BOSCH

Access Easy Master Controller

en Software Manual

Table of contents

1 Copyright, Safety and Warranty

1.1 Copyright information

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.

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

1.2 Important safety notes

1. **Read, Follow, and Retain Instructions** – All safety and operating instructions must be read and followed properly before putting the unit into operation. Retain instructions for future reference.
2. **Consider all Warnings** – Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** – Use only accessories recommended by the manufacturer or those sold with the product. Accessories not recommended by the manufacturer shall not be used, as they may cause hazards.
4. **Installation Precautions** – Do not place this unit on an unstable stand, tripod, bracket, or mount. The unit may fall, causing serious injury to persons and damage to the unit. Mount the unit according to the manufacturer's instructions.
5. **Service** – Do not attempt to service this unit by yourself. Opening or removing covers may expose you to dangerous voltages or other hazards. Refer all servicing to qualified service personnel.
6. **Damage Requiring Service** – Disconnect the unit from the main AC or DC power source and refer servicing to qualified service personnel under the following conditions:
   - When the power supply cord or plug is damaged.
   - If liquid has been spilled or an object has fallen into the unit.
   - If the unit has been exposed to water and/or inclement weather (rain, snow, etc.).
   - If the unit does not operate normally, when following the operating instructions. Adjust only those controls specified in the operating instructions. Improper adjustment of other controls may result in damage, and require extensive work by a qualified technician to restore the unit to normal operation.
   - If the unit has been dropped or the cabinet damaged.
   - If the unit exhibits a distinct change in performance, this indicates that service is needed.
7. **Replacement Parts** – When replacement parts are required, the service technician shall use replacement parts that are specified by the manufacturer. Unauthorized substitutions may result in fire, electrical shock or other hazards.
8. **Safety Check** – Upon completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure that the unit operates properly.
9. **Power Sources** – Operate the unit only from the type of power source indicated on the label. If unsure of the type of power supply to use, contact your dealer.
   - For units intended to operate from battery power, refer to the operating instructions.
   - For units intended to operate with External Power Supplies, use only the recommended approved power supplies.
10. **Lightning** – For added protection during a lightning storm, or when this unit is left unused for long periods of time, disconnect the unit from power. This will prevent damage to the unit due to lightning and excessive power line surges.
11. **Restricted Access Locations** are required for the installation.
12. **DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE IS BELOW -20°C (-4°F) OR ABOVE 65°C (149°F). IT MAY DAMAGE THE EQUIPMENT.**

1.3 FCC information

Notice!
This device complies with Part 15 FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

1.4 Safety precautions

Caution!
There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions and your local government’s recycling or disposal directives.

2 Before You Begin

The Access Easy Master Software User Manual contains two detailed software setup information:

- Access Easy Master Controller software
- Access Easy for Master Controller software

Access Easy Master software is the main software that administers and controls all Access Easy Controllers whereas Access Easy for Master software only supports minimal functions on its respective Access Easy Controller.

In this manual, we will use the following terminologies to describe the following software.

Name	Terminology
Access Easy Master Controller software	Access Easy Master
Access Easy For Master Controller software	Access Easy for Master
Access Easy Controller Hardware	Access Easy Controller

This manual will describe the Access Easy Master Controller software from Chapter 3 to 18 whereas Chapter 19 to 20 will describe the Access Easy for Master Controller software.

2.1 Terms and Conventions

If you are a Microsoft Windows user, the terms in this User Manual should be familiar to you. If you have not used Windows before, or would like a refresher course, please read this section to become familiar with some common terms.

- Pointer refers to the arrow-shaped cursor on the screen.
- Choose means to move the pointer to a menu, command, tool, or button and press the left mouse button. This term is synonymous with click.
- Select means to mark an item with the selection cursor, which can appear as a highlight, a dotted rectangle, or both.
- Double-click means to press the left mouse button twice rapidly.
- Drag means to hold down the left mouse button, move the pointer to another location on the screen, and release the mouse button.
- Field is a category of information. It could be card numbers, names, shift codes or dates.

In addition to these terms, the following conventions are used:-

- Menu, command, table names are shown in bold or italic type.
- When two keys are used together to perform a task, they are separated with a plus sign. For example, the key combination Ctrl + F4 means you hold down the Ctrl key and press the F4 key.

3 Introduction to Access Easy Master

Access Easy Master 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 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 have to be re-developed before it can run on another operating system.

Access Easy Master uniquely combines the features of web technologies and access control functionality 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 Master adopts the common desktop metaphor for all Windows applications for consistency and ease of use. The same "look-and-feel" such as buttons and check boxes that you have experienced in other Windows applications will be seen in Access Easy Master.

The unique feature in Access Easy Master is, all the Access Easy Controller can be centrally administered from a single Access Easy Master.

3.1 Features of Access Easy Master

- Cross-operating platform/system interoperability. Whether it is a PC, Mac or Unix machine, Access Easy Master gives you complete flexibility of operating on these platforms without any extra effort in setting up.
- Easy to install as Access Easy Master adopts the 'Plug n Play' concept. Simply connect a network cable from the Access Easy Master to a network hub, follow by running a web browser program to set up the Access Easy Master and the system will be up and running in no time.
- Easy to operate for end users as it uses the intuitive web interface that makes controlling or monitoring the system like performing Internet surfing! This also implies that minimum training is needed for installers, distributors and end users.
- Easy to access Access Easy Master from any computer (or client) that exists in your network, be it in a LAN or WAN configuration! No longer are users required to have a dedicated computer to handle the controller as any computer can now be used to access the Access Easy Master. Such powerful feature allows users to save costs by fully optimizing their existing resources and cutting down on any unnecessary spending on new hardware.
- Easy to maintain or upgrade the system as it is not dependent on any operating platform/system to run on. Upgrading the Access Easy Master does not require users to upgrade their computers and operating systems. Likewise, upgrading the operating system will not affect the Access Easy Master system configuration. Such investment produces long term cost savings for the users.
- Time and cost savings in the installation, testing and commissioning of Access Easy Master as no application programs are required to be installed on central computer(s). This implies greater profits at a shorter time for both distributors and installers.

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

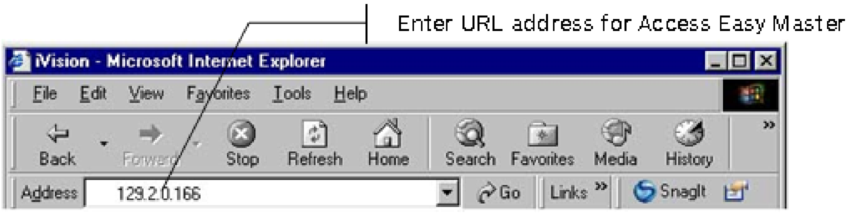
4 Logging In and Understanding Access Easy Master

Before the user starts to understand the Access Easy Master features, let us take a look at the procedures of logging in first.

4.1 Logging Into Access Easy Master

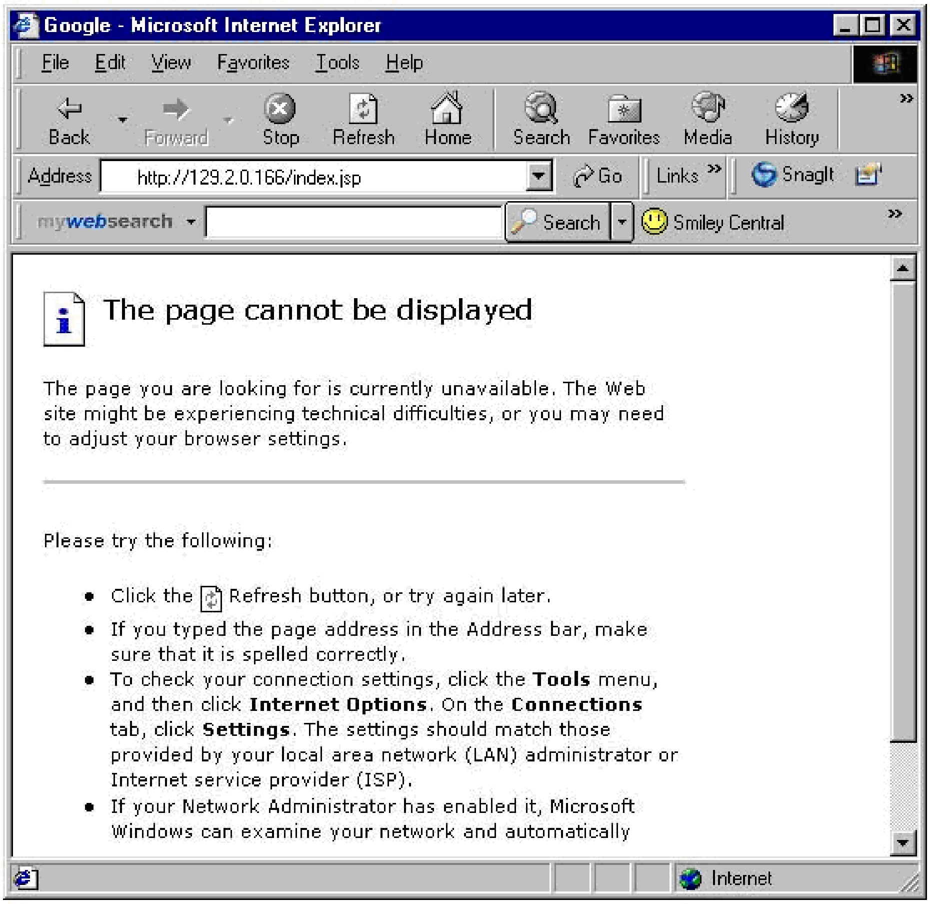
In order to login to Access Easy Master, a computer with a standard web browser program such as Internet Explorer is required on the computer.

1. To get connected to Access Easy Master, run your web browser page with the default URL address for the Access Easy Master.


Enter URL address for Access Easy Master

iVision - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History
Address 129.2.0.166 Go Links SnagIt

2. If the page cannot be displayed as shown below, follow steps 3 to 8. If the **Security Alert** dialog box appears, follow steps 7 to 8.


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History
Address http://129.2.0.166/index.jsp Go Links SnagIt
mywebsearch Search Smiley Central
Internet

The page cannot be displayed

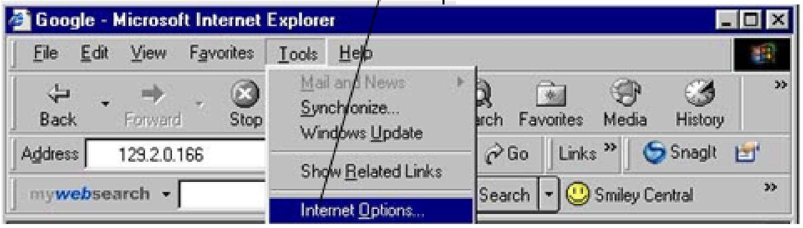
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically

3. Go to the menu items of the web browser and select **Tools > Internet Options**.

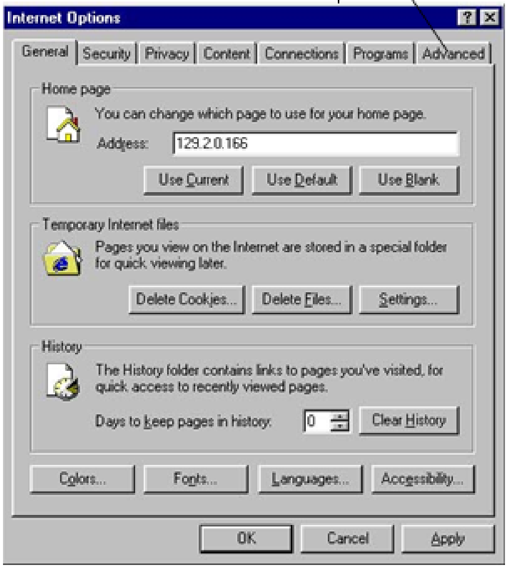
Select *Tools, Internet Options*



Address: 129.2.0.166

4. The **Internet Options** window appears as shown below. Select the **Advanced** tab.

Select *Advanced*



You can change which page to use for your home page.

Address: 129.2.0.166

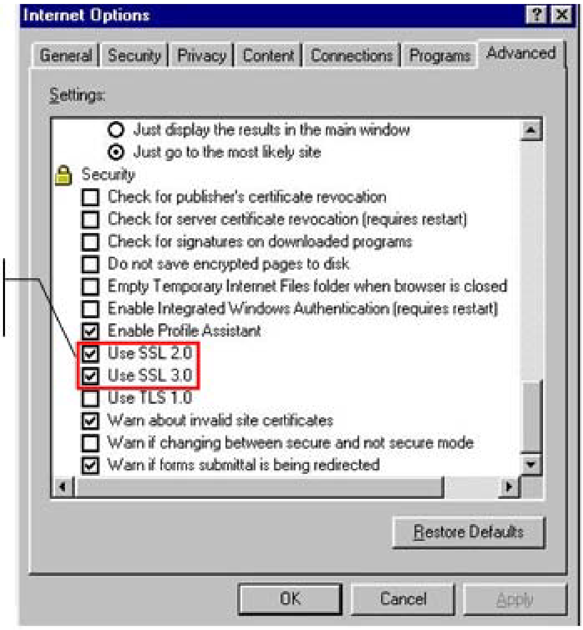
Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 0

5. A screen as shown below appears. Check both the **Use SSL 2.0** and **Use SSL 3.0** checkboxes.

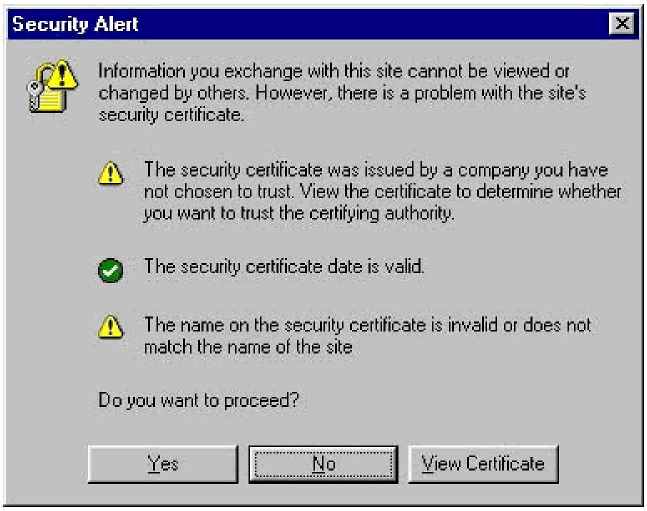
Check the *Use SSL 2.0* and *Use SSL 3.0* box



Settings:

- ○ Just display the results in the main window
- ● Just go to the most likely site
- Security
  - □ Check for publisher's certificate revocation
  - □ Check for server certificate revocation (requires restart)
  - □ Check for signatures on downloaded programs
  - □ Do not save encrypted pages to disk
  - □ Empty Temporary Internet Files folder when browser is closed
  - □ Enable Integrated Windows Authentication (requires restart)
  - ☑ Enable Profile Assistant
  - ☑ Use SSL 2.0
  - ☑ Use SSL 3.0
  - □ Use TLS 1.0
  - ☑ Warn about invalid site certificates
  - □ Warn if changing between secure and not secure mode
  - ☑ Warn if forms submittal is being redirected

6. Click the **OK** button and go to the menu items of the web browser. Select **View > Refresh**. The **Security Alert** dialog box appears on the screen.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

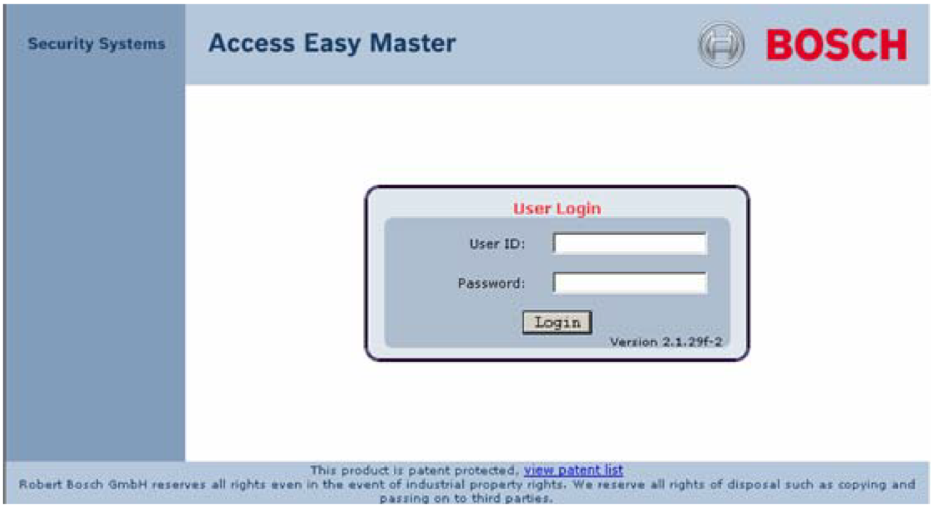
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

7. Click the **Yes** button to proceed and the **User Login** page appears. If the **No** button is selected, the page remains blank and the user will not be able to see the **User Login** page. To proceed, go to the menu items of the web browser and select **View > Refresh**. The **Security Alert** dialog box will appear again. Click the **Yes** button to proceed.



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.

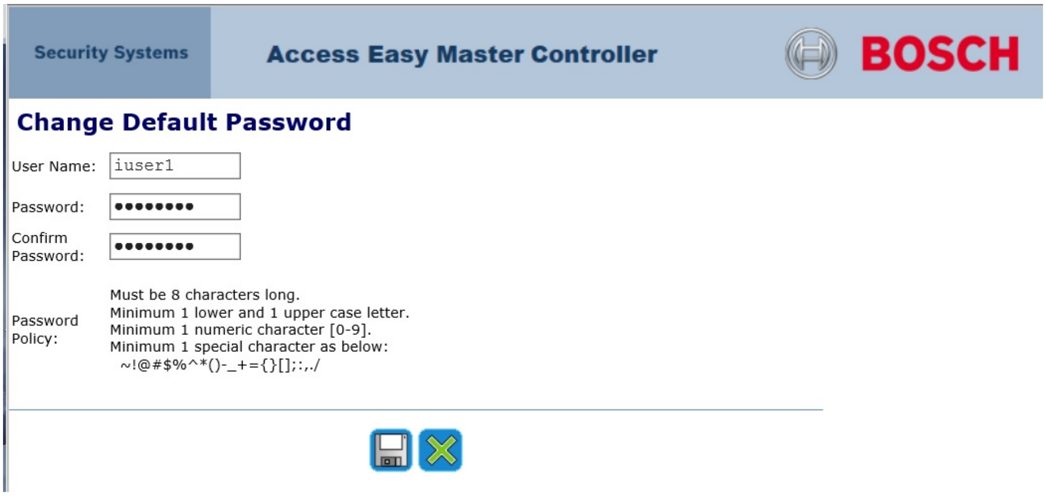
8. If you are logging in for the first time, please refer to the section below. Otherwise, enter your assigned user ID in the **User ID** field and password in the **Password** field. Click the **Login** button to login.

Notice!
The default user ID is “iuser1” and the default password is “8088”.

Logging into Access Easy Master for the first time

1. Enter your assigned user ID in the **User ID** field.
2. Enter you assigned password in the **Password** field.
3. Click the **Login** button to login.

4. You will be redirected to the **Change Default Password** page to change your user ID and/or password immediately.



Change Default Password

User Name: iuser1

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Password Policy:
Must be 8 characters long.
Minimum 1 lower and 1 upper case letter.
Minimum 1 numeric character [0-9].
Minimum 1 special character as below:
~!@#$%^*()-_+={}[];:,./

5. Enter your new user ID in the **User Name** field if you wish to change your user ID. Otherwise, you may ignore it.
6. Enter your new password in the **Password** field.
7. Reenter you new password in the **Confirm Password** field.

⚠

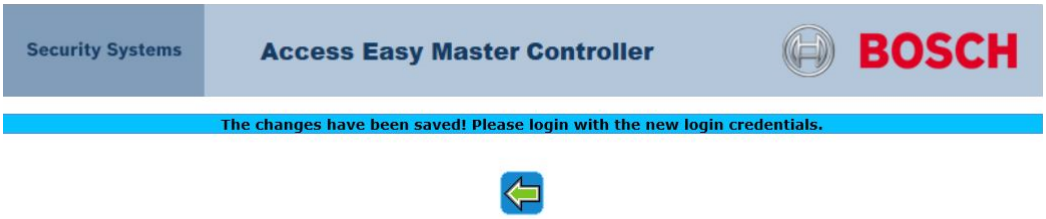
Caution!

The password is case-sensitive. For security reasons, every character entered in the password field is represented by a dot.

The passwords must meet the following requirements:

must be 8 characters long
must consist of at least
- 1 lowercase letter,
- 1 uppercase letter,
- 1 number, and
- 1 special character from ~`!@#$%^*()-_+={}[];:,./

8. Click the 💾 button to save the changes. If the **Password** and **Confirm Password** fields match and meet the password requirement policy, a confirmation page appears.

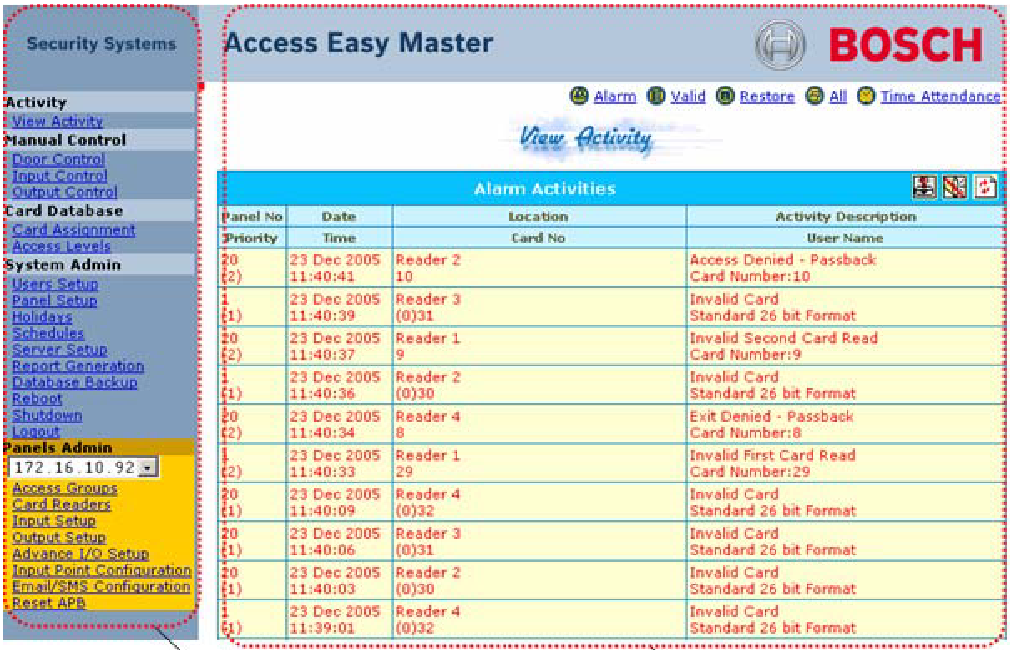


The changes have been saved! Please login with the new login credentials.

9. Click the ⇦ button to return to the **User Login** screen.
10. Login using the new credentials.

Successful login

Upon successful login to the Access Easy Master, the user will see the **View Activity** page in alarm transactions. It is the default page whenever the user logins to Access Easy Master.



Alarm Activities

Panel No Priority	Date Time	Location Card No	Activity Description User Name
20 (2)	23 Dec 2005 11:40:41	Reader 2 10	Access Denied - Passback Card Number:10
1 (1)	23 Dec 2005 11:40:39	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:37	Reader 1 9	Invalid Second Card Read Card Number:9
1 (1)	23 Dec 2005 11:40:36	Reader 2 (0)30	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:34	Reader 4 8	Exit Denied - Passback Card Number:8
1 (2)	23 Dec 2005 11:40:33	Reader 1 29	Invalid First Card Read Card Number:29
20 (1)	23 Dec 2005 11:40:09	Reader 4 (0)32	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:06	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:03	Reader 2 (0)30	Invalid Card Standard 26 bit Format
1 (1)	23 Dec 2005 11:39:01	Reader 4 (0)32	Invalid Card Standard 26 bit Format

Left Pane
The left pane displays the main menu items for ease of operation. Those in bright yellow background are the Panel's menu group.

Right Pane
The right pane displays the work area of the menu items selected.

The pages will consist of the main menu items on the left pane and the work area on the right pane. This presentation is standard throughout all pages of the Access Easy Master.

4.2 Progressive delays between login attempts

The system utilizes progressive delays between login attempts for better security and protection from unauthorized access. Progressive longer delays are enforced between subsequent logins after a number of unsuccessful login attempts. The section below describes the progressive delay operation.

After the third unsuccessful login, a 20 seconds' delay kicks in before the user can attempt the fourth login. This delay duration appears within the log on screen and starts counting down. The user may attempt to login during this duration but the system will ignore these login attempts. After the countdown has completed, the user can then attempt to login again. Note that each subsequent unsuccessful login will trigger a delay duration that is twice longer than the previous delay.

Clearing the progressive delays

Clear the progressive delay by performing one of the following:

- Log in successfully with the correct credentials.
- Restart the AEMC.
- Administrator changing the password or username of the user who failed the login attempts.

4.3 Main Menu Items

The main menu items are shown on the left pane of each page. Each Access Easy Master main menu item in explained in brief below.

4.3.1 Activity

The **Activity** menu allows the user to view the activities that occurred in the system. The submenu items of **Activity** is **View Activity**.

View Activity

The **View Activity** page shows transactions generated due to access control, system control, and alarm conditions. The transactions are categorized into the following: **Alarm**, **Valid**, **Restore** and **Time Attendance**. User can view only one specific category at a time as mentioned above or all transactions at once.

Using Java Applet technique, all the activities and status on the **Manual Control** pages (**Door Control**, **Input Control** and **Output Control**) will automatically be updated in real time.

4.3.2 Manual Control

The **Manual Control** menu allows the user to control the door, input points and output points manually by having priority over the control set by the system. The submenu items of **Manual Control** are **Door Control**, **Input Control** and **Output Control**.

Door Control

The **Door Control** page allows the user to check the status of all the doors and send a command to either momentarily unlock, or permanently unlock or lock the door without having to be at the door location.

Input Control

The **Input Control** page allows the user to check the status of all the input points assigned to specific alarm zones and to send a command to arm or disarm the zone manually.

Output Control

The **Output Control** page allows the user to check the status of all the output points and send a command to turn on or off the points manually.

4.3.3 Card Database

The **Card Database** menu allows the user to administer the card details, functionality and the access levels of the card. The submenu items of **Card Database** are **Card Assignment** and **Access Levels**.

Card Assignment

The **Card Assignment** page allows the administrator to assign cards to users. The access level for the user and the card functionality is also configured in this section.

Access Levels

The **Access Levels** page allows the user to define access groups of different Access Easy Controller into groups. When assigned to a cardholder, these groups allow the cardholder to access doors over multiple Access Easy Controllers, hence enabling the administrator to manage cardholders' access in a centralized location.

4.3.4 System Admin

The **System Admin** menu allows the user to setup the different aspects of the system such as the users, controller and server configuration. It also allows the user to generate reports from the system and backup database of the system. The submenu items of **System Admin** are **Users Setup**, **Panel Setup**, **Holidays**, **Schedules**, **Server Setup**, **Report Generation**, **Database Backup**, **Reboot**, **Shutdown** and **Logout**.

Users Setup

The **Users Setup** item allows the user to set up the user ID and password including access rights to the various menu items.

Panel Setup

The **Panel Setup** item allows the user to admit Access Easy Controller to join the system network.

Holidays

The **Holidays** item allows the user to setup centralized holiday dates that are applicable to all the Access Easy Controllers.

Schedules

The **Schedules** item allows the user to setup centralized schedules available to all the Access Easy Controllers, that can be assigned to readers or access groups.

Server Setup

The **Server Setup** item allows the user to configure the following settings:

- Network Settings
- Auto Logout Timer
- Card Format
- View Activity Setting
- Company Profile
- Set Date and Time
- Default Settings
- Housekeeping
- Alarm Event Setup

Report Generation

The **Report Generation** item allows the user to generate activity reports for particular dates and time based on devices, cardholders and events.

Database Backup

The **Database Backup** item allows the user to save a backup of the database to the local hard disk and also allows the user to restore the database in the event of any controller failure.

Reboot

The **Reboot** item allows the user to reboot the Access Easy Master remotely without having to be at the Access Easy Master itself.

Shutdown

The **Shutdown** item allows the user to shutdown the system remotely without having to be at the Access Easy Master itself.

Logout

The **Logout** item allows the user to do a proper exit from the Access Easy Master.

4.3.5 Panels Admin

The **Panels Admin** menu allows the user to administer the individual Access Easy Controller. The submenu items of **Panels Admin** are **Access Groups**, **Card Readers**, **Input Setup**, **Output Setup**, **Advance I/O Setup**, **Input Point Configuration**, **Email/SMS Configuration** and **Reset APB**.

Access Groups

The **Access Groups** item allow the user to define a list of readers, which the cardholders can access within certain authorized time periods (predefined schedule).

Card Readers

The **Card Readers** item is used to define the function of the readers and their parameters, such as door settings, and so on.

Input Setup

The **Input Setup** item is used to set up alarm monitoring point to be armed or disarmed based on schedule or via an assigned reader. It also allows the mapping of output points to be triggered should an alarm be detected.

Output Setup

The **Output Setup** item is used to set up the triggering of output relay based on schedules. For example, this can be used to turn on lighting in an area after office hours.

Advance I/O Setup

The **Advance I/O Setup** item enables 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.

Input Point Configuration

The **Input Point Configuration** item allows the user to invert the logical state of the input that is seen by the Access Easy Controller, as well as to select the monitoring state of the input point.

Email/SMS Configuration

The **Email/SMS Configuration** item allows the user to setup the email and SMS server settings, to allow the Access Easy Controller to send out messages or email to selected mobile numbers or email addresses according to the selected devices, cardholders and events. Lateness report can also be sent to configured email addresses.

Reset APB

The **Reset APB** item allows the user to reset the anti-passback (APB) feature once it is violated.

4.4 Usage of the Buttons

Another important part to understand is the usage of the buttons. The buttons that appear at the bottom of each screen can be explained as follows:

Button	Description
💾	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 used in place of the cancel button to abort changes. However, condition applies that none of the other buttons namely, the next, previous 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 used to reset APB violation. – It is used to clear the field in the Holiday date setting.
✖	The cancel button abort changes and revert to previously saved settings.

5 Activity

Each activity transaction such as “Door Forced Open”, “Door Held Open” and others is captured by Access Easy Master and displayed on the **View Activity** page in real-time mode according to the transaction date and time.

The activity transactions are categorized into four groups. They are:

- Alarm Activity,
- Valid Activity,
- Restore Activity, and
- Time Attendance.

Please refer to *APPENDIX C Activity Transactions, page 234* for the activity transactions in the different groups.

5.1 View Activity

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

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

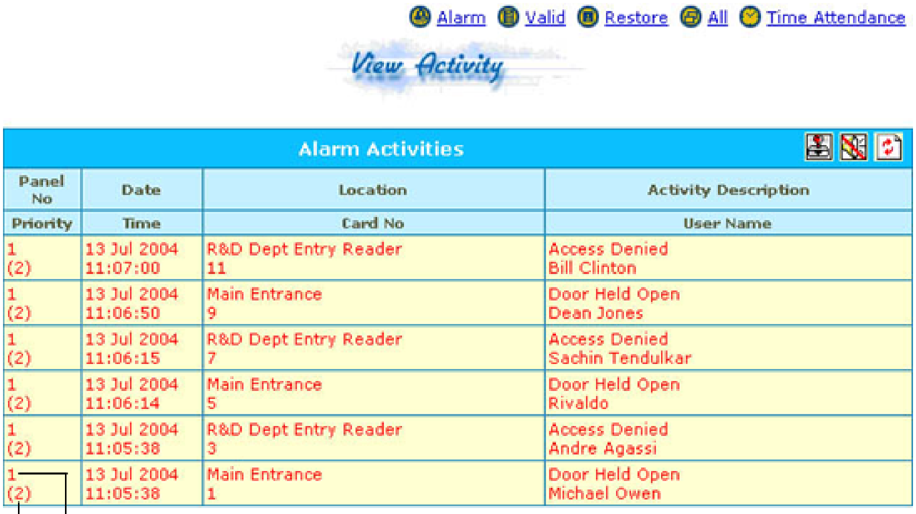
The number of records to view on screen is configurable by the user, which is up to a maximum of 70 records. Please refer to *View Activity Setting, page 87* for details on setting the number of transaction records to view on screen.

Notice!
The **View Activity** 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 acknowledged" alarm transaction up to the latest transaction.

When any of the alarm activity transactions is transacted, an alert audio tone is sent to the PC. Please ensure that the PC's audio system is in working order and the volume is set to a reasonable level.

5.1.1 How to View Activity

Upon login to the Access Easy Master, the **View Activity** page for alarm transactions will be displayed. However, you can select **View Activity** from the left pane to view the activities from any other pages.



Alarm Activities

Panel No	Date	Location	Activity Description
Priority	Time	Card No	User Name
1 (2)	13 Jul 2004 11:07:00	R&D Dept Entry Reader 11	Access Denied Bill Clinton
1 (2)	13 Jul 2004 11:06:50	Main Entrance 9	Door Held Open Dean Jones
1 (2)	13 Jul 2004 11:06:15	R&D Dept Entry Reader 7	Access Denied Sachin Tendulkar
1 (2)	13 Jul 2004 11:06:14	Main Entrance 5	Door Held Open Rivaldo
1 (2)	13 Jul 2004 11:05:38	R&D Dept Entry Reader 3	Access Denied Andre Agassi
1 (2)	13 Jul 2004 11:05:38	Main Entrance 1	Door Held Open Michael Owen

Access Easy Controller ID

Alarm Priority ('2' indicates that Door Held Open has priority 2 under alarm transactions. 1 has the highest priority, followed by 2 and so on.)

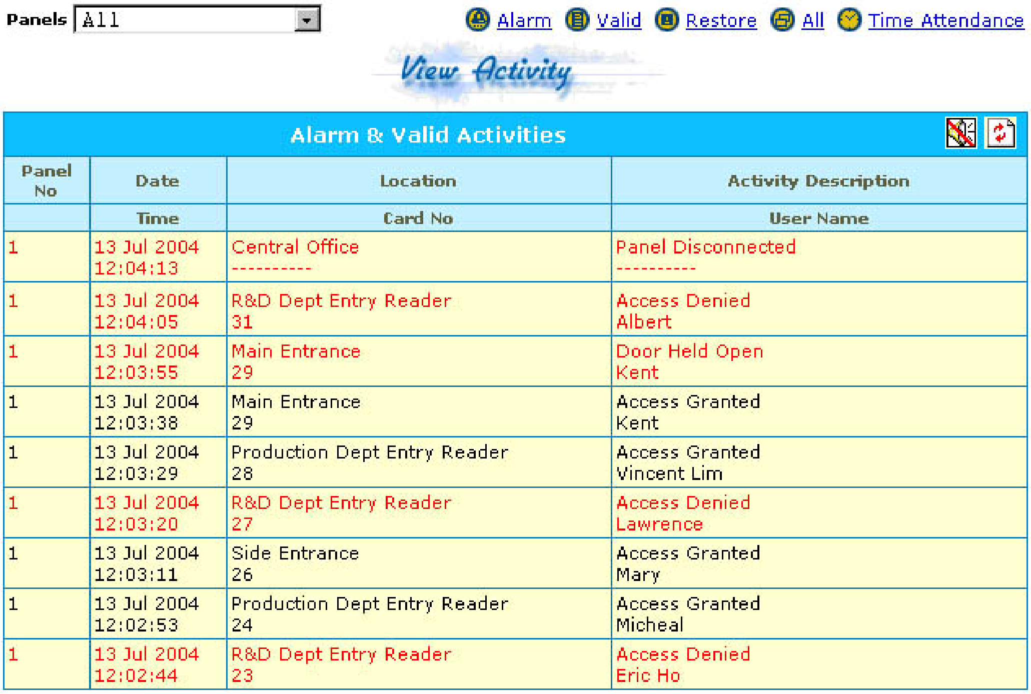
Notice!
The transactions are sorted by the alarm priority, and date and time. Alarms having the highest priority are shown at the top of the list. Alarms with the same priority will be sorted again by the date and time. Hence, the newest and highest priority alarm will always be shown at the top of the list. Please refer to *Alarm Priority Setup, page 96* for more details.

These are some of the view activity menu items explained in brief.

Options	Description
Alarm	To display only alarm transactions.
Valid	To display valid and alarm transactions.
Restore	To display restored and alarm transactions.
All	To display all transactions.
Time Attendance	To display only time clocking transactions.
☑	To acknowledge alarm transactions.
🔇	This will silence the audible tones on the Access Easy For Master.
🔊	This will enable the audible tones on Access Easy For Master.
Panels All ▾	To select an Access Easy Controller for which the user wants to view the activity only. We can view the activity for all the controllers or for selected controllers. This drop-down list will not be available in the **Alarm View**.

1. Login to Access Easy Master and the **View Activity** page appears, showing the alarm activities. This is the default page for **View Activity** menu.

2. To include valid transactions in **View Activity** page, click the Valid link. The screen will refresh and show valid and alarm activities.

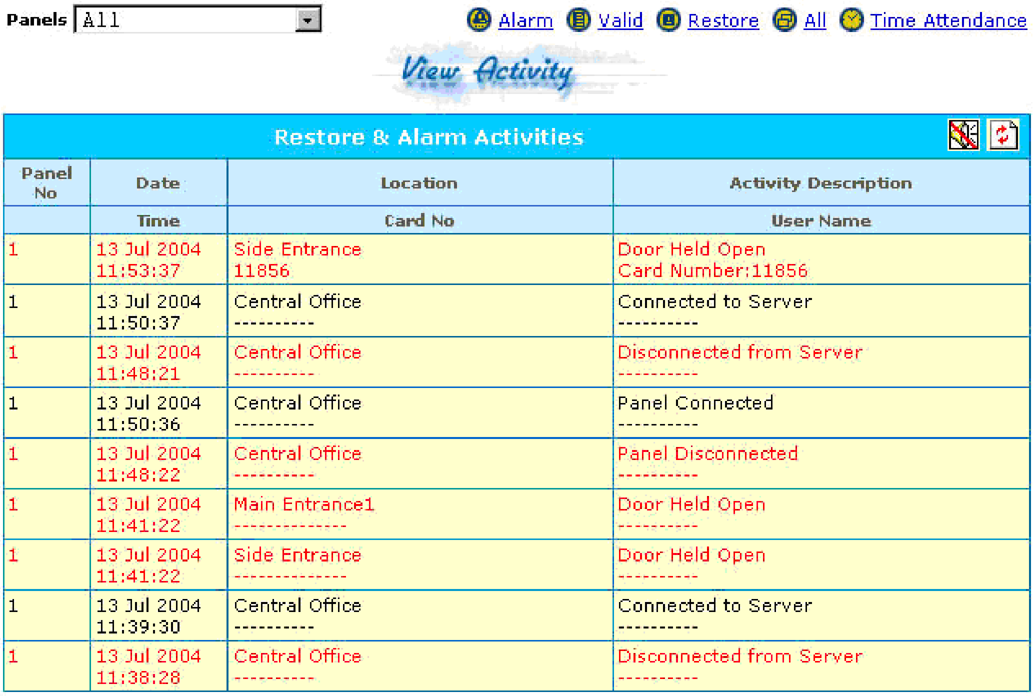


Panels: All

Alarm & Valid Activities

Panel No	Date Time	Location Card No	Activity Description User Name
1	13 Jul 2004 12:04:13	Central Office ----------	Panel Disconnected ----------
1	13 Jul 2004 12:04:05	R&D Dept Entry Reader 31	Access Denied Albert
1	13 Jul 2004 12:03:55	Main Entrance 29	Door Held Open Kent
1	13 Jul 2004 12:03:38	Main Entrance 29	Access Granted Kent
1	13 Jul 2004 12:03:29	Production Dept Entry Reader 28	Access Granted Vincent Lim
1	13 Jul 2004 12:03:20	R&D Dept Entry Reader 27	Access Denied Lawrence
1	13 Jul 2004 12:03:11	Side Entrance 26	Access Granted Mary
1	13 Jul 2004 12:02:53	Production Dept Entry Reader 24	Access Granted Micheal
1	13 Jul 2004 12:02:44	R&D Dept Entry Reader 23	Access Denied Eric Ho

3. To include restored transactions in the **View Activity** page, click the Restore link. The screen will refresh and show restored and alarm activities.

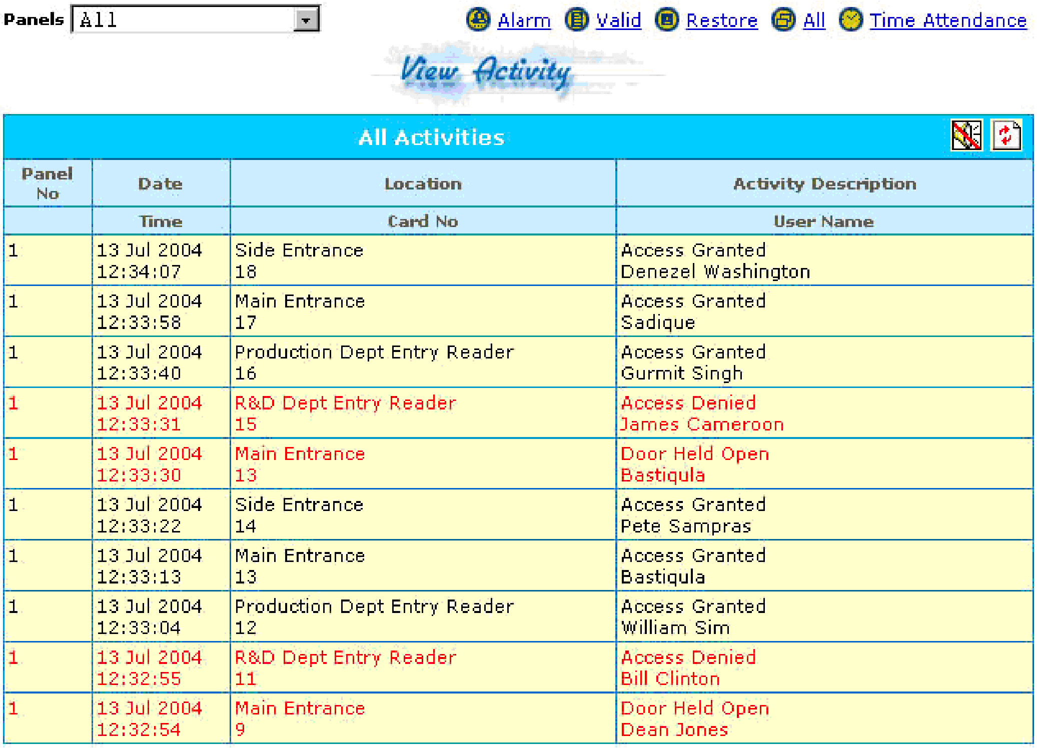


Panels: All

Restore & Alarm Activities

Panel No	Date Time	Location Card No	Activity Description User Name
1	13 Jul 2004 11:53:37	Side Entrance 11856	Door Held Open Card Number:11856
1	13 Jul 2004 11:50:37	Central Office ----------	Connected to Server ----------
1	13 Jul 2004 11:48:21	Central Office ----------	Disconnected from Server ----------
1	13 Jul 2004 11:50:36	Central Office ----------	Panel Connected ----------
1	13 Jul 2004 11:48:22	Central Office ----------	Panel Disconnected ----------
1	13 Jul 2004 11:41:22	Main Entrance1 --------------	Door Held Open ----------
1	13 Jul 2004 11:41:22	Side Entrance --------------	Door Held Open ----------
1	13 Jul 2004 11:39:30	Central Office ----------	Connected to Server ----------
1	13 Jul 2004 11:38:28	Central Office ----------	Disconnected from Server ----------

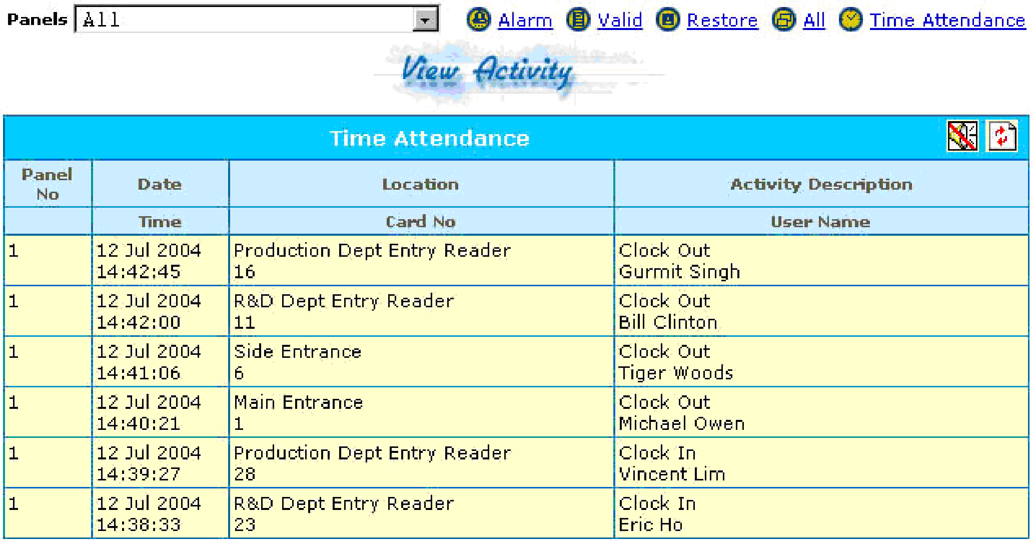
4. To show all activities, click the All link. The screen will refresh and show all the activities.


Panels All

All Activities

Panel No	Date	Location	Activity Description
	Time	Card No	User Name
1	13 Jul 2004 12:34:07	Side Entrance 18	Access Granted Denezel Washington
1	13 Jul 2004 12:33:58	Main Entrance 17	Access Granted Sadique
1	13 Jul 2004 12:33:40	Production Dept Entry Reader 16	Access Granted Gurmit Singh
1	13 Jul 2004 12:33:31	R&D Dept Entry Reader 15	Access Denied James Cameroon
1	13 Jul 2004 12:33:30	Main Entrance 13	Door Held Open Bastiqula
1	13 Jul 2004 12:33:22	Side Entrance 14	Access Granted Pete Sampras
1	13 Jul 2004 12:33:13	Main Entrance 13	Access Granted Bastiqula
1	13 Jul 2004 12:33:04	Production Dept Entry Reader 12	Access Granted William Sim
1	13 Jul 2004 12:32:55	R&D Dept Entry Reader 11	Access Denied Bill Clinton
1	13 Jul 2004 12:32:54	Main Entrance 9	Door Held Open Dean Jones

5. To show time attendance activities, click the Time Attendance link. The screen will refresh and show the time attendance activities.


Panels All

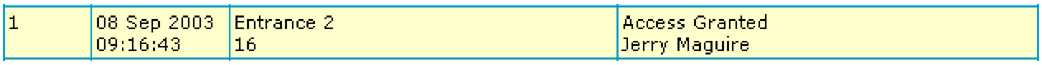
Time Attendance

Panel No	Date	Location	Activity Description
	Time	Card No	User Name
1	12 Jul 2004 14:42:45	Production Dept Entry Reader 16	Clock Out Gurmit Singh
1	12 Jul 2004 14:42:00	R&D Dept Entry Reader 11	Clock Out Bill Clinton
1	12 Jul 2004 14:41:06	Side Entrance 6	Clock Out Tiger Woods
1	12 Jul 2004 14:40:21	Main Entrance 1	Clock Out Michael Owen
1	12 Jul 2004 14:39:27	Production Dept Entry Reader 28	Clock In Vincent Lim
1	12 Jul 2004 14:38:33	R&D Dept Entry Reader 23	Clock In Eric Ho

5.1.2 How to Process Alarms/Events

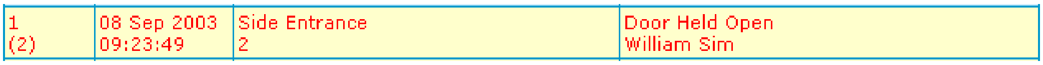
The **View Activity** page provides an easy color scheme to differentiate between new transactions, new alarms and acknowledged alarms.

– All new transactions have a yellow background. The new transactions will appear in the **View Activity** page in real-time mode.



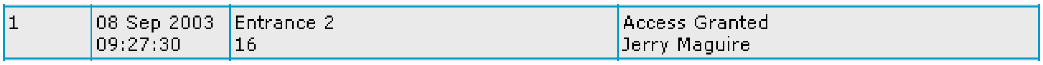
1	08 Sep 2003 09:16:43	Entrance 2 16	Access Granted Jerry Maguire

- All alarm transactions have red colored text wording while other transactions have black colored text wording.



1 (2)	08 Sep 2003 09:23:49	Side Entrance 2	Door Held Open William Sim

- When the web page refreshes automatically, the yellow background is replaced with grey background, except for alarm transactions, which remain unless the acknowledge button is activated.



1	08 Sep 2003 09:27:30	Entrance 2 16	Access Granted Jerry Maguire

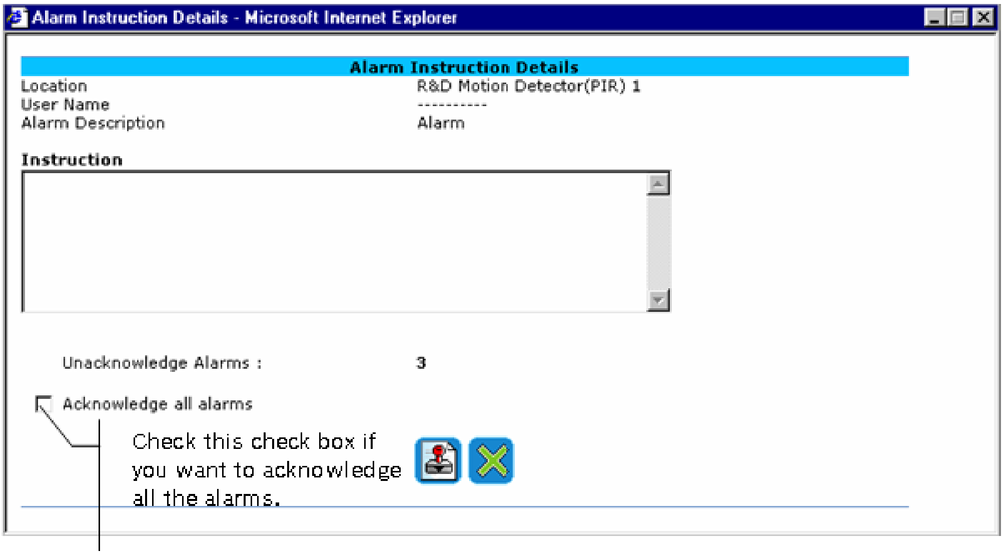
Process Event Transactions

New valid and restored transactions are shown in yellow background and black text. When the web page refreshes, the background changes from yellow to grey. Depending on the **View Activity Setting**, the screen is restricted to the number of transactions shown. However, unacknowledged alarms remain on the screen until they are acknowledged by the user.

Process Alarm Transactions

New alarms are shown in yellow background and red text. They will remain so until the user acknowledges the alarms. Refreshing the screen will not change the background to grey, as it does for valid and restored transactions.

User needs to acknowledge the alarm, by clicking on the button. This action will cause the **Alarm Instruction Details** window to appear as shown below. However, this button is only shown when the **View Activity** page is for alarm transactions. When viewing valid, restore, all or time attendance transactions, the button is not shown.



Alarm Instruction Details - Microsoft Internet Explorer

Alarm Instruction Details

Location	R&D Motion Detector(PIR) 1
User Name	----------
Alarm Description	Alarm

Instruction

Unacknowledge Alarms : 3

□ Acknowledge all alarms

Check this check box if you want to acknowledge all the alarms.

The screen above shows the alarm you are acknowledging and its pre-configured instruction message.

Notice!
Access Easy Master allows the user to configure instruction messages for different alarms. These instruction messages can be configured in *Alarm Instruction Message setup, page 102*.

6 Manual Control

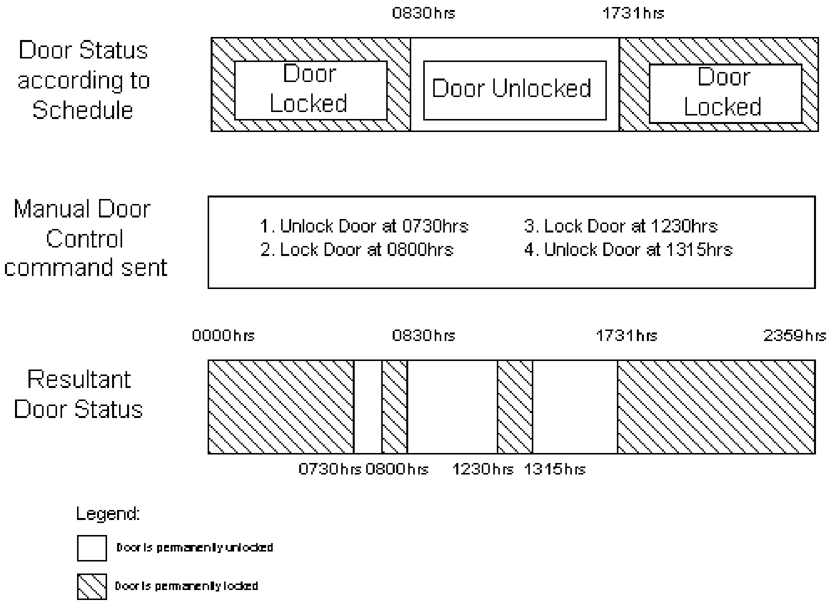
The **Manual Control** menu in Access Easy Master comprises of **Door Control**, **Input Control** and **Output Control.** Each control provides a method to easily modify and control any card reader, input or output points in the system. Each of the control will be discussed in detail in the following sections.

6.1 Door Control

The **Door Control** page allows the user to check the status of all the doors and send a command to either momentarily unlock, or permanently unlock or lock the door from remote.

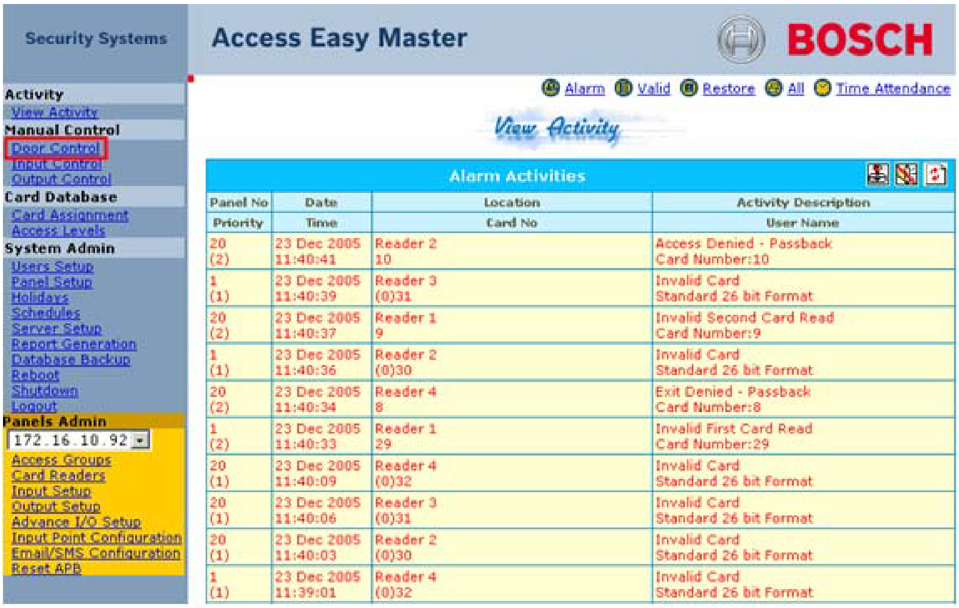
As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid schedule interval.

Here is 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 resumes normal operation according to schedule at 0830hrs and 1731hrs.

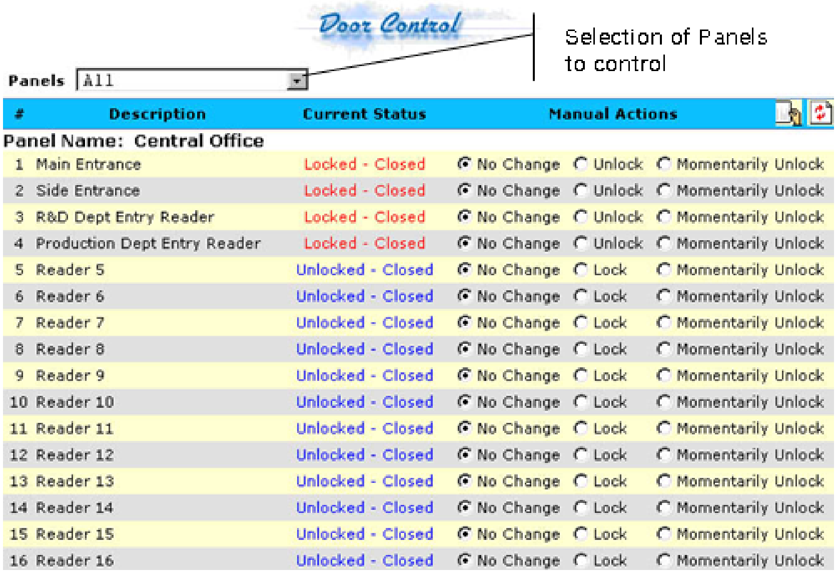
1. From the Access Easy Master main menu page, click on **Door Control** menu.



Alarm Activities

Panel No Priority	Date Time	Location Card No	Activity Description User Name
20 (2)	23 Dec 2005 11:40:41	Reader 2 10	Access Denied - Passback Card Number:10
1 (1)	23 Dec 2005 11:40:39	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:37	Reader 1 9	Invalid Second Card Read Card Number:9
1 (1)	23 Dec 2005 11:40:36	Reader 2 (0)30	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:34	Reader 4 8	Exit Denied - Passback Card Number:8
1 (2)	23 Dec 2005 11:40:33	Reader 1 29	Invalid First Card Read Card Number:29
20 (1)	23 Dec 2005 11:40:09	Reader 4 (0)32	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:06	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:03	Reader 2 (0)30	Invalid Card Standard 26 bit Format
1 (1)	23 Dec 2005 11:39:01	Reader 4 (0)32	Invalid Card Standard 26 bit Format

2. The **Door Control** screen appears.



Selection of Panels to control

Panels: All

#	Description	Current Status	Manual Actions
Panel Name: Central Office			
1	Main Entrance	Locked - Closed	● No Change ○ Unlock ○ Momentarily Unlock
2	Side Entrance	Locked - Closed	● No Change ○ Unlock ○ Momentarily Unlock
3	R&D Dept Entry Reader	Locked - Closed	● No Change ○ Unlock ○ Momentarily Unlock
4	Production Dept Entry Reader	Locked - Closed	● No Change ○ Unlock ○ Momentarily Unlock
5	Reader 5	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
6	Reader 6	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
7	Reader 7	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
8	Reader 8	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
9	Reader 9	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
10	Reader 10	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
11	Reader 11	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
12	Reader 12	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
13	Reader 13	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
14	Reader 14	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
15	Reader 15	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock
16	Reader 16	Unlocked - Closed	● No Change ○ Lock ○ Momentarily Unlock

The **Description** column provides the controller name and the door readers allocated to it.

The **Current Status** column provides us with the current door status, whether the door is “Locked - Closed”, “Locked - Opened", “Unlocked - Closed" or “Unlocked - Opened".

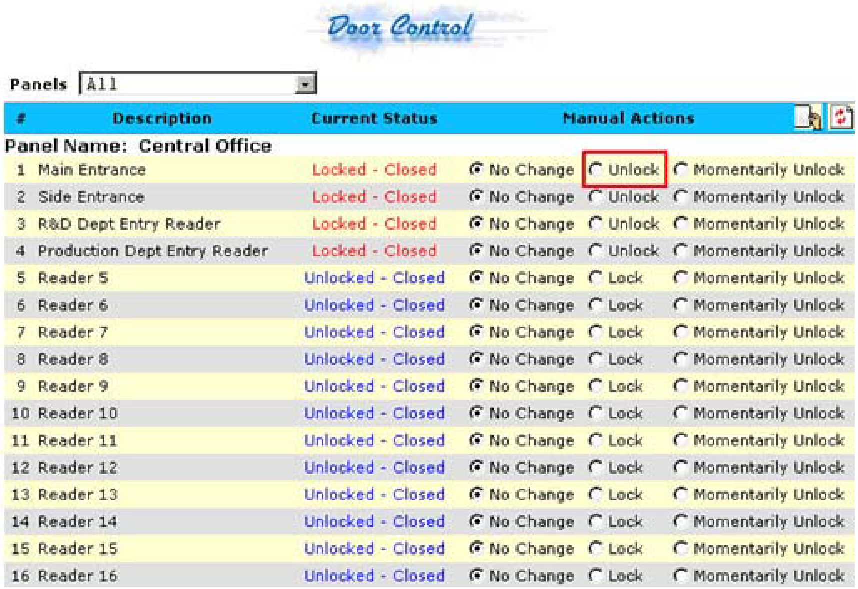
The **Manual Actions** column allows us to manually unlock the door if it is locked, and manually lock the door if it is unlocked. It also allows us to momentarily unlock the door. The momentarily unlock command will only work if the door is currently locked.

Notice!
Exit readers are not shown in the **Door Control** menu.

By default, all readers, except for exit readers, in the system will be shown on the screen. However, if you want to view a specific controller's readers, you can select them from Panels All ▾ drop-down list. You can select a controller from the list of all online controllers. This will refresh the screen only with readers from the selected controller.

6.1.1 How to Unlock Reader Controlled Door

1. To unlock a specific door for an extended period of time, click on the **Unlock** radio button.



Door Control

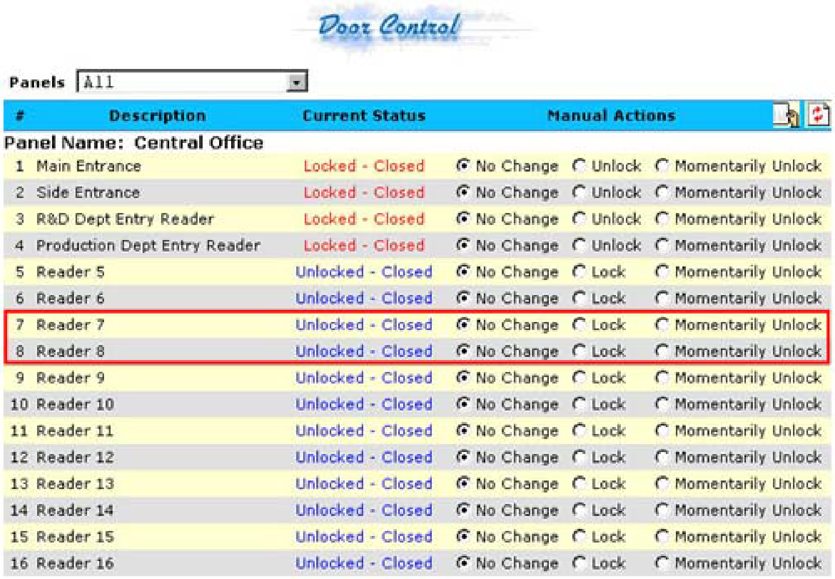
Panels All ▾

#	Description	Current Status	Manual Actions		
Panel Name: Central Office					
1	Main Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
2	Side Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
3	R&D Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
4	Production Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
5	Reader 5	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
6	Reader 6	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
7	Reader 7	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
8	Reader 8	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
9	Reader 9	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
10	Reader 10	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
11	Reader 11	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
12	Reader 12	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
13	Reader 13	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
14	Reader 14	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
15	Reader 15	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
16	Reader 16	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock

2. Click on icon to submit/send the command.

The selected door will now be unlocked. Cardholders can now pass through the door without presenting a card to the reader. The door will remain unlocked until they are relocked. At the same time that the door is unlocked, Access Easy Master will refresh the **Door Control** screen and update both the **Current Status** column, and the command radio buttons of the **Command Actions** column, so that they will be ready for the next command.

The following screen shows an example of the current status of two doors, named “Reader 7” and “Reader 8”, in “Unlocked - Closed” mode with the **Lock** radio button ready.

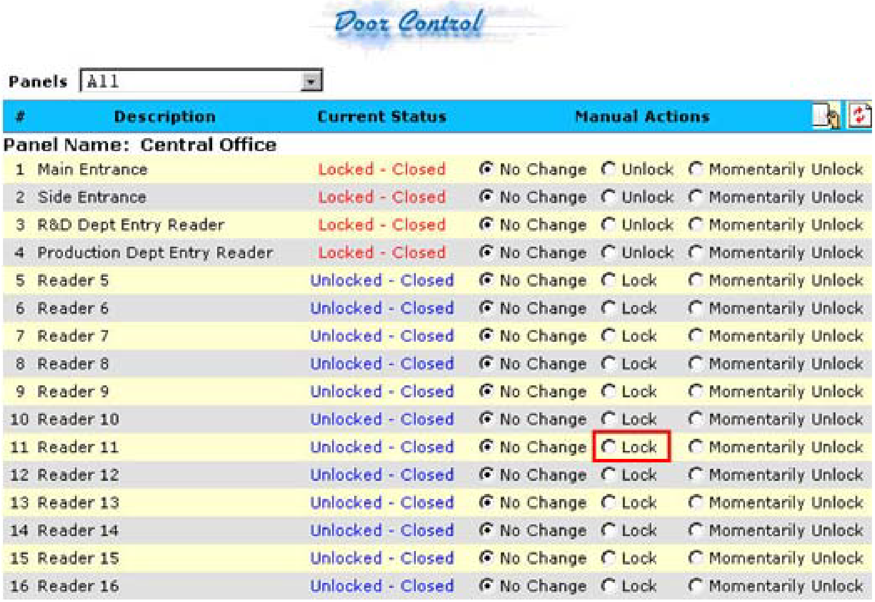


Panels All

#	Description	Current Status	Manual Actions		
Panel Name: Central Office					
1	Main Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
2	Side Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
3	R&D Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
4	Production Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
5	Reader 5	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
6	Reader 6	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
7	Reader 7	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
8	Reader 8	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
9	Reader 9	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
10	Reader 10	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
11	Reader 11	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
12	Reader 12	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
13	Reader 13	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
14	Reader 14	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
15	Reader 15	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
16	Reader 16	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock

6.1.2 How to Lock Reader Controlled Door

1. To lock a specific door for an extended period of time, click on the **Lock** radio button.



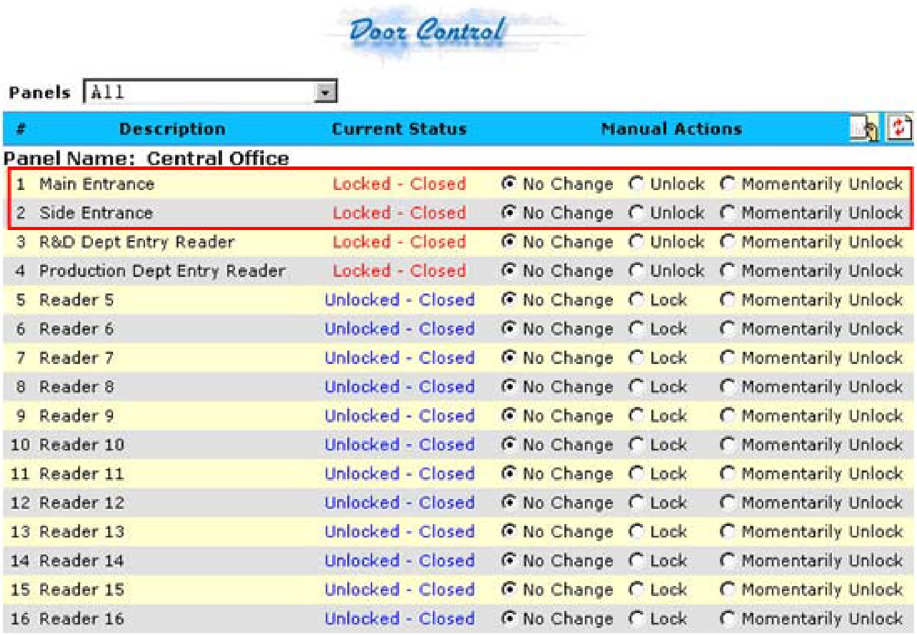
Panels All

#	Description	Current Status	Manual Actions		
Panel Name: Central Office					
1	Main Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
2	Side Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
3	R&D Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
4	Production Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
5	Reader 5	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
6	Reader 6	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
7	Reader 7	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
8	Reader 8	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
9	Reader 9	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
10	Reader 10	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
11	Reader 11	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
12	Reader 12	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
13	Reader 13	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
14	Reader 14	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
15	Reader 15	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
16	Reader 16	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock

2. Click on icon to submit/send the command.

The selected door will be locked immediately. Cardholders will now be required to present their card to the reader in order to pass through the door. At the same time that the door is locked, Access Easy Master will refresh the **Door Control** screen and update both the **Current Status** column and the command radio buttons of **Manual Actions** column, so that they will be ready for the next command.

The following screen shows an example of the current status of two doors, named “Main Entrance” and “Side Entrance”, in “Locked - Closed" mode with the **Unlock** radio button ready.



Door Control

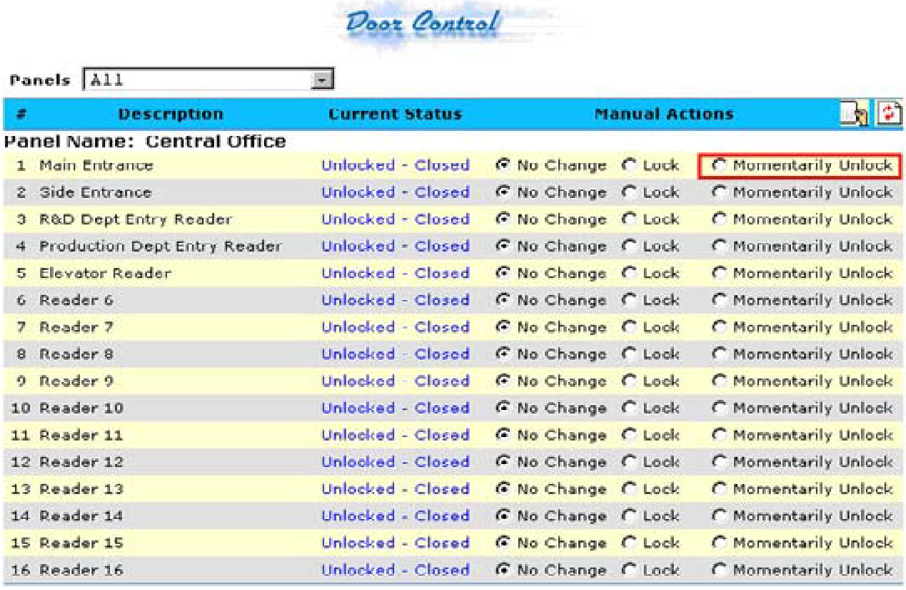
Panels: All

Panel Name: Central Office

#	Description	Current Status	Manual Actions		
1	Main Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
2	Side Entrance	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
3	R&D Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
4	Production Dept Entry Reader	Locked - Closed	● No Change	○ Unlock	○ Momentarily Unlock
5	Reader 5	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
6	Reader 6	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
7	Reader 7	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
8	Reader 8	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
9	Reader 9	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
10	Reader 10	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
11	Reader 11	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
12	Reader 12	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
13	Reader 13	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
14	Reader 14	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
15	Reader 15	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
16	Reader 16	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock

6.1.3 How to Momentarily Unlock Reader Controlled Door

1. To momentarily unlock a specific door, click on the **Momentarily Unlock** radio button.



Door Control

Panels: All

Panel Name: Central Office

#	Description	Current Status	Manual Actions		
1	Main Entrance	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
2	Side Entrance	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
3	R&D Dept Entry Reader	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
4	Production Dept Entry Reader	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
5	Elevator Reader	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
6	Reader 6	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
7	Reader 7	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
8	Reader 8	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
9	Reader 9	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
10	Reader 10	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
11	Reader 11	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
12	Reader 12	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
13	Reader 13	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
14	Reader 14	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
15	Reader 15	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock
16	Reader 16	Unlocked - Closed	● No Change	○ Lock	○ Momentarily Unlock

2. Click on icon to submit/send the command.

The selected door will unlock momentarily. The door will remain unlocked for the duration of the time specified in the reader configuration (usually 5 to 10 seconds). At the expiration of the unlock duration, the door will automatically relock.

Notice!
If you momentarily unlock a door, you will not be able to see its true status.

6.2 Input Control

The **Input Control** menu allows us to check the status of all the input points and whether they are assigned to specific alarm zones, and to send a command to manually arm or disarm the input point or zone. As this is a manual control, it has priority over the controls set by the system. However the system will take over once it encounters a valid schedule.

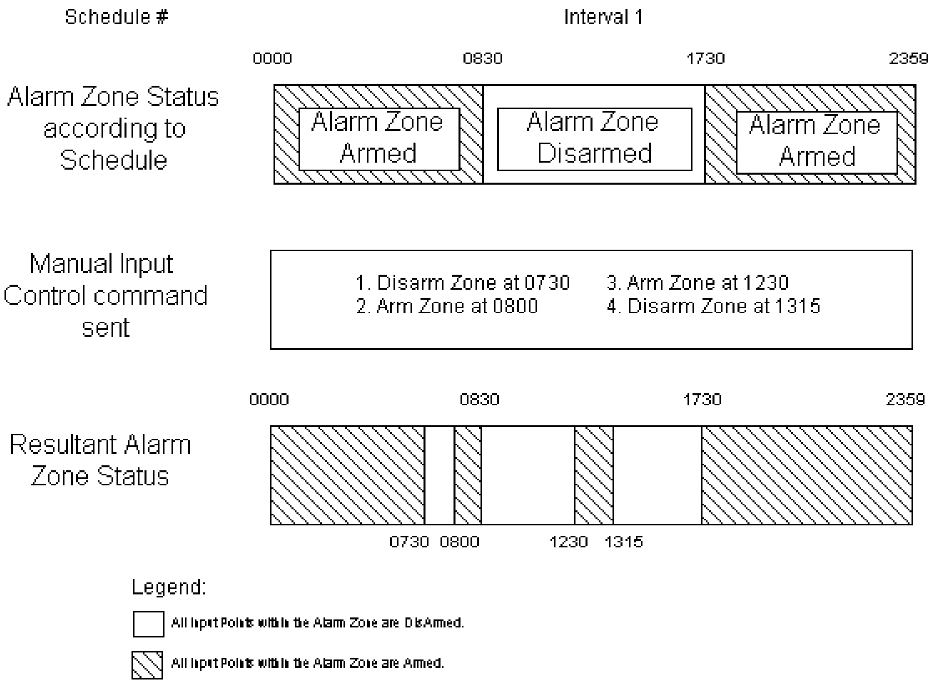
Devices that are usually monitored by input points are motion detectors, skylights, and temperature sensors. Besides monitoring the status of these input sensors, the **Input Control** screen provides an easy way for the user to arm or disarm these alarm points.

Disarming an alarm point is the same as turning it off. When an input point is disarmed, it no longer reports alarms to the **View Activity** screen.

Arming an alarm point means that you are turning it back on. When an input point is armed, monitoring of that point is re-enabled and events from the point will once again be reported to the **View Activity** screen.

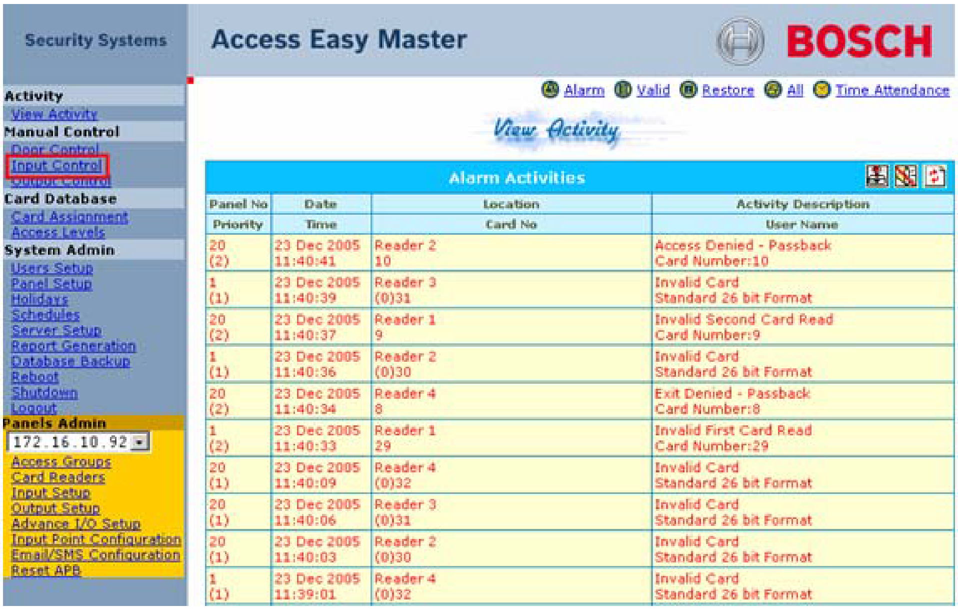
For configuration of system control, please refer to *Input Setup, page 141*.

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



Notice that the system resumes normal operation according to schedule at 0830hrs and 1731hrs.

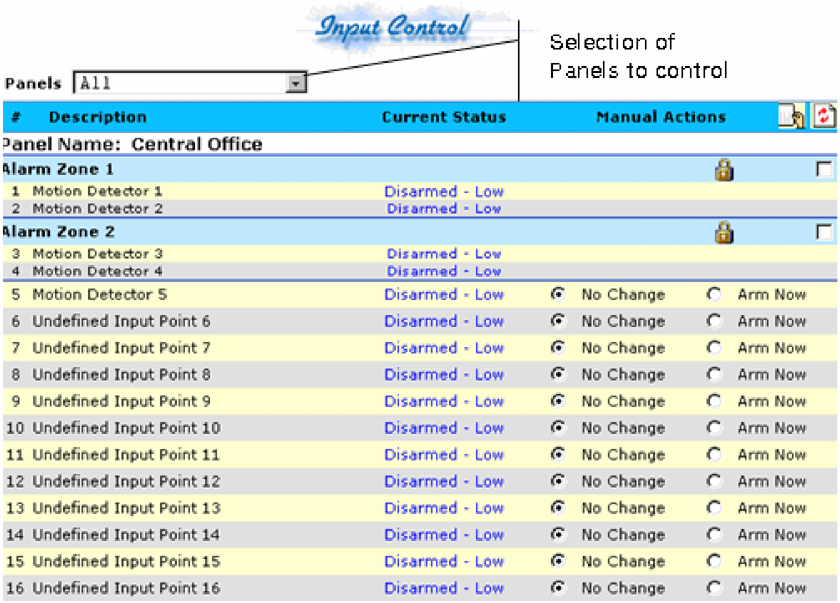
1. From the Access Easy Master main menu page, click on **Input Control** menu.



Alarm Activities

Panel No Priority	Date Time	Location Card No	Activity Description User Name
20 (2)	23 Dec 2005 11:40:41	Reader 2 10	Access Denied - Passback Card Number:10
1 (1)	23 Dec 2005 11:40:39	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:37	Reader 1 9	Invalid Second Card Read Card Number:9
1 (1)	23 Dec 2005 11:40:36	Reader 2 (0)30	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:34	Reader 4 8	Exit Denied - Passback Card Number:8
1 (2)	23 Dec 2005 11:40:33	Reader 1 29	Invalid First Card Read Card Number:29
20 (1)	23 Dec 2005 11:40:09	Reader 4 (0)32	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:06	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:03	Reader 2 (0)30	Invalid Card Standard 26 bit Format
1 (1)	23 Dec 2005 11:39:01	Reader 4 (0)32	Invalid Card Standard 26 bit Format

2. The **Input Control** screen appears.



Selection of Panels to control

Panels All

#	Description	Current Status	Manual Actions	
Panel Name: Central Office				
Alarm Zone 1				□
1	Motion Detector 1	Disarmed - Low		
2	Motion Detector 2	Disarmed - Low		
Alarm Zone 2				□
3	Motion Detector 3	Disarmed - Low		
4	Motion Detector 4	Disarmed - Low		
5	Motion Detector 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

The **Description** column provides grouping of the input point, if any. The blue horizontal strips are the alarm zones of which the input points belong to. The alarm zones are separated by a blue line. Independent input points do not belong to any alarm zones. In this case, “Input Point 1” and “Input Point 2” belong to “Alarm Zone 1”. “Input Point 3” and “Input Point 4” belong to “Alarm Zone 2” and “Input Point 5” is an independent input point.

The table below describes the possible grouping of the input points.

Alarm Zone 1	Input points in Alarm Zone 1 are displayed together. They are to be armed or disarmed together.
Alarm Zone 2	Input points in Alarm Zone 2 are displayed together. They are to be armed or disarmed together.

Alarm Zone 3	Input points in Alarm Zone 3 are displayed together. They are to be armed or disarmed together.
Alarm Zone 4	Input points in Alarm Zone 4 are displayed together. They are to be armed or disarmed together.
Independent Input Point	These are independent input points which can be armed or disarmed by itself.

The **Current Status** column provides us with the current status of the input points.

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 closed.
Disarmed - High	The respective input point is disarmed and its current status is open.
Alarm	An alarm is detected from the input point.
Alarm-Restored	The alarm has been restored so that the input point is no longer in alarm state.
Bypassed-Low	If the status of the input point is currently at Bypassed-High, after the input point contact is closed, it becomes Bypassed-Low.
Bypassed-High	The input point has been bypassed though the alarm zone is armed. This situation happens when the current status of the input point is open before the input point is armed.

For each alarm zone, there is a checkbox for selection to issue a command to the input points of the alarm zone.

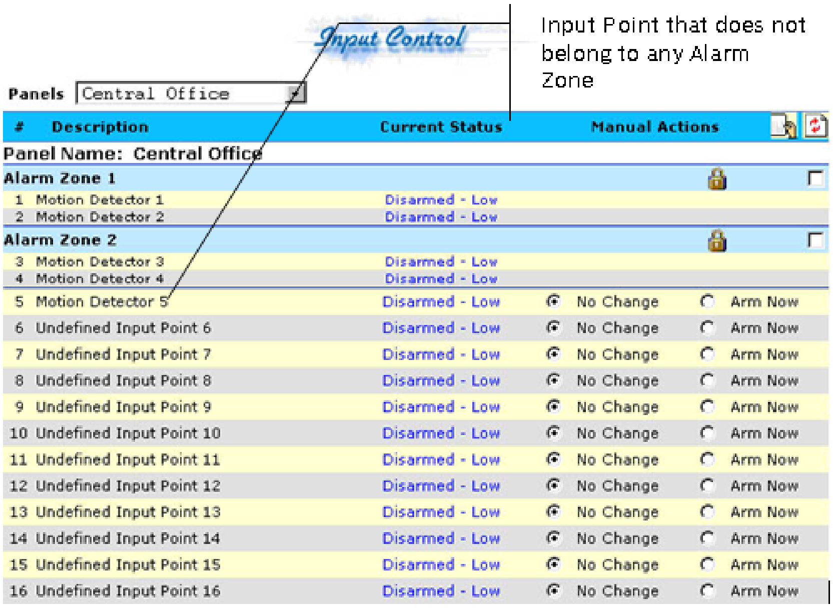
There are two types of action commands available:

🔒	This icon means that by selecting the check box, an arming command will be issued when submitted. Alternatively, click on the icon to arm the alarm zone.
🔓	This icon means that by selecting the check box, a disarming command will be issued when submitted. Alternatively, click on the icon to disarm the alarm zone.

By default, all the input points in the system will be shown on the screen. However, if you wish to view a specific controller's inputs, you can select it from Panels All drop-down list. The drop-down list consists of all the on-line controllers. Selecting a controller from the drop-down list will cause the screen to refresh with only the input points from the selected controller.

6.2.1 How to Arm or Disarm an Independent Input Point

These are input points that are not included in any of the alarm zones, nor is it controlled by schedule. They are independent input points that could be armed or disarmed by itself.



Input Point that does not belong to any Alarm Zone

Panels: Central Office

#	Description	Current Status	Manual Actions	
Panel Name: Central Office				
Alarm Zone 1				□
1	Motion Detector 1	Disarmed - Low		
2	Motion Detector 2	Disarmed - Low		
Alarm Zone 2				□
3	Motion Detector 3	Disarmed - Low		
4	Motion Detector 4	Disarmed - Low		
5	Motion Detector 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

1. Select the desired radio button from the **Manual Actions** column.
2. Click on the button to send the command. The web page will refresh to reflect the new status.

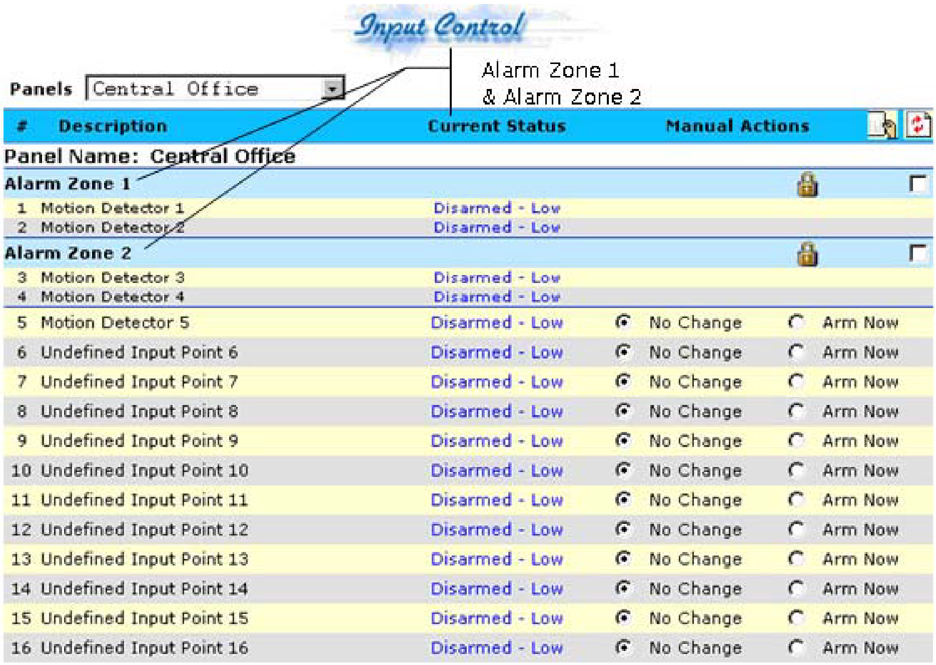
Notice!

If the current status of the input point is armed, the **Manual Actions** column will show the ○ Disarm Now radio button. This means that you can send a disarm command to this input by selecting the radio button and click the button. Likewise, if the input point is currently disarmed, the **Manual Actions** column will show the ○ Arm Now radio button.

6.2.2 How to Arm or Disarm an Alarm Zone

Input points can be grouped together if they are to be armed or disarmed together. This forms a group which is known as alarm zone. In each of the Access Easy Controller, up to four alarm zones are allowed. These alarm zones can be armed or disarmed by means of arming or disarming readers, or from the **Input Control** screen.

Access Easy Master consolidates all the alarm zones from each Access Easy Controller that is managed from a single screen. User can arm or disarm any alarm zone directly from this screen. The following screen shows an example of the **Input Control** screen with “Alarm Zone 1” and “Alarm Zone 2” from an Access Easy Controller called “Central Office”.



Input Control

Panels Central Office

#	Description	Current Status	Manual Actions	
Panel Name: Central Office				
Alarm Zone 1			🔒	□
1	Motion Detector 1	Disarmed - Low		
2	Motion Detector 2	Disarmed - Low		
Alarm Zone 2			🔒	□
3	Motion Detector 3	Disarmed - Low		
4	Motion Detector 4	Disarmed - Low		
5	Motion Detector 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

How to arm an alarm zone

The 🔒 icon indicates that the alarm zone is currently disarmed. Click on 🔒 to arm the alarm zone immediately.

How to disarm an alarm zone

The 🔓 icon indicates that the alarm zone is currently armed. Click on 🔓 to disarm the alarm zone immediately.

How to arm or disarm a group of alarm zones

If you want to arm or disarm multiple alarm zones, select the alarm zones selecting their respective checkboxes and clicking on the submit 📄 icon.

6.3 Output Control

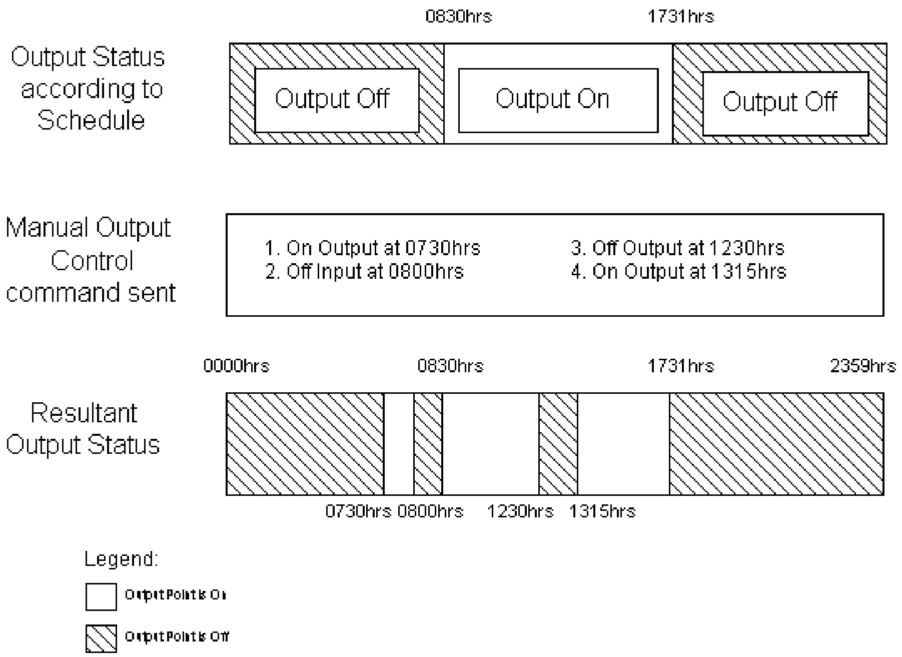
The **Output Control** is one of the menu items of the **Manual Control** group. It allows user to check the status of all the output points and send a command to turn the points on or off manually. However, if the output point is linked to an input point as a status output, the status will not be indicated here.

Devices that can be controlled by the output points are alarm bells, lighting circuits, electric garage door openers, and so on. Essentially, any device that can be turned on or off can be controlled from the **Output Control** screen.

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.

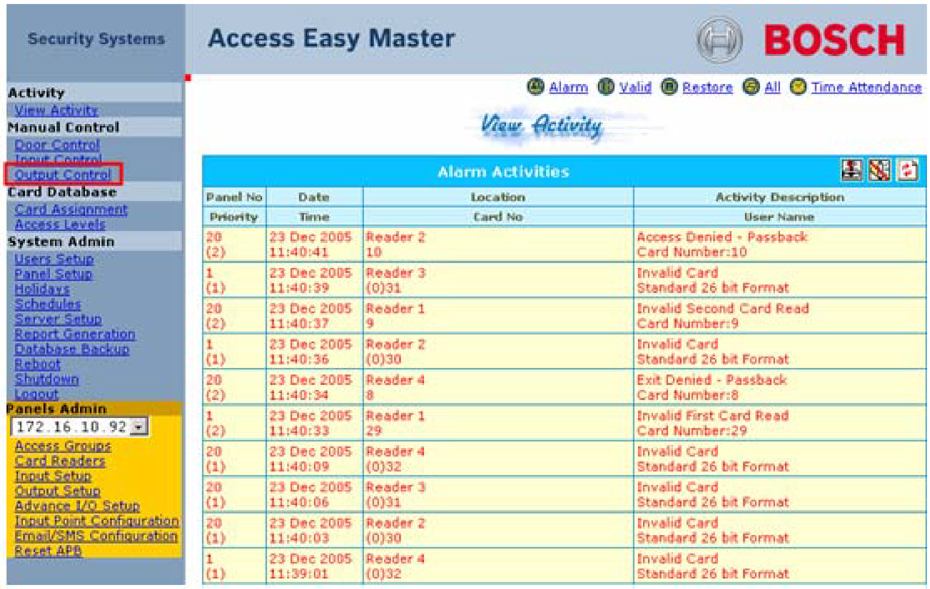
For configuration of system control, please refer to *Output Setup, page 146*.

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 resumes normal operation according to schedule at 0830hrs and 1731hrs.

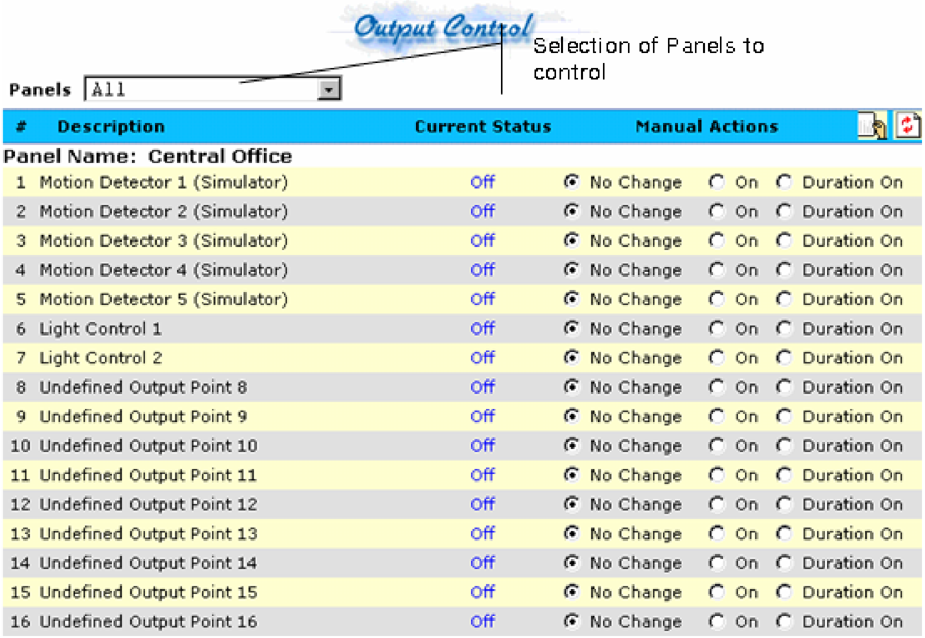
1. From the Access Easy Master main menu page, click on **Output Control** menu.



Alarm Activities

Panel No Priority	Date Time	Location Card No	Activity Description User Name
20 (2)	23 Dec 2005 11:40:41	Reader 2 10	Access Denied - Passback Card Number:10
1 (1)	23 Dec 2005 11:40:39	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:37	Reader 1 9	Invalid Second Card Read Card Number:9
1 (1)	23 Dec 2005 11:40:36	Reader 2 (0)30	Invalid Card Standard 26 bit Format
20 (2)	23 Dec 2005 11:40:34	Reader 4 8	Exit Denied - Passback Card Number:8
1 (2)	23 Dec 2005 11:40:33	Reader 1 29	Invalid First Card Read Card Number:29
20 (1)	23 Dec 2005 11:40:09	Reader 4 (0)32	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:06	Reader 3 (0)31	Invalid Card Standard 26 bit Format
20 (1)	23 Dec 2005 11:40:03	Reader 2 (0)30	Invalid Card Standard 26 bit Format
1 (1)	23 Dec 2005 11:39:01	Reader 4 (0)32	Invalid Card Standard 26 bit Format

2. The **Output Control** screen appears.



Output Control

Selection of Panels to control

Panels All

#	Description	Current Status	Manual Actions
Panel Name: Central Office			
1	Motion Detector 1 (Simulator)	Off	● No Change ○ On ○ Duration On
2	Motion Detector 2 (Simulator)	Off	● No Change ○ On ○ Duration On
3	Motion Detector 3 (Simulator)	Off	● No Change ○ On ○ Duration On
4	Motion Detector 4 (Simulator)	Off	● No Change ○ On ○ Duration On
5	Motion Detector 5 (Simulator)	Off	● No Change ○ On ○ Duration On
6	Light Control 1	Off	● No Change ○ On ○ Duration On
7	Light Control 2	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 **Description** column provides the controller name and the output points allocated to it.

The **Current Status** column provides us with the current status of the output points. The “On” status indicates that the output point is currently activated, and the “Off” status indicates that the output point is currently not activated.

The **Manual Actions** column provide us with radio button options for performing manual actions. There are four types of action command available:

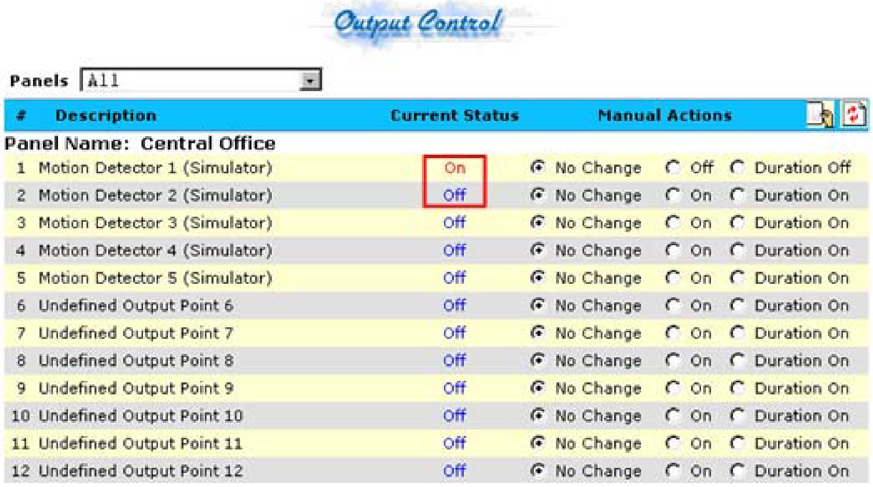
On	Selecting the radio button next to it will send a command to turn on the output point when submitted.
Off	Selecting the radio button next to it will send a command to turn off the output point when submitted.
Duration On	Selecting the radio button next to it will send a command to turn on the output point for a pre-defined duration when submitted.
Duration Off	Selecting the radio button next to it will send a command to turn off the output point for a pre-defined duration when submitted.

The predefined duration for the “**Duration On”** and “**Duration Off”** radio buttons is determined in the **Duration** field in *Output Setup, page 146*.

By default, all the outputs in the system will be shown on the screen. However, if you wish to view a specific controller's outputs, you could select it from the drop-down list. The drop-down list consists of all the on-line controllers. Selecting a controller from the drop-down list will cause the screen to refresh with only the output points from the selected controller.

6.3.1 How to Turn On or Off Output Points

1. To activate the selected output point, select ○ On or ○ Off radio button.



Output Control

Panels All

#	Description	Current Status	Manual Actions		
Panel Name: Central Office					
1	Motion Detector 1 (Simulator)	On	● No Change	○ Off	○ Duration Off
2	Motion Detector 2 (Simulator)	Off	● No Change	○ On	○ Duration On
3	Motion Detector 3 (Simulator)	Off	● No Change	○ On	○ Duration On
4	Motion Detector 4 (Simulator)	Off	● No Change	○ On	○ Duration On
5	Motion Detector 5 (Simulator)	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

2. Click on icon to submit the command.

Clicking on the icon will refresh the web page and reflect its new status.

Notice!

If the current status of the output point is “Off”, the **Manual Action** column will show the ○ On radio button, which means you can send a command to turn on this output when the button is clicked. Likewise, if the output point is currently “On”, the **Manual Action** column will show the ○ Off radio button.

7 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 additional fields for user to configure additional card information like department and user defined fields. **Card Assignment** consists of the following parameters:

Card Details

- Card Number
- Facility Code
- Card Format
- User Name
- Department
- User Field 1
- User Field 2
- Access Level

Card Functionality

- Whether cardholder is able to arm/disarm
- Whether cardholder must abide by holiday schedules
- Whether to allow exit reader usage only in accordance with time schedules
- Whether card + PIN is required on keypad readers
- Whether cardholder is “One Time Access” only, with the access status as valid or expired
- Setting of user PIN (1-7 digits)
- Setting of extended duration for door access
- Card validation dates
- Dual card assignment

Assignment of cards is done in the **Card Assignment** page. Click on **Card Assignment** from the main menu to see the list of currently configured cards.

In the Access Easy Master, cards that are added will be synchronized to all the online controllers at the moment the cards are added. If a new controller is connected to the Access Easy Master after the cards are added, user will have to manually synchronize the card database to the controller by clicking on the 👆 button for that controller, in the **Panel Setup** page. Please refer to *Panel Setup, page 70* for details.

Cards that are added allow its cardholder to access doors from different Access Easy Controllers that are managed by the Access Easy Master, provided the access levels, access groups and schedules are properly configured.

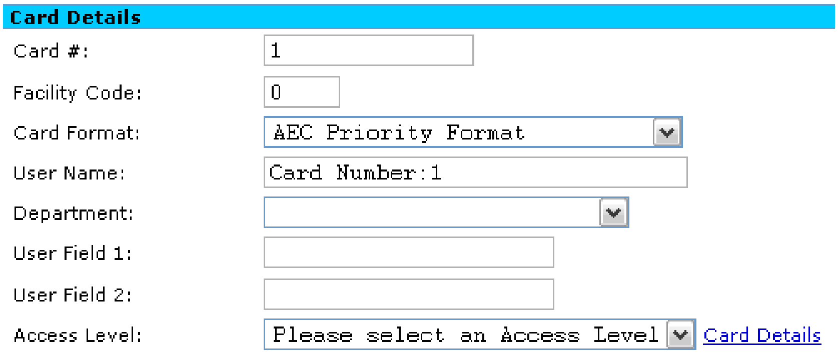
7.1 The Card Parameters

Each card has its own field that identifies its operation and usage. We will need to preconfigure these fields properly before it can be used by the cardholder.

The **Card Assignment** screen is divided into 2 sections, **Card Details** and **Card Functionality**. The **Card Details** section contain the settings to identify the card and the kind of access it has, while the **Card Functionality** section contain the settings of the operation and usage.

7.1.1 Card Details

Card Details section consist of the **Card #**, **Facility Code**, **Card Format**, **User Name**, **Department**, **Access Level** and two configurable (**User Field 1** and **User Field 2**) fields as shown below.



Card Details

Card #:	1
Facility Code:	0
Card Format:	AEC Priority Format
User Name:	Card Number:1
Department:	
User Field 1:	
User Field 2:	
Access Level:	Please select an Access Level Card Details

Card

This field contains the card number, the number that is printed on the card itself. Depending on the card format, this number could range from 1 to any number.

For example:
Standard 26 bit Wiegand format cards could only have a range of numbers from 0 to 65535.

Facility Code

This code prevents unauthorized card with the same card number to access your system. Some customers practice using a unique facility code that is controlled by the manufacturer. This gives additional security over the entire system. Ask your card supplier what is the facility code for your card. Without this code, the system will not be able to recognize your card. Similar to the card number, the range of numbers for this code is dependent on the card format used.

For example:
Standard 26 bit Wiegand format could have a range from 0 to 255.

Card Format

Access Easy Master is able to support up to a maximum of 15 user definable card formats. By default, “AEC Priority Format” and “Standard 26 bit Format” is pre-configured into the system. Refer to *Card Format, page 84* for details on the configuration of card formats.

User Name

This field contains the name of the cardholder.

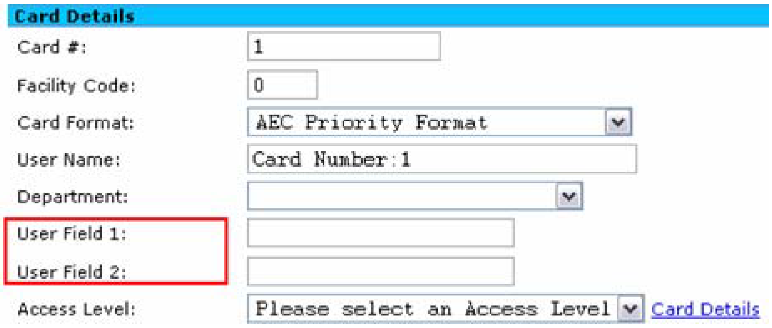
Department

This field contains the department in which the cardholder belongs to. Access Easy Master is able to support up to a maximum of 255 user definable departments. Refer to *How to Edit the Department List, page 89* for details on the configuration of departments.

User Field 1 and User Field 2

These two fields are user configurable fields, it can be configured to hold non operation data such as mobile number, home contact number, office extension number, destination, staff ID, and others. Refer to *How to Edit the User Definable Fields, page 92* for details on the configuration of **User Field 1** and **User Field 2**.

For example:
User Field 1 is configured as “Mobile number”.
User Field 2 is configured as “Home contact number”.
On the **Card Assignment** page, user will see **User Field 1** replaced by “Mobile number”, and **User Field 2** replaced by “Home contact number”, as shown below.



Card Details

Card #:	1
Facility Code:	0
Card Format:	AEC Priority Format
User Name:	Card Number:1
Department:	
User Field 1:	
User Field 2:	
Access Level:	Please select an Access Level Card Details

Access Level

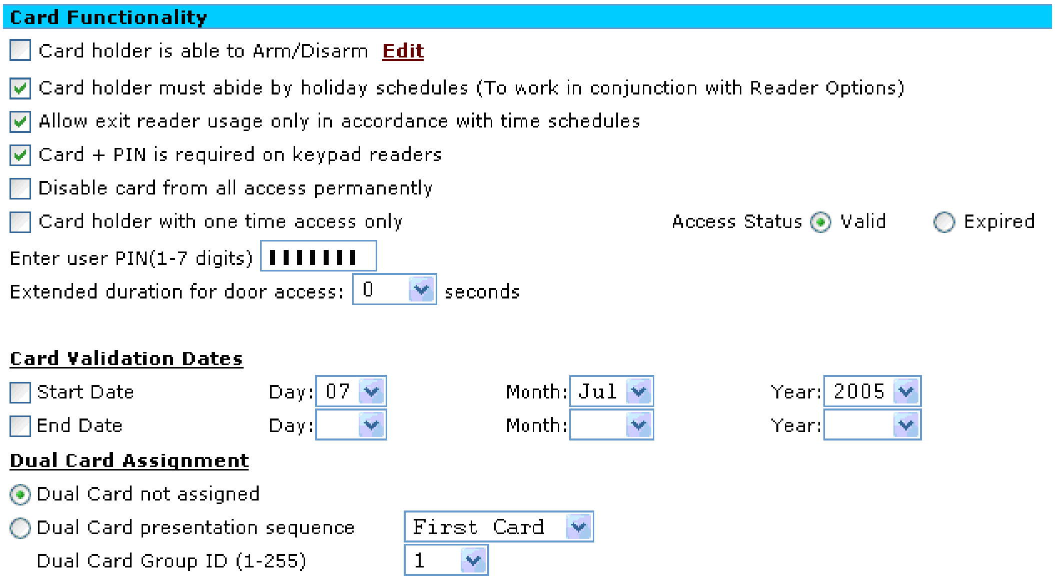
In order to control the accessibility of doors for each cardholder, an access level is assigned to each card. Each access level consists of one or more access group from different Access Easy Controllers. An access group is a list of readers within certain authorized time periods (predefined schedules) that the cardholders can access.

Access Easy Master has up to 1024 user definable access levels. Please refer to *Access Levels, page 64* for details on the configuration of access levels.

7.1.2 Card Functionality

Card Functionality consists of the arm/disarm access rights, access behavior, validation dates and dual card assignment status. Each card can be configured to behave differently.

However, some settings would only be activated with the coordination of the **Card Readers** parameters such as “Card + PIN” mode and cardholder must abide by holiday schedules. The screen below shows the card functionality for a user.



Card Functionality

☐ Card holder is able to Arm/Disarm **Edit**

☑ 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 + PIN is required on keypad readers

☐ Disable card from all access permanently

☐ Card holder with one time access only Access Status ● Valid ○ Expired

Enter user PIN(1-7 digits) IIIIIII

Extended duration for door access: 0 seconds

Card Validation Dates

☐ Start Date	Day: 07	Month: Jul	Year: 2005
☐ End Date	Day:	Month:	Year:

Dual Card Assignment

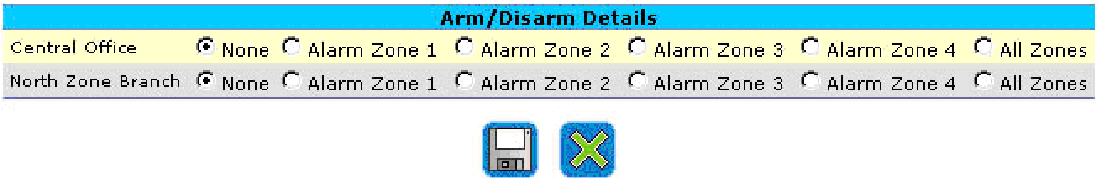
● Dual Card not assigned

○ Dual Card presentation sequence First Card

Dual Card Group ID (1-255) 1

Card holder is able to Arm/Disarm

If this option is checked, it implies that the cardholder is given the authority to arm/disarm a specific alarm zone or all alarm zones using his card on the zone's arm/disarm reader. To select an alarm zone, click on the **Edit** link Card holder is able to Arm/Disarm Edit. The arm/disarm details will appear as shown below.



Arm/Disarm Details

Central Office	● None	○ Alarm Zone 1	○ Alarm Zone 2	○ Alarm Zone 3	○ Alarm Zone 4	○ All Zones
North Zone Branch	● None	○ Alarm Zone 1	○ Alarm Zone 2	○ Alarm Zone 3	○ Alarm Zone 4	○ All Zones

Select the alarm zone that the cardholder can arm/disarm for each Access Easy Controller ("Central Office" and "North Zone Branch" in this case) by selecting the appropriate radio buttons and click 💾. If the cardholder can arm/disarm all the alarm zones, select the "All Zones" radio button. If not required, select the "None" radio button. To close the window, click ❎.

Notice!

If cardholder has access rights to the arm/disarm reader, he has to press <0> on the reader keypad before he presents his arm/disarm card, else reader will only grant him access. In addition, user will also be granted access at the moment he disarms the alarm zone at the reader if he has access rights to the arm/disarm reader.

The reader must be configured as an entry and arm/disarm reader for the specified zone before the cardholder can arm/disarm the alarm zone at the reader.

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

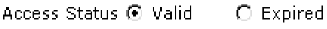
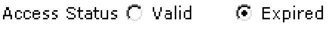
This option must be checked if the cardholders' access rights are different during holidays, either regular holidays or special holidays. This mode works in conjunction with the reader options, **On Holidays**, follow holiday schedules (to work in conjunction with card functionality). If the reader option is not checked, cardholders' access rights to the readers will follow the schedule for normal days of the week. Reader options can be configured under *Reader Options, page 126* of the selected Access Easy Controller menu.

Allow exit reader usage only in accordance with time schedules
This option is useful in case an exit reader is present. If you select this mode, the reader will allow the cardholders to exit within their schedule intervals. If this mode is not selected, the cardholders can exit at all times, regardless of holidays or schedules.

Card + PIN is required on keypad readers
When this option is selected, user will have to assign a PIN to the card in the **Enter user PIN (1-7 digits)** field. If this mode is selected, cardholders will have to present their card first before entering their PIN code to gain access at the reader before the keypad times out, which is configured in the page *Reader Options, page 126*.

Disable card from all access permanently
When this option is selected, user card will be denied access from the system. 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 option will enable the administrator to assign card holder 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, he needs to request the administrator to reactivate the one time access right again.

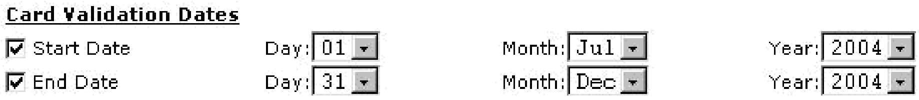
To enable this mode, check **Cardholder with one time access only** checkbox. Ensure that the valid radio button is selected for **Access Status**  Access Status ● Valid ○ Expired. After the card has been used for one time access, the access status will expire immediately and the **Access Status** field will be updated to **Expired**  Access Status ○ Valid ● Expired automatically.

Enter user PIN (1-7 digits)
User PIN is to be used together with the “Card + PIN” mode. This field will contain up to maximum 7 digit.

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 a handicapped person who needs longer time to access the door.

To select the extended time duration, select the time in seconds on the drop-down list 0 seconds beside the **Extended duration for door access** field. 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

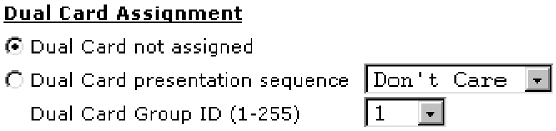
☑ End Date Day: 31 Month: Dec Year: 2004

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.

Notice!
User must check the respective **Start Date** or **End Date** checkboxes in order for it to be effective.

Dual Card Assignment

This option is useful if two cards are required to be presented in sequence to the reader to unlock the door. The first card has to be presented before the second card, otherwise 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 **Dual Card presentation sequence** radio button 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 drop-down list First Card ▾. User will also have to select the **Dual Card Group ID** from the drop-down list 1 ▾. Two 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 on the following page.

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

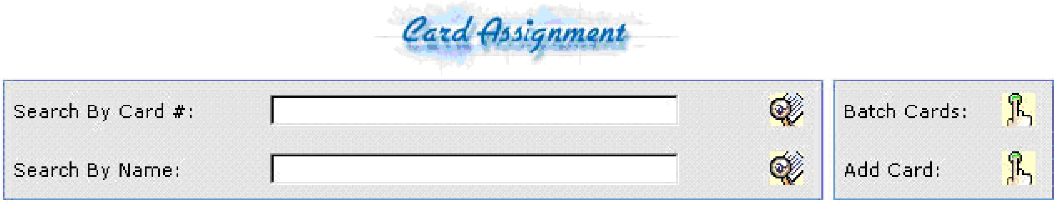
This mode works in conjunction with **Card Access Admin**, **Card Readers**, **Dual Card Configuration** of the Access Easy Controller. Please ensure that the setting in the Access Easy Controller is configured properly.

Notice!
For the first combination in the table above, the “Don't Care” cards must be two different cards from the same **Dual Card Group ID**.

7.2 Adding and Deleting Cards

This section will describe how to add a new card, how to add a batch of cards and how to delete a batch of cards. Under the section on how to add a batch of cards, user will also learn to add a batch of cards with reference to an existing card, how to automatically replace the existing card, and what happens during an unsuccessful card adding operation.

7.2.1 How to Add a New Card



Card Assignment

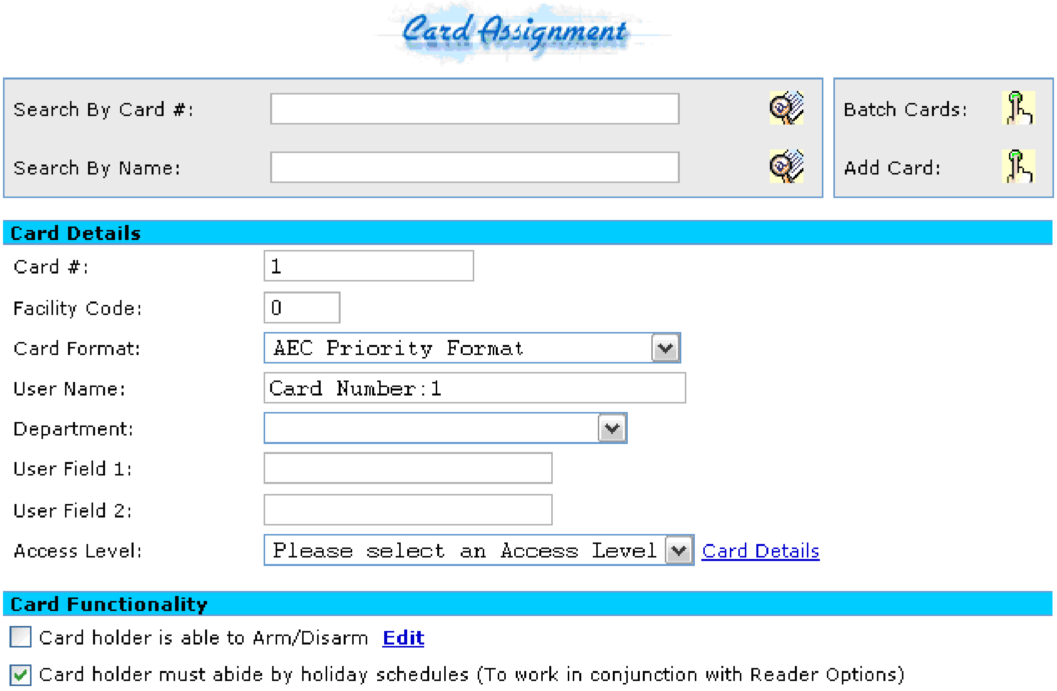
Search By Card #:

Search By Name:

Batch Cards:

Add Card:

In the **Card Assignment** screen, click on Add Card: to add a new card. The **Card Assignment** screen appears as shown below.



Card Assignment

Search By Card #:

Search By Name:

Batch Cards:

Add Card:

Card Details

Card #: 1

Facility Code: 0

Card Format: AEC Priority Format

User Name: Card Number:1

Department:

User Field 1:

User Field 2:

Access Level: Please select an Access Level Card Details

Card Functionality

□ Card holder is able to Arm/Disarm Edit

☑ Card holder must abide by holiday schedules (To work in conjunction with Reader Options)

Enter the information in the fields accordingly and click 💾 to save the settings. The functionality of each field is described in the previous section *The Card Parameters, page 42.*

Notice!

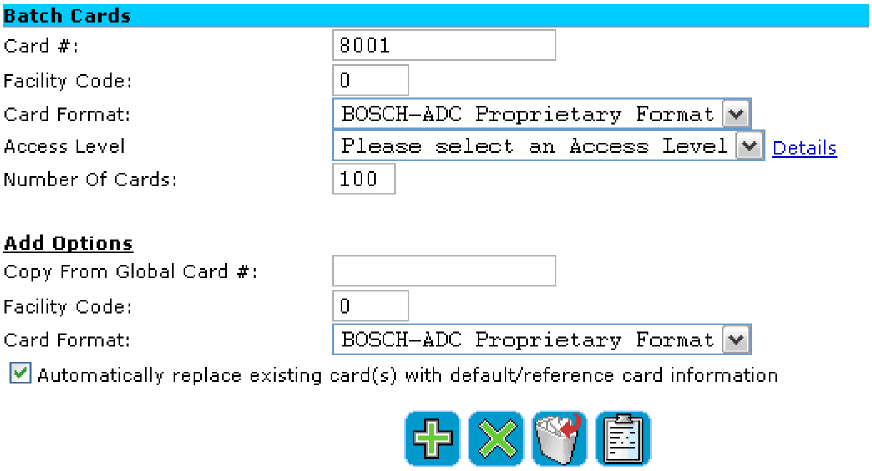
During an add card operation, when adding card numbers beginning with the digit “0”, for example “09”, the “0” digit will be truncated and the card number becomes “9”.

7.2.2 How to Add a Batch of Cards

In the **Card Assignment** screen, you are allowed to add a batch of cards in a single process. This is extremely useful when adding a large group of cardholders into the system within the shortest period of time. The following steps guide you how to perform this operation.

Let us take an example, presuming you need to add a batch of cards with the number ranging from “8001” to “8100”.

1. Click on the ☝ icon for **Batch Cards** section on the **Card Assignment** screen. The following screen shows the default settings when **Batch Cards** is selected.



Batch Cards

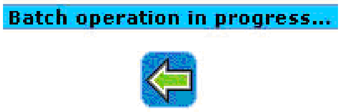
Card #:	8001
Facility Code:	0
Card Format:	BOSCH-ADC Proprietary Format
Access Level	Please select an Access Level Details
Number Of Cards:	100

Add Options

Copy From Global Card #:	
Facility Code:	0
Card Format:	BOSCH-ADC Proprietary Format

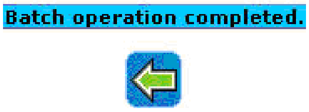
☑ Automatically replace existing card(s) with default/reference card information

2. Enter the starting card ID in the **Card #** field (the number specified here will be the starting number of the batch card operation and will be included). In this example, enter “8001”.
3. The number that appears in the **Facility Code** is configured in *Default Settings, page 92*. If the code is different from the default, then change it. Enter “0” if the card format doesn't support the facility code.
4. Select the appropriate format from the **Card Format** drop-down list. The configuration of the card format is done under *Card Format, page 84*. Only card formats that have been configured will appear in the drop-down list. By default, “BOSCH-ADC Proprietary Format” and “Standard 26 bit Format” is pre-configured into the system.
5. Select the access level for the card in the **Access Level** field. Only access levels that have at least one controller selected will appear in the **Access Level** drop-down list.
6. Enter the number of card(s) to add in the **Number Of Cards** field. For this example, enter “100”.
7. Click on the ✚ icon. When the add operation is in progress, a message as shown below appears.



Batch operation in progress...

8. If the operation is successful, a message “Batch operation completed” as shown below appears.



Batch operation completed.

9. Click on the icon to go back to the **Batch Cards** menu or wait for a few seconds for the screen to return to **Batch Cards** menu automatically.
10. Click on the icon to return to the first page of **Card Assignment** screen.

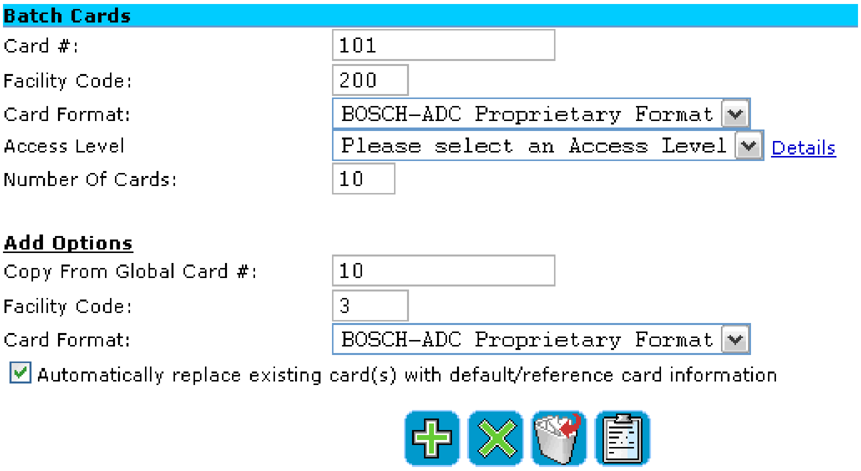
How to Add a Batch of Cards with Reference to an Existing Card

This function allows addition of a range of card numbers with data entries copied from a reference card number. All card number(s) added will be copied with the data or parameters of the reference card.

Notice!
Parameters such as facility code, card format, user name and access level will not be copied, as all these parameters relate to the individual cardholder.

Consider an example to assign cards with numbers from “101” to “110“ to certain staff. This range of cards has the facility code of “200” and of “Standard 26 bit Format” card format. Using card number “10” of facility code “3” and “BOSCH-ADC Proprietary Format” card format to be our reference card for the new card setting, we proceed as follows.

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



Batch Cards

Card #: 101
Facility Code: 200
Card Format: BOSCH-ADC Proprietary Format
Access Level: Please select an Access Level
Number Of Cards: 10

Add Options
Copy From Global Card #: 10
Facility Code: 3
Card Format: BOSCH-ADC Proprietary Format
☑ Automatically replace existing card(s) with default/reference card information

2. Click on the icon to proceed. If there is no error during the card numbers addition, the “Batch operation completed” message would be shown.

How to Use 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, facility code and card number) during **Batch Cards** function. It allows recycling of card number allocation when employee resigns.

The function will be activated when a check mark appears in **Automatically replace existing card(s) with default/reference card information** checkbox.

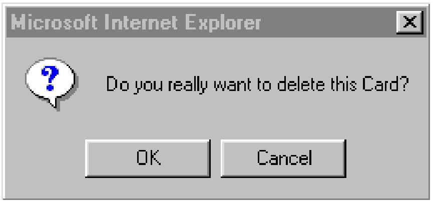
Unsuccessful Card Add Operation

There are a few occasion when the card add operation is not successful. When this occurs, the following messages will be displayed on the screen.

Card No already exist	An existing card with the same card number, facility code and card format is found in the system and **Automatically replace existing card(s) with default/reference card information** option is not selected. The system will not overwrite the existing card and the new card will not be added.
Reference card number not found	Reference card is not found in the database. It could be due to incorrect information in card format, facility code or card number.

7.2.3 How to Delete a Batch of Cards

1. You can delete a range of card numbers in a way similar to adding cards. Click on the 🗑 icon instead to delete card numbers.
2. A dialog box as shown below appears. Select the **OK** button to delete cards.



Microsoft Internet Explorer

Do you really want to delete this Card?

3. After the cards are successfully deleted, a “Batch operation completed” message appears.

Notice!

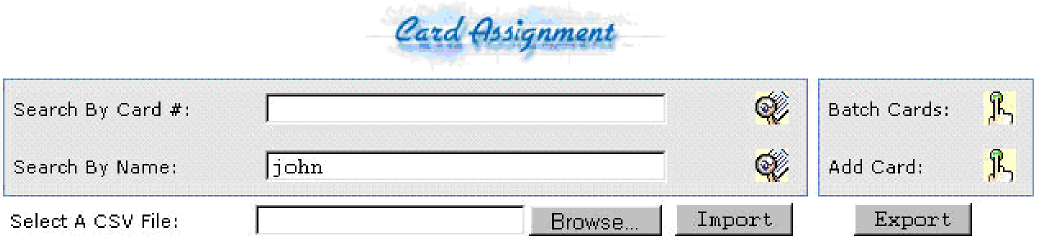
Deleting a range of cards is irreversible, so you have to be careful while deleting.

7.3 How to Import and Export Card Database

Card database can be exported in the CSV format to be stored in the user's PC. Users can then make changes to the file and import the amended file into the system.

7.3.1 How to Export the Card Database

1. On the first page of **Card Assignment** screen, click on the Export button located below the **Add Card** function, as shown below.



Card Assignment

Search By Card #:

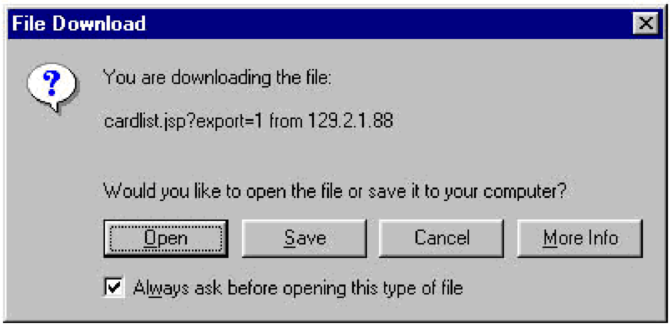
Search By Name: john

Batch Cards:

Add Card:

Select A CSV File:

2. The **File Download** dialog box appears, as shown below.



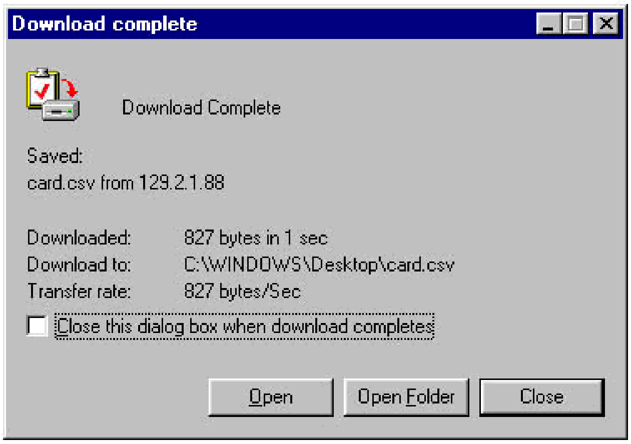
File Download

You are downloading the file:

cardlist.jsp?export=1 from 129.2.1.88

Would you like to open the file or save it to your computer?

3. Click on the **Save** button to save the card database to your computer, or the **Open** button to open the file.
4. Upon clicking the **Save** button, the **Download Complete** dialog box will appear, as shown below after the download is successful,



Download complete

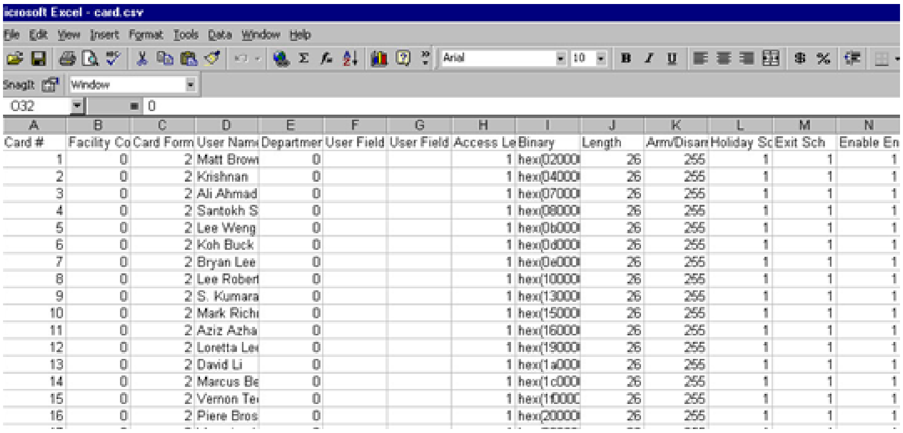
Download Complete

Saved:
card.csv from 129.2.1.88

Downloaded: 827 bytes in 1 sec
Download to: C:\WINDOWS\Desktop\card.csv
Transfer rate: 827 bytes/Sec

5. Click on the **Close** button to close the box, or the **Open** button to open the downloaded file.

A sample of the saved CSV file is shown as below.



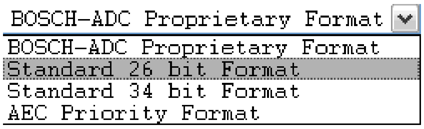
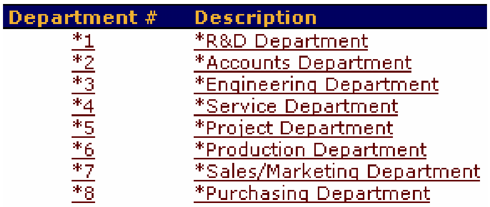
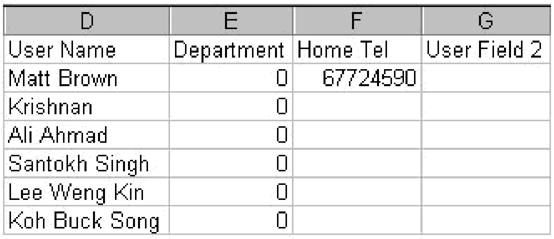
icrosoft Excel - card.csv
File Edit View Insert Format Tools Data Window Help
Arial
10
SnagIt
Window
O32
0

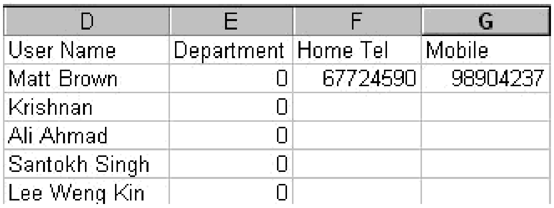
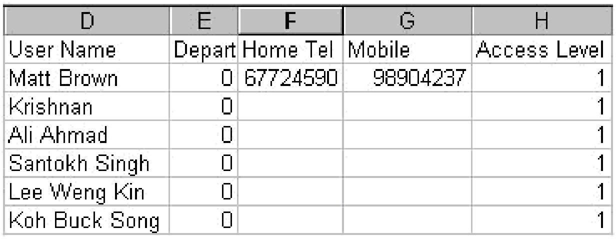
A	B	C	D	E	F	G	H	I	J	K	L	M	N
Card #	Facility Co	Card Form	User Nam	Departmer	User Field	User Field	Access Le	Binary	Length	Arm/Disan	Holiday Sc	Exit Sch	Enable En
1	0	2	Matt Brow	0			1	hex(02000	26	255	1	1	1
2	0	2	Krishnan	0			1	hex(04000	26	255	1	1	1
3	0	2	Ali Ahmad	0			1	hex(07000	26	255	1	1	1
4	0	2	Santokh S	0			1	hex(08000	26	255	1	1	1
5	0	2	Lee Weng	0			1	hex(0b000	26	255	1	1	1
6	0	2	Koh Buck	0			1	hex(0d000	26	255	1	1	1
7	0	2	Bryan Lee	0			1	hex(0e000	26	255	1	1	1
8	0	2	Lee Robert	0			1	hex(10000	26	255	1	1	1
9	0	2	S. Kumara	0			1	hex(13000	26	255	1	1	1
10	0	2	Mark Richi	0			1	hex(15000	26	255	1	1	1
11	0	2	Aziz Azha	0			1	hex(16000	26	255	1	1	1
12	0	2	Loretta Le	0			1	hex(19000	26	255	1	1	1
13	0	2	David Li	0			1	hex(1a000	26	255	1	1	1
14	0	2	Marcus Be	0			1	hex(1c000	26	255	1	1	1
15	0	2	Vernon Te	0			1	hex(1f000	26	255	1	1	1
16	0	2	Piere Bros	0			1	hex(20000	26	255	1	1	1

The file above is only an example of how the CSV file looks like. There are more fields than shown in the example above. For each of the field in the file saved, refer to the table below.

The following details are saved in the database:

Item	**Description**

<table>
<tr><td>Card Number</td><td>Limited to a length of 14 digits, consisting of 0 ~ 9.</td></tr>
<tr><td>Facility Code</td><td>The range of numbers for this code is dependent on the Card format used, up to a maximum of 5 digits.
For example:
Standard 26 bit Wiegand format could have a range from 0 to 255.</td></tr>
<tr><td>Card Format -</td><td>Can be “BOSCH-ADC Proprietary Format”, “Standard 26 bit Format” or any other format, configurable up to a total of 16 types of card formats, including the above two mentioned format. The number “2” in the <b>Card Format</b> column in the exported CSV file represents the second listed card format in Access Easy Master. In this example, “2” represents “Standard 26 bit Format”, as shown below.

BOSCH-ADC Proprietary Format
BOSCH-ADC Proprietary Format
Standard 26 bit Format
Standard 34 bit Format
AEC Priority Format</td></tr>
<tr><td>User Name</td><td>Limited to a length of 30 alphanumeric characters,</td></tr>
<tr><td>Department</td><td>Configurable up to 255 departments. The number “'0” in the <b>Department</b> column in the exported CSV file means that department is not selected for the cardholder. The number “1” means that the department is the first listed in Access Easy Master. In this example, the number “1” represents “R&D Department”, as shown below.

<table>
<tr><th>Department #</th><th>Description</th></tr>
<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>
</table></td></tr>
<tr><td>User Field 1</td><td>Limited to a length of 20 alphanumeric characters, including digits, alphabets, symbols such as # & [ ] and space. When <b>User Field 1</b> is configured as “Home Tel”, the heading <b>User Field 1</b> in the exported CSV file would appear as <b>Home Tel</b>. And for example, the <b>Home Tel</b> of Matt Brown is 67724590. 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>Matt Brown</td><td>0</td><td>67724590</td><td></td></tr>
<tr><td>Krishnan</td><td>0</td><td></td><td></td></tr>
<tr><td>Ali Ahmad</td><td>0</td><td></td><td></td></tr>
<tr><td>Santokh Singh</td><td>0</td><td></td><td></td></tr>
<tr><td>Lee Weng Kin</td><td>0</td><td></td><td></td></tr>
<tr><td>Koh Buck Song</td><td>0</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>User Field 2</td><td>Limited to a length of 20 alphanumeric characters, including digits, alphabets, symbols such as # & [ ] and space. When <b>User Field 2</b> is configured as “Mobile”, the heading <b>User Field 2</b> in the exported</td></tr>
</table>

<table>
<tr><td></td><td>CSV file would appear as <b>Mobile</b>. And for example, the <b>Mobile</b> of Matt Brown 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></tr>
<tr><td>User Name</td><td>Department</td><td>Home Tel</td><td>Mobile</td></tr>
<tr><td>Matt Brown</td><td>0</td><td>67724590</td><td>98904237</td></tr>
<tr><td>Krishnan</td><td>0</td><td></td><td></td></tr>
<tr><td>Ali Ahmad</td><td>0</td><td></td><td></td></tr>
<tr><td>Santokh Singh</td><td>0</td><td></td><td></td></tr>
<tr><td>Lee Weng Kin</td><td>0</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Access Level</td><td>Can be any of the 1024 access level. The number “1” in the <b>Access Level</b> column in the exported CSV file means that the first access level is selected. The number “1024” means that access level #1024 is selected. In this example, <b>Access Level</b> for Matt Brown is selected as the first access level, 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>Depart</td><td>Home Tel</td><td>Mobile</td><td>Access Level</td></tr>
<tr><td>Matt Brown</td><td>0</td><td>67724590</td><td>98904237</td><td>1</td></tr>
<tr><td>Krishnan</td><td>0</td><td></td><td></td><td>1</td></tr>
<tr><td>Ali Ahmad</td><td>0</td><td></td><td></td><td>1</td></tr>
<tr><td>Santokh Singh</td><td>0</td><td></td><td></td><td>1</td></tr>
<tr><td>Lee Weng Kin</td><td>0</td><td></td><td></td><td>1</td></tr>
<tr><td>Koh Buck Song</td><td>0</td><td></td><td></td><td>1</td></tr>
</table></td></tr>
<tr><td>Binary</td><td>The user can leave this field blank when he is entering data in the CSV file.</td></tr>
<tr><td>Length</td><td>User has to enter the length in the CSV file. Without this field, the card will not be imported into the system.
For example:
For “Standard 26 bit Format”, the length is “26”.</td></tr>
<tr><td>Arm/Disarm Zone</td><td>The number in the <b>Arm/Disarm Zone</b> column in the exported CSV file represents the alarm zone that the user can arm or disarm. The numbers representing the alarm zones are as follows:
1. Alarm Zone 1 - 0 - represented by 0
2. Alarm Zone 2 - 1 - represented by 1
3. Alarm Zone 3 - 2 - represented by 2
4. Alarm Zone 4 - 3 - represented by 3
5. All Alarm Zones - 5 - represented by 5
6. User cannot arm/disarm any alarm zone - 255</td></tr>
<tr><td>Holiday Schedule</td><td>The number “0” indicates that the <b>Cardholder must abide by holiday schedules (To work in conjunction with Reader Options)</b> checkbox is not checked. The number “1” indicates that the checkbox is checked.</td></tr>
<tr><td>Exit Sch</td><td>The number “0” indicates that the <b>Allow exit reader usage only in accordance with time schedules</b> checkbox is not checked. The number “1” indicates that the checkbox is checked.</td></tr>
<tr><td>Enable Enroll</td><td>The number “0” indicates that the <b>New enrolment for the reader schedules</b> checkbox is not checked. The number “1” indicates that the checkbox is checked.</td></tr>
</table>

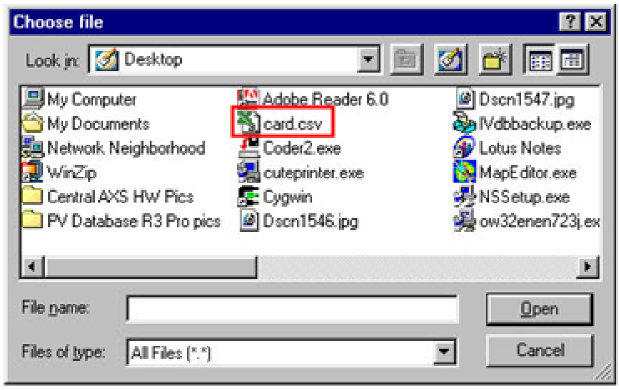
One Time Access	The number “0” indicates that the **Cardholder with one time access only** checkbox is not checked. The number “1” indicates that the checkbox is checked.
Card + PIN	The number “0”' indicates that the **Card + PIN is required on keypad readers** checkbox in Access Easy Master is not checked. The number “1” indicates that the checkbox is checked.
Extended	The number in the **Extended** column indicates the extended duration for door strike and keypad timeout. For example, the number “0” indicates that there is no extended duration for door strike and keypad timeout. The number “10” indicates that there is an extended duration of 10 seconds for door strike and keypad timeout for the cardholder.
Start Date	The number “0” indicates that the **Start Date** checkbox in Access Easy Master is not checked. The number “1” indicates that the checkbox is checked.
Year	The number in this **Year** column in the exported CSV file represents the year for the **Start Date** for the card to take effect.
Month	The number in this **Month** column in the exported CSV file represents the month for the **Start Date** for the card to take effect.
Day	The number in this **Day** column in the exported CSV file represents the day for the **Start Date** for the card to take effect.
End Date	The number “0” indicates that the **End Date** checkbox in Access Easy Master is not checked. The number “1” indicates that the checkbox is checked.
Year	The number in this **Year** column in the exported CSV file represents the year for the **End Date** for the card to cease being effective.
Month	The number in this **Month** column in the exported CSV file represents the month for the **End Date** for the card to cease being effective.
Day	The number in this **Day** column in the exported CSV file represents the day for the **End Date** for the card to cease being effective.
Dual Card Assignment	The number “0” indicates that the **Dual Card not assigned** radio button is not selected. The number “1” indicates that the **Dual Card presentation sequence** radio button is selected.
Dual Card Presentation Sequence	The number “0” indicates that “First Card” is selected for **Dual Card presentation sequence**, The number '1' indicates that “Second Card” is selected, and the number “2” indicates that “Don't Care” is selected.
Group ID	The number in the **Dual Card Group ID** column indicates the group ID the card falls into.
Card Pin	The number in the **Card PIN** column indicated the encrypted card PIN number. Default card PIN number is set at “1234000”.

Card Disabled	The number “0” indicates that user card is not disabled for access, The number “1” indicates user card is disabled from all access to the system permanently.

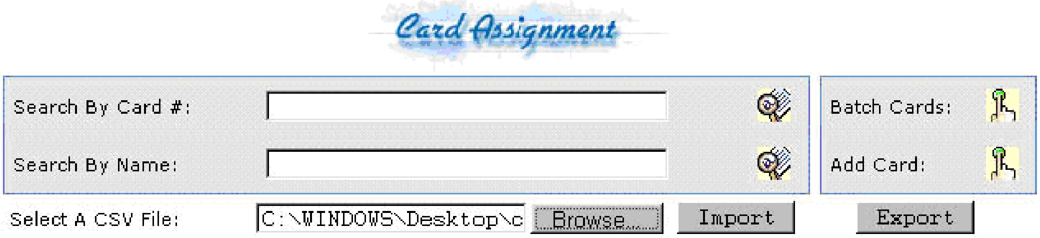
7.3.2 How to Import the Card Database

Sometimes, user may have a lot of changes to make or new cards to add before importing the card database into the system.

1. To import card database into the system, select a file to be imported by clicking on the Browse... button. The **Choose File** dialog box appears for user to choose the file to be imported, as shown below.

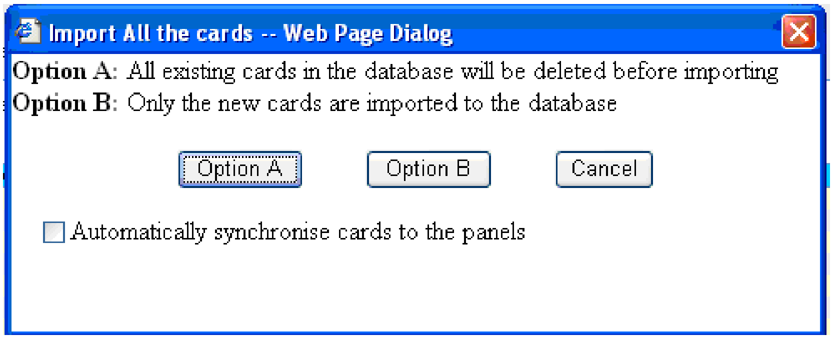


2. Select the file in CSV format to be imported to the system and click the **Open** button.
3. The file name and directory will appear in the **Select a CSV File** field as shown below.



Select A CSV File: C:\WINDOWS\Desktop\c

4. Click on the Import button to import the card database into the system. The window as shown below appears.



Option A: All existing cards in the database will be deleted before importing
Option B: Only the new cards are imported to the database

□ Automatically synchronise cards to the panels

5. There are 3 options that user can choose from:
Option A - When this option is selected, the existing database will be deleted before the new database are imported.
Option B - When this option is selected, only the new cards are imported to the database.
Cancel - Cancel the import function.

Notice!
If you wish to synchronize the new database to all the controllers, please check the **Automatically synchronise cards to the panels** checkbox first before clicking your desired option.

6. The card database will be imported into the system.

7.3.3 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.

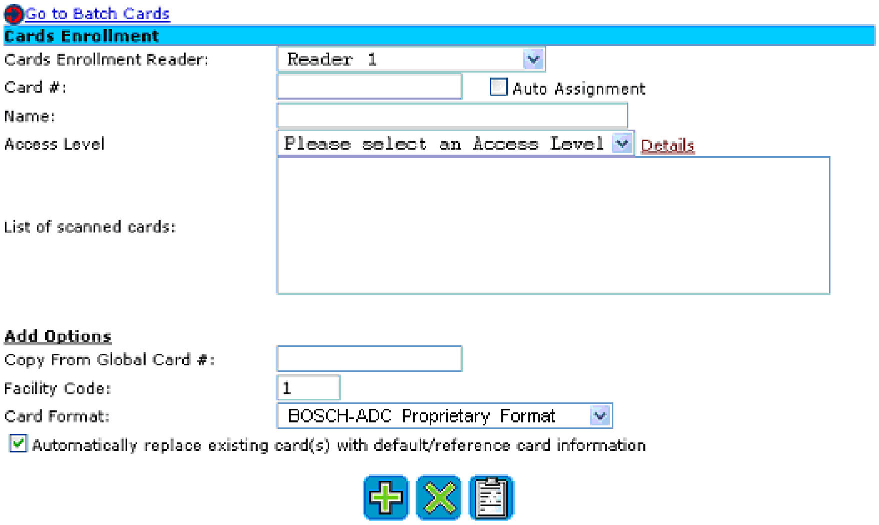
7.3.4 Card Enrolment of Card with Unknown Wiegand Format

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** menu from the left pane, followed by **Batch Cards** Batch Cards: at the top-right corner, and lastly select **Go to Cards Enrolment** Go to Cards Enrollment. The screen as shown below will appear.



Go to Batch Cards

Cards Enrollment

Cards Enrollment Reader: Reader 1

Card #: □ Auto Assignment

Name:

Access Level Please select an Access Level Details

List of scanned cards:

Add Options

Copy From Global Card #:

Facility Code: 1

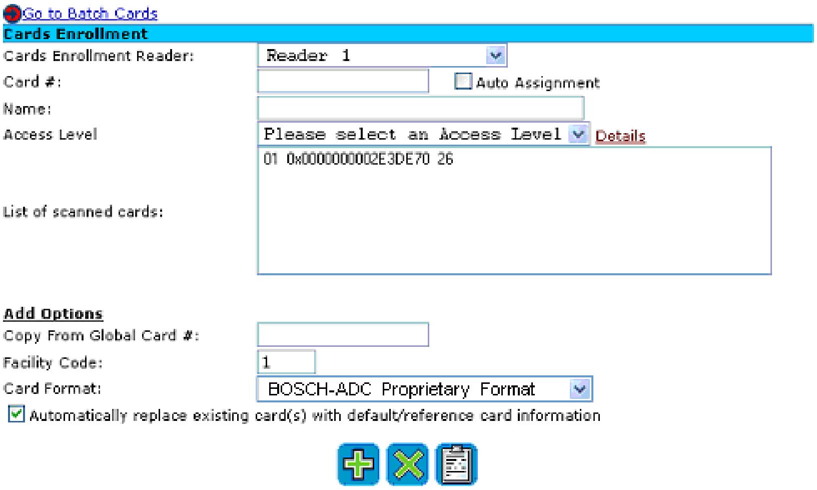
Card Format: BOSCH-ADC Proprietary Format

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

Select a reader to be the enrolment reader. In this example, we select “Reader 1” to be the enrolment reader.

2. Click on the ✚ button to activate the selected reader as the enrolment reader.

3. 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 **List of scanned cards** list box as shown in the screen below.



Go to Batch Cards

Cards Enrollment

Cards Enrollment Reader: Reader 1

Card #: □ Auto Assignment

Name:

Access Level: Please select an Access Level Details

List of scanned cards: 01 0x0000000002E3DE70 26

Add Options

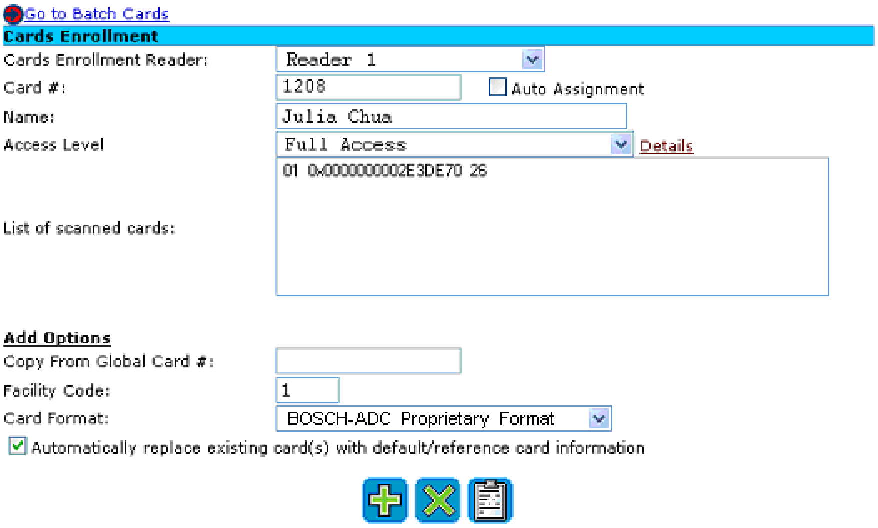
Copy From Global Card #:

Facility Code: 1

Card Format: BOSCH-ADC Proprietary Format

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

4. The administrator can now assign any card number, name and access level to the card. In the screen below, the **Card #** is assigned as “1208”, the **Name** of the cardholder as “Julia Chua” and the **Access Level** as “Full Access”. Refer to *Access Levels, page 64* for more details.



Go to Batch Cards

Cards Enrollment

Cards Enrollment Reader: Reader 1

Card #: 1208 □ Auto Assignment

Name: Julia Chua

Access Level: Full Access Details

List of scanned cards: 01 0x0000000002E3DE70 26

Add Options

Copy From Global Card #:

Facility Code: 1

Card Format: BOSCH-ADC Proprietary Format

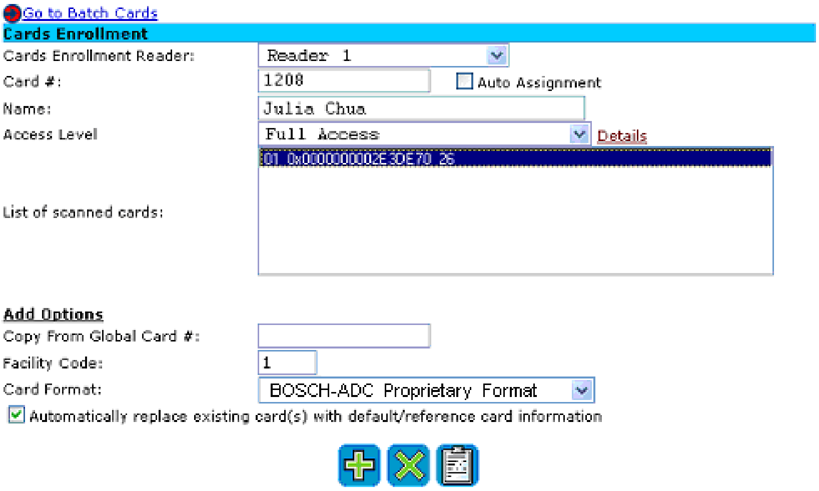
☑ Automatically replace existing card(s) with default/reference card information

Notice!

If you have a number of cards to enrol, for example 20 cards, you can select the auto assignment feature which will automatically increment the card number after you enrol the first card.

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.

5. Highlight the card in the **List of scanned cards** list box that you are assigning the card number and name to, as shown in the screen below.



Go to Batch Cards

Cards Enrollment

Cards Enrollment Reader:	Reader 1	
Card #:	1208	□ Auto Assignment
Name:	Julia Chua	
Access Level	Full Access	Details
List of scanned cards:	01 0x000000002E3DE70 26	

Add Options

Copy From Global Card #:	
Facility Code:	1
Card Format:	BOSCH-ADC Proprietary Format

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

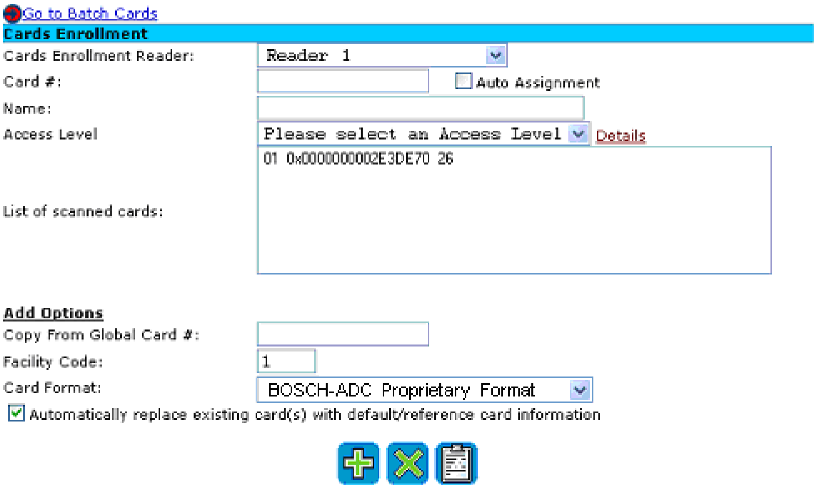
6. Click on the ✚ button to add the card with the assigned card number and name to the database.

Card Enrolment Using Pre-Assigned Enrolment Card

A pre-assigned enrolment card is a user card that has been checked with the **Card Holder Can Enable Enrolment Operation** option. For details on how to set a card to be a pre-assigned enrolment card, refer to the section 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** menu from the left pane, followed by **Batch Cards** Batch Cards: at the top-right corner, and lastly select **Go to Cards Enrolment** Go to Cards Enrollment. The screen as shown below will appear.



Go to Batch Cards

Cards Enrollment

Cards Enrollment Reader:	Reader 1	
Card #:		□ Auto Assignment
Name:		
Access Level	Please select an Access Level	Details
List of scanned cards:	01 0x000000002E3DE70 26	

Add Options

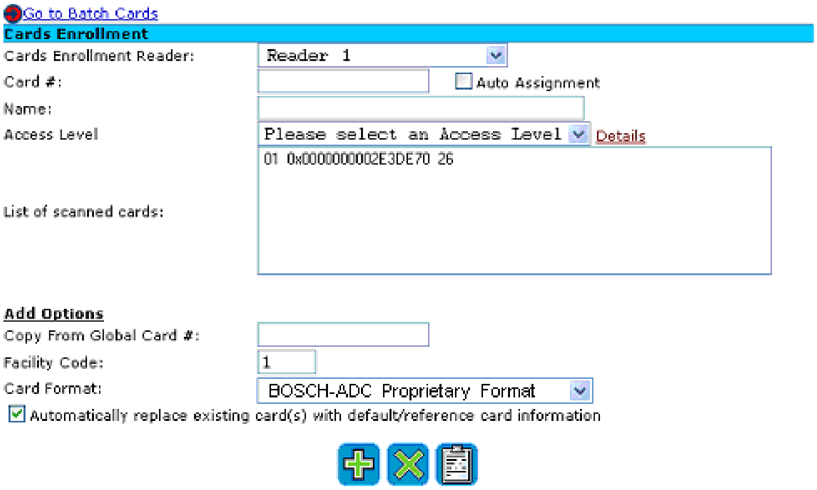
Copy From Global Card #:	
Facility Code:	1
Card Format:	BOSCH-ADC Proprietary Format

☑ Automatically replace 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 *Reader Options, page 126*.

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


Go to Batch Cards

Cards Enrollment

Cards Enrollment Reader:	Reader 1
Card #:	□ Auto Assignment
Name:	
Access Level	Please select an Access Level Details
List of scanned cards:	01 0x0000000002E3DE70 26

Add Options

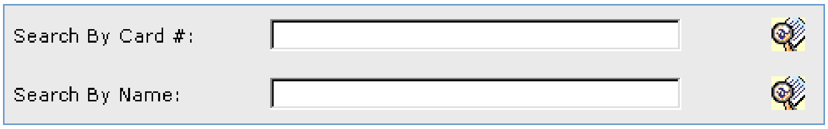
Copy From Global Card #:	
Facility Code:	1
Card Format:	BOSCH-ADC Proprietary Format

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

4. To add in the new card to the card database, refer to **Steps 5 to 6** in the **Card Enrolment Using Web Page** section above.

7.4 How to Use Search Function

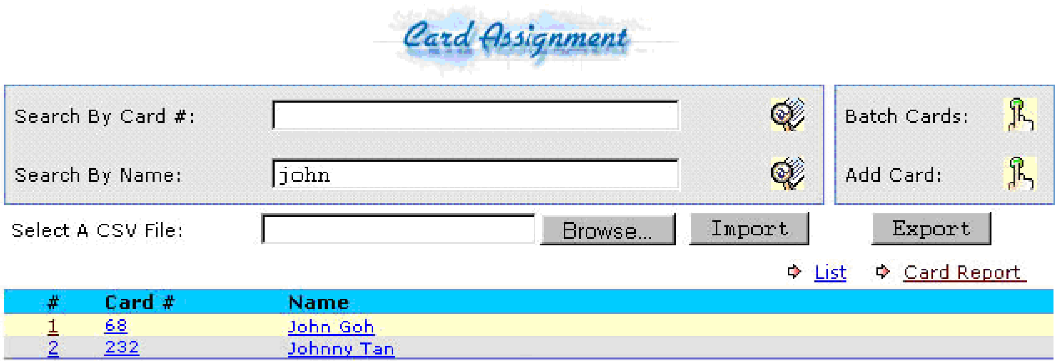
The **Card Assignment** menu allows us to search for cards by name or by card number.


Search By Card #:

Search By Name:

If you want to search by card number, you may enter the card number in the **Search By Card #** field. If you want to search by user name, enter the user name in the **Search By Name** field.

Let us consider an example. Suppose we want to search for a cardholder named “John”. The resultant screen will be as follows.


Card Assignment

Search By Card #:

Search By Name: john

Batch Cards:

Add Card:

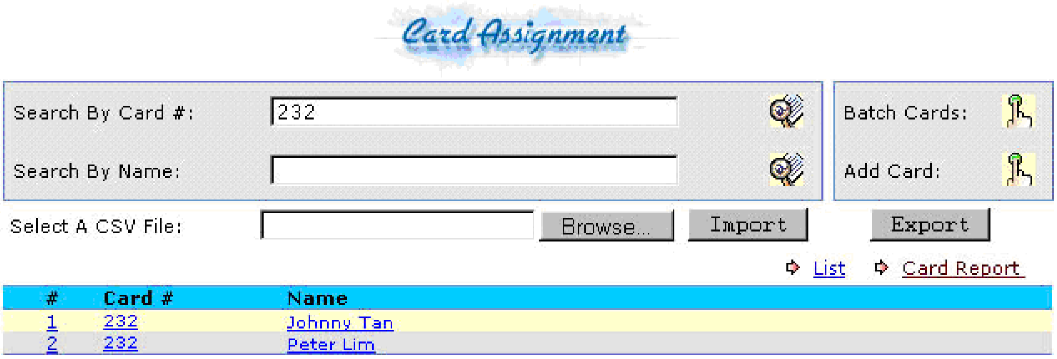
Select A CSV File: Browse... Import Export

List Card Report

#	Card #	Name
1	68	John Goh
2	232	Johnny Tan

Searching for a cardholder named “John” will display all users with “John” in their names. You can directly click on the user to go to the user details page.

Let us consider another example. Suppose we want to search for a card number “232”. The resultant screen will show card information of the search, as shown on the following page.



Search By Card #: 232

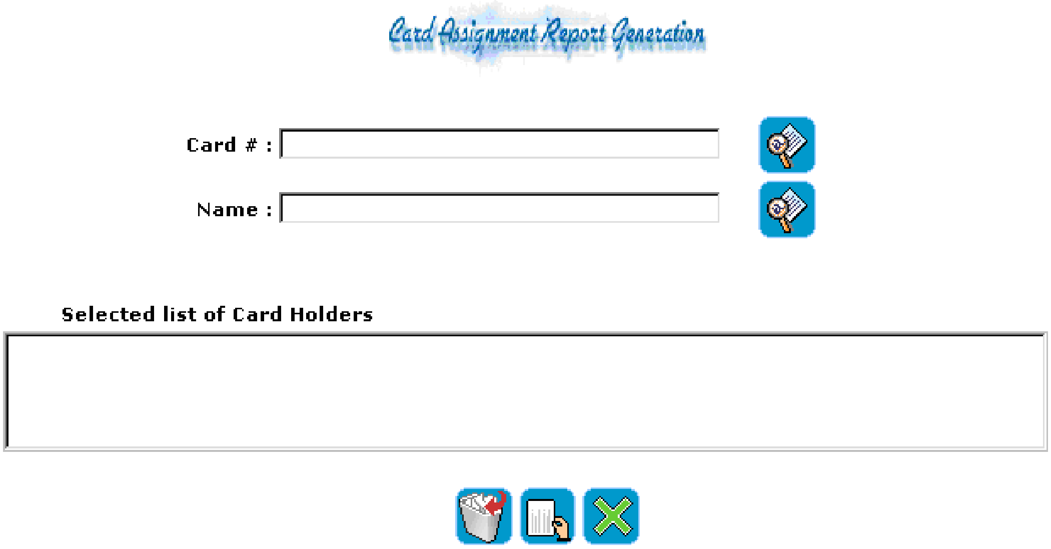
#	Card #	Name
1	232	Johnny Tan
2	232	Peter Lim

Searching for a card with card number “232” will display all cards with card number “232”. If the system has two or more cards with exactly the same card number, but with different card format or facility code, a list of user names will be listed for your selection.

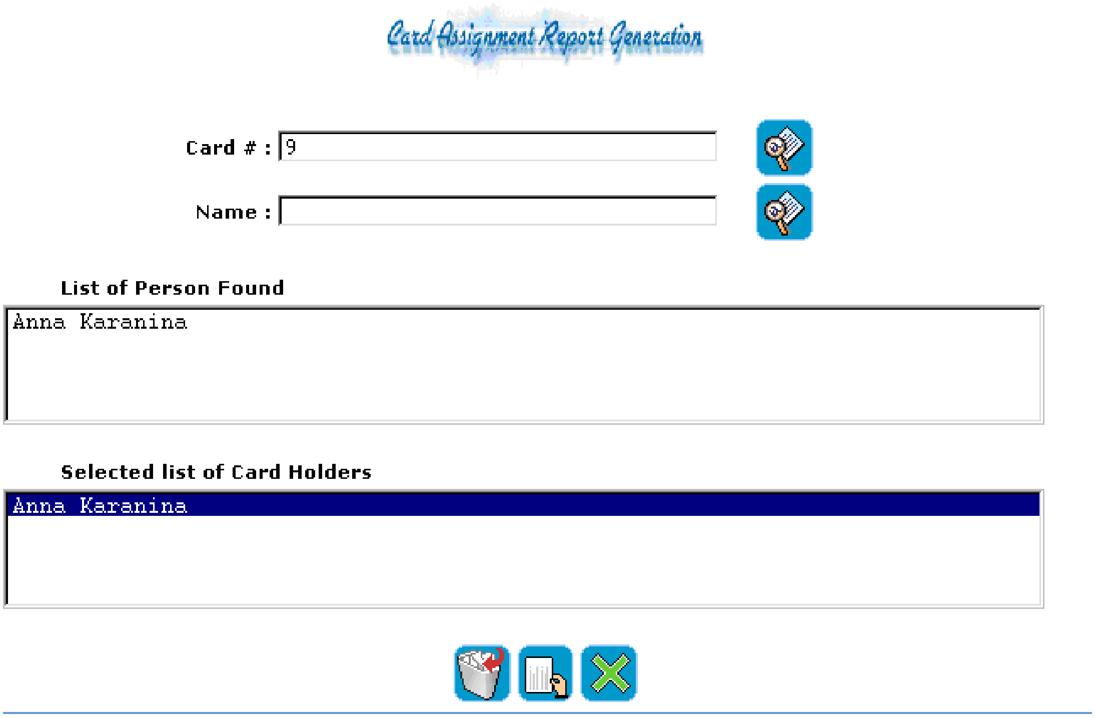
7.5 How to Generate Card Assignment Report

The **Card Assignment Report Generation** feature allows us to view a report on all or selected cardholders based on their name or their card number.

When we select on the **Card Report** link Card Report on the first page of **Card Assignment** screen, we will see a screen as shown below.


Card Assignment Report Generation
Card # :
Name :
Selected list of Card Holders

We may either search for a cardholder by card number or by name and add to the selected list of cardholders. When we perform a search by card number, you will see a screen as shown below. Let us assume that we are searching for a card number “9”.


Card Assignment Report Generation

Card # : 9

Name :

List of Person Found

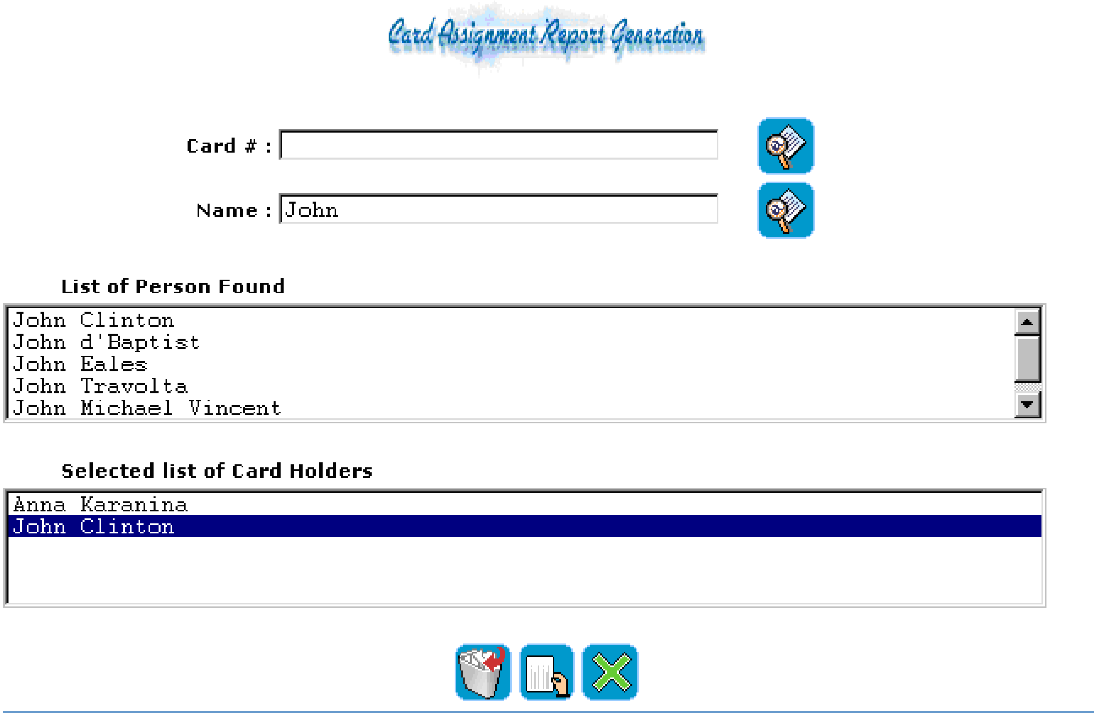
Anna Karanina

Selected list of Card Holders

Anna Karanina

When we search for a card number “9” (for example), you will see a screen as above. We will be able to see the name of the person corresponding to the card number. Clicking once on the person's name will add that person to the **Selected list of Card Holders** field.

We may also perform a search by name. Let us consider, for example, that we are searching for a name “John”. When we perform a search for “John”, we will be able to see all persons having “John” in their name.


Card Assignment Report Generation

Card # :

Name : John

List of Person Found

John Clinton
John d'Baptist
John Eales
John Travolta
John Michael Vincent

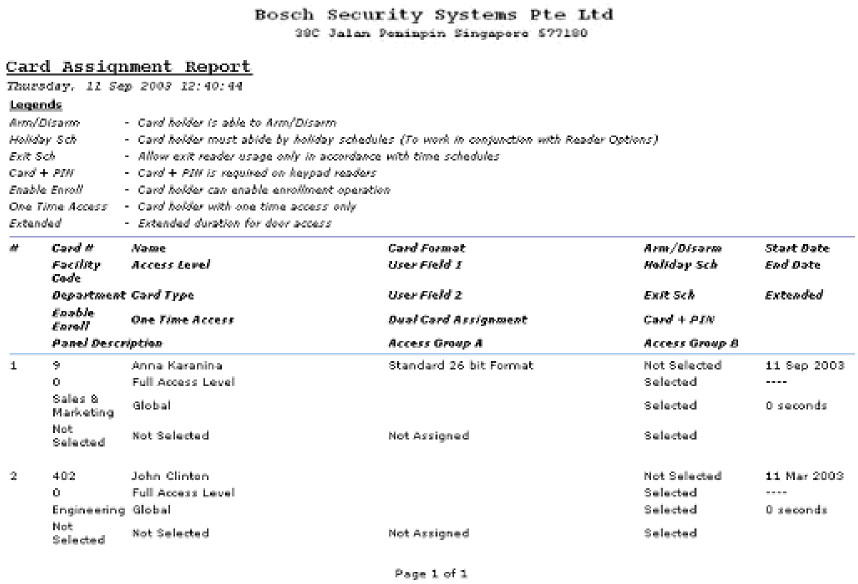
Selected list of Card Holders

Anna Karanina
John Clinton

We may select the person you want to add to the **Selected list of Card Holders** field by clicking once on the person's name in the **List of Person Found** field.

To generate a cardholders report based on the parameters above, click on the submit icon.

A sample report is shown below.



Bosch Security Systems Pte Ltd
30C Jalan Pemimpin Singapore 577180

Card Assignment Report

Thursday, 11 Sep 2003 12:40:44

Legends

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

#	Card #	Name	Card Format	Arm/Disarm	Start Date
	Facility Code	Access Level	User Field 1	Holiday Sch	End Date
	Department	Card Type	User Field 2	Exit Sch	Extended
	Enable Enroll	One Time Access	Dual Card Assignment	Card + PIN	
	Panel Description		Access Group A	Access Group B	
1	9	Anna Karanina	Standard 26 bit Format	Not Selected	11 Sep 2003
	0	Full Access Level		Selected	----
	Sales & Marketing	Global		Selected	0 seconds
	Not Selected	Not Selected	Not Assigned	Selected	
2	402	John Clinton		Not Selected	11 Mar 2003
	0	Full Access Level		Selected	----
	Engineering	Global		Selected	0 seconds
	Not Selected	Not Selected	Not Assigned	Selected	

Page 1 of 1

It contains all the details found under *The Card Parameters, page 42*.

8 Access Levels

An access level is defined as a group of access groups, while an access group defines a list of readers within certain authorized time periods (predefined schedule) that the cardholders can access. There are 1024 programmable access levels.

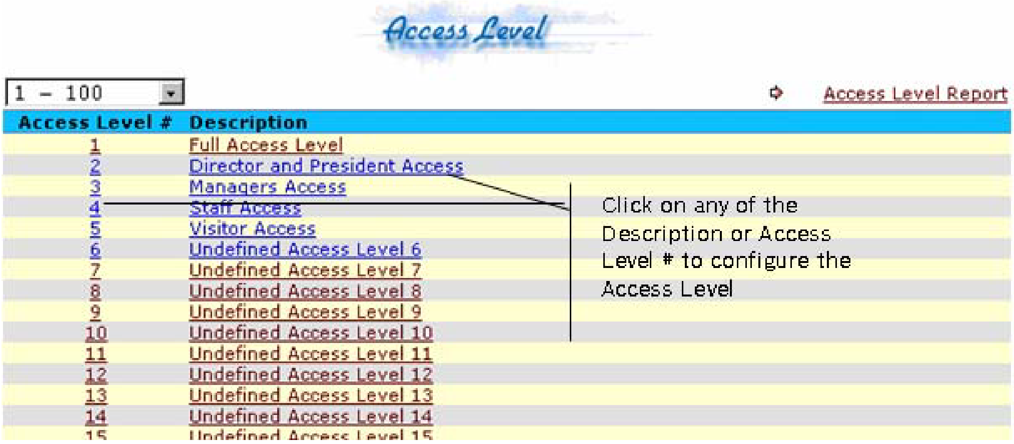
In addition, there are two more unique access levels. They are the full access level that allows cardholders to access all readers at all times, usually reserved for the President, Chairman, or Directors of the company and the unused level that prohibits cardholder to access any reader at all times.

Access level is implemented to simplify the process of assigning cardholder's access rights to each reader in each Access Easy Controller. In a system where more than one Access Easy Controller are implemented to control the access of doors, we will need to configure the cardholder number into each and every one of the Access Easy Controller. This is a very time consuming process. With Access Easy Master, we could configure cards for the cardholders by assigning them with access levels. Each access level could define the access groups that the cardholder belongs to in each Access Easy Controller.

It is highly recommended that detail planning be done before setting up the access levels.

8.1 The Access Levels page

To activate **Access Levels** screen, click on **Access Levels** link from the main menu page. The **Access Levels** screen will appear as shown below.



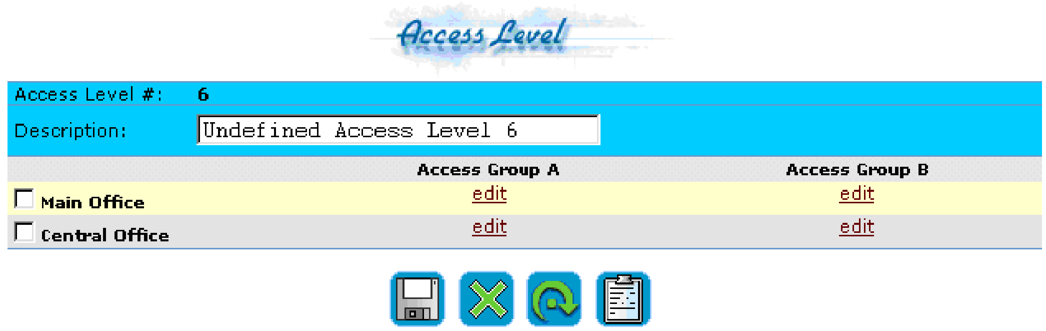
Access Level #	Description
1	Full Access Level
2	Director and President Access
3	Managers Access
4	Staff Access
5	Visitor Access
6	Undefined Access Level 6
7	Undefined Access Level 7
8	Undefined Access Level 8
9	Undefined Access Level 9
10	Undefined Access Level 10
11	Undefined Access Level 11
12	Undefined Access Level 12
13	Undefined Access Level 13
14	Undefined Access Level 14
15	Undefined Access Level 15

Click on any of the Description or Access Level # to configure the Access Level

The **Access Levels** screen will show the different access levels with their descriptions. After activating the access levels, we need to configure the access levels for granting access across different controllers. Select from the drop-down list on the top left corner to select access level numbers that are more than 100.

8.2 How to Configure Access Levels

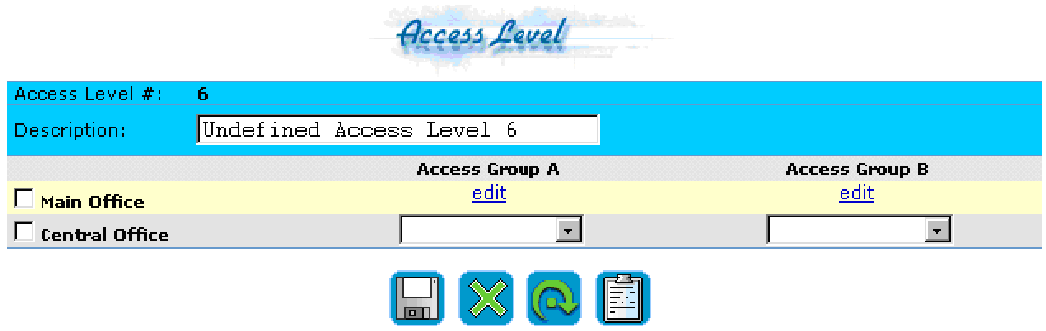
1. Click on the access level (can be any of the 1024 undefined access levels) you want to configure. You will see a screen as shown below.



Access Level

Access Level #:	6	
Description:	Undefined Access Level 6	
	Access Group A	Access Group B
□ Main Office	edit	edit
□ Central Office	edit	edit

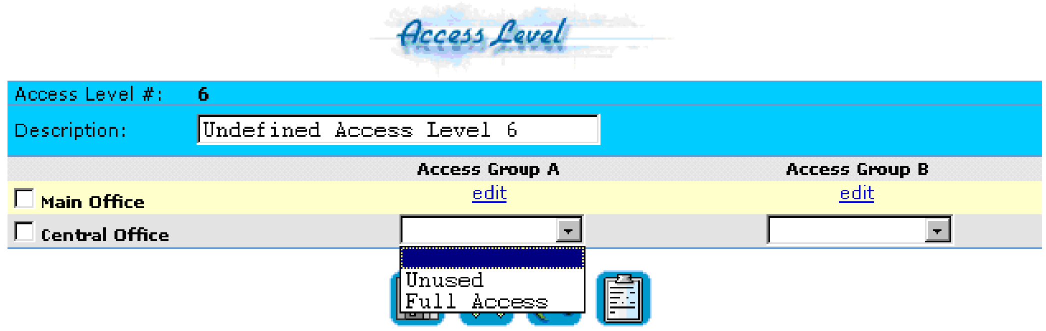
2. Enter the description for the access level in the **Description** field.
3. You will see a list of available Access Easy Controllers in the **Access Level** screen.
4. Check on the controllers you wish to add in the access level. For this example, the controller is “Central Office” ☑ Central Office.
5. Click on the **edit** link under **Access Group A** or **Access Group B** columns to select the appropriate access grouping from the list. There is no priority or precedents in **Access Group A** or **Access Group B**. When any of the **edit** hyperlink is clicked for that row, the screen as shown below appears.



Access Level

Access Level #:	6	
Description:	Undefined Access Level 6	
	Access Group A	Access Group B
□ Main Office	edit	edit
□ Central Office	▾	▾

6. Click on the down-down list to select an access group for **Access Group A** and **Access Group B**. Leave the entry as blank or select “Unused” if it is not required.



Access Level

Access Level #:	6	
Description:	Undefined Access Level 6	
	Access Group A	Access Group B
□ Main Office	edit	edit
□ Central Office	▾	▾

Unused
Full Access

7. Click 💾 to save the new settings.

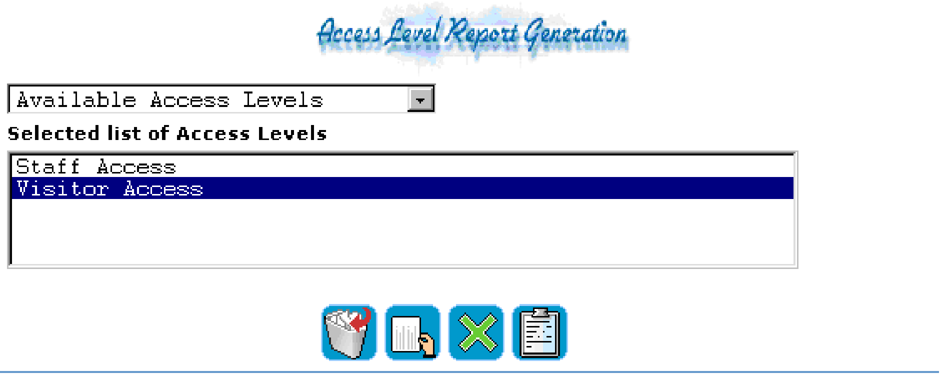
Notice!
The access groups in each controller has to be predefined in the controller itself. To define the access groups in the individual controller, go to *How to Setup Access Groups, page 120*.

8.3 How to Print Access Level Report

An **Access Level** report contain details of all the access levels which are configured. Undefined access levels will not be included in the report.

To print an **Access Level Report**, click on Access Level Report located on the top right corner of the **Access Levels** first page.

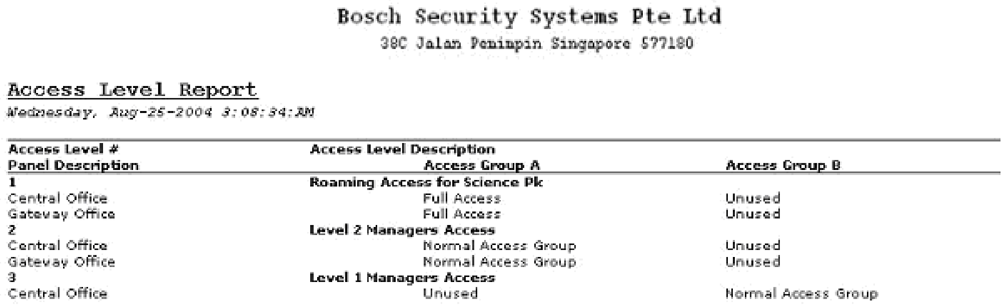
The **Access Level Report Generation** web page has a drop-down list which shows all the configured access levels. Select the access levels you want to include in the **Access Level Report** by clicking once on the access level in the drop-down list. The **Selected list of Access Levels** list box will display the access levels you want to be included in the **Access Level Report**.


Access Level Report Generation
Available Access Levels
Selected list of Access Levels
Staff Access
Visitor Access

Notice!
Only configured access levels will be shown in the list box for selection. Configured access levels are those with at least one Access Easy Controller checked and at least one access group configured and not left blank.

To print an **Access Level Report**, click on the submit icon.

A sample **Access Level Report** is as shown below.



Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Access Level Report
Wednesday, Aug-25-2004 3:08:54:AM

Access Level #	Access Level Description	
Panel Description	Access Group A	Access Group B
1	Roaming Access for Science Pk	
Central Office	Full Access	Unused
Gateway Office	Full Access	Unused
2	Level 2 Managers Access	
Central Office	Normal Access Group	Unused
Gateway Office	Normal Access Group	Unused
3	Level 1 Managers Access	
Central Office	Unused	Normal Access Group

9 Users Setup

Each user can be assigned access rights to access and carry out configuration on certain or all functions of the Access Easy Master. Access Easy Master can support up to 25 users, including the Superuser whose access rights cannot be changed.

The **Users Setup** menu item allows the System Administrator to define different access to users, by selecting whether a particular user can have view and/or save access rights to configurable features.

It is important that only authorized users are able to change the following settings, as the implication could be a security breach, if unauthorized user gives themselves access to important feature in the system, such as full access for their cards or unlock a door.

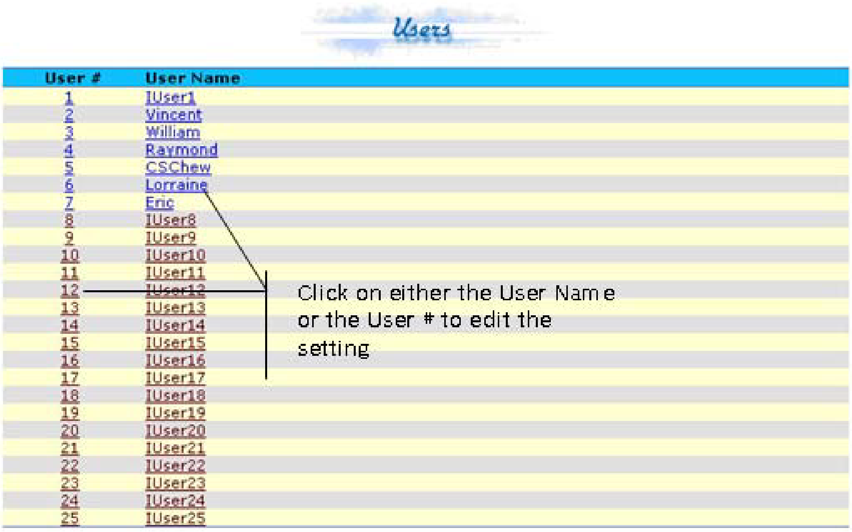
Notice!
The default password and user ID should be changed once the system is in operation!

In the following sections of this chapter, we will be referring to “Login User” as the user who will login to the Access Easy Master from any computer using a web browser program and operates the system.

9.1 Setting User Access

This section describes how to change the user name and password, and how to change the access to menu items.

The following is a screen of the **Users Setup** page.



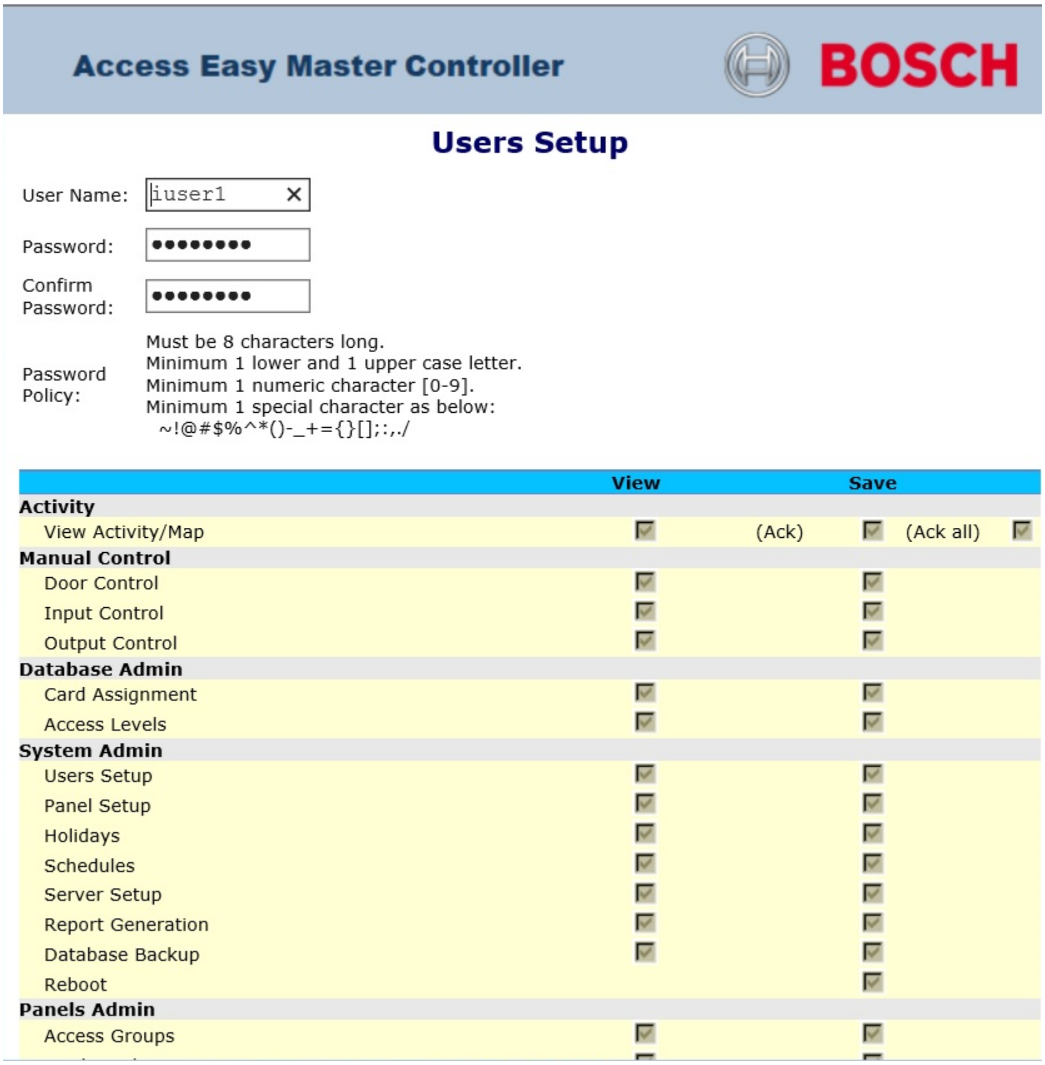
Users

User #	User Name
1	IUser1
2	Vincent
3	William
4	Raymond
5	CSChew
6	Lorraine
7	Eric
8	IUser8
9	IUser9
10	IUser10
11	IUser11
12	IUser12
13	IUser13
14	IUser14
15	IUser15
16	IUser16
17	IUser17
18	IUser18
19	IUser19
20	IUser20
21	IUser21
22	IUser22
23	IUser23
24	IUser24
25	IUser25

Click on either the User Name or the User # to edit the setting

9.1.1 How to Change User Name and Password

1. Click on the user name or its user number and the following screen will appear.



Users Setup

User Name: iuser1

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Password Policy: Must be 8 characters long.
Minimum 1 lower and 1 upper case letter.
Minimum 1 numeric character [0-9].
Minimum 1 special character as below:
~!@#$%^*()-_+={}[];:,./

	View		Save		
Activity					
View Activity/Map	☑	(Ack)	☑	(Ack all)	☑
Manual Control					
Door Control	☑		☑		
Input Control	☑		☑		
Output Control	☑		☑		
Database Admin					
Card Assignment	☑		☑		
Access Levels	☑		☑		
System Admin					
Users Setup	☑		☑		
Panel Setup	☑		☑		
Holidays	☑		☑		
Schedules	☑		☑		
Server Setup	☑		☑		
Report Generation	☑		☑		
Database Backup	☑		☑		
Reboot			☑		
Panels Admin					
Access Groups	☑		☑		

Notice!
The first "Login User" will always be the Superuser. A Superuser has access to all menu items and its settings cannot be changed except for the user name and password.
Checkboxes that are greyed out like this ☑ indicate that the setting cannot be changed.

2. To edit the **User Name**, delete the default user name and enter the new user name.
3. To edit the **Password**, delete the default password and enter the new password.
4. Enter the new password again in the **Confirm Password** field.

Caution!

The password is case-sensitive. For security reasons, every character entered in the password field is represented by a dot.

The passwords must meet the following requirements:
must be 8 characters long
must consist of at least
- 1 lowercase letter,
- 1 uppercase letter,
- 1 number, and
- 1 special character from ~`!@#$%^*()-_+={}[];:,./

5. Click on the 💾 icon to save the settings. If the passwords in the **Password** and **Confirm Password** fields match and meet the password policy requirements, a change confirmation message appears. The new settings will only take effect upon the next successful login.

9.1.2 How to Change the Access to Menu Items

View

Refers to having the access right to view the contents of the menu item.

Save

Refers to having the access right to edit the contents of the menu item.

If only the **Save** checkbox for the menu item is checked, the system would treat that both the **View** and **Save** function as being selected, as **View** option is a subset of the **Save** option.

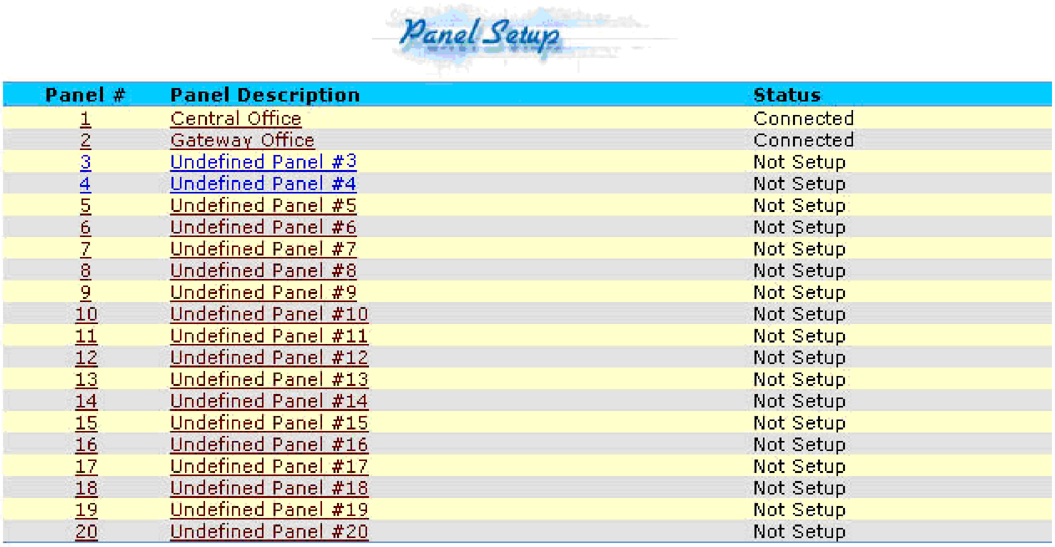
1. To assign the various menu item access rights, check the checkboxes of the desired menu item under **View** and/or **Save** columns. To unselect the point, click on it again.
2. Click on the 💾 icon to save the settings. The new settings will only take effect upon the next successful login.

10 Panel Setup

This chapter will provide a step by step guide to how to add an Access Easy Controller.

The **Panel Setup** screen allows us to identify the Access Easy Controller that will be managed by the Access Easy Master. It will also show the connection status of the Access Easy Controller with the Access Easy Master.

Below is a screen of the **Panel Setup**.



Panel Setup

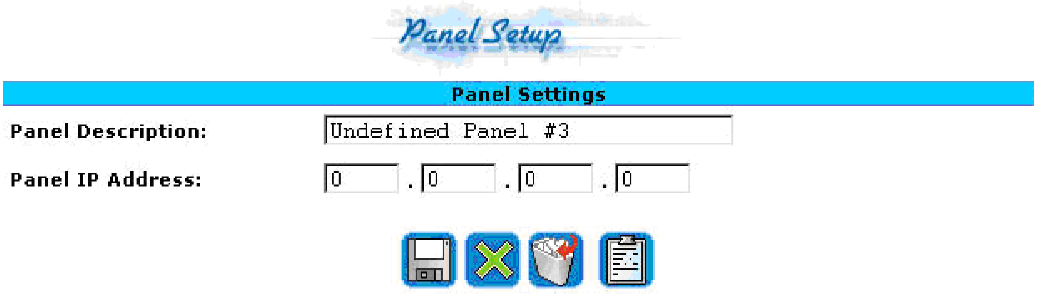
Panel #	Panel Description	Status
1	Central Office	Connected
2	Gateway Office	Connected
3	Undefined Panel #3	Not Setup
4	Undefined Panel #4	Not Setup
5	Undefined Panel #5	Not Setup
6	Undefined Panel #6	Not Setup
7	Undefined Panel #7	Not Setup
8	Undefined Panel #8	Not Setup
9	Undefined Panel #9	Not Setup
10	Undefined Panel #10	Not Setup
11	Undefined Panel #11	Not Setup
12	Undefined Panel #12	Not Setup
13	Undefined Panel #13	Not Setup
14	Undefined Panel #14	Not Setup
15	Undefined Panel #15	Not Setup
16	Undefined Panel #16	Not Setup
17	Undefined Panel #17	Not Setup
18	Undefined Panel #18	Not Setup
19	Undefined Panel #19	Not Setup
20	Undefined Panel #20	Not Setup

Access Easy Master is able to support up to 20 Access Easy Controllers.

10.1 How to Add an Access Easy Controller

Before the user proceeds with the following steps, he should ensure that the Access Easy Master IP address is also registered in the Access Easy Controller. Log in to the Access Easy Controller itself to register the Access Easy Master IP address.

1. Click on any of the undefined controller (in this example, “Panel #3” is not configured yet) and the following screen will appear.



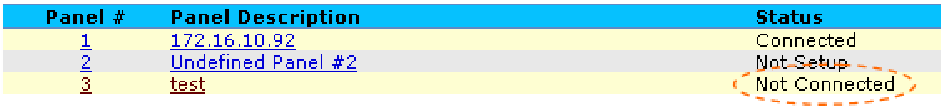
Panel Setup

Panel Settings

Panel Description:	Undefined Panel #3
Panel IP Address:	0 . 0 . 0 . 0

2. Enter the description in the **Panel Description** field and the IP address in the **Panel IP Address** field. Click on the 💾 icon to save your settings. To delete a controller, click on the 🗑 icon.

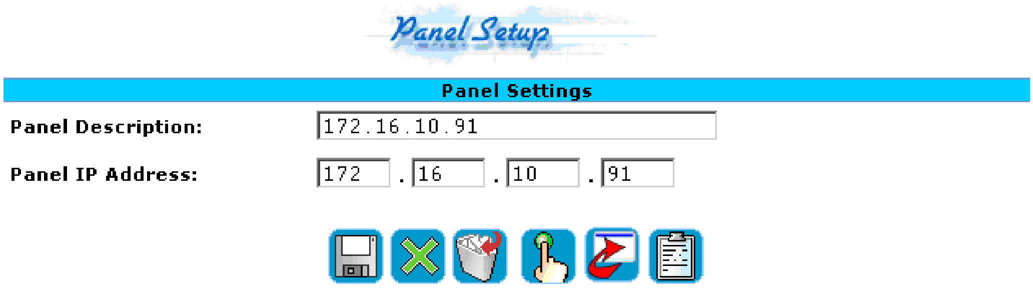
3. Once the IP address of the new Access Easy Controller has been added to the **Panel Setup** page, Access Easy Master will attempt to connect to the new controller and synchronize the database. If Access Easy Master fails to connect to Access Easy controller, the status will show that it is not connected.



Panel #	Panel Description	Status
1	172.16.10.92	Connected
2	Undefined Panel #2	Not Setup
3	test	Not Connected

The **Status** column shows the status of the Access Easy Controllers connection with the Access Easy Master:
“Not Connected” - Access Easy Master is unable to detect the Access Easy Controller.
“Initialising” - Access Easy Master is synchronizing with the Access Easy Controller. This will only happen when a new controller is added and new database has to be created.
“Deleting” - Access Easy Master is deleting the database. This will only happen when a controller is deleted.
”Connected” - Access Easy Master is able to detect the Access Easy Controller.
“Not Setup” - There is no Access Easy Controller setup.

4. After the controller is successfully connected to the server, there will be two extra button and in the **Panel Settings**, as shown below. This is for the user to synchronize the following data and settings configured in the Access Easy Master to the controller: Card Database, Holidays, Schedules and the groups under controllers admin such as Access Groups, Card Readers, Input Setup, Output Setup, Advance I/O Setup, Input Point Configuration and Email/SMS Configuration.



Panel Setup

Panel Settings

Panel Description: 172.16.10.91

Panel IP Address: 172 . 16 . 10 . 91

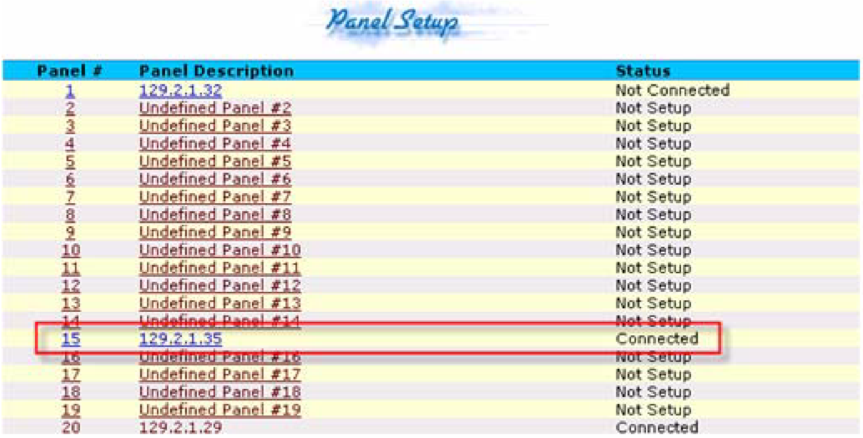
10.2 How to Download Database to Panel

User can download database to the controller. This allows user more control to select desired controller to update the database. This feature is useful if some controllers in the system are not fully operational and the user does not wish to update these controllers yet. Or a faulty controller has been replaced with a new one, hence the user could use this feature to download the database back to the new controller.

Notice!
Only controllers with the status "Connected" are able to download any new database to the controller.

Download Database to Controller

1. Click on the desired controller (in this example, “Panel #15” is selected).



Panel Setup

Panel #	Panel Description	Status
1	129.2.1.32	Not Connected
2	Undefined Panel #2	Not Setup
3	Undefined Panel #3	Not Setup
4	Undefined Panel #4	Not Setup
5	Undefined Panel #5	Not Setup
6	Undefined Panel #6	Not Setup
7	Undefined Panel #7	Not Setup
8	Undefined Panel #8	Not Setup
9	Undefined Panel #9	Not Setup
10	Undefined Panel #10	Not Setup
11	Undefined Panel #11	Not Setup
12	Undefined Panel #12	Not Setup
13	Undefined Panel #13	Not Setup
14	Undefined Panel #14	Not Setup
15	129.2.1.35	Connected
16	Undefined Panel #16	Not Setup
17	Undefined Panel #17	Not Setup
18	Undefined Panel #18	Not Setup
19	Undefined Panel #19	Not Setup
20	129.2.1.29	Connected

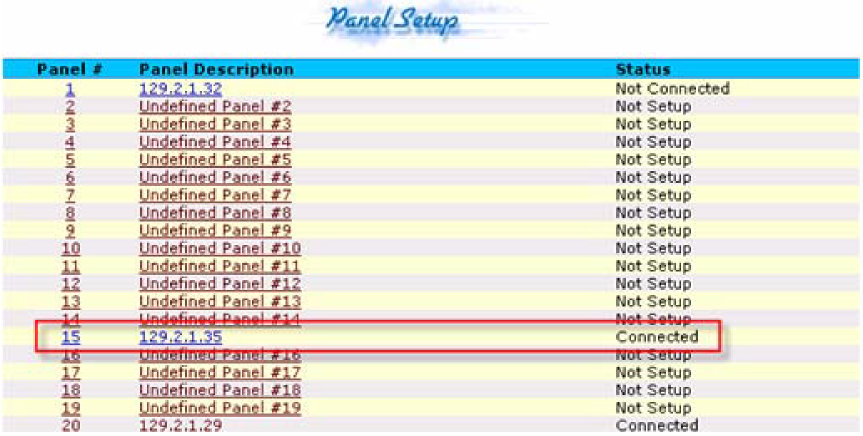
2. Click on the icon to download the database.
3. Click the **OK** button to start overwrite the existing database of the selected controller.
4. Once the new database is downloaded, click on the icon to return.

Notice!

The following database will be downloaded to the controller: **Card Assignment**, **Access Level**, **Holidays**, **Schedule**, **Department List**, **Access Group**, **Card Readers**, **Input Setup**, **Output Setup**, **Advance I/O Setup**, **Input Point Configuration** and **Email/SMS Configuration** database.

Download Card Database to Controller

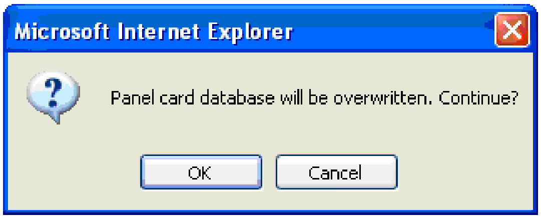
1. Click on the desired controller (in this example, “Panel #15” is selected).



Panel Setup

Panel #	Panel Description	Status
1	129.2.1.32	Not Connected
2	Undefined Panel #2	Not Setup
3	Undefined Panel #3	Not Setup
4	Undefined Panel #4	Not Setup
5	Undefined Panel #5	Not Setup
6	Undefined Panel #6	Not Setup
7	Undefined Panel #7	Not Setup
8	Undefined Panel #8	Not Setup
9	Undefined Panel #9	Not Setup
10	Undefined Panel #10	Not Setup
11	Undefined Panel #11	Not Setup
12	Undefined Panel #12	Not Setup
13	Undefined Panel #13	Not Setup
14	Undefined Panel #14	Not Setup
15	129.2.1.35	Connected
16	Undefined Panel #16	Not Setup
17	Undefined Panel #17	Not Setup
18	Undefined Panel #18	Not Setup
19	Undefined Panel #19	Not Setup
20	129.2.1.29	Connected

2. Click on the icon to download the card database.
3. Click the **OK** button to start overwrite the existing database of the selected controller.



Microsoft Internet Explorer

Panel card database will be overwritten. Continue?

4. Once the new card database is downloaded, click on the ⇦ icon to return to the previous screen.

11 Holidays

Holidays are applicable to all the Access Easy Controllers managed by the Access Easy Master. Holidays have to be set up only if the system operation behavior is required to be different during those times. Some examples of how the parameters affect the system operation behavior 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.

By providing a centralized configuration of holidays, the Server Administrator can just configure holidays in the Access Easy Master and it will synchronize with all the Access Easy Controllers automatically.

This section covers the step-by-step guide to set up holiday parameters.

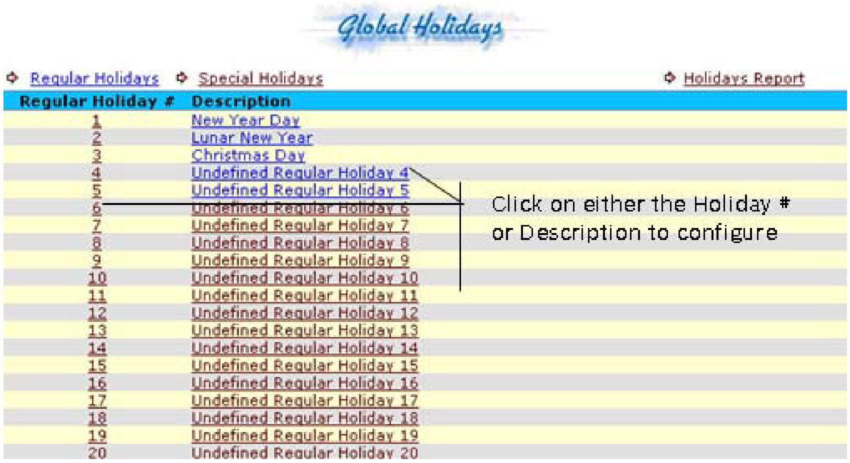
Holidays set-up consist of 64 holidays selection, of which 32 are assigned to regular holiday dates and the other 32 assigned to special holiday dates. There is no difference between the operational behaviors of both types. For simplicity, you may treat the special holiday set up for use during the eve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

Each holiday has the feature to include the year in the processing. If the **Include year in processing?** radio button is set to “No” option, 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, for example New Year’s Day and Christmas Day needs only to be defined once. Those holiday dates that vary from year to year will have to be updated at the beginning of the year, and the **Include year in processing?** radio button should be selected as “Yes” option.

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

11.1 How to Configure Holidays

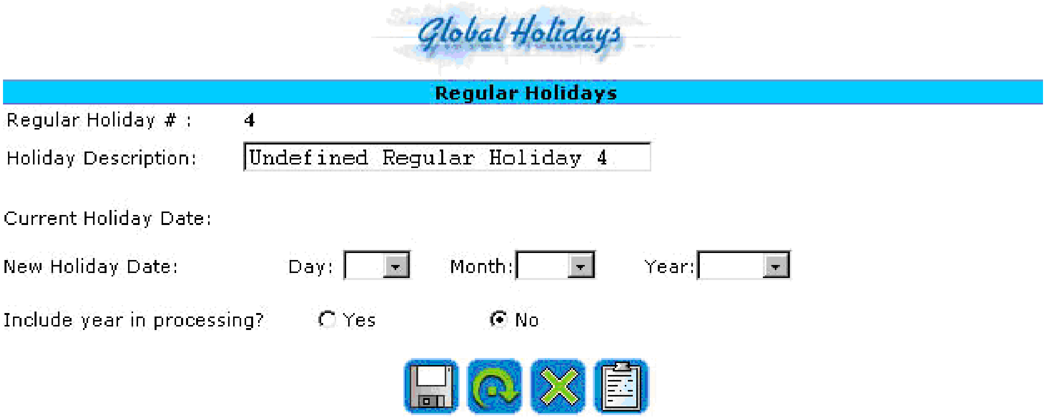
1. From the left pane, select **Holidays** menu. A screen as shown below appears.



Regular Holiday #	Description
1	New Year Day
2	Lunar New Year
3	Christmas Day
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

Click on either the Holiday # or Description to configure

2. Click on the ➪ Regular Holidays or ➪ Special Holidays link to list the appropriate holiday type.
3. Click on the entry in the **Holiday #** or the **Description** column to proceed. A screen as shown below appears.



Global Holidays

Regular Holidays

Regular Holiday # : 4

Holiday Description: Undefined Regular Holiday 4

Current Holiday Date:

New Holiday Date: Day: Month: Year:

Include year in processing? ○ Yes ● No

4. Delete the default text and enter the new description in the **Holiday Description** field.
5. Select the **New Holiday Date** from the **Day**, **Month** and **Year** drop-down list. After it is selected and saved, the date will be reflected on the **Current Holiday Date** field.
6. If the holiday date is fixed, then select the “No” option for the **Include year in processing?** radio button. Otherwise, select the “Yes” option.
7. Do one of the following:

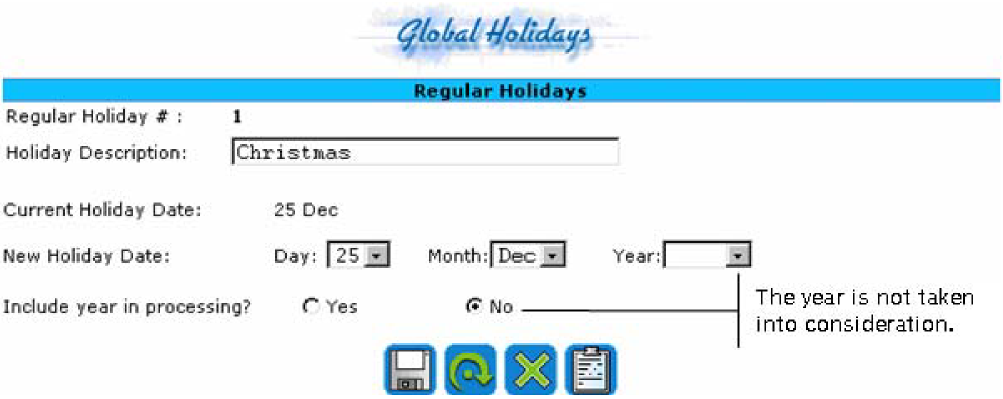
   - To confirm the entries, click on the 💾 button. This will cause the Access Easy Master to start replicating the changes to the rest of the Access Easy Controllers.

   - 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 #1” is used for Christmas in the year 2004. Since the date always fall on the December 25th, the **Include year in processing?** radio button is set to the “No” option.



Global Holidays

Regular Holidays

Regular Holiday # : 1

Holiday Description: Christmas

Current Holiday Date: 25 Dec

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

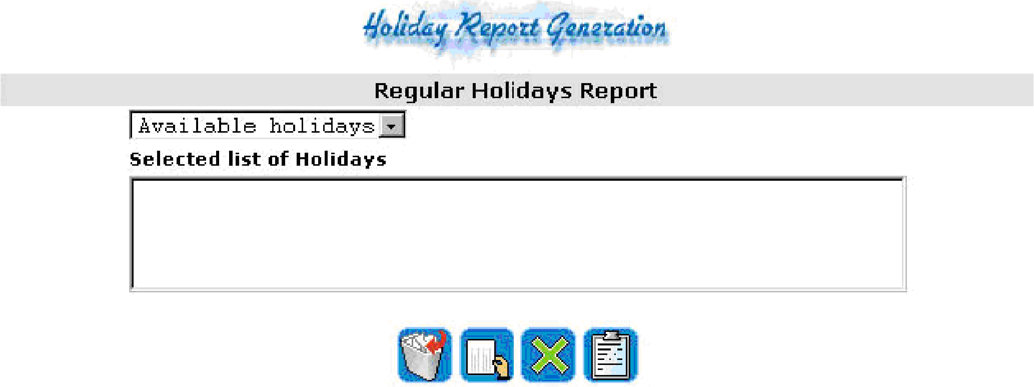
Include year in processing? ○ Yes ● No

The year is not taken into consideration.

11.2 How to Generate a Holidays 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, follow the steps below.

1. From the first page of either the **Regular Holidays** or **Special Holidays**, click on the ➪ Holidays Report link. The example below shows the **Regular Holidays Report** generation.



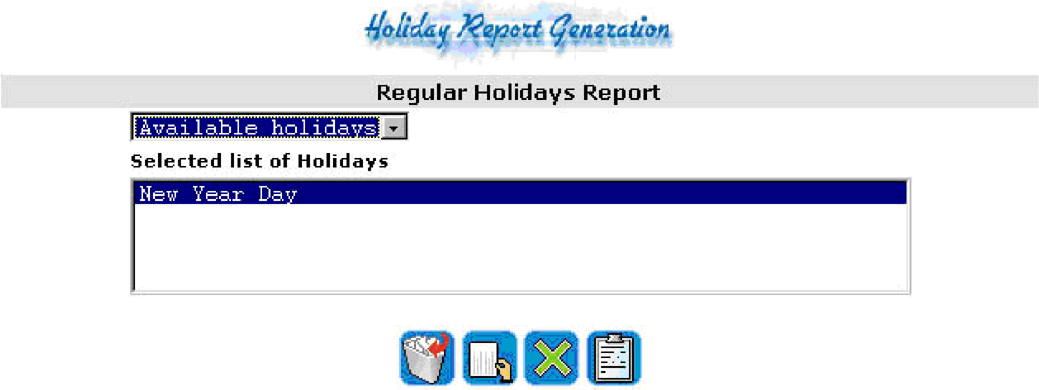
Holiday Report Generation

Regular Holidays Report

Available holidays

Selected list of Holidays

2. Select the desired holiday from the drop-down list and it will appear on the **Selected list of Holidays** list box, as shown below. If no holiday is selected from the drop-down list, all the available holidays with date settings will be included in the report.



Holiday Report Generation

Regular Holidays Report

Available holidays

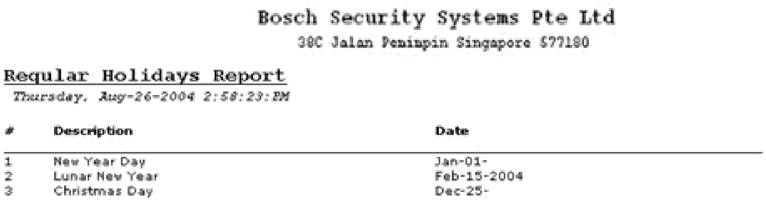
Selected list of Holidays

New Year Day

3. To remove the selected holiday from the **Selected list of Holidays** list box, select that holiday and click on the 🗑 button.
4. Click on the 📄 button for a print preview of the report.

The following screen-capture shows an example of the **Regular Holidays Report**.

Notice!
Only holidays with date setting will be shown.



Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Regular Holidays Report
Thursday, Aug-26-2004 2:58:23:PM

#	Description	Date
1	New Year Day	Jan-01-
2	Lunar New Year	Feb-15-2004
3	Christmas Day	Dec-25-

12 Schedules

Schedules can be used in the following manner:

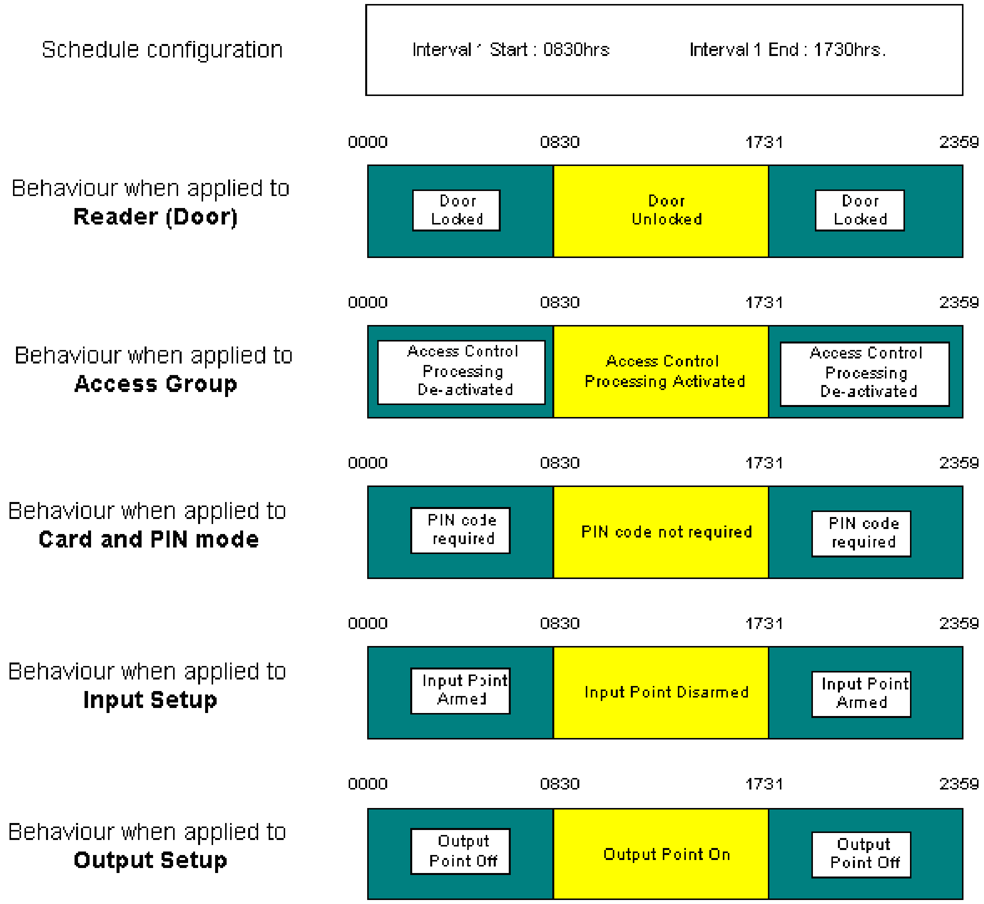
- Schedules are allocated to card readers for access groupings. This is to specify whether cardholders can access specific readers at specific time, or cardholders need to enter PIN at specific time.
- Schedules are allocated to the card readers to activate or deactivate readers at specified time. It 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 or 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.

Schedules are common to all the Access Easy Controllers managed by the Access Easy Master.

Notice!
All entries for time are based on 24-hour, 4-digits format.

12.1 System Behavior when using Schedule

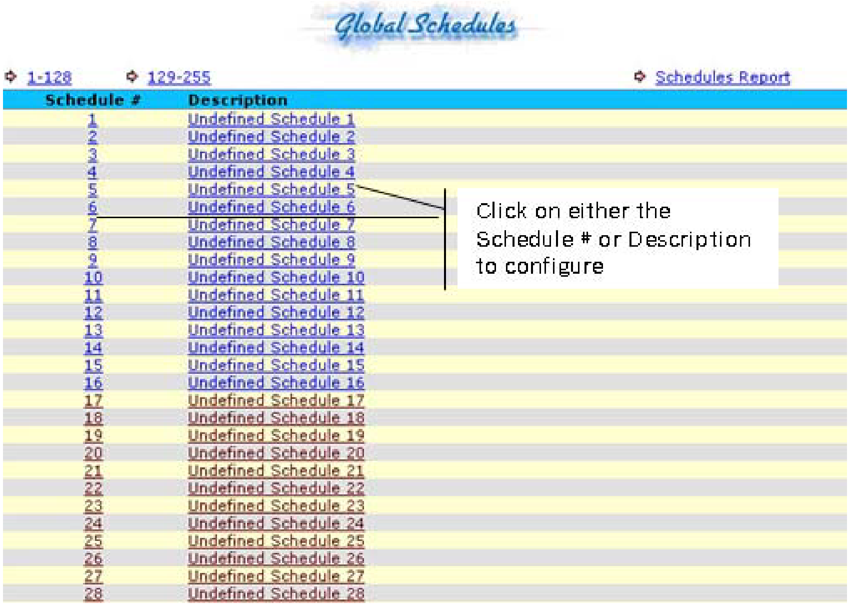
The diagram below provides a graphical representation of the system's behavior when a schedule is used on the various functions.



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.

12.2 How to Configure Schedules

1. From the left pane, select **Schedules** menu. A screen as shown below appears.



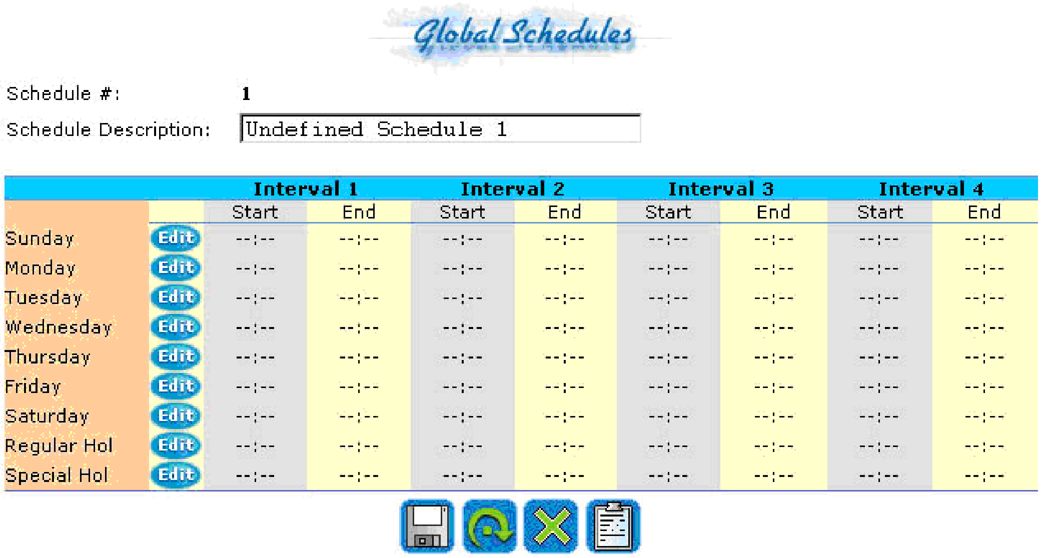
Global Schedules

1-128 129-255 Schedules Report

Schedule #	Description
1	Undefined Schedule 1
2	Undefined Schedule 2
3	Undefined Schedule 3
4	Undefined Schedule 4
5	Undefined Schedule 5
6	Undefined Schedule 6
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
24	Undefined Schedule 24
25	Undefined Schedule 25
26	Undefined Schedule 26
27	Undefined Schedule 27
28	Undefined Schedule 28

Click on either the Schedule # or Description to configure

2. Click on the 1-128 or 129-255 link to list the appropriate schedule range.
3. Click on the **Schedule #** or the **Description** text to proceed. A screen as shown below appears.



Global Schedules

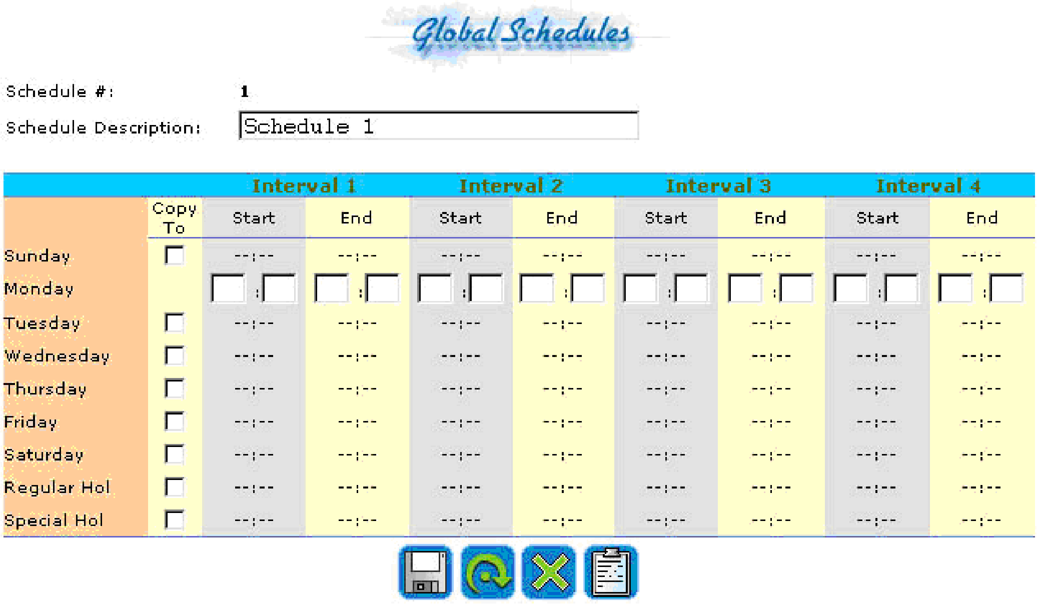
Schedule #: 1

Schedule Description: Undefined Schedule 1

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

4. Delete the default text and enter the description in the **Schedule Description** field.
5. Click on the 💾 button.

6. Click on the Edit button beside the day of week (DOW) row. This will enable the whole row for editing as shown on the following page.



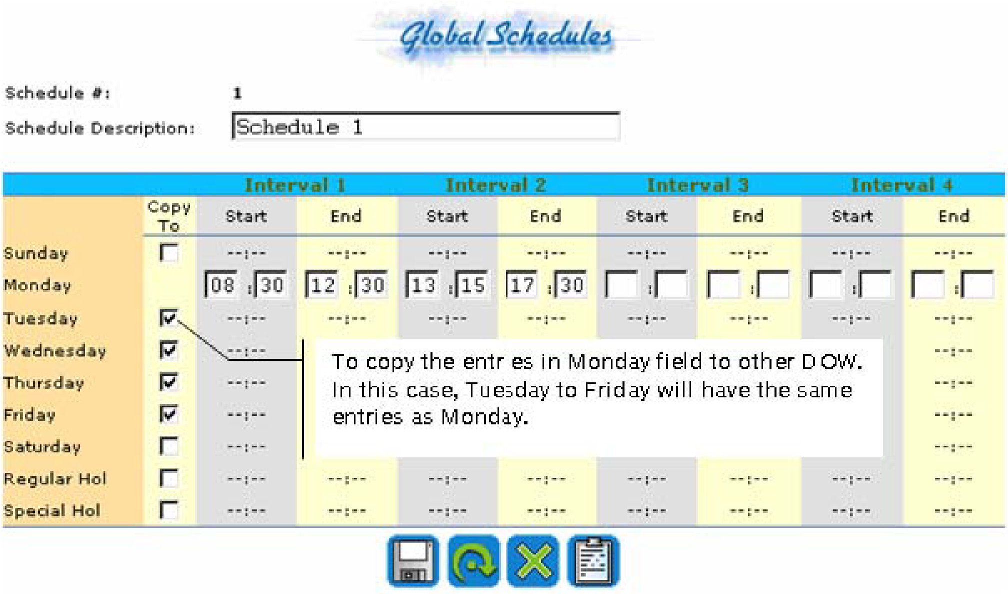
Global Schedules

Schedule #: 1

Schedule Description: Schedule 1

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

7. Click on the required field, starting from **Interval 1 - Start**, and enter the appropriate time in 24-hour, 4 digits format.
8. Repeat step 7 until all applicable entries are entered.
9. If the time of operation is the same for “Monday” to “Friday”, check the **Copy To** checkboxes. This will duplicate the setting to other DOWs, as shown below. To unselect the DOW, click on the corresponding checkbox again.



Global Schedules

Schedule #: 1

Schedule Description: Schedule 1

		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 entr es in Monday field to other D OW. In this case, Tuesday to Friday will have the same entries as Monday.

10. Do one of the following:

- To confirm the entries, click 💾 on the button. This will cause the Access Easy Master to replicate the schedule to the rest of the Access Easy Controller.

- To clear the entries, click on the button.

- To cancel the operation, click on the button.

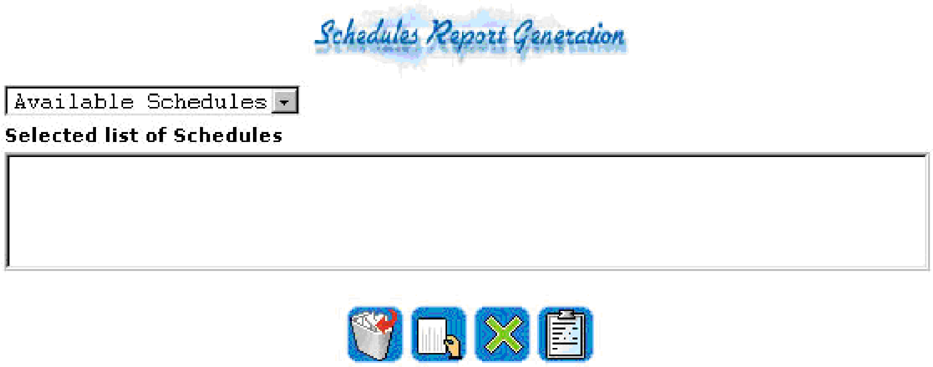
- To return to the first page, click on the button.

11. Proceed to edit the other DOWs or holidays where applicable. If the company does not operate during Sunday or on a holiday, leave the entries in these 3 fields unchanged as “-- : --“. This will indicate to the controller that these are to be ignored.

12.3 How to Generate a Schedule Report

Once you have completed configuring the required schedules, a hardcopy can be printed out.

1. From the first page of the **Schedules** screen, click on the Schedules Report link. A screen as shown on the following page.

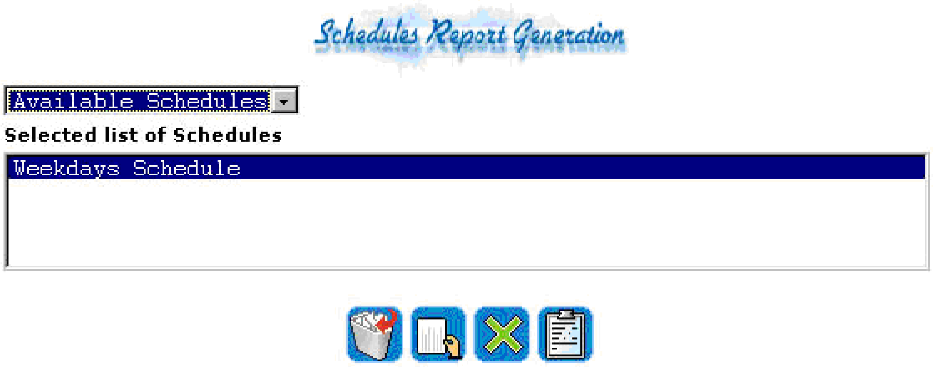


Schedules Report Generation

Available Schedules

Selected list of Schedules

2. Select the desired schedule from the drop-down listbox and it will appear on the **Selected list of Schedules** list shown below. If no schedule is selected from the list, all the available schedules with time settings will be included in the report.



Schedules Report Generation

Available Schedules

Selected list of Schedules

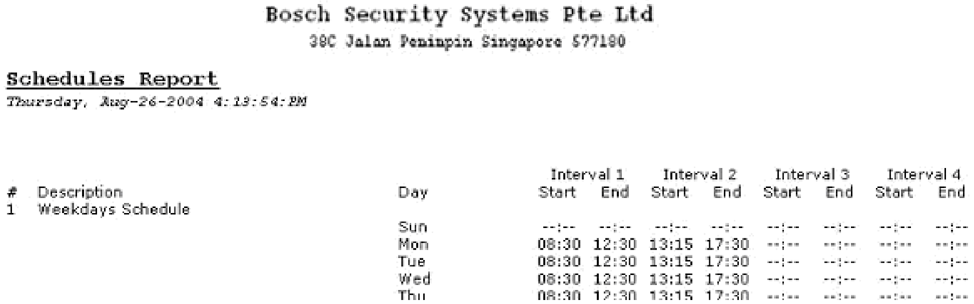
Weekdays Schedule

3. To remove the selected schedule from the **Selected list of Schedules** list, select that schedule and click on the button

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

The following screen-capture shows an example of the **Schedules Report**.

Notice!
Only schedules with time setting will be shown.



Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Schedules Report
Thursday, Aug-26-2004 4:13:54:PM

			Interval 1		Interval 2		Interval 3		Interval 4	
#	Description	Day	Start	End	Start	End	Start	End	Start	End
1	Weekdays 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	--:--	--:--	--:--	--:--

13 Server Setup

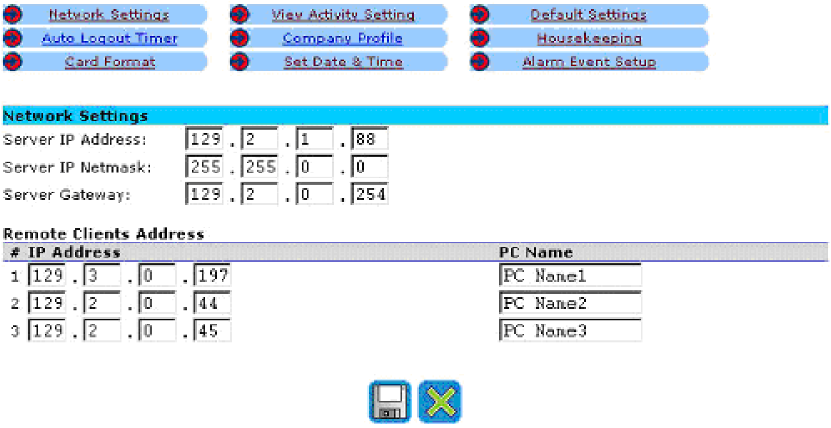
The server setup involves setting up the Access Easy Master and configuring its various parameters.

These parameters include:-

- Network Settings,
- Auto Logout Timer,
- Card Format,
- View Activity Setting,
- Company Profile,
- Set Date and Time,
- Default Settings,
- Housekeeping,
- Alarm Event Setup.

13.1 Network Settings

Network settings involve configuring the various network parameters for Access Easy Master such as IP address, subnet mask and gateway. It also involves setting up the IP address of remote clients. Click on **Network Settings** from the menu item list and you will see a screen as shown below.



Network Settings

Server IP Address: 129 . 2 . 1 . 88

Server IP Netmask: 255 . 255 . 0 . 0

Server Gateway: 129 . 2 . 0 . 254

Remote Clients Address

#	IP Address	PC Name
1	129 . 3 . 0 . 197	PC Name1
2	129 . 2 . 0 . 44	PC Name2
3	129 . 2 . 0 . 45	PC Name3

This configuration allows user to enter the server IP address, netmask and gateway. In addition, user can define three remote client addresses for data transfer purposes.

13.1.1 How to Edit Network Settings

1. Delete the default number in each of the **Server IP Address**, **Server IP Netmask** and **Server Gateway** fields and enter the appropriate number.
2. Click on the 💾 icon to save the settings.

Notice!
In order for the new IP address to take effect, the Access Easy Master needs rebooting.

13.2 Auto Logout Timer

This configuration allows user to set the timer for the Access Easy Master software to logout automatically if it detects no user activity. Default setting is “1 hour”. Click on **Auto Logout Timer** from the menu item list and you will see a screen as shown below.

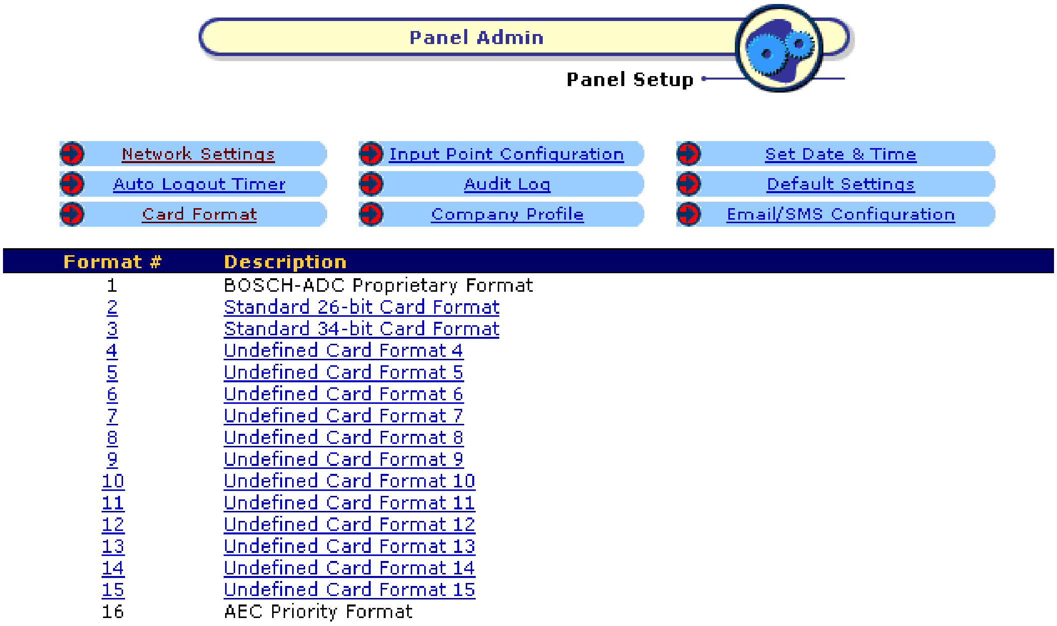
Notice!
This timer setting is applicable to all menu items except **View Activity** screen.

13.2.1 How to Set the Auto Logout Timer

1. Select the hour and minute from **Hour** and **Minute** drop-down list.
2. Click on the 💾 icon to save your setting. Click on the ❎ icon to clear the setting.

13.3 Card Format

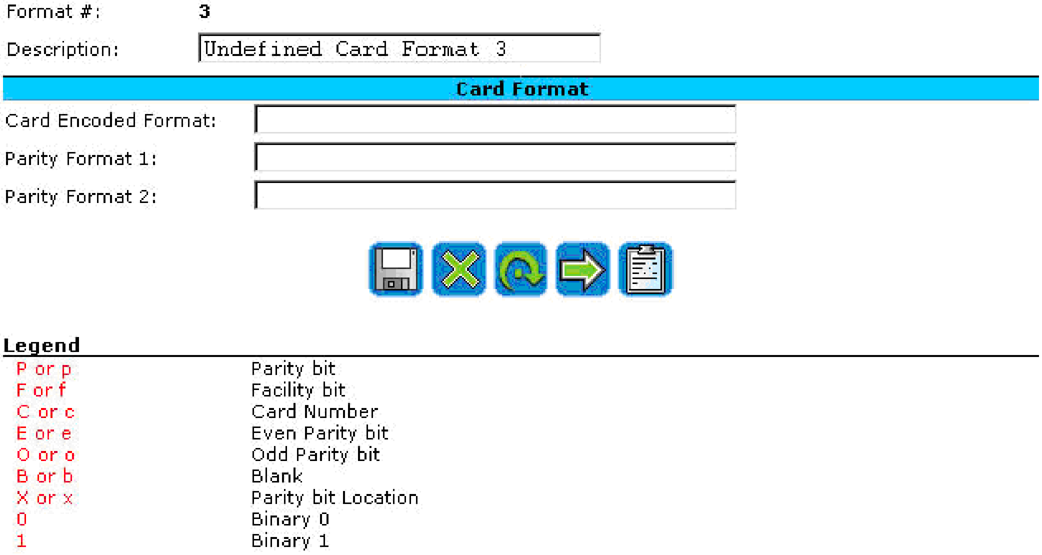
This setting allows user to customize the Access Easy Master to accept up to 16 different types of Wiegand card formats, inclusive of the “BOSCH-ADC Proprietary Format” and the standard “AEC Priority Format”, which have been pre-assigned to “Format #1” and “Format #16” respectively. Card format up to a maximum of 64-bit and up to 8 parity format is configurable. Click on **Card Format** from the menu item list and you will see a screen as shown below.



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

13.3.1 How to Configure New Card Format

1. Click on the **Format #** or **Description** text of any “Undefined Card Format” to proceed. A screen as shown below appears.



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 bit
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. Delete the default text and enter a description for this card format in the **Description** field.
3. Enter the card format in the **Card Encoded Format** field accordingly.
4. Enter the parity format in **Parity Format 1** and **Parity Format 2** fields.

Notice!
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 field entries (**Parity Format 2** to **Parity Format 8**).
If the card format doesn't support parity checking, leave 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 consist of two parity bits and 24 code bits. The first transmitted bit is the even parity bit (E) and it is calculated over the first 12 bits. The last bit transmitted is the odd parity bit (O) and it is calculated over the last 12 bits.

The string of bits for this code format is shown 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

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

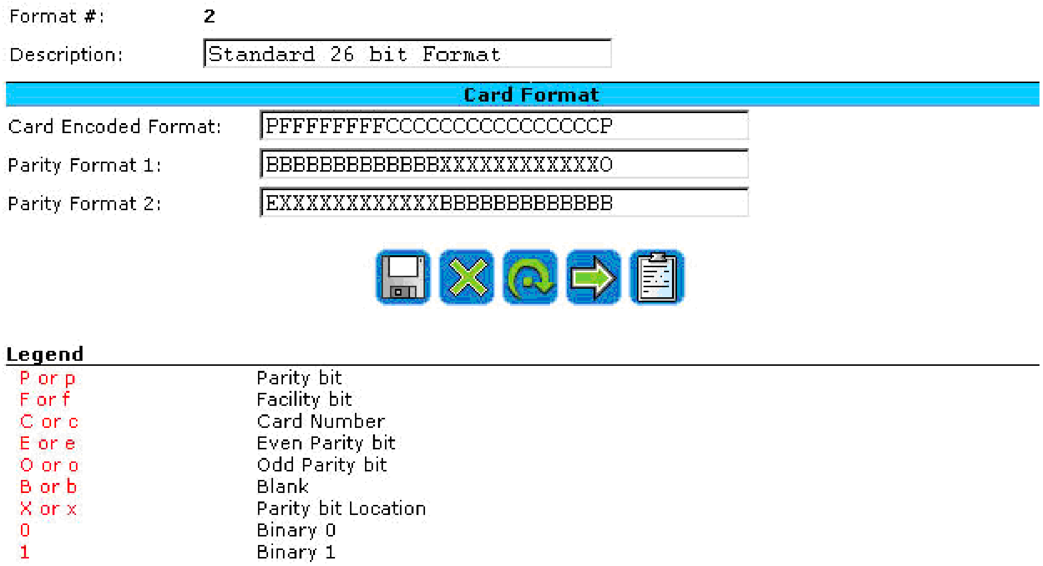
For the odd parity format

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

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.



Format #: 2

Description: Standard 26 bit Format

Card Format

Card Encoded Format: PFFFFFFFFCCCCCCCCCCCCCCCCP

Parity Format 1: BBBBBBBBBBBBBXXXXXXXXXXXXO

Parity Format 2: EXXXXXXXXXXXXBBBBBBBBBBBBB

Legend

P or p	Parity bit
F or f	Facility bit
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

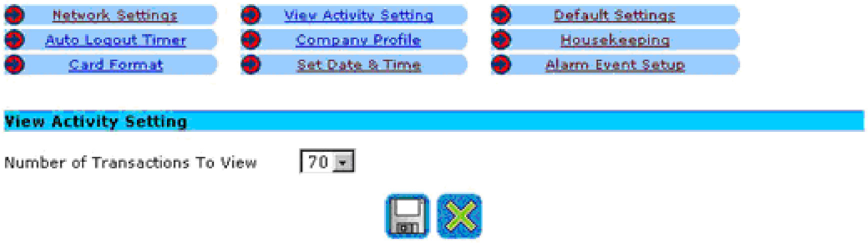
If you have card format that has more than two parity format (maximum is 8), click on the ➡ button to configure them else just save the configuration.

Tip: To best distinguish between the alphabet "O" and the number "0", it is recommended that you use all lower case entries.

13.4 View Activity Setting

This setting affects the number of transaction records to view on screen for the **View Activity** menu. However, should there be alarms that are 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 words, 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 steps of 10 records. Click on **View Activity Setting** from the menu item list and you will see a screen as shown below.



View Activity Setting

Number of Transactions To View 70

13.4.1 How to Edit View Activity Setting

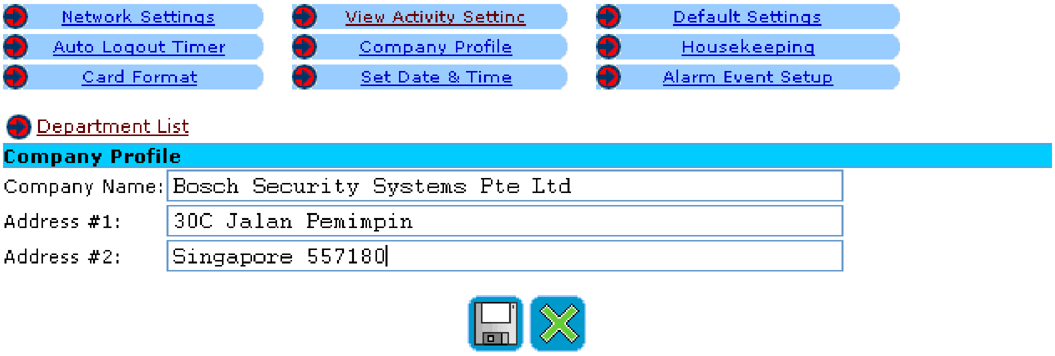
1. Select the appropriate number from the **Number of Transactions To View** drop-down list.
2. Click on the 💾 icon to save your setting.

13.5 Company Profile

The **Company Profile** feature is used as a letterhead in all the reports generated as shown below:-

- Card Report,
- Access Level Report,
- Holidays Report,
- Schedules Report,
- Audit Log Report,
- Access Groups Report,
- Card Reader Report,
- Input Point Report,
- Output Point Report and
- Advance I/O Report.

Each field is limited to 50-characters, including punctuation. In this section, user can also configure the departments available in the company. Click on **Company Profile** from the menu item list and you will see a screen as shown below.



Company Name: Bosch Security Systems Pte Ltd
Address #1: 30C Jalan Pemimpin
Address #2: Singapore 557180

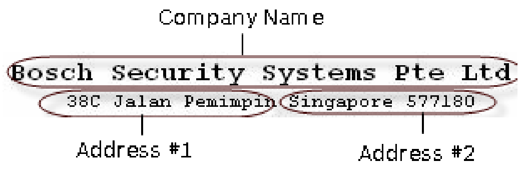
13.5.1 How to Edit Company Profile

1. Delete the default text and enter the desired name in the **Company Name** field.
2. Do likewise for the **Address #1** and **Address #2** fields.
3. Click on the 💾 button.

As an example, we enter the following information in the respective fields:

Company Name: Bosch Security Systems Pte Ltd
Address #1: 30C Jalan Pemimpin
Address #2: Singapore 577180

For the information entered above, the letterhead will appear as shown below. Notice that **Address #1** and **Address #2** are automatically separated by a comma.

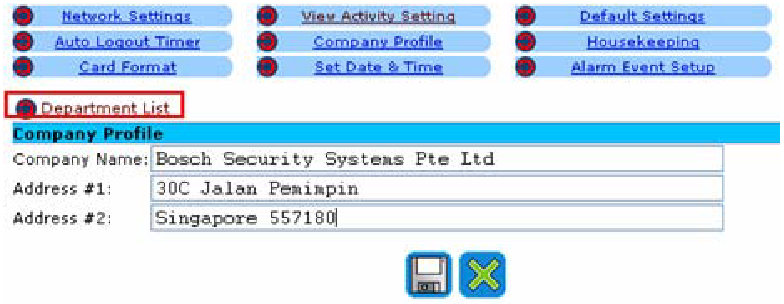


13.5.2 How to Edit the Department List

User can configure the departments available in the company in the **Department List** screen. User can then select the department that the cardholders belong to when allocating card assignment. Please refer to *Card Details, page 43* for the assignment of departments to cardholders.

To edit the department list, follow the steps below:

1. From the **Company Profile** main page as shown below, click on the Department List link.



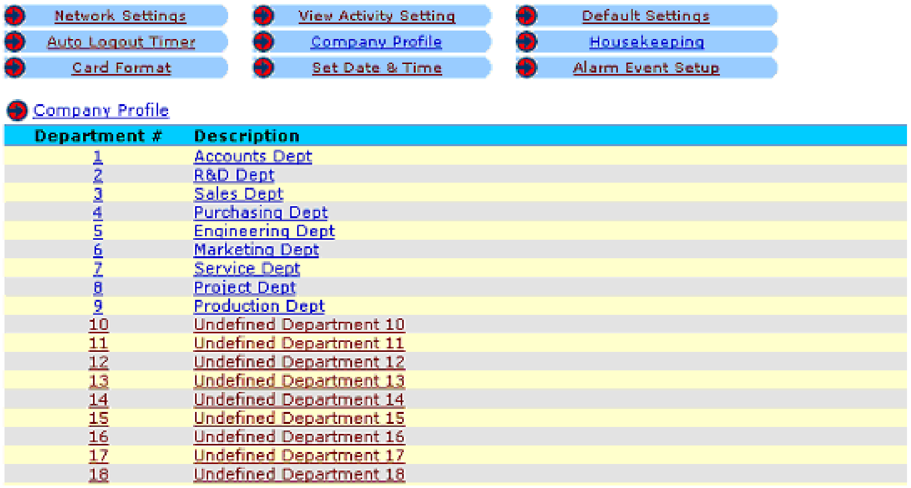
Company Profile

Company Name: Bosch Security Systems Pte Ltd

Address #1: 30C Jalan Pemimpin

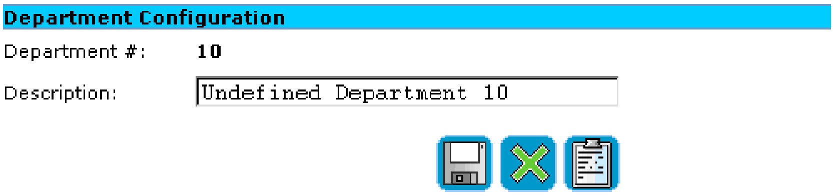
Address #2: Singapore 557180

2. The screen as shown below appears.



Department #	Description
1	Accounts Dept
2	R&D Dept
3	Sales Dept
4	Purchasing Dept
5	Engineering Dept
6	Marketing Dept
7	Service Dept
8	Project Dept
9	Production Dept
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

3. Click on any undefined **Department #** or its **Description** to configure a new department. The screen as shown below appears.



Department Configuration

Department #: 10

Description: Undefined Department 10

4. Enter a description for the department in the **Description** field and click on the button.

13.6 Set Date & Time

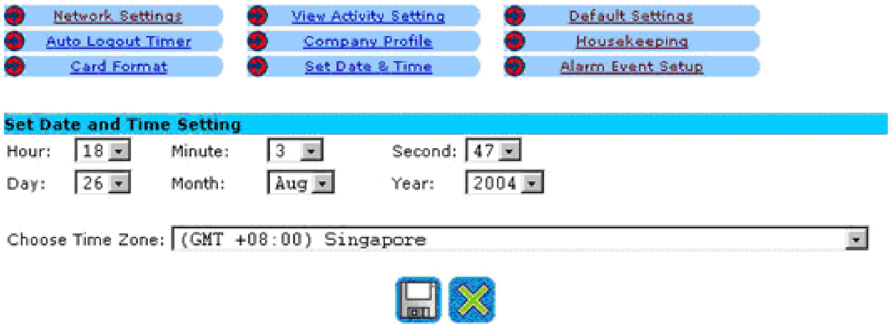
The Access Easy Master software allows user to set the date and time of the real-time clock within the server. When the date and time is set in the server, the date and time is synchronized to the controller. User can also choose the time zone in which the server is operating in.

On the other hand, the controller can have a different time zone from the server if the controller is operating in another time zone. The time from the server would be synchronized to the controller accordingly.

Time setting is in the 24-hour format.

Click on **Set Date & Time** from the menu item list and you will see a screen as shown below.

Notice!
For the transactions in **View Activity** screen, transactions from “Panel #1” will send the date and time of the activities that have taken place to the server, and the server will convert the time according to the server's time zone if the operating time zones are different.



Set Date and Time Setting

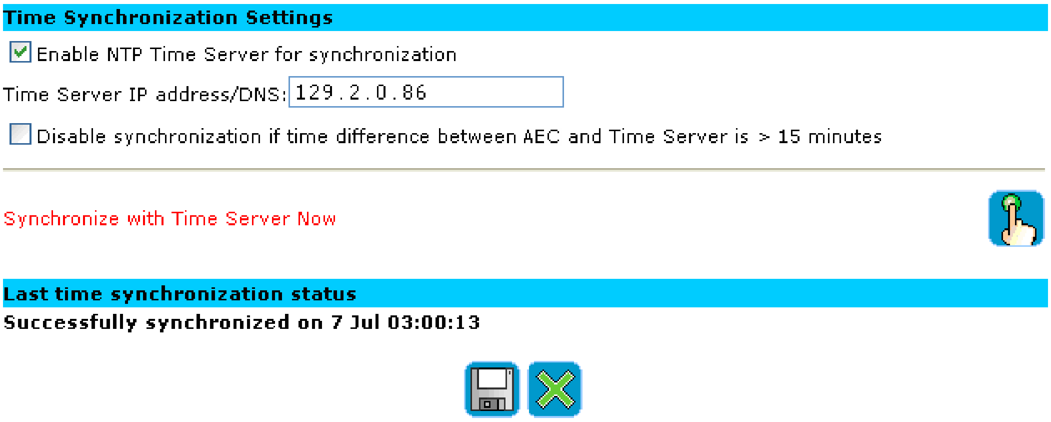
Hour: 18 Minute: 3 Second: 47
Day: 26 Month: Aug Year: 2004

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

13.6.1 How to Set the Date & Time

1. Select the appropriate time from the **Hour**, **Minute** and **Second** drop-down list.
2. Do likewise for the **Day**, **Month**, and **Year** fields.
3. Select the appropriate time zone from the **Choose Time Zone** drop-down list.
4. Click on the 💾 button.

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 controllers can be analyzed correctly.



Time Synchronization Settings

☑ Enable NTP Time Server for synchronization

Time Server IP address/DNS: 129.2.0.86

□ Disable synchronization if time difference between AEC and Time Server is > 15 minutes

Synchronize with Time Server Now

Last time synchronization status

Successfully synchronized on 7 Jul 03:00:13

1. Select **Enable NTP Time Server for synchronization** checkbox and key in the IP address of the timeserver PC in the **Time Server IP address/DNS** field.

Notice!

Refer to *APPENDIX E Setting up a Timeserver, page 239*. **Time Server IP address/DNS** field is the IP address of the PC being configured as a time server PC. Access Easy Controller is only able to synchronize with an NTP time server and will synchronize at 3 a.m. daily automatically. Auto time synchronization at 3 a.m. is only logged at transaction. However, if user manually synchronizes with the timer server, information will be logged in audit log.

2. Select **Disable synchronization if time difference between AEC and Time Server is > 15 minutes** checkbox if you want the Access Easy Controller to synchronize it's 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 time zone is incorrect.

Synchronizing date and time with an 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 IP address/DNS** field. Do not enter the domain name of the time server (e.g. time.windows.gov) in this field. Access Easy Controller will not be able to resolve the name to an IP address.

Synchronizing date and time with an intranet Time Server

It is recommended that the 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 its date and time with an Internet (external) time server, while all other PCs in the office synchronize with this intranet time server.

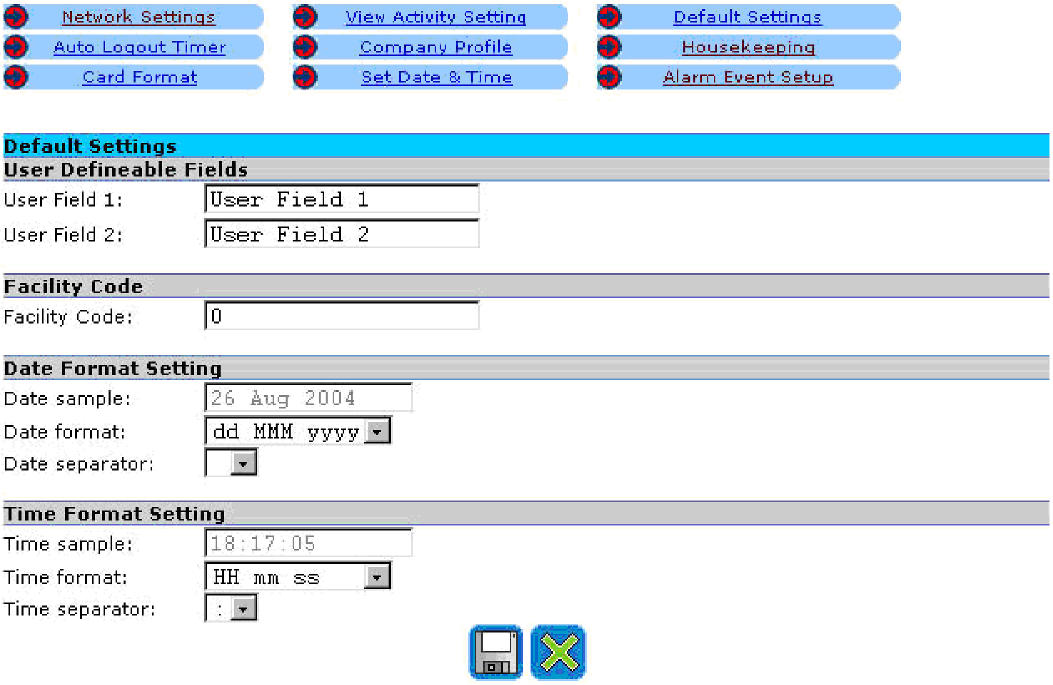
If the office does not have an Intranet time server, you could setup any existing PC on the network as a time server, hence, the Access Easy Controller could synchronize its' date and time with this PC. There are numerous freeware available that you could install in this PC to synchronize its date and time with an external time server.

In *APPENDIX E Setting up a Timeserver, page 239*, we will briefly describe how you could setup a PC as a time server.

13.7 Default Settings

This setting allows user to define the descriptive name for the two user fields, **User Field 1** and **User Field 2**, and the facility code that will appear when **Add Card** or **Batch Card** is selected from **Card Assignment** menu. The user fields are limited to 20 character each while the facility code range depends on the card format in use. User can also select the date format and the time format that he prefers to view in the **View Activity** page and all the reports to be generated.

Click on **Default Settings** from the menu item list and you will see a screen as shown below.



Default Settings

User Defineable Fields

User Field 1:	User Field 1
User Field 2:	User Field 2

Facility Code

Facility Code:	0

Date Format Setting

Date sample:	26 Aug 2004
Date format:	dd MMM yyyy
Date separator:	

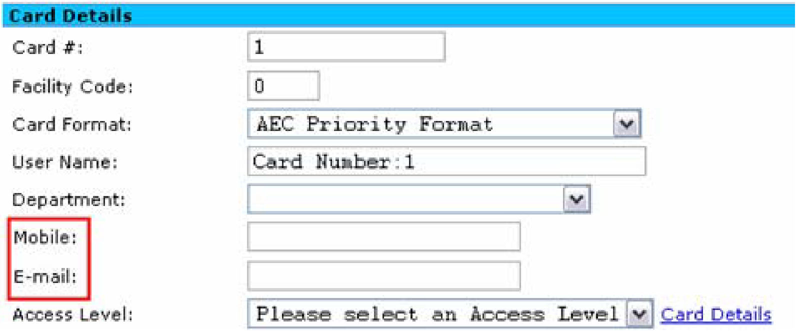
Time Format Setting

Time sample:	18:17:05
Time format:	HH mm ss
Time separator:	:

13.7.1 How to Edit the User Definable Fields

1. Delete the default text and enter the new description for **User Field 1.**
2. Repeat for **User Field 2**.
3. The above example shows that “Mobile” is used in **User Field 1** and “E-mail” is used for **User Field 2.**
4. Click on the 💾 button.

After **User Field 1** and **User Field 2** are changed, user can then see “Mobile” and “E-mail” instead when user selects **Add Card** from **Card Assignment** menu, as shown below.



Card Details

Card #:	1
Facility Code:	0
Card Format:	AEC Priority Format
User Name:	Card Number:1
Department:	
Mobile:	
E-mail:	
Access Level:	Please select an Access Level

‘

13.7.2 How to Edit the Facility Code

1. Delete 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).
2. Click on the 💾 button.

User can then see the facility code appear as default when user selects **Add Card** or **Batch Card** from **Card Assignment** menu.

13.7.3 How to Edit the Date Format

1. Select the preferred **Date format** from the drop-down list. This format is used for **View Activity** page and in all the reports generated.
2. Select a **Date separator** if desired.
3. Click on the 💾 button.

User can then see a sample of the date that will appear in the **View Activity** page and the reports to be generated in the date sample box.

13.7.4 How to Edit the Time Format

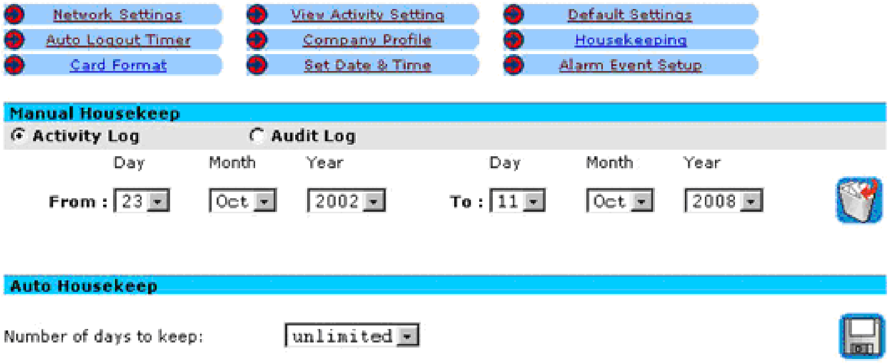
1. Select the preferred **Time format** from the drop-down list. This format is used in the **View Activity** page and in all the reports generated.
2. Select a **Time separator** if desired.
3. Click on the 💾 button.

User can then see a sample of the time that will appear in the **View Activity** page and the reports to be generated in the time sample box.

13.8 Housekeeping

Housekeeping page allows the user to manage the activity log and audit log in the system. User can delete the unwanted logs that are no longer required manually, as well as to specify the number of days of the logs to be kept in the system. The system will store the logs of the most recent specified number of days only in the system.

Click on **Housekeeping** from the menu item list and you will see a screen as shown below.



Manual Housekeep

● Activity Log ○ Audit Log

	Day	Month	Year		Day	Month	Year
From :	23	Oct	2002	To :	11	Oct	2008

Auto Housekeep

Number of days to keep: unlimited

13.8.1 How to Use the Manual Housekeeping

1. Select either the **Activity Log** or the **Audit Log** radio button for housekeeping.
2. Select the **Day**, **Month** and **Year** of the **From** and **To** date from the drop-down list. This range of dates are the dates in which the user would like to delete the activity log or the audit log (depending on which the user chooses) from the system.
3. After the range of date is selected, click on the 🗑 button to clear the log that falls within the date range.

13.8.2 How to Use the Auto Housekeeping

1. Choose the **Number of days to keep** drop-down list for the number of days that the activity and audit logs are to be kept in the system. Users are given a choice of “30”, “60”, “90” and “120” days. For example, if user chooses “30” days, the system will automatically delete the activity and audit logs from the system if they are more than 30 days from today's date. User can also choose unlimited, which means the system will not delete the logs from the system.
2. Click on the 💾 button to save the settings.

13.9 Alarm Event Setup

An alarm event is any abnormal activity which we would like to monitor and be alert when such occurrence happens. All the alarm descriptions are listed below.

Access Denied	Input Point Fault - Opened
Access Denied - Card Disabled	Input Point Fault - Shorted
Access Denied - Passback	Invalid Card
Access Denied - Time APB	Invalid End Date
Access Denied - Wrong Pin	Invalid First Card Read
Alarm	Invalid Schedule
Convertor Communication Failed	Invalid Second Card Read
Dial In - Invalid Password	Invalid Start Date
Dial In - Invalid User Name	Panel AC Failure

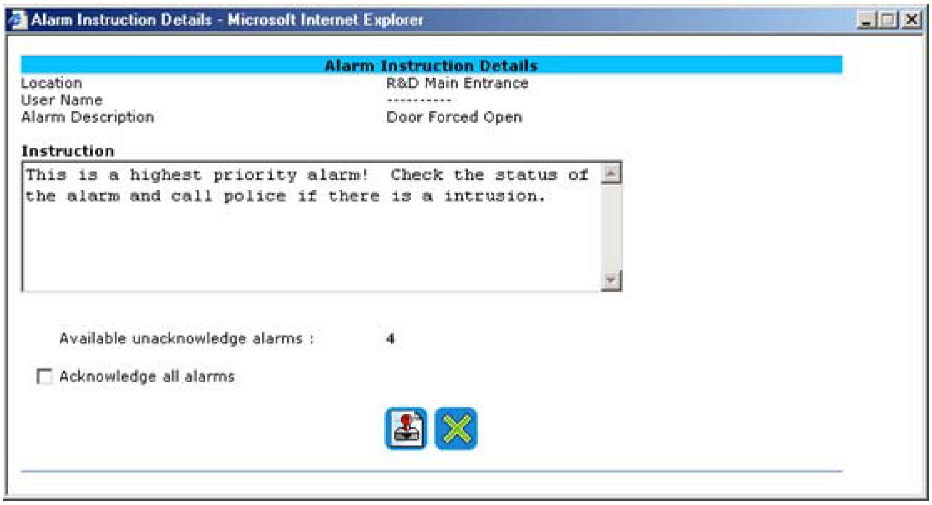
Dial In - Lockout	Panel Disconnected
Disconnected from Server	Panel Not Registered
Door Contact - Input Fault - Opened	Panel Not Registered in Server
Door Contact - Input fault - Shorted	Panel Tamper
Door Forced Open	Reader Lockout
Door Held Open	Request To Exit -Input Fault - Opened
Duress	Request To Exit -Input Fault - Shorted
Exit Denied - Passback	System Halted
Guard Tour Key Not Remove	Time Synchronization Failed

The **Alarm Event Setup** provides the required settings which will affect how the **View Activity** page will arrange the alarms and how it will respond to the user when acknowledged.

The setup includes:
- Alarm Priority Setup
- Alarm Event Condition Setup
- Alarm Instruction Message Setup

Consider this as an example. You would like all the “Door Forced Open” alarm to be given the highest global priority. The earliest “Door Forced Open” alarm will have to be acknowledged first before processing the rest of the alarms with lower global priority.

Furthermore, you would like to group the doors in terms of their location, such as “R&D Dept”, “Production Dept”, and others. These grouping will allow you to customize an alarm instruction message for each group. Hence, when the operator acknowledges a “Door Forced Open” alarm of “R&D Dept” group from the **View Activity** page, an instruction will be displayed on the screen as shown in the following screen shot.



Alarm Instruction Details

Location	R&D Main Entrance
User Name	----------
Alarm Description	Door Forced Open

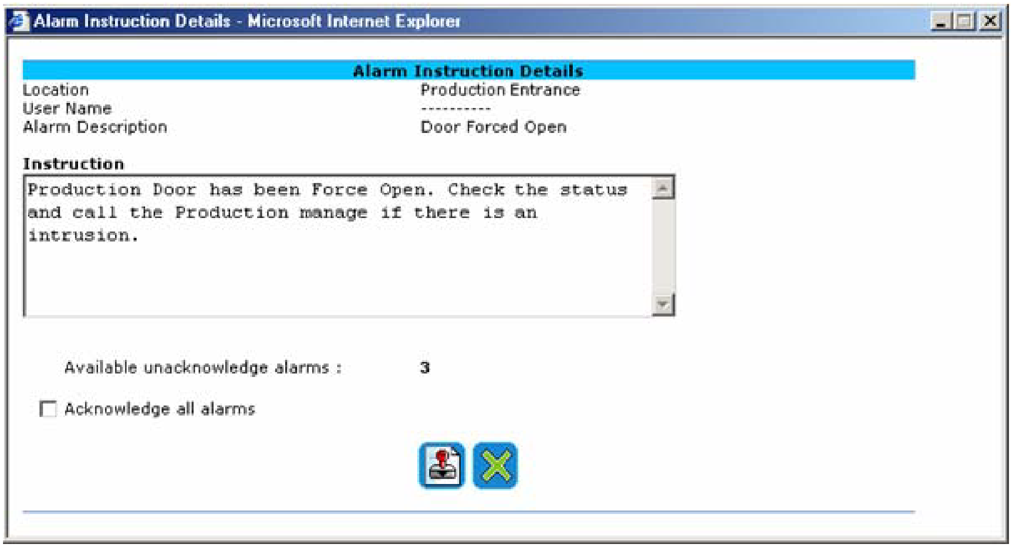
Instruction

This is a highest priority alarm! Check the status of the alarm and call police if there is a intrusion.

Available unacknowledge alarms : 4

☐ Acknowledge all alarms

While acknowledging a “Door Forced Open” alarm of “Production Dept”, a different instruction will be displayed on the screen as shown below.



Alarm Instruction Details

Location	Production Entrance
User Name	----------
Alarm Description	Door Forced Open

Instruction

Production Door has been Force Open. Check the status and call the Production manage if there is an intrusion.

Available unacknowledge alarms : 3

□ Acknowledge all alarms

The system also provides an individual alarm priority feature. This allows you to configure a very important location with a higher priority than other location when the same alarm is activated. For example, the “Store Room” is considered to be an important location to monitor. It is configured with an individual priority of “2”, while the “Door Forced Open” alarm is configured with global priority 3. Hence, if the following “Door Forced Open” alarm is activated, the “Door Forced Open” alarm of the “Store Room” will be listed on top of the rest even though it has occurred last.

Examples:
Store Room Door Forced Open 11:00am
R&D Room Door Forced Open 10:00am
Production Room Door Forced Open 10:30am

This chapter will guide you step by step in configuring the alarm events to respond the way you prefer.

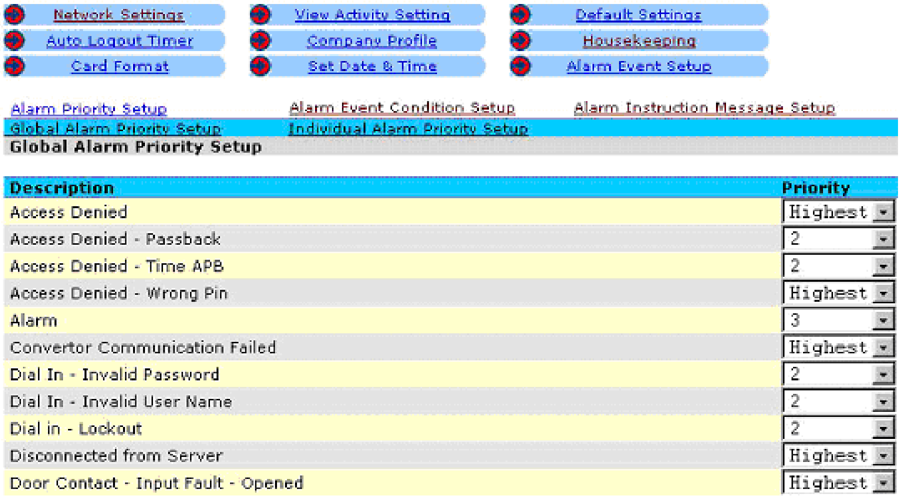
13.9.1 Alarm Priority Setup

Alarm Priority Setup can be grouped into **Global Alarm Priority Setup** and **Individual Alarm Priority Setup.** This section will describe how to configure the global and individual alarm priority.

How to Configure Global Alarm Priority Setup

This part of the setting allows you to define the hierarchy of priorities for alarms.

1. Click on **Alarm Event Setup** from the menu item list and you will see a screen as shown below. The default screen is the **Global Alarm Priority Setup** screen.



Global Alarm Priority Setup

Description	Priority
Access Denied	Highest
Access Denied - Passback	2
Access Denied - Time APB	2
Access Denied - Wrong Pin	Highest
Alarm	3
Convertor Communication Failed	Highest
Dial In - Invalid Password	2
Dial In - Invalid User Name	2
Dial in - Lockout	2
Disconnected from Server	Highest
Door Contact - Input Fault - Opened	Highest

2. Select the priority of each type of alarm from the **Priority** drop-down list. The priority of the alarms can range from “1” to “128”, with priority “1” as the highest priority and is denoted by “Highest”, and priority “128” the lowest priority and is denoted by “Lowest”.

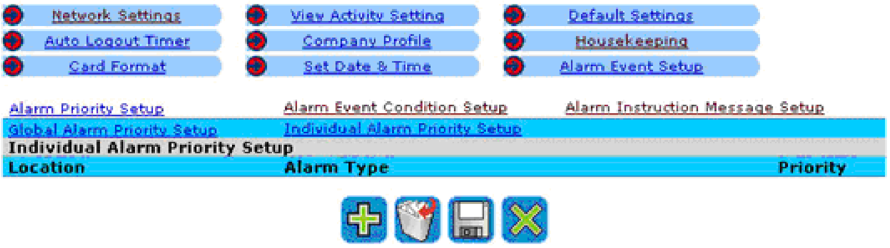
3. To complete the setting, click on the icon to save.

Notice!
View Activity page will sort the alarms in the following order: (1) priority (2) date and time of occurrence.

How to Configure Individual Alarm Priority Setup

This part of the setting allows you to define the hierarchy of priorities for individual location alarms.

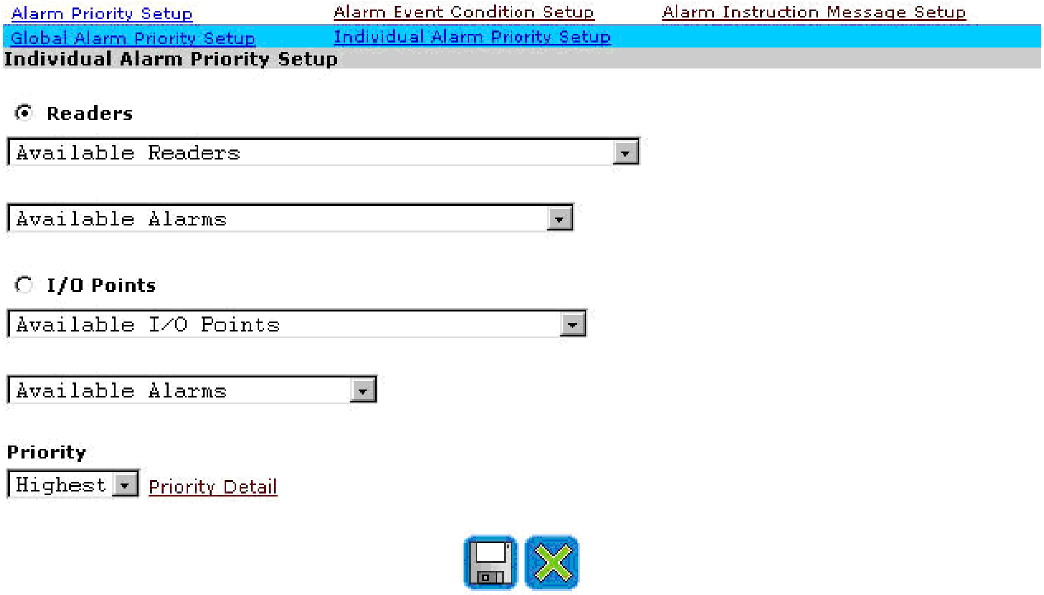
1. From the **Global Alarm Priority Setup** screen, click on the **Individual Alarm Priority Setup** link. A screen as shown below appears.



Individual Alarm Priority Setup

Location	Alarm Type	Priority

2. Click on the ✚ button to add a new individual alarm priority to the system. The screen as shown below appears.



Alarm Priority Setup　Alarm Event Condition Setup　Alarm Instruction Message Setup

Global Alarm Priority Setup　Individual Alarm Priority Setup

Individual Alarm Priority Setup

● Readers

Available Readers

Available Alarms

○ I/O Points

Available I/O Points

Available Alarms

Priority

Highest　Priority Detail

3. Select the appropriate option button.
   If **Reader** radio button is selected, you will need to select which readers to assign this priority from the **Available Readers** drop-down list. The **Available Alarms** drop-down list allows you to choose which type of alarm this selected reader will have the priority.
   If **I/O Points** radio button is selected, you will need only to select which input point from the **Available I/O Points** drop-down list to assign this priority.
4. Next select the level of priority from the **Priority** drop-down list.
5. To save the setting, click on the 💾 button.

13.9.2 Alarm Event Condition Setup

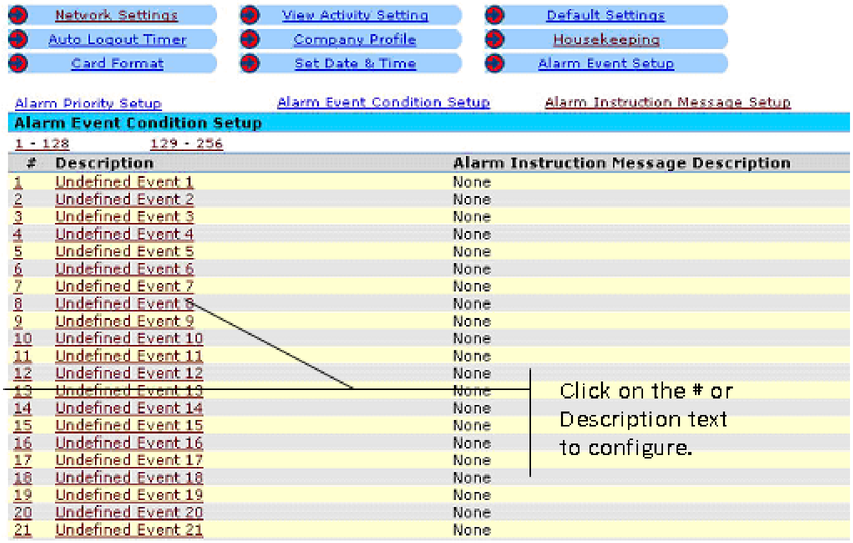
This part of the setting allows you to define up to 256 different alarm event. Each alarm event can consist of a combination of alarms, devices and alarm instruction message.

An alarm event allows you to customize the alarm instruction message that will be displayed when the user acknowledges an alarm from the **View Activity** page.

Referring to the previous example, let’s say you would like the user to see an instruction message for the “Door Forced Open” alarm and “Invalid Card” alarm in “R&D Dept” and a different instruction message for the “Door Forced Open” alarm and “Invalid Card” alarm in “Production Dept”.

You will need to configure two different alarm events. Let's use this example as we guide you through the configuration.

1. From the **Alarm Event Setup** screen, click on the **Alarm Event Condition Setup** link. The **Alarm Event Condition Setup** screen will appear as shown below.



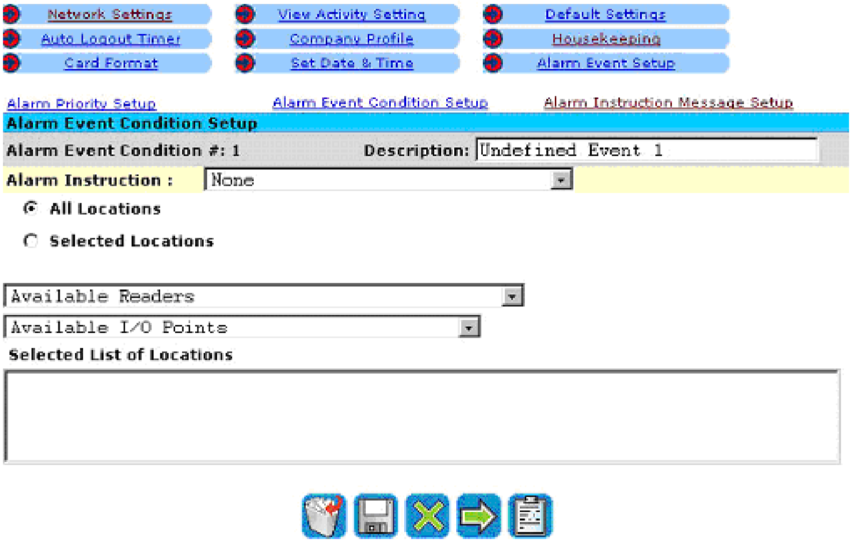
Alarm Event Condition Setup

1 - 128 129 - 256

#	Description	Alarm Instruction Message Description
1	Undefined Event 1	None
2	Undefined Event 2	None
3	Undefined Event 3	None
4	Undefined Event 4	None
5	Undefined Event 5	None
6	Undefined Event 6	None
7	Undefined Event 7	None
8	Undefined Event 8	None
9	Undefined Event 9	None
10	Undefined Event 10	None
11	Undefined Event 11	None
12	Undefined Event 12	None
13	Undefined Event 13	None
14	Undefined Event 14	None
15	Undefined Event 15	None
16	Undefined Event 16	None
17	Undefined Event 17	None
18	Undefined Event 18	None
19	Undefined Event 19	None
20	Undefined Event 20	None
21	Undefined Event 21	None

Click on the # or Description text to configure.

2. Select any of the “Undefined” events to configure an alarm event condition. The following screen will appear.



Alarm Event Condition Setup

Alarm Event Condition #: 1 Description: Undefined Event 1

Alarm Instruction : None

● All Locations

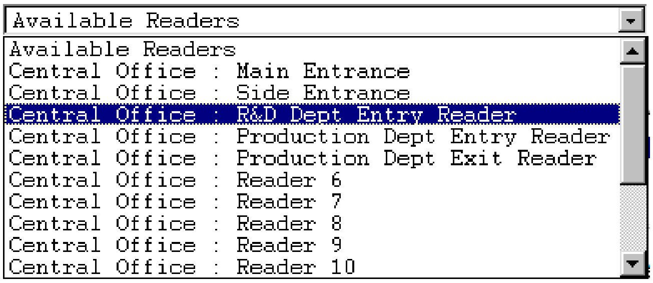
○ Selected Locations

Available Readers

Available I/O Points

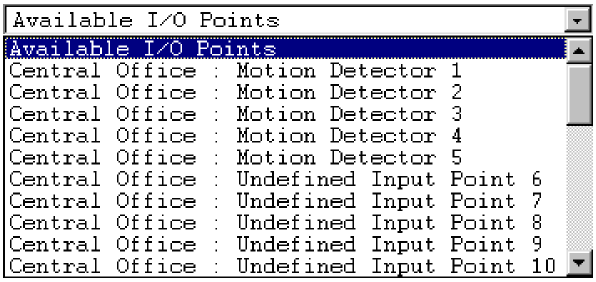
Selected List of Locations

3. Enter a name for the alarm event in the **Description** field.
4. Choose the appropriate radio button.
   Choose **All Locations** radio button if all readers, input points and output points are monitored for the events.
   Choose **Selected Locations** radio button if the devices in the **Selected list of Locations** list box are monitored for the events.
   In the case of this example, choose **Selected Locations** radio button, as we only want those doors belonging to “R&D Dept” to display the alarm instruction message.
5. If **Selected Locations** radio button is chosen, you will need to select the readers or input points or output points from the drop-down list.
   The **Available Readers** drop-down list contains all the readers that are available in the entire system.



```
Available Readers
Available Readers
Central Office : Main Entrance
Central Office : Side Entrance
Central Office : R&D Dept Entry Reader
Central Office : Production Dept Entry Reader
Central Office : Production Dept Exit Reader
Central Office : Reader 6
Central Office : Reader 7
Central Office : Reader 8
Central Office : Reader 9
Central Office : Reader 10
```

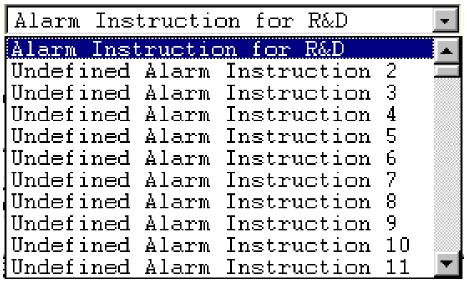
The **Available I/O Points** drop-down list contains all the input points and output points that are available in the entire system.



```
Available I/O Points
Available I/O Points
Central Office : Motion Detector 1
Central Office : Motion Detector 2
Central Office : Motion Detector 3
Central Office : Motion Detector 4
Central Office : Motion Detector 5
Central Office : Undefined Input Point 6
Central Office : Undefined Input Point 7
Central Office : Undefined Input Point 8
Central Office : Undefined Input Point 9
Central Office : Undefined Input Point 10
```

Choose the desired readers, input points or output points to be added to the **Selected list of Locations** list box by clicking on the description of the device. For this example, “R&D Dept Entry Reader” is selected, as shown above.

6. After selecting all the devices to be included in the **Selected list of Location** list box, the next step is to select the relevant alarm instruction message that you would like the user to see when they acknowledge the alarm.
7. The **Alarm Instruction** drop-down list provides a list of available messages that you could select.



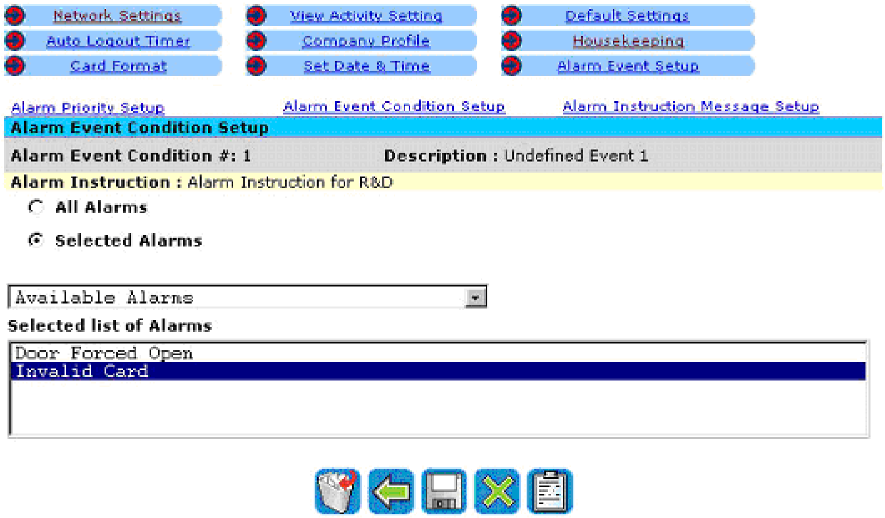
```
Alarm Instruction for R&D
Alarm Instruction for R&D
Undefined Alarm Instruction 2
Undefined Alarm Instruction 3
Undefined Alarm Instruction 4
Undefined Alarm Instruction 5
Undefined Alarm Instruction 6
Undefined Alarm Instruction 7
Undefined Alarm Instruction 8
Undefined Alarm Instruction 9
Undefined Alarm Instruction 10
Undefined Alarm Instruction 11
```

Select the appropriate alarm instruction message as shown above.

Notice!
Alarm instruction messages are configured in the **Alarm Instruction Message Setup**. Please refer to the next section for details

8. Click the ➡ button to save and go to next page.

9. The next page that appears allows you to select the type of events that will display the alarm instruction messages that you have just selected.



Alarm Event Condition Setup

Alarm Event Condition #: 1 **Description :** Undefined Event 1

Alarm Instruction : Alarm Instruction for R&D

○ **All Alarms**

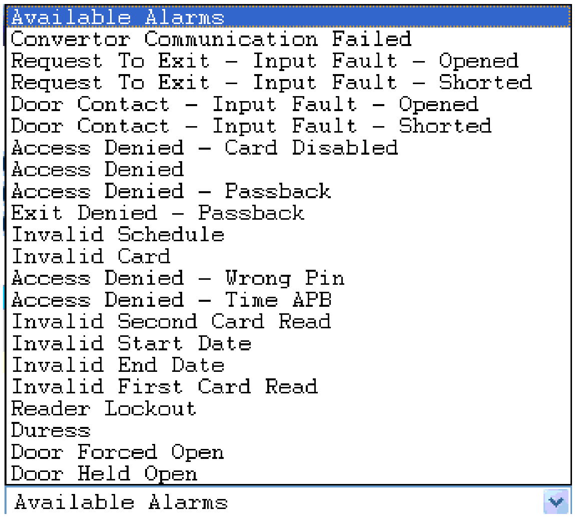
● **Selected Alarms**

Available Alarms

Selected list of Alarms

Door Forced Open
Invalid Card

10. Choose the appropriate radio button.
Choose **All Alarms** radio button if all the alarms will use the same alarm instruction message as configured earlier.
Choose **Selected Alarms** radio button if only the alarms in the **Selected list of Alarms** list box will display the alarm instruction message as configured earlier.
In this example, choose **Selected Alarms** radio alarm as we only want those “Door Forced Open” alarm and “Invalid Card” alarm to display the alarm instruction message.
11. If **Selected Alarms** radio button is chosen, you will need to select the type of alarms from the drop-down list. The **Available Alarms** contains all the different types of alarms that are available in the entire system.



```
Available Alarms
Convertor Communication Failed
Request To Exit - Input Fault - Opened
Request To Exit - Input Fault - Shorted
Door Contact - Input Fault - Opened
Door Contact - Input Fault - Shorted
Access Denied - Card Disabled
Access Denied
Access Denied - Passback
Exit Denied - Passback
Invalid Schedule
Invalid Card
Access Denied - Wrong Pin
Access Denied - Time APB
Invalid Second Card Read
Invalid Start Date
Invalid End Date
Invalid First Card Read
Reader Lockout
Duress
Door Forced Open
Door Held Open
Available Alarms
```

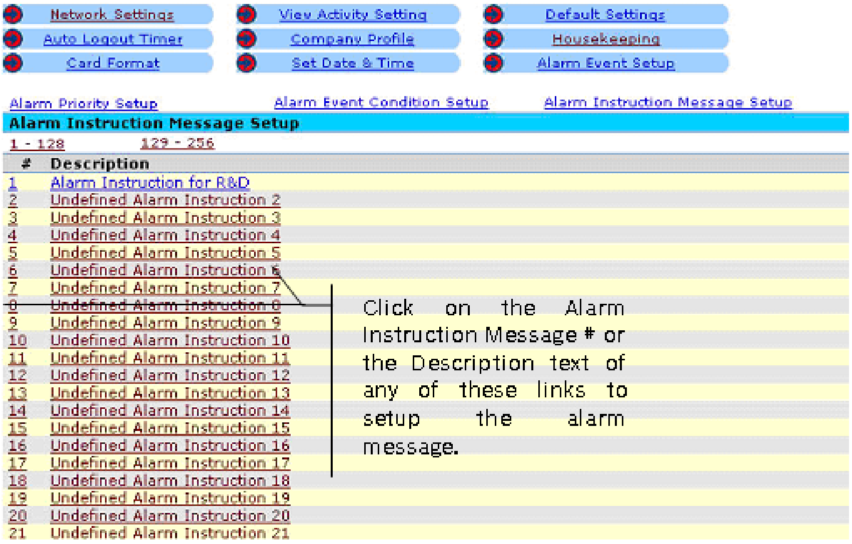
Choose the desired alarms to be added to the **Selected list of Alarms** list box by clicking on the description of the alarm. For the example, “Door Forced Open” and “Invalid Card” care selected.

12. Lastly, click on 💾 to save the settings.

13.9.3 Alarm Instruction Message setup

This part of the setting allows you to define up to 255 different alarm instruction message for the alarm event conditions.

1. From the **Alarm Event Setup** screen, click on the **Alarm Instruction Message Setup** link. The **Alarm Instruction Message Setup** screen will appear as shown below.



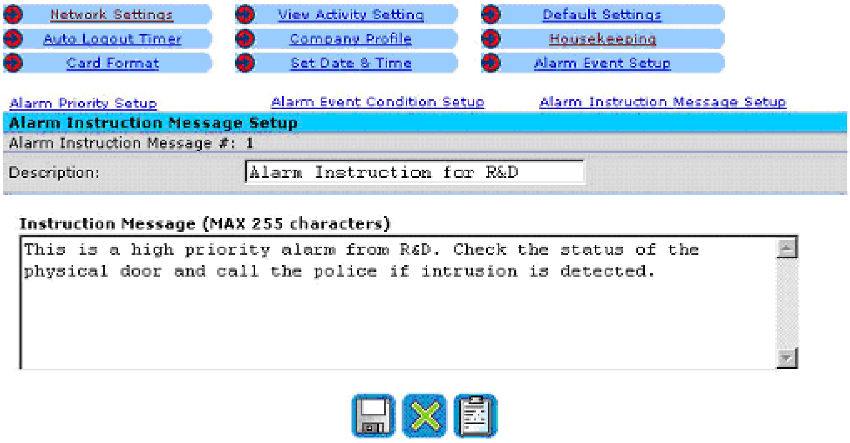
Alarm Instruction Message Setup

1 - 128 129 - 256

#	Description
1	Alarm Instruction for R&D
2	Undefined Alarm Instruction 2
3	Undefined Alarm Instruction 3
4	Undefined Alarm Instruction 4
5	Undefined Alarm Instruction 5
6	Undefined Alarm Instruction 6
7	Undefined Alarm Instruction 7
8	Undefined Alarm Instruction 8
9	Undefined Alarm Instruction 9
10	Undefined Alarm Instruction 10
11	Undefined Alarm Instruction 11
12	Undefined Alarm Instruction 12
13	Undefined Alarm Instruction 13
14	Undefined Alarm Instruction 14
15	Undefined Alarm Instruction 15
16	Undefined Alarm Instruction 16
17	Undefined Alarm Instruction 17
18	Undefined Alarm Instruction 18
19	Undefined Alarm Instruction 19
20	Undefined Alarm Instruction 20
21	Undefined Alarm Instruction 21

Click on the Alarm Instruction Message # or the Description text of any of these links to setup the alarm message.

2. Click on any of the “Undefined” alarm instruction to configure an alarm instruction message. The following screen will appear.



Alarm Instruction Message Setup

Alarm Instruction Message #: 1

Description: Alarm Instruction for R&D

Instruction Message (MAX 255 characters)

This is a high priority alarm from R&D. Check the status of the physical door and call the police if intrusion is detected.

3. Enter a name for the alarm instruction message in the **Description** fied.
4. The **Instruction Message** textbox provides a space for you to enter up to 255 characters. You could enter the instruction that you want to pop up on the screen when the user acknowledges the alarm. Please refer to the previous section for the assignment of alarm instruction message to alarm event condition.
5. To complete the setup click on 💾 to save the settings.

14 Report Generation

Report Generation feature allows us to generate report for activities which have occurred. It has a filtering mechanism to find and sort out activities based on the criteria set by the user. The criteria that could be defined are:

1. Date/Time
2. Devices
3. Card Holders
4. Events

By combining the correct combination, the user could generate a detail and specific report. The criteria can also be saved for further use.

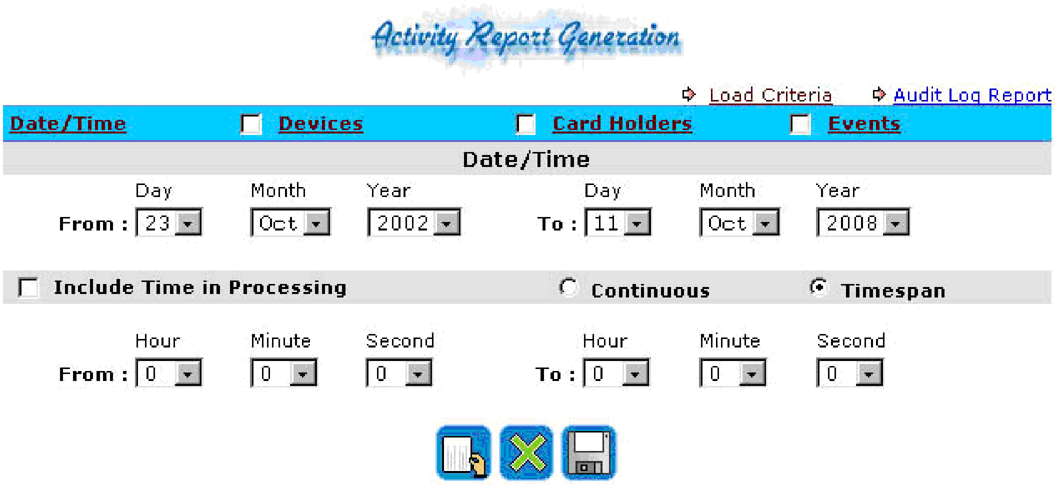
Notice!
The more criteria is defined, the more accurate and precise is the report. However, an incorrect mix of criteria will result in not finding the information you need. Please refer to *APPENDIX A Selecting Events, Devices and Cardholders for Reports, page 231* for information on selecting the criteria.

Notice!
The **Report Generation** can only generate 2000 records each time. Users will be warned by a message box to reduce the range of the date and time selection if the records exceed 2000.

The following sections will provide a step-by-step guide to configuring a criteria for report generation purpose.

14.1 How to Set Criteria for Report Generation

Select the **Report Generation** link on the left pane and the **Report Generation** page will appear as shown below.



Activity Report Generation

Load Criteria   Audit Log Report

Date/Time   □ Devices   □ Card Holders   □ Events

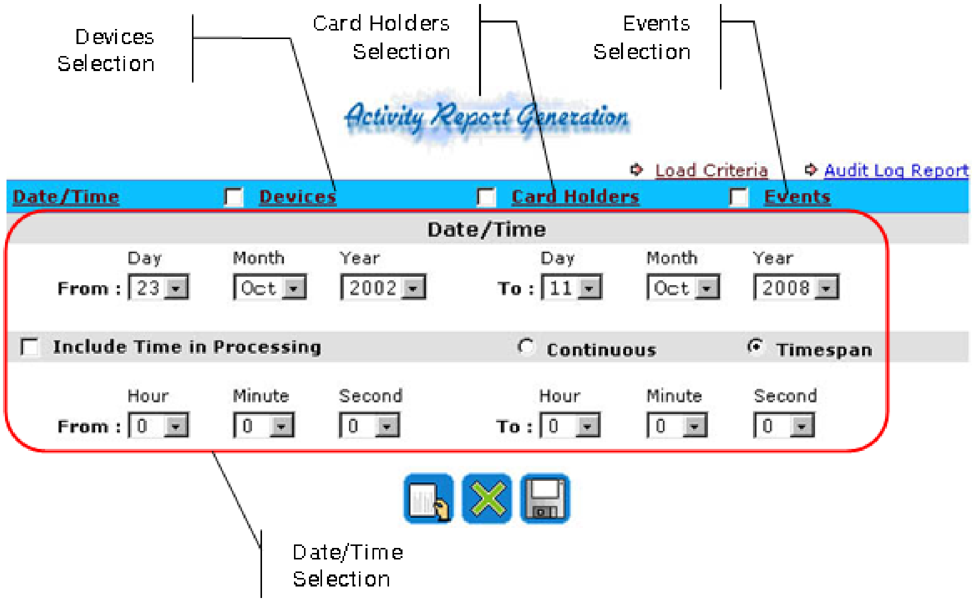
Date/Time

	Day	Month	Year		Day	Month	Year
From :	23	Oct	2002	To :	11	Oct	2008

□ Include Time in Processing   ○ Continuous   ● Timespan

	Hour	Minute	Second		Hour	Minute	Second
From :	0	0	0	To :	0	0	0

Now let us take a brief look at the screen layout of the **Report Generation** page.



Activity Report Generation

Load Criteria Audit Log Report

Date/Time □ Devices □ Card Holders □ Events

Date/Time

From : Day 23 Month Oct Year 2002 To : Day 11 Month Oct Year 2008

□ Include Time in Processing ○ Continuous ● Timespan

From : Hour 0 Minute 0 Second 0 To : Hour 0 Minute 0 Second 0

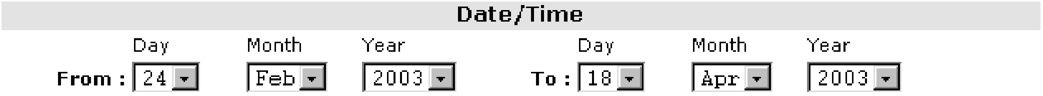
In order to successfully generate a report, you will need to specify the criteria for the Access Easy Master. The following will explain the purpose and usage of each selection.

Selection Criteria	Usage
Date/Time	Date is a compulsory selection. User needs to identify what is the range of date the report should cover. The activities that occur within these dates will be listed in the report. Time, however, is an optional selection. User could specify the time period of interest that the activities have occurred. The activities that occur during this period of time will be listed in the report.
Devices	This is an optional selection. It lists devices such as reader and I/O point for selection. The activities that are generated by the selected list of devices will be listed in the report.
Card Holders	This is an optional selection. Specific card holder can be chosen. The activities that are generated by the selected list of card holders will be listed in the report.
Events	This is an optional selection. User could specify the type of activities to be included in the report.

By creating a combination of all the selections, the user would print a summary of the required report in the shortest time. Let us look into an example as we go through the steps of configuring the criteria.

We would like to print out all the “Door Forced Open” alarms (events) that occur to “R&D Main Entrance Door” (device) from “24 Feb 2003 to 18 April 2003” (date) between “8am to 5pm” (time).

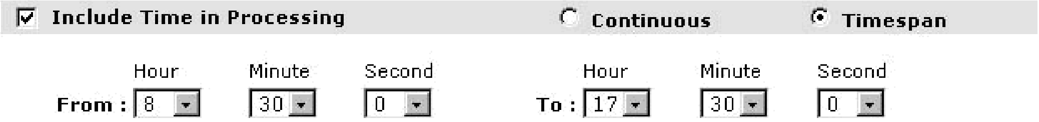
1. First of all, select the **From Date** and the **To Date** from the **Date/Time** section.



Date/Time

From : Day 24 Month Feb Year 2003 To : Day 18 Month Apr Year 2003

2. Next, select the **From Time** and the **To time** and check the **Include Time in Processing** checkbox. User also has to select whether the time is continuous or according to timespan by selecting the appropriate radio button. Continuous time means that the report will be generated all the way from the starting time of the starting date to the end time of the ending date. Timespan means that the report will be generated from the starting time to the ending time for each day in the selected date range.

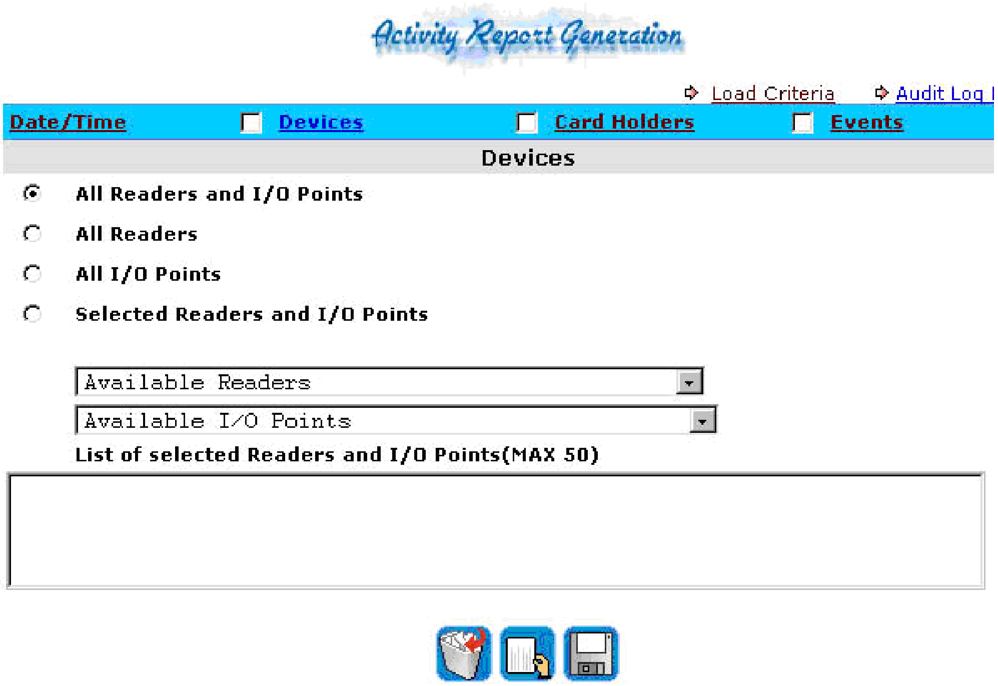


☑ Include Time in Processing ○ Continuous ● Timespan

	Hour	Minute	Second		Hour	Minute	Second
From :	8	30	0	To :	17	30	0

Notice!
If the **Include Time in Processing** checkbox is not selected, the report will be generated according to the other selected criteria, without any time filtering.

3. To configure the devices selection, click on the **Devices** link and the following screen will appear.



Activity Report Generation

Date/Time □ Devices □ Card Holders □ Events

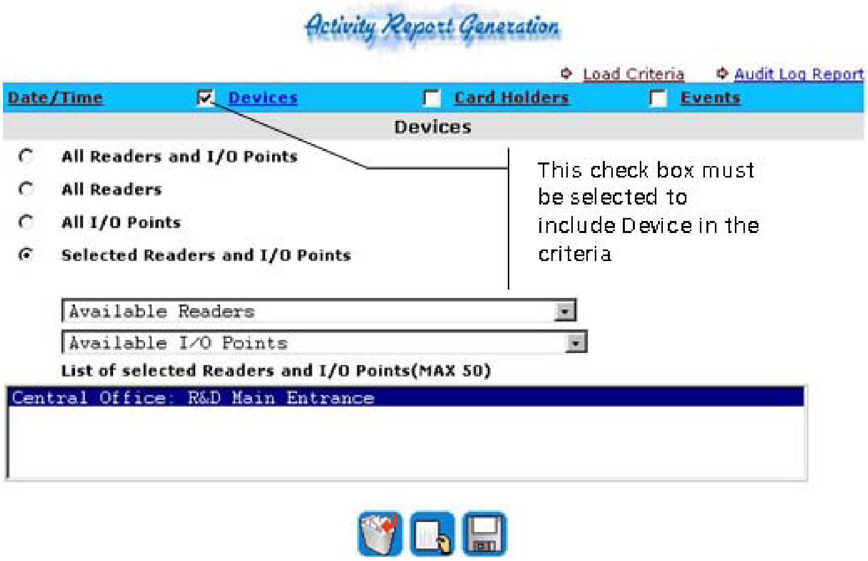
Devices

● All Readers and I/O Points
○ All Readers
○ All I/O Points
○ Selected Readers and I/O Points

Available Readers
Available I/O Points
List of selected Readers and I/O Points(MAX 50)

4. Choose the appropriate radio button.
Choose **All Readers and I/O Point** radio button if all activities of devices such as readers, input points and output points are taken into account in the generation of report.
Choose **All Readers** radio button if only activities of readers will be taken into account in the generation of report. Selection of this option will result in only readers' activities to be included in the report.
Choose **All I/O Points** radio button if only activities of input points and output points will be taken into account in the generation of report. Selecting this option will result in only I/O points' activities to be included in the report.
Choose **Selected Readers and I/O Points** radio button if only selected devices' activities listed in the **List of selected Readers and I/O Points** list box will be taken into account in the generation of report.
In this example, choose **Selected Readers and I/O Points**, as we only want “Door Force Open” alarms from “R&D Main Entrance” to be included in the report, as shown below.

5. Check the **Devices** checkbox to indicate that devices selection is to be included in the criteria, as shown below.



☑ Devices □ Card Holders □ Events

○ All Readers and I/O Points
○ All Readers
○ All I/O Points
● Selected Readers and I/O Points

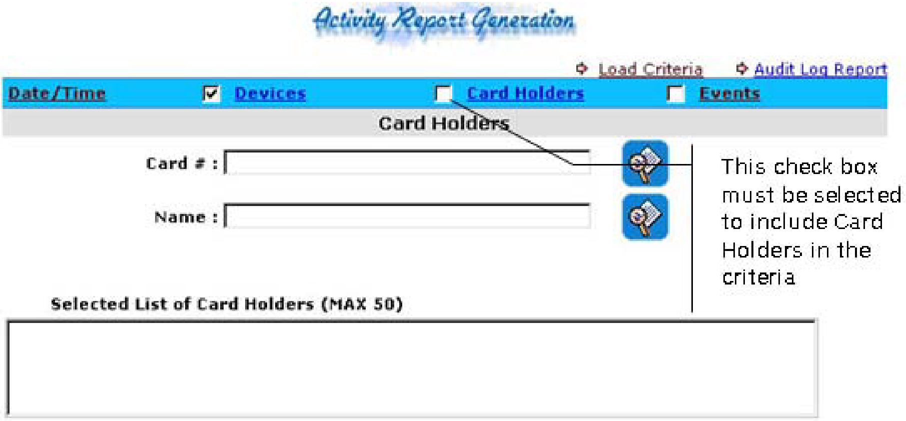
List of selected Readers and I/O Points(MAX 50)

Central Office: R&D Main Entrance

This check box must be selected to include Device in the criteria

Notice!
The selected device will not be taken into consideration during the generation of the report if the **Devices** checkbox is not selected.

6. Click on the **Card Holders** link to go to the next configuration page. A screen as shown below appears.



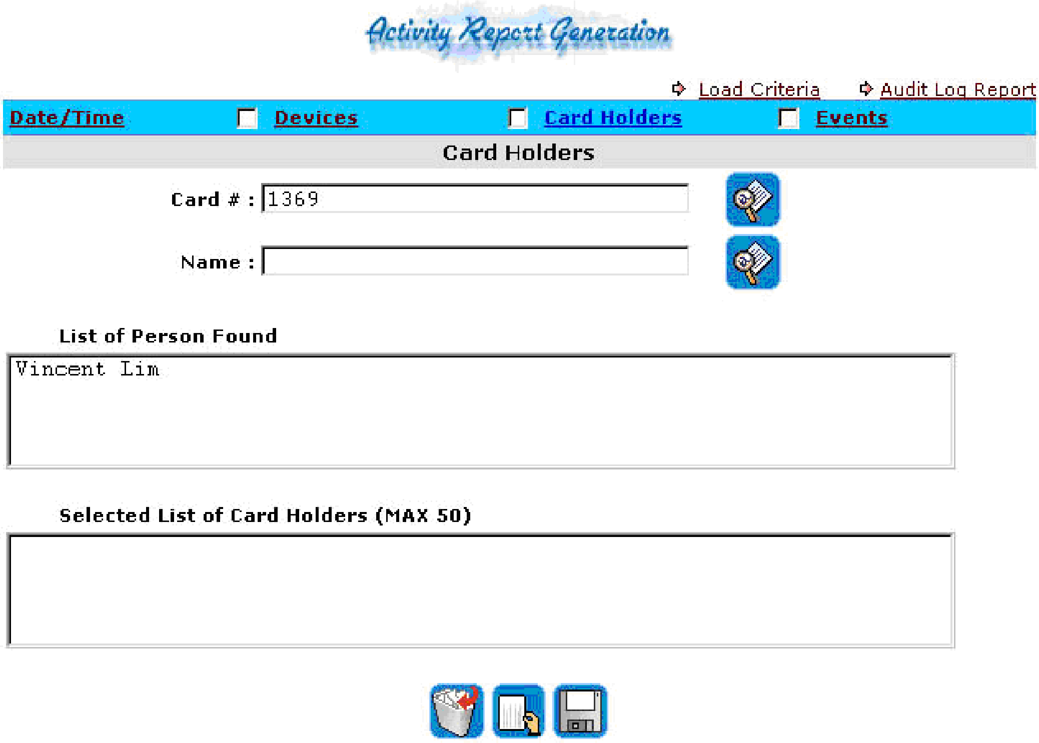
☑ Devices □ Card Holders □ Events

This check box must be selected to include Card Holders in the criteria

7. This page allows you to configure the cardholders that should be included in the report criteria. Check the **Card Holders** checkbox to include this selection in the criteria. Take note that some of the activities do not have the cardholder's ID included. Activities such as “Panel Tampered”, “Exit Grant”, “Door Force Open”, and others do not require the card holder selection to be configured.
In the case of this example, we will not select the card holder selection as the activities we need to generate do not require this selection, which is “Door Forced Open” alarm from “R&D Main Entrance” door.

Notice!
Care should be taken when including the card holders selection into the criteria. By including the card holders into the criteria, activities that do not require this will not appear in the report, such as
"Panel Tampered", "Exit Grant", "Door Force Open", and others. Please refer to *APPENDIX A Selecting Events, Devices and Cardholders for Reports, page 231* for a guide in selecting the correct combination of selection for criteria.
The card holder will not be taken into consideration during the generation of the report if the **Card Holders** checkbox is not selected.

8. For the activities that require the card holders selection to be included in the criteria, follow steps 9 to 13.
9. Only cardholders' ID indicated in the **Selected List of Card Holders** list box will be included in the criteria. To add a cardholder's ID to the list, you could search by card number or by name.
10. To search by card ID, enter the card ID in the **Card #** text box and click on the corresponding button. Access Easy Master will search through the card database and list out the cards that have the ID in the **List of Person Found** list box as shown on the following page.



Activity Report Generation

Card Holders

Card # : 1369

Name :

List of Person Found

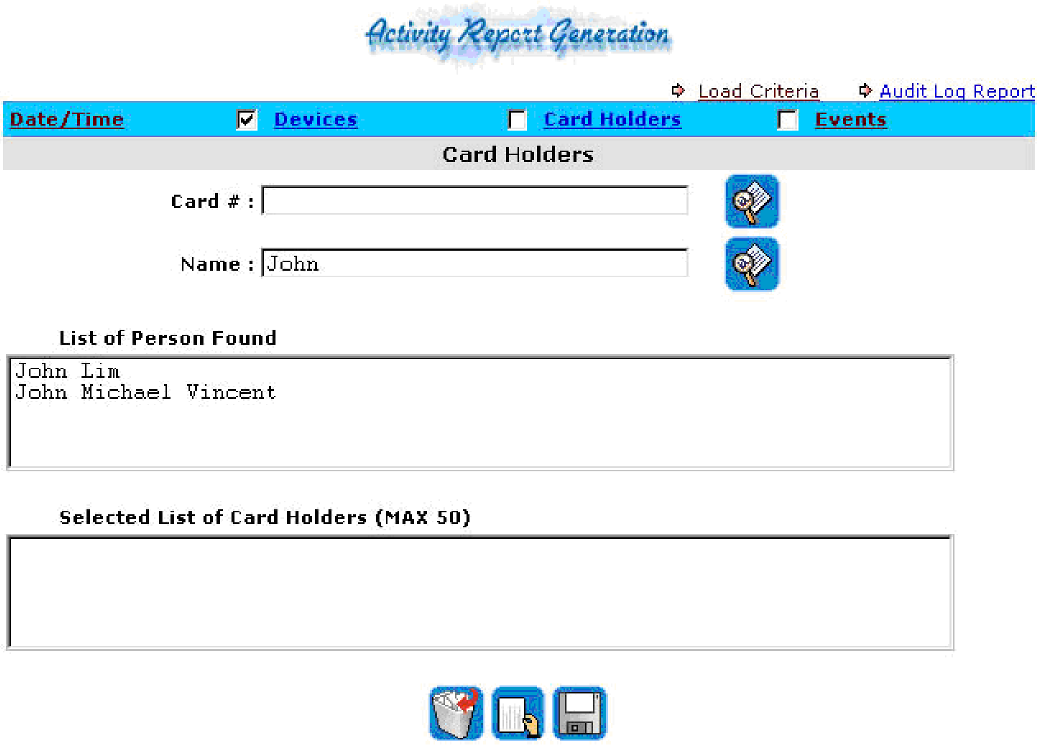
Vincent Lim

Selected List of Card Holders (MAX 50)

11. Click on the name of the cardholder from the **List of Person Found** list box to add to the **Selected List of Card Holders** list box.

Notice!
If there are two or more IDs that are the same but with different facility code or card format, the search will still show all of them in the **List of Persons Found** list box.

12. To search by cardholder's name, enter the name in the **Name** textbox and click on the corresponding 🔍 button. Access Easy Master will search through the card database and list out the cards that has similar name in the **List of Person Found** list box as shown below.



Card # :

Name : John

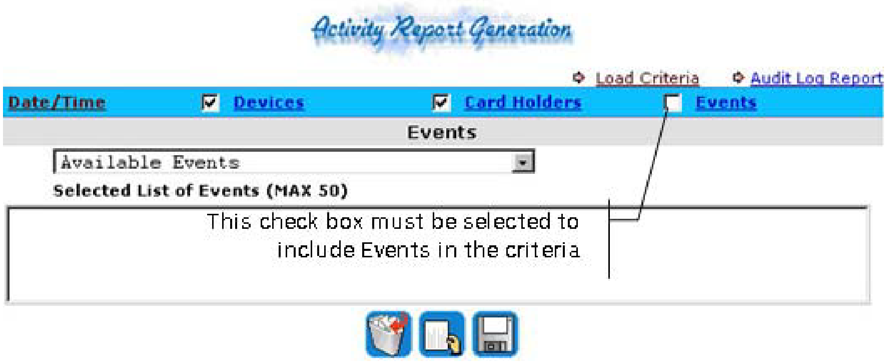
List of Person Found

John Lim
John Michael Vincent

Selected List of Card Holders (MAX 50)

Notice!
The above screen shows two names in the **List of Persons Found** list box. This is the result of searching the name "John". Access Easy Master will show all names that are similar, allowing the user to find the one that he needs without knowing the full name of the cardholder.

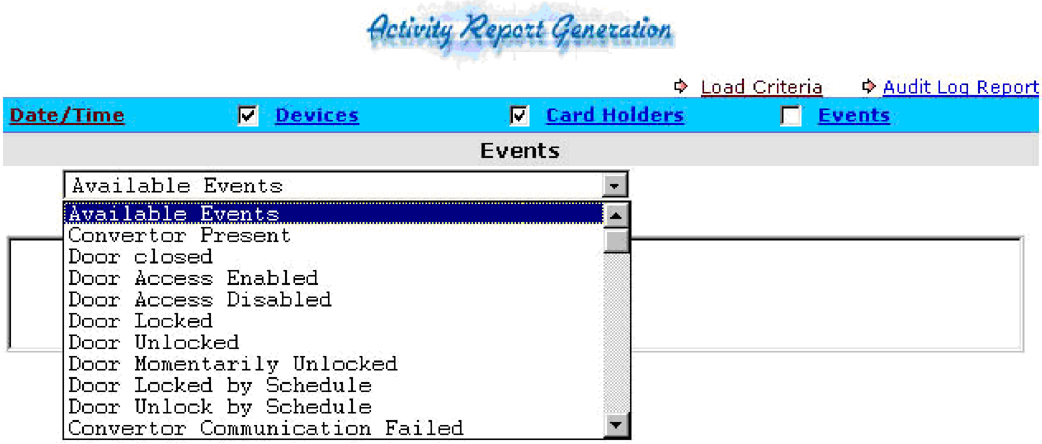
13. Click on the name of the cardholder from the **List of Person Found** list box to add to the **Selected List of Card Holders** list box.
14. The next step will be to configure the events selection. Click on the **Events** link and the following screen will appear.



This check box must be selected to include Events in the criteria

Notice!
The events will not be taken into consideration during the generation of the report if the **Events** checkbox is not selected.

15. Select the relevant events from the drop-down list. Click on the events, such as “Door Forced Open”, to add them to the **Selected List of Events** list box.



Activity Report Generation

Load Criteria Audit Log Report

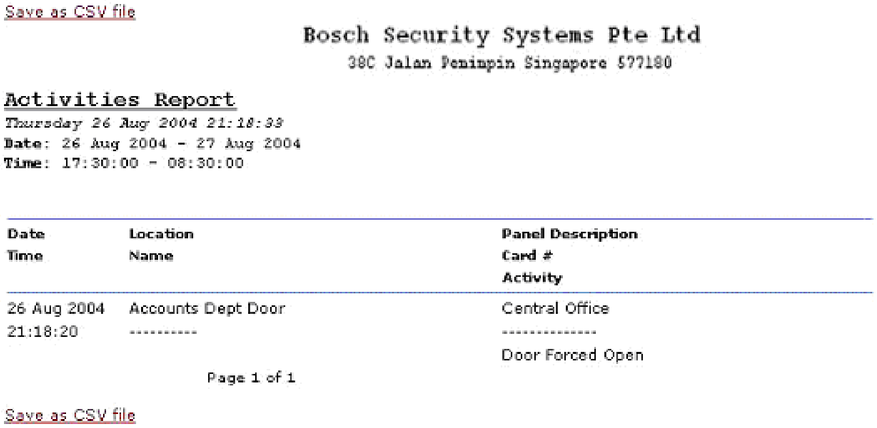
Date/Time ☑ Devices ☑ Card Holders □ Events

Events

Available Events

- Available Events
- Convertor Present
- Door closed
- Door Access Enabled
- Door Access Disabled
- Door Locked
- Door Unlocked
- Door Momentarily Unlocked
- Door Locked by Schedule
- Door Unlock by Schedule
- Convertor Communication Failed

16. To start generating the report, click . The following is a sample of the report generated.



Save as CSV file

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Activities Report
Thursday 26 Aug 2004 21:18:33
Date: 26 Aug 2004 - 27 Aug 2004
Time: 17:30:00 - 08:30:00

Date Time	Location Name	Panel Description Card # Activity
26 Aug 2004 21:18:20	Accounts Dept Door ----------	Central Office -------------- Door Forced Open

Page 1 of 1

Save as CSV file

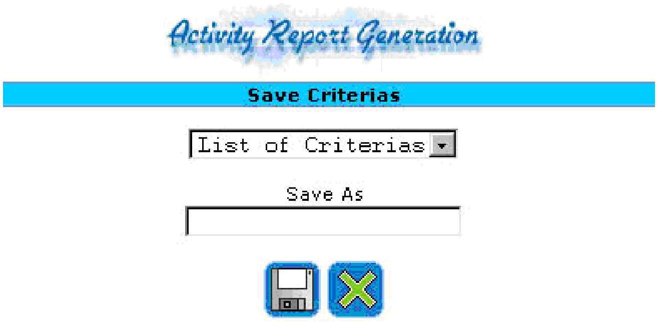
Notice!
The report can be saved in a CSV format. This format is basically a text file in which the data are separated by a comma “,”. To save in CSV format, click on the **Save as CSV file** link and a dialog box will appear for you to download the file to your local PC.

14.2 How to Save Criteria for Future Use

Criteria created in the previous section can be saved in the Access Easy Master for future use. This is very helpful when the user needs to generate daily, weekly or monthly reports. By saving the criteria, the user need not re-configure the selections. Instead he could just call out the criteria that have been saved previously and generate the report with new date and time settings.

The following step shows you how to save the criteria in the Access Easy Master.

1. After configuration the criteria, click on the 💾 to save the criteria. The following screen shows the **Save Criteria** page.

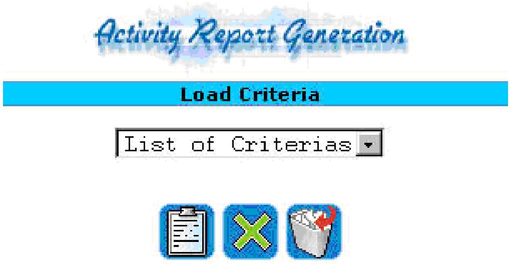


2. Type a name in the **Save As** textbox and click on the 💾 button.

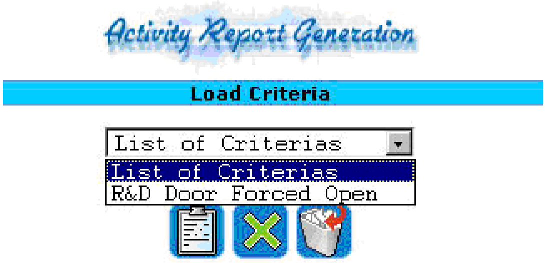
14.3 How to Generate Report Using Saved Criteria

To generate reports using previously saved criteria, you will need to load the criteria from the Access Easy Master.

1. From the **Report Generation** page, click on ➪ Load Criteria at the top right corner of the page and the **Activity Report Generation** screen will appear as shown below.



2. You could now select the criteria from the **List of Criterias** drop-down list.



3. After selecting the criteria that you need, click on the 📋 to load it.
4. The screen will refresh and the **Report Generation** page will be shown with the settings of the loaded criteria. Now all you need to do is set the date and time range and you could click 📄 to generate your report based on the loaded criteria.

14.4 How To Generate Audit Log Report

Audit log records all the changes to the system parameters and who made the changes. It is a means to trace back what was done to the system by the login user. There are two types of audit trail report that can be generated, they are:

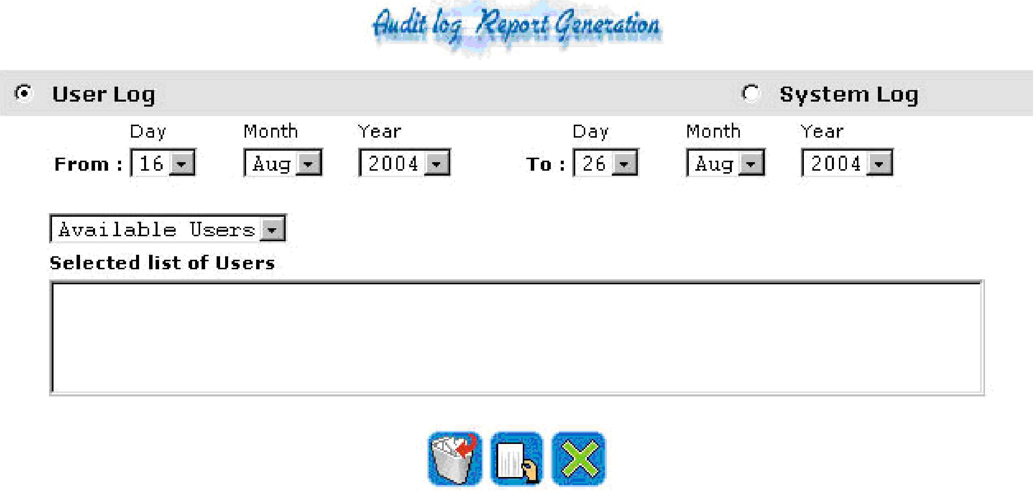
- User Log
- System Log

The following section provides a step-by-step guide to generate the reports.

14.4.1 User Log

The **User Log** report provides a report on who has login and when it was done. It also captures the changes done by the User in the system.

1. From the **Report Generation** page, click on ➪ Audit Log Report and the **Audit Log Report** page will appear as shown below. By default, the **User Log** page is shown.



Audit log Report Generation

● User Log ○ System Log

From : Day 16, Month Aug, Year 2004

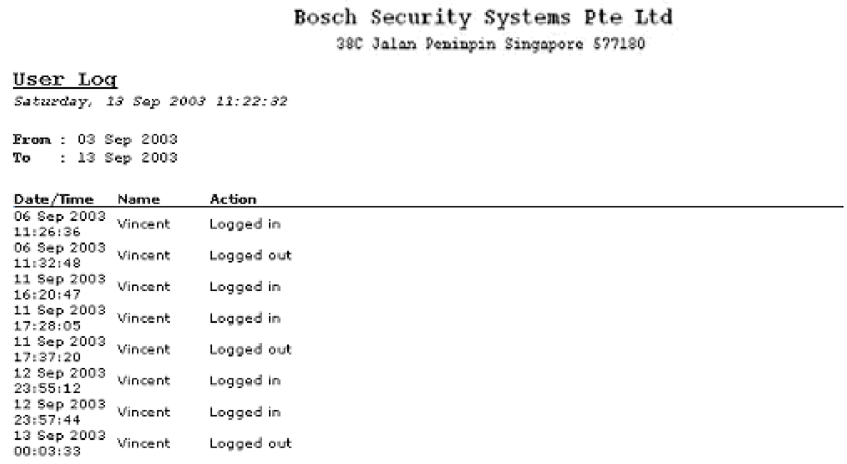
To : Day 26, Month Aug, Year 2004

Available Users

Selected list of Users

2. Select the **From Date** and **To Date**.
3. The **User Log Report** allows you to generate report for all users or selected users only. To generate a report for all users, just click on the , leaving the **Selected list of Users** list box blank. To generate a report for selected user, select the users from the **Available Users** drop-down list.

4. Click on to start generating the log. The following shows a sample of the report generated for user by the name of “Vincent”.



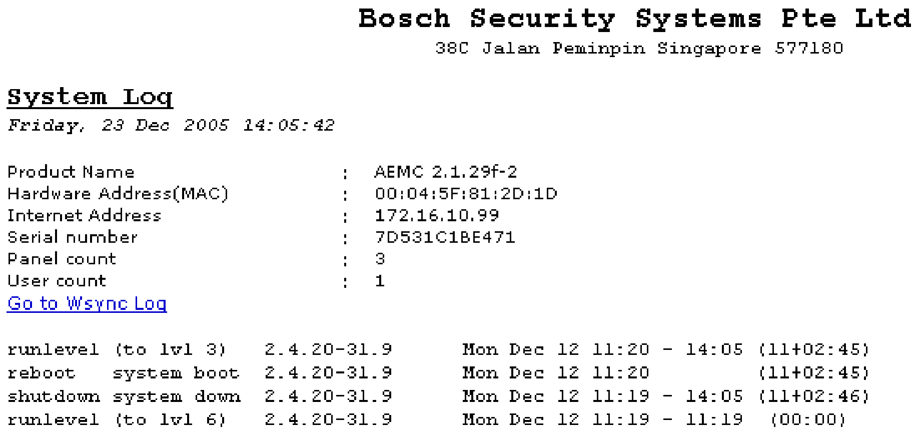
```
                 Bosch Security Systems Pte Ltd
                38C Jalan Peminpin Singapore 577180

User Log
Saturday, 13 Sep 2003 11:22:32

From : 03 Sep 2003
To   : 13 Sep 2003

Date/Time    Name      Action
06 Sep 2003  Vincent   Logged in
11:26:36
06 Sep 2003  Vincent   Logged out
11:32:48
11 Sep 2003  Vincent   Logged in
16:20:47
11 Sep 2003  Vincent   Logged in
17:28:05
11 Sep 2003  Vincent   Logged out
17:37:20
12 Sep 2003  Vincent   Logged in
23:55:12
12 Sep 2003  Vincent   Logged in
23:57:44
13 Sep 2003  Vincent   Logged out
00:03:33
```

14.4.2 System Log

The **System Log** report provides a report on the system status.

1. To generate the **System Log** report, select the **System Log** radio button.
2. Click on to start generating the Log.

The following is a sample of the report.



```
                         Bosch Security Systems Pte Ltd
                       38C Jalan Peminpin Singapore 577180

System Log
Friday, 23 Dec 2005 14:05:42

Product Name                 :  AEMC 2.1.29f-2
Hardware Address(MAC)        :  00:04:5F:81:2D:1D
Internet Address             :  172.16.10.99
Serial number                :  7D531C1BE471
Panel count                  :  3
User count                   :  1
Go to Wsync Log

runlevel (to lvl 3)   2.4.20-31.9     Mon Dec 12 11:20 - 14:05 (11+02:45)
reboot   system boot  2.4.20-31.9     Mon Dec 12 11:20         (11+02:45)
shutdown system down  2.4.20-31.9     Mon Dec 12 11:19 - 14:05 (11+02:46)
runlevel (to lvl 6)   2.4.20-31.9     Mon Dec 12 11:19 - 11:19  (00:00)
```

The report provides some critical information such as :

Hardware Address (MAC)	This is the physical address of the Access Easy Master. It is a unique number. We could use this number to set the IP address of the Access Easy Master using the ARP command.
Internet Address	This is the IP address of the Access Easy Master.
Serial Number	Each SAM in the Access Easy Master has a unique number. It serves as a license to the owner. If the owner wants to increase the number of login User or connect more Access Easy Controller to the Access Easy Master, he will have to register with Bosch using this number.

Panel Count	The total number of Access Easy Controller s that are licensed and connected to the Access Easy Master.
User Count	The total number of login users that are licensed.
Go to Wsync log	Shows the wsync log between server and panel.

15 Database Backup

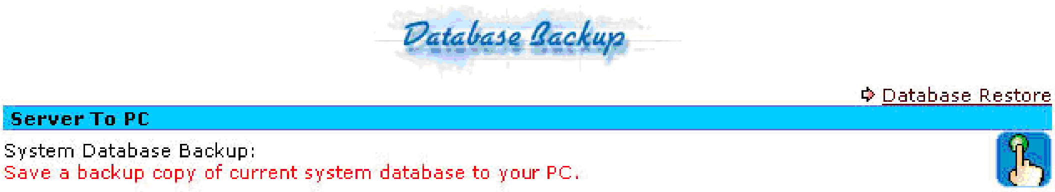
The **Database Backup** feature allows the user to save a backup copy of current system database to the local PC. It provides downloading of information which relates to the setting up of Access Easy Master, for example schedules details, card readers parameters, and others. It allows user to download the history of the activity and attendance in Comma Separated Variable (CSV) formatted file.

The **Database Backup** also allows user to restore the database to the Access Easy Master. It acts as a restore utility.

The following sections will guide you to perform both the operations.

15.1 How to Perform Database Backup

To activate **Database Backup**, click on **Database Backup** menu item from the left pane. A screen as shown below appears.

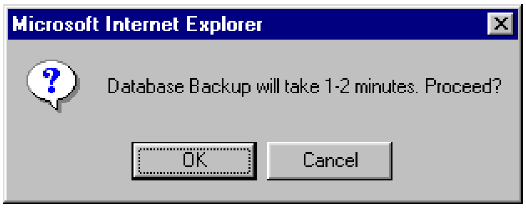


System Database Backup:
Save a backup copy of current system database to your PC.

1. To start the backup, click on .

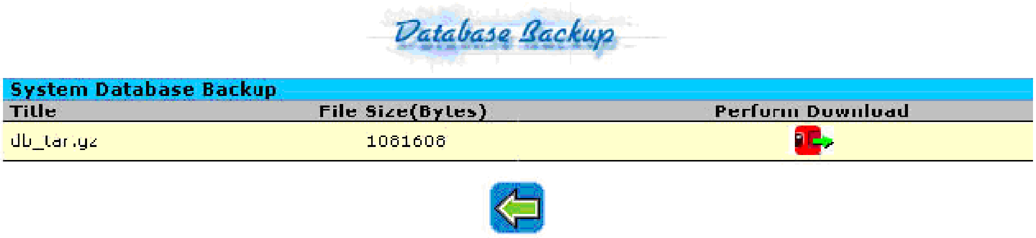
Notice!
A database backup typically takes about 1-2 minutes. During this period, it is advisable not to change other system parameters. However, the Access Easy Master and the Access Easy Controllers will not be affected by the action. All operations, such as door access and alarm monitoring, will still operate as usual.

2. A dialog box will appear, confirming whether to proceed with the backup. Database backup will take 1 ~ 2 minutes.



Database Backup will take 1-2 minutes. Proceed?

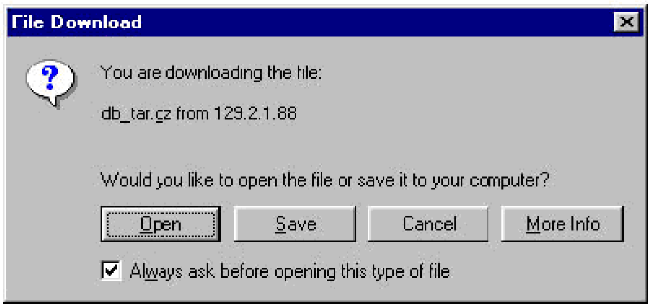
3. Click the **OK** button to proceed with the database backup operation.
4. During backup, the **Database backup in progress...** message will appear on the screen.
5. Once the backup has completed, a new screen will appear as shown below.



System Database Backup

Title	File Size(Bytes)	Perform Download
db_tar.gz	1061608	

6. You could now save the db_tar.gz file to your local PC by clicking on the button.
7. The **File Download** dialog box will appear, showing the file to be downloaded and the IP address of the Access Easy Master.



File Download

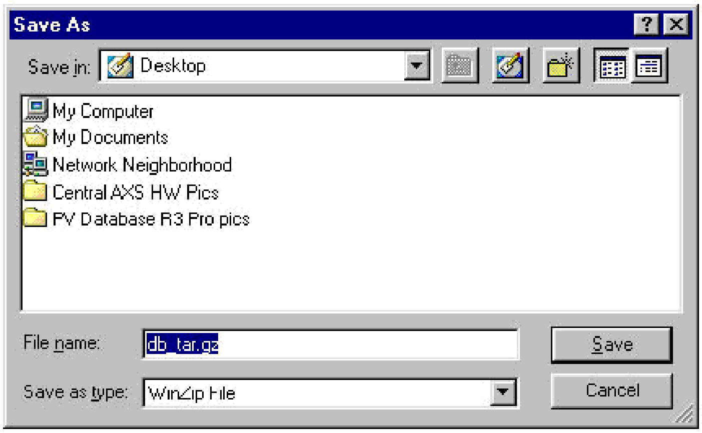
You are downloading the file:

db_tar.gz from 129.2.1.88

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

8. Click on the **Save** button to save the file to your local PC.
9. The user will be prompted to choose a location and file name to save the file.



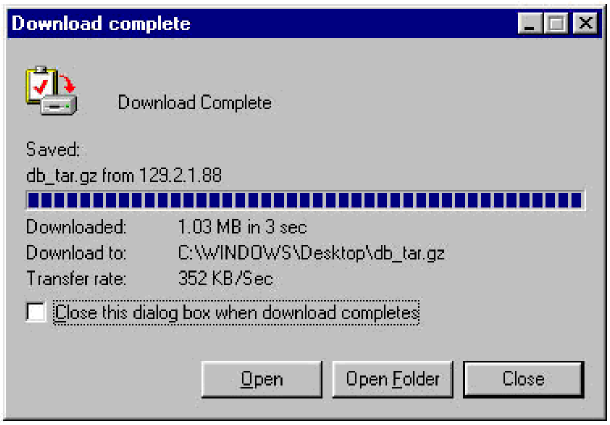
Save As

Save in: Desktop

File name: db_tar.gz

Save as type: WinZip File

10. When the download is completed, the **Download Complete** dialog box will appear.



Download complete

Download Complete

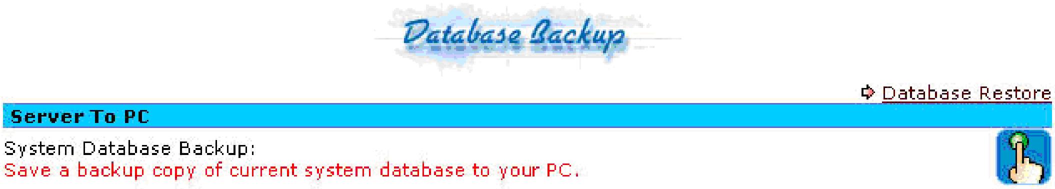
Saved:
db_tar.gz from 129.2.1.88

Downloaded: 1.03 MB in 3 sec
Download to: C:\WINDOWS\Desktop\db_tar.gz
Transfer rate: 352 KB/Sec

☐ Close this dialog box when download completes

15.2 How To Restore System Database

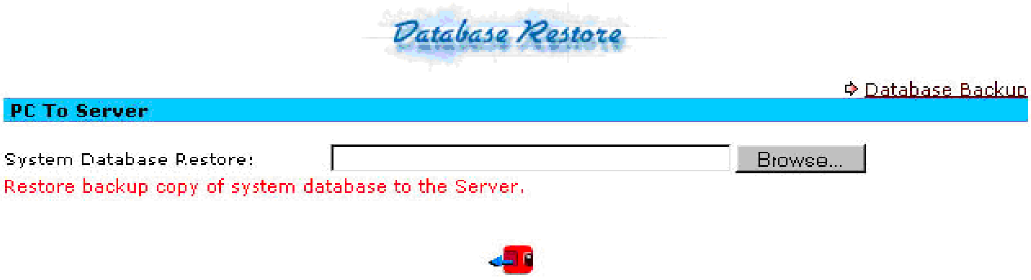
To activate **Database Backup**, click on **Database Backup** menu item from the left pane. A screen as shown below appears.



Server To PC

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

1. Click on the ➪ Database Restore link at the top right corner of the page and the **Database Restore** page will appear as shown below.



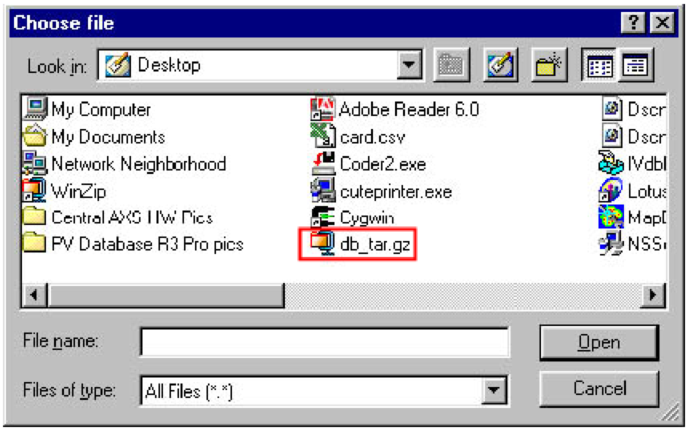
Database Restore

PC To Server

System Database Restore:

Restore backup copy of system database to the Server.

2. Click on the **Browse** button to bring up the **Choose File** dialog box as shown below.



3. Chose the db_tar.gz file and click the **Open** button.

4. To start the restore process, click on the button.

After successfully restoring the system database to the Access Easy Master, you will need to reboot the Access Easy Master for the database to take effect.

Notice!

A database restore typically takes about 1-2 minutes. During this period, it is advisable not to change other system parameters. However, the Access Easy Master and the Access Easy Controllers will not be affected by the action. All operations, such as door access and alarm monitoring, will still operate as usual.

It is recommended that you perform a synchronization of the Access Easy Master database to Access Easy Controller after you restore the database. Please refer to *How to Add an Access Easy Controller, page 70* on the synchronization operation.

16 Reboot, Shutdown and Logout

The user can also to perform various maintenance activities for the panel like reboot, shutdown and logout functions. These will be discussed in the following chapters.

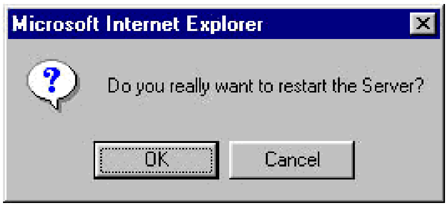
16.1 Reboot Function

The **Reboot** function allows user to reboot the server after upgrading to the system software is completed or in order to allow changes made to take effect, especially changes made to the network setting or panel's IP address.

Notice!
During a reboot, it is important that the **Database Backup** function is carried out before proceeding to reboot the Access Easy Master.

The **Reboot** function can be activated only from the left pane menu item.

1. From any menu item page, click on the **Reboot** link from the left pane. The following dialog box appears for confirmation.



Microsoft Internet Explorer

Do you really want to restart the Server?

2. Click on the **OK** button to proceed.
3. It takes a few minutes for the process to complete.

Notice!
During the rebooting process, the Access Easy Master disconnects itself from the computer and the web page on the computer screen will show "Rebooting System..." before the web page becomes blank. User must close and relaunch the web browser program. Login to Access Easy Master again after the process is completed.

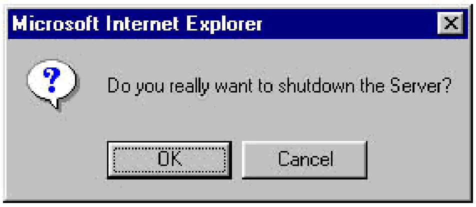
Once the server is up and running again, please reenter the server URL address and proceed with the login.

16.2 Shutdown Function

The **Shutdown** function allows user to stop the Access Easy Master system properly if the user is required to.

The **Shutdown** function can be activated only from the left pane menu item.

1. From any menu item page, click on the **Shutdown** link from the left pane. The following dialog box appears for confirmation.



Microsoft Internet Explorer

Do you really want to shutdown the Server?

2. Click on the **OK** button to proceed.
3. It takes about 2 minutes for the system to shutdown.

Notice!
During the shutting down process, the Access Easy Master disconnects itself from the computer and the web page on the computer screen will show "System shutting down...".

16.3 Logout Function

The **Logout** function allows the user to do a proper exit from the web browser.

The **Logout** function can be activated only from the left pane menu item.

From any menu item page, click on the **Logout** link from the left pane. The web browser will logout immediately without any prompt. To login again, refer to *Logging In and Understanding Access Easy Master, page 14*.

17 Panels Admin

Panels Admin functions refer to the administration and configuration of individual Access Easy Controller, which are currently connected to the Access Easy Master.

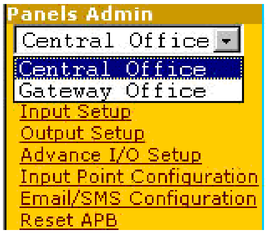
Under **Panels Admin** menu of the Access Easy Master main menu, you will see the various parameters to configure for each individual Access Easy Controller such as **Access Groups**, **Card Readers**, **Input Setup**, **Output Setup**, **Advance I/O Setup**, **Input Point Configuration**, **Email/SMS Configuration** and **Reset Anti-Passback** settings.

Panels Admin provides the Server Administrator the convenience of centrally accessing and configuring individual Access Easy Controllers that are currently having a connection with it.

17.1 How To Choose Individual Panel To Admin

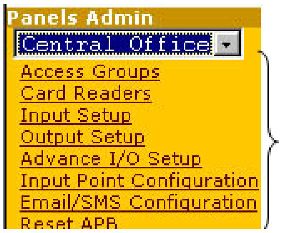
The Access Easy Master is able to detect which Access Easy Controller are set up and panels that are currently having a connection to it. For panels that are off-line due to network problem, they will still be shown in the list of panels in **Panels Admin** page.

Their settings can still be changed and when the panels are connected, the new settings will be synchronized to the panels. As shown below, 2 panels named “Central Office” and “Gateway Office” are currently set up to the Access Easy Master.



To configure any item (**Access Groups**, **Card Readers**, **Input Setup**, **Output Setup**, **Advance I/O Setup**, **Input Point Configuration**, **Email/SMS Configuration** or **Reset APB**) of a particular Access Easy Controller, you will need to first select the panel description from the drop-down list as shown above.

After selecting the panel to administer, you could click on any links to the items that you want to configure.



Click on any of these links to go to the selected Access Easy Controller.

Once you click on any of the links as mentioned above, the page showing the selected function will appear for the selected panel.

17.2 How to Setup Access Groups

An access group a list of readers within certain authorized time periods (predefined 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.

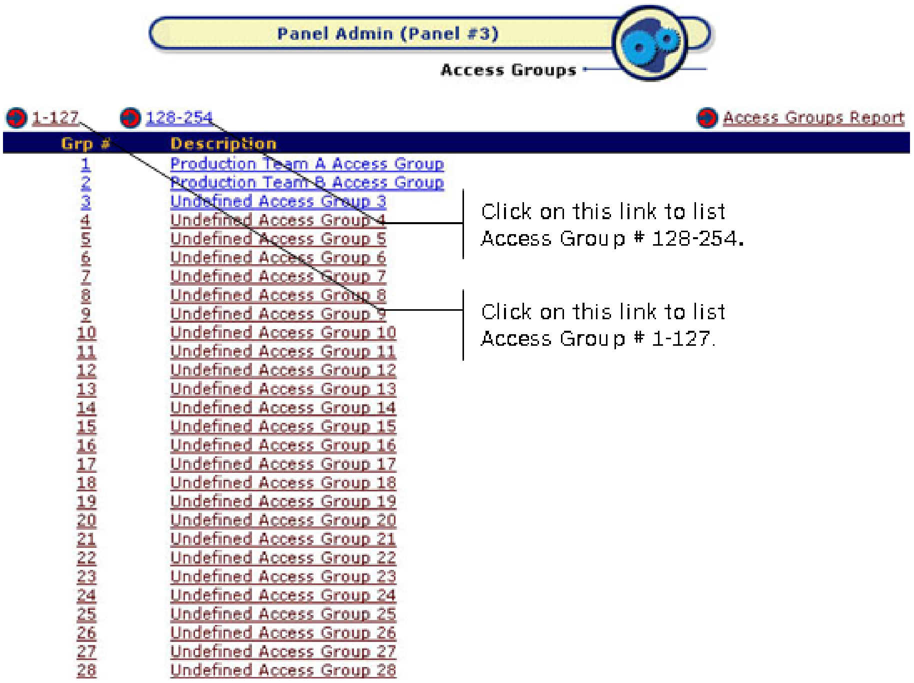
In addition, there are two more unique access groups. They are the “Full access” group that allows cardholders to access all readers at all times, usually reserved for the President, Chairman or Directors of the company, and the “Unused” group that prohibits cardholder to access any reader at any time. These two access groups are not listed in the **Access Groups** page. They can be selected when the user goes to **Access Levels** page.

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 setup the access group, select the target Access Easy Controller and click on the **Access Groups** link. The following screen will appear.



Panel Admin (Panel #3)

Access Groups

1-127 128-254 Access Groups Report

Grp #	Description
1	Production Team A Access Group
2	Production Team B Access Group
3	Undefined Access Group 3
4	Undefined Access Group 4
5	Undefined Access Group 5
6	Undefined Access Group 6
7	Undefined Access Group 7
8	Undefined Access Group 8
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

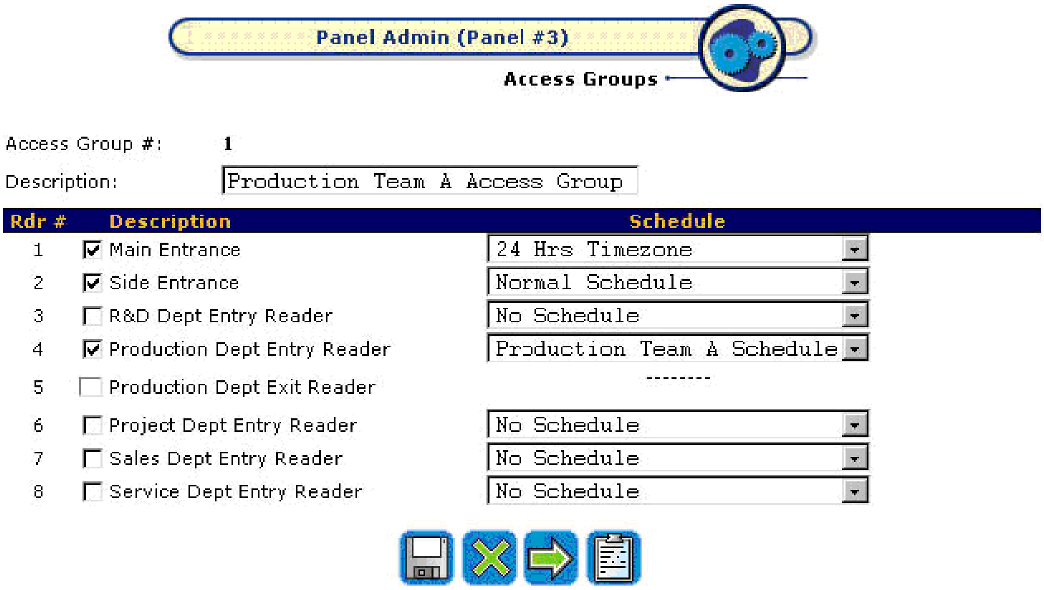
Click on this link to list Access Group # 128-254.

Click on this link to list Access Group # 1-127.

1. Click on the 1-127 or 128-254 link to list the specific access groups ranges.
2. Alternatively, you can click on the ⇨ button to go to the 128-254 range listings or the ⇦ button to go to the 1-127 range listings.

17.2.1 How to Configure/Edit Access Group Parameters

1. Click on the number in the **Grp #** column, or the text in the **Description** column to proceed. A screen as shown below appears.



Access Group #: 1

Description: Production Team A Access Group

Rdr #	Description	Schedule
1	☑ Main Entrance	24 Hrs Timezone
2	☑ Side Entrance	Normal Schedule
3	□ R&D Dept Entry Reader	No Schedule
4	☑ Production Dept Entry Reader	Production Team A Schedule
5	□ Production Dept Exit Reader	--------
6	□ Project Dept Entry Reader	No Schedule
7	□ Sales Dept Entry Reader	No Schedule
8	□ Service Dept Entry Reader	No Schedule

Notice!
The reader's **Description** field shown above is configured in the **Card Readers** setting. “Reader #5” is configured as exit reader for the “Production Department”. Its operational behavior will follow that of the entry Reader and thus no schedule can be configured.

2. Delete the default text and enter the new text in the **Description** field.
3. Click on the appropriate check boxes to indicate a check mark, for reader(s) that is to be assigned to this access group.
4. Select the appropriate schedule from the **Schedule** drop-down list for each selected reader.

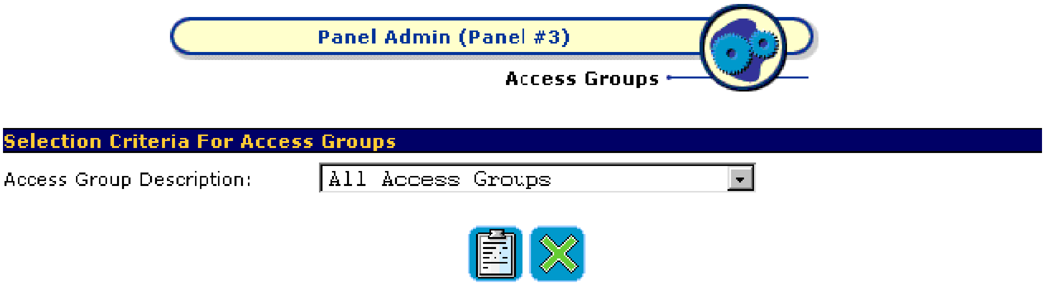
Notice!
The above example shows that staff from “Production Department Team A” can have 24 hours access to the “Main Entrance” and access to their own department according to their work shift. In addition, other than the normal work hours, they are not allowed to come in by the “Side Entrance” as its schedule is not 24 hours access.

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 steps 3 and 4.
6. To confirm the setting, click on 💾 button.

17.2.2 How to Generate a Print Preview of the Access Groups 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.

1. From the first web page of the **Access Groups** menu item, click on the Access Groups Report link. A screen as shown below appears.



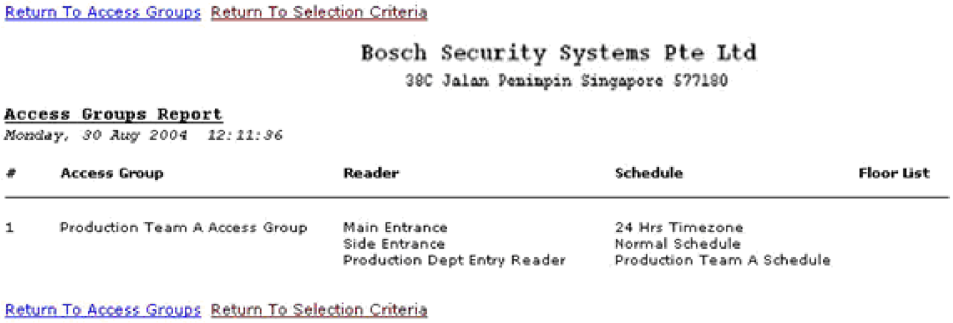
Panel Admin (Panel #3)

Access Groups

Selection Criteria For Access Groups

Access Group Description: All Access Groups

2. Select the desired access group from the **Access Group Description** drop-down list. If no specific access group is selected, all the available access groups will be used to generate the report.
3. Click on the 📋 button for a print preview of the report. The following screen-capture shows a sample of the **Access Groups Report** for “Production Team A” access group.



Return To Access Groups Return To Selection Criteria

Bosch Security Systems Pte Ltd

38C Jalan Pemimpin Singapore 577180

Access Groups Report

Monday, 30 Aug 2004 12:11:36

#	Access Group	Reader	Schedule	Floor List
1	Production Team A Access Group	Main Entrance Side Entrance Production Dept Entry Reader	24 Hrs Timezone Normal Schedule Production Team A 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. Alternatively, click on **File** and select **Print** from the menu.

Notice!

All access groups are available for selection. However, access groups that are not defined with at least a reader will generate an empty report.

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 Return To Access Groups link.

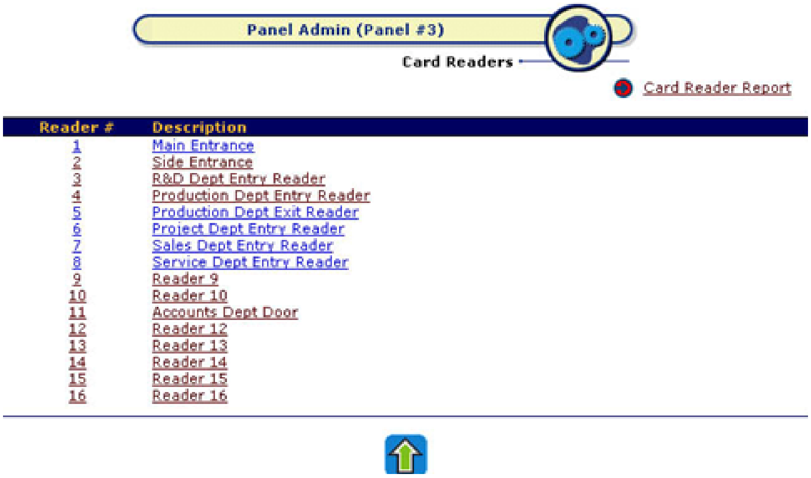
17.3 How to Setup Card Readers

Card reader 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

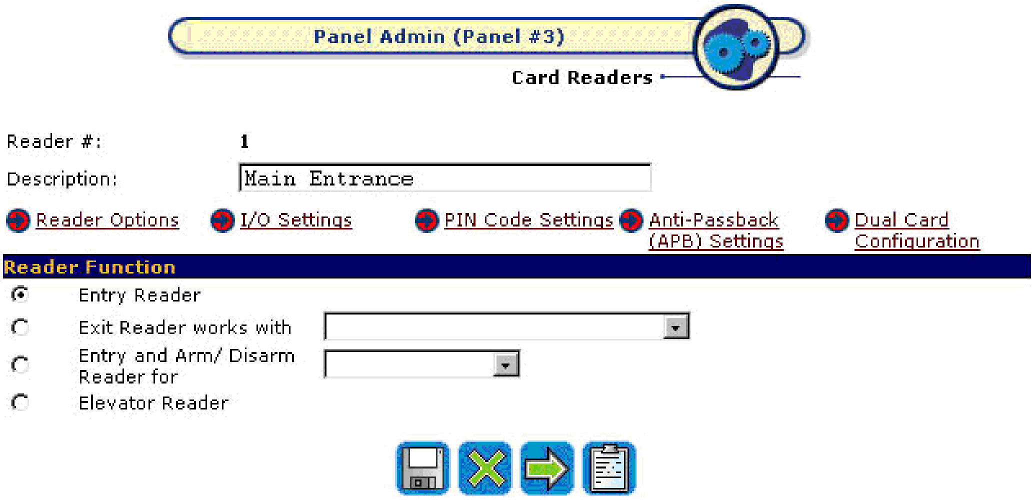
All Access Easy Controller card readers can be configured to work either as an entry reader, an exit reader, an entry and arm/disarm reader, or an elevator reader.

To setup the card readers, select the target Access Easy Controller and click on the **Card Readers** link. 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 number in the **Reader #** column, or the text in the **Description** column to proceed. A screen as shown below appears.



Reader #: 1

Description: Main Entrance

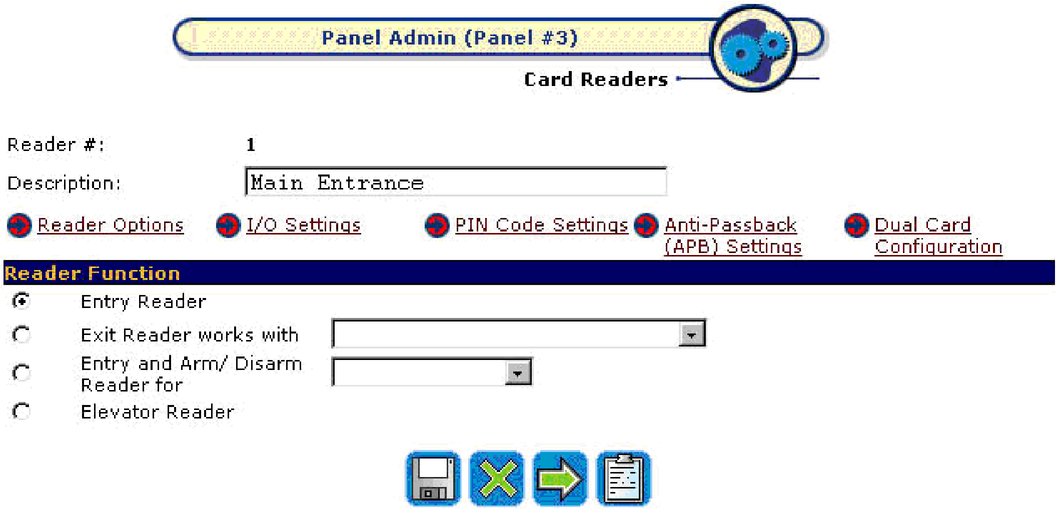
Reader Function

- ● Entry Reader
- ○ Exit Reader works with
- ○ Entry and Arm/ Disarm Reader for
- ○ Elevator Reader

2. Delete the default text and enter the new text in the **Description** field to describe the reader.

3. Click on the button.

17.3.1 Reader Function



Reader #: 1

Description: Main Entrance

Reader Function

● Entry Reader

○ Exit Reader works with

○ Entry and Arm/ Disarm Reader for

○ Elevator Reader

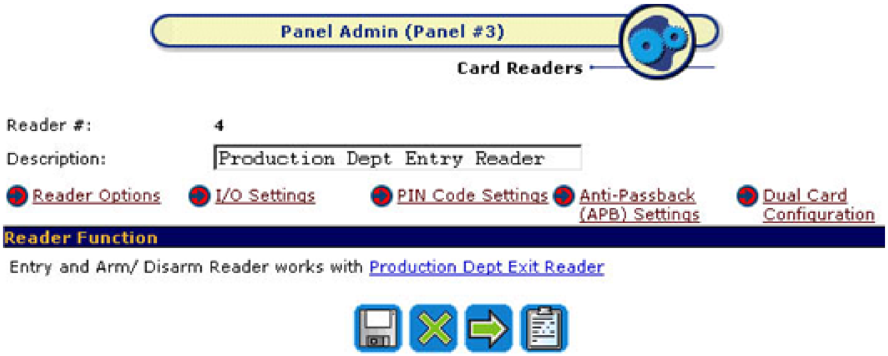
This section allows user to define the use of the reader, either as an entry reader, exit reader, entry and arm/disarm reader, or an elevator reader. By default, all 16 readers are set as entry readers.

A screen of the **Reader Function** page is shown above.

Entry Reader

This is the default setting. All 16 readers are configured as entry readers 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 link. User can click on it to re-configure the exit reader.



Reader #: 4

Description: Production Dept Entry Reader

Reader Function

Entry and Arm/ Disarm Reader works with Production Dept 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 behavior of the entry reader such as door open timer and door strike timer. If the entry reader for this exit reader is also an arm/disarm reader, user can also arm/disarm the same alarm zone at the exit reader as it now has the operational behavior of the entry reader.

ℹ **Notice!**
Once a reader is configured as an exit reader, the reader will only be accessible to **Reader Function**. 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, i.e. this reader can be used for door access control and it can also be used to perform alarm zone arm/disarm function.

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 armed state, all valid access cards will be disabled. Only an arm/disarm card can disarm the alarm zone and enable the door back to normal card access operation. Note: **Card holder is able to Arm/Disarm** checkbox must be selected under **Card Assignment** page.

During an armed 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 rights 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.

ℹ **Notice!**
In order for the reader to work properly, additional wiring is required. Please consult your System Installer for advice.

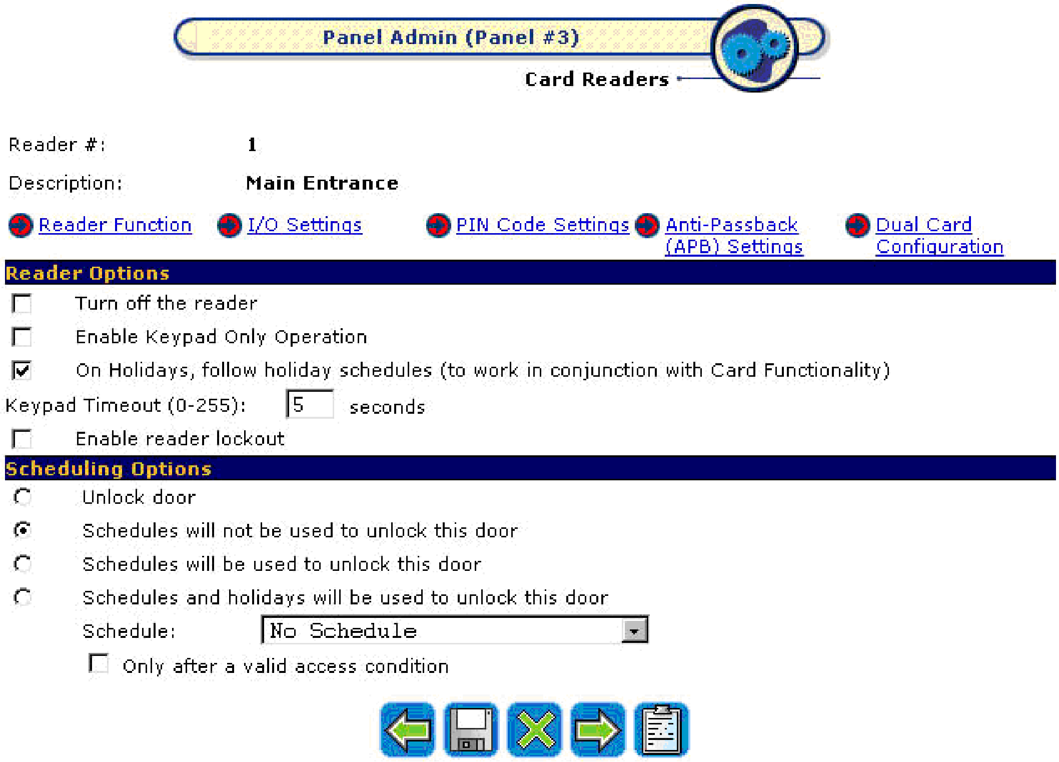
Elevator Reader

Similar concept of door access right assignment in other readers is also implemented in the elevator reader floor assignment.

However, elevator readers do not have the **Anti-Passback (APB) Settings** function. 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 exits to more than one floor (you can consider the elevator has more than one exit).

Besides without the **Anti-Passback (APB) Settings** function, the **I/O Settings of Elevator Reader** is also different from that of an entry reader and an entry and arm/disarm reader. Elevator reader only has **Floor Output Settings** and **Output Link**, compared to the **Door Output Settings**, **Door Input Settings** and **Output Link** in entry readers, and entry and arm/disarm readers. The **Output Link** is also reduced to controlling **Invalid Card Output** only in an elevator reader.

17.3.2 Reader Options



Panel Admin (Panel #3)

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): 5 seconds

□ Enable reader lockout

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: No Schedule

□ Only after a valid access condition

This section allows user to configure parameters in relation to the reader. User can deactivate 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 NOTICE 1). Instead, the cardholder only has to key in his/her card number, (see NOTICE 2) followed by its PIN code (only if PIN function is required).

Notice!

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.

2. User has to activate the 4 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 **Cardholder must abide by holiday schedules** checkbox in the **Card Assignment** page. If both checkboxes are checked and the current date is a holiday, the panel will apply the four 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).

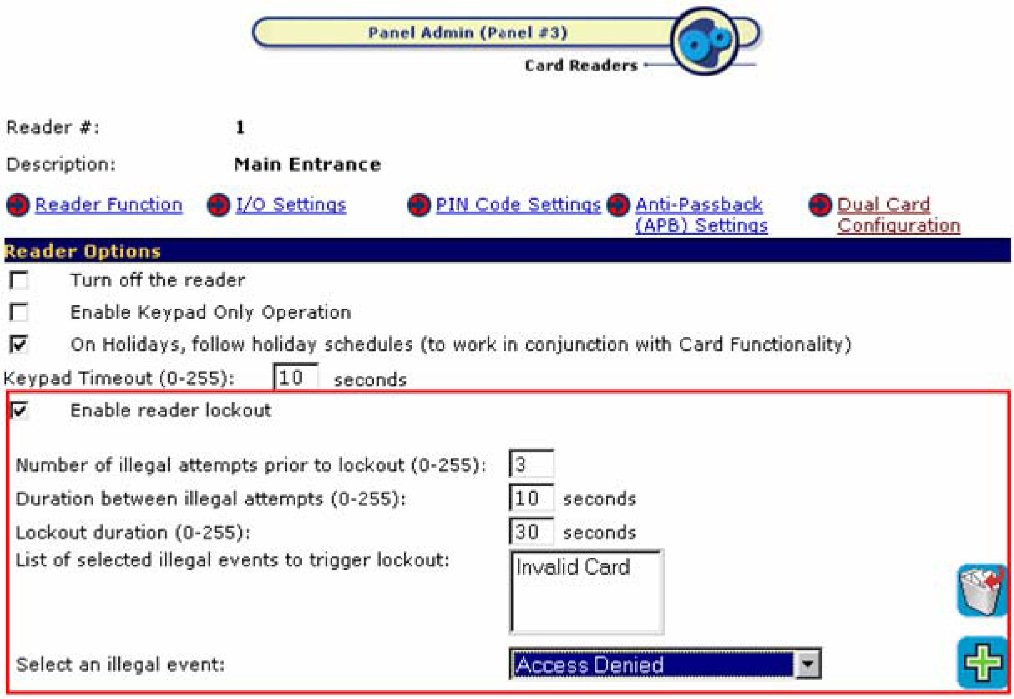
Keypad Timeout

Keypad Timeout relates to the interval where the panel 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 panel 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** checkbox and click on the button. A screen as shown below appears.



Reader #: 1
Description: Main Entrance

☐ 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 the **Select an illegal event** drop-down list and click on the button.
3. The illegal events will appear on the **List of selected illegal events to trigger lockout** list box.
4. To remove the illegal event from the **List of selected illegal events to trigger lockout** list box, highlight the event and click on the button.
5. Enter the **Number of illegal attempts prior to lockout** textbox. The default is set to 3.

6. Enter the **Duration between illegal attempts** textbox. It ranges from 0 to 255 seconds.
7. Enter the **Lockout duration** textbox. It ranges from 0 to 255 seconds.

In the above example, the user will be locked out after the third attempt when he uses an invalid card to access the reader three 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 to access the reader twice 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.

Notice!
Once reader is locked out, it will not be accessible by any cardholder. Only after the lockout duration can the reader be used again.

17.3.3 Scheduling Options

The Access Easy Controller can be programmed to activate or deactivate the reader based on preprogrammed 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 comes 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 *Reader Options, page 126*.

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 ○ Unlock door function is applicable to entry reader, and entry and arm/disarm reader. For elevator reader, this function is replaced by a similar function **Disable Elevator Reader**, in the section below.

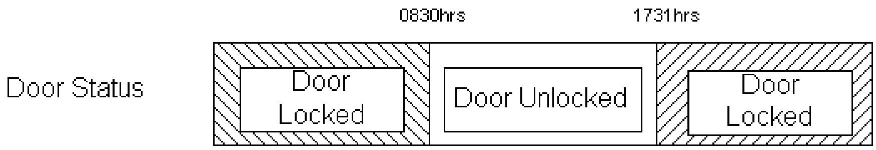
Disable Elevator Reader (For Elevator Reader Only)
When this mode is selected, the elevator that is controlled by the particular reader is permanently unlocked. There is free access to everyone. This ○ Disable Elevator Reader function is applicable to elevator reader only. For entry reader, and entry and arm/disarm reader, it is replaced by a similar **Unlock door** function, in the section above.

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 or her card and PIN code, if 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 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.



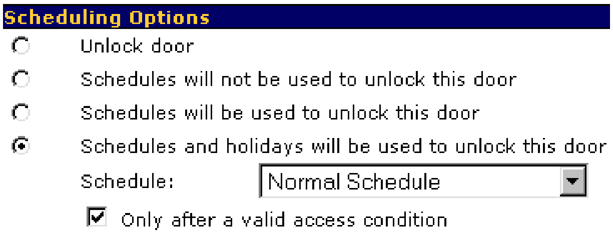
Notice that the door is locked only at 1731hrs instead of 1730hrs. The reason is that Access Easy Controller takes 17:30:59hrs as a valid end time for 1730hrs.

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 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 deselect the selected radio button, click on other radio buttons. By default, the **Schedules will not be used to unlock this door** radio button is selected.
2. If the either **Schedules will be used to unlock this door** or **Schedules and Holidays will be used to unlock this door** radio button is selected, please proceed to step 3 to select the schedule.
3. Select the desired schedule rom the **Schedule** drop-down list.
4. When either **Schedules will be used to unlock this door** or **Schedules and Holidays will be used to unlock this door** radio button is selected, the door will unlock on time even if nobody is in the premises. However, if **Only after a valid access condition** checkbox is checked, the system will only unlock the door after a valid access card is presented during the schedule time period.

Example:



Scheduling Options

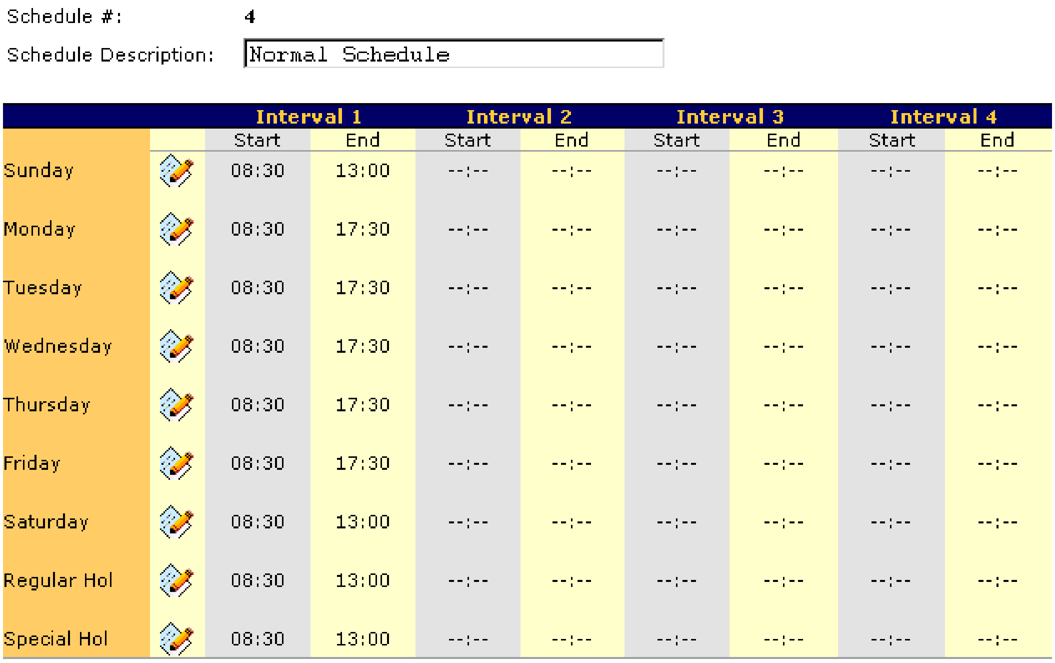
○ Unlock door
○ Schedules will not be used to unlock this door
○ Schedules will be used to unlock this door
● Schedules and holidays will be used to unlock this door

Schedule: Normal Schedule

☑ Only after a valid access condition

In the screen above, the **Schedules and holidays will be used to unlock this door** radio button is selected, and the selected **Schedule** is “Normal Schedule”. In addition, the **Only after a valid access condition** checkbox is checked.

The screen below shows the schedule for “Normal Schedule”, which has been selected.



Schedule #: 4

Schedule Description: Normal Schedule

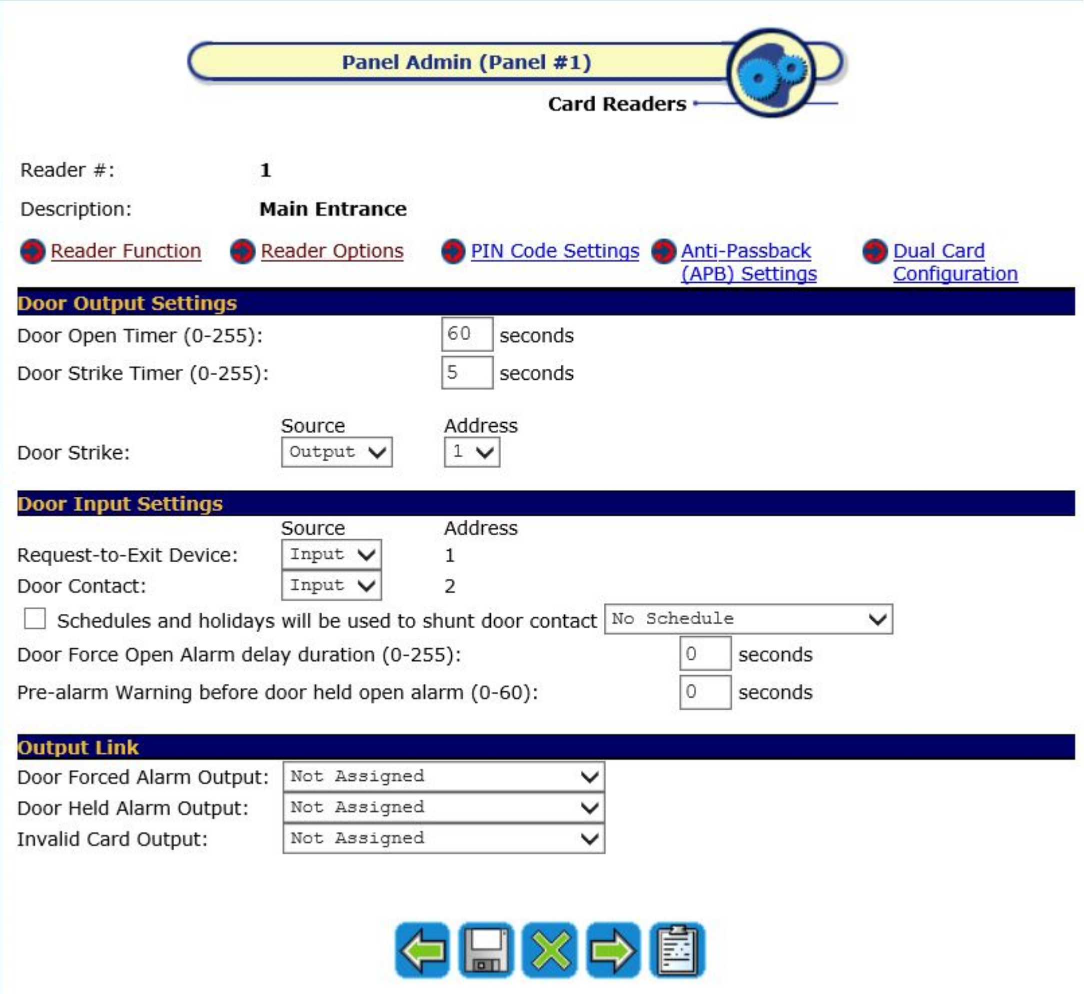
		Interval 1		Interval 2		Interval 3		Interval 4	
		Start	End	Start	End	Start	End	Start	End
Sunday	✎	08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Monday	✎	08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Tuesday	✎	08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Wednesday	✎	08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
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 **Schedules and holidays will be used to unlock this door** radio button is selected, the door will unlock every Monday to Friday from 0830hrs to 1730hrs and every Saturday, Sunday, regular and special holiday from 0830hrs to 1300hrs.

However, with **Only after a valid access condition** checkbox selected, 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.

17.3.4 Door Output Settings (For Entry Reader, Entry and Arm/Disarm Reader)

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 below.



Reader #: 1

Description: Main Entrance

Reader Function | Reader Options | PIN Code Settings | Anti-Passback (APB) Settings | Dual Card Configuration

Door Output Settings

Door Open Timer (0-255): 60 seconds

Door Strike Timer (0-255): 5 seconds

Door Strike: Source: Output; Address: 1

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): 0 seconds

Pre-alarm Warning before door held open alarm (0-60): 0 seconds

Output Link

Door Forced Alarm Output: Not Assigned

Door Held Alarm Output: Not Assigned

Invalid Card Output: Not Assigned

Door Open Timer

This setting defines how long the door can be held open, after an access/exit is granted, before the panel 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-energize 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 panel locks it back again. It can range from 0 to 255 seconds. The factory default is 5 seconds.

Notice!

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 Acivity** will only show “Invalid Card”.

Door Strike

For the output device, such as door strike, though it is predefined, user can still change the default address to other available addresses within the same reader board, should the original output relay is defective.

To allocate an output for the door strike, select “Output” from the **Source** drop-down list. This defines the physical output on the reader board. 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. Proceed to select an address for it from the **Address** drop-down list. The default address is “1”.

Otherwise, user can disable the output channel by selecting “None” from the **Source** drop-down list.

Notice!

Address for **Door Strike** is selectable only to within the card's spare output channels. **Door Forced Alarm Output**, **Door Held Alarm Output and Invalid Card Output** is selectable only within the user programmable 32 outputs.

17.3.5 Door Input Settings (For Entry Reader, Entry and Arm/Disarm Reader)

A screen of the Door Input Settings section is shown in *Door Output Settings (For Entry Reader, Entry and Arm/Disarm Reader), page 130*.

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 input 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” from the **Source** drop-down list. This defines the physical input on the reader board. Input channel assignment for devices connected in relation to reader is fixed and cannot be changed. The address for **Request-to-Exit Device** is fixed and cannot be changed.

Otherwise, user can disable the input channel by selecting “None” from the **Source** drop-down list.

Door Contact
To allocate an input address for **Door Contact**, select “Input” from the **Source** drop-down list. The address for **Door Contact** is fixed and cannot be changed. Otherwise, select “None” from the **Source** drop-down list.

If the door contact is ignored, there will not be any alarms like "Door Held Open" or "Door Forced Open" on that particular reader.

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. Select the checkbox and the corresponding schedule from the drop-down list.

If a schedule is selected, the door contact will be ignored during the time interval. 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.

Door Force Open Alarm delay duration
This is to facilitate some special exit requirement. For example, a handicap user will need a longer time to access the open door than a normal user does. This can also be used to prevent “Door Forced Open” false alarm due to interference at the cables.

Enter the timing in seconds in the **Door Forced Open Alarm delay duration** text box if desired. The timing can range from 0 to 255 seconds.

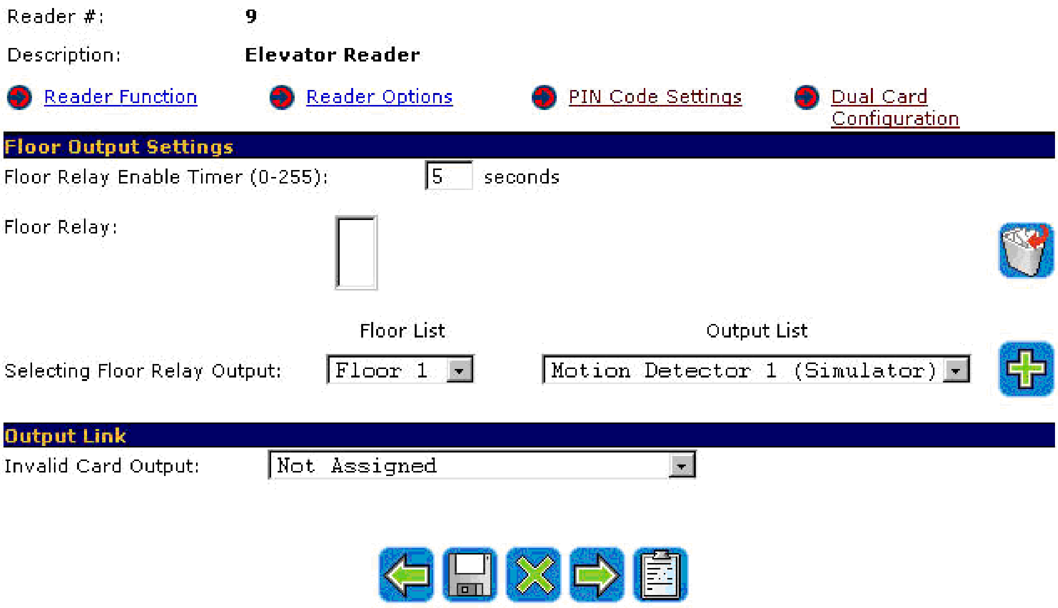
Pre-alarm Warning before door held open alarm
With the pre-alarm function, a user would be reminded with a slow beeping that the door he has just gained access is still opened. An example is he can set the **Pre-alarm Warning before door held open alarm** setting to 5 seconds, so that he will be alerted to close the door on time before the “Door Held Open” alarm. The timing can range from 0 to 60 seconds.

Notice!
Addresses for **Request-to-Exit Device** and **Door Contact** are fixed and cannot be changed. If the input channel is disabled, the address will not be shown.

17.3.6 Floor Output Settings (For Elevator Reader Only)

When a reader is enabled as a elevator reader, it will not have any door input or output setting. Instead it will be replaced by floor output settings.

A screen of the **Floor Output Settings** page is shown below.



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:

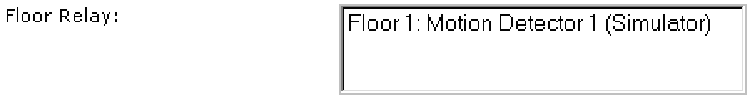
Selecting Floor Relay Output: Floor List: Floor 1 | Output List: Motion Detector 1 (Simulator)

Output Link

Invalid Card Output: Not Assigned

This section allows user to set any of the 32 programmable output point to the selected floor.

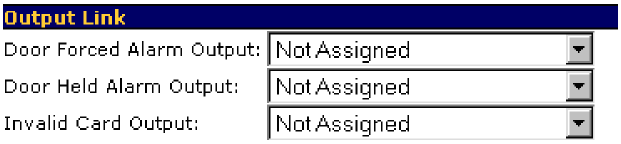
1. To configure **Selecting Floor Relay Output**, select a floor from the **Floor List** drop-down list.
2. Select an output point from the **Output List** drop-down list.
3. Click on the ➕ button to add the selected output point to the selected floor. The selected items would appear on the **Floor Relay** 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 and enter a new timing in seconds. The default timing is 5 seconds.

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 as “Not Assigned”.



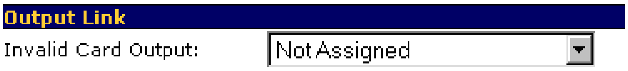
Output Link

Door Forced Alarm Output: Not Assigned

Door Held Alarm Output: Not Assigned

Invalid Card Output: Not Assigned

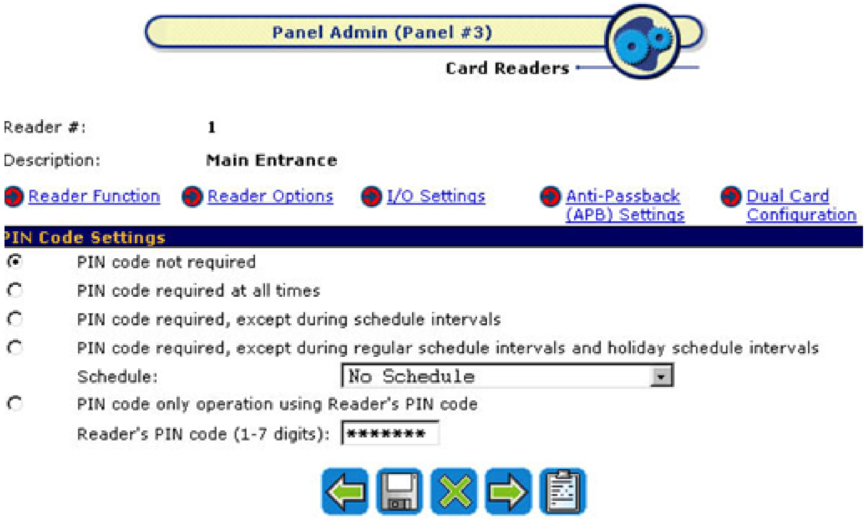
However, in an elevator reader, this section only allows user to set any of the 32 programmable output point to **Invalid Card Output**. By default, it is set as “Not Assigned“.



Output Link

Invalid Card Output: Not Assigned

17.3.7 PIN Code Settings



Reader #: 1

Description: Main Entrance

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.

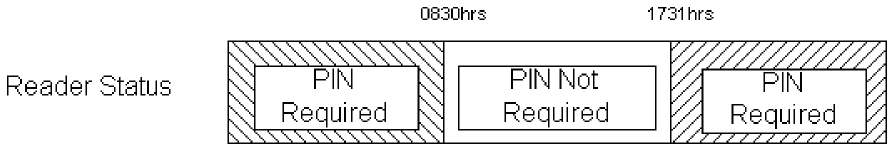
PIN code not required
When this mode is selected, users accessing this reader do not have to key in the PIN code.

PIN code required at all times
When this mode is selected, users are required to key in the PIN code.

Notice!
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 *Card Details, page 43*.

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.

Notice!
To use this feature as intended, the cardholder should be given access rights to the reader(s). 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 is “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)** field.

To set the schedule:

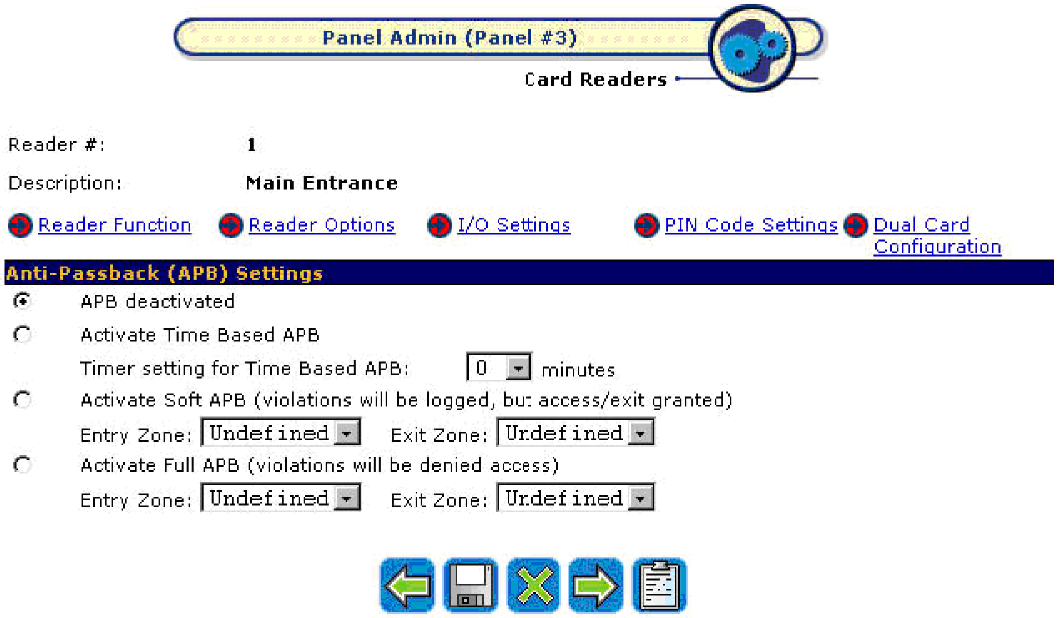
1. If the **PIN code required, except during schedule intervals**, or **PIN code required, except during regular schedule intervals and holiday schedule intervals** radio button is selected, the schedule must be set.
2. Select the appropriate schedule from the **Schedule** drop-down list.

To set the reader's PIN code

1. If the **PIN code only operation using Reader's PIN code** radio button is selected, the reader’s PIN code must be set.
2. To configure the PIN code, enter the new PIN code in the **Reader's PIN code (1-7 digits)** field. See NOTICE 1 and 2.

Notice!
Note 1: User can enter from 1 to 7 digits for the **Reader's PIN code** (default code is “1234000”).
Note 2: For security reason, every character entered for the PIN code is represented by an asterisk. For a Macintosh user, it is represented by a dot instead.

17.3.8 Anti-Passback (APB) Settings



Panel Admin (Panel #3)

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 the time based, soft and full APB. Each mode provides different levels of security and is explained in detail in the following sections.

APB deactivated

By default, the **APB deactivated** radio button is selected. 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 panel will not accept the same card until the timer setting for time based APB has elapsed.

To select this mode, select the **Activate Time Based APB** radio button.

When this mode is selected, the timer must be set. Choose the timing in minutes from the **Timer setting for Timed Based APB** drop-down list, from a range of 0 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 follows another person in or out of the controlled area, the transactions "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 the APB violation in order to clear the transaction. Refer to *Reset APB, page 175* for more details.

To select this mode, select the **Activate Soft APB** radio button. The entry and exit zones must be selected from the **Entry Zone** and **Exit Zone** drop-down list for this mode to work properly.

Activate Full APB

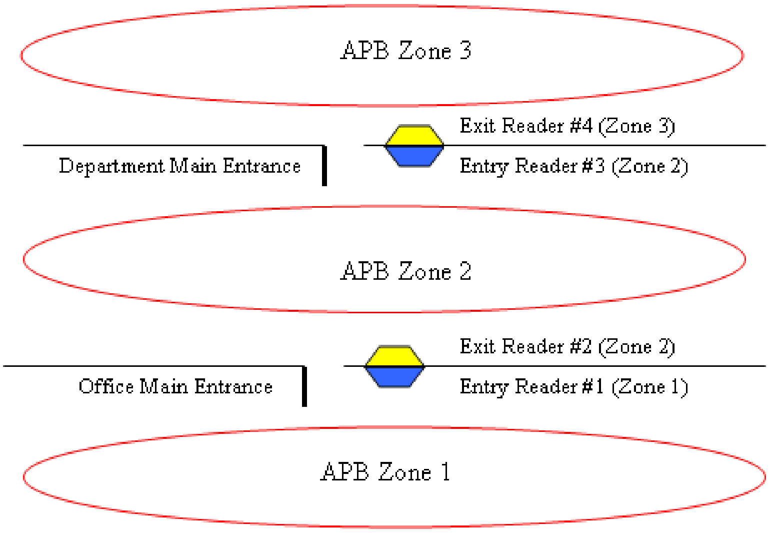
When this mode is selected, user must first enter using the entry reader in order to exit from the corresponding exit reader. If the cardholder violates this, access will be denied. The administrator needs to reset the APB violation before the cardholder can have access again. Refer to *Reset APB, page 175* for more details.

To select this mode, select the **Activate Full APB** radio button. The entry and exit zones must be selected from the **Entry Zone** and **Exit Zone** drop-down list 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 and full APB.
Access Easy Controller is able to support up to 254 soft APB entry and 254 soft APB exit zones, 254 full APB entry and 254 full APB exit zones.

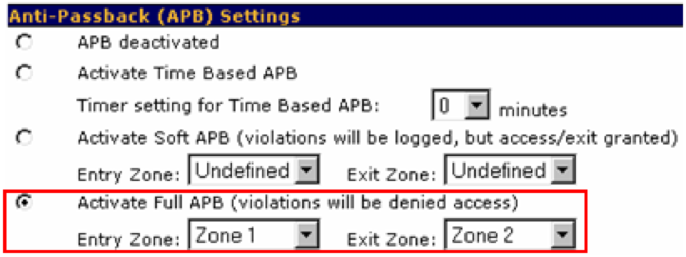


Any reader assigned to operate soft or full APB mode will be given an entry and exit zone. When a cardholder presents his/her card at “Entry Reader #1”, the system will verify whether he has been registered in “Zone 1”. If he has been registered in “Zone 1”, access is granted to him. However, if he is verified to be in other zones instead of “Zone 1”, access will be denied to him. If he is granted access, when he opens the door to gain access such that the door contact sensing is opened, he will then be registered to be in “Zone 2”.

Notice!
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 a zone to gain access to any other zones. 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”, “Zone 1” will be selected from the **Entry Zone** drop-down list, and “Zone 2” will be selected from the **Exit Zone** drop-down list as shown below.



Anti-Passback (APB) Settings

○ APB deactivated

○ Activate Time Based APB

Timer setting for Time Based APB: 0 minutes

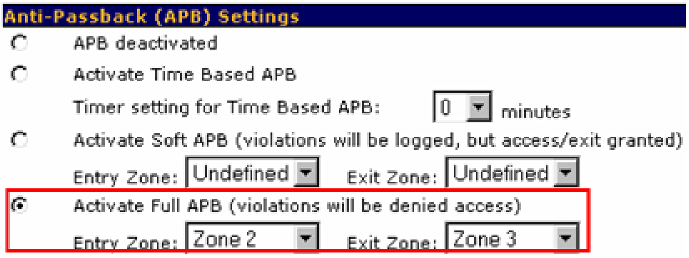
○ Activate Soft APB (violations will be logged, but access/exit granted)

Entry Zone: Undefined Exit Zone: Undefined

● Activate Full APB (violations will be denied access)

Entry Zone: Zone 1 Exit Zone: Zone 2

Similarly, for “Entry Reader #3”, “Zone 2” will be selected from the **Entry Zone** drop-down list, and “Zone 3” will be selected from the **Exit Zone** drop-down list as shown below.



Anti-Passback (APB) Settings

○ APB deactivated

○ Activate Time Based APB

Timer setting for Time Based APB: 0 minutes

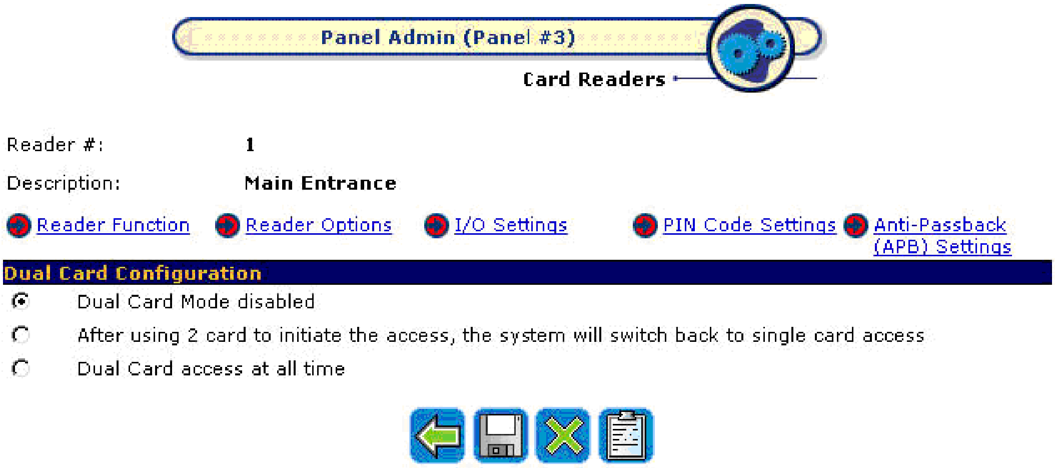
○ Activate Soft APB (violations will be logged, but access/exit granted)

Entry Zone: Undefined Exit Zone: Undefined

● Activate Full APB (violations will be denied access)

Entry Zone: Zone 2 Exit Zone: Zone 3

17.3.9 Dual Card Configuration



Reader #: 1

Description: Main Entrance

Dual Card Configuration

● Dual Card Mode disabled

○ After using 2 card to initiate the access, the system will switch back to single card access

○ Dual Card access at all time

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 two 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 two 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, two 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.

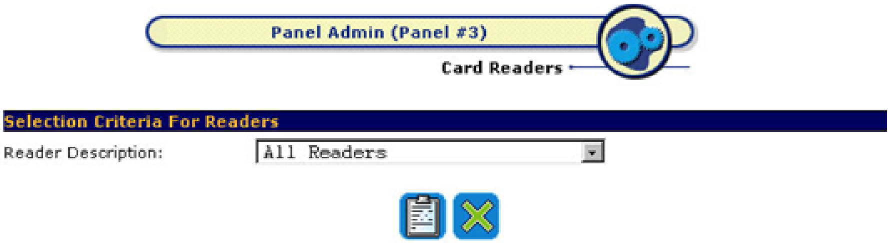
Dual Card access at all time

If this mode is selected, it means that two 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 in *Card Assignment, page 42* as to whether there is any order in the presentation of cards.

17.3.10 How to Generate a Print Preview of the Card Reader Report

Once you have completed configuring the card readers, a hardcopy can be printed out.

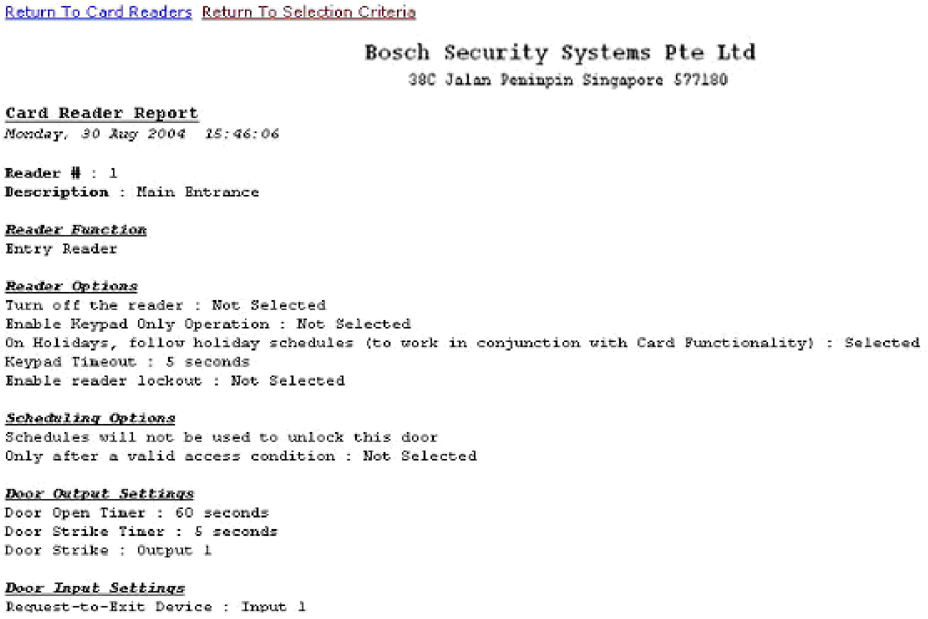
1. From the first web page of the **Card Readers** menu item, click on the ➔ Card Reader Report link. A screen as shown below appears.



Reader Description: All Readers

2. Select the desired reader from the **Reader Description** drop-down list. If no reader is selected, the report will include all the available readers in the selected panel. 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 “Main Entrance”.



Return To Card Readers Return To Selection Criteria

```
                          Bosch Security Systems Pte Ltd
                         38C Jalan Pemimpin Singapore 577180

Card Reader Report
Monday, 30 Aug 2004  15:46:06

Reader # : 1
Description : Main Entrance

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 : 5 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
```

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 **File** and select **Print** menu.
5. To return to the **Card Readers** first web page, click on the Return To Card Readers link.

17.4 Input Setup

The Access Easy Controller has 32 user programmable input points that will be used for alarm monitoring purposes. The addresses for these input points range from 33 to 64 and are 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 provide the same function. The only difference is the way each is being armed/ disarmed. Access Easy Controller allows user to configure up to four alarm zones.

An alarm zone (see NOTICE 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, or manually by user via the web page. To arm/disarm an input point via the web page, go to *Input Control, page 34*.

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 labeled 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.

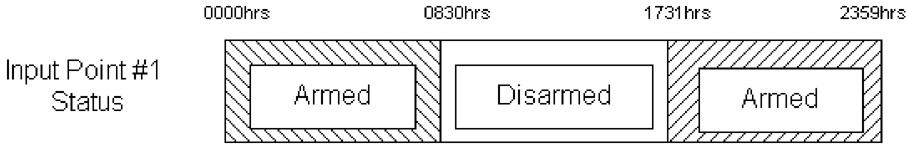
Any alarm detected by any of the input points would also trigger the common alarm output relay, at address 8, and is only restored when all the input points is restored back to their normal state.

Notice!
Note 1: The input control web page will display the status of the alarm zones as well as the status of individual input points. Please refer to *Input Control, page 34*.
Note 2: All input points configured to an alarm zone follow 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.

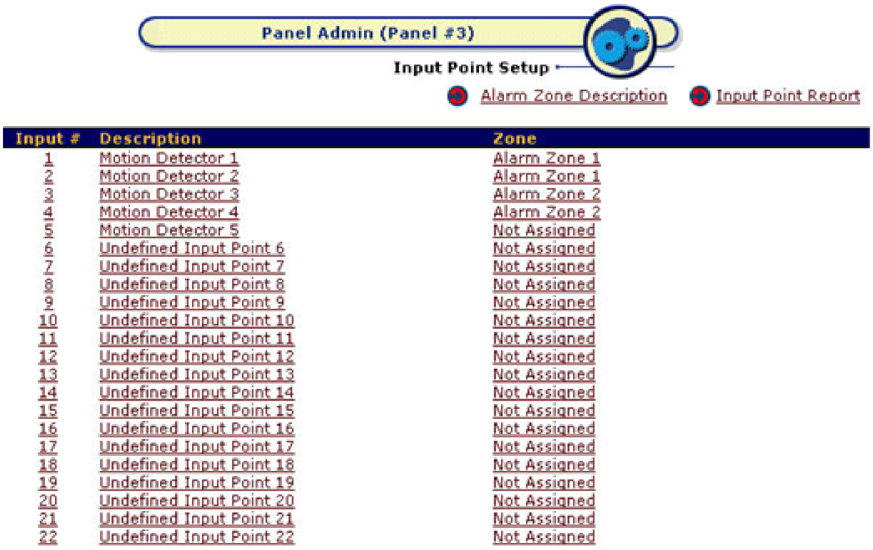
When the Schedule #2 is tied to Input Point #1, the input point will arm and disarm accordingly.



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.

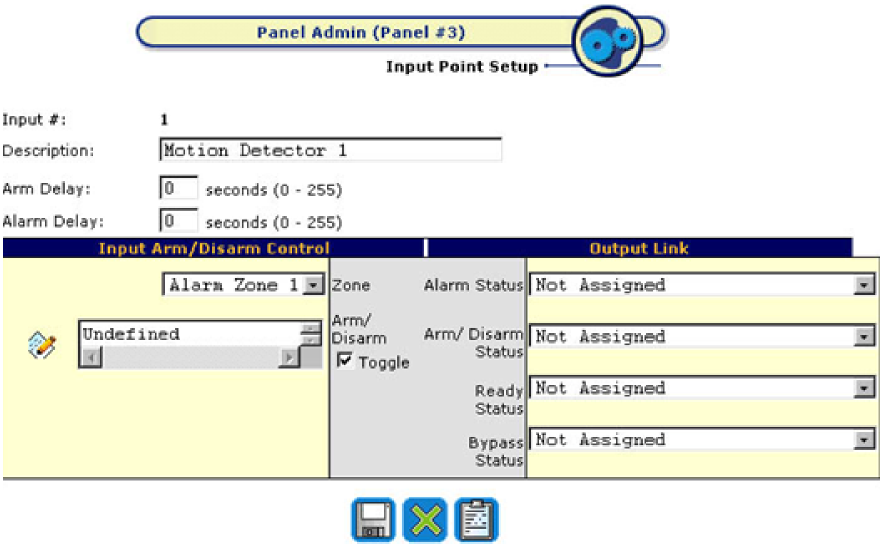
Notice!
Before you configure any input point(s), please ensure that the alarm monitoring device with the EOL resistor is in place with the necessary logic inversion on the **Input Point Configuration** web page.

1. To setup the input point select the target Access Easy Controller, and click on the **Input Setup** link. The following screen will appear.



Input #	Description	Zone
1	Motion Detector 1	Alarm Zone 1
2	Motion Detector 2	Alarm Zone 1
3	Motion Detector 3	Alarm Zone 2
4	Motion Detector 4	Alarm Zone 2
5	Motion Detector 5	Not Assigned
6	Undefined Input Point 6	Not Assigned
7	Undefined Input Point 7	Not Assigned
8	Undefined Input Point 8	Not Assigned
9	Undefined Input Point 9	Not Assigned
10	Undefined Input Point 10	Not Assigned
11	Undefined Input Point 11	Not Assigned
12	Undefined Input Point 12	Not Assigned
13	Undefined Input Point 13	Not Assigned
14	Undefined Input Point 14	Not Assigned
15	Undefined Input Point 15	Not Assigned
16	Undefined Input Point 16	Not Assigned
17	Undefined Input Point 17	Not Assigned
18	Undefined Input Point 18	Not Assigned
19	Undefined Input Point 19	Not Assigned
20	Undefined Input Point 20	Not Assigned
21	Undefined Input Point 21	Not Assigned
22	Undefined Input Point 22	Not Assigned

2. Click on the corresponding text in the **Input #**, **Description** or **Zone** columns to proceed. A screen as shown below appears.



Input #: 1

Description: Motion Detector 1

Arm Delay: 0 seconds (0 - 255)

Alarm Delay: 0 seconds (0 - 255)

Alarm Zone 1	Zone	Alarm Status	Not Assigned
Undefined	Arm/ Disarm ☑ Toggle	Arm/ Disarm Status	Not Assigned
		Ready Status	Not Assigned
		Bypass Status	Not Assigned

3. Delete the default and enter the new description in the **Description** field.
4. Delete the default entry for **Arm Delay** field, and enter the new value (this field appears as a link to the first input point if this is the second or subsequent input point of an alarm zone). If you want immediate arming or 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 considered as an alarm.
5. Delete the default entry for **Alarm Delay** and enter the new value (this field appears as a link 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 when it is armed, leave it as 0. Value from 1 to 255 will cause a delay before alarm activation. During this delay period, if the input point is restored to normal, or user disarms the alarm zone, no alarm will be activated. Alarm activation will cause the output relay configured in the **Alarm Status** drop-down list to be turned on.

Notice!
The **Alarm Status** output relay assigned here is the same one that is listed at the **Output Setup.** Setting the **Duration** field to a value other than 0 at the **Output Setup** page will cause the **Alarm Status** output relay to turn on for that configured duration only. Leaving it as 0 will cause the output relay to remain on till the alarm zone is disarmed, or the input point has been restored to normal condition. Please refer to the section on *Output Setup, page 146* for more details.

6. Select the alarm zone to which this input point is to be grouped with, from the **Zone** drop-down list. If you do not wish to assign it to an alarm zone, just select “Not Assigned”. However, it must at least be assigned to a schedule for this configuration to function.
7. Select the schedule from the list. If you do not wish to assign it to a schedule, just leave it as “Undefined”. However, it must at least be assigned to an alarm zone for this configuration to function. Note: This field is disabled if this is the second or subsequent input point of an alarm zone.
8. Select the appropriate output point, for the corresponding status outputs, from their drop-down list. By default, “Not Assigned” are selected for these outputs.

Notice!
The output points listed/assigned here are the same as those listed at the **Output Setup**. By setting the **Duration** field 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 section on *Output Setup, page 146* for more details.

9. Click on the 💾 button (see NOTICE1, 2, and 3).

Notice!

Note 1: Activating the 💾 button will cause all active (armed) input points within the alarm zone to be set to default, which is the disarmed state.

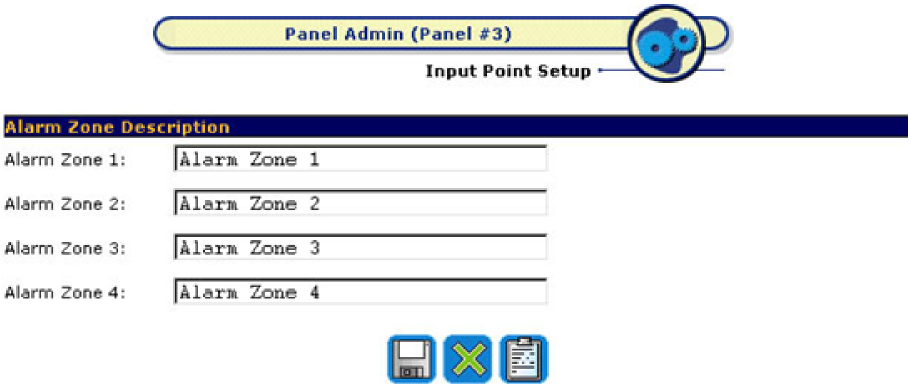
Note 2: Activating the 💾 button outside the predefined schedule intervals will cause the input point to be armed.
Note 3: When an alarm zone is also armed/disarmed by schedule, the condition similar to NOTICE 2 has the priority over NOTICE 1.

Proceed to configure other input points by clicking on the 📋 button to return to main page.

17.4.1 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 (Panel #3)

Input Point Setup

Alarm Zone Description

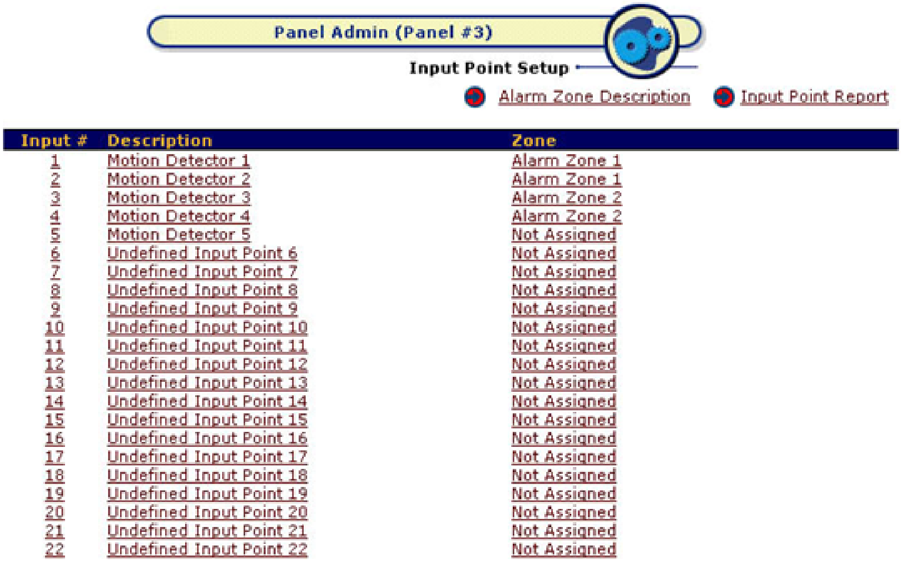
Alarm Zone 1:	Alarm Zone 1
Alarm Zone 2:	Alarm Zone 2
Alarm Zone 3:	Alarm Zone 3
Alarm Zone 4:	Alarm Zone 4

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.
2. Click the 💾 button to save the changes.

17.4.2 How to Generate a Print Preview of the Input Point Report

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.


Panel Admin (Panel #3)

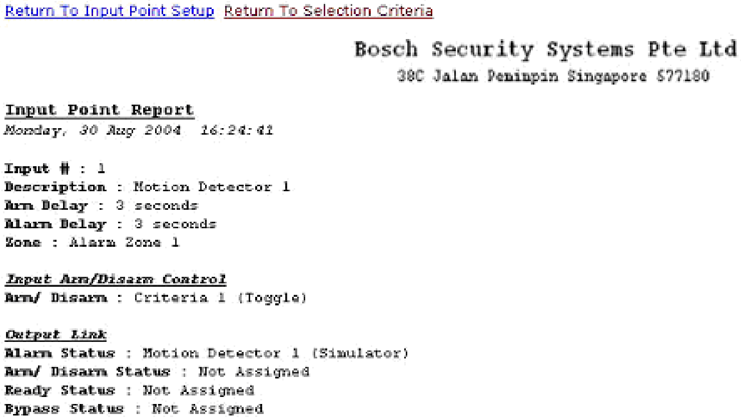
Input Point Setup

➜ Alarm Zone Description ➜ Input Point Report

Input #	Description	Zone
1	Motion Detector 1	Alarm Zone 1
2	Motion Detector 2	Alarm Zone 1
3	Motion Detector 3	Alarm Zone 2
4	Motion Detector 4	Alarm Zone 2
5	Motion Detector 5	Not Assigned
6	Undefined Input Point 6	Not Assigned
7	Undefined Input Point 7	Not Assigned
8	Undefined Input Point 8	Not Assigned
9	Undefined Input Point 9	Not Assigned
10	Undefined Input Point 10	Not Assigned
11	Undefined Input Point 11	Not Assigned
12	Undefined Input Point 12	Not Assigned
13	Undefined Input Point 13	Not Assigned
14	Undefined Input Point 14	Not Assigned
15	Undefined Input Point 15	Not Assigned
16	Undefined Input Point 16	Not Assigned
17	Undefined Input Point 17	Not Assigned
18	Undefined Input Point 18	Not Assigned
19	Undefined Input Point 19	Not Assigned
20	Undefined Input Point 20	Not Assigned
21	Undefined Input Point 21	Not Assigned
22	Undefined Input Point 22	Not Assigned

2. Select the desired input point from the **Input Description** drop-down 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 Penimpin Singapore 577180

Input Point Report
Monday, 30 Aug 2004 16:24:41

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 **File** and select **Print** menu.

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.

17.5 Output Setup

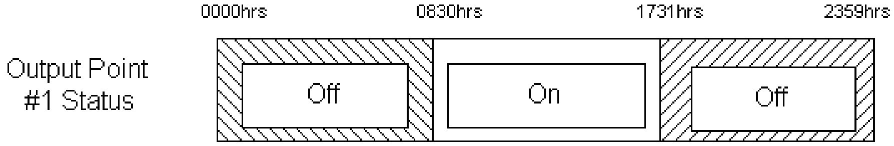
The Access Easy Controller has 32 user programmable output points that will be used for utility triggering purposes. The addresses for these input points range from 33 to 64 and are available on the I/O card. Each card can provide up to 8 output points.

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 *Input Setup, page 141* for details.

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 *Output Control, page 38* for details.

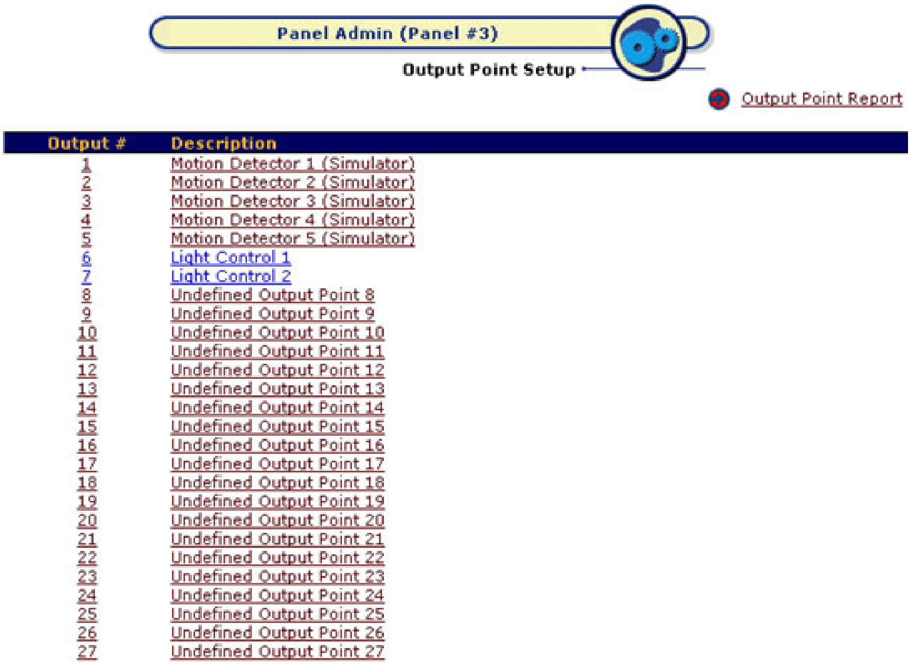
Before we start, here is a brief description of how the Access Easy Controller interprets the schedule intervals for output points triggering status.

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.



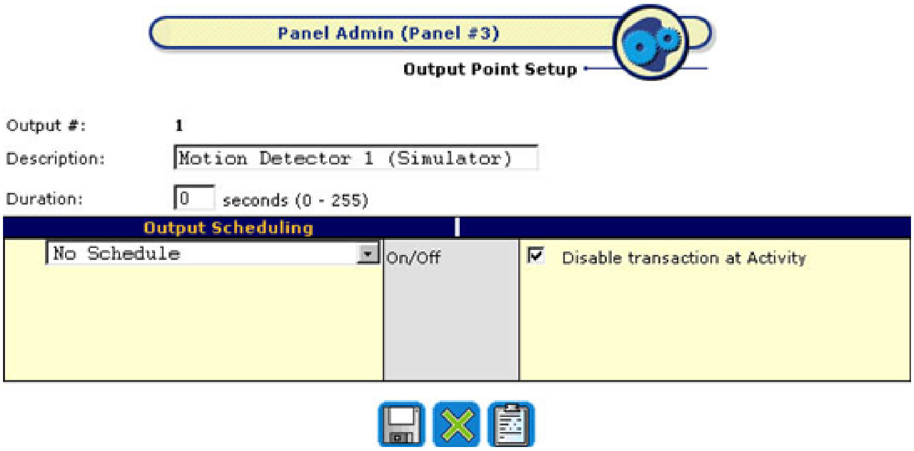
Take note that the output point switches “On” at exactly 0830hrs but switches “Off” at 1731hrs, a minute delay, as compared to the Schedule #2 setting. The reason is that Access Easy Controller takes 17:30:59hrs as a valid end time for 1730hrs.

To setup the output point, select the target Access Easy Controller.



Output #	Description
1	Motion Detector 1 (Simulator)
2	Motion Detector 2 (Simulator)
3	Motion Detector 3 (Simulator)
4	Motion Detector 4 (Simulator)
5	Motion Detector 5 (Simulator)
6	Light Control 1
7	Light Control 2
8	Undefined Output Point 8
9	Undefined Output Point 9
10	Undefined Output Point 10
11	Undefined Output Point 11
12	Undefined Output Point 12
13	Undefined Output Point 13
14	Undefined Output Point 14
15	Undefined Output Point 15
16	Undefined Output Point 16
17	Undefined Output Point 17
18	Undefined Output Point 18
19	Undefined Output Point 19
20	Undefined Output Point 20
21	Undefined Output Point 21
22	Undefined Output Point 22
23	Undefined Output Point 23
24	Undefined Output Point 24
25	Undefined Output Point 25
26	Undefined Output Point 26
27	Undefined Output Point 27

1. Click on the corresponding link in **Output #** or **Description** columns to proceed. A screen as shown below appears.



Output #: 1

Description: Motion Detector 1 (Simulator)

Duration: 0 seconds (0 - 255)

Output Scheduling

No Schedule | On/Off | ☑ Disable transaction at Activity

2. Delete the default text and enter the new description in the **Description** field.
3. Delete the default entry and enter the new value in seconds the **Duration** field.
4. By checking the **Disable transaction at Activity** checkbox, user can disable any of the 32 output points activity, especially when they are activated by other type of function or elevator operation which don't require any logging.

Notice!

This setting for the **Duration** field is applicable for manual output control (refer to *Output Control, page 38*). 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.

5. Select the appropriate schedule from the drop-down list. By default, an unused output point is tied to “No Schedule”, which means that the output will not be triggered.
6. Click on the button.

Notice!

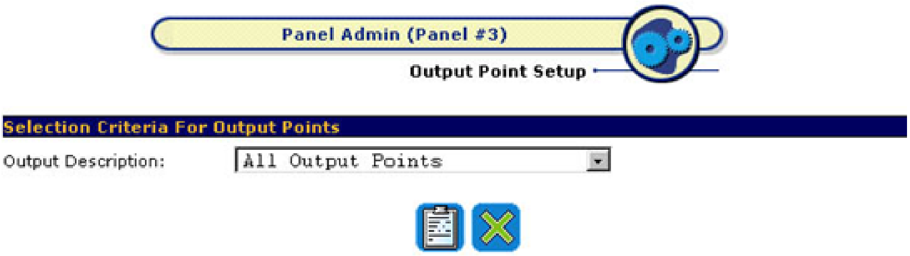
Activating the button within the predefined schedule intervals will cause the output relay to turn on.

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

17.5.1 How to Generate a Print Preview of the Output Point Report

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.



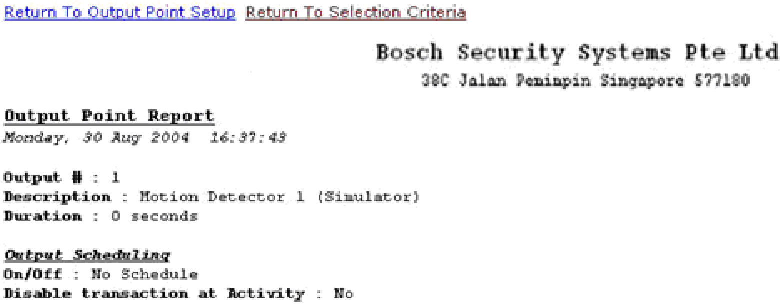
Panel Admin (Panel #3)

Output Point Setup

Selection Criteria For Output Points

Output Description: All Output Points

2. Select the desired output point from the **Output Description** drop-down list. If all output points are required, select the “All Output Points” item.
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

Monday, 30 Aug 2004 16:37:43

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.

17.6 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”.

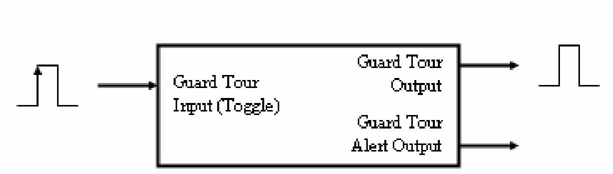
Some of the advance functions that it can support are:

- 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.

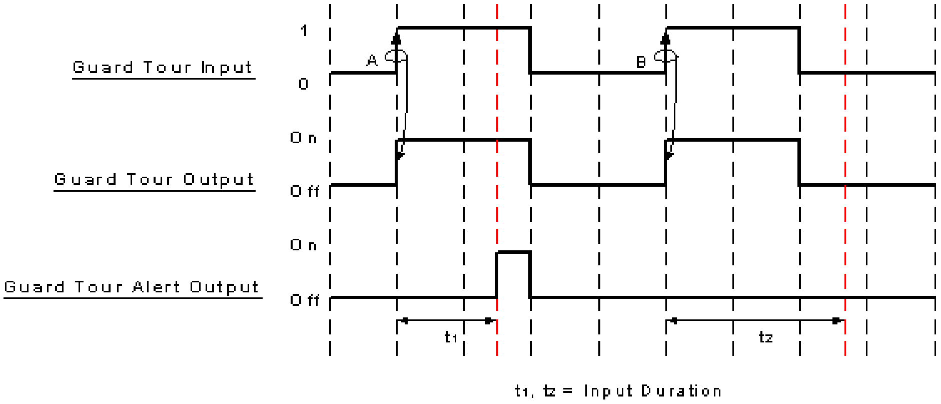
17.6.1 Guard Tour

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 the “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.



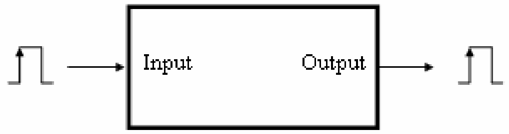
In the timing diagram above, Guard Tour Input at transition A and B will cause the Guard Tour Output to be turned on for the duration when the Guard Tour Input is triggered. When the Input Duration t1, has lapsed and the Guard Tour Input is still at High (1), the Guard Tour Alert Output will be turned on until the Guard Tour Input is switched to Low (0). Whereas for t2, the Input Duration is such that the Guard Tour Input has already been switched to Low (0) before the Input Duration t2, 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, an 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.

17.6.2 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.

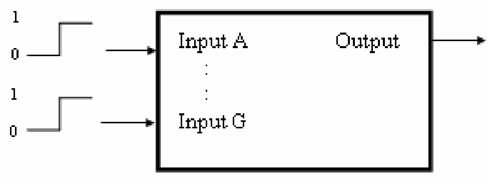
This function will enable any type of output such as physical output, link or reader control to follow the input such as physical input, physical output, link, criteria or schedule. Level or toggle input behavior can be selected.



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.

17.6.3 OR Logic

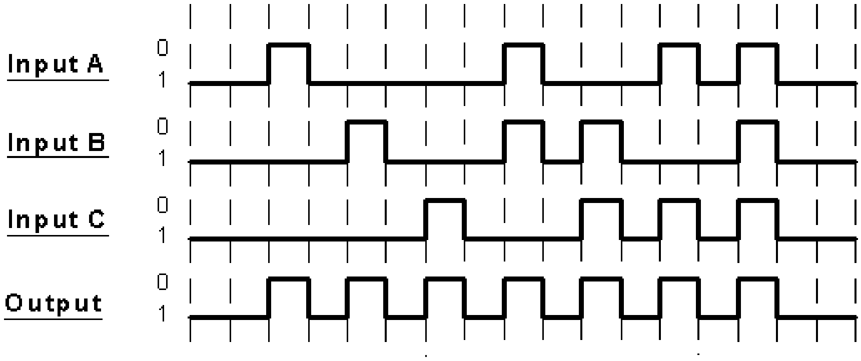
This function is used in cases whereby the output of a function block is to be triggered when any one or more of the stated conditions is fulfilled. In **Advance I/O Setup**, a maximum of seven conditions is allowed.



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.

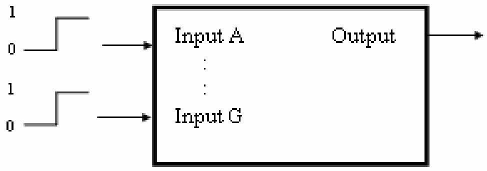
Input A	Input B	Input C	Output
0	0	0	0
1	0	0	1
0	1	0	1
0	0	1	1
1	1	0	1
0	1	1	1
1	0	1	1
1	1	1	1

The timing diagram below gives a graphical description of the function.



17.6.4 AND Logic

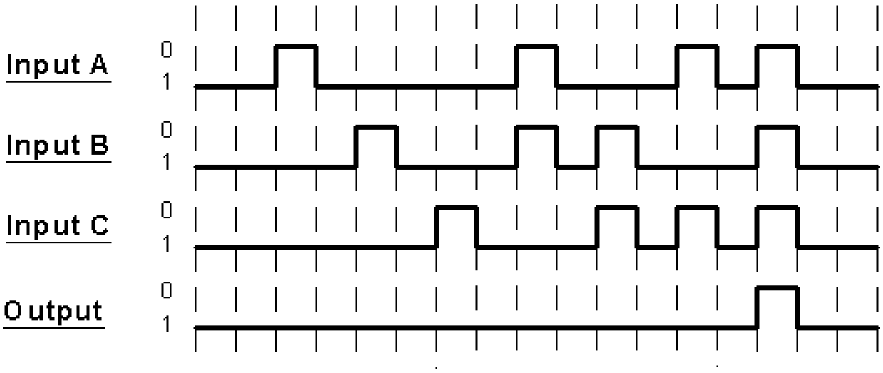
This function is used in cases whereby the output of a function block is to be triggered when all the stated conditions are fulfilled. In **Advance I/O Setup**, a maximum of seven conditions is allowed.



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.

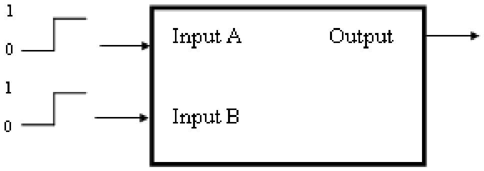
Input A	Input B	Input C	Output
0	0	0	0
1	0	0	0
0	1	0	0
0	0	1	0
1	1	0	0
0	1	1	0
1	0	1	0
1	1	1	1

The timing diagram below gives a graphical description of the function.



17.6.5 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 seven conditions is allowed.

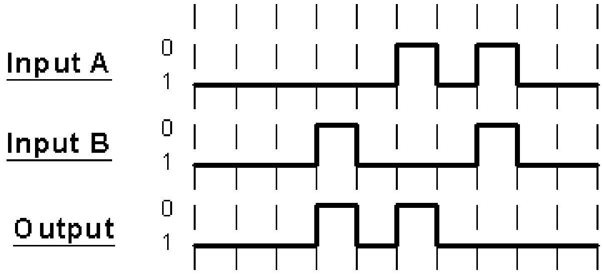


The output is set to high when all the stated inputs are at different states. The following table depicts the XOR logic operation, assuming only two inputs are used.

Input A	Input B	Output
0	0	0
0	1	1

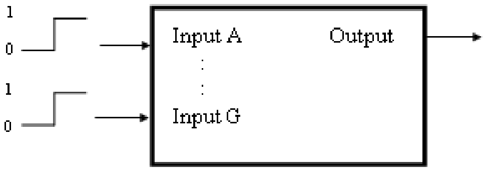
1	0	1
1	1	0

The timing diagram below gives a graphical description of the function.



17.6.6 NAND Logic

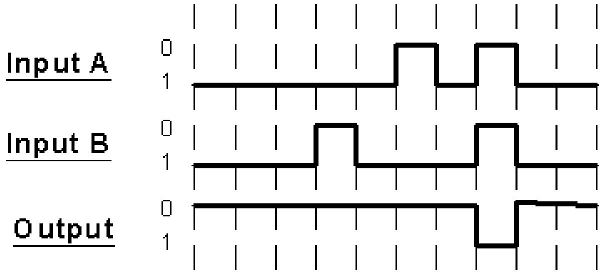
This function is used in cases whereby the output of a function block is to be triggered when one or more of the input states is low.



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 two 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.



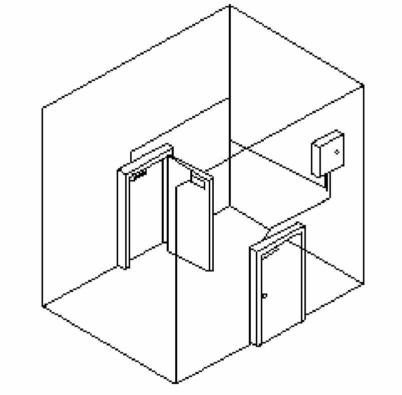
17.6.7 Interlock / Man Trap

Interlock Operation

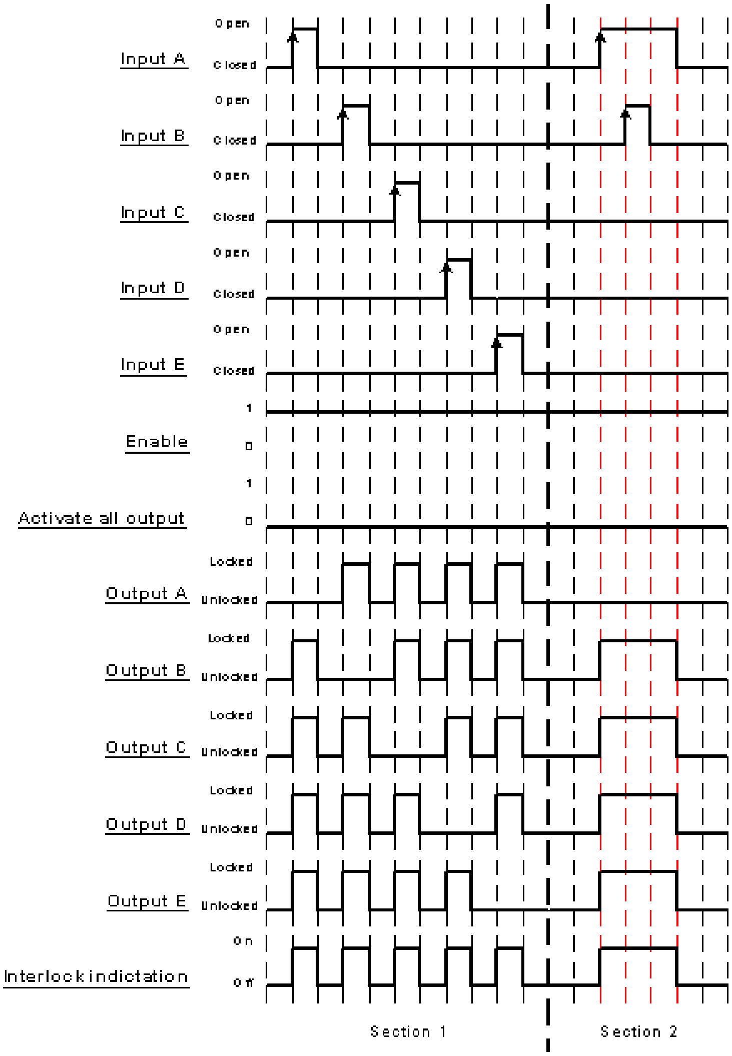
All doors will remain closed and unlocked. Opening any of the doors will cause all other doors to be locked until the opened door returns to the closed position. In Access Easy Controller, a maximum of five doors is configurable.

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 two doors.



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.

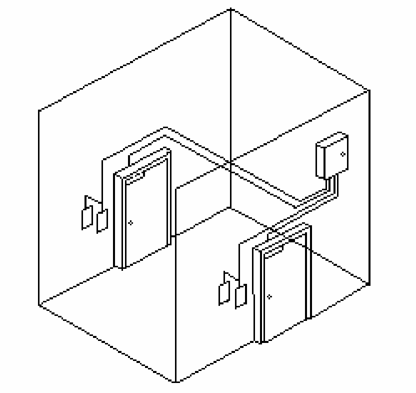
But before door at A is closed, someone tries to open door at B. He cannot open the door at B as it is locked (Output B-High) as door at A has not been closed back to original position.

Man Trap Operation

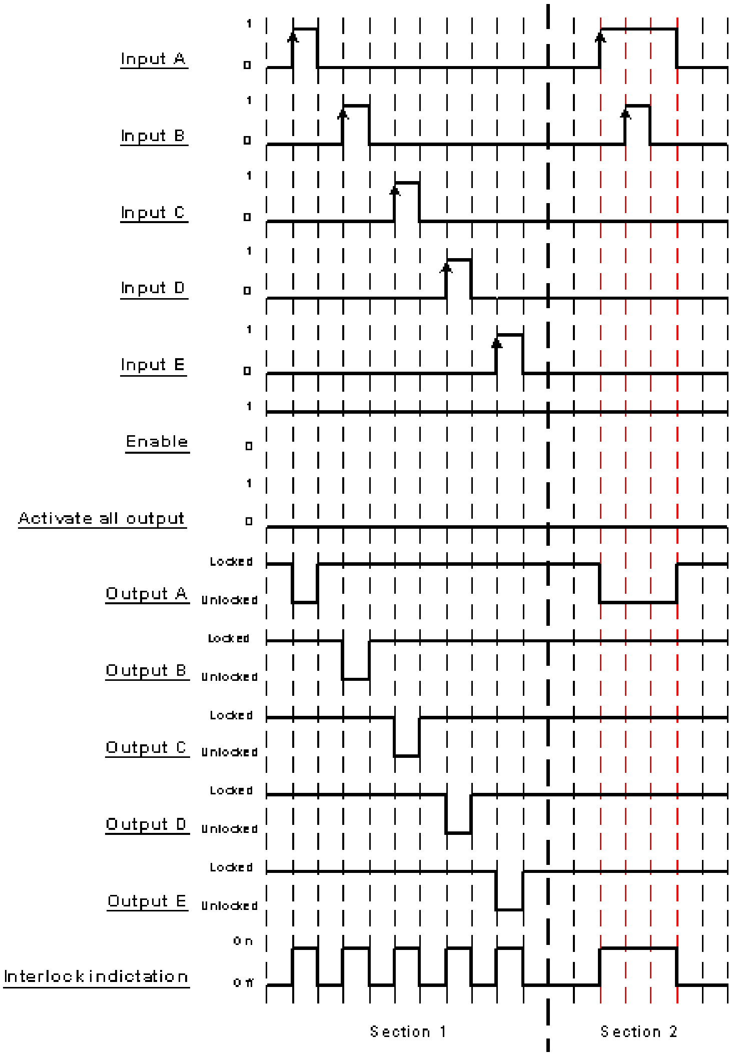
All doors are normally closed and locked. Unlocking any door by reader causes the other doors to be incapable of being unlocked. In Access Easy Controller, a maximum of five doors is configurable.

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 two doors.



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, that is 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).

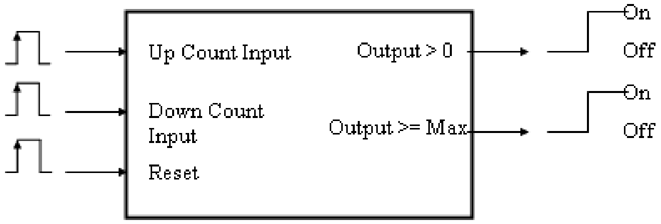
But before door A is locked back, someone presents his card at door B. He cannot unlock door B as it is incapable of being unlocked (Output B-High).

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.

17.6.8 Up-Down Counter

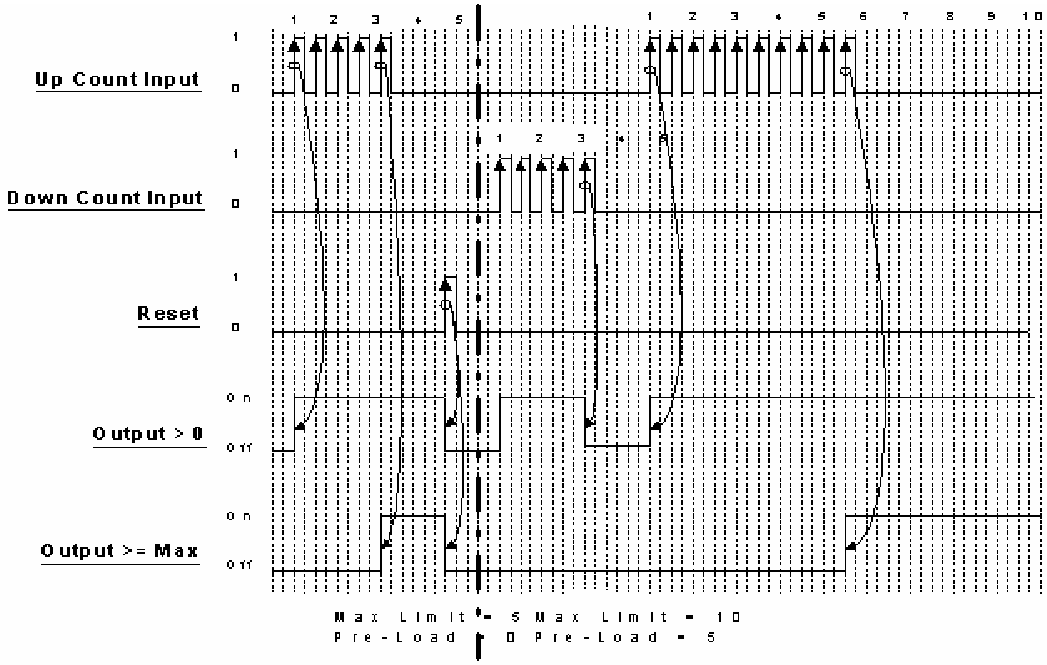
This function enables the tracking of the number of card holder/event and is able to trigger output or control based on the maximum configuration limit.



Maximum Limit = XXXXX (0 to 65535)
Pre-load counter value = XXXXX (0 to

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.

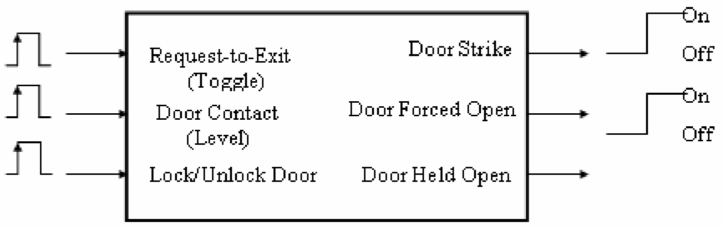
Max Limit = 5 and Pre-Load = 0
With the 2 defined parameters, the Output >= Max will be driven high on the 5th pulse on the Up Count input. However, the Output > 0 is driven high on the first pulse. A Reset pulse clears both outputs to zero.

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.

17.6.9 Exit Door

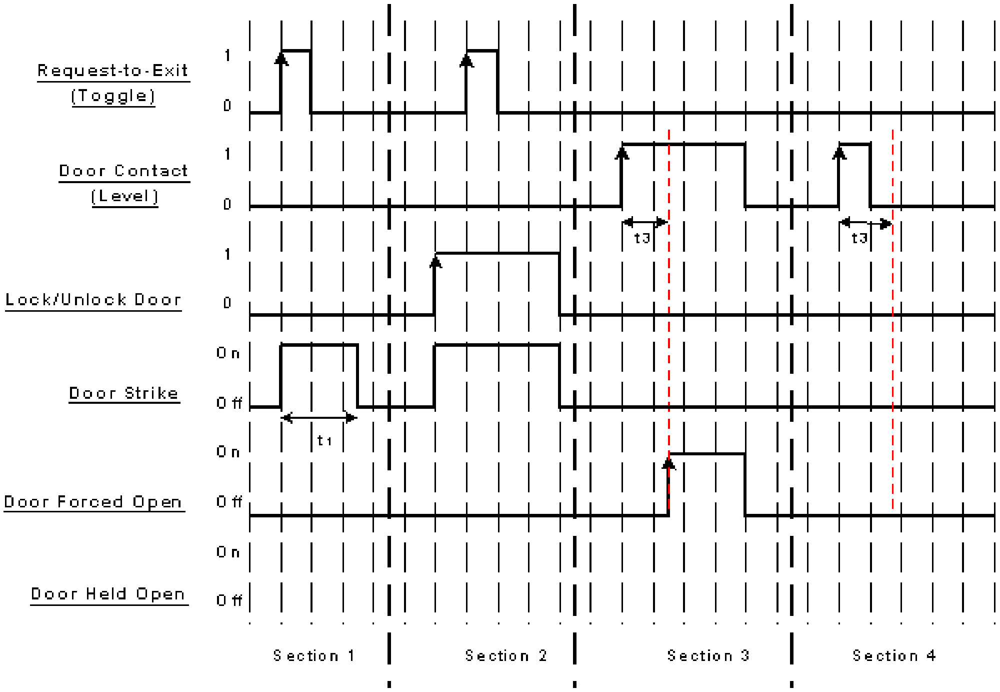
This function is mainly used to monitor and control emergency exit doors.



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



t1 = Door Strike Duration, t3 = Door Forced Open Alarm Delay Duration

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 t1, 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-energized, 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 t3. 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.

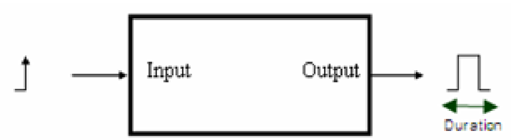
Section 4

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 t3. Therefore the Door Forced Open output is not activated. This is because the signal detected could be due to noise or interference.

17.6.10 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.

17.7 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.

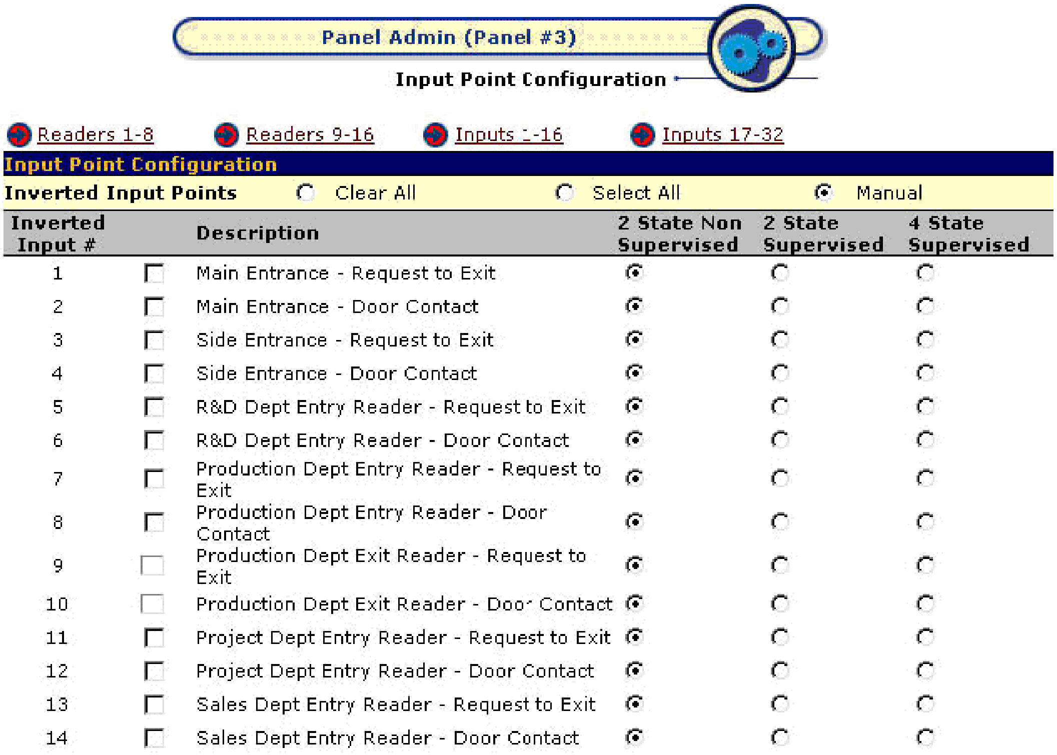
In simple term, this configuration allows user to inverts the logical state of the input that is seen by the Access Easy Controller thus allowing such devices to be used.

Access Easy Controller allows all the input points to be inverted except those assigned to exit readers and arm/disarm readers.

In this section, users can also select the input point to be in 2-state non-supervised, 2-state supervised or 4-state supervised monitoring state.

17.7.1 To activate Input Point Configuration

To configure the **Input Point Configuration**, select the target Access Easy Controller and click on the **Input Point Configuration** link. The following screen will appear.



Panel Admin (Panel #3)

Input Point Configuration

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 - Doo' Contact	●	○	○
11	□	Project Dept Entry Reader - Request to Exit	●	○	○
12	□	Project Dept Entry Reader - Door Contact	●	○	○
13	□	Sales Dept Entry Reader - Request to Exit	●	○	○
14	□	Sales Dept Entry Reader - Door Contact	●	○	○

Notice!

Input 9 and 10 are assigned to Reader #5 - Production Dept Exit Reader. Since Reader #5 is defined as an exit reader, the checkboxes are disabled.

To select Input Point Configuration

Using **Manual**

1. To assign the required **Input Point Configuration f**or the inversion, click on the corresponding **Input Point Configuration** checkboxes to show a check mark. To deselect the point, click on it again.
2. Click on the 💾 button. Alternatively, click on the ➡ button to select the next sets of input points. User can also select from the sets of inputs from the links at the top, such as **Readers 1-8**, **Readers 9-16**, **Inputs 1-16** or **Inputs 17-32**.

Using **Select All**

This is very useful if the number of input points need to be selected is more than three quarter of what is displayed. You can use this function then deselect those unwanted input points.

Notice!
The **Select All** and **Clear All** function will only select / clear the 16 input points seen on the current web page. For the other input points on the other pages, user will have to go to the page and select / clear.

1. To select all, click on the **Select All** radio button. To deselect, click on **Clear All** or **Manual** radio button.
2. Click on the 💾 to refresh the screen and the selection returns to default (**Manual** radio button is selected). If not all inverted input points are required, proceed to deselect by clicking on its corresponding checkboxes. 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. User can also select from the sets of inputs from the links at the top, such as **Readers 1-8**, **Readers 9-16**, **Inputs 1-16** or **Inputs 17-32**.

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

17.7.2 To Select 2 State Non-Supervised, 2 State Supervised or 4 State Supervised

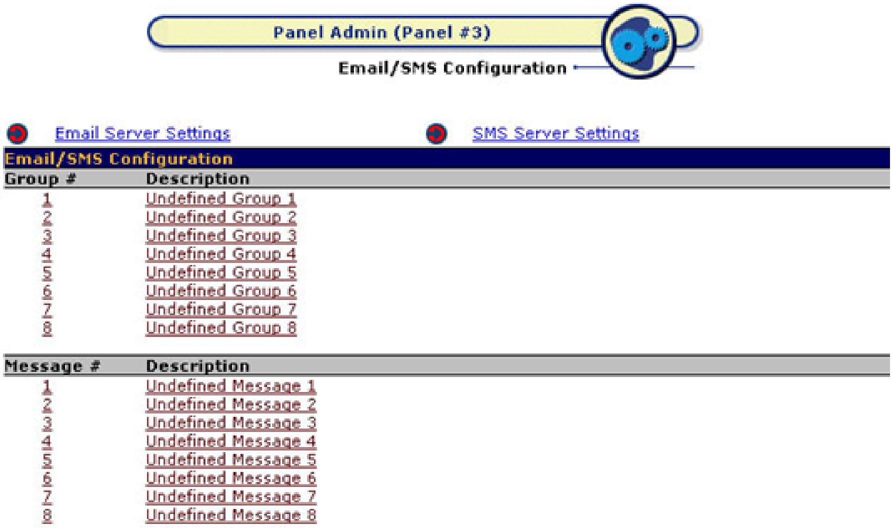
This will provide the system installer to have the flexibility of configuring any input in the panel to be in any monitoring requirement.

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

To select either the 2 state non-supervised, 2 state supervised or 4 state supervised state, select the radio button belonging to the input point accordingly.

17.8 Email/SMS Configuration

To configure the **Email/SMS Configuration**, select the target Access Easy Controller and click on the **Email/SMS Configuration** link. The following screen will appear.



Email/SMS Configuration

Group #	Description
1	Undefined Group 1
2	Undefined Group 2
3	Undefined Group 3
4	Undefined Group 4
5	Undefined Group 5
6	Undefined Group 6
7	Undefined Group 7
8	Undefined Group 8

Message #	Description
1	Undefined Message 1
2	Undefined Message 2
3	Undefined Message 3
4	Undefined Message 4
5	Undefined Message 5
6	Undefined Message 6
7	Undefined Message 7
8	Undefined Message 8

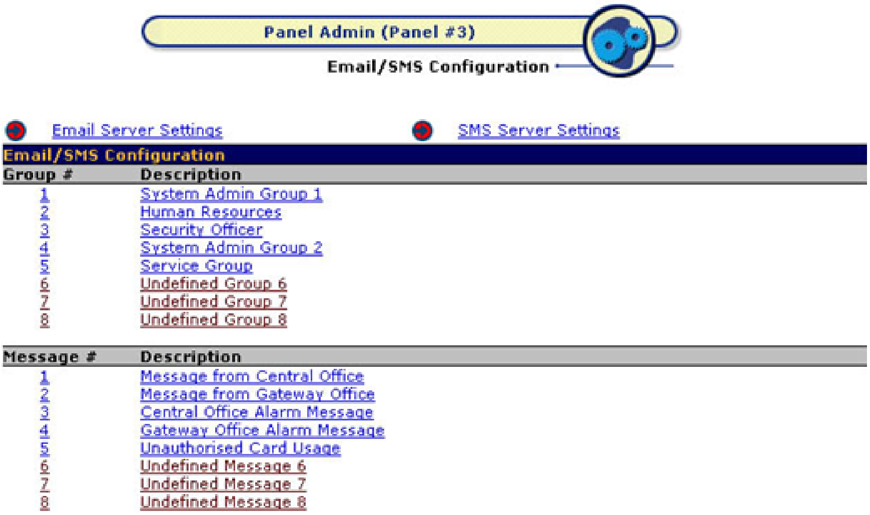
This function allows user to configure the Access Easy Controller to send out messages or Lateness Report using Simple Mail Transfer Protocol (SMTP) to email addresses. A total of eight groups and eight messages field are available for configuration. Each group has three "Send To" and three "Carbon Copy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

1. From the left pane, click on the **Email/SMS Configuration** link. The screen as shown below appears.



Email/SMS Configuration

Group #	Description
1	System Admin Group 1
2	Human Resources
3	Security Officer
4	System Admin Group 2
5	Service Group
6	Undefined Group 6
7	Undefined Group 7
8	Undefined Group 8

Message #	Description
1	Message from Central Office
2	Message from Gateway Office
3	Central Office Alarm Message
4	Gateway Office Alarm Message
5	Unauthorised Card Usage
6	Undefined Message 6
7	Undefined Message 7
8	Undefined Message 8

2. Click on any corresponding entry in the **Group #** or **Description** columns and you will be shown the **Send To** page.

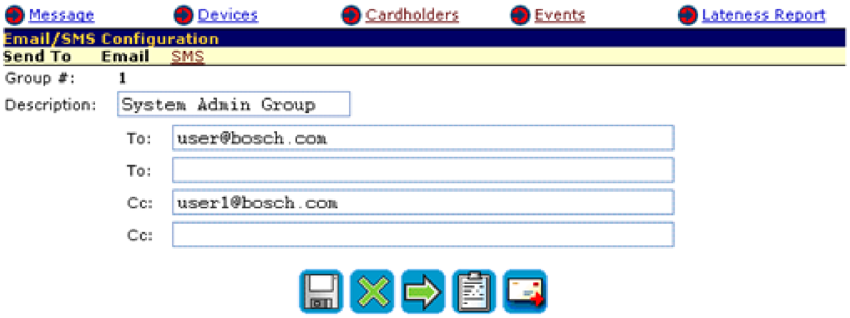
17.8.1 Send To

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** fields. Each **To** and **Cc** field should only contains one email address. Entering more than one email address separated by a coma (,) or semi-coma (;) will be taken as a single email address, hence it will not able to send out the mail to the recipients.

Send To Configuration (Email)

To edit the **Send To** configuration for email:

1. Click on the corresponding item in **Group #** or **Description** column to proceed. The following email configuration screen appears by default. Otherwise, click the **Email** link.



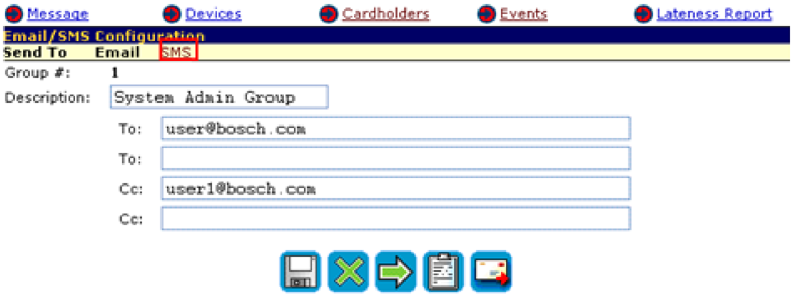
Group #: 1
Description: System Admin Group
To: user@bosch.com
To:
Cc: user1@bosch.com
Cc:

2. Highlight the default text and enter a description for the group in the **Description** field.
3. Enter the email addresses in the appropriate fields.
4. Click on the button.

Send To Configuration (SMS)

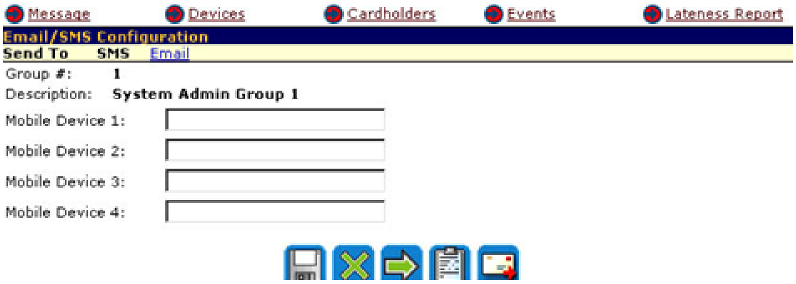
To edit the **Send To** configuration for SMS:

1. Click on the corresponding item in **Group #** or **Description** column to proceed. The following email configuration screen appears by default.



Group #: 1
Description: System Admin Group
To: user@bosch.com
To:
Cc: user1@bosch.com
Cc:

2. From the screen above, click on the **SMS** link to configure the **Send To** configuration for SMS. The screen as shown below appears.



Email/SMS Configuration

Send To **SMS** Email

Group #: 1

Description: **System Admin Group 1**

Mobile Device 1:

Mobile Device 2:

Mobile Device 3:

Mobile Device 4:

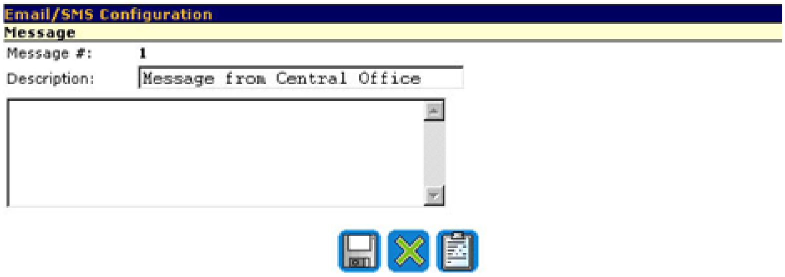
3. Enter the mobile numbers in the appropriate fields.
4. Click on the 💾 button.

17.8.2 Message field

The **Message** field makes up the body of the text while the event is to appear as the **Subject** field of the dispatched email.

To edit the **Message** field:

1. Click on the item in the **Message #** or **Description** column to proceed.



Email/SMS Configuration

Message

Message #: 1

Description: Message from Central Office

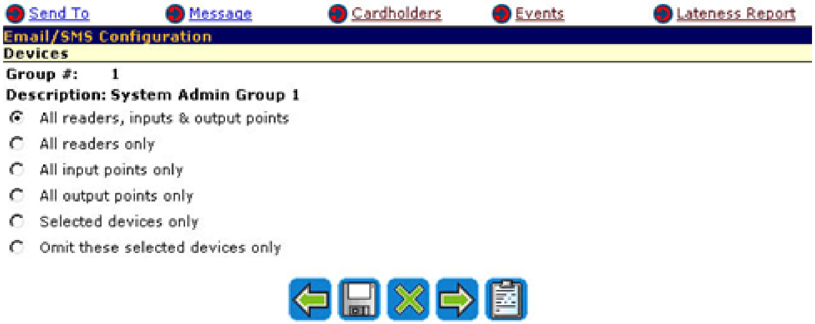
2. Highlight the default text and enter a description for the message in the **Description** field.
3. Enter the new message limiting to 127 characters including punctuation in the text box.
4. Click on the 💾 button.
5. Click on the 📋 button to return.

17.8.3 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)**:

1. Click on the **Device** link or the button from the **Sent To** web page.



Email/SMS Configuration

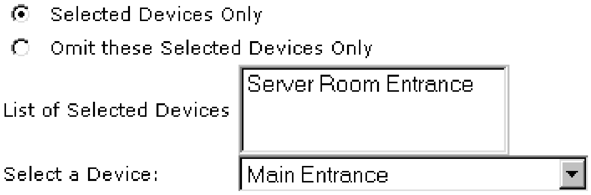
Devices

Group #: 1

Description: System Admin 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

2. 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** radio buttons, a window and a drop-down list appears as shown below.



● Selected Devices Only
○ Omit these Selected Devices Only

List of Selected Devices: Server Room Entrance

Select a Device: Main Entrance

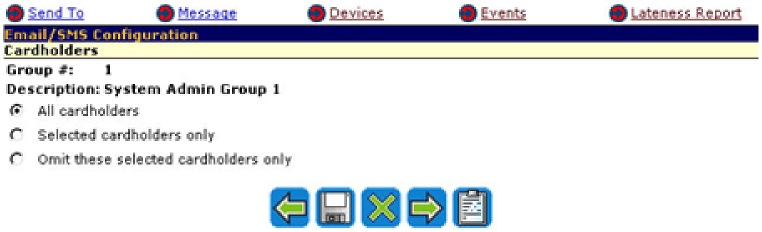
3. Select a device from the drop-down list and click on the button. The selected device appears in the **List of Selected Devices** list box. Repeat step 3 if you have other devices to put on the list.
4. To delete selected device(s), click on the device name in the window followed by the button. Repeat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

17.8.4 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 from the **Devices** web page.



Email/SMS Configuration

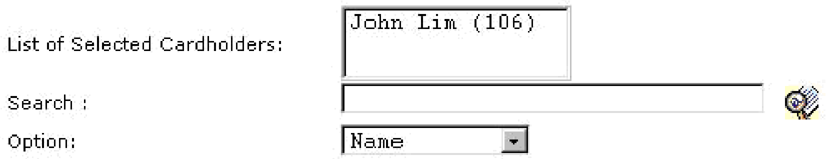
Cardholders

Group #: 1

Description: System Admin Group 1

● All cardholders
○ Selected cardholders only
○ Omit these selected cardholders only

2. Select the desired radio button, and click on the button. If either **Selected cardholders only** or **Omit these selected cardholders only** radio button is selected, a window and the **Search** field appear as shown below. You have the option to search by name, card number or the 2 user fields by selecting from the **Option** drop-down list.



List of Selected Cardholders: John Lim (106)

Search :

Option: Name

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 *Card Assignment, page 42* for more details.

3. Select the cardholder and click on the ✚ button. The selected cardholder appears in the **List of Selected Cardholders** list box. Repeat step 3 if you have other cardholders to put on the list.

Notice!
The **List of Selected Cardholders** list box has a limit of up to 80 entries.

4. To delete selected cardholder(s), click on the cardholder's name in the window followed by the 🗑 button. Repeat step 4 if necessary.

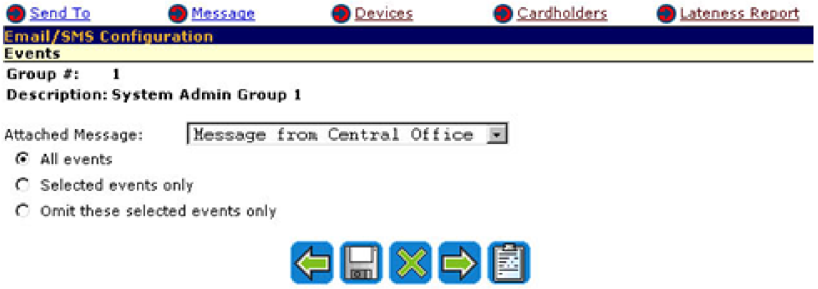
5. When you finish with your selection, click on the 💾 button.

17.8.5 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)**:

1. Click on the **Events** link, or the ➡ button from the **Cardholders** web page.



Email/SMS Configuration

Events

Group #: 1

Description: System Admin Group 1

Attached Message: Message from Central Office

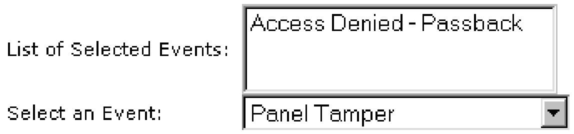
● All events

○ Selected events only

○ Omit these selected events only

2. Select the predefined message from the **Attached Message** drop-down list.

3. Select the desired radio button and click on the 💾 button. If either **Selected events only** or **Omit these selected events only** radio button is selected, a window and a drop-down list appear as shown below.



List of Selected Events: Access Denied - Passback

Select an Event: Panel Tamper

4. Select the desired event and click on the ➕ button. The selected event appears in the **List of Selected Events** list box. Repeat step 4 if you have other events to add 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. When you finish your selection, click on the 💾 button.

User can refer to *APPENDIX D Email/SMS Configuration Table, page 236* for the combination of devices, cardholders and events to select.

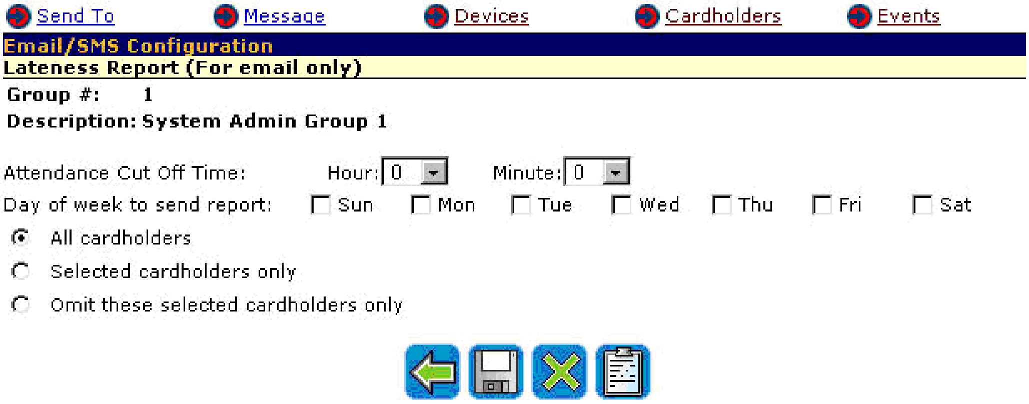
17.8.6 Lateness Report

This web page allows user to configure the Lateness Report.

Notice!
The Lateness Report is to be 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 from the **Events** web page.



Send To Message Devices Cardholders Events

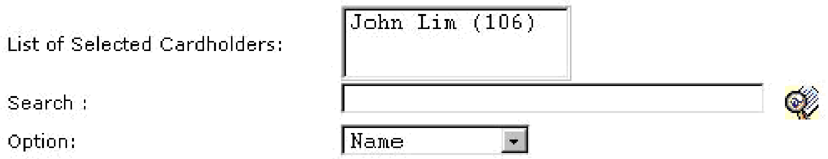
Email/SMS Configuration
Lateness Report (For email only)

Group #: 1
Description: System Admin Group 1

Attendance Cut Off Time: Hour: 0 Minute: 0
Day of week to send report: □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

● All cardholders
○ Selected cardholders only
○ Omit these selected cardholders only

2. Select the hour and minutes from the drop-down list of **Attendance Cut Off Time**. The **Attendance Cut off Time** defines the time on which the panel 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** checkboxes. The **Day of the week to send report** defines the day on which the panel 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 either **Selected cardholders only** or **Omit these selected cardholders only** radio button is selected, 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 list.



List of Selected Cardholders: John Lim (106)

Search :

Option: Name

The **Selection By Card #** and **Selection By Name** function is similar to the **Search By Card #** and **Search By Name** function respectively. Please refer to the explanation in the section *How to Use Search Function, page 60* for more detail.

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

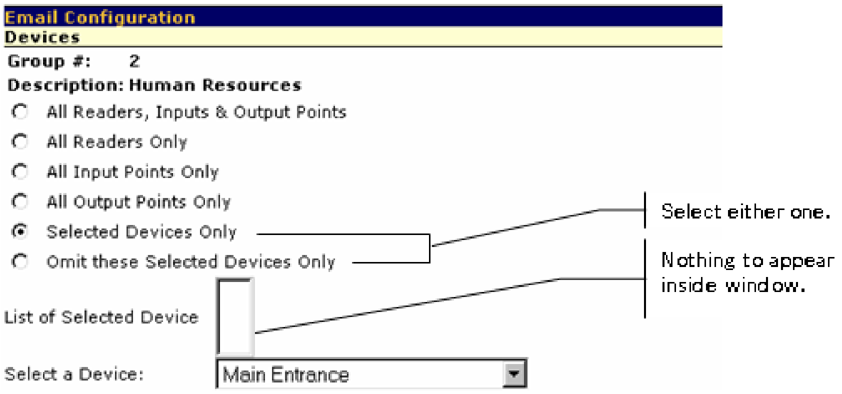
Notice!
The **List of Selected Cardholders** list box has a limit of up to 80 entries.

6. To delete selected cardholder, click on the cardholder's name in the **List of Selected Cardholders** list box 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 *APPENDIX D Email/SMS Configuration Table, page 236* 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

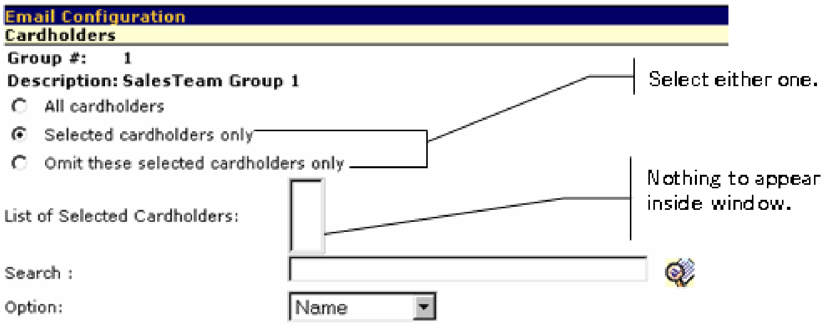
○ All Readers, Inputs & Output Points
○ All Readers Only
○ All Input Points Only
○ All Output Points Only
● Selected Devices Only
○ Omit these Selected Devices Only

List of Selected Device

Select a Device: Main Entrance

Select either one.

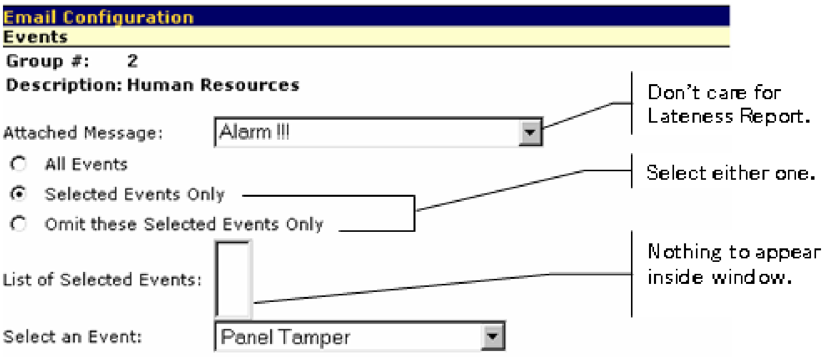
Nothing to appear inside window.



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: Name

Select either one.

Nothing to appear inside window.

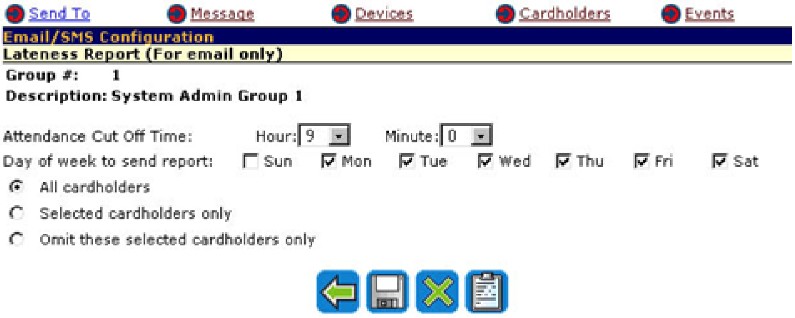


Email Configuration
Events
Group #: 2
Description: Human Resources
Attached Message: Alarm !!!
○ All Events
● Selected Events Only
○ Omit these Selected Events Only
List of Selected Events:
Select an Event: Panel Tamper

Don't care for Lateness Report.

Select either one.

Nothing to appear inside window.

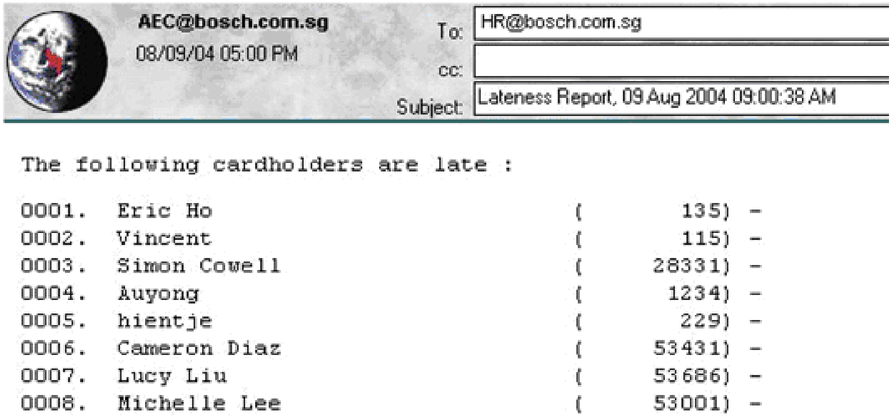


Email/SMS Configuration
Lateness Report (For email only)
Group #: 1
Description: System Admin Group 1
Attendance Cut Off Time: Hour: 9 Minute: 0
Day of week to send report: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
● All cardholders
○ Selected cardholders only
○ Omit these selected cardholders only

With such configuration, the panel will keep track of the cut-off time from Monday through Saturday (at 0900hrs) and will send out the Lateness Report to the recipient(s).

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

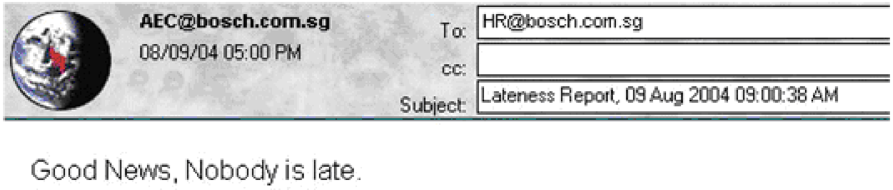
– The following Cardholders are late.



AEC@bosch.com.sg
08/09/04 05:00 PM
To: HR@bosch.com.sg
cc:
Subject: Lateness Report, 09 Aug 2004 09:00:38 AM

```
The following cardholders are late :

0001.  Eric Ho                             (      135) -
0002.  Vincent                             (      115) -
0003.  Simon Cowell                        (    28331) -
0004.  Auyong                              (     1234) -
0005.  hientje                             (      229) -
0006.  Cameron Diaz                        (    53431) -
0007.  Lucy Liu                            (    53686) -
0008.  Michelle Lee                        (    53001) -
```

– All Employees are punctual.



AEC@bosch.com.sg
08/09/04 05:00 PM

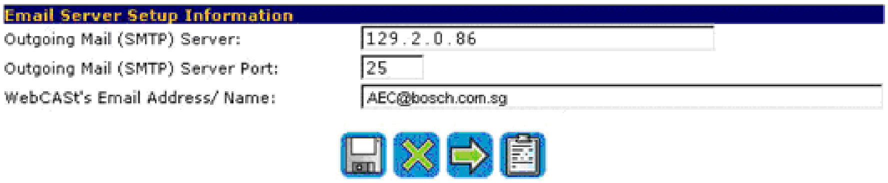
To: HR@bosch.com.sg
cc:
Subject: Lateness Report, 09 Aug 2004 09:00:38 AM

Good News, Nobody is late.

17.8.7 Email Server Settings

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 Settings link to go to the **Outgoing Mail (SMTP) Server Configuration** page.

The **Outgoing Mail (SMTP) Server** defines the server that will provide your email facilities. The Access Easy Controller's email address/name is the reply address for emails sent by the Access Easy Controller, which is the address name that appears in the **Sent To** field of the dispatched email.



Email Server Setup Information

Outgoing Mail (SMTP) Server:	129.2.0.86
Outgoing Mail (SMTP) Server Port:	25
WebCASt's Email Address/ Name:	AEC@bosch.com.sg

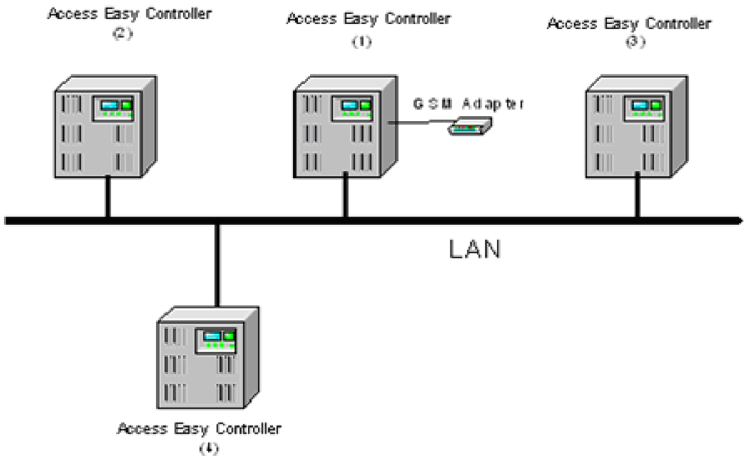
To edit the Email Server Setup Information

1. Highlight the default text in the **Outgoing Mail (SMTP) Server** field and enter the IP address.
2. The default number 25 is the commonly used port number for the **Outgoing Mail (SMTP) Server Port**. 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 screen-capture 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.

17.8.8 SMS Server Settings

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 Controllers in the network. These panels work stand-alone but share 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 Controllers' messages to the Service Provider.

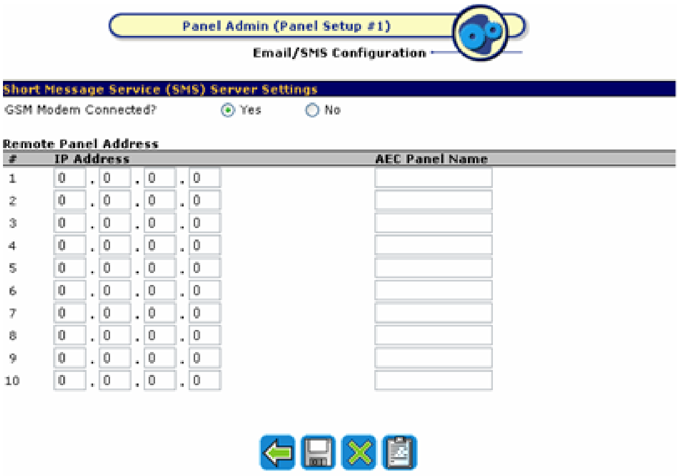
Whenever there is any SMS message that needed to be send, the respective Access Easy Controller will send the SMS messages over to the Access Easy Controller SMS server and the SMS server will send via the GSM adapter to the Service Provider. These panels are said to be acting as the SMS client. Hence, there is a need to control which IP addresses are allowed to send SMS to prevent unauthorized personnel sending SMS via your Access Easy Controller.

Notice!
Please ensure that GSM adapter baudrate is configure at 115200bps, 8bit data, 1 stop bit and no parity settings. Please refer to the APPENDIX G Modem Setup for details.

To Configure Access Easy Controller as an SMS Server

By default, the SMS server IP address is blank. If this panel is attached to a GSM adapter, you will need to configure the IP address of other Access Easy Controllers that will send SMS messages through it.

1. To change this setting, click on the ➔ SMS Server Settings link. The screen as shown below appears.



Short Message Service (SMS) Server Settings

GSM Modem Connected? ● Yes ○ No

Remote Panel Address

#	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	

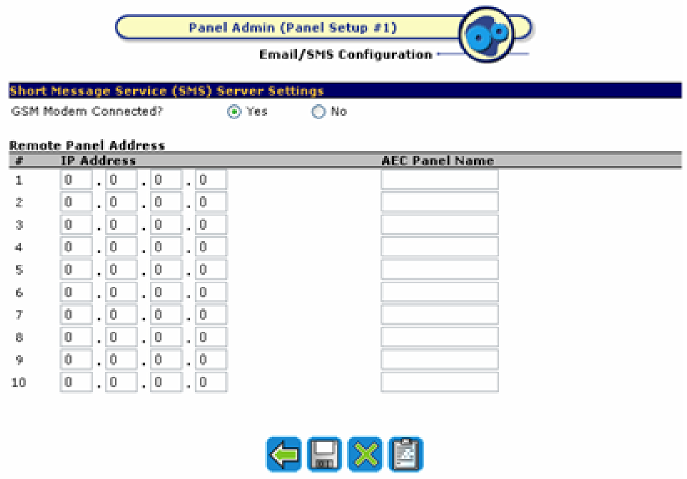
2. By default, the **GSM Modem Connected?** radio button is selected as “Yes”.
3. There are up to 10 remote panel addresses that you can configure. These are the IP addresses of the Access Easy Controllers that can send SMS messages via the SMS server.
4. After the IP addresses are configured, click on the 💾 button.
5. You will need to reboot the Access Easy Controller for the changes to take effect.

Notice!
To allow the Access Easy Controller that is acting as the SMS server to send SMS message, its IP address has to be included in the list as well.

To Configure Access Easy Controller as an SMS Client

By default, the SMS server IP address is blank. If this panel is not attached to a GSM adapter, it is an SMS client and hence, it needs to identify the IP address of the SMS server.

1. To change this setting, click on the ➜ SMS Server Settings link. The screen as shown below appears.



Panel Admin (Panel Setup #1)
Email/SMS Configuration

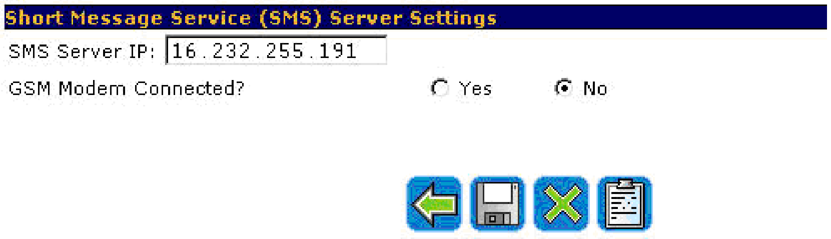
Short Message Service (SMS) Server Settings

GSM Modem Connected? ● Yes ○ No

Remote Panel Address

#	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	

2. Select “No” for **GSM Modem Connected?** radio button, and click on the 💾 button. The screen as shown below appears.



Short Message Service (SMS) Server Settings

SMS Server IP: 16.232.255.191

GSM Modem Connected? ○ Yes ● No

3. Since this is an SMS Client, delete the default IP address in the **SMS Server IP** field and enter the IP address of the SMS Server.
4. Click on the 💾 button.
5. You will need to reboot the Access Easy Controller for the changes to take effect.

Notice!
As there is only one available serial com port in the CPU, only either the GSM adapter or the analog dial-up modem can be connected to the Access Easy Controller. Hence, dial-up features will not be enabled when SMS server is configured. Likewise the SMS server when dial-up has been set up. By default the dial-up feature is enabled and the SMS feature is disabled.

17.9 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.

Notice!
This feature is applicable to full and soft anti-passback only.

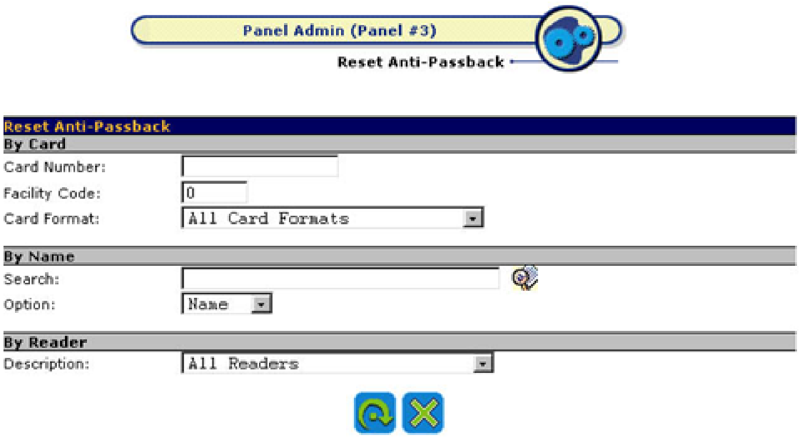
Please refer to the previous section on *Anti-Passback (APB) Settings, page 137*.

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 reset APB, select the target Access Easy Controller and click on the **Reset APB** link. The following page will appear in a new window.



Reset Anti-Passback

By Card

Card Number:

Facility Code: 0

Card Format: All Card Formats

By Name

Search:

Option: Name

By Reader

Description: All Readers

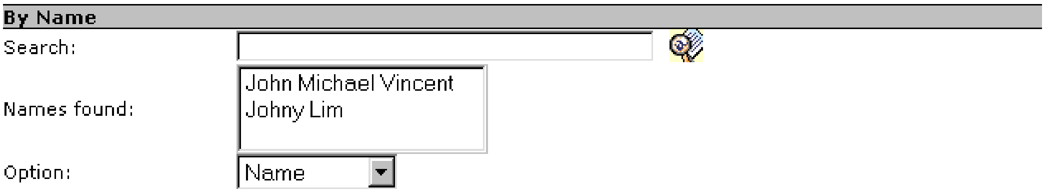
17.9.1 How To Reset APB by Card Number wrt Reader / All Readers

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 in the **Card Number** field.
2. Enter the facility code in the **Facility Code** field if the code is different from the default. Facility code is configured in **Default Settings** of the **Panel Setup**.
3. Select the card format from the **Card Format** drop-down list.
4. Select the reader from the **Description** drop-down list. If you want to reset APB with respect to 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 and zones with respect to reader / all readers will be displayed.
6. Click on the ⇦ button to return.

17.9.2 How to Reset APB based on Name wrt Reader / All Readers

1. Enter a character, a portion, or the full name in the **Search** field, and click on the 🔍 button. If a match is found that satisfies the entry, the names will appear in the **Names found** list box. For example, enter “John” and click 🔍 button will result in:



By Name

Search: 🔍

Names found: John Michael Vincent
Johny Lim

Option: Name

2. From the **Names found** list box, select the appropriate name. The selected name will appear in the **Search** field.
3. Select the reader from **Description** drop-down 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 will be displayed.
5. Click on the ⇦ button to return.

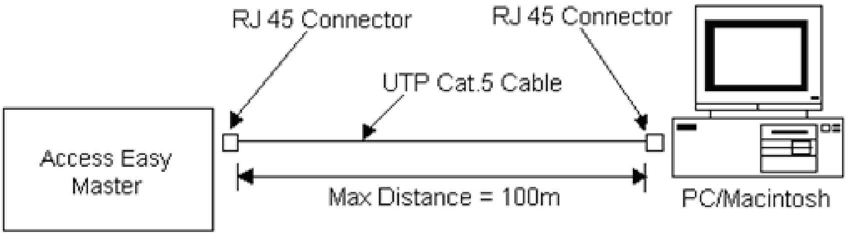
17.9.3 How to Reset APB by All Card Numbers wrt Reader / All Readers

1. Select the readers from the **Description** drop-down 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 and zones with respect to reader / all readers will be displayed.
3. Click on the ⇦ button to return.

18 How to Configure the Access Easy Master IP Address

Configuring the IP address of the Access Easy Master requires you to initially prepare a PC/ Macintosh. This PC/Macintosh will need to have network enabled. In other words, it needs a network card pre-installed.

Refer to the figure below.



1. Connect the PC/Macintosh to the Access Easy Master with a RJ45 cross cable.
2. Set the IP address of the PC/Macintosh to 129.2.0.40 and subnet mask as 255.255.0.0.

18.1 For PC Users

18.1.1 Changing the PC's IP Address

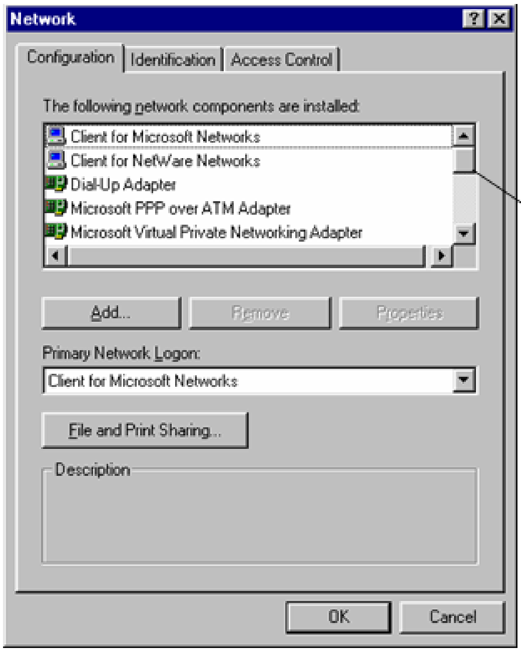
Setting the IP address of the PC is rather simple. However, if you have doubt, do ask your Network Administrator to assist you.

The purpose of changing the IP address of the PC is to allow it to access the Access Easy Master which has a default IP address of 129.2.0.42 (factory setting). If you do not change the IP address of the PC, you will not able to access the Access Easy Master at all. Hence it is important to have your PC pre-configured with the correct IP address before you proceed any further.

We will guide you in the following steps to configure a typical PC's IP address to 129.2.0.40. The following series of screen captures is taken with reference from Win 98. Reader should refer to their Network Administrator if their OS is not Win 98.

1. Click on the Start button, followed by **Settings > Control Panel**.

2. Double-click on the Network icon, the **Network** dialog box appears.



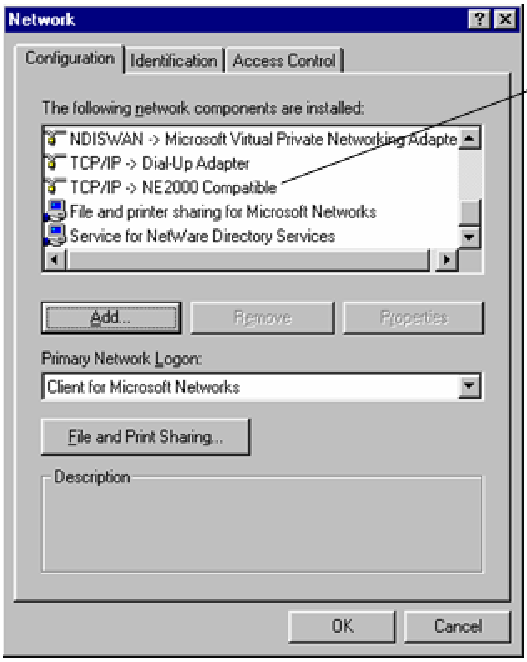
The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- Dial-Up Adapter
- Microsoft PPP over ATM Adapter
- Microsoft Virtual Private Networking Adapter

Primary Network Logon: Client for Microsoft Networks

Use this scroll bar to view the installed network components.

3. Look for the **TCP/IP** item from the list box as shown in the following diagram. However if this component is not found, proceed from step 4 to step 7 to install it, else jump to step 8.



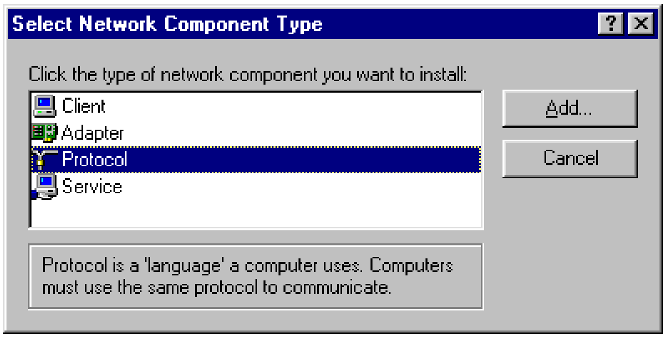
The following network components are installed:

- NDISWAN -> Microsoft Virtual Private Networking Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> NE2000 Compatible
- File and printer sharing for Microsoft Networks
- Service for NetWare Directory Services

Primary Network Logon: Client for Microsoft Networks

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.

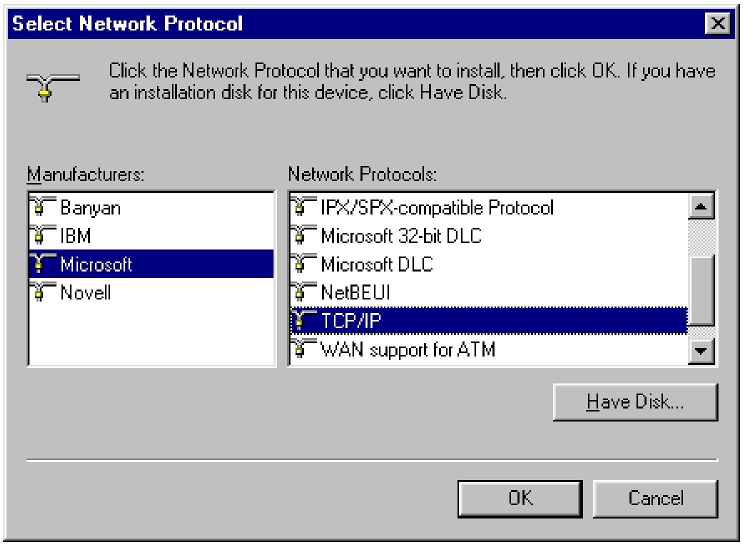


Click the type of network component you want to install:

- Client
- Adapter
- Protocol
- Service

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

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 in the following screenshot.



Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:

- Banyan
- IBM
- Microsoft
- Novell

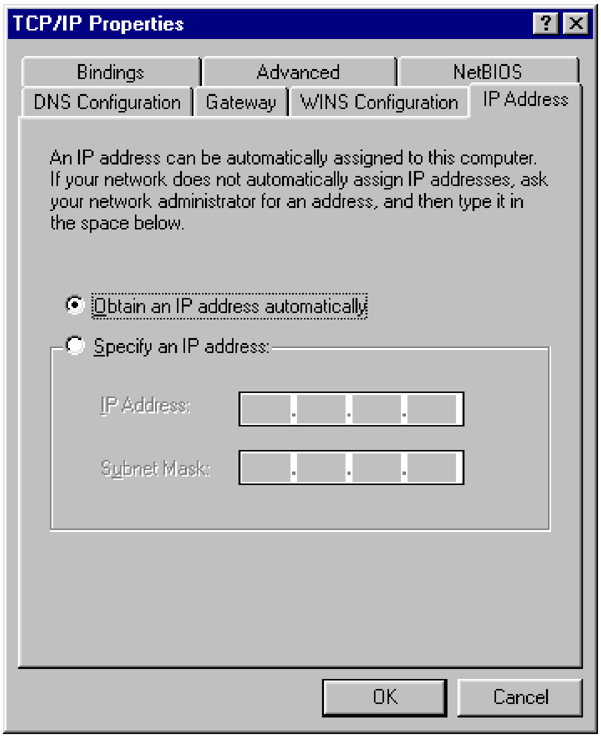
Network Protocols:

- IPX/SPX-compatible Protocol
- Microsoft 32-bit DLC
- Microsoft DLC
- NetBEUI
- TCP/IP
- WAN support for ATM

7. Click on the **OK** button to proceed with the component installation. Follow through the on-screen instruction to complete.

Notice!
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.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

9. Click on the **Specify an IP address** radio button. This will enable the **IP Address** and **Subnet Mask** fields.
10. Enter the **IP Address** and **Subnet Mask**. This will be the PC's IP Address for this initial set-up.
11. Click the **OK** button.
12. Reboot the computer in order for the setting to take effect.

Notice!
The example described above is based on Windows 98 and IE5. 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.

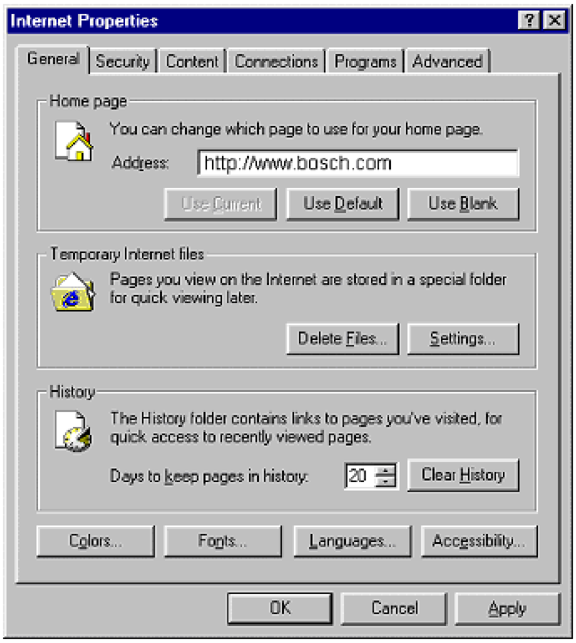
18.1.2 Settings to be Made to the Web Browser

Now that you have successfully changed the PC's IP address, you will need to configure some settings on the Web browser that you intended to use to view the pages on the Access Easy Master.

Access Easy Master supports most of the popular Web browsers, such as IE5.5, Netscape4, etc. Depending on the Web browser that your PC is installed with, the following procedures will different, but the settings required are common to most Web browsers. Ask your Network Administrator for advice if you are unsure of where to configure these settings.

The following procedure is using IE5.5 as an example.

1. From the Windows **Control Panel**, click on the Internet Options icon. The **Internet Options** dialog box appears.



Home page

You can change which page to use for your home page.

Address: http://www.bosch.com

Temporary Internet files

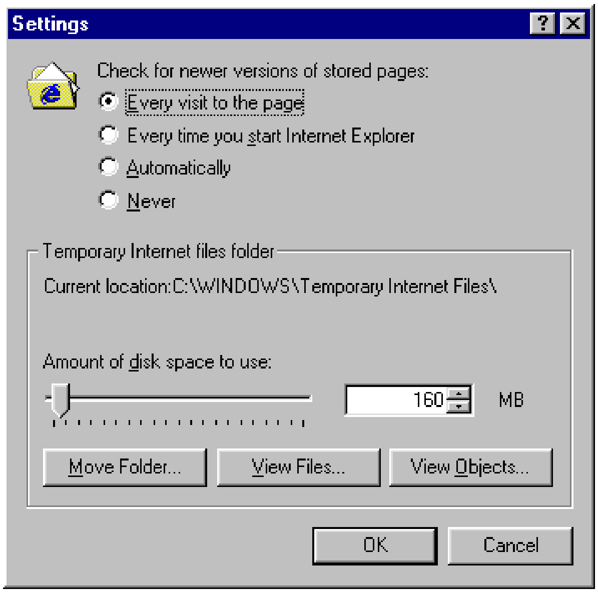
Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

2. Under the **Temporary Internet files** section, 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** option, 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.



Check for newer versions of stored pages:

● Every visit to the page

○ Every time you start Internet Explorer

○ Automatically

○ Never

Temporary Internet files folder

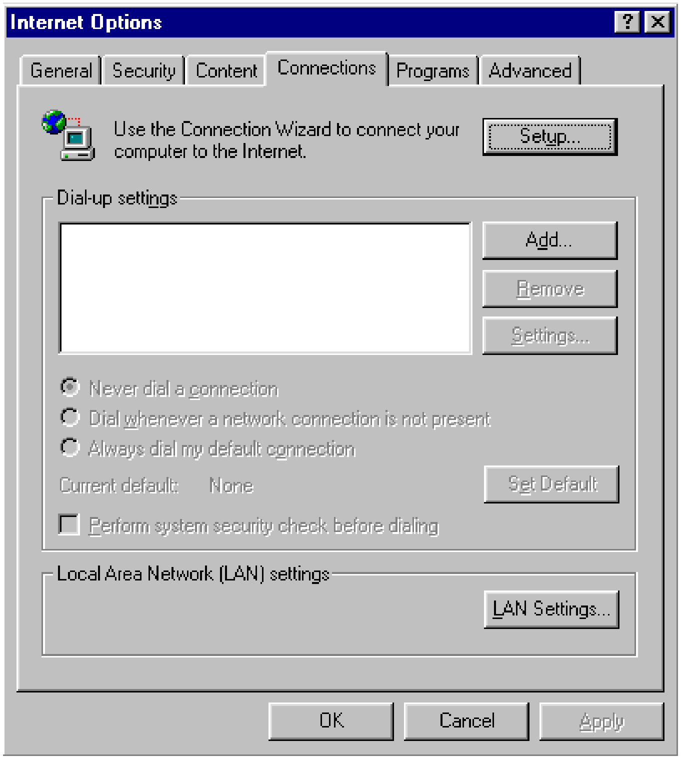
Current location:C:\WINDOWS\Temporary Internet Files\

Amount of disk space to use:

160 MB

3. Click on the **OK** button to exit to previous dialog box.

4. If your office network does not have a proxy server for accessing Internet, you could skip the following steps, else please read on.



Internet Options

General | Security | Content | Connections | Programs | Advanced

Use the Connection Wizard to connect your computer to the Internet. [Setup...]

Dial-up settings

[Add...] [Remove] [Settings...]

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current default: None [Set Default]

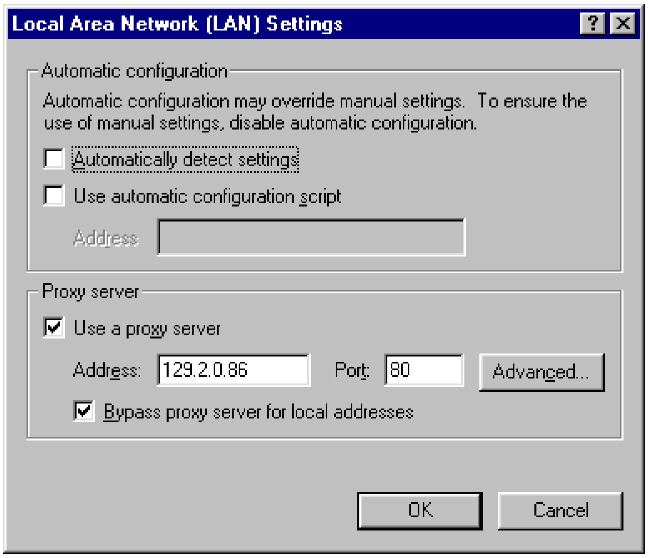
□ Perform system security check before dialing

Local Area Network (LAN) settings

[LAN Settings...]

[OK] [Cancel] [Apply]

5. Under the **Connections** tab, click on the **LAN Settings** button The **LAN Settings** dialog box appears. Check the **Bypass proxy server for local addresses** checkbox if the Access Easy Master exists on the LAN.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

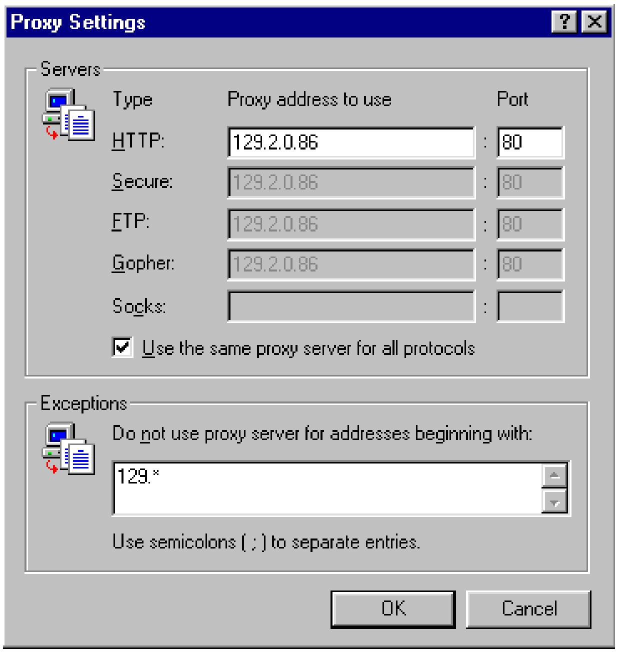
☑ Use a proxy server

Address: 129.2.0.86 Port: 80 [Advanced...]

☑ Bypass proxy server for local addresses

[OK] [Cancel]

6. Click on the **Advanced** button. The **Proxy Settings** dialog box appears.



HTTP: 129.2.0.86 : 80
Secure: 129.2.0.86 : 80
FTP: 129.2.0.86 : 80
Gopher: 129.2.0.86 : 80
Socks: :

☑ Use the same proxy server for all protocols

Do not use proxy server for addresses beginning with:
129.*
Use semicolons (;) to separate entries.

7. As shown in the above, the proxy address used is 129.2.0.86, this is IP address of the proxy server in this example, it will differ in your own office. Port setting is also dependent on your office network setup. However, if the PC you are configuring has always been able to access the Internet before, you will need only to enter the IP address of your Access Easy Master. Including a “*” like the above means to bypass the proxy server for all IP addresses starting with the 129 address.
8. Since the default IP addresses for the Access Easy Master and the Access Easy Controllers are 129.x.x.x, you may directly access the Access Easy Master and the Access Easy Controllers without going through a proxy server. Now that the browser and IP addresses have been configured, we will now be able to view the Access Easy Master and the Access Easy Controllers through our web browser.

To change the IP address of the Access Easy Master, follow the steps in *Changing the IP Address of Access Easy Master, page 186*.

18.2 For Macintosh Users

18.2.1 Changing the Macintosh's IP Address

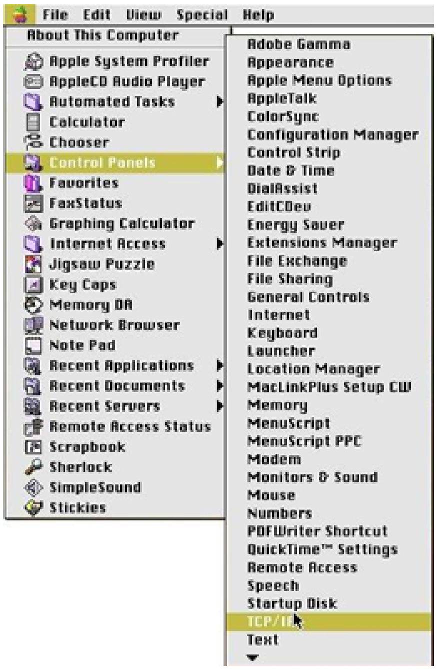
Setting the IP address of the Macintosh is rather simple. However, if you have doubt, do ask your network administrator to assist you.

The purpose of changing the IP address of the Macintosh is to allow it to access the Access Easy Master which has a default IP address of 129.2.0.42 (factory setting). If you do not change the IP address of the Macintosh, you will not able to access the Access Easy Master at all. Hence it is important to have your Macintosh pre-configured with the correct IP address before you proceed any further.

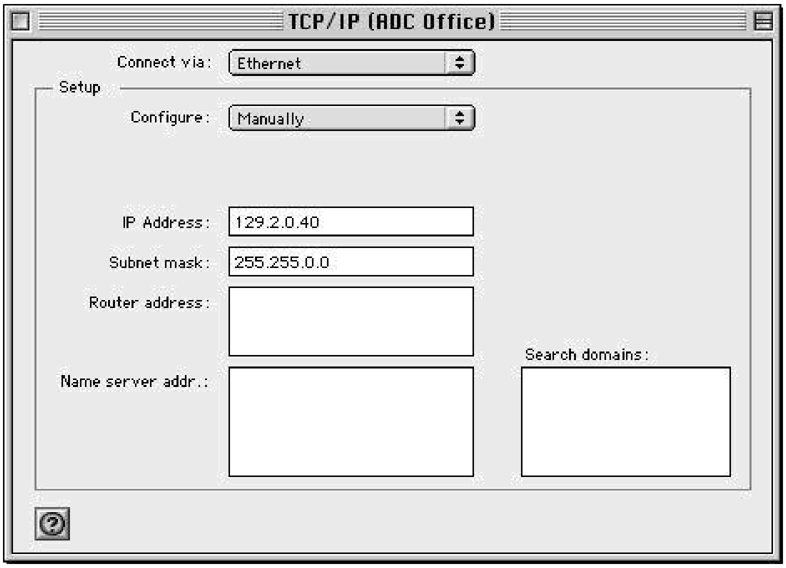
We will guide you in the following steps to configure a typical Macintosh's IP address to 129.2.0.40.

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.



3. Enter the **IP Address** and the **Subnet mask** as shown below. This will be the Macintosh's IP Address for this initial set-up.



TCP/IP (ADC Office)

Connect via: Ethernet

Setup

Configure: Manually

IP Address: 129.2.0.40

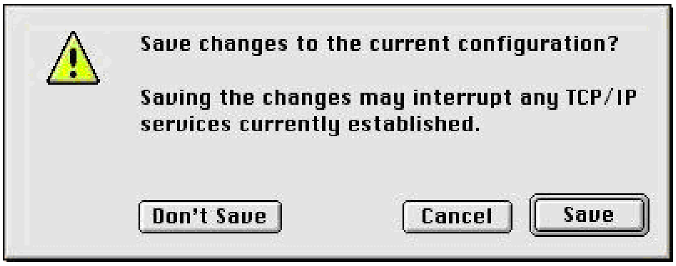
Subnet mask: 255.255.0.0

Router address:

Name server addr.:

Search domains:

4. Click on the **Save** button when prompted. This message will appear when you attempt to close the dialog box.

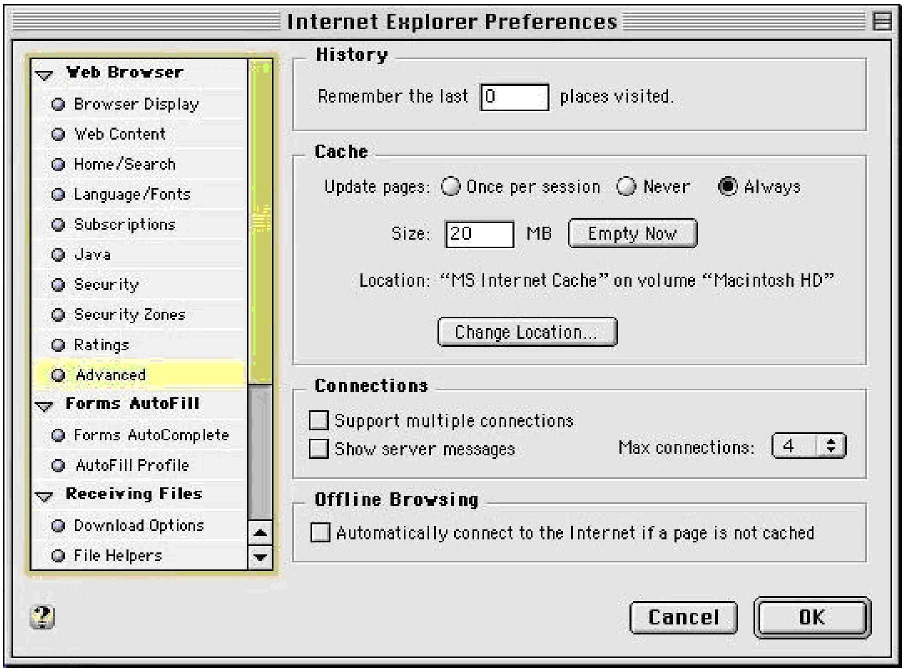


Save changes to the current configuration?

Saving the changes may interrupt any TCP/IP services currently established.

18.2.2 Settings to be Made to the Web Browser

1. Launch the Internet Explorer for Macintosh.
2. From the **Toolbars**, click on **Preferences**.
3. Under **Web Browser**, select **Advanced** (see diagram below).
4. From the **Cache** section, select **Always** option for **Update pages** radio button.



Internet Explorer Preferences

History

Remember the last 0 places visited.

Cache

Update pages: ○ Once per session ○ Never ● Always

Size: 20 MB

Location: “MS Internet Cache” on volume “Macintosh HD”

Connections

□ Support multiple connections

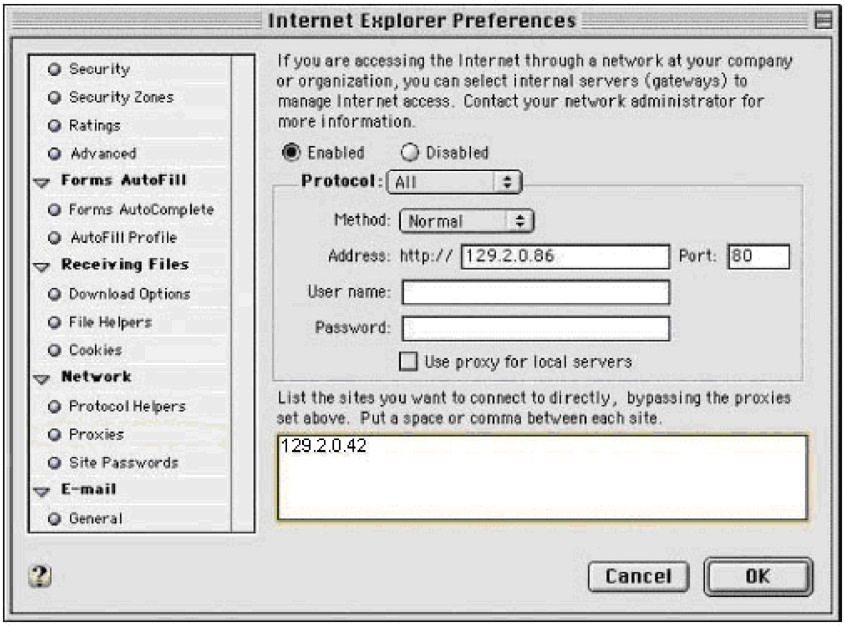
□ Show server messages

Max connections: 4

Offline Browsing

□ Automatically connect to the Internet if a page is not cached

5. Scroll down the listing to look for **Proxies**.



Internet Explorer Preferences

If you are accessing the Internet through a network at your company or organization, you can select internal servers (gateways) to manage Internet access. Contact your network administrator for more information.

● Enabled ○ Disabled

Protocol: All

Method: Normal

Address: http:// 129.2.0.86 Port: 80

User name:

Password:

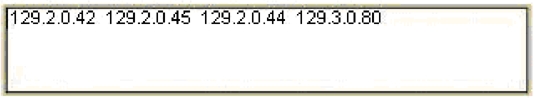
□ Use proxy for local servers

List the sites you want to connect to directly, bypassing the proxies set above. Put a space or comma between each site.

129.2.0.42

6. Enter the Access Easy Master default IP address into the box as shown above. IP addresses enter here will bypass the proxies and connect directly.

7. If the IP addresses of the Access Easy Controllers have been assigned, continue to enter the addresses in the field, separating each address by a space or a comma. The screen-capture shows the default IP address for Access Easy Master and three assigned Access Easy Controllers IP addresses, 129.2.0.45, 129.2.0.44, and 129.3.0.80.



129.2.0.42 129.2.0.45 129.2.0.44 129.3.0.80

8. Click on the **OK** button to close the dialog box. With this settings done, we can proceed to access the Access Easy Master.

To change the IP address of the Access Easy Master, follow the steps in *Changing the IP Address of Access Easy Master, page 186*.

18.3 Changing the IP Address of Access Easy Master

To get connected to Access Easy Master, use the web browser to login to Access Easy Master. Please refer to *Logging Into Access Easy Master, page 14* for details.

After getting connected to Access Easy Master, you can change the IP address of the Access Easy Master from default, to the actual IP you intend to use for the server. The **View Activity** page will be the first screen that the user sees after a successful login.

To change the IP address of your Access Easy Master, refer to *Network Settings, page 83*. Configure the network settings for Access Easy Master by setting the appropriate IP address, subnet mask and gateway. Click on the 💾 icon at the bottom of the web page to save the new setting.

Notice!
Access Easy Master needs to be rebooted before the new IP address setting takes effect.

19 Accessing and Understanding Access Easy for Master

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

Access Easy for Master software graphical user interface (GUI) is the same as Access Easy Controller software GUI but Access Easy for Master software only support minimal functions as most of the functions are centrally administered and controlled by Access Easy Master software.

In order to operate one or more controllers from one or more computers, a standard web browser program such as Internet Explorer on each of the central monitoring computer is required.

19.1 Connecting to Access Easy for Master

Before Access Easy for Master can be accessed, it must be configured properly and integrated in the existing computer network.

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

However, for general knowledge, a description is presented in *APPENDIX F Initial Setup To Access Easy Controller, page 249*.

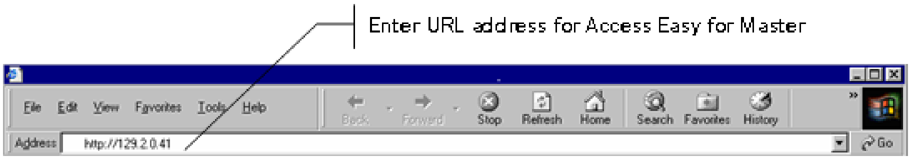
For users using their own computer, please read up on the section *Settings to be Made to the Web Browser, page 254*.

19.2 Logging into Access Easy for Master

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

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

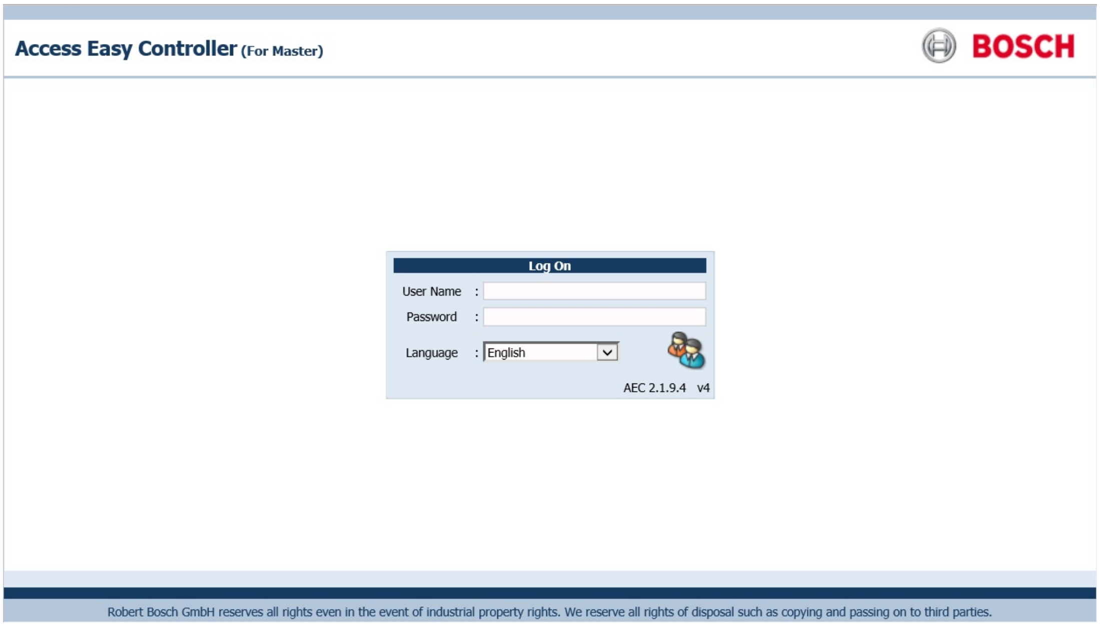
The following screen capture shows an example of a typical web browser page with the default URL address for the Access Easy for Master. The outlook of the screen might differ from what is shown here, depending on the version in use.



Enter URL address for Access Easy for Master

Address: http://129.2.0.41

After entering the URL address for Access Easy for Master, the **Log On** screen appears.



Access Easy Controller (For Master)

User Name :

Password :

Language : English

AEC 2.1.9.4 v4

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.

This **Log On** screen provides a security control that protects the Access Easy for Master from unauthorized access. It requires a user to enter his or her user ID followed by a password before he or she can access the Access Easy for Master.

The Access Easy for Master has only two assigned user IDs and passwords. Up to two users are able to log into the same Access Easy for Master concurrently using different computers.

Notice!
The user ID and password are case-sensitive and can be changed.

The default user IDs have restricted access rights to the features of Access Easy for Master. For the first user, the default user ID is “user1” and the default password is “8088”. For the second user, the default user ID is “user2” and the default password is “8088”.

Notice!
Once the system is commissioned and handed-over, change the default user ID and password as soon as possible to prevent unauthorized access.

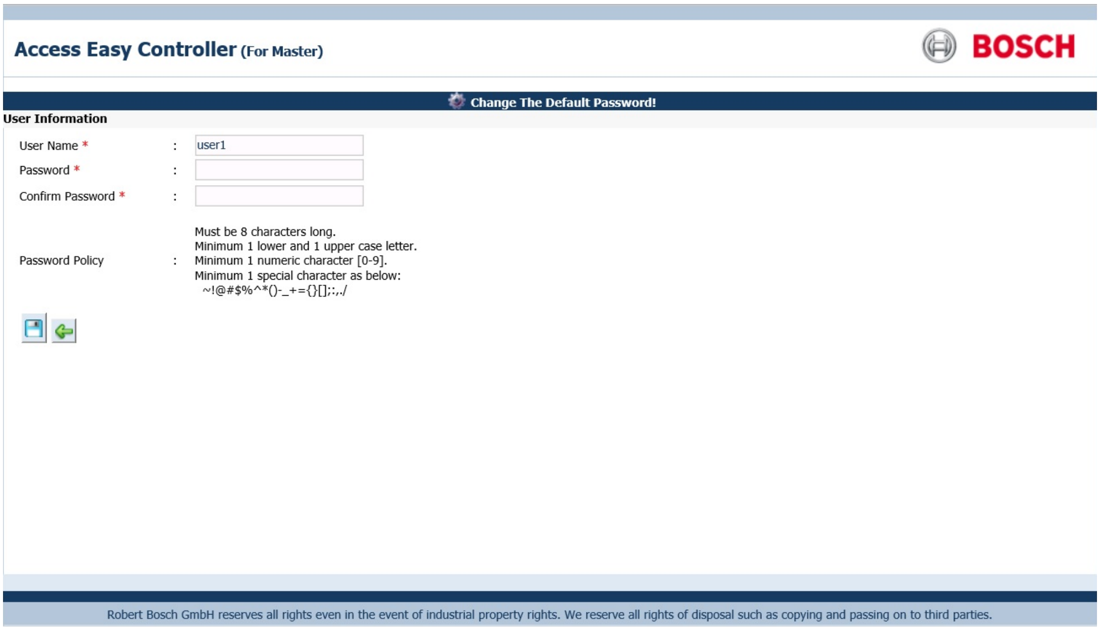
19.2.1 Logging in to Access Easy for Master

1. Enter your assigned user ID in the **User Name** field.
2. Enter your assigned password in the **Password** field.
3. Select the required GUI language from the **Language** drop-down list.
4. 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 configured by the Access Easy for Master System Administrator.

Logging in using the default password

If you are logging in using the default user ID and default password, you will be redirected to **Change The Default Password** page to change the user ID and/or password immediately.



Access Easy Controller (For Master)

Change The Default Password!

User Information

User Name *	:	user1
Password *	:	
Confirm Password *	:	
Password Policy	:	Must be 8 characters long. Minimum 1 lower and 1 upper case letter. Minimum 1 numeric character [0-9]. Minimum 1 special character as below: ~!@#$%^*()-_+={}[];:,./

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.

1. Enter your new user ID in the **User Name** field if you wish to change the user ID. Otherwise, ignore the field.
2. Enter your new password in the **Password** field.
3. Re-enter your new password in the **Confirm Password** field.

Caution!

The user ID and password are case-sensitive. For security reasons, every character entered in the password field is represented by a dot.

The passwords must meet the following requirements:

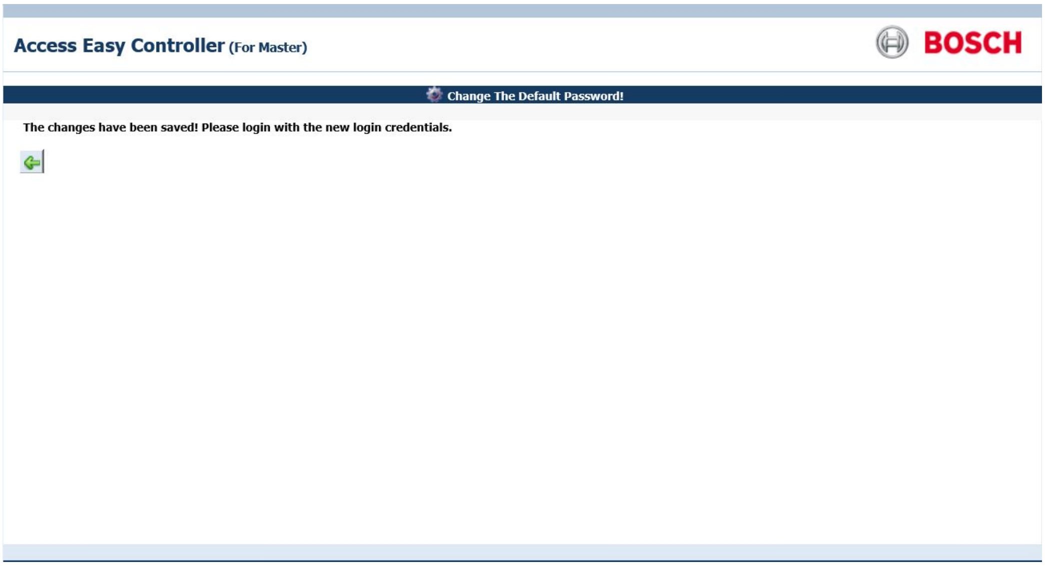
must be 8 characters long

must consist of at least

- 1 lowercase letter,
- 1 uppercase letter,
- 1 number, and
- 1 special character from ~`!@#$%^*()-_+={}[];:,./

4. Click the back ⇦ button to return to the **Log On** page without changing the user ID and password. You will not have access to Access Easy for Master until you have changed the default password.

5. Otherwise, click the save button to save the changes. If the passwords in the **Password** and **Confirm Password** fields match and meet the password policy requirements, a change confirmation page appears.



Access Easy Controller (For Master)
BOSCH
Change The Default Password!

The changes have been saved! Please login with the new login credentials.

6. Click the back button to return to the **Log On** page.
7. Log in using the new credentials. You will now have access to Access Easy for Master.

19.2.2 Progressive delays between login attempts

The system utilizes progressive delays between login attempts for better security and protection from unauthorized access. Progressive longer delays are enforced between subsequent logins after a number of unsuccessful login attempts. The section below describes the progressive delay operation.

After the third unsuccessful login, a 20 seconds' delay kicks in before the user can attempt the fourth login. This delay duration appears within the log on screen and starts counting down. The user may attempt to login during this duration but the system will ignore these login attempts. After the countdown has completed, the user can then attempt to login again. Note that each subsequent unsuccessful login will trigger a delay duration that is twice longer than the previous delay.

Clearing the progressive delays

Clear the progressive delay by performing one of the following:

- Log in successfully with the correct credentials.
- Restart the AEMC.
- Administrator changing the password or username of the user who failed the login attempts.

19.2.3 Logging off from Access Easy for Master

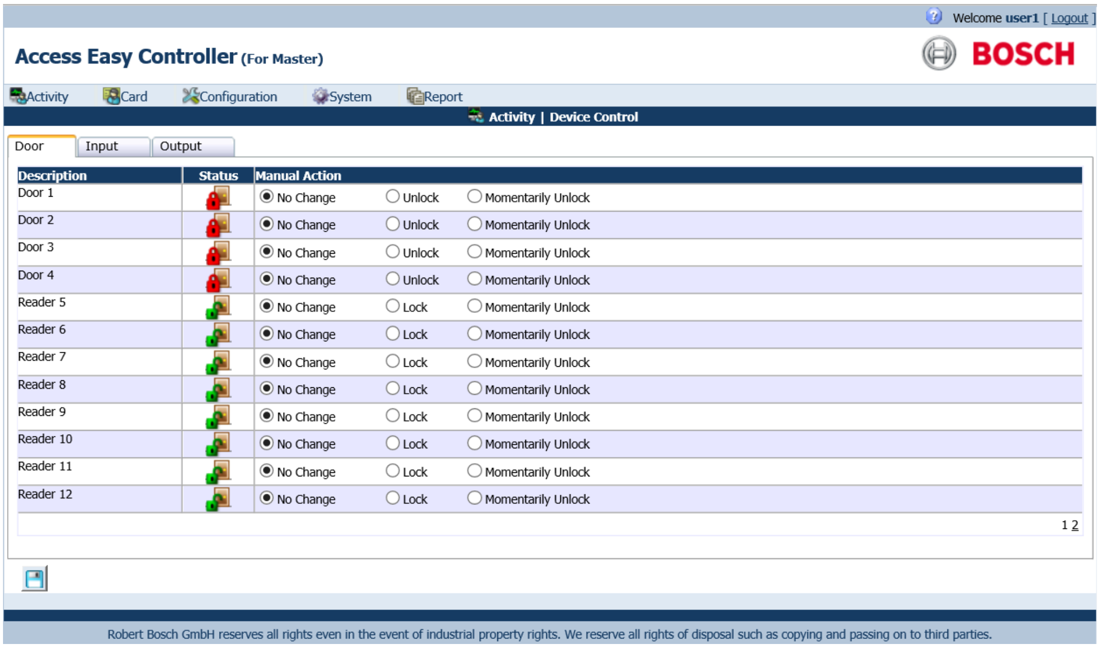
After you have finished your session with Access Easy for Master, or need to be away from the computer, it is recommended to log off from the Access Easy for Master.

To log off, click on the **Logout** link at the top right corner of Access Easy for Master screen.

19.3 Understanding the Access Easy for Master Main Menu

The default or home page of the Access Easy for Master is the **Device Control** page. When you log in to Access Easy for Master, this will be the first page that you see.

The screen capture below shows the home page.



Description	Status	Manual Action		
Door 1	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Door 2	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Door 3	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Door 4	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Reader 5	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 6	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 7	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 8	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 9	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 10	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 11	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 12	🔓	● No Change	○ Lock	○ Momentarily Unlock

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.

Only minimal features are available on Access Easy for Master. Features that are not available are disabled from the menu. The various features that are available on Access Easy for Master will be covered in the following chapters. Brief descriptions of each item will be presented here.

Notice!
Most of the features are incorporated into Access Easy Master. This allows Access Easy Master to centrally control and administer all changes of the Access Easy Controller.

19.3.1 Activity

The **Activity** menu relates to the transactions generated by the system and the video features. This feature is only available for the “user2” user ID. Features that are available relate to the manual control of door, input and output devices.

19.3.2 Card

The **Card** menu relates to the card parameter set up and administration, including arming and disarming of alarm zones and assigning access groups. However, these features are not available for Access Easy for Master. From this menu, you can only perform the reset of anti-passback (APB) violations.

19.3.3 System

User IDs and passwords including access rights to the various menu items are set in the **System** menu. You can set up the panel for the following configurations:

- Network Settings
- Date & Time
- Advance Settings
- Default Settings
- System Log

19.3.4 Report

The **Report** menu relates to the various reports that you can generate, including reports for activities, cards and others. However, in the Access Easy for Master, you can generate reports for the **Audit Log** only.

19.3.5 Logout

To log off from Access Easy for Master.

20 Operating the Access Easy for Master

The following chapters describe usage of the accessible features of Access Easy for Master in detail.

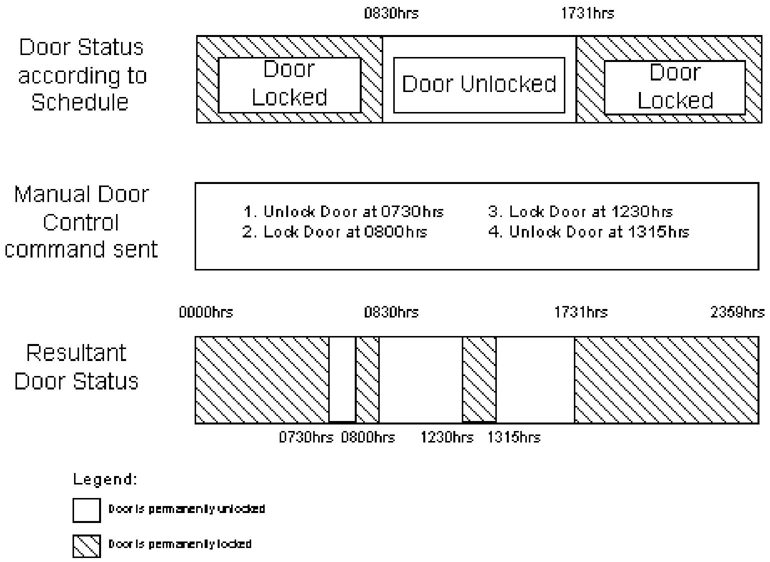
20.1 Device Control

The **Device Control** submenu refers to the manual door settings of the system. The **Device Control** page consists of three tabs namely, the **Door**, **Input** and **Output** controls. These three tabs are explained in detail in the following pages.

20.1.1 Door Control

The **Door** control option allows you to check the status of the doors and momentarily unlock or lock the door without having to be present at the door location. This is a manually operated control and has priority over the system control. However, the system will resume normal operation once it encounters a valid schedule interval.

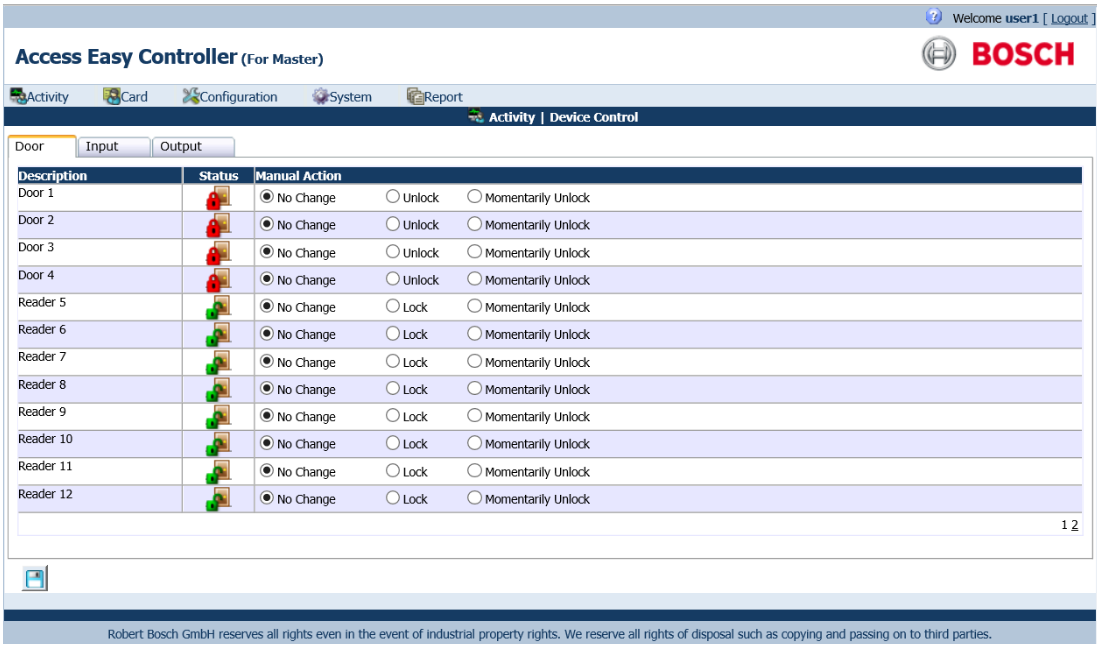
Here is an example to illustrate the condition.
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2, 3, and 4 has no setting.



Notice that the system resumes normal operation according to schedule at 0830hrs and 1731hrs.

To activate Door control

Click **Activity > Device Control** menu. In the **Device Control** main page, select the **Door** tab to manually control the settings for doors. The screen below shows the **Door control** page.



Welcome **user1** [Logout]

Access Easy Controller (For Master) BOSCH

Description	Status	Manual Action		
Door 1	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Door 2	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Door 3	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Door 4	🔒	● No Change	○ Unlock	○ Momentarily Unlock
Reader 5	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 6	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 7	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 8	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 9	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 10	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 11	🔓	● No Change	○ Lock	○ Momentarily Unlock
Reader 12	🔓	● No Change	○ Lock	○ Momentarily Unlock

1 2

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.

The **Door** control page consists of three main columns, namely **Description**, **Status** and **Manual Action**. The **Description** column provides the door description. The **Status** column refers to the current status of the door. Point your mouse on the icon in the **Status** column to display the tool tip or to find out about the icon representation.

The **Manual Action** column provides radio buttons to select the manual action to be performed. The first radio button option is to retain the door action, therefore by default, “No Change” option is selected. The second radio button option is the opposite of the current status, toggling between “Lock” and “Unlock” status. The third radio button option, “Momentary Unlock”, is used to send a command to momentarily unlock the door for the duration as specified in the **Door Strike Timer**. This command is only effective when the current status of the door is locked.

Notice!
Only readers configured as entry readers will be shown in the **Door** control page.

To control the Doors manually

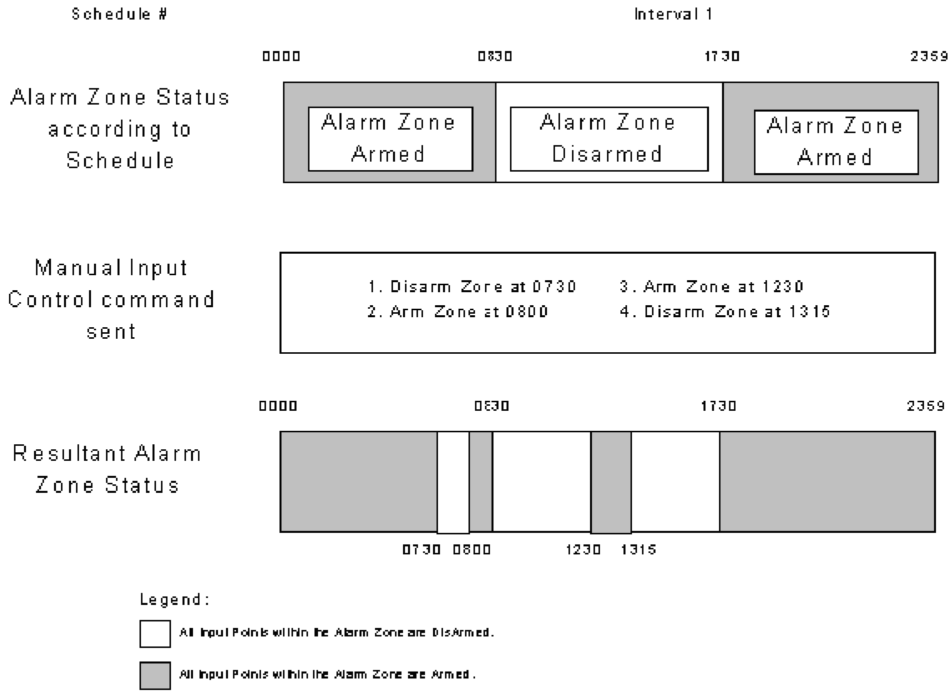
1. Select the desired option from the **Manual Action** radio buttons.
2. Click the save 💾 button to send the command. The page then refreshes and reflects the new status.

Notice!
Select only door(s) that you want to send command to. The current status of the door for a momentarily unlock command will not be shown.

20.1.2 Input Control

The **Input** control page allows you to check the status of all the input points and send a command to arm or disarm the device manually. This is a manually operated control and has priority over the system set control. However, the system will resume normal operation once it encounters a valid schedule interval.

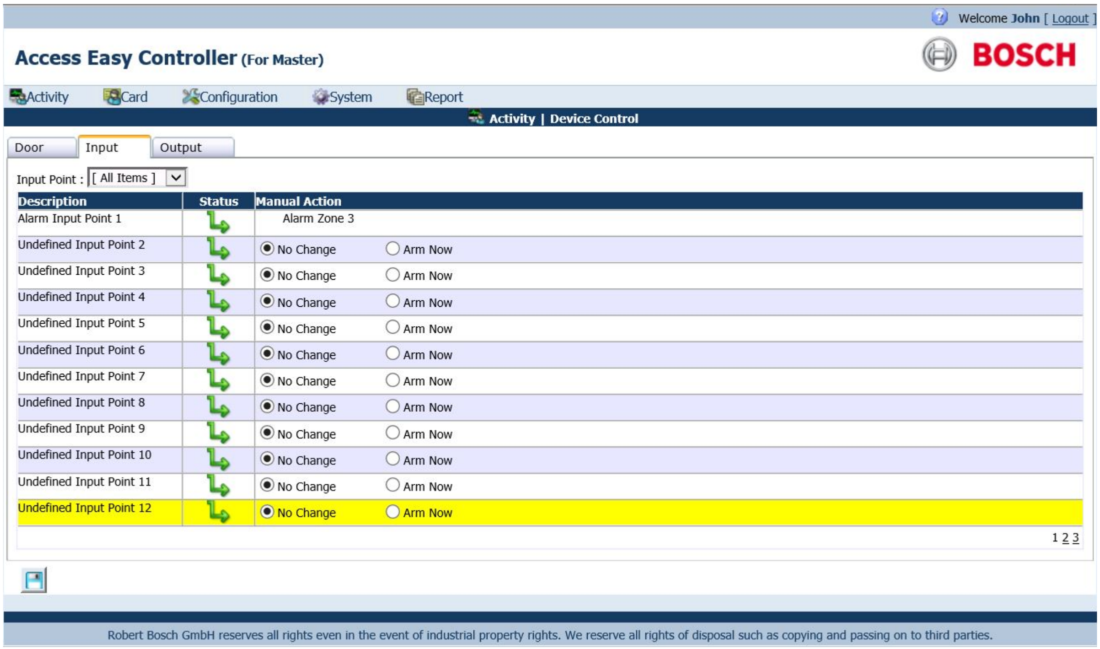
Before we begin, here is an example to illustrate the operational behavior.
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2, 3 and 4 has no setting.



Notice that the system resumes normal operation according to schedule at 0830hrs and 1731hrs.

To activate Input control

Click **Activity > Device Control** menu. In the **Device Control** main page, select the **Input** tab to manually control the settings of input points. The screen below shows the **Input** control page.



Input Point : [All Items]

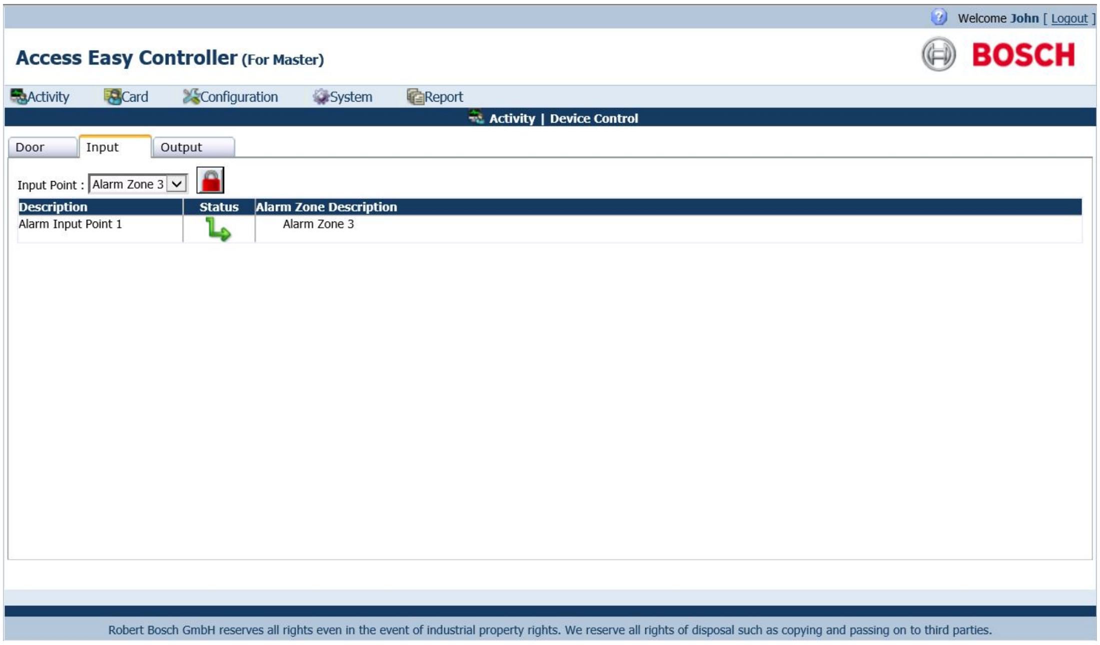
Description	Status	Manual Action	
Alarm Input Point 1	↳	Alarm Zone 3	
Undefined Input Point 2	↳	● No Change	○ Arm Now
Undefined Input Point 3	↳	● No Change	○ Arm Now
Undefined Input Point 4	↳	● No Change	○ Arm Now
Undefined Input Point 5	↳	● No Change	○ Arm Now
Undefined Input Point 6	↳	● No Change	○ Arm Now
Undefined Input Point 7	↳	● No Change	○ Arm Now
Undefined Input Point 8	↳	● No Change	○ Arm Now
Undefined Input Point 9	↳	● No Change	○ Arm Now
Undefined Input Point 10	↳	● No Change	○ Arm Now
Undefined Input Point 11	↳	● No Change	○ Arm Now
Undefined Input Point 12	↳	● No Change	○ Arm Now

1 2 3

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.

The **Input** control page consists of three main columns, namely **Description**, **Status** and **Manual Action**. The **Description** column provides the input point description. The **Status** column refers to the current status of the input point. Point your mouse on the icon in the **Status** column to display the tool tip or to find out about the icon representation.

Each row provides information of which alarm zone that the input point belongs to. In the screen above, “**Alarm Input Point 1”** belongs to “Alarm Zone 3**”** and “Undefined Input Point 2**”** is an independent input point. Select a zone from the **Input Point** drop-down list to arm or disarm the input points of that alarm zone. The screen below shows an example of an input point set in an alarm zone.



Input Point : Alarm Zone 3

Description	Status	Alarm Zone Description
Alarm Input Point 1	↳	Alarm Zone 3

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.

Click the arm 🔒 or disarm 🔓 button beside the **Input Point** drop-down list to arm or disarm the input points that belong to the selected alarm zone.

The **Manual Action** column provides radio buttons to select the manual action to be performed. The first radio button option is used to retain the door alarm zone, therefore by default, “No Change” option is selected. The second radio button option is the opposite of the current status, and toggles between **“**Disarm Now” and “Arm Now” options.

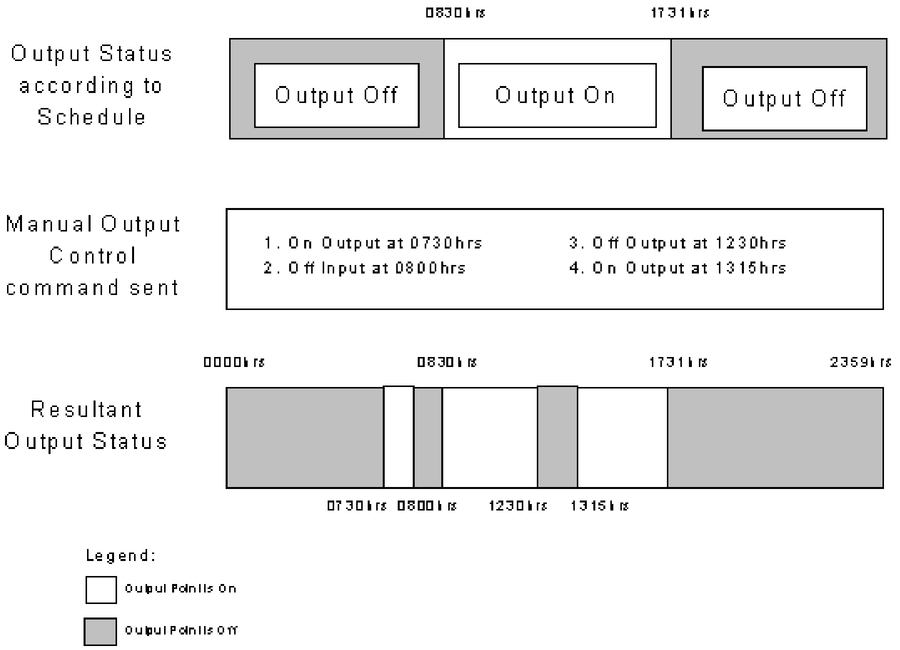
To control the Input points

1. Select the desired option from the **Manual Action** radio buttons.
2. Click the save 💾 button to arm or disarm the input point. The page will refresh to reflect the new status.

20.1.3 Output Control

The **Output** control page allows you to check the status of all the output points and send a command to turn the output points on or off manually. This is a manually operated control and has priority over the system set control. However, the system will resume normal operation once it encounters a valid schedule interval.

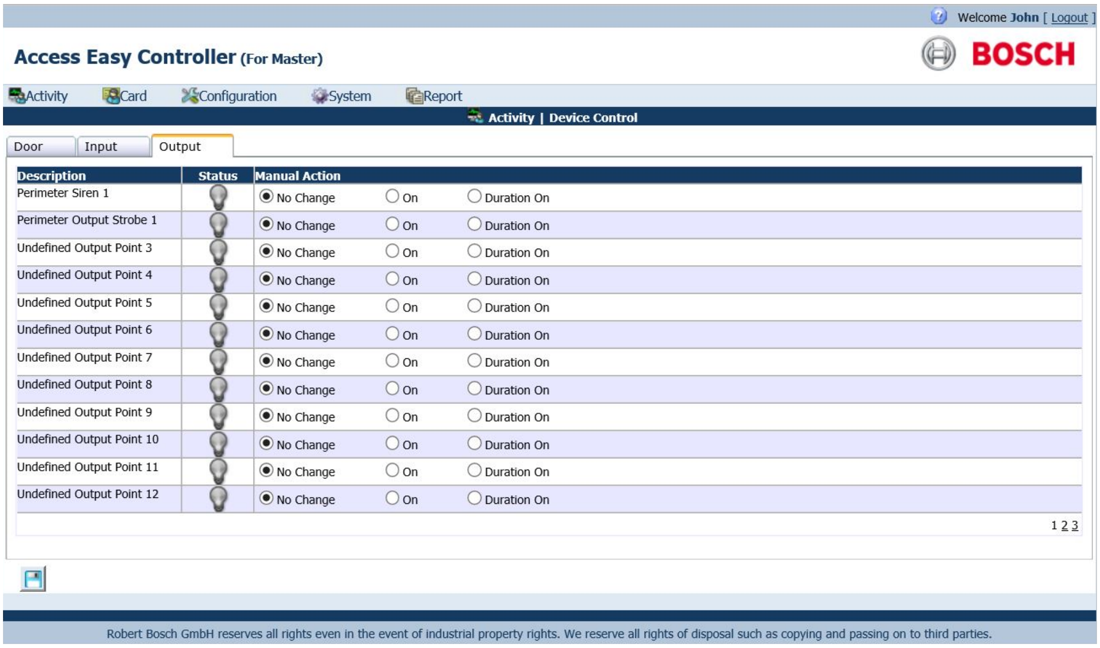
Before we begin, here is an example to illustrate the operational condition
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2, 3 and 4 has no setting.



Notice that the system resumes normal operation according to schedule at 0830hrs and 1731hrs.

To activate Output control

Click **Activity > Device Control** menu. In the **Device Control** page, click the **Output** tab to control the output settings manually. The screen below shows the **Output** control page.



Description	Status	Manual Action		
Perimeter Siren 1	💡	● No Change	○ On	○ Duration On
Perimeter Output Strobe 1	💡	● No Change	○ On	○ Duration On
Undefined Output Point 3	💡	● No Change	○ On	○ Duration On
Undefined Output Point 4	💡	● No Change	○ On	○ Duration On
Undefined Output Point 5	💡	● No Change	○ On	○ Duration On
Undefined Output Point 6	💡	● No Change	○ On	○ Duration On
Undefined Output Point 7	💡	● No Change	○ On	○ Duration On
Undefined Output Point 8	💡	● No Change	○ On	○ Duration On
Undefined Output Point 9	💡	● No Change	○ On	○ Duration On
Undefined Output Point 10	💡	● No Change	○ On	○ Duration On
Undefined Output Point 11	💡	● No Change	○ On	○ Duration On
Undefined Output Point 12	💡	● No Change	○ On	○ Duration On

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.

The **Output** control page consists of three main columns, namely **Description**, **Status** and **Manual Action**. The **Description** column provides the output description. The **Status** column refers to the current status of the output point. If the **Manual Action** radio button shows the “On” option, the **Status** column indicates that the output point is turned off (normal bulb icon). Likewise, if the **Manual Action** radio button shows the “Off” option, the **Status** column indicates that the output point is turned on (glowing bulb icon).

The **Manual Action** column provides radio button options to select the manual action that can be performed on the device. The second radio button is the opposite of the state in the **Status** column, and toggles between turning the device “On” and “Off”. The third radio button option, “Duration On” or “Duration Off” also reflects the opposite of the current status, and is used to send the command to turn the output point on or off for the duration as configured in the **Duration** field of **Output Setup** menu item.

To control the Output points

1. Select the desired option from the **Manual Action** radio buttons.
2. Click the save button to save the settings. The page will refresh to reflect the new status.

Notice!
Select only output point(s) that you want to send command to. The current status of the output point for which the “Duration On” or “Duration Off” command is sent will not show the true status after the duration has elapsed. To show true status, refresh the web page by clicking the save button.

20.2 Reset APB

The **Reset APB** menu allows you to reset the anti-passback (APB) violations.

Notice!
This feature is applicable to full and soft anti-passback only.

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" of violator's subsequent access or exit respectively.

You have the option to reset APB violations with the following combinations:

- By All Cards
- By Individual Card

To reset APB by All Cards

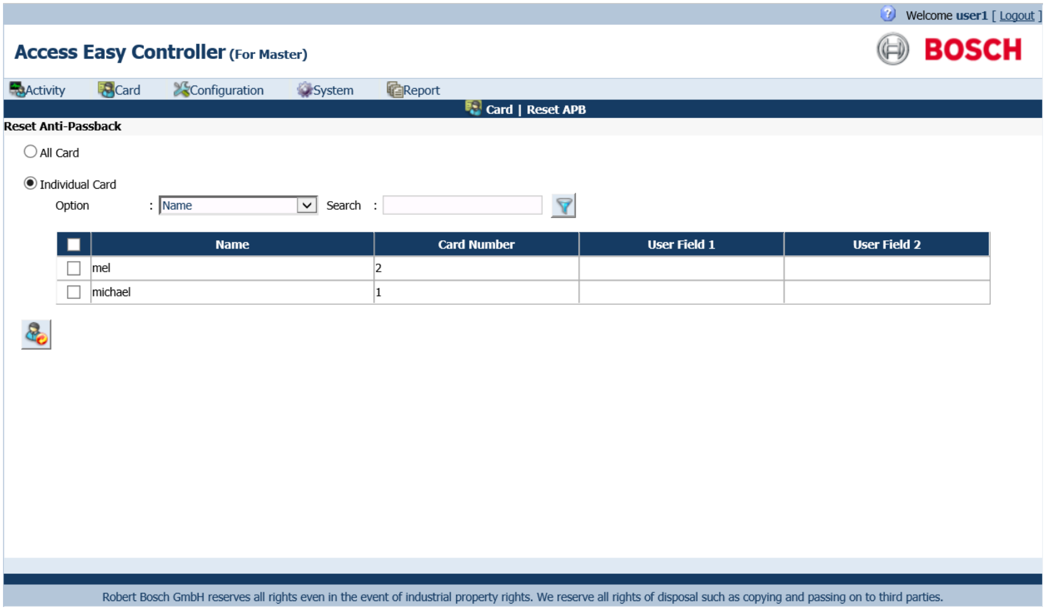
1. Select the **All Card** radio button to reset APB for all the cards in the database.
2. Click the reset APB button to proceed. If the command is executed successfully, a message indicating APB reset for card number is displayed.

To reset APB by Individual Card

You can reset APB of an individual card based on the name, card number, user fields 1 and 2. To reset APB based on card number, you should know the card number, its facility code, and its card format.

The reset APB window lists all the cardholders name and details in the main page.

1. Click the **Individual Card** radio button to reset APB for a particular card as shown below.



Reset Anti-Passback

○ All Card

● Individual Card

Option : Name Search :

☐	Name	Card Number	User Field 1	User Field 2
☐	mel	2		
☐	michael	1		

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.

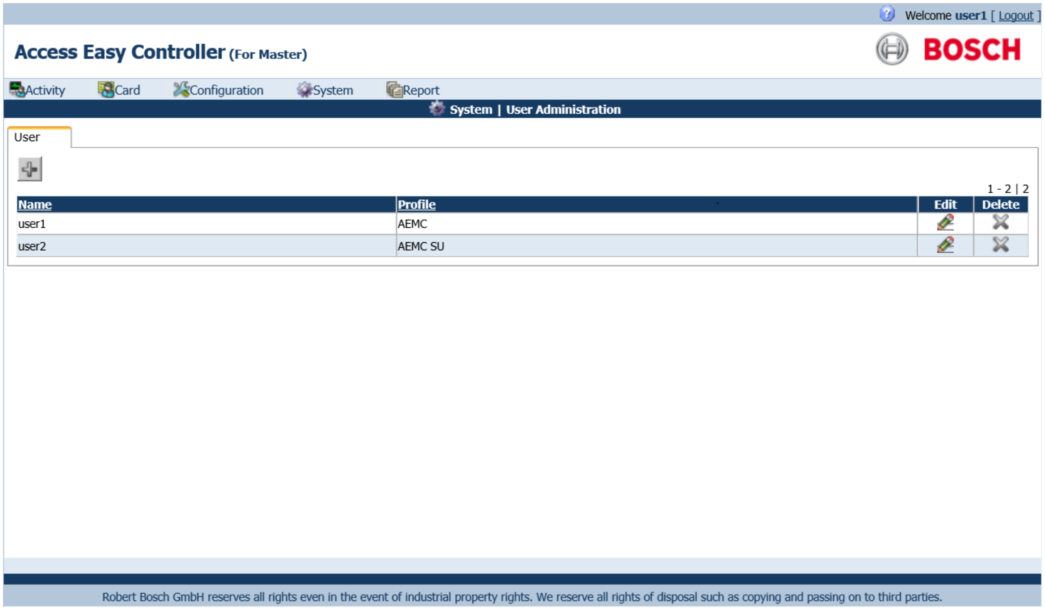
2. Select the criteria to search from the **Option** drop-down list. The options available are “Name”, “Card Number”, “User Field 1” and “User Field 2”.
3. Enter the search criteria of the APB violator in the **Search** field.
4. Results of the search criteria appear in a table.
5. Select the checkboxes beside the names from the search result.
6. Click the reset APB button to reset the APB violation.

20.3 User Administration

Only one user can be assigned access rights to carry out the functions of the Access Easy for Master. By default, “user1” and “user2” are defined as the Superuser having access to these Access Easy for Master features.

To edit user ID and password

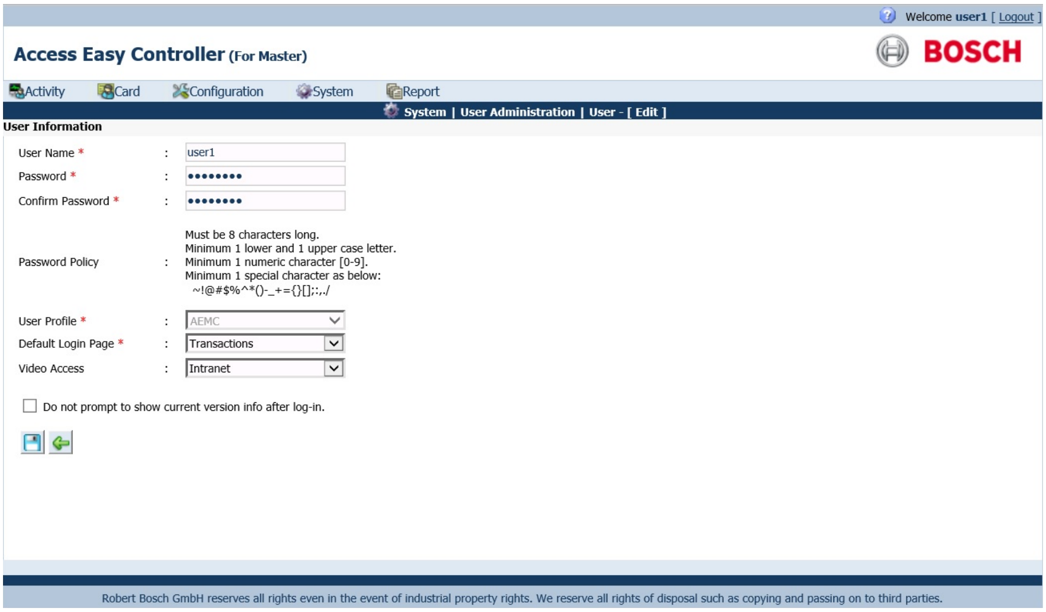
1. Click **System > User Administration** menu to access the user details page. The screen below shows the **User Administration** home page.



Name	Profile	Edit	Delete
user1	AEMC	✎	✕
user2	AEMC SU	✎	✕

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.

2. Click the button to edit the settings of the existing user.


Welcome user1 [Logout]
Access Easy Controller (For Master)
BOSCH
Activity
Card
Configuration
System
Report
System | User Administration | User - [Edit]

User Information

User Name *	:	user1
Password *	:	••••••••
Confirm Password *	:	••••••••
Password Policy	:	Must be 8 characters long. Minimum 1 lower and 1 upper case letter. Minimum 1 numeric character [0-9]. Minimum 1 special character as below: ~!@#$%^*()-_+={}[];:,./
User Profile *	:	AEMC
Default Login Page *	:	Transactions
Video Access	:	Intranet

□ Do not prompt to show current version info after log-in.

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.

3. Change the user ID in the **Username** field.
4. Change the password in the **Password** field.
5. Re-enter the password in the **Confirm Password** field. The passwords entered in the **Password** and **Confirm Password** fields must match and meet the password policy requirements. Otherwise, an error message will appear.

Caution!

The user ID and password are case-sensitive. For security reasons, every character entered in the password field is represented by a dot.

The passwords must meet the following requirements:

must be 8 characters long

must consist of at least

- 1 lowercase letter,

- 1 uppercase letter,

- 1 number, and

- 1 special character from ~` !@#$%^*()-_+={}[];:,./

6. The **User Profile** drop-down list is disabled. Changes to this field is not allowed.
7. Select the home page for the user from the **Default Login Page** drop-down list. This setting will load this page as the default page every time the user logs in.

Notice!

The **Video Access** feature is not applicable to Access Easy for Master. Selecting any value from the drop-down list has no effect.

8. Select or deselect the **Do not prompt to show current version info after log-in.** checkbox accordingly. If you want the system to check the current Access Easy for Master version and available updates each time you log into the system, do not select this option. Selecting it will disable the check for updates.

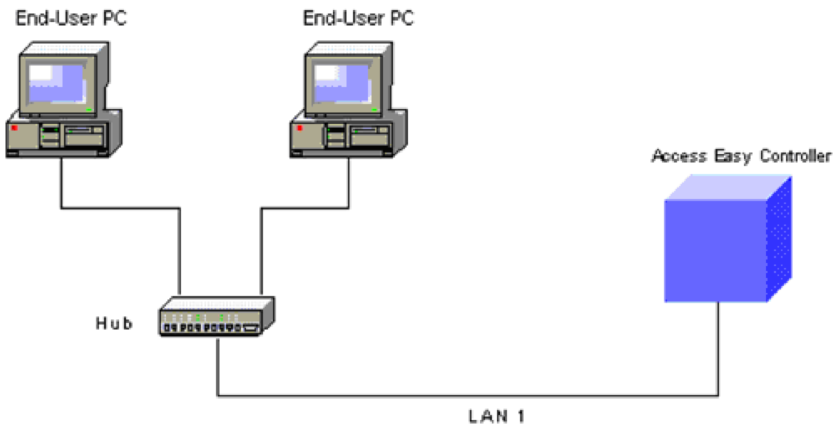
9. Click the **save** button to save the settings. Click the **back** button to cancel the settings and return to the **User Administration** main page.

20.4 Network Settings

The **Network Settings** menu allows you to configure the panel’s IP address, netmask and gateway address. In addition, you can define the address of the email and SMS server, configure the dial-in user, AEMC IP and the LAN convertor settings.

20.4.1 Network

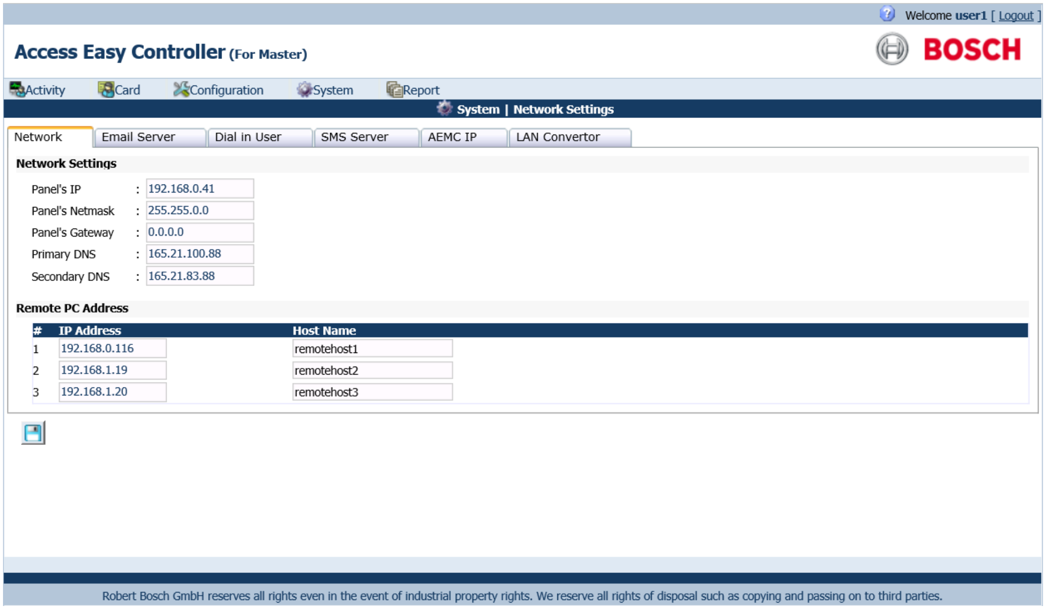
Each Access Easy Controller comes with two LAN ports labeled LAN1 and LAN2. These LAN ports are physically individual ports that have their own IP address. LAN1 is connected to the network where the Access Easy Controller is accessed by other workstations and is usually the office network. LAN2 is used to cater for further expansions.



You can also set three dedicated PCs for download and upload of parameters to Access Easy Controller using DB Backup utility program.

To edit Network Settings

1. Click **System > Network Settings** menu. In the **Network Settings** page, click the **Network** tab. The network configuration for LAN1 is presented here. The screen below shows the settings.



Network Settings

Panel's IP	:	192.168.0.41
Panel's Netmask	:	255.255.0.0
Panel's Gateway	:	0.0.0.0
Primary DNS	:	165.21.100.88
Secondary DNS	:	165.21.83.88

Remote PC Address

#	IP Address	Host Name
1	192.168.0.116	remotehost1
2	192.168.1.19	remotehost2
3	192.168.1.20	remotehost3

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.

2. Change the panel IP address in the **Panel's IP** field.
3. Repeat the step for the **Panel's Netmask** and **Panel’s Gateway** fields.
4. Change the **Primary DNS** and **Secondary DNS** fields if you are using a DNS server.
5. Click the save button to save the settings.

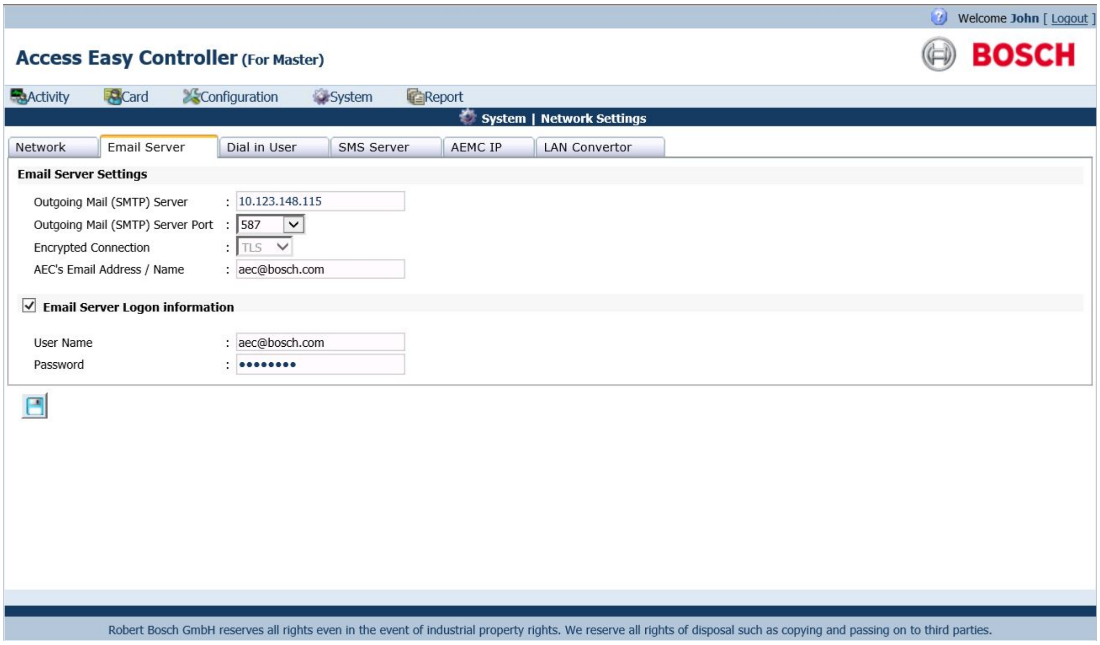
Notice!
In order for the new IP address to take effect, the controller has to be rebooted. Always backup the database before rebooting.

To edit Remote PC Address

1. Enter the IP addresses of the remote PCs in the **IP Address** fields.
2. Enter the PC names as complete words, without spacing in the **Host Name** fields.
3. Click the save button to save the settings.

20.4.2 Email Server

Click **System > Network Settings** menu. In the **Network Settings** page, click the **Email Server** tab. The screen below shows the **Email Server** page.



Email Server Settings

Outgoing Mail (SMTP) Server : 10.123.148.115
Outgoing Mail (SMTP) Server Port : 587
Encrypted Connection : TLS
AEC's Email Address / Name : aec@bosch.com

☑ Email Server Logon information

User Name : aec@bosch.com
Password : ••••••••

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.

This **Email Server** settings page allows you to configure the IP address of the outgoing mail (SMTP) server and the ports to use. You can also specify the reply address of emails sent by the Access Easy Controller, which is the address appearing in the “Sent To” field of the emails.

To configure Email Server settings

1. Enter the outgoing mail (SMTP) server’s IP address in the **Outgoing Mail (SMTP) Server** field.
2. Select the port number from the **Outgoing Mail (SMTP) Server Port** drop-down list. The default number “25” is the commonly used port. We suggest that you skip this field unless your port number is different.
3. If you have chosen a custom port number for the **Outgoing Mail (SMTP) Server Port**, you can select the **Encrypted Connection** from the dropdown list. Otherwise, the default **Encrypted Connection** is based on the selected **Outgoing Mail (SMTP) Server Port**.
4. Enter the email address or name as a complete word, without spacing for the **AEC’s Email Address / Name** field. You can use the underscore “_” character to denote spacing. The information specified in this field will be used as the email address of the Access Easy Controller. In the above screen, the email address will be AEC@BOSCH.COM.
5. If the email service requires authentication to send emails, select the **Email Service Logon Information** checkbox for authentication.
6. Enter the credentials of the email service in the **User Name** and **Password** fields (up to 16 characters long).
7. Click the save 💾 button to save the settings.

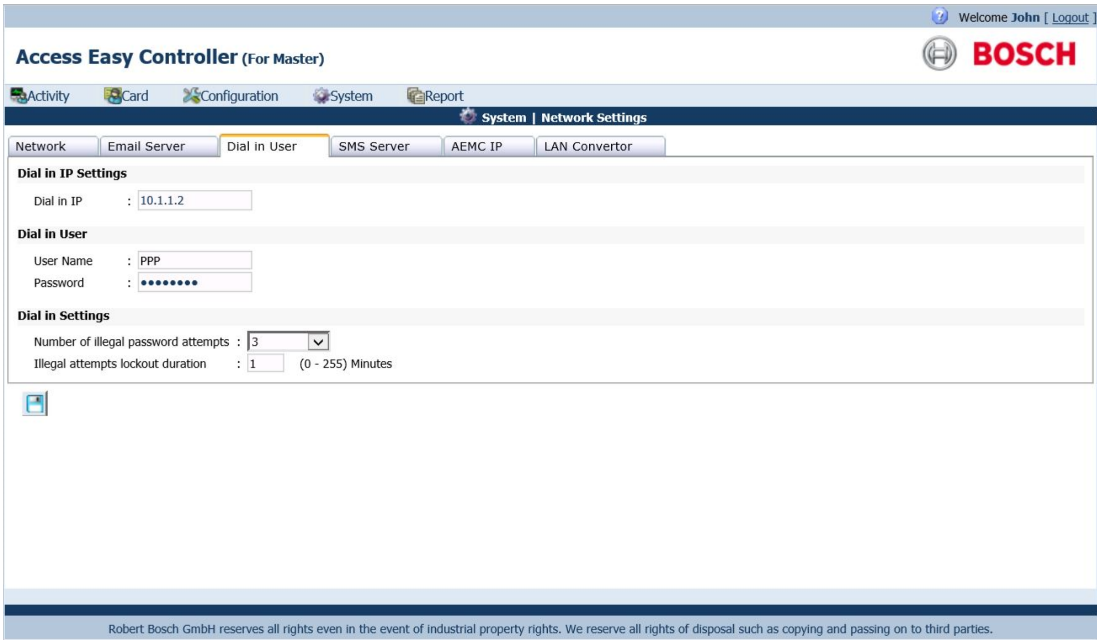
20.4.3 Dial In User

The **Dial In User** page allows you to configure the dial in IP that is required for PPP protocol for remote access. In order to have remote access ability using a modem connection, a temporary IP address has to be issued to the incoming connection.

When you dial in from home, using your 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 the connection is established.

By default, this dial in IP address is set as “10.1.1.2”. This works fine on most network setups. However, change the IP address if you encounter connection problems.

To change this setting, click **System > Network Settings** menu. In the **Network Settings** page, click the **Dial In User** tab. The screen below shows the **Dial In User** page.



Dial in IP Settings

Dial in IP : 10.1.1.2

Dial in User

User Name : PPP

Password : ••••••••

Dial in Settings

Number of illegal password attempts : 3

Illegal attempts lockout duration : 1 (0 - 255) Minutes

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.

To edit the Dial In User settings

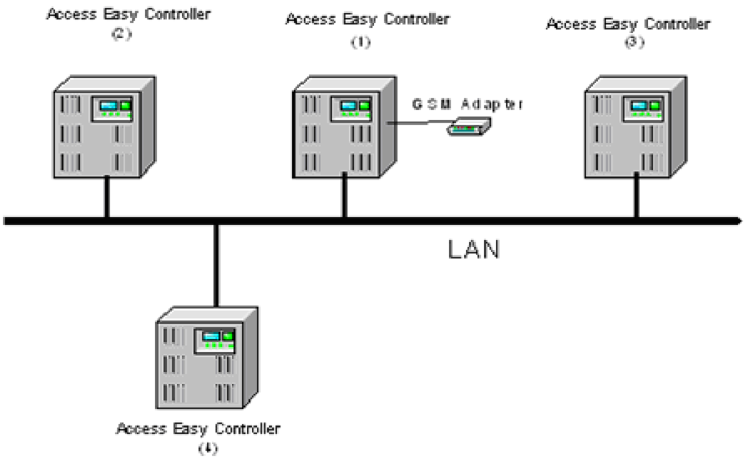
1. Enter the IP address in the **Dial In IP** field.
2. Enter a user ID and password in the **User Name** and **Password** fields for the user to access the Access Easy for Master through the dial In process.
3. Select a number from the **Number of illegal password attempts** drop-down list for the number of illegal attempts that the user can try before successfully logging in the system.
4. Select a time from the **Illegal attempts lockout duration** drop-down list. This is the time duration that is set to prevent successive illegal login attempts. The time range is between 1 to 255 minutes.
5. Click the save 💾 button to save the settings.

Notice!
US Robotics 56K modems are tested with the Access Easy for Master for dial up functionality. For other brands, refer the hardware manual for protocol requirement.

20.4.4 SMS Server

The **SMS Server** page allows you to define the IP address of the Access Easy Controller that has a GSM adapter attached to its serial com to act as an SMS server. To briefly understand how the SMS feature works, we need to understand how the system should be configured.

The following diagram shows more than one Access Easy Controller in the network. These controllers work stand-alone but share a common GSM adapter, which is attached to a dedicated Access Easy Controller serial com port.


Access Easy Controller (2)
Access Easy Controller (1)
Access Easy Controller (3)
GSM Adapter
LAN
Access Easy Controller (4)

The Access Easy Controller (1) has the GSM adapter connected to its serial com port, hence, it acts as an SMS server to help relay Access Easy Controller messages to the service provider.

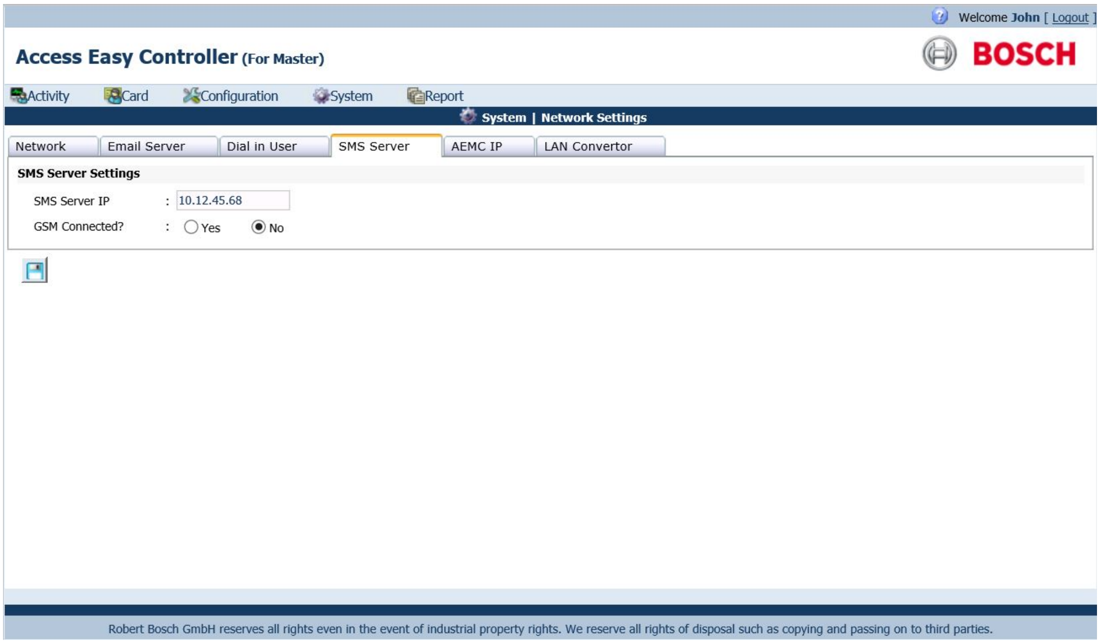
Whenever there is any SMS message that needed to be sent, the respective Access Easy Controller will send the SMS messages over to the Access Easy Controller SMS server. The SMS server will in turn send via the GSM adapter to the Service Provider. These other controllers are defined as the SMS clients.

Hence, there is a need to control the IP addresses that is allowed to send SMS messages. This is to prevent unauthorized personnel sending SMS messages using your Access Easy Controller.

Notice!
Access Easy Controller supports Sierra Wireless GL8200 and WAVECOM GSM modems. Please ensure that GSM adapter baud rate is configured at 115200bps, 8bit data, 1 stop bit and no parity settings.

To configure Access Easy Controller as an SMS Server

Click **System > Network Settings** menu. In the **Network Settings** page, select the **SMS Server** tab. The screen below shows the **SMS Server** page.



SMS Server Settings

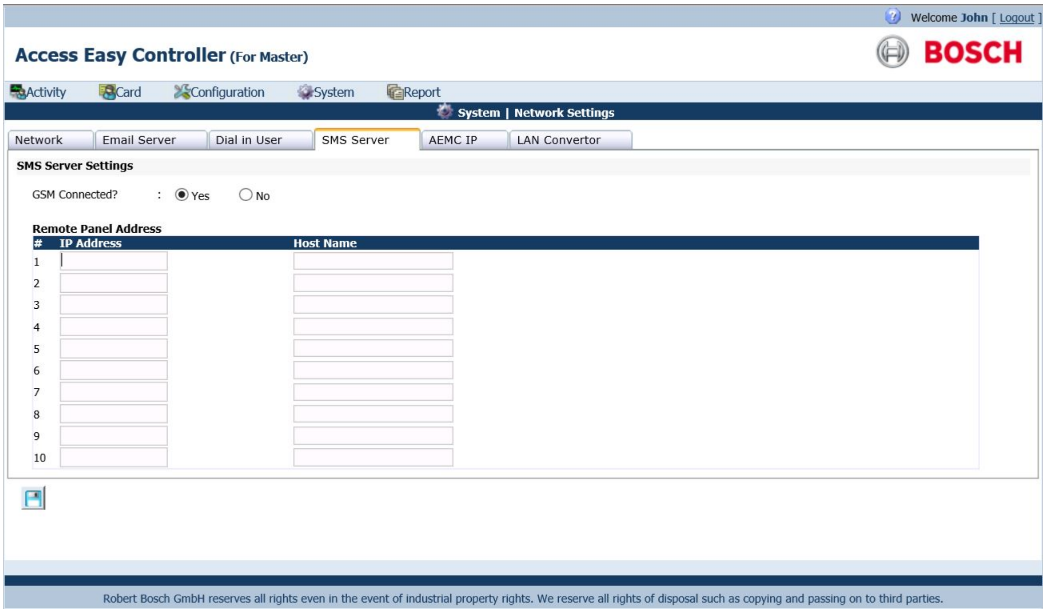
SMS Server IP : 10.12.45.68

GSM Connected? : ○ Yes ● No

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.

By default, the **SMS Server IP** field is blank. If this controller is attached to a GSM adapter, you will need to configure the IP addresses of other Access Easy Controllers that can send SMS messages through this controller.

1. Since this is an SMS server, enter the IP address of the controller in the **SMS Server IP** field.
2. Select the “Yes” option for the **GSM Connected?** radio buttons.



SMS Server Settings

GSM Connected? : ● Yes ○ No

Remote Panel Address

#	IP Address	Host Name
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

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.

3. In the **Remote Panel Address** section, you can specify up to 10 controllers (SMS clients) that can send SMS messages via this SMS server. Enter the IP addresses of these controllers in the **IP Address** fields and their computer names in the **Host Name** fields.

Notice!
Be sure to include the SMS server IP address as one of the SMS client entries. Otherwise, the SMS server would not be able to send its own SMS messages.

4. Click the save 💾 button to save the settings.

To configure Access Easy Controller as an SMS Client

By default, the **SMS Server IP** field is blank. If this controller is not attached to a GSM adapter, it is an SMS client and hence need to identify the IP address of the SMS server.

1. Enter the IP address of the SMS server in the **SMS Server IP** field.
2. Since this is an SMS client, select the “No” option beside the **GSM Connected?** radio buttons.
3. Click the save 💾 button to save the settings.

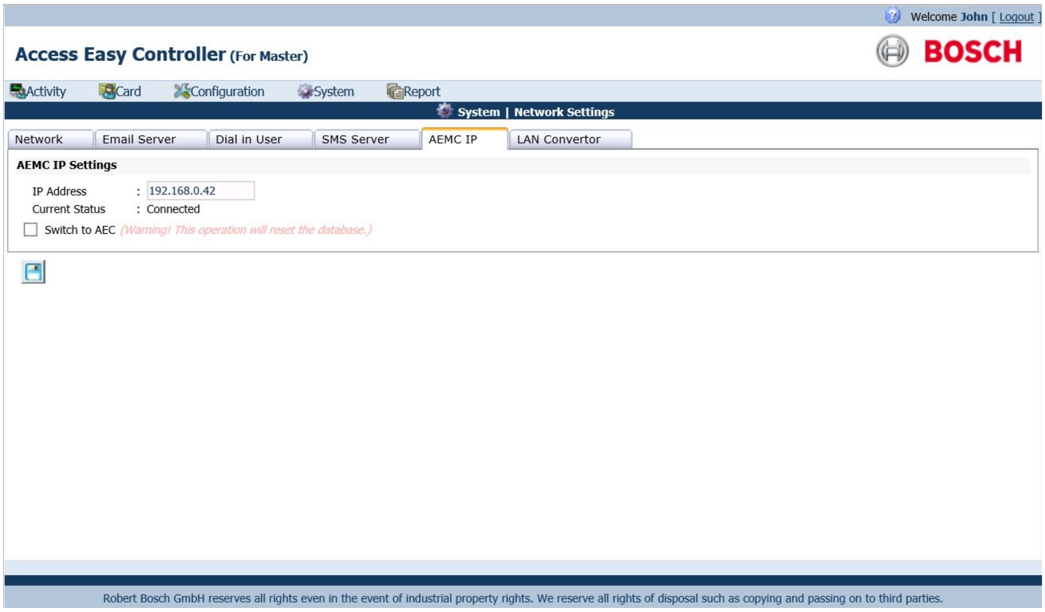
Notice!

Due to limited number of serial COM ports available in the CPU, only either the GSM adapter or the analog dial-up modem can be connected to the Access Easy Controller. Hence, dial-up features will not be enabled when the SMS server is configured. Likewise the SMS server will not be enabled when dial-up has been set up.

20.4.5 AEMC IP

This **AEMC IP** page allows you to define the IP address of Access Easy Master for connecting multiple Access Easy Controllers.

1. Click **System > Network Settings** menu. In the **Network Settings** page, select the **AEMC IP** tab. The screen below shows the **AEMC IP** page.


Welcome John [Logout]
Access Easy Controller (For Master)
BOSCH
Activity
Card
Configuration
System
Report
System | Network Settings
Network
Email Server
Dial in User
SMS Server
AEMC IP
LAN Convertor
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.

AEMC IP Settings

IP Address : 192.168.0.42

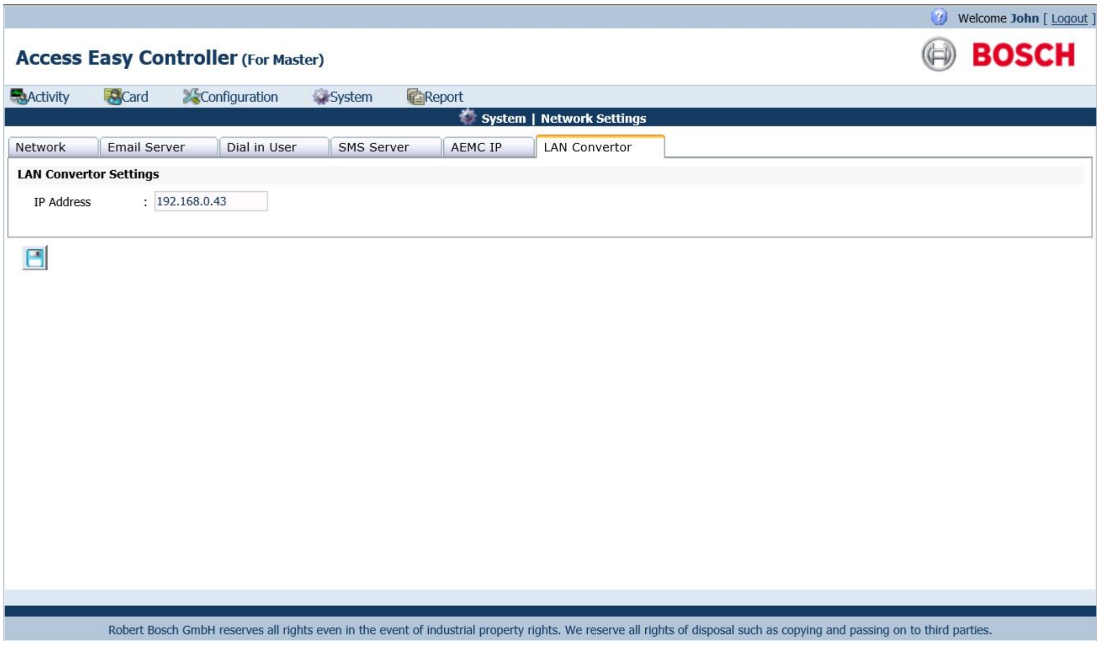
Current Status : Connected

□ Switch to AEC *(Warning! This operation will reset the database.)*

2. Enter the IP address of the Access Easy Master in the **IP Address** field.
3. Click on the 💾 button to save the settings.

20.4.6 LAN Convertor

The **LAN Convertor** page relates to network settings of the LAN convertor. Connecting through the LAN converter, the Access Easy system can be upgraded to 16 interface boards. Click **System > Network Settings** menu. Select the **LAN Convertor** tab to bring up the **LAN Convertor** page.



LAN Convertor Settings

IP Address : 192.168.0.43

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.

The default IP address of the LAN convertor is 192.168.2.42. If you are connecting it to the CPU LAN2, enter the IP address in the range of 192.168.2.x, where x can be any number except 41 since the IP address 192.168.2.41 is reserved for LAN2.

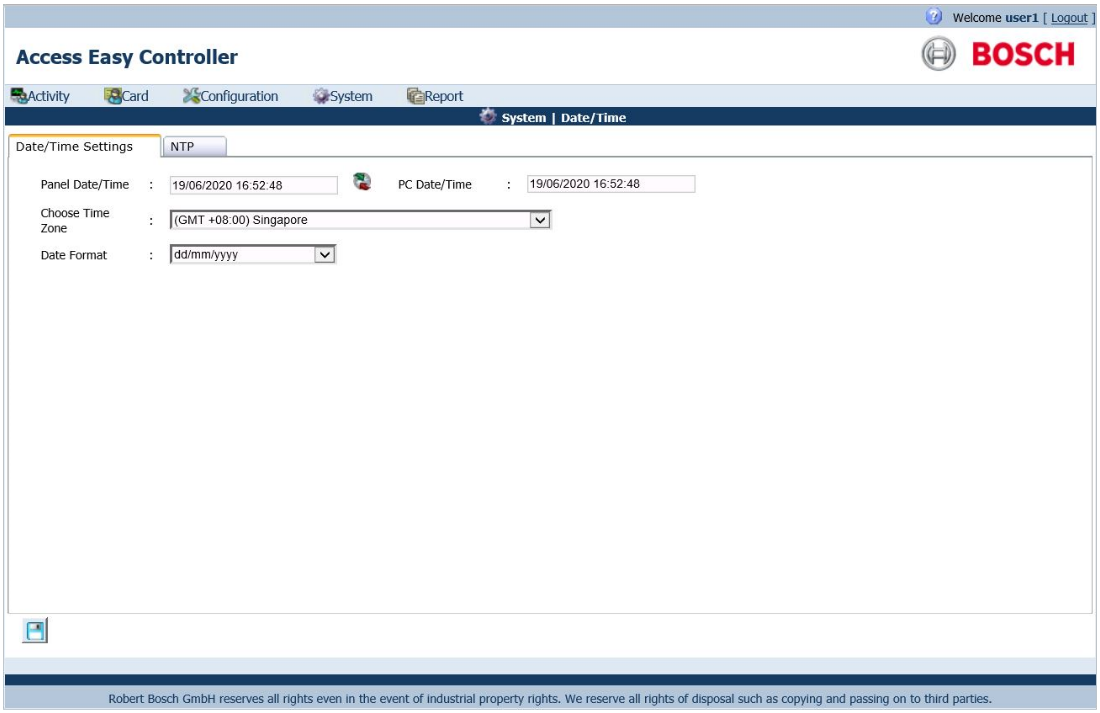
1. Enter the IP address of the LAN convertor in the **IP Address** field.
2. Click the save 💾 button to save the setting.

20.5 Date & Time

Access Easy for Master allows you to set the date and time of the real-time clock within the Access Easy Controller. For countries that practice daylight saving time, this feature is also included. Time setting is in the 24-hour format.

To activate Date & Time screen

Click **System > Date & Time** menu and the screen below appears.



Panel Date/Time : 19/06/2020 16:52:48

PC Date/Time : 19/06/2020 16:52:48

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

Date Format : dd/mm/yyyy

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.

To set the date and time

1. The **Date / Time** page shows the **Panel Date/Time** and **PC Date/Time** fields. Click the synchronize button to synchronize the panel date/time with the PC date/time.
2. Select the appropriate time zone corresponding to the country from the **Choose Time Zone** drop-down list.
3. Select the format of the date from the **Date Format** drop-down list.
4. Click the save button to save the settings.

Notice!
If your country is not listed, please select an alternative country that uses the same time zone.

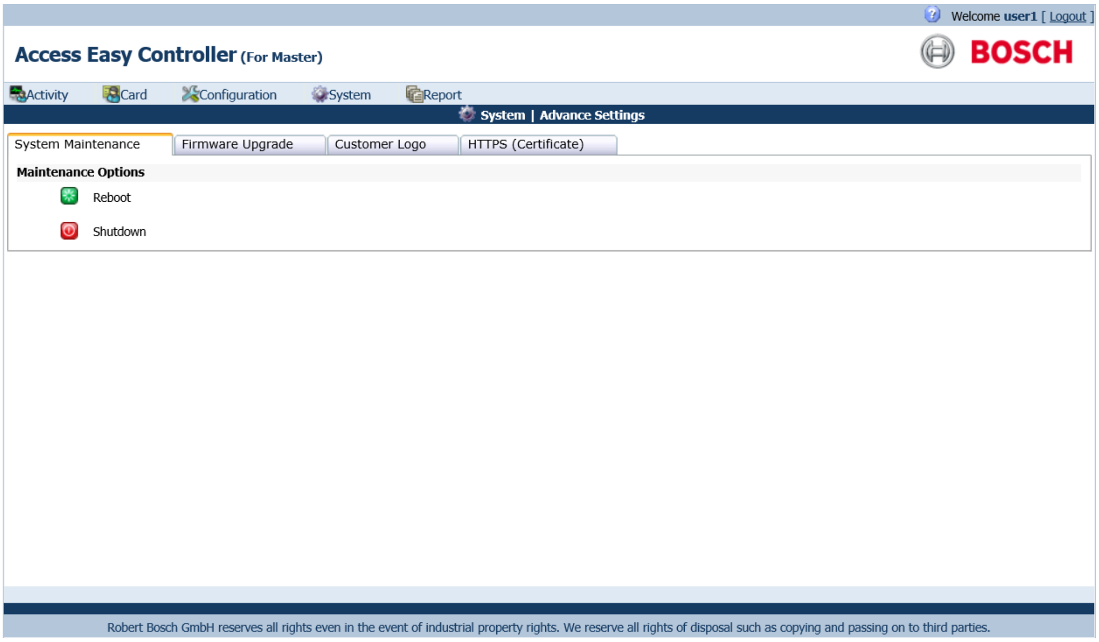
20.6 Advance Settings

The **Advance Settings** submenu refers to the advance settings of the system, including system maintenance, system upgrades and HTTPS setup.

20.6.1 System Maintenance

The **System Maintenance** page allows you to perform various maintenance activities for the panel.

Click **System > Advance Settings** menu. In the **Advance Settings** page, select the **System Maintenance** tab. The screen below shows the **System Maintenance** tab.



Welcome user1 [Logout]
Access Easy Controller (For Master)
BOSCH
Activity
Card
Configuration
System
Report
System | Advance Settings
System Maintenance
Firmware Upgrade
Customer Logo
HTTPS (Certificate)
Maintenance Options
Reboot
Shutdown
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.

To initiate Reboot of panel

Since the Access Easy for Master software is residing within its hardware, the reboot function allows you to reboot the controller after upgrading the system software. It also allows any changes made to take effect, especially changes made to **Network Settings**, such as panel's IP address.

Caution!

During a reboot function, all settings and parameters are taken from the flash memories. In such a case, it is important that the database backup function is carried out before proceeding to reboot the Access Easy Controller.

1. Click the **Reboot** 🟩 button to reboot the panel.
2. A message box appears for confirmation. Click the **OK** button to proceed.
3. It takes about two minutes for the process to complete.

Notice!

During the rebooting process, the Access Easy Controller disconnects itself from the computer and the web page on the computer screen might show an error message or be completely blank. You should close and relaunch the web browser program. Login to Access Easy for Master again after the process is completed.

4. Once the controller is up and running again, reenter the Access Easy for Master URL Address and proceed to log in.

To initiate Shutdown of panel

The shutdown function allows you to shutdown the controller hardware properly. This is usually done when controller hardware requires a hardware upgrade or maintenance.

1. Click the **Shutdown** 🟥 button to shutdown the panel.
2. A message box appears for confirmation. Click the **OK** button to proceed.

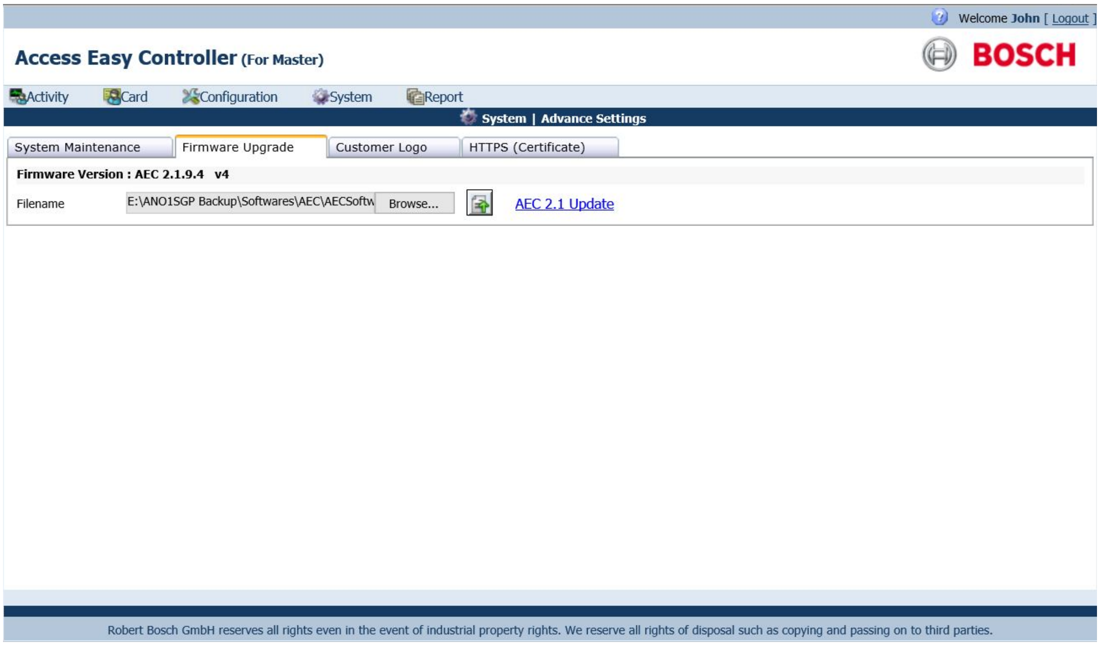
3. You need to manually switch on the power at the controller once the necessary changes are done at the controller.

20.6.2 Firmware Upgrade

The **Firmware Upgrade** page allows update of Access Easy Controller parameters (database recovery) to the flash memory.

Notice!
Check with BOSCH SECURITY SYSTEMS or its authorized dealers for the upgrade.
For database recovery, you must have the previous parameter setting in encrypted zipped format file (db_tar.gz) in the local hard disk. Refer to *Database Backup, page 114* for more information.
The remote PC IP needs to be configured first in the **Network Settings** pages; else the panel will not allow connection.

Click **System > Advance Settings** menu. In the **Advance Settings** page, select the **Firmware Upgrade** tab. The screen below shows the **Firmware Upgrade** page.



Firmware Version : AEC 2.1.9.4 v4

Filename E:\ANO1SGP Backup\Softwares\AEC\AECSoftw

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.

Notice!
The uploading of db_tar.gz file will replace all settings and configurations. This action is irreversible. Make sure that the current settings and configurations are backed up before commencing.

Due to the constant development of the software, the **Firmware Upgrade** page also allows you to upgrade to the newest version by uploading a file. To differentiate between uploading settings and configurations (database recovery) and updating the panel software, the names of these files are fixed.

To upload settings and configurations to the panel, you will use the db_tar.gz file.

To update the panel software, you will use the aec_sys file.

To upload settings and configurations or update the panel software

1. Prepare the file on the PC. If you are updating the panel software, click on the **AEC2.1 Update** link to download the files from the Bosch product page.

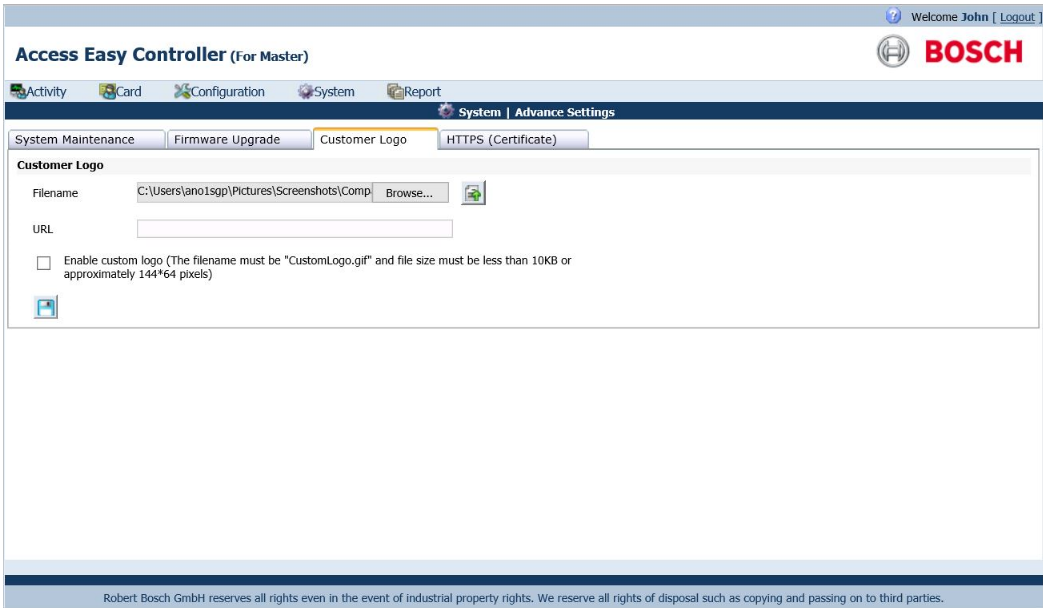
Notice!
Use db_tar.gz file to upload settings and configurations.
Use aec_sys file to update the panel software.

2. Click the **Browse** button to open the file dialog window. Select the file that you wish to upload from.
3. Click the upload button to upload the file.
4. A message box appears for confirmation. Click the **OK** button to proceed with the upload.
5. Once the upload process has completed without error, another confirmation message will appear.
6. Click the **OK** button to reboot the panel.

20.6.3 Customer Logo

The **Customer Logo** page allows you to customize the software with your own logo.

1. Click **System > Advance Settings** menu.
2. In the **Advance Settings** page, select the **Customer Logo** tab. The screen below shows the **Customer Logo** page.



Customer Logo

Filename C:\Users\ano1sgp\Pictures\Screenshots\Comp

URL

□ Enable custom logo (The filename must be "CustomLogo.gif" and file size must be less than 10KB or approximately 144*64 pixels)

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.

3. Click the **Browse** button to open the file dialog window. Select the logo file from the hard disk.

Notice!
The file to be uploaded must be named "CustomerLogo.gif", with a file size of less than 10 kB.

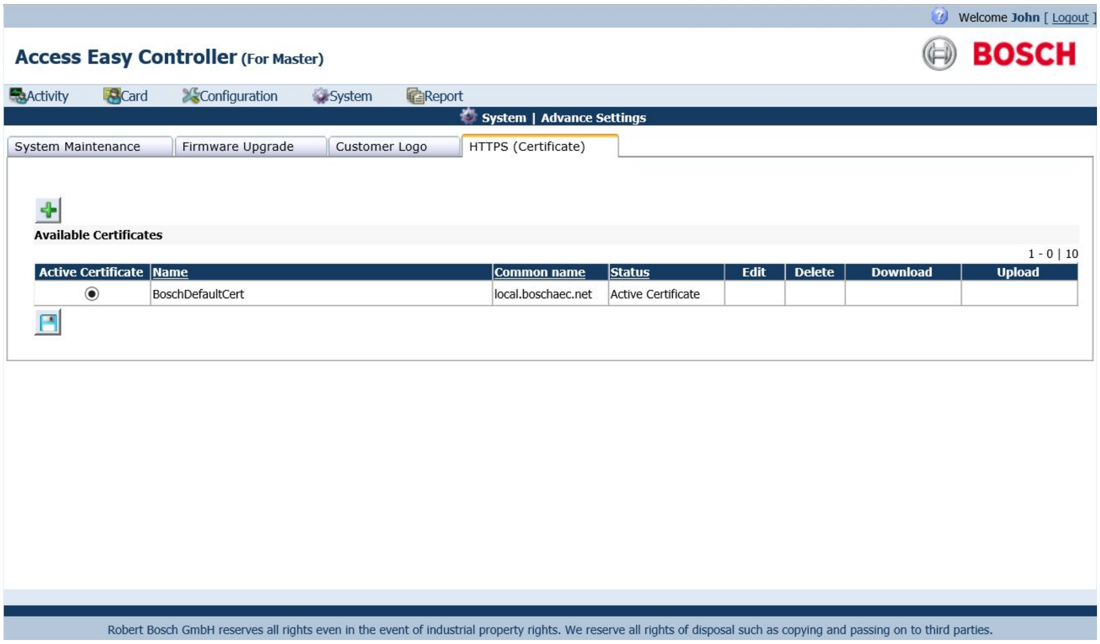
4. Click the upload button to upload the file.
5. Specify a web page address in full in the **URL** field so that the web browser loads the web page when you click on the custom logo. Otherwise, leave the field blank.
6. Select the **Enable custom logo** checkbox for the custom logo to take effect.
7. Click the save button to save the settings.

20.6.4 HTTPS (Certificate)

The **HTTPS (Certificate)** page allows you to manage, create and maintain the SSL/TLS certificates for secure communication over the network using HTTPS protocol.

Caution!
The system may be rebooted during the processes below, so that the changes can take effect.

Go to **System > Advance Settings** menu. In the **Advance Settings** page, select the **HTTPS (Certificate)** tab. The screen below shows the **HTTPS (Certificate)** page. You can see a default certificate by the name of "BoschDefaultCert" in the **Available Certificates** list.



Available Certificates

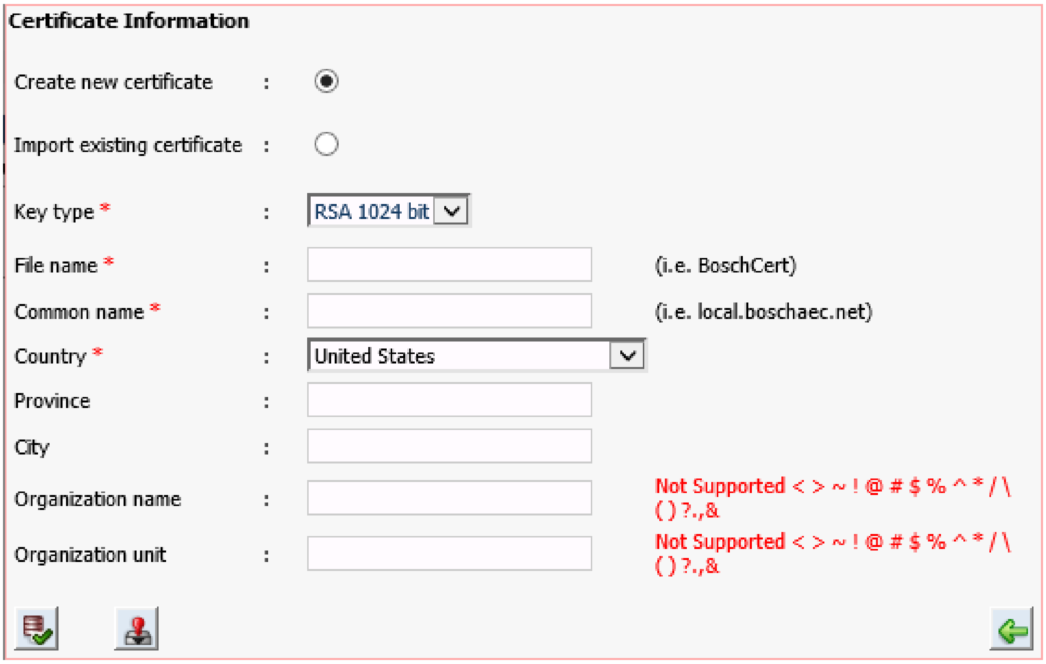
1 - 0 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
●	BoschDefaultCert	local.boschaec.net	Active Certificate				

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.

To generate certificate signing request

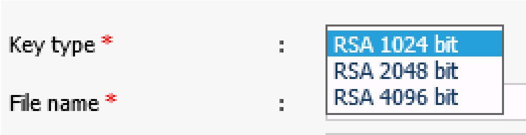
1. Click the add certificate + button to generate a new certificate signing request. The following dialog window appears.



Certificate Information

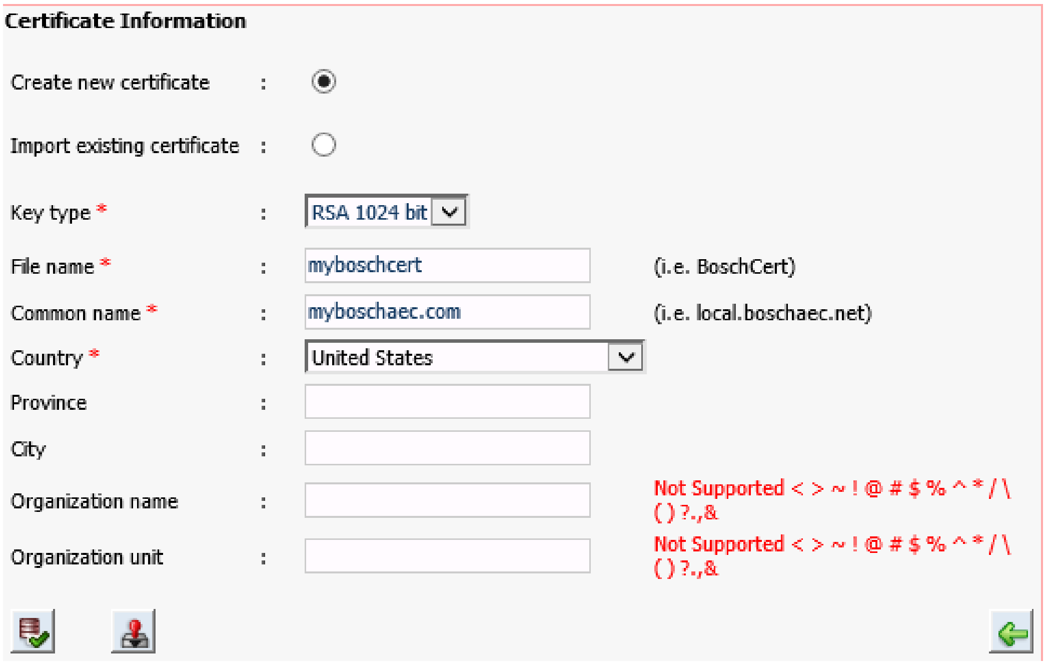
Create new certificate : ●
Import existing certificate : ○
Key type * : RSA 1024 bit
File name * : (i.e. BoschCert)
Common name * : (i.e. local.boschaec.net)
Country * : United States
Province :
City :
Organization name : Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&
Organization unit : Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&

2. Select the **Key type** from the drop-down list. The **Key type** supports: RSA 1024 bit, RSA 2048 bit, and RSA 4096 bit.



Key type * : RSA 1024 bit
RSA 2048 bit
RSA 4096 bit
File name * :

3. Fill in the rest of the certificate information accordingly (see example below).

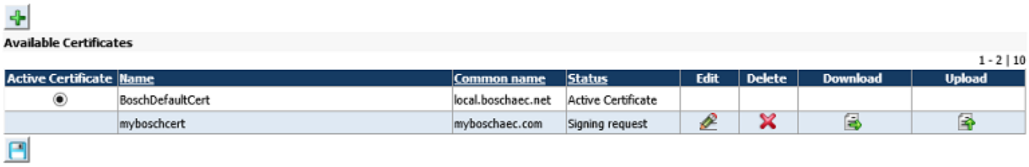


Certificate Information

Create new certificate : ●
Import existing certificate : ○
Key type * : RSA 1024 bit
File name * : myboschcert (i.e. BoschCert)
Common name * : myboschaec.com (i.e. local.boschaec.net)
Country * : United States
Province :
City :
Organization name : Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&
Organization unit : Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&

Notice!
The **File name** provided must be unique within each Access Easy Controller system.
The **Common name** provided must be unique to the network.

4. Click the generate certificate signing request button to generate the certificate signing request. Be patient as it will take some time for the process to complete. The new certificate signing request will then be visible in the **Available Certificates** list.

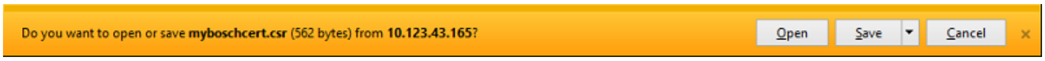


Available Certificates

1 - 2 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
●	BoschDefaultCert	local.boschaec.net	Active Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✗		

5. Click the Download button of the corresponding certificate signing request to save the CSR file to the local computer. Send this file to your trusted certificate authority to be signed and validated.



Do you want to open or save **myboschcert.csr** (562 bytes) from **10.123.43.165**?

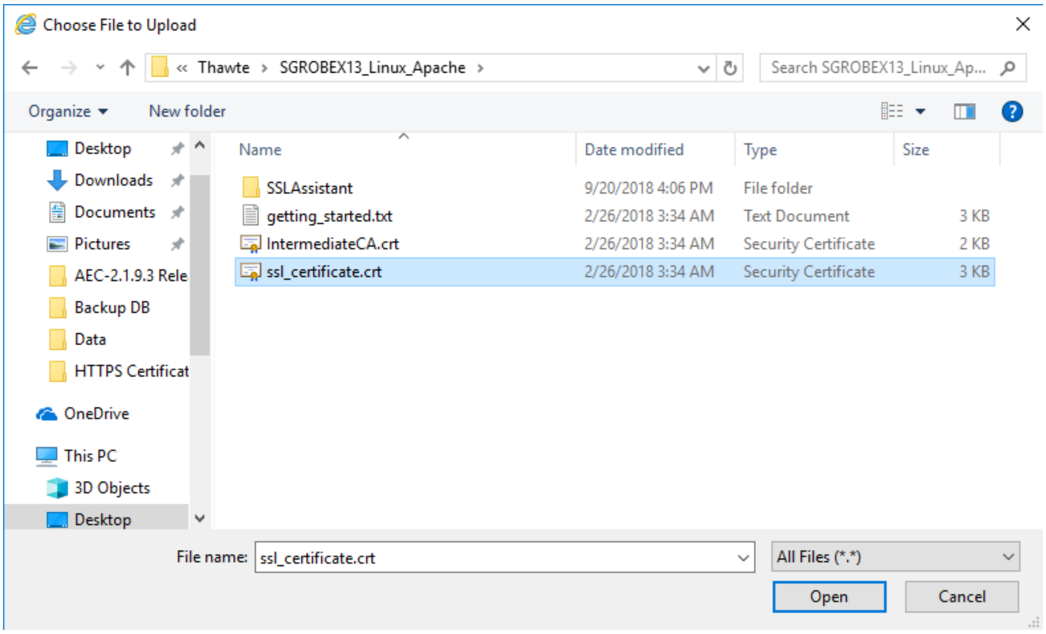
Notice!
Do not delete the certificate signing request. If it is somehow deleted, you will not be able to use the signed certificate (Root CA) you received from your trusted certificate authority.

6. Proceed to upload the signed certificate upon receiving the file from your trusted certificate authority in the next section.

To use a new signed certificate

1. Upon receiving your newly signed certificate from your trusted certificate authority, copy it to the local computer.
2. Go to **System > Advance Settings > HTTPS (Certificate)** tab.

3. Click the Upload button of the corresponding certificate signing request. The **Choose File to Upload** dialog window appears.



Choose File to Upload

« Thawte › SGROBEX13_Linux_Apache ›

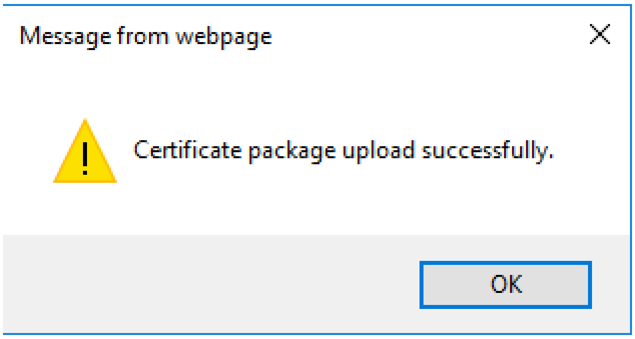
Search SGROBEX13_Linux_Ap...

Name	Date modified	Type	Size
SSLAssistant	9/20/2018 4:06 PM	File folder	
getting_started.txt	2/26/2018 3:34 AM	Text Document	3 KB
IntermediateCA.crt	2/26/2018 3:34 AM	Security Certificate	2 KB
ssl_certificate.crt	2/26/2018 3:34 AM	Security Certificate	3 KB

File name: ssl_certificate.crt

All Files (*.*)

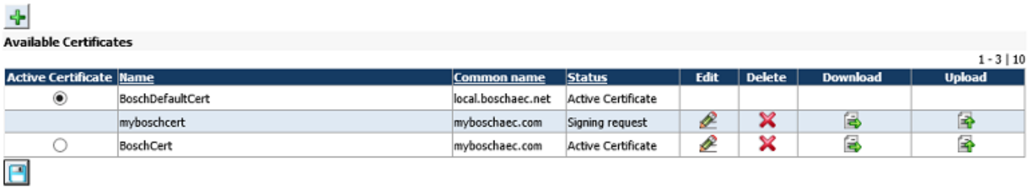
4. Navigate the folders and select the newly signed certificate to be uploaded to the system. Click the **Open** button to start the uploading process.
5. If the upload is unsuccessful, an error message dialog window will appear. If you encounter an error, check if the correct file has been uploaded correctly, or if there are other issues.
6. If the upload is successful, a completion successful message will appear. Click the **OK** button.



Message from webpage

Certificate package upload successfully.

7. You will see the newly uploaded signed certificate in the **Available Certificates** list with an unselected radio button.

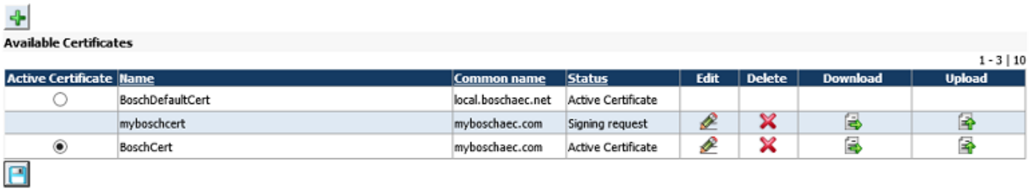


Available Certificates

1 - 3 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
●	BoschDefaultCert	local.boschaec.net	Active Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✖		
○	BoschCert	myboschaec.com	Active Certificate	✎	✖		

8. Select the radio button of the signed certificate to enable it as the active certificate.

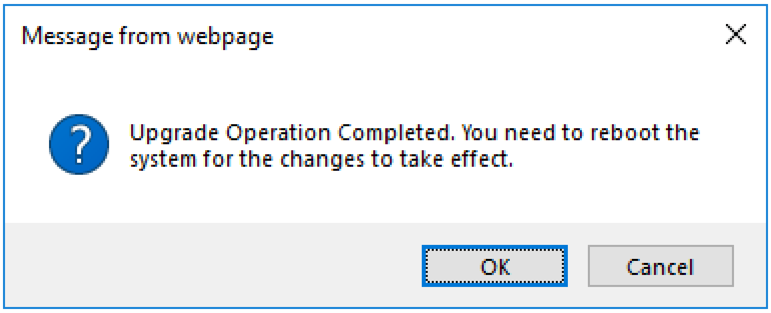


Available Certificates

1 - 3 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
○	BoschDefaultCert	local.boschaec.net	Active Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✖		
●	BoschCert	myboschaec.com	Active Certificate	✎	✖		

9. Click the save button, and the following dialog window appears. The system needs to be rebooted for the changes to take effect. Click the **OK** button to reboot the system.



Message from webpage

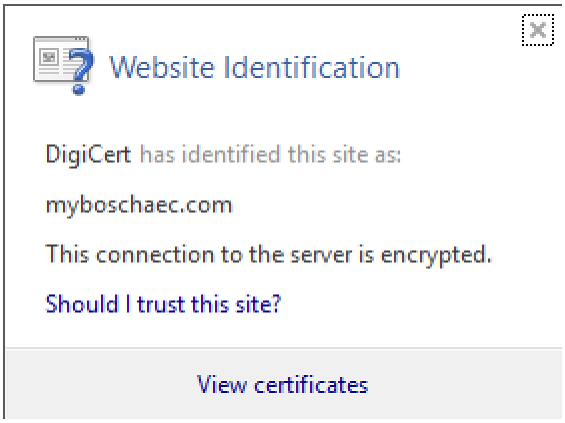
Upgrade Operation Completed. You need to reboot the system for the changes to take effect.

10. Wait a while (no longer than 3 minutes) for the system to reboot. After rebooting, the web browser will automatically refresh itself, and return to the login page.

11. From the web browser, enter the HTTPS protocol and your website name. You should see a lock icon on the web browser address bar. The certificate has been successfully installed.

https://myboschaec.com/login.aspx

12. You can click on the lock icon to view details of the certificate from the **Website Identification** dialog window.



Website Identification

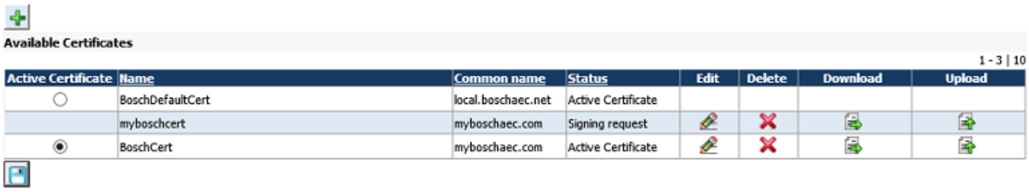
DigiCert has identified this site as:

myboschaec.com

This connection to the server is encrypted.

To backup and restore an existing certificate

1. To back up the signed certificates, go to **System > Advance Settings > HTTPS (Certificate)** tab. You will see the signed certificates in the **Available Certificates** list.

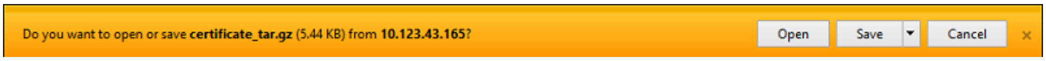


Available Certificates

1 - 3 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
○	BoschDefaultCert	local.boschaec.net	Active Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✖		
●	BoschCert	myboschaec.com	Active Certificate	✎	✖		

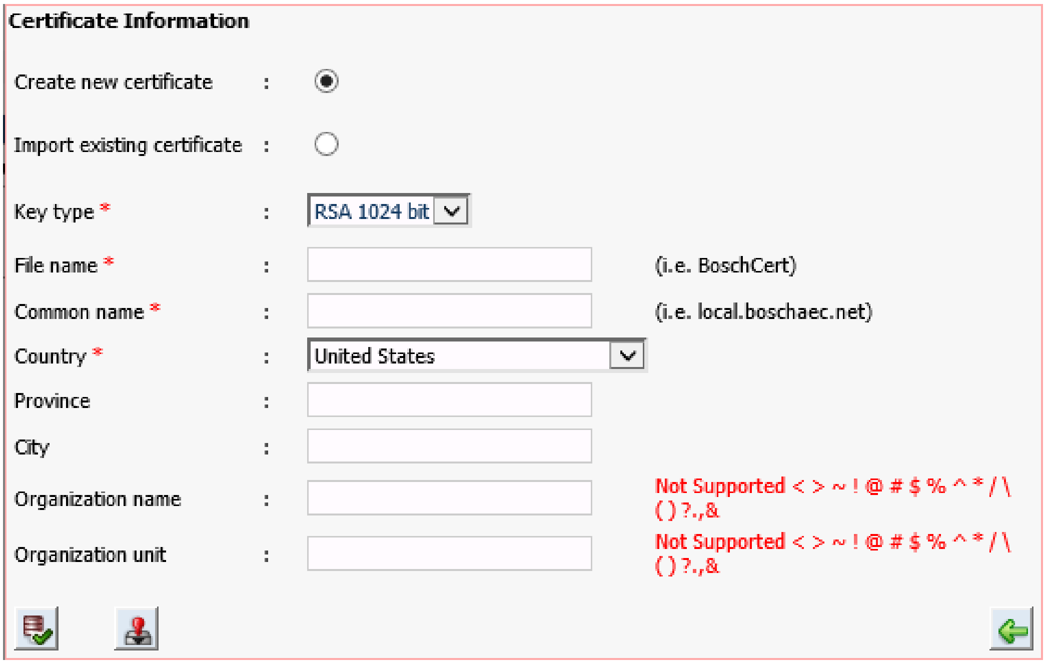
2. Click the Download button of the signed certificate to create a backup copy. This file "certificate_tar.gz" should be stored elsewhere as a backup.



Do you want to open or save **certificate_tar.gz** (5.44 KB) from **10.123.43.165**?

3. If the signed certificate has been deleted, you can restore the signed certificates using the backup certificate file "certificate_tar.gz". Go to **System > Advance Settings > HTTPS (Certificate)** tab.

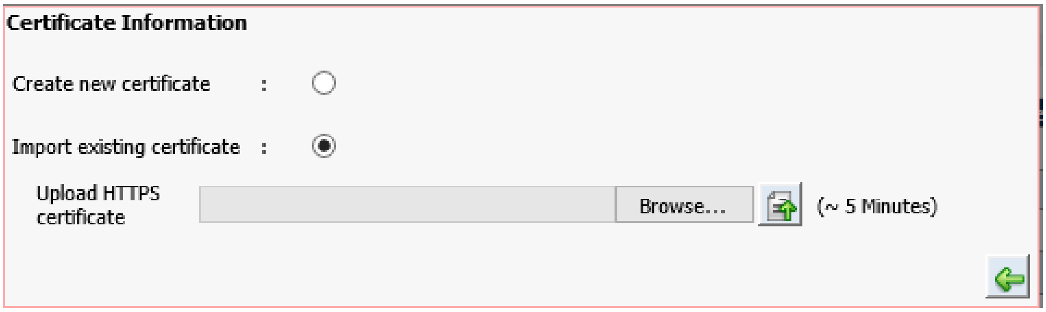
4. Click the Add certificate button. The following dialog window appears.



Certificate Information

Create new certificate	:	●	
Import existing certificate	:	○	
Key type *	:	RSA 1024 bit	
File name *	:		(i.e. BoschCert)
Common name *	:		(i.e. local.boschaec.net)
Country *	:	United States	
Province	:		
City	:		
Organization name	:		Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&
Organization unit	:		Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&

5. Click the **Import existing certificate** radio button and the following dialog window appears.

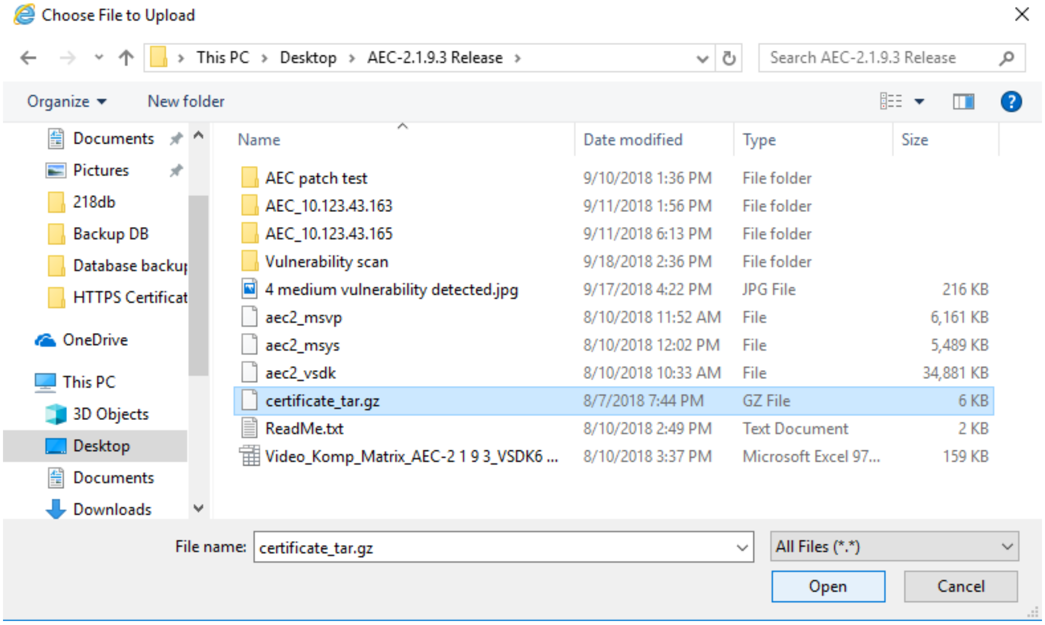


Certificate Information

Create new certificate	:	○
Import existing certificate	:	●

Upload HTTPS certificate — Browse... (~ 5 Minutes)

6. Click the **Browse** button to navigate the folders, and select the backup certificate file "certificate_tar.gz" to be uploaded to the system.



Choose File to Upload

This PC > Desktop > AEC-2.1.9.3 Release >

Search AEC-2.1.9.3 Release

Organize ▾ New folder

Documents, Pictures, 218db, Backup DB, Database backup, HTTPS Certificat, OneDrive, This PC, 3D Objects, Desktop, Documents, Downloads

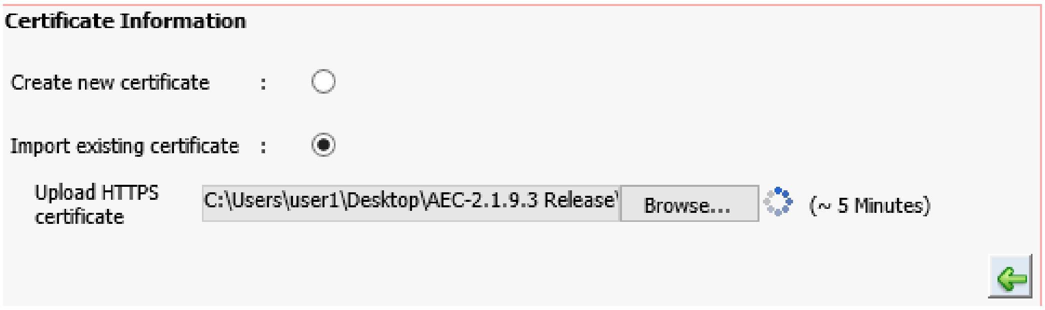
Name	Date modified	Type	Size
AEC patch test	9/10/2018 1:36 PM	File folder	
AEC_10.123.43.163	9/11/2018 1:56 PM	File folder	
AEC_10.123.43.165	9/11/2018 6:13 PM	File folder	
Vulnerability scan	9/18/2018 2:36 PM	File folder	
4 medium vulnerability detected.jpg	9/17/2018 4:22 PM	JPG File	216 KB
aec2_msvp	8/10/2018 11:52 AM	File	6,161 KB
aec2_msys	8/10/2018 12:02 PM	File	5,489 KB
aec2_vsdk	8/10/2018 10:33 AM	File	34,881 KB
certificate_tar.gz	8/7/2018 7:44 PM	GZ File	6 KB
ReadMe.txt	8/10/2018 2:49 PM	Text Document	2 KB
Video_Komp_Matrix_AEC-2 1 9 3_VSDK6 ...	8/10/2018 3:37 PM	Microsoft Excel 97...	159 KB

File name: certificate_tar.gz

All Files (*.*)

Open Cancel

7. Click the Upload button to start the uploading process.



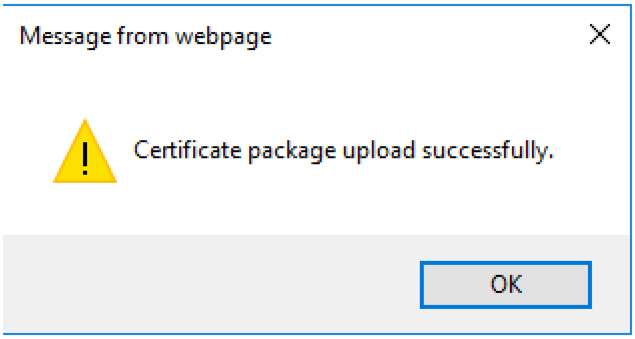
Certificate Information

Create new certificate : ○

Import existing certificate : ●

Upload HTTPS certificate C:\Users\user1\Desktop\AEC-2.1.9.3 Release\ Browse... (~ 5 Minutes)

8. If the upload is unsuccessful, an error message will appear. If you encounter an error, check if the correct file has been uploaded correctly, or if there are other issues.
9. If the upload is successful, a completion successful message will appear. Click the **OK** button.

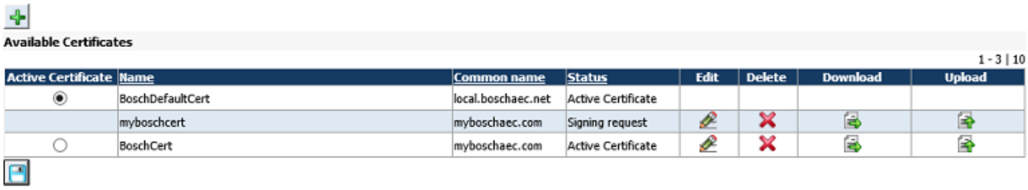


Message from webpage

Certificate package upload successfully.

OK

10. You will see the signed certificate in the **Available Certificates** list with an unselected radio button.

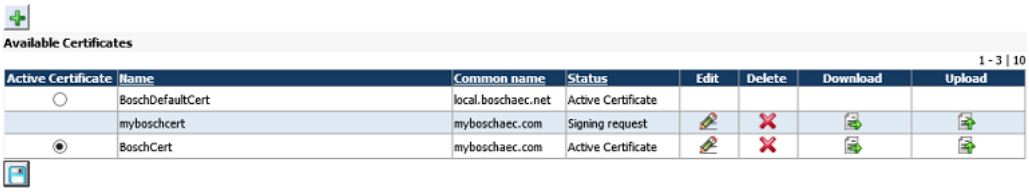


Available Certificates

1 - 3 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
●	BoschDefaultCert	local.boschaec.net	Active Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✗	⬇	⬆
○	BoschCert	myboschaec.com	Active Certificate	✎	✗	⬇	⬆

11. Select the radio button of the signed certificate to enable it as the active certificate.

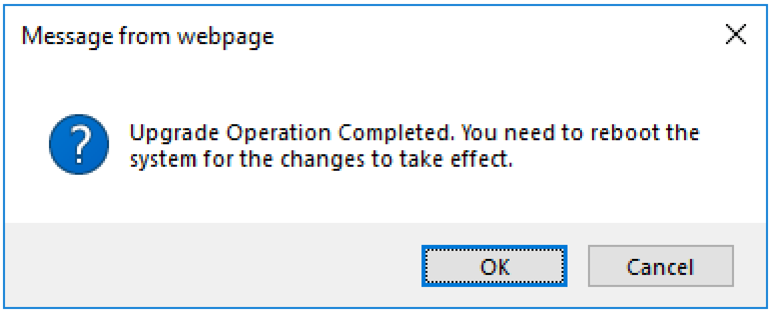


Available Certificates

1 - 3 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
○	BoschDefaultCert	local.boschaec.net	Active Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✗	⬇	⬆
●	BoschCert	myboschaec.com	Active Certificate	✎	✗	⬇	⬆

12. Click the Save button and the following dialog window appears. The system needs to be rebooted for the changes to take effect. Click the **OK** button to reboot the system.



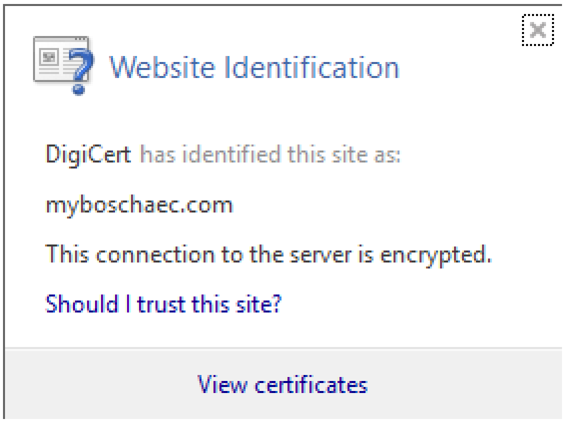
Message from webpage

Upgrade Operation Completed. You need to reboot the system for the changes to take effect.

13. Wait a while (no longer than 3 minutes) for the system to reboot. After rebooting, the web browser will automatically refresh itself, and return to the login page.
14. From the web browser, enter the HTTPS protocol and your website name. You should see a lock icon on the web browser address bar. The certificate has been successfully installed.

https://myboschaec.com/login.aspx

15. You can click on the lock icon to view details of the certificate from the **Website Identification** dialog window.



Website Identification

DigiCert has identified this site as:

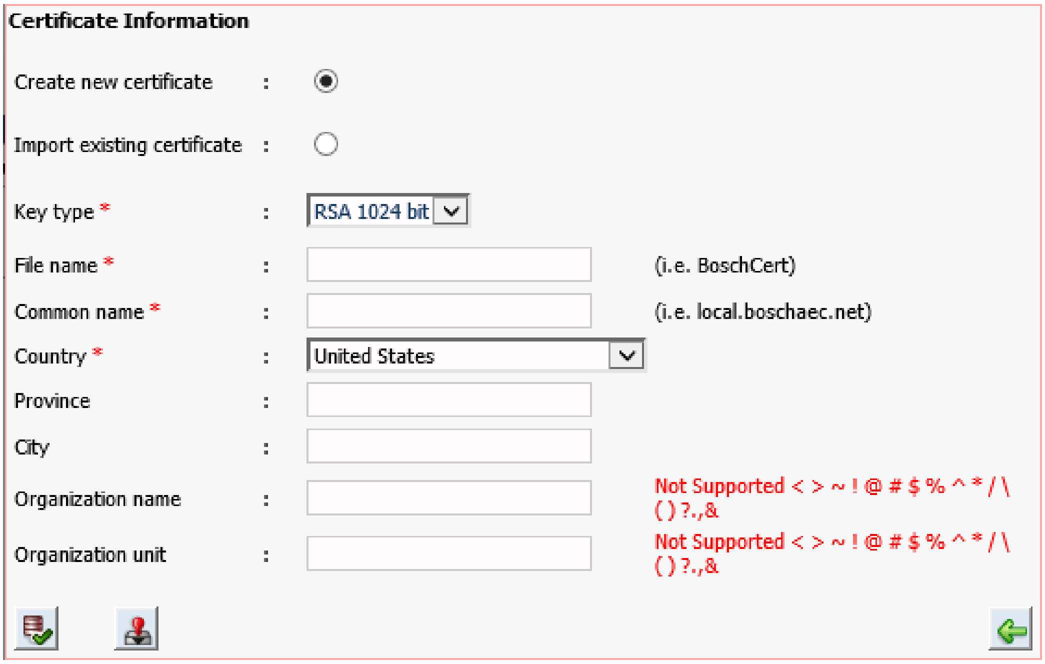
myboschaec.com

This connection to the server is encrypted.

To create a self signed certificate

1. Go to **System > Advance Settings > HTTPS (Certificate)** tab.

2. Click the Add certificate ✚ button. The following dialog window appears.

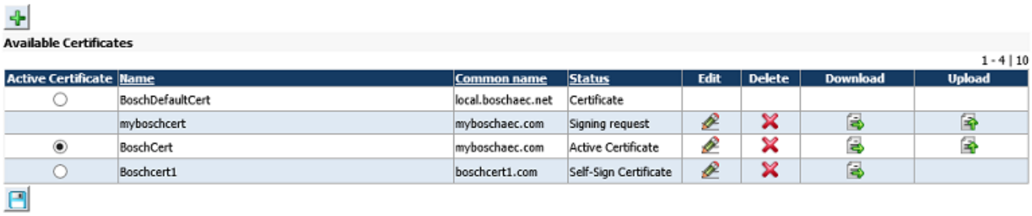


Certificate Information

Create new certificate	:	●	
Import existing certificate	:	○	
Key type *	:	RSA 1024 bit	
File name *	:		(i.e. BoschCert)
Common name *	:		(i.e. local.boschaec.net)
Country *	:	United States	
Province	:		
City	:		
Organization name	:		Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&
Organization unit	:		Not Supported < > ~ ! @ # $ % ^ * / \ ( ) ?.,&

3. Fill in the necessary information to create a self signing certificate.

4. Click the Create self signing certificate button. The self signing certificate now appears in the **Available Certificates** list.



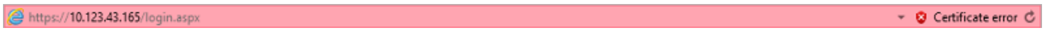
Available Certificates

1 - 4 | 10

Active Certificate	Name	Common name	Status	Edit	Delete	Download	Upload
○	BoschDefaultCert	local.boschaec.net	Certificate				
	myboschcert	myboschaec.com	Signing request	✎	✗	⇨	⇧
●	BoschCert	myboschaec.com	Active Certificate	✎	✗	⇨	⇧
○	Boschcert1	boschcert1.com	Self-Sign Certificate	✎	✗	⇨	

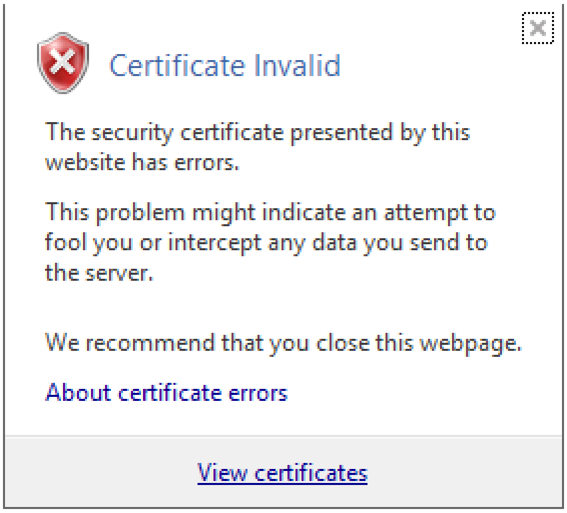
5. Select the radio button of the self signing certificate, and click the save button. The system will automatically reboot for the change to take effect.

6. Wait a while (no longer than 3 minutes) for the system to reboot. After the reboot, the web browser will automatically refresh itself, and return to the login page. From the web browser, you will see a certificate error indication on the address bar.



https://10.123.43.165/login.aspx Certificate error

7. Click the certificate error indication to open the **Certificate Invalid** dialog.



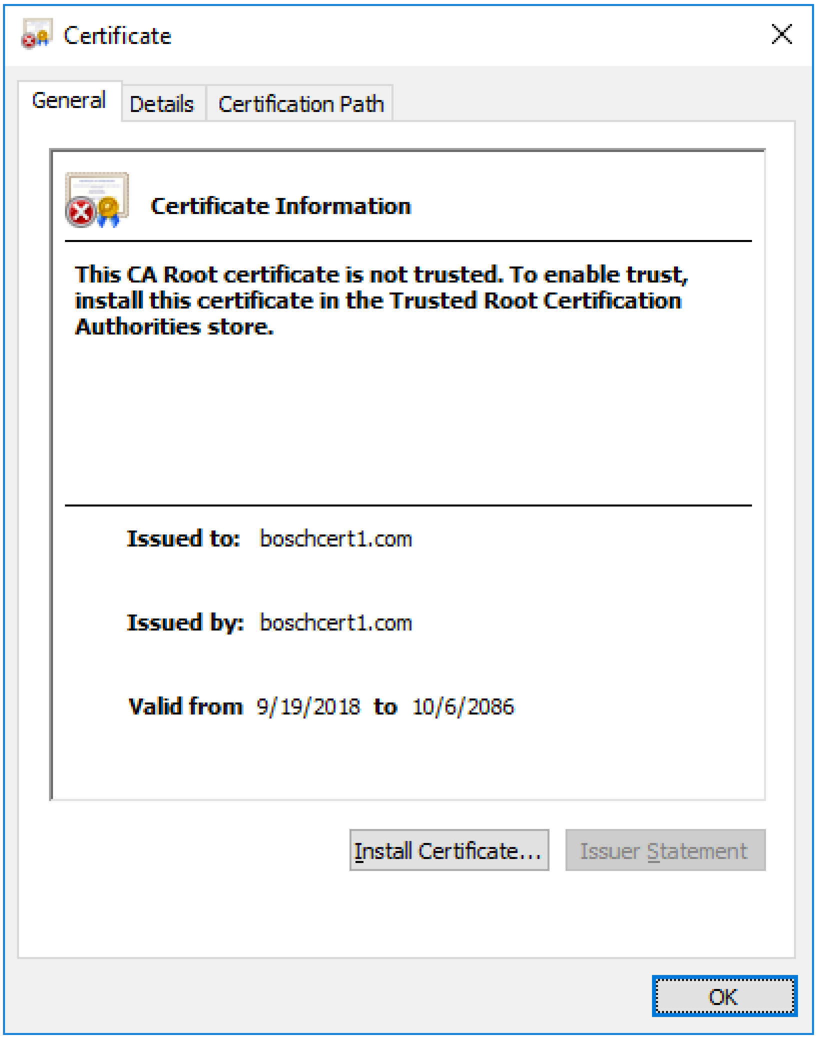
Certificate Invalid

The security certificate presented by this website has errors.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

8. Click the **View certificates** link to open the **Certificate** dialog window.



Certificate Information

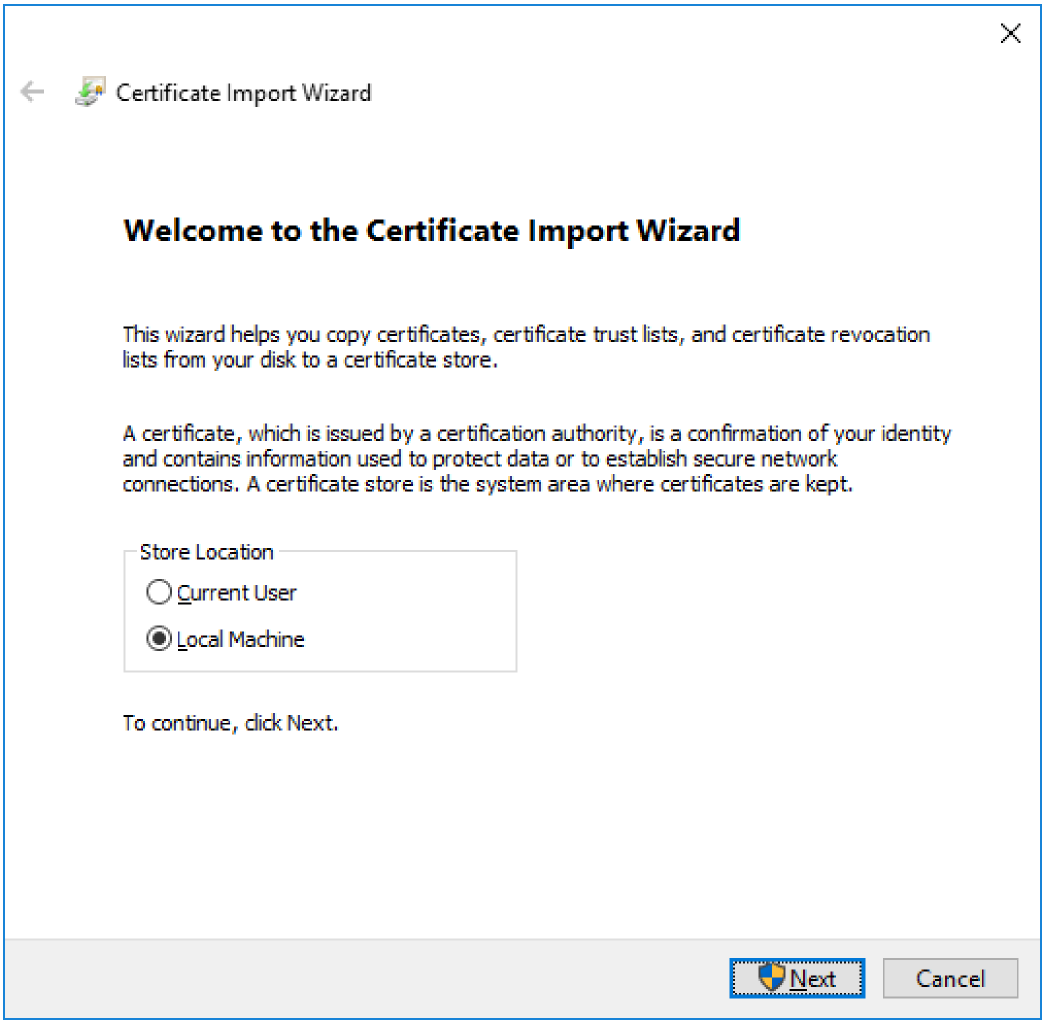
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: boschcert1.com

Issued by: boschcert1.com

Valid from 9/19/2018 to 10/6/2086

9. Click the **Install Certificate** button to open the **Certificate Import Wizard** window, and select the **Local Machine** radio button option.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

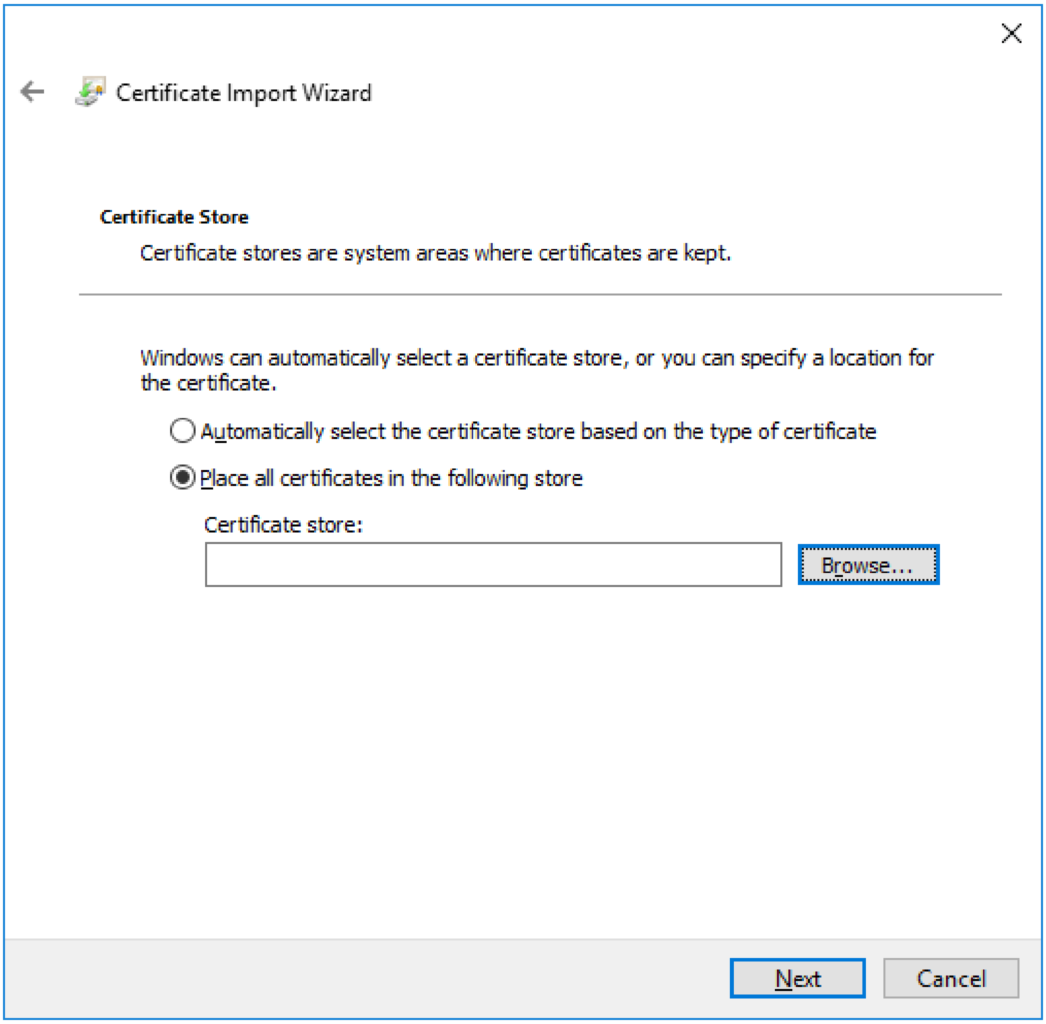
Store Location

○ Current User

● Local Machine

To continue, click Next.

10. Click the **Next** button. The following dialog appears.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

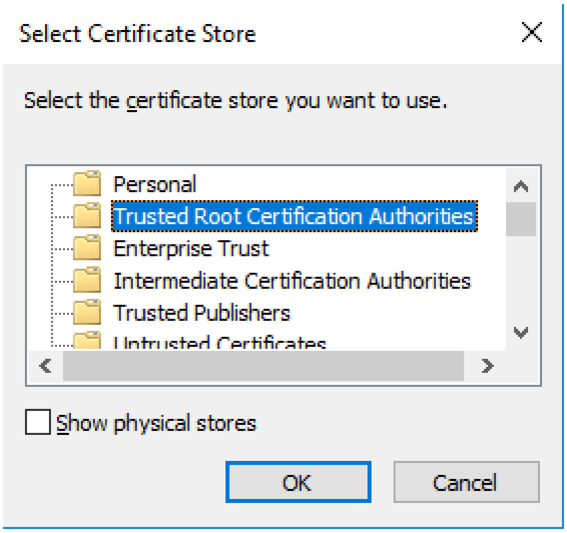
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

11. Click the **Browse** button and select the **Trusted Root Certification Authorities** from the **Select Certificate Store** dialog window.



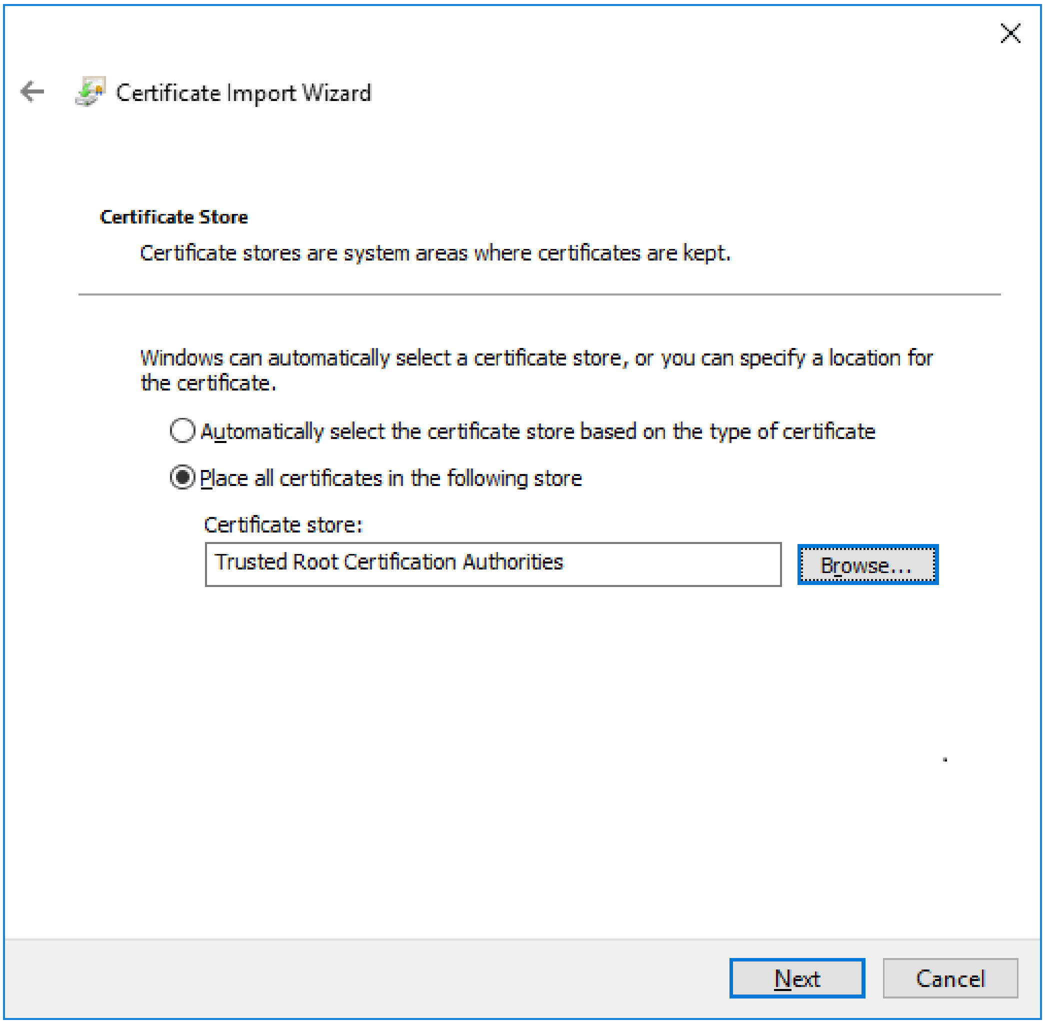
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

12. Click the **OK** button to return to the previous dialog. Note that the store is now indicated in the **Certificate store** textbox.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

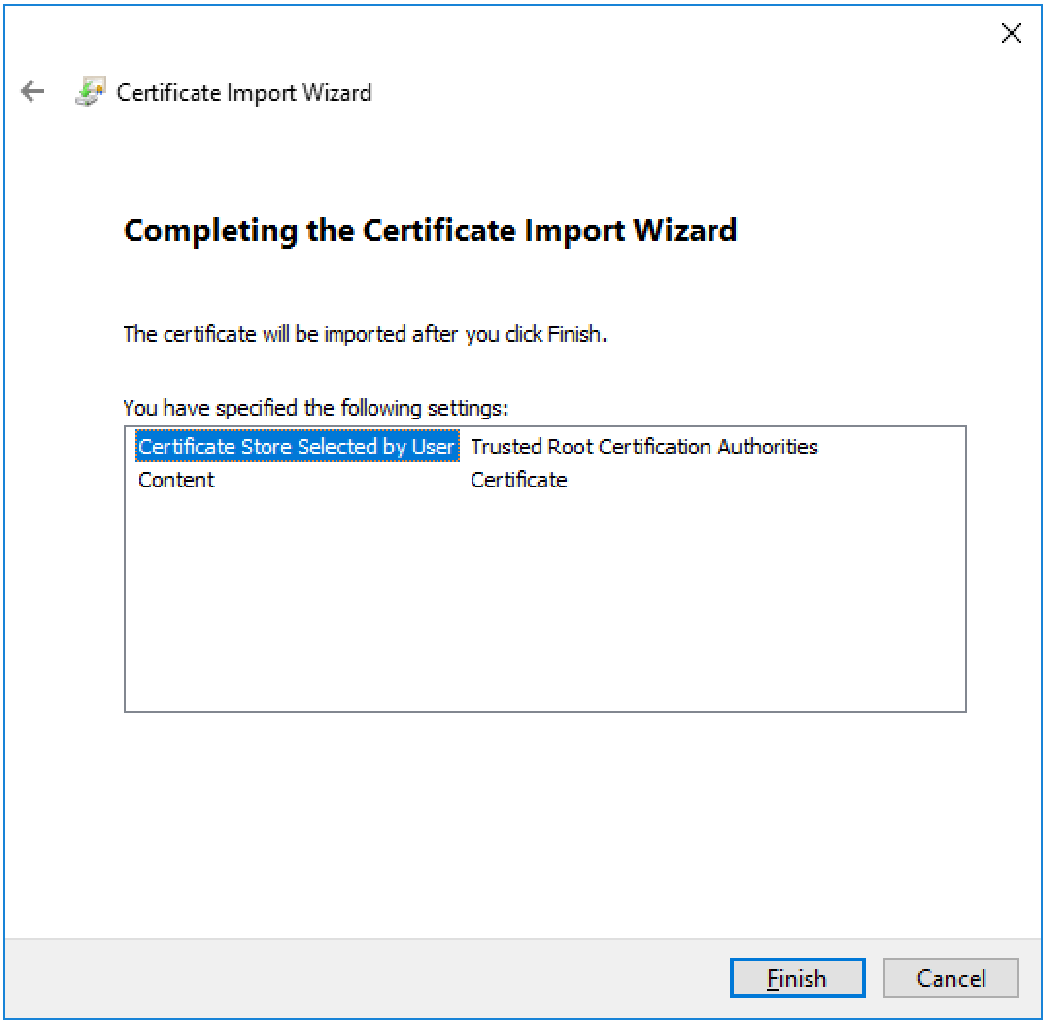
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

13. Click the **Next** button to proceed to the next dialog.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

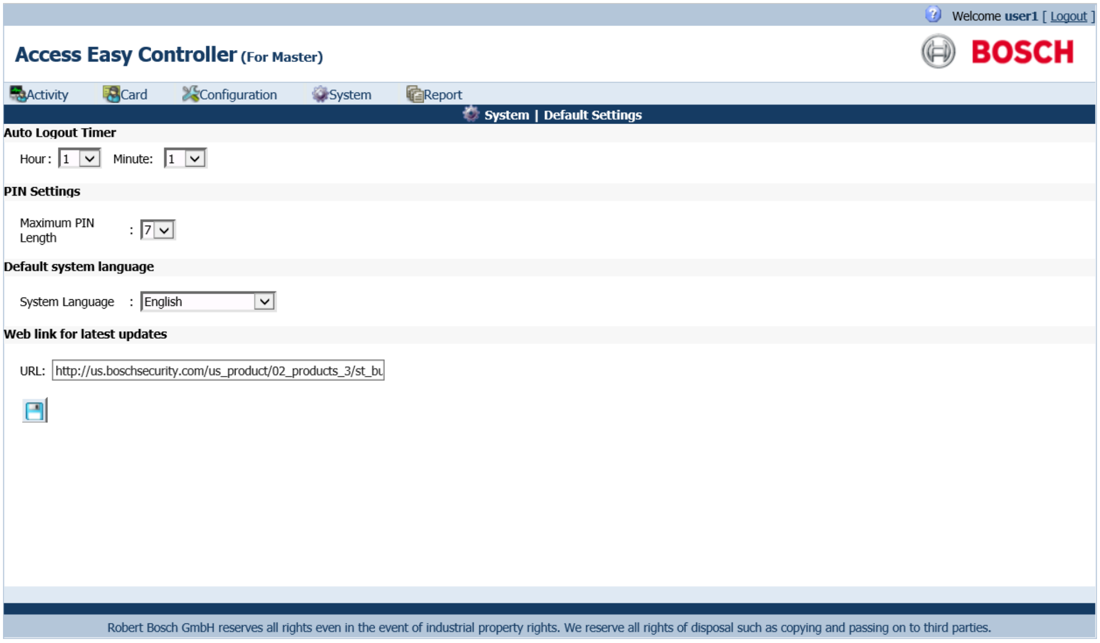
14. Click the **Finish** button to complete the certificate import. The system will automatically reboot for the changes to take effect.
15. Wait a while (no longer than 3 minutes) for the system to reboot. After the reboot, the web browser will automatically refresh itself, and return to the login page.
16. From the web browser, enter the https protocol and your website name. You should see a lock icon on the web browser address bar.

https://myboschaec.com/login.aspx

If the web browser is still showing the certificate error indication, clear the cache, close the web browser, and reboot your computer. This should clear the error and you should be able to connect to your website without the certificate errors.

20.7 Default Settings

The **Default Settings** page allows you to configure various default settings of the system. Click **System > Default Settings** menu. The screen below shows the **Default Settings** page.



Welcome **user1** [Logout]

Access Easy Controller (For Master)

System | Default Settings

Auto Logout Timer

Hour : 1 Minute: 1

PIN Settings

Maximum PIN Length : 7

Default system language

System Language : English

Web link for latest updates

URL: http://us.boschsecurity.com/us_product/02_products_3/st_bu

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.

To set the Auto Logout Timer

The auto logout timer allows you to set the timer for the Access Easy for Master software to logout automatically if it detects no user activity. Default setting is 1 hour.

Notice!
This timer setting is applicable to all menu items.

1. Select the hour and minutes for the auto logout timer from the **Hour** and **Minute** dropdown list of the **Auto Logout Timer** section.
2. Click the save button to save the settings.

To set the maximum PIN length

The PIN settings option allows you to set the maximum PIN length.

1. Select the number of characters from the **Maximum PIN length** dropdown list of the **PIN Settings** section.
2. Click the save button to save the settings.

To set Default system language

The **Default system language** section allows you to set the default system language of the Access Easy Controller.

1. Select the default language from the **System Language** dropdown list in the **Default system language** section.
2. Click the save button to save the settings.

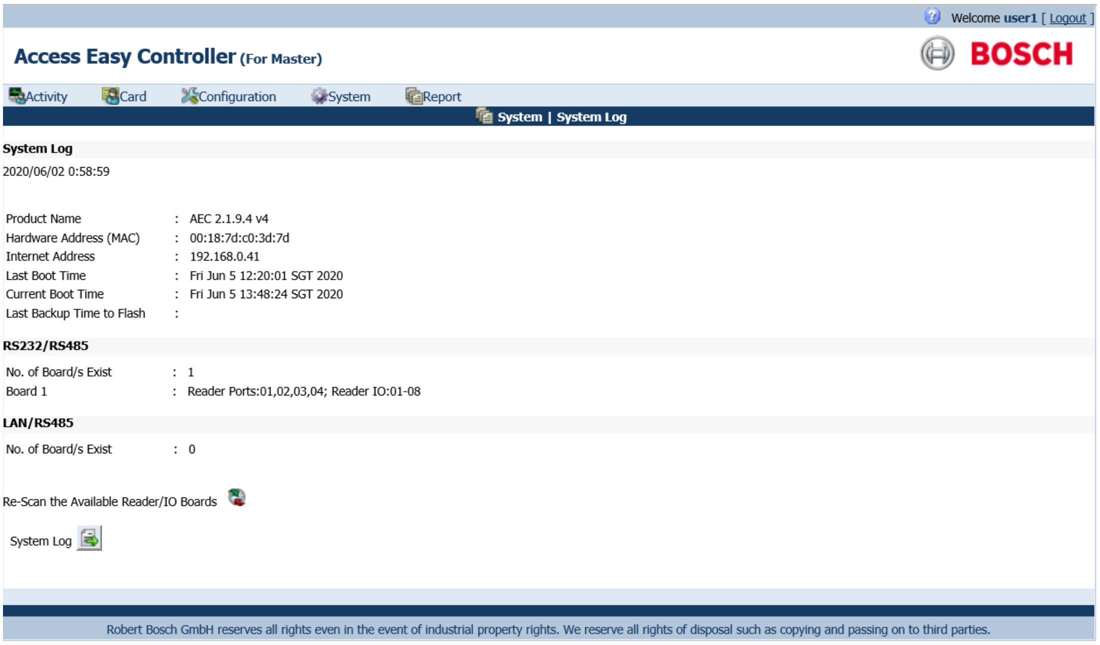
To configure the Web link for latest updates

The **Web link for latest updates** section allows you to configure the Internet link for the latest Access Easy Controller software updates.

1. Enter the Internet link in the **URL** text box of the **Web link for latest updates** section.
2. Click the save button to save the settings.

20.8 System Log

The **System Log** page allows you to view the information of the system. Click **System > System Log** menu and the screen below appears.



```
System Log
2020/06/02 0:58:59

Product Name                 :  AEC 2.1.9.4 v4
Hardware Address (MAC)       :  00:18:7d:c0:3d:7d
Internet Address             :  192.168.0.41
Last Boot Time               :  Fri Jun 5 12:20:01 SGT 2020
Current Boot Time            :  Fri Jun 5 13:48:24 SGT 2020
Last Backup Time to Flash    :

RS232/RS485
No. of Board/s Exist         :  1
Board 1                      :  Reader Ports:01,02,03,04; Reader IO:01-08

LAN/RS485
No. of Board/s Exist         :  0

Re-Scan the Available Reader/IO Boards

System Log
```

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.

You can find system information of the Access Easy Controller on this page.

- **Product Name**: version information of the firmware/software installed
- **Hardware Address (MAC)**: the hardware address of the controller
- **Internet Address**: IP address of the controller
- **Last Boot Time**: the previous time when the controller was restarted
- **Current Boot Time**: the most recent time when the controller was restarted
- **Last Backup Time to Flash**: last time when upload of settings and configurations, or panel software is done

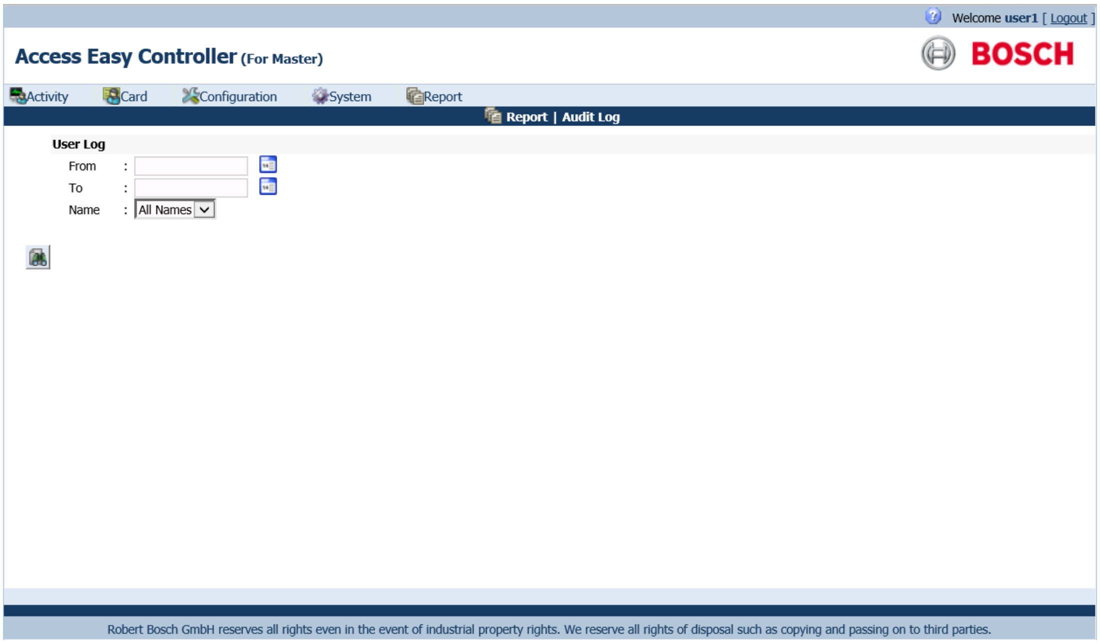
The **RS232/RS485** section provides information of how many panels are connected to the Access Easy Master via RS-232/RS-485 connection (**No. of Boards Exist** field) and the information and type of each board.

The **LAN/RS485** section provides information of how many boards are connected to the Access Easy Master via LAN connection (**No. of Boards Exist** field) and the information and type of each board.

You can also can re-scan the available reader/IO boards by clicking on the button. This will refresh the **System Log** page.

20.9 Audit Log

The system tracks user operations on the Access Easy for Master, and logs all the action performed by the user, such as manual control of any output, change settings for a cardholder, setting the date and time, and so on. Click **Report > Audit Log** menu to access the user log reports. The **Audit Log** page is shown as below:



User Log

From :

To :

Name : All Names

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.

To view the User Log

1. Choose the **From** date and **To** date, from the calendar picker.
2. Select the name from the **Name** drop-down list. If a particular user has been selected, the report will only show the operation of that user. If “All Names” is selected, the report will show all the actions performed by all users on the system.
3. Click the view report button to see a preview of the report.
4. Click **save as CSV or XSL** file to save the report in a CSV or XSL format in the PC.
5. Click the back button to return to the **Audit Log** page.

21 APPENDIX A Selecting Events, Devices and Cardholders for Reports

	Devices							***Cardholders***	
Events	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
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
Events	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
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

22 APPENDIX B Configuring Alarm Events

	Devices							***Cardholders***	
Events	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
Panel Tamper	x	x	x	x	x	x	x	x	
Panel AC Failure	x	x	x	x	x	x	x	x	
Alarm	x			x	x			x	
Door Forced Open	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
Access Denied - Timed APB	x	x	x					x	x
Access Denied - Wrong PIN	x	x	x					x	x
Invalid Card	x	x	x					x	
Invalid End Date	x	x	x					x	x
Exit Denied - Passback	x	x	x					x	x
Invalid Schedule	x	x	x					x	x
Invalid Start Date	x	x	x					x	x

23 APPENDIX C Activity Transactions

This appendix list the various Activity transactions found within each category.

23.1 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

23.2 Restore Activity

No	Transactions
1	Door Closed
2	Tamper Restored
3	Alarm Restored
4	Power Restored

23.3 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

23.4 Time Attendance

No	Transactions
1	Clock In
2	Clock Out

24 APPENDIX D 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, choose "Alarm" and "Alarm Restored".

Cardholders
All Cardholders option

For this scenario, never choose **Selected Cardholders Only** option for cardholders settings or **Selected Readers** or **All Readers** option for devices setting. These settings will result in no events that will meet the criteria, because the events for "Alarm" and "Alarm Restored" will never come with a cardholder's ID and it will never happen on a reader.

	Devices							***Cardholders***	
Events	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
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	
Events	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
Door Locked	x	x	x					x	
Door Unlocked	x	x	x					x	
Door Momentarily Unlocked	x	x	x					x	

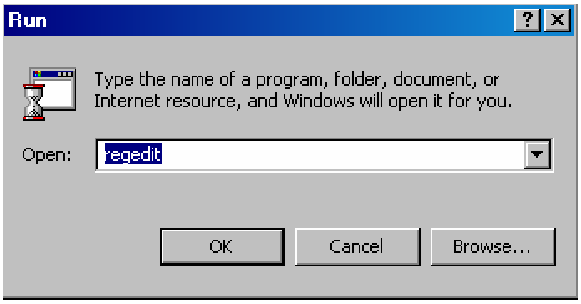
Door Locked By Schedule	x	x	x					x	
Door Unlocked By Schedule	x	x	x					x	
Turned On	x					x	x	x	
Turned Off	x					x	x	x	
Duration On	x					x	x	x	
Duration Off	x					x	x	x	
Turned On By Schedule	x					x	x	x	
Turned Off By Schedule	x					x	x	x	
Clock In	x	x	x					x	x
Clock Out	x	x	x					x	x

25 APPENDIX E Setting up a Timeserver

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.

25.1 For Windows 2000

1. Click Start Start button and select **Run** button.
2. Type “regedit” in the window.

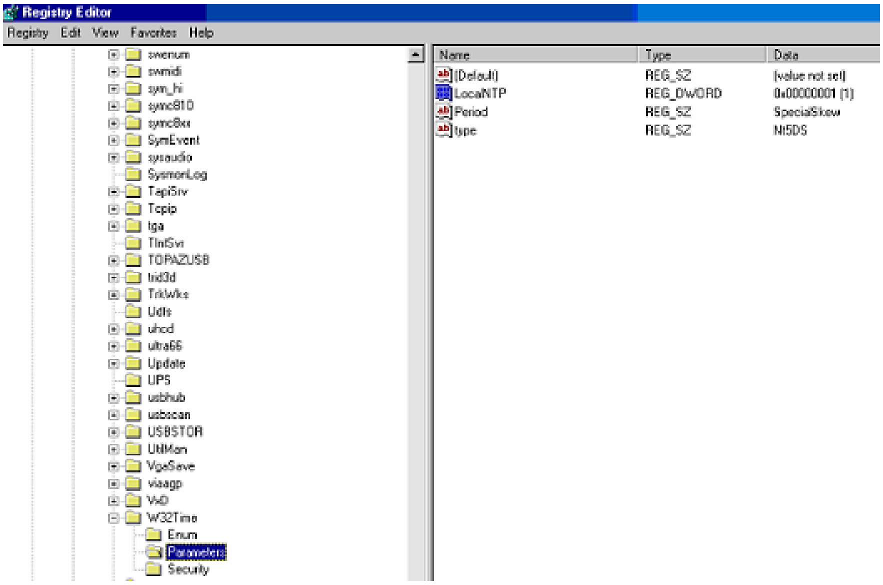


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

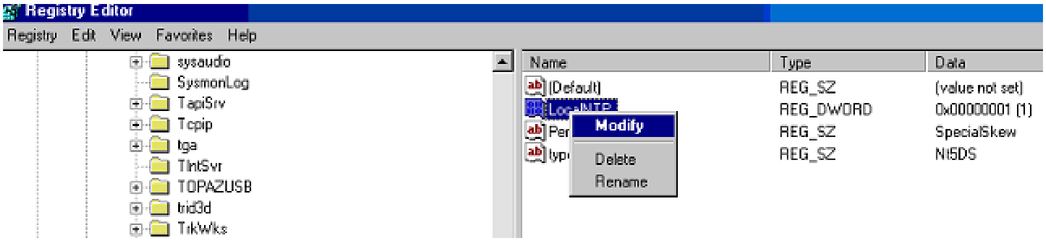
Open: regedit

3. Select HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/PARAMETERS.



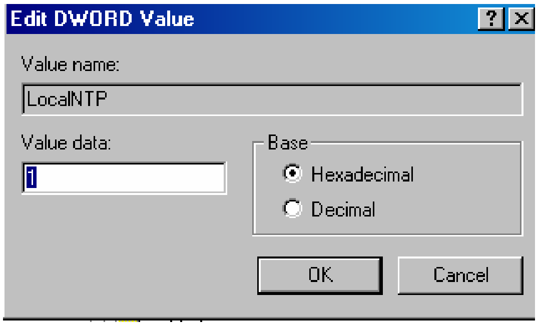
Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Period	REG_SZ	SpecialSkew
type	REG_SZ	Nt5DS

4. Right click “Local NTP” and select **Modify**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Per	REG_SZ	SpecialSkew
typ	REG_SZ	Nt5DS

5. Enter “1” for **Value data** field and click the **OK** button.

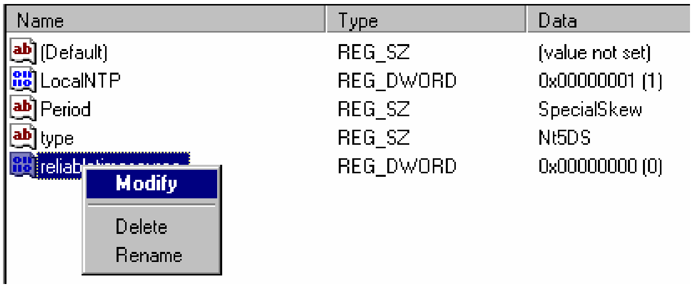


Value name: LocalNTP

Value data: 1

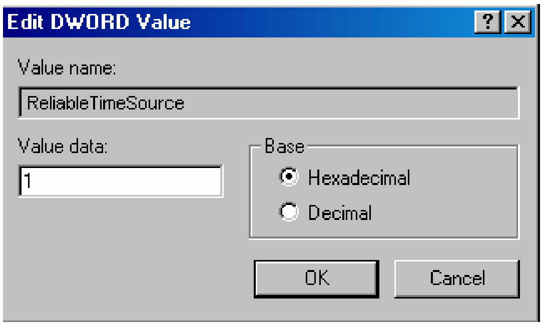
Base: ● Hexadecimal ○ Decimal

6. Right click “ReliableTimeSource” and select **Modify**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Period	REG_SZ	SpecialSkew
type	REG_SZ	Nt5DS
reliab	REG_DWORD	0x00000000 (0)

7. Enter “1” for **Value data** field and click the **OK** button.



Value name: ReliableTimeSource

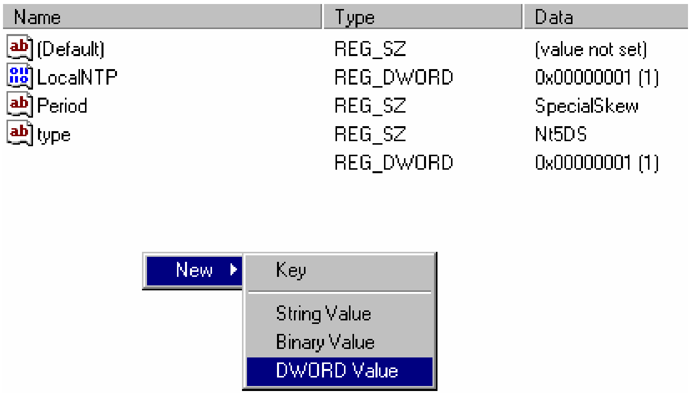
Value data: 1

Base: ● Hexadecimal ○ Decimal

Notice!

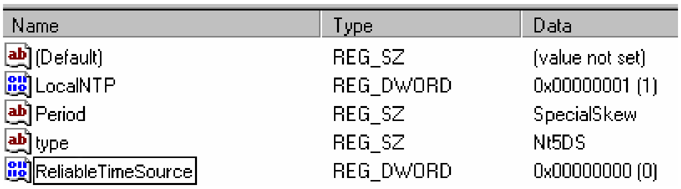
If HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/PARAMETERS doesn't contain the “ReliableTimeSource” settings, user will have to create one. Follow steps 8 to 9 otherwise proceed to step 10.

8. Right click on an empty space in the right panel and select **New/DWORD Value**.



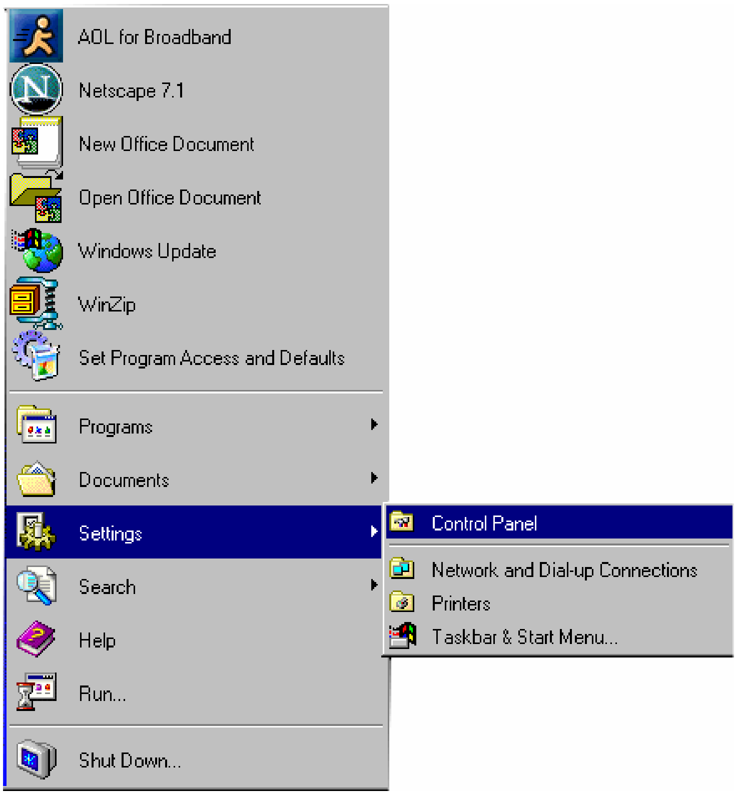
Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Period	REG_SZ	SpecialSkew
type	REG_SZ	Nt5DS
	REG_DWORD	0x00000001 (1)

9. Key in “ReliableTimeSource”.

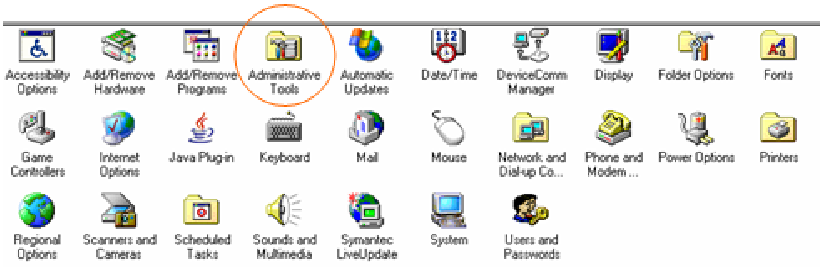


Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalNTP	REG_DWORD	0x00000001 (1)
Period	REG_SZ	SpecialSkew
type	REG_SZ	Nt5DS
ReliableTimeSource	REG_DWORD	0x00000000 (0)

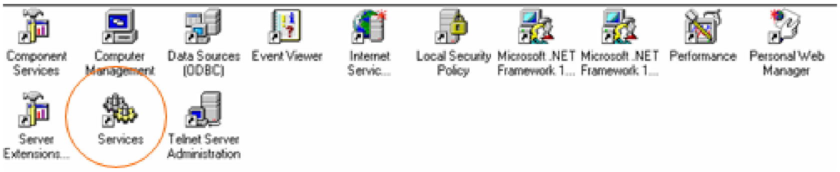
10. Click the Start Start button and select **Settings > Control Panel**.



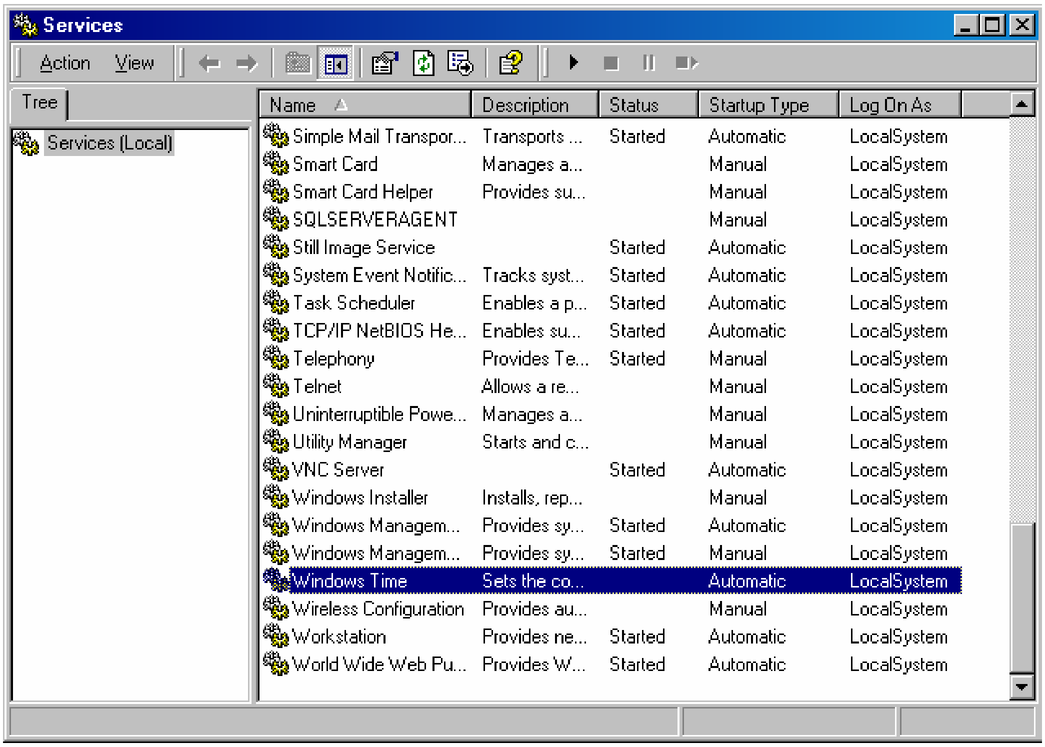
11. Double click on **Administrative Tools** icon.



12. Double click on **Services** icon.

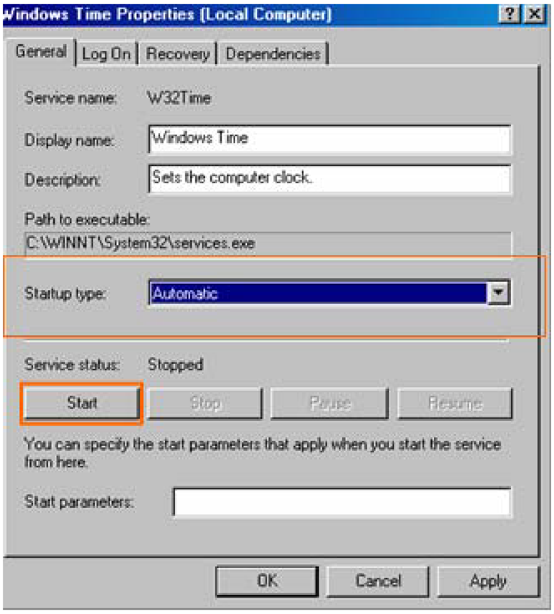


13. Scroll down to “Windows Time” and double click it.



Name	Description	Status	Startup Type	Log On As
Simple Mail Transpor...	Transports ...	Started	Automatic	LocalSystem
Smart Card	Manages a...		Manual	LocalSystem
Smart Card Helper	Provides su...		Manual	LocalSystem
SQLSERVERAGENT			Manual	LocalSystem
Still Image Service		Started	Automatic	LocalSystem
System Event Notific...	Tracks syst...	Started	Automatic	LocalSystem
Task Scheduler	Enables a p...	Started	Automatic	LocalSystem
TCP/IP NetBIOS He...	Enables su...	Started	Automatic	LocalSystem
Telephony	Provides Te...	Started	Manual	LocalSystem
Telnet	Allows a re...		Manual	LocalSystem
Uninterruptible Powe...	Manages a...		Manual	LocalSystem
Utility Manager	Starts and c...		Manual	LocalSystem
VNC Server		Started	Automatic	LocalSystem
Windows Installer	Installs, rep...		Manual	LocalSystem
Windows Managem...	Provides sy...	Started	Automatic	LocalSystem
Windows Managem...	Provides sy...	Started	Manual	LocalSystem
Windows Time	Sets the co...		Automatic	LocalSystem
Wireless Configuration	Provides au...		Manual	LocalSystem
Workstation	Provides ne...	Started	Automatic	LocalSystem
World Wide Web Pu...	Provides W...	Started	Automatic	LocalSystem

14. Select “Automatic” from the **Startup type** drop-down list and click the **Start** button.



Service name: W32Time

Display name: Windows Time

Description: Sets the computer clock.

Path to executable:
C:\WINNT\System32\services.exe

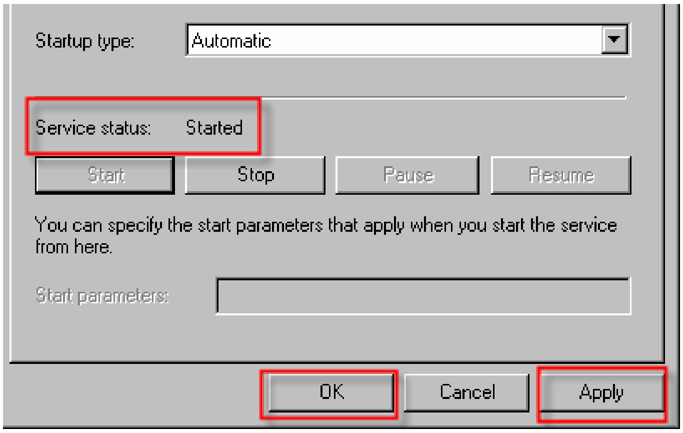
Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

15. Once **Service status** is “Started”, click the **Apply** and **OK** button to exit.



Startup type: Automatic

Service status: Started

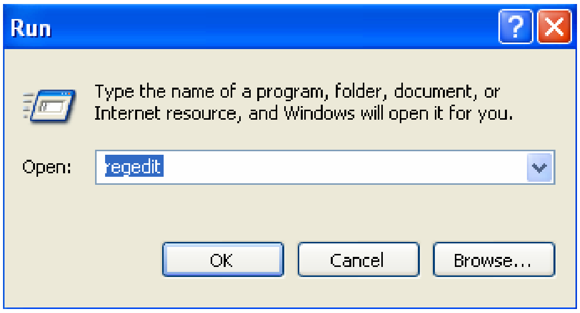
You can specify the start parameters that apply when you start the service from here.

Start parameters:

16. Reboot PC.

25.2 For Windows XP Professional

1. Click Start start button and select the **Run** button.
2. Type “regedit” in the window.

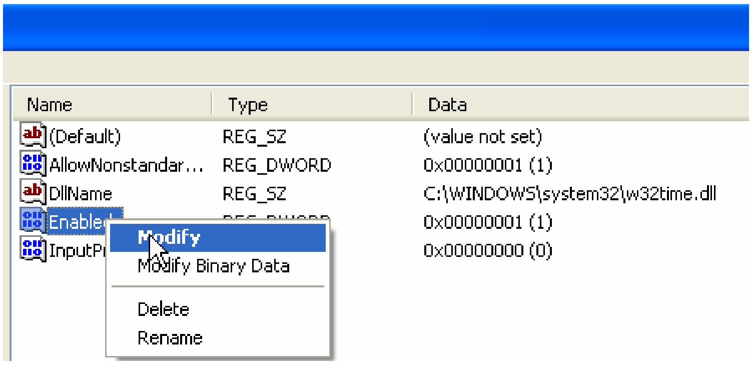


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

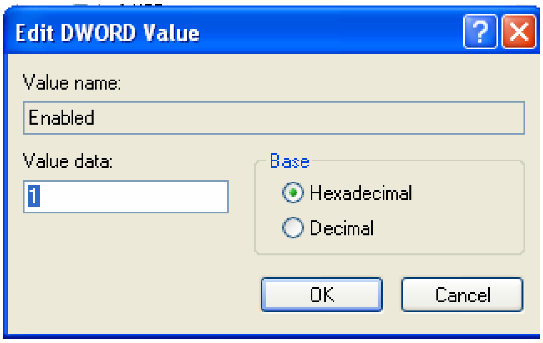
Open: regedit

3. Select HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/TIMEPROVIDERS/NTPSERVER.
4. Right click “Enabled” and select **Modify**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowNonstandar...	REG_DWORD	0x00000001 (1)
DllName	REG_SZ	C:\WINDOWS\system32\w32time.dll
Enable	REG_DWORD	0x00000001 (1)
InputP		0x00000000 (0)

5. Enter “1” for the **Value data** field and click the **OK** button.



Edit DWORD Value

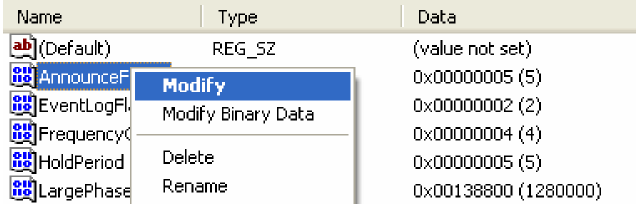
Value name: Enabled

Value data: 1

Base: ● Hexadecimal ○ Decimal

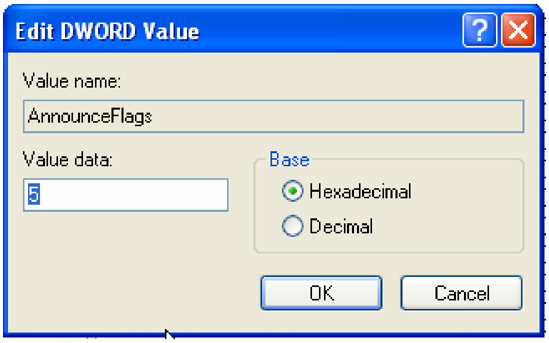
6. Select HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/CONFIG

7. Right click “AnnounceFlags” and select **Modify**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
AnnounceF		0x00000005 (5)
EventLogFl		0x00000002 (2)
Frequency(		0x00000004 (4)
HoldPeriod		0x00000005 (5)
LargePhase		0x00138800 (1280000)

8. Enter “5” for the **Value data** field and click the **OK** button.



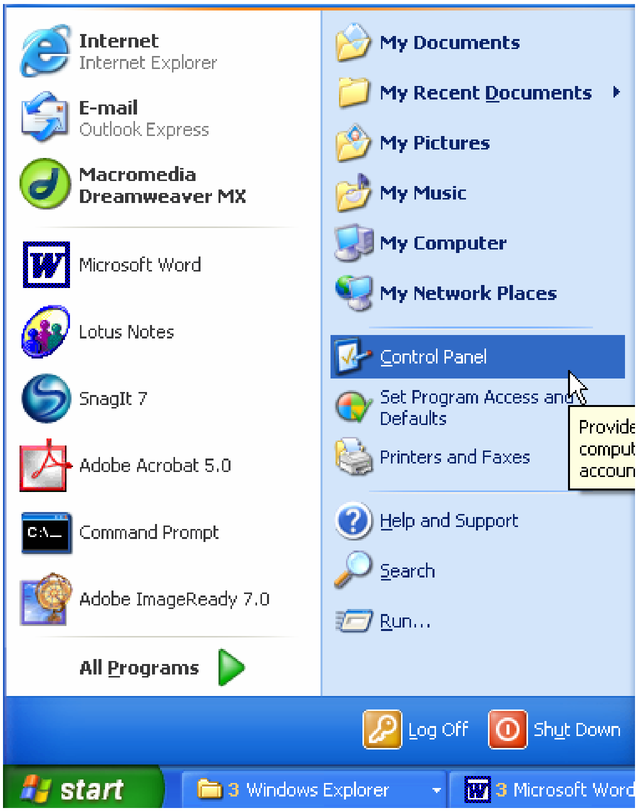
Edit DWORD Value

Value name: AnnounceFlags

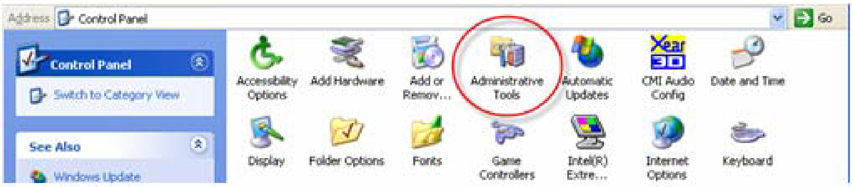
Value data: 5

Base: ● Hexadecimal ○ Decimal

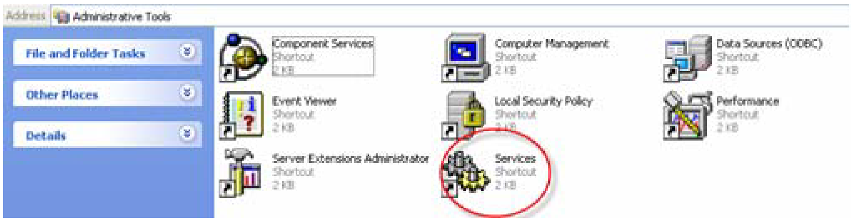
9. Click the Start start button and select **Control Panel**.



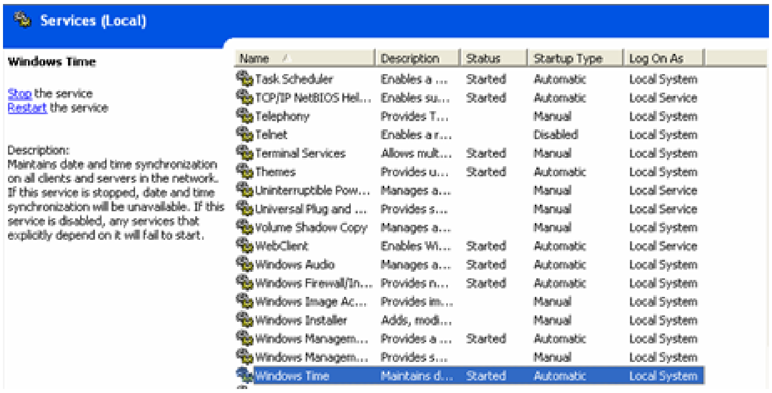
10. Double click on **Administrative Tools** icon.



11. Double click on **Services** icon.



12. Scroll down to “Windows Time”.


Services (Local)

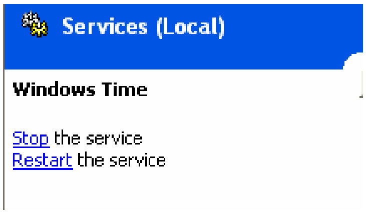
Windows Time

Stop the service
Restart the service

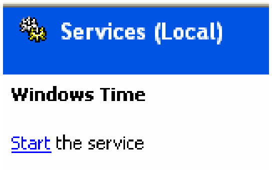
Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	Local Service
Telephony	Provides T...		Manual	Local System
Telnet	Enables a r...		Disabled	Local System
Terminal Services	Allows mult...	Started	Manual	Local System
Themes	Provides u...	Started	Automatic	Local System
Uninterruptible Pow...	Manages a...		Manual	Local Service
Universal Plug and ...	Provides s...		Manual	Local Service
Volume Shadow Copy	Manages a...		Manual	Local System
WebClient	Enables Wi...	Started	Automatic	Local Service
Windows Audio	Manages a...	Started	Automatic	Local System
Windows Firewall/In...	Provides n...	Started	Automatic	Local System
Windows Image Ac...	Provides im...		Manual	Local System
Windows Installer	Adds, modi...		Manual	Local System
Windows Managem...	Provides a ...	Started	Automatic	Local System
Windows Managem...	Provides s...		Manual	Local System
Windows Time	Maintains d...	Started	Automatic	Local System

13. Select **Stop the service**.



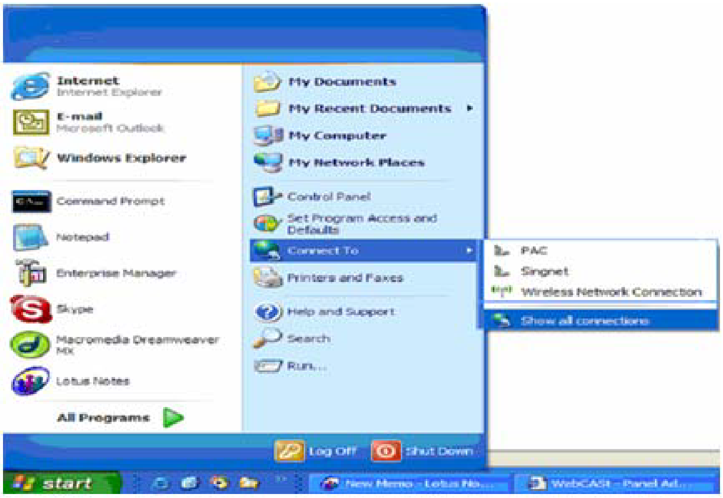
14. Once service is stopped, click **Start the service**.



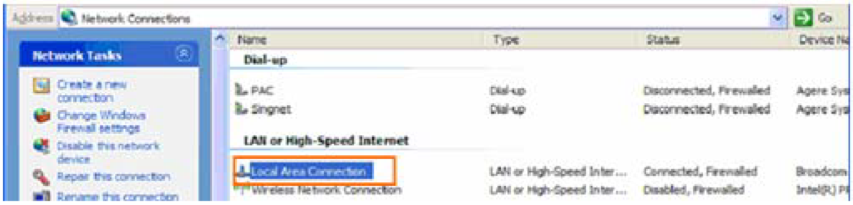
15. Reboot PC.

Notice!
If user is using windows XP professional with service pack 2 for the timeserver, user has to bypass the firewall protection. Follow steps 1 to 9.

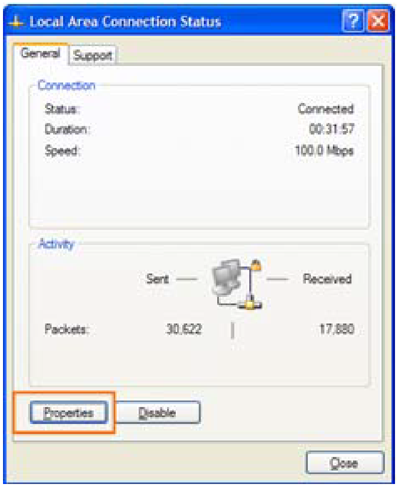
1. From the desktop, click the Start button and look for **Connect To** and select **Show all connections**.



2. Click on the **Local Area Connection**.



3. The following screen will appear, click on the **Properties** button.



Connection

Status: Connected

Duration: 00:31:57

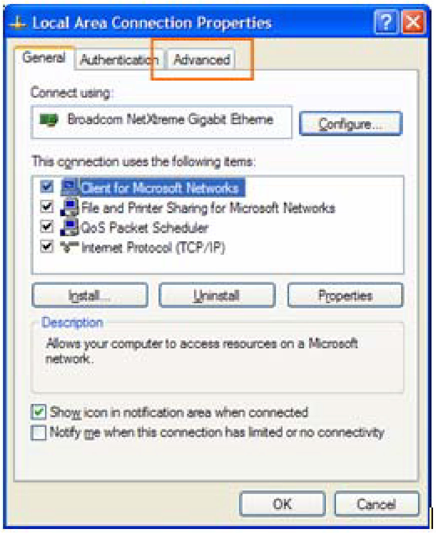
Speed: 100.0 Mbps

Activity

Sent — — Received

Packets: 30,622 | 17,880

4. Click on **Advanced** tab.



Connect using:

Broadcom NetXtreme Gigabit Etherne

This connection uses the following items:

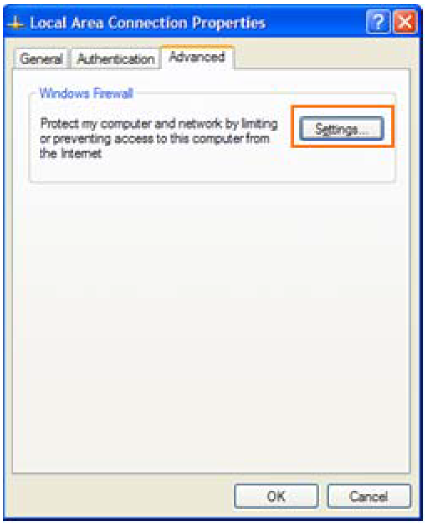
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected
☐ Notify me when this connection has limited or no connectivity

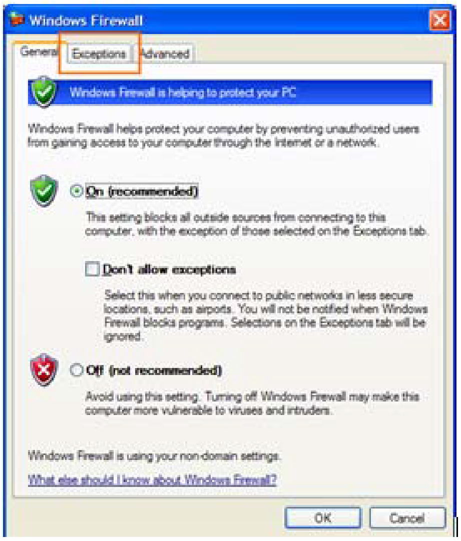
5. Click on **Settings** button.



Windows Firewall

Protect my computer and network by limiting or preventing access to this computer from the Internet

6. The below screen will appears, click on **Exceptions** tab.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

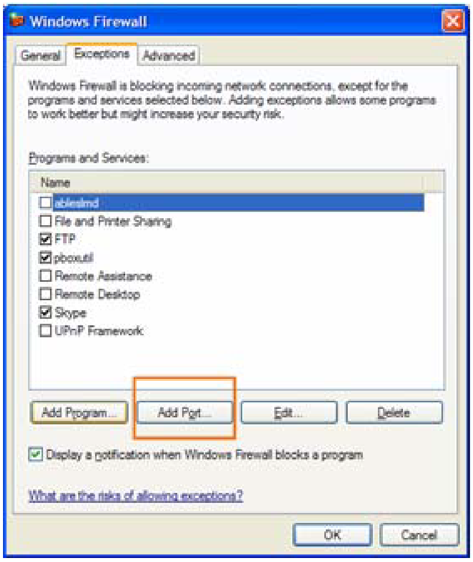
○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Windows Firewall is using your non-domain settings.

What else should I know about Windows Firewall?

7. Click on the **Add Port** button.



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

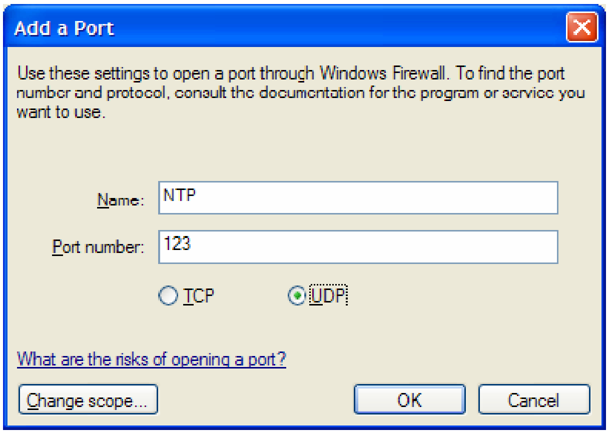
Programs and Services:

Name
□ ablesImd
□ File and Printer Sharing
☑ FTP
☑ pboxutil
□ Remote Assistance
□ Remote Desktop
☑ Skype
□ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

8. Enter the following data in the following fields.
Name: “NTP”
Port number: “123”



Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: NTP

Port number: 123

○ TCP ● UDP

What are the risks of opening a port?

9. Click the **OK** button to save the settings.

26 APPENDIX F Initial Setup To Access Easy Controller

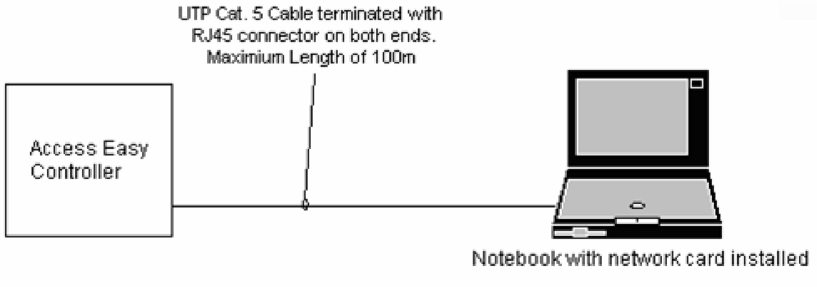
Before connection is made to Access Easy for Master, there are few conditions that must be taken into consideration. They are:

1. If the central monitoring computer (CMC) is not connected to a network, and acts as a stand-alone.
2. If the CMC is connected to a Network.

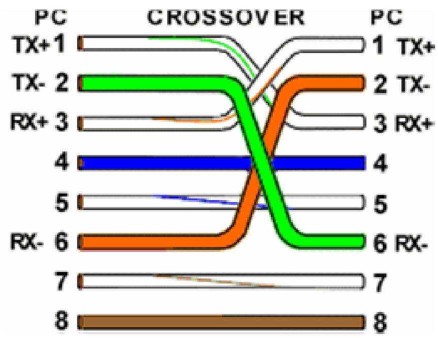
For case 1, having the CMC as a stand-alone unit, either IP address for the Access Easy for Master or CMC can be changed to suit each other.

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.

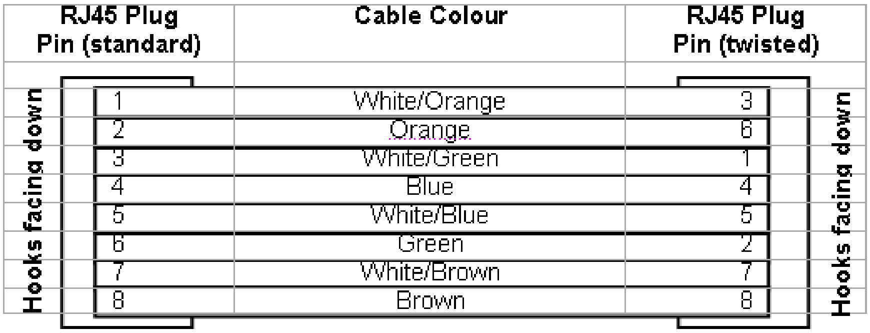
Connect the Access Easy Controller server and notebook using the industrial standard UTP Category 5 cable as shown below.


UTP Cat. 5 Cable terminated with RJ45 connector on both ends. Maximium Length of 100m
Access Easy Controller
Notebook with network card installed

Notice!
The cable has to be terminated and polarized 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 color 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

Hooks facing down
Hooks facing down

The individual conductors should be arranged as indicated above, taking reference to the pin numbers on the left (standard).

26.1 Procedure to Set the IP Address of Computer

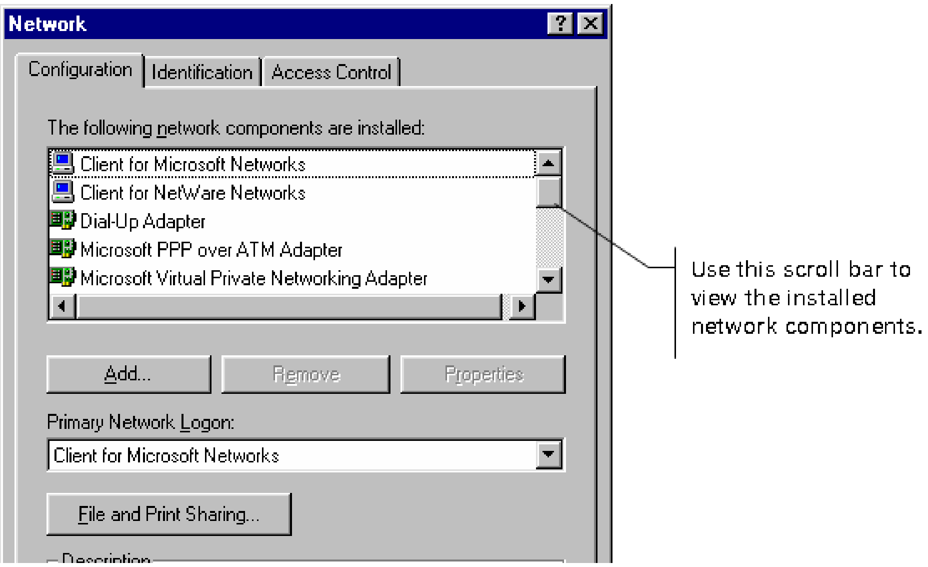
This section provides procedure to set the IP address for the PC and Macintosh.

26.1.1 For PC Users

Follow through the procedures to set the IP Address of the PC.

Notice!
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 Start button, followed by Settings | Control Panel.
2. Double-click on the Network icon, the Network dialog box appears.



Network

Configuration | Identification | Access Control

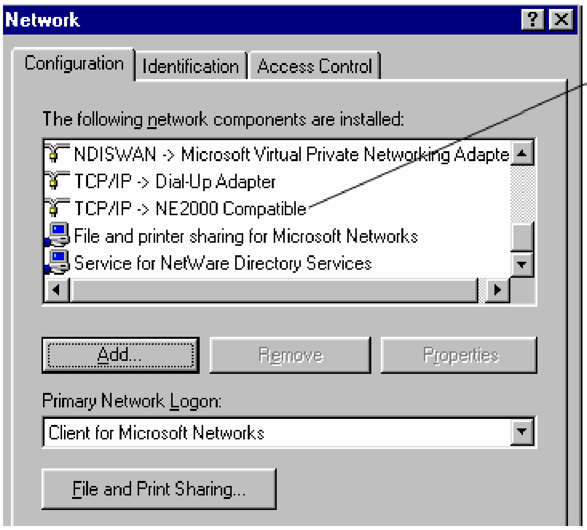
The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- Dial-Up Adapter
- Microsoft PPP over ATM Adapter
- Microsoft Virtual Private Networking Adapter

Primary Network Logon: Client for Microsoft Networks

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.



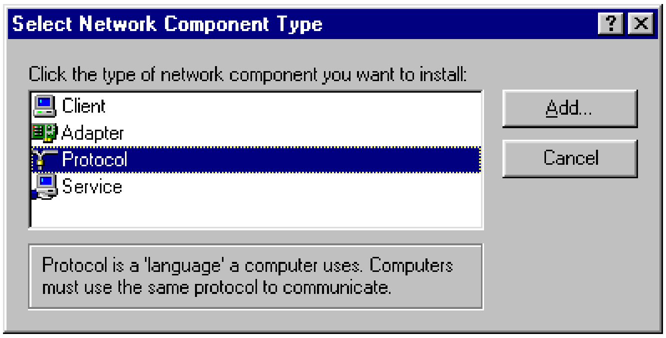
The following network components are installed:

- NDISWAN -> Microsoft Virtual Private Networking Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> NE2000 Compatible
- File and printer sharing for Microsoft Networks
- Service for NetWare Directory Services

Primary Network Logon: Client for Microsoft Networks

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.

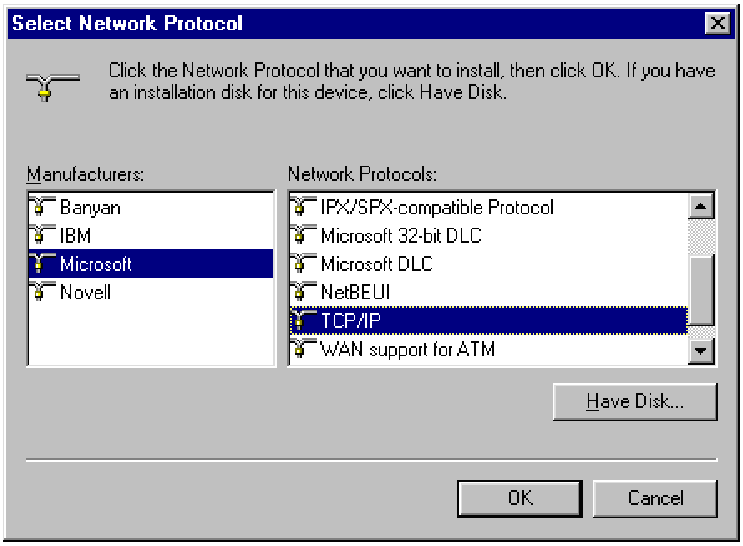


Click the type of network component you want to install:

- Client
- Adapter
- Protocol
- Service

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

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.



Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:

- Banyan
- IBM
- Microsoft
- Novell

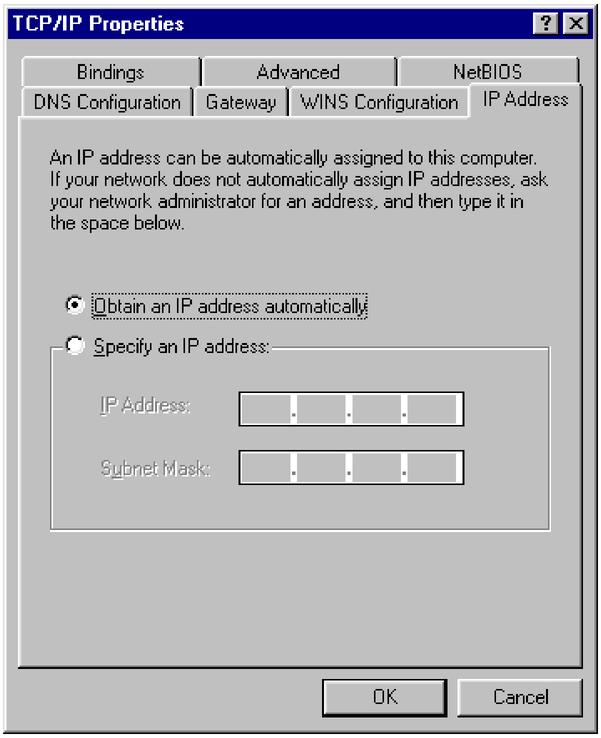
Network Protocols:

- IPX/SPX-compatible Protocol
- Microsoft 32-bit DLC
- Microsoft DLC
- NetBEUI
- TCP/IP
- WAN support for ATM

7. Click on the **OK** button to proceed with the component installation. Follow through the on-screen instruction to complete.

Notice!
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.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

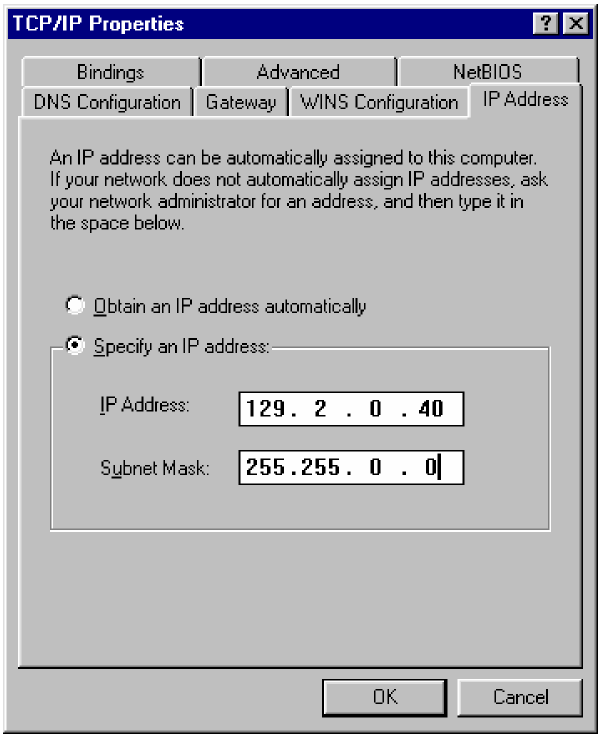
○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

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.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 129. 2 . 0 . 40

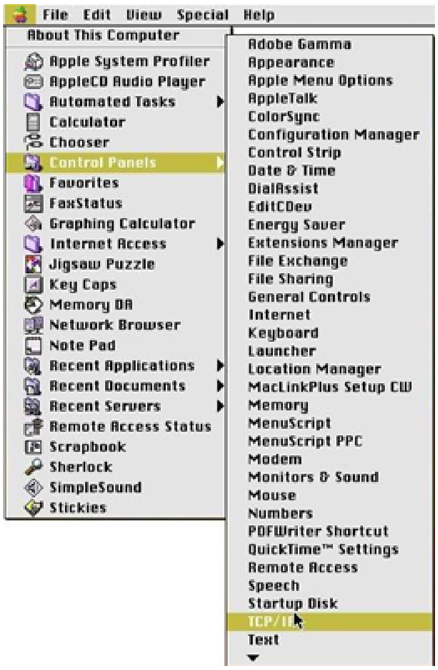
Subnet Mask: 255.255. 0 . 0

11. Click on **O**K button.
12. Reboot the computer in order for the setting to take effect.

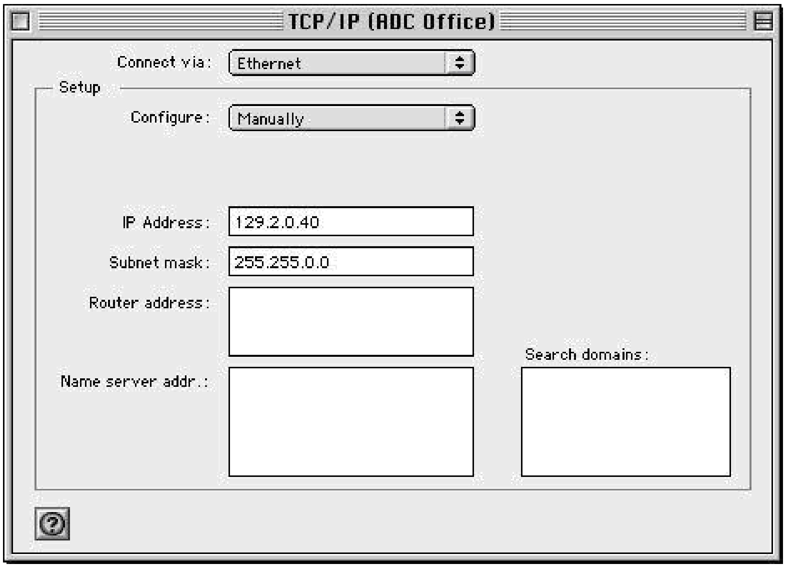
26.2 For Macintosh Users

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.



3. Enter the **IP Address** and the **Subnet mask** fields as shown below. This will be the Macintosh's IP address for this initial set-up.



TCP/IP (ADC Office)

Connect via: Ethernet

Setup

Configure: Manually

IP Address: 129.2.0.40

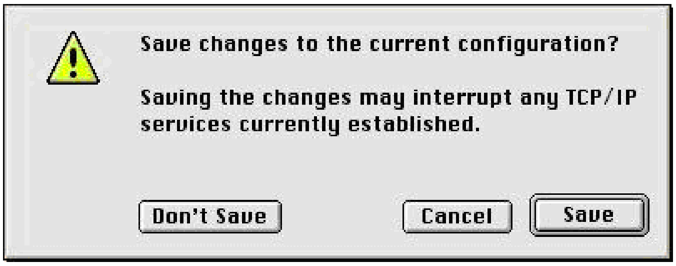
Subnet mask: 255.255.0.0

Router address:

Name server addr.:

Search domains:

4. Click on the **Save** button when prompted. This message will appear when you attempt to close the dialog box.



Save changes to the current configuration?

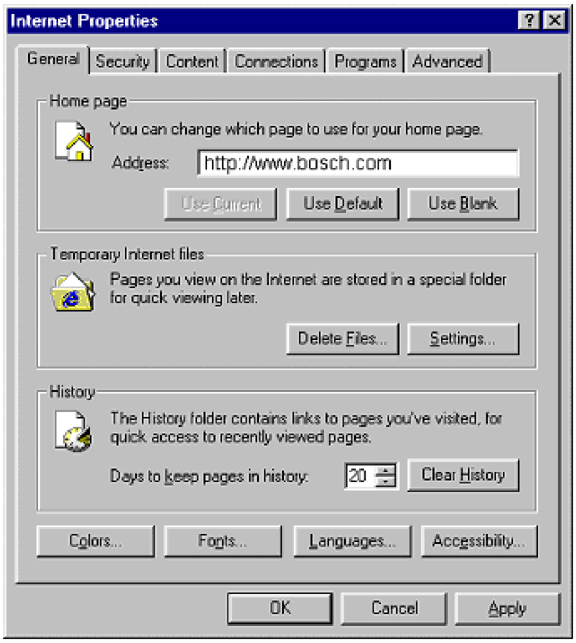
Saving the changes may interrupt any TCP/IP services currently established.

26.3 Settings to be Made to the Web Browser

26.3.1 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.



Internet Properties

Home page

You can change which page to use for your home page.

Address: http://www.bosch.com

Temporary Internet files

Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

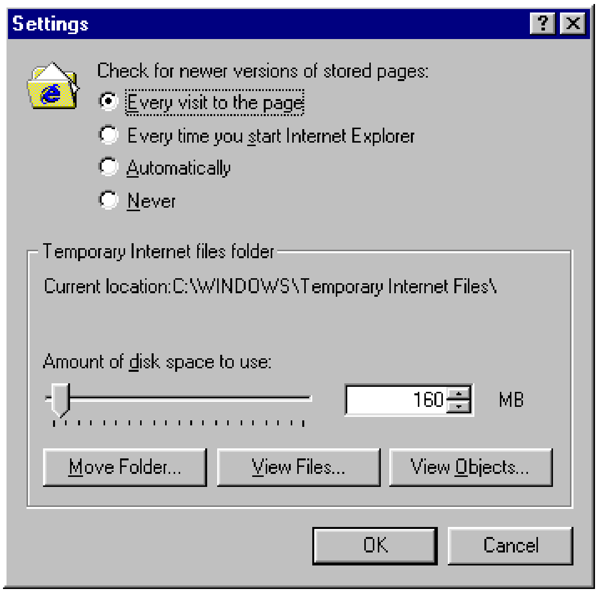
Days to keep pages in history: 20

2. If you wish to show the Access Easy for Master **Login** page every time you activate your web browser program, then change the home page **Address** field to the IP address of Access Easy for Master. Otherwise, leave it as what was defined previously.

Notice!
The Network Administrator should assign the IP address if the Access Easy for Master is to be connected to the network.

3. Under the **Temporary Internet files** section, click on the **Settings** button to go into the next dialog box. Confirm that the **Check for newer versions of stored pages** radio button is set to **Every visit to the page** option, 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.



Settings

Check for newer versions of stored pages:

● Every visit to the page

○ Every time you start Internet Explorer

○ Automatically

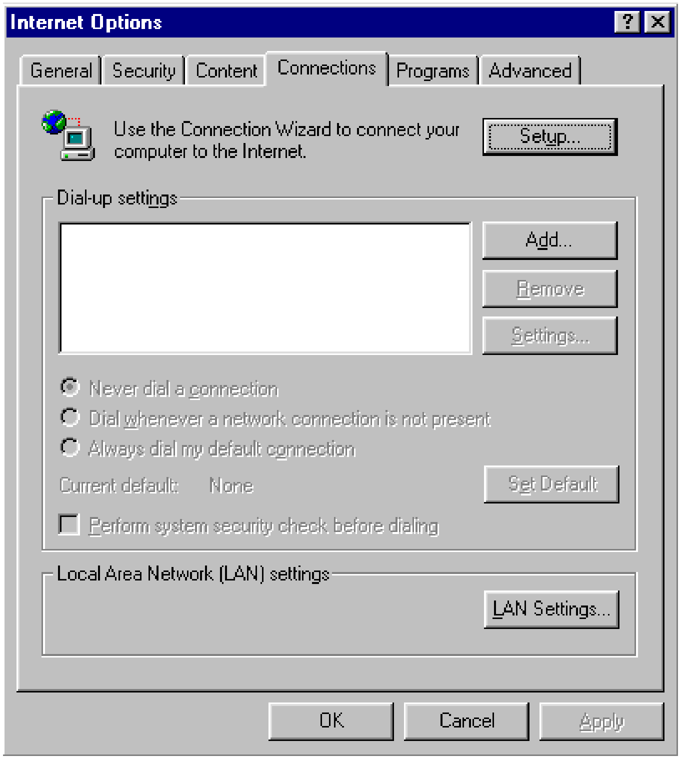
○ Never

Temporary Internet files folder

Current location:C:\WINDOWS\Temporary Internet Files\

Amount of disk space to use: 160 MB

4. Click on the **OK** button to exit to previous dialog box.



Internet Options

Use the Connection Wizard to connect your computer to the Internet.

Dial-up settings

● Never dial a connection

○ Dial whenever a network connection is not present

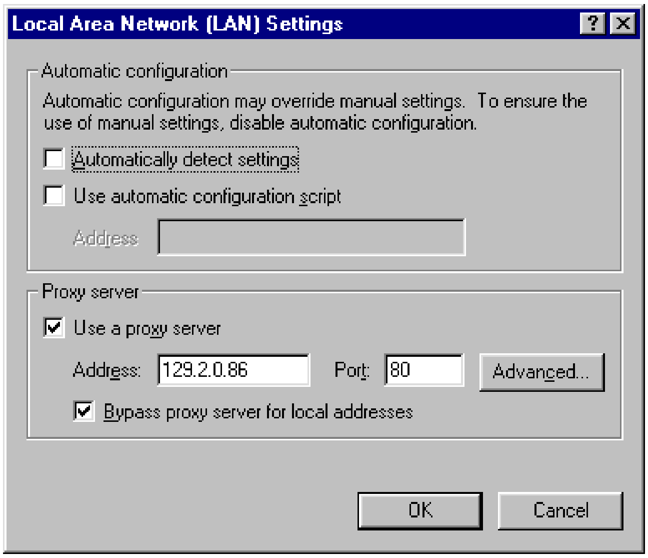
○ Always dial my default connection

Current default: None

□ Perform system security check before dialing

Local Area Network (LAN) settings

5. Under the **Connections** tab, click on the **LAN Settings** button The **LAN Settings** dialog box appears.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

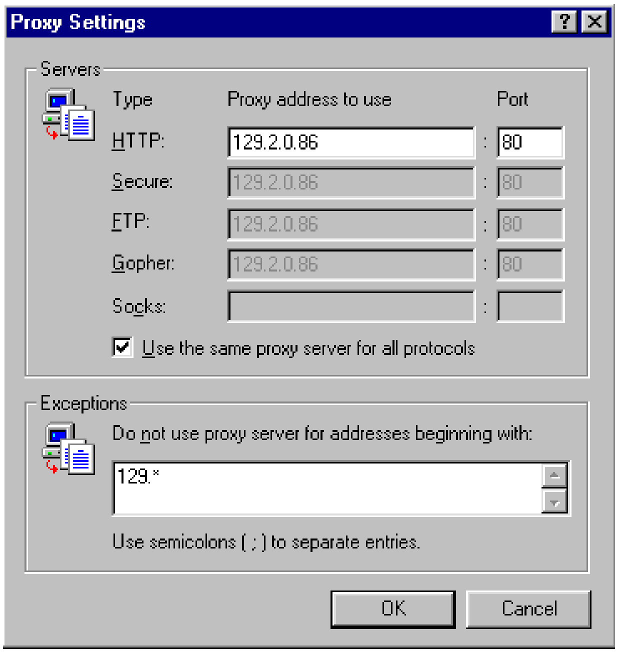
Proxy server

☑ Use a proxy server

Address: 129.2.0.86 Port: 80

☑ Bypass proxy server for local addresses

6. Click on the **Advanced** button. The **Proxy Settings** dialog box appears.



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	129.2.0.86	80
Secure:	129.2.0.86	80
FTP:	129.2.0.86	80
Gopher:	129.2.0.86	80
Socks:		

☑ Use the same proxy server for all protocols

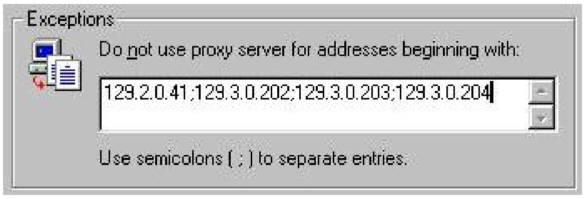
Exceptions

Do not use proxy server for addresses beginning with:

129.*

Use semicolons (;) to separate entries.

7. Enter the default IP address of the Access Easy for Master in the **Exceptions** list box as shown above.
8. If the IP address of the Access Easy for Master(s) has been assigned, continue to enter the address in the **Exceptions** list box, separating each address with a semicolon “;”. The next screen-capture shows the default IP address for Access Easy for Master, and three assigned Access Easy for Master IP addresses: 129.3.0.202, 129.3.0.203 and 129.3.0.204.



Exceptions

Do not use proxy server for addresses beginning with:

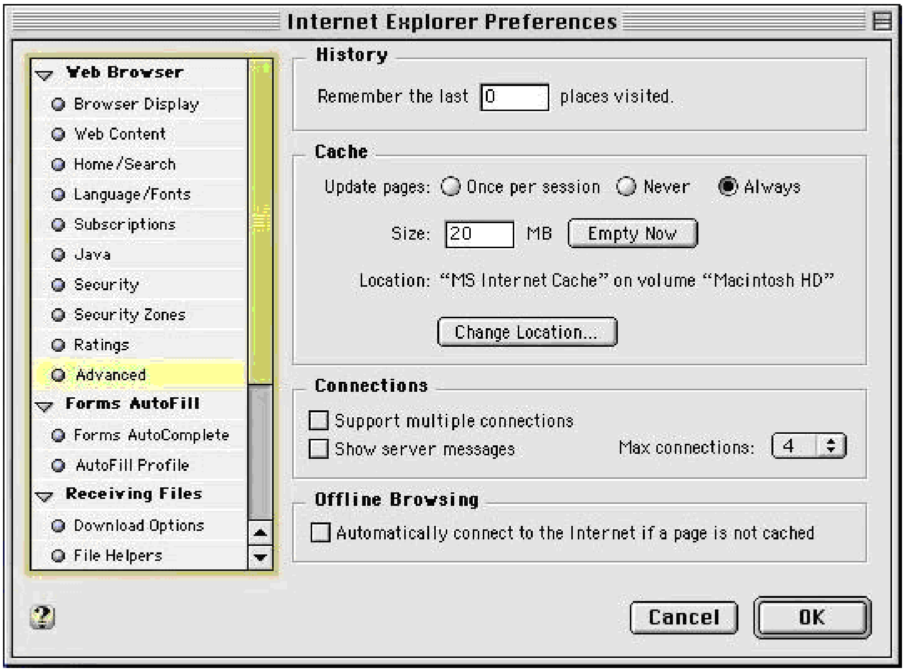
129.2.0.41;129.3.0.202;129.3.0.203;129.3.0.204

Use semicolons (;) to separate entries.

9. Click on the **OK** button repeatedly to exit the **Internet Options** setting.
10. Close the **Control Panel**.

26.3.2 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 “Always” option for the **Update pages** radio buttons for the **Cache** section.



History

Remember the last 0 places visited.

Cache

Update pages: ○ Once per session ○ Never ● Always

Size: 20 MB

Location: “MS Internet Cache” on volume “Macintosh HD”

Connections

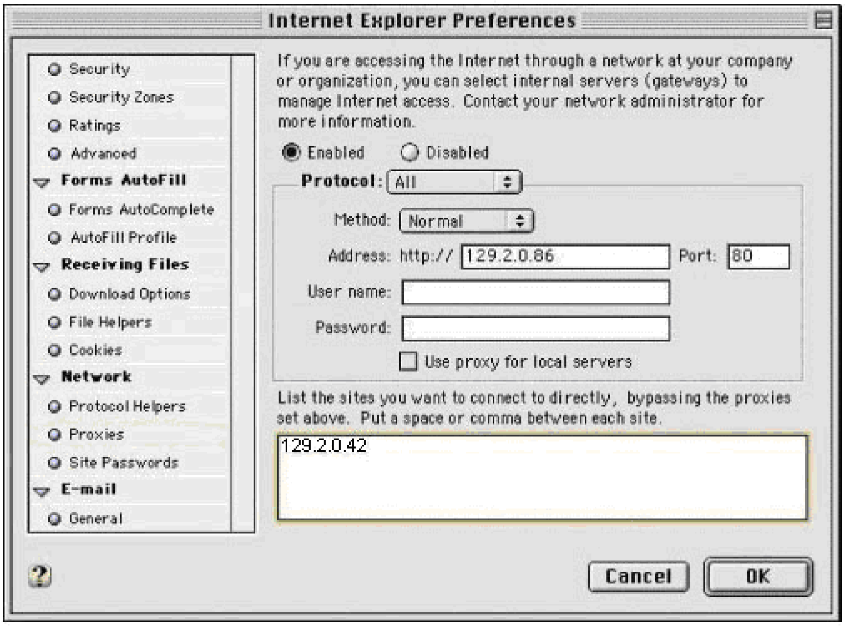
□ Support multiple connections

□ Show server messages Max connections: 4

Offline Browsing

□ Automatically connect to the Internet if a page is not cached

5. Scroll down the listing to look for **Proxies** item.



If you are accessing the Internet through a network at your company or organization, you can select internal servers (gateways) to manage Internet access. Contact your network administrator for more information.

● Enabled ○ Disabled

Protocol: All

Method: Normal

Address: http:// 129.2.0.86 Port: 80

User name:

Password:

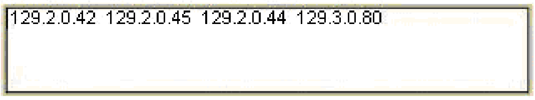
□ Use proxy for local servers

List the sites you want to connect to directly, bypassing the proxies set above. Put a space or comma between each site.

129.2.0.42

6. Enter the Access Easy for Master default IP address into the list box as shown above. IP addresses entered here will bypass the proxies and connect directly.

7. If the IP address of the Access Easy for Master(s) has been assigned, continue to enter the address in the field, separating each address with a space or a comma “,”. The screen-capture shows the default IP address for Access Easy Controller and three assigned Access Easy for Master IP addresses: 129.2.0.45, 129.2.0.44, and 129.3.0.80.



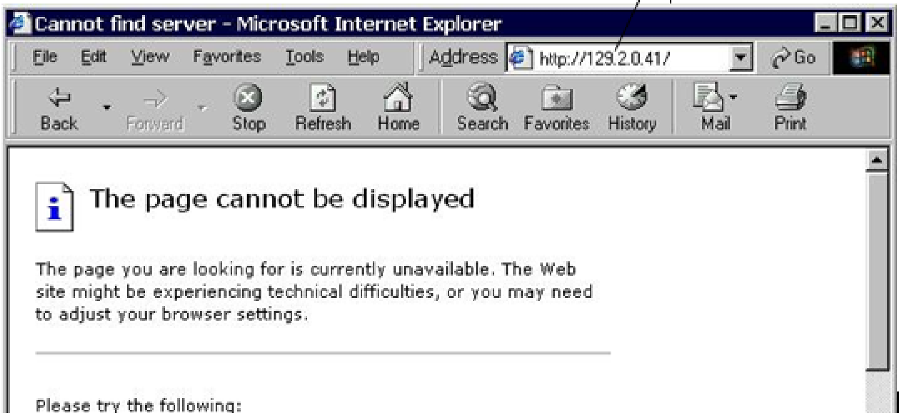
129.2.0.42 129.2.0.45 129.2.0.44 129.3.0.80

8. Click on the **OK** button to close the dialog box.

With this settings done, we can proceed to access the Access Easy for Master.

Now run the web browser program from Windows /Macintosh. Enter the Access Easy for Master default URL address as shown.

Notice!
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.



Address: http://129.2.0.41/

The page cannot be displayed

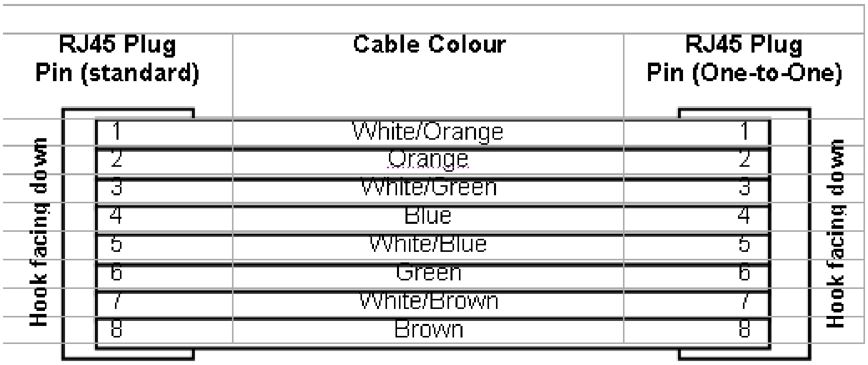
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

Enter default URL Address for Access Easy for Master

1. Press the **Enter** key or click on the Go button. This should bring you to the Access Easy for Master **User Login** page.
2. Proceed with the login (see the following NOTICE).

Notice!
If the Access Easy Controller is connected to the CMC via a hub, as in a network configuration, the UTP Cat. 5 cable connecting the Access Easy Controller and the hub must be polarized 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

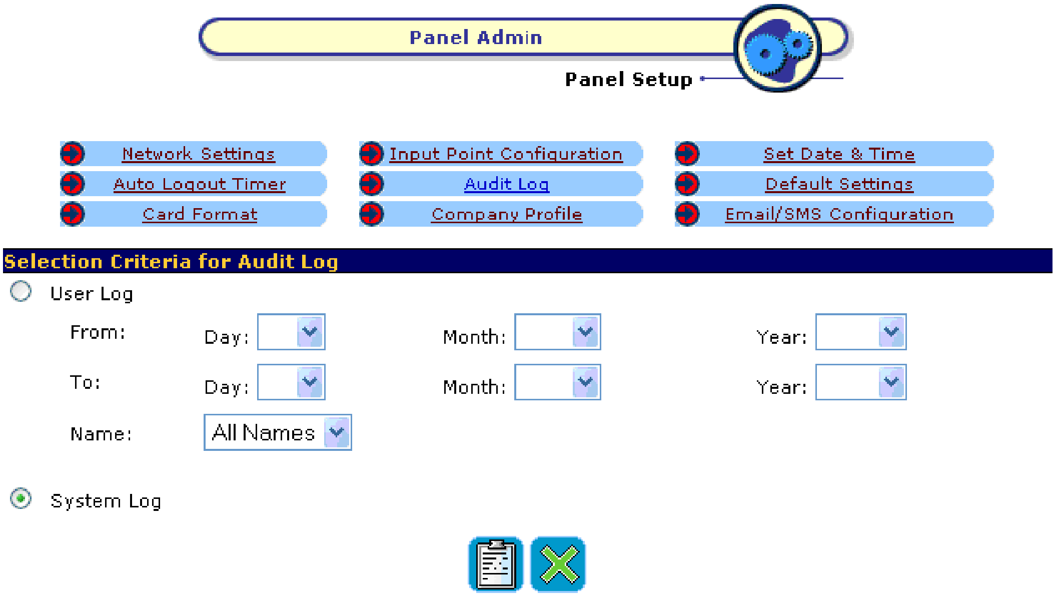
26.4 Setting the Access Easy Controller IP Address Through Address Resolution Protocol (ARP)

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 customized 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 follow the steps as shown on the following page:

Click on **Panel Admin** link from the home page of the Access Easy for Master. Click on **Panel Setup** on the left panel menu selection. Click on **Audit Log** link to bring you to the page as shown in the following.



Selection Criteria for Audit Log

○ User Log

From: Day: Month: Year:

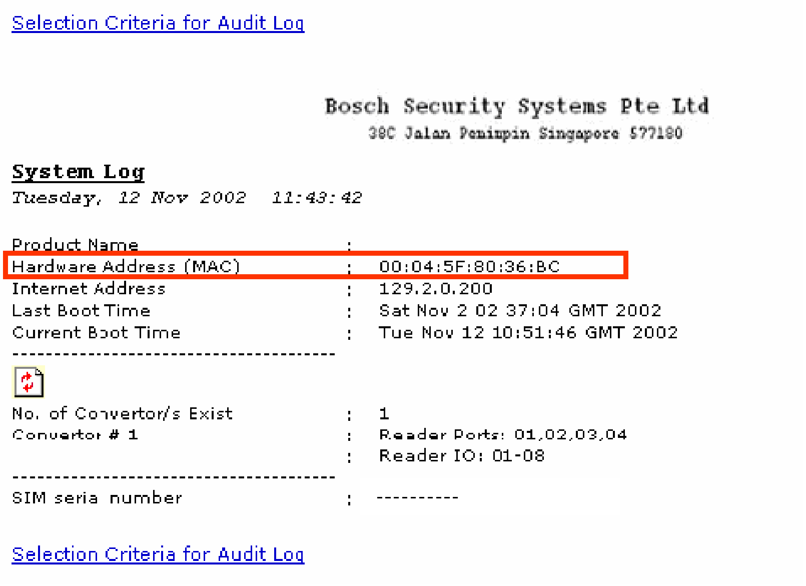
To: Day: Month: Year:

Name: All Names

● System Log

Check the **System Log** radio button, and click the list button to show the report.

The following show 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 Pemimpin 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 Convertor/s Exist              :   1
Convertor # 1                         :   Reader Ports: 01,02,03,04
                                      :   Reader IO: 01-08
----------------------------------------
SIM seria number                      :   ----------
```

Selection Criteria for Audit Log

With the MAC address, we could now use “arp” to change the IP address of the Access Easy for Master. 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 for Master> <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 for Master 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 for Master> <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 for Master 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 for Master> <mac address of your Access Easy Controller > temp
ping <new address you have just set>

For example, if you want to change the address of your Access Easy for Master 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 rebooted. After it has rebooted, it will resume operation using the new IP address that you have set.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

202106240836