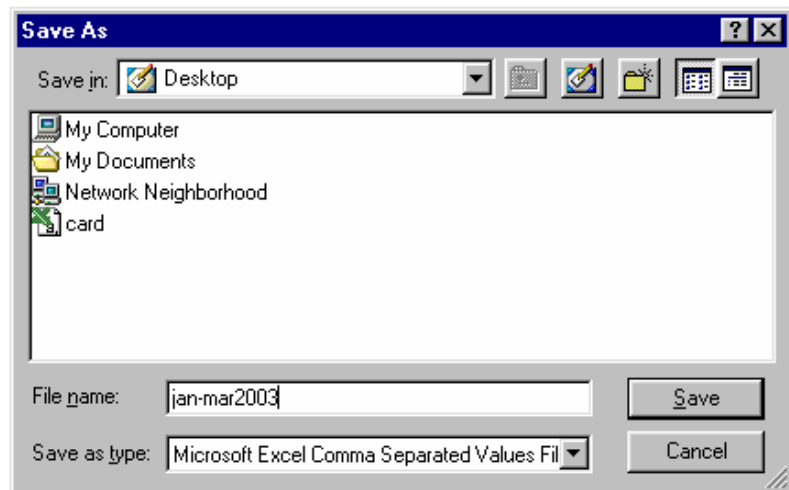
Exporting the Card Database

For the steps on exporting the card database, refer to the steps below:-

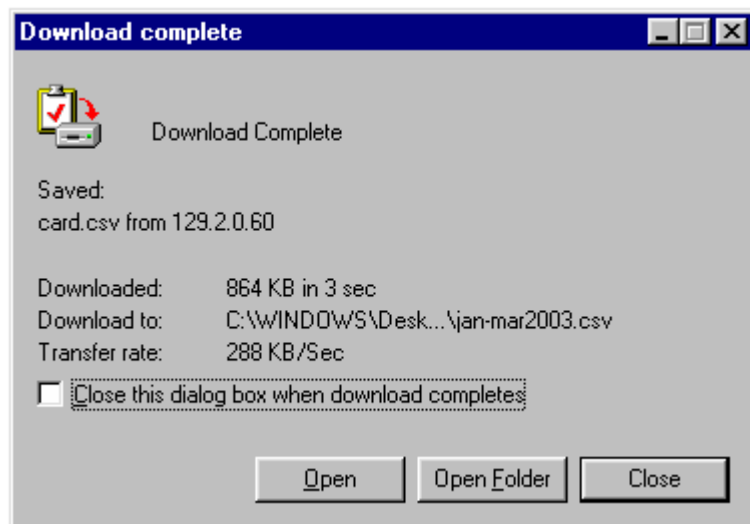
1. To export the card database, click [Export]. A screen as shown below will appear.



2. To open the file, click [Open]. To save the file to a local hard disk or an external drive, click [Save]. When [Save] is clicked, the screen as shown below will appear.



3. Select the drive you want to save the file in and give an appropriate File Name for the file saved. Now you can click on [Save].
4. After the download of the file is completed, the screen as shown below will appear.

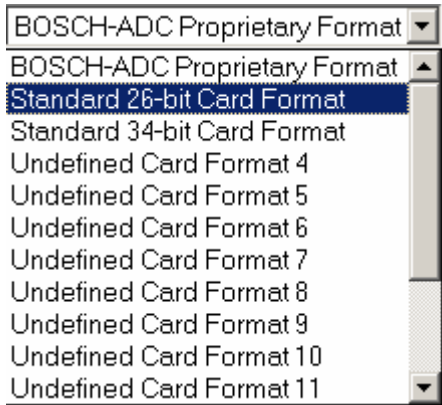


5. To view the file now, click [Open], else click [Close].

A sample of the file saved is as shown below.

Microsoft Excel - card database														
File Edit View Insert Format Tools Data Window Help														
O32 = 0														
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Card Num	Facility co	Card Form	User Name	Departmen	User Field	User Field	Access Gr	Access Gr	Binary	Length	ArmDisarm	Holiday Sc	Allow Exit
2	*****	*****	*****	*****	*****	*****	*****	*****	*****	*****	*****	*****	*****	*****
3	1	0	2	Vincent Lin	0			0	255	2E+14	26	255	1	1
4	2	0	2	William Si	0			0	255	4E+14	26	255	1	1
5	3	0	2	Y. Y. Choc	0			0	255	7E+14	26	255	1	1
6	4	0	2	Seng Chor	0			0	255	8E+14	26	255	1	1
7	5	0	2	Tan Yam L	0			0	255	0b0000000	26	255	1	1
8	6	0	2	C. S. Chev	0			0	255	0d0000000	26	255	1	1
9	7	0	2	Gow Huey	0			0	255	0.00E+00	26	255	1	1
10	8	0	2	Jane Smith	0			0	255	1E+15	26	255	1	1
11	9	0	2	Anna Kara	0			0	255	1.3E+15	26	255	1	1
12	10	0	2	Tony Harri	0			0	255	1.5E+15	26	255	1	1

The following details are saved in the database:

Card Number	- Limited to a length of 14 digits, consisting of 0 ~ 9.																		
Facility Code	- Limited to a length of 5 digits, consisting of 0 ~ 9.																		
Card Format	- Can be BOSCH-ADC Proprietary Card Format, Standard 26 bit Format or any other format, configurable up to a total of 16 types of card formats. '2' in the Card Format column in the exported CSV file represents the second listed card format in AEC. In this example, '2' represents 'Standard 26 bit Format', as shown below. 																		
User Name	- Limited to a length of 30 alphanumeric characters, including digits, alphabets, symbols such as # & [] and space.																		
Department	- Configurable up to 255 departments. '0' in the Department column in the exported CSV file means that department is NOT selected for the cardholder. '1' would mean that the department is the first listed in AEC. In this example, '1' represents 'R&D Department', as shown below. <table border="1"> <thead> <tr> <th>Department #</th><th>Description</th></tr> </thead> <tbody> <tr> <td>*1</td><td>*R&D Department</td></tr> <tr> <td>*2</td><td>*Accounts Department</td></tr> <tr> <td>*3</td><td>*Engineering Department</td></tr> <tr> <td>*4</td><td>*Service Department</td></tr> <tr> <td>*5</td><td>*Project Department</td></tr> <tr> <td>*6</td><td>*Production Department</td></tr> <tr> <td>*7</td><td>*Sales/Marketing Department</td></tr> <tr> <td>*8</td><td>*Purchasing Department</td></tr> </tbody> </table>	Department #	Description	*1	*R&D Department	*2	*Accounts Department	*3	*Engineering Department	*4	*Service Department	*5	*Project Department	*6	*Production Department	*7	*Sales/Marketing Department	*8	*Purchasing Department
Department #	Description																		
*1	*R&D Department																		
*2	*Accounts Department																		
*3	*Engineering Department																		
*4	*Service Department																		
*5	*Project Department																		
*6	*Production Department																		
*7	*Sales/Marketing Department																		
*8	*Purchasing Department																		
User Field 1	- Limited to a length of 20 alphanumeric characters, including digits, alphabets, symbols such as # & [] and space. When User Field 1 is configured as 'Home Tel', the heading 'User Field 1' in the exported CSV file would appear as Home Tel. And for example, the Home Tel of Vincent Lim is 67725490. In the CSV file, it will appear as shown below.																		

	<table><tr><th>D</th><th>E</th><th>F</th><th>G</th></tr><tr><td>User Name</td><td>Department</td><td>Home Tel</td><td>User Field 2</td></tr><tr><td>*****</td><td>*****</td><td>*****</td><td>*****</td></tr><tr><td>Vincent Lim</td><td>0</td><td>67725490</td><td></td></tr><tr><td>William Sim</td><td>1</td><td></td><td></td></tr><tr><td>Y. Y. Choo</td><td>0</td><td></td><td></td></tr><tr><td>Seng Chong Sing</td><td>0</td><td></td><td></td></tr><tr><td>Tan Yam Ling</td><td>0</td><td></td><td></td></tr></table>	D	E	F	G	User Name	Department	Home Tel	User Field 2	*****	*****	*****	*****	Vincent Lim	0	67725490		William Sim	1			Y. Y. Choo	0			Seng Chong Sing	0			Tan Yam Ling	0										
D	E	F	G																																						
User Name	Department	Home Tel	User Field 2																																						
*****	*****	*****	*****																																						
Vincent Lim	0	67725490																																							
William Sim	1																																								
Y. Y. Choo	0																																								
Seng Chong Sing	0																																								
Tan Yam Ling	0																																								
User Field 2	- Limited to a length of 20 alphanumeric characters, including digits, alphabets, symbols such as # & [] and space. When User Field 2 is configured as 'Mobile', the heading 'User Field 2' in the exported CSV file would appear as Mobile. And for example, the Mobile of Vincent Lim is 98904237. In the CSV file, it will appear as shown. <table><tr><th>D</th><th>E</th><th>F</th><th>G</th><th>H</th></tr><tr><td>User Name</td><td>Department</td><td>Home Tel</td><td>Mobile</td><td>Access Group A</td></tr><tr><td>*****</td><td>*****</td><td>*****</td><td>*****</td><td>*****</td></tr><tr><td>Vincent Lim</td><td>0</td><td>67725490</td><td>98904237</td><td>0</td></tr><tr><td>William Sim</td><td>1</td><td></td><td></td><td>0</td></tr><tr><td>Y. Y. Choo</td><td>0</td><td></td><td></td><td>0</td></tr><tr><td>Seng Chong Sing</td><td>0</td><td></td><td></td><td>0</td></tr><tr><td>Tan Yam Ling</td><td>0</td><td></td><td></td><td>0</td></tr></table>	D	E	F	G	H	User Name	Department	Home Tel	Mobile	Access Group A	*****	*****	*****	*****	*****	Vincent Lim	0	67725490	98904237	0	William Sim	1			0	Y. Y. Choo	0			0	Seng Chong Sing	0			0	Tan Yam Ling	0			0
D	E	F	G	H																																					
User Name	Department	Home Tel	Mobile	Access Group A																																					
*****	*****	*****	*****	*****																																					
Vincent Lim	0	67725490	98904237	0																																					
William Sim	1			0																																					
Y. Y. Choo	0			0																																					
Seng Chong Sing	0			0																																					
Tan Yam Ling	0			0																																					
Access Group A	- Can be Unused, Full Access or any of the other 254 Access Group. '0' in the Access Group A column in the exported CSV file means that Full Access is selected. '255' means that Unused is selected. In this example, Access Group A for Vincent Lim is selected as Full Access, as shown below. <table><tr><th>D</th><th>E</th><th>F</th><th>G</th><th>H</th></tr><tr><td>User Name</td><td>Department</td><td>User Field 2</td><td>User Field 3</td><td>Access Group A</td></tr><tr><td>*****</td><td>*****</td><td>*****</td><td>*****</td><td>*****</td></tr><tr><td>Vincent Lim</td><td>1</td><td></td><td></td><td>0</td></tr><tr><td>William Sim</td><td>1</td><td></td><td></td><td>0</td></tr><tr><td>Y. Y. Choo</td><td>0</td><td></td><td></td><td>0</td></tr></table>	D	E	F	G	H	User Name	Department	User Field 2	User Field 3	Access Group A	*****	*****	*****	*****	*****	Vincent Lim	1			0	William Sim	1			0	Y. Y. Choo	0			0										
D	E	F	G	H																																					
User Name	Department	User Field 2	User Field 3	Access Group A																																					
*****	*****	*****	*****	*****																																					
Vincent Lim	1			0																																					
William Sim	1			0																																					
Y. Y. Choo	0			0																																					
Access Group B	- Can be Unused, Full Access or any of the other 254 Access Group. '0' in the Access Group B column in the exported CSV file means that Full Access is selected. '255' means that Unused is selected. In this example, Access Group B for Vincent Lim is selected as Unused, as shown below. <table><tr><th>D</th><th>E</th><th>F</th><th>G</th><th>H</th><th>I</th></tr><tr><td>User Name</td><td>Department</td><td>User Field 2</td><td>User Field 3</td><td>Access Group A</td><td>Access Group B</td></tr><tr><td>*****</td><td>*****</td><td>*****</td><td>*****</td><td>*****</td><td>*****</td></tr><tr><td>Vincent Lim</td><td>1</td><td></td><td></td><td>0</td><td>255</td></tr><tr><td>William Sim</td><td>1</td><td></td><td></td><td>0</td><td>255</td></tr><tr><td>Y. Y. Choo</td><td>0</td><td></td><td></td><td>0</td><td>255</td></tr></table>	D	E	F	G	H	I	User Name	Department	User Field 2	User Field 3	Access Group A	Access Group B	*****	*****	*****	*****	*****	*****	Vincent Lim	1			0	255	William Sim	1			0	255	Y. Y. Choo	0			0	255				
D	E	F	G	H	I																																				
User Name	Department	User Field 2	User Field 3	Access Group A	Access Group B																																				
*****	*****	*****	*****	*****	*****																																				
Vincent Lim	1			0	255																																				
William Sim	1			0	255																																				
Y. Y. Choo	0			0	255																																				
Binary	-																																								
Length	-																																								

Arm/Disarm Zone	- The number in the Arm/Disarm Zone column in the exported CSV file represents the Alarm Zone that the user can arm/disarm. The number representing the Alarm Zone is as follows:- • Alarm Zone 1 – 0 • Alarm Zone 2 – 1 • Alarm Zone 3 – 2 • Alarm Zone 4 – 3 • All Alarm Zones – 5 • User cannot arm/disarm any alarm zone – 255
Holiday Schedule	-
Allow Exit Reader	- '0' indicates that the box for <i>Allow exit reader usage only in accordance with time schedules</i> is NOT checked. '1' indicates that the box for <i>Allow exit reader usage only in accordance with time schedules</i> is checked.
Enrolment	- '0' indicates that the box for <i>Cardholder can enable enrolment operation</i> in AEC is NOT checked. '1' indicates that the box for <i>Cardholder can enable enrolment operation</i> in AEC is checked.
One Time	-
PIN Access	- '0' indicates that the box for <i>Card + PIN is required on keypad readers</i> in AEC is NOT checked. '1' indicates that the box for <i>Card + PIN is required on keypad readers</i> in AEC is checked.
Extended Duration	-
Start Date Selected	- '0' indicates that the box for <i>Start Date</i> in AEC is NOT checked. '1' indicates that the box for <i>Start Date</i> in AEC is checked.
Start Year	- The number in the Start Year column in the exported CSV file represents the year stated for the card to take effect.
Start Month & Day	-

End Date Selected	- '0' indicates that the box for <i>End Date</i> in AEC is NOT checked. '1' indicates that the box for <i>End Date</i> in AEC is checked.
End Year	- The number in the End Year column in the exported CSV file represents the year stated for the card to stop taking effect.
End Month and Day	-
Dual Card Assignment	- '0' indicates that the radio button for <i>Dual Card not assigned</i> is selected. '1' indicates that the radio button for <i>Dual Card presentation sequence</i> is selected.
Dual Card Presentation Sequence	-
Group ID	-

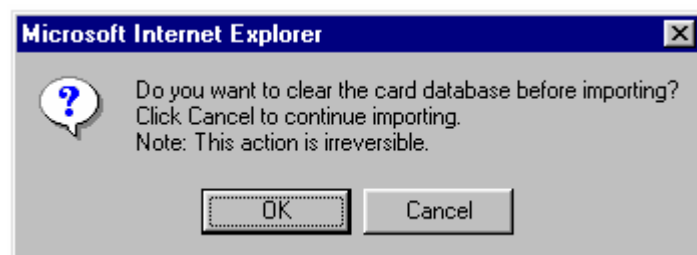
Importing the Card Database

To import a card database file, refer to the steps below:-

1. To import the card database, select a CSV file using the [Browse...] button or enter the directory and the file name directly in the space provided beside *Select a CSV file*.

Select a CSV file:

2. Click on [Import]. A screen as shown below will appear.



3. Click [Cancel] to continue importing the file back into the controller. Click [OK] to clear the card database before importing the file back into the controller.

The Search Function

The *Card Assignment* menu item has some useful built-in features that allow user to search the card database for a particular card. User can search either by Card Number, Name, User Field or an Empty Slot in the card database.

To find a particular Cardholder based on Card Number.

If you wish to find a Cardholder's details whose Card Number is known, use the *Search* function as shown below. You have the option to search by **Name** or **Card Number** or **User Field** by selecting from the Option drop down box.



1. Enter the exact Card Number in the *Search* field.
2. Click the corresponding  button.

During the *Search By Card #* function, one of the following cases can happen:

- a. If the card number specified is not configured in the card database, the **No such card number** message appears, or
- b. It will bring you directly to the Card Details page.

To find a particular Cardholder based on Name

If you wish to find a Card Number whose Name is known, use the Option drop down box and select *Name*.

1. Enter the first few characters of the person's name in the *Search* field and click on the  button.

TIP: To speed up the search function, enter the exact full name of the Cardholder you wish to find.

During the *Search* function, one of the following cases can happen:

- a. If the name specified is not found in the card database, the **No such name** message appears, or
- b. If the result has only one match, the Card Details page of the Cardholder will appear, or
- c. If the result yields more than one match, a window will appear below the function field for further selection by user.

We will elaborate on case c as the first two cases are fairly straightforward and easily understood.

In this example, we wish to search the database for Cardholder with the name “John”.

1. Enter the word **John** in the *Search* field.
2. Click on the  button resulted in the following find.

Names Found:	John d'Baptist (1) John (4)
--------------	--

The database contains two Cardholders whose name satisfied the word “John”.

3. Click on the desired name in the *Names Found* box.
4. The name will appear in the *Search* field.

Search:	John	
Option:	Name	

Names Found:	John d'Baptist (1) John (4)
--------------	--

5. Click on the  button to go directly to the Card Details page of the Cardholder.

To search for Empty Slot

1. Click on the corresponding *Find* button to conduct a search for empty slot.

Batch Cards:	
Empty Slot:	

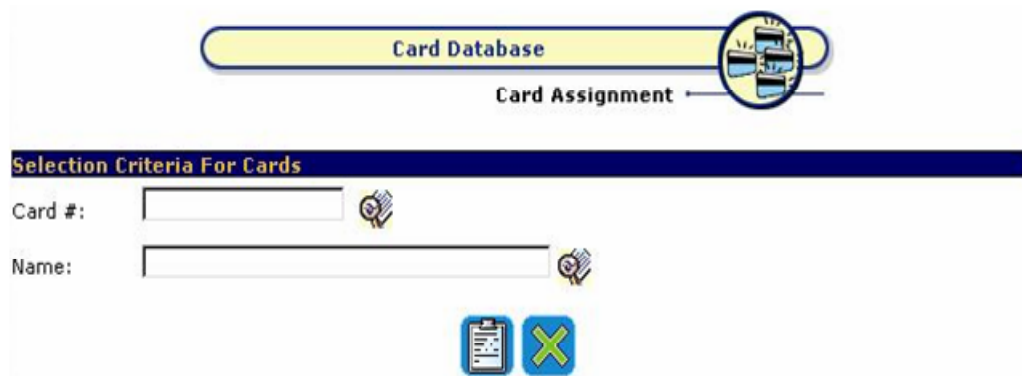
If an *Empty Slot* is available, it would show the blank Card Details. However, if there is no more *Empty Slot*, the screen will display the 1-100 listing page.

To generate a Print Preview of the report

Once you have completed configuring the Card Assignment, a hardcopy can be printed out. To print a particular cardholder or all cardholder's parameter settings, follow the procedure.

To generate a Card Assignment report

1. From the first web page of the Card Assignment menu item, click on the  [Card Assignment Report](#) link.



If you wish to generate report pertaining to a particular Cardholder, enter the Card number in the Card # field or Name in the Name field and click on the  button. (These functions is similar to the Search By Card # and Search By Name function, please refer to the section on *To find a particular Cardholder based on Card Number and based on Name* respectively for detail).

2. Click on the  button for a print preview of the report.
If you are generating all configured Cardholder's detail, skip the Find function.
The following screen-capture shows an example of the report.

NOTE: Only Cards that are entered into the database will be shown and printed out.

[Return To Card Assignment](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Card Assignment Report

Tuesday, 30 Aug 2005 17:27:42

Legends

Facil Code - Facility code
Arm/Disarm - Card holder is able to Arm/Disarm
Holiday Sch - Card holder must abide by holiday schedules (to work in conjunction with Reader Options)
Exit Sch - Allow exit reader usage only in accordance with time schedules
Card + PIN - Card + PIN is required on keypad readers
Enable Enroll - Card holder can enable enrollment operation
One Time Access - Card holder with one time access only
Extended - Extended duration for door access

1-41 of 41

ID	Card #	Name	Card Format	Arm/Disarm	Zone
	Facil Code	Access Group A	Alphabet	Holiday Sch	Start Date
	Department	Access Group B	Number	Exit Sch	End Date
	Enable Enroll	One Time Access	Dual Card Assignment	Card + PIN	Extended
1	61240	May	Standard 26 bit Format	Not Selected	----
	113	Full Access	abcd	Selected	None
	Undefined	Unused	1234	Selected	None
	Department				
	255				
	Not Selected	Not Selected	Second Card(Group ID:28)	Selected	0 seconds
2	1	Card Number:1	Standard 26 bit Format	Not Selected	----
	0	Full Access		Selected	None
	Not Selected	Unused		Selected	None
	Not Selected	Not Selected	Not Assigned	Selected	0 seconds
3	2	Card Number:2	Standard 26 bit Format	Not Selected	----
	0	Full Access		Selected	None

If you are satisfied with the configuration and wish to print out a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

- To return to the Access Groups first web page, click on the [Go Back To Card Assignment](#) link.
- To generate a preview of other configuration, click on the [Return To Selection Criteria](#) link.

This Page Intentionally Left Blank

CHAPTER 5

Schedules

This chapter covers the step by step guide to set up *Schedules* parameters. There are 255 programmable Schedules. Each Schedule defines 4 sets of start and end time for 7 days in a week. Regular and Special Holiday have its own 4 sets of time intervals. Schedules can be used in the following way:

- Schedules are allocated to Card Readers for Access Groupings. This is to specify whether cardholders can access specific readers at specific time or cardholders need to enter PIN at specific time.
- Schedules are allocated to the Card Readers to activate or deactivate readers at specified time. It is also used to define whether PIN mode will be used for the reader at specified time.
- It is used to define the time intervals to Arm / Disarm Alarm Zone.
- It is used to define the time intervals for triggering of the Output Points. For example, this is used for scheduled triggering of lighting utility for an area.

The implementation of Schedule makes the system very flexible as its behaviour can be programmed to be different for different time of a day, different days, or even during Holidays. A good example is cardholders have to enter PIN only after office hours.

NOTE: All entries for *time* are based on 24-hour, 4-digits format.

To activate Schedule

Since Schedules is the first menu item of the **Card Access Admin** group, from the *Home* page, click on Card Access Admin or its icon button. However, if you are in other menu item page, click directly on the Schedules hyperlink.

Card Access Admin

Schedules

1-128 129-255 Schedules Report

Schedule #	Description
1	Auto Lock/Unlock Door Schedule
2	Main Entrance Door Schedule
3	Lighting Control for Perimeter
4	Access to Recreational Room
5	Access for Production Workers
6	Arm / Disarm Alarm Control
7	Undefined Schedule 7
8	Undefined Schedule 8
9	Undefined Schedule 9
10	Undefined Schedule 10
11	Undefined Schedule 11
12	Undefined Schedule 12
13	Undefined Schedule 13
14	Undefined Schedule 14
15	Undefined Schedule 15
16	Undefined Schedule 16
17	Undefined Schedule 17
18	Undefined Schedule 18
19	Undefined Schedule 19
20	Undefined Schedule 20
21	Undefined Schedule 21
22	Undefined Schedule 22
23	Undefined Schedule 23

Click HERE to list Schedule # 129-255.

Click HERE to list Schedule # 1-128.

1. Click on the [1-128](#) or [129-255](#) link to list the appropriate Schedule range.

Alternatively, you can click on the button, to go to 129-255 range

listings or the button, to go to the 1-128 range listings.

To edit Schedule parameters

1. Click on the *Schedule* numbering or the *Description* text to proceed.

Schedule #: **3**
 Schedule Description: **Auto Lock/Unlock Door Schedule**

		Interval 1		Interval 2		Interval 3		Interval 4	
		Start	End	Start	End	Start	End	Start	End
Sunday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Monday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Tuesday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Wednesday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Thursday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Friday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Saturday		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Regular Hol		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Special Hol		--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--

2. Highlight the default text and enter the *Schedule Description*.



3. Click on the  button.

4. Click on the  button of the *Day of Week* (DOW), *Regular Hol* or *Special Hol* row.

This will enable the whole row for editing as shown below.

		Interval 1		Interval 2		Interval 3		Interval 4	
	Copy To	Start	End	Start	End	Start	End	Start	End
Sunday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Monday	☐	11:00	12:00	12:00	13:00	13:00	14:00	14:00	15:00
Tuesday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Wednesday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Thursday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Friday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Saturday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Regular Hol	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Special Hol	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--

5. Click on the required field, starting from Interval 1 – Start, and enter the appropriate time in 24-hour, 4 digits format.
6. Repeat step 5 until all applicable entries are entered.
7. If the time of operation is the same for Monday to Friday, click on the **Copy To** check boxes to indicate a tick (✓) mark. This will duplicate the setting to other DOW. To de-select the *DOW*, click on it again.

		Interval 1		Interval 2		Interval 3		Interval 4	
	Copy To	Start	End	Start	End	Start	End	Start	End
Sunday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Monday		08:30	12:30	13:15	17:30				
Tuesday	☒	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Wednesday	☒	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Thursday	☒	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Friday	☒	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Saturday	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Regular Hol	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
Special Hol	☐	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--

To copy the entries in Monday field to other DOW. In this case, Tuesday to Friday will have the same entries as Monday

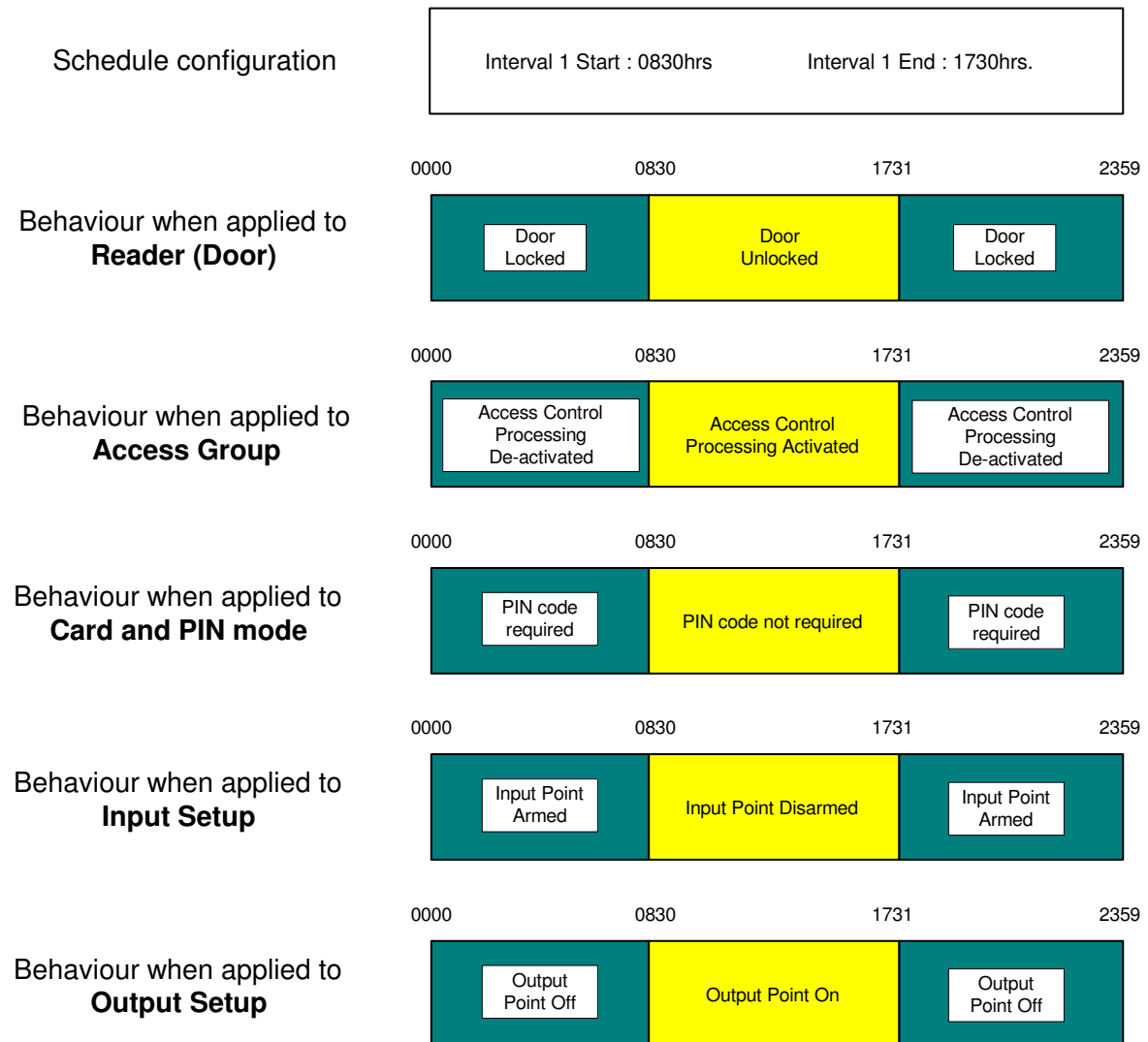
8. Do one of the following: -

- To confirm the entries, click on the  button.
- To clear the entries, click on the  button.
- To cancel the operation, click on the  button.
- To return to the first page, click on the  button.

9. Proceed to edit the other *DOW or Holiday* where applicable. If the company does not operate during Sunday or Holiday, leave the entries in these 3 fields unchanged as -- : --. This will indicate to the Access Easy Controller that these are to be ignored.

System Behaviour when using Schedule

The diagram below provides a graphical representation of the system's behaviour when a Schedule is used on the various functions.



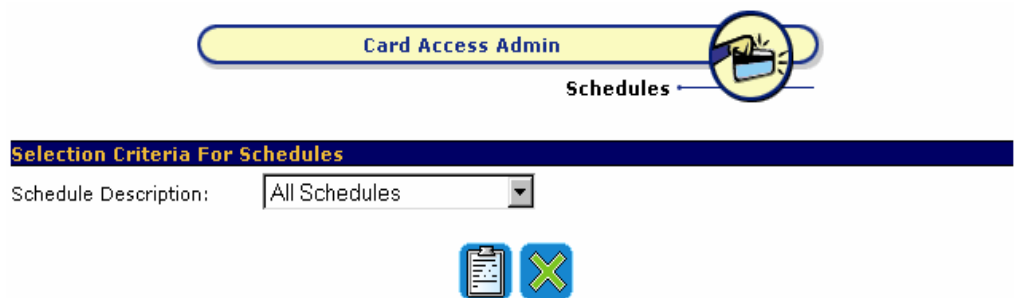
Notice that all the functions toggle its state only at 1731hrs instead of 1730hrs. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

To generate a Print Preview of the report

Once you have completed configuring the required Schedules, a hardcopy can be printed out. To print any one or all Schedules, select from the list box.

To generate a Schedule report

1. From the first web page of the Schedules menu item, click on the  [Schedules Report](#) link.



2. Select the desired Schedules from the list.
3. Click on the  button for a print preview of the report.
The following screen-capture shows an example of the report.

NOTE: Only Schedules # with interval settings will be shown and printed out.

[Return To Schedules](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Schedules Report

Tuesday, 15 Sept 2005 15:15:15

#	Description	Day	Interval 1		Interval 2		Interval 3		Interval 4	
			Start	End	Start	End	Start	End	Start	End
1	Auto Lock/Unlock Door Schedule	Sun	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
		Mon	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Tue	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Wed	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Thu	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Fri	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Sat	08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
		RHol	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
		SHol	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--

[Return To Schedules](#) [Return To Selection Criteria](#)

If you are satisfied with the configuration and wish to obtain a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the *Schedules* web page, click on the [Go Back To Schedules](#) link.
5. To generate a preview of other configuration, click on the [Return To Selection Criteria](#) link.

This Page Intentionally Left Blank

CHAPTER 6

Access Groups

This chapter covers a step by step guide to set up the *Access Groups*. An *Access Group* defines a list of readers within certain authorised time periods (pre-defined *Schedule*) that the cardholders can access. This means that only within this *Schedule*, cardholders with this access group can access this reader. There are 254 programmable *Access Groups*.

In addition, there are two more unique access groups. They are the *Full Access* group that allows cardholders to access all readers at all times, usually reserved for the *President*, *Chairman* or *Directors* of the company and the *Unused* group that prohibits cardholder to access any reader at all times.

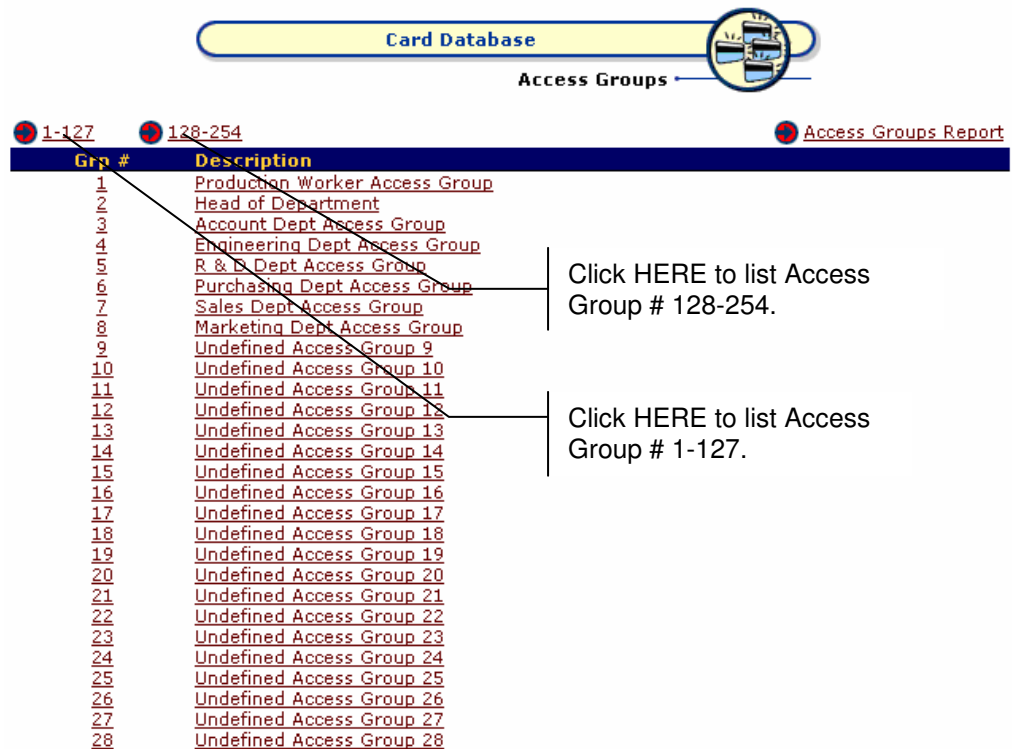
Access Group is implemented to simplify the process of assigning cardholder's access rights to each reader. Usually a group of cardholders can access the same group of readers and usually using a common *Schedule*. Rather than assigning each reader to one of the cardholder and going through the same steps repeatedly, grouping of *Access Group* is implemented.

It is highly recommended that detail planning be done before setting up the *Access Groups*.

Each *Access Group* can configure up to 16 readers with each reader linked to a *Schedule*.

To activate Access Groups

Since the Access Groups is the first menu item of the **Card Database** group, from the Home page, click on Card Database or its icon button. However, if you are in other menu item page, click directly on the Access Groups hyperlink.



Card Database

Access Groups

1-127 128-254 Access Groups Report

Grp #	Description
1	Production Worker Access Group
2	Head of Department
3	Account Dept Access Group
4	Engineering Dept Access Group
5	R & D Dept Access Group
6	Purchasing Dept Access Group
7	Sales Dept Access Group
8	Marketing Dept Access Group
9	Undefined Access Group 9
10	Undefined Access Group 10
11	Undefined Access Group 11
12	Undefined Access Group 12
13	Undefined Access Group 13
14	Undefined Access Group 14
15	Undefined Access Group 15
16	Undefined Access Group 16
17	Undefined Access Group 17
18	Undefined Access Group 18
19	Undefined Access Group 19
20	Undefined Access Group 20
21	Undefined Access Group 21
22	Undefined Access Group 22
23	Undefined Access Group 23
24	Undefined Access Group 24
25	Undefined Access Group 25
26	Undefined Access Group 26
27	Undefined Access Group 27
28	Undefined Access Group 28

Click HERE to list Access Group # 128-254.

Click HERE to list Access Group # 1-127.

1. Click on the  [1-127](#) or  [128-254](#) link to list the appropriate Access Groups ranges.

Alternatively, you can click on the  button to go to 128-254 range

listings or the  button to go to the 1-127 range listings.

To configure/edit Access Group parameters

1. Click on the *numbering* or the *Description* text to proceed.

Card Database

Access Groups

Access Group #: 2

Description: Extended Access Group

Rdr #	Description	Schedule
1	☒ Production Dept Entry Reader	8 A.M - 8 P.M
2	☐ Production Dept Exit Reader	-----
3	☒ R & D Dept Entry Reader	9 A.M - 6 P.M
4	☐ Arming Reader	No Schedule
5	☐ Reader 5	No Schedule
6	☐ Reader 6	No Schedule
7	☐ Reader 7	No Schedule
8	☐ Reader 8	No Schedule






NOTE 1: The Reader's *Description* shown above is configured in *Card Readers* setting. Please refer to the Chapter on Card Readers for details.

NOTE 2: Reader #2 is configured as Exit Reader for the Production Department. Its operational behaviour will follow that of the Entry Reader.

2. Highlight the default text and enter the new *Description*.
3. Click on the appropriate check boxes to indicate a tick (✓) mark, for reader(s) to be assigned to this *Access Group*.
4. Select the appropriate Schedule, from the list, for each selected Reader.

NOTE: The above example of Schedule selection (8 A.M – 8 P.M) indicates when the Production Workers have access to the reader.

5. If you have completed the settings for the first 8 Readers, proceed to the next 8 Readers (only if required) by clicking on the  button. Repeat step 3 and 4.

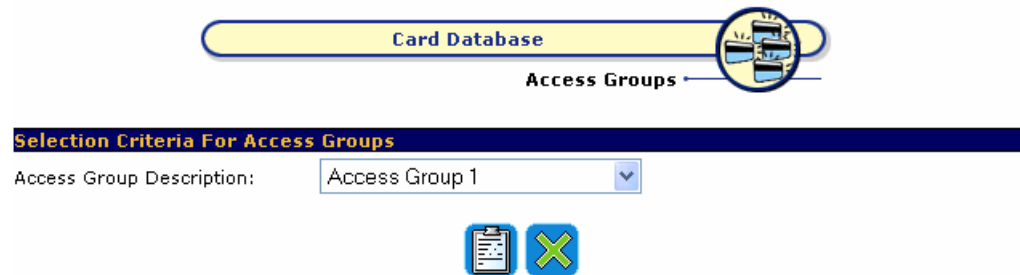
6. To confirm the setting, click on  button.

To generate a Print Preview of the report

Once you have completed configuring the required Access Groups, a hardcopy can be printed out. To print any one or all Access Groups report, select from the list box.

To generate an Access Groups report

1. From the first web page of the Access Groups menu item, click on the  [Access Groups Report](#) link.



2. Select the desired Access Group from the list.
3. Click on the  button for a print preview of the report.
The following screen-capture shows an example of the report.

NOTE: Only Access Groups that are defined will be shown.

[Return To Access Groups](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Access Groups Report

Tuesday, 30 Aug 2005 18:13:56

#	Access Group	Reader	Schedule	Floor List
1	Access Group 1	Reader 1	Schedule 255	
		Reader 2	Undefined Schedule 1	
		Reader 3	Undefined Schedule 1	
		Reader 4	Undefined Schedule 1	
		Reader 5	Undefined Schedule 1	
		Reader 6	Undefined Schedule 1	
		Reader 7	Undefined Schedule 1	
		Reader 8	Undefined Schedule 1	
		Reader 9	Schedule 255	
		Reader 10	Schedule 255	
		Reader 11	No Schedule	
		Reader 12	No Schedule	
		Reader 13	No Schedule	
		Reader 14	No Schedule	
		Reader 15	No Schedule	
		Reader 16	No Schedule	

[Return To Access Groups](#) [Return To Selection Criteria](#)

If you are satisfied with the configuration and wish to print out a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Selection Criteria, click on the [Return To Selection Criteria](#) link.
5. To return to the Access Groups first web page, click on the [Go Back To Access Groups](#) link.

This Page Intentionally Left Blank

CHAPTER 7

Holidays

This chapter covers the step by step guide to set up *Holidays* parameters. Holiday parameters have to be set up only if the system operation behaviour is required to be different during holidays. Some samples of how the parameters affect the system operation behaviour are: -

- The controller unlocks a specific door during certain working hours of the day. However, during a holiday, the door will remain locked the whole day.
- A cardholder is allowed access to certain areas during working hours. However during a holiday, the cardholder is not allowed access.

Holidays set-up consist of 64 Holidays selection, of which 32 are assigned for *Regular Holiday* dates and the other 32 assigned to *Special Holiday* dates. There is no difference between the operational behaviour of both types. For simplicity, you may treat the *Special Holiday* set up for use during the eve of a holiday.

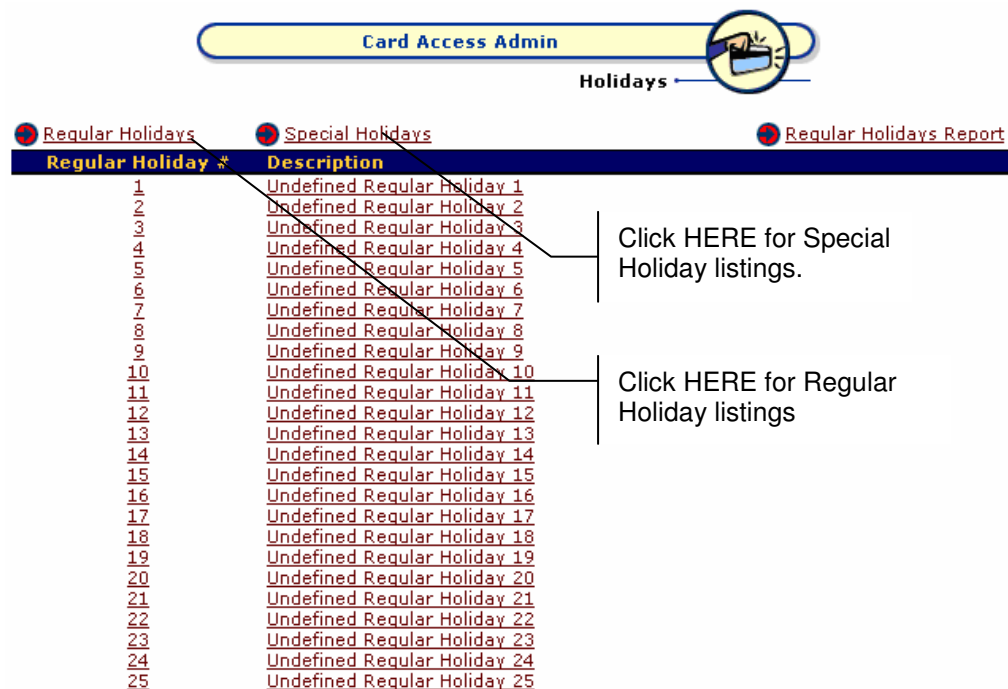
Each *Holiday #* has the feature *Include year in processing?*, if it is set to *NO*, the controller will not consider the *Year* during a date check. This is very useful if the holiday date falls on the same date year after year e.g. *New Year day* and *Christmas Day*, need to be defined only once. While those holiday dates that varies from year to year has to be updated at the beginning of the year, shall be selected to *YES*.

User can use this feature to ease the updating of holiday dates every year by allocating, for example, the first 10 *Holiday IDs* for fixed holiday dates and the rest of the IDs for variable holiday dates. In this way, user just need to update on the variable holiday dates and skip the fixed holiday dates at the beginning of the year.

To activate Holidays

The *Holidays* can be activated only from the menu item page.

1. From any menu item page, click on Holidays hyperlink.



The screenshot shows the 'Card Access Admin' interface. At the top, there is a 'Holidays' button with a calendar icon. Below it, there are three links: 'Regular Holidays', 'Special Holidays', and 'Regular Holidays Report'. A table titled 'Regular Holiday #' and 'Description' lists 25 'Undefined Regular Holiday' entries. Two callouts point to the 'Special Holidays' link and the 'Regular Holidays' link, with text indicating where to click for special and regular holiday listings.

Regular Holiday #	Description
1	Undefined Regular Holiday 1
2	Undefined Regular Holiday 2
3	Undefined Regular Holiday 3
4	Undefined Regular Holiday 4
5	Undefined Regular Holiday 5
6	Undefined Regular Holiday 6
7	Undefined Regular Holiday 7
8	Undefined Regular Holiday 8
9	Undefined Regular Holiday 9
10	Undefined Regular Holiday 10
11	Undefined Regular Holiday 11
12	Undefined Regular Holiday 12
13	Undefined Regular Holiday 13
14	Undefined Regular Holiday 14
15	Undefined Regular Holiday 15
16	Undefined Regular Holiday 16
17	Undefined Regular Holiday 17
18	Undefined Regular Holiday 18
19	Undefined Regular Holiday 19
20	Undefined Regular Holiday 20
21	Undefined Regular Holiday 21
22	Undefined Regular Holiday 22
23	Undefined Regular Holiday 23
24	Undefined Regular Holiday 24
25	Undefined Regular Holiday 25

2. Click on the [Regular Holidays](#) or [Special Holidays](#) link to list the appropriate holiday type.

Alternatively, you can click on the  button to go to *Special Holiday* listings or the  button to go to the *Regular Holiday* listings.

To edit Holidays parameters

1. Select the appropriate Holiday Type.
2. Click on the *Holidays numbering* or the *Description* text to proceed.

Card Access Admin 

Holidays

 [Regular Holidays](#)
 [Special Holidays](#)
 [Regular Holidays Report](#)

Regular Holiday #	Description
1	New Year Day
2	Undefined Regular Holiday 2
3	Undefined Regular Holiday 3
4	Undefined Regular Holiday 4
5	Undefined Regular Holiday 5
6	Undefined Regular Holiday 6
7	Undefined Regular Holiday 7
8	Undefined Regular Holiday 8
9	Undefined Regular Holiday 9
10	Undefined Regular Holiday 10
11	Undefined Regular Holiday 11
12	Undefined Regular Holiday 12
13	Undefined Regular Holiday 13
14	Undefined Regular Holiday 14
15	Undefined Regular Holiday 15
16	Undefined Regular Holiday 16
17	Undefined Regular Holiday 17
18	Undefined Regular Holiday 18
19	Undefined Regular Holiday 19

Click on either one of the links of the same row.

Card Access Admin 

Holidays

Regular Holiday #: **1**

Holiday Description:

Current Holiday Date:

New Holiday Date: Day: Month: Year:

Include year in processing? ☐ Yes ☒ No





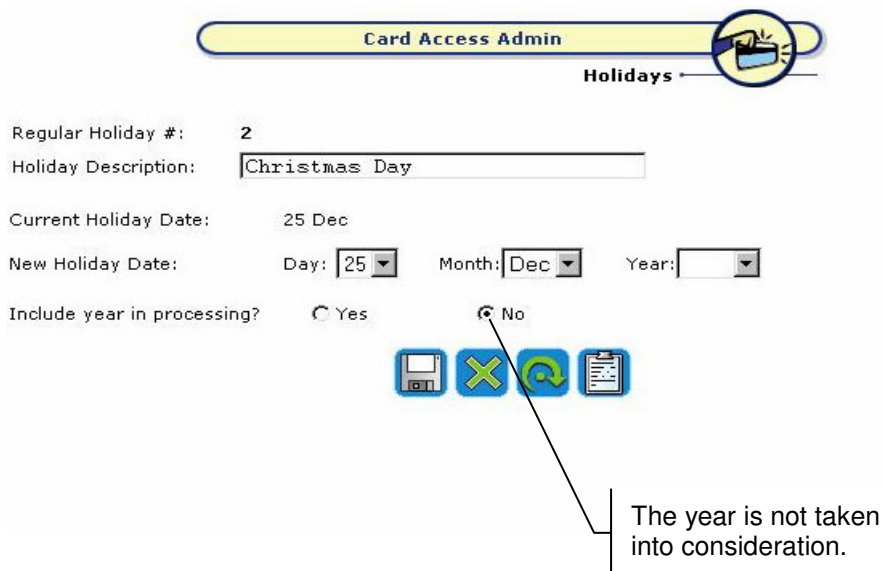

3. Highlight the default text and enter the new *Holiday Description*.
4. Select the appropriate *Day* from the list.
5. Do likewise for the *Month* and the *Year* (if the year is required for processing) field.
6. If the *Holiday* date is fixed, then click on the radio button of the *Include year in processing?* to *No*, otherwise click *Yes*.
7. Do one of the following: -

- To confirm the entries, click on the  button.
- To clear the entries, click on the  button.
- To cancel the operation, click on the  button.

- To return to the first page, click on the  button.

8. Proceed to configure other Holiday dates where applicable.

The example below shows selection of *Regular Holiday #2* used for *Christmas Day* in the year 2000. Since the date always fall on the December 25th, the *Include year in processing?* was set to *No*.



Card Access Admin

Holidays

Regular Holiday #: 2

Holiday Description: Christmas Day

Current Holiday Date: 25 Dec

New Holiday Date: Day: 25 Month: Dec Year:

Include year in processing? ☐ Yes ☒ No

The year is not taken into consideration.

To generate a Print Preview of the report

Once you have completed configuring the required Holidays, a hardcopy can be printed out. To print any one or all Holidays (Regular or Special) configuration, select from the list box.

To generate a Holidays report

1. From the web page of the Holidays menu item, click on the link. Either  [Regular Holidays](#) or  [Special Holidays](#) will be shown.



2. Select the desired Holiday from the list.
3. Click on the  button for a print preview of the report. The following screen-capture shows an example of the report.

NOTE: Only Holiday # with date setting will be shown.

[Return To Holidays](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Regular Holidays Report

Wednesday, 31 Aug 2005 09:29:29

#	Description	Date
1	christmas	24 Dec 2005

[Return To Holidays](#) [Return To Selection Criteria](#)

If you are satisfied with the configuration and wish to print out a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Holidays web page, click on the [Go Back To Holidays](#) link.
5. To generate a preview of other configuration, click on the [Return To Selection Criteria](#) link.

This Page Intentionally Left Blank

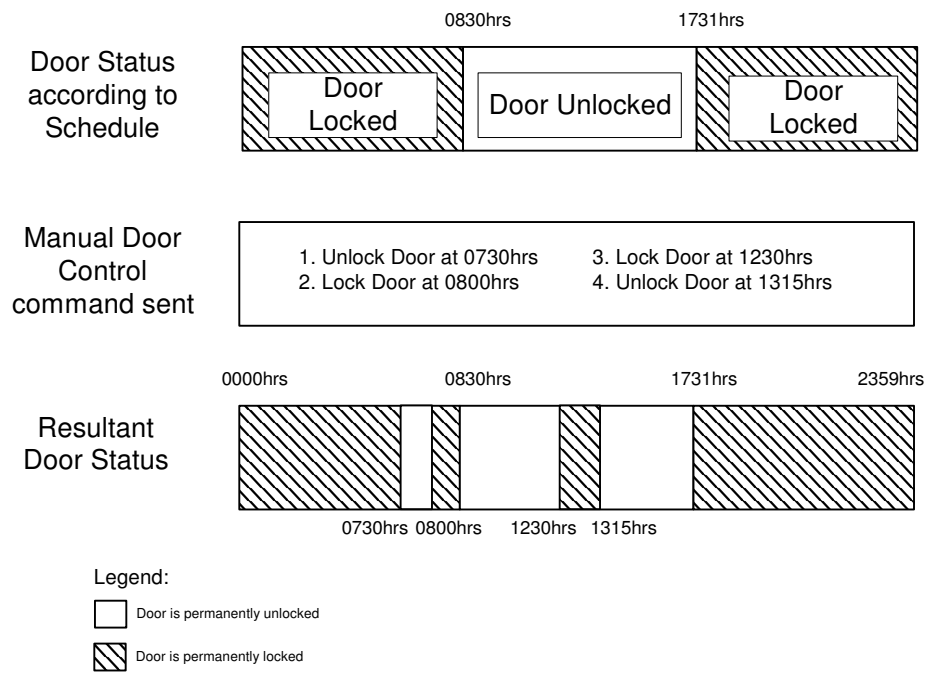
CHAPTER 8

Door Control

The Door Control is one of the menu items of the **Manual Control** Group. It allows user to check the status of all the doors and send a command to either momentarily unlock or permanently unlock / lock the door without having to be at the door location.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

We show an example to illustrate the condition.
The setting for Interval 1 is Start – **0830hrs** and End – **1730hrs**.
Interval 2,3, and 4 has no setting.



Notice that the system resume normal operation as according to Schedule at 0830hrs and 1731hrs.

To activate Door Control

There are various ways to activate the Door Control menu item. They are: -

1. From the Home page, click on Manual Control or its icon button.
2. From the View Activity page, click on Door Control hyperlink.
3. From any of the menu items page of the Manual Control Group.



Door #	Description	Current Status	Manual Actions
1	Production Dept Entry Reader	Locked - Closed	☒ No Change ☐ Unlock ☐ Momentarily Unlock
2	Production Dept Exit Reader	Locked - Closed	☒ No Change ☐ Unlock ☐ Momentarily Unlock
3	Reader 3	Locked - Closed	☒ No Change ☐ Unlock ☐ Momentarily Unlock
4	Reader 4	Locked - Closed	☒ No Change ☐ Unlock ☐ Momentarily Unlock
5	Reader 5	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
6	Reader 6	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
7	Reader 7	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
8	Reader 8	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
9	Reader 9	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
10	Reader 10	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
11	Reader 11	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
12	Reader 12	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
13	Reader 13	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
14	Reader 14	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
15	Reader 15	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock
16	Reader 16	Door Held Open	☒ No Change ☐ Unlock ☐ Momentarily Unlock

The following paragraphs provide some description of what will you see on the web page.

Current Status: provide user with the current status of the door. There are 5 door control status.

Status	Description
Locked – Closed	Indicates that the door is locked permanently.
Unlocked – Open	Indicates that the door is unlocked and open.
Unlocked – Closed	Indicates that the door is unlocked and close.
Door Forced Open	Indicates that door is forced open.
Door Held Open	Indicates that door is held open beyond a period of time(Exceeded the time settings of Door Open Timer)

Manual Actions: provide user with radio buttons selection of what manual action to perform.

The description of the second radio button is the opposite of the current status and it will toggle between **Lock** and **Unlock**.

The third radio button, *Momentary Unlock*, is used to send a command to momentarily unlocked the door for a duration as specified by the *Door Strike Timer*. This command is only effective when the current status of the door is **Locked**.

NOTE: Only readers configured as Entry Readers will be shown on the web page.

To control the Doors manually

1. Select the desired action radio button(s) (see NOTE 1).
2. Click on either  or  button to send the command.
The web page will refresh to reflect the new status.

NOTE 1: Select only door(s) that you want to send command to.

NOTE 2: The current status of the door for a Momentarily Unlocked command will not show the true status after the *Door Strike Timer* has elapsed, unless the user refreshes the web page by click on the  button.

This Page Intentionally Left Blank

CHAPTER 9

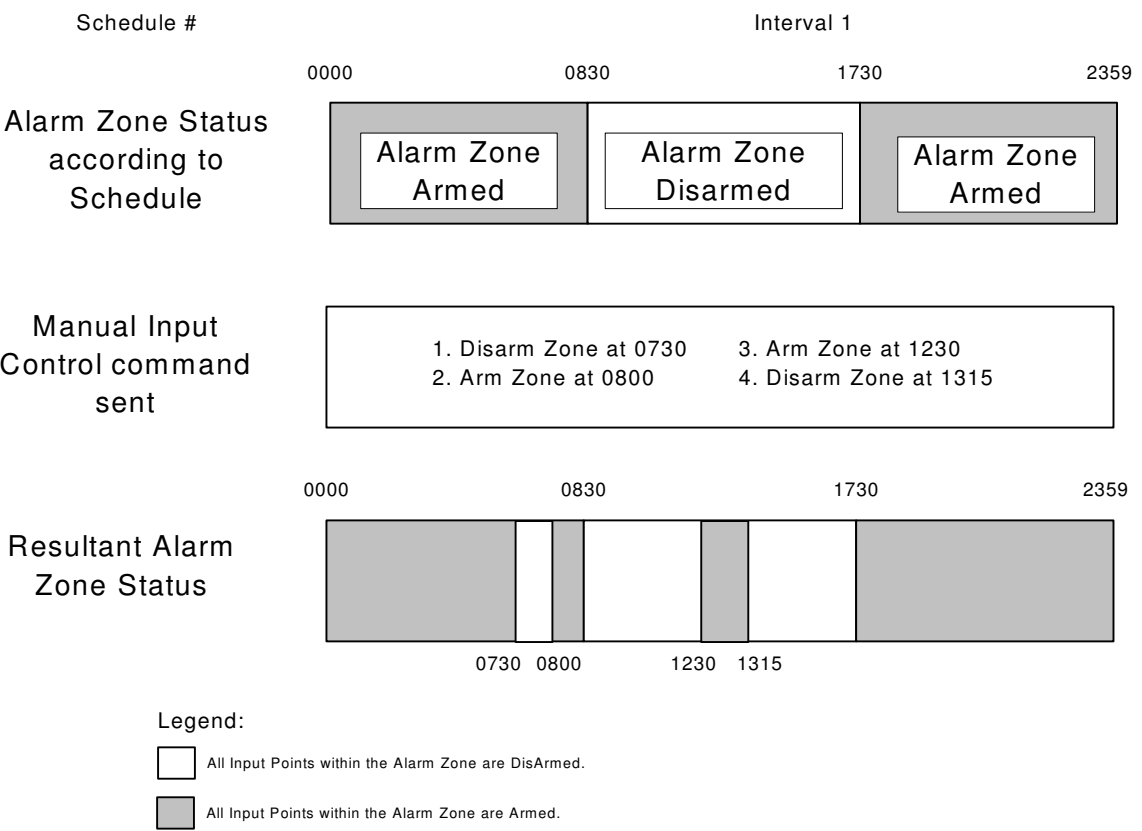
Input Control

The Input Control is one of the menu items of the **Manual Control** Group. It allows user to check the status of all the Input Points assigned to specific Alarm Zones and to send a command to Arm / Disarm the Zone manually.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

For configuration of system control, please refer to the Chapter on *Input Point Setup*.

Before we begin, we show an example to illustrate the operational behaviour. The setting for Interval 1 is Start – **0830hrs** and End – **1730hrs**. Interval 2,3, and 4 has no setting.



Notice that the system resume normal operation as according to Schedule at 0830hrs and 1731hrs.

To activate Input Control

There are various ways to activate the Input Control. They are: -

1. From any menu item page, click on [Input Control](#) hyperlink.
2. From the View Activity page, click on [Input Control](#) hyperlink.
3. From any of the menu items page of the Manual Control Group.

Input #	Description	Current Status	Manual Actions
1	Input Point 1	Disarmed - Low	☒ No Change ☐ Arm Now
2	Input Point 2	Disarmed - Low	Alarm Zone 1
3	Undefined Input Point 3	Disarmed - Low	☒ No Change ☐ Arm Now
4	Undefined Input Point 4	Disarmed - Low	☒ No Change ☐ Arm Now
5	Undefined Input Point 5	Disarmed - Low	☒ No Change ☐ Arm Now
6	Undefined Input Point 6	Disarmed - Low	☒ No Change ☐ Arm Now
7	Undefined Input Point 7	Disarmed - Low	☒ No Change ☐ Arm Now
8	Undefined Input Point 8	Disarmed - Low	☒ No Change ☐ Arm Now
9	Undefined Input Point 9	Disarmed - Low	☒ No Change ☐ Arm Now
10	Undefined Input Point 10	Disarmed - Low	☒ No Change ☐ Arm Now
11	Undefined Input Point 11	Disarmed - Low	☒ No Change ☐ Arm Now
12	Undefined Input Point 12	Disarmed - Low	☒ No Change ☐ Arm Now
13	Undefined Input Point 13	Disarmed - Low	☒ No Change ☐ Arm Now
14	Undefined Input Point 14	Disarmed - Low	☒ No Change ☐ Arm Now
15	Undefined Input Point 15	Disarmed - Low	☒ No Change ☐ Arm Now
16	Undefined Input Point 16	Disarmed - Low	☒ No Change ☐ Arm Now

This is the View Status page. It allows user to view the current status of all assigned Input Points and the respective Alarm Zone the Input Points belongs to.

NOTE: Only Input Points that are not controlled specifically based on Schedule will be shown on the web page.

Description provides the grouping of the Input Point, if any. The horizontal strip in blue provides the Alarm Zone to which the Input Points belong. The Alarm Zones are separated by a blue line. Independent Input Points do not belong to any Alarm Zone. In this case, Input Point 2 belongs to Alarm Zone 1. Input Point 1 is an independent input point.

The table below describes the possible grouping of the Input Point.

Alarm Zone 1	Input Points in Alarm Zone 1 are displayed together. They are to be armed / disarmed together.
Alarm Zone 2	Input Points in Alarm Zone 2 are displayed together. They are to be armed / disarmed together.
Alarm Zone 3	Input Points in Alarm Zone 3 are displayed together. They are to be armed / disarmed together.
Alarm Zone 4	Input Points in Alarm Zone 4 are displayed together. They are to be armed / disarmed together.
Independent Input Point	These are Independent Input Points which can be armed / disarmed by itself.

Current Status column provides us with the current input point status.

The table below describes the possible status of the Input Point.

Current Status	Description
Armed	The respective Input Point is Armed.
Disarmed - Low	The respective Input Point is Disarmed and its current status is close.
Disarmed - High	The respective Input Point is Disarmed and its current status is open.
Alarm	An Alarm is detected from the Input Point.
Bypassed - Low	The Input Point has been bypassed though the alarm zone is armed. This situation can only happen when the input point status is close while the alarm zone is armed.
Bypassed - High	The Input Point has been bypassed though the alarm zone is armed. This situation can only happen when the input point status is open while the alarm zone is armed.

Manual Actions column provides the check box for selection of the input points to issue the command.

There are 2 types of action command available:

	This icon means that by selecting the check box, an Arming command will be issued when submitted.
	This icon means that by selecting the check box, a Disarming command will be issued when submitted.

To control (Arm/Disarm) an Input Point

These are Input points that are not included in any of the 4 Alarm Zones nor are it controlled by Schedule. They are independent points that could be armed or disarmed manually.

Manual Control

Input Control

Door Control
 Output Control
 Reset APB
 View Activity

1-16
 17-32
 Alarm Zone 1
 Alarm Zone 3
 Alarm Zone 4

Input #	Description	Current Status	Manual Actions
1	Input Point 1	Disarmed - Low	☒ No Change ☐ Arm Now
2	Input Point 2	Disarmed - Low	Alarm Zone 1
3	Undefined Input Point 3	Disarmed - Low	☒ No Change ☐ Arm Now
4	Undefined Input Point 4	Disarmed - Low	☒ No Change ☐ Arm Now
5	Undefined Input Point 5	Disarmed - Low	☒ No Change ☐ Arm Now
6	Undefined Input Point 6	Disarmed - Low	☒ No Change ☐ Arm Now
7	Undefined Input Point 7	Disarmed - Low	☒ No Change ☐ Arm Now
8	Undefined Input Point 8	Disarmed - Low	☒ No Change ☐ Arm Now
9	Undefined Input Point 9	Disarmed - Low	☒ No Change ☐ Arm Now
10	Undefined Input Point 10	Disarmed - Low	☒ No Change ☐ Arm Now
11	Undefined Input Point 11	Disarmed - Low	☒ No Change ☐ Arm Now
12	Undefined Input Point 12	Disarmed - Low	☒ No Change ☐ Arm Now
13	Undefined Input Point 13	Disarmed - Low	☒ No Change ☐ Arm Now
14	Undefined Input Point 14	Disarmed - Low	☒ No Change ☐ Arm Now
15	Undefined Input Point 15	Disarmed - Low	☒ No Change ☐ Arm Now
16	Undefined Input Point 16	Disarmed - Low	☒ No Change ☐ Arm Now



Input Points that does not belongs to any Alarm Zone

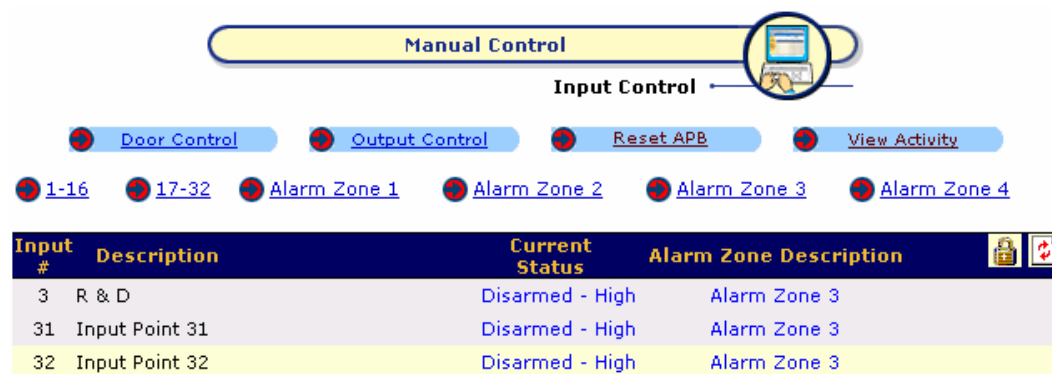
- Click on the appropriate link, 1-16 or 17-32, to display the correct range of Input Points. Alternatively, you can click on the or button.
- Select the desired radio button(s) (see NOTE 1).
- Click on either or button to send the command. The web page will refresh to reflect the new status.

NOTE 1: If the current status of the Input Point is Armed, the Manual Action will shows ☐ Disarm Now, which means you could send a disarm

command to this input when the button is click. Likewise, if the Input Point is currently Disarmed, the Manual Action will shows ☐ Arm Now

To control (Arm/Disarm) the Alarm Zone

1. Click on the appropriate Alarm Zone link to display the list of Input Points configured to that zone. For example, click on the [Alarm Zone 3](#) link will only list those Input Points configured for Alarm Zone 3 as shown below.



The screenshot shows the 'Manual Control' section of the interface. Under the 'Input Control' tab, there are several links: 'Door Control', 'Output Control', 'Reset APB', 'View Activity', and a row of alarm zone links: '1-16', '17-32', 'Alarm Zone 1', 'Alarm Zone 2', 'Alarm Zone 3', and 'Alarm Zone 4'. Below these links is a table with the following data:

Input #	Description	Current Status	Alarm Zone Description
3	R & D	Disarmed - High	Alarm Zone 3
31	Input Point 31	Disarmed - High	Alarm Zone 3
32	Input Point 32	Disarmed - High	Alarm Zone 3

2. Click on the  button to arm the Input Points within the Alarm Zone. The web page will refresh to reflect the new status and the button changes to , clicking on it will Disarm all the Input Points within the Alarm Zone.

This Page Intentionally Left Blank

CHAPTER 10

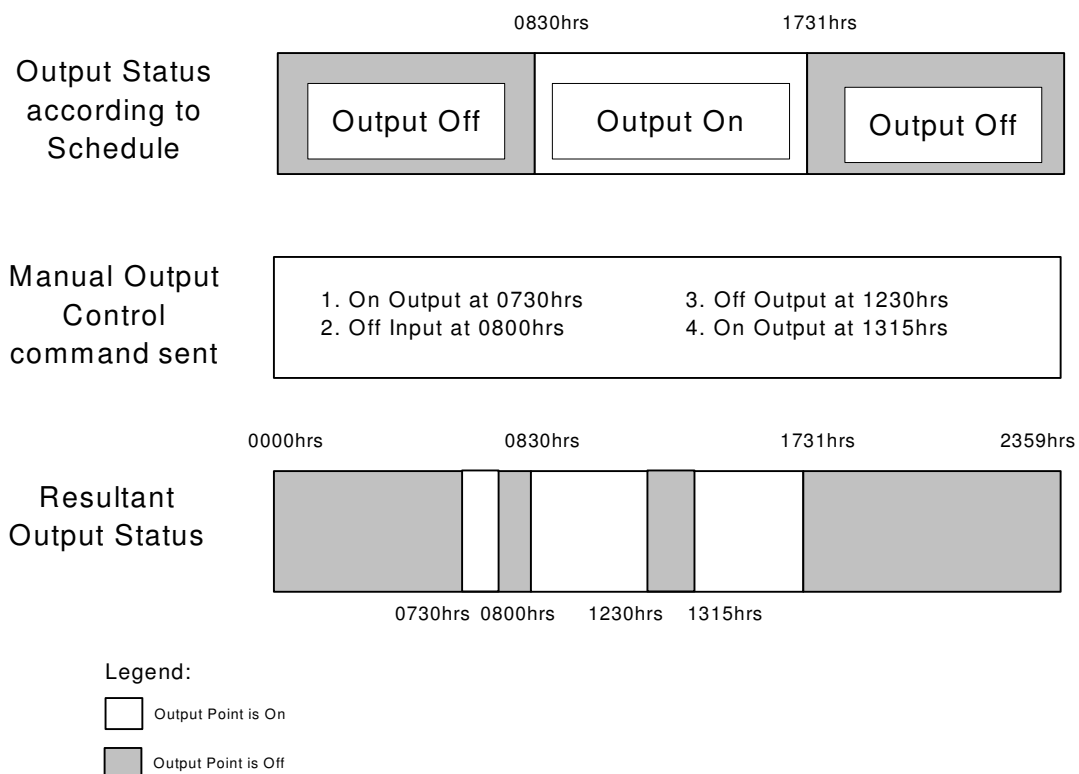
Output Control

The Output Control is one of the menu items of the **Manual Control** Group. It allows user to check the status of all the Output Points and send a command to turn On / Off the points manually. However, if the Output Point is linked to an Input Point as a Status Output, the status will not be indicated here.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

For configuration of system control, please refer to the Chapter on *Output Setup*.

Before we begin, we show an example to illustrate the operational condition. The setting for Interval 1 is Start – **0830hrs** and End – **1730hrs**. Interval 2,3, and 4 has no setting.



Notice that the system resume normal operation as according to Schedule at 0830hrs and 1731hrs.

To activate Output Control

There are various ways to activate the Output Control. They are: -

1. From any menu item page, click on [Output Control](#) hyperlink.
2. From the View Activity page, click on [Output Control](#) hyperlink.
3. From any of the menu items page of the Manual Control Group.



Output #	Description	Current Status	Manual Actions
1	Simulation of Alarm Sensor #1	Off	No Change On Duration On
2	Simulation of Alarm Sensor #2	Off	No Change On Duration On
3	Simulation of Alarm Sensor #3	Off	No Change On Duration On
4	Warehouse Lighting	On	No Change Off Duration Off
5	CCTV Activation	Off	No Change On Duration On
6	Undefined Output Point 6	Off	No Change On Duration On
7	Undefined Output Point 7	Off	No Change On Duration On
8	Undefined Output Point 8	Off	No Change On Duration On
9	Undefined Output Point 9	Off	No Change On Duration On
10	Undefined Output Point 10	Off	No Change On Duration On
11	Undefined Output Point 11	Off	No Change On Duration On
12	Undefined Output Point 12	Off	No Change On Duration On
13	Undefined Output Point 13	Off	No Change On Duration On
14	Undefined Output Point 14	Off	No Change On Duration On
15	Undefined Output Point 15	Off	No Change On Duration On
16	Undefined Output Point 16	Off	No Change On Duration On

The following paragraphs provide some description of what you will see on the web page.

Current Status: provide user with the current status of the Output Points. **On** status indicates that the Output Point is “on” and **Off** status indicates that the Output Point is “off”.

Manual Actions: provide user with radio buttons selection of what manual action to perform.

The description of the second radio button is the opposite of the current status and it will toggle between **On** and **Off**.

The third radio button, *Duration On* or *Duration Off*, which is the opposite of the current status, is used to send a command to turn on or turn off the Output Point for a duration as depicted in the *Duration* field in *Output Setup* menu item. Please refer to the Chapter on *Output Setup* for detail.

To control the Output Points

4. Click on the appropriate link,  [1-16](#) or  [17-32](#), to display the correct range of Output Points. Alternatively, you can click on the  or  button.
5. Select the desired radio button(s) (see NOTE 1).
6. Click on either  or  button to send the command. The web page will refresh to reflect the new status.

NOTE 1: Select only Output Point(s) that you want to send command to.

NOTE 2: The current status of the Output Point for a *Duration On* or *Duration Off* command will not show the true status after the *Duration* has elapsed, unless the user refreshes the web page by clicking on the  button.

This Page Intentionally Left Blank

CHAPTER 11

Reset APB

The Reset APB is the final menu item of the **Manual Control** Group. It allows user to reset the Anti-Passback (APB) feature once it is violated.

NOTE: This feature is applicable to *Full* and *Soft Anti-Passback* only.

Please refer to the Chapter on *Card Readers, Anti-Passback Settings*.

If Full APB is used, this command will reset the violation and allow violator(s) to access or exit the controlled door. However, if Soft APB is used, this command will reset the Activity transactions for “Access Granted, Soft APB” and “Exit Granted, Soft APB” for violator’s subsequent access or exit respectively.

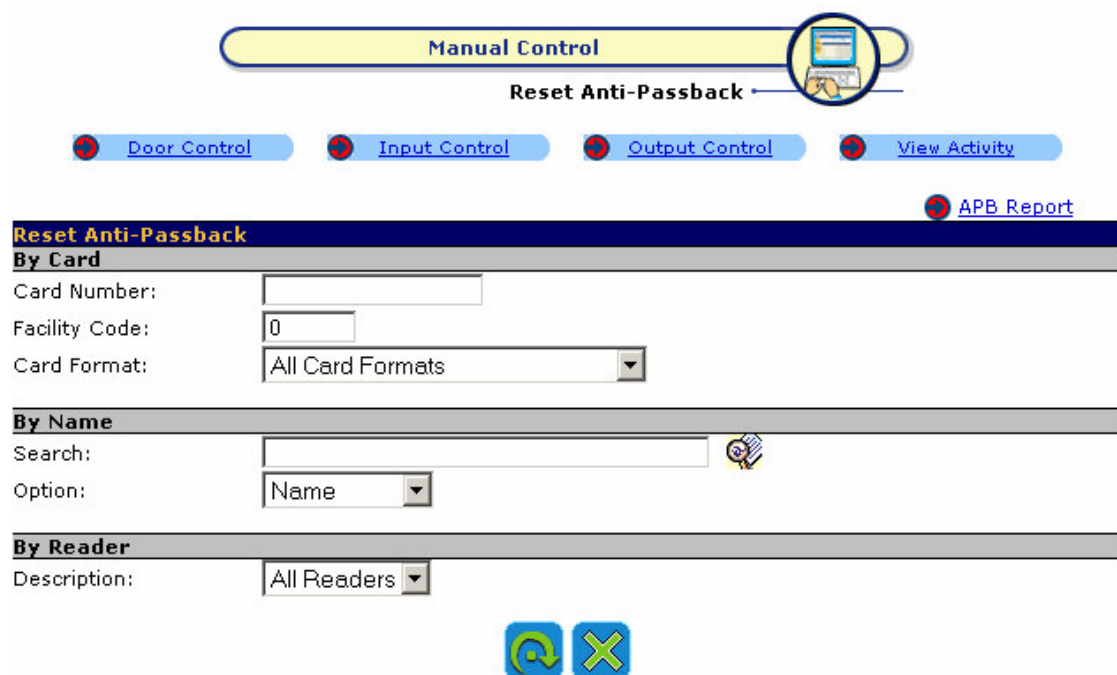
User is given the option to reset the APB violation with the following combination: -

- By Card number with respect to (wrt) Reader / All Readers, or
- By Name with respect to Reader / All Readers, or
- By All Card numbers with respect to Reader / All Readers.

To activate Reset APB

There are various ways to activate the Reset APB menu item. They are: -

1. From any menu item page, click on Reset APB hyperlink.
2. From the View Activity page, click on Reset APB hyperlink.
3. From any of the menu items page of the Manual Control Group.



The screenshot shows the 'Manual Control' interface. At the top, there is a yellow bar labeled 'Manual Control'. Below it, a blue bar contains the text 'Reset Anti-Passback'. To the right of this bar is a circular icon with a computer monitor and a hand. Below the blue bar, there are four buttons: 'Door Control', 'Input Control', 'Output Control', and 'View Activity', each with a red circular icon containing a plus sign. To the right of these buttons is a blue bar labeled 'APB Report' with a red circular icon containing a plus sign. Below the 'APB Report' bar, there is a section titled 'Reset Anti-Passback' with a yellow background. Under this section, there are three tabs: 'By Card', 'By Name', and 'By Reader'. The 'By Card' tab is selected. Under 'By Card', there are three fields: 'Card Number:' with a text input field, 'Facility Code:' with a text input field containing '0', and 'Card Format:' with a dropdown menu showing 'All Card Formats'. The 'By Name' tab is also visible, with a 'Search:' field and an 'Option:' dropdown menu showing 'Name'. The 'By Reader' tab is also visible, with a 'Description:' dropdown menu showing 'All Readers'. At the bottom of the form, there are two buttons: a green circular button with a white circular arrow and a blue square button with a white 'X'.

To reset APB based on Card Number wrt Reader / All Readers

To Reset APB based on Card Number, you must know the following, Card Number, its Facility Code, and its Card Format.

1. Enter the *Card Number* of the APB violator.
2. The number in the Facility Code field is configured in *Panel Setup, Default Settings*, if the code is different from the default, then change it.
3. Select the *Card Format* from the list.
4. Select the *Reader* from the list. If you want to Reset APB wrt all readers, select *All Readers*.

5. Click on the  button to proceed.
If the command is executed successfully, a message indicating APB reset by card & zones with respect to reader / all readers will be displayed.

6. Click on the  button to return.

To reset APB based on Name wrt Reader / All Readers

1. Enter a character, a portion, or the full name and click on the  button.
If a match is found that satisfied the entry, a window will appear with the Names. For example, enter John and click  button resulted in: -

By Name

Search: 

Names found:

John d'Baptist
John

Option:

Name ▼

2. From the window, select the appropriate name.
The selected name appears in the Name field.
3. Select the *Readers* from the list. If you want to Reset APB with respect to all readers, select *All Readers*.
4. Click on the  button to proceed.
If the command is executed successfully, a message indicating APB reset by name & zones with respect to reader / all readers will be displayed.
5. Click on the  button to return.

To reset APB by All Card numbers wrt Reader / All Readers

1. Select the *Readers* from the list. If you want to Reset APB with respect to all readers, select *All Readers*.
2. Click on the  button to proceed.
If the command is executed successfully, a message indicating APB reset by all cards & zones with respect to reader / all readers will be displayed.
3. Click on the  button to return.

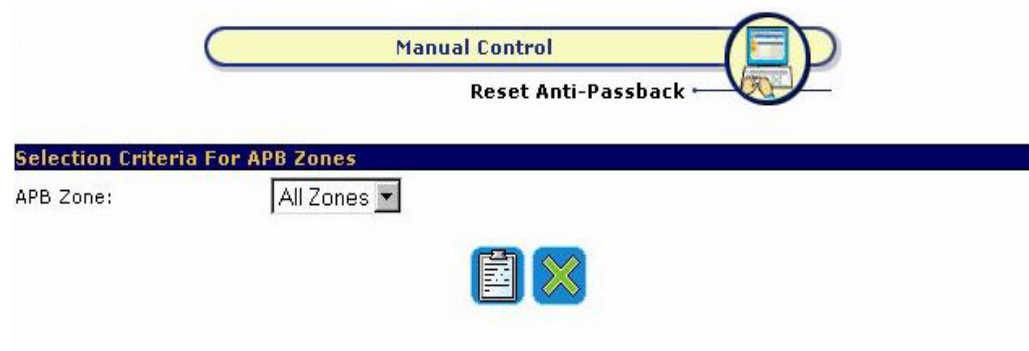
To generate a Print Preview of the report

The APB Zones report allows user to know which cardholder is in the APB Zone at the time of the preview. Should there be a need to Reset APB for a particular cardholder, the user can use this report to verify that the cardholder has actually violated the APB and not due to other condition such as an Expired Card Number.

To generate APB Zones Report

This report shows who are the cardholders still in the APB zones. When a cardholder enter an APB zone, by opening a door from an APB entry reader, he will be registered in the system as present in the APB zone governed by the APB entry reader. Similarly, when he exit the APB zone, by opening a door from an APB exit reader, he will be de-registered in the system as been present in the APB zone governed by the APB exit reader.

1. From the first web page of the Reset APB menu item, click on the  [APB Zones Report](#) link.



2. Select the desired *Zone* from the list.
3. Click on the  button for a print preview of the report.
The following screen-capture shows an example of the report.

[Return to View Activity](#) [Return To Reset APB](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

APB Report

Wednesday, 31 Aug 2005 14:00:47

APB Zone : All Zones

No	Card #	Name	Zone
1	23743	Bill Lee TH	Zone 2
2	23741	Micheal Gordon	Zone 1

[Return to View Activity](#) [Return To Reset APB](#) [Return To Selection Criteria](#)

If you wish to print out a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Reset APB web page, click on the [Return To Reset APB](#) link.
5. To return to the view activity page, click on the [Return to View Activity](#) link.
- 6.
7. To generate a preview of other zone, click on the [Return To Selection Criteria](#) link.

This Page Intentionally Left Blank

CHAPTER 12

Database Backup

This menu item allows user to choose two options, *Backup Database* to the Flash Memory or to the PC.

Backup Database To Flash Memory allows user to overwrite the database in the flash memory with the current parameters in the Dynamic Random Access Memory (DRAM). The flash memory acts as a permanent storage just like the computer's hard disk drive. Every time a Reboot is initiated, the Access Easy Controller software will access the flash memory for parameter setting, card database, ...etc. User is given the option to allow the Access Easy Controller to carry out an automatic backup at specific time of the day or to do it manually.

Backup Database To PC provides downloading of information which relates to the setting up of Access Easy Controller, for example: - Schedules details, Card Readers parameters...etc. It also allows user to download the history of the Activity and Attendance in *Comma Separated Variable* (CSV) format.

With the downloading, user can save the parameters (in encrypted zipped file) and the transactions as a backup on your computer hard disk or other external storage media, or floppy diskette.

WARNING!

This function required at least 2-3 minutes to complete. During this period, please do not switch off power to the Access Easy Controller or close your Web Browser application. You MUST wait till the downloading page appears before you could proceed to other page or close the Web Browser application. If this step is not followed, the backup operation will not be completed.

To activate Database Backup

The *Database Backup* can be activated only from the menu item page.

1. From any menu item page, click on the Database Backup hyperlink.

Panel Admin

Database Backup

Backup database To Flash Memory

Daily Backup Schedule: Hour Minute:

To PC

System Database Backup:
Save a backup copy of current RAM system database to your PC.

Activity, Audit Log and Attendance Records Backup:
Save a backup copy of current RAM activity, audit log and attendance records to your PC.

To define Daily Backup Schedule

1. Select the appropriate hour from the list.
2. Select the appropriate minute from the list.

3. Click on the button to confirm.

If you wish to disable this feature, select the “blank” for both Hour and Minute field as illustrated below.

Backup database To Flash Memory

Daily Backup Schedule: Hour Minute:

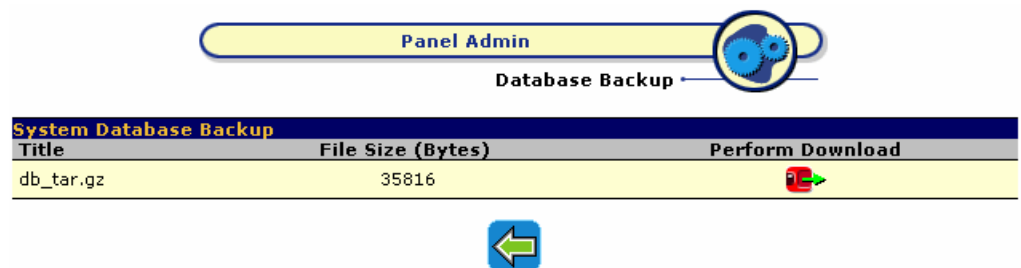
To Backup System Database To PC

This process involves two stages, when activated; the software will collect all parameter settings and zipped them up in an encrypted file called db_tar.gz. This encrypted file is only recognisable by the access easy controller thus providing security of its contents.

WARNING!

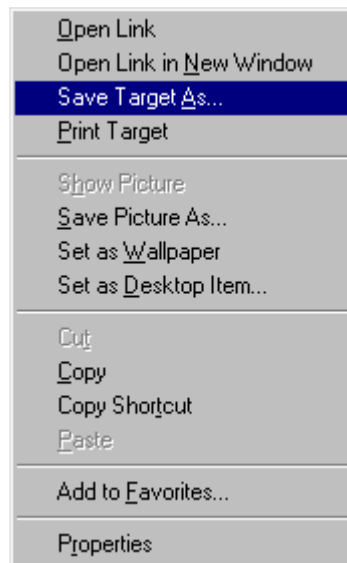
This function required at least 2-3 minutes to complete. During this period, please do not switch off power to either the computer or the Access Easy Controller.

1. Click on the  button and the system will start backing up the System Database into the encrypted file. Once that is done, the following web page appears.

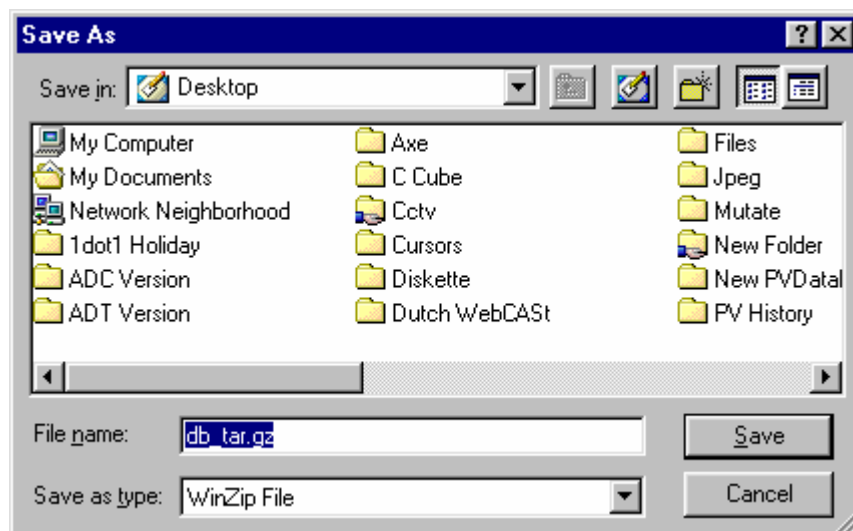


The web page shows the file name db_tar.gz with the file size.

2. Position the mouse pointer over the animating floppy diskette-like  icon and do a right click.
3. Select *Save Target As..* from the selection box.



The *Save As* dialog box appears.



The function of the *Save As* dialog box is the same as any Windows 95/98/NT software application, so it is very easy to select the destination location of the zip file.

NOTE: Do not change the default file name of the file. The Access easy controller will not recognise it when you port it back for database recovery purpose.

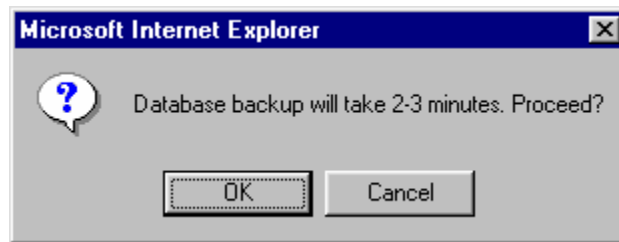
4. Click on the  button to proceed.

5. Click on the  button to return to the Database Backup web page.

Note : Some of the Web Browser application need only to click on the icon and it will prompt you immediately to save or to open the file. If that is the case choose the save option.

To Backup Activity, Audit log and/or Attendance Records to PC

1. Click on the  button. The following dialog box appears for confirmation.

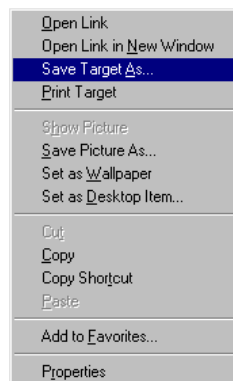


2. Click on the **OK** button to proceed.
The access easy controller software will update the activity.csv, auditlog.csv and attendance.csv file before showing the next web page.

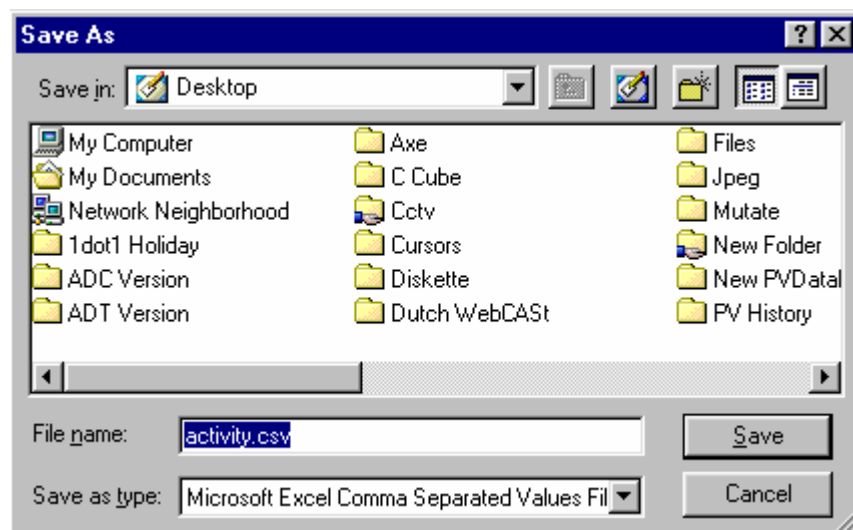
Panel Admin		
Database Backup		
Activity, Audit Log and Attendance Records Backup		
Title	File Size (Bytes)	Perform Download
activity.csv	469279	
auditlog.csv	12073	
attendance.csv	0	



3. Position the mouse pointer over the appropriate animating floppy diskette-like  icon and do a right click.
4. Select Save Target As.. from the selection box.



The Save As dialog box appears.



The function of the *Save As* dialog box is the same as any Windows 95/98/NT software application, so it is very easy to select the destination location of the csv file.

5. Click on the  button to proceed.
6. Click on the  button to return to the Database Backup web page.

CHAPTER 13

Panel Setup

This chapter covers a step by step guide to set up the *Panel Setup*.
In the *Panel Setup*, user is allowed to set the following configuration: -

- Network Settings,
- Input Point Configuration,
- Set Date & Time Setting,
- Auto Logout Timer,
- Audit Log,
- Default Settings,
- Card Format,
- Company Profile, and
- Email/SMS Configuration.
- Email Server Settings
- Dial in IP Settings
- Access Easy Master Settings
- SMS Server Settings

To activate Panel Setup

The *Panel Setup* can be activated only from the menu item page.

1. From any menu item page, click on Panel Setup link.

The screenshot shows the 'Panel Admin' interface. At the top, there is a 'Panel Admin' header with a gear icon and a 'Panel Setup' link. Below this, there are several menu items: Network Settings, Auto Logout Timer, Card Format, Input Point Configuration, Audit Log, Company Profile, Set Date & Time, Default Settings, Email/SMS Configuration, Email Server Settings, Dial In IP Settings, AEMC Settings, and SMS Server Settings. The 'Network Settings' menu item is selected, and the configuration page is displayed. The page shows fields for 'Panel's IP Address', 'Panel's IP Netmask', and 'Panel's Gateway'. Below these, there is a table for 'Remote PC Address' with columns for '#', 'IP Address', and 'PC Name'. At the bottom, there are three icons: a floppy disk, a red X, and a green arrow.

Panel Admin

Panel Setup

Network Settings, Auto Logout Timer, Card Format, Input Point Configuration, Audit Log, Company Profile, Set Date & Time, Default Settings, Email/SMS Configuration, Email Server Settings, Dial In IP Settings, AEMC Settings, SMS Server Settings

Network Settings

Panel's IP Address: 129 . 2 . 1 . 73
 Panel's IP Netmask: 255 . 255 . 0 . 0
 Panel's Gateway: 129 . 2 . 0 . 254

Remote PC Address

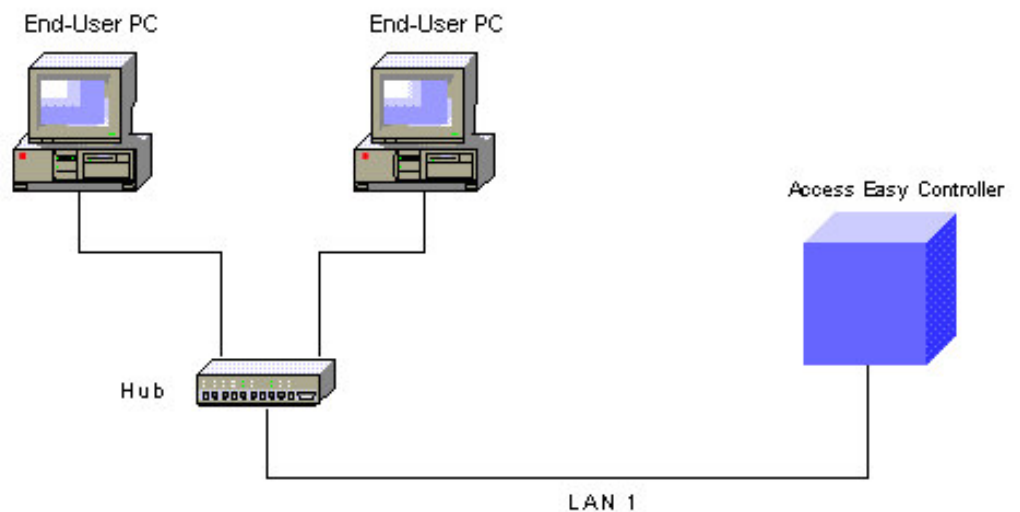
#	IP Address	PC Name
1	129 . 2 . 0 . 157	remotehost1
2	129 . 2 . 0 . 189	remotehost2
3	129 . 2 . 0 . 43	remotehost3

Save, Cancel, Next

Network Setting

This configuration allows user to configure the Panel's *IP*, *Netmask*, and *Gateway Address*. Each Access Easy Controller comes with 2 LAN ports, they are labelled as LAN1 and LAN2. These LAN ports are physically individual ports that have its own IP address.

LAN1 is connected to the network where the Access Easy Controller are accessed by other workstations, this is usually the office network. LAN2 is cater for further expansion.



In addition, user can define 3 Remote PC Addresses for ftp purposes and the address of the email server. User using Data Collector will also need to include the PC(IP Address) running the Data Collector software as one of the remote PC.

To Configure LAN 1 Network Setting

1. Click on the Network Setting to go to the Network Setting page. The IP Address setting presented is the network setting for LAN 1.
2. Highlight the default number in each of the IP Address's field and enter the appropriate number.
3. Repeat the above step for the Panel's *Netmask* and *Gateway*.
4. Click on the  button (see NOTE 1 and 2).

NOTE 1: In order for the new IP Address to take effect, the Controller needs rebooting.

NOTE 2: Always backup the Database before rebooting.

Remote PC Addresses

This allows user to set 3 dedicated personal computer's IP Address to allow user to download parameters using the utility program, Access Easy Controller Database Converter, and download/upload parameters to Access Easy Controller using other third party *File Transfer Protocol (FTP)* software.

NOTE: The use of the Access Easy Controller Database Converter program is governed by the user's access rights. Please refer to the Chapter for *Users* for detail. For usage of the utility program, please refer to the *Access Easy Controller Utility Programs User Manual*.

To edit Remote PC Addresses

1. Highlight the default number in each of the IP Address's field and enter the appropriate number.
2. Enter the PC Name as a complete word, with no spacing in between. You can use the **underscore** (_) to denote spacing.
3. Click on the  button.

Email Server Setup Information

This section allows user to define the address of the Outgoing Mail (SMTP) server, the SMTP port to use and the Access Easy Controller Email Address/Name. Click on the *Email Server Setting* link to goes to the Outgoing Mail (SMTP) server configuration page.

The screenshot shows the 'Panel Admin' interface with a 'Panel Setup' menu. The 'Email Server Settings' link is highlighted with a red box. Below the menu, the 'Network Settings' section is expanded, showing fields for Panel's IP Address (129.2.1.73), Panel's IP Netmask (255.255.0.0), and Panel's Gateway (129.2.0.254). Below this is a table for 'Remote PC Address' with three entries. At the bottom are icons for save, cancel, and back.

#	IP Address	PC Name
1	129.2.0.157	remotehost1
2	129.2.0.189	remotehost2
3	129.2.0.43	remotehost3

The Outgoing Mail (SMTP) Server defines the server that is to provide your email facilities and the Access Easy Controller Email Address/Name is the reply address for emails sent by the Access Easy Controller that is, the name address that is to appear in the 'sent to' field of the dispatched email.

The screenshot shows the 'Panel Admin' interface with a 'Panel Setup' menu. The 'Email Server Setup Information' link is highlighted. Below the menu, the 'Email Server Setup Information' section is expanded, showing fields for Outgoing Mail (SMTP) Server (129.2.0.86), Outgoing Mail (SMTP) Server Port (25), and AEC's Email Address/ Name (AEC@bosch.com.sg). At the bottom are icons for back, save, cancel, and forward.

To Configure the Email Server Setup Information

1. Highlight the default text in the Outgoing Mail (SMTP) Server field and enter the appropriate text.
2. The default number (25) is the commonly used port number for the Outgoing Mail (SMTP) Server, unless your configuration is different, we suggest you skip this field.
3. Enter the Access Easy Controller Address/Name as a complete word, with no spacing in between. You can use the **underscore** (_) to denote spacing. The Address/Name specified in this field will be used together with the Domain name to form the email address of the Access Easy Controller. Referring to the diagram and with the Domain name “bosch.com.sg”, the email address of Access Easy Controller becomes,

AEC@bosch.com.sg

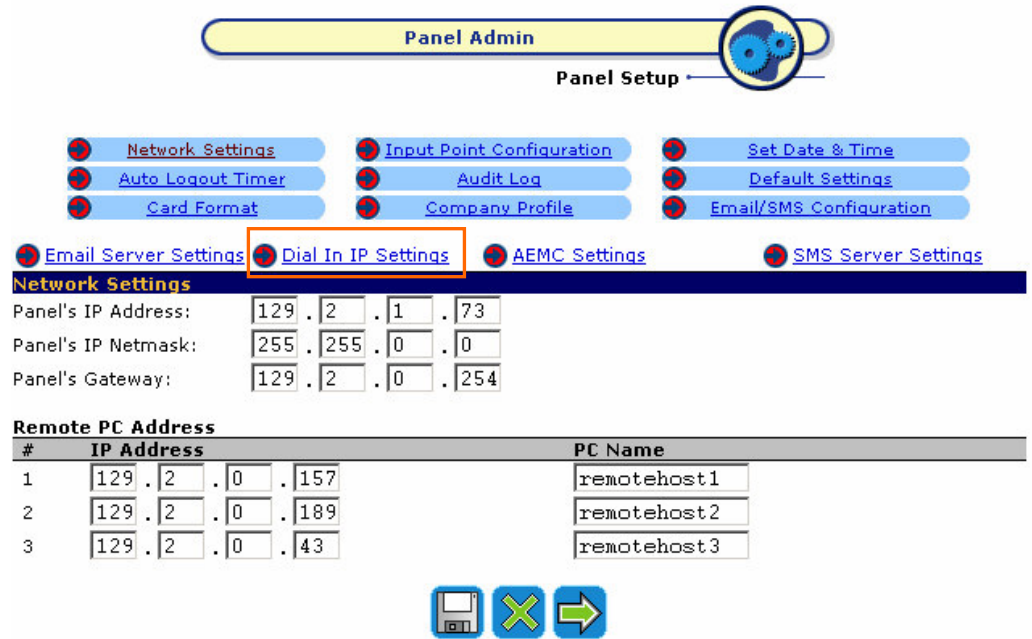


4. Click on the  button.

Dial In IP Setup Information

This section allows user to configure the Dial In IP that is required for PPP protocol. In order to have remote access ability using a modem for connection, a temporary IP address has to be issued to the incoming connection. When a user dialled in from home, using his PC and a modem, the Access Easy Controller's modem will answer the incoming call and negotiate with the remote modem for a suitable connection protocol and speed. If the process is successful, a temporary IP is issued to the remote modem and hence, connection is established.

By default, this *Dial in IP* address is set at **10.1.1.2**. It will work fine on most network setup, however, if the user encounters connection problem, it will need to be changed. To change this setting, click on the *Dial In IP Settings* to access to the setting page.



Panel Admin

Panel Setup

- Network Settings
- Auto Logout Timer
- Card Format
- Input Point Configuration
- Audit Log
- Company Profile
- Set Date & Time
- Default Settings
- Email/SMS Configuration
- Email Server Settings
- Dial In IP Settings**
- AEMC Settings
- SMS Server Settings

Network Settings

Panel's IP Address: 129 . 2 . 1 . 73

Panel's IP Netmask: 255 . 255 . 0 . 0

Panel's Gateway: 129 . 2 . 0 . 254

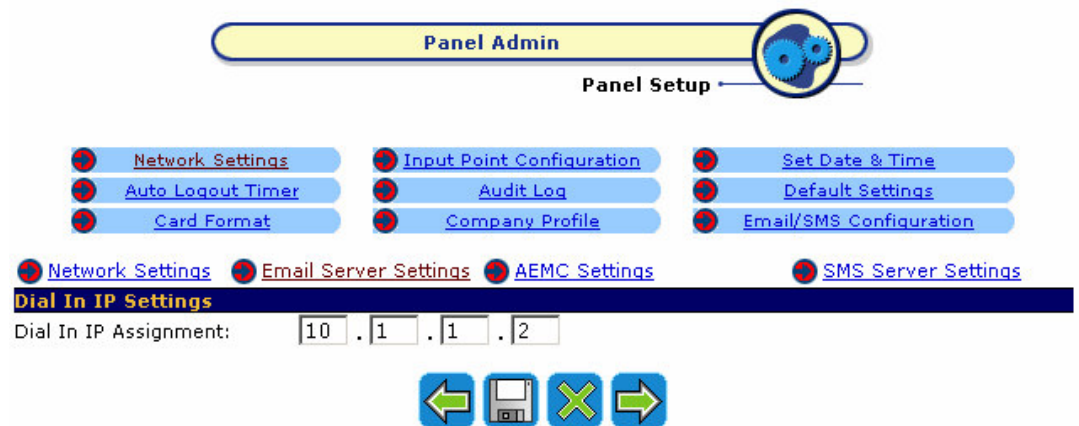
Remote PC Address

#	IP Address	PC Name
1	129 . 2 . 0 . 157	remotehost1
2	129 . 2 . 0 . 189	remotehost2
3	129 . 2 . 0 . 43	remotehost3

Save Cancel Back Forward

To edit the Dial In IP Settings Information

1. Highlight the default text in the Dial In IP Assignment fields and enter the appropriate IP address.



Panel Admin

Panel Setup

- Network Settings
- Auto Logout Timer
- Card Format
- Input Point Configuration
- Audit Log
- Company Profile
- Set Date & Time
- Default Settings
- Email/SMS Configuration
- Network Settings**
- Email Server Settings**
- AEMC Settings**
- SMS Server Settings**

Dial In IP Settings

Dial In IP Assignment: 10 . 1 . 1 . 2

Back Save Cancel Forward

2. Click on the  button.

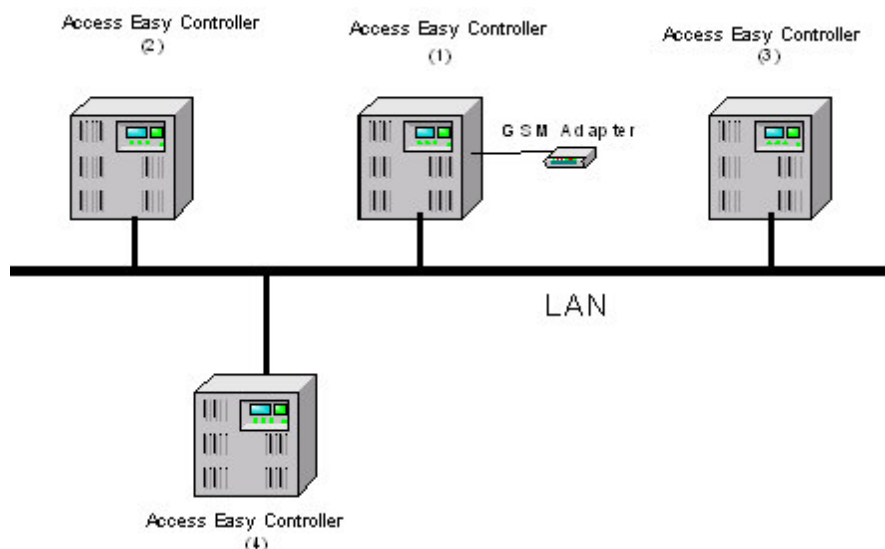
Access Easy Master Controller Settings

This section is not applicable for Access Easy Controller.

SMS Server Settings Information

This section allows user to define the IP address of the Access easy controller that has a GSM adapter attached to its serial com acting as the SMS server. To briefly understand how the SMS feature works, we need to understand how the system should be configured.

The following diagram shows a drawing that has more than one Access easy controller in the network. These controllers work stand-alone but shared a common GSM adapter, which is attached to a dedicated access easy controller serial com port.



The access easy controller (1) has the GSM adapter connected to its serial com port, hence, it is also acting as a SMS Server to help relay the other Access easy controller messages to the Service Provider.

Whenever, there is any SMS message that needed to be send, the respective Access easy controller will send the SMS messages over to the Access easy controller SMS Server and the SMS Server will send via the GSM adapter to the Service Provider. These controllers are defined as the SMS Client. Hence, there is a need to control which is the IP Address that is allowed to send SMS, this is to prevent unauthorised personnel sending SMS via your access easy controller.

To Configure Access easy controller as a SMS Server

By default, the *SMS Server IP* address is blank. If this controller is attached to a GSM adapter, you will need to configure the IP address of other Access easy controller that will send SMS message through it. To change this setting, click on the *SMS Server IP Settings* to access to the setting page, as shown in the following diagram.

Panel Admin

Panel Setup

- Network Settings
- Auto Logout Timer
- Card Format
- Input Point Configuration
- Audit Log
- Company Profile
- Set Date & Time
- Default Settings
- Email/SMS Configuration
- Email Server Settings
- Dial In IP Settings
- AEMC Settings
- SMS Server Settings**

Network Settings

Panel's IP Address: 129 . 2 . 1 . 73

Panel's IP Netmask: 255 . 255 . 0 . 0

Panel's Gateway: 129 . 2 . 0 . 254

Remote PC Address

#	IP Address	PC Name
1	129 . 2 . 0 . 157	remotehost1
2	129 . 2 . 0 . 189	remotehost2
3	129 . 2 . 0 . 43	remotehost3

Icons: Save, Cancel, Back

1. The SMS Server Setting page is shown below:

Panel Admin

Panel Setup

- Network Settings
- Auto Logout Timer
- Card Format
- Input Point Configuration
- Audit Log
- Company Profile
- Set Date & Time
- Default Settings
- Email/SMS Configuration
- Network Settings
- Email Server Settings
- Dial In IP Settings
- AEMC Settings
- Short Message Service (SMS) Server Settings**

Short Message Service (SMS) Server Settings

SMS Server IP:

GSM Modem Connected? ☐ Yes ☒ No

Icons: Back, Save, Cancel

2. Since this is an SMS Server, we will select "Yes" for GSM Modem Connected?" and click the save button.
3. You will need to reboot the Access easy controller for the changes to take place.

4. After rebooting, goes back to the SMS Server page and you will see the following :

[Network Settings](#) [Input Point Configuration](#) [Set Date & Time](#)
[Auto Logout Timer](#) [Audit Log](#) [Default Settings](#)
[Card Format](#) [Company Profile](#) [Email/SMS Configuration](#)

[Network Settings](#) [Email Server Settings](#) [Dial In IP Settings](#) [AEMC Settings](#)

Short Message Service (SMS) Server Settings

GSM Modem Connected? ☒ Yes ☐ No

#	IP Address	AEC Panel Name
1	0 . 0 . 0 . 0	
2	0 . 0 . 0 . 0	
3	0 . 0 . 0 . 0	
4	0 . 0 . 0 . 0	
5	0 . 0 . 0 . 0	
6	0 . 0 . 0 . 0	
7	0 . 0 . 0 . 0	
8	0 . 0 . 0 . 0	
9	0 . 0 . 0 . 0	
10	0 . 0 . 0 . 0	

5. There are up to 10 Remote Controller addresses that you could configure. These addresses are the IP Address of those access easy controllers that send SMS messages via the SMS Server.



6. Click on the  button to save the new settings.

To Configure Access easy controller as a SMS Client

By default, the *SMS Server IP* address is blank. If this controller is not attached to a GSM adapter, it is a SMS Client and hence need to identify the IP Address of the SMS Server. To change this setting, click on the *SMS Server IP Settings* to access to the setting page, as shown in the following diagram.

Panel Admin

Panel Setup

- Network Settings
- Input Point Configuration
- Set Date & Time
- Auto Logout Timer
- Audit Log
- Default Settings
- Card Format
- Company Profile
- Email/SMS Configuration
- Email Server Settings
- Dial In IP Settings
- AEMC Settings
- SMS Server Settings**

Network Settings

Panel's IP Address: 129 . 2 . 1 . 73

Panel's IP Netmask: 255 . 255 . 0 . 0

Panel's Gateway: 129 . 2 . 0 . 254

Remote PC Address

#	IP Address	PC Name
1	129 . 2 . 0 . 157	remotehost1
2	129 . 2 . 0 . 189	remotehost2
3	129 . 2 . 0 . 43	remotehost3

Icons: Save, Cancel, Next

1. The SMS Server Setting page is shown below:

Panel Admin

Panel Setup

- Network Settings
- Input Point Configuration
- Set Date & Time
- Auto Logout Timer
- Audit Log
- Default Settings
- Card Format
- Company Profile
- Email/SMS Configuration
- Network Settings
- Email Server Settings
- Dial In IP Settings
- AEMC Settings

Short Message Service (SMS) Server Settings

SMS Server IP:

GSM Modem Connected? ☐ Yes ☒ No

Icons: Back, Save, Cancel

2. Since this is an SMS Client, we will need to enter the IP Address of the SMS Server in the "SMS Server IP" field and click the save button.
3. You will need to reboot the Access easy controller for the changes to take place.

Note : Due to there is a limited number of Serial com port available in the CPU, only either the GSM adapter or the Analogue Dial-up modem can be connected to the Access easy controller, hence, dial-up features will not be enable when SMS server is be configured, like wise to the SMS server when Dial-up is been setup.

Input Point Configuration

The state of each Input point must be closed in order for the Access Easy Controller to treat it as *normal* state. However, there are some devices whereby its normal state is open thus, representing an activated / alarm state.

When such devices are connected to these Input points, without inverting an input's to the *normal* state, it would cause unexpected or false alarm. In simple term, this configuration allows user to invert the *logical* state of the input that is seen by the Access Easy Controller thus allowing such devices to be used.

Access Easy Controller allows all the Input Points to be inverted except those assigned to Exit Readers and Arm/Disarm Readers.

To activate Input Point Configuration

1. From the *Panel Setup* screen, click on the *Input Point Configuration* link.

The screenshot shows the 'Panel Admin' interface with a 'Panel Setup' menu. The 'Input Point Configuration' link is highlighted. Below the menu, there are sections for 'Readers 1-8', 'Readers 9-16', 'Inputs 1-16', and 'Inputs 17-32'. The 'Input Point Configuration' section is expanded, showing a table of input points.

Inverted Input #	Description	2 State Supervised	Non 2 State Supervised	4 State Supervised
1	Main Entrance - Request to Exit	☐	☒	☐
2	Main Entrance - Door Contact	☐	☒	☐
3	Side Entrance - Request to Exit	☐	☒	☐
4	Side Entrance - Door Contact	☐	☒	☐
5	R&D Dept Entry Reader - Request to Exit	☐	☒	☐
6	R&D Dept Entry Reader - Door Contact	☐	☒	☐
7	Production Dept Entry Reader - Request to Exit	☐	☒	☐
8	Production Dept Entry Reader - Door Contact	☐	☒	☐
9	Production Dept Exit Reader - Request to Exit	☒	☐	☐
10	Production Dept Exit Reader - Door Contact	☒	☐	☐
11	Elevator Reader - Request to Exit	☒	☐	☐
12	Elevator Reader - Door Contact	☒	☐	☐

NOTE: Input 9 and 10 are assigned for Reader #1 and #2 respectively. Since these two readers are defined as Exit Reader and Arm/Disarm Reader respectively, the check boxes are disabled.

To select Input Point Configuration

Using Manual

This is the default selection.

1. To assign the required *Input Point Configuration* for the inversion, click on the corresponding *Input Point Configuration* check boxes to show a tick (✓) mark. To de-select the point, click on it again.
2. Select the appropriate state.

3. Click on the  button. Alternatively, click on the  button to select the next sets of Input Points.

Using Select All

This is very useful if the number of Input Points need to be selected is more than ¾ of what is displayed. You can use this function then de-select those unwanted Input Points.

NOTE: The **Select All** and the **Clear All** function will only select / clear the 16 Input Points seen on the current web page, the other 48 Points are not affected.

4. To select all, click on the *Select All* radio button. To de-select, click on *Clear All* or *Manual* radio button.

5. Click on the  to refresh the screen and the selection returns to default (Manual is selected).

If not all *the Inverted Input Points* are required, proceed to de-select by clicking on its corresponding check boxes. However, if all Points are

required, you can straight away click on the  button to save.

Alternatively, click on the  button to go to next sets of Input Points.

Using Clear All

This function works in reverse of the *Select All* function. Please refer to the above procedure.

Support Configurable 2 State Non-Supervised, 2 State Supervised and 4 State Supervised For All Input Points in The Panel

This will provide the system installer to have the flexibility of configuring any input in the panel to be in any monitoring requirement.

The panel will report fault in open or short condition only when the input is configured as 4 State Supervised monitoring.

[Readers 1-8](#)
[Readers 9-16](#)
[Inputs 1-16](#)
[Inputs 17-32](#)

Input Point Configuration

☐ Inverted Input Points
 ☐ Clear All
 ☐ Select All
 ☒ Manual

Inverted Input #	Description	2 State Non Supervised	2 State Supervised	4 State Supervised
1	☐ Main Entrance - Request to Exit	☐	☒	☐
2	☐ Main Entrance - Door Contact	☐	☒	☐
3	☐ Side Entrance - Request to Exit	☐	☒	☐
4	☐ Side Entrance - Door Contact	☐	☒	☐
5	☐ R&D Dept Entry Reader - Request to Exit	☐	☒	☐
6	☐ R&D Dept Entry Reader - Door Contact	☐	☒	☐
7	☐ Production Dept Entry Reader - Request to Exit	☐	☒	☐
8	☐ Production Dept Entry Reader - Door Contact	☐	☒	☐
9	☒ Production Dept Exit Reader - Request to Exit	☒	☐	☐
10	☒ Production Dept Exit Reader - Door Contact	☒	☐	☐
11	☐ Elevator Reader - Request to Exit	☒	☐	☐
12	☐ Elevator Reader - Door Contact	☒	☐	☐

Set Date & Time

The Access Easy Controller software allows user to set the *Date* and *Time* of the real-time clock within the controller. For countries that practice Daylight Saving Time, the feature is included. Time setting is in the 24-hour format.

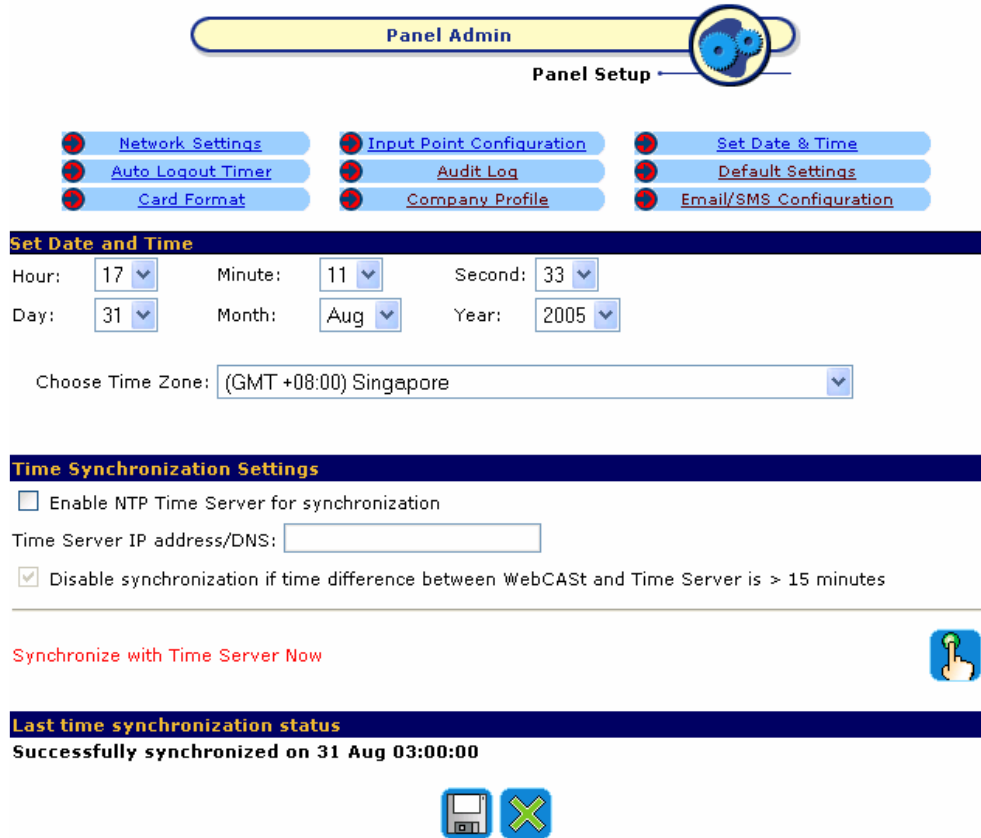
The Date and Time set here is displayed on the status bar of the web browser during the View Activity.

An additional function is implemented to allow user to maintain date and time synchronization with a timeserver. With synchronization on all of Access easy controller, user can ensure that events that happen in sequence on different controller can be analysed correctly.

Access easy controller only support NTP Time server, it will performs synchronization with the NTP Time server every night at 3am.

To activate Date & Time Setting

1. From the *Panel Setup* screen, click on the *Set Date & Time* bar.



The screenshot shows the 'Panel Admin' interface with a 'Panel Setup' tab selected. Under the 'Panel Setup' tab, there are several configuration options: Network Settings, Auto Logout Timer, Card Format, Input Point Configuration, Audit Log, Company Profile, Set Date & Time, Default Settings, and Email/SMS Configuration. The 'Set Date & Time' option is highlighted.

Set Date and Time

Hour: 17 Minute: 11 Second: 33
 Day: 31 Month: Aug Year: 2005

Choose Time Zone: (GMT +08:00) Singapore

Time Synchronization Settings

☐ Enable NTP Time Server for synchronization

Time Server IP address/DNS:

☒ Disable synchronization if time difference between WebCAST and Time Server is > 15 minutes

Synchronize with Time Server Now 

Last time synchronization status

Successfully synchronized on 31 Aug 03:00:00

To set the Date & Time

1. Select the appropriate hour from the list.
2. Do likewise for the *Minute*, *Second*, *Day*, *Month*, and *Year* field.
3. Select your Time Zone from the list and click on the  button.

NOTE: If your country is not listed, please select an alternative country that uses the same Time Zone.

To set the Time Synchronization

1. Select *Enable NTP Time server for synchronization* and key in the IP address of the Timeserver PC

Note: Refer to Appendix D on *Setting up a Timeserver PC*. *Time Server Address/DNS* input is the IP address of the PC being configured as a time server PC. Access easy controller is only able to synchronize with a NTP time server and will sync at 3 A.M daily automatically.

Auto Time synchronization at 3 A.M is only logged at transaction, however if user manually synchronise with the timer server, audit log will be logged.

2. Select *Disable synchronization if time difference between Access easy controller and Time Server is >15 minutes* if you want the access easy controller to synchronize its time even if the difference is more than 15 minutes. This feature should be enabled to prevent the access easy controller from synchronizing the wrong time with the Time server that is not accurate or timezone that is incorrect.

Synchronizing date & time with a internet Time Server

Access easy controller is not able to synchronize with an internet Time Server if it is behind a firewall or proxy server. If it is outside the firewall or in a DMZ, you could enter the IP address of the Time Server in the *Time Server Address/DNS* input. Do not enter the domain name of the Time Server (eg. Time.windows.gov) in this input, access easy controller will not be able to resolve the name to an IP address.

Synchronizing date & time with an intranet Time Server

It is recommended that access easy controller should synchronize its date & time to an intranet (internal) Time Server. Most of the office has an internal Time Server, this Time Server will synchronize it's date & time with an internet (external) Time Server, while all other PCs in the office synchronize with this intranet Time Server.

If the office does not have a intranet Time Server, you could setup any existing PC on the network as a Time Server, hence, the access easy controller could synchronize its' date and time with this PC. There are numerous freeware available that you could install in this PC to synchronize its date and time with an external Time Server.

In Appendix D, we will briefly descript how you could setup a PC as a Time Server.

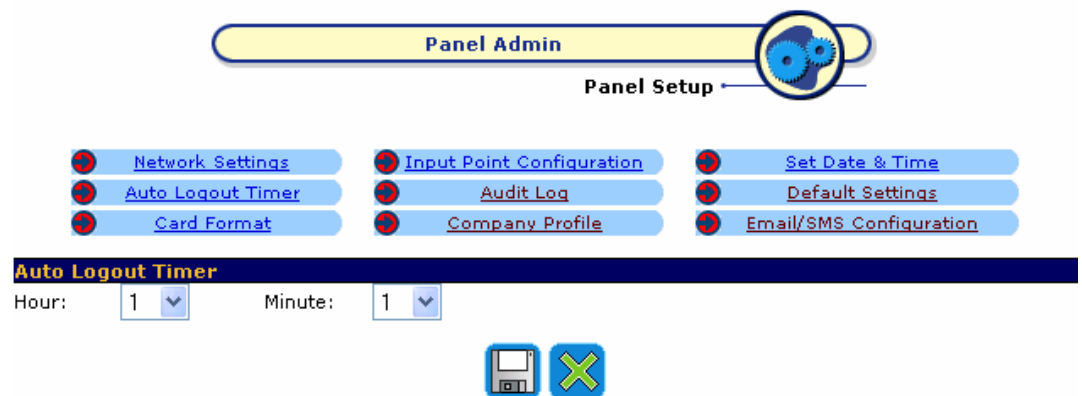
Auto Logout Timer

This configuration allows user to set the timer for the Access Easy Controller software to *Logout* automatically if it detects no user activity. Default setting is 1 hour.

NOTE: This Timer setting is applicable to all menu items except View Activity.

To activate Auto Logout Timer

1. From the *Panel Setup* screen, click on the *Auto Logout Timer* link.



To edit the Auto Logout Timer

1. Select the hour and minutes from the list.
2. Click on the  button.

Audit Log

The Access Easy Controller keeps 2 types of log.

- User Log
- System Log

User log tracks the Users operation on the Access Easy Controller, it logs all the action performed by the user, such as manual on/off any output, change the settings for a Cardholder, set the date and time, etc.

It is a form of audit trail that could be used to keep track of what are the changes done of the system.

System log keep track of some of the important information of the system, such as mac address, last boot time, current boot time, version of the software, etc.

To View the User Log

1. Click on the *Audit Log* on any of the *Panel Setup* page and the following page will be shown.

The screenshot shows the 'Panel Admin' interface. At the top, there is a yellow bar with 'Panel Admin' and a blue gear icon. Below it, a blue bar contains 'Panel Setup'. A grid of nine blue buttons with red circular icons is displayed, including 'Network Settings', 'Input Point Configuration', 'Set Date & Time', 'Auto Logout Timer', 'Audit Log' (highlighted), 'Default Settings', 'Card Format', 'Company Profile', and 'Email/SMS Configuration'. Below this grid is a dark blue header 'Selection Criteria for Audit Log'. Under this header, there are two radio buttons: 'User Log' (selected) and 'System Log'. The 'User Log' section contains form fields for 'From' and 'To' dates, each with 'Day', 'Month', and 'Year' dropdown menus, and a 'Name' dropdown menu currently set to 'All Names'. At the bottom of the form are two icons: a clipboard and a green 'X'.

2. Select the radio button for the User Log, as shown above.
3. Choose the From date and To date, from the pull-down list.
4. Select the User Name from the pull-down list box of the field Name. If a particular User has been selected, the report will only shows the operation of that User. If "All Names" is selected, the result will be a report containing all the action taken by all users on this system.



5. Click the  button to request Access Easy Controller to enquiry for the report.
6. The following is a screen capture of how the report will look like.

Selection Criteria for Audit Log

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

User Log

Tuesday, 13 Sep 2005 14:35:54

From : -----
To : -----
Name : All Names

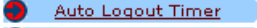
No	Date/Time	Name	Action Description
1	12 Sep 2005/15:51:44	USER1	Logged in
2	12 Sep 2005/15:52:04	USER1	Added card #1
3	12 Sep 2005/15:54:57	USER1	Logged out
4	12 Sep 2005/15:57:42	USER1	Logged in
5	12 Sep 2005/16:07:45	USER1	Logged in
6	12 Sep 2005/16:12:37	USER1	Changed card setting #111
7	12 Sep 2005/16:13:42	USER1	Changed reader setting:Reader 2
8	12 Sep 2005/16:14:22	USER1	Changed schedule:Undefined Schedule 1
9	12 Sep 2005/16:19:28	USER1	Changed schedule:Undefined Schedule 1
10	12 Sep 2005/16:20:03	USER1	Changed schedule:Undefined Schedule 1
11	12 Sep 2005/16:21:37	USER1	Changed reader setting:Reader 5
12	12 Sep 2005/16:21:51	USER1	Changed reader setting:Reader 6

To View System Log

1. Click on the Audit Log on any of the Panel Setup page and the following page will be shown.



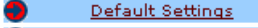
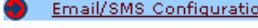








Selection Criteria for Audit Log

☐ User Log

From: Day: Month: Year:

To: Day: Month: Year:

Name:

☒ System Log



2. Select the radio button for the System Log, as shown above.
3. Click on the button to request Access Easy Controller to enquiry for the report.
4. The following is a sample of the System Log.

[Selection Criteria for Audit Log](#)**Bosch Security Systems Pte Ltd**

38C Jalan Peminpin Singapore 577180

System Log

Friday, 23 Dec 2005 15:35:07

```

Product Name           : AEC 5.6.37.27-2
Hardware Address (MAC) : 00:04:5F:80:36:A8
Internet Address       : 172.16.10.92
Last Boot Time        : Wed Dec 21 19:15:31 SGT 2005
Current Boot Time     : Fri Dec 23 15:16:19 SGT 2005
Last Backup Time to Flash : -----

```



```

No. of Converter/s Exist : 2
Converter # 1             : Reader Ports: 01,02,03,04,05,06,07,08
                          : Reader IO: 01-08,09-16
Converter # 3             : Reader Ports: 09,10,11,12,13,14,15,16
                          : Reader IO: 17-24,25-32
SIM serial number        : 7D5B0F18FBD1

```

[Selection Criteria for Audit Log](#)

The following table provides a brief explanation of the content of the System Log.

Items on the report	Explanation
Product Name	Version number of the Access easy controller
Hardware Address (MAC)	This is the mac address of the Access easy controller, it is the physical address. This information could be used in the ARP command to set the IP address of the Access easy controller.
Internet Address	This is the IP address of the Access easy controller.
Last Boot Time	This indicates the previous time that the controller was rebooted via the <i>Reboot</i> link.
Current Boot Time	This indicates the most recent time that the controller was rebooted via the <i>Reboot</i> link. The next reboot using the <i>Reboot</i> link will shift this information to the Last Boot Time column.
Last Backup Time to Flash	This indicates the most recent time that the Database was backup. Database Backup could be done manually, or automatically on a daily basis.
No. of Converter/s exists	Shows how many Converter(s) card are connected to the CPU.
Converter # n (“n” denotes the address of the Converter Card)	This indicates the Readers, Input and outputs that this Converter is connected to.
SIM Serial Number	The serial number of the SIM card in the Secure/Communication Card.

Default Settings

This setting allows user to define the descriptive *Name* for the two user fields and the global Facility Code that will appear under the title *Card Details* in *Card Assignment*. These user fields are limited to 20 character entries each while the Facility code range depends on the Card Format in use.

Other than that, the number of transaction records to view on screen for the View Activity menu can also be set in the *Default Setting* screen. Although this setting affect the number of transaction records to view on screen, should there be alarms that is not acknowledged by the user, the View Activity records will expand to show all transactions from the first “not acknowledged” alarm up to the latest transaction. In simple word, the View Activity is dynamic and will show those “not acknowledged” Alarm transactions up to the latest transactions. The number of records to view ranges from 10 to 70 in step of 10 records.

Please refer to the Chapter on *View Activity* for detail on Acknowledging (ACK) alarms.

By default, when the user click on the *View Activity* hyperlink, it will bring him to the Alarm View, however, the user is able to customized the default view screen by changing the setting in the *Default Setting*.

To activate Default Settings

1. From the *Panel Setup* screen, click on the *Default Settings* link.

Panel Admin

Panel Setup

[Network Settings](#)
[Input Point Configuration](#)
[Set Date & Time](#)

[Auto Logout Timer](#)
[Audit Log](#)
[Default Settings](#)

[Card Format](#)
[Company Profile](#)
[Email/SMS Configuration](#)

Default Settings

User Definable Fields

User Field 1:

User Field 2:

Facility Code

Facility Code:

View Activity Setting

Number of Transactions To View:

Default Activity View:

To edit View Activity Setting

1. Select the appropriate number from the list.
2. Click on the  button to save.

To edit Default Activity View Setting

1. Select the appropriate view from the list. There are 5 types of views; All, Alarm, Valid, Restore and Time Attendance.
2. Click on the  button to save.

To edit the User Definable Fields and Facility Code

1. Highlight the default text and enter the new *Description* for *User Field 1*.
2. Repeat for *User Field 2*.
The above example shows that the *User Field 1 and 2* is used for *Mobile* and *Emergency Number* entry in the *Card Assignment* respectively.
3. Highlight the default text and enter the new *Facility Code* (you can obtain this code from your card supplier, enter "0" if the Card Format doesn't support Facility Code).
4. Click on the  button.

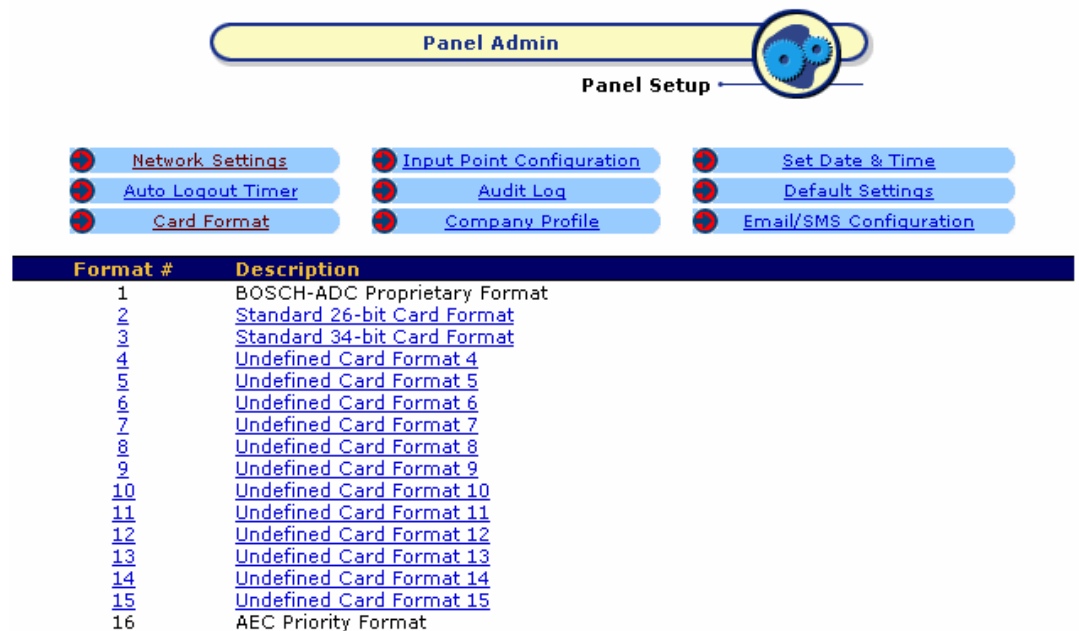
Card Format

This setting allows user to customise the Access Easy Controller to accept up to 16 different types of Wiegand Card Format. Card Format up to a maximum of 64-Bit and up to 8 Parity Format is configurable.

By default, the **BOSCH-ADC Proprietary Card Format** and the standard **AEC Priority Format**, which have been pre-assigned to Format #1 and #16 respectively.

To activate Card Format

1. From the *Panel Setup* screen, click on the *Card Format* link.



Format #	Description
1	BOSCH-ADC Proprietary Format
2	Standard 26-bit Card Format
3	Standard 34-bit Card Format
4	Undefined Card Format 4
5	Undefined Card Format 5
6	Undefined Card Format 6
7	Undefined Card Format 7
8	Undefined Card Format 8
9	Undefined Card Format 9
10	Undefined Card Format 10
11	Undefined Card Format 11
12	Undefined Card Format 12
13	Undefined Card Format 13
14	Undefined Card Format 14
15	Undefined Card Format 15
16	AEC Priority Format

To configure Card Format

1. Click on the *Card Format's* numbering or the *Description* text to proceed.

The screenshot shows the 'Panel Admin' software interface. At the top, there is a yellow header bar with 'Panel Admin' and a gear icon. Below it, a blue bar indicates 'Panel Setup'. A grid of nine blue buttons with red circular icons is displayed, including 'Network Settings', 'Auto Logout Timer', 'Card Format', 'Input Point Configuration', 'Audit Log', 'Company Profile', 'Set Date & Time', 'Default Settings', and 'Email/SMS Configuration'. The 'Card Format' button is highlighted. Below the buttons, the 'Format #' is set to '3' and the 'Description' field contains 'Undefined Card Format 3'. The 'Card Format' section is expanded, showing fields for 'Card Encoded Format:', 'Parity Format 1:', and 'Parity Format 2:'. Below these fields are five icons: a floppy disk, a red X, a circular arrow, a green arrow, and a clipboard. A 'Legend' section is at the bottom, listing symbols for Parity Bit, Facility code, Card Number, Even Parity Bit, Odd Parity Bit, Blank, Parity Bit Location, Binary 0, and Binary 1.

Panel Admin

Panel Setup

Network Settings Input Point Configuration Set Date & Time

Auto Logout Timer Audit Log Default Settings

Card Format Company Profile Email/SMS Configuration

Format #: 3

Description: Undefined Card Format 3

Card Format

Card Encoded Format:

Parity Format 1:

Parity Format 2:

Legend

P or p	Parity Bit
F or f	Facility code
C or c	Card Number
E or e	Even Parity Bit
O or o	Odd Parity Bit
B or b	Blank
X or x	Parity Bit Location
0	Binary 0
1	Binary 1

2. Highlight the default text and enter a Description for this *Card Format*.
3. Enter the format for the Card Encoded Format field accordingly.
4. Repeat for Parity Format 1 (see NOTE 1).

NOTE 1: The entries to this field must not contain Parity Bit Location that depends on the resultant Parity Bit of the next or higher (Parity Format 2 to 8) Parity Format field entries.

5. Repeat for Parity Format 2 (please apply the condition in NOTE 1 here and for subsequent Parity Format fields).

NOTE 2: If the Card Format doesn't support Parity checking, leave the All Parity Format fields blank.

In order to understand how to configure the different format, the standard 26-Bit Wiegand Card Format will be used as an example.

Example: 26-Bit Wiegand Card Format

The 26-bits of transmission from the reader to the Access Easy Controller consists of two parity bits and 24 code bits. The first transmitted bit is the Even parity bit E, it is calculated over the first 12 bits. The last bit transmitted is the Odd parity O, it is calculated over the last 12 bits.

The string of bits for this code format is show in the following tables. Due to the lack of space, the 26-Bits is split into two separate rows of 13 each.

Code Format

1	2	3	4	5	6	7	8	9	10	11	12	13
E	F	F	F	F	F	F	F	F	C	C	C	C

14	15	16	17	18	19	20	21	22	23	24	25	26
C	C	C	C	C	C	C	C	C	C	C	C	O

Legend:

E: Resultant Even Parity Bit

F: Facility Code Bit

C: Card Number Bit

O: Resultant Odd Parity Bit

Parity Format

1	2	3	4	5	6	7	8	9	10	11	12	13
P	E	E	E	E	E	E	E	E	E	E	E	E

14	15	16	17	18	19	20	21	22	23	24	25	26
O	O	O	O	O	O	O	O	O	O	O	O	P

Legend:

E: Even Parity Bit Location

P: Resultant Even and Odd Parity Bit

O: Odd Parity Bit Location

In order for the Access Easy Controller to decode the data string correctly, we need to configure the code accordingly.

Referring to the Code Format Table

For Card Encoded Format

1. Enter P or p for the resultant Even (E) and Odd (O) Parity Bit
2. Enter F or f for the Facility Code Bit (F)
3. Enter C or c for the Card Number Bit (C)

Referring to the Parity Format Table

For the Odd Parity Format (Parity Format 1).

1. Enter O or o for the resultant Odd Parity Bit (O)
2. Enter X or x for Odd Parity Bit Location.
3. Enter B or b otherwise.

For the Even Parity Format (Parity Format 2).

1. Enter E or e for the resultant Even Parity Bit (E)
2. Enter X or x for Even Parity Bit Location.
3. Enter B or b otherwise.

With the information, proceed to configure the Card Format as shown below.

Panel Admin


Panel Setup

 [Network Settings](#)

 [Input Point Configuration](#)

 [Set Date & Time](#)

 [Auto Logout Timer](#)

 [Audit Log](#)

 [Default Settings](#)

 [Card Format](#)

 [Company Profile](#)

 [Email Configuration](#)

Format #:

Description:

Card Format

Card Encoded Format:

Parity Format 1:

Parity Format 2:







Legend

P or p	Parity Bit
F or f	Facility code
C or c	Card Number
E or e	Even Parity Bit
O or o	Odd Parity Bit
B or b	Blank
X or x	Parity Bit Location
0	Binary 0
1	Binary 1

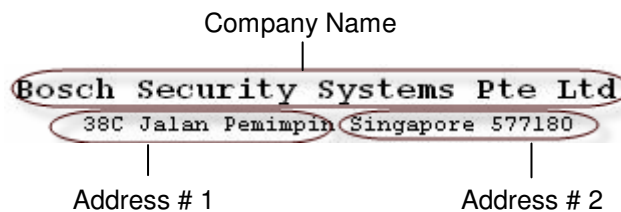
If you have Card Format that has more than 2 Parity Format (maximum is

8), click on the  button to configure them else just save the configuration and list.

TIP: To best distinguish between the alphabet “O” and the number “0”, it is recommended that you use all lower case entry.

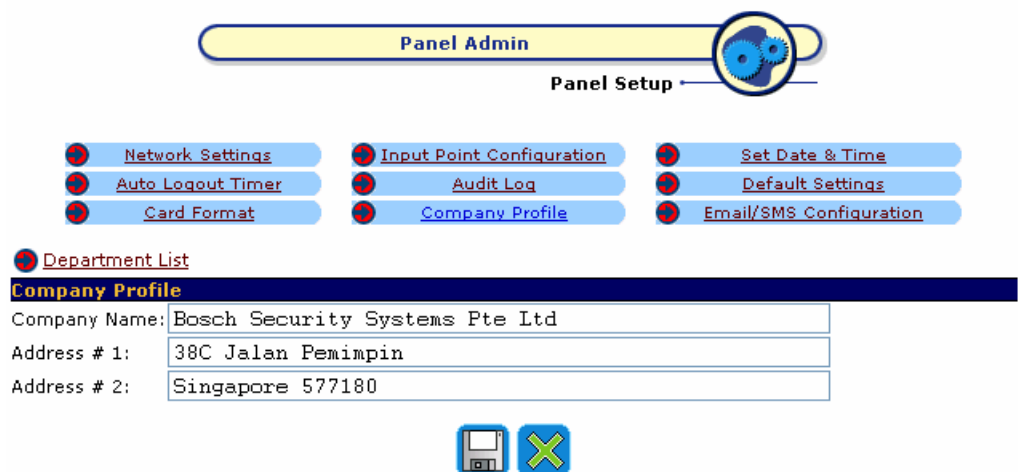
Company Profile

The Company Profile feature is used as a letterhead in all the report generation. Each field is limited to a 50-characters entry, including punctuation. Using the default as an example, the letterhead will have the following format: -



To activate Company Profile

1. From the *Panel Setup* screen, click on the *Company Profile* link.



To edit Company Profile

1. Highlight the default text and enter the desired *Company Name*.
2. Do likewise for the Address #1 and Address #2 field.
3. Click on the  button.

To edit Department List

1. To create a new department in the Department List, go to *Panel Setup*, *Company Profile* and *Department List*. The screen as shown below will appear.

 [Company Profile](#)

Department #	Description
1	R&D
2	Accounts Department
3	Production
4	Projects
5	Sales & Marketing
6	Administration
7	Human Resource
8	Engineering
9	Undefined Department 9
10	Undefined Department 10
11	Undefined Department 11
12	Undefined Department 12
13	Undefined Department 13
14	Undefined Department 14
15	Undefined Department 15
16	Undefined Department 16
17	Undefined Department 17
18	Undefined Department 18
19	Undefined Department 19
20	Undefined Department 20

2. Click on any unused link to create a new department. In this example, we select link #9. A screen as shown below will appear.

Department Configuration

Department #: **9**

Description:

3. Enter the name of the department to be created in the space provided beside *Description*. A combination of a total length of 30 alphabets, numbers or symbols found from the keyboard, such as () - _ [] can be entered. In this example, we enter Service Department for the Description.

Department Configuration

Department #: **9**

Description:

4. Click on the  button, after which the Description of the department will be seen in the Department drop-down list on the page *Card Assignment*, *Card Details*, as shown below.

Card Details	
Card Number:	135
Facility code:	1
Card Format:	Standard 26 bit Format
User Name:	HL
Department:	
User Field 1:	
User Field 2:	
Access Group A:	
Access Group B:	

- R&D
- Accounts Department
- Production
- Projects
- Sales & Marketing
- Administration
- Human Resource
- Engineering
- Service Department**
- Undefined Department 10

Email/SMS Configuration

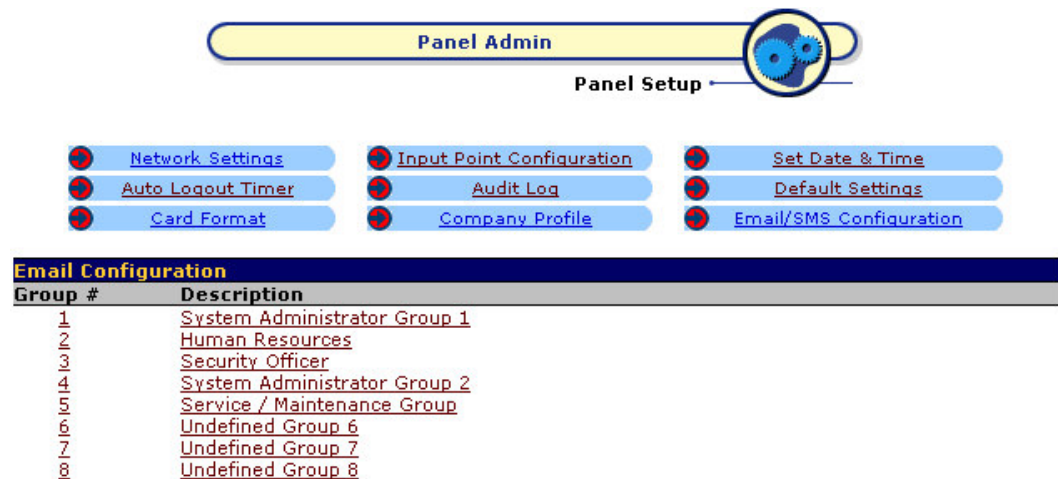
This function allows user to configure the Access Easy Controller to send out messages or Lateness Report using Simple Mail Transfer Protocol (SMTP) to email addresses. A total of eight groups and eight messages field are available for configuration. Each group has two “**Send To**” and two “**Carbon Copy (Cc)**” email addresses.

In order for the feature to work, user has to configure the various items, **Devices**, **Cardholders**, and **Events** in an AND operation. To exclude/disable an item(s) from the operation, the option **Selected Only** or **Omit Only** should be used with nothing selected. While for the Lateness Report, the feature is disable if no selection is made on any of the day of week (DOW).

A sample configuration for Lateness Report is presented at the end of the section.

To activate the Email Configuration

1. From the *Panel Setup* screen, click on the *Email/SMS Configuration* link.



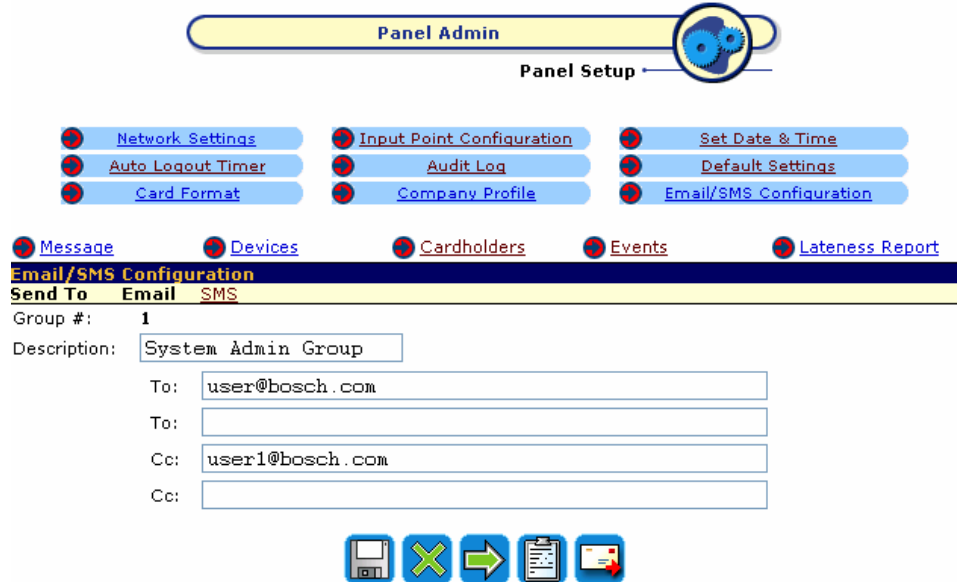
2. Click on any of the Group and you will be shown the Send To page.

Send To

This web page allows user to configure the email addresses of the recipients. Up to two **To** and two **Cc** email addresses per group are available. The Access Easy Controller will ignore any configurations made for the group if there is no email address in any of the **To** fields even though there is email address in the **Cc** field. Each **To** and **Cc** should only contains one email address, entering more than one email address separating by a coma (,) or semi-coma (;) will be taken as a single email address, hence, not able to send out the mail to the recipients.

To edit the Email Configuration (Send To)

1. Click on the *Group's* numbering or the *Description* text to proceed.



Panel Admin

Panel Setup

Network Settings Input Point Configuration Set Date & Time
 Auto Logout Timer Audit Log Default Settings
 Card Format Company Profile Email/SMS Configuration

Message Devices Cardholders Events Lateness Report

Email/SMS Configuration

Send To Email SMS

Group #: 1

Description: System Admin Group

To: user@bosch.com

To:

Cc: user1@bosch.com

Cc:

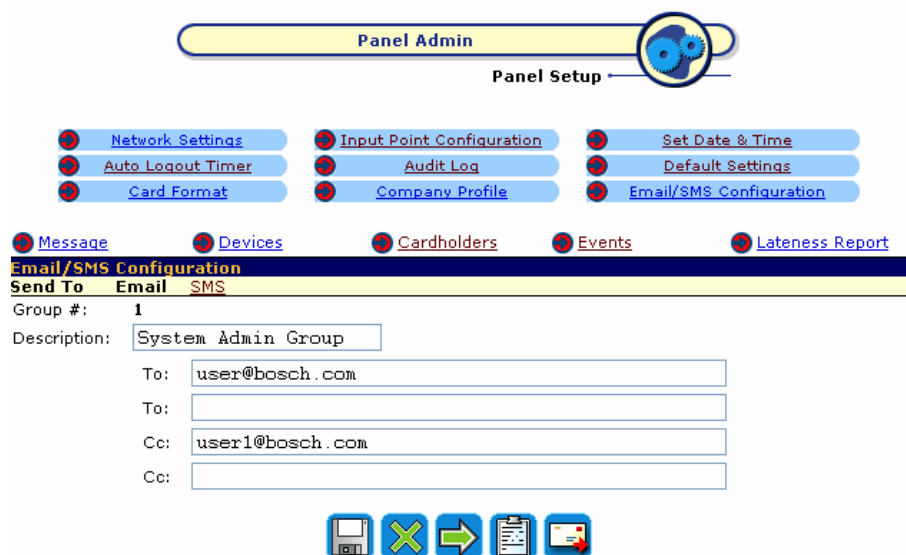
Save Cancel Apply Print Mail

2. Highlight the default text and enter a Description.
3. Enter the email address in the appropriate field.

4. Click on the  button.

To test the Email sent verification

1. Click on the  button.



Panel Admin

Panel Setup

Network Settings Input Point Configuration Set Date & Time
 Auto Logout Timer Audit Log Default Settings
 Card Format Company Profile Email/SMS Configuration

Message Devices Cardholders Events Lateness Report

Email/SMS Configuration

Send To Email SMS

Group #: 1

Description: System Admin Group

To: user@bosch.com

To:

Cc: user1@bosch.com

Cc:

Save Cancel Apply Print Mail

2. A successful test message will be shown

Test email sent successfully



3. If you are unable to sent out the email, please check your Email Server Settings again.

Message field

The **Message** field makes up the 'body text' while the **Event** is to appear in the 'subject' field of the dispatched email.

To edit the Message field

1. Click on the *Message's* numbering or the *Description* text to proceed.

The screenshot shows the 'Panel Admin' interface. The 'Panel Setup' section is active, displaying various configuration options like Network Settings, Input Point Configuration, Set Date & Time, Auto Logout Timer, Audit Log, Default Settings, Card Format, Company Profile, and Email/SMS Configuration. The 'Email/SMS Configuration' section is expanded, showing the 'Message' field. The 'Message #' is set to 1, and the 'Description' is 'Undefined Message 1'. Below the description is a large text area for editing the message body. At the bottom are three buttons: a floppy disk icon (Save), a green X icon (Cancel), and a clipboard icon (Return).

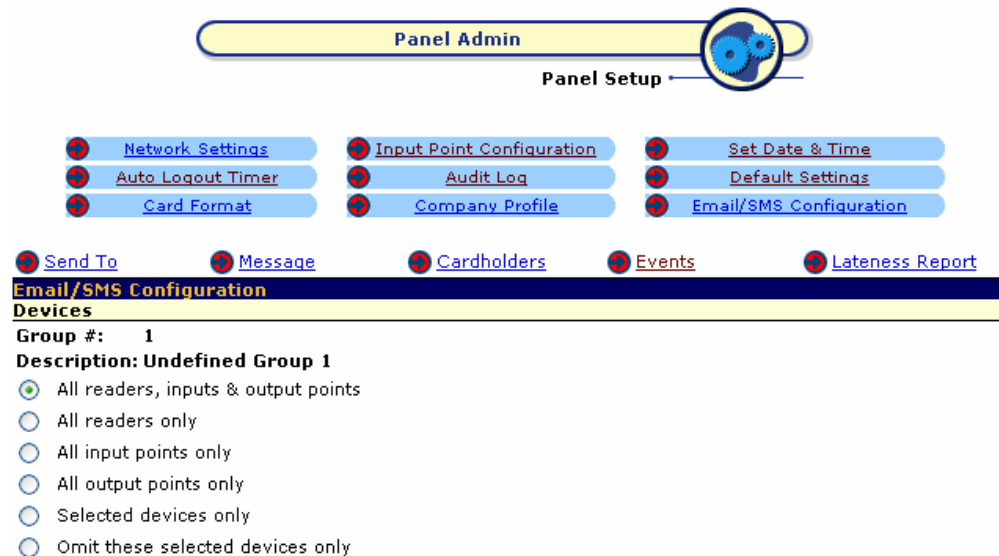
2. Highlight the default text and enter a Description.
3. Enter the new message limiting to 127 characters including punctuation.
4. Click on the  button.
5. Click on the  button to return.

Devices

This web page allows user to configure the first (**Devices**) of the three items for the AND operation.

To edit the Email Configuration (Devices)

- Click on the *Device* link or the  button in the **Sent To** web page.



Panel Admin

Panel Setup

Network Settings Input Point Configuration Set Date & Time

Auto Logout Timer Audit Log Default Settings

Card Format Company Profile Email/SMS Configuration

Send To Message Cardholders Events Lateness Report

Email/SMS Configuration

Devices

Group #: 1

Description: Undefined Group 1

☒ All readers, inputs & output points

☐ All readers only

☐ All input points only

☐ All output points only

☐ Selected devices only

☐ Omit these selected devices only

- Select the desired radio button and click on the  button. If selection is made on either **Selected Devices Only** or **Omit these Selected Devices Only**, a window and a pull-down list appears as shown in the following diagram.



☒ Selected Devices Only

☐ Omit these Selected Devices Only

List of Selected Devices

Server Room Entrance

Select a Device:

Main Entrance

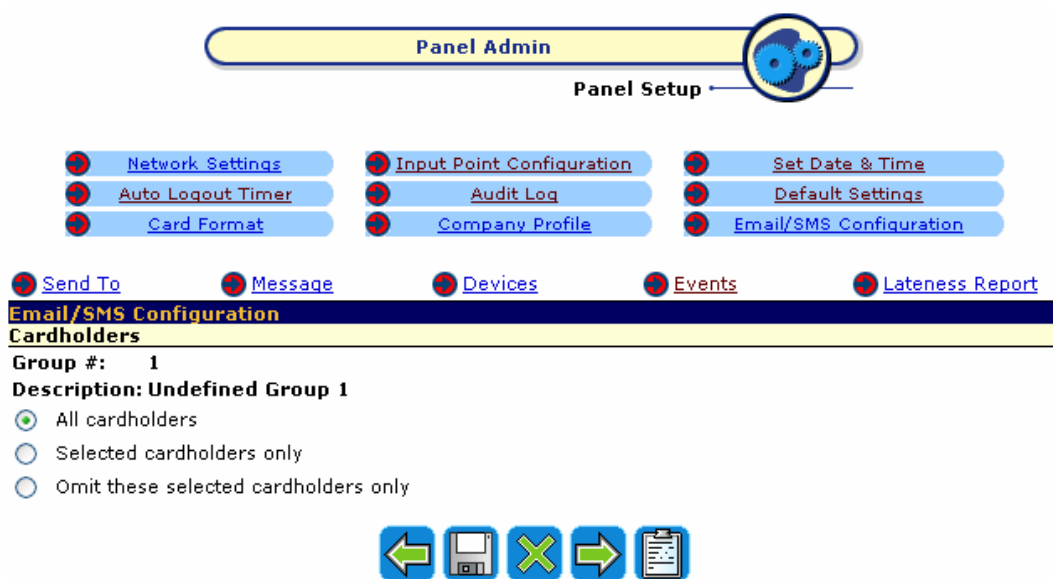
- Select a device from the pull-down list and click on the  button. The selected device appears in the **List of Selected Devices** window. Repeat step 3 if you have other Devices to put on the list.
- To delete selected device(s), click on the device name in the window followed by the  button. Repeat step 4 if necessary.
- When you finish with your selection, click on the  button.

Cardholders

This web page allows user to configure the second (**Cardholders**) of the three items for the AND operation.

To edit the Email Configuration (Cardholders)

1. Click on the *Cardholders* link or the  button in the **Devices** web page.



2. Select the desired radio button and click on the  button. If selection is made on either **Selected Cardholders Only** or **Omit these Selected Cardholders Only**, a window and the Search field appear as shown below. You have the option to search by **Name** or **Card Number** or **User Field** by selecting from the Option drop down box.



The function of **Select By Card #** and **Select By Name** is similar to the **Search By Card #** and **Search By Name** function respectively. Please refer to the explanation in the section on *Card Assignment, The Search Function* for detail.

3. Select the Cardholder and click on the  button. The selected cardholder appears in the **List of Selected Cardholders** window. Repeat step 3 if you have other cardholders to put on the list (see NOTE below).

NOTE: The **List of Selected Cardholders** window has a limit of up to 80 entries.

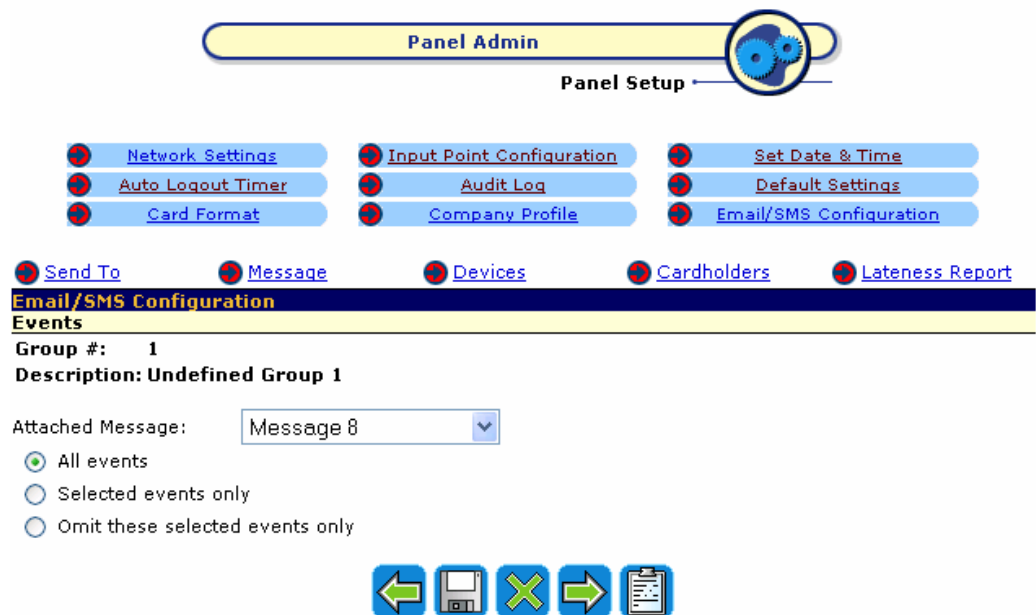
- To delete selected Cardholder(s), click on the Cardholder's name in the window followed by the  button. Repeat step 4 if necessary.
- When you finish with your selection, click on the  button.

Events

This web page allows user to configure the last (**Events**) of the three items for the AND operation.

To edit the Email Configuration (Events)

- Click on the *Events* link or the  button in the **Cardholders** web page.



The screenshot shows the 'Panel Admin' web interface. At the top, there is a 'Panel Setup' section with a gear icon. Below this, there are several links: 'Network Settings', 'Auto Logout Timer', 'Card Format', 'Input Point Configuration', 'Audit Log', 'Company Profile', 'Set Date & Time', 'Default Settings', and 'Email/SMS Configuration'. The 'Email/SMS Configuration' link is highlighted. Below the links, there is a section for 'Email/SMS Configuration' with a sub-section for 'Events'. The 'Events' section shows 'Group #: 1' and 'Description: Undefined Group 1'. There is a dropdown menu for 'Attached Message' with 'Message 8' selected. Below this, there are three radio buttons: 'All events' (selected), 'Selected events only', and 'Omit these selected events only'. At the bottom of the 'Events' section, there are five icons: a green arrow, a floppy disk, a red X, a green arrow, and a clipboard.

- Select the pre-defined **Message** from the list.
- Select the desired radio button and click on the  button. If selection is made on either **Selected Events Only** or **Omit these Selected Events Only**, a window and a pull-down list appear as shown below.



The screenshot shows a window titled 'List of Selected Events:'. It contains a text box with the text 'Access Denied - Passback'. Below the text box, there is a label 'Select an Event:' followed by a dropdown menu with 'Panel Tamper' selected.

4. Select the desired Event and click on the  button.
The selected Event appears in the **List of Selected Events** window. Repeat step 4 if you have other Events to put on the list.
5. To delete selected Event(s), click on the Event in the window followed by the  button. Repeat step 5 if necessary.
6. When you finish your selection, click on the  button.

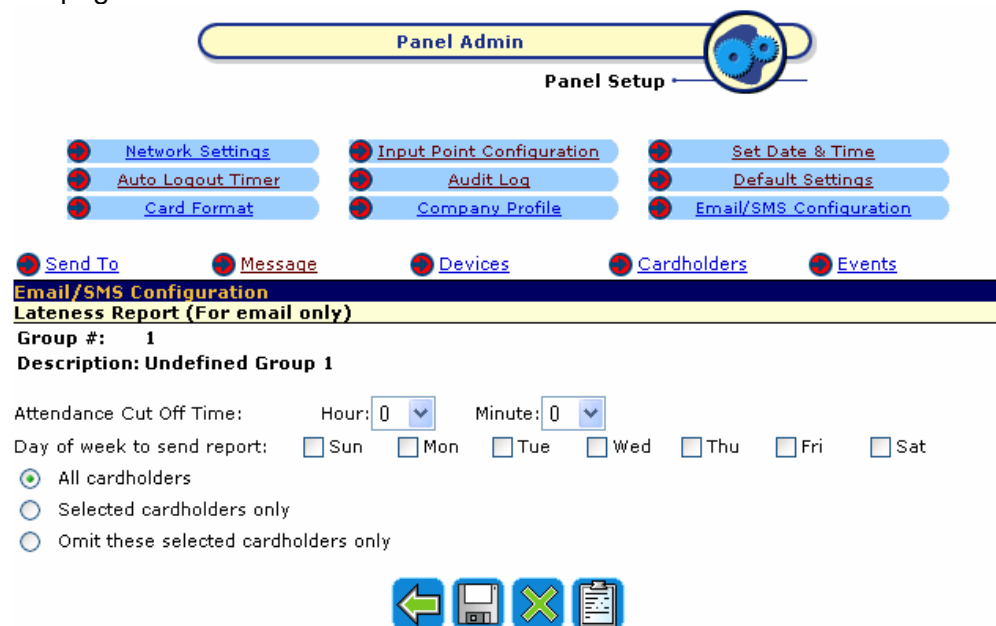
Lateness Report

This web page allows user to configure the Lateness Report.

The Lateness Report is used for keeping track of employee presence at the work place. It will consider an employee to be present for work once a transaction, bearing the employee's card number, is transacted. Card number(s) not transacted after the Attendance Cut off Time is regarded as late for work.

To edit the Email Configuration (Lateness Report)

1. Click on the *Lateness Report* link or the  button in the **Events** web page.



The screenshot shows the 'Panel Admin' web interface. At the top, there is a navigation bar with 'Panel Admin' and 'Panel Setup' (highlighted with a gear icon). Below this is a grid of configuration links: Network Settings, Auto Logout Timer, Card Format, Input Point Configuration, Audit Log, Company Profile, Set Date & Time, Default Settings, and Email/SMS Configuration. The 'Email/SMS Configuration' link is selected, leading to a page titled 'Email/SMS Configuration' and 'Lateness Report (For email only)'. The page shows 'Group #: 1' and 'Description: Undefined Group 1'. It includes fields for 'Attendance Cut Off Time' with 'Hour' and 'Minute' dropdowns, and a 'Day of week to send report' section with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. Below these are three radio button options: 'All cardholders' (selected), 'Selected cardholders only', and 'Omit these selected cardholders only'. At the bottom of the form are four icons: a left arrow, a save icon, a delete icon, and a refresh icon.

2. Select the **Attendance Cut off Time** Hour and Minutes from the list.
The *Attendance Cut off Time* defines the time on which the Controller checks through the current date's transactions for the presence of Card

numbers and making comparison with respect to the Card database and the Selected/Omission list.

3. Select the appropriate **Day of the week to send report** check boxes. The *Day of the week to send report* defines the day on which the Controller will keep track of the cut off time and to send out the report to the respectively email addresses.

4. Select the desired radio button and click on the  button. If selection is made on either **Selected Cardholders Only** or **Omit these Selected Cardholders Only**, a window and the **Search** field appear as shown below. You have the option to search by **Name** or **Card Number** or **User Field** by selecting from the Option drop down box.

List of Selected Cardholders:

Search :

Option:

John d'Baptist (1)

Name ▼



The function of **Selection By Card #** and **Selection By Name** is similar to the **Search By Card #** and **Search By Name** function respectively. Please refer to the explanation in the section on *Card Assignment, The Search Function* for detail.

5. Select the Cardholder and click on the  button. The selected cardholder appears in the **List of Selected Cardholders** window. Repeat step 5 if you have other cardholders to put on the list.

NOTE: The **List of Selected Cardholders** window has a limit of up to 80 entries.

6. To delete selected Cardholder, click on the Cardholder's name in the window followed by the  button. Repeat step 6 if necessary.

7. When you finish your selection click on the  button.

Sample Email Configuration for Lateness Report

This section provides you with sample configuration for Lateness Report. The sample will instruct you on what to select for the four selection criteria (Devices, Cardholders, Events, and Lateness Report) in order to send out the email successfully. Please refer to the Appendix “*Email Configuration Table*” for more detailed configuration based on other Events.

For Lateness Report to be sent out, the items, Devices, Cardholders, and Events have to be disabled. That is, the **Selected** or **Omit** option is chosen but no specific parameter is selected. The following screen-capture shows the selection criteria for Devices, Cardholders, Events and Lateness Report respectively.

Email Configuration

Devices

Group #: 2

Description: Human Resources

☐ All Readers, Inputs & Output Points
☐ All Readers Only
☐ All Input Points Only
☐ All Output Points Only
☒ Selected Devices Only
☐ Omit these Selected Devices Only

List of Selected Device: 

Select a Device: 

Select either one.

Nothing to appear inside window.

Email Configuration

Cardholders

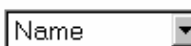
Group #: 1

Description: SalesTeam Group 1

☐ All cardholders
☒ Selected cardholders only
☐ Omit these selected cardholders only

List of Selected Cardholders: 

Search : 

Option: 

Select either one.

Nothing to appear inside window.

Email Configuration**Events****Group #:** 2**Description:** Human Resources

Attached Message:

HR AEC Alarm !!

Don't care for
Lateness Report.☐ All Events☒ Selected Events Only

Select either one.

☐ Omit these Selected Events OnlyNothing to appear
inside window.

List of Selected Events:

Select an Event:

Panel Tamper

Email Configuration**Lateness Report****Group #:** 1**Description:** SalesTeam Group 1

Attendance Cut Off Time:

Hour: 8

Minute: 30

Day of week to send report:

☐ Sun☒ Mon☒ Tue☒ Wed☒ Thu☒ Fri☒ Sat☐ All cardholders☒ Selected cardholders only☐ Omit these selected cardholders only

List of Selected Cardholders:

John d'Baptist (1)
John (4)

Search :

Option:

Name

With such configuration, the Controller will keep track of the cut-off time from Monday through Saturday (at 0830hrs) and will send out the Lateness Report to the recipient(s) slightly after 0830hrs.

The screen-capture below illustrates what the email recipient(s) is expected to receive.

- The following Cardholders are late.

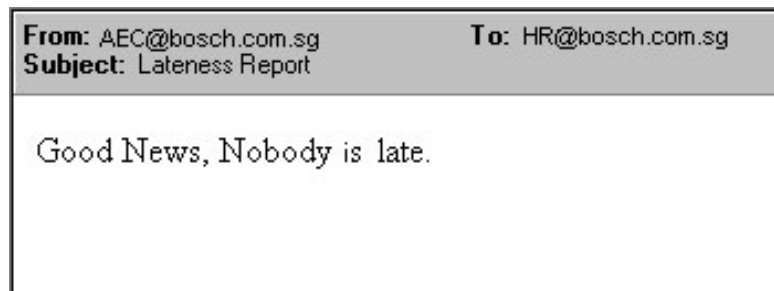
From: AEC@bosch.com.sg
Subject: Lateness Report

To: HR@bosch.com.sg

The following Cardholders are late :

0001. Lilian Koh PT	(90) - Acct
0002. Soh Swee Lee	(91) - Acct
0003. Sharon Tan YY	(92) - Prod
0004. Bill Lee TH	(101) - Engg

- All Employees are punctual.

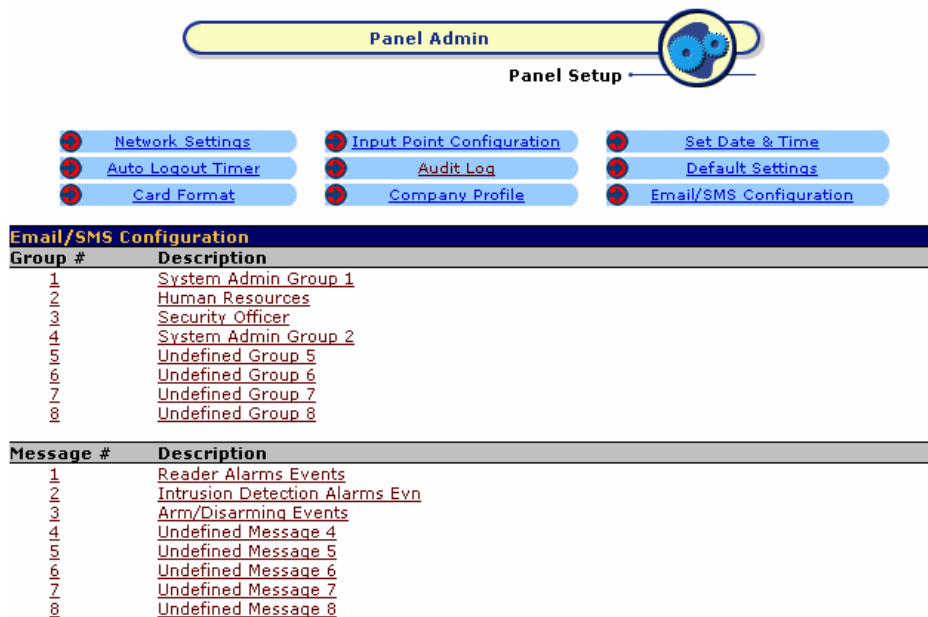


SMS Configuration

SMS function is implemented to allow user to configure the Access Easy Controller to send out Short Message Service (SMS). A total of eight groups and eight messages field are available for configuration. Each group has up to 4 mobile phone numbers for SMS messaging.

To activate the SMS Configuration

1. From the *Panel Setup* screen, click on the *Email/SMS Configuration* link.



2. Click on any of the Group and you will be shown the Send To page.
3. Next click on the SMS link as shown in the following diagram to configure the mobile phone numbers of the recipients.



Click here to configure the mobile phone numbers

Send To

This web page allows user to configure the mobile phone number of the recipients. Up to four numbers can be configured per group.

To edit the SMS Configuration (Send To)

1. Click on the *Group's* numbering or the *Description* text to proceed.

The screenshot shows the 'Panel Admin' interface. At the top, there's a 'Panel Setup' menu with a gear icon. Below it, there are several configuration options: Network Settings, Auto Logout Timer, Card Format, Input Point Configuration, Audit Log, Company Profile, Set Date & Time, Default Settings, and Email/SMS Configuration. The 'Email/SMS Configuration' option is selected. Below this, there are tabs for 'Message', 'Devices', 'Cardholders', 'Events', and 'Lateness Report'. The 'Send To' tab is active, showing the configuration for 'Group #: 1' with the description 'System Admin Group 1'. There are four input fields for 'Mobile Device 1' through 'Mobile Device 4'. The first two fields contain the numbers '92847267' and '94758264' respectively. At the bottom, there are five icons: a floppy disk (save), a red X (cancel), a green arrow (next), a document (help), and a mail icon (send).

2. Highlight the default text and enter a Description.
3. Enter the mobile phone numbers in the appropriate field. Each of the Mobile Device field could only contain one mobile phone number.

4. Click on the  button.

Message field

The **Message** field makes up the 'body text' while the **Event** is appended to the front of the Message. The configuration steps are the same as those for the Email setup. Please refer to the previous section "To edit Message Field".

Devices

This web page allows user to configure the first (**Devices**) of the three items for the AND operation. This configuration will determine what are the devices that will be monitored for Events (that will be configured in the next section) will trigger a SMS message to the recipients.

The steps to configure the Devices are the same as those for the Email Device setup. Please refer to the previous section "To edit the Email Configuration (Devices)".

Cardholders

This web page allows user to configure the second (**Cardholders**) of the three items for the AND operation. If some of the Events are caused by a Cardholder, such as Access Grant, Time Clock IN, etc. this setting here will filter out those Cardholders that are not in this list.

The steps to configure the Cardholders are the same as those for the Email Cardholders setup. Please refer to the previous section "To edit the Email Configuration (Cardholders)".

Events

This web page allows user to configure the last (**Events**) of the three items for the AND operation. This configuration will determine what are the kinds of Events that will be monitored.

The steps to configure the Events are the same as those for the Email Events setup. Please refer to the previous section "To edit the Email Configuration (Events)".

CHAPTER 14

Input Setup

The Access Easy Controller has 32 user programmable Input Points that will be used for Alarm Monitoring purposes. The address for these Input Points ranges from 33 to 64 and is available on the I/O Card. Each card provides up to eight Input Points.

These Input Points can be assigned into a Group (called an Alarm Zone) or as an Individual. Both types provides the same function, the only difference is the way each is being arm/disarm. Access Easy Controller allows user to configure up to four Alarm Zones.

An Alarm Zone (see NOTE 2 below) can be armed/disarmed by the following methods: -

- manually by user via a dedicated Arm/Disarm Reader, or
- manually by user via the web page (Input Control), or
- system control based on Schedule Intervals.

An Individual Input Point can be armed / disarmed only by **Schedule** intervals.

All Input Points, Group or Individual, can be configured to trigger 1 to 4 Output Points (of the I/O Card) for the purpose of status indication. The Outputs are labelled as: -

Alarm Status	- Turns "ON" during an Alarm condition.
Arm/Disarm Status	- Turns "ON" when it is Armed .
Ready Status	- Turns "ON" when the Input Point is not in the normal condition. It is said to be Not Ready for Arming.
Bypass Status	- Turns "ON" when the Input Point is Bypassed .

Any alarm detected by any of the Input Points would also trigger the *Common Alarm Output* relay, at address 8, and is only restored when all the Input Points is restored back to *Normal* state.

NOTE 1: The Input Control web page will only display the status of the Alarm Zones, status of Individual Input Points will not be displayed. Please refer to the Chapter on Input Control for detail.

NOTE 2: All Input Points configured to an Alarm Zone follows the First Input Point's setting for Arm Delay, Alarm Delay, and Schedule of that Zone.

Before we start, here is a brief description of how the Access Easy Controller interprets the Schedule Intervals for Input Points arming and disarming statuses

For example,

If the setting for Schedule #2 is: -

Interval 1 **Start** 0830hrs **End** 1730hrs

Interval 2, 3, and 4 has no setting.

When the Schedule #2 is tied to Input Point #1, the point will arm and disarm accordingly.



Take note that the Input Point is disarmed at exactly 0830hrs but re-armed at 1731hrs a minute delay as compared to the Schedule #2 setting. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

NOTE: Before you configure any Input Point(s), please ensure that the Alarm Monitoring Device with the EOL resistor is in place with the necessary logic inversion on the Input Point Configuration web page.

To activate the Input Setup

The *Input Setup* can be activated only from the menu item page.

1. From any menu item page, click on Input Setup link.

Panel Admin

Input Point Setup

Input #: 1

Description: Input Point 1

Arm Delay: 0 seconds (0 - 255)

Alarm Delay: 0 seconds (0 - 255)

Input Arm/Disarm Control		Output Link	
NotAssigned	Zone	Alarm Status	Undefined Output Point 1
Undefined	Arm/Disarm	Toggle	NotAssigned
	Toggle	Arm/Disarm Status	NotAssigned
	Ready Status	Bypass Status	NotAssigned

Icons: Save, Cancel, Print

2. Highlight the default text in the *Description* field and enter the new *Description*.
3. Highlight the default entry for *Arm Delay* and enter the new Arm Delay (this field is a hyperlink to the first Input Point if this is the second or subsequent Input Point of an Alarm Zone). If you want immediate arming/disarming, leave it as 0. Value from 1 to 255 will cause a delay before the Alarm Zone is armed, during this delay any triggering of the Input Points will not be consider as an Alarm.
4. Highlight the default entry for *Alarm Delay* and enter the new Alarm Delay (this field is a hyperlink to the first Input Point if this is the second or subsequent Input Point of an Alarm Zone). If you want the Alarm to be activated immediately when the Input Point is triggered during Arm condition, leave it as 0. Value from 1 to 255 will cause a delay before Alarm activation, during this delay period, if the Input Point restored to normal or user Disarm the Alarm Zone, no alarm will be activated. Alarm activation will cause the Output Relay configured in the *Alarm Status* and the CAO to turn on.

NOTE: The *Alarm* status Output Relay assigned here are the same one that is listed at the **Output Setup**. By setting the *Duration* to a value other than 0 at the **Output Setup**, will cause the *Alarm* status Output Relay to turn on for the configured duration only. Leaving it as 0 will cause the Output Relay to remains on till the Alarm Zone is disarmed or the Input Point has restored to normal condition. Please refer to the Chapter on **Output Setup** for more details.

If the Toggle checkbox for Alarm Status is selected, output point assigned to the Alarm Status will be turned on at the instant an alarm is triggered at the input point and will remain on even after the alarm is restored, until the user manually disarms the input point at the Input Control settings or turns the output off at the output control settings.

5. Select the Alarm Zone to which this Input Point is to group with, from the list. If you do not wish to assign it to Alarm Zone, just select *Not Assigned*, however, it must at least be assign to an Arm/Disarm input control for this configuration to function.

NOTE: Please refer to the Chapter on **Advance I/O Setup** for more details on setting up the various Arm/Disarm input control.

6. Select the desired Arm/Disarm input control from the list. If you do not wish to assign it to a Arm/Disarm input control, just select *undefined*, however, it must at least be assign to an **Alarm Zone** for this configuration to function. (This field is disabled if this is the second or subsequent Input Point of an Alarm Zone).
7. Select the appropriate Output Point, for the various Status Outputs, from the list. By default, these Outputs are *Not Assigned*.

NOTE: The Output Points listed/assigned here are the same one that is listed at the **Output Setup**. By setting the *Duration* to a value other than 0 at the **Output Setup**, will cause the Status Output Relays to turn on for the configured duration. Leaving it as 0 will cause the Output Relays to remain on till the Status has changed. Please refer to the Chapter on **Output Setup** for more details.



8. Click on the  button (see NOTE 1, 2, and 3).



NOTE 1: Activating the  button will cause all active (Armed) Input Points within the Alarm Zone to be set to default, i.e. Disarmed.



NOTE 2: Activating the  button outside the pre-defined Schedule intervals will cause the Input Point to be Armed.

NOTE 3: When an Alarm Zone is also armed/disarmed by Schedule, the condition similar to NOTE 2 has the priority over NOTE 1.



Proceed to configure other Input Points by clicking on the  button to return to main page.

Alarm Zone Description

The *Alarm Zone Description* allows the user to change the description for each Alarm Zone to the description he prefers so that he may better visualize the location of the alarm zone.

From the first web page of the *Input Setup*, click on the  [Alarm Zone Description](#) link. A screen as shown below appears.



Panel Admin

Input Point Setup

Alarm Zone Description	
Alarm Zone 1:	Alarm Zone 1
Alarm Zone 2:	Alarm Zone 2
Alarm Zone 3:	Alarm Zone 3
Alarm Zone 4:	Alarm Zone 4



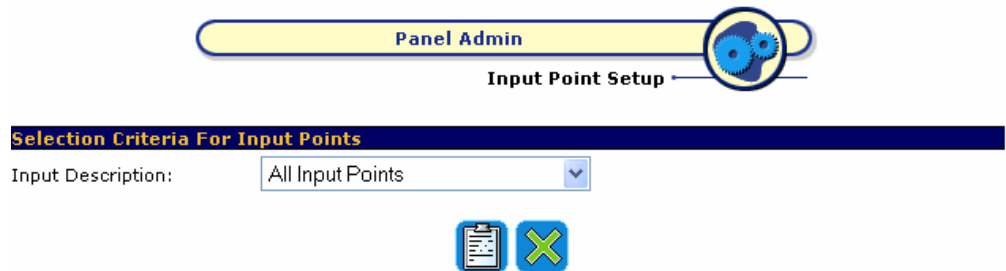


1. To change the *Alarm Zone Description* for each Alarm Zone, delete the default description from each *Alarm Zone* and enter the new description accordingly.

To generate a Print Preview of the Input Point

Once you have completed configuring the Input Points, a hardcopy can be printed out.

1. From the first web page of the Input Setup, click on the  [Input Point Report](#) link. A screen as shown below appears.



2. Select the desired Input Point from the *Input Description* list. If all Input Points are required, select *All Input Points*.
3. Click on the  button for a print preview of the report. The following screen-capture shows a sample of the report.

[Return To Input Point Setup](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Input Point Report

Tuesday, 15 Sept 2005 15:15:15

Input # : 1
Description : Motion Detector 1
Arm Delay : 3 seconds
Alarm Delay : 3 seconds
Zone : Alarm Zone 1

Input Arm/Disarm Control

Arm/ Disarm : Criteria 1 (Toggle)

Output Link

Alarm Status : Motion Detector 1 (Simulator)
Arm/ Disarm Status : Not Assigned
Ready Status : Not Assigned
Bypass Status : Not Assigned

If you wish to print out a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Input Setup web page, click on the [Return To Input Point Setup](#) link.
5. To generate a preview of other input points, click on the [Return To Selection Criteria](#) link.

This Page Intentionally Left Blank

CHAPTER 15

Output Setup

The Access Easy Controller has 32 user programmable Output Points that will be used for Utility Triggering purposes. The address for these Input Points ranges from 33 to 64 and is available on the I/O Card. Each card provide up to 8 Output Points

The Output Points are triggered manually by user via the web page, or based on Schedule Intervals, or be triggered by an Input Point as a Status indicator, please refer to section on Input Setup for detail.

The status of all the Output Points is displayed in the Output Control web page except those points that are triggered by Input Points. Please refer to the Chapter on Output Control for detail.

Before we start, here is a brief description of how the Access Easy Controller interprets the Schedule Intervals for Output Points triggering status

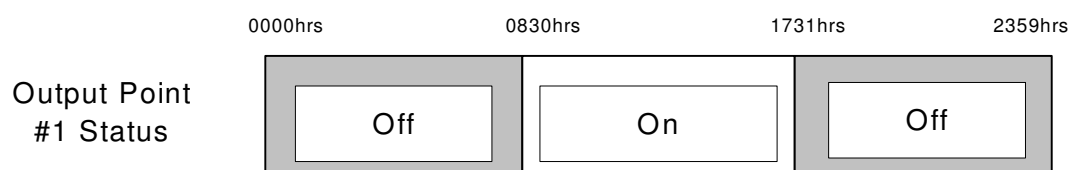
For example,

If the setting for Schedule #2 is: -

Interval 1 **Start** 0830hrs **End** 1730hrs

Interval 2, 3, and 4 has no setting.

When the Schedule #2 is tied to Output Point #1, the point will turn on and off accordingly.



Take note that the Output Point switches On at exactly 0830hrs but switches Off at 1731hrs a minute delay as compared to the Schedule #2 setting. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

To activate the Output Setup

The *Output Setup* can be activated only from the menu item page.

1. From any menu item page, click on Output Setup link.

Output #: 1

Description: Undefined Output Point 1

Duration: 0 seconds

Output Scheduling		
No Schedule	On/Off	☐ Disable transaction at Activity





2. Highlight the default text in the *Description* field and enter the new *Description*.
3. Highlight the default entry for Duration and enter the new Duration (see NOTE below).

NOTE: This setting for the *Duration* field is applicable for Manual Output Control (refer to the Chapter on Output Control). User can *force* the Output Point(s) to toggle its current state for the duration specified here. User could also assign the Output Point as a Status Output for the Input Point, however, if the *Duration* field has a value other than 0, the Output Point will not remain on when the respective status is activated, instead, it will turn on only for the duration as specified here.

If Duration Field is Always On, output point will be turned on infinitely when triggered until the user turns it off manually at the Output Control settings. E.g. If Output Point 1 is assigned to Door Forced Alarm Output of Reader 1, when door at Reader 1 is forced open, Output Point 1 will be turned on, and will remain on even after the door is closed, until the user turns it off manually at the output control settings.

4. Select the appropriate Schedule from the list. By default, an unused Output Point is tied to *No Schedule* i.e. the Output will not be triggered.



5. Click on the button.



NOTE: Activating the button within the pre-defined Schedule intervals will cause the Output Relay to turn On.



6. Click on the button to return to main page.

Disable Activity From Output Point

This will allow the user to disable any of the 32 output points activity to be logged, especially when they are activated by other type of function or elevator operation which do not require logging. This means that the activity transactions associated with the Output Point will not be logged at the *View Activity* page.

1. To use this feature, go to *Output Setup*, select an Output Point that you do not want its activity transactions to be logged. A screen as shown below will appear.

Output #: 1
Description: Motion Detector 1 (Simulator)
Duration: 0 seconds (0 - 255)

Output Scheduling		
No Schedule	On/Off	☒ Disable transaction at Activity

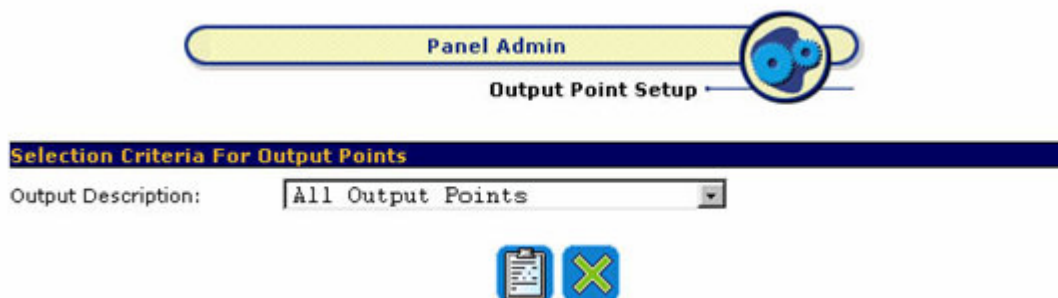
2. Check the *Disable Transaction at Activity* box.

3. Click on the  button. In the example above, the activity transactions associated with Output # 1, Motion Detector 1 (Simulator) will not be logged and cannot be viewed at the *View Activity* page.

To Generate a Print Preview of the Output Point

Once you have completed configuring the Output Points, a hardcopy can be printed out.

1. From the first web page of the Output Setup, click on the  [Output Point Report](#) link. A screen as shown below appears.



2. Select the desired Output Point from the *Output Description* list. If all Output Points are required, select *All Output Points*.
3. Click on the  button for a print preview of the report. The following screen-capture shows an example of the report.

[Return To Output Point Setup](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Output Point Report

Tuesday, 15 Sept 2005 15:15:15

Output # : 1

Description : Motion Detector 1 (Simulator)

Duration : 0 seconds

Output Scheduling

On/Off : No Schedule

Disable transaction at Activity : No

4. To return to the Output Setup web page, click on the [Return To Output Point Setup](#) link.
5. To generate a preview of other output points, click on the [Return To Selection Criteria](#) link.

CHAPTER 16

Card Readers

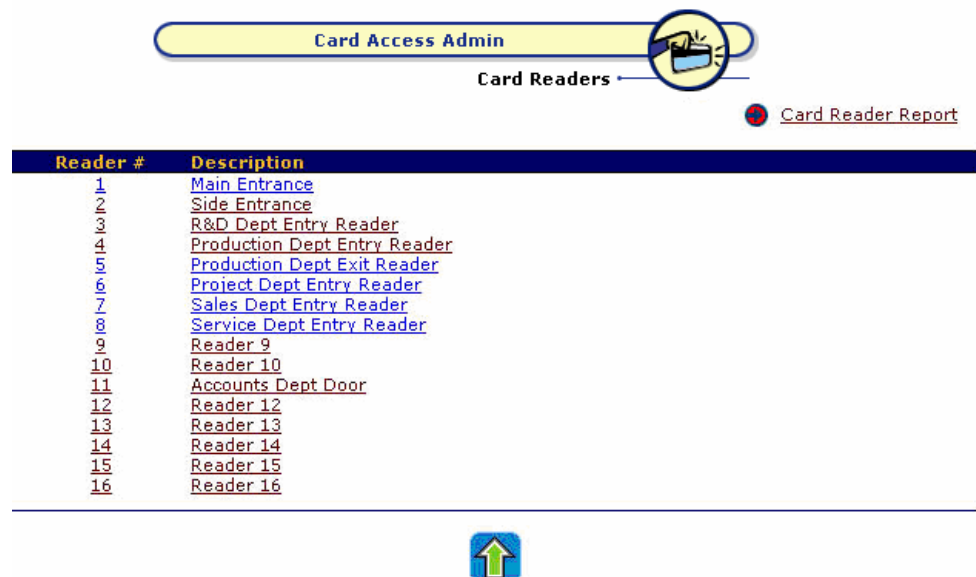
Access Easy Controller software is designed to integrate with its hardware to provide a total solution as an integrated Access Control System.

Before the System is fully functional, we have to set up the hardware-related parameters. In this chapter, you will learn about the setting up of the most essential parameters of the Access Easy Controller system, namely the Card Reader parameters, comprising of the following sections: -
Card Readers parameters are the most essential parameters, comprising of:-

- Reader Function
- Reader Options
- I/O Settings
- PIN Code Settings
- Anti-Passback (APB) Settings
- Dual Card Configuration

All Access easy controller Card Readers can be configured to work either as an Entry Reader, an Exit Reader, an Entry and Arm/Disarm Reader or an Elevator Reader.

To Setup the Card Readers, select the target Access easy controller and click on the *Card Readers* hyperlink. The following screen will appear.



Reader #	Description
1	Main Entrance
2	Side Entrance
3	R&D Dept Entry Reader
4	Production Dept Entry Reader
5	Production Dept Exit Reader
6	Project Dept Entry Reader
7	Sales Dept Entry Reader
8	Service Dept Entry Reader
9	Reader 9
10	Reader 10
11	Accounts Dept Door
12	Reader 12
13	Reader 13
14	Reader 14
15	Reader 15
16	Reader 16

1. Click on the *Reader #* or the *Description* text to proceed. A screen as shown below appears.

Card Access Admin

Card Readers

Reader #: 1

Description: Main Entrance

Reader Options I/O Settings PIN Code Settings Anti-Passback (APB) Settings Dual Card Configuration

Reader Function

☒ Entry Reader

☐ Exit Reader works with [dropdown]

☐ Entry and Arm/ Disarm Reader for [dropdown]

☐ Elevator Reader

[Card Reader Icon] [X] [Arrow] [Clipboard]

2. Delete the default text and enter the new *Description* for the Reader.
3. Click on the  button.

Reader Function

Card Access Admin

Card Readers

Reader #: 1

Description: Main Entrance

Reader Options I/O Settings PIN Code Settings Anti-Passback (APB) Settings Dual Card Configuration

Reader Function

☒ Entry Reader

☐ Exit Reader works with [dropdown]

☐ Entry and Arm/ Disarm Reader for [dropdown]

☐ Elevator Reader

[Card Reader Icon] [X] [Arrow] [Clipboard]

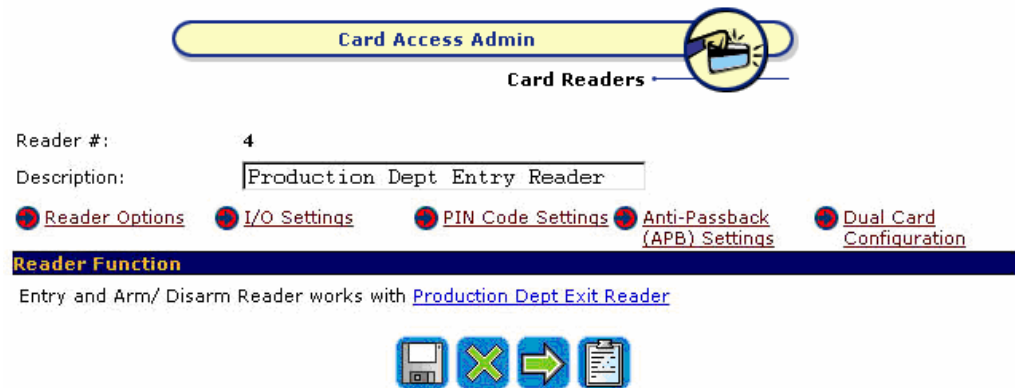
This section allows user to define the use of the Reader, either an Entry Reader, an Exit Reader, an Entry and Arm/Disarm Reader or an Elevator Reader. By default, all 16 Readers are set as Entry Reader.

A screen of the *Reader Function* page is shown above.

Entry Reader

This is the default setting. All 16 readers are configured as Entry Reader allowing Door Access.

If an Entry Reader is defined to work with an Exit Reader, the Reader Function for the Entry Reader will change to reflect the status. A sample is shown in the screenshot below. The Exit Reader's description becomes a hyperlink. User can click on it to re-configure the Exit Reader.



Exit Reader

When this mode is selected, this Reader will operate as an Exit Reader. User has to define the Entry Reader that this Exit Reader has to work with.

This Exit Reader will follow the operational behaviour of the Entry Reader such as Door Open Timer and Door Strike Timer. If the Entry Reader for this Exit Reader is also a Arm/Disarm Reader, user can also arm/disarm the same Alarm Zone at the Exit Reader as it now has the operational behaviour of the Entry Reader.

NOTE Once a Reader is configured as an Exit Reader, the Reader will only be accessible to Reader Functions. The rest of the configuration, such as Reader Options, I/O Settings, PIN Code Settings, Anti-Passback (APB) Settings and Dual Card Configuration will not be available until it is changed to an Entry Reader, or an Entry and Arm/Disarm Reader.

Entry and Arm/Disarm Reader

When this mode is selected, this Reader will have all the functions of an Entry Reader and it can be used for Arming and Disarming a specific Alarm Zone. The Alarm Zone is to be selected from the drop-down box beside it.

To arm an Alarm Zone using the same access Reader, card holder with the Arm/Disarm control just has to press the <0> key on the Keypad before presenting his card.

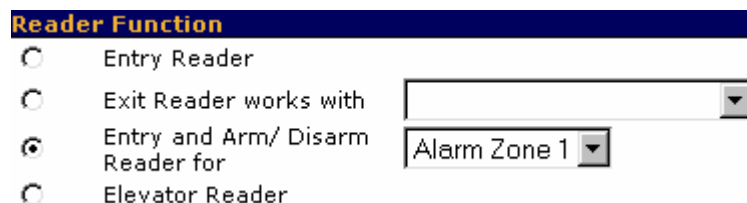
During an Arm state, all valid access card will be disabled. Only a Arm/Disarm card (Card must be checked at *Card holder is able to Arm/Disarm* under *Card Assignment*.) can disarm the Alarm Zone and enable the door back to normal card access operation.

During Arm state, if the door is unlocked by Schedule or manually from Door control page, the alarm zone will be disarmed first before door is unlocked.

If the Reader is **ONLY** used for Arm/Disarm purpose, user just has to assign the cardholder with Arm/Disarm function without given access right to the Reader. This will allow the cardholder to arm the Alarm Zone without pressing the <0> key.

To switch the Reader back to normal access card Reader, press <0> on the Keypad after finishing the Arm/Disarm operation.

To go to this page, select *Card Readers, Reader Function*.



Reader Function

☐ Entry Reader

☐ Exit Reader works with

☒ Entry and Arm/ Disarm Reader for

☐ Elevator Reader

NOTE In order for the Reader to work properly, additional wiring is required. Please consult your System Installer for advice.

Elevator Reader

Similar concept of door access right assignment in door Readers is also implemented in the *Elevator Reader* floor assignment. However, there are a number of differences between an Elevator Reader and an Entry Reader (or an Entry and Arm/Disarm Reader). The differences are listed below:-

- No Anti-Passback Setting
- Floor Output Settings instead of Door Output Settings and Door Input Settings
- Output Link can control only Invalid Card Output

Each item is explained in detail below.

No Anti-Passback (APB) Setting

Elevator Readers do not have the function *Anti-Passback (APB) Settings*. This is because it would be complicated to register a zone for the user after he has entered the elevator and flashed his card to the Elevator Reader, since the elevator has exit to more than one floor (You can consider the Elevator has more than one exit).

Floor Output Settings instead of Door Output Settings and Door Input Settings

The settings of an *Elevator Reader* is also different from that of an *Entry Reader* (or an Entry and Arm/Disarm Reader). Elevator Reader only has *Floor Output Settings* whereas an Entry Reader (or an Entry and Arm/Disarm Reader) has *Door Output Settings* and *Door Input Settings*. This can be seen in the screen below.

To go to this page, select *Card Readers*, select a Reader as an Elevator Reader and click on the Save button, and select *I/O Settings*.

This feature allows user to set any of the 32 programmable Output Point to the selected Floor.

1. To configure the *Selecting Floor Relay Output*, select a Floor from the *Floor List*.
2. Select an Output Point from the *Output List*.

3. Click on the  button to add the selected Output Point to the selected Floor. The selected items would appear on the *Floor Relay* list box, as shown below. **Each Floor and Output Point can only be selected once.**

4. To delete any selected items from the *Floor Relay* list box, highlight

the item and click on the  button.

5. To configure the *Floor Relay Enable Timer*, delete the default timing in seconds and enter a new timing for it. The default timing is 5 seconds.

In the above screen, Button 1 is already assigned to Floor 1 as seen in the *Floor Relay* list box and the *Floor Relay Enable Timer* is set to 5 seconds. Let us assume that by pressing Button 1, the elevator will take the passenger to Floor 1. When the passenger presents his card to the Elevator Reader, he must press Button 1 within 5 seconds so that the elevator will take him to Floor 1. If he presses Button 1 more than 5 seconds later after he presents his card to the Elevator Reader, Button 1 will be de-activated and the passenger will have to present his card to the reader again.

Output Link can control only Invalid Card Output

For an Elevator Reader, the *Output Link* is used to control *Invalid Card Output* only. This can be seen in the screen below.



In the above screen, Elevator Alarm Output is assigned to *Invalid Card Output*. This means that when an invalid card is presented to the

Reader Options

The screenshot shows the 'Card Access Admin' software interface. At the top, there is a yellow header bar with 'Card Access Admin' and a 'Card Readers' button with a card icon. Below the header, the 'Reader #' is set to '1' and the 'Description' is 'Main Entrance'. There are five tabs: 'Reader Function' (selected), 'I/O Settings', 'PIN Code Settings', 'Anti-Passback (APB) Settings', and 'Dual Card Configuration'. The 'Reader Options' section is highlighted in blue. It contains the following options:

- ☐ Turn off the reader
- ☐ Enable Keypad Only Operation
- ☒ On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)
- Keypad Timeout (0-255): seconds
- ☐ Enable reader lockout

The 'Scheduling Options' section is also highlighted in blue. It contains the following options:

- ☐ Unlock door
- ☒ Schedules will not be used to unlock this door
- ☐ Schedules will be used to unlock this door
- ☐ Schedules and holidays will be used to unlock this door
- Schedule:
- ☐ Only after a valid access condition

At the bottom of the form, there are five icons: a green left arrow, a floppy disk, a green X, a green right arrow, and a document with a pencil.

This section allows user to configure parameters in relation to the Reader. User can de-activate the Reader to prevent access by anyone, or allow access by entering the Card Number manually, and/or access in accordance to Holiday Schedules.

A screen of the *Reader Options* page is shown above.

Turn off the reader

Once a Reader is turned off, it will not read any card. The door will be locked and all access will be denied. For Arm/Disarm Reader, turning off the reader prevents arming and disarming through the Reader.

Enable Keypad Only Operation

When this mode is selected, the user need not present his/her card to gain access or Arm/Disarm the Alarm Zone (see NOTE 1). Instead, the cardholder only has to key in his/her card number, (see NOTE 2) followed by its PIN code (Only if PIN function is required).

NOTE 1 Cardholder can still present his/her card to gain access or Arm/Disarm. If PIN code is required, user has to present card followed by PIN code.

NOTE 2 User has to activate the  key first before entering the card number.

On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)

This mode works in conjunction with the *Card Assignment*, *Cardholder must abide by holiday schedules*. If both are checked and the current date is a holiday, the controller will apply the 4 sets of Schedule intervals setting in the Regular or Special Holiday, depending on which Holiday Type the current date setting is on, for processing (for each cardholder).

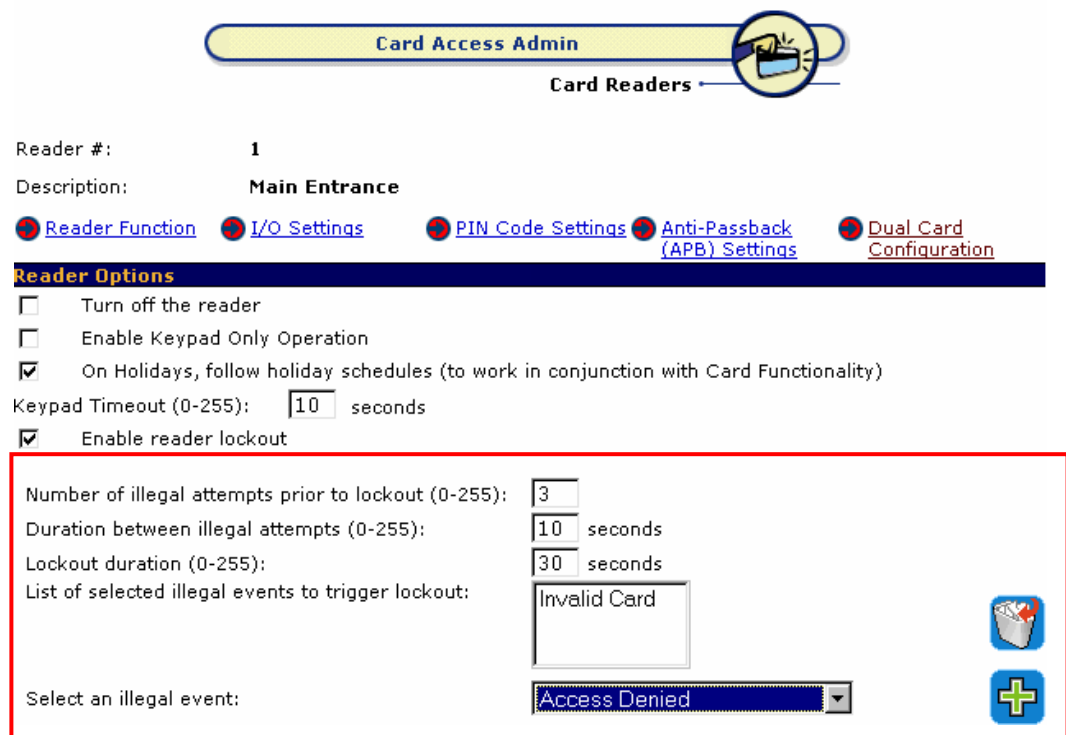
Keypad Timeout

Keypad Timeout relates to the interval where the Controller expects key entry via the reader's keypad from the user. If the user does not press any key within this duration or when the user forgets to quit from a specific operation, the Controller will return to the normal mode to wait for card presentation or user action during a PIN change or Manual Card Number Entry operation. To edit the **Keypad Timeout**, delete the default number and enter the new timeout value. It should range from 0 – 255. The factory default is 10 seconds.

Enable Reader Lockout

When this mode is selected, there is a restriction on the number of times a user with invalid access can present his card at the Reader.

1. Check on the *Enable Reader Lockout* and click on the  button. A screen as shown below appears.



Card Access Admin

Card Readers

Reader #: 1

Description: Main Entrance

[Reader Function](#)
[I/O Settings](#)
[PIN Code Settings](#)
[Anti-Passback \(APB\) Settings](#)
[Dual Card Configuration](#)

Reader Options

☐ Turn off the reader
☐ Enable Keypad Only Operation
☒ On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)

Keypad Timeout (0-255): 10 seconds

☒ Enable reader lockout

Number of illegal attempts prior to lockout (0-255): 3

Duration between illegal attempts (0-255): 10 seconds

Lockout duration (0-255): 30 seconds

List of selected illegal events to trigger lockout:

Invalid Card

Select an illegal event: Access Denied




2. Choose the events that you would like to lock the users out by selecting from *Select an illegal event* and click on the  button.

3. The illegal events will appear on the *List of selected illegal events to trigger lockout*.
4. To remove the illegal event from the *List of selected illegal events to trigger lockout*, highlight the event and click on the  button.
5. Enter the *Number of illegal attempts prior to lockout*. The default is set to 3.
6. Enter the *Duration between illegal attempts*. It ranges from 0 to 255 seconds.
7. Enter the *Lockout duration*. It ranges from 0 to 255 seconds.

In the above example, the user will be lockout after the **3rd** attempt when he uses an **Invalid Card** to access the Reader 3 times within 10 seconds. He would not be able to access the Reader for **30 seconds**, meaning the Reader will lock him out for 30 seconds. However, if he only attempted 2 times with an invalid card, the Reader will reset the illegal attempt counter 10 seconds after the very first time the user uses an invalid card to access the Reader.

NOTE: Once a reader is lockout, it will not be accessible by any cardholder. Only after the lockout duration can the reader be used again.

Scheduling Options

The Access easy controller can be programmed to activate or de-activate the reader based on pre-programmed Schedules. This is particularly useful if the reader is used for controlling door access and the door is required to be unlocked during certain period of the day, but to be locked back at different time period for the same day.

The above scenario is a typical operation of a Main Entrance Door of a building. During the time when staff normally come to work, you might want to unlock the door throughout the office working hours and automatically lock back after work.

A screen of the *Scheduling Options* page is shown in the section *Reader Options*.

Unlock door (For Entry Reader, Entry and Arm/Disarm Reader)

When this mode is selected, the door that is controlled by the particular reader is permanently unlocked. There is free access to everyone. This function is applicable to Entry Reader, and Entry and Arm/Disarm Reader  Unlock door. For Elevator Reader, this function is replaced by a similar function *Disable Elevator Reader*, in the below section.

Disable Elevator Reader (For Elevator Reader Only)

When this mode is selected, the elevator that is controlled by the particular reader is permanently unlocked. There is free access to everyone. This function is applicable to Elevator Reader only  Disable Elevator Reader. For Entry Reader, and Entry and Arm/Disarm Reader, it is replaced by a similar function *Unlock door*, in the above section.

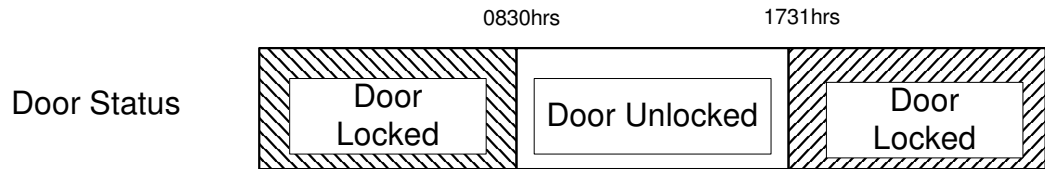
Schedules will not be used to unlock this door

When this mode is selected, the reader access mode will be activated. Gaining access will require the user to present his / her card and PIN code (if PIN code is required).

Schedules will be used to unlock this door

When this mode is selected, the Reader access mode will function based on the Schedule intervals setting. To set the scheduling options, refer to the section on *To set the Scheduling Options* below.

For example: - The Start and End time for **Interval 1** of Schedule settings is set to **0830hrs** and **1730hrs** respectively. In this period, the door will be unlocked between 0830 to 1731 hrs. The drawing below provides a pictorial representation of the function.



Notice that the Door is locked only at 1731hrs instead of 1730hrs. The reason is that Access easy controller takes 17:30:59hrs as a valid End time for 1730hrs.

Schedules and Holidays will be used to unlock this door

When this mode is selected, during a Holiday, the Cardholder will be allowed to access this Reader during the specific period as defined in Schedule intervals setting for holiday. To set the scheduling options, refer to the section on *To set the Scheduling Options* below.

To set the Scheduling Options(For Schedules will be used to unlock this door and Schedules and Holidays will be used to unlock this door)

1. To assign the *Scheduling Options*, click on the desired radio button. To de-select that point, click on other radio buttons. By default, it is set at *Schedules will not be used to unlock this door*.
2. If the selection is made on either ***Schedules will be used to unlock this door*** or ***Schedules and Holidays will be used to unlock this door***, please proceed to step 3 to select the Schedule.
3. Select the desired Schedule from the *Schedule* list box.
4. When *Schedules will be used to unlock this door* or *Schedules and Holidays will be used to unlock this door* is selected, the door will unlock on time even if nobody is in the premises. However, with the *Only after a valid access condition* checked, the system will only unlock the door after a valid access card is presented during the schedule time period.

Example

The screenshot shows the 'Scheduling Options' window with the following settings:

- Scheduling Options:**
 - ☐ Unlock door
 - ☐ Schedules will not be used to unlock this door
 - ☐ Schedules will be used to unlock this door
 - ☒ Schedules and holidays will be used to unlock this door
- Schedule:** Normal Schedule (selected in the dropdown menu)
- ☒ Only after a valid access condition

In the screen above, the mode *Schedules and Holidays will be used to unlock this door* is selected, and the selected *Schedule* is Normal Schedule. In addition, the checkbox *Only after a valid access condition* is checked.

The screen below shows the schedule for 'Normal Schedule', which has been selected.

Schedule #: 4
 Schedule Description: Normal Schedule

		Interval 1		Interval 2		Interval 3		Interval 4	
		Start	End	Start	End	Start	End	Start	End
Sunday		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Monday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Tuesday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Wednesday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Thursday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Friday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Saturday		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Regular Hol		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Special Hol		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--

According to the schedule in 'Normal Schedule' above, when the mode *Schedules and Holidays will be used to unlock this door* is selected, the door will unlock every Monday to Friday from 0830hrs to 1730hrs and every Saturday, Sunday, Regular Holiday and Special Holiday from 0830hrs to 1300hrs. However, with *Only after a valid access condition* is checked, the door will only unlock after a valid access card is presented to the Reader during the schedule time period. For example, on a Monday, the first person to present his card to the Reader arrives at 0845hrs. Therefore, the door will only unlock from 0845hrs to 1730hrs on that particular Monday, instead of from 0830hrs to 1730hrs.

Door Output Settings (For Entry Reader, Entry and Arm/Disarm Reader)

[Reader Function](#)
[Reader Options](#)
[PIN Code Settings](#)
[Anti-Passback \(APB\) Settings](#)
[Dual Card Configuration](#)

Door Output Settings

Door Open Timer (0-255): seconds
 Door Strike Timer (0-255): seconds

Door Strike: Source Address

Door Input Settings

Request-to-Exit Device: Source Address
 Door Contact: Source Address

☒ Schedules and holidays will be used to shunt door contact

Door Force Open Alarm delay duration (0-255): seconds
 Pre-alarm Warning before door held open alarm (0-60): seconds

Output Link

Door Forced Alarm Output:
 Door Held Alarm Output:
 Invalid Card Output:

This parameter allows user to set the timer duration that is related to the door.

A screen of the *Door Output Settings* page is shown above.

Door Open Timer

This setting defines how long the door can be held open, after an access/exit is granted, before the Controller registers it as **Door Held Open** transaction. If the reader has a built-in buzzer, it will generate a beeping alert signal and will stop once the door is closed back. It can range from 0 to 255 seconds. The factory default is 60 seconds.

Door Strike Timer

This setting defines the duration to de-energise the Door Strike when the Momentarily Unlock command is sent via the Door Control web page or when an access/exit is granted.

When access is granted to a Cardholder, sufficient time must be given for the person to open the door before the Controller locks it back again. It can range from 0 to 255 seconds. The factory default is 5 seconds.

Note: When the Door Strike Timer is set to 0, and a valid card is presented at the Reader, the door becomes unlocked (View Activity shows Door Unlocked) until the same card or another valid card is presented at the Reader, only then the Reader will go back to locked mode (View Activity shows Door Locked). Presenting an invalid card will not change the status. View Activity will only show Invalid Card.

Door Strike

For the Output device, such as Door Strike, though it is pre-defined, user can still change the default address to other available addresses within the same CRC Card, should the original output relay is defective.

To allocate an Output Address for *Door Strike*, select *Output* for *Source*, else select *None*. After allocating *Output* to *Source*, select an *Address* for it. The default Address is 1. The *Address* can be chosen from a selectable range.

Output

It defines the physical output on the CRC Card. The output channels are applicable for *Door Strike*, *Door Forced Alarm Output*, *Door Held Alarm Output* and *Invalid Card Output*. Output channel assignment for devices connected in relation to the Reader is selectable within the spare Output channels of the card. User can disable the Output channel by selecting *None*.

None

This setting will disable the Output channel.

An additional feature is the enabling schedules and holidays to be used for shunt door contact.

If a schedule is selected, during the time interval, the door contact will be ignored. This is the same as setting the door contact to "None".

If the door contact is ignored, there will not be any alarms like "Door Held Open" or "Door Forced Open" on that particular reader

NOTE	Address for <i>Door Strike</i> is selectable only to within the Card's spare Output channels. <i>Door Forced Alarm Output</i> , <i>Door Held Alarm Output</i> and <i>Invalid Card Output</i> is selectable only within the user programmable 32 outputs.
-------------	--

Door Input Settings (For Entry Reader, Entry and Arm/Disarm Reader)

A screen of the *Door Input Settings* page is shown in the section *Door Output Settings*.

The Access easy controller has the capability to support a maximum of 16 wiegand card readers, 64 input (I) monitoring points, and 64 relay output (O) points.

Of the 64 I/Os, only 32 Inputs and Outputs are user programmable, the other 32 I/Os are assigned to the Readers.

The addresses for Input devices (Request-to-Exit device and Door Contact) connected in relation to the Reader, are pre-defined and cannot be changed. The following is the list of hardware to configure: -

- Request-to-Exit Device,
- Door Contact,
- Door Forced Open Alarm delay duration,
- Pre-alarm Warning before door held open alarm.

Request-to-Exit Device

To allocate an Input Address for Request-to-Exit Device, select Input, else select *None*. The Address for Request-to-Exit Device is fixed and cannot be changed.

Door Contact

To allocate an Input Address for Door Contact, select *Input* for *Source*, else select *None*. The Address for Door Contact is fixed and cannot be changed.

Input

It defines the physical input on the CRC Card. The input channels are applicable to *Request-to-Exit device* and *Door Contact*. Input channel assignment for devices connected in relation to Reader is fixed and cannot be changed. However, user can disable the Input channel by selecting *None*.

None

This setting will disable the Input channel.

If the door contact is ignored, there will not be any alarms like "Door Held Open" or "Door Forced Open" on that particular reader.

Door Forced Open Alarm delay duration

This feature is available for Entry Reader, and Entry and Arm/Disarm Reader only. To go to this page, select *Card Readers, I/O Settings*.

This is to facilitate some special exit requirement. User may just want to open the door to exit without pushing any exit button. This is also to prevent Door Forced Open false alarm due to poor mechanical problem.

Enter the timing in seconds at the *Door Forced Open Alarm delay duration* if desired. The timing can range from 0 to 255 seconds.

Door Input Settings		
	Source	Address
Request-to-Exit Device:	Input	1
Door Contact:	Input	2
☐ Schedules and holidays will be used to shunt door contact		No Schedule
Door Force Open Alarm delay duration (0-255):		2 seconds
Pre-alarm Warning before door held open alarm (0-8):		0 seconds

Schedules and holidays will be used to shunt door contact

An additional feature is the enabling schedules and holidays to be used for shunt door contact.

If a schedule is selected, during the time interval, the door contact will be ignored. This is the same as setting the door contact to "None".

If the door contact is ignored, there will not be any alarms like "Door Held Open" or "Door Forced Open" on that particular reader.

Pre-alarm Warning before door held open alarm

This feature is available for Entry Reader, and Entry and Arm/Disarm Reader only. To go to this page, select *Card Readers, I/O Settings*.

With the pre-alarm function, a user would be reminded with a slow beeping that the door he has just gained access is still open. An example is he can set *Pre-alarm Warning before door held open alarm* to 5 seconds so that he will be alerted to close the door on time before the Door Held Open Alarm. The timing can range from 0 to 60 seconds.

Door Input Settings		
	Source	Address
Request-to-Exit Device:	Input	1
Door Contact:	Input	2
☐ Schedules and holidays will be used to shunt door contact		No Schedule
Door Force Open Alarm delay duration (0-255):		2 seconds
Pre-alarm Warning before door held open alarm (0-8):		0 seconds

NOTE Address for *Request-to-Exit Device* and *Door Contact* is fixed and cannot be changed. If the Input channel is disabled, the address will not be shown.

Floor Output Settings (For Elevator Reader Only)

Reader #: 9

Description: Elevator Reader

[Reader Function](#) [Reader Options](#) [PIN Code Settings](#) [Dual Card Configuration](#)

Floor Output Settings

Floor Relay Enable Timer (0-255): 5 seconds

Floor Relay:  

Floor List Output List

Selecting Floor Relay Output: Floor 1 Motion Detector 1 (Simulator) 

Output Link

Invalid Card Output: Not Assigned

This section allows user to set any of the 32 programmable Output Point to the selected Floor.

A screen of the *Floor Output Settings* page is shown above.

1. To configure the *Selecting Floor Relay Output*, select a Floor from the *Floor List*.
2. Select an Output Point from the *Output List*.

3. Click on the  button to add the selected Output Point to the selected Floor. The selected items would appear on the *Floor Relay* list box, as shown below. **Each Floor and Output Point can only be selected once.**

Floor Relay:

Floor 1: Motion Detector 1 (Simulator)

4. To delete any selected items from the Floor Relay list box, highlight the item and click on the  button.
5. To configure the *Floor Relay Enable Timer*, delete the default timing in seconds and enter a new timing for it. The default timing is 5 seconds.

Output Link

A screen of the *Output Link* page is shown in the section *Door Output Settings* for Entry Reader, and Entry and Arm/Disarm Reader. These output links allow the user to configure individual outputs to trigger when a Door Forced Open, Door Held Open or Invalid Card alarm occurs at the Reader.

A screen of the *Output Link* page is shown in the section *Floor Output Settings* for Elevator Reader.

In an Entry Reader, and Entry and Arm/Disarm Reader, it allows user to set any of the 32 programmable Output Point to *Door Forced Alarm Output*, *Door Held Alarm Output* and *Invalid Card Output*. By default, all the 3 are set to *Not Assigned*.

Output Link	
Door Forced Alarm Output:	Not Assigned
Door Held Alarm Output:	Not Assigned
Invalid Card Output:	Not Assigned

However, in an Elevator Reader, this section only allows user to set any of the 32 programmable Output Point to *Invalid Card Output*. By default, it is set to *Not Assigned*.

Output Link	
Invalid Card Output:	Not Assigned

PIN Code Settings

Card Access Admin

Card Readers

Reader #: 1

Description: Main Entrance

[Reader Function](#)
[Reader Options](#)
[I/O Settings](#)
[Anti-Passback \(APB\) Settings](#)
[Dual Card Configuration](#)

PIN Code Settings

☒ PIN code not required
☐ PIN code required at all times
☐ PIN code required, except during schedule intervals
☐ PIN code required, except during regular schedule intervals and holiday schedule intervals
 Schedule: No Schedule
☐ PIN code only operation using Reader's PIN code
 Reader's PIN code (1-7 digits): *****

This section allows user to set the parameter on when the Personal Identification Number (PIN) is to be used.

A screen of the *PIN Code Settings* page is shown above.

PIN code not required

When this mode is selected, users accessing this Reader do not have to key in the PIN code.

PIN code required at all times

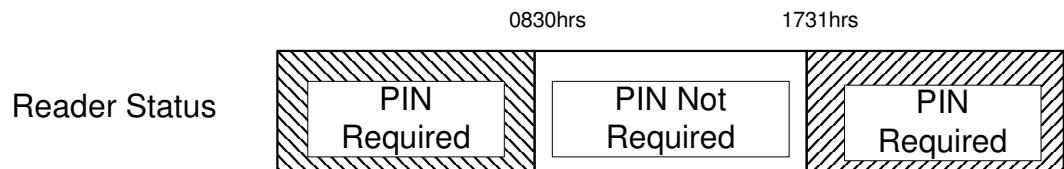
When this mode is selected, users are required to key in the PIN code.

NOTE In order for the feature to work, the Cardholder's *Card + PIN is required on keypad readers* mode must be activated, and the PIN must be set at the card in Card Assignment page. For the setting of the PIN, please refer to *Chapter Card Assignment, Card Functionality, Card + PIN is required on Keypad readers*.

PIN code required, except during schedule intervals

When this mode is selected, users are not required to key in his/her PIN code during specific periods defined in the Schedule settings.

As an example, the Start and End time for **Interval 1** of the Schedule is set to **0830hrs** and **1730hrs** respectively. The Reader status will be set accordingly. The following drawing provides a pictorial representation of the function.



Notice that PIN is required at 1731hrs instead of 1730hrs. The reason is that Access easy controller takes 17:30:59hrs as a valid End time for 1730hrs.

This mode is not affected by Holiday setting, i.e. during holiday, it will still use the Day of Week schedule.

NOTE 1 To use this feature as intended, the cardholder should be given access rights to the reader(s).

NOTE 2 In order for the feature to work, the cardholder's *Card + PIN is required on keypad readers* mode must be activated.

PIN code required, except during regular schedule intervals and holiday schedule intervals

When this mode is selected, the operation is the same as the previous mode, except that during holiday the Holiday schedule is used instead of the normal Day of Week schedule.

PIN code only operation using Reader's PIN code

When this mode is selected, all cardholders will use a pre-defined Reader's PIN code (default code 1234000) to gain access to the controlled area or to arm/disarm the Alarm Zone. No card is required.

The Reader's PIN code is defined in the *Reader's PIN code (1-7 digits)* edit field.

To set the Schedule

1. If selection is made on **PIN code required, except during schedule intervals** or **PIN code required, except during regular schedule intervals and holiday schedule intervals**, the *Schedule* field must be set.
2. To edit the Schedule, select the appropriate schedule from the *Schedule* list box.

To set the Reader's PIN Code

1. If the selection is made on *PIN code only operation using Reader's PIN code*, the *Reader's PIN code (1-7 digits)* field must be entered.
2. To edit the *Reader's PIN code*, delete the default PIN and enter the new *Reader's PIN code*, limited to 7 digits. See NOTE 1 And 2.

NOTE 1 User can enter from 1 to 7 digits for the *Reader's PIN code* (default code 1234000).

NOTE 2 For security reason, every character entered for the PIN code is represented by an asterisk (*). For *Macintosh* user, it is represented by a dot () instead.

Anti-Passback (APB) Settings

Card Access Admin

Card Readers

Reader #: 1

Description: Main Entrance

[Reader Function](#)
[Reader Options](#)
[I/O Settings](#)
[PIN Code Settings](#)
[Dual Card Configuration](#)

Anti-Passback (APB) Settings

☒ APB deactivated
☐ Activate Time Based APB
 Timer setting for Time Based APB: 0 minutes
☐ Activate Soft APB (violations will be logged, but access/exit granted)
 Entry Zone: Undefined Exit Zone: Undefined
☐ Activate Full APB (violations will be denied access)
 Entry Zone: Undefined Exit Zone: Undefined

A screen of the *Anti-Passback (APB) Settings* page is shown above.

Anti-Passback (APB) function prevents a cardholder from passing his/her card to another person to gain access to the door after he has accessed through it. It is normally implemented in sensitive area having high security.

Three types of APB modes are available; namely: - Time Based APB, Soft APB, and Full APB. Each mode provides different level of security and is explained in detail in the following sections.

APB deactivated

By default, it is set to *APB deactivated*. This means that there is no APB setting for the Readers on this Access easy controller.

Activate Time Based APB

Time Based APB relates to *Entry Reader* only, implying that the Controller will not accept the same card until the Timer setting for Time Based APB has elapsed.

To select this mode, select *Activate Time Based APB*.

When this mode is selected, the *Timer setting for Timed Based APB* must be set. Choose the timing from the list box, in minutes, from a range of 0 minutes to 60 minutes.

Activate Soft APB

Soft APB mode operation requires a cardholder to present his/her card at the *Entry Reader* and *Exit Reader* at all times. However, if he/she follow another person in or out the controlled area, the transaction “Exit Granted, Soft APB” or “Access Granted, Soft APB” will be shown on his/her next exit or entry respectively.

The administrator needs to *Reset APB* in order to clear the above transaction. Refer to the Chapter on Reset APB for detail.

To select this mode, select *Activate Soft APB*. The *Entry Zone* and *Exit Zone* must be selected for this mode to work properly.

Activate Full APB

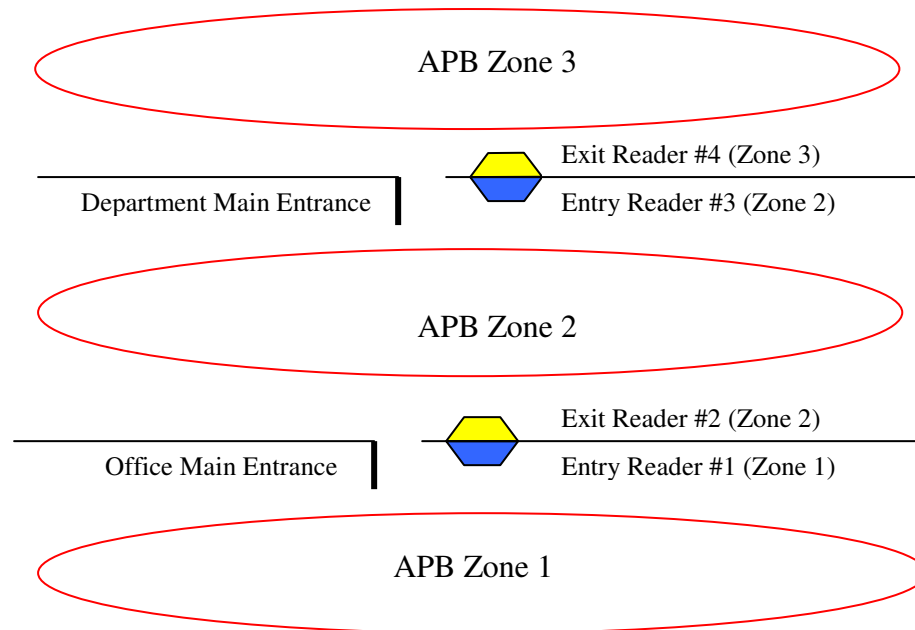
When this mode is selected, user must first enter using the *Entry Reader* in order to exit from the corresponding *Exit Reader*. If cardholder violates this, access will be denied. The administrator needs to *Reset APB* before the cardholder can have access again. Refer to the Chapter on Reset APB for detail.

To select this mode, select *Activate Full APB*. The *Entry Zone* and *Exit Zone* must be selected for this mode to work properly.

The main difference between the Soft and Full APB is that, for Soft APB, the user is allowed to exit the controlled area via the Exit Reader even if he/she entered the controlled area previously by following another person. Full APB does not allow that.

Understanding the APB Zone

APB Zone is applicable to Soft APB and the Full APB mode. Access easy controller is able to support up to 254 *Soft APB Entry Zones*, 254 *Soft APB Exit Zone*, 254 *Full APB Entry Zone* and 254 *Full APB Exit Zone*.



Any Reader assigned to operate Soft APB mode or Full APB mode will be given an *Entry Zone* and *Exit Zone*. When a cardholder presents card at Entry Reader #1, the system will verify whether he has been registered in Zone 1. If he has been registered in Zone 1, access is granted to him. When he opens the door to gain access such that the door contact sensing is opened, he is registered to be in Zone 2. However, if he is verified to be in other zones instead of Zone 1, access will be denied to him.

NOTE In the case that he is verified to be in Zone 1 and is granted access but he did not open the door to gain access, he will not be registered in Zone 2. He will only be registered in Zone 2 when he is granted access and opens the door to gain access.

Using this verification method, no card can bypass any zone to gain access to any other zone. In addition, zone will only be registered into the card if the user has opened the door physically (based on door contact sensing).

For the above example, assume that the mode *Activate Full APB (violations will be denied access)* is selected. For Entry Reader #1, the *Entry Zone* will be selected as Zone 1 and *Exit Zone* selected as Zone 2, as shown below.

Anti-Passback (APB) Settings

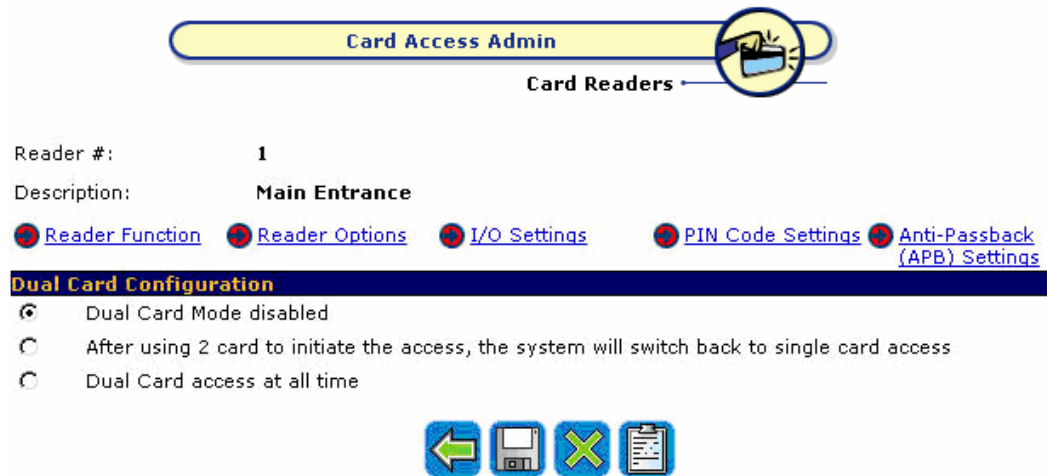
- ☐ APB deactivated
- ☐ Activate Time Based APB
Timer setting for Time Based APB: minutes
- ☐ Activate Soft APB (violations will be logged, but access/exit granted)
Entry Zone: Exit Zone:
- ☒ Activate Full APB (violations will be denied access)
Entry Zone: Exit Zone:

Similarly, for Entry Reader #3, the *Entry Zone* will be selected as Zone 2 and *Exit Zone* selected as Zone 3, as shown below.

Anti-Passback (APB) Settings

- ☐ APB deactivated
- ☐ Activate Time Based APB
Timer setting for Time Based APB: minutes
- ☐ Activate Soft APB (violations will be logged, but access/exit granted)
Entry Zone: Exit Zone:
- ☒ Activate Full APB (violations will be denied access)
Entry Zone: Exit Zone:

Dual Card Configuration



In the *Dual Card Configuration*, the Reader can either be configured as *Dual Card Mode disabled*, *After using 2 card to initiate the access, the system will switch back to single card access* or *Dual Card access at all time*.

A screen of the *Dual Card Configuration* page is shown above.

Dual Card Mode disabled

If this mode is selected, it means that no 2 cards are needed to activate the Reader.

After using 2 card to initiate the access, the system will switch back to single card access

If this mode is selected, it means that after 2 cards are presented to the same Reader to unlock the door, the Reader will switch back to single card access.

An example of the scenario would be as follows:

In the morning, 2 authorized personnel with dual card function have to present their card at the high security door Reader before the door can be accessed normally. Subsequently the rest of the employees would access the door using their own card. At the end of the day, either of the 2 authorized personnel holding the dual card will have to revert the system back to dual card mode by pressing the <3> key on the Keypad before presenting their cards.

Dual Card access at all time

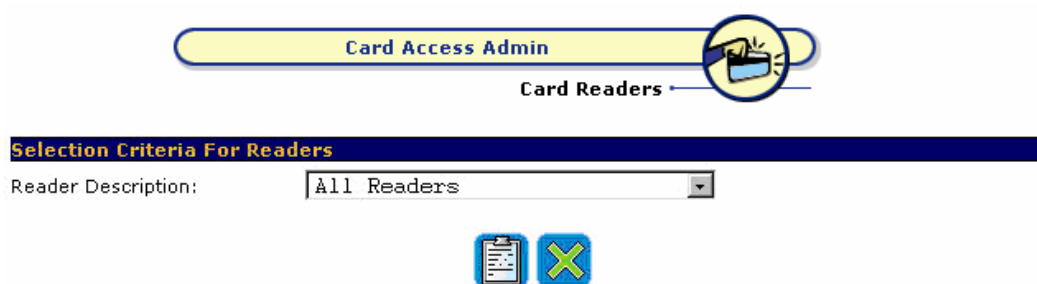
If this mode is selected, it means that 2 cards have to be presented to the Reader at all times to unlock the door.

This mode works in conjunction with the *Dual Card Assignment* under the chapter *Card Assignment* as to whether there is any order in the presentation of cards.

To generate a Print Preview of the Card Reader Report

Once you have completed configuring the Card Readers, a hardcopy can be printed out.

1. From the first web page of the Card Readers menu item, click on the  [Card Reader Report](#) link. A screen as shown below appears.



2. Select the desired Reader from the *Reader Description* list box. If no reader is selected, the report generated will include all the available readers in the selected controller. In this example, all the readers in Panel #3 will be included in the report.
3. Click on the  button for a print preview of the report. The following screen-capture shows an example of the report for the Main Entrance.

[Return To Card Readers](#) [Return To Selection Criteria](#)

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Card Reader Report

Tuesday, 19 Sep 2005 13:55:07

Reader # : 1

Description : Reader 1

Reader Function

Entry Reader

Reader Options

Turn off the reader : Not Selected

Enable Keypad Only Operation : Not Selected

On Holidays, follow holiday schedules (to work in conjunction with Card Functionality) : Selected

Keypad Timeout : 10 seconds

Enable reader lockout : Not Selected

Scheduling Options

Schedules will not be used to unlock this door

Only after a valid access condition : Not Selected

Door Output Settings

Door Open Timer : 60 seconds

Door Strike Timer : 5 seconds

Door Strike : Output 1

Door Input Settings

Request-to-Exit Device : Input 1

Door Contact : Input 2

Schedules and holidays will be used to shunt door contact: No Schedule

Door Force Open Alarm delay duration : 0 seconds

Pre-alarm Warning before door held open alarm : 0 seconds

4. If you wish to view other Reader's configuration, click on the [Return To Selection Criteria](#) link and reselect.

If you are satisfied with the configuration and wish to print out a hardcopy, click on the **Print** button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

5. To return to the Card Readers first web page, click on the [Return To Card Readers](#) link.

CHAPTER 17

Advance I/O Setup

The basic need for such an operation is to enable the rerouting of physical or logical information from one operation to another. Due to its flexibility, the type of operation it can achieve is dependent on the installer. Besides normal input, output and schedule selection, some functions will allow:-

- Inter-connection with other functions.
- Criteria to select 'Where', 'What' and 'Who' (individual and access group) as well as Key input.
- Always 'On' or 'Off'.

Some of the advance functions that it can support are:-

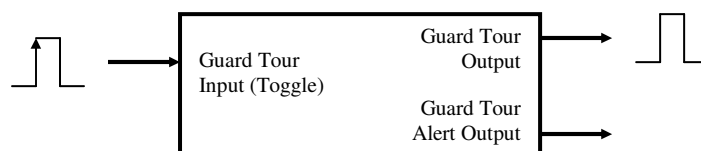
- Guard Tour
- Feed Through
- OR Logic
- AND Logic
- XOR Logic
- NAND Logic
- Interlock / Man Trap
- Up-Down Counter
- Exit Door
- One Shot

A description of each item will be given below.

Guard Tour

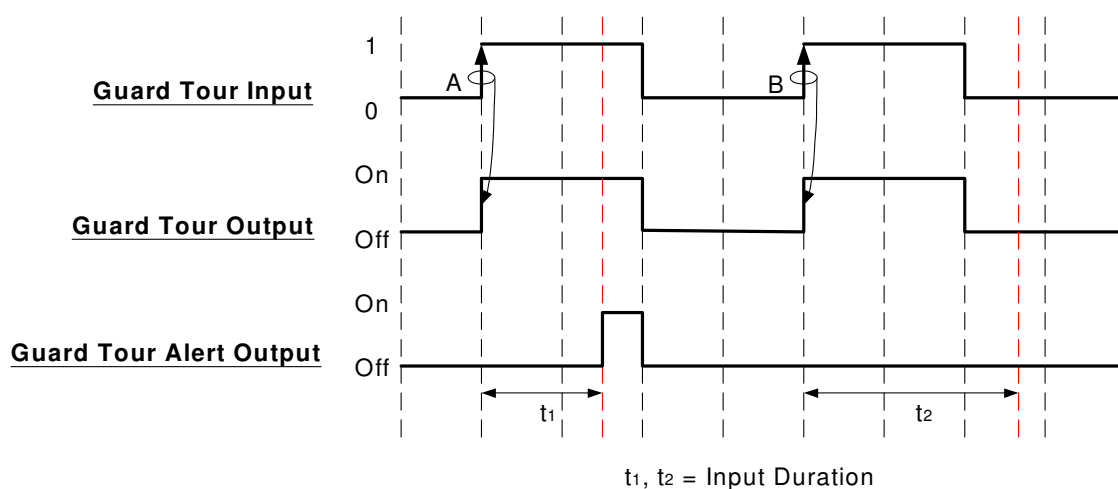
This function is used when the block is used as one of the guard tour stations in the guard tour routes.

A toggle key switch can be used to activate guard tour registration. If key is switched to ON state and is not removed, a reminder alarm will be activated.



Input/Output	Description
Guard Tour Input	This input is edge triggered from '0' to '1' (leading edge) & toggling. A key switch can be connected to this input.
Guard Tour Output	A LED is normally connected to this output. The LED will be turned on for the duration when the guard tour input is triggered.
Guard Tour Alert Output	A LED is normally connected to this output. The LED will be turned on when the Input Duration has lapsed and the key switch, which is switched to ON state, is still not removed. A reminder alarm will be activated.

The timing diagram below gives a graphical description of the function.



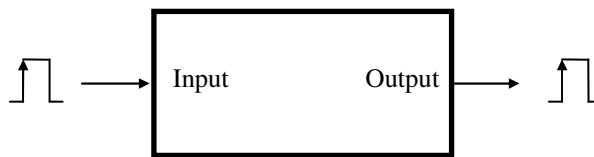
In the timing diagram above, Guard Tour Input at transition A and B will cause the Guard Tour Output to be turned On for the duration when the Guard Tour Input is triggered. When the Input Duration, t_1 , has lapsed and the Guard Tour Input is still at High (1), the Guard Tour Alert Output will be turned On until the Guard Tour Input is switched to Low (0). Whereas for t_2 , the Input Duration is such that the Guard Tour Input has already been switched to Low (0) before the Input Duration, t_2 , has lapsed. Therefore the Guard Tour Alert Output is not triggered.

In practical scenario, a key switch is normally connected to the Guard Tour Input, a LED connected to Guard Tour Output and a LED and/or an alarm is connected to the Guard Tour Alert Output. When the guard goes for his daily routine, he would turn his key switch to On state. This will cause the LED in the Guard Tour Output to be turned On. And if the key is not removed after the Input Duration has lapsed, the LED in the Guard Tour Alert Output will be turned On and the alarm will be activated to remind the guard that he has not removed the key from the key switch.

Feed Through

This function is used when the output of a function block has to be fed into the input of another function block for further action.

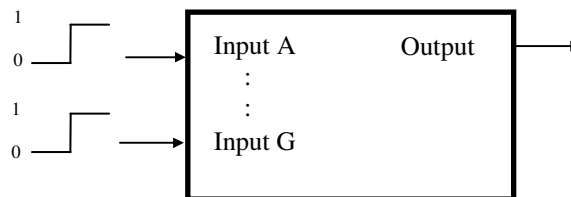
This function will enable any type of output such as physical output, link or reader control to follow the input such as physical input, physical output, link, criteria or schedule. Each item is explained in the above section *Input Point Able to Arm/Disarm by Other Type of Input*. Level or toggle input behavior can be selected.



Input/Output	Description
Input source	The input will be linked to the output directly. It is edge triggered from '0' to '1' (leading edge) & toggling.
Output	The output is a direct link of the input.

OR Logic

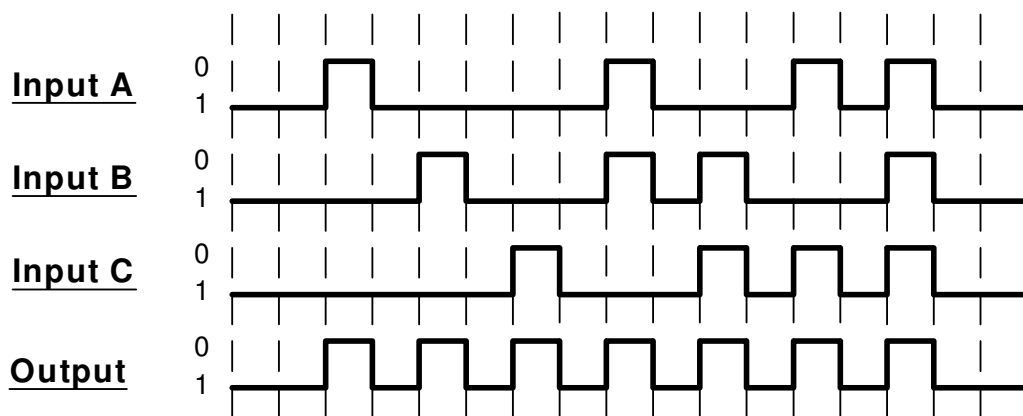
This function is used in cases whereby the output of a function block is to be triggered when any one or more of the stated conditions is fulfilled. In Advance I/O Setup, a maximum of 7 conditions is allowed.



The output is set to high when one or more of the stated inputs is set to high. The following table depicts the OR logic operation, assuming only 3 inputs are used.

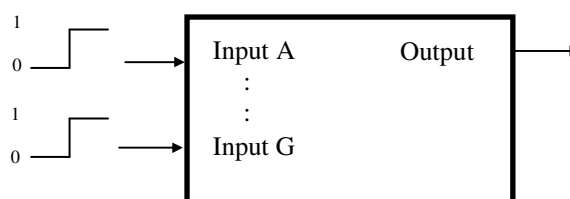
Input A	Input B	Input C	Output
0	0	0	0
1	0	0	1
0	1	0	1
0	0	1	1
1	1	0	1
0	1	1	1
1	0	1	1
1	1	1	1

The timing diagram below gives a graphical description of the function.



AND Logic

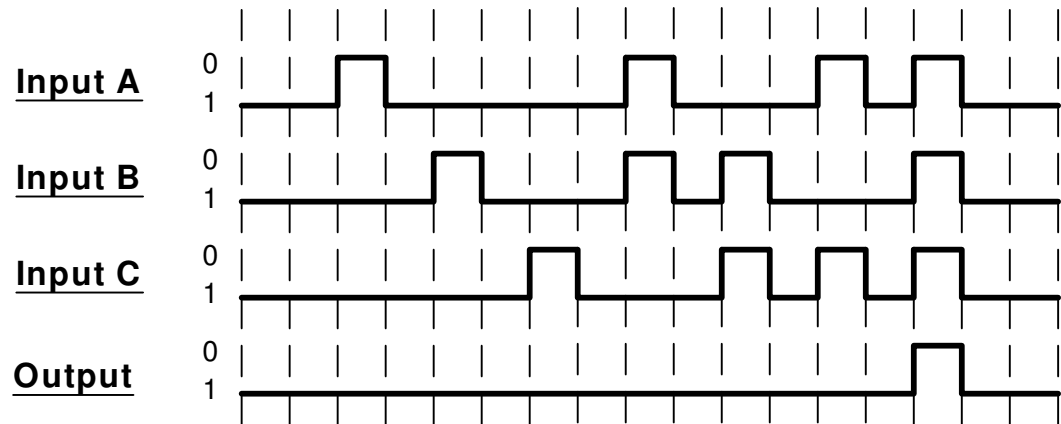
This function is used in cases whereby the output of a function block is to be triggered when all the stated conditions are fulfilled. In Advance I/O Setup, a maximum of 7 conditions is allowed.



The output is set to high when all of the stated inputs are set to high. The following table depicts the AND logic operation, assuming only 3 inputs are used.

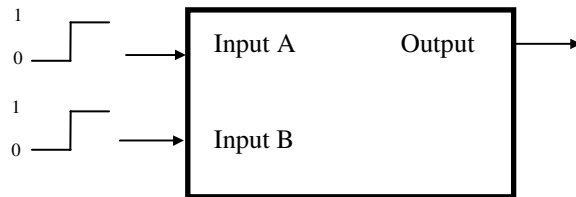
Input A	Input B	Input C	Output
0	0	0	0
1	0	0	0
0	1	0	0
0	0	1	0
1	1	0	0
0	1	1	0
1	0	1	0
1	1	1	1

The timing diagram below gives a graphical description of the function.



XOR Logic

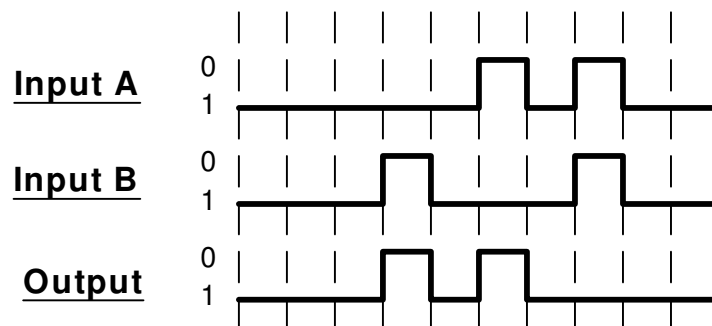
This function is used in cases whereby the output of a function block is to be triggered when all the stated conditions are different. In Advance I/O Setup, a maximum of 7 conditions is allowed.



The output is set to high when all the stated inputs are at different states. The following table depicts the XOR logic operation, assuming only 2 inputs are used.

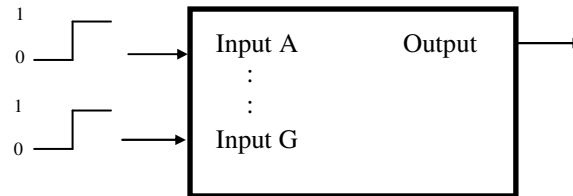
Input A	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	0

The timing diagram below gives a graphical description of the function.



NAND Logic

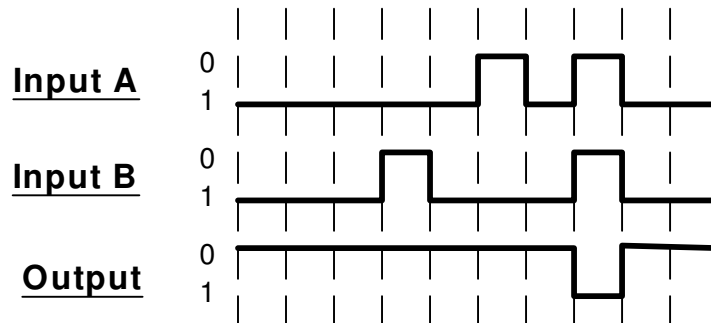
This function is used in cases whereby the output of a function block is to be triggered when one or more of the input states is low.



The output is set to high when one or more of the input states is low. The following table depicts the NAND logic operation, assuming only 2 inputs are used.

Input A	Input B	Output
0	0	1
0	1	1
1	0	1
1	1	0

The timing diagram below gives a graphical description of the function.



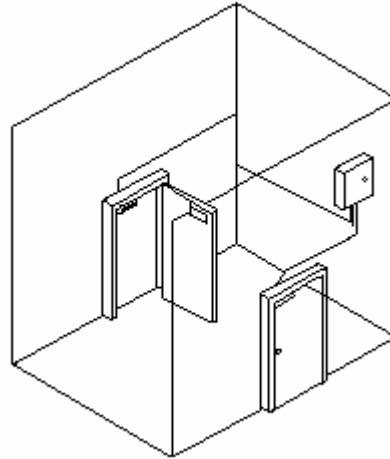
Interlock / Man Trap

i. Interlock Operation

All doors will remain closed and unlocked. Opening any of the doors will cause all other doors to be locked until the opened door returns to the closed position. In Access easy controller, a maximum of 5 doors is configurable.

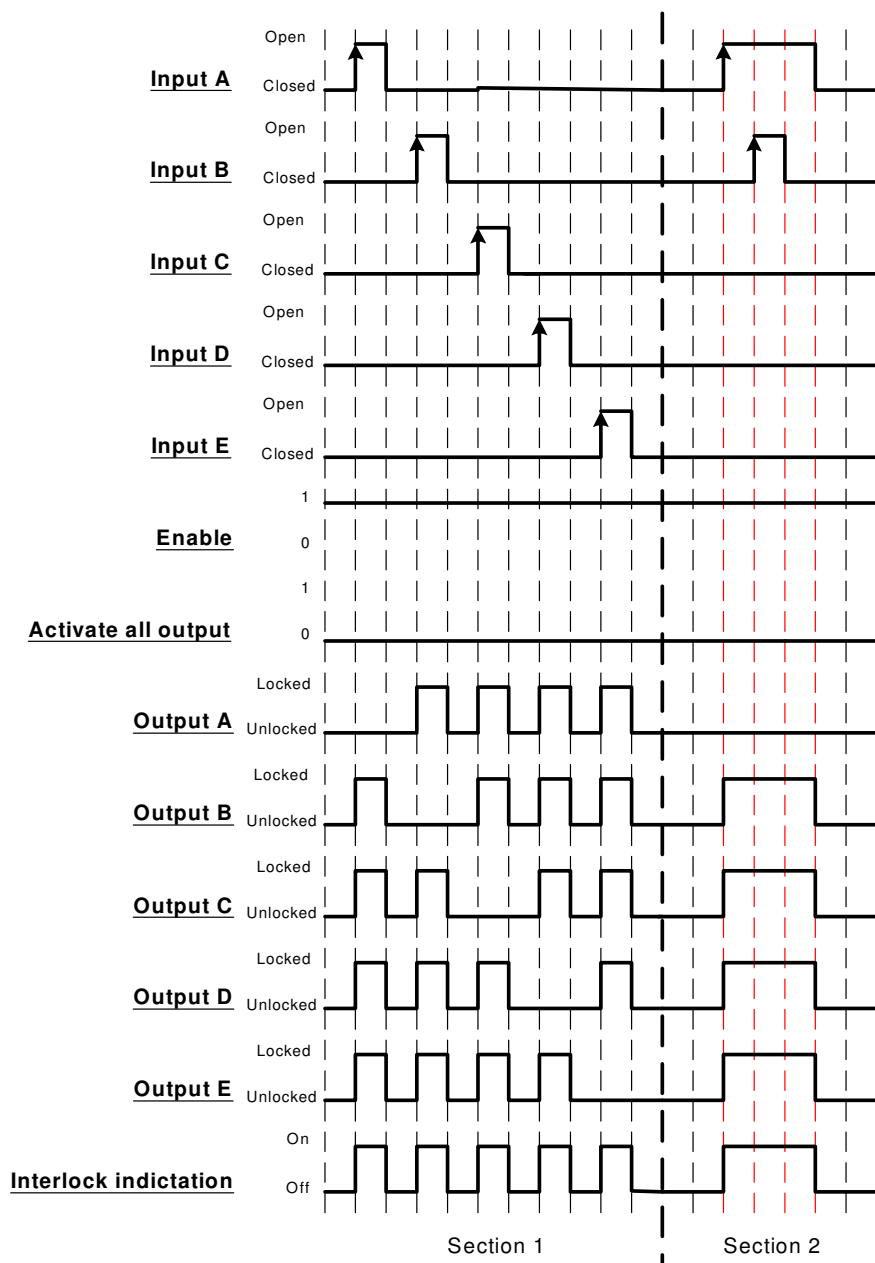
Examples of such applications are darkrooms, laboratories, clean rooms, airlock rooms, X-ray or other treatment rooms.

The figure below shows an illustration of Interlock Operation for 2 doors.



Interlock Configuration

The timing diagram below gives a graphical description of the function.



Section 1

In Section 1, a leading edge from '0' to '1' is detected at Input A first. This means that the door at A is opened. This causes the door at A to be unlocked (Output A-Low) and the rest of the doors to be locked (Output-High) until door at A is closed. The same applies when each door is opened in turn.

Enable is always high (In Access easy controller configuration, *Enable* can be configured as "Always On"). *Activate all output* is always low (In Access easy controller configuration, *Activate all output* can be configured as "Always Off").

Section 2

In Section 2, a leading edge from '0' to '1' is first detected at Input A. From Section 1, we know that the door at A is opened and this causes the door at A to be unlocked (Output A-Low) and the rest of the doors to be locked (Output-High) until door at A is closed.

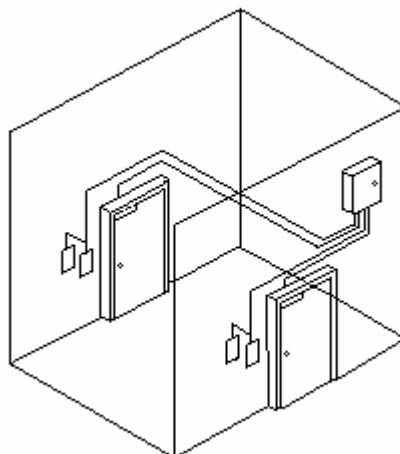
But before door at A is closed, someone tries to open door at B. He cannot open the door at B as it is locked (Output B-High) as door at A has not been closed back to original position.

ii. Man Trap Operation

All doors are normally closed and locked. Unlocking any door by reader causes the other doors to be incapable of being unlocked. In Access easy controller, a maximum of 5 doors is configurable.

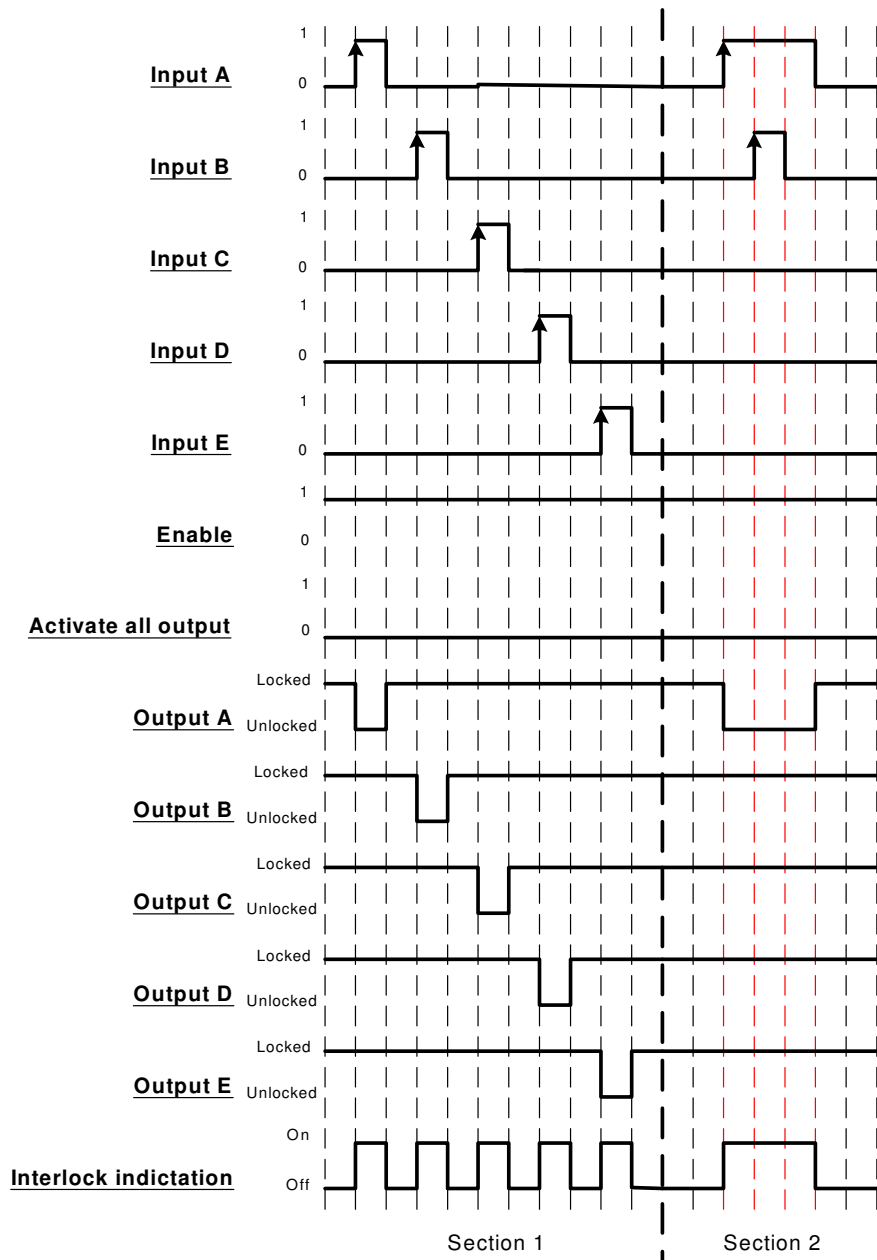
Examples of such applications are restricted darkrooms, laboratories, clean rooms, airlocks, showers, money counting rooms and computer rooms.

The figure below shows an illustration of Mantrap for 2 doors.



Man Trap

The timing diagram below gives a graphical description of the function.



Section 1

In Section 1, a leading edge from '0' to '1' is first detected at Input A, i.e. someone presents his card at reader for door A. This means that door A will be unlocked (Output A-Low) and the rest of the doors will be incapable of being unlocked (Output-High). The same applies when card is presented to the readers at the other doors in turn.

Enable is always high (In Access easy controller configuration, *Enable* can be configured as "Always On"). *Activate all output* is always low (In Access easy controller configuration, *Activate all output* can be configured as "Always Off").

Section 2

In Section 2, a leading edge from '0' to '1' is first detected at Input A. From Section 1, we know that when someone presents his card at reader for door A, door A will be unlocked (Output A-Low) and the rest of the doors to be incapable of being unlocked (Output-High).

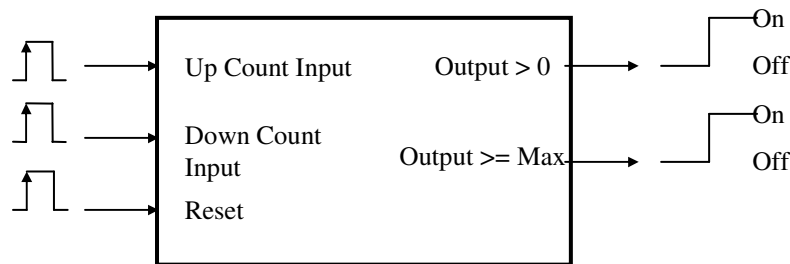
But before door A is locked back, someone presents his card at door B. He cannot unlock door B as it is incapable of being unlocked (Output B-High).

Both the above operations, Interlock Operation and Mantrap can be easily configured by monitoring the door strike and contact status.

The number of doors that can be configured for these operations is only limited by the number of I/O and Reader available per controller.

Up-Down Counter

This function enables the tracking of the number of card holder/event and is able to trigger output or control based on the maximum configuration limit.

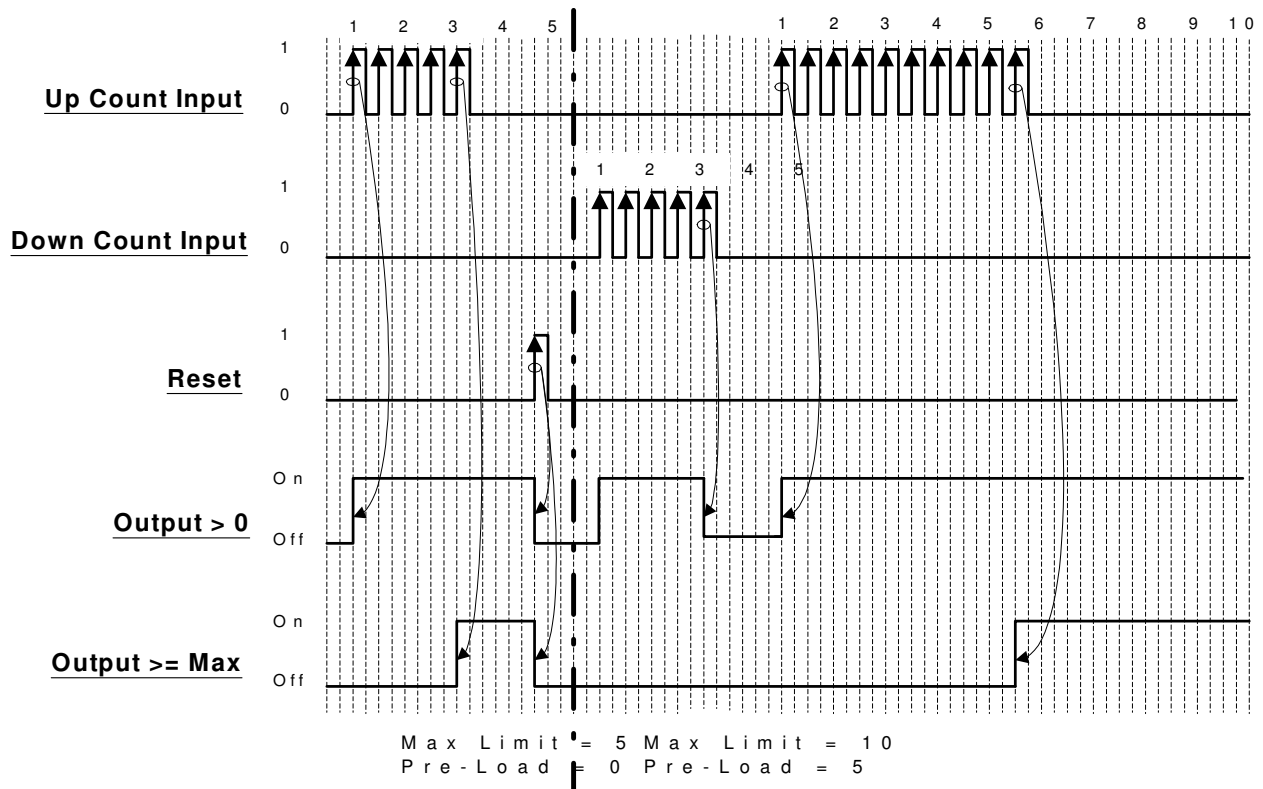


Maximum Limit = XXXXX (0 to 65535)

Pre-load counter value = XXXXX (0 to 65535)

Input/Output	Description
Up count Input	Increment the counter when a low to high edge is detected.
Down count Input	Decrement the counter when a low to high edge is detected.
Reset	Reset the counter to zero when a low to high edge is detected.
Output > 0	Set high when the counter is not zero, and set low when the counter is zero.
Output >= Max	Set high when the counter is greater than or equal to the maximum limit, else set low.

The timing diagram below gives a graphical description of the function.



In the timing diagram, the basic operation of the function is outlined below: -

Max Limit = 5 and Pre-Load = 0

With the 2 defined parameters, the **Output>=Max** will be driven high on the 5th pulse on the *Up Count* input. However, the **Output>0** is driven high on the first pulse. A *Reset* pulse clears both outputs to zero.

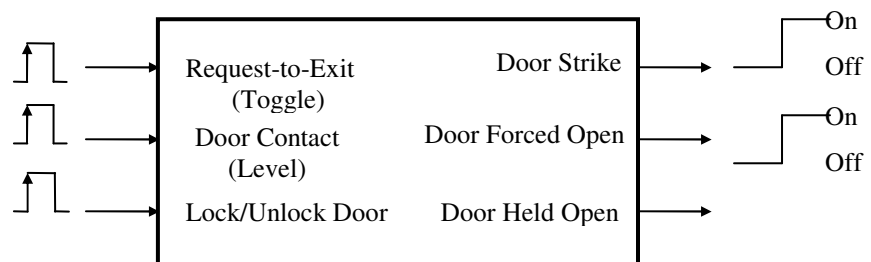
Max Limit = 10 and Pre-Load = 5

With a Pre-Load of 5 count, the **Output>0** is driven high. This **Output>0** will be cleared on the 5th pulse on the *Down Count* input.

A pulse on the *Up Count* input drives the **Output>0** high again and the **Output>=Max** will be driven high on the 10th pulse.

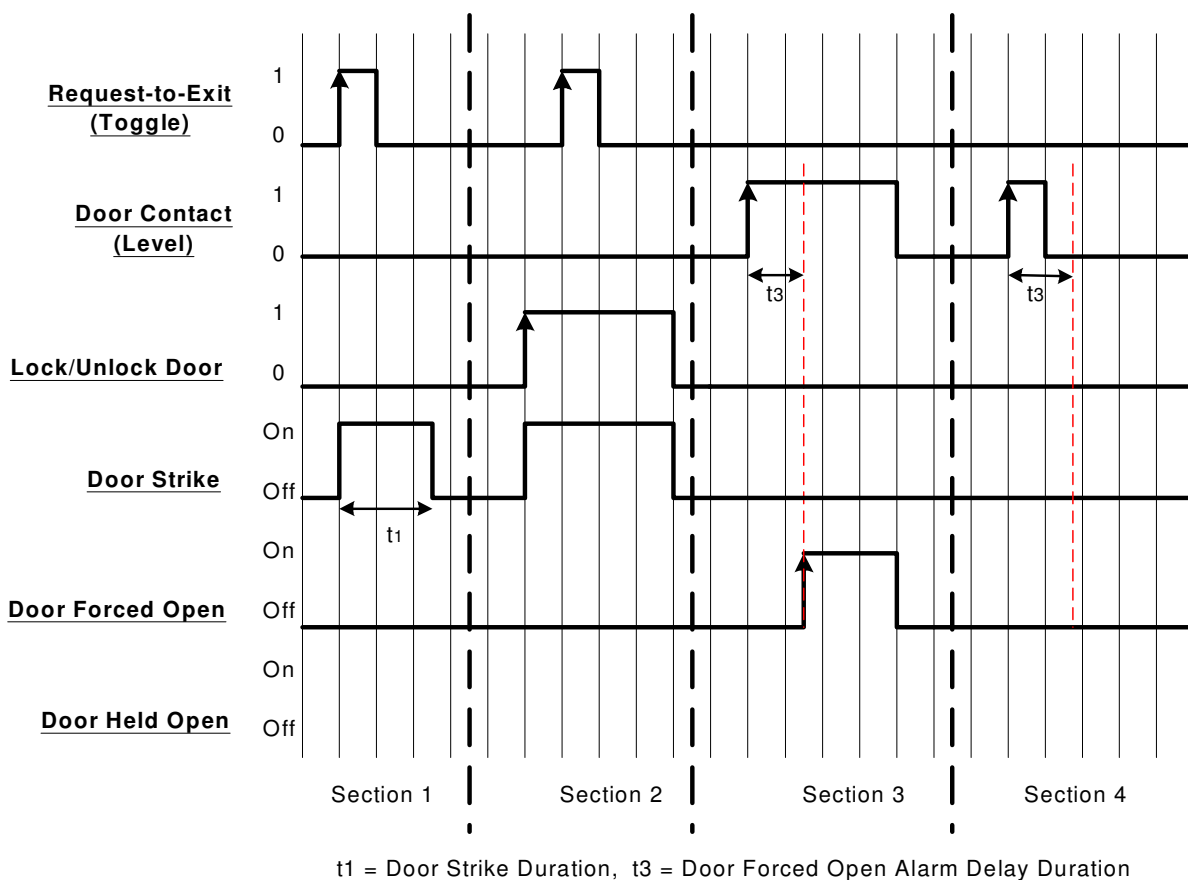
Exit Door

This function is mainly used to monitor and control emergency exit doors.



Input/Output	Description
Request-to-Exit (Toggle)	This input is edge triggered from '0' to '1' (leading edge) & toggling. It activates the Door Strike output for a period of the Door Strike Duration when a leading edge is detected.
Door Contact (Level)	This input is edge triggered from '0' to '1' (leading edge). It activates the Door Forced Open output when a leading edge is detected and a period of the Door Forced Open Alarm Delay Duration has passed.
Lock/Unlock Door	Permanently locks/unlocks the door when activated.
Door Strike	Driven to high for a period of Door Strike Duration when a leading edge is detected at Request-to-Exit.
Door Forced Open	Driven to high for the duration when Door Contact is high when a leading edge is detected at Door Contact and the Door Forced Open Alarm Delay Duration has lapsed.
Door Held Open	Driven to high when the Door Strike Duration is over and subsequently, the Door Open Duration is over.

The timing diagram below gives a graphical description of the function.



In the timing diagram, it is divided into 4 sections. The basic operation of each section is outlined below: -

Section 1

In Section 1, a leading edge from '0' to '1' is detected at Request-to-Exit. This causes the Door strike to be driven high for a duration of t_1 , the Door Strike Duration.

Section 2

In Section 2, a leading edge is first detected at Lock/Unlock Door. This causes the Door strike to be driven high for the duration when the Lock/Unlock Door is triggered. Since the Door Strike is already at state high, meaning it is de-energised, when a leading edge is detected at Request-to-Exit, there is no difference in Door Strike.

Section 3

In Section 3, a leading edge is detected at Door Contact. However there is a Door Forced Open Alarm Delay Duration of period t_3 . Hence the Door Forced Open is driven high only after the Door Forced Open Alarm Delay Duration has passed and remains high until the Door Contact is triggered low. The Door Forced Open Alarm Delay Duration is to ensure that the alarm is genuine and not caused by noise or interference.

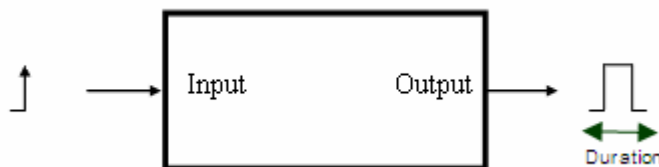
Section 4

In Section 4, a leading edge is detected at Door Contact. However the signal lasts for a period less than the Door Forced Open Alarm Delay Duration of period t_3 . Therefore the Door Forced Open output is not activated. This is because the signal detected could be due to noise or interference

One Shot

This function is similar to *Feed Through* except it is used when the output of a function block is triggered for a predefined duration when input state is high.

This function will enable any type of output such as physical output, link or reader control to follow the input such as physical input, physical output, link, criteria or schedule.



Input/Output	Description
Input source (Toggle)	The input will be linked to the output directly. It is edge triggered from '0' to '1' (leading edge).
Output	The output is a direct link of the input.

Ability to accept other types of Arm/Disarm Input Control

In Access easy controller, the arm/disarm input control can accept any type of input such as link, physical output, physical input, schedule, criteria or it can be set to always on or always off.

Input Setup is also used in conjunction with Advance I/O Setup. Each item is explained below.

Inter-connection

Inter-connection is used when the user would like to link a few functional blocks together. Each connection between two functional blocks is expressed as a Link.

Output

Output consists of physical outputs from the Reader Board and the I/O Board. Each system can provide a total of 32 Reader Board Output and 32 I/O Board Output Points.

Input

Input refers to the input of readers such as Request-to-Exit and Door Contact, and the input of I/O Board. Each system can support a total of 16 readers, hence there is a total of 16 Request-to-Exit and 16 Door Contact. Each system can support 32 Input Points. Input also includes input to the Main Power and Panel Tamper.

Schedule

Schedule refers to the time schedule that we have already learnt in *Chapter Schedule*. Please refer to *Chapter Schedule* for the usage on schedules.

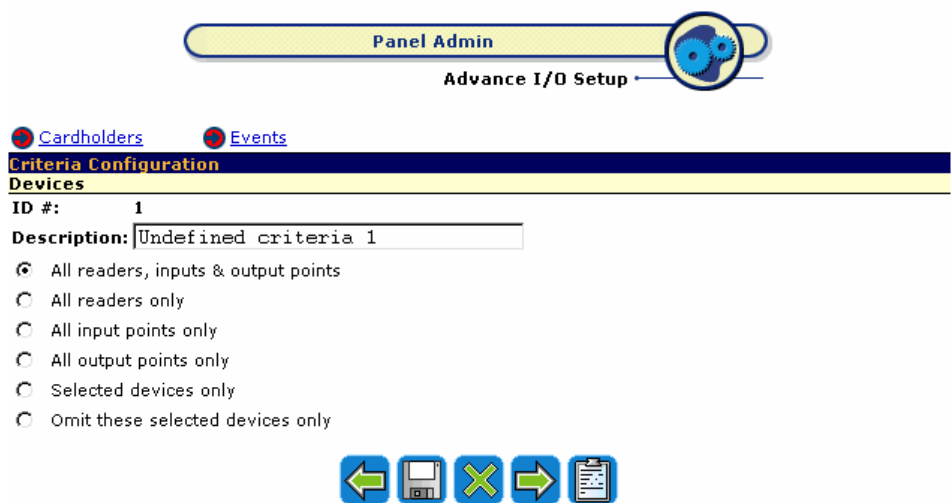
Criteria

Criteria are some of the conditions or limitations that we would like to impose on the input to the functional block. Conditions or limitations can be imposed on the devices, cardholders or events. The user can choose to include items to trigger the output or the user can choose to omit items so that it will not trigger the output of the functional block. A table listing the choice that can be selected under each item is shown below.

Criteria Configuration	Choice that can be selected
Devices	• All readers, input & output points • All readers only • All input points only • All output points only • Selected devices only • Omit these selected devices only
Cardholders	• All cardholders

	• Selected cardholders only • Omit these selected cardholders only • Selected Access Group only
Events	• All events • Selected events only • Omit these selected events only

1. To set the criteria, select *Advance I/O Setup* on the Left Pane and click on  [Criteria List](#).
2. Click on the *ID#* or *Criteria Description* of any unused criteria. The screen as shown below will appear.



Panel Admin

Advance I/O Setup

 Cardholders  Events

Criteria Configuration

Devices

ID #: 1

Description: Undefined criteria 1

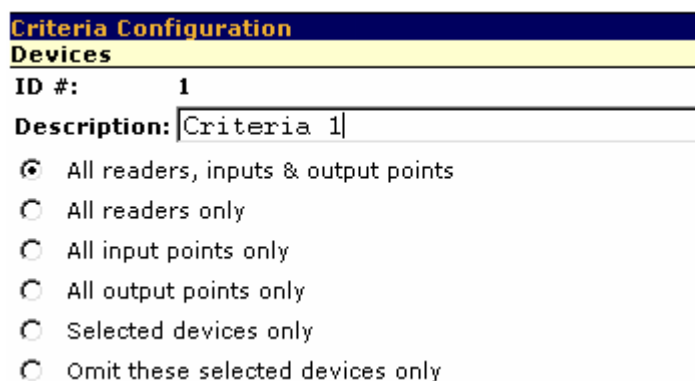
☒ All readers, inputs & output points
☐ All readers only
☐ All input points only
☐ All output points only
☐ Selected devices only
☐ Omit these selected devices only







3. Enter the *Description* for the criteria in the space provided.
4. From the *Devices* page, select the appropriate radio button.



Criteria Configuration

Devices

ID #: 1

Description: Criteria 1

☒ All readers, inputs & output points
☐ All readers only
☐ All input points only
☐ All output points only
☐ Selected devices only
☐ Omit these selected devices only

When *Selected devices only* is chosen

Criteria Configuration	
Devices	
ID #:	1
Description:	Criteria 1
☐ All readers, inputs & output points ☐ All readers only ☐ All input points only ☐ All output points only ☒ Selected devices only ☐ Omit these selected devices only	
List of Selected Devices	
Select a Device:	Reader 1

- i. To add an item to the *List of Selected Devices*, select an item from the *Select a Device* drop-down list and click on the button.
- ii. Repeat *Step i* to add more items to the *List of Selected Devices*. When the items are added to the *List of Selected Devices*, it means that only these devices will be able to trigger an output.
- iii. To remove an item from the *List of Selected Devices*, select the item on the list and click on the button.
- iv. Repeat *Step iii* to remove more items from the *List of Selected Devices*.

When *Omit these selected devices only* is chosen

Criteria Configuration	
Devices	
ID #:	1
Description:	Criteria 1
☐ All readers, inputs & output points ☐ All readers only ☐ All input points only ☐ All output points only ☐ Selected devices only ☒ Omit these selected devices only	
List of Selected Devices	
Select a Device:	Reader 1

- i. To add an item to the *List of Selected Devices*, select an item from the *Select a Device* drop-down list and click on the button.
- ii. Repeat *Step i* to add more items to the *List of Selected Devices*. When the items are added to the *List of Selected Devices*, it means that only these devices will be omitted and will not be able to trigger an output.

- iii. To remove an item from the *List of Selected Devices*, select the item on the list and click on the  button.
- iv. Repeat *Step iii* to remove more items from the *List of Selected Devices*.
5. To go to the *Cardholders* page, click on the  button from the *Devices* page or click on  [Cardholders](#).
6. From the *Cardholders* page, select the appropriate radio button.

Criteria Configuration
Cardholders

ID #: 1

Description: Criteria 1

☒ All cardholders

☐ Selected cardholders only

☐ Omit these selected cardholders only

☐ Selected Access Group only

Reader Control Key: 

When *Selected cardholders only* is chosen

Criteria Configuration
Cardholders

ID #: 1

Description: Criteria 1

☐ All cardholders

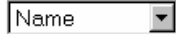
☒ Selected cardholders only

☐ Omit these selected cardholders only

☐ Selected Access Group only

List of Selected Cardholders: 

Search : 

Option: 

Reader Control Key: 



- i. To add an item to the *List of Selected Cardholders*, user can make a search for the cardholder by using the *Option* drop-down list to search by his Name, Card Number, User Field 1 or User Field 2.
- ii. After selecting the appropriate *Option*, user has to enter a corresponding character in the space provided beside *Search* and click on . If the user selects Name in the *Option*, alphabet/s must be entered in the space, whereas if the user selects Card Number in the *Option*, number/s must be entered in the space provided. For example, we are searching for 'Joey Tan' and we make a search by Name with the alphabet 'j'. The screen as shown below will appear.

Criteria Configuration**Cardholders**

ID #: 1

Description: Criteria 1

- ☐ All cardholders
☒ Selected cardholders only
☐ Omit these selected cardholders only
☐ Selected Access Group only

List of Selected Cardholders:

Search :

Option:

Cardholders Found:

Reader Control Key:



- iii. Select 'Joey' and click on the  button. The Name 'Joey Tan' will appear in the *List of Selected Cardholders*.
- iv. Repeat *Step i, ii* and *iii* to add more items to the *List of Selected Cardholders*. When the items are added to the *List of Selected Cardholders*, it means that only these cardholders will trigger an output.
- v. To remove an item from the *List of Selected Cardholders*, select the  item on the list and click on the  button.
- vi. Repeat *Step v* to remove more items from the *List of Selected Cardholders*.

When *Omit these selected cardholders only* is chosen**Criteria Configuration****Cardholders**

ID #: 1

Description: Criteria 1

- ☐ All cardholders
☐ Selected cardholders only
☒ Omit these selected cardholders only
☐ Selected Access Group only

List of Selected Cardholders:

Search :

Option:

Reader Control Key:



- i. To add an item to the *List of Selected Cardholders*, user can make a search for the cardholder by using the *Option* drop-down list to search by his Name, Card Number, User Field 1 or User Field 2.
- ii. After selecting the appropriate *Option*, user has to enter a corresponding character in the space provided beside *Search* and click on . If the user selects Name in the *Option*, alphabet/s must be entered in the space, whereas if the user selects Card Number in the *Option*, number/s must be entered in the space provided. For example, we are searching for 'Joey Tan' and we make a search by Name with the alphabet 'j'. The screen as shown below will appear.

Criteria Configuration
Cardholders

ID #: 1
Description: Criteria 1

☐ All cardholders
☒ Selected cardholders only
☐ Omit these selected cardholders only
☐ Selected Access Group only

List of Selected Cardholders:

Search :

Option:

Name
 Joey Tan (8888)
 Janet Lim (8090)

Cardholders Found:

Reader Control Key:









- iii. Select 'Joey' and click on the  button. The Name 'Joey Tan' will appear in the *List of Selected Cardholders*.
- iv. Repeat *Step i, ii* and *iii* to add more items to the *List of Selected Cardholders*. When the items are added to the *List of Selected Cardholders*, it means that only these cardholders will be omitted and will not be able to trigger an output.
- v. To remove an item from the *List of Selected Cardholders*, select the item on the list and click on the  button.
- vi. Repeat *Step v* to remove more items from the *List of Selected Cardholders*.

When *Selected Access Group only* is chosen

Criteria Configuration
Cardholders

ID #: 1

Description: Criteria 1

☐ All cardholders
☐ Selected cardholders only
☐ Omit these selected cardholders only
☒ Selected Access Group only

List of Selected Access Groups:

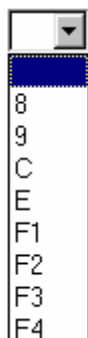
Option: Full Access Group

Reader Control Key:



- i. To add an item to the *List of Selected Access Groups*, select an item from the *Option* drop-down list and click on the  button.
 - ii. Repeat *Step i* to add more items to the *List of Selected Access Groups*. When the items are added to the *List of Selected Access Groups*, it means that only cardholders in these access groups will trigger an output.
 - iii. To remove an item from the *List of Selected Access Groups*, select the item on the list and click on the  button.
 - iv. Repeat *Step iii* to remove more items from the *List of Selected Access Groups*.
7. After selecting the appropriate radio button, user must select the *Reader Control Key*, as shown below. If it is not required, select the blank space. When the Reader Control Key is selected, for example, '8' is selected, it means that the user must press the key '8' on the reader keypad before presenting the card to the reader. Of course, all other conditions are to be satisfied.

Reader Control Key:



Note For C3 Smart Card Readers Series, the key is 'C' and 'E'. For ProxPro Reader with keypad, the key 'C' is replaced by '*' and the key 'E' is replaced by '#'.

8. To go to the *Events* page, click on the  button from the *Cardholders* page or click on  [Events](#).

9. From the *Events* page, select the appropriate radio button.

Criteria Configuration

Events

ID #: 1

Description: Criteria 1

- ☒ All events
- ☐ Selected events only
- ☐ Omit these selected events only

When *Selected events only* is chosen

Criteria Configuration	
Events	
ID #:	1
Description:	Criteria 1
☐ All events ☒ Selected events only ☐ Omit these selected events only	
List of Selected Events:	
Select an Event:	Panel Tampered

- i. To add an item to the *List of Selected Events*, select an item from the *Select an Event* drop-down list and click on the button.
- ii. Repeat *Step i* to add more items to the *List of Selected Events*. When the items are added to the *List of Selected Events*, it means that only these events will trigger an output.
- iii. To remove an item from the *List of Selected Events*, select the item on the list and click on the button.
- iv. Repeat *Step iii* to remove more items from the *List of Selected Events*.

When *Omit these selected events only* is chosen

Criteria Configuration	
Events	
ID #:	1
Description:	Criteria 1
☐ All events ☐ Selected events only ☒ Omit these selected events only	
List of Selected Events:	
Select an Event:	Panel Tampered

- i. To add an item to the *List of Selected Events*, select an item from the *Select an Event* drop-down list and click on the button.
- ii. Repeat *Step i* to add more items to the *List of Selected Events*. When the items are added to the *List of Selected Events*, it means that only these events will be omitted and will not be able to trigger an output.
- iii. To remove an item from the *List of Selected Events*, select the item on the list and click on the button.

- iv. Repeat *Step iii* to remove more items from the *List of Selected Events*.

Note For each criteria, please ensure that there is no conflict in the configuration of the Devices, Cardholders and Events. The combination of the selection of the Devices, Cardholders and Events should be logical.

An example of using the Criteria

In this example, we are configuring the settings for criteria ID #1 and we name it Criteria 1.

1. In the *Devices* page, select the radio button *Selected devices only*. In this example, we select 'Reader 1' as the device that will trigger an output.

Criteria Configuration	
Devices	
ID #:	1
Description:	Criteria 1
☐ All readers, inputs & output points ☐ All readers only ☐ All input points only ☐ All output points only ☒ Selected devices only ☐ Omit these selected devices only	
List of Selected Devices	Reader 1
Select a Device:	Reader 1

2. In the *Cardholders* page, select the radio button *Selected cardholders only*. In this example, we select the Name 'Michael Tay' as the cardholder who will trigger an output.

Criteria Configuration	
Cardholders	
ID #:	1
Description:	Criteria 1
☐ All cardholders ☒ Selected cardholders only ☐ Omit these selected cardholders only ☐ Selected Access Group only	
List of Selected Cardholders:	Michael Tay (10250)
Search :	
Option:	Name
Reader Control Key:	

- In the *Events* page, select the radio button *Selected events only*. In this example, we select the event 'Access Granted' as the event that will trigger an output.

Criteria Configuration	
Events	
ID #:	1
Description: Criteria 1	
☐ All events ☒ Selected events only ☐ Omit these selected events only	
List of Selected Events:	Access Granted
Select an Event:	Panel Tampered

Now we use Criteria 1 as the arm/disarm input control. We configure the settings for Input #1 and we name it Input Point 1. The settings for Input #1 is as shown below.

Input #:	1
Description:	Input Point 1
Arm Delay:	5 seconds (0 - 255)
Alarm Delay:	5 seconds (0 - 255)

Input Arm/Disarm Control		Output Link	
 Criteria 1	NotAssigned Zone Arm/ Disarm ☐ Toggle	Alarm Status Output Point 1	Arm/ Disarm Status Output Point 2
		Ready Status Output Point 3	Bypass Status Output Point 4

When the arm/disarm input control is set to Criteria 1, and the cardholder 'Michael Tay' was 'granted access' at 'Reader 1', Input #1 will be armed and Output Point 2 is turned on.

Always On/Off

When the arm/disarm input control is selected as Always On, the input point is armed and will be in the armed state until it is disarmed again.

An example of using the Always On/Off

In this example, we use Always On as the arm/disarm input control. We configure the settings for Input #1 and we name it Input Point 1. The settings for Input #1 is as shown below.

Input #: **1**

Description:

Arm Delay: seconds (0 - 255)

Alarm Delay: seconds (0 - 255)

Input Arm/Disarm Control		Output Link	
NotAssigned	Zone	Alarm Status	Output Point 1
 Always On	Arm/ Disarm ☐ Toggle	Arm/ Disarm Status	Output Point 2
		Ready Status	Output Point 3
		Bypass Status	Output Point 4

After the arm/disarm input control is set to Always On, Input #1 will be armed and Output Point 2 is turned on.

This Page Intentionally Left Blank

CHAPTER 18

Users

Each user can be assigned access rights to access and carry out programming of certain or all functions of the Access Easy Controller.

The *Users* menu item allows the *System Administrator* to define different access to users, by selecting whether a particular user can have *View* and/or *Save* rights to programming functions.

Another 24 users can be assigned. By default, User1 is defined as the *Super-User* having access to all the Access Easy Controller features.

NOTE: The access rights to User1 are hard-coded and cannot be changed. Only the User Name and Password can be changed.

The default *Super-User* can define the access rights (View and/or Save) of the remaining 24 users, up to the level equivalent to the Super-User.

The Access Easy Controller software will not display the  button on the screen when users without the *Supervisory Access Level* rights login, implying that changes or settings made cannot be saved.

Another indication of not having access right to certain menu item(s) is that the menu item(s) is not underlined and moving the pointer over it

doesn't cause the pointer to change to a finger () symbol.

To activate Users

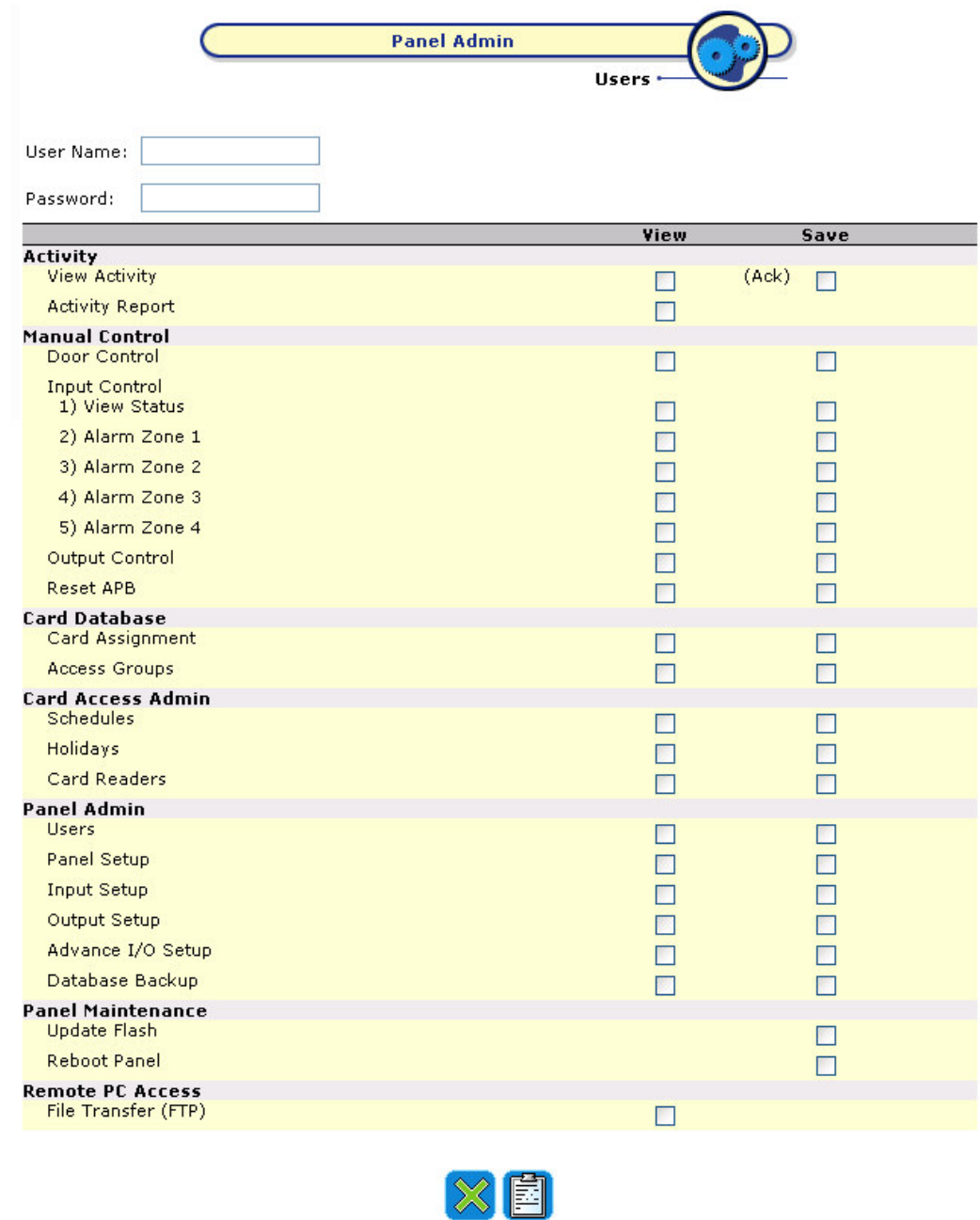
Since Users is the first menu item of the **Panel Admin** group, from the Home page, click on Panel Admin or its icon button. However, if you are in other menu item page, click directly on the Users link.



The procedures following this assumed that you have login as the *Super-User*.

To edit User ID and Password

1. Click on the *numbering* or the *Description* text to proceed.



	View	Save
Activity		
View Activity	☐	(Ack) ☐
Activity Report	☐	
Manual Control		
Door Control	☐	☐
Input Control		
1) View Status	☐	☐
2) Alarm Zone 1	☐	☐
3) Alarm Zone 2	☐	☐
4) Alarm Zone 3	☐	☐
5) Alarm Zone 4	☐	☐
Output Control	☐	☐
Reset APB	☐	☐
Card Database		
Card Assignment	☐	☐
Access Groups	☐	☐
Card Access Admin		
Schedules	☐	☐
Holidays	☐	☐
Card Readers	☐	☐
Panel Admin		
Users	☐	☐
Panel Setup	☐	☐
Input Setup	☐	☐
Output Setup	☐	☐
Advance I/O Setup	☐	☐
Database Backup	☐	☐
Panel Maintenance		
Update Flash		☐
Reboot Panel		☐
Remote PC Access		
File Transfer (FTP)	☐	

2. To edit the *User Name*, highlight the default *User Name* and enter the new *User Name*, limiting to eight alphanumerical characters including punctuation marks.
3. To edit the *Password*, highlight the default *Password* and enter the new *Password*, limiting to eight alphanumerical characters including punctuation marks (see NOTE 1 and 2).

NOTE 1: The *Password* is case-sensitive.

NOTE 2: For security reason, every character entered for the *Password* is represented by an asterisk (*). For *Macintosh* user, it is represented by a dot (•) instead.

To select access right to Access Easy Controller menu items

Please refer to the corresponding chapters to understand the various menu items before assigning the access rights. However, there are access rights for the title, File Transfer (FTP) that was not discussed in this manual. The FTP title refers to the use of the separate Access Easy Controller Utility program called the Database Converter. Please refer to *Access Easy Controller Utility Programs User Manual* for details.

View

Refers to having the right to access and view the contents of that menu item.

Save

Refers to having the right to access and edit the setting within the menu item.

When only the *Save* function for the menu item is checked, the system would treat that both *View* and *Save* function is enabled.

1. To assign the various menu item access rights, check the checkbox of the desired menu item(s) under *View* and/or *Save* column. To de-select the point, click on it again.

CHAPTER 19

Update Flash

This function allows Access Easy Controller parameters update (database recovery) to the flash to be carried out merely by a few clicks of the mouse button. User can easily use a simple ftp program (using third party program) to transfer file(s) either from *Bosch Security Systems web site* or *Bosch Security Systems dealers* to a designated location in Access Easy Controller directory, initiate the *Update Flash* and allow the Access Easy Controller software to install the program / update the flash automatically.

Note 1: Please check with BOSCH SECURITY SYSTEMS or its authorised dealers for the upgrade.

Note 2: For Database Recovery, user must have the previous parameters setting in encrypted zipped format (db_tar.gz) in their local hard disk. Please refer to the Chapter on Database Backup for detail.

Note 3: Before attempting to ftp to the Access Easy Controller, the Remote PC IP needs to be configured first in the Panel Setup, else the panel will not allow connection. Goes to the Panel Setup of the Access Easy Controller and configure into any of the 3 remote PC setting, the PC's IP address that you intend to use for.

Panel Admin

Panel Setup

[Network Settings](#) [Input Point Configuration](#) [Set Date & Time](#)
[Auto Logout Timer](#) [Audit Log](#) [Default Settings](#)
[Card Format](#) [Company Profile](#) [Email/SMS Configuration](#)
[Email Server Settings](#) [Dial In IP Settings](#) [AEMC Settings](#) [SMS Server Settings](#)

Network Settings

Panel's IP Address: 129 . 2 . 2 . 116
 Panel's IP Netmask: 255 . 255 . 0 . 0
 Panel's Gateway: 129 . 2 . 0 . 254

Remote PC Address

#	IP Address	PC Name
1	129 . 3 . 0 . 178	remotehost1
2	129 . 2 . 0 . 206	remotehost2
3	129 . 3 . 0 . 178	remotehost3

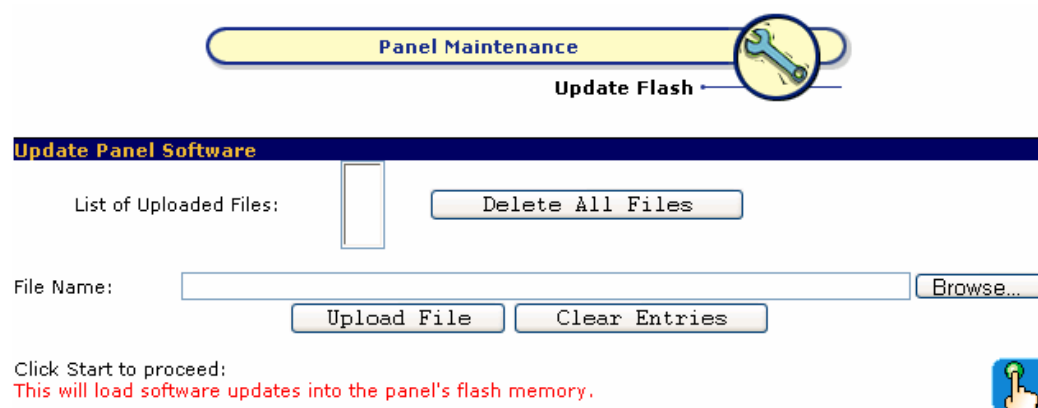
Enter the IP address of the PC in one of the below.

File(s) for upgrading can be categorised as program enhancement, bugs fixing, new features... etc. For the flash update, this is usually carried out when the Access Easy Controller's CPU Card flash memories become corrupted or that the CPU Card is out of service and needed replacement to resume normal operation.

This function will permanently overwrite your existing data in the flash memories.

To activate Update Flash

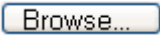
Since Update Flash is the first menu item of the **Panel Maintenance** group, from the Home page, click on Panel Maintenance or its icon button. However, if you are in other menu item page, click directly on the Update Flash link.

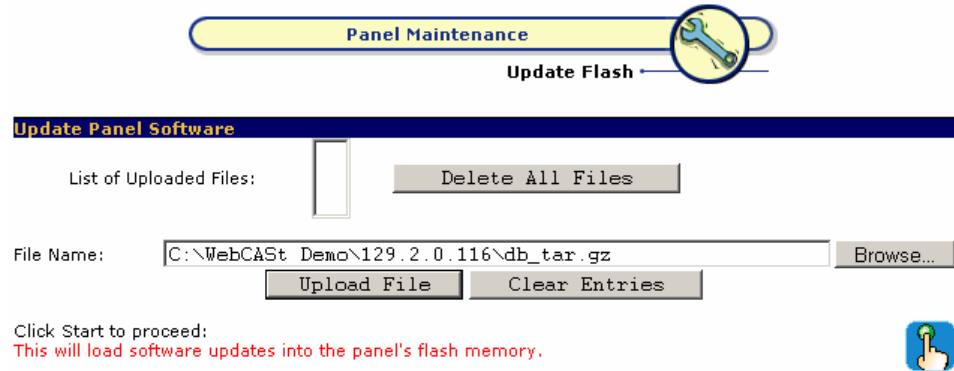


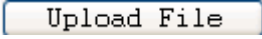
The screenshot shows the 'Panel Maintenance' section of a web interface. At the top, there is a yellow bar with the text 'Panel Maintenance' and a blue wrench icon. Below this, a blue bar contains the text 'Update Flash'. The main content area has a dark blue header 'Update Panel Software'. Below the header, there is a 'List of Uploaded Files:' label next to an empty table. To the right of the table is a 'Delete All Files' button. Below the table, there is a 'File Name:' label next to a text input field. To the right of the input field is a 'Browse...' button. Below the input field, there are two buttons: 'Upload File' and 'Clear Entries'. At the bottom, there is a red text warning: 'Click Start to proceed: This will load software updates into the panel's flash memory.' To the right of the warning is a small icon of a hand pointing at a screen.

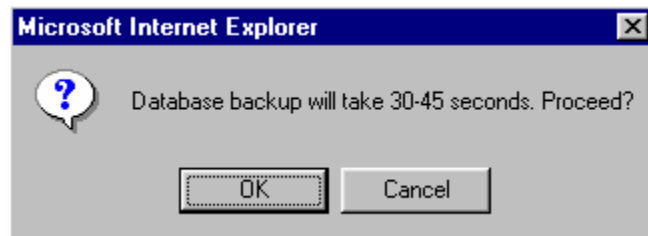
NOTE: The uploading of db_tar.gz will replace all configurations except IP address. This action is irreversible.

To Update Panel Software

1. Click on  button to select the file you wish to upload. example, if you are uploading the backup system database, select the db_tar.gz from your local director



2. Click on  button to upload.
3. Once the file appears in the "List of Uploaded Files, you could now click on the  icon to start the updating process. The following dialog box will appear for confirmation.



4. Click on the **OK** button to proceed.
5. Once the process is completed without error, the following message will appear.

Upgrade Operation Completed. You need to reboot the system for the changes to take effect.



6. Click on the  button and reboot the Access Easy Controller.

This Page Intentionally Left Blank

CHAPTER 20

Reboot Panel, Shutdown Panel

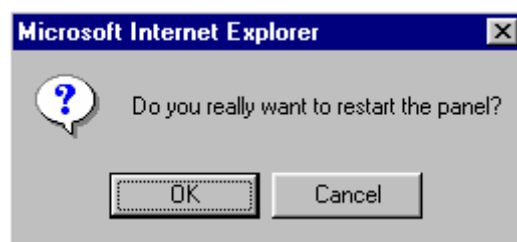
To activate Reboot Panel

Since the Access Easy Controller's software is residing within its hardware. The *Reboot Panel* menu item allows user to reboot the controller after upgrading to the system software is completed or in order to allow changes made to take effect, especially changes made to *Network Setting, Panel's IP Address*.

CAUTION!	During a <i>Reboot Panel</i> function, all settings and parameters are taken from the <i>flash memories</i>. In such a case, it is important that the <i>Database Backup</i> function is carried out before proceeding to reboot the Access Easy Controller .
-----------------	--

The *Reboot Panel* can be activated only from the menu item page.

1. From any menu item page, click on the Reboot Panel hyperlink. The following dialog box appears for confirmation.



2. Click on the **OK** button to proceed.
3. It takes about two minutes for the process to complete (see NOTE).

NOTE:	During the rebooting process, the Access Easy Controller <i>disconnect</i> itself from the computer and the web page on the computer screen might show an error message or be completely blank. User(s) must close and re-launch the web browser program. Login to Access Easy Controller again after the process is completed.
--------------	---

4. Once the Access Easy Controller is up and running again, please re-enter the Access Easy Controller URL Address and proceed with the Login.

To Shutdown Panel

The Shutdown Panel function allows the user to do a proper shutdown of the controller hardware. This is usually done when controller hardware require ant harware upgrades or maintenance

Shutdown Panel can be activated only from the Left Pane menu item.

1. From any menu item page, click on the *Shutdown Panel* link from the Left Pane. The following dialog box appears for confirmation.



5. Click on the **OK** button to proceed. User need to manually switch on the power at the controller once the necessary changes are done at the controller.

CHAPTER 21

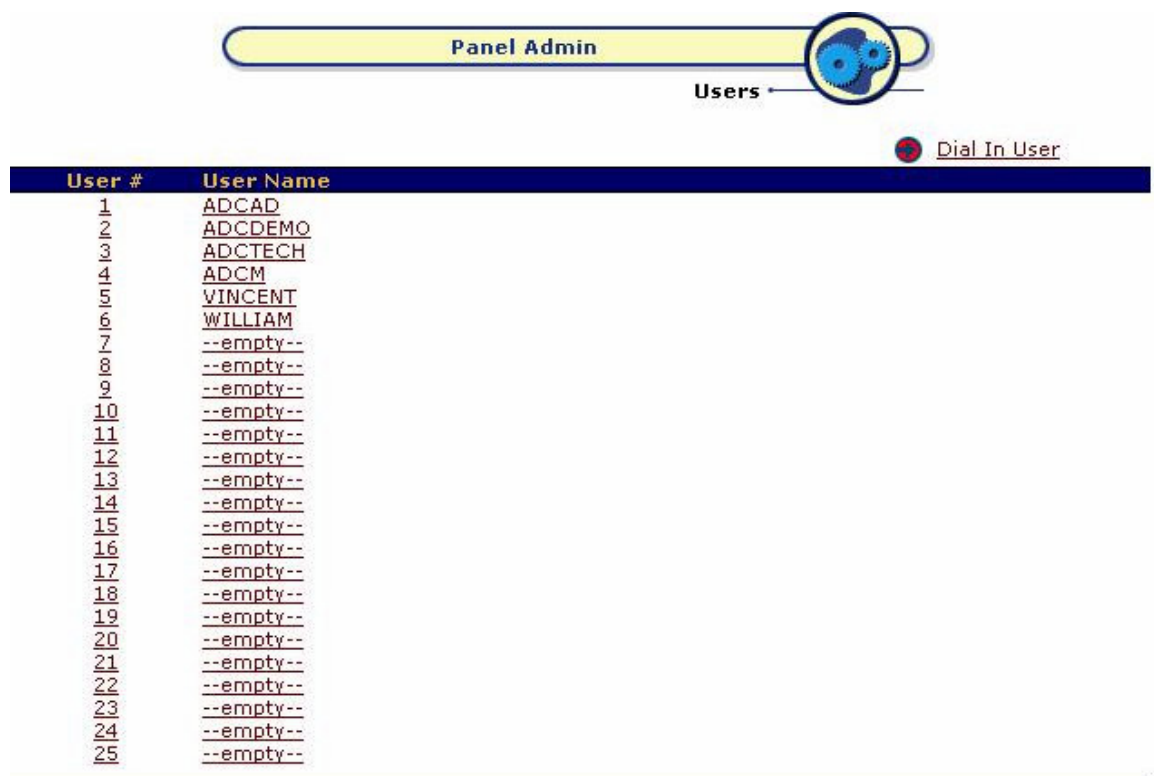
Dial in User

Dial-in user is a feature available in Access Easy Controller by which a user can connect to Access Easy Controller through telephone dial-in. This feature is useful when a user wants to remotely connect to his Access Easy Controller. The following steps will explain how to use this feature.

Setting up Windows for Dial-in

The steps below will explain how to make your Access Easy Controller receive a dial-in request from a PC.

1. Log on to Access Easy Controller. From any window of Access Easy Controller, click on users. You will see a screen that displays the users. On this screen, click on the dial-in user button as shown in the screen shot below.



2. Next you will come to a screen which displays the dial-in user name and password. Enter the User name and password in the appropriate boxes and click on save button indicated by floppy icon.



The interface shows a yellow header bar with the text "Panel Admin" and a blue gear icon. Below it, the word "Users" is displayed. The main content area has a dark blue header bar with the text "Dial In User". Below this, there are two input fields: "User Name:" with the text "PPP" and "Password:" with the text "*****". Below these fields is a grey header bar with the text "Dial In Settings". Below this, there are two settings: "Number of illegal password attempts:" with a dropdown menu showing "Undefined" and "Illegal attempts lockout duration:" with a text box showing "0" and the text "minutes (0 - 255)". At the bottom, there are three icons: a floppy disk, a green X, and a document with a pencil.

Panel Admin

Users

Dial In User

User Name:

Password:

Dial In Settings

Number of illegal password attempts:

Illegal attempts lockout duration: minutes (0 - 255)

IMPORTANT: CHANGE THE DEFAULT USER NAME AND PASSWORD AND SAVE THE NEW SETTINGS BY CLICKING ON SAVE BUTTON INDICATED BY FLOPPY ICON

3. The default user name and password has to be changed for security reasons. Enter the changed user name and password. You may also set the number of illegal password attempts and the illegal attempts lockout duration as shown in the screen.
4. The Number of illegal password attempts drop down box allows you to set the number of times the system will let you enter an illegal password before locking you out.
5. The Illegal attempts lockout duration box allows you to set the duration to disable the dial-in feature after a number of illegal password attempts as specified in step 4.
6. Click Save button to save configuration.
7. Make sure that a 56K modem is connected to your Access Easy Controller and is powered up. The modem must be connected to your telephone line to receive a dial-in request. Access Easy Controller will initialise the modem when it is re-booted.
8. Re-boot the Access Easy Controller.
9. Now your Access Easy Controller is ready to receive a dial-in request.

IMPORTANT: The modem has to be power up and connected to the Access Easy Controller before the Access Easy Controller reboots. Access Easy Controller will initialise the modem to auto answer mode .If initialising is not done, dial-in will not be successful

NOTE: Once initialised, the modem will always go into auto answer mode when power up.

The following setup will guide you through the settings that are needed on your PC in order to dial into the Access Easy Controller.

1. Firstly, you will need to change the IP address of your PC which you intend to use to connect to Access Easy Controller via modem to a different network segment.

For example : the Access Easy Controller having a IP address of 129.2.0.41 and the subnetmask is **255.255.255.0**, the dial-in PC could have any IP address but the subnetmask must not be **255.255.255.0**, it could be **255.255.0.0** or **255.0.0.0**

After changing the IP address of your dial-in PC, remember to reboot the PC before proceeding to the next step.

2. Now you will need to setup the dial-in connection. Click on Start button. Select Programs-Accessories-Communications- Dial-up networking as shown below and click on Dial-Up Networking.

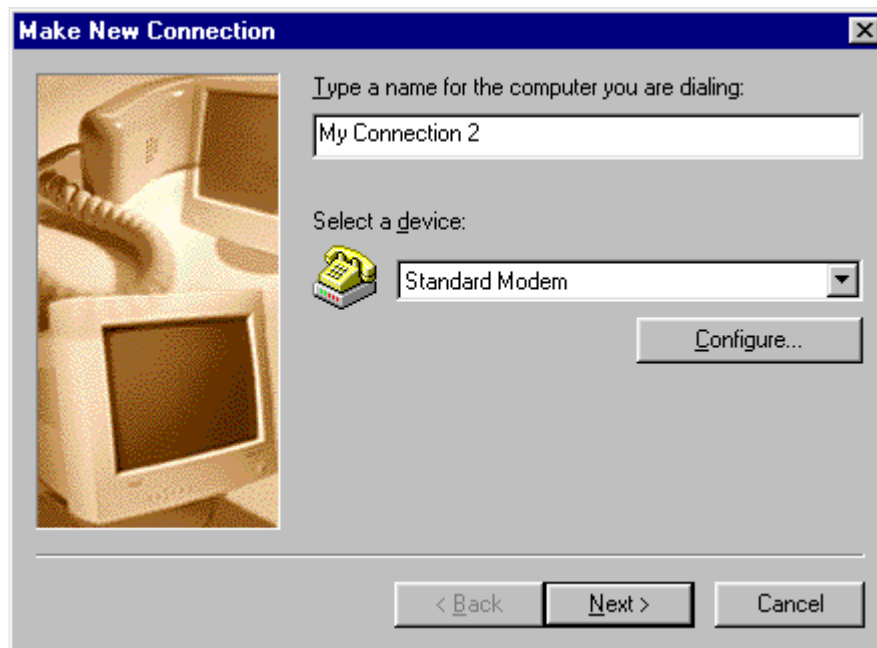


3. You will be led to a screen as shown below.

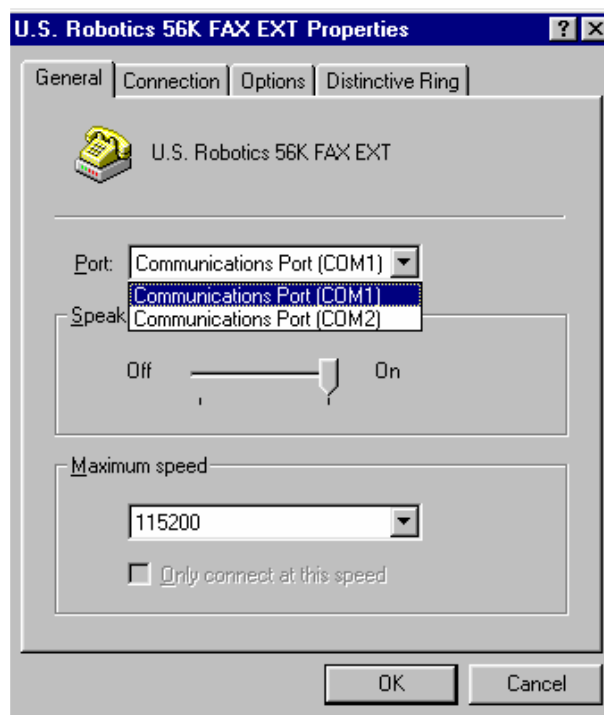


Double click on the Make New Connection icon to make a new connection.

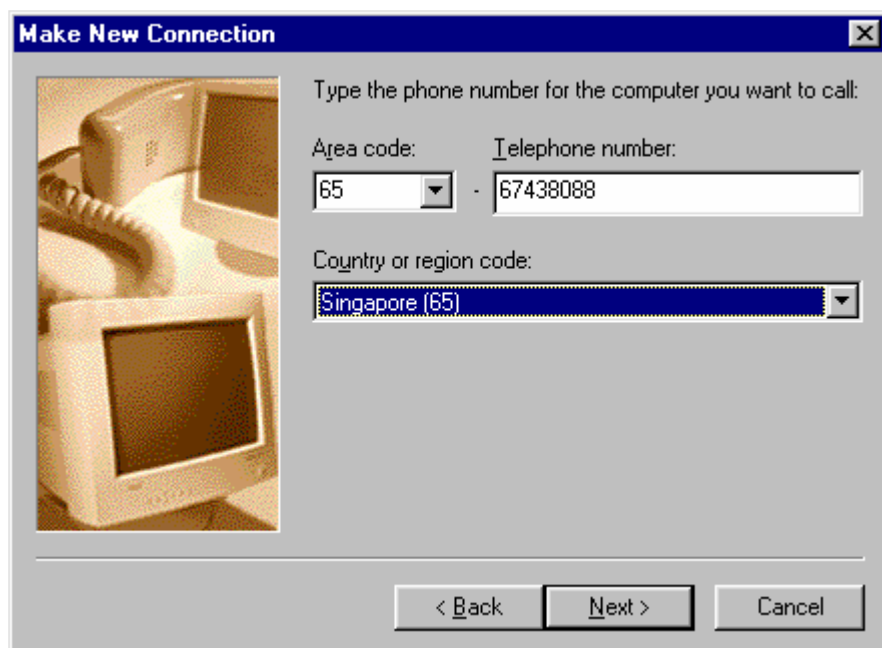
4. You will be led to a screen as shown below.



5. Follow the instructions on the screen. Make sure that a modem is connected to your PC. Select the appropriate modem by clicking on the Select a device drop down box.
6. Next, configure your modem by clicking on the configure button and entering the various configuration options as shown in the next screen shot.

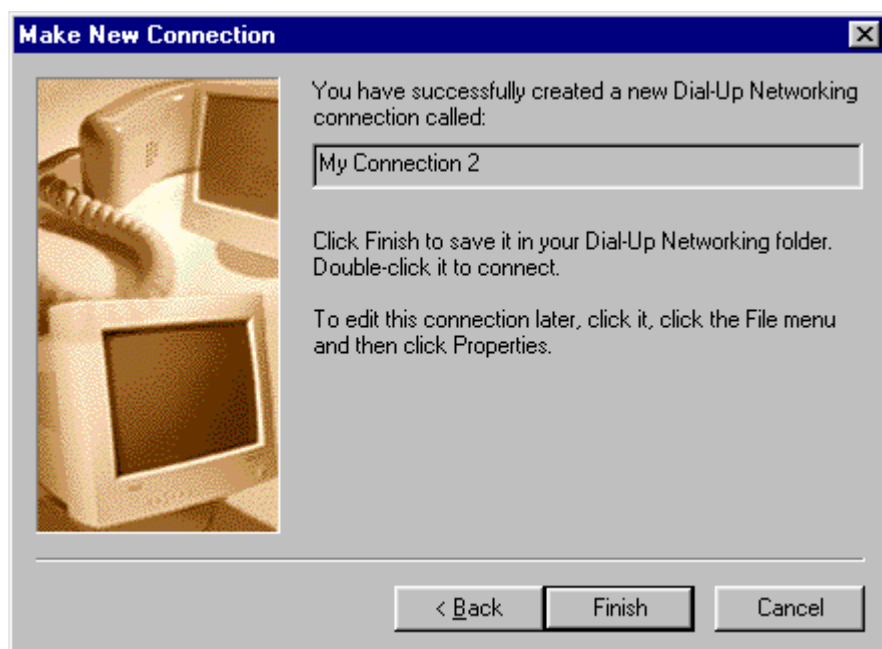


7. After configuring your modem, click on next and you will see a screen as shown in the next screen shot.



Enter the telephone number for the Access Easy Controller that you want to connect to and click on next.

8. You will see a screen as shown below.



Click on Finish to complete your connection.

9. After clicking on Finish you would have created a new connection named 'My Connection 2' as shown below

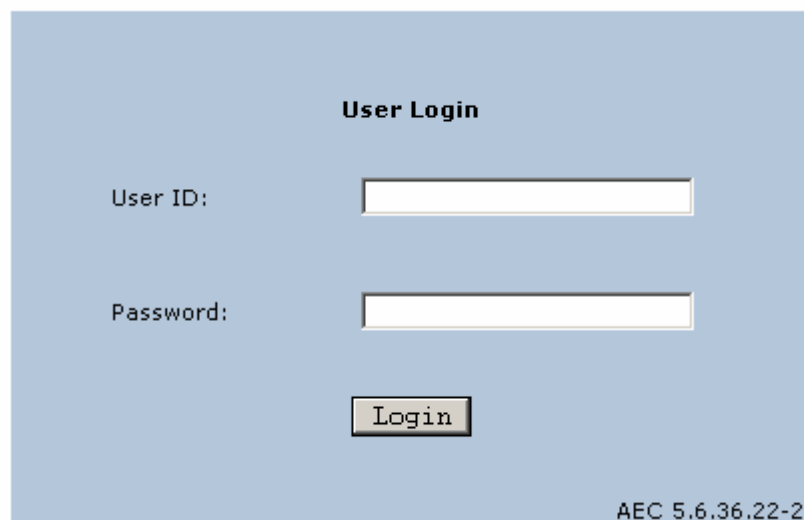


10. To Connect to the Access Easy Controller, double click on My Connection and you will be led to a screen as shown below.



In the User name and Password box, enter the **Dial-In** User name and Password of the Access Easy Controller which you want to connect to. In the phone number box, enter the phone number for the Access Easy Controller you want to connect to and then click on the Connect button.

11. After successfully connecting, you have to log on to the Access Easy Controller as shown in the screenshot below from the Web Browser application.
12. Enter the User ID and Password of the Access Easy Controller in the appropriate fields.

A screenshot of a web-based login interface. The background is a solid light blue. At the top center, the text "User Login" is displayed in a bold, black, sans-serif font. Below this, there are two rows of input fields. The first row is labeled "User ID:" on the left, followed by a white rectangular text box with a thin black border. The second row is labeled "Password:" on the left, followed by a similar white rectangular text box. Below these two rows, centered horizontally, is a button with a black border and the word "Login" in a black, sans-serif font. In the bottom right corner of the light blue area, the text "AEC 5.6.36.22-2" is visible in a small, black, sans-serif font.

User Login

User ID:

Password:

Login

AEC 5.6.36.22-2

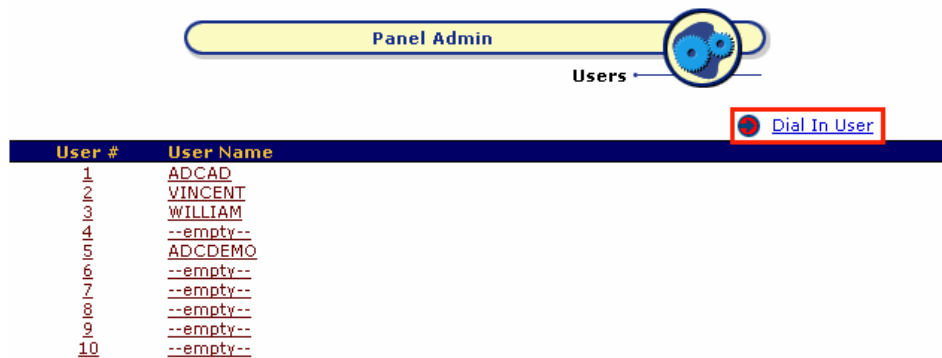
Note : Do **NOT** enter the Dial-In User Name and Password, it should be the normal login User ID and Password that you use to login the Access Easy Controller in a LAN environment.

13. After successful log in to the Access Easy Controller, you can now proceed with the normal operation as if you are in the office.

Setting up Macintosh for Dial-in

The above steps pertain to PC. For Mac OS, please follow the steps as explained.

1. Log on to Access Easy Controller. From any window of Access Easy Controller, click on users. You will see a screen that displays the users. On this screen, click on the dial-in user button as shown in the screen shot below.



2. Next you will come to a screen which displays the dial-in user name and password. Enter the User name and password in the appropriate boxes..

Dial In User

User Name:

Password:

Dial In Settings

Number of illegal password attempts:

Illegal attempts lockout duration: minutes (0 - 255)

IMPORTANT: CHANGE THE DEFAULT USER NAME AND PASSWORD AND SAVE THE NEW SETTINGS BY CLICKING ON SAVE BUTTON INDICATED BY FLOPPY ICON

3. The default user name and password has to be changed for security reasons. Enter the changed user name and password. You may also set the number of illegal password attempts and the illegal attempts lockout duration as shown in the screen.
4. The Number of illegal password attempts drop down box allows you to set the number of times the system will let you enter an illegal password before locking you out.
5. The Illegal attempts lockout duration box allows you to set the duration to disable the dial-in feature after a number of illegal password attempts as specified in step 3.



6. Next, click the save  button to confirm the changes and backup the Database now.
7. Make sure that a 56K modem is connected to your Access Easy Controller and is powered up. The modem must be connected to your telephone line to receive a dial-in request. Access Easy Controller will initialise the modem when it is re-booted.
8. Re-boot the Access Easy Controller.
9. Now your Access Easy Controller is ready to receive a dial-in request.

IMPORTANT: The modem has to be power up and connected to the Access Easy Controller before the Access Easy Controller reboots. Access Easy Controller will initialise the modem to auto answer mode .If initialising is not done, dial-in will not be successful

NOTE: Once initialised, the modem will always go into auto answer mode when power up.

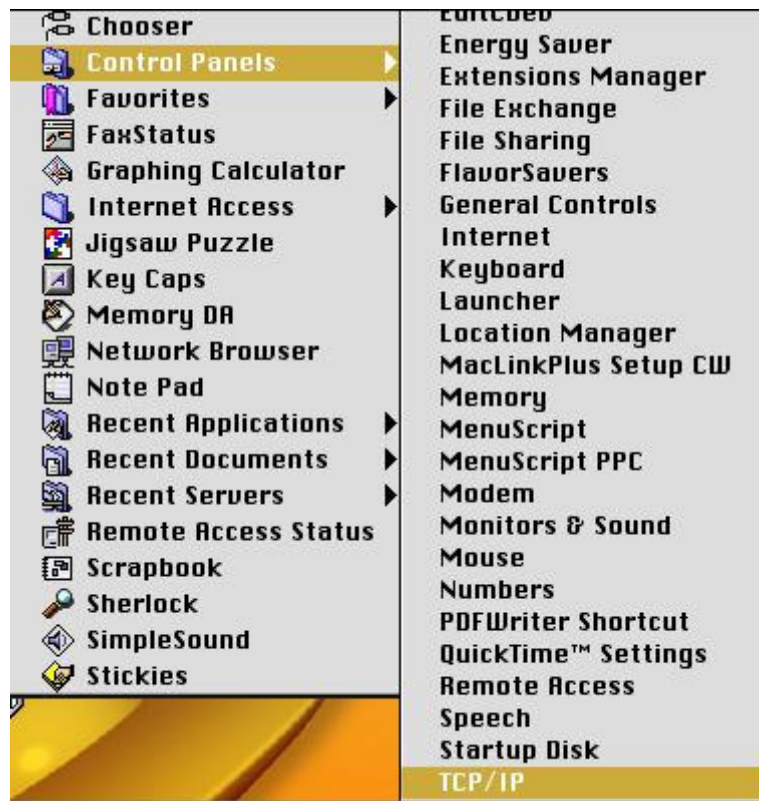
The following setup will guide you through the settings that are needed on your Mac in order to dial into the Access Easy Controller.

1. Firstly, you will need to change the IP address of your Mac which you intend to use to connect to Access Easy Controller via modem to a different network segment.

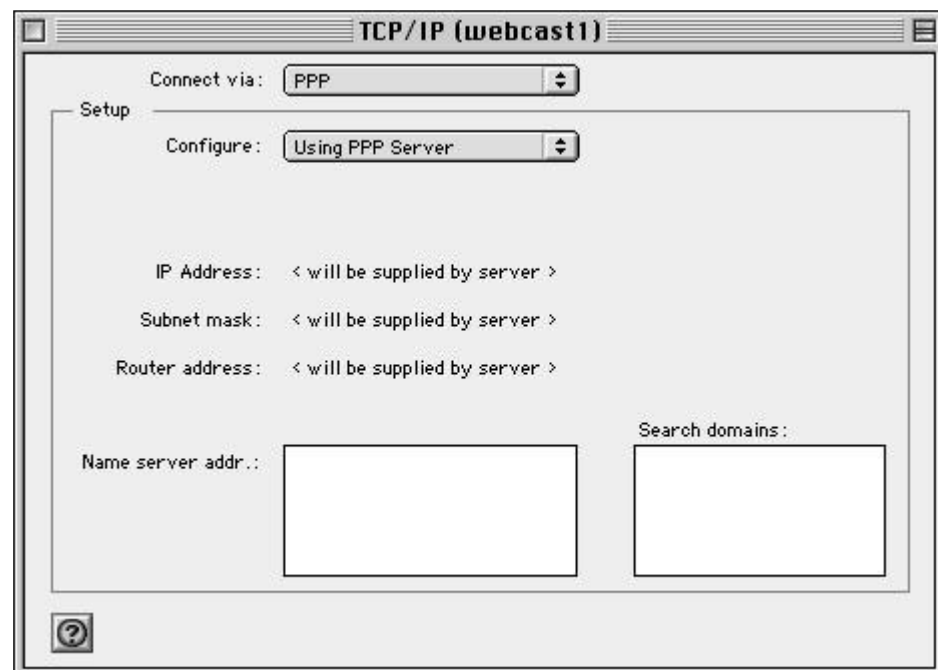
For example : the Access Easy Controller having a IP address of 129.2.0.41 and the subnetmask is **255.255.255.0**, the dial-in Mac could have any IP address but the subnetmask must not be **255.255.255.0**, it could be **255.255.0.0** or **255.0.0.0**

2. After changing the IP address of your dial-in Mac, remember to reboot the Mac before proceeding to the next step

3. Select Control Panels from the apple menu and from the Control Panels sub-menu select TCP/IP. Refer screenshot below.



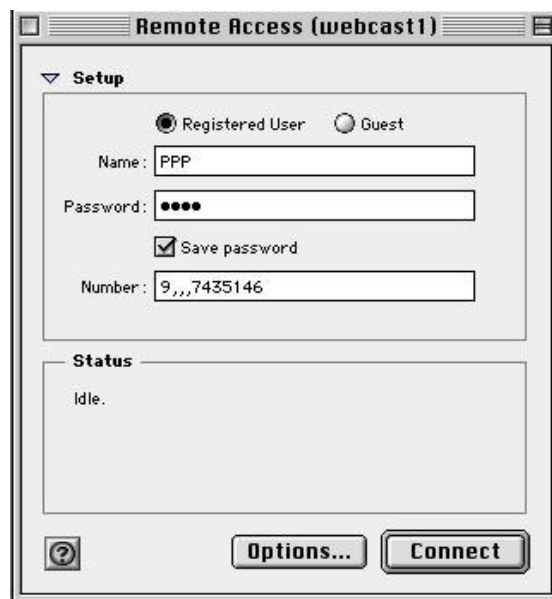
3. You will be led to a screen as shown below. Change the connection settings to PPP.



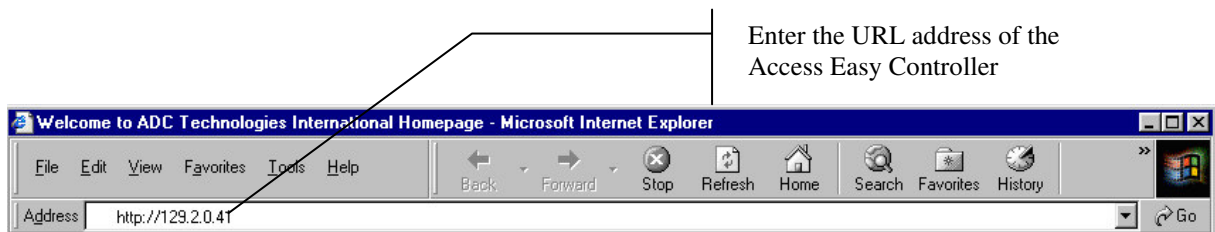
- Next, select Remote Access from the Control Panels sub-menu.



- You will be led to a screen as shown in the following. Enter the user name and password for the Access Easy Controller, which you want to connect to. Also enter the dial-in number in the Number box. Click on Connect button to remotely access the Access Easy Controller.



- After successfully connecting to Access Easy Controller remotely, you may log on to Access Easy Controller from any browser by supplying the IP address for the Access Easy Controller and the correct Access Easy Controller user name and password.



Note : Do **NOT** enter the Dial-In User Name and Password, it should be the normal login User ID and Password that you use to login the Access Easy Controller in a LAN environment.

7. After successful log in to the Access Easy Controller, you can now proceed with the normal operation as if you are in the office.

This Page Intentionally Left Blank

APPENDIX A

Initial Setup To Access Easy Controller

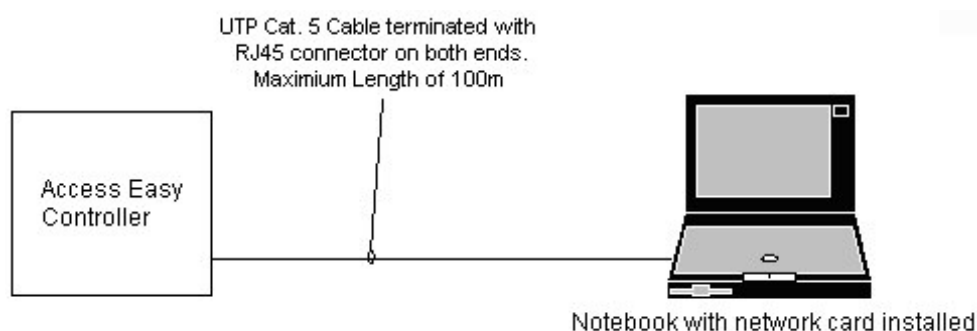
Before connection is made to Access Easy Controller, there are few conditions that must be taken into consideration. They are: -

1. If the *Central Monitoring Computer (CMC)* is not connected to a Network as in a stand-alone.
2. If the *CMC* is connected to a Network.

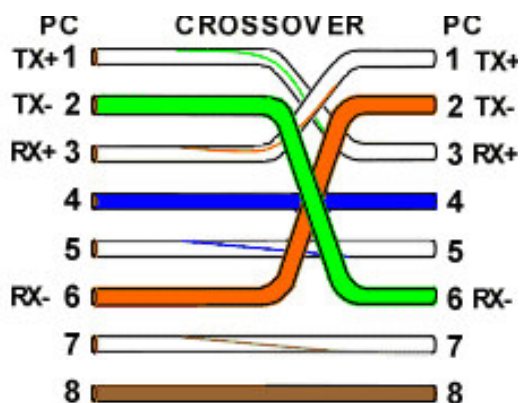
For case 1, having the CMC as a stand-alone unit, either IP Address for the Access Easy Controller or CMC can be changed to suit the other.

For an initial set-up, a Notebook or a Personal Computer either stand-alone or taken from an existing network have to be used. For either case, there must be a *10Base-T Ethernet card* installed and with a running web browser program such as *Internet Explorer, version 4.0 and above* or *Netscape Navigator, version 4.0 and above*.

Connect the Access Easy Controller server and Notebook using the industrial standard UTP Category 5 cable as shown below.



NOTE: The cable has to be terminated and polarised accordingly as shown.



The above drawing shows the *Transmit* (T_+ & T_-) and *Receive* (R_+ & R_-) lines between both end of the connectors being twisted. The wires for pins 4, 5, 7 and 8 are connected without twisting at both end of the connectors, but are not drawn above. The drawing below shows the full pin-to-pin connections with cable colour coding.

RJ45 Plug Pin (standard)	Cable Colour	RJ45 Plug Pin (twisted)
1	White/Orange	3
2	Orange	6
3	White/Green	1
4	Blue	4
5	White/Blue	5
6	Green	2
7	White/Brown	7
8	Brown	8

The individual conductors should be arranged as indicated above, taking reference to the pin numbers on the left (standard).

Procedure to set the IP Address of computer

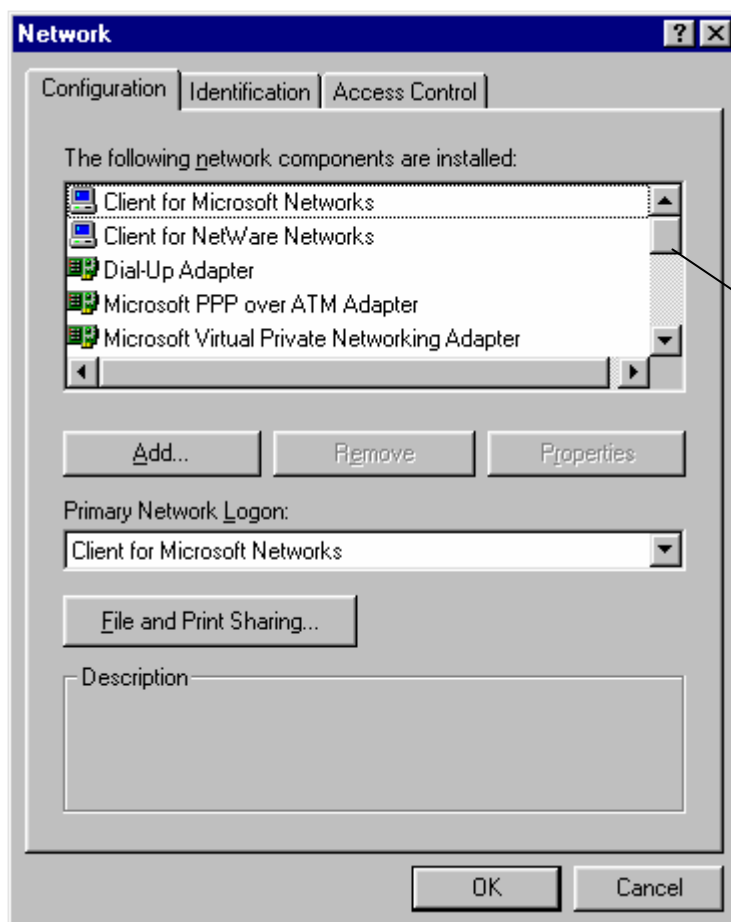
This section provides procedure to set the IP Address for the PC and Macintosh.

For PC Users

Follow through the procedures to set the IP Address of the PC.

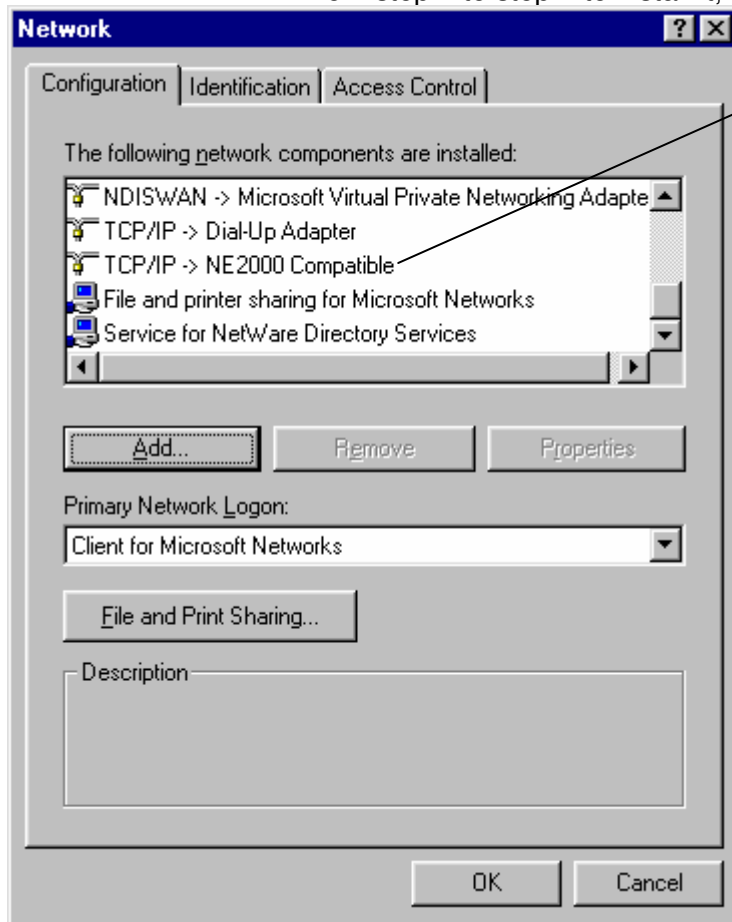
NOTE: The example described here is based on *Windows 98* and *Internet Explorer 5*. Differences might appear for the dialog box, displays, or description if other version or different operating system is used. However, the principle of setting is the same.

1. Click on the  button, followed by *Settings / Control Panel*.
2. Double-click on the  icon, the Network dialog box appears.



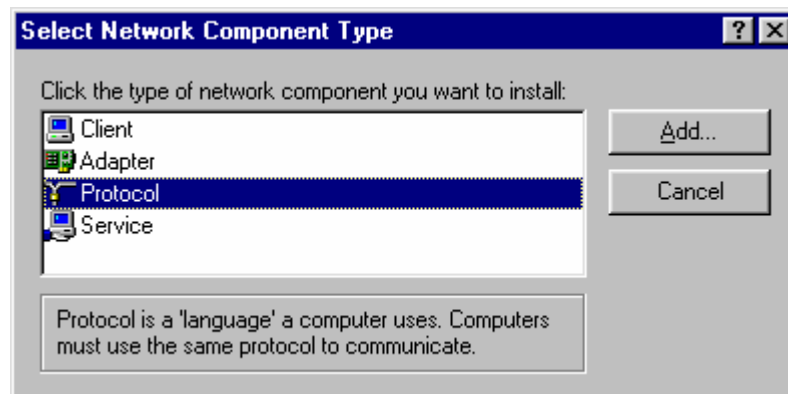
Use this scroll bar to view the installed network components.

3. Use the *Scroll Bar* to look up for *TCP/IP* from the list as shown in the following diagram. However if this component is not found, proceed from step 4 to step 7 to install it, else skip to step 8.

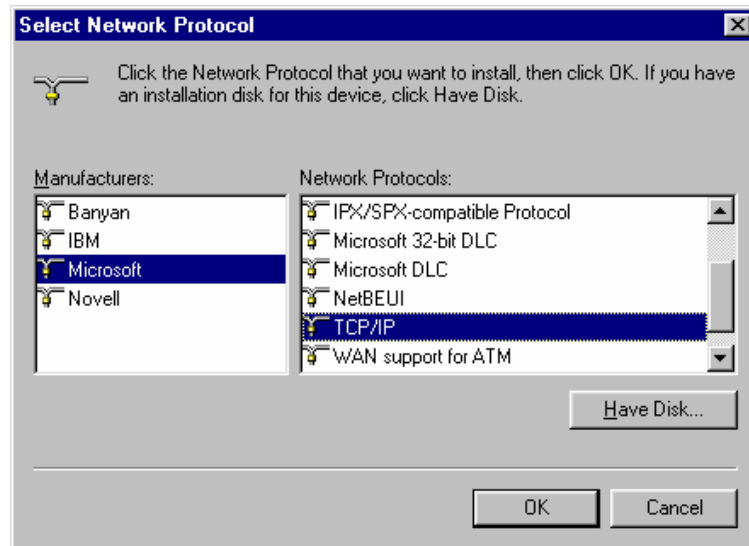


Look for component similar to this. If the installed Network Adapter has a "specified" description such as **32-Bits PCI Fast Ethernet Adapter [NDIS3]**, look for it instead. That is, **TCP/IP -> 32-Bits PCI Fast Ethernet Adapter [NDIS3]**.

4. To add the TCP/IP component, click on the **Add** button. The *Select Network Component Type* dialog box appears.



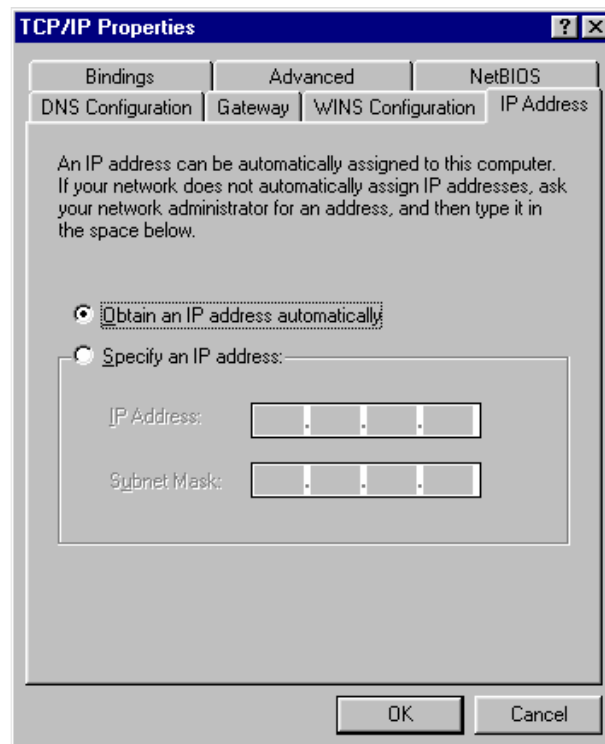
5. Click on component type *Protocol* and click on the **Add** button. The *Select Network Protocol* dialog box appears.
6. Click on *Microsoft* and *TCP/IP* as shown below.



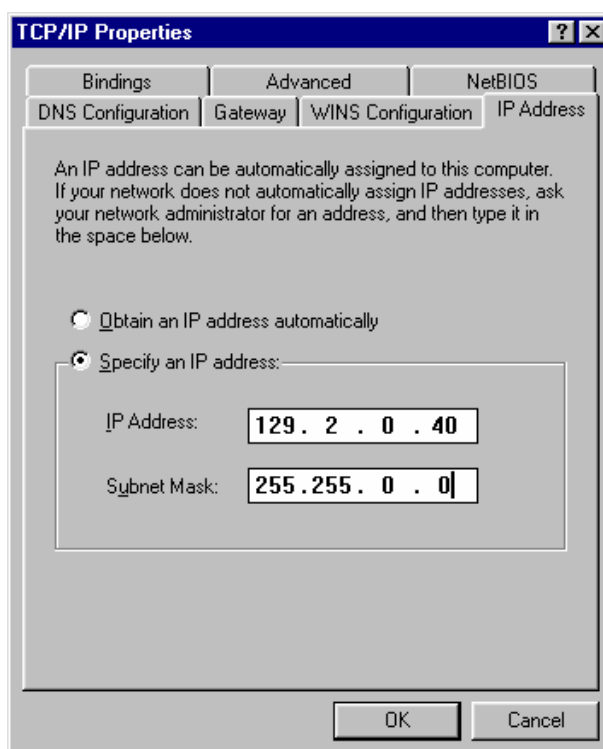
7. Click on the **OK** button to proceed with the component installation. Follow through the on-screen instruction to complete.

NOTE: You might be required to have your *Windows Installation Disk* in your CD ROM drive.

8. Continuing from step 3, click on the **Properties** button. The *TCP/IP Properties* dialog box appears.



9. Click on the *Specify an IP address* radio button. This will enable the field for *IP Address* and *Subnet Mask*.
10. Enter the *IP Address* and *Subnet Mask* as shown. This will be the PC's IP Address for this initial set-up.

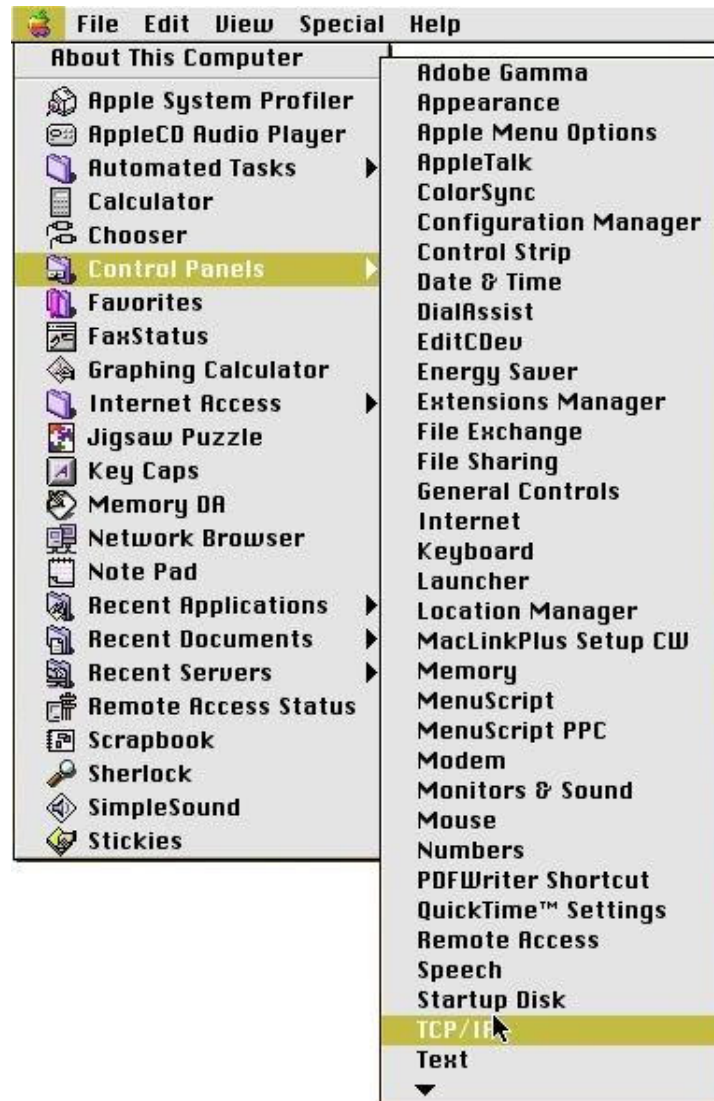


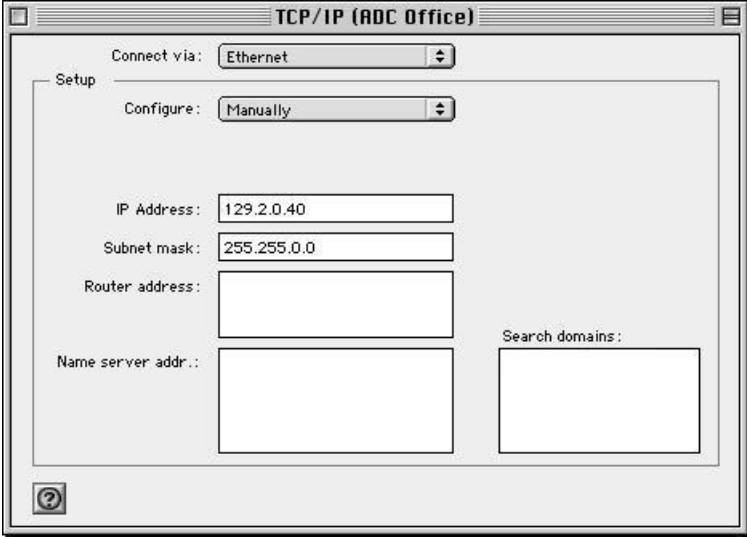
11. Click on **OK** button.
12. Reboot the computer in order for the setting to take effect.

For Macintosh Users

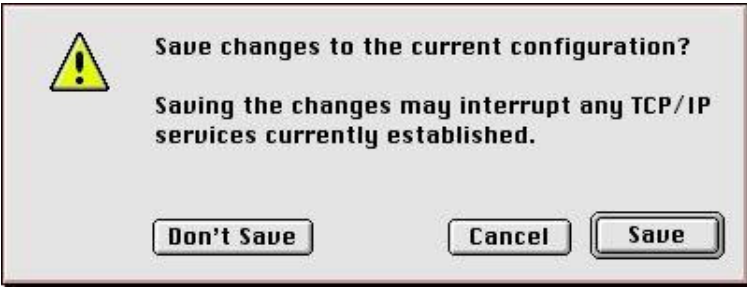
Follow through the procedures to set the IP Address for the Macintosh.

1. Click on the Apple icon to show a list of control function.
2. Select Control Panels, TCP/IP
The TCP/IP dialog box appears.



A screenshot of a Macintosh-style dialog box titled "TCP/IP (ADC Office)". It has a "Setup" section with two dropdown menus: "Connect via:" set to "Ethernet" and "Configure:" set to "Manually". Below these are four text input fields: "IP Address:" containing "129.2.0.40", "Subnet mask:" containing "255.255.0.0", "Router address:" which is empty, and "Name server addr.:" which is empty. To the right of the "Name server addr.:" field is a "Search domains:" text input field, also empty. A small question mark icon is in the bottom-left corner of the dialog box.

3. Enter the *IP Address* and the *Subnet mask* as shown above. This will be the Macintosh's IP Address for this initial set-up.
4. Click on the **Save** button when prompted.
This message will appear when you attempt to close the dialog box.

A screenshot of a warning dialog box with a yellow triangle icon containing an exclamation mark. The text inside reads: "Save changes to the current configuration?" followed by "Saving the changes may interrupt any TCP/IP services currently established." At the bottom, there are three buttons: "Don't Save", "Cancel", and "Save".

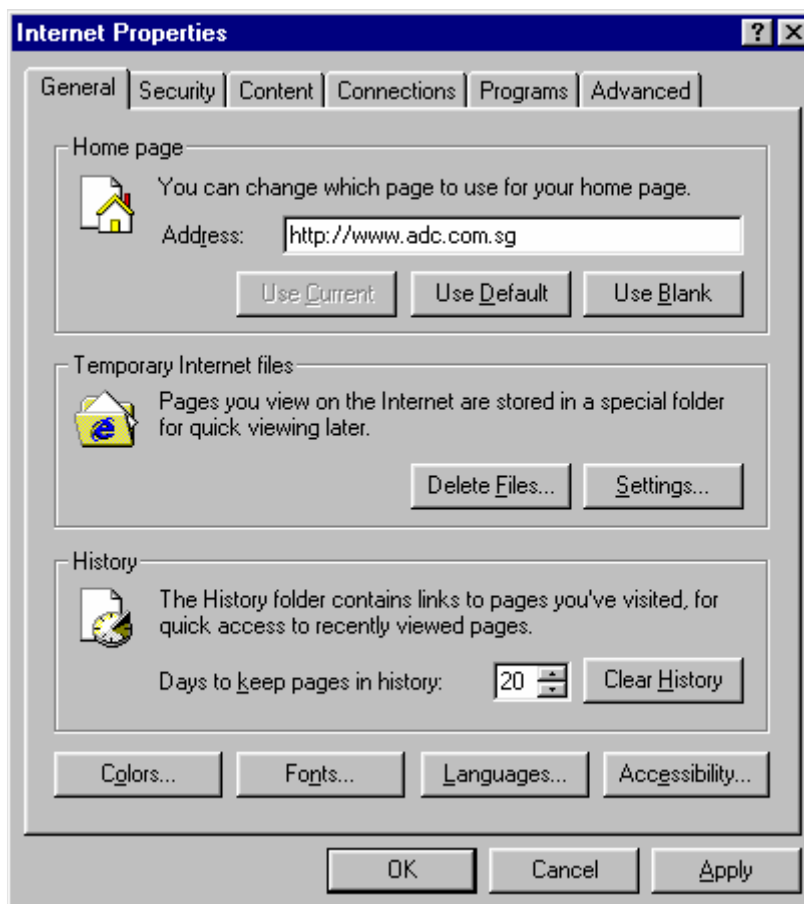
Setting to be made to the Web browser

For PC User

Follow the procedure to set up the Web browser options.



1. From the *Windows Control Panel*, click on the *Internet Options* icon. The Internet Options dialog box appears.



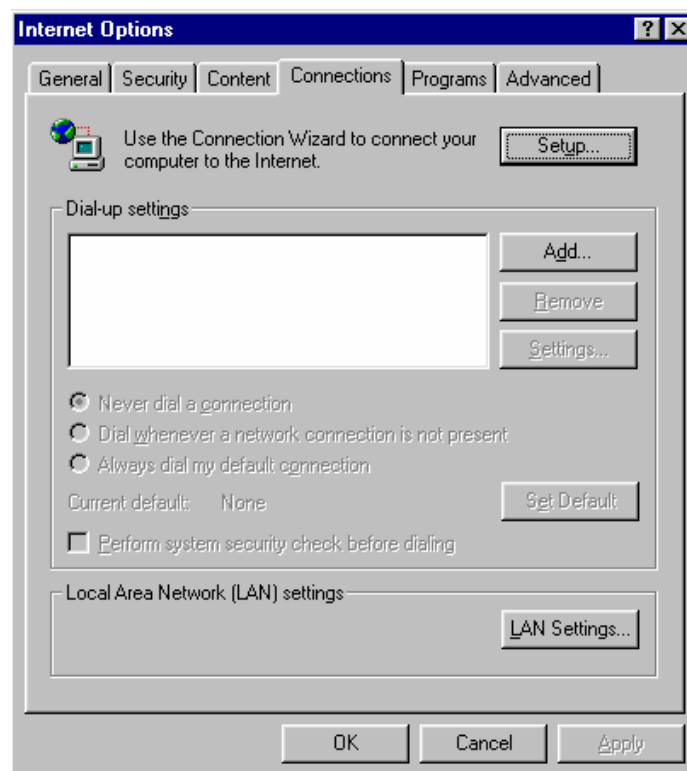
2. If you wish to show the Access Easy Controller *Login* page every time you activate your web browser program, then change the *Home page Address* to the Access Easy Controller *assigned* IP address (see NOTE) else, leave it as what was defined previously.

NOTE: The *Network Administrator* should assign the *IP Address* if the Access Easy Controller is to be connected to the Network.

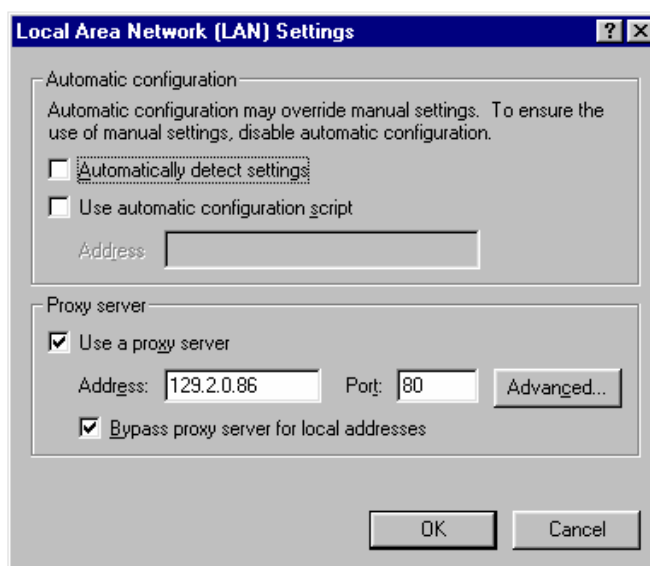
3. Under the *Temporary Internet files* heading, click on the **Settings** button to go into the next dialog box. Confirm that the *Check for newer versions of stored pages* is set to *Every visit to the page*, as shown in the following diagram. If it is not, click on the corresponding radio button.
This step is necessary in order for the view in View Activity to be updated periodically.



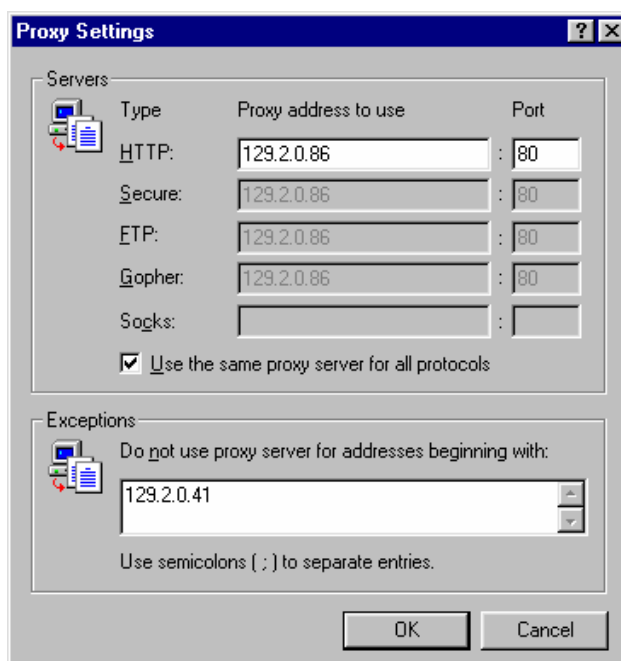
4. Click on the **OK** button to exit to previous dialog box.



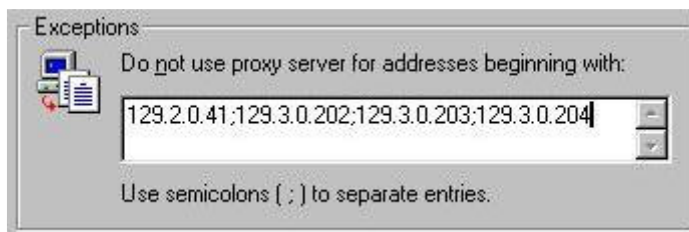
5. Under the **Connections** tab, click on the **LAN Settings** button. The *LAN Settings* dialog box appears.



6. Click on the **Advanced** button. The *Proxy Settings* dialog box appears.



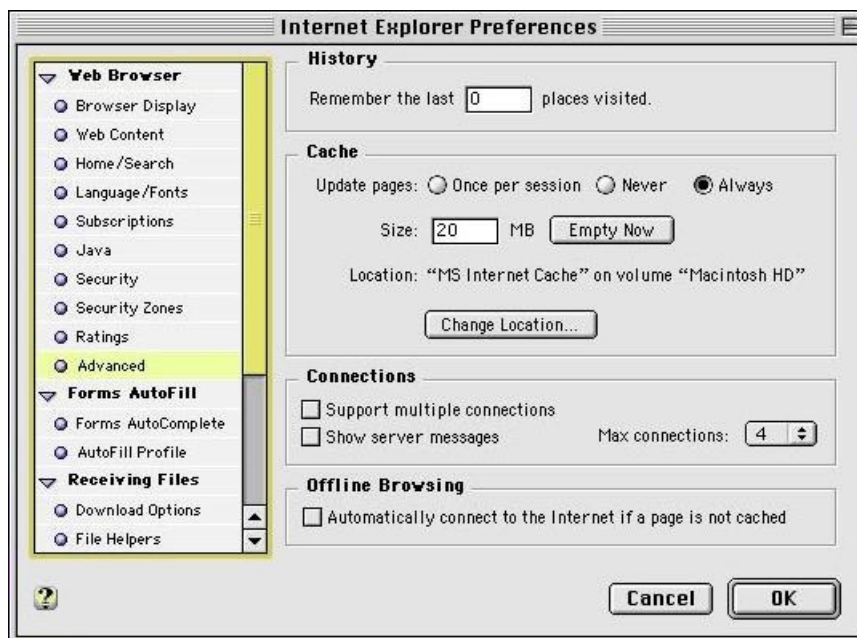
7. Enter the default *IP address* for the Access Easy Controller in the *Exceptions* edit field as shown above.
8. If the IP Address of the Access Easy Controller(s) has been assigned, continue to enter the address in the *Exceptions* edit field, separate each Address by a semicolon [;]. The next screen-capture shows the Default IP Address for Access Easy Controller and three assigned Access Easy Controller IP Addresses, 129.3.0.202, 129.3.0.203 and 129.3.0.204.



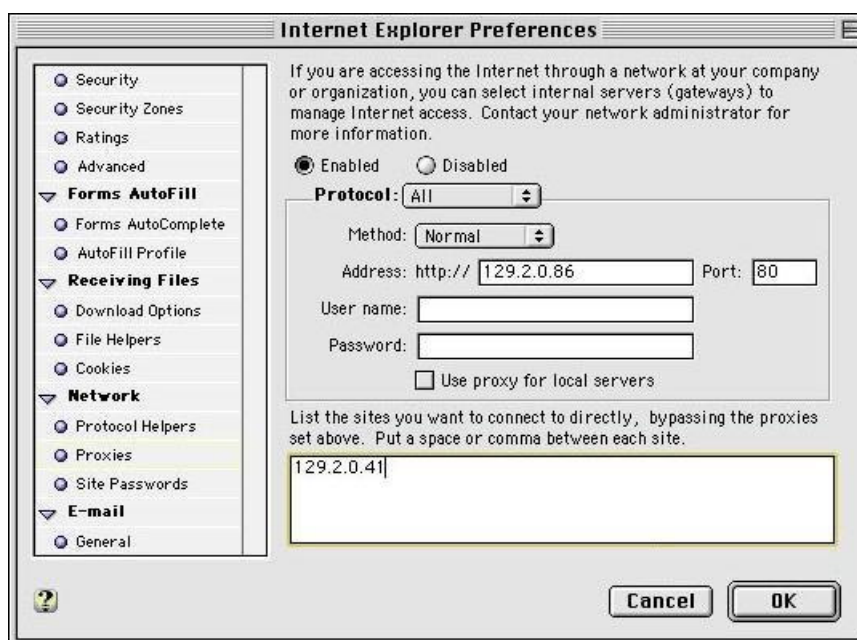
9. Click on the **OK** button repeatedly to exit the *Internet Options* setting.
10. Close the *Control Panel*.

For Macintosh Users

1. Launch the Internet Explorer for Macintosh.
2. From the Toolbars, click on **Preferences**.
3. Under **Web Browser**, select *Advanced* (see diagram below).
4. Select Update pages – Always for **Cache**.



5. Use the Scrollbar to scroll down the listing to look for *Proxies*.



6. Enter the Access Easy Controller default IP Address into the box as shown above. IP Addresses enter here will bypass the proxies and connect directly.

7. If the IP Address of the Access Easy Controller(s) has been assigned, continue to enter the address in the field, separate each Address by a space or a comma. The screen-capture shows the Default IP Address for Access Easy Controller and three assigned Access Easy Controller IP Addresses, 129.2.0.45, 129.2.0.44, and 129.3.0.80.

129.2.0.41 129.2.0.45 129.2.0.44 129.3.0.80

8. Click on the **OK** button to close the dialog box.

With this settings done, we can proceed to access the Access Easy Controller.

Now run the Web Browser program from Windows /Macintosh.
Enter the Access Easy Controller default URL address as shown.

NOTE: As the current configuration has no connection to the network or modem, accessing an Internet address is not possible. An error message will appear, a sample of which is shown below.



1. Press the **Enter** key or click on the  button. This should bring you to the Access Easy Controller *User Login* page.
2. Proceed with the *Login* (see the following NOTE).

NOTE: Please Login using **USER1** for the User ID. This is necessary, as the *Backup Database* function need to be used at a later stage.

3. From the *Home* page, click on the *Panel Admin, Panel Setup*. The *Network Settings* web page appears. Change the following setting to suit your network setting.
 - Panel's IP Address,
 - Panel's Netmask, and
 - Panel's Gateway.
 - Make changes also to the IP Address under *Remote PC Addresses*.

Please refer to the chapter on *Panel Setup* on how to make changes. Save the changes made on the Access Easy Controller setting (see REMINDER).

REMINDER: Remember to perform a *Backup Database* function so that the setting is written into the flash memory. Refer to the Chapter on *Database Backup, Backup Database* function for detail.

4. Reboot the Access Easy Controller.
5. Revert the computer to its original IP Address and Reboot the computer.
6. Connect the Access Easy Controller to the network (see NOTE) and power up. Proceed with the Login.

NOTE: If the Access Easy Controller is connected to the Central Monitoring Computer via a *Hub*, as in a Network configuration, the *UTP Cat. 5* cable connecting the Access Easy Controller Controller and the Hub must be polarised accordingly as shown on the following drawing.

RJ45 Plug Pin (standard)	Cable Colour	RJ45 Plug Pin (One-to-One)
1	White/Orange	1
2	Orange	2
3	White/Green	3
4	Blue	4
5	White/Blue	5
6	Green	6
7	White/Brown	7
8	Brown	8

Hook facing down

Hook facing down

Setting the Access Easy Controller IP Address Through Address Resolution Protocol (ARP)

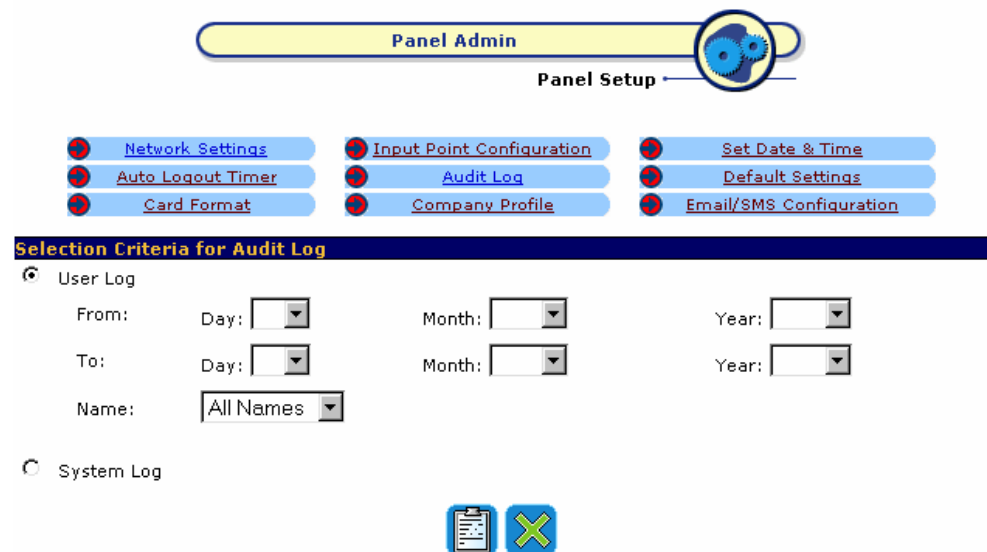
An address is a set of unique numbers by which you identify your PC or Access Easy Controller.

A mac address is the hardware address of the network device.

With the help of the arp command, the address of the Access Easy Controller can be customised according to your network. You need not know the previous address of your Access Easy Controller to use the arp command, but you will need to know the mac address of the Access Easy Controller. The mac address is listed in the System Audit log of the Access Easy Controller.

To find out the mac address, you will need to first log in to the Access Easy Controller and follows the steps as shown below :

Click on Panel Admin at the Home page of the Access Easy Controller .
Click on Panel Setup on the left panel menu selection.
Click on Audit Log to bring you to the page as shown in the following.



The screenshot displays the 'Panel Admin' section of the web interface. At the top, there is a yellow bar with 'Panel Admin' and a blue bar with 'Panel Setup'. Below these are several menu items: Network Settings, Input Point Configuration, Set Date & Time, Auto Logout Timer, Audit Log, Default Settings, Card Format, Company Profile, and Email/SMS Configuration. The 'Audit Log' menu item is highlighted. Below the menu items is a section titled 'Selection Criteria for Audit Log'. This section has two radio buttons: 'User Log' (selected) and 'System Log'. Under 'User Log', there are fields for 'From:' and 'To:' with dropdown menus for Day, Month, and Year. There is also a 'Name:' field with a dropdown menu set to 'All Names'. Below the 'System Log' radio button, there are two icons: a clipboard with a list and a green 'X' button.

Check the System Log radio button and click the list  button to shows the report.

The following shows the report generated, take note of the Hardware address, which is the mac address that we need.

[Selection Criteria for Audit Log](#)

Bosch Security Systems Pte Ltd
38C Jalan Peninpin Singapore 577180

System Log

Tuesday, 12 Nov 2002 11:43:42

Product Name	:	
Hardware Address (MAC)	:	00:04:5F:80:36:BC
Internet Address	:	129.2.0.200
Last Boot Time	:	Sat Nov 2 02:37:04 GMT 2002
Current Boot Time	:	Tue Nov 12 10:51:46 GMT 2002



No. of Converter/s Exist	:	1
Converter # 1	:	Reader Ports: 01,02,03,04
	:	Reader IO: 01-08

SIM serial number	:	7D2B051690D1
-------------------	---	--------------

[Selection Criteria for Audit Log](#)

With the mac address, we could now use arp to change the IP address of the Access Easy Controller, however, in order for Access Easy Controller to recognise the command, the following steps has to be taken first.

Initially connect a jumper to JP1 on the Secure/Comm Card and reboot the controller.

Remove the jumper after your Access Easy Controller has successfully rebooted.

From any of your remote PCs, issue the following commands from the command prompt

If you are using Windows NT or Windows 98

```
arp-s <new address you want to specify for your Access Easy Controller >
<mac address of your Access Easy Controller>
ping <new address you have just set> to check connectivity to the Access
Easy Controller.
```

for example : if you want to change the address of your Access Easy Controller to 129.3.0.99 and the mac address of your Access Easy Controller is 52-54-4c-0-0-2c, the command will be :

```
arp -s 129.3.0.99 52-54-4c-0-0-2c
ping 129.3.0.99
```

If you are using Windows 95

arp-s <new address you want to specify for your Access Easy Controller >
<mac address of your Access Easy Controller > <address of your PC>
ping <new address you have just set>
for example : if you want to change the address of your Access Easy Controller to 129.3.0.99 and the mac address of your Access Easy Controller is 52-54-4c-0-0-2c and the address of your PC is 129.3.0.77, the command will be :

```
arp -s 129.3.0.99 52-54-4c-0-0-2c 129.3.0.77  
ping 129.3.0.99
```

If you are using Unix/Linux and OS/2

arp-s <new address you want to specify for your Access Easy Controller >
<mac address of your Access Easy Controller > temp
ping <new address you have just set>

for ex: if you want to change the address of your Access Easy Controller to 129.3.0.99 and the mac address of your Access Easy Controller is 52-54-4c-0-0-2c , the command will be :

```
arp -s 129.3.0.99 52-54-4c-0-0-2c temp  
ping 129.3.0.99
```

After you have issue the ping command to the Access Easy Controller, it should reboot. After it has rebooted, it will resume operation using the new IP address that you have set.

APPENDIX B

Activity Transactions

This appendix list the various Activity transactions found within each category.

Alarm Activity

No	Transactions
1	Access Denied
2	Invalid Schedule
3	Invalid Start Date
4	Invalid End Date
5	Duress
6	Access Denied - Wrong PIN
7	Access Denied – Passback
8	Access Denied – Timed APB
9	Exit Denied – Passback
10	Invalid Card
11	Door Forced Opened
12	Door Held Open
13	Panel Tamper
14	Panel AC Failure
15	Alarm

Restore Activity

No	Transactions
1	Door Closed
2	Tamper Restored
3	Alarm Restored
4	Power Restored

Valid Activity

No	Transactions
1	Access Granted
2	Exit Granted
3	Access Granted, Soft APB
4	Exit Granted, Soft APB
5	PIN Changed
6	Disarmed
7	Armed
8	Turn On
9	Turn Off
10	Door Locked
11	Door Unlocked
12	Door Locked By Schedule
13	Door Unlocked By Schedule
14	Door Momentarily Unlocked
15	Door Access Enabled
16	Door Access Disabled
17	Armed By Schedule
18	Disarmed By Schedule
19	Bypassed
20	Turned Off By Schedule
21	Turned On By Schedule
22	Duration Off
23	Duration On

Time Attendance

No	Transactions
1	Clock In
2	Clock Out

APPENDIX C

Email/SMS Configuration Table

This Appendix provides information on how to select the appropriate item options with reference to the Events list. For each Event, an “X” indicates the possible selection that can be made under the Devices and Cardholders column.

For example, in order for Access Easy Controller to send an Email or SMS when an “Alarm” or “Alarm Restored” occurs on Input 1. The following must be set :

Devices :

“Selected Device Only option” and choose only Input 1.

Events :

“Selected events only” option and choose “Alarm” and “Alarm Restored”

Cardholders

“All Cardholders”

For this scenario, never choose “Selected Cardholders only” for Cardholders settings or “Selected Readers” or “All Readers” for Devices setting, these settings will result in not receiving any events that will meet the criteria. Cause the events for “Alarm” and “Alarm Restored” will never comes with a cardholder’s ID and it will never happens on a reader.

	Devices							Cardholders	
	All Readers, Inputs and Output Point	All Readers	Selected/Omit Readers	All Input Points	Selected/Omit Input Points	All Output Points	Selected/Omit Output Points	All Cardholders	Selected/Omit Cardholders
Events									
Panel Tamper	X	X	X	X	X	X	X	X	
Tamper Restored	X	X	X	X	X	X	X	X	
Panel AC Failure	X	X	X	X	X	X	X	X	
Power Restored	X	X	X	X	X	X	X	X	
Alarm	X			X	X			X	
Alarm Restored	X			X	X			X	
Door Forced Open	X	X	X					X	
Door Held Open	X	X	X					X	
Door Closed	X	X	X					X	
Duress	X	X	X					X	X
Access Denied	X	X	X					X	X
Access Denied – Passback	X	X	X					X	X
Exit Denied – Passback	X	X	X					X	X
Access Denied – Timed APB	X	X	X					X	X
Access Denied – Wrong PIN	X	X	X					X	X
Invalid Schedule	X	X	X					X	X
Invalid Card	X	X	X					X	
Invalid start Date	X	X	X					X	X
Invalid End Date	X	X	X					X	X
Armed	X	X	X	X	X			X	X
Disarmed	X	X	X	X	X			X	X
Armed By schedule	X			X	X			X	
Disarmed By Schedule	X			X	X			X	
Bypassed	X			X	X			X	
Access Granted	X	X	X					X	X
Exit Granted	X	X	X					X	X
Access Granted – Soft APB	X	X	X					X	X
Exit Granted – Soft APB	X	X	X					X	X
PIN Changed	X	X	X					X	X
Door Access Enabled	X	X	X					X	
Door Access Disabled	X	X	X					X	
Door Locked	X	X	X					X	
Door Unlocked	X	X	X					X	
Door Momentarily Unlocked	X	X	X					X	
Door Locked By Schedule	X	X	X					X	
Door Unlocked By Schedule	X	X	X					X	
Turned On	X					X	X	X	
Turned Off	X					X	X	X	
Duration On	X					X	X	X	
Duration Off	X					X	X	X	
Turned On By Schedule	X					X	X	X	
Turned Off By Schedule	X					X	X	X	
Clock In	X	X	X					X	X
Clock Out	X	X	X					X	X

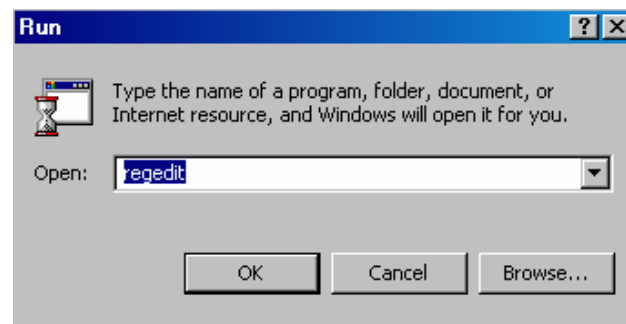
APPENDIX D

Setting up a Timeserver (Windows 2000 and XP Professional)

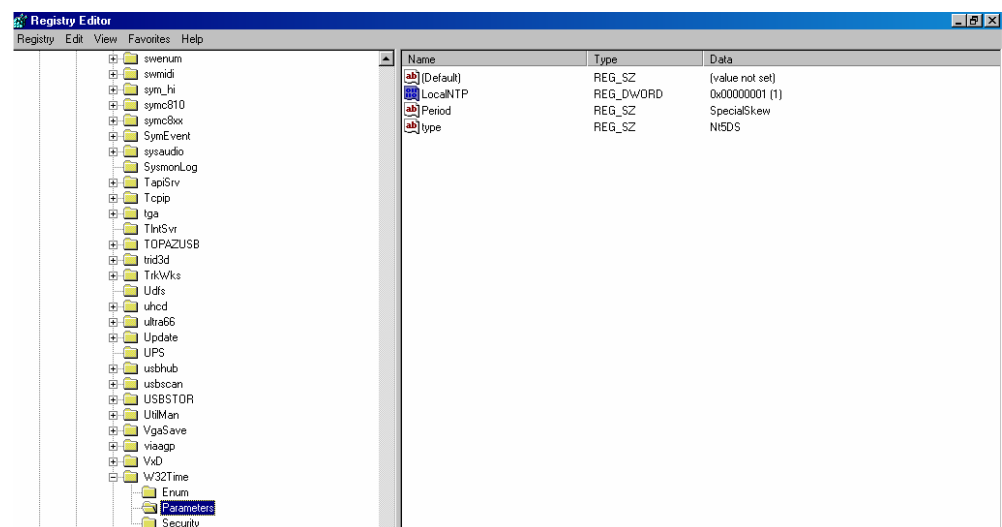
This Appendix provides information on how to set up a timeserver on windows 2000, XP Pro PC. The following section uses Windows 2000 and XP Pro to illustrate how the timeserver is set up.

For Windows 2000

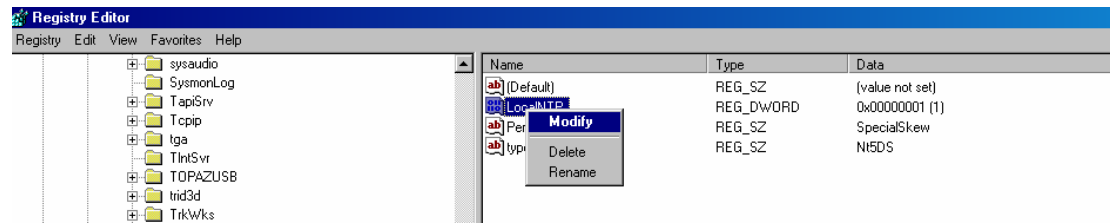
1. Click  *Start* button and select *Run* button.
2. Type *regedit* in the window.



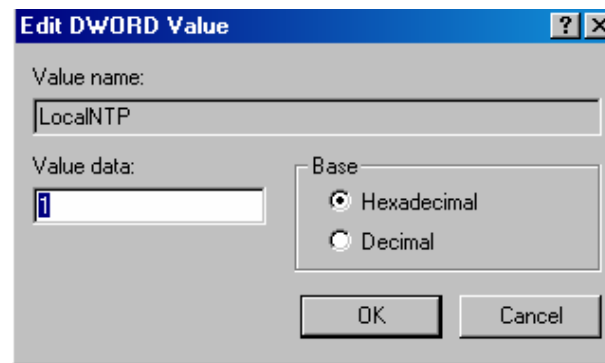
3. Select
HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/PARAMETERS.



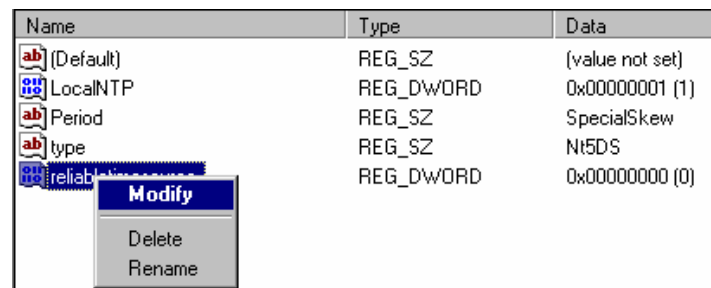
4. Right click *LocalNTP* and select *Modify*.



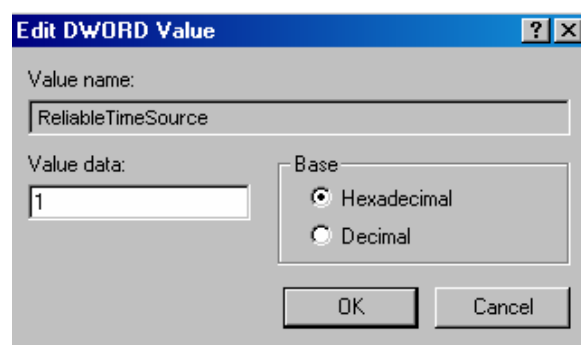
5. Enter 1 for *Value data* and click *OK*.



6. Right click *ReliableTimeSource* and select *Modify*.



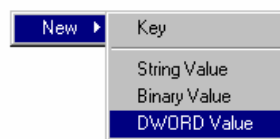
7. Enter 1 for *Value data* and click *OK*.



Note: If HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/PARAMETERS doesn't contain the ReliableTimeSource settings; user will have to create one. Follow steps 8- 9 otherwise proceed to step 10

8. Right click on a empty space in the right panel and select *New/DWORD Value*.

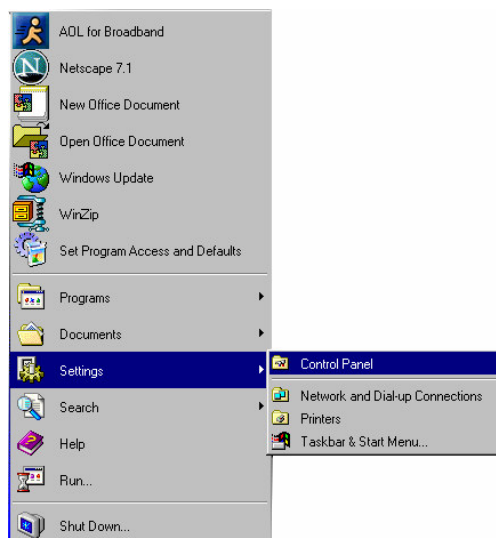
Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Period	REG_SZ	SpecialSkew
type	REG_SZ	Nt5DS
	REG_DWORD	0x00000001 (1)

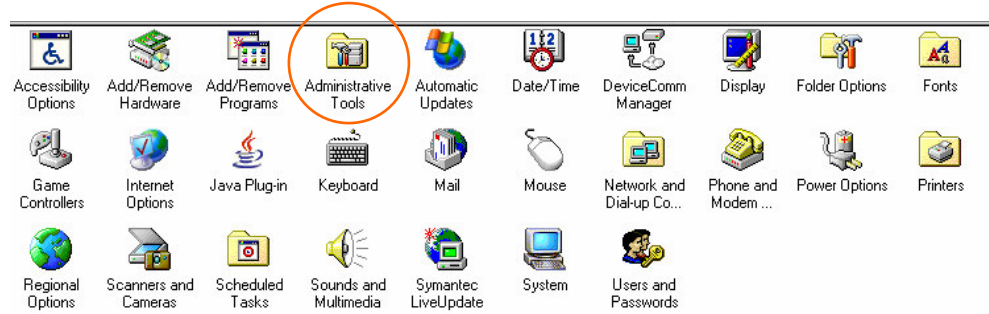
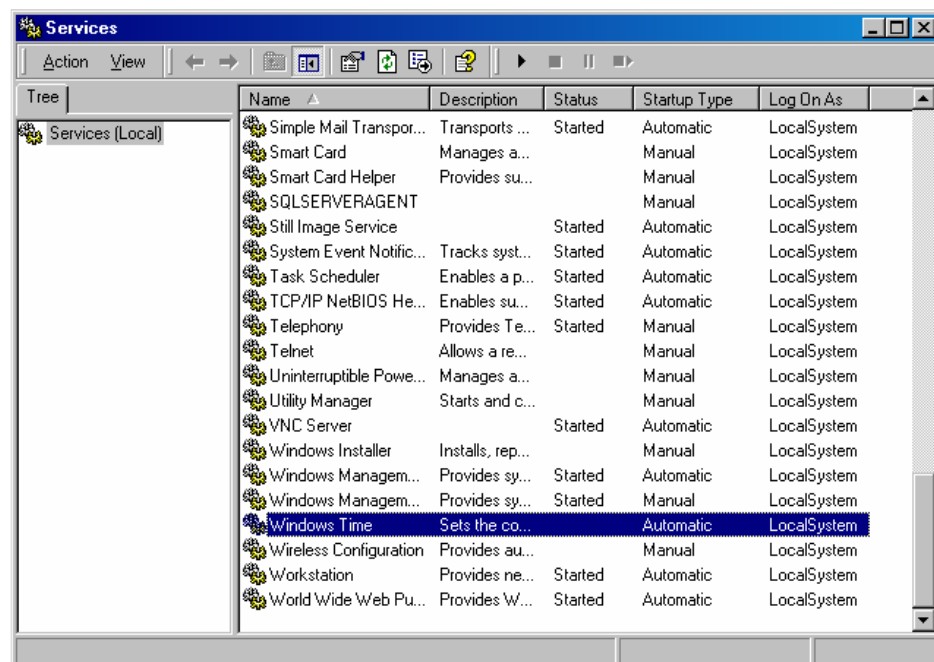


9. Key in ReliableTimeSource

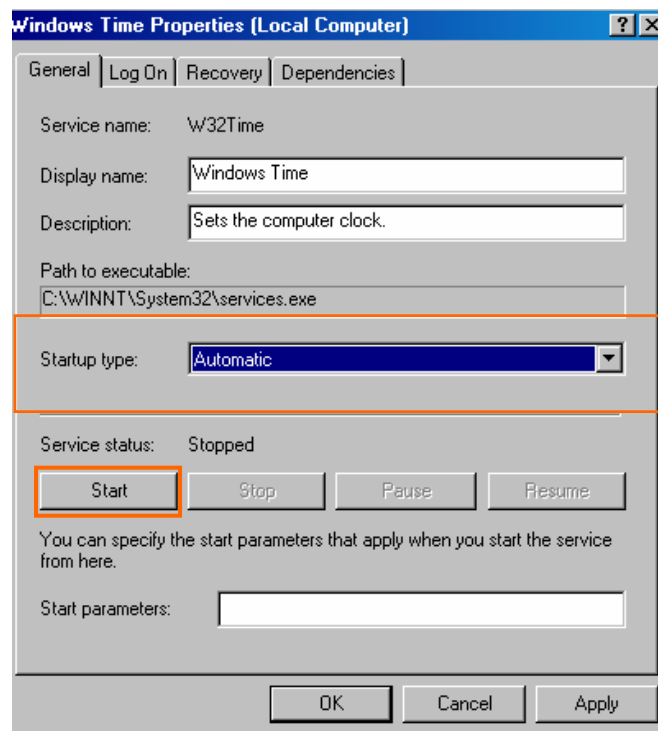
Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Period	REG_SZ	SpecialSkew
type	REG_SZ	Nt5DS
ReliableTimeSource	REG_DWORD	0x00000000 (0)

10. Click  *Start* button and select Settings/Control Panel.

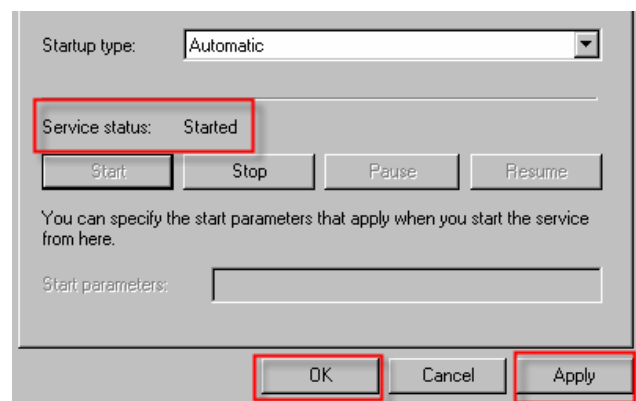


11. Double click on *Administrative Tools* icon12. Double click on *Services* icon.13. Scroll down to *Windows Time* and double click it.

14. Select *Automatic* from the *Startup Type* drop down list and click *Start*.



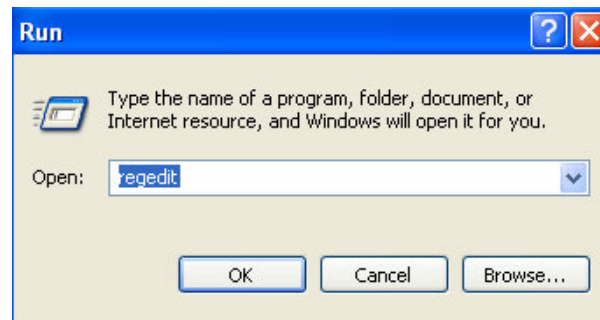
15. Once service status is started, click *Apply* and *OK* to exit.



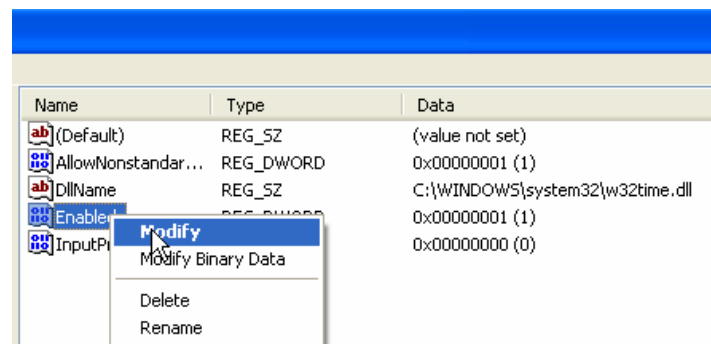
16. Reboot PC.

For Windows XP Professional

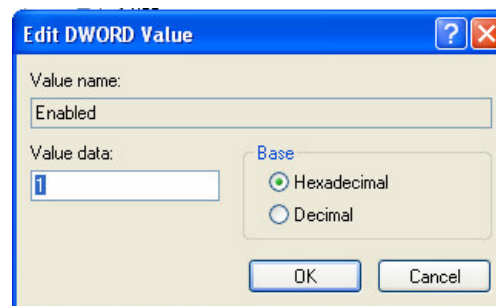
1. Click  *Start* button and select *Run* button.
2. Type *regedit* in the window



3. Select
HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/TIMEPROVIDERS/NTPSERVER.
4. Right click *Enabled* and select *Modify*.



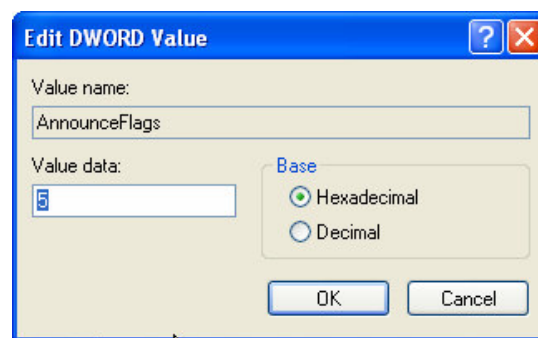
5. Enter 1 for *Value data* and click *OK*.



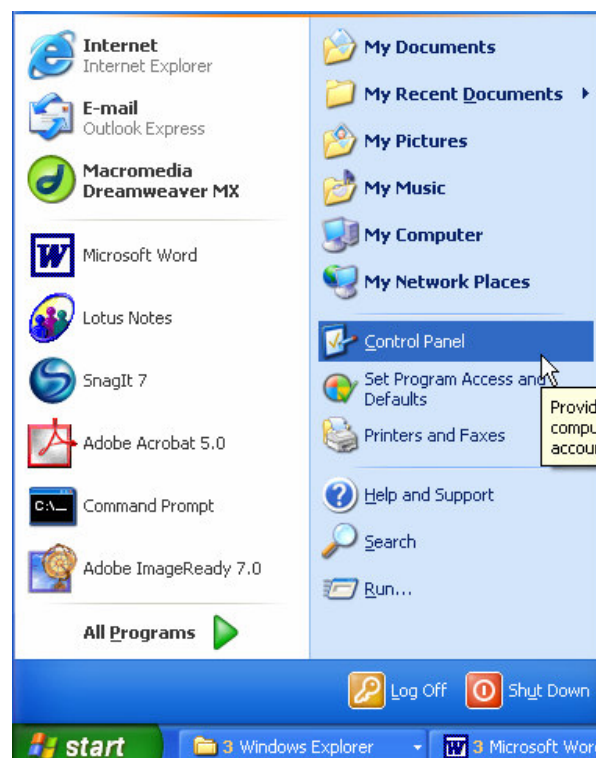
6. Select
HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/CONFIG
7. Right click *AnnounceFlags* and select *Modify*.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AnnounceF	Modify	0x00000005 (5)
EventLogFl	Modify Binary Data	0x00000002 (2)
FrequencyC		0x00000004 (4)
HoldPeriod	Delete	0x00000005 (5)
LargePhase	Rename	0x00138800 (1280000)

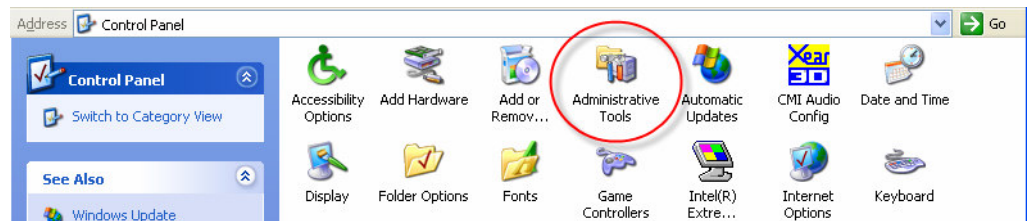
8. Enter 5 for *Value data* and click *OK*.



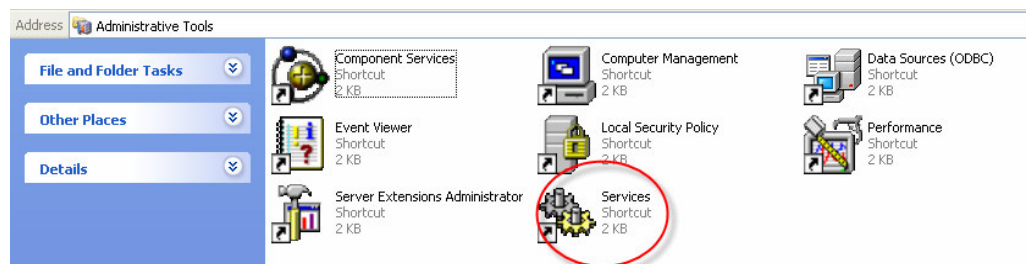
9. Click  button and select *Control Panel*.



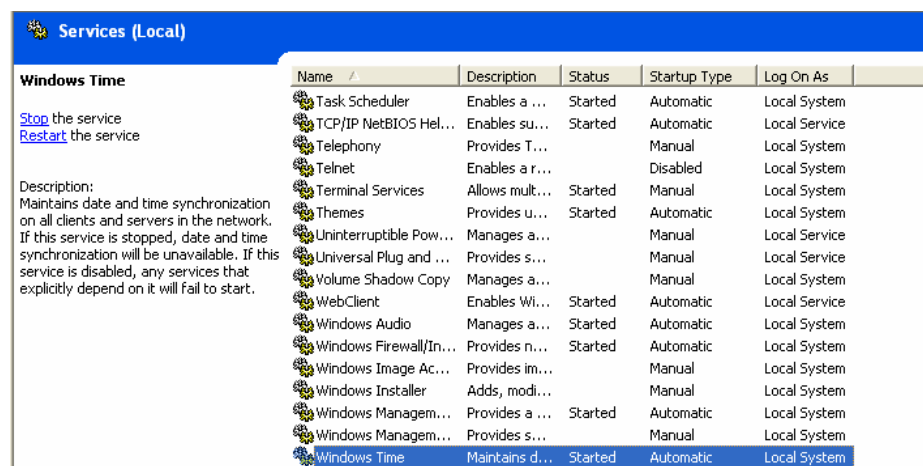
10. Double click on *Administrative Tools* icon.



11. Double click on *Services* icon.



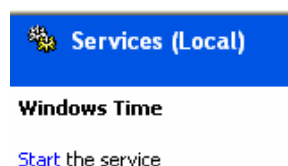
12. Scroll down to *Windows Time*.



13. Select *Stop the service*.



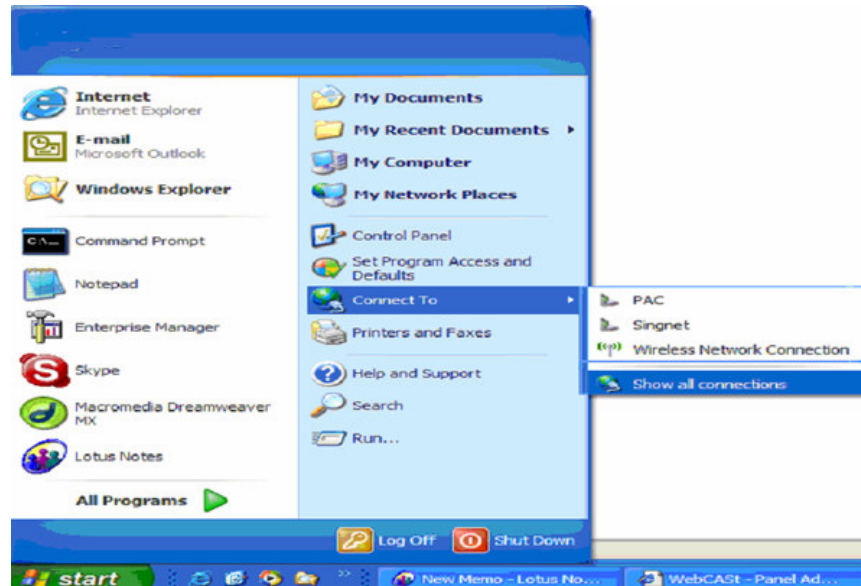
14. Once service is stop, click *Start the service*.



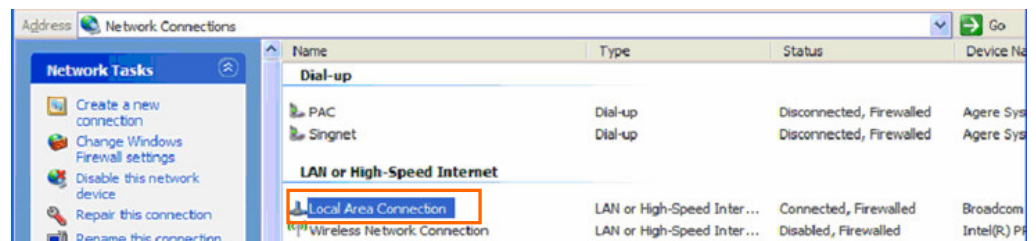
15. *Reboot PC.*

Note: If user is using windows XP professional with service pack 2 for the timeserver, user has to bypass the firewall protection. Follow steps 1 - 9

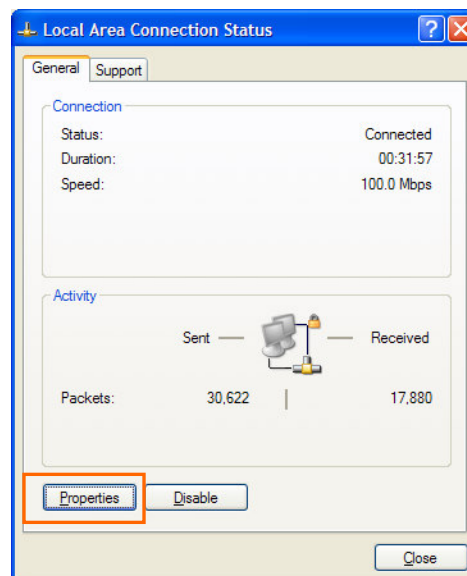
1. From the desktop, select *Start* and look for *Connect To* and select *show all connections*.

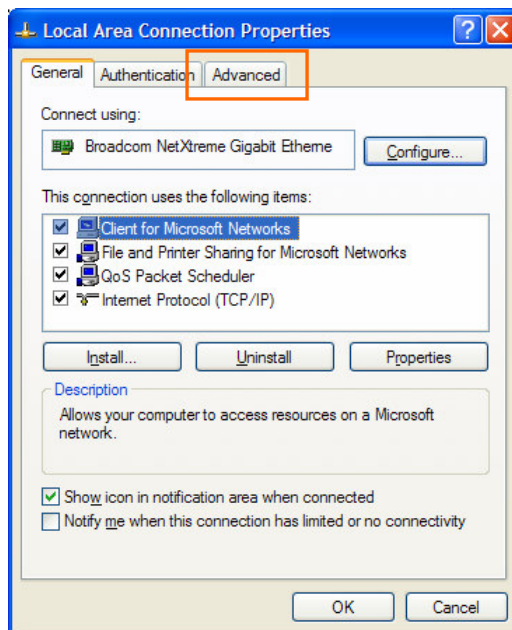
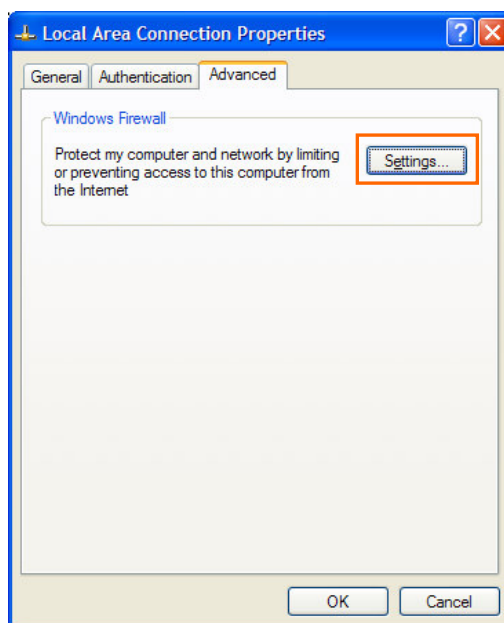


2. Click on the *Local Area Connection*.

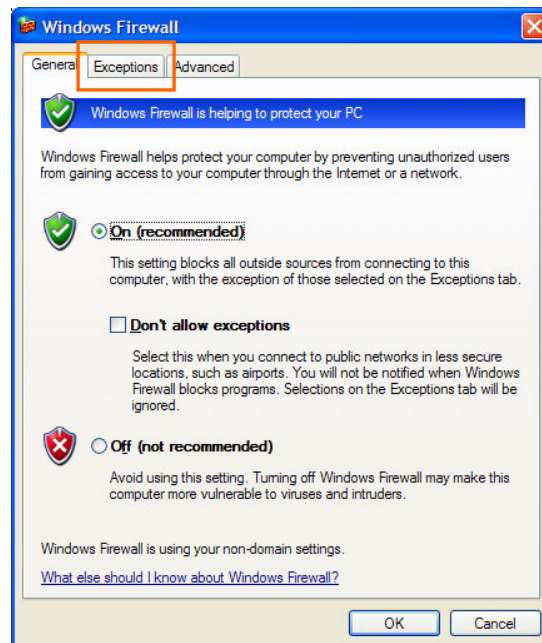


3. The following screen will appear, click on *properties*.

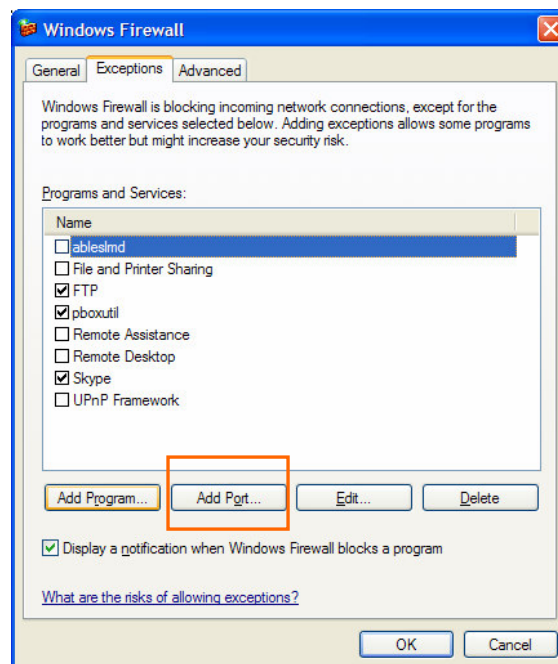


4. Click on *Advanced*.5. Click on *Settings*.

6. The below screen will appear, click on *Exceptions*.



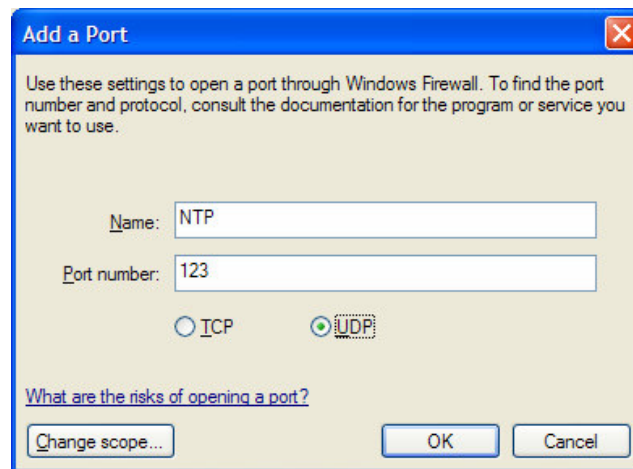
7. Click on the *Add port*.



8. Enter the following data.

Name: NTP

Port number: 123



9. Click *OK* to save the settings

APPENDIX E

Blank Configuration Forms

The next following pages provide some blank configuration forms which user can use to plan the various parameter settings before doing the actual configuration on the Access Easy Controller software.

User can either make photocopies of the forms from this user manual or create similar forms using any of the available software application such as Microsoft Words® or Microsoft Excel®.

Access Grouping

Page ____ of ____

Access Group # (1,2, etc..) : _____

Description (R&D Dept, Management, etc...): _____

Rdr #	Description / Location (Max 30 characters)	Schedule
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

NOTE:

The stated Schedule here refers to the periods where the Cardholders are allowed access to the Doors.

Prepared by : _____

Dated : _____

Door Parameters

Page ____ of ____

Reader # (to be fill up by ADC)	Description (e.g. "Podium Level 1 Main Door") (max. 30 characters)	Reader Schedule		PIN Schedule		Common PIN	APB Mode	
		#	Holiday	#	Holiday		N/S/T/F	TO
1			☐		☐			
2			☐		☐			
3			☐		☐			
4			☐		☐			
5			☐		☐			
6			☐		☐			
7			☐		☐			
8			☐		☐			
9			☐		☐			
10			☐		☐			
11			☐		☐			
12			☐		☐			
13			☐		☐			
14			☐		☐			
15			☐		☐			
16			☐		☐			

APB Mode: N No Anti-Passback
 T Time Based Anti-Passback Mode
 S Soft Anti-Passback Mode
 F Full Anti-Passback Mode
 TO: Timer setting for Time Based APB

Common PIN : Reader Common PIN
 # : "NIL" means door on AutoDoor Unlock mode / no PIN required
 "24hr" means door on card access mode for 24hr/day / PIN required for 24hrs
 Any other number means door operates based on the Schedule specified

Note : 1. Reader Schedule here refers to the periods where the door will be unlocked for free access, refer to the AutoDoor Unlock Schedule configuration.
 2. PIN Schedule here refers to the period where the User does not require to enter the PIN for access, refer to the PIN Deactivation Schedule configuration.
 3. Check the Holiday column if the reader access mode is different during holiday.

Prepared by : _____

Dated : _____

BOSCH SECURITY SYSTEMS

AutoDoor Unlock Schedule Configuration

Page ____ of ____

Each day is configurable up to 4 intervals, each interval consists of a Start-End time. Do not overlap the intervals, such that the next Start time is not earlier than the previous End time (maximum of 30 characters for Description field).

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Prepared by : _____

Dated : _____

Card Access Schedule Configuration

Page ____ of ____

Each day is configurable up to 4 intervals, each interval consists of a Start-End time. Do not overlap the intervals, such that the next Start time is not earlier than the previous End time (maximum of 30 characters for Description field).

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Prepared by : _____

Dated : _____

PIN Deactivation Schedule Configuration

Page ____ of ____

Each day is configurable up to 4 intervals, each interval consists of a Start-End time. Do not overlap the intervals, such that the next Start time is not earlier than the previous End time. (maximum of 30 characters for Description field).

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Schedule # :		Description :							
Daily	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reg. Holiday	Sp. Holiday
Interval 1									
Interval 2									
Interval 3									
Interval 4									

Prepared by : _____

Dated : _____

Card Assignment (I)

Page ____ of ____

Card #	Facility Code	Card Format	Name (maximum 30 characters)	Department (maximum 4 characters)	User Field 1 : (as defined in Panel Setup, Default Settings)	User Field 2 : (as defined in Panel Setup, Default Settings)	Access Group	
							A	B

NOTE:

Start Date : denotes the date that the card will be effective

Expiry Date : denotes the date that the card will be ineffective

(leaving both entry empty denotes that the card will not expire)

Maximum of 20 character entry for User Field 1 and 2 each.

Prepared by: _____

Dated: _____

Card Assignment ()

Page ____ of ____

Card #	Facility Code	Card Format	Name (maximum 30 characters)	Card Functionality					Validation Date	
				Alarm Zone	Exit by Sch	Holiday	Card & PIN	PIN	Start	End
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			
					☐	☐	☐			

NOTE:

Card Functionality :

- Alarm Zone : If Cardholder is able to Arm/Disarm then enter the Alarm Zone.
 Holiday : Check box if operation on holiday is different from normal day of the week.
 Exit by Sch : Check box if exit is controlled by card access right Schedule
 Card & PIN : Check box if the card is to operate on Card & PIN mode.

Prepared by : _____

Dated : _____