CEM SYSTEMS
From Tyco Security Products

Getting Started Guide

AC2000 v8.0

A2SE8-UG-0316-1

Notice

The information in this manual was correct at the time of publication. Tyco Security Products reserves the right to modify this product. All specifications are subject to change without notice.

Trademarks

The trademarks, logos, and service marks displayed on this document are registered in the United States (or other countries). Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region. Contact your sales representative for more information.

Licence information

Your use of this product is governed by certain terms and conditions.

Support

If you require technical assistance using CEM products, please contact the CEM Support team using the following telephone number:

Telephone:+44(0)2890 456656

Email: cem.support@tycoint.com

- Please provide our support engineers with as much information as possible. This may include:
- Site name
- Product name and model
- CEM software version
- Description of the problem

Publication Date

April 2017

Contents

Chapter 1
Using the guide

1.1 Introduction

This book can be used as an introductory step-by-step guide to setting up a basic AC2000 system, with the aim of validating a card and using it to achieve a valid swipe at an attached reader for the first time. The guide covers only the most basic functions of each of the applications used in this process. For information on additional application functionality, see the **AC2000 Setup Guide**.

1.2 Prerequisites

Following a successful installation, AC2000 is ready for configuration. The following hardware is required:

- Devices, including a connection to the validation reader if you want to set up a VIPPS (Visual Imaging and Pass Production System) workstation
- Readable card

The following hardware can be included as part of the system setup, but its use is not covered by this book:

- Printer: To print a card design on to a card
- Camera: To record a personnel portrait on the system

Other information necessary is:

- Connection details for the validation reader
- Device address information
  - It is important to carefully plan the setup for the devices, including physical location, description, and IP address if ethernet readers are being used
- A company logo image file in JPEG, BMP, TGA, or TIFF format
  - This logo file is included on the company record

1.3 The AC2000 system

The AC2000 system can consist of multiple servers and devices that communicate with each other using ethernet or serial communications.

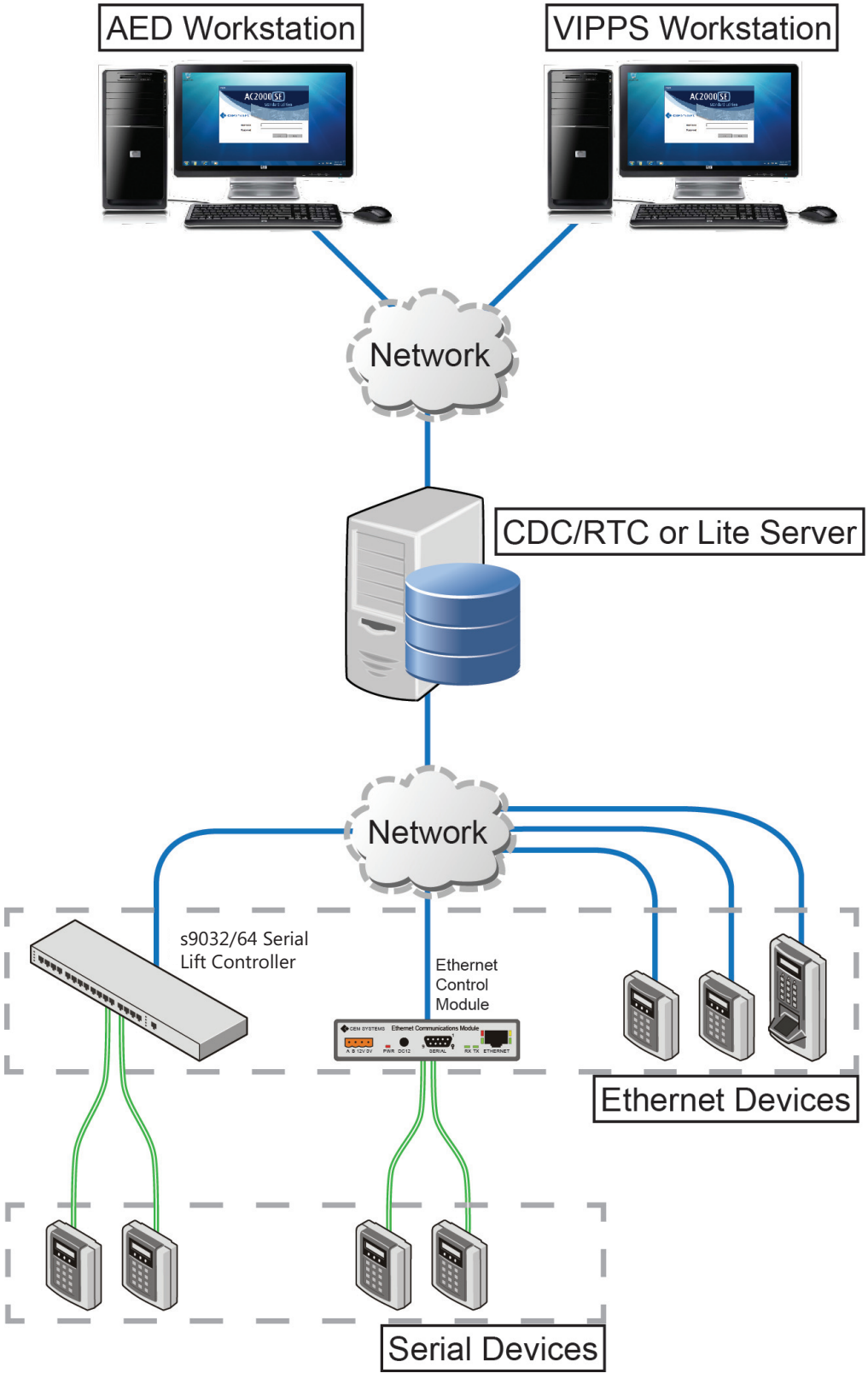

Figure 1 Illustration of an AC2000 network

1.4 Key AC2000 terminology

This guide uses CEM specific terminology throughout, this list contains a brief description of the most commonly used terms.

CDC	The Central Database Computer is the database that stores all AC2000 data. It is central to the system. All device, controller, user, cardholder, and alarm information is stored on the server.
RTC	The Real Time Computer communicates with the ethernet devices on the system. Configuration updates are made on the CDC and passed through the RTC to relevant devices on the AC2000 network. Alarms and real time events at the devices are passed through the RTC to the CDC.
Lift Controller	The s9032/64 lift controller can control 2 lift readers and 2 LCIs.
ECM	The Ethernet Control Module provides a means of including serial devices on an ethernet network. The ECM communicates with the CDC/RTC or Lite Controller through ethernet and can control up to 16 serial devices.
CDC / RTC	The majority of systems use a single server to host both the CDC and RTC software. The CDC and RTC still operate as separate entities, but with the benefits of only having one server to purchase and maintain.
Workstations	A workstation is a desktop PC that runs the AC2000 software to set up, configure and administrate the system. These workstations can be as generic or specialised as required, with functionality limited per user. This means that a single workstation may be an AED Workstation, a VIPPS Workstation or any other possible connotation as controlled by the applications that any given user can access.
AED Workstation	The Alarm & Event Display Workstation is a reference to a workstation that is specifically used for monitoring and responding to alarms and events on the system.
VIPPS Workstation	The Visual Imaging and Pass Production System Workstation is a reference to a workstation that is specifically used for capturing images, creating cardholder records and printing cards on the system.
Validation Reader	A Validation Reader is a specialist reader that is used with a VIPPS Workstation to validate a card. Validation is the name given to the process of assigning a card to a specific cardholder record.

1.5 Guide structure

The guide is structured to lead users through the steps required to set up a basic AC2000 system in the most efficient order.

Important: When using the Getting Started wizard, ensure that each step is completed before moving on to the next. Initial setup involves many interconnected applications, many of which are dependent on prerequisite steps being completed before they can be used.

1.5.1 The Getting Started Wizard

Use Getting Started Wizard to set up AC2000.

To open Getting Started Wizard, complete the following steps:

1. Log in to the AC2000 application as user **cem**.

Note: If you do not know the password, contact CEM Support.

2. From the **AC2000 Floatbar**, click **Administration**, and click **Getting Started**.

Use the wizard to perform the following tasks:

- Configure the validation reader attached to the system.
- Perform the initial setup applications in the correct order.

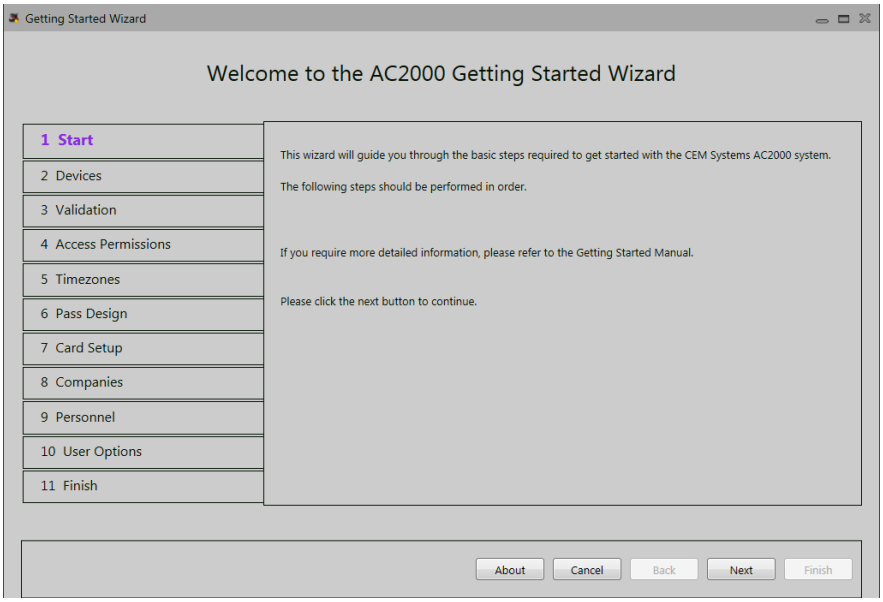

Figure 2 The Getting Started Wizard interface

Important: The wizard is not used to configure the applications, but can be used to launch them. For the purposes of this manual, the wizard is only used to configure the validation reader.

1.5.2 Navigating through the wizard

Each step in the wizard must be navigated in order. The left pane highlights the name of application that is currently open and the right pane contains information about the application. Each application also has a button to launch the application and a button to open the help file.

To use the wizard, complete the following steps:

1. When the current step is complete, click **Next** to move on to the next step.

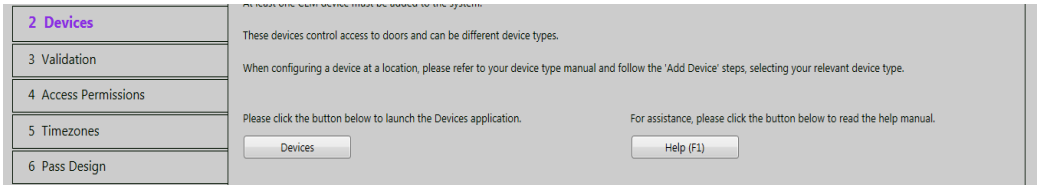

Figure 3 Example screen capture of an application screen in the wizard

2. To open the application, click the button with the application name. In the example show, in Figure 3, Devices is the application.

Note: The wizard launches the application with full functionality.

3. To open the help file for the selected application, click **Help**.

4. When all steps are complete, click **Finish** to close the **Getting Started Wizard**.

Important: This guide has been written to be used independently from the wizard. However, it is recommended that the wizard be used for the validation step as this simplifies the process.

1.6 Initial Setup Process Flow

The following flowchart describes the flow of the steps required to perform the basic configuration of an AC2000 system.

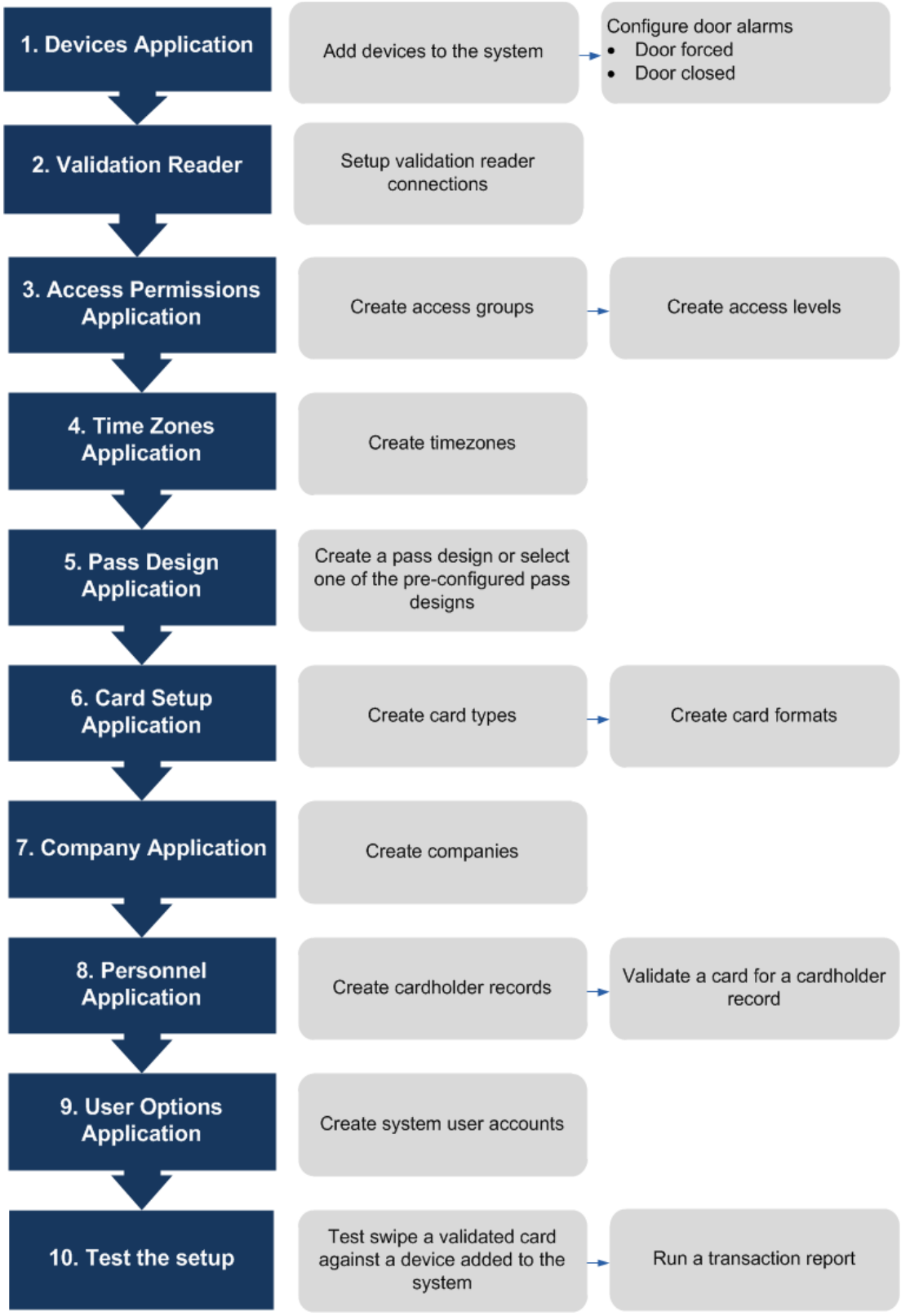

Figure 4 The Getting Started process flow

Chapter 2
Devices

2.1 Introduction

Use the Devices application to set up and configure all access control devices used in the AC2000 system. You can also use it to set up and configure device inputs for the purpose of triggering alarms on the real time monitoring applications, such as Alarm + Event Display and Rolling Transaction Display.

Note: If you are using a partitioned system, see the **Partitioning** manual.

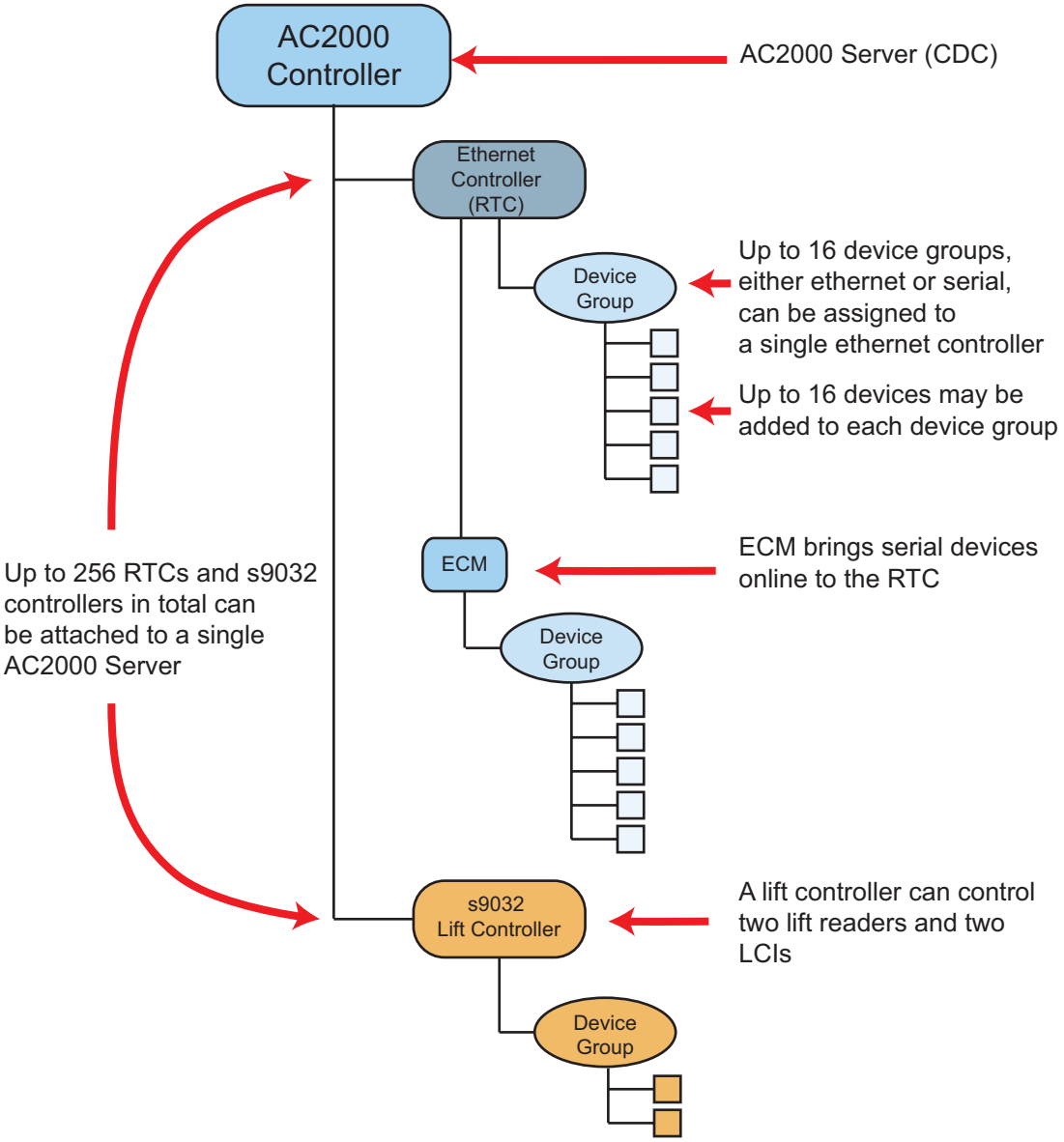

Figure 5 Illustration of the AC2000 devices hierarchy

2.2 Controllers

You can add serial lift controllers and ethernet controllers to the AC2000 system. Controllers control messages between the Central Database Computer (CDC) and the individual readers.

Ethernet controllers (RTCs)

Use ethernet controllers (RTCs) to manage up to 256 ethernet or serial devices grouped together into 16 groups of 16. The controllers relay device-specific data between the AC2000 database and the devices, including configuration, alarms, and events.

Lift controllers (s9032)

A lift controller is an s9032 controller that is set in lift mode. In this mode, the s9032 can support up to 2 lift devices. When adding an s9032 as a lift controller in the Devices application, the location must start with the letters “LCM”. For more information, see the **Lift Controller** manual.

Ethernet Control Module (ECM)

The ECM provides a means of including serial devices on an ethernet network. The ECM communicates with the CDC, RTC or Lite Controller through ethernet and can control up to 16 serial devices. For more information, see the **ECM Quick Guide**.

2.3 Adding an RTC

Note: The most common setup of AC2000 is as a CDC/RTC. You only need to add an RTC to AC2000 if a site has a standalone CDC or needs to add an extra RTC.

To add an RTC, complete the following steps:

1. In **Devices**, from the left pane, click **AC2000**.
2. Click **Add**, and click **Add Controller**.
3. Enter the relevant information for the controller and click **Add**.

Important: The controller must be initialised using AC2000 WEB. See the **AC2000 WEB** manual for details.

2.4 Adding a lift controller

Important: Controllers can only be added to AC2000 Standard and Airport Edition.

For more information on lift controllers, see the **Lift Controller** manual.

2.5 Configuring devices

All readers connected to AC2000 are added to an ethernet or lift controller. It is essential that all exit and auxiliary devices are also added.

Ethernet devices have extended properties that need to be completed.

2.5.1 Adding a device

To add a device, complete the following steps:

1. In **Devices**, select the controller and device group to add the device to from the overview pane.

2. Click **Add** and select **Add device**. Alternatively, right-click the device group and select **Add Device**.
3. Configure the parameters of the Settings pane and the Extended pane. For more information, see *Settings* on page 13 and *Extended properties* on page 14.

Settings

The following settings must be completed for both serial and ethernet devices. To do this, select a device and edit the Settings pane on the right of the window:

Device Number:

Select a device number for the device. This forms part of the device address. Only numbers that have not been used are available.

Device Location:

Enter a unique description of the location of this device.

Slave Location:

Where a slave device has been included in the Device Type, Slave Location appears. Enter a unique description of the Location of the Slave device.

2nd Location:

This option only appears for the EDCM 300/350 MAST/MAST and SDCM 300/350 MAST/MAST device types. Enter a unique description for the second location of the device.

Device Family:

Select the device family from the drop-down list for the access control terminal.

Device Type:

Select the specific type of device from the drop-down box, which has been filtered by the choice of Device Family in the drop-down above it.

Note: If an exit or auxiliary device is to be added to the master reader, select the correct **Device type**. For example, a **600E** device with an Exit Reader would have a **Device type** of **600E+Slave**. This configures the Master device with an attached slave device.

Any Exit reader added to a Master appears as a child node in the Overview Pane of the Master reader to which it is associated.

Configuration Mode: Select the Configuration Mode from the drop-down list.

Note: Configuration Mode contains default settings, however these can be user defined.

Priority of Alarms:

In a range of 0 to 8999, the alarms of a device can be given a greater priority than the defaulted 0. This escalates the alarms from the device in AED or Security Hub.

Maintenance Mode:

Select the box if alarms generated from this device are to be ignored until maintenance or installation is completed. If selected, all alarms generated are ignored in AED and Security Hub. unless selected in those applications.

Restricted Reader:

This field is used to indicate that the reader is restricted. This is not available in AC2000 Lite Edition.

Soft Anti-Passback:

Enabling this field sets the reader into soft anti-passback mode. This means that the same card can be used twice in a row to gain access but an alarm is sent to the Alarm + Event Display application.

Look at Camera (emerald terminals only)

Enabling this field means that a cardholder must look at a camera after a valid card swipe. A guard monitoring the camera sends a One Shot command to the terminal to open the door.

Time and Attendance:

This field is used to indicate that it is being used for Time and Attendance monitoring. This is not available in Lite or Standard Edition.

Extended properties

This section is only for ethernet devices.

MAC Address:

Enter the unique MAC address of the device.

IP Address:

Enter the unique IP address of the device.

Offline Database:

Select the appropriate offline database for the device. **Card Number** offers an offline database of card numbers only. **Card Number**, **Timezone**, **Status**, **PIN** provides the named detail in the offline database. This is the default selection.

Threat Level Properties

If threat levels has been enabled on the system the option to assign a reader to a threat level group will become available. The group to which the reader is to be assigned should be selected from the menu.

Note: Threat level groups are created and configured in the Threat Level Def application.

2.6 Device inputs

AC2000 handles two different types of alarms on the system:

- Internal input alarms that are generated by the system when specific criteria have been met.
- External input alarms that are generated by input state changes on the readers.

Internal input alarms

Internal input alarms are alarms that are generated by the system. Each of the alarms have been pre-configured by CEM Systems to be activated on particular events, for example, a Door Held alarm. This alarm is generated by the system when a door which has been opened fails to close in the pre-defined Close Time period.

External input alarms

External input alarms are associated to input sensors outside of the system, such as Door Position Sensors, Break Glass, and Request to Exits. Each external alarm that is to be monitored must be configured in Devices Inputs and associated to the correct change of state, either Open or Closed, and Tamper if 4-state is being used.

The following is an example of how a typical door is configured. Each of the numbered items represents different external and input devices which, when wired to the input of a reader, represent external input alarms. Exceptions 1 and 2 are the DIU and reader.

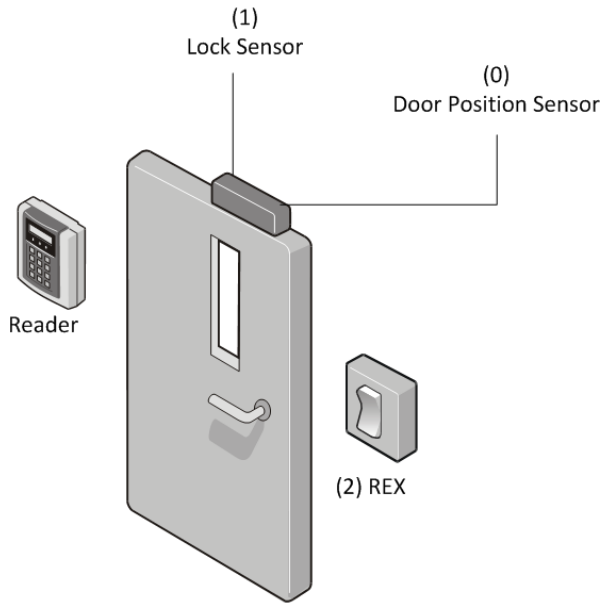

Figure 6 Illustration of door input positioning

Reserved inputs

External Inputs can be further classified under CEM Reserved Inputs or Normal (General Purpose). The following 4 Inputs are CEM Reserved, however each can be reconfigured to be a General Purpose input:

Input Number	Input Name	Input State	Alarm Type
0	Door position sensor	Open Closed	Door forced Door closed
1	Lock sensor (disabled by default)	Open Closed	Lock not engaged Lock engaged
2	REX	Open Closed	
3	Interlock / General purpose	Open Closed	

Table 1: CEM reserved inputs

No alarms are required to be configured for Input 2 and 3. However it is possible to assign alarms to them.

Note: Input 3 is set to interlock when normal is unchecked.

2.7 Mapping alarms to device inputs

This section details how to map alarms to inputs. To create an alarm, consult the **Alarm Configuration** chapter in the **Operator Guide**.

To map alarms to inputs, complete the following steps:

1. In **Devices**, select the device to which an alarm for an input is to be applied from the devices tree on the left.

2. Select the **Inputs** tab.

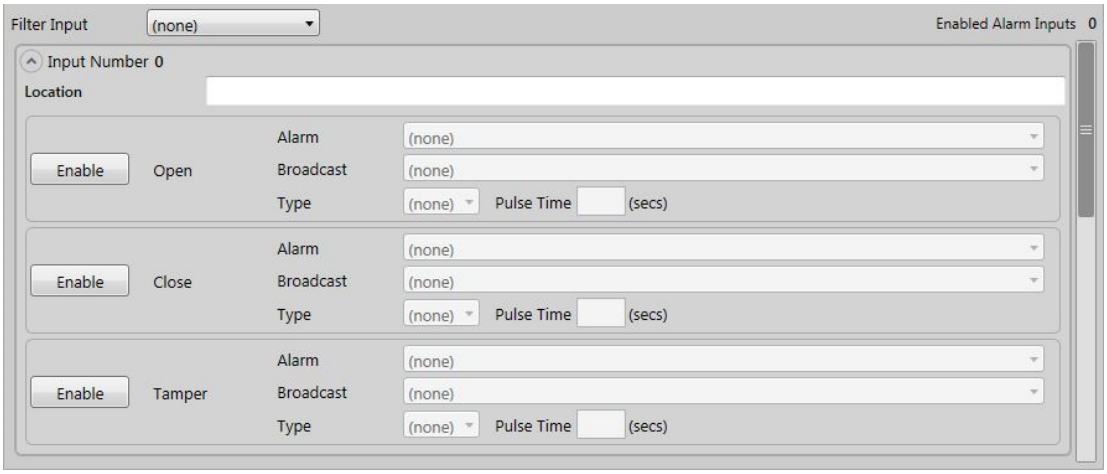

Figure 7 Input configuration pane

3. Select an input. The details of that input expands.
4. In the **Location** field, type a location.
5. Click the **Enable** button on each state that you want to enable for that input.
6. Select the relevant **Alarm** for each state using the drop-down lists.
7. Click **Save** to apply the configured Device Inputs.

Chapter 3
Validation

3.1 Introduction

Before a card can be used to access readers, it must be validated against a cardholder. Cards can be validated manually using a validation reader that is attached to the workstation. The card validation readers must be set up first using the **Getting Started Wizard**.

To get to this part of the wizard, complete the following steps:

1. From the **Getting Started Wizard**, navigate to **Validation**.

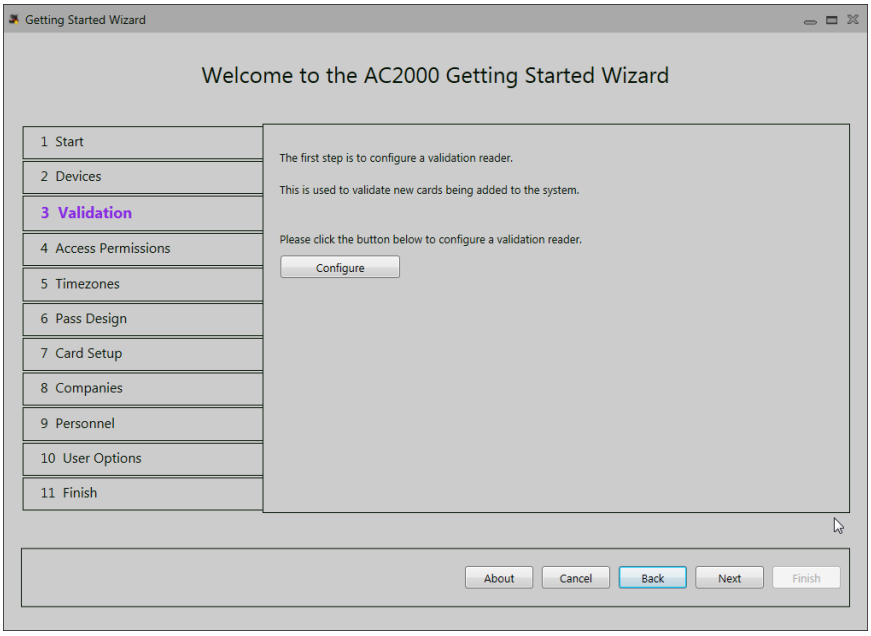

Figure 10 Validation pane

2. Click **Configure**.
3. Select the type of validation reader.
   - If the reader is a serial device, complete the following steps:
     a. Select the **AC2000 Serial** radio button.
     b. Enter the port number being used by the validation reader. It can not be longer than two characters. For more information, see the validation reader quick guide.
     c. Click **Update**.
     d. Click **Close**.
   - If the reader is an biometric device, complete the following steps:
     a. Select the **AC2000 Fingerprint** radio button.
     b. Enter the **IP Address** of the validation reader.
     c. Click **Update**.
     d. Click **Close**.
   - If the reader is an online reader, do the following:

a. Select **AC2000 Online Reader**.

b. Enter the 5-digit AC2000 device address of the reader.

c. Click **Update**.

d. Click **Close**.

– If the reader is another type of validation device, do the following:

a. Select the **Other** radio button.

b. Refer to the manufacturer's guide for configuring the validation reader.

c. Click **Close**.

4. If you are using the wizard to open the applications, click **Next** to move to the next step. If you are finished with the wizard, click the **Next** button until the **Finish** pane is displayed. Click **Finish**.

Chapter 4
Access Permissions

4.1 Introduction

Use the Access Permissions application to organise access control devices into meaningful access groups that can be assigned to cardholders using access levels. You can also use the application to manage floor allocation for CEM Systems Lift Controllers.

Note: If you are using a partitioned system, see the **Partitioning** manual.

4.2 Access groups

Access groups are collections of readers arranged into logical categories. It is recommended that these groups are organised and described as geographical locations. For example, a group of readers controlling access to a reception area might be named Reception. In Figure 11, two access groups have been created containing devices related in their geographic location and access function.

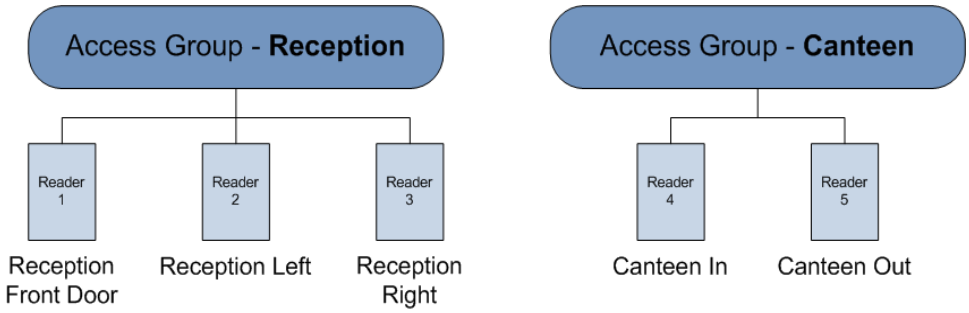

Figure 11 Illustrative example of Access Group creation

4.3 Access levels

Access levels are the primary means of controlling cardholder access on a site. It is recommended that access levels are representative of human resource or personnel hierarchy on a site. For example, access levels might be created for management, IT staff, general staff, contractors, and more. In the example shown in Figure 12, the access level General Staff has been allocated both the Reception and Canteen access groups, whereas Contractors has only been allocated the Reception access group.

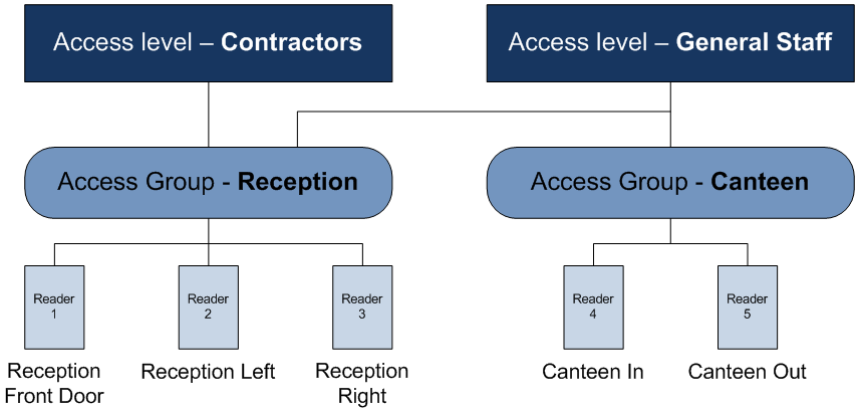

Figure 12 Illustrative example of Access Level creation

4.4 Adding an access group

To add an access group, complete the following steps:

1. Click the **Access Groups** tab.
2. Click **Add**.
3. Enter a descriptive name for the access group. It is recommended that this description is representative of a geographic location, for example, Server room, Lobby, and so on.
4. Select the readers to add.
5. If lift floors are to be added to the device group, complete the following steps:
    1. Click the **Floors** tab.
    2. Select the floors to add.
6. Click **Save**.

4.5 Adding an access level

To add an access level, complete the following steps:

1. Click the **Access Levels** tab.
2. Click **Add**.
3. Enter a descriptive name for the access level. It is recommended that this description is representative of an HR or personnel function.
4. Click the access groups to be added to the level by selecting the corresponding check boxes of the device groups. If the required access group does not exist, you can create it by clicking the **New Access Group** option on the access level dialog box.
5. Click **Save**.

The access levels are listed in the left information pane. A white arrow denotes list entries that are expandable. Click the arrow to expand the list. A dark grey arrow denotes an expanded list.

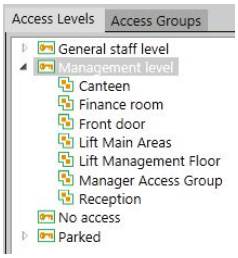

Figure 13 Diagram showing Access Levels with assigned and unassigned access groups

Chapter 5
Timezones

5.1 Introduction

The Timezones + Holidays application is used to create timezones and holiday periods to control cardholder access to controlled areas within specific dates and times.

Note: If you are using a partitioned system, see the **Partitioning** manual.

5.2 Timezones

It is probable that multiple timezones are required to control access on a site. Timezones grant access to assigned cardholders within the days and times laid out in the timezone. For example, the following site requires three timezones.

- Timezone 1: Day Staff and grant access from Monday to Friday between the times of 8am and 6pm.

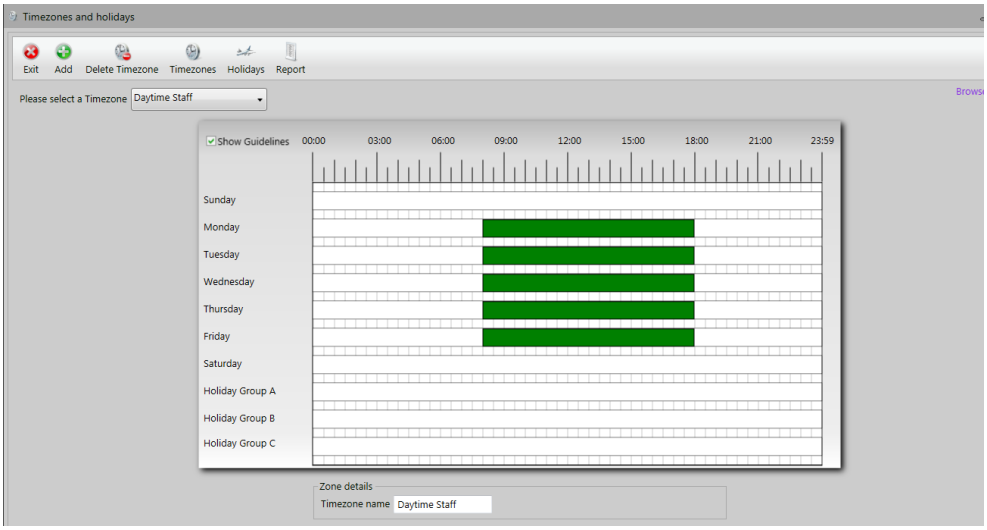

Figure 14 Example Mon - Fri, 8am - 6pm timezone

- Timezone 2: Evening Staff and grant access from Monday to Friday between the times of 5pm and 11pm.

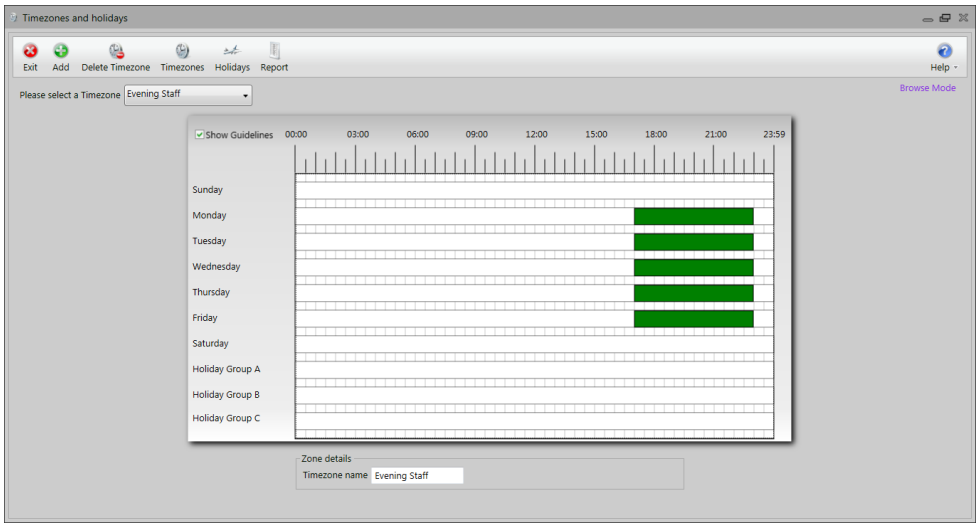

Figure 15 Example Mon - Fri, 5pm - 11pm timezone

- Timezone 3: ALL THE TIME and grants access every day all day. This timezone is set up by default on a newly installed system.

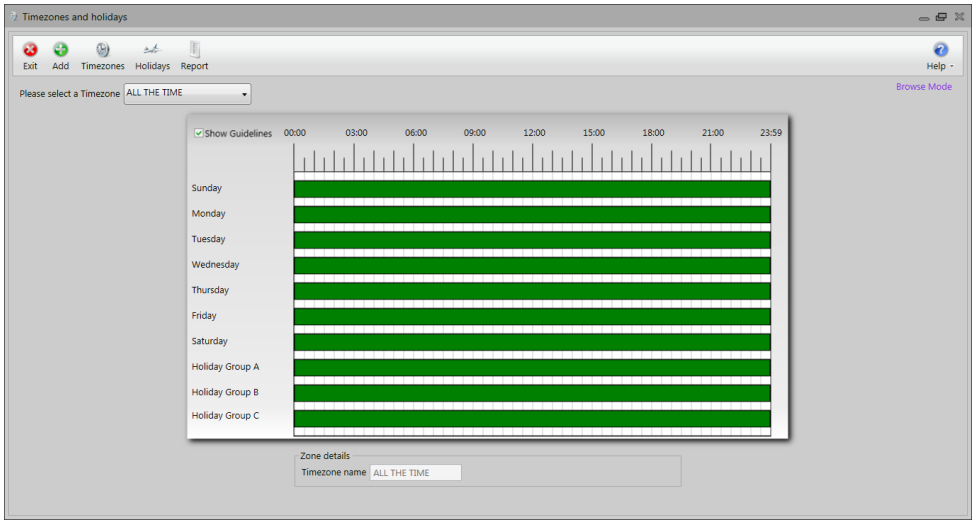

Figure 16 Example All The Time timezone

5.2.1 Creating a timezone

To create a timezone, complete the following steps:

1. From the toolbar, click **Add**.
2. Type the name of the new timezone in the **Timezone name** field at the bottom of the pane.
3. Click in the day sector to be configured for the timezone in the approximate region of the required start time.

Figure 17 Screen capture of a newly inserted timezone section

4. Using the handles on the left and right of the inserted segment, drag the segment to the desired start and end times.

5. Configure the times as required by using the up and down arrows next to the **Start Time** and **End Time** fields at the bottom right of the screen.

Figure 18 Screen capture of the Start Time and End Time fields

Note: The **Start Time** seconds always displays 00 and the **End Time** seconds always displays 59.

6. Repeat the steps for each individual day and time sector required. If the same time sector is to be used on multiple days, it can simply be copied from one day to the other.

   i. Select the time sector to be copied.

   ii. Drag the time sector to the day where it is required.

   iii. Repeat for each similar day.

7. Multiple time sectors can be accommodated in any day. To do this, complete steps 4 - 7 but using a different insertion point within the day.

Figure 19 Example of a multiple time sectors in one day

Note: A maximum of 10 unique time sectors can be created in the application. If time sectors are repeated, it is important to use the copy technique rather than create a new sector manually because an error of even one minute creates a unique time sector that contributes to the application total.

8. When the timezone sectors have been completed, click **Save**.

Chapter 6
Pass Design

6.1 Introduction

Use the Pass Design application to create unique card designs that can be printed on to access control cards. You can create multiple designs assigned to them different card formats, which in turn can be assigned to different cardholders.

Note: If you are using a partitioned system, consult the Partitioning manual.

6.2 Using a default pass design

AC2000 provides default pass designs. Use a default pass design for a quick setup or if you are not going to print the passes.

To use a default pass design, complete the following steps:

1. In **Pass Design**, click **File**, and select **Load Badge**.
2. Select a pass file. The following pass files are available:
   - visitors
   - portrait
   - landscape
   - permits
   - vehicles
3. Click **Open**.

6.3 Creating a pass design

The following section explains how to create a new card design with the most commonly used features of the application.

To create a new pass design, complete the following steps:

1. Click **File**, and click **New**.
2. Enter a file name for the design, a maximum length of 20 characters.
3. Click **Create**. The **Badge Layout** dialog box opens.

6.3.1 Configuring the badge layout

To configure the badge layout, complete the following steps:

1. Configure the **Badge size** parameters.

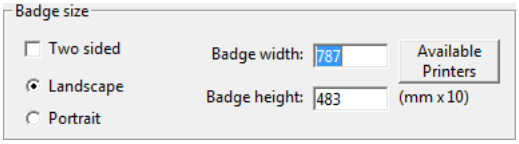

Figure 20 Badge size parameters

2. Select whether you want to use a simple mono-colour background or a background image by leaving the **Use shared image file** check box blank or populated respectively.

Note: Where a manufacturer has printed the background image or colour unto the card, it is possible to prevent these from being printed, by clearing the **Print background** check box.

3. Select whether to include a plain border around the outside of the pass design.

4. The SQL button is used to bring data into the pass design from tables other than the default **Personnel** table.

Important: It is recommended that you contact CEM support team if this functionality is required.

5. Select the **Magnetic encoding options**. These options are used to encode up to three segments of data on the magnetic strip of a compatible card. This information takes the format of dynamic fields from the **Personnel** application, for example, card format or expiry date.

6. When all **Badge Layout** properties have been configured, click **OK**.

6.3.2 Adding text fields to a design

Text controls can be either static or dynamic. If the control you place is dynamic, there are some additional options available.

Adding a static text field to a design

Static fields are always printed, regardless of the cardholder. For example, a static control can be placed adjacent to a dynamic control to indicate what the dynamic control is displaying. For example, a static control can display the “Date of Birth” of a cardholder beside a dynamic control that displays a date value for that same cardholder.

To add text fields to a design, complete the following steps:

1. Click and drag the text object to the design canvas from the toolbar. The **Text Properties** dialog box is displayed.

Note: Text object properties are displayed when the object is first added to the canvas. It can also be displayed by double-clicking on an object already placed, or by selecting the object and clicking **Edit** and **Control Properties**.

2. With the **Static text** radio button checked, type the information you want displayed into the **Static text** field.

3. Set the **text background** properties.

4. Set the **text foreground** properties.

5. A more precise positioning of text can be accomplished by using the **Position** tab.

Resizing placed objects

When an object such as a text field has been placed, it can be resized using the yellow handles attached to the object. To resize or move an object, complete the following steps:

Figure 21 Object resizing handles

1. Click and hold its perimeter points, a 2 headed arrow appears; move the mouse in the desired direction and, when you are satisfied with the size of the object, release the mouse button. This resizes the object.
2. Click and hold anywhere within the perimeter of the object, and drag it to required location. Alternatively, position the object using the **Position** tab parameters. This moves the object.

Adding a dynamic text field to a design

Dynamic text is used to add database fields to a pass design. This can be done by adding a single field or using the expression builder.

To add a dynamic text field to a design, complete the following steps:

1. Dynamic text is created as a single field.
   i. Select **Dynamic text**. This changes the property window.

Figure 22 Dynamic text selection check box screen

   ii. Select the field from the database to be inserted from the drop-down list. The list of available fields is dependent on the SQL that is generated for the card design.
   iii. Enter **Sample text**. This can be used to preview what text can look like during a print.

Chapter 7
Card Setup

7.1 Introduction

Use the Card Setup application to view, edit, and add card types and card formats.

Note: If you are using a partitioned system, see the **Partitioning** manual.

7.1.1 Card definitions

Card definitions define how the card must be read when presented to a reader. Card definitions are added to the system using the Card Setup application.

7.1.2 Card types

A card type is used to assign the global properties of a card, such as its hotstamp number, reading configuration, and validation type. A system can have multiple card types, these are named according to site specific criteria.

For example, a site might two card types. The first card type is a readable permanent card type for staff to gain access to controlled areas. The second card type is a non-readable vehicles card type. It is not used to grant access at readers directly. It is printed and displayed on a vehicle in order to provide security personnel at barrier controls with visual confirmation that the vehicle is registered on the system and has access rights.

7.1.3 Card formats

Each card type created on an AC2000 system can have multiple card formats attached. Card formats are assigned to cardholders and control factors such as which access levels the cardholder can be assigned and the length of time for which the card is valid.

Figure 23 Illustration of the Card Setup hierarchy

7.2 Adding a card type

To add a card type, complete the following steps:

1. From the **Card Setup** toolbar, click **Add Card Type**.
2. In the **Description** field, type a description for the new card type.
3. Select the **Readable** check box if the card is readable.

Note: Readable cards can be read by access control devices. If you want the card type to control access using readers, it must be readable.

4. From the **Validation Options** drop-down menu, select the validation option for the card. For more information, see *Validation options* on page 29.

Note: If the card type is not readable, validation options are not available.

5. If you want the card type to be exportable from one AC2000 system to another, select the **Exportable** check box.
6. If you want the hotstamp to auto-generate, select the **Auto-Generate Hotstamp** check box.

Note: It is important to establish whether hotstamp numbers are printed on the cards being used. If the hotstamp number is printed on the card, that number must be used and the auto-generate field left blank. If the card is blank, auto-generate should be used and the Pass Design configured to print the generated number on to the card.

7. In the **Minimum hotstamp** field, type the first hotstamp number in the range for the card type.

Note: Card types that auto-generate hotstamp numbers must have a unique hotstamp number range. Card types that do not auto-generate hotstamp numbers can have overlapping hotstamp ranges.

8. In the **Maximum hotstamp** field, type the last hotstamp number in the range for the card type.
9. Select **Save**.

Note: When a card format, belonging to the selected card type, is assigned to a cardholder, the following fields can no longer be edited:

- Exportable
- Auto-Generate Hotstamp
- Readable
- Validation Options

7.2.1 Validation options

Validation is the process of associating a card with a cardholder record. This is typically accomplished by swiping a card on a validation reader next to the card issuing workstation. This table describes card validation options.

Validation option	Description
CUSTOM DESFIRE	This is a customer-specific validation option. The Desfire option is not used for validation of Desfire cards. It is used specifically for personalising Desfire information. If this option is required, please contact CEM support.
GEN CNUM & BIO	If the cards do not have internal card numbers, this option generates a number at the validation stage. The fingerprint of the cardholder is captured as part of the validation process.
GENERATE CARD NUM	If the cards do not have internal card numbers, this option generates a number at the validation stage. This is most often used when printing barcode cards.
HK JOCKEY CLUB	This is a customer-specific validation option.
ONLINE READER	Enables a card to be validated by swiping it on any online reader connected to the AC2000 network. The online reader must possess the same read head technology as the card being validated.
READ AES UID	Enables an AES card to be validated by an Omnikey reader.
READ CARD NUM	Validates the card by reading the internal card number.
READ CNUM & BIO	Validates the card by reading the internal card number. The fingerprint information of the cardholder is captured as part of the process.
SALTO SHIP	Enables a card to be validated by swiping it on any online Salto SHIP validation reader connected to the AC2000 network.

Table 2: Validation options

7.3 Adding a card format

To add a card format, complete the following steps:

1. In **Card Setup**, from the list of card types in the left pane, select the existing **Card Type** to which you want to associate the card format. When you add the card format, the card type selected in the left pane expands to display all card formats associated with it.
2. From the **Card Setup** toolbar, click **Add Card Format**.
3. In the **Description** field, type a description for the card format.
4. From the **Application** drop-down list, select the application in which the format is to be used. The options are as follows: **Personnel**, **Permits**, **Vehicles**, or **Visitors**.
5. Select the pass design that will be printed on the card. You can add designs in the Pass Design application or select a default pass design.
6. If the card format is the default format for the selected application, select the **Default format for application** check box.
7. Select whether or not the cards are reusable. A reusable card may be returned to the system using the Personnel, Visitors, or Vehicles applications when the card is no longer required by the cardholder. This means the card can then be associated with another cardholder record. This is not an option normally used on a system that is printing cardholder information on cards.
8. Select the default number of valid days.

Note: This is the number of days for which the card is valid. When a card exceeds this number of days from validation, it must be revalidated. This can be extended up to the maximum number of valid days. For example, when you select the card format in Personnel, the application sets the expiry date to the start date plus the default number of valid days. The expiry date can be changed to any date up to the start date plus the maximum number of valid days.

9. Select the maximum number of valid days that can be attributed to a card using this card format in Personnel.
10. Set the number of about to expire days before expiry. This field denotes how many days before expiry the cardholder will see an “About to Expire” message on readers.
11. Set the number of days after expiry when purged. This is the number of days after the card expires when the card will be purged from the database. When a card is purged the cardholder record is not removed from the system, but the details of the card are removed.
12. From the **Access levels not used by format pane**, select which access levels can be used with the card format by selecting the relevant check boxes.
    Note: If the card type is readable, you must select at least one access level to proceed. If the card is non-readable, this pane is not available.
13. **Optional:** Select which access level should be used as **Default Access Level** for the card format.
14. **Optional:** Select the time zone should be used as **Default Timezone** for the card format.
15. Click **Save**. The new card format is displayed in the list panel.

Note: All card formats have the **Parked** access level assigned to them automatically on creation.

Chapter 8
Company

8.1 Introduction

Use the Company application to create and manage company records and authorisers.

Note: If you are using a partitioned system, see the **Partitioning** manual.

8.2 Adding a company record

To add a company record to the system, complete the following steps:

1. Click **Add**.
2. Configure the parameters of the Company Information pane. For more information, see Parameters of the Company Information pane on page 31.
3. If required, complete the fields of the **Contact Details** tab to add the primary contact for the company.
4. Click **Save**.

8.2.1 Parameters of the Company Information pane

This table describes the parameters of the Company Information pane.

Parameter	Description
Partition	Defines the partition of the company in a partitioned system. This field is not editable.
Company	The left **Company** field defines the ID of the company. The right **Company** field defines the name of the company.
Previous Company Name	Defines the previous name of the company. This field is not editable when adding a new company record.
Address	Defines the address of the company.
Postcode	Defines the postcode of the company.
Telephone	Defines the telephone number of the company.
Ext	Defines a contact extension number for the company.
Fax	Defines the fax number of the company.

Table 3: Descriptions of the Company Information pane parameters

8.2.2 Importing a company logo

When you add a company record, you can import a company logo image that can be incorporated into the card design. It is recommended that you import a logo after you have saved the new company information. Alternatively search for and display the company record, and then add the logo.

Note: To add a company logo, you must enable the function in the Workstation Configuration Tool. For more information, see the **Workstation Configuration Tool** manual.

To import a company logo, complete the following steps:

1. Perform a search for the company to which you want to add a company logo.
2. When the correct record is displayed, in the Company Logo pane, click **Capture Logo**. The **Capture an image** application is launched.
3. In the **Capture an image** window, click **Import**.
4. Navigate to the logo, select the logo, and click **Open**.
5. If required, use the image editing tools on the right of the window.
6. Click **Save** and click **Close**. The logo is displayed in Company Logo pane. The date the logo was added is displayed below.

Chapter 9
Personnel

9.1 Introduction

Use the Personnel application to view, edit, and add the personal, employment, and card data for all personnel. You can issue more than one card to the record of a cardholder. You can assign more than one company to the record of a cardholder.

Note: If you are using a partitioned system, see the **Partitioning** manual.

9.2 Prerequisites

Before adding personnel records to the system using Personnel, ensure the following prerequisites are met:

- At least one company record has been added to the system in the Company application
- Times zones have been added to the system in the Timezones + Holidays application
- Access levels have been added to the system in the Access Permissions application
- Card types and card formats have been added to the system using the Card Setup application

9.3 Adding a cardholder record

To add a cardholder record, complete the following steps:

1. From the **Personnel** toolbar, click **Add**.
2. Configure the personal details of the cardholder in the Personnel Details pane.
3. Configure the parameters of the Employment Details pane. For more information, see *Parameters of the Employment Details pane* on page 34.
4. Configure the parameters of the Card Details pane. For more information, see *Parameters of the Card Details pane* on page 34.
5. Click **Save**.
6. You can add multiple cards to one cardholder record. To add another card, click the small green add icon at the top right of the Card Details pane and repeat steps 4 and 5.

9.3.1 Parameters of the Employment Details pane

This table describes the parameters of the Employment Details pane.

Parameter	Description
Company	Defines the company or companies assigned to the cardholder. From the **Company** drop-down list, select one or more companies. If you select more than one company, the **Company Information** window opens. If the employee has a different job title or works for a different department in each company, select each company and configure the **Job Title** and **Department** fields. Click **Apply**. **Note:** If more than one company is assigned to a cardholder, the number of companies is displayed in a new label next to the **Company** field.
Department	Defines the department of the cardholder for the company selected in the **Company** parameter.
Job Title	Defines the job title of the cardholder for the company selected in the **Company** parameter.
Payroll Number	Defines the payroll number of the cardholder.
Contact Num	Defines a contact number for the cardholder.
PIN	Defines the PIN for the cardholder to be used on PIN access readers.
Special Usage	Defines that the cardholder is given extra time to pass through a door after a reader has been swiped.
Last Device	Defines the AC2000 address of the last device the cardholder accessed.
Last Time	Defines the last time the cardholder presented a card at an access control reader.

Table 4: Employment Details pane

9.3.2 Parameters of the Card Details pane

This table describes the parameters of the Card Details pane.

Parameter	Description
Card Format	Defines the card format the cardholder's new card is assigned.
Access Level	Defines the access level assigned to the cardholder's card.
Timezone	Defines the time the cardholder can gain access using this card.
Start Date	Defines the start date of the cardholder's card.
Expiry Date	Defines the expiry date of the cardholder's card.
Card Status	Defines the status of the card. When adding a card, the default card status is **(none)**. After the card is validated, more options become available to choose from in the **Card Status** drop-down menu. For more information, see *Card Status* on page 35.
Reason	Defines the reason for issuing the card and the charge associated with it, if any. **Note:** If this field is required and is not displayed, ensure the **enable_charging** value is set to **Y** in Configured.
Total Cards	The total number of cards in the cardholder record. This parameter is not editable.

Table 5: Describing Card Details parameters

Parameter	Description
Card Serial	The serial number of the card.
Hotstamp	Defines the hotstamp number of the card. If the hotstamp is auto-generated, the field is blank and the label **Generated** is displayed next to the field.
Added By	The name of the user that added the card. This parameter is not editable.
Creation Date	The date the card was added. This parameter is not editable.
Pass Print Date	The date the card was printed. This parameter is not editable.
Authoriser	Defines the name of the authoriser for the company. **Note**: If this field is not displayed, you need to enable authorisers. Enable the **Authoriser** function in the Configured application. To do this, set the **using_authorisers** value to **Y**. Add an authoriser to a company record in the Company application.
Company	Defines the company to which the card is assigned.
Last Update Time	The date the card details were last updated. This parameter is not editable.
Last Updated By	The name of the user that last updated the card details. This parameter is not editable.

Table 5: Describing Card Details parameters

9.3.3 Card Status

This table describes the card status values.

Card Status	Description
(none)	Defines the default card status of a card.
Current	Defines the status of a card after it has been validated.
Lost/Stolen	Defines that the card has been lost or stolen. If the card is used at a reader, it will not provide access.
Not Yet Operational	Defines that the cardholder's start date is a future date.
About to Expire	Defines that the card is set to expiry within a set period of time. This value depends on the About to expire days value for the selected card format. This value is set in Card Setup. For more information, see the Card Setup chapter in this guide.
Expired	Defines that the **Expiry Date** of the card has passed.
Purged	Defines that the card has not been used for a set period of time or that a reusable card has been returned.

Table 6: Card Status values

9.4 Capturing a portrait

To add a portrait image, you must enable the function in the Workstation Configuration Tool. See the **Workstation Configuration Tool** manual for more information.

To add a portrait image to the cardholder record, complete the following steps:

1. Perform a search for the cardholder. For more information, see *Searching for a cardholder record* on page 36.

2. When you hover the cursor over the empty grey box on the right-hand side of the pane, the words **Capture Portrait** and an image of a camera are displayed in the box. Click the box to open the **Capture an image** application.
3. In the **Capture an image** window, click **Import**.
4. Navigate to the image, select the image, and click **Open**.
5. If required, use the image editing tools on the right of the window.
6. Click **Save** and click **Close**. The image is displayed in the portrait box. The date the image was added is displayed below the image.

9.5 Searching for a cardholder record

When you search for a cardholder record, the first matching record is displayed. Use the navigation arrows, as shown in Figure 24, to search the results. Use the previous and next arrows to skip between each individual record in the order that they are saved. Use the first and last arrows to jump quickly to the first record or the last record. Click the **List view** icon to generate a report containing a list of the results.

Figure 24 Navigation arrows

Enter valid search criteria in to any of the available fields. If you do not enter search criteria, all cardholder records are returned in the results. Depending on the number of cardholders, this can take longer than specifying search criteria. It is recommended that you enter one or more search criterion to filter the results and reduce the time taken to return them.

To search for a cardholder record, complete the following steps:

1. In **Personnel**, click **Search**.
2. Enter one or more search criterion and click **Apply**.
3. If no search criteria is entered, click **Yes** to acknowledge the warning message.

4. If more than one record is found in the search, use the navigation arrows to locate the correct cardholder record.

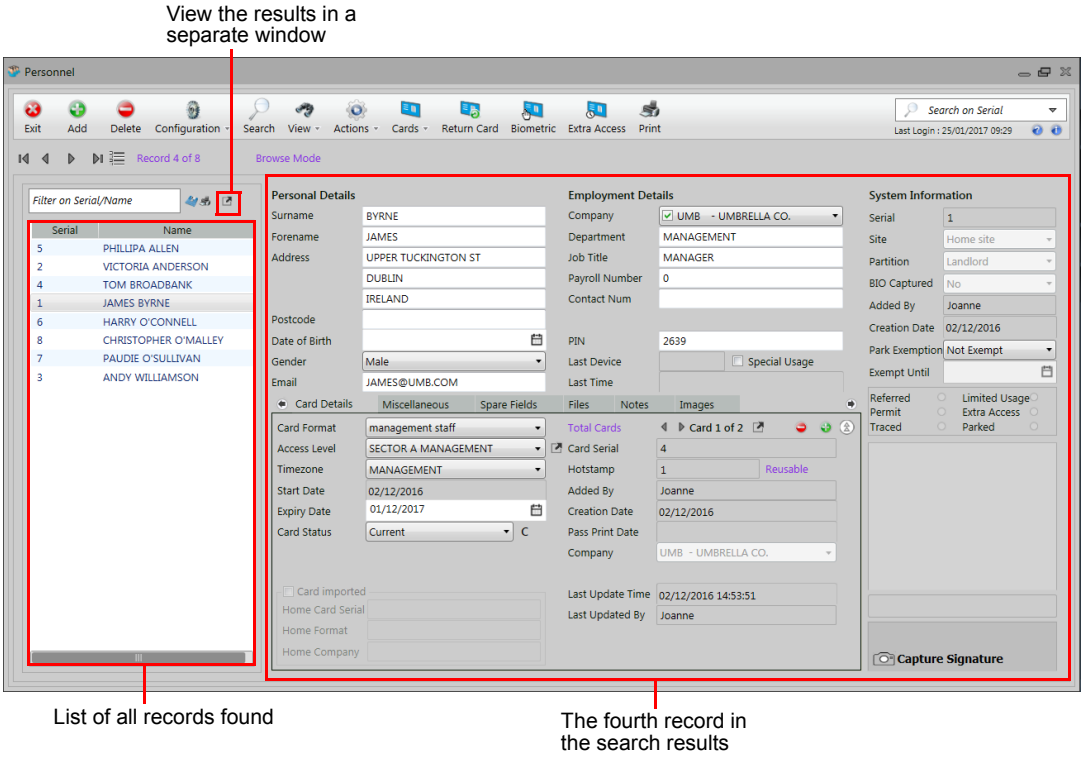

Figure 25 Viewing the search results

5. To see a list view of the result records, click the icon next to the left and right arrows.
6. Click the pop-out icon to view the results in a separate window.

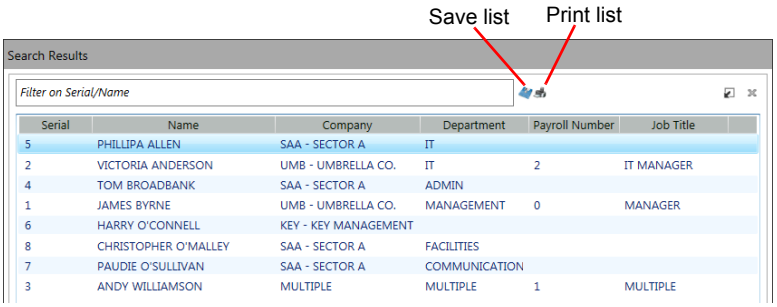

Figure 26 Viewing the search results in a separate window

7. To save the results, click the **Save list** icon.
8. To print the results, click the **Print list** icon.

9.6 Validating a card

Before a card can be used to access readers, it must be validated against a cardholder.

Cards can be validated in Personnel in one of two ways:

- Automatic validation, using preloaded card information from a **Load Cards** operation in the Card Setup application. For more information, see *Automatic card validation* on page 38.
- Manual validation, using a validation reader that is attached to the workstation. For more information, see *Manual card validation using an online reader* on page 38 and *Manual card validation using a fingerprint reader* on page 38.

9.6.1 Automatic card validation

Before a card can be validated, you must create the correct card format in the Card Setup application. If there is preloaded card information on the system, you can validate cards automatically.

Note: If the card type is set to **GENERATE CARD NUM**, you do not need to preload card numbers on to the system.

To validate a card in Personnel automatically, complete the following steps:

1. In **Personnel**, perform a search for the cardholder.
2. If the cardholder has more than one card, scroll through the cards to find the card to validate.
3. In the toolbar, click **Validate**.
4. If prompted for a hotstamp number, type the hotstamp number into the **Hotstamp** field.
5. Click **Validate** and click **Yes** to accept automatic validation.

9.6.2 Manual card validation using an online reader

Before a card can be validated, you must create the correct card format in the card types application. For example, if you want to use an online reader connected to the AC2000 network on which to perform card validation, the **ONLINE READER** validation option must be selected in the Card Setup application.

To manually validate a card, complete the following steps:

1. In the **Personnel** toolbar, click **Validate** to display the **Online Card Validation** window.
2. If prompted to type a hotstamp number, type the hotstamp number into the **Hotstamp** field. If the card type has **Auto-Generate Hotstamp** enabled, the hotstamp generates automatically and you can not edit the value.
3. Type the five-digit hexadecimal AC2000 address of the online reader into the **Device Address** field.
   Note: If you have setup the device address in the Getting Started wizard application, you will not be prompted to manually enter the device address.
4. Click **Validate** to display the swipe timeout prompt.
5. Swipe the card over the reader.

Note: Validation of a card must be performed on a reader that is compatible with that card technology, for example, a MiFare card must be validated on a MiFare reader.

Note: Where cards do not have an encoded internal number, it is recommended that the card's validation method is set to **GENERATE CARD NUM**. It is also advisable that the hotstamp number is included in the pass design.

9.6.3 Manual card validation using a fingerprint reader

Before a card can be validated, you must create the correct card format in the card types application. For example, if you want to use an fingerprint reader connected to the AC2000 network on which to perform card validation, the **READ CNUM & BIO** validation option must be selected in the Card Setup application.

To manually validate a card, complete the following steps:

1. In the **Personnel**, click **Validate** to display the **Validation** window.
2. If prompted to type a hotstamp number, type the hotstamp number into the **Hotstamp** field. If the card type has **Auto-Generate Hotstamp** enabled, the hotstamp generates automatically and you can not edit the value.

3. Click **Validate.**
4. In the **IP Address** fields, type the IP address of the validation reader.
5. Click **Save** to display the **Capture Biometrics** pane.
   Note: If you are not prompted to enter the IP address of the biometric reader, it has been set already using the Getting Started application.
6. Select **Capture** and place one of your fingers on the biometric reader.
7. When your first finger's biometric information has been captured and the fingerprint image displays, place another one of your fingers on the biometric reader.
8. Click **Accept** to proceed or **Cancel** to abort.
9. Swipe the card over the reader.

Chapter 10
User Options

10.1 Introduction

Use the User Options application to create and manage user accounts on the AC2000 system. You can also restrict the access of a user to particular applications or functionality within applications.

Note: If you are using a partitioned system, see the **Partitioning** manual.

10.2 User accounts

Unique user accounts are used to access AC2000 applications and perform system functions. They consist of the following elements:

- A unique username and password
- An authorisation level
- Application permissions
- Company restrictions
- Oneshot restrictions
- System permissions
- User template

10.3 Adding a user account

To add a user, complete the following steps:

1. From the list of users in the left pane, click **Users**.
2. From the toolbar, click **Action**, and click **Add User**.
3. Configure the parameters of the Add User pane. For more information, see *Parameters of the Add User pane* on page 41.
4. Click **Save**.

Note: All new accounts are configured with the default system settings. Change these to restrict the user permissions of the individual.

10.3.1 Parameters of the Add User pane

This table describes the parameters of the Add User pane.

Parameter	Description
Username	The username for the user account
Password	The password for the user account
Confirm Password	The password for the user account
Authorisation level	The authorisation level of the user account
Copy User	The existing user account settings you want to apply to the new user account. For more information on copying user settings, see *Copying an existing user* on page 41.
Assign template	The template you want to apply to the user account.

Table 7: Utilities and applications

10.4 Copying an existing user

When you add a user, you can copy the application settings of that user to any other user.

To copy the settings of a user, complete the following steps:

1. From the list of users in the left pane, select **Users**.
2. From the toolbar, click **Action**, and select **Add User**.
3. Configure the parameters of the **Add User** pane. For more information, see *Parameters of the Add User pane* on page 41.
4. From the **Copy User** drop-down list, select the user account whose settings you want to copy. The **Details to copy** parameter is displayed.

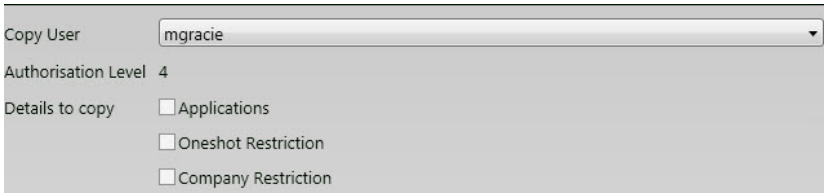

Figure 27 The Copy User details options

5. Select the check box for the settings you want to copy. The options are as follows:
   - **Applications**
   - **Oneshot Restriction**
   - **Company Restriction**
6. Click **Save**.

10.4.1 Using the Applications tab

Use the **Applications** tab to assign and remove access to users for specific applications. There are three tabs in the **Applications** tab: **Workstation**, **Web**, and **Security Hub**.

Assigning applications

To assign applications to a user, complete the following steps:

1. From the list of users in the left pane, select the user.

2. Click the **Applications** tab.
3. From the **Not Selected** pane, select the applications you want to make available to the user by selecting the check box.
4. Click **Save**.

Note: Selected applications move to the **Selected** pane.

Removing applications

To remove applications from a user, complete the following steps:

1. From the list of users in the left pane, select the user.
2. Click the **Applications** tab.
3. From the **Selected Pane**, clear the check boxes corresponding to the applications you want to make unavailable to the user.
4. Click **Save**.

Chapter 11
Testing

11.1 Introduction

When you complete the Getting Started Wizard, test the card and generate a transaction report to check that everything is working as it should.

Important: CEM Systems recommends testing one card before validating more cards on the system, to ensure the card and system have been setup correctly.

11.2 Test Card

To test a card, complete the following steps:

1. Swipe a validated card at a door reader. Do not use a validation reader.
2. Check the reader response.

Message	Description
DOOR OPEN/CARD VALID	The configuration has been set up correctly.
WRONG ZONE	The card has been validated but is not set up to access the reader. Check access levels and access groups.
CARD NOT IN SYSTEM	The card number is not validated on the system. This may be a validation issue with the setup of the validation reader.
INVALID CARD	An incorrect card format or site code has been selected. Check the card type.
CARD EXPIRED	Check the card status in Personnel.

Table 8: Reader messages

11.2.1 Generate a transaction report

If the validation reader does not have an LCD display and therefore cannot display the reader messages as described in Table 8 on page 43, generate a Transaction report to test the configuration.

To generate a transaction report, complete the following steps:

1. From the **AC2000 Floatbar**, click **Administration**, and click **Extended Reports**.
2. Click **Reports** and select **Transaction Report**.
3. Click **Generate**.

Refer to Table 8 on page 43 for an explanation of any reader messages and their meaning.