# Table of Contents

**Part I Introduction**  
1. Access Control ................................................................. 2  
2. Terminology ........................................................................... 3  
3. Copyright and version .......................................................... 5

**Part II Part One - Getting Started**  
1. Software Basics ........................................................................ 6  
   - Logging In ............................................................................. 6  
   - The Main Screen ................................................................. 7  
2. Quick how to guide ............................................................... 10  
   - Add or Delete a User ............................................................ 10  
   - Create an Access Group ....................................................... 11

**Part III Part Two - Using the System**  
1. Setup .................................................................................. 14  
   - Users .................................................................................. 14  
     - Insert/Edit Users ............................................................... 18  
     - Bulk Add Users ............................................................... 19  
   - Access Groups ................................................................. 20  
   - Timezones .......................................................................... 22  
   - Holidays ............................................................................ 24  
   - Daylight Savings .............................................................. 25  
   - Change Password ............................................................ 26  
   - Devices ............................................................................. 26  
     - Doors ............................................................................... 27  
     - Floors ............................................................................ 28  
     - Areas ............................................................................... 29  
     - Parking ........................................................................... 31  
   - Reports ............................................................................... 33  
     - System Data ..................................................................... 34  
     - History ........................................................................... 35  
2. Administration ....................................................................... 38  
   - Backup and Restore ........................................................... 38  
   - Operators .......................................................................... 39  
   - Printer Setup ...................................................................... 42  
   - Set System Time ............................................................... 43  
   - Workstation Settings ........................................................ 44  
   - Email Alarms ..................................................................... 45  
   - Set Display Font .............................................................. 46

**Part IV Part Three - Setting Up the System**  
1. Hardware ........................................................................... 47  
   - Locations .......................................................................... 47  
   - Controllers ...................................................................... 50  
   - Add/Edit Door Controllers ................................................ 51  
   - Add/Edit Readers .............................................................. 53  
   - Input Options ..................................................................... 56  
   - Relays ............................................................................... 57  
   - Add/Edit Lift Controllers .................................................. 59

© 2009 CS Technologies
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Card Options</td>
<td>60</td>
</tr>
<tr>
<td>Lifts</td>
<td>62</td>
</tr>
<tr>
<td>Alarms</td>
<td>64</td>
</tr>
<tr>
<td>Alarm Areas</td>
<td>65</td>
</tr>
<tr>
<td>Alarm Inputs</td>
<td>68</td>
</tr>
<tr>
<td>Upload to Controllers</td>
<td>70</td>
</tr>
<tr>
<td>Direct Commands</td>
<td>71</td>
</tr>
<tr>
<td>2 Technician</td>
<td>71</td>
</tr>
<tr>
<td>Features</td>
<td>72</td>
</tr>
<tr>
<td>External Interface</td>
<td>73</td>
</tr>
<tr>
<td>Utilities</td>
<td>81</td>
</tr>
<tr>
<td>Set Time On One Controller</td>
<td>82</td>
</tr>
<tr>
<td>Customise</td>
<td>82</td>
</tr>
<tr>
<td>PC Setup</td>
<td>83</td>
</tr>
<tr>
<td>Macros</td>
<td>84</td>
</tr>
<tr>
<td>Global Events</td>
<td>86</td>
</tr>
<tr>
<td>3 Input/Output Calculators</td>
<td>87</td>
</tr>
</tbody>
</table>
1 Introduction

Thank you for using the CS Technologies Access Control System. The Evolution software allows you to program and manage the CS Technologies Access Control System.

This manual has been split into three parts each covering different aspects of the Evolution software package. The three parts are highlighted below.

Part One - Getting Started
Getting started is intended for all users highlighting the fundamentals of this software package along with a quick reference 'How to??' guide for many commonly used features.

Software Basics
Quick how to guide

Part Two – Using the System:
Using the System is intended for the system operators such as building managers and administrative personnel who use the system. It covers the following topics:

Setup
Devices
Reports
Administration

Part Three – Setting Up the System:
Setting up the system covers functions typically required by those setting up and servicing the system.

Hardware
Technician

More information on CS Technologies products such as installation guides and product specifications can be found at the CS Technologies website: http://www.cstech.biz

CS Technologies can be contacted by email at support@cstech.biz.

or by writing to

CS Technologies
3/27 Bank Street (PO Box 1054)
Meadowbank NSW 2114
Australia

Tel: +61 2 9809 5176
Fax: +61 2 8878 0222
1.1 Access Control

What is access control?

Access control is simply the letting the right people into an area at the right time,

or

"Saying who can go where when"

Security vs Access Control?
Access control often plays a key role in a building’s security system, but in one key aspect the two are directly opposed:
Security systems are designed to keep the wrong people out, access control systems are designed to let the right people in.
For example, security includes bars, cement, guards, dogs, electric fences, alarms, detectors and the like. They are all aimed at detecting an intrusion and responding to it.
An access control system is the "loop hole" in the security system that allows the right people to enter and exit. The better the access control, the less wrong people will be able to enter. PIN numbers are easy to pass around and provide a minimum amount of security at a cheap price. Biometrics (eg retina scanners) provides a high level of security at a very expensive price.
The best solution weighs the risk and cost of intrusion versus the cost of the security and access control systems.

Who?
All users of the system will be assigned a credential. This credential may identify an individual (eg a key or card) or a group of people (eg a PIN).
The better credentials are those that can not be copied. They should also be easy to use and convenient to carry.
Lost credentials can be immediately removed from the system providing immediate security.
Unassigned keys will also be denied access

Where?
Users will be typically assigned to a group (called an access level). This simplifies the administration of a large number of like users. The group will have what doors and floors members will be able to access. It is possible to have different areas covered by different groups.
For example, tenant, department, or even an individual could define a group. It is also common to have slight variations in groups to provide for the option of parking and other benefits.

When?
Time zones provide the ability to specify what times are secure and unsecured. Time zones will then be combined with doors in groups to specify what times users have access.
It is possible to provide different times to different doors within one group. For example users could have 24-hour access into the building but only office hour access to certain floors.
Doors can also be allocated time zones that will automatically lock and unlock them. This provides public (ie non-credential holder) access.
Start and end dates allow keys to be automatically added and removed from the system. This allows keys to be sent to contractors, guests etc and they will not have access until they are officially allowed in.
1.2 Terminology

Overview

There are a number of terms used within the access control industry. They are summarised by the following diagram:

- **Users**
  - **Door Access Levels**
  - **Floor Access Levels**
  - **Doors**
  - **Floors**
  - **Time Zones**
  - **Lift Banks**
  - **Holidays**

It is expected that the operator will spend most of their time changing the upper levels of this diagram (ie changing users access). Occasionally they would be required to change or create a new access level, or change a time zone. Holidays only need to be edited once a year.

**Users**

Users are the people who actually use the credentials and readers to gain access to the premises. The system records important information about each user, including:

- **User name** - the person's name is what appears on the screen whenever they use the system.
- **Credential** - the key, card or PIN number used to identify that person to the controller.
- **Access levels** – define when and where the user can access different parts of the system.

The system also allows a database of optional information to be stored about each such as company, phone number or Car registration, with the categories customised to suit any particular application or site.

**Doors**

Doors are any parts of the system where a credential is required to gain access to one point only. It includes normal doors as well as car parks (with boom gates, roller doors etc) and other devices. It is basically a method of limiting access from one area to another.

**Lift Banks & Floors**

Lifts and doors differ in that lifts provide access to a number of areas, not just between two.

The Evolution software package simplifies a building lift system by grouping all identical lifts into groups called 'Lift Banks'. This saves time and minimizes the chance of mistakes.
A floor is one level accessed by the lifts. Access can be limited on a per floor basis.

**Timezones**

Time zones are just a collection of times and days of week. The time zone will change from secured to unsecured at the specified times and days.

A time zone does not do anything on its own!

When a time zone is assigned to a door, the door will automatically unlock when the time zone is unsecured. When it is assigned to a floor, the floor will automatically be available for selection when the time zone is unsecured.

It is common for a 9am to 5pm Monday to Friday (or similar) time zone to be created for doors and floors. This provides convenient access during the day. Anyone can access the area, making it ideal for front doors.

Holidays provide the ability to override the operation of a time zone if required. For example, it may be necessary for a time zone to be secured during a public holiday (to stop the public entering the office!).

**Access Levels**

To simplify user programming, the idea of Door Access Levels and Lift Access Levels was introduced. An access level is the grouping of like users. For example, all computer staff may be assigned an access level.

Each access level contains a list of doors (or floors) and an associated time zone. Anyone with that access level will be able to enter the door at the times specified by the access level.

It is possible to have different doors with different time zones within the one access level. For example, it may be necessary to provide 24 hour access to the building, but only restricted access times to other secure areas inside the same building.

**Hardware**

The following terms may be encountered throughout the system, and when talking to technicians:

*Controller:* A "black box" that is the intelligence of the system. It controls the doors, floors and alarm points, and decides who has access. One controller typically controls four doors so there be many of these around each controlling a separate set of doors.

*Strike:* The device that makes the door locked or unlocked. The equivalent of the old fashioned mechanical lock.

*Fail safe:* A lock that requires power to stay locked. This provides access if the power fails and is good from a safety point of view, in particular when there is a fire. It is not good from a security point of view.

*Fail secure:* A lock that requires power to unlock. This provides security if the power fails. A mechanical means of opening the door may be required if the door is used for exiting during a fire.

*RQE:* Request to exit. Typically a push button or motion sensor can be used to unlock the door for exiting. This means that only valid users can enter, providing security, but anyone can leave, providing convenience.

*Door reed:* A magnetic switch attached to a door which signals to the controller whether the door is open or closed.
Credential: The unique key, card or PIN which identifies a user to the system.

1.3 Copyright and version

Copyright (C) 2008 CS Technologies. All rights reserved.

This document is copyright. No part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission from CS Technologies.

Although every effort has been made to be accurate CS Technologies cannot accept any responsibility for any errors in this document and reserves the right at any time to change the contents of this document as well as the construction and design of the products designed herein. CS Technologies does not accept any responsibility for any damage or loss consequential or otherwise however caused resulting from any application of products manufactured or sold by them.

Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29th June 2008</td>
<td>0.1</td>
<td>Anthony Chandra</td>
<td>Create new help file for Evolution Software package. Layout and content based on original Advent help file.</td>
</tr>
<tr>
<td>25th July 2008</td>
<td>1.0</td>
<td>Anthony Chandra</td>
<td>Completed basic Evolution help file. More how to guides and step by step programming help to be added in next version.</td>
</tr>
</tbody>
</table>
2 Part One - Getting Started
This is a brief summary of setting up and navigating through the system.

For quick reference there are some commonly used functions described in the following sections:

- Login
- Add or Delete a User
- Create an Access Level

2.1 Software Basics
This section will take you over the basics of operating the Evolution Access system starting from the basic main screen below.

2.1.1 Logging In
Starting on the main screen, before anything can be done you will need to log in. To log in firstly select the padlock icon in the top left hand corner as shown below. Then on the login window that comes up simply select your username and put in your password and selecting 'Login Now'. The default username is 123 with the password 123.
2.1.2 The Main Screen

Once successfully logged in you will be presented with the main screen. Each part of the screen is described below:

**MENU BAR**

- Quit
- Setup
- Devices
- Reports
- Administrator
- Hardware
- Technician
- Help
Firstly up the top you will find the menu bar which allows you to control the Evolution software. A brief summary of the menus are listed below:

**Setup** - To add/delete/edit user details, access levels, and timezones.
**Devices** - To view/change state of any door, floor, alarm area connected to the system.
**Reports** - Creates reports on either the system setup or history of events that have occurred.
**Administration** - Make simple adjustments on how the software and connected hardware operates.
**Hardware** - To manage CS controllers connected to the system.
**Technician** - Make advanced adjustment on how the software and connected hardware operates.

### PHOTO & SYSTEM WINDOWS

By default to the left of the main screen you will see a blank user image and some quick launch options for the Access Groups, Timezones, and User menus. The picture shown will be of the last user who has used the specified door. Details on how to set the door can be found here.

The system and photo windows can be hidden/made visible using the quick display options on the bottom of the screen.

![Image of system and photo windows]

### EVENT WINDOW

Thu 08/05/08 16:31 FC-1 Operator 123 program: exit
Thu 08/05/08 08:41 FC-1 Automatic System Backup Started
Thu 08/05/08 08:41 Com port 3 failure. 0 ERROR
Thu 08/05/08 08:41 FC-1 Program startup
Thu 08/05/08 08:41 Liverpool CTTT L3 PC-2 workstation offline
Thu 08/05/08 08:41 Gosford PC-3 workstation offline
Thu 08/05/08 08:41 FC-1 Automatic System Backup Complete
Thu 08/05/08 08:52 FC-1 Operator 123 log on

The current system status and events are shown in this part of the screen. You can turn on/off different parts of the screen using the options on the bottom of this area.
The option of Log Window is default and should be selected if not already done so. The other options (Alarms and All) are advanced options which will be described in more detail later on in this guide.

**LOG WINDOW**
The main window by default will show the Log Window, which displays current system events as they are happening. Events highlighted by **GREEN** are users granted door/lift access in the system. **RED** is for users that have been denied, **BLUE** is for any operator actions for anyone using the Evolution software and all other events are **BLACK**.

**ALARM WINDOW**
This will show all the alarms currently happening on the system, including system errors (controller panels not communicating) and general alarms (alarms set up in the system triggered). This window will show with the log window.

**ALL**
This will show all available windows which include Log, Alarm, Armed Areas and Disarmed Area windows. More information on this will be described in later sections.

**DEBUG WINDOWS**

These are advanced windows used mainly by technicians for trouble shooting purposes. The program windows show all the commands that the Evolution software has prepared to send to the CS Controller Panels where the comms window shows in real time which commands have actually been sent.

**SYSTEM STATUS**

The bottom of the main screen shows some important information about the status of some of the hardware connected to the system.

The first field on the right shows the status CS controllers that are directly connected to your PC. The numbers represent controller numbers and it will continuously scroll through. If the number is **BLACK** than the controller is online and if **BLUE** the controller is online and currently transferring information. If it is **RED** than the controller is offline, and is not communicating with the PC. Note any changed in the software made while controllers are showing red will not take effect until the controller is back online.

The next information field shows which workstations (Other PC’s) which share the same database are currently online. If this information is in **RED** than the specified workstation is not communicating with your PC. Note that this field will only show in sites with workstations set up.

An optional field for locations will also appear on the right most side for sites set up for it. If this information is in **RED** than the specified location is not communicating with your PC. Note that this field will only show in sites with multiple locations.
2.2 Quick how to guide

This section will contain a complete list of quick reference step by step guides in working with the Evolution software. Currently the following guides are available:

- Add or Delete a User
- Create an Access Group

2.2.1 Add or Delete a User

First step is to log into the system (more information can be found here).

Once you are in the Evolution main screen there are several ways to get to the Add User screen with the most common being going to the Setup Menu, then Users.

The following screen will show. To Add a user select the insert option circles in RED below.

The following fields need to be filled in: Name, Access Groups and the users Card/Key details.
- **Name**: Should identify the user, not the credential itself. i.e. ‘Card 156’ is not a recommended name

- **Access Groups**: This is where and when the user is allowed to go. For a card to work at least one access level must be in the access groups field. There is only one default access group **1. Permanent Access to All Doors** which allows the card to be used at any door at any time. Information on creating new Access Groups can be found [here](#).

- **Card/Key Details**: Depending on the type of system you are using you will need to add the details for the card/key here. For most card system you need to add a Site Code and Card number here. For Silkey iButton systems you only need to add the Key number. Note the key number is not the same as the number on the key itself. For both types of systems if you are unsure of the Key or Card number, you can swipe a key on any door which should bring up the details on the main screen.

### 2.2.2 Create an Access Group

First step is to log into the system (more information can be found [here](#)).

Once you are in the Evolution main screen there are several ways to get to the Add Access Group screen with the most common being going to the Setup Menu, then Access Groups and select Door.
The following screen will be presented, listing all the existing Access Groups in the system. To add a new group select the Add New Access Group button circled below.

The following screen is presented with a list of all the doors in the system. By default they all have a timezone (More here) associated with it of "0 - Never" which means in this access group that these particular doors are never allowed to be accessed.

To make this access group have access to a particular door simply select a door and using the timezone selection drop down box on the bottom, change the timezone associated with the door.

In the sample below I have selected the "1-Always" timezone and have now set it to the chosen door.
3 Part Two - Using the System

Part Two – Using the System:
This part is intended for the system operators such as building managers and administrative personnel who use the system. It covers the following menus in the software toolbar:

- **Setup** - Used for managing Users, Access Levels, Timezones & Holidays
- **Devices** - Used for managing and monitoring doors and lifts.
- **Reports** - Allows you to create reports on the setup and history of the system and users.
- **Administration** - Basic setup of the visuals and operation of the system.

3.1 Setup

The setup menu consists of the following Menus:

![Setup Menu Diagram]

- **Users** - To manage users and their access to the building/premises.
- **Access Groups** - Create and edit access groups which are groups of doors/floors with specific times that are assigned to users.
- **Timezones** - Create groups of specific time periods based on a weekly basis that can be assigned to access groups, doors, and lift floors.
- **Holidays** - Manage holidays that may effect the system.
- **Daylight Saving** - Set daylight saving dates.
- **Change Password** - Changes the user login password for the currently logged in operator.

3.1.1 Users

The user option is used to manage people using the access control system. This is where all user information, which can include name, company, address information, phone numbers and vehicle registration is stored, along with a photo. This information is then linked to a credential (Proximity Card number, PIN code, key number) and an Access Group, which then will allow the User, with the correct credential to access a door/floor based on the assigned access group.

The main part of the screen shows a large list of all the Users in the system. This can be sorted by any of the headings at the top of the list by simply selecting the corresponding heading. You can also sort via the **Sort By** option on the bottom right of the screen.
The bottom of the screen has a few options that allow you to manage the users in the system:

- **Insert** - Allows you to add a user. More information in the next section or [here](#).

- **Search** - Will bring up a search window which will allow you to search for a text string in the user database.

The search function will search only the field which the 'sort by' section is set to. So to search for a key number you would firstly set the 'sort by' field to key number before selecting the Search function.

- **Delete** - Is used to permanently delete users from the system. To use simply highlight the users you want to delete from the main list and then select the delete option.
• **Bulk Add** - Used to add multiple users, all with the same access group quickly in one go. More information can be found [here](#).

• **Edit** - Once a user is selected in the list this option will bring up that particular users details screen. Alternatively you can double click on a user in the main screen to do the same thing. More details can be found [here](#).

• **Done** - Exits the User menu.

The top of the main user screen also has a few different options regarding the display and setup of the user screen.

- **User Display Type** - The credential type that is displayed on the user list. Usually just set to one option depending on the site, but can be useful if a site has more than one type of credential being used simultaneously (i.e. a site with a proximity card and PIN number system).

- **Random PIN Digits** - Only used for PIN sites to set up how many numbers are used when a random PIN number is created.

- **User expiry date/time** - Turns on the expiry date and time feature in the individual user screen allowing you to add a time and date for when a users credential (i.e. card) is valid for. NOTE: The PC needs to be turned on for the activation/expiry information to go through the system at the set time.

- **User titles** - Editable data fields that can be added to a Users data page. For example you may want to add contact phone number or company information for each user. Up to 12 fields can be created, with up to four being able to be displayed on the main Even window as the user uses their card/key.
3.1.1.1 Insert/Edit Users

The following screen will show when the INSERT option in the Users screen is selected or when an existing user is Edited.

- **Name** - The name of the User who the credential will be issued to.

- **Inside/Outside** - Only visible when Anti-Passback is enabled. This will monitor if a user is inside or outside a particular area.

- **Access Groups** - This is a list of all the current ACCESS GROUPS assigned to the user. Options on the right are used to add or remove ACCESS GROUPS on the list. To setup a user to be able to use all doors at the same time insert the 1-ALWAYS access group into this window.

- **User Expiry Date/Time** - If the option is turned on (Option on main user screen) then the following options will be presented. It allows for a card to be activated/deactivated on a certain date and time. Note: The activation/deactivation information is stored on the PC itself, so for any activation/deactivation information to be sent the PC needs to be turned on and connected at the time of the change.
CARD/KEY/PIN NUMBER

Depending on each particular system this area will look different. In most situations there will only be one field where you will need to insert the CARD, KEY or PIN number. But there may be systems where multiple fields are shown, where more than one type of credential may be used.

- **Key** - There is a Imprinted Number field where usually the number printed on the key is put in. The Key Number field holds the internal serial number of the key which is different to the Imprinted number. If the Key Number is unknown then the Touch Key option can be used if set up by your installer (more here) or alternatively you can use the key at any door, which should bring up the Key Number (as Denied) on the main Even Log screen. You can then copy this information to the Key Number Field.

- **Card** - The card field. If there is an option for a site code you will need to put that in as well as the CARD number. The Swipe Card option can be used to get the card information from the card if set up by your installer (more here). If the card information is unknown then a swipe of the card at any door will bring up the information, including the site code, which can then be used to insert a user.

- **PIN** - There is only one field to enter the PIN number in. The PIN number can be any number less than 4294967294. Alternatively there is a Random Pin generator which will create a PIN number.

- **Data fields** - additional information about each user in the system, such as what company they work for, what level they work on, car registration number or contact phone numbers. The fields themselves can be setup and edited here.

- **Last Transactions** - Once a user has been setup, a small log is kept here on the last few times they have used their card. This makes it easier to monitor a cards usage with out the need for creating a report.

- **Photo ID** - A photo for each user is displayed here. To set up an already stored photo simply select the SELECT PHOTO option which will allow you to explore your computer to find an image file. Alternatively if there is a camera setup on your PC you can use that to take a photo. Select the START VIDEO option to turn on the camera and select the SELECT PHOTO option when you are ready to take a photo.

### 3.1.1.2 Bulk Add Users

This is an optional quick way of adding multiple users. This option is only used in special circumstances as it will add multiple users with only the same access rights and generic names (for example ‘Card 103’) which would need to be changed manually later on.
- **Number of users** - How many users are going to be added
- **Type of** - The type of credential to be added (usually card)
- **Starting from** - The starting number of the credential to be added
- **Site Code** - The common site code of all the cards
- **Access Levels** - Add the access level(s) that will be assigned to all the cards
- **Imprinted Number** - The number printed on the cards (usually "Same as credential")
- **Value** - If Imprinted number option is set to a specific value it goes in here.
- **Data [1-4]** - Any information you would like in the data fields for all the cards
- **Activation/Deactivation date & time** - Set the common active time period for all the cards. Blank fields mean the cards will always be active.
- **Use Count** - Cards can be set so they only work a specific amount of times
- **Add Quickly** - Not recommended to be used. It will speed up the process but may create errors.

### 3.1.2 Access Groups

This section is for setting up and managing the access groups which are assigned to users. These groups are used to restrict when and where a user is allowed to gain access.

**DOOR ACCESS GROUPS**
Access Groups 0 & 1 are predefined, where 0 is no access to any doors at any time, and 1 is permanent access to all doors at all times. All other access groups in between need to be created, which is done by selecting the ADD NEW ACCESS GROUP option on the right.

The following screen will show. At the top there is an Access Group number and Name which are just used to identify the groups. Underneath there is a list containing all the doors in the system. Each door has a timezone associated with it, specifying what time that particular door can be accessed in this Access Group. By default all doors in the group have the 0 Never timezone. The timezone for a door can be changed by firstly selecting a timezone from the drop down box at the bottom of the screen, highlighting a door (or multiple doors) and selecting the CHANGE TIMEZONE option. The EDIT TIMEZONE option will take you to the timezone page where you can create and edit timezones (more here)
On the right of each door listed there is an options section. Options will only show if that particular door has access to them, such as anti-passback and alarm options. If a tick box does appear, hold the mouse cursor over the box to find out what it is relating to.

There is also a COPY FROM OTHER option which is used to copy another access groups settings to the current access group. This is useful in large systems where there are many doors with access groups only having small differences.

**LIFT ACCESS GROUPS**

Lift access groups are exactly the same as door access groups with the only difference being instead of all the doors in the system, all the floors are listed. In the same way as above you can change the timezone for each floor for when it can be accessed.

### 3.1.3 Timezones

Timezones in the system are used to unlock doors automatically, as well as restricting user access to specific doors. There are two types of timezones - standard timezones which define the same time period each day and extended timezones which are combinations of the standard timezones. Using this method extremely complex timezone arrangements can be defined.
Once the timezones are defined their main uses are for unlocking of doors and for restriction of user access by associating them with the access group programming (more here).

**STANDARD TIMEZONES**

There are two predefined standard timezones which are 0-Never and 1-Always. All others need to be created, by simply selecting the Add button. The following screen will appear:

The timezone name is used to identify the timezone and should be something that is relatively self explanatory to help programming in the future. The start and end times need to be filled in (24 hour format) with the days of the week check boxes selected for each timezone. Underneath there is an option to add the type of holidays that this timezone is effected or overridden by (more here). So for the example above for normal office hours, it is active Monday to Friday, 9:00am to
5:00pm everyday, but is not active on public holidays.

**EXTENDED TIMEZONES**

Extended timezones are combinations of multiple standard timezones. These are used to create more complex timezones than programmable in a standard timezone. For example for a office which is open from 9:00am to 5:00pm Monday to Friday, but also open from 9:00am to 12:00pm, an extended timezone would need to be created, combining a regular Monday to Friday timezone with a separate Saturday timezone. To add timezones to an extended timezone simply use the add button on the right.

**3.1.4 Holidays**

This menu is used to define holiday periods in which anything controlled by a timezone which is associated with holidays will be overridden on these specific periods.

**HOLIDAY PERIODS**

In this section the holiday periods are defined. When selecting the ADD option it will ask for a name to identify the holiday, a start time/date and an end time/date, along with the type of holiday it is (Public Holiday by default). For a single day holiday the start time filled in should be 00:00 and an end time of 24:00. The holiday period can be set up for any period of time, like say a whole week during Christmas.
Also it is important to remember to update the holiday dates after the holidays are competed. Alternatively for holidays that you know are going to be on the same date every year (i.e. Christmas) you can select the MAKE YEARLY EVENT option.

HOLIDAY TYPES

This is used to define different types of holidays that the system might control making management easier. For most systems the only type required will be the default Public Holidays, but for example if a system is being shared by two different companies each with different holiday periods, they can be added and sorted by additional holiday types, then by assigning these to various timezones.

3.1.5 Daylight Savings

For locations which are effected by daylight savings. Once the daylight savings dates are set, at 2am on the appropriate date the controller time will adjusted forward or backward by one hour as appropriate. The Get Dates from Windows option can be used to find out and automatically add the dates into the system, but you still need to go to this window and select ok for any changes to be sent to the system.
3.1.6 Change Password

This option can be used to change the current logged on operator password. To add/edit operator access or for more details on operators please see here.

3.2 Devices

The Devices menu option provides the ability to view and control the doors, lift floors, alarm areas and inputs and parking groups in the system. Depending on the configuration, the menu may contain some or all of the following options: Doors, Floors, Areas and Parking groups.

- Doors
- Floors
- Areas
- Parking Groups

There may also be other quick access commands available on this drop down menu depending on how the system is set up. Cancel Overrides is an example which will put all doors and lifts to the normal state cancelling any lock or unlock overrides.
3.2.1 Doors

A list of all doors in the system is displayed. From this screen it is possible to select a door and:

- **Edit** - Change its settings.
- **Trigger** - This is the equivalent of using a valid key or request to exit push button.
- **Override TZ** - This bypasses all timezone settings.
- **Unlock** - Permanently release it until it is returned to normal.
- **Lock** - Permanently lock it until it is returned to normal.
- **Normal** - Returns any overrides to normal

Note that locking and unlocking a door require that the door be returned to normal to operate normally.

It is possible to view the actual status of a door as well as change some of its parameters by clicking on the 'edit' button. The screen below will be displayed.

This screen shows the current status of the door, allows the operator to set some of the more common parameters, and also to override the door status if necessary.

The parameters which can be set from this screen are:
• **Door** - The name of the door can be edited
• **Release time** - The number of seconds that the door unlocks when a valid card is used
• **Automatic Unlock Time** - The timezone which is used to unlock the door. Clicking Edit gives quick access to the timezone menu (more here). Note: the timezone '1 Always' will leave the doors open permanently leave the door open. '0 Never' will always keep the door closed unless open by an authorised user (default).
• **Door open too long time** - if the door is alarmed it is possible to set the amount of time before a door open too long alarm occurs.
• **Forced door delay** - if the door is alarmed it is possible to set the amount of time that the door may be open before a forced entry alarm occurs.

From this screen the current status of the door can also be viewed, including its unlocked/locked status and in alarm/normal status. If the door is not alarmed then the alarm status fields will not display.

This screen also gives access to the trigger, override timezone, unlock, lock and normal buttons.

### 3.2.2 Floors

The Floors menu is used to display and control the current status of the floors controlled by the system. Various parameters related to the floor operation can also be set. The system has been designed so it is only necessary to change or override individual features of each floor once, and this will automatically load into all the information to each lift bank.

A list of all floors in the system is displayed. From this screen it is possible to select a floor and:

• **Edit** - Change its settings for the floor.
• **Trigger** - This is the equivalent of using a valid card/key on a lift.
• **Override TZ** - This bypasses all timezone settings.
• **Unlock** - Permanently release the floor until it is returned to normal.
• **Lock** - Permanently lock the floor until it is returned to normal.
• **Normal** - Returns any overrides to normal

**Note that locking and unlocking a floor require that the door be returned to normal to operate with credentials and time zones again.**

If there is more than one lift in the bank, then for any of the override commands a box will appear asking whether you wish for this command to apply to all lifts in the bank or only to a single lift, and if so which one.

It is also possible to look at the current status of any of the floors and if desired to change some of the more common parameters.
When editing one of the floors the screen below will be displayed.

This screen shows the current status of the floor, allows the operator to set some of the more common parameters, and also to override the floor status if necessary.

The parameters which can be set from this screen are:

- **Trigger time** - the number of seconds available to the user in the lift after presenting their card to select a floor
- **Timezone** - the automatic opening timezone for this floor

The status of the floor also displays on this screen. Because there is no limit to the number of lifts which can be in a bank it is difficult to display the status of the floors in every lift on this screen. Instead, if the status of the floors is the same in all lifts in the bank the status will display; if they differ (because some of the lifts are overridden or triggered by a card read for example) the status will display as 'Partial'.

The floor can be triggered, unlocked, locked down or returned to normal from this screen. When one of these options is selected, if there are more than one lift in the bank then you will be asked which lift you wish the command to go to.

### 3.2.3 Areas

The Areas screen is used to display and control the current state of the alarm areas in the system. Various parameters associated with the area operation can also be set from this screen.

When the Areas menu selection is chosen the screen below is displayed.
From this screen it is possible to quickly arm all or disarm all areas. Also it is possible to view areas which are 'Armed', 'Disarmed', 'In alarm' or 'Isolated'.

By selecting a particular area and clicking on the 'Edit' button the area status can be viewed as below.

The current status is displayed (offline in the above diagram because the controller is not connected to the PC). The status can be changed by clicking the 'toggle' button to arm or disarm the area. The masking timezone can also be changed (and edited). The masking timezone is used in conjunction with other parameters (defined by technicians) to automatically arm and disarm the alarm area if desired.

This screen also displays the list of inputs associated with this area. These inputs can be edited by double-clicking on the relevant device, or by selecting it and clicking on the 'edit pig' button. When this is done the screen below is displayed.
This screen allows the name of the device to be changed. The current status of the input is shown (unknown in the above diagram because the controller is offline).

Parameters associated with the input which can be modified on this screen are as follows:

- **Isolate** - It is possible to isolate the input which means effectively disabling the input so that it cannot cause the area to go into alarm.
- **Tamper bypass** - If annoying 'tamper messages' are being displayed this input can be bypassed so that these messages no longer appear. If they are being displayed this indicates a problem which should be addressed by technical staff.
- **Delay** - This sets the amount of time that the input can be 'in alarm' before actually causing its associate alarm area to go into alarm. This is used in situations where for example a door might be allowed to be open for a short time but should go into alarm if left open too long. A typical situation where this is used is for fire doors, where users can exit using the handle but if left open they should cause an alarm.
- **Report status change** - Normally alarm inputs only show their status changing when the relevant area is armed, and as their status changes they go into alarm and then restore. If this box is ticked then the status is shown whether the area is armed or not.
- **Entry delay** - Sets the number of seconds that the input can be in alarm to allow someone to enter the premises to disarm the area. Not often used with CS Technologies systems, as they can generally be disarmed from outside the premises via the access control system which is a much more secure method.
- **Exit delay** - Sets the number of seconds that the input can be in alarm after the alarm is turned on. If it stays in alarm longer than this amount of time the area will go into alarm. Allows time for movement detectors etc to reset if they regularly cause alarms on exit.
- **Abnormal** - This sets the message which displays on the screen and in the history log when the input becomes abnormal i.e. when the area is not armed and the input is activated. This might be for example 'open' if the input is associated with a door.
- **Normal** - This sets the message which displays on the screen and in the history log when the input returns to normal i.e. when the area is not armed and the input returns to its normal state. This might be for example 'closed' if the input is associated with a door.
- **Alarm** - This sets the message which displays on the screen and in the history log when the input goes into alarm i.e. when the area is armed and the input is activated.
- **Restore** - This sets the message which displays on the screen and in the history log when the input returns to normal i.e. when the area is armed and the input returns to its normal state.

### 3.2.4 Parking

Parking groups allow a carpark with a limited number of spaces to be 'partitioned' between different tenants. For example, a carpark may have 100 spaces, and a tenant may have 10 spaces allocated. With parking groups set up only the first 10 people who are part of that tenant will get access to the carpark; thereafter the tenant will be denied access to the carpark until someone else leaves.

Parking groups are set up under Devices -> Parking groups. The screen below will be displayed.
This shows the current parking groups which have been defined. Additional groups can be defined using the ‘add’ button, groups can be deleted using the ‘delete’ button and edited using the ‘edit’ button or by double-clicking.

If the ‘add’ button is selected it allows a new parking group to be defined. The screen below will be shown.

- **Name** - sets the name of the parking group. Give it a name which describes the group of users who are to be restricted by this parking group.
- **Capacity** – defines the number of people in that parking group who will be able to gain access to the carpark at any one time
- **Controller** – select the carpark controller to which this parking group applies.

Parking groups are controlled within individual controllers. In order to configure a system for parking control, controllers must be defined as having parking control activated ([More here](#)), anti passback must be enabled ([Information here](#)) and the readers on the controller must be defined as being entry, exit or don't care as appropriate.

When editing an existing parking group the screen below is displayed.

This allows the name to be edited. It also displays the current value (unknown in the example because the controller is offline) – this defines the number of people currently occupying the carpark. The capacity can be edited, and the current value can also be set to allow
synchronization of the carpark with its actual current occupancy. For example when setting up the system there might be one car already in the carpark; it is possible to set this as the current value using this screen.

When additional people in this parking group enter the carpark, the 'current value' field will be incremented, and when they leave the 'current value' field will be decremented. If for some reason the initial value is incorrect the system won't decrement past 0. Once the current value reaches the capacity then additional people from this parking group won't be allowed access.

Users are assigned to parking groups under their access level definitions.

### 3.3 Reports

The Report menu allows generation of reports for the system. There are two options in this menu.

- **System data** - The system data reports allow lists of all system settings. Reports of users, controllers, timezones, holidays, access levels, alarm and lift programming can be generated.

- **History** - History reports allow generation of reports of activities on the system. History reports can be for all transactions during a particular period, or for activities of a particular user or activities at a particular reader. History reports can be displayed on the screen or printed, or also exported to a text file for importing into other programs if required.

When a report has been generated it is displayed on the screen in a scrolling window which allows the entire report to be easily viewed. It also allows the report to be printed, saved as a text file or just closed.

- If the Print button is clicked, the report will be printed on the currently selected report printer (More information [here](#)).

- If the Save button is clicked, a dialog box will be displayed asking for a destination file name and directory. The report will be saved as an ASCII text file which can be edited or otherwise manipulated by other programs.

- The Another button allows the current report to be re-run, allowing the user to modify a selection parameter in the report without having to go back through the menu.

- If the Close button is clicked the report will be closed and the normal transaction logging window will be displayed.
3.3.1 System Data

The system data reports provide an easy way to summarize the current system settings. There are several menu selections available, to allow printing of all data or just selected items.

**USERS**

This will create a report of the Users in the system. When selected it gives option for how the users are sorted:

- **Users by Name** - This report sorts the users alphabetically by name.
- **Users by Imprinted number** - This report sorts the users alphabetically by the imprinted number data field.
- **Users by Key/Card/PIN number** - This report sorts the users alphabetically by their credential number. The sort order is dependent on the current setting for the user display type (set in the Setup-->User menu).
- **Users by Access level** - This report sorts the users and displays them in order of access level.
- **Users with Access to…** - This report prints out users with access to a chosen specific door/ floor/area.
- **User by expiry days** - If user expiry date is set then it is sorted by how many days of access they have left.
- **Users by expiry dates** - Reports users sorted by when their credential expires (more [here](#))
- **Users by Data [1-4]** - If the system is set up to use User Titles (more [here](#)), a report can be generated using the data fields (1 to 4 only) for the users with a matching data field search string, which can then be sorted by name or card number.

**ALL PROGRAMMING REPORT**

This menu selection will generate a report consisting of all users (sorted alphabetically by name), controllers, timezones, holidays and access levels in a single report.

**ACCESS LEVEL REPORT**

This report generates a listing of the currently programmed access levels. If the system includes elevators the lift access level information will also be included in the report.

**TIMEZONE REPORT**

This report generates a listing of the currently programmed timezones.
HOLIDAY REPORT

This report generates a listing of the currently programmed holidays.

CONTROLLER REPORT

This report generates a listing of all of the current controller setups. If the system includes elevators then the lift bank settings are displayed here. If the system includes alarms then the alarm settings are displayed here.

CAL & CTZ REPORT

This report generates a Controller Access levels (CAL) report and Controller Timezones (CTZs) report. The CAL & CTZ report gives a report on all controllers listing which access levels and timezones are applied to that controller.

3.3.2 History

The history report menu allows generation of reports of transactions on the system. Every time anything happens on the controller network - a person goes through a door, an exit pushbutton is pressed, a timezone operation of a door, an alarm event etc - it is logged on the hard disk of the computer. The history report menu provides a way to produce reports of these transactions.

When the history report menu is selected a dialog box appears which allows entry of the parameters for the required report.

The parameters, which can be entered to generate the report, are as follows:

Report Period
**Start/End date and time** - The beginning and end of when you want your history report to cover.

**Daily start and end times** - Occasionally it is useful to be able to retrieve all the transactions during a particular part of the day for a time period. For example, someone might require everyone who entered the carpark during the hours of 9.00am to 5.00pm over the last month to be listed in a report. The daily start and end times allow selection of just part of the day over the period of the report to be included in the report.

**User Selection**

Access granted – display users who were granted access during the appropriate period

Access denied – display users who were denied access during the appropriate period

**Name** - By default is set to 'All Users' but can be used to create a report for a single user in a system.

**Card No** - You can create a report for a particular card number using this field.

**Data ##** - For systems where the optional User Data fields are used, they appear on this form also. In the example above the user titles are set to 'Tenant' and 'Data 2', and this allows generation of reports for just users whose data matches the information entered in these fields. Thus reports for all users from a particular company etc can be generated.

**Doors/Floors**

**Location** - Allows you to narrow the reporting down to a particular location. By default 'All Locations'

**Name** - You can create a report on a single door or floor in the system. By default 'All Doors & Floors'

**Exit requests** – Display exit request transactions which occurred during the appropriate period

**Timezones** – Display timezone changes which occurred during the appropriate period

**Areas**

© 2009 CS Technologies
Alarms - If set up will show any alarms that have occurred in the report period.

Abnormals - Will show any area areas that have had an abnormal status in the report period.

Arming/Disarming – Display arming/disarming of alarm areas

For Name – Allows you to select a specific Area to report on. By default ‘All Areas’

Special Reports

Operator Actions - Every time an operator access a menu on the system it is logged in the history data file. The operator actions can be reported by ticking this box.

FBT Report - The FBT report is used for Fringe Benefits Tax reporting. Under the Australian Tax Act, companies who provide parking for their staff as a fringe benefit must pay tax on the usage of the parking for each staff member who uses it. Given a period defined by the start and end dates, the FBT report will show, for each ‘user’ in the selected group (all users, or select by individual user or tenant) how many days they are recorded as having access granted to the selected doors (usually set to ‘carpark’ for example). This is used to calculate their usage of company-provided car parking.

Other – Tick this box to report all other transaction types during the selected period.

Time and attendance –. These reports record when each user arrived on site each day, and what time they left, and they also calculate totals of time on site. This information can in turn be used to interface with payroll systems etc. To implement Time and attendance anti passback must be set up and enabled

Email Transactions - This will report on any email alarms that have been sent.

Show inactive users (Invert) - This menu option allows the report criteria to be inverted. Whatever parameters are set up for display in the access report, this check-box will produce a report which inverts them. For example, if the report was run to show all users who have gained access in the last three months, then by selecting this option to invert the output the report would show users who have NOT gained access in the last three months. This can be used to show users who are inactive.

Tally by Data 1 – Will sort all data alphabetically using data from the Data 1 field.
3.4 **Administration**

The Administration menu is used to control the day to day operation of the system.

It contains the following menus:

- *Forgive all users* - Is used with anti passback systems, to reset the status (whether they are inside or outside) of all users.
- *Backup and Restore* - Is a sub-menu which contains functions allowing you to backup and restore of the Evolution database and related options.
- *Operators* - Used for creating and setting up the users of the Evolution software.
- *Printer setup* - Windows printer setup dialogue box.
- *Set system time* - Provides the ability to set the time in the door controllers.
- *Workstation settings* - Allows you to modify display, login and registration settings of Evolution.
- *Email alarms* - Modification of email alarm settings for alarms to be sent out via email.
- *Set display font* - Sets the font used in the windows on the screen.
- *Windows to Default Positions* - Arranges the windows on the main screen into their default positions.

### 3.4.1 Backup and Restore

Contains processes and settings for backing up and restoring the Evolution database.

#### Automatic Backup Settings
Contains options for the daily automated backup system of Evolution. The **Auto Backup** box needs to be ticked to enable the function which will then ask for a time that you would like the backup to occur (by default 00:05) and a location on the computer or network that you would like the backups stored in. There is also an option to delete older backups. If the Evolution software is turned off at the time it is meant to do a backup it will do the backup at the next available time when it is restarted. Note only the database files are backed up, which does not include log (or history) files or user images.

**Backup Database**

This is a manual backup option of the database files (not including logs or user images). The backup filename field needs to contain a name for the backup file. Optionally a computer drive address and the filename can be included to place the backup in a specific location. If a computer drive address is not included the backup will be created in the automatic backup directory from above.

**Restore Database**

This is the manual restore option for the Evolution database files. It will ask for a location and filename for the backup file to restore to. It is important that restore function should only be used if there are corruptions in the Evolution database and acknowledge that any changes to the database made after the time the backup was created will be lost in the restore process.

**PC Transfer Wizard**

This option is used to create a complete backup or restoration of the Evolution system including the backup of history files and user images. The file is much bigger and takes longer to create but is useful if transferring the software over to a new PC and ensuring everything has been moved over. Options similar to above are presented for the location and name of the backup file.

### 3.4.2 Operators

The operators of the system are the people who are authorized to use the Evolution software for programming the access control system. When Evolution is first installed the default operator name and password are ‘123’. However many different operators can be defined in the system, and each can be authorized for different activities. Each time the operator logs on or off this is recorded in the audit trail.
Edit Operators

Used to add, delete or edit operators in the system. The operator list will appear, initially with the default operator 123 displayed.

Click on the 'Insert' button to add a new operator, or 'Edit' to edit an existing operator. The following screen will be displayed:

- **Operator Name** - Enter the name which will identify this operator. The name must be entered when logging into the system. The name is not case-sensitive.

- **Password** - Enter the password for the operator. This password will not display and can be any mixture of numbers and letters. Note that when the password is entered for login case is ignored. The password must be entered twice to ensure that it has been entered correctly.

- **Type** - Enter a description of the type of the operator. A drop down list will provide a list of existing operator types, or else press the Edit button to create or modify an existing type.
Note: When adding new operators it is impossible to add an operator with more permission than the currently logged in operator. This ensures the security of the system. It is also impossible to delete the last technician level operator in the system, and also impossible to delete the currently logged in operator.

Operator Types

Used to add, delete or modify operator types. The following screen will appear:

The operator type “Technician” can not be edited or deleted. It provides access to all menus.

Pressing Add will create a new operator type and will enter the edit screen. Pressing edit will open the edit screen for the currently selected operator type. Pressing delete will bring up a confirmation screen and then delete the currently selected operator.

The edit screen contains a list of the main menu items, and allows the setting of which items each user has access to. For each of the main menu items it is possible to select 'All', 'None' or 'Partial'. If 'All' is selected, operators of that type will have access to all of the options in that menu. If 'None' is selected, operators of that type will have access to none of the options in that menu. If 'Partial' is selected, the Edit button can be used to individually grant or deny access to options in that menu.

An operator can only allocate menus they have access to. For example, if an operator does not personally have access to the hardware menu, they cannot assign that menu to another operator.

Most of the choices under 'partial' just list the possible menu selections under that menu. The exceptions are the Setup and Devices menus.

Setup Partial Menu
As well as having options for all of the items in the menu, there is a list of 5 access levels which can be defined for this operator type which are the access levels that can be programmed by this type of operator. In this way it is possible to restrict the access levels which can be programmed by a particular type of operator.

An example of an application where this is useful is in a situation where a single installation of the software is controlling two separate units. Each unit is owned by someone different; each owner wants to be able to program additional users with access to his unit, but doesn't want the owner of the other unit to be able to program users to access his unit. By allocating two different operator types, each of which is only able to program access levels for his own unit, this restriction can be maintained with complete security.

**Devices Partial Menu**

As well as listing the sub-menus in the devices menu there are check-boxes for restriction of the operator ability to override the door and floor status. Usually operators are able to unlock and relock doors; however when doors are in these 'overridden' states it can cause problems because timezones do not work and sometimes users are restricted from accessing the doors.

Because of this it is possible to stop operators from overriding the status of doors and floors via the restriction in this screen. Unless the 'override' check-boxes are ticked the operators are unable to unlock or relock the doors/floors.

### 3.4.3 Printer Setup

The Printer setup sets the printer which is used for printout of reports. The default is the windows default printer but using this menu selection it is possible to choose any currently configured printer.
Note that if the printer is offline or not available, when a report is attempted to be run this will cause errors. If errors occur when printing a report, always check that the windows printer currently selected is actually accessible from the PC which is running the program.

3.4.4 Set System Time

This option allows the time on all of the controllers to be synchronized to the time on the PC. Because the CS Technologies system is fully distributed, each controller in the system has its own real-time clock and can keep track of the time. The clocks within the controllers are accurate to within 2 minutes per month – in fact their accuracy is much greater than the typical PC clock.

However the PC clock and/or the controller clocks may drift with time. This menu selection makes it easy to synchronize the time on all of the controllers, and also sets the time on the PC to the same time.

Note that with Master Clock mode enabled (more here) this synchronization occurs automatically at 12.05am every day.
3.4.5 Workstation Settings

This box opens when the Workstation settings option is selected. It allows you to modify certain settings of Evolution.

**Display**

- **Workstation title** - This allows the caption displayed at the top of the main window to be set. This is usually something like "15 Bennett Street Access Control System". As well as setting this caption, it also sets the heading on any report printout. In this way the installation can be customized.

- **Start up minimized** - Evolution will start up minimized.

- **Remember my windows** - All customized window positions will be remembered and loaded up at startup.

- **Show picture on all door transactions** - By default only people using the registration reader (more information below) have their picture displayed on the main screen. If this option is selected then all users on all doors will have their picture displayed.

**Local Settings**

- **Password Timeout** - The time of inactivity in minutes before the current logged in operator is automatically logged out.

- **Exit from login** - Allows the software to be shutdown without logging in.

- **Select All Lifts** - Normally unselected. Used for grouping overrides.

- **Alarm Sound** - A selection of the sound that is played when a system or device alarm has been created.

- **Event Printer** - The output for a serial printer, which will continuously print everything that is being displayed on the event log.
- **Run As Service** - This allows Evolution to be run in the background of the Windows operating system, starting up automatically and not being displayed on the windows task bar. Instead, Evolution will run from the Windows service tray (bottom right corner of Windows with the clock).

**Registration**

Allows you to select the controller and reader that is to be used for the registration of new users. So once set up the touch card/key option can be used in the edit user screen to automatically put card/key information into the fields required.

- **Auto register** - Will bring up the edit user screen for a new or existing user automatically if a card/key is presented at the set reader.

Note: This reader is also used as the reader used to bring up user photos as the door is used.

### 3.4.6 Email Alarms

Evolution software is able to email all system alarms. This first window is used to set up where and when the email alarms are sent.

- **Send alarms by email** - Enables the email alarm feature
- **Recipient Email** - The email address for the recipient of alarm email
- **Recipient Name** - The name of the user that is going to receive the email (optional)
- **Subject** - Information that will come up in the subject field when an email alarm is sent.
- **CC** - A secondary email address that the email alarms can be sent to.
- **Disable email alarms in timezone** - Email alarms can be disabled at a certain time zones using this feature. For example you may not want alarms emailed to you during 9am - 5pm as you are directly monitoring the system at this time.
- **Select [Plain Text]** - The email alarm is sent as a plain text
- **Select [Plain Text Attached]** - The email alarm is sent as a plain text attachment to a blank email
- **Select [HTML Table Attached]** - The email alarm is sent in the HTML format
• **Configure Settings** - These are advanced settings on email transmission settings. Default settings use the CS Technologies mail server to send alarms, but in some specific environments this can be modified. This should only be set up by IT staff as it requires some advanced details about the email system being used.

![Configure Settings](image)

3.4.7 **Set Display Font**

This menu option allows the font used in all the windows to be set.

![Set Display Font](image)

This is a standard Windows font selection box. Select the desired font, size and style and click OK. This change does not take effect until the program is closed and restarted.
Part Three - Setting Up the System

This part covers functions typically required by those setting up and servicing the system. The options and setting here should not be modified without knowledge on how the system is connected together and configured. These cover the following menus:

- **Hardware** - Used to set up CS Network controllers currently connected to the system
- **Technician** - Allows you to configure the software on how it works with the hardware connected.

### 4.1 Hardware

The hardware menu is for the configuration of all devices attached to the Evolution system including doors, lift systems and alarms.

- **Locations** - Configure different location settings for Evolution. By default there is one MAIN location.
- **Controllers** - Allows CS door/lift controllers and doors to be added to the system or modified.
- **Lifts** - Allows lift banks to be added or modified. Note: A lift controller must be added before this menu option will be available.
- **Alarms** - Allows alarm areas and alarm inputs to be configured.
- **Upload to controllers** - Forces a download of database information to a selected controller or all controllers.
- **Direct commands** - Sends a command to a controller. A useful tool for diagnostics.

#### 4.1.1 Locations

Locations are used to manage different sites using the same Evolution database. Majority of systems only have the one default location MAIN, but some larger installations may have multiple buildings each with a separate location name and settings.

The locations are listed in the following window with options to Add Edit and Delete them.
If adding a new location or editing a current location the following window will display

- **Location Name** - The identifying name of the location. It should be descriptive of the actual location to aid in programming (for example not just location 2)

- **PC Number** - The specific PC that this location is attached to (more info [here](#))

- **Short Name** - A short identifier which will be displayed at the bottom of the main screen informing if the location is online

- **Don't display global** - This option will only allow local events that are happening on the specified PC and connected CS Controllers to be shown on this PC. If un-ticked all events from all other locations and PC's are displayed.

- **Don't display local** - This option if selected will stop any local events (except alarms) being displayed on the local PC.
Controller Connection Type

Depending on how the controllers on this location are connected different options are presented. Information is set out below for each type.

**Com Port**

Most commonly used option. A direct com port is set up in the Edit Direct Port option.

**56K Modem**

- **Phone Number** - The number to be dialed by the modem. Make sure to insert a 0 in front of the number or are codes if required.
- **Connect and download periodically** - The software can be set to automatically connect and download, with the period in minutes set below.
- **Connect and load programming commands immediately** - If any changes are made in the Evolution software and the controllers are not connected then this option will set it to connect and download any changes made automatically.
- **Hang up if all controllers offline** - This option will disconnect the modem if all the controllers are offline. This will allow it to reconnect next time which may fix the communications problem.
- **Stay online if all transactions emptied** - This option will keep the modem connected even after all commands have been downloaded by the automatic connections above.
- **Don't wait for modem response** - Not normally used, this option will force Evolution to send commands continuously without waiting for the modem to respond.
- **Modem Settings** - Gives advanced options on the modem settings including the com port it is connected to, initialisation string and comms timing options. See your modem installation guide for more details.
TCP/IP

This option allows an IP address be used for the location of the CS Controllers. More information is provided with the installation manual for the IP converter used.

4.1.2 Controllers

This menu is used to manage all CS Network controllers in the access control system. When setting up a system the primary task is to define which controllers are in the network. Each controller operates a certain group of doors, floors, alarms or other functionality and once defined the software communicates with the controllers in order to operate the system. The main screen below brings up a list of all the controllers in the system.
Controller information such as location, name and type are given on this table. Also to the far right there is an Active option. If unticked the Evolution software will not try to communicate to that specified controller. This option is useful during diagnostics or system when working on the system.

There are also options to Add, Edit and delete controllers from this screen, along with an advanced card options screen.

### 4.1.2.1 Add/Edit Door Controllers

If you Add a new controller or Edit a current controller the following window will appear:

- **Location** - Specify the location (more [here](#)) that this controller is associated with. The location has a connection type associated with it and this controller must be connected to that connection.

- **No** - The controller number that has been physically addressed on this controller. For example if this controller is No. 2 then the controller out on site needs to be physically
addressed to the number 2 (in binary)

- **Type** - Is set to either Door or Lift depending on what it is doing (Door in this case. For a lift controller see [here](#)).

- **Info** - Brings up a window with internal information of that controller (only if the controller is currently communicating)

![Controller Information](image)

Information includes firmware version and type, internal user and history memory and internal time and date. There is also an option for programmable relays that should not be touched. Note this window will display information it received last time that this information was refreshed or a full download occurred so it may not be current. To refresh this information the refresh button needs to be selected and it will take around 10 seconds for the information to download.

- **Name** - The name for this controller.

- **Where Installed** - A description for where this controller is installed. This information may be useful in finding controllers at a later date in a large site.

- **Doors** - Gives a list of the current doors setup in the system (Maximum 4). There are options to Add, Edit and Delete these doors. More information can be found [here](#).

- **Invert LEDs** - This will invert the LED outputs for each reader (Pins OUT1 to OUT4) to their normal operation.

- **Input Options** - This is a advanced input menu for PIG 1-wire devices. These devices include silicon key readers and PIG2/3 input and output devices.

- **Relays** - This option is for managing relays on the specified controller. More information can be found [here](#).
When the Add or Edit option is selected in the doors section of the controller screen the following window will appear.

- **Name** - Enter the name for the door that this reader is for.

- **No** - The reader number. Note this number is linked with one of the four ports on the CS controller that the reader is wired into.

- **Reader Type** - Select the type of reader that is being used.

**Relay and LED options**

- **Valid Read Triggers** - Here you can set which relay is going to trigger if a valid credential is presented at the reader. There is also space here for a second relay if required.

- **LED** - This is the LED output pin to be used for the reader (OUT1-OUT4). It is usually the same as the LED set in the edit relay menu (more [here](#)).

- **Invalid Read Trigger** - This is the relay triggered if an invalid credential is presented at the reader. Usually blank but can be used to create an alarm when an unauthorized user tries to access a door.

- **No Re trigger** - Normally if a credential is presented continuously at a reader, the timer for how long the relay is to trigger will reset from whenever the last valid read was. If this tick box is checked it will accept the first credential, then not read anymore until the relay has timed out and locked again.

- **Lockout Denied User** - If an invalid credential is presented more than 3 times it will lock the reader so no more credentials can be used. The lockout time is initially 60 seconds, but increases in blocks of 20 seconds each time the credential is re-tried.

**Anti Pass Back** - These are settings to set up Anti-pass back which is to set up a system where a person must first enter an area, then exit before being allowed to enter the same area again.
Part Three - Setting Up the System

- A/P - This is to set the door for how it will operate in the Anti Pass back system
  Don't Care - Not involved in anti-pass back decisions
  Entry - Door used as entry to an area
  Exit - Used as an exit to an area
  Inside - A door Inside an area
  Outside - A door outside an area

- Enforce - If not selected then credentials are only monitored if they are inside or outside and area. If selected then the system will not allow the credential to break anti-pass back rules such as entering an area twice without exiting.

- Timed anti-pass back delay - The time in minutes before anti-passback is reset for a credential

- Global anti-passback - If un-ticked anti-passback only applies to the one controller. If selected then all controllers work together in a system to create one large ant-passback system. Note for this to work the PC and Evolution software must be turned on and communicating for this feature to work.

- Midnight Forgive - This option will reset all anti-passback statuses for all credentials every midnight.

Exit Request Input - Sets up exit request system for the specified door

- Input - The input PIN or location for where the exit request input has been wired into. More information on Select Input found here.

- NO/NC - Option to select between a normally open or normally closed input.

- Options - The following window will appear. It gives more advanced options for exit request settings.

  - Disable RQE Display in timezone - Selects a timezone for when exit request triggers are not shown on the event log.

  - RQE Triggers - Selects the relay to be triggered when the exit request input is triggered. There is space for upto 2 relays to be triggered. Usually only one relay is used, which is the same as the door relay.

  - In Timezone - Selects the timezone in which this relay will trigger. Normally 1-Always.

  - Exit Request Text - Sets what will be displayed on the event log when th Exit Request is triggered.

  - Exit Request Retriggers - If set will allow the exit request timer to reset every time the exit request is retriggers. If not set the system will not accept any additional exit request triggers until the current trigger is timed out.

Door Monitoring - Sets up monitoring of the wether the door is physically open or not
(usually using a reed switch)

- **Input** - The input PIN or location for where the door monitoring input has been wired into. More information on Select Input found [here](#).

- **NO/NC** - Option to select between a normally open or normally closed input.

- **Options** - The following window will appear. It gives more advanced options for door monitoring settings.

  ![Door Monitoring Options](image)

  - **Door Open too Long Time** - Door open too long an alarm created if someone has used their credential then held the door open for an extended period of time. This is the time in seconds before the alarm is triggered.

  - **Forced Door Open Delay Time** - Forced door alarms are created when a door is opened without the use of a credential or exit request. This is usually set to 0 seconds.

  - **Disable Door Monitoring in Timezone** - The timezone where you would like the door monitoring features disabled.

  - **Disable Forced Door Alarm in Timezone** - The timezone you want the forced door monitoring to be disabled.

  - **Forced Door/DOTL Relay(s)** - There are two spaces for relays that can be set for a forced door and Door Open too Long alarms

  - **Alarm/Restore Text** - Sets what will be displayed on the Event Log when the door monitoring goes into alarm/restores

**Area Arming/Disarming** - Set up if this area is used to arm or disarm an alarm area.

- **Area** - The alarm Area associated with the reader.

- **Disarms** - This will allow that reader to be able to disarm the selected area.

- **Arms** - This will allow that reader to be able to arm the selected area.

- **Arms on third swipe** - This will allow that reader to be able to arm the selected area after 3 consecutive key/card swipes.

**Mantrap/Ground loop** - This is to set up a ground loop input that must be triggered before the reader is made active
Input - The input PIN or location for where the mantrap/groud loop input has been wired into. More information on Select Input found here.

NO/NC - Option to select between a normally open or normally closed input.

4.1.2.1.2 Input Options

This is for advanced configuration for input and PIG expansion setup. The following will display:

- **Pig tamper timeout** - When the controller is unable to communicate with PIGs it generates a tamper message indicating that there is a problem in the communication. However often this tamper message is related to temporary noise and the devices very quickly restore from the tamper state. By setting the pig tamper timeout this can reduce the occurrence of these types of messages. This setting determines the number of seconds that a pig must be in tamper before it reports as a transaction. This is typically set to say 5 seconds but could be as much as 120 in a very noisy environment.

- **Pig tamper retries** - When scanning pigs they are scanned one at a time sequentially. This setting sets the number of times the controller will scan an individual pig in succession when
checking to see if it is offline. This is typically set to 3.

- **Pig change retries** - In an environment prone to electronic/electrical noise occasionally false alarms can occur. By setting this parameter the controller is being commanded to confirm any change in state of the pig by reading it several times in succession. This is typically set to 3.

- **Pig timing value** - PIGs have an inherent value which determines the speed of signals transmitted to and from them. This value should be set to 1 or 2; if it is set to 0 then PIGs will not communicate (where supported by firmware).

- **Tamper relay** - It is possible to report the fact that a pig has gone into tamper via a relay. This is selected here.

- **PIG Boosters** - PIG boosters are devices which extend the distance and reliability of the PIG bus. When a pig booster is fitted it uses up an additional input port – i.e. if you have a pig booster on say IN7 then the pig bus takes up both IN7 and IN8. The check-boxes here allow you to define where pig boosters are fitted.

- **Don't scan 1-wire bus on** - The firmware is multi-functional and with some revisions any input or output can be used for driving PIGs. However when inputs are used for readers or direct digital inputs then they should be disabled from use as PIG inputs because the PIG input ports are constantly scanned and this can interfere with the other functionality of the ports. Thus for example any inputs where readers (other than Silicon Key readers) are connected should be disabled for use as PIG ports.

The ports which are checked will not be scanned for any Dallas Semiconductor 1-wire devices which include PIGs, temperature sensors and Silicon Keys.

4.1.2.1.3 Relays

When the relay option is selected the following window will appear with a full list of all relays associated with the controller (Normally 4).

![Edit Relays Window](image)

There are options to Add, Edit and Delete relays. When selecting the Add or Edit button in the relay box brings up the display below.
- **Name** - Enter the name for this relay. This may be associated with some function of the relay (e.g. 'over-temperature alarm') or a description of the hardware (e.g. C1 relay 3).

- **Relay number** - This is where the relay hardware is associated with the relay. Pressing the 'calculate' button will bring up a calculator which will make it easier to define the settings for this relay (more on calculators [here](#)). Basically relays 1-4 are the on-board relays but relays can also be fitted to expansion boards and PIGs.

- **LED** - Select the number of the LED (OUT1 to OUT4 pins) which will indicate the status of this relay. Leave at 0 to have no LED associated. If a relay is associated with a LED, when the relay is either triggered or on a timezone the LED will be on.

- **Timezone** - This is the timezone during which the relay will be energised. It is the same timezone as when set up in the Devices menu (more [here](#)).

- **Trigger time** - Enter the trigger time for the relay (1-65535 seconds). If set to 0 the relay will toggle. This can be set to either seconds or 100ms pulses.

- **Reverse relay contacts** - Click this box to make the contacts fail-safe (relays are normally energised and turn off when triggered).

- **Display in devices** - Usually it is not desirable to display each relay individually in the Devices/Doors list because relays are associated with Doors which themselves will appear in the list. However if the relay is being used for some type of control function it may be desired to be able to check its status or override it in some way from the Devices/Doors screen and if this box is checked then the relay will appear in this list.

- **Report Status** - If selected every time the relay has been triggered, turned on or off, will be reported on the event log.
4.1.2.2 Add/Edit Lift Controllers

If you Add a new controller or Edit a current controller the following window will appear:

- **Location** - Specify the location (more [here](#)) that this controller is associated with. The location has a connection type associated with it and this controller must be connected to that connection.

- **No** - The controller number that that has been physically addressed on this controller. For example if this controller is No. 2 then the controller out on site needs to be physically addressed to the number 2 (In binary)

- **Type** - Is set to either Door or Lift depending on what it is doing (Lift in this case. For a Door controller see [here](#)).

- **Info** - Brings up a window with internal information of that controller (only if the controller is currently communicating)

Information includes firmware version and type, internal user and history memory and internal time and date. There is also an option for programmable relays that should not be touched. Note this window will display information it received last time that this information was refreshed or a full download occurred so it may not be current. To refresh this information the refresh button needs to be selected and it will take around 10 seconds for the information to download.

- **Name** - The name for this controller. Lift controllers are usually named after which lift number it is associated with.

- **Where Installed** - A description for where this controller is installed. This information may be useful in finding controllers at a later date in a large site.
- **Lift Bank** - Associate the controller with a Lift bank profile. More information in creating lift banks can be found here.

- **Reader Type** - Select the type of reader being used in this lift.

- **Destination reporting** - Input boards can be configured, linked with the call buttons within the lift, to indicate which floor was selected when a person was using their credential within the lift. If this box is checked then the controller will be configured for destination reporting. Among other things this will mean that when a credential is presented at the reader no transaction will be recorded until either a floor is selected or the selection times out.

- **Pre-sense** - The destination reporting can be configured for either 'pre-sensing' or 'post-sensing (Default)'. This refers to when the floor relay operates during an attempt to gain access. With post sensing, the relays operate immediately a credential is used, then drop out when a floor is selected. With pre-sensing the relays don't operate until a floor button is pressed; then only the relevant relay operates. This provides higher security but will only be able to be done where the lift circuitry allows.

- **Select Relay using PIN** - This is an Advanced option for PIN keypad systems where the same PIN number can be used to trigger different relays by the addition to a separate number to the original PIN number.

- **Invert LED** - Inverts the LED PIN for the reader output (PIN OUT1) from its normal operation.

### 4.1.2.3 Edit Card Options

Depending on the type of controller, card parameters allow customisation of the way that cards are read by the system. For example, with a wiegand insertion key a different number is read from the key depending on which way the key is inserted into the reader. Card parameters allow an 'inverted' key to be interpreted correctly by the system.

Clicking on the 'Edit Card Options' button within the Technician/Site screen brings up the following dialog.
This allows various parameters to be defined for different card types and provides great flexibility in the configuration of the system to read different types of cards.

- **Don't display bad card reads** - This option, which applies to both wiegand and magstripe controllers, stops bad card reads from displaying on the screen. This is used where noise or other interference is causing bad card reads which annoyingly fill up the log. Ticking this box will ensure that a bad card read does not appear. If this box is not ticked then when a bad card read occurs a message 'bad card read – n bits' will appear in the transaction log.

**Wiegand parameters:** The wiegand parameters are relevant for wiegand controllers only.

- **Allow inverted cards** - This option treats cards with the 'data 1' and 'data 0' signals reversed as possible cards. It is used in applications where the card is reversible – for example a wiegand insertion key, where this occurs if the key is turned over. If this is ticked then when a card is read it is processed normally, and if not found in the database is inverted and then processed again.

- **Rotate 25 or 31 bit cards** - This option is used to 'guess' a missing bit in the card; if 25 bits are received (instead of 26), or 31 bits (instead of 32) the system guesses the missing bits. Not recommended; can guess incorrectly. But some reader technologies are not reliable enough to provide all the bits all the time.

- **27-bit special cards** - This option is used to process 27-bit Motorola/Indala cards for Chubb Building Automation correctly. These cards are in a particular format which requires a special non-standard reader and processing slightly differently.

- **Restrict to card lengths** - This allows up to three particular 'card lengths' to be processed by the system. If all of these are blank or zero then any card length will be read by the system and treated as a valid card. But using these parameters it is possible to restrict the system to only read cards of a particular length (say 36 bits) and ignore other lengths (i.e. treat them as bad card reads).

**Magstripe parameters:** The magstripe parameters allow powerful processing of information from mag-stripe cards. Essentially it is possible to extract different parts of the card and treat it as a full card number. This enables just about any mag-stripe card to be used with the system – including credit cards.

To do this the system supports up to two 'fields' of data extracted from the mag-stripe. The first field is known as the 'site code' and the second field as the 'card number'. The system simply joins these together to form a large number which is the unique credential to identify the cardholder.

- **Site code start** - Select the position of the site code on the card. The first digit on the card after the start sentinel has position 1.

- **Site code length** - Enter the length of the site code.

- **Count site code from start or end** - This affects the way that the 'start position' of the site code is counted. If 'start' is checked then the position for the start of the site code is counted from the start of the card. If 'end' is checked then the position for the start of the site code is counted from the end of the card.

- **Card number start** - Enter the position of the start of the card number on the card.

- **Card number length** - Enter the length of the card number.

- **Count card number from start or end** - This affects the way that the 'start position' of the card number is counted. If 'start' is checked then the position for the start of the card number is counted from the start of the card. If 'end' is checked then the position for the start of the card number is counted from the end of the card.
- **Card type** - Select the card type from the drop-down list. This affects various parameters within the controller including the start sentinel and card format. The default is track 2 but also track 1 and a special ‘infineer’ format are also supported. Different card types must also correspond with the correct reader type i.e. a track 1 card must be read by a track 1 reader, with the card type also set to track 1.

- **No error checking** - Normally when reading cards there is a checksum (LRC) encoded on the card and this information is used to verify that the card has been read correctly. However some cards (notably Presco) do not incorporate this error mechanism and accordingly this check box provides a means to disable error checking on the cards.

- **Turn on diagnostics** - With this feature enabled, every time a card is read a ‘diagnostic’ message is sent out the com port. This occurs transparently if PC3 is running, but if PC3 is not running then this provides a means of capturing the raw card data as the card is swiped through the reader. The com port on the controller can be connected to a cash register or other type of data capture information and the card information will be available for logging.

- **Allow access to undefined cards** - If this box is checked then the system will provide access to ALL cards, regardless of whether they are in the database. If a card is in the database then the access level information will be processed but if it is not in the database then it will be granted access. This is useful in situations like a library where there may be tens or even hundreds of thousands of cards on issue, and it is desired to grant access to all cards but have the ability to 'lock out' certain cards because of problems being caused by those particular users.

- **Match site code** - This parameter works in conjunction with the ‘allow access to undefined cards’ and provides some small restriction to the cards – rather than ALL cards being allowed access, only cards which have the site code matching the data entered here will be valid for the system.

- **Enforce length** - This parameter also works in conjunction with the ‘allow access to undefined cards’ and provides the restriction that valid cards must have a particular length.

### 4.1.3 Lifts

A unique feature of the CS Technologies system is the way it handles multiple lifts, simplifying the operation and programming of even the most complex of elevator configurations. One controller is required for each elevator, and as the controllers are defined they are each associated with a ‘lift bank’.

Once the controllers have been defined as lift controllers, and associated with their respective lift bank numbers, the actual lift banks can be set up using this menu. Firstly a list of all lift banks in the system will appear with option to Insert, Edit and Delete lift banks.

![Image of Lift Banks Menu]

Each lift bank consists of a number of floors (each of which corresponds to a relay output on the appropriate controllers which comprise the bank).
To add a new lift bank, click the 'Insert' button, or to edit an existing lift bank select it and click the 'Edit' button. A dialog box will display allowing entry of the lift bank number and name, as well as definition of the floors which comprise the bank.

The lift bank number is an arbitrary number, and is used along with the Controller definitions to associate a number of controllers with this lift bank. The name is used when editing the lift bank and lift access level definitions so should be descriptive of the general grouping of lifts.

The floors which comprise the lift bank are now defined using the Insert, Edit and Delete floor buttons.

When inserting a new floor or editing an existing floor the following appears.

Parameters which can be programmed for each lift floor are as follows:

- **Floor Name** - This is the name of the floor, and appears (together with the lift/controller name) on transaction reports when the floor goes onto or off security on timezone.

- **Relay** - This is the physical relay number on all the controllers in the bank which will be used for this floor. More information on the Relay Calculator can be found here.

- **Reverse Relay Contacts** - Can be used to make the reverse normal relay operation and make the relays fail-safe.

- **Trigger time** - When a valid credential is presented in the lift this is the amount of time (in seconds) that the relay will operate.
• **Timezone** - This is where the lift level can be put onto a timezone for automatic activation and deactivation of the security on the floor. If the timezone is 0 then the floor will be permanently on security (requiring a credential for access to be granted).

• **Floor destination input** - Where floor destination sensing is available, the ‘input’ used for sensing the destination of the lift is programmed here. The input is normally open (N/O) or normally closed (N/C) can be set here also. More information on the input calculator can be found [here](#).

• **Intercom input** - Each floor can also have defined an optional input used to sense a request for the floor to be desecured by an intercom trigger or exit button of some sort. The input is normally open (N/O) or normally closed (N/C) can be set here also. More information on the input calculator can be found [here](#).

• **Intercom pulse time** - When a floor is triggered from an intercom input, the trigger time is usually longer than when a credential is used within the lift. Accordingly the intercom trigger time can be set here.

• **Intercom timezone** - In some situations it is desired to only make the intercom work during certain hours. This timezone is used to set this (Default 1-Always)

### 4.1.4 Alarms

The CS Technologies system provides a powerful and effective means of integrating access control with alarm systems. The systems can be configured so that credentials automatically disarm and arm associated areas; there are rich features which make programming of effective access control and alarm integration easy, and the system supports thousands of alarm areas and thousands of inputs.

When setting up an alarm controller, if there are readers used for arming or disarming areas then they are set up just like the readers for the door controller (see [here](#)). Alarm readers can be used to unlock doors and also to arm and disarm alarm areas to provide full integration of alarms with access control.

When using Alarms it is possible to use inputs and outputs (relays) from:

• the on-board inputs and outputs on the controller
• 16 way expansion input and output boards
• PIG inputs/outputs – these point identification gadgets provide easy input and output expansion

Note: Where 16-way input and output expansion boards are used the controller ports IN3-IN8, OUT2-OUT4 and PIG1-PIG2 are not available for either readers or PIG connections.

Note: All inputs and outputs must relate to a single door controller so it is not possible for an input on one door controller to trigger an output on another controller.

Alarms are split into two sections. Alarm Areas and Alarms Inputs which are associated with the alarm areas. Before starting work on setting up alarms you first will need to add a door controller (more [here](#)) including any additional relays that are going to be used in the alarm system.
4.1.4.1 Alarm Areas

Once you have added a controller to be used in the alarm system you can come to this menu to add an Alarm Area.

Using this screen areas can be added, edited or deleted.

When adding or editing an alarm area a screen as below will appear.

- **Location** - Set the location that the controller to be used is in.
- **Name** - The name of the area. For example 'Level 1 office' or 'Front Door Break Glass'.
- **Controller** - The controller that this area is part of. This drop-down list will have only controllers which can be used for alarm areas i.e. only door controllers in the set location with the correct firmware.

- **Timezone** - The timezone for an area determines the time period of automatic arming and disarming.

- **Disarm at start/Arm at end** - The timezone from above also works in conjunction with the 'disarm at start' and 'arm at end' check boxes. If the 'disarm at start' box is ticked, then every time this timezone starts the area will disarm. Similarly if the 'arm at end' box is ticked then every time this timezone ends the area will attempt to arm.

- **Arm on Full download** - The area will attempt to arm when a full download to a controller is done.

- **Auto re-arm delay** - When the timezone is not active and the alarm system is deactivated (by a user entering the premises typically), the auto re-arm timer starts. After the delay time expires the alarm system starts an arming sequence, activating the buzzer relay for the buzzer time and thereafter arming the area. Thus using the auto re-arm delay it is possible to ensure that the alarm automatically turns itself back on after hours without any reliance on user interaction.

**Re-arm timer triggered by** - When the auto re-arm timer is running it is possible to re-trigger it (i.e. start the timeout again) by the occurrence of various events. These are:

- **Priority read** - The re-arm timer will be retriggered if a credential is used at a reader associated with this area, as long as that credential has permission to arm and disarm the area in question.

- **Any read** - The re-arm timer will be retriggered if a credential is used at a reader associated with this area, as long as that credential has permission to enter the area in question (whether or not the credential can arm or disarm the area).

- **Activity** - The re-arm timer will be retriggered whenever any input associated with the area changes state. This can be used for example to make the timer retrigger whenever movement is detected within the area.

**Alarm Indication**

- **Alarm Relay A/B/C** - Each controller can have up to three alarm relays. An alarm relay is defined as a relay which operates when the area is armed and one of the inputs in that area becomes abnormal i.e. an alarm occurs.

- **Alarm relay modes** - The mode refers to 'what happens' to the relay when it is triggered by the area going into alarm. There are three possibilities:
  
  - **Latch** – the relay turns on and stays on until the alarm is disarmed. This might be used for something like a strobelight which is intended to indicate that the area has gone into alarm.
  
  - **Pulse** – the relay is triggered for the pulse time (in seconds). This might be used for something like a siren which is intended to be triggered for say 10 minutes when the area goes into alarm.
  
  - **Follow** – the relay 'follows' the alarm status of the inputs in the area. Whenever one of them is 'in alarm' the relay is on; if all of them have returned to their normal state then the relay turns off. This might be used to link the area to a dialler to indicate that the alarm has activated and restored.

- **Pulse on arm** - This is used to indicate the arming and disarming via a siren or strobelight. If this is ticked then for the relevant relay it will 'pulse' for a very short time (about 200ms) on arming, and pulse twice on disarming, to provide audible or visual feedback of the area status changing.
- **Armed relay** - The armed relay is on whenever the area is armed.

- **Disarmed relay** - The disarmed relay is on whenever the area is disarmed. Can be used for lighting control for an area.

- **Buzzer relay** - The buzzer relay is used in conjunction with the 'buzzer time', alarm timezone and re-arm delay. If the buzzer time (below) is set to non-zero, then when the area is armed rather than immediately arming, the buzzer relay will be activated. This is usually connected to a series of sounders which indicate that the alarm is about to turn on.

- **Buzzer time** - The buzzer time can be set from 1 to 255 seconds. If set, then when arming rather than immediately arming the buzzer relay will activate, as a 'pre-alarm' warning to staff that the alarm is about to turn on.

- **Abnormal relay** - The abnormal relay operates whenever an input in the area is abnormal when the area is not armed.

- **Ready LED** - The Ready LED is intended to be used to indicate that the area is 'ready to arm'. If the area is unsealed then the ready LED is off; if all sectors in the area are sealed then the area is ready to arm and the ready LED will turn on. Typically a green LED might be connected for the ready LED.

- **Armed LED** - The Armed LED indicates the armed status of the area. It is off if the area is disarmed, and on if the area is armed. If the area is in alarm then the armed LED flashes. Typically a red LED might be connected for the armed.

- **Pulse Arm/Disarm Relay** - A separate pulsing relay used for indication if an area has been armed/disarmed.

### Auxiliary (PC-Controlled) relays for global lighting and alarm control

In some situations it is desired to have relays operated not on the same controller but associated with the alarm areas. In Evolution the concept of Auxiliary or Global relays meets this need.

There are two different types of global relays – "disarmed" relays and "buzzer" relays. They are used to allow relays on other controllers to operate lighting etc and thus reduce wiring. However note that global relays are operated by the PC so it must be operating for them to work properly.

#### Global disarmed relays

Up to four global disarmed relays can be defined for each area. These relays are defined as being "ON" if the associated area is disarmed. The control of these relays is accomplished by Evolution sending 'unlock' and 'normal' commands. Evolution runs through the relays every second or so. For each relay, if any of the areas is using that relay as a global disarmed relay and the area is disarmed, it will turn the relay on. If no areas that use that relay are disarmed then the relay is turned off. The relays can thus be used for lighting control, to ensure that lights are on whenever any of the associated areas are disarmed.

Select the appropriate disarmed relay from the drop-down list. The drop-down list consists of all doors which are defined in the system including fire doors and other relays.

#### Global buzzer relay

The global buzzer relay is used in conjunction with the timezone for each area, its buzzer time and auto re-arm delay to provide for automation of the after-hours arming of a premises so that common areas can be armed for example.

During the timezone for the area the system operates normally – when users enter their area is disarmed, and when they leave their area is armed. At the end of the timezone however it is possible to set the system to automatically arm the areas as required – areas which have been inadvertently left disarmed (due to users tail-gating or other reasons) will automatically arm. The
units don’t immediately arm however – instead the 'global buzzer relay' turns on. This is linked to some sort of sounder in the premises which warns anyone on site that the system is about to arm. The global buzzer relay operates for the 'buzzer time' which can be up to 4 minutes.

During the buzzer time, if a user wishes to stop the alarm from turning on they simply use their credential at an entry reader. This will disarm their unit and stop the auto-arming sequence. Other units which are auto-arming will continue to do so but the buzzer will stop because there is now a disarmed area in the system.

Now the ‘auto re-arm delay’ comes into action. This can be a time period from 1 minute up to 8 hours in length. At the expiry of this time period the unit will again automatically attempt to arm. The buzzer will operate and warn people on site that the area is about to arm and again they can stop it by using their credential at an entry reader.

It is also possible to set the system so that the global lighting relays will flash during the buzzer time. This provides a visible as well as audible indication of the impending arming of the system.

Select the global buzzer relay from the drop-down list and tick the 'flash' checkbox if desired. If the flash checkbox is selected then the associated global disarmed (lighting) relays will flash during the buzzer time. The flash frequency is set under Technician/Site.

### 4.1.4.2 Alarm Inputs

Once the areas are defined, alarm inputs are added to each area as required using this menu. When this selection is chosen a list of the currently defined alarm inputs is displayed.

![Alarm Input Menu](image)

Individual inputs can be added, edited and deleted by selecting the appropriate buttons on this screen.

Note that when deleting inputs or changing areas for inputs it is wise to follow the programming by initiating a full download, as deletion of inputs is not supported in the firmware; rather a full download is done to clear all the data and load just the required information into the controller.

When editing or adding an input, the input screen is displayed as below.
The information which can be programmed for each alarm input is as follows.

- **Input name** - Enter a descriptive name for the input – e.g. 'North fire door'. This is the description which will appear in any transaction reports associated with this input.

- **Input number** - The input number refers to which piece of hardware is used to terminate this input. More information on the input calculator can be found [here](#).

- **Area** - Select the area that the input belongs to from the drop-down list of currently defined areas. Note that this will also select the controller to which the input is connected, because each area is associated with a particular controller.

- **Input delay** - This parameter is used to select the number of seconds that the input can be 'abnormal' before generating an alarm. It is normally set to 0; if noise on the input is a problem it can be 1 or 2 seconds, and in some circumstances can be defined as a longer delay depending on the requirements.

- **Normally open/closed** - Select the normal state for the input from the available radio buttons.

- **Isolate** - Tick this box to 'isolate' the input i.e. make it inactive.

- **Tamper bypass** - Tick this box to disable the reporting of 'tamper' alarms for this input. When inputs are connected to PIGs then the pigs are constantly scanned for their presence. If they are not found then they are defined as being 'in tamper'. Ticking this box disables the reporting of the tamper alarms for this input.

- **Alarm input or arming input** - These radio buttons allow the functionality of this input to be defined. If the input is a normal alarm input then various parameters can be defined. If the input is an arming input then transactions on this input can be used to arm and/or disarm the area.

### For Arming Inputs

- **Report status change** - If this box is ticked then each time the input changes state a transaction will be reported on the screen. If this is not ticked then only transactions when the area is armed (i.e. alarms) will be reported.

- **Follow/Global Follow Relays** - Relays that will trigger if the input state has been changed regardless of the area settings. There is space for one local and two global relays.
- **Allow forced arming** - If forced arming is allowed, then the area will be able to be armed regardless of the state of this input. If forced arming is not allowed then unless the input is in its normal state the area will not be able to be armed.

- **Auto-isolate** - If forced arming is allowed, then ticking this box will mean that if the area is armed when the input is abnormal it will automatically isolate the input.

- **Auto-include** - If forced arming is allowed, and auto-isolate is ticked then if this box is ticked then the area will be automatically 're-included' in the secured area when it returns to normal. Typically a movement detector will have 'forced arming allowed', 'auto-isolate' and 'auto-include' all ticked. This means that the alarm can always be turned on even if the detector has picked up someone moving in the office, but once it arms it will automatically isolate the input, and then when the detector returns to normal it will be automatically included in the secure area once again.

- **Entry delay** - The entry delay sets the number of seconds that the input can be abnormal when the area is armed before generating an alarm. If the area is disarmed within this amount of time then the input will not cause an alarm. This entry time is intended to provide time to enter the area and turn off the alarm.

- **Exit delay** - The exit delay sets the number of seconds that the input is ignored for after arming.

- **Descriptions** - It is possible to enter the description which appears as part of the transaction log for each of the four possible states of the input – when it becomes abnormal, returns to normal, goes into alarm and restores.

**For Area arm/disarm**

If the input is configured as an 'arming input' then using these check boxes determines the function of the input – whether it arms the area only, disarms the area only or does both arming and disarming.

### 4.1.5 Upload to Controllers

Whenever any programming is done on the software it automatically loads into the controller network – into all controllers which are online at that time. However occasionally it may be required to do programming when a controller is offline or not communicating. Moreover in the event of a controller failure it may be required to fully reload the information to reinstate the controller status with the current programming.

There are several options available for downloading. Whichever option is chosen, a dialog box will appear asking which controller is to be downloaded, or if the download is to apply to all controllers.

- **All programming** - This option clears all information from the controller, sets the controller time
then fully loads all programming into the controller.

- **Users** - This option loads the user information into the controller. Note that it does not delete any users from the controller; it just loads all users into the controller over the top of the existing user list. If a user is already in the controller it will overwrite the information; if a user is not already in the controller it will add it, but users who are in the controller but not in the PC database will not be deleted.

- **Timezones** - This option loads the timezones and public holiday settings into the controller. Again it does not delete any timezones or public holidays from the controller.

- **Access levels** - This option loads the access level information into the controller.

- **Setups** - This option loads the controller, relay, area and input settings into the controller.

- **Clear data** - This option simply clears all information from the controller. Use this option with caution, as all programming will be lost. This clears all users, timezones, access levels and setups from the controller; instead of doing a 'load all' you can select this option (clear data) to clear everything and then download users, timezones, access levels and setups to return the controller to its fully programmed state.

- **Firmware** - Firmware refers to the 'program' which runs inside the 'chip' on the controller board. This is an advanced option which should not be used unless under specific instruction as not all versions of CS Controllers are supported and it could permanently disable the CS controllers.

### 4.1.6 Direct Commands

Direct commands are available as a low level interface directly to the controllers, and are not generally used except by technicians. The direct commands menu is part of the hardware menu.

When this menu selection is made a dialog box appears which allows the entry of direct commands into the controller. There are many different direct commands, and the commands have changed from firmware type to firmware type, so this should only be done if you know what you are doing.

This should not be done in the normal course of events but only under supervision for diagnostic purposes. When a command is entered the 'programming window' will display showing the command and any response from the controller. With some firmware types a response always displays in the programming window, but with other types there is no response and no indication that a command has succeeded or failed.

### 4.2 Technician

The Technician menu allows the setup of all PC hardware related options as well as the more complex technician-related features of the system.

It should only be used by qualified technicians, as parameters within this area can affect the operation of the system and must not be tampered with unnecessarily.
- **Features** - Advanced options for the controller and Evolution software.

- **Utilities** - Provides special utilities to accomplish particular tasks like data conversions.

- **Set Time on One Controller** - This feature can be used by technicians to set the internal time on a single CS controller for testing and diagnostic purposes.

- **Customise** - Allows the system to be customised for a particular vendor including product name, copyright notices and logos for printouts.

- **PC Setup** - Configures the database server and location as well as workstation number and ID.

- **Macros** - Allows programming macros for the additional toolbar buttons as well as actions for alarm acknowledge/alarm timeout.

- **Global Events** - Allows you to link events on one controller to create events on a separate controller.

### 4.2.1 Features

This menu contains some advanced options for the Evolution software and CS Technologies controllers.

#### Software Features

- **Debug** - Bring up additional information in the program window about exactly what the system is doing as programming changes are made

- **Don't Display Tamper Messages** - Disables all tamper warnings for alarms and PIG expansion boards

- **No Alarms for Controller Offline** - Will disable alarms appearing for CS Controllers stopping communication with the Evolution software.

**Self Storage:** These are advanced options for self storage sites. These features require extra licensing where additional information is provided.

**Controller Features**
- **Master Clock** - This will synchronise the CS Controller panel time with the PC time every midnight.

**External Interface**: These are advanced options for interfacing with external programs. It provides options to automatically import and export data. More details on this area are found [here](#).

### 4.2.1.1 External Interface

External interfaces are defined to allow import and export of user and other information to and from other programs. The external interfaces work using defined file formats and basically provide a means to manager the PC3 databases externally, and to export transaction data for processing by other programs.

**Importing information**

**External interface**

Tick this box to enable the external interface for importing of user and other information.

**Interface type**

Currently there are three defined interface types, which are selectable here from a drop-down menu. All interface types involve an external program creating a file which has commands in it in a prescribed format. Evolution scans for the existence of this file and if it exists processes the commands within it. These commands can allow users to be added, deleted etc and provide an easy way to automate the management of the system from another program.

The 'hotel' interface type involves another program creating a file which remains in existence. The file is shared by both the external program and Evolution, with a record pointer indicating the current status of the file. More details of this interface are below.

The 'normal' and 'PTI' interfaces involve the external program creating a file which is consumed by Advent and then deleted. Details of the format of the file are below.

**Lock file name**

Enter the filename of the file which will be used to pass information from another program into PC3. This is usually 'LOCK.DAT' but can be called anything at all. If desired a pathname can also be entered if the file is located elsewhere than in the advent directory.

With the PTI interface the file is usually called GENLINK.FIL.

**Poll time**

Enter the time in seconds between scans for the existence of the 'lock file name'. This is typically set to 5 seconds which means that PC3 looks for the file every 5 seconds.

**Timeout**

Enter the time in seconds that PC3 will wait for an exchange of data from the external program before raising an alarm that the interface is down. This is only relevant for the 'hotel' type interface.

**User import options**

When importing data, these options provide an easy way to manage the access levels assigned to users if they already exist in the database. The dialog box below is displayed.
The options here are fairly self-explanatory.

The first three options relate to what to do if an imported user is already in the database – the access level can be changed to the imported access level, the imported access level can be ignored, or the imported access level can be ignored unless it is a prescribed value.

For example there may be an existing database of users, but the external program may send through cards to be 'deleted' – in this case the existing database would prevail unless the cards sent through have an access level of 0 in which case they will be deleted.

The second group of options describes what to do if the imported card is not already in the database. The imported access level can be used, or the imported cards can be assigned a default access level.

**Import file format – Hotel interface**

The hotel format consists of a file which is created by the external program. The file contains records in the following format (in the 'C' programming language):

```c
typedef struct {
    char type;
    char room[4];
    char name[20];
    char cardno[5];
} HOTEL_REC;
```

The full record has 30 bytes in it.

The file contains 500 of these records. The first two records are special, in that they are defined as the 'in' and 'out' pointers for the records in the file. For these two records the 'cardno' information in the record is a text string containing the value of either the 'in pointer' (record 0) or 'out pointer' (record 1). These pointer values can be from 2 to 499.

The 'type' of records is either 'A', 'D' or 'L. If 'A' then the information refers to an 'add user' request. If 'D' then the information refers to a 'delete user' request'. If 'L' then the information is a 'link test' request used to verify that the interface is working.

The external program writes records into this file and updates the in pointer; PC3 reads records from the file and updates the out pointer.

If an 'A' record then the room number, name and card number are used to update the transaction record. The room number is linked to an access level via the ‘room database’ settings under
Setup/Room Database. This menu only appears if an external interface of type 'hotel' is active in the system.

If a 'D' record then the user in the system with the card number specified in the record is deleted (if they exist).
If a 'L' record then the transaction is used to retrigger the 'interface timeout' time.

Extensive debugging information on the process of reading the hotel interface file can be obtained by enabling 'debug' in the Technician/Features menu. This will give information on the opening, locking, updating, unlocking and reading of the interface file each time it is processed.

**Import file format - Normal interface**

The normal format is slightly easier to process than the hotel format, because it does not require both programs to access the interface file simultaneously. With the normal format, the external program simply writes the interface file whenever it needs to, and then Advent, which is looking for the file all the time, sees it, reads it and then deletes it.

The interface file for normal format contains lines of comma-delimited text. Each line in the file is a command to Advent to allow some sort of manipulation of the database. Lines which are not in any recognisable format are ignored. When the file has been fully processed it is deleted.

Commands which are available in the normal interface format are:

**Timezones**

\[ \text{T,<TZNUM>,<START>,<END>,<DAYS>} \text{ (standard timezone)} \]
\[ \text{T,<TZNUM>,<S1>+<S2>+S3>+…+<S8>} \text{ (extended timezone)} \]

This command is used to program timezones. The first 'T' command received will delete the existing timezone file (both standard and extended timezones) (STZ.DAT, ETZ.DAT).
TZNUM refers to the timezone number which is to be added. This number is 2-20 for standard timezones, and 21-40 for extended timezones.
If the timezone number is 2-20 (standard timezone) then the start and end time are processed as colon-delimited 24-hour times (e.g. 15:00 for 3pm), and the Days field is processed as a string of digits indicating the days on which the timezone is valid. For example

\[ \text{T,2,09:00,17:00,12345 <CR>} \text{ - would program timezone 2 as 9am-5pm Monday to Friday.} \]

If the timezone number is 21-40 (extended timezone) then the following field is interpreted as a list of standard timezones which will link together to make the extended timezone. For example

\[ \text{T,21,2+3+5+0+0+0+0+0 <CR>} \text{ - would program timezone 21 as the combination of timezone 2, 3 and 5.} \]

**Access levels**

\[ \text{A,<ALNUM>,<C1-D1-T1>,<C2-D2-T2>,…,<Cn-Dn-Tn>} \]

This command is used to program access levels. The first 'A' command received will delete the existing access level files (ACCESS.DAT, DAL.DAT, DALEL.DAT, CAL.DAT, CALINST.DAT).
ALNUM refers to the access level number which is to be added.
The following fields are a list of controller, door number and timezone number. An access level is built up of these combinations. There is no limit to the number of combinations which make up an access level.
A,2,1-1,1-2-1 <CR> would program access level 2 as doors 1 and 2 in controller 1 with timezone 1.

**Users**

\[ \text{U,RESET} \]
This command clears the user database of all users.

**U,<CREDENTIAL>,<NAME>,<ACCESS LEVEL>,<DATA 1>**

This command adds a user with the appropriate information. The <credential> is stored in a field in the user database depending on the type of the first controller defined – if the controller is a 'KEY' controller then it will be stored in the key number field; if it is 'CARD' or 'ABACARD' then it will be stored in the card number field; if it is 'PIN' then it will be stored in the PIN field. The <data 1> and <data 2> fields are 8 characters in width and will be stored in the optional user data fields (enabled under Administration/Titles).

Note that because the data is comma delimited it is not possible to insert commas within the user names using this command.

U,1234,BLOGGS JOE,1,54321 <CR> would add user with credential 1234, name BLOGGS JOE, access level 1 and data field 1 (could be employee number for example) 54321.

**U,<CREDENTIAL>,DELETE**

This command deletes the appropriate user if it exists.

**Member magic interface**

The 'Member Magic' interface works with software for club management created by Thyme Software. It is similar to the 'U' command but provides extra flexibility in the definition of the credential type.

**M,RESET**

This command clears the user database of all users.

**M,<CREDENTIAL>,<TYPE>,<NAME>,<ACCESS LEVEL>,<DATA 1>**

This command adds a user with the appropriate information.

CREDENTIAL is the key, card or PIN number (the full 32 bits including site code if applicable for a card system).

TYPE is C for a card, K for a key and P for a PIN. It determines the field in the user database which is used to store the credential.

NAME is the name of the user.

ACCESS LEVEL is the access level number for this user.

DATA 1 is the first optional data field.

When adding a user with the M command the importing 'rules' as set up under Technician/Features/User Import Options are followed when assigning access levels. Also, if the specified credential is not found the system searches for someone with the same name; if this is not found a new user is created.

M,1234,P,BLOGGS JOE,1,54321 <CR> would add user with PIN 1234, name BLOGGS JOE, access level 1, and data field 1 (could be employee number for example) 54321.

**M,<CREDENTIAL>,<TYPE>,DELETE**

This command searches for a user with the appropriate credential (taking into account the type C, K or P) and deletes if it exists.

**Pulse club interface**

This special interface format is used when interfacing to a Pulse Club Management software package. It provides some extra flexibility in the definition of user names (allows commas within the name because it is pipe delimited), and also matches access level information by the access level name rather than number. This allows club member classifications to correspond exactly with access level name definitions in Advent.

**P|RESET**

This command clears the user database of all users.

**P|<CREDENTIAL>|<TYPE>|<USERNAME>|<ACCESS LEVEL NAME>|<DATA 1>|<DATA 2>|<ACTIVATION DATE>|<ACTIVATION TIME>|<DEACTIVATION DATE>|<DEACTIVATION TIME>**

This command adds a new user to the system.

CREDENTIAL is the key, card or PIN number (the full 32 bits including the site code if applicable
for a card system). TYPE is C for a card, K for a key and P for a PIN. It determines the field in the user database which is used to store the credential.

USERNAME is the name of the user.

ACCESS LEVEL NAME is the name of the access level. If this name doesn't exist in the access level list the message will be ignored.

DATA 1 is the first optional data field.

DATA 2 is the second optional data field.

ACTIVATION DATE/ ACTIVATION TIME is for when the user is activated in the format of DDMMYY and HHMM respectively.

DEACTIVATION DATE/ DEACTIVATION TIME is for when the user is deactivated in the format DDMMYY and HHMM respectively.

P|1234|P|BLOGGS, JOE|STAFF|54321 <CR> would add a user named BLOGGS, JOE with a PIN 1234 to the access level called STAFF and give him data 1 (say employee number) 54321.

**Caravan Park interface**

The 'Z' command, which requires caravan park licensing, accepts commands in the following format:

Z|CARDNUMBER|C|EXPIRY DATE|EXPIRY TIME

This is used by RMS to set the expiry date and time without any other parameters.

**Self storage interface**

This interface is used when interfacing with Self Storage software. It allows downloading of user information as well as associated alarm areas for disarming and arming.

**S,RESET**

This command removes all users from the database. It is usually issued prior to a full download from the Self Storage software.

S,0,VACANT,<UNIT>,0,0

This command vacates a unit – deletes the access of all users to that unit. For each user if this is the only unit to which they have access then the user is deleted, and the unit is marked as vacant.

S,<CREDENTIAL>,<NAME>,<UNIT>,0/1,<ACCESS LEVEL>,<ACTIVATION DATE>,<ACTIVATION TIME>,<EXPIRY DATE>,<EXPIRY TIME>

This command adds or modifies the access of a particular user.

CREDENTIAL is the key, card or PIN for that user.

NAME is the name of the user.

UNIT is a string consisting of a unit number (i.e. an area name). The system tracks units by number, and if additional users have access to a particular unit they come through the interface with a letter appended to the end e.g. 110 for the first user who has access to unit 110, 110A for the second user, 110B for the third and so on.

0/1 is 0 to lock that user out, 1 to activate that user.

ACCESS LEVEL corresponds to the access level that the users are to be assigned. With Evolution the access levels 0 and 1 are predefined whereas in Self Storage Software the access levels 0 and 1 can be used for anything; accordingly all the access levels sent through the interface are incremented by 1. Access level 1 from the interface corresponds to Advent access level 2 and so on.

The logic used when adding or modifying a user through this interface is as follows:

- if the area name corresponding to the numeric part of <UNIT> exists, mark it as occupied.
- If a user exists with the same <UNIT>, change the user's name and credential and access level in accordance with the command. If a user exists with the same credential then delete it to ensure integrity (the same credential cannot be used twice). If the 0/1 is 0 then make the access level 0 otherwise make it the <ACCESS LEVEL> plus 1. Similarly set the lift access level to the same value.
- If no user exists with the same <UNIT>, check whether that same credential is used by another user. If so, we are adding a new unit to an existing user so just add the unit to that user, changing the name if necessary.
- If we haven't added it yet, just check whether a credential exists with the same name and if so
just add the unit to that user.

- Otherwise just add the user to the database.

<ACTIVATION DATE>/<DEACTIVATION DATE> is the date the user is activated/deactivated. The format of the date is in DDMMYY.

<ACTIVATION TIME>/<DEACTIVATION TIME> is the time that the user is activated/deactivated. The format of time is in HHMM.

Thus the key field for determining whether a the 'S' message corresponds to an existing user is the UNIT. The next priority is given to the CREDENTIAL and then the NAME. If no match is found in any of these a new user is added.

**Release door commands**

It is possible via the external interface to release doors on the first controller. Up to four doors can be connected to this controller.

**R,<DOOR>**

This will trigger the door (1-4) on controller 1 for its release time.

**Import area and input information**

It is possible to import area and associated input information. With a self storage system there can be hundreds or even thousands of areas. In general each area has a single associated input. This information can be defined in the self storage software or indeed in a text file with the format below to make definition of areas and inputs easy.

The format of the import command is as follows.

**I,RESET**

This command will delete all of the areas and inputs in the database. Use with care!

**I,<UNIT>,<CONTROLLER>,<INPUT NO>,A/B,<DISARMED RELAY>,<ALARM RELAY>**

This command adds an area to the system as well as an input which is part of that area. UNIT is the area name. This must be numeric.

CONTROLLER is the controller number that the area is part of. This controller must exist in the database prior to the import being done.

INPUT NO is the input number which is part of this area. The input is usually a PIG number.

A/B is A for port A on the PIG or B for port B on the pig

DISARMED RELAY is the relay on this controller which is to be turned on if the area is disarmed. This is NOT the global disarmed relay but rather the relay on that controller (1-4 or 0 if no disarmed relay).

ALARM RELAY is the relay on this controller which is to be turned on if the area is in alarm. 1-4 or 0 for no alarm relay.

**Import file format - PTI interface**

This file format is associated with Space Control self storage management software. This software creates a file under a PTI gate interface generally called GENLINK.FIL stored in the C:\PTI directory.

The format of this file is as follows. Each line is ASCII text 64 characters in length.
When used with Advent, if the status is '0' then the unit is vacated and all associated users are denied access to that unit.

If the opcode is 'D' then the associated user is deleted.

If the unit exists set it as occupied. We then take the 'Password' field and add the user name and access level offset by 1 as with the 'S' interface.

### Exporting information

These options exist to allow transaction information to be captured by another program for processing. For example a time and attendance/payroll package can capture the data and process it to produce timesheets.

When exporting transactions the appropriate file is created or appended to every time a transaction is logged to the screen. The files are standard text files. If the file exists a line is added to it; if the file doesn't exist it is created and the line added. External programs can thus scan for the file, read it and delete it if necessary.

**Export transactions**

Tick this box to enable the exporting of transactions.

**Format**

Select the desired export format from the drop down list. Currently supported export formats are:

- **Simplex** – a 'pipe' delimited format for transactions designed to be compatible with the Simplex time and attendance packages.

- **Self Storage** – a comma-delimited format for transactions designed for import into Self Storage package. This is the most versatile format for import into other programs including Excel®. Details of the formats are below.

**Export filename**

Enter the filename (including path if desired) of the file into which the transactions are to be written.

**Export file formats**
Simplex

The Simplex file format is used with the Simplex time and attendance software. It contains several fields most of which are not used in the PC3 application. The format is as follows:

```
<BLANK3>YYYYMMDD|HHMM00|00|<CREDENTIAL>|<BLANK11>|000000|0000|0000|
<NAME>|<BLANK6>|<BLANK6>|0|0|<READER6>|<READER6>|<READER6>|</READER6>|</READER6>|</READER6>
<READER6>|</READER12>|</CR></LF>
```

BLANKKn is a string of space (blank) characters - e.g. blank6 means 6 spaces and so on.

YYYYMMDD is the year of the transaction

HHMM is the time of the transaction in 24 hour time

CREDENTIAL is the credential number, as an 11 character string

NAME is the user name, as a 15 character string

READER6 is the first 6 characters of the reader name, padded with blanks if necessary

READER12 is the first 12 characters of the reader name, padded with blanks if necessary

Self Storage

The Self Storage file format is used with numerous self storage management software, but is useful for importing to Excel or a database program. Only access (granted or denied) transactions are sent through into the transaction file. The format is as follows:

```
DD/MM/YYYY,HH:MM,<NAME>,<CREDENTIAL>,<DOOR>,<G>,<DATA1>,
<DATA2><CR><LF>
```

DD/MM/YYYY is the date of the transaction

HH:MM is the time of the transaction

NAME is the user name

CREDENTIAL is the key, card or PIN used

DOOR is the name of the door

G is 1 for access granted, 0 for access denied

DATA1 and DATA2 are the optional data fields (if enabled under Administration/Titles).
4.2.2 Utilities

This section contains small executables that may need to be used for some advanced Evolution functions.

![Utilities Menu]

Reinitialise controller access levels (CALs)
This option is used if it is suspected that there is some corruption in the controller access level database. It clears the controller access levels and then recalculates them based on the door access level information.

The controller access levels are a mapping from the door access levels into the individual controllers. Because the CS Technologies database is fully distributed across the controllers, only users and access levels applicable to each individual controller are loaded into each controller. These users and access levels are calculated each time the controller is downloaded, and are stored in the CAL and CALINST data files. This menu option deletes these files and recalculates them in the event of any corruption.

Following this procedure a full download of all controllers must be undertaken.

Verify a user database (clear duplicates)
Checks the user database for any duplicates and deletes them.

Reinitialise Controller timezones
This recreates and sorts all timezones within a system. This is normally done if a timezone has been deleted from the system.

PIG registration wizard
The pig registration wizard is used for adding in PIG2 and PIG3 devices.

- **Registration controller** – Select the controller, which is being used to add the PIG devices.
- **Starting area number** – PIG devices can be assigned to an area.
- **Clear areas/inputs** – This deletes all areas and inputs from the database.
- **2 input pigs** – Select this if PIG2 devices are being added.
- **Input plus relay** – Select this if PIG3 devices are being added.
- **Single port pigs** – Select this if single port pigs are being added.
- **Inputs normally closed** – Select this if PIG3 relay contacts are either normally closed. If they are normally open, do not select this check box.
• **All inputs in a single area** – Selecting this will add all PIG devices to the same area.

**Reindex areas and inputs**
This recreates and sorts all areas and inputs within a system. This is normally done if an area or input has been deleted from the system.

**Export/Import Users as CSV File**
Will import/export all users in the system as a CSV (comma separated value) file

### 4.2.3 Set Time On One Controller

This feature can be used by technicians to set the internal time on a single CS controller for testing and diagnostic purposes.

![Set time on one controller](image)

- **Controller** - Select the controller that you would like to edit.
- **Time** - Set the time on the selected controller
- **Date** - Set the date for the selected controller

### 4.2.4 Customise

This menu option allows the customisation of the Evolution software. The product name and associated copyright and technical support strings can be customised, and a custom logo can be defined for the report printouts. This changes what appears on the Help --> About screen as well as the report printout header and footer.

The standard Help --> About screen is shown below.

![Customise](image)
The customise menu selection will display the following dialog.

- **Customise** - Tick this box to make the settings on this page active.

- **Program title 1** - Enter the name of the program. The default setting is EVOLUTION.

- **Program title 2** - Enter the description of the program. The default setting is Access Control Software.

- **Copyright 1** - Enter the first line of the copyright string.

- **Copyright 2** - Enter the second line of the copyright string. The default setting is Tel: +61 2 9809 5176 Fax: +61 2 9809 2446.

- **Support 1** - Enter the first line of the support string. The default setting is email: sales@cstech.biz

- **Support 2** - Enter the second line of the support string. The default setting is web: www.cstech.biz

- **Logo filename** - Enter the filename of the logo. This must be a .BMP filename which must be located in the same directory as the Evolution program.

### 4.2.5 PC Setup

PC Setup menu is used to set the type of workstation and location of the database files is set.

- **PC number** - Set the PC number. This number defines the workstation (or comms server) to which controllers are connected. PC number 1 is set to be the main PC and has options to
define how many other PC’s are associated with this location

- **Number Of PCs** - Only if PC Number is set to ‘1’ will this option appear. Allows you to set how many other workstations are set on this location and using the same database.

- **Remote Database** - Only enabled if PC number is set to ‘1’. If unchecked the Evolution software will run from its default location (C:\CSTECH\Evolution), is selected will allow the database to be located elsewhere, such as a network drive.

- **Programming Enabled** - Only available if PC number is set to anything other than ‘1’. This asks if the current workstation is allowed to modify the database or just view it.

- **Database Location** - Only available if PC number is set to ‘1’ and Remote Database is selected, or PC number is set to anything other than ‘1’. This allows you to set the location of the Evolution database.

- **Background Timer** - Timing value of the Evolution software on the CPU. Recommended default is 30 ms but a higher number can decrease the load on the PC's CPU.

### 4.2.6 Macros

The Macros menu allows definition of macros for the system. Macros are pre-programmed commands which can be executed from the PC either from customised toolbar buttons or related to alarm acknowledgement activity.

Selecting the Macros option will show the list of currently defined macros.

![Macros Screen](image)

By using the Add, Edit or Delete buttons macros can be added, edited or deleted.

When editing a macro the following screen will appear.
- **Name** - Enter the name of the macro. This description appears as a new entry in the Administration menu.

- **Type [Button]** - Button is the most common type of macro. Up to 20 button macros can be defined. Button macros appear under the Administration menu and are automatically assigned a keyboard shortcut. They can also be assigned an icon which appears as a toolbar button in the toolbar menu.

- **Type [Instant Alarm]** - The instant alarm macro defines something which occurs as soon as any alarm happens (as long as the software is running on the PC). Only one instant alarm macro can be defined.

- **Type [Delayed alarm]** - The delayed alarm macro defines activity which occurs a time delay (defined in the macro) after an instant alarm unless it has been silenced or acknowledged in the meantime. Only one delayed alarm macro can be defined.

- **Type [When acknowledge]** - The When Acknowledge alarm macro defines activity which occurs whenever an alarm is acknowledged. Together with the instant alarm and delayed alarm macros, the system can be set up to activate a sounder immediately an alarm occurs (via the instant alarm) and to silence this sounder when the alarm is acknowledged on the PC. If the alarm is not acknowledged within a certain time another relay can operate via the delayed alarm macro to send a message to a monitoring station via a dialler. Only one 'when acknowledge' macro can be defined.

- **Number** - Select the macro number (1-20) from the drop-down list.

- **Icon** - This drop-down list is used with 'button' macros to define the icon which is displayed on the toolbar for each macro. Currently defined icons are:

- **Delay time (seconds)** - This field is only available with the 'delayed alarm' macro. It defines the number of seconds after an alarm occurs that the delayed alarm action will be initiated by the PC.

**Commands**

This lists the commands which will be issued by the PC when this macro executes. Up to 20 commands can be included in the list, which is manipulated by using the Add, Edit and Delete buttons.

Commands which can be initiated have three parameters:
- **Type** - The type of a command can be Door, Area or Input

- **Select** - Once the type is chosen then this drop-down list will allow selection from the list of all defined items of that type in the database. For example, if 'type' is set to Area then the 'Select' list will consist of all the areas in the database.

Under the select list there will also be an extra item at the end which consists of all of the items of that type in the database. For example if 'type' is set to Door, the 'select' list will have all the doors individually listed plus an entry at the end designated as 'all doors'.

- **Action** - This is where the activity which is to occur is defined. The actions are different for each type.

- **Door actions** - Possible door actions are Trigger, Unlock, Lock Down and Make Normal

- **Area actions** - Possible area actions are Arm and Disarm.

- **Input actions** - Possible input actions are Isolate and De-Isolate.

Notes on macros

It is important to understand that when macros are executed it is exactly the same as if those commands were issued from the Devices menu. The PC sends commands to the controllers to perform the appropriate activities. Thus the PC must be operating for the actions to occur, and the transactions are recorded as though an operator had performed them.

### 4.2.7 Global Events

The global events window can be used to sound an alarm when a certain event or action occurs at a site.

- **Name** – Give an appropriate name for the global event

- **When** – From this list the user can choose from the following,

- **Type** - Select the type of device this event is programmed for (Door, area, relay, Input or other)

- **Object** - Depending on the type chosen, this drop down menu will display the appropriate objects related to that type. Eg: if type doors is chosen, then object will list all doors that are in the system.

- **Event** - User can choose from a list of events based on type and what events.

- **Do** - The user can choose alarm only, thus when the particular event occurs an alarm is turned on.
4.3 Input/Output Calculators

Input and Output (Relay) calculators are used to help determine the input number from what pins are actually wired up in the hardware.

**INPUT CALCULATOR**

Select the type of input (Main board, expansion board or PIG) by choosing the appropriate radio button.

- **Input [Main Board]** - If the input is on the main board, select the pin on the controller board itself where the input is terminated. On-board inputs are numbered 1-8 (IN1-IN8), 9-12 (OUT1-OUT4) and 13-14 (PIG1-PIG2).

- **Input [Expansion Board]** - If the input is on an expansion board, select the appropriate board number (set by the rotary dial on the board) and input number.

- **Input [PIG]** - If the input is on a PIG the PIG number can be entered. If it is a PIG2 then select whether it is port A or B. PIG numbers can also be determined by clicking on the 'touch' button; when this is clicked you have 30 seconds to touch the PIG to the registration pig bus. The registration bus is defined as any configured PIG bus on the 'registration controller' (defined here) which has only 1 PIG connected to it.

**RELAY CALCULATOR**

Select the type of input (Main board, 4-way expansion board, 16-way expansion or PIG) by choosing the appropriate radio button.

- **Relay [Main Board]** - If the Relay is on the main board, select from one of the 4 available.

- **Relay [4-Way Expansion Board]** - If the relay is on a 4-Way expansion board, select the appropriate relay number. Note only a maximum of 3 of these boards can be added. For information on how the relays are numbered please see the 4-way expansion installation guide.

- **Relay [16-Way Expansion Board]** - If the relay is on an expansion board, select the appropriate board number (set by the rotary dial on the board) and relay number.
- **Relay [PIG]** - If the input is on a PIG the PIG number can be entered. PIG relays are only found on PIG3 devices where the relay is always on port A. PIG numbers can also be determined by clicking on the 'touch' button; when this is clicked you have 30 seconds to touch the PIG to the registration pig bus. The registration bus is defined as any configured PIG bus on the 'registration controller' (defined [here](#)) which has only 1 PIG connected to it.