

Controlsoft Identity Access

The screenshot displays the Controlsoft Identity Access Management software interface. The interface is divided into several sections:

- User Status:** Shows ON SITE (54) and OFF SITE (48) counts. Includes a 'Reset' button and 'Reset all APB' option.
- Controller Status:** Shows ON LINE (6) and OFF LINE (0) counts. Includes 'Release' and 'Sync Time' buttons.
- Doors:** Lists various locations such as Conference Room, Main Entrance, Production Door, Sales Office, Server Room, Staff Entrance Door, Tenants Door, Training / Presentation Room, and Warehouse Barrier. Includes 'Refresh', 'Grant Access', 'Remote Release', and 'Re-lock' buttons.
- Lockdown Status:** Shows Level 0, Level 1, and Level 2 indicators.
- Access Log:** A table showing recent access events. Columns include Date, Time, Last Name, First Name, Reader, Location, Token Number, Facility Code, Company, Department, Result, and Reason.
- Reader Monitor 1:** Shows a live video feed of Arun Pandhya with a timestamp of 2024/03/28 14:57:00 and 'Access Allowed' status.
- Reader Monitor 2:** Shows a live video feed of Heather Payne with a timestamp of 2024/03/28 15:01:24 and 'Access Allowed' status.

Date	Time	Last Name	First Name	Reader	Location	Token Number	Facility Code	Company	Department	Result	Reason
28/Mar/2024	15:01:24	Payne	Heather	Main Entrance Out Re...	Moved outside	1174		*Landlord - ABC Healt...	Directors	Access Allowed	Group access allowed
28/Mar/2024	15:00:01	Gray	Justin	Sales Office In Reader		1029		*Landlord - ABC Healt...	Accounts	Access Allowed	Group access allowed
28/Mar/2024	14:58:09	Gray	Justin	Training / Presentatio...		1029		*Landlord - ABC Healt...	Accounts	Access Allowed	Group access allowed
28/Mar/2024	14:57:49	Farrell	Byron	Conference Room In R...		1152		*Landlord - ABC Healt...	Dispatch	Access Allowed	Group access allowed
28/Mar/2024	14:57:21	Payne	Heather	Office Lift		1174		*Landlord - ABC Healt...	Directors	Access Allowed	Group access allowed
28/Mar/2024	14:57:00	Pandhya	Arun	Main Entrance In Read...	Moved inside	1093		Tenant - Delta Accoun...	Accounts	Access Allowed	Group access allowed
28/Mar/2024	14:56:36	Brooks	Aston	Staff Entrance Door In...		1031		*Landlord - ABC Healt...	Accounts	Access Allowed	Group access allowed
28/Mar/2024	14:56:15	Cameron	Carl	Main Entrance In Read...	Moved inside	11133		*Landlord - ABC Healt...	Practitioners	Access Allowed	Group access allowed
28/Mar/2024	14:55:28	Adams	Deanna	Main Entrance In Read...	Moved inside	2539		*Landlord - ABC Healt...	HR	Access Allowed	Group access allowed

OPERATORS GUIDE

Version 9.1.88 © 2024 Controlsoft Ltd

Contents

1. Introduction.....	3
2. Starting the Identity Access Software	3
3. The Dashboard.....	5
4. Configuring Operators.....	7
4.1. Editing the Default Operators.....	7
4.2. Adding an Administrator	9
4.3. Adding an Operator	10
5. Configuring Groups (Access Levels).....	13
5.1. Creating Groups.....	14
5.2. Allocating Users to Groups.....	17
6. Users.....	17
6.1. User General.....	19
6.2. User Photo.....	20
6.3. User Fingerprints.....	21
6.4. User Mobile Access	23
6.5. Multiple Tokens	27
6.6. User Extra Data.....	27
6.7. User Contact.....	29
6.8. User Events	Error! Bookmark not defined.
6.9. User Notes	29
6.10. Bulk Enrol.....	30
6.11. Importing Users	31
7. Configure Time Zones.....	32
7.1. Creating Time Zones	33
8. Public Holidays.....	35
8.1. Creating Public Holidays.....	36
9. Companies and Departments	37

Controlsoft Identity Access Operator Guide

9.1.	Creating Companies and Departments	38
10.	Event Viewers and Reports	40
10.1.	Event Viewers	40
10.2.	Access Control Reporting	41
10.3.	System Log Reporting	43
10.4.	Fire Rollcall Report.....	44
10.5.	Access Control Status Report.....	44
10.6.	Groups Status Report	45
10.7.	Inactivity Report.....	46
10.8.	System Log	47

1. Introduction

The Identity Access (IA) Management Software from Controlsoft© is a PC-based Access Control Management system. The Identity Access software manages the access control database, which is downloaded to one or more i-Net® Controllers. The i-Net controller(s) make the decisions as to whether access is granted or denied.

NOTE: Your system may not support all the features described in this manual, depending on the configuration of the system and the type of license applied. For details, please contact your system integrator Conventions used in manual:

2. Starting the Identity Access Software

To launch the Identity Access software:

1. Select **Start > Controlsoft > Identity Access**

NOTE: The Splash screen may show "**Error: Checking connection to the main database... Retrying**". This is because the SQL 2022 database engine takes longer to start. Wait 2 minutes and Identity Access will connect.



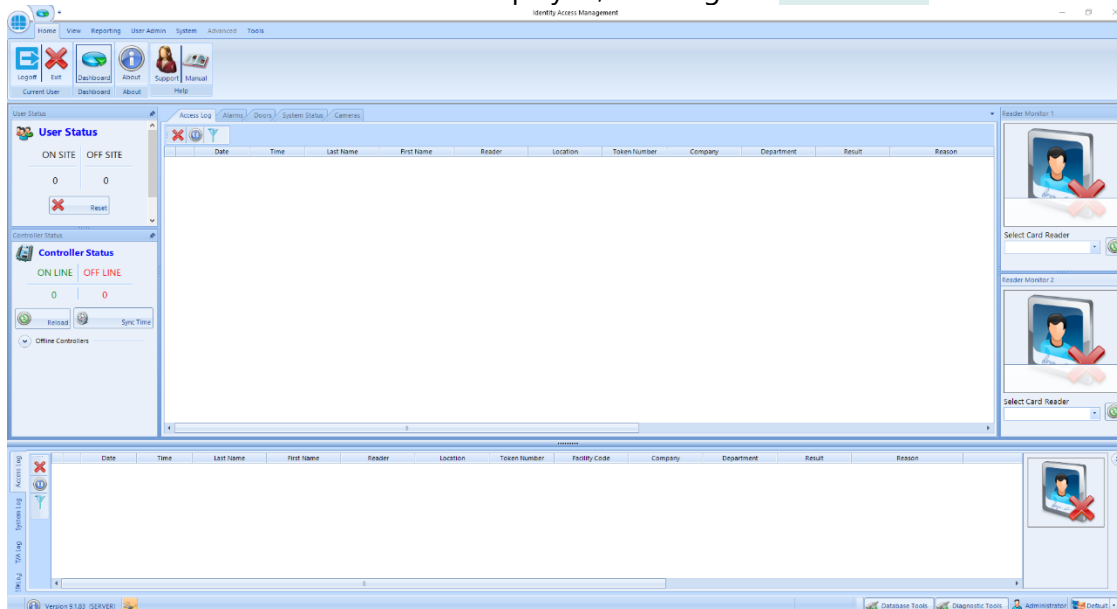
Controlsoft Identity Access Operator Guide

2. Select your user and type in your password. **NOTE: Your password will have been setup on the software installation, for details please contact your system integrator.**



The screenshot shows the 'Logon' window of the Identity Access Management software. It features a blue header with the 'Logon' title and a large blue arrow icon. Below the header, there is a 'Welcome to Identity Access. Please enter your username and password.' message. The form includes three input fields: 'Username' with a dropdown menu set to 'Administrator', 'Password' with a text box, and 'Language' with a dropdown menu set to 'English'. At the bottom, there are two buttons: a blue 'Logon' button with a white arrow icon and a red 'Cancel' button with a white 'X' icon. A small disclaimer at the bottom reads: 'IMPORTANT Using this program constitutes acceptance of the licence terms and conditions as described in Help topics. © 2018 Controlsoft Ltd.'


3. The main user interface will then be displayed, showing the **Dashboard**:

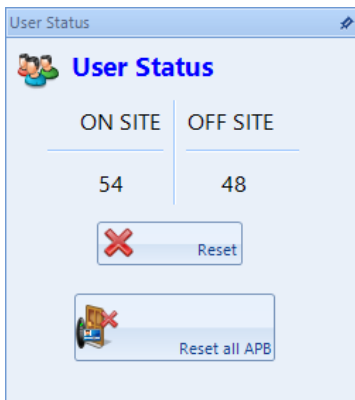


The screenshot displays the main dashboard of the Identity Access Management software. The interface is divided into several sections. On the left, there are two panels: 'User Status' showing 'ON SITE' and 'OFF SITE' counts (both at 0) with a 'Reset' button, and 'Controller Status' showing 'ON LINE' and 'OFF LINE' counts (both at 0) with 'Refresh' and 'Sync Times' buttons. The central area is a large table with columns for 'Date', 'Time', 'Last Name', 'First Name', 'Reader', 'Location', 'Token Number', 'Company', 'Department', 'Result', and 'Reason'. The table is currently empty. On the right side, there are two 'Reader Monitor' panels, each showing a camera feed of a person at a card reader and a 'Select Card Reader' dropdown menu. The top navigation bar includes 'Home', 'View', 'Reporting', 'User Admin', 'System', 'Advanced', and 'Tools'. The bottom status bar shows 'Version 5.1.0.0 (SERVER)', 'Database Tools', 'Diagnostic Tools', and the user 'Administrator'.

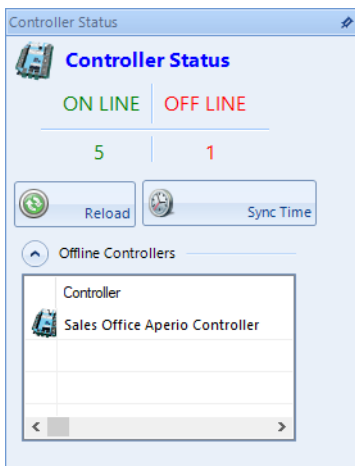
3. The Dashboard

The Dashboard is where Operators can monitor the system on a day to day basis. Each section is dynamically updated, without the need to press a refresh button or similar.

The Dashboard can be accessed from anywhere in the software by clicking the  symbol in the top left of the screen (or click on the **Home** tab and select **Dashboard**)



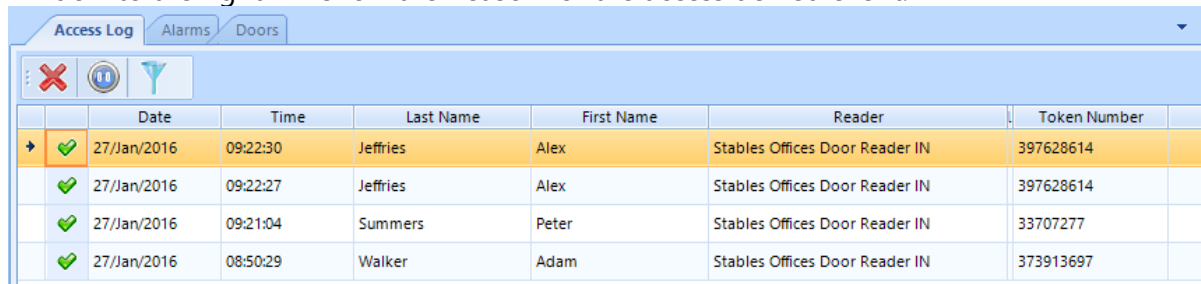
On the left-hand display is a box called **User Status** that shows how many users are currently on site. This is only relevant where there are IN and OUT readers to and from the premises. In the example here, there are 2 users, and both are currently off site.



Also on the left, is the **Controller Status** box, this shows how many door controllers are online and offline. Any offline controllers will be listed individually using the drop down arrow. If any are showing as Offline, please report this to your system integrator as door controller will not be updated while it is in this state.

Access Log Tab

The **Access Log** Tab shows a live view of access events from all around the premises. Whenever the software is closed this window viewer will be cleared. Where the event shows a tick the controller has granted access, where the event shows a red cross someone has been denied access. Scrolling the viewer window to the right will show the Reason for the access denied event.



	Date	Time	Last Name	First Name	Reader	Token Number
→ ✓	27/Jan/2016	09:22:30	Jeffries	Alex	Stables Offices Door Reader IN	397628614
✓	27/Jan/2016	09:22:27	Jeffries	Alex	Stables Offices Door Reader IN	397628614
✓	27/Jan/2016	09:21:04	Summers	Peter	Stables Offices Door Reader IN	33707277
✓	27/Jan/2016	08:50:29	Walker	Adam	Stables Offices Door Reader IN	373913697

Alarms Tab

Controlsoft Identity Access Operator Guide

The **Alarms** Tab will show various user defined software alarms, such as Door Forced Open or Fire Alarms. The operator can view these alarms, once investigated the event can be acknowledged with the **[Accept]** button, then cleared with the **[Clear]** button. If the event is on-going the alarm will reappear in the Alarm Tab.

Doors Tab

The **Doors** tab is available to remotely Grant Access or to Force a Door Open. Simply select the door you wish to open. Clicking **[Grant Access]** will unlock the door for its defined unlock time (default = 5 seconds). Clicking **[Remote Release]** will latch the door open. This door will then remain open until **[Relock]** is clicked which will then override the Forced Open command.

The symbols next to the doors indicate the last event at the door. The options are:



Access Granted via Operator: This symbol indicates that access was granted through the software by the operator.



Door Forced Open via Operator: This symbol indicates that the door was latched open through the software by the operator.



Door Forced Closed via Operator. This symbol indicates that the door was latched closed through the software by the operator.



Pushbutton. This symbol indicates that the door was accessed by pressing a Request to Exit pushbutton.



Access Granted. This symbol indicates that access was granted via the reader to unlock the door.



Access Denied. This symbol indicates that access was denied via the reader and the door was not unlocked.



Door has not been accessed since the software has been opened.

The doors tab also has facility for Site Lockdown. If enabled, this allows an operator to deny access to some or all users, depending on whether Level 1 or Level 2 lockdown is selected. Simply click the relevant button to change the lockdown state

System Status tab

This screen provides information as to whether the Log Service and Download Service are running and whether Azure ID and the Mobile Access Portal are available. The Log Service and Download Service must be running for Identity Access to operate correctly.

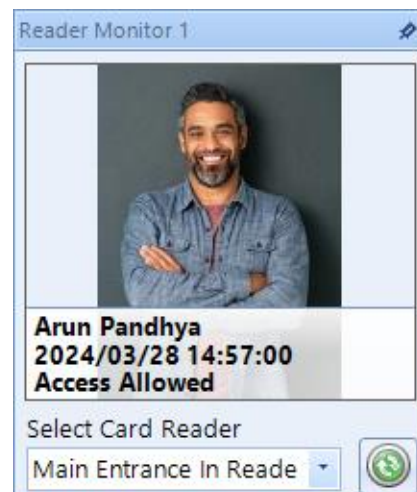
Cameras tab

This screen allows an image from a single camera to be viewed. Pan, Tilt and Zoom buttons are provided for moving PTZ cameras

Controlsoft Identity Access Operator Guide

Reader Monitor

On the right-hand side of the Dashboard are 2 Reader Monitor screens. Select the Card Reader you wish to monitor. When someone accesses the reader, their photograph (if programmed) will be displayed in the Reader Monitor display alongside their name and time of entry.

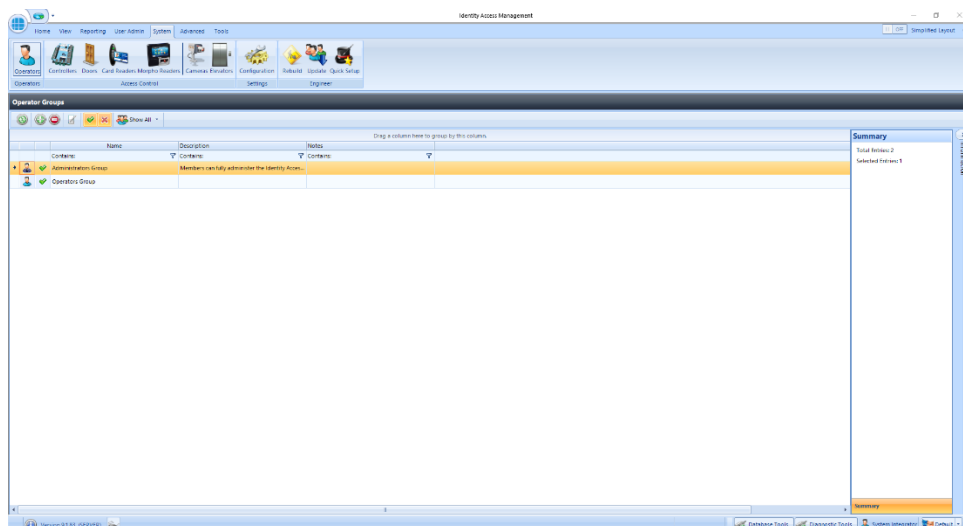


4. Configuring Operators

On Identity Access V9.1.83 and newer, an Administrator Group and Operators Group are predefined. Anyone given access via the Administrators Group has full control over the software. The Operators Group is user defined on first setup, for further information see Adding an Operator.

Multiple Operators Groups can be configured, giving different restrictions from system functions (e.g. "Receptionists" can enroll visitors to the system whereas "Human Resources" can enroll Employees, Contractors and Visitors).

Click on **System** and select **Operators**:



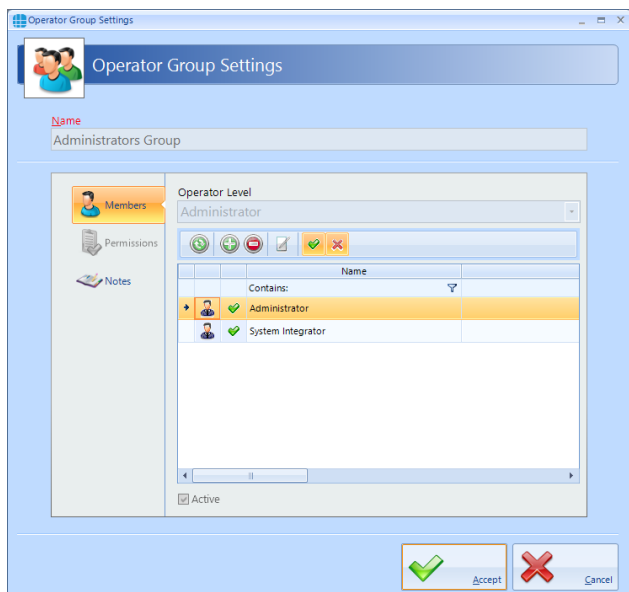
4.1. Editing the Default Operators

On first installation the default "Administrator" and "System Integrator" passwords are requested. To change the credentials for these operators

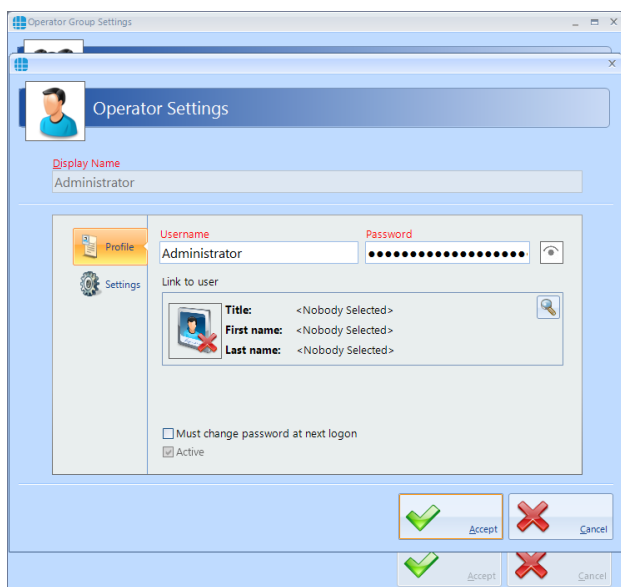
1. Double click on the Administrators group

Controlsoft Identity Access Operator Guide

2. Double click on operator that requires changing



3. Change the **Username** and/or **Password** as required:



The **Display Name** for the default Administrator cannot be changed.

NOTE: Once a Password has been entered, it can no longer be viewed.

NOTE: The default credentials are Admin and Password (both case sensitive).

If the option **Must change password at next logon** is selected, the operator will be forced to change their password when they next log on to increase security.

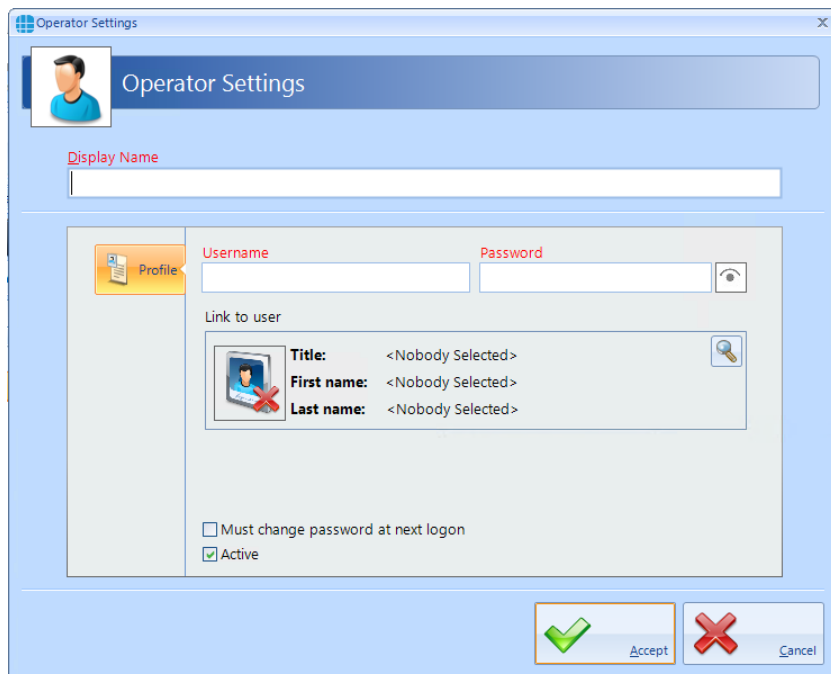
Tick the option **Active** to make the operator active. Un-ticking this at any time will stop the Operator from working, without having to delete the Operator's details.

Click **[Accept]** when done.

4.2. Adding an Administrator

To Add a new Administrator to the group:

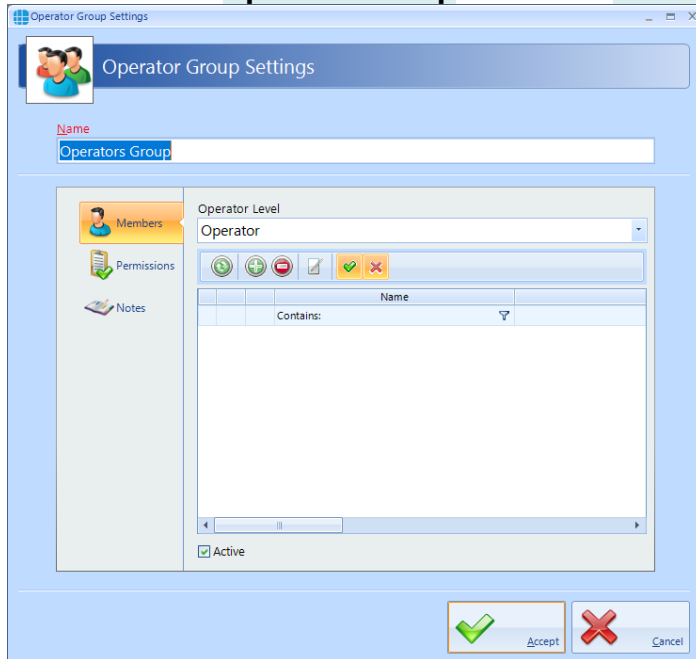
1. Double click on **Administrators** in the Operators window and click the **Add** icon:



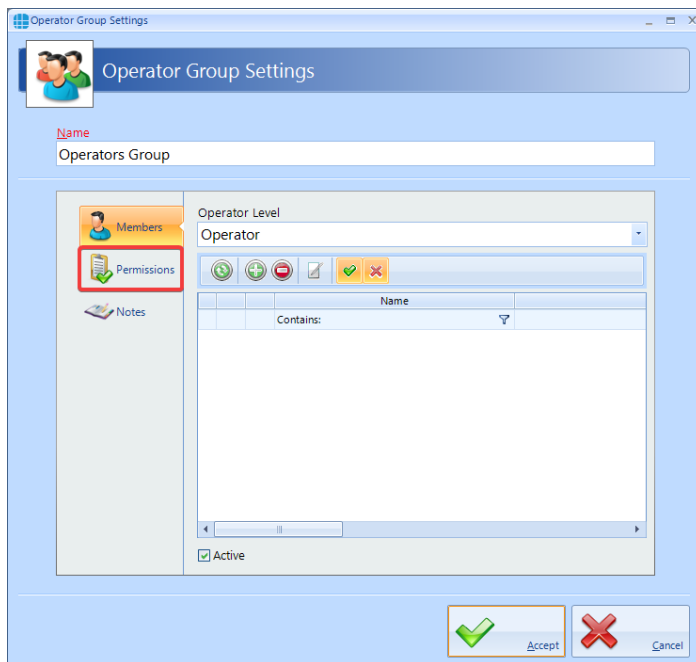
2. Enter a name for the new Administrator under **Display Name**.
3. Enter a **Username** and **Password** as required. To check the password while entering it, click the 'eye' symbol to the right of the Password box. Once a Password has been entered, it can no longer be viewed.
4. If the option **Must change password at next logon** is selected, the operator will be forced to change their password when they log on to increase security.
5. Tick the option Active to make the operator active. Un-ticking this at any time will stop the Operator from working, without having to delete the Operator's details.
6. Click **Accept** when done.

4.3. Adding an Operator

1. Double click the **Operators Group** or click the **Add New** button to create a new Group.

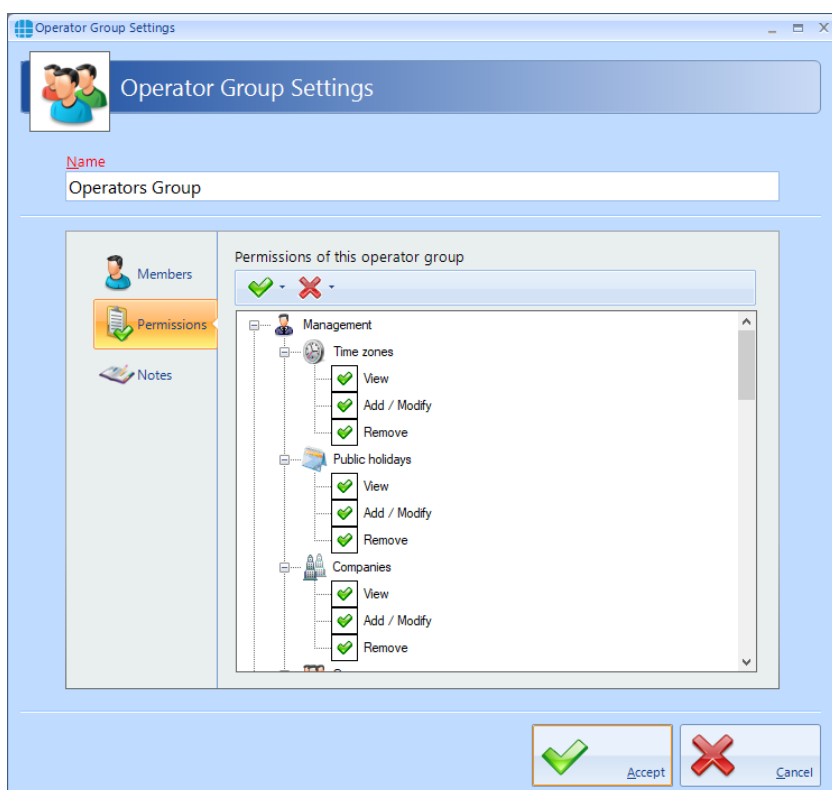



2. Select the **Permissions** tab.





Controlsoft Identity Access Operator Guide

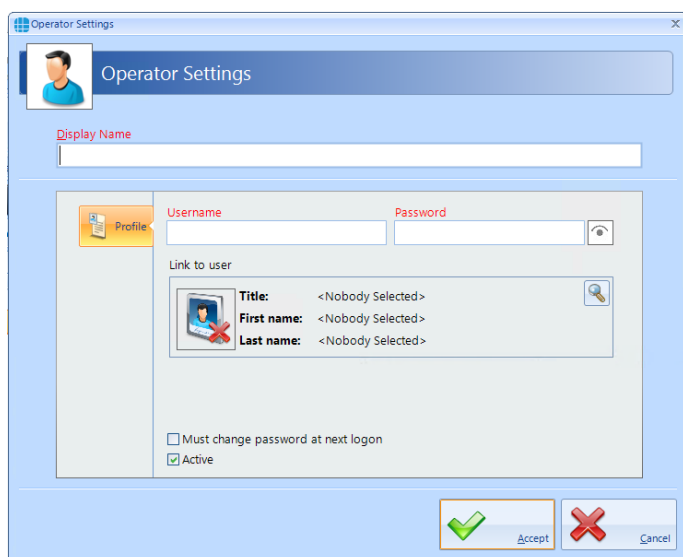
3. Double clicking an item will change the green tick to a red cross indicating that the item has been disabled. Double clicking the item again will enable it.



 will enable all items, selected items or all items within a permissions group

 will disable all items, selected items or all items within a permissions group

4. Select **Members** in the side bar, then select the Add icon  to add a new member within the group



5. Enter a name for the new Operator under **Display Name**.

Controlsoft Identity Access Operator Guide

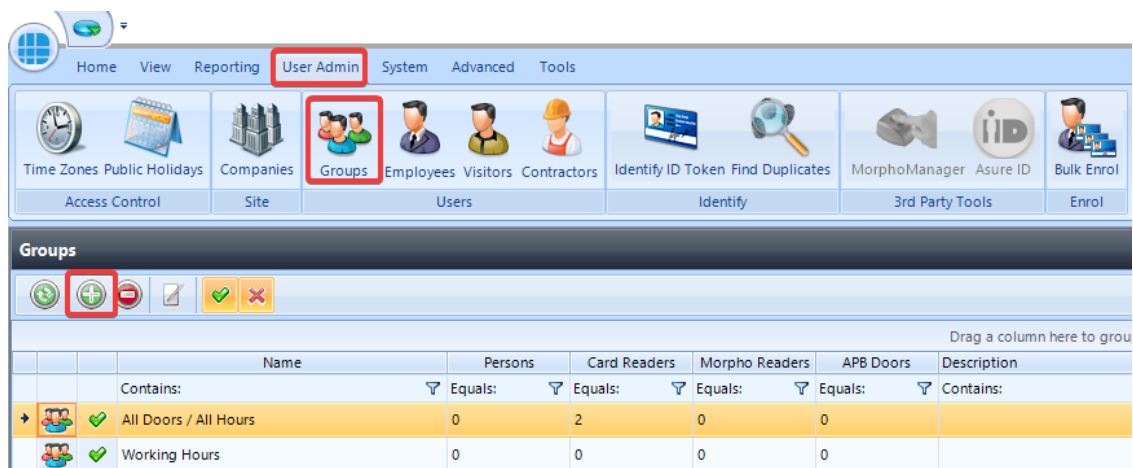
6. Enter a **Username** and **Password** as required. To check the password while entering it, click the 'eye' symbol to the right of the Password box. Once a Password has been entered, it can no longer be viewed.
7. Tick the option **Must change password at next logon** to force the operator to enter a new password when they next log on.
8. Tick the option **Active** to make the operator active.
9. Click **[Accept]** when done.

5. Configuring Groups (Access Levels)

Each Group is allocated a combination of Readers and Time Zones, so each new user allocated to that Group will automatically inherit all the relevant "Access Rights".

Within Identity Access there are 2 default groups, All Doors / All Hours has access to everything on the system as it is added. Working hours can be edited to suit your system, or you can add a new Group to further customise your access control system.

To create a new Group, select the **User Admin** tab, then select **Groups** from the ribbon bar.



This Groups window shows that there are no Groups in the database. The option buttons are:



Refresh: Updates the list of Groups



Add: Creates a new Group in the list



Delete: Removes the selected Group/s from the list



Edit: edits the selected Group



Show/Hide Active: This button will show or hide Groups selected as Active.



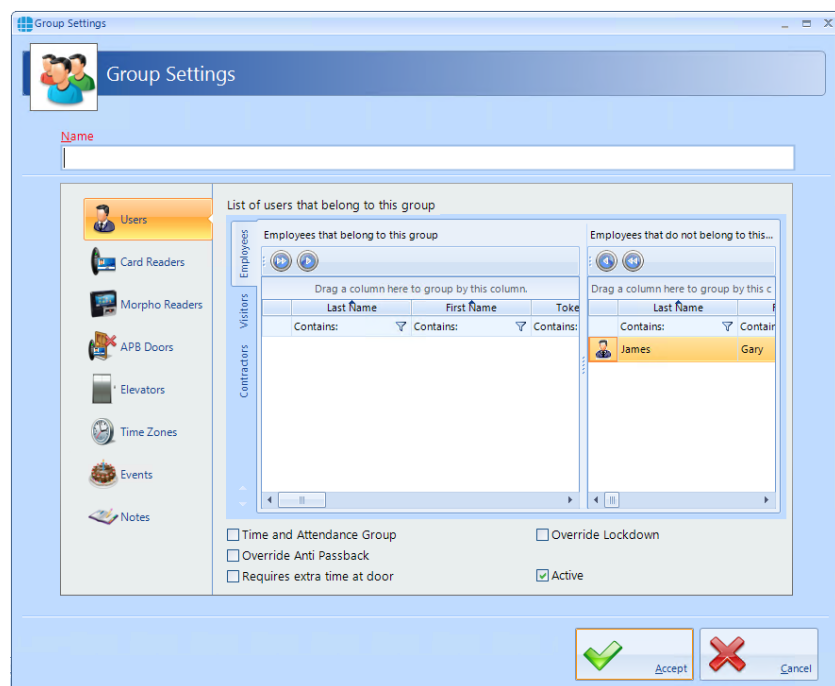
Show/Hide Inactive: This button will show or hide Groups not selected as Active.

Select the **Add** New button



5.1. Creating Groups



To configure the Group, use the Group Properties Window:



Enter a **Name** for the Group

The **Employees that belong to this group** window displays users who are currently allocated to the group

Conversely, **Employees that do not belong to this group** displays all users who are NOT currently allocated to the group

To allocate one or more user to the Group, simply select the required user/s in the right-hand column and click the  button. To place all users in the group, use the  button.

Tick the **Time and Attendance Group** box if members of this Group are to be monitored for Time & Attendance.

Tick **Override Anti Passback** if members of this group are to be excluded from APB constraints.

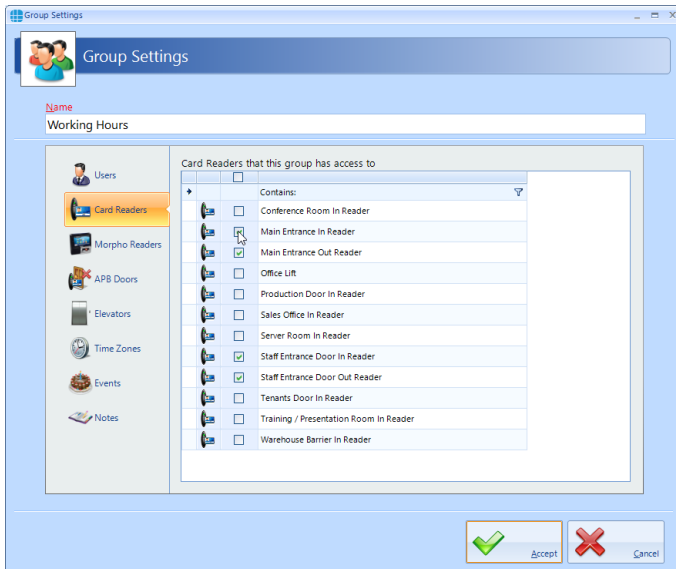
Tick **Requires extra time at door** to use the Extended Door Open Time

Tick **Override Lockdown** for users in this group to operate doors during Lockdown Level 1

Tick the **Active** box to ensure that users in this Group are operational.

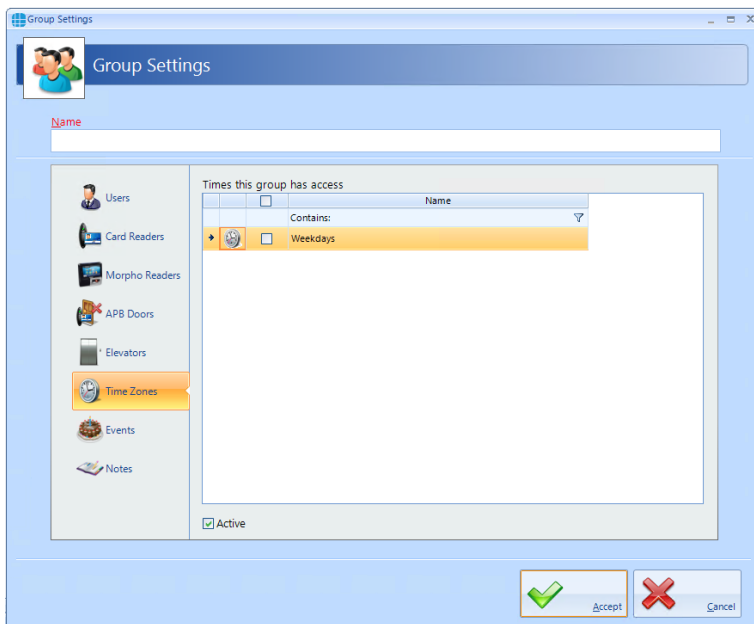
Select **Card Readers** in the side bar, select the readers that members of this Group will have access to. To select all readers, tick the **All** box highlighted above:

Controlsoft Identity Access Operator Guide



To restrict when the users can access the doors:

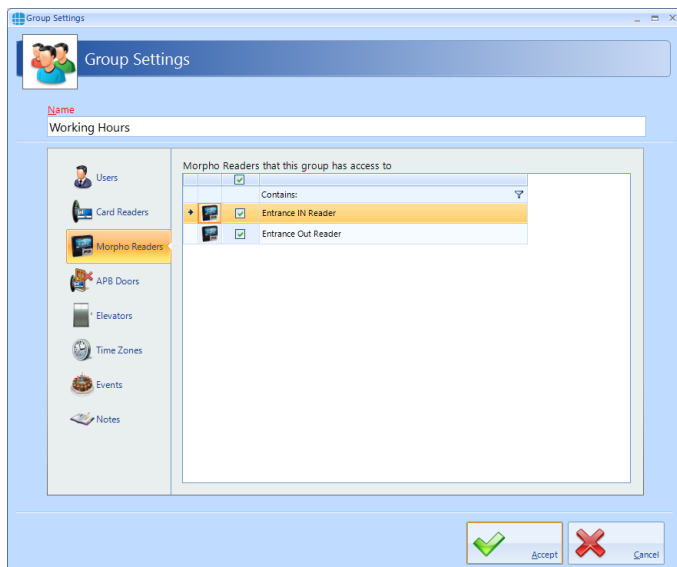
Select **Time Zones** in the side bar, select the Time Zone that members of this Group will have access to (information on how to add a Time Zone can be found in Chapter 7):



Controlsoft Identity Access Operator Guide

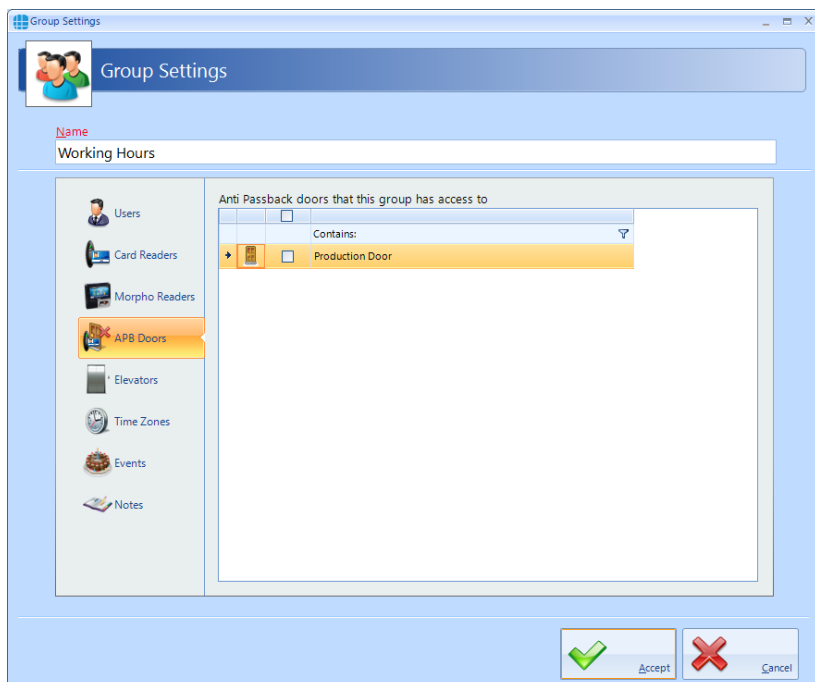
If you wish to give access to a specific fingerprint reader:

Select **Morpho Readers** in the side bar, readers that members of this Group will have access to. To select all readers, tick the **All** box.



If you wish to give access to a specific anti-passback door:

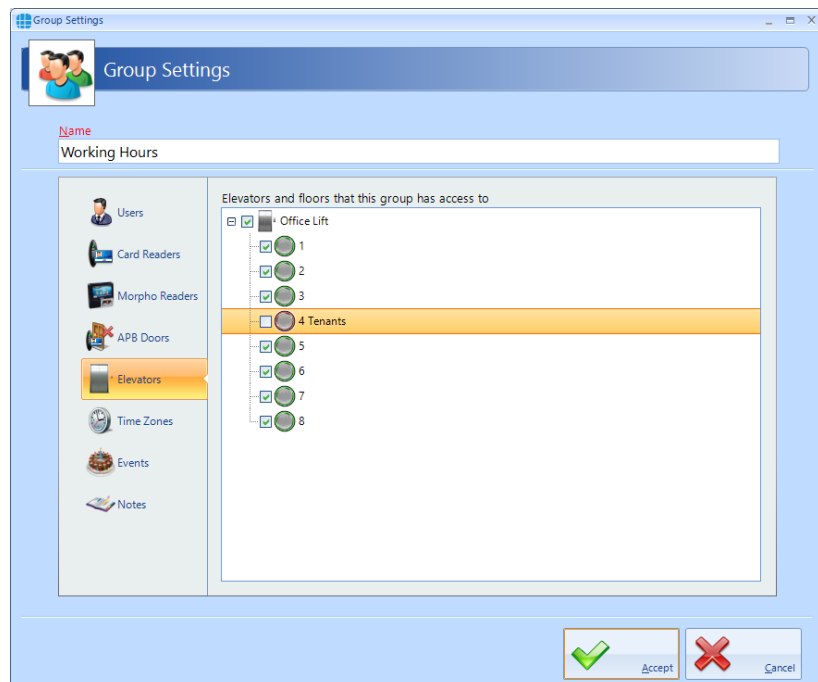
Select **APB Doors** in the side bar, select one or more Doors where members of this Group will be subject to AntiPassBack:



Controlsoft Identity Access Operator Guide

If you wish to give access to a specific elevator floor:

Select the **Elevators** in the side bar to define which floors are accessible to users in this group, tick all the floors to be accessible to these users:



5.2. Allocating Users to Groups

A user can be allocated to a Group in one of 2 ways:

1. From within the User Properties Window.
2. From within the Group Properties Window.

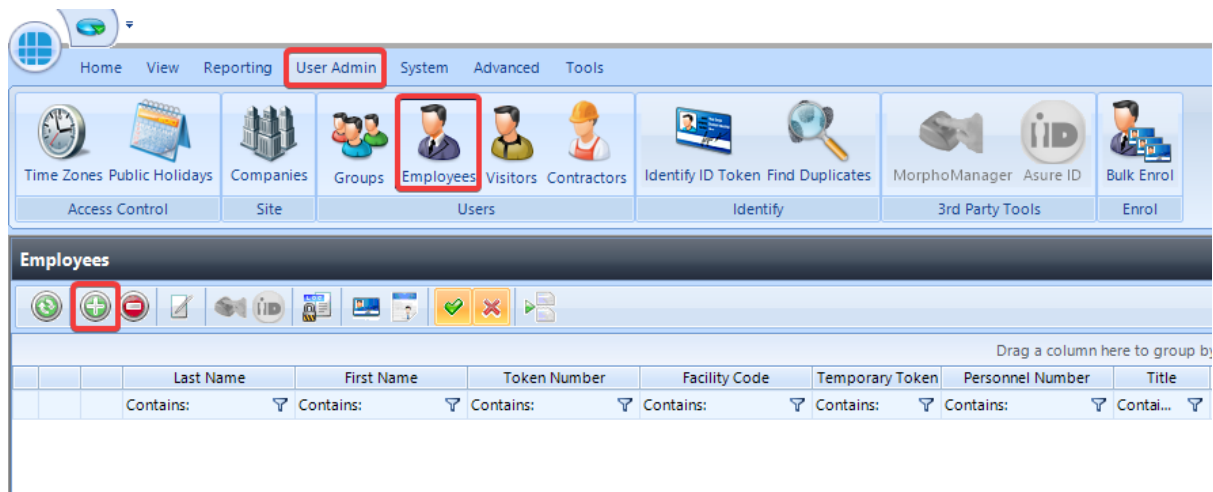
6. Users

"Users" is a collective term for Employees, Visitors and Contractors. These user types have been separated as they often have different requirement for Access Rights. Furthermore, separating Employees, Visitors and Contractors makes reporting on each type of user easier and more flexible.

NOTE: Programming screens for Employees, Visitors and Contractors are the same.

Controlsoft Identity Access Operator Guide

Select the **User Admin** tab, then select **Employees** / **Visitors** / **Contractors** from the ribbon bar:



The option icons are as follows:



Refresh: Updates the list of Users



Add: Creates a new User to the list



Delete: Removes the selected User/s from the list



Edit: edits the selected User



Enrol fingerprint using MorphoManager: This icon will be greyed out (as shown) if MorphoManager is not enabled.



Print: Prints a card for the selected user



Report: Run an access log report for the selected user



Temporary Token: Assign or remove Temporary Token for a User



Import: Adds a new User to the list from a vCard



Show/Hide Active: This button will show or hide Users selected as Active.




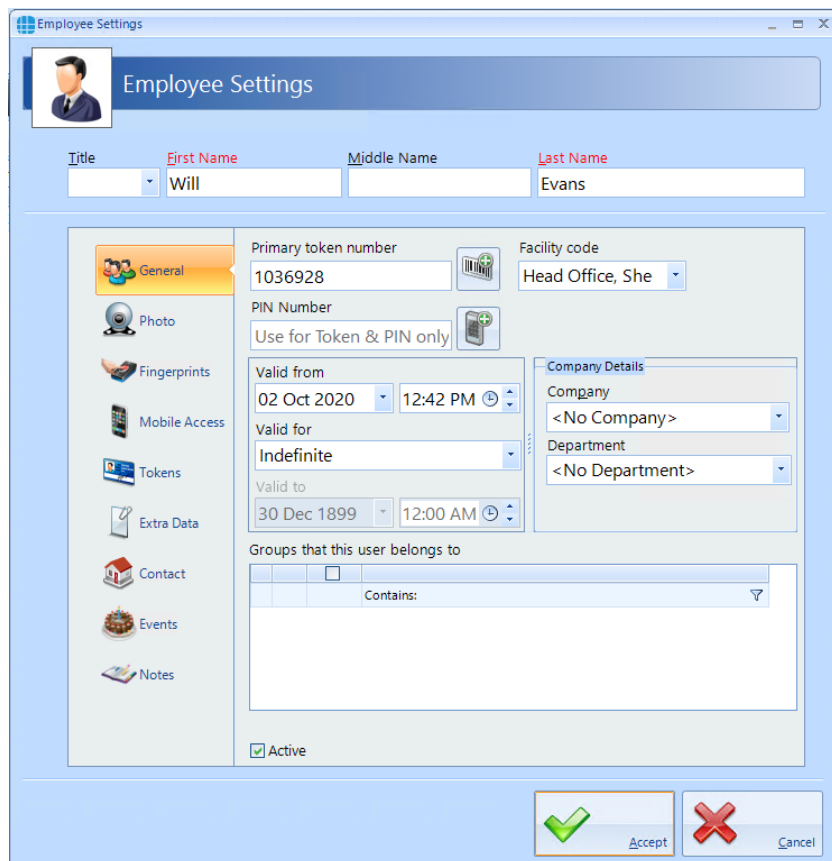
Show/Hide Inactive: This button will show or hide Users not selected as Active.



Paging Mode: Splits the list of users into manageable pages to avoid too much scrolling up and down.

6.1. User General

To create a new Employee, select the **Add New**  button:



Enter the **First Name** and **Last Name** of the user (**Title** is optional).

Enter the **Primary Token Number** of the card allocated to this user. This may be written on the card, read via an Enrolment reader, or may be a sequential number in systems using fingerprint only. Pressing the icon to the right of the Token Number field will automatically generate a token number. This is useful when using fingerprint readers.

The **Facility Code** dropdown list displays all the Facility Codes relevant to this system, simply select the appropriate one for this employee (in this instance, the employee works at the Head Office). If you have a new pack of cards you may need to use the **Add New** button to add a new Facility Code to the system

If the system has readers with a keypad, enter a **PIN Number** for the user. Pressing the icon to the right of the PIN Number field will automatically generate a PIN. **NOTE: If you are using keypads in 'PIN Only' or 'PIN OR Proximity' modes, the required PIN Number should be added as a Token Number.**

The user will have no access to the system until the **Valid from** date and time (the default is the date that the user profile was created). Similarly, the user will have no access to the system after the **Valid for** expires (default is Indefinite, but this can be changed in the Server Configuration utility).

Allocate the user to a **Company** and a **Department** (if used). Companies and Departments can be a useful filter when running reports on users.

Controlsoft Identity Access Operator Guide

Groups that this user belongs to lists all the available Groups within the system. To allocate the user to a group, simply tick the box for that group.



Ensure that the **Active** box is ticked for this user to have access to the system

NOTE: Users can be allocated to more than one Group

6.2. User Photo

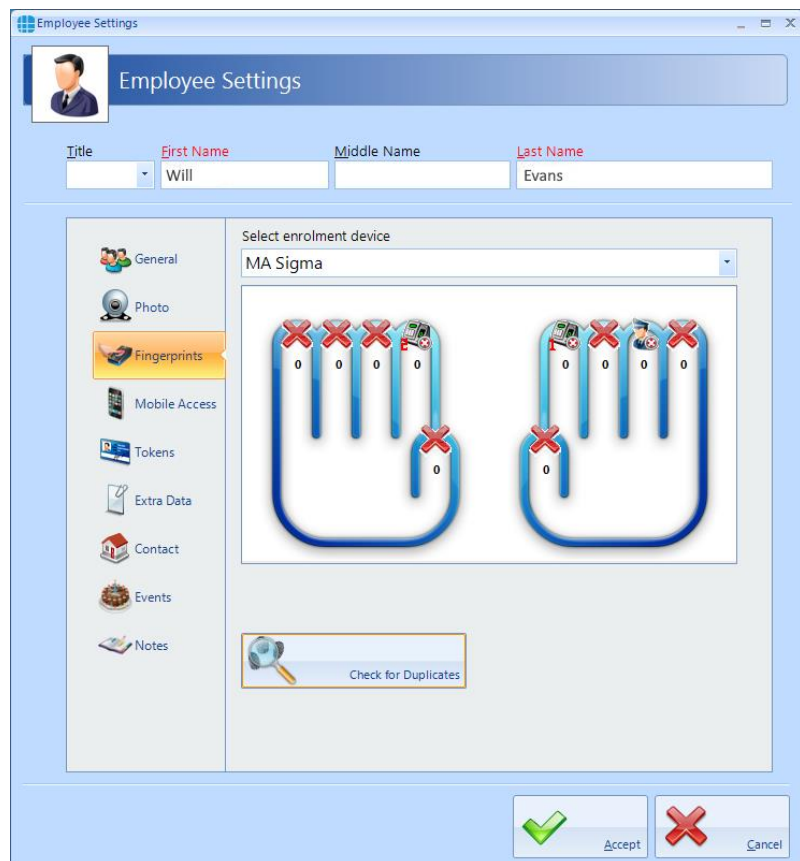
Allocating a photo to a user can be useful when identifying a lost card as it is possible to read the card and display the photo and other details of the relevant user. As standard there are two Reader Monitors located in the Dashboard to view the photos of people entering and exiting the premises.



Select the import icon  to import a previously saved image. It is possible to import a .jpg or .png picture file. The camera icon  can be used to capture a photo from a webcam.

6.3. User Fingerprints

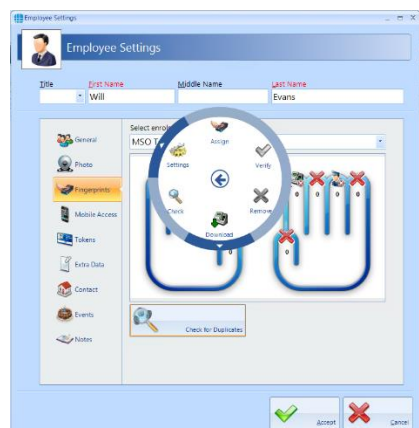
To enrol a fingerprint for a user, first define the enrolment device to be used. This could be an "MSO Takeon Device" such as an MSO-300 or MSO-1300, or, if configured, a fingerprint reader at a particular door.



NOTE: If Facility Codes have been specified for the Morpho reader, the screen will include a prompt to ensure that the Facility Codes entered for the user matches the Facility Code of the relevant Morpho readers

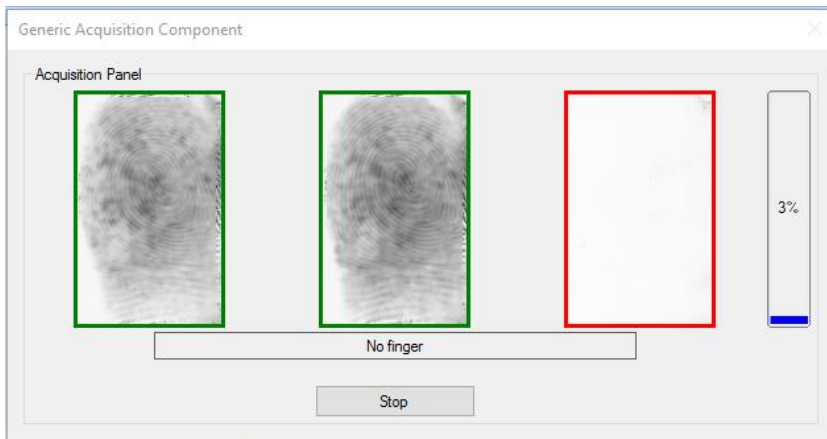
Enrol a fingerprint as follows:

Specify the finger to be enrolled by left-clicking on the required fingertip, then select **Assign** from the Option Wheel:



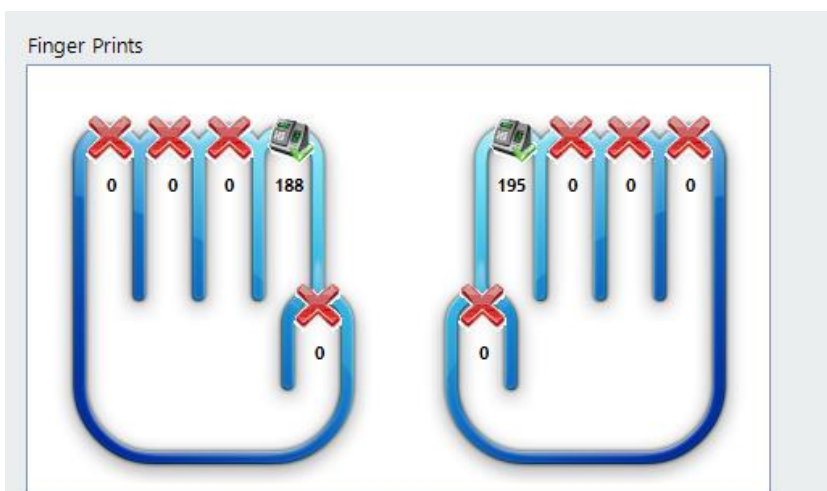
Controlsoft Identity Access Operator Guide

Place the selected finger on the enrolment reader 3 times, following the on-screen instructions where necessary.



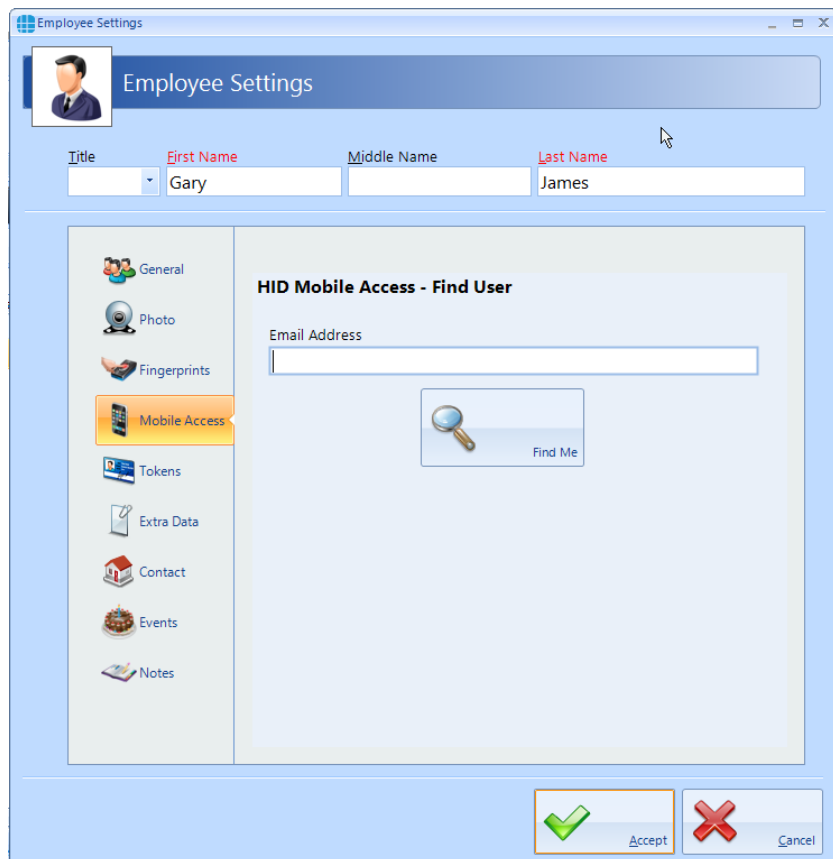
Assign a second finger. Qualify that both fingers have been enrolled and the score is satisfactory.

NOTE: The higher the enrolment scores the better the biometric reader will perform on a day to day basis. It may be necessary to enrol multiple fingerprints and use the fingerprints with the highest score.



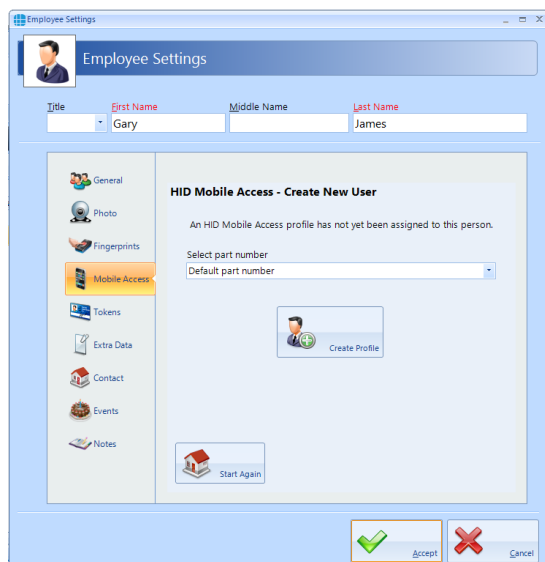
6.4. User Mobile Access

If you have a Mobile Access account, you can allocate mobile credentials from within Identity Access.



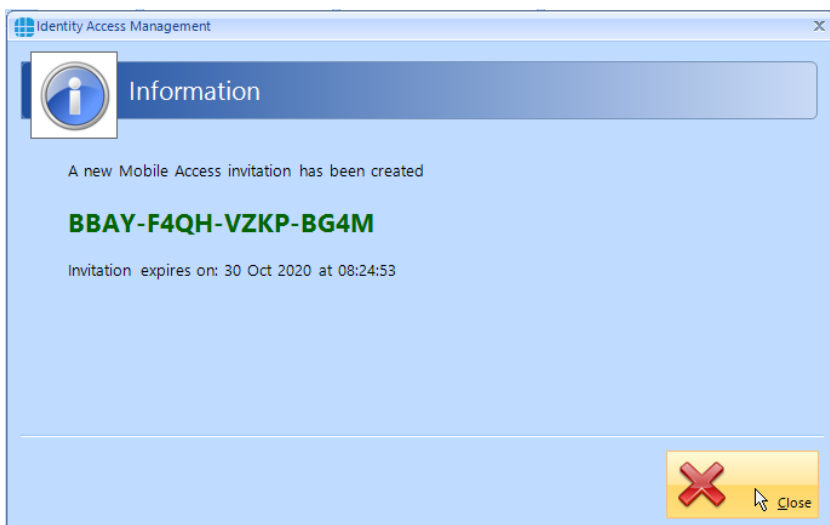
Having first entered the required information in the **General** screen and the user's email address in the **Contact** screen, select the **Mobile Access** tab and click **[Find Me]**

If the employee has never been issued with a Mobile Access credential, the following screen will be displayed

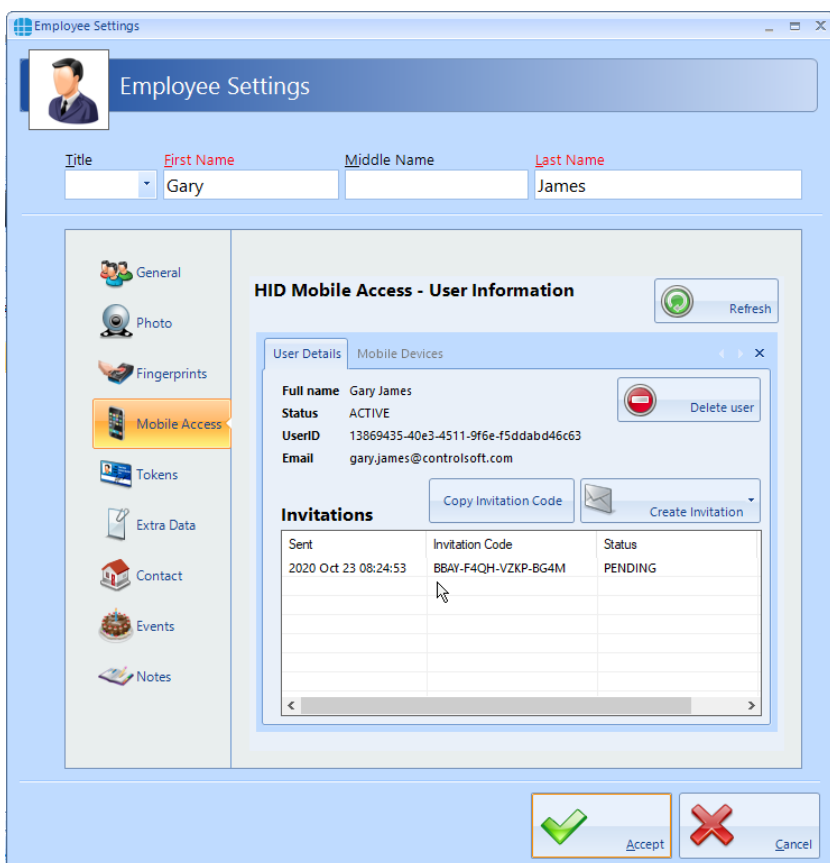


Controlsoft Identity Access Operator Guide

Leave the part number as **Default part number** and click on the **[Create Profile]** button. Once the system has created the profile for this employee, the invitation code will automatically be emailed to that employee (assuming that the option is selected in the IA Configuration utility)



Click **[Close]** and the next screen shows the Invitation Status as **PENDING**



NOTE: This invitation code is time limited and must be activated promptly.

The employee now needs to download and install the HID Mobile Access app on their phone. This is a free app available from the Google Play Store for Android phones, or from the App Store for Apple phones.

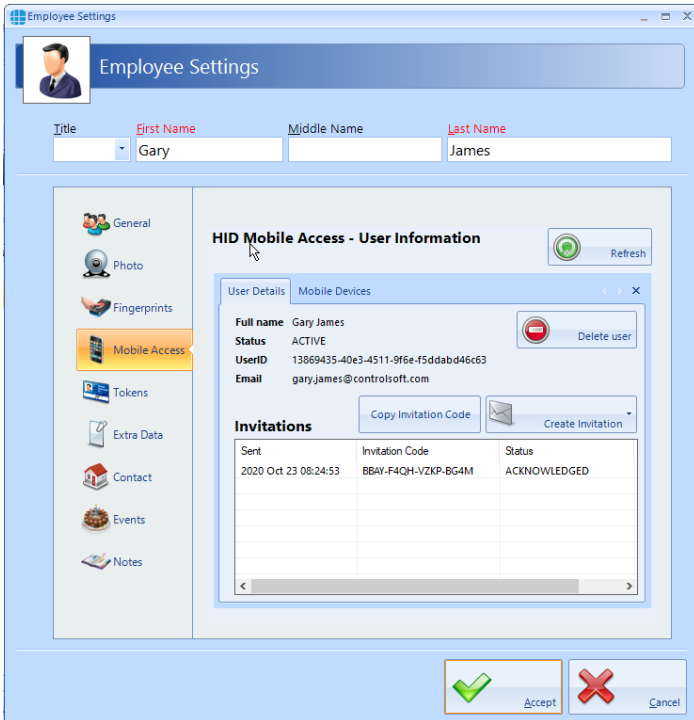
Open the app and select **"Start using the services"**

Enter the invitation code and click **[REGISTER]**

Controlsoft Identity Access Operator Guide

Look through the instruction on how to use HID Mobile Access or click **[Skip]**

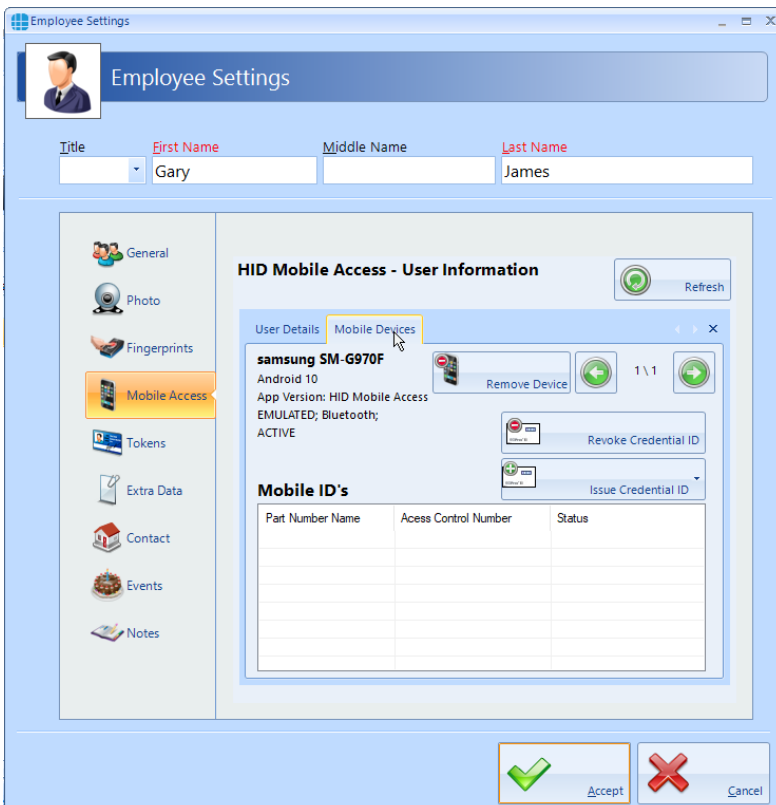
In the Identity Access User Information screen, click the **[Refresh]** button



The Invitation Status is now showing as **ACKNOWLEDGED**.

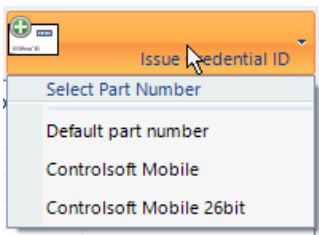
NOTE: An option exists in the IA Configuration utility called "Issue Mobile Credential ID with invitation". If this option has been selected, the invitation Status will now show as ISSUED and the next few instructions can be ignored.

Select the **Mobile Devices** tab

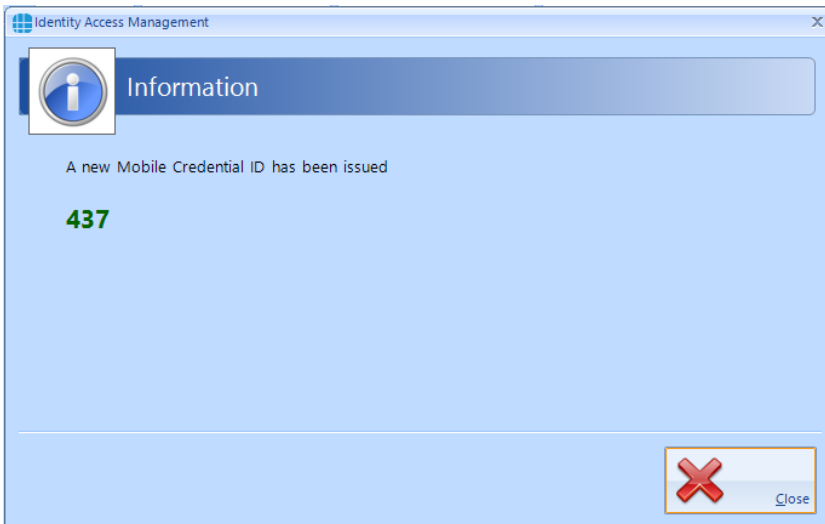


Controlsoft Identity Access Operator Guide

Now click the **[Issue Credential ID]** button and select the type of credential required, either **Default part number** or a specific type if different credentials are available.



An information box will now show the credential number issued



Click **[Close]** and the screen will be updated showing the status of credential 437 as **ISSUED**.



6.5. Multiple Tokens

Each user can be given more than 1 token to allow for multiple credential types (e.g. an Employee may have a card, a mobile credential and a windscreen tag for the car park). The **Tokens** tab allows these secondary credentials to be allocated to the user. Whichever credential is used, it will be recognised and the same user, hence Fire Roll Call, AntiPassBack etc. will continue to operate correctly.

The screenshot shows the 'Employee Settings' window with the 'Tokens' tab selected. The 'General' section shows the user's name as 'Will Evans'. The 'Tokens' section contains four 'Secondary token' entries, each with a corresponding 'Facility code' dropdown menu. Below these, the 'HIK Vision ANPR number' is set to '4138416' and the 'Number plate' is 'OK123VEH'. At the bottom right, there are 'Accept' and 'Cancel' buttons.

The titles **Secondary token 1**, **Secondary token 2** etc. can be renamed in the IA Configuration utility to provide more meaning titles such as "Mobile Credential" or "Windscreen Tag".

If the Use HIK Vision ANPR option is enabled in the IA Configuration utility, then Secondary Token 5 will automatically be renamed to **HIK Vision ANPR number** as in the above screenshot. This field will be filled in automatically when a vehicle number plate is entered into the **Number plate** field.

NOTE: The ANPR number plate must be unique

Please contact your installer / maintenance company for assistance in changing these options.

6.6. User Extra Data

It is sometimes useful to have additional information logged against a user, depending on the work environment. For example, a Courier company may want to log whether a driver has a valid driving license, store the expiry date of the license or even store a scan of the license itself.

The Extra Fields are configured within the IA Configuration software (ask your installer / maintenance company for further information on this).

To use an Extra Field previously configured, select the **Extra Data** tab:

Controlsoft Identity Access Operator Guide

The screenshot shows the 'Employee Settings' window for a user named Will Evans. The 'Extra Data' tab is selected in the left-hand navigation menu. The main area displays a table with one row for 'Valid Driver's License' and a radio button interface below it.

Index	Extra Field	Value
0	Valid Driver's License	

Valid Driver's License

Yes

No

Apply

Accept Cancel

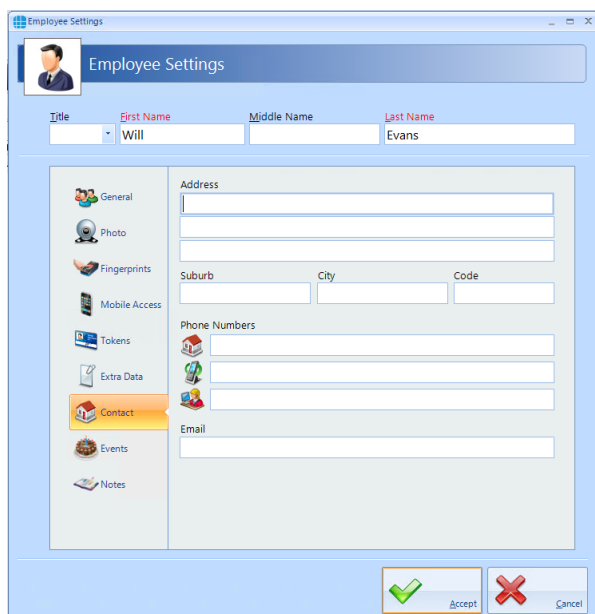
In this instance, the Extra Data Field has been configured to record whether the user has a valid driver's license. Simply select **Yes** or **No** as appropriate, followed by **[Apply]** and **[Accept]**.

The Extra Data tab can display a variety of information as the data fields can be text, numeric, lists, checkbox, date, time, or image.

Controlsoft Identity Access Operator Guide

6.7. User Contact

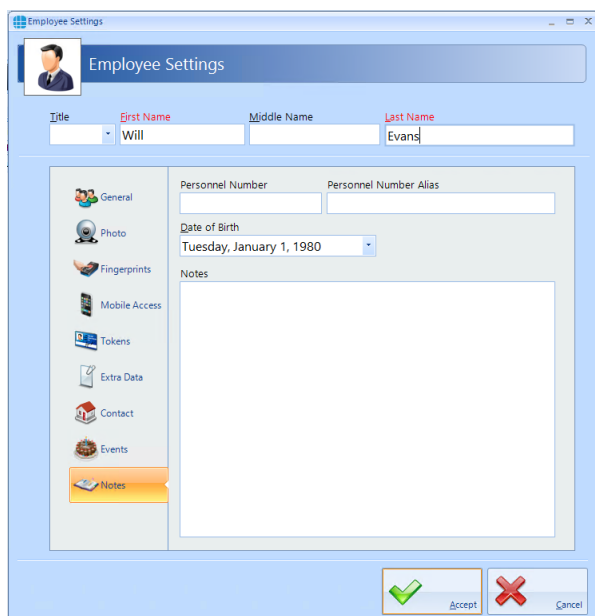
The Contact Details in this tab are not mandatory, but can be recorded if required:



The screenshot shows the 'Employee Settings' window with the 'Contact' tab selected. The window title is 'Employee Settings'. At the top, there is a header bar with a profile picture and the text 'Employee Settings'. Below this, there are fields for 'Title', 'First Name', 'Middle Name', and 'Last Name'. The 'First Name' field contains 'Will' and the 'Last Name' field contains 'Evans'. The main content area is divided into several sections: 'Address' (with a large text input field), 'Suburb', 'City', and 'Code' (each with a text input field), 'Phone Numbers' (with a text input field), and 'Email' (with a text input field). On the left side, there is a vertical navigation menu with icons and labels for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens', 'Extra Data', 'Contact' (highlighted), 'Events', and 'Notes'. At the bottom right, there are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

6.8. User Notes

Information in this tab is not mandatory, but can be recorded if required:



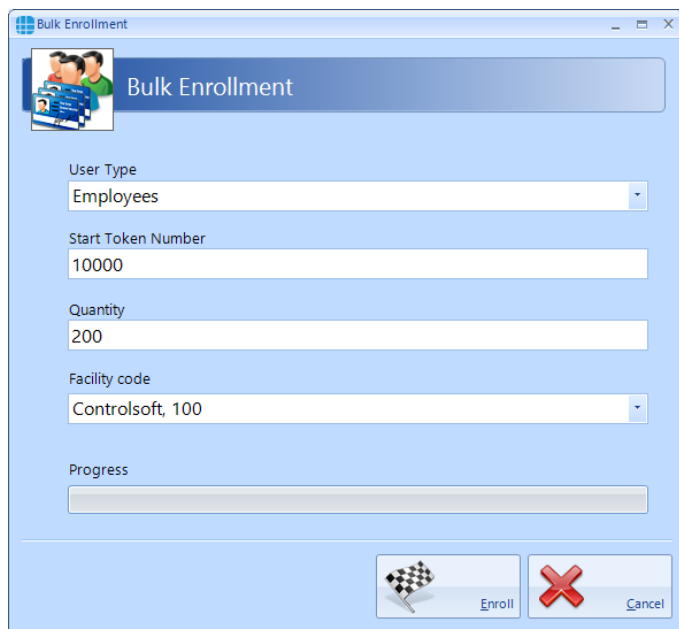
The screenshot shows the 'Employee Settings' window with the 'Notes' tab selected. The window title is 'Employee Settings'. At the top, there is a header bar with a profile picture and the text 'Employee Settings'. Below this, there are fields for 'Title', 'First Name', 'Middle Name', and 'Last Name'. The 'First Name' field contains 'Will' and the 'Last Name' field contains 'Evans'. The main content area is divided into several sections: 'Personnel Number' and 'Personnel Number Alias' (each with a text input field), 'Date of Birth' (with a date picker showing 'Tuesday, January 1, 1980'), and 'Notes' (with a large text area). On the left side, there is a vertical navigation menu with icons and labels for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens', 'Extra Data', 'Contact', 'Events', and 'Notes' (highlighted). At the bottom right, there are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

The **Personnel Number** is displayed in the Employee Properties screen and can be selected to be unique via the IA Configuration utility.

6.9. Bulk Enrol

This feature makes it easy to enrol when cards have been ordered with sequential numbering. Bulk Enrol allows you to add all the numbering, the end user can then simply edit the user with their name and access levels rather than requiring them to manually add each card to the system.

To start a Bulk Enrolment select the **User Admin** tab and select **Bulk Enrol** from the ribbon bar:



The screenshot shows the 'Bulk Enrollment' dialog box. It has a title bar with the text 'Bulk Enrollment' and a close button. Below the title bar is a header area with a small icon of people and the text 'Bulk Enrollment'. The main area contains several fields: 'User Type' is a dropdown menu with 'Employees' selected; 'Start Token Number' is a text box with '10000'; 'Quantity' is a text box with '200'; 'Facility code' is a dropdown menu with 'Controlsoft, 100' selected; and 'Progress' is a progress bar. At the bottom right, there are two buttons: 'Enroll' with a checkered flag icon and 'Cancel' with a red 'X' icon.

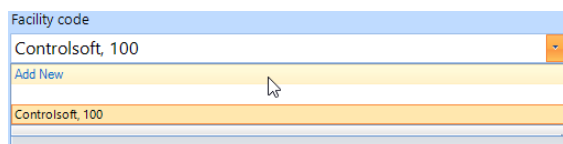
Select the **User Type** from the dropdown box.

Enter the **Start Token Number**

Enter the **Quantity** to add in this batch

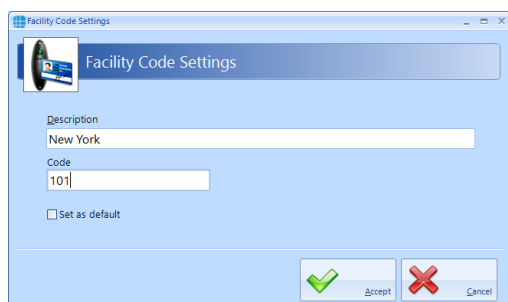
Select or Add a new **Facility Code**.

To add a new Facility Code, select the **Facility Code** field and select **Add New**



The screenshot shows a close-up of the 'Facility code' dropdown menu. The current selection is 'Controlsoft, 100'. Below the dropdown, there is an 'Add New' button. A mouse cursor is pointing at the 'Add New' button. Below the 'Add New' button, there is a list of existing facility codes, with 'Controlsoft, 100' highlighted.

Fill in a **Description** for this facility code (this can be the same value as the facility code itself) and the **Facility Code** value. You can set the facility code to default, so it appears by default for all new user by ticking **Set as Default**.



The screenshot shows the 'Facility Code Settings' dialog box. It has a title bar with the text 'Facility Code Settings' and a close button. Below the title bar is a header area with a small icon of a card and the text 'Facility Code Settings'. The main area contains several fields: 'Description' is a text box with 'New York'; 'Code' is a text box with '101'; and 'Set as default' is a checkbox that is currently unchecked. At the bottom right, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red 'X' icon.

Controlsoft Identity Access Operator Guide

6.10. Importing Users

When importing from a .csv file, it is also necessary to map the fields in the file to the correct fields in Identity Access.

To import data, select **Import Data** from the **Tools** menu and follow the Import Wizard:

Under **Select Import Source**, select the appropriate source, for example, to import from a csv file, select **Text File** from the dropdown list and click **[Next]**

Under **Source File**, click the **[...]** button to browse to the .csv file. Select **Delete old data before importing new data** if required. Click **[Next]**.

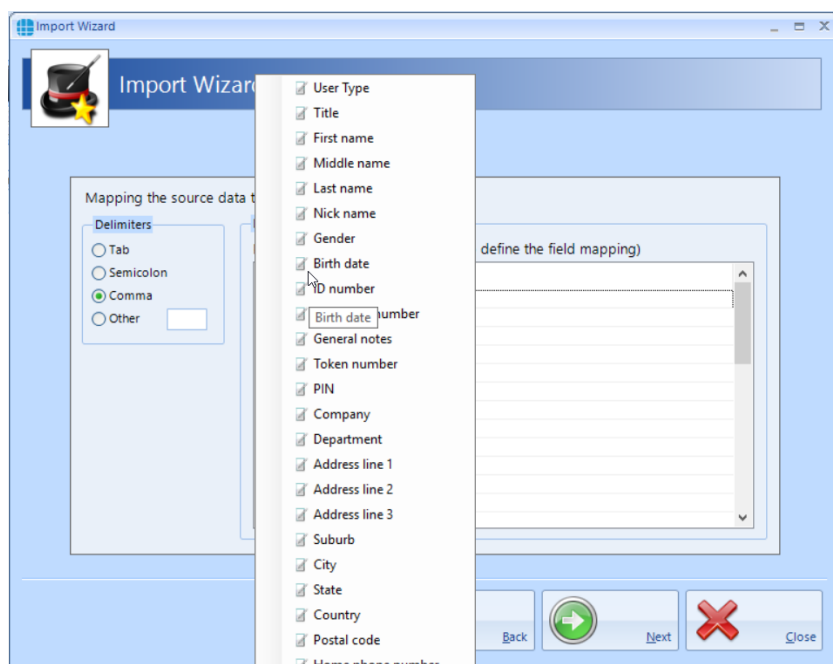
Select Destination should be set to define the types of user being imported (Employee, Visitor or Contractor). Select **Ignore duplicate names** to avoid duplicate entries. Click **[Next]**

NOTE: While this will stop a User appearing in the list twice, it will also stop a new User from being imported if they have the same name as an existing User. To avoid this, always ensure that there are differences between similar names (e.g. Fred Smith, Fred A Smith and Freddie Smith)

Selecting the source file's format defines how the .csv file is configured (the actual settings required will depend on how the .csv file has been configured). Click **[Next]**

Under **Delimiters**, choose which character has been used in the .csv to separate data (usually commas or tabs).

Under **Data Preview**, link each column in the .csv file to the corresponding database field. Click on each column header and select the required field from the dropdown list:



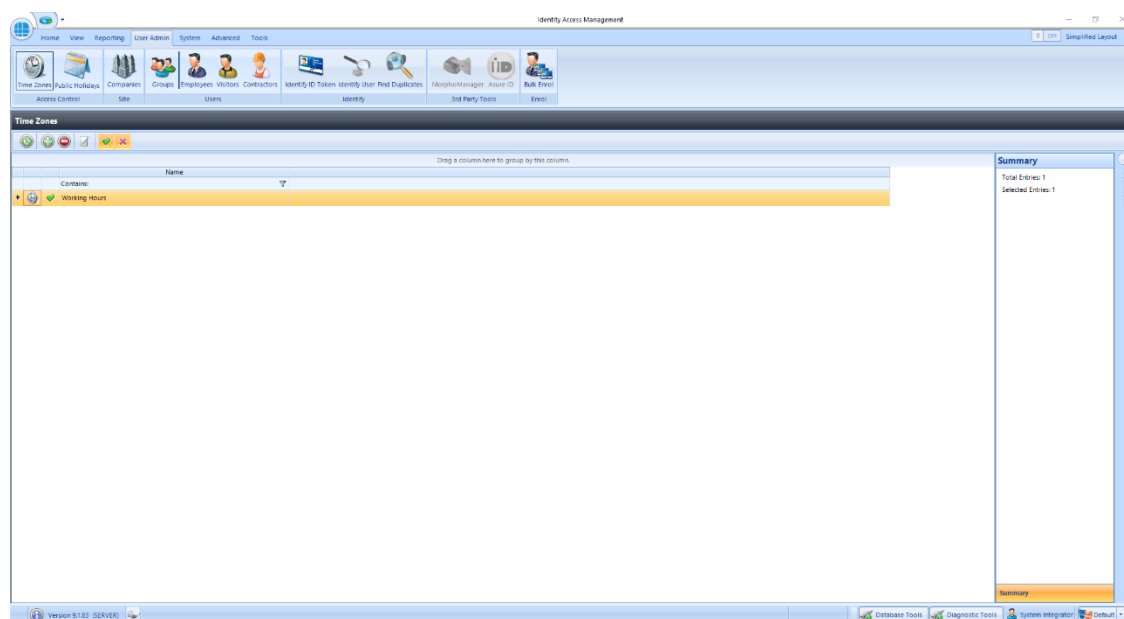
7. Configure Time Zones

Time Zones is a useful facility as it modifies the operation of the system at given times. Time Zones can be used in 2 ways:

If a Time Zone is allocated to a Group, all Users in that Group will have access through the relevant doors only within the Time Zone period

If a Time Zone is allocated to a Door, the door will provide free access within the Time Zone period

To use Time Zones, select the **User Admin** tab, then click **Time Zones** in the ribbon bar.



This Time Zones window shows that there are no Time Zones in the database. The option buttons are:



Refresh: Updates the list of Time Zones



Add: Creates a new Time Zone in the list



Delete: Removes the selected Time Zone/s from the list



Edit: edits the selected Time Zone



Show/Hide Active: This button will show or hide Time Zones selected as Active.



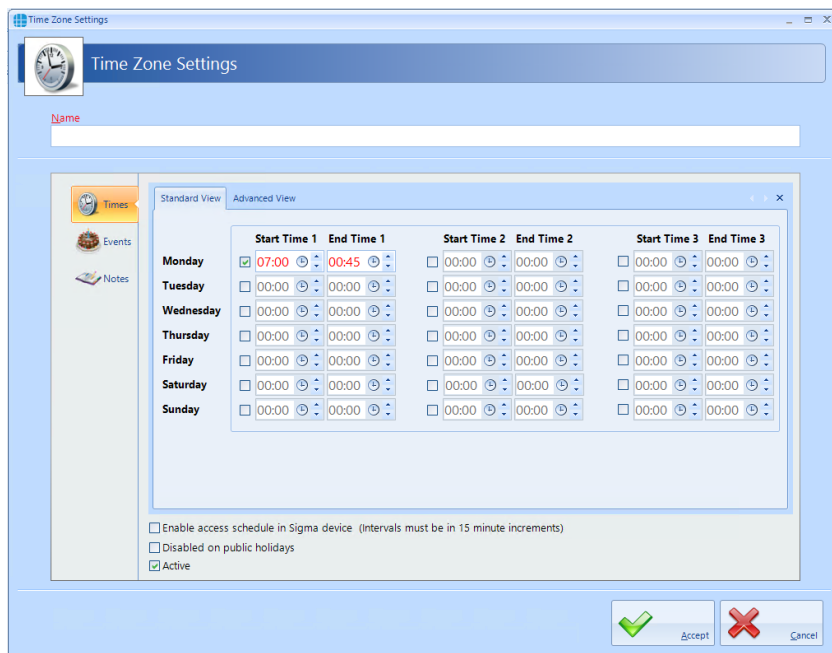
Show/Hide Inactive: This button will show or hide Time Zones not selected as Active.

To create a Time Zone, select the **Add** New button



7.1. Creating Time Zones

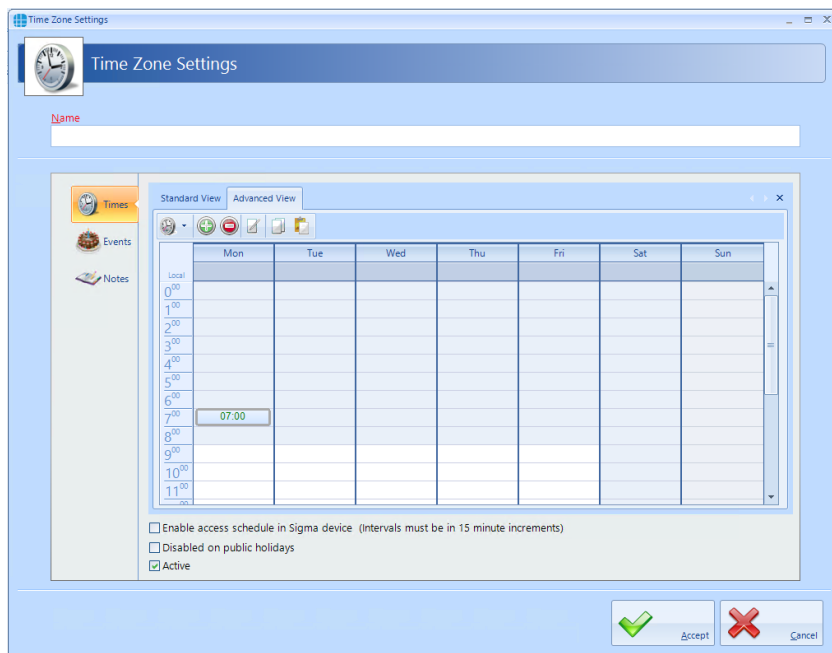
Use the Time Zone Properties screen to configure the Time Zones:



Enter a **Name** for the Time Zone

Each Time Zone can have up to 3 segments, each with its own Start Time and End Time. Unlike previous versions of Identity Access, Time Zones can now be entered to 1 minute resolution.

Time Zones can be created graphically rather than entering times by selecting the **[Advanced View]** tab



The following buttons are available in Advanced View:

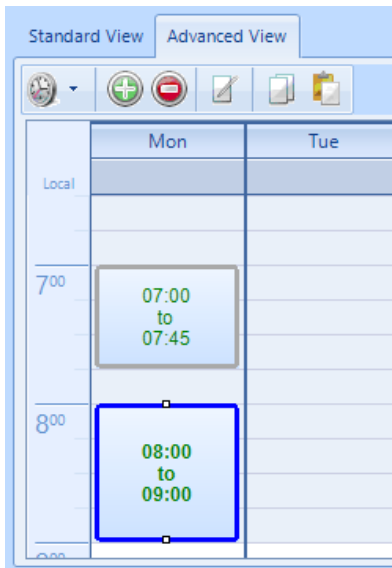


The display can be adjusted to show 1 hour, 30 minute, 15 minute, 5 minute or 1 minute resolution

Controlsoft Identity Access Operator Guide



Adds a time entity. Drag the mouse to select a time period, then click this button. Once created, the display will show the relevant Start Time and End Time Example:



Deletes the selected time entity



Edits the selected time entity



Copies the selected time entity



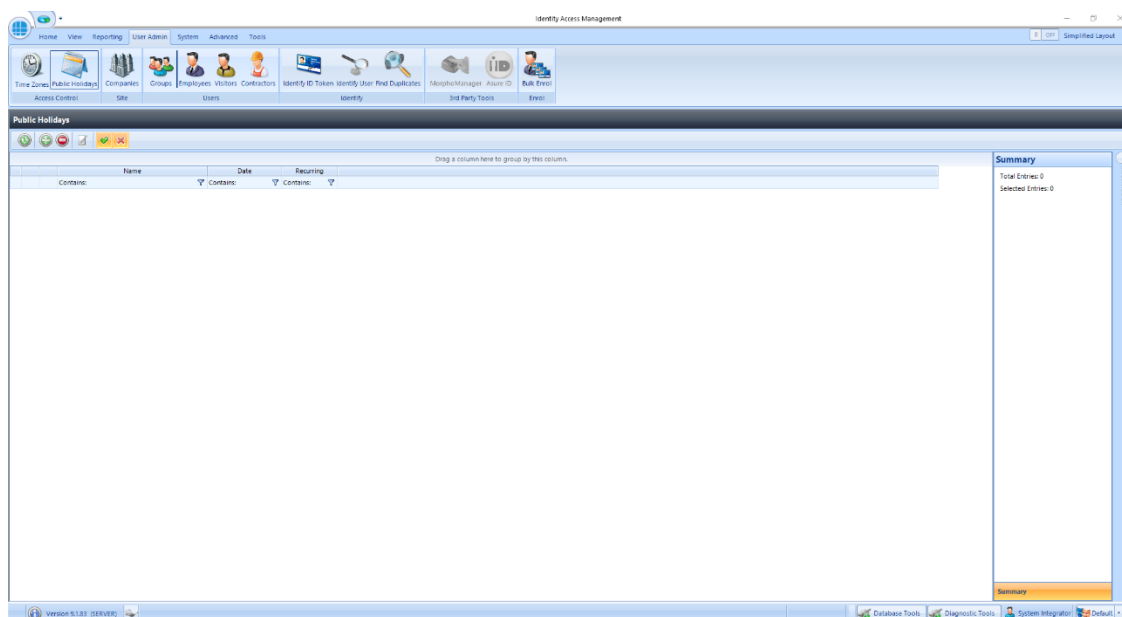
Pastes the selected time entity

In either view, if **Disabled on public holidays** is selected, the Time Zone will not be active during defined public holidays.

Ensure that **Active** is ticked otherwise it will not be possible to use the Time Zone.

8. Public Holidays

To configure a Public Holiday, select the **User Admin** tab, then select **Public Holiday** in the ribbon bar



This Public Holidays window shows that there are no Public Holidays in the database. The option buttons are:



Refresh: Updates the list of Public Holidays



Add: Creates a new Public Holiday in the list



Delete: Removes the selected Public Holiday/s from the list



Edit: edits the selected Public Holiday



Show/Hide Active: This button will show or hide Public Holidays selected as Active.



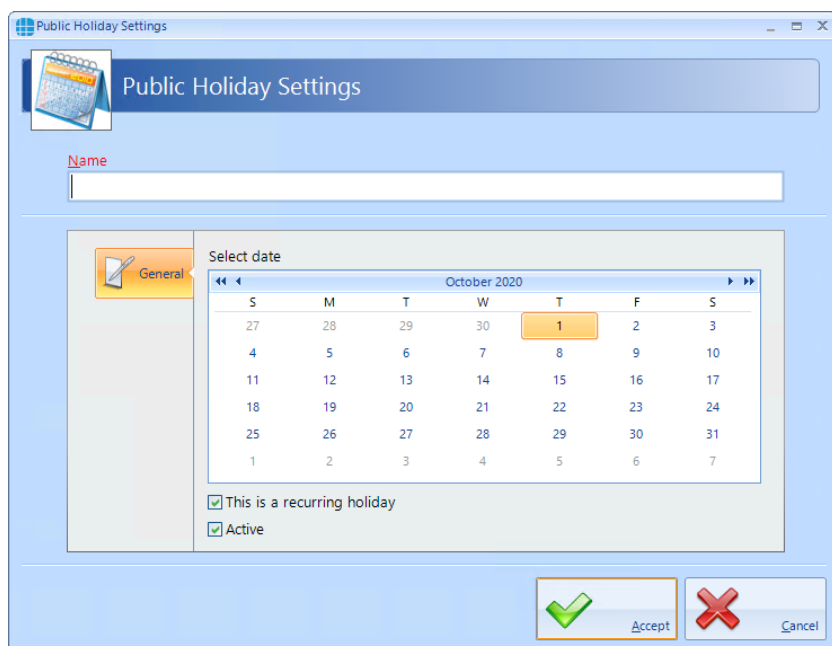
Show/Hide Inactive: This button will show or hide Operators who are not Active.

To create a new Public Holiday, click the **Add** New button



8.1. Creating Public Holidays

To configure a Public Holiday:

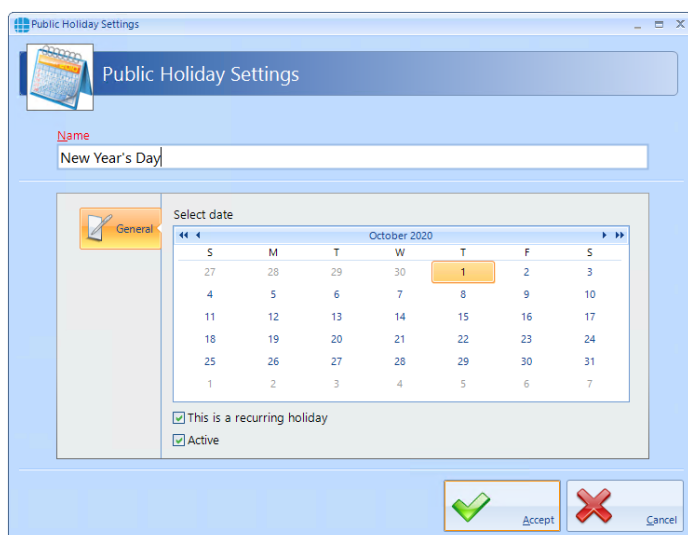


Enter a **Name** for the Public Holiday

Select date of the Public Holiday from the calendar

Select **This is a recurring holiday** if appropriate (e.g. New Year's Day)

Ensure that **Active** is ticked to use the Public Holiday date.



Click **[Accept]** when done.

9. Companies and Departments

Companies and Departments can be a useful tool when running reports to filter out unwanted data. It would be possible, for example, to run a report only on users in the Finance department.

To configure Companies and Departments, select **Companies** from the **User Admin** tab:

Name	Departments
Contano	Equals
*Landlord - ABC Healthcare	6
Contractor - Footrot Plumbing	1
Contractor - Delta Facilities	2
Tenant - Delta Accounting	3
Contractor - General	1



Refresh: Updates the list of Companies / Departments



Add: Creates a new Company / Department in the list



Delete: Removes the selected Company / Department/s from the list



Edit: Edits the selected Company / Department




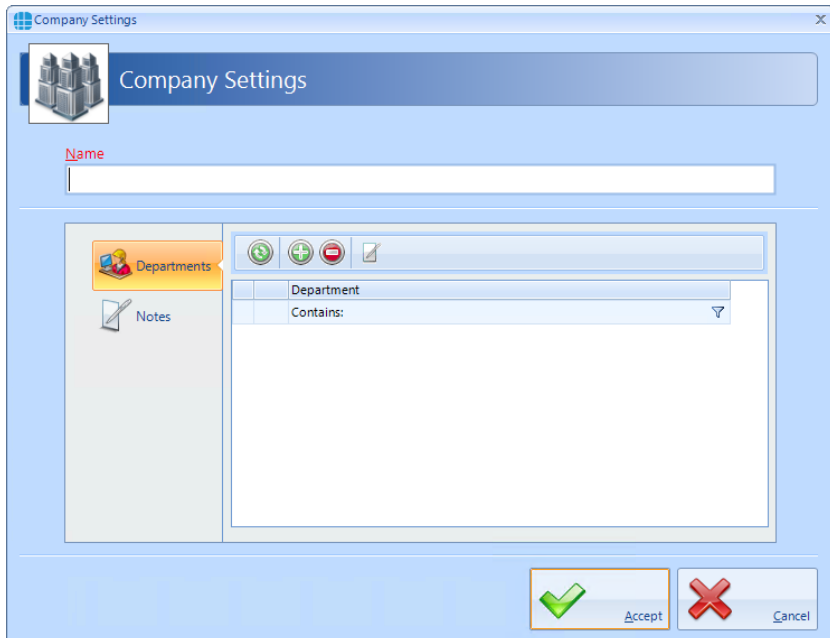
Show/Hide Active: This button will show or hide Companies / Departments selected as Active.




Show/Hide Inactive: This button will show or hide Companies / Departments not selected as Active.


9.1. Creating Companies and Departments

Select the Add button  to display the Company Properties screen below:




Department
Contains:


 Refresh: Updates the list of Departments

 Add: Creates a new Department in the list

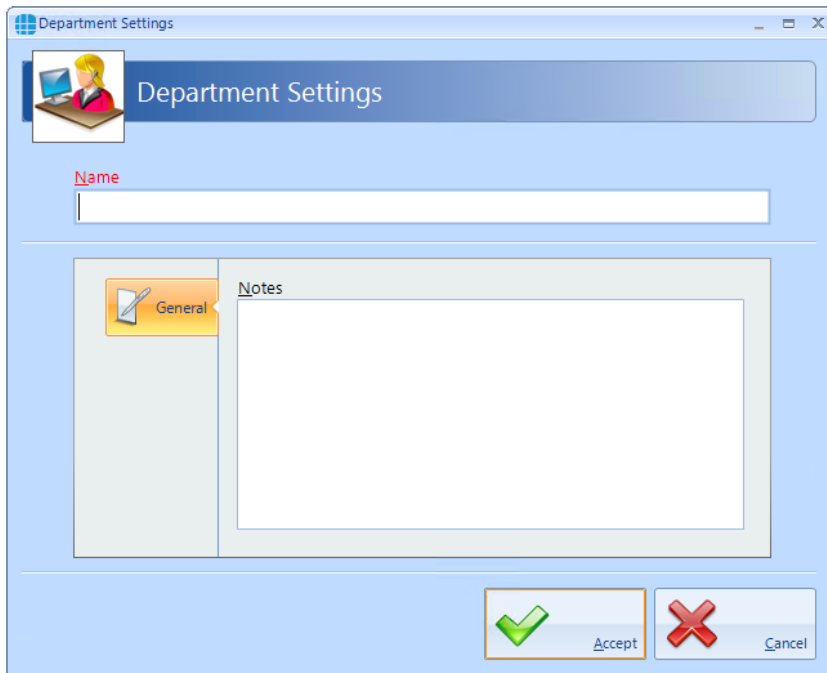
 Delete: Removes the selected Department/s from the list

 Edit: Edits the selected Department

Name: Add a name for the new Company

Click the Add button  to create a Department for the Company

Controlsoft Identity Access Operator Guide



The screenshot shows a window titled "Department Settings" with a standard Windows-style title bar. Inside the window, there is a header area with a small icon of a person at a computer and the text "Department Settings". Below this is a text input field labeled "Name". Underneath the input field is a tabbed interface with a single tab labeled "General" containing a large, empty text area labeled "Notes". At the bottom right of the window, there are two buttons: "Accept" with a green checkmark icon and "Cancel" with a red X icon.

Name: Add a name for the new Department

Notes: Add any notes which could make the configuration easier to understand in the future.

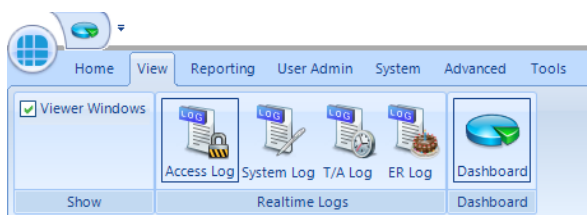
NOTE: A Company can support multiple Departments.

10. Event Viewers and Reports

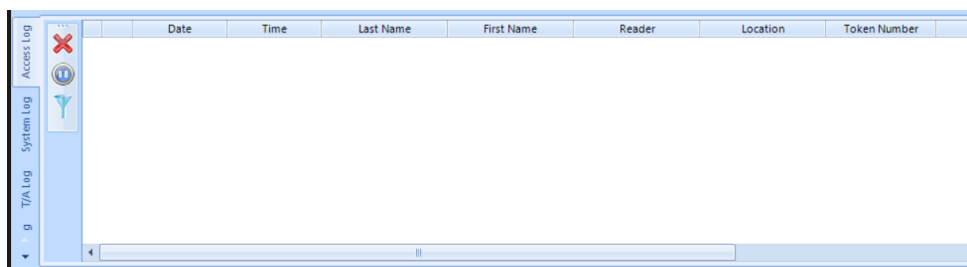
The Event Viewer in Identity Access software is a powerful tool for analysing system activity.

10.1. Event Viewers

Identity Access provides a live view of events, useful for trouble-shooting or tracking users through the system. To view live events, ensure that the option **Viewer Windows** is selected in the **View** tab.



When selected, the viewer window will be visible in the lower half of the screen:



Clear Window: Clears all events in the Viewer Window

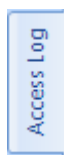


Pause/Run: Pausing the Viewer Window will temporarily suspend events from being displayed.



Enable filters to selectively display required information. This can be useful to display the movement of a single user through the system

The information to be displayed is controlled by the 3 tabs below the Viewer Window:



Displays events from the Access Log.

Controlsoft Identity Access Operator Guide

System Log

Displays events from the System Log.

T/A Log

Displays events from the Time & Attendance Log

ER Log

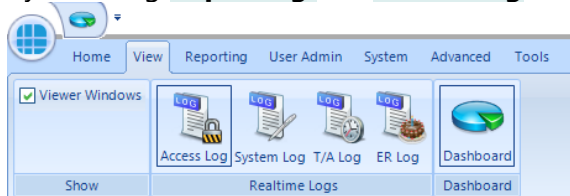
Displays Events and Actions from each controller

NOTE: The size of the viewer window can be adjusted simply by dragging the top of the window up or down.

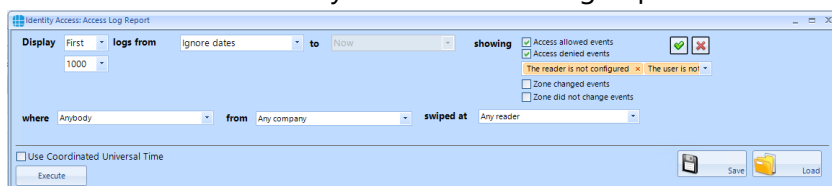
10.2. Access Control Reporting

An Access Control report is a record of when people have used their token at a reader, providing an audit trail of when someone entered or exited areas of the premises.

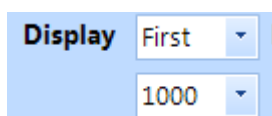
Within Identity Access there are multiple ways to run Access Control reports. It is possible to run reports based on specific date / times, specific readers, or specific users. The Access Report menu can be accessed by selecting **Reporting** and **Access Log** in the **Access** group.



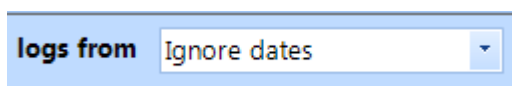
This then runs the Identity Access: Access Log Report form as shown below:



The options on generating the report are as follows:

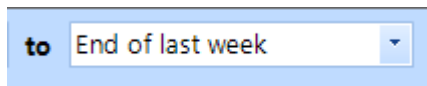


- defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.

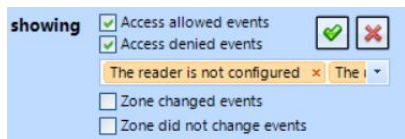


- defines the date that the report starts (Example ignore dates, start of last month or 1st January 2016)


Controlsoft Identity Access Operator Guide



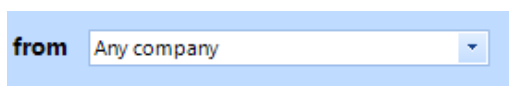
- defines the date that the report ends (Example today or end of last month)



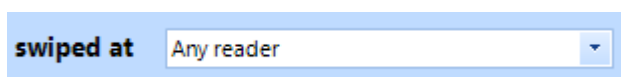
- defines which events are to be reported on, Access Allowed and/or Access Denied and any combination of events from the drop down list. The Tick selects all events in the dropdown list and the Cross deselects all events in the dropdown list. When AntiPassBack is enabled for a door, the system will also log changes to zone (e.g. "Moved to Inside" or "Moved to Outside"). These events can be included in the report if required.



- defines which user/s to report on

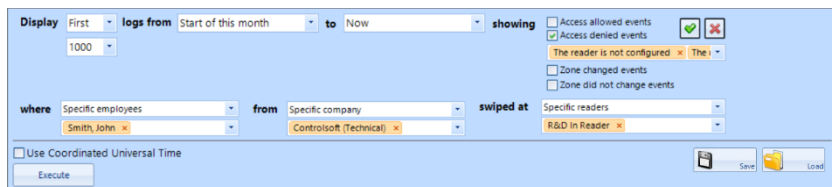


- defines which Company and Department to report on



- defines which reader/s to report on.

As an example, to generate a report to see if John Smith tried to get into R&D this month, the configuration would look like:





Once configured, click the **[Execute]** button to generate the report.



saves the current query for later use



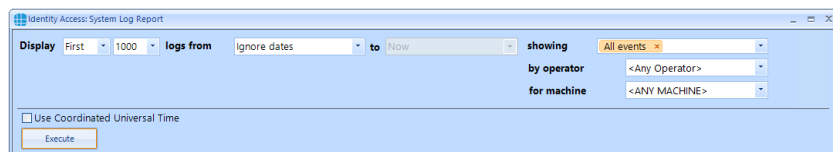
loads a saved query

To run a report on a specific person it is also possible to go to **User Admin** and **Employee / Visitor / Contractor** (depending on who you wish to run your report on). Highlight the user by left-clicking their entry and click the  icon. This will automatically generate a report for this specific person. To run a report on several people it is possible to hold down the [Ctrl] key and highlight multiple entries, then click the  icon.

10.3. System Log Reporting

The System Log report is a record of all Identity Access system events, such as when people have logged on / off the software, when doors have been forced open or when database entries have been modified. The System Log Report menu can be accessed by selecting **Reporting** and **System Log**.

The way System Log reports are configured is similar to the Access log Reports, but with fewer options:

The screenshot shows the 'Identity Access System Log Report' configuration window. It features several dropdown menus and a checkbox. The 'Display' dropdown is set to 'First' and the number of events is set to '1000'. The 'logs from' dropdown is set to 'Ignore dates' and the 'to' dropdown is set to 'Now'. The 'showing' dropdown is set to 'All events'. The 'by operator' dropdown is set to '<Any Operator>' and the 'for machine' dropdown is set to '<ANY MACHINE>'. There is a checkbox for 'Use Coordinated Universal Time' which is unchecked, and an 'Execute' button at the bottom.

Display First 1000 - defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.

logs from Ignore dates - defines the date that the report starts (Example ignore dates, start of last month or 1st January 2016)

to End of last week - defines the date that the report ends (Example today or end of last month)

showing All events - defines which events are to be reported on, such as startup & shutdowns, which Operators have logged on.

by operator <Any Operator> - defines which Operator to report on

for machine <ANY MACHINE> - defines which Client machine to report on

Once configured, click the **Execute** button to generate the report.

Controlsoft Identity Access Operator Guide

10.4. Fire Rollcall Report

The Fire Rollcall is a report that indicates who is currently inside the building. For the Fire Rollcall to be available there must be dedicated IN and OUT readers that everyone uses when they enter and exit the building. The Fire Rollcall report can be accessed by selecting **Reporting** and **Fire Rollcall**.

When generating a Fire Rollcall report, no configuration is required, simply click the Fire Rollcall button



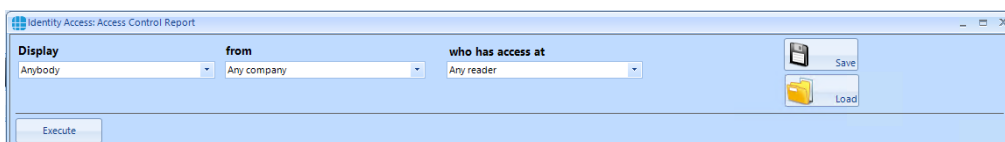
NOTE: The Fire Rollcall report is NOT available in Identity Access unless an Identity Access Professional or Enterprise license is applied.

10.5. Access Control Status Report

The Access Control Status report shows which readers are accessible to one or more users. The report is generated by clicking **Access Control** in the **Status** area of the reporting ribbon bar



Options when running the report are as follows:

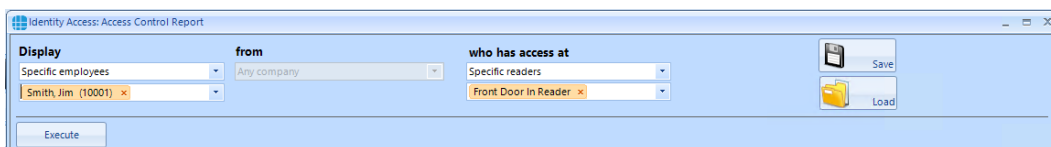


Display - selects specific users to report on

from - selects specific Companies and Departments to report on

who has access at - selects the readers to report on


EXAMPLE: to report whether a specific user has access through a particular reader, the report configuration would look as follows:



Clicking **[Execute]** would then generate the following report:

Controlsoft Identity Access Operator Guide

Access Control Report Monday, October 5, 2020



Access Control Report

Monday, October 5, 2020
4:48:56 PM

Front Door In Reader
All staff

Last Name	First Name	Company	Department
Smith	Jim		

This report shows that the reader called "Front Door In Reader" is accessible by the group "All staff" which includes the user "Jim Smith"

10.6. Groups Status Report

The Groups Status report shows which users, card readers, fingerprint readers and AntiPassBack doors are associated with one or more groups. The report is generated by clicking Groups in the Status area of the reporting ribbon bar:



Options when running the report are as follows

Identity Access: Group Status Report

Show all

Persons Card Readers Morpho Readers APB Doors That belongs to

Anybody Any reader Any Morpho reader Any APB door Any group

from

Any company

Execute

Persons - choose any combination of users to include in the report

Card Readers - choose any combination of card readers to include in the report

Morpho Readers - choose any combination of fingerprint readers to include in the report

APB Doors - choose any combination of AntiPassBack doors to include in the report

That belong to - choose any combination of groups to report on

From - if configured, define the Company and Department to report on

When the above options have been configured, click **[Execute]** to run the report.

NOTE: This report can be run for a specific Group by selecting the required Group in the Groups screen, then right click and select report from the Option Wheel

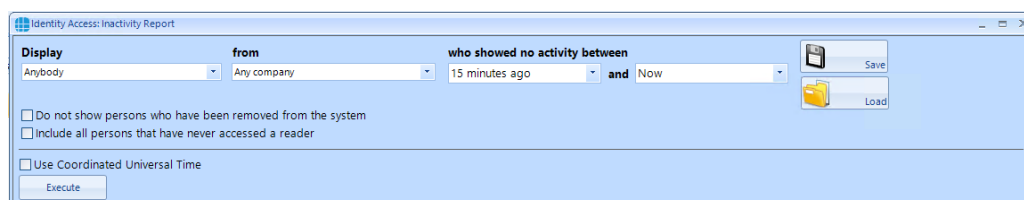
10.7. Inactivity Report

The Inactivity report is used to identify users who are no longer using the system, to allow an operator to effectively manage the user database.

To run an Inactivity Report, select the **Reporting** tab.



Now select the **Inactivity** button to run the report



Display - selects specific users to report on


from - selects specific Companies and Departments to report on


who showed no activity between - selects the time range to report on

Do not show persons who have been removed from the system will exclude any users who have already been deleted.

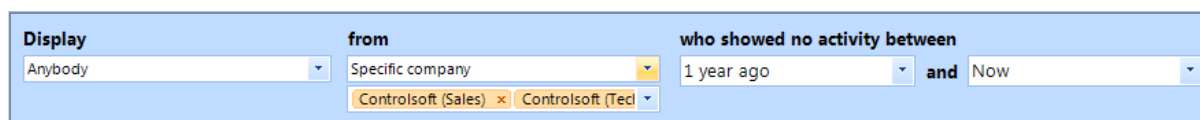
Include all persons that have never accessed a reader will include users on the system who have never used their token.

Use Coordinated Universal Time can be selected where controllers are configured with different International UTC Zones to ensure that events in the report are displayed chronologically

 Save saves the current query for later use

 Load loads a saved query

EXAMPLE: to report inactivity on anyone in Controlsoft Sales or Technical within the past year, the report configuration would look as follows:

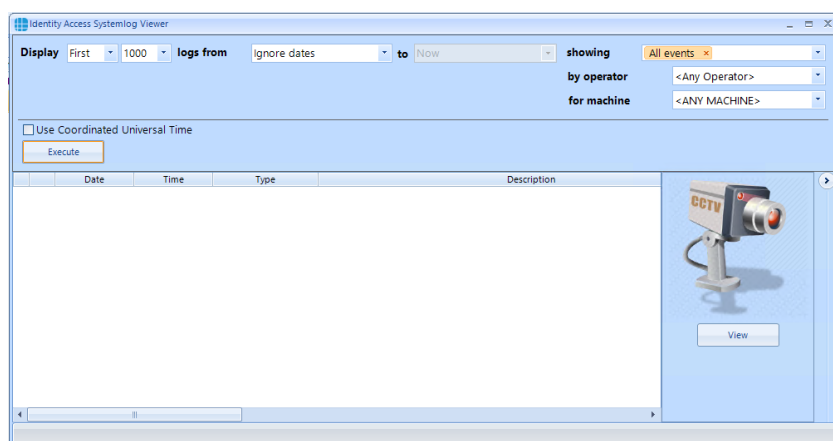


10.8. System Log

To view events in the System Log, select the **Reporting** menu



Now click the **System Log** button to start the viewer.



Display - defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log

logs from - defines the date that the report starts (Example ignore dates, start of last month or 1st January 2020)

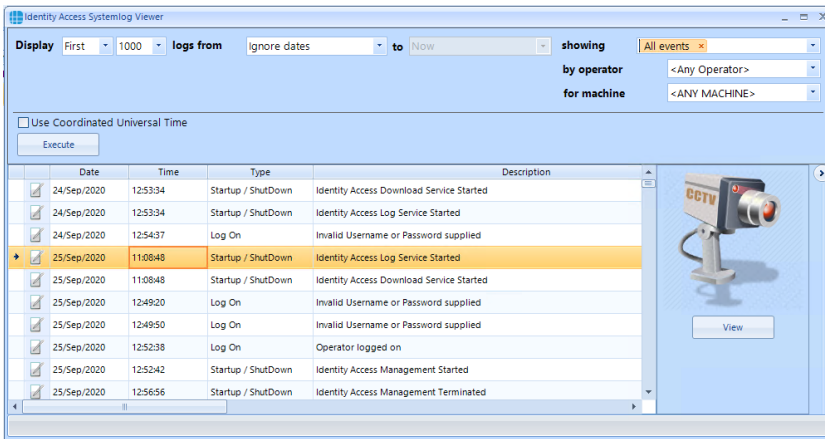
showing - which events are to be reported on, any combination of events from the drop down list.

by operator - defines which Operator to report on

for machine - defines which Client machine to report on

When the report is configured, simply click the **Execute** button

Controlsoft Identity Access Operator Guide



If an entry in the System Log contains an image (for example a snapshot generated as an action from an event), the image can be viewed by clicking the **[View]** button