

Access Easy Controller™

Quick User Guide

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
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.

Table of Contents

WELCOME.....	1
BASICS OF ACCESS CONTROL SYSTEMS.....	1
OVERVIEW OF ACCESS EASY CONTROLLER	2
LOGGING ONTO ACCESS EASY CONTROLLER	4
LOGGING OFF FROM ACCESS EASY CONTROLLER.....	5
ACCESS EASY CONTROLLER SCREEN NAVIGATION.....	5
<i>View Activity.....</i>	<i>6</i>
<i>Manual Control</i>	<i>6</i>
<i>Card Database</i>	<i>6</i>
<i>Card Access Admin.....</i>	<i>7</i>
<i>Panel Admin¹</i>	<i>7</i>
<i>Panel Maintenance¹</i>	<i>7</i>
<i>Logout.....</i>	<i>7</i>
SCHEDULES	8
<i>To define a new Schedule</i>	<i>9</i>
HOLIDAYS	9
<i>To define a Holiday Date.....</i>	<i>9</i>
ACCESS GROUPS	10
<i>To define an Access Group.....</i>	<i>10</i>
CARD ASSIGNMENT	11
<i>To add a range of Card Number.....</i>	<i>11</i>
<i>To add a range of Card Number with same data entries.....</i>	<i>11</i>
<i>Adding a Card to the database.....</i>	<i>12</i>
<i>Card Enrolment of Card with Unknown Wiegand Format.....</i>	<i>13</i>
VIEW ACTIVITY	15
MANUAL CONTROL (DOOR).....	17
<i>To control the Doors</i>	<i>17</i>
MANUAL CONTROL (INPUT).....	17
<i>To control the Alarm Zone's Input Points.....</i>	<i>17</i>
<i>To control the Individual Input Points.....</i>	<i>18</i>
MANUAL CONTROL (OUTPUT).....	18
<i>To control the Output Points</i>	<i>18</i>
RESET APB	19
<i>To Reset APB based on Card Number with respect to Reader / All Readers</i>	<i>19</i>
<i>To Reset APB based on Name with respect to Reader / All Readers.....</i>	<i>19</i>
<i>To Reset APB by All Card numbers with respect to Reader / All Readers</i>	<i>20</i>
HOW TO PRINT A REPORT	21

Welcome

We're glad that you have chosen Bosch Security Systems Access Easy Controller Access Control System for your access control needs. This quick user guide supplements the user manual and is not intended to be used as a standalone document.

Basics of Access Control Systems

To begin, it is helpful to define exactly what is meant by an “access control system”. In essence, an access control system is a computerised control over entry to any area that can be secured with a lock and key and the monitoring of alarm points. The control involves the locking and unlocking of doors and the tracking of who has been in a certain area during a specific point in time. The monitoring of alarm points involves the monitoring of anything you have defined as an alarm point. In general terms, an alarm point can be anything from a door to a motion detector that changes state. In the case of the door, if it remains open longer than the time you have specified, it changes to an alarm state.

An access control system provides the capability to automatically grant and deny access to areas which can be entire buildings, individual offices, specified designated areas, parking lots and/or outside gated areas. Corporate management can determine who, when and where access will be granted by configuring the Access Easy Controller with pertinent information.

- Cards are assigned to persons. A card acts as a key to unlock secured areas and allows access. Each card has an internal encoded number which is used to identify the card to the Access Control System. When a card is read by a Reader, the encoded number is used to locate the person's information in the Access Easy Controller database. The database is configured with information about the person along with access rights.
- Access rights provide a way of granting or denying access based on a criterion, such as management, department, or any other scheme fitting your environment. Access rights are assigned to him/her, enabling when and where access will be granted. Schedules may be set up, controlling when certain Access rights are valid and the locking or unlocking of areas based on a time criterion.

Overview of Access Easy Controller

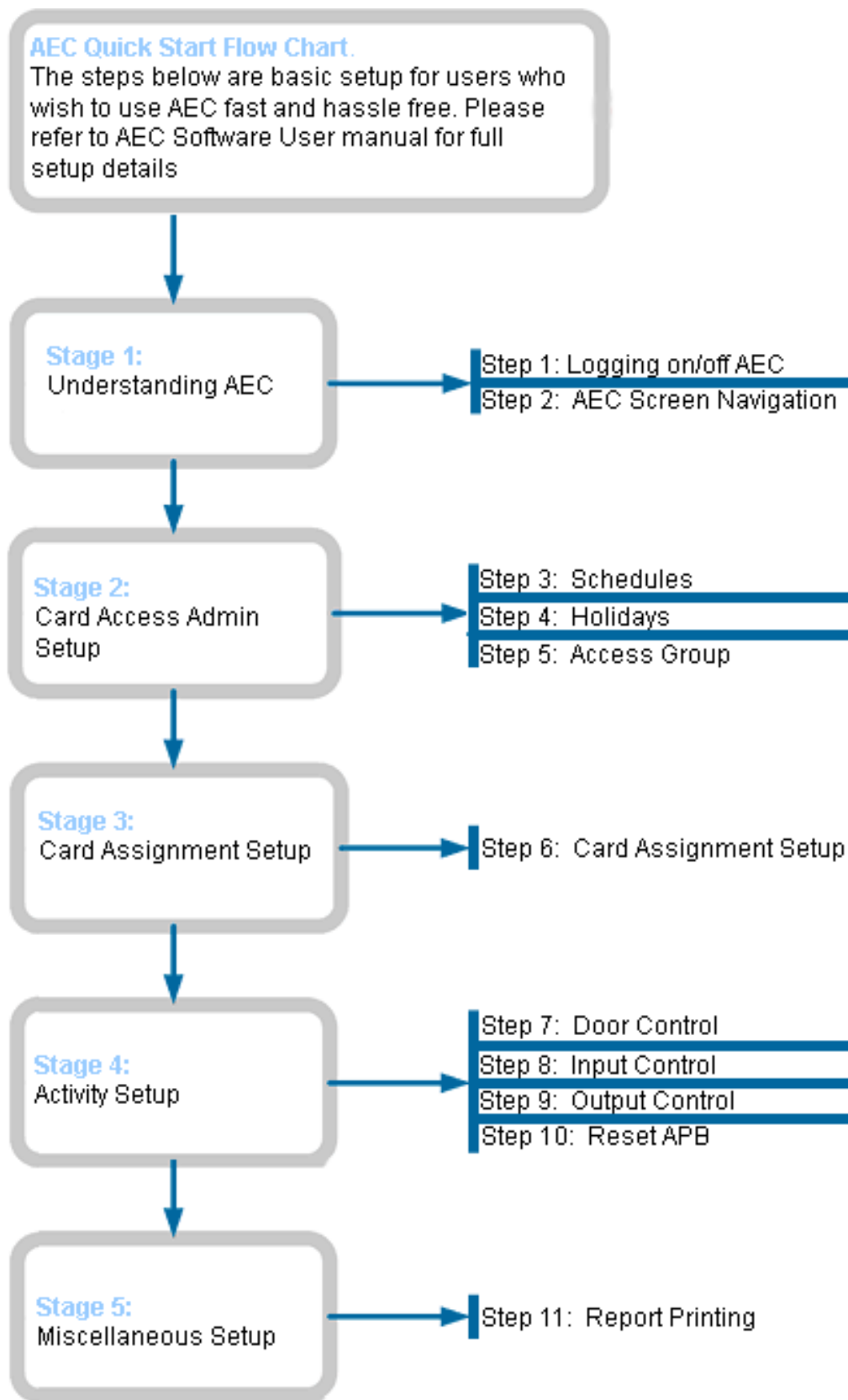
Access Easy Controller is a revolutionary invention that takes advantage of the web technology age by changing the way an electronic access control system is implemented.

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.

Pleaser refer to quick start flowchart on the next page for an overview of the steps taken.



*AEC: Access Easy Controller

Logging onto Access Easy Controller

A working knowledge of Windows or Macintosh and the standard web browser program, either Internet Explorer, version 4.0 or higher, or Netscape Navigator, version 4.0 or higher, and the ability to manoeuvre with a mouse pointer is required to complete the appropriate screens.

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*. The access rights cannot be disabled. However, the *User ID* and *Password* can be changed.

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

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

To access Access Easy Controller, launch your web browser program and enter the URL address of the Access Easy Controller. The User Login page appears.

Enter your User ID and Password to begin operations.

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.

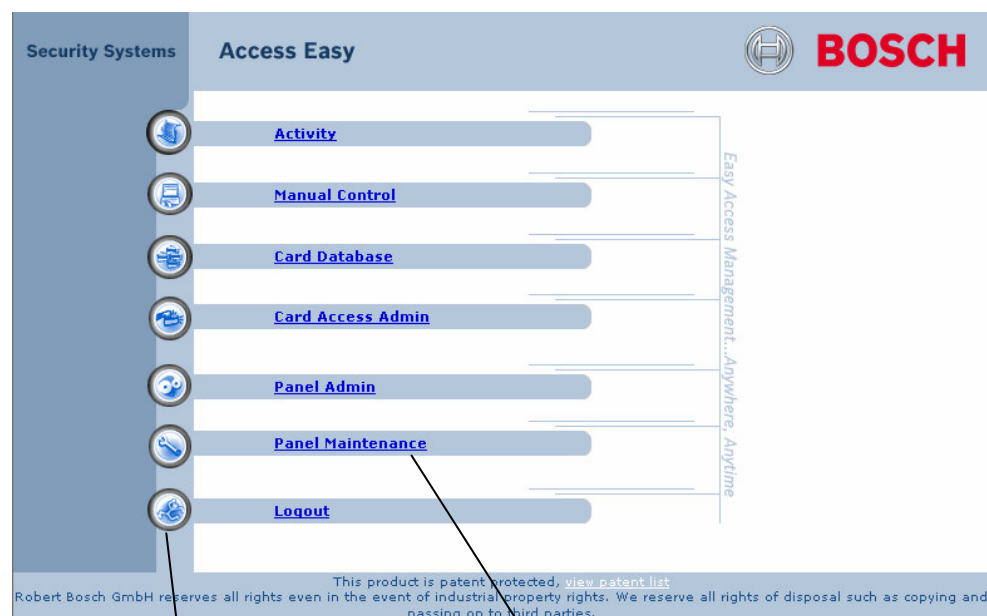
To log off, click on the **Logout** link, you be prompted by a message box to Backup the Database. Click on the appropriate button to proceed.

ALWAYS LOG OFF BEFORE LEAVING THE COMPUTER!

Access Easy Controller Screen Navigation

The **Home** page appears following a successful log on to the system. As shown below, the **Home** page consists of Menu Item groups and Icon buttons. If you are given access rights to one or more menu items of a group, click on the group link or icon button will display the menu item web page.

The full list of “*access rights dependent*” menu items will shown on the left pane of the web pages once you go beyond the **Home** page. The diagram on the next page shows the web page of one of the menu item.



Icon buttons linking to the page of the access rights dependent menu item in the group

Main Menu group

Security Systems **Access Easy** **BOSCH**

Activity
[View Activity](#)
[Activity Report](#)
Manual Control
[Door Control](#)
[Input Control](#)
[Output Control](#)
[Reset APB](#)
[View Activity](#)
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](#)
[Shutdown Panel](#)
[Logout](#)
[Home](#)

Manual Control
Door Control
☐ Input Control ☐ Output Control ☐ Reset APB ☐ View Activity

Door #	Description	Current Status	Manual Actions
1	Reader 1	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
2	Reader 2	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
3	Reader 3	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
4	Reader 4	Door Held Open	☐ 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 10	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
9	Reader 11	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
10	Reader 12	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
11	Reader 13	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
12	Reader 14	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
13	Reader 15	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock
14	Reader 16	Door Held Open	☐ No Change ☐ Unlock ☐ Momentarily Unlock

This product is patent protected, [view patent list](#)
 Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

Access Rights dependent menu item on the left pane

You can manoeuvre around the various web pages by clicking on the various menu items' link. A brief description of each menu item is presented below.

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.

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

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

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

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 Readers¹ are used to define the function of the Reader and its parameters, such as Door Settings, Hardware Setup...

Panel Admin¹

Users is to set-up the User ID and Password including access rights to the various menu items. This menu-item is only done by System Administrator.

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 schedule. For example, to turn on lighting in an area after office hours.

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.

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

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

Panel Maintenance¹

Update Flash is a utility that is used when there is a program upgrade. Usually carried out for firmware enhancement, new feature, and bug fixing. It can also be used for database recovery.

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

Logout

To log off from Access Easy Controller

¹ These parameter's settings are to be configured by the System Administrator only.

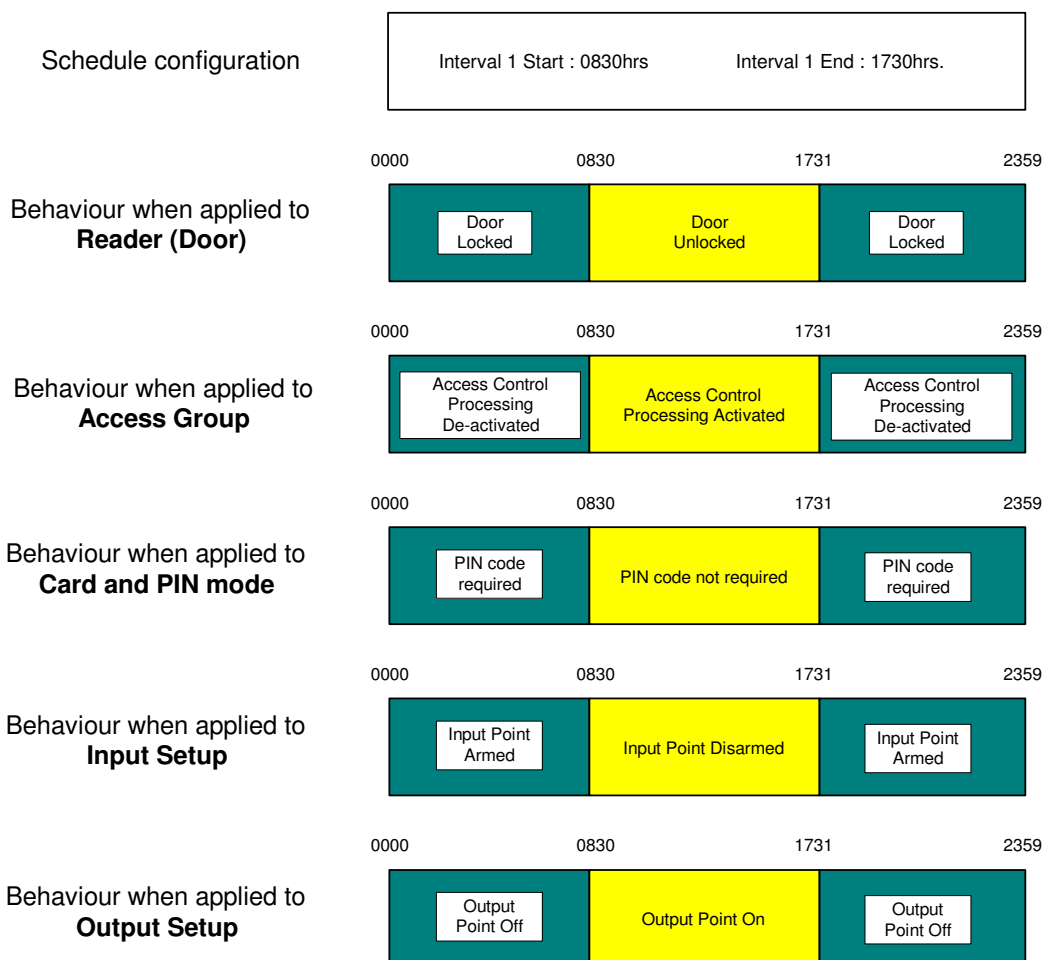
Schedules

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.
- 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 interval to arm / disarm the Input Points for Alarm Monitoring.
- It is used to define the time interval for triggering of the Output Points. For example, this is used for scheduled triggering of lighting utility for an area.

As Schedules affects the operational behaviour of the Access Control System and when the Alarm Monitoring function is active, it is recommended that you seek your System Administrator's permission before making changes or configuring new schedules

The diagram below shows the behaviour of the system when configured to a Schedule.



To define a new Schedule

1. Click on the **Schedule** link.
2. Click on an **Undefined Schedule**.
3. Highlight the default text and enter the new *Description* and 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.
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 check boxes to indicate a tick (✓) mark. This will duplicate the current setting to other DOW. To de-select the *DOW*, click on it again.
8. Click on the  button.

Holidays

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 menu-item are categorised to *Regular Holiday* dates and *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.

To define a Holiday Date

1. Click on the Holidays link.
2. Select the appropriate Holiday, **Regular** or **Special**.
3. Click on the next **Undefined Holiday**.
4. Highlight the default text and enter the new *Holiday Description*.
5. Select the holiday date.
6. If the holiday date is the same year after year, then select the **No** radio button for the **Include year in processing?**
7. Click on the  button.

Access Groups

An *Access Group* defines a list of readers within certain authorised time period(s) that the cardholders can access. This means that only within this *Schedule*, cardholders with this access group can access those readers.

To define an Access Group

1. Click on the **Access Groups** link.
2. Select the next **Undefined Access Group** number. Your System Administrator would have predetermined the description of the Readers in use.
3. Highlight the default text and enter the new *Access Group Description*.
4. Click on the appropriate check boxes to indicate a tick (✓) mark in the box, for reader(s) to be assigned to this *Access Group*.
5. For each Reader, select the appropriate Schedule.
6. 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 4 to 5.
7. Click on  button.

Card Assignment

To add a range of Card Number

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

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

To add a range 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 range 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 range 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.

Card Database

Card Assignment 

[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.
3. Proceed to edit the newly added card number parameters by clicking on the desired card number link (Follow steps 3 to 14 under *Adding a Card to the database* for editing card number parameters).

Adding a Card to the database

1. To add a Card Number, click on Card Assignment link.
2. Click on the empty slot  link.
3. Enter the card number into the **Card Number** field. **This is a required field. If you do not place any information in this field, Access Easy Controller will prompt you with an error message.**
4. Leave the **Facility Code** field as it is, the code have been predetermined by your System Administrator.
5. Select the **Card Format** from the pull-down list. The format have been predetermined by your System Administrator.
6. Enter the cardholder's name in the **User Name** field.
7. Enter the **Department** of the cardholder.
8. Enter the appropriate entry in the following two fields. The description of the fields have been predetermined by your System Administrator.
9. Select the appropriate **Access Group** from the pull-down list. **Access Group** are a combination of assigned Card Readers and Schedules, defining when and where a person is to be granted access. Up to two **Access Groups** are assigned to each Cardholder. The description of the Access Group have been predetermined by your System Administrator.
10. Click on the  button to proceed.
11. The **Card Functionality** is used to define how and when the Cardholder is to use his/her card.
 - Card holder is able to Arm/Disarm – allow cardholder to arm or disarm an Alarm Zone via a dedicated Card Reader.
 - Card holder must abide by holiday schedules – access to the Reader is determined by Holiday schedules.

- Allow exit reader usage only in accordance with time schedules – card holder is only allow exit as determined by the time schedules.
 - Card holder can enable card enrolment operation – Allow selected card holders to have the right to use their card to activate a Reader to be in enrolment mode
 - 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 car
 - 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* automaticall
 - Card + PIN is required on keypad readers – this is the Card plus PIN mode.
12. If required, highlight the **default user PIN** (1234000) and enter a new PIN code of 1 to 7 digits.
 13. The **Card Validation Dates** is used to define when the card is valid and/or when it is to expire. Check the appropriate check box(es) before selecting the date(s).
 14. 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
 15. Also select the Dual Card Group ID from the drop-down box.
 16. At this point, you are ready to save the card parameters. Click the  button.

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 Enrollment](#)
2. Select a Reader to be the enrolment Reader.
3. Click on the  button to activate the selected Reader as the enrolment Reader.
4. Present the card with unknown Wiegand Format to the enrolment Reader.
The card that has been presented to the enrolment Reader will appear in the box for *List of scanned cards*
5. The administrator can now assign any Card # and Name to the card.

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.
-------------	--

6. Highlight the card in the *List of scanned cards* that you are assigning the Card # and Name to
7. Click on the  button to add the card with the assigned Card # and Name to the database

View Activity

The View Activity feature allows you to view activity transactions. The transactions are displayed in real-time mode according to the transaction occurrence date and time.

Click on the appropriate link to view the following categorised transactions:

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

When any of the “**Alarm**” Activity transactions is transacted, an alert tone will be sent to the monitoring computer’s audio system.

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



[Alarm](#)

To display only Alarm transactions.



[Valid](#)

To display Valid and Alarm transactions.



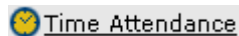
[Restore](#)

To display Restore and Alarm transactions.



[All](#)

To display All transactions.



[Time Attendance](#)

To display only Time Clocking transactions.



To acknowledge Alarm transactions. This will also silent the audible tones on the CMC.



To update the web page for the latest transactions.



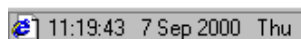
[APB Report](#)

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.

- 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 Alarm transactions, which remains unless the  button is activated.

We will explain in more detail through an example.



Activity
View Activity
Activity Report
Manual Control
Door Control
Input Control
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
Shutdown Panel
Logout
Home

Activity
View Activity

Door Control Input Control Output Control Reset APB

Alarm Valid Restore All Time Attendance

All Activities

No	Date	Location	Activity Description
	Time	Card No	User Name
6	22 May 2000 17:57:26	Main Entrance 115	Clock Out Simon Tay GH
5	22 May 2000 17:10:07	Panel -----	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	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	Panel -----	Tamper Restored -----
0	22 May 2000 16:50:23	Panel -----	Panel Tamper -----

Reference to the above diagram.

- 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).

Manual Control (Door)

The Door Control feature allow you to check the status of all the doors and to send a command to either momentarily unlock or permanently unlock 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.

To control the Doors

1. Select the desired action radio button(s) (see NOTE1). Your System Administrator would have pre-determined the Reader's description.
2. Click on either  or  button to send the command. The web page will refresh to reflect the new status.

NOTE1: Select only door(s) that you want to send command to.

NOTE2: The current status of the door for a Momentary 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.

Manual Control (Input)

The Input Control feature allow you to check the status of all the Input Points in pre-determined Alarm Zone and to send a command to Arm or 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.

To control the Alarm Zone's Input Points

1. Click on the appropriate link,  [1-16](#) or  [17-32](#), to display the desired Alarm Zone. Your System Administrator would have pre-determined and grouped the Input Points to their respective Alarm Zones. At this time, you should able to see the status of the selected Zone and the appropriate  or  button would appear.
2. Click on the button to toggle the status. The web page will refresh to reflect the new status.

To control the Individual Input Points

1. Click on the Input Control Link to shows status of the inputs.
2. You should able to see the status of all the individual inputs that are not grouped to any Alarm Zones.
3. Select the radio button ☐ Arm Now or ☐ Disarm Now and click on the refresh button  to arm or disarm.

Manual Control (Output)

The Output Control feature allow you to check the status of all the Output Points and to send a command to turn On or turn Off the point(s). However, if the Output Point is linked to an Input Point as an Alarm 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.

To control the Output Points

1. Click on the appropriate link,  1-16 or  17-32, to display the correct range of Output Points.
2. Select the desired radio button(s) (see NOTE1). Your System Administrator would have pre-determined the Output Points description.
3. Click on either  or  button to send the command. The web page will refresh to reflect the new status.

NOTE1: Select only Output Point(s) that you want to send command to.

NOTE2: 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 click on the  button.

Reset APB

The **Reset APB** feature allow you to reset the Anti-Passback (APB) feature once it is violated. It is only applicable to Full and Soft APB.

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 stop logging the Activity transactions, "Access Granted, Soft APB" and "Exit Granted, Soft APB" for violator's subsequent access or exit respectively.

You can reset the APB violation with the following combination: -

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

To Reset APB based on Card Number with respect to 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. Click on the Reset APB link.
2. Enter the *Card Number* of the APB violator.
3. Leave the **Facility Code** field as it is, the code have been predetermined by your System Administrator.
4. Select the **Card Format** from the pull-down list.
5. Select the appropriate Reader or All Readers.
6. Click on the  button to proceed.
If the command is executed successfully, a message indicating APB reset by card number & zones with respect to reader / all readers will be displayed.
7. Click on the  button to return.

To Reset APB based on Name with respect to Reader / All Readers

1. Enter a character, a portion, or the full name in the Name field 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 appropriate Reader or 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 with respect to Reader / All Readers

1. Select the appropriate Reader or 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.

How to Print a Report

There are several reports that may be generated from Access Easy Controller. The reports available are listed in the Table.

Report Types	Description
View Activity	This report shows the activities/events that happened during the system operation. The report are further categorised into five different types. They are Alarm, Valid, Restore, All, and Time Attendance.
APB Report	This report shows the cardholder(s) who are in the specific APB Zone(s) at the time of report preview.
Card Assignment	This report shows details of all the cards in the database.
Access Groups	This report shows the Access Groupings available to cardholders to have access to specified reader(s) and during specified schedule.
Schedules	This report shows the intervals definition for different Day of Week (DOW) of each Schedule
Holidays (Regular or Special)	This report shows the defined Holiday description and dates.
Card Readers	The report shows details of all the Card Readers in use.

To print any of the report, go to the first web page of the menu items and click on the report link.

You will be shown a **Selection Criteria** page.



Make your selection and click on the  button for a report preview.

To print the report, select **Print** from the **File** drop down menu on the Menu bar.

Notes

Notes