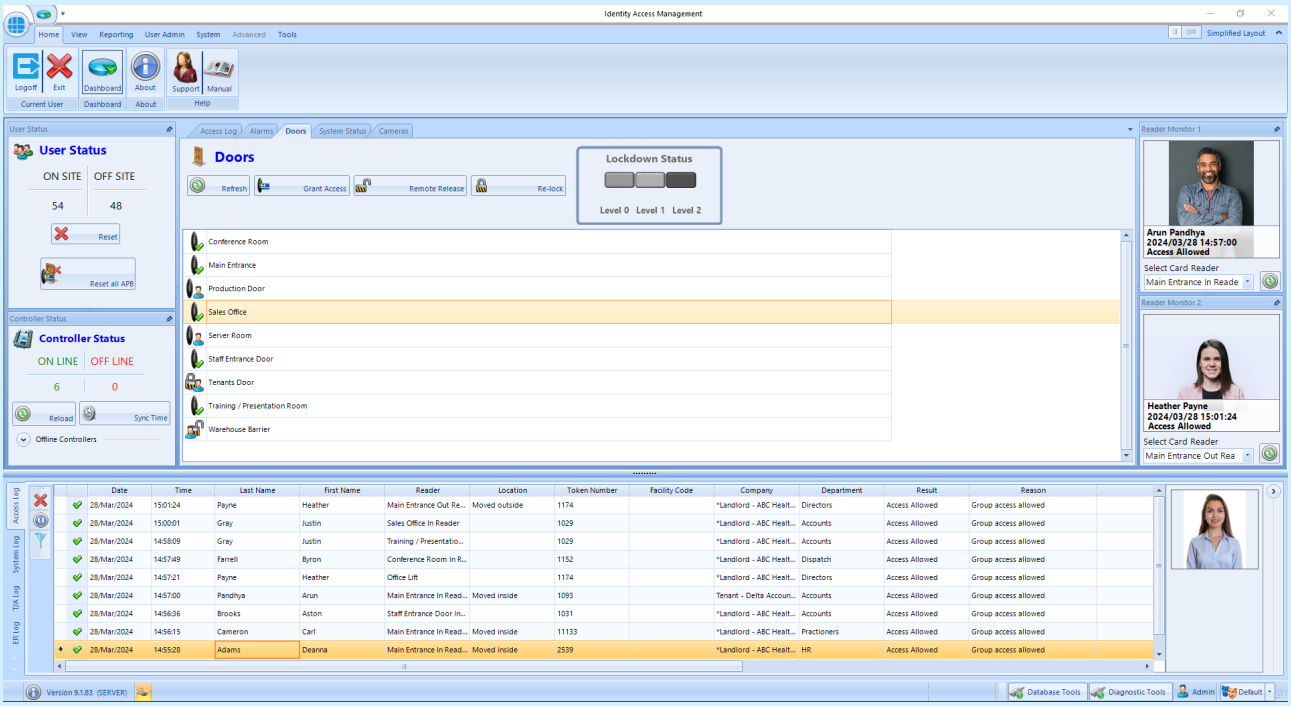
Controlsoft Identity Access Management Software



SOFTWARE GUIDE

Version 9.1.99 © 2026 Controlsoft Ltd

Document No: 9010-0053 Issue 12

controlsoft® access control

1. Introduction 7

2. PC Specifications 11

3. System Architecture 14

4. Identity Access - Express Commissioning Guide 17

4.1 Step 1. Pre Installation Checks 18
4.2 Step 2. Installing Identity Access Software 18
4.3 Step 3. (Optional) Licensing Identity Access 20
4.4 Step 4. Launching the Identity Access Software 20
4.5 Step 5. Configure IP Controller(s) 21
4.6 Step 6. Add IP Controller(s) 23
4.7 Step 7. Add Downstream RS-485 Controllers 24
4.8 Step 8. Add Doors / Readers using Door Wizard 26
4.9 Step 9. Add Employee 27
4.10 (Optional) Configure Groups (Access Levels) 29
4.11 (Optional) Configure Time Zones (Access Schedules) 31
4.12 (Optional) Backups / Installing Identity Access Client 34

5. Identity Access Software Overview 37

5.1 Identity Access Header and Footer 38
5.2 The Option Wheel 39
5.3 The Dashboard 39
5.4 Identity Access Home Tab 42
5.5 Identity Access ViewTab 44
5.6 Identity Access Reporting Tab 45
5.7 Identity Access User Admin Tab 46
5.8 Identity Access System Tab 46
5.9 Identity Access Advanced Tab 47
5.10 Identity Access Tools Tab 48

6. System > Operators 52

6.1 Editing the Default Operators 54
6.2 Adding an Administrator 56
6.3 Adding an Operator 57

7. System > Controllers 60

 © 2026 Controlsoft Ltd

7.1 Controller General 62
7.2 Controller Settings 65
7.3 Controller Timeouts 70
7.4 Controller Sirens 72
7.5 Controller Events 74
7.6 Controller Notes 76

8. System > Doors 77
8.1 Door Properties General 79
8.2 Door Properties I/O Settings 81
8.3 Door Properties Time Zones 86
8.4 Door Properties Events 87
8.5 Door Properties Notes 88

9. System > Card Readers 89
9.1 Card Reader General 91
9.2 Card Reader Time Zones 93
9.3 Card Reader Settings 94
9.4 Card Reader Events 95
9.5 Card Reader Notes 96

10. System > Morpho Readers 97
10.1 Morpho Reader General 99
10.2 Morpho Reader Settings 101
10.3 Morpho Reader Time Zones 102
10.4 Morpho Reader Notes 103

11. System > Elevators 104
11.1 Elevators General 106
11.2 Elevators Settings 107
11.3 Elevators Floors 108
11.4 Elevators Time Zones 108

12. System > DropBox 110

13. User Admin > Time Zones 112
13.1 Time Zones Times 114
13.2 Time Zones for Morpho Readers 118
13.3 Time Zones Events 118

14. User Admin > Public Holidays 120

© 2026 Controlsoft Ltd

15. User Admin > Companies and Departments 123
15.1 Creating Companies and Departments 125
16. User Admin > Groups 127
16.1 Groups Properties Users 129
16.2 Groups Properties Card Readers 130
16.3 Groups Properties Morpho Readers 131
16.4 Groups Properties APB Doors 132
16.5 Group Properties Elevators 133
16.6 Groups Properties Time Zones 134
16.7 Group Properties Events 134
16.8 Allocating Users to Groups 135
17. Enrolment Readers 136
18. User Admin > Employees / Visitors / Contractors 138
18.1 User General 141
18.2 User Photo 143
18.3 User Fingerprints 147
18.4 User Mobile Access 151
18.5 User Tokens 160
18.6 User Extra Data 161
18.7 User Contact 163
18.8 User Events 163
18.9 User Notes 165
18.10 Importing Users 165
19. User Admin > Bulk Enrolment 171
20. Advanced Tab 174
20.1 Advanced > Object Groups 176
20.2 Advanced > Counters 178
20.3 Advanced > Timers 181
20.4 Advanced > Inputs 183
20.5 Advanced > Outputs 186
20.6 Advanced > Graphics Designer 189
20.7 Advanced > Events 195
20.8 Typical Examples of Events & Actions 204
21. Event Viewers and Reports 217

© 2026 Controlsoft Ltd

21.1 Event Viewers 218
21.2 Fire Rollcall Report 220
21.3 Access Control Reports 220
21.4 System Log Reports 222
21.5 Time & Attendance Report 223
21.6 Access Control Status Report 227
21.7 Groups Status Report 228
21.8 Inactivity Report 229
21.9 System Log 231

22. Engineer Tools and Services 233
22.1 Database Tools (Log Service) 234
22.2 Diagnostic Tools (Download Service) 235
22.2.1 Home 236
22.2.2 iNet Controllers 237
22.2.3 Biometric Devices 240
22.3 Service Manager 242

23. Identity Access Configuration 244
23.1 IA Configuration > System Info 245
23.2 IA Configuration > Data Retention 246
23.3 IA Configuration > Reports 246
23.4 IA Configuration > Cards & Readers 247
23.5 IA Configuration > HID Mobile Access 255
23.6 IA Configuration > Biometrics 256
23.7 IA Configuration > Badge Printing 262
23.8 IA Configuration > Extra Data Fields 262
23.9 IA Configuration > Email 264
23.10 IA Configuration > Password Policy 267
23.11 IA Configuration > Lockdown 269
23.12 IA Configuration > User Profiles 269
23.13 IA Configuration > User Interface 270
23.14 IA Configuration > Backup 271
23.15 IA Configuration > Databases 275
23.16 IA Configuration > Network 276
23.17 IA Configuration > Services 277

24. Appendix A - Product History 279

25. Appendix B - Types of Door 288

 © 2026 Controlsoft Ltd

25.1 Normal Door 289
25.2 Turnstile 290
25.3 Airlock 291
25.4 Aperio Door 293
26. Appendix C - HID Asure ID Software 294
27. Appendix D - Facility Codes 296
28. Appendix E - iNet webpage 300
29. Appendix F - AntiPassBack 307
30. Appendix G - IA Morpho Configurator 314
31. Appendix H - Controller Status 317
32. Appendix I - Duress 324
33. Appendix J - Database Importer 327
33.1 Installing Database Importer 330
34. Appendix K - Identity Access Web Client 335
35. Appendix L - Site Selector 337
36. Appendix M - Licence Terms & Conditions 339
37. Appendix N - Glossary 341
38. Controlsoft Contact Details 345

0

© 2026 Controlsoft Ltd

Introduction

1 Introduction

Identity Access (IA) Software Version 9 from Controlsoft© is a PC-based Access Control Management system.

The Identity Access software manages the access control database, which is downloaded to the iNet® Controllers. The iNet controls access through the doors, either directly or via Downsteam RS-485 Controllers.

The latest version of Identity Access software can be downloaded from our website www.controlsoft.com/login

The below table shows the differences between our free Identity Access Lite and paid for Identity Access Professional and Enterprise versions. The same installation files are used for either Identity Access Lite, Professional or Enterprise and can be licensed at any time.

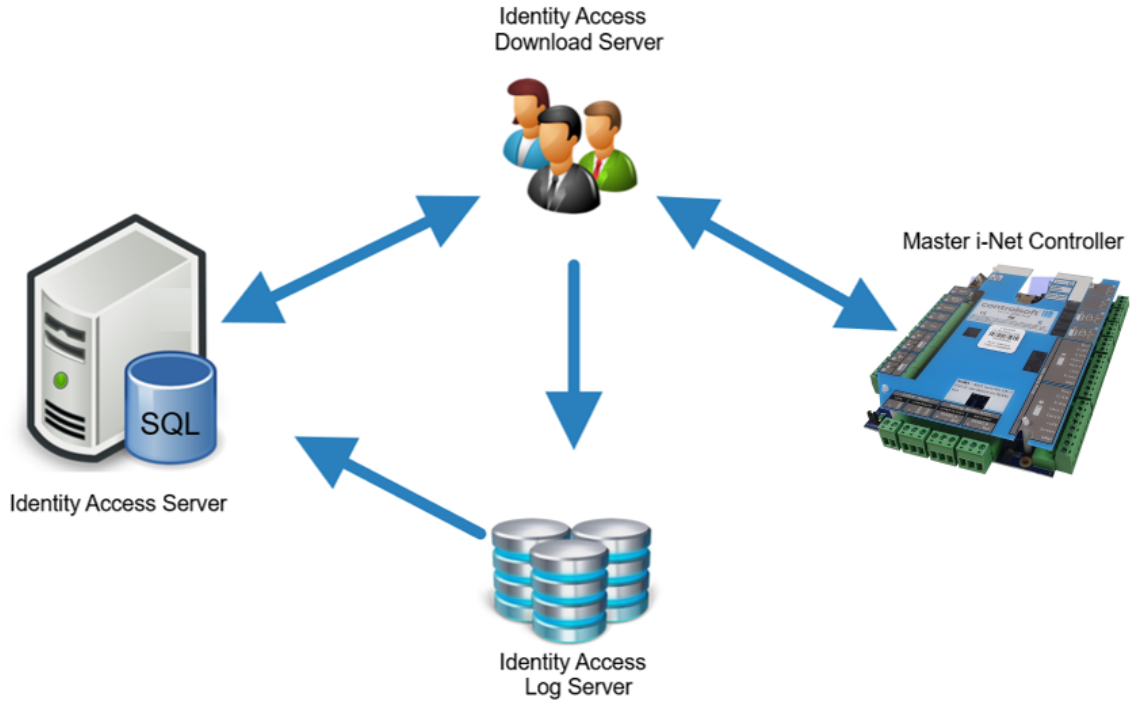
	FREE LITE SOFTWARE (IA-LITE/SUB-LITE)	PROFESSIONAL LICENCE (IA-PRO / SUB-PRO)	ENTERPRISE LICENCE (IA-ENT/SUB-ENT)
Maximum Number of Doors or Readers	12	64	Unlimited
Unlimited Number of Cardholders	✓	✓	✓
Group Management	✓	✓	✓
Real Time Access and Alarms Events Viewers	✓	✓	✓
Employee, Visitor and Contractor Management	✓	✓	✓
Unlimited Number of Client PCs	✓	✓	✓
Support for HID OSDP Readers	✓	✓	✓
Support for Assa Abloy APERIO Wireless locks	✓	✓	✓
Controller, Door and Report Wizards	✓	✓	✓
Time Zones to Schedule Group, Door & PIN Pad operation	✓	✓	✓
Issue Temporary Cards	✓	✓	✓
Multiple Sites	✓	✓	✓
Users On Site / Off Site Counter	✓	✓	✓
Operator Software Door Control	✓	✓	✓
Configurable User Data Fields	✓	✓	✓
Display User's Photo on Card Swipe	✓	✓	✓
Microsoft SQL Database Platform	✓	✓	✓
Snow Day Rule	✓	✓	✓

© 2026 Controlsoft Ltd

Photo ID Card Printing *	✓	✓	✓
Bulk Enrolment	✓	✓	✓
Web Client	×	✓	✓
Site Lockdown	×	✓	✓
Wiegand ANPR/ALPR Integration (SHA-1 26-Bit)	×	✓	✓
Fire Alarm Roll Call Report	×	✓	✓
Time & Attendance Reporting	×	✓	✓
Fingerprint Enrolment	×	✓	✓
Direct Integration with IDEMIA Biometric readers	×	✓	✓
Email Notifications	×	✓	✓
AntiPassBack	×	✓	✓
Preconfigured Logic for Airlocks & Turnstiles	×	✓	✓
Elevators	×	✓	✓
Counters and Timers	×	✓	✓
Programmable Inputs and Outputs	×	✓	✓
Interactive Site Maps	×	✓	✓
Customizable Events and Actions Wizard	×	✓	✓

* Badge printing requires an Asure ID licence per PC (Ordering Part No. IA-AID).

The Controlsoft Identity Access Server software is made up a several constituent parts, as described below:



© 2026 Controlsoft Ltd

Identity Access is the main software which includes the User Interface. This handles commissioning the system and saving it to the 'IAMain' database, viewing events and generating reports from the 'Access', 'System' and 'T&A' logs. This User Interface looks the same whether Identity Access has been installed as a Server or as a Client.

Download Service communicates with the iNets over an IP network, sending configuration data to the controllers and receiving event logs from them. This software is not accessible on a Client installation.

The **Log Service** accepts events from the Download Service and saves them in the relevant SQL database. This software is not accessible on a Client installation.

Microsoft SQL Server Database is used to store all data from the system, including system configuration data, all event logs, system passwords etc.

Other software is installed as described below. Once configured, these programs will not be required for day to day use.

IA Configuration 245 is only used to configure the Server.

IA Morpho Configurator is used to configure the fingerprint readers

IA Service Manager 234 allows for administration of the Download Service and the Log Service

iNet IP Utility is used to configure the iNet controllers

Licensing Utility is used to apply any licenses to the software

In addition, the following software may be run on the same or separate PCs connected across the network:

Identity Access Client provides one or more additional points at which the user interface can be operated.

HID Asure ID is used for card printing. Once a template has been created in Asure ID, it then accesses user information from the 'IAMain' database to populate and print the cards.

NOTE: Asure ID supplied with Identity Access is a 30 day trial version. To use Asure ID beyond this 30 day trial period, you will need to license the software. Please contact your vendor for further information.

© 2026 Controlsoft Ltd

PC Specifications

2 PC Specifications

Recommended Identity Access Operating Systems:

- Windows 10 (x64).
- Windows 11 (x64).
- Windows Server 2016.
- Windows Server 2020.
- Windows Server 2022.
- Windows Server 2025

Recommended Identity Access Server PC Specification

- Intel i5 processor @ 3GHZ
- 8GB RAM
- 100GB Free Disk Space
- 10/100 Network Card
- USB Port
- Screen Resolution = 1280x800 or better

Recommended Identity Access Server Performance PC Specification (more than 10,000 users)

- Intel i7 processor @ 3GHZ
- 16GB RAM
- 250GB Free Disk Space
- 10/100 Network Card
- USB Port
- Screen Resolution = 1280x800 or better

Recommended Identity Access Client PC Specification

- Intel i3 processor @ 3GHZ
- 4GB RAM
- 100GB Free Disk Space
- 10/100 Network Card
- USB Port

© 2026 Controlsoft Ltd

- Screen Resolution = 1280x800 or better

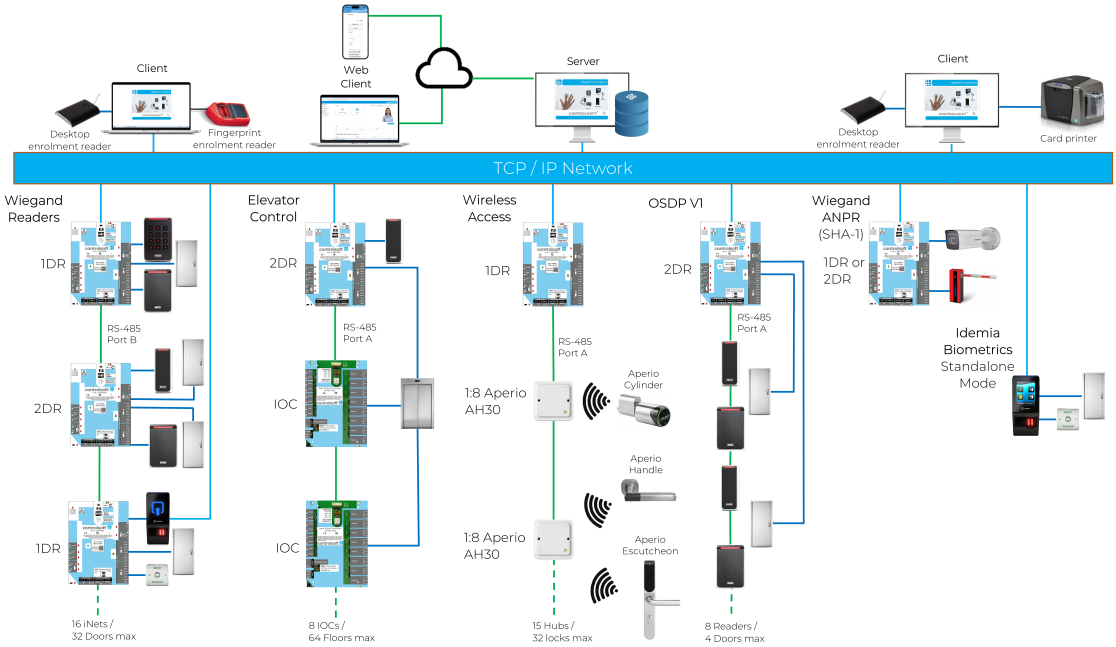
© 2026 Controlsoft Ltd

System Architecture

3 System Architecture

Before we start to do anything with the software, we will review how the hardware is configured and how this relates to the programming. Two types of iNet controller are available, the One Door Controller (1DR) with 5 inputs, 2 output relays & 2 Wiegand reader ports, and the Two Door Controller (2DR) with 9 inputs, 4 output relays and 2 Wiegand reader ports.

As well as iNet controllers, the system can support Input/Output modules, OSDP/RS-485 readers, Aperio Wireless handles Idemia Morpho biometric readers and HID Mobile Access readers.



Option 1 – IP Controllers:

A channel comprises of an iNet controller connected to the Identity Access software via IP . The system can be expanded simply by adding further iNets connected via IP. The Master iNet continues to control its doors if there is a problem with the network. Once the problem is restored, all events are transferred from the iNet to the Database.

Option 2 – Downstream RS-485 Controllers: The channel comprises of an iNet controller connected to the Identity Access software via IP. The other controllers are called Downstream iNets and are connected to the IP controller via RS-485.

The Master and all Downstream iNets each hold a copy of the access control database, so each Downstream controller continues to control its doors if a fault occurs on the RS485 bus. Once the fault is restored, all events are transferred from the Downstream iNet to the Master iNet and then to the Database.

Option 3 – Input / Output Controllers

The channel comprises of an iNet controller connected to the Identity Access software via IP.

© 2026 Controlsoft Ltd

The Input/Output Controllers are connected to the iNet controller via RS-485. This topology is used for Elevator Control.

Option 4 – OSDP/RS-485 Readers:

The channel comprises of an iNet controller connected to the Identity Access software via IP.

Up to 8 OSDP (RS-485) readers (Two Door Controllers) or up to 2 OSDP readers (One Door Controller) are then connected to the iNet via RS-485.

Option 5 – RS-485 Aperio Hubs:

The channel comprises of an iNet controller connected to the Identity Access software via IP.

Up to 8 RS-485 Aperio Hubs are then connected to the RS485 bus, each Hub supporting up to 8 Aperio Locks, to a maximum of 32 locks per iNet controller.

NOTE: It is NOT possible to combine Downstream iNets / Input/Output Controllers / OSDP Readers / Aperio Hubs on the same iNet controller, although a system can support multiple channels with each option:

© 2026 Controlsoft Ltd

Identity Access - Express Commissioning Guide

4 Identity Access - Express Commissioning Guide

4.1 Step 1. Pre Installation Checks

Before you start the installation, it is important to run through the following pre-installation checks.

1. Temporarily **disable** your anti-virus for the duration of the install.
2. Ensure that you have **Administrator** access to the PC you are installing on.
3. Ensure that all **Windows Updates** are applied before installation.

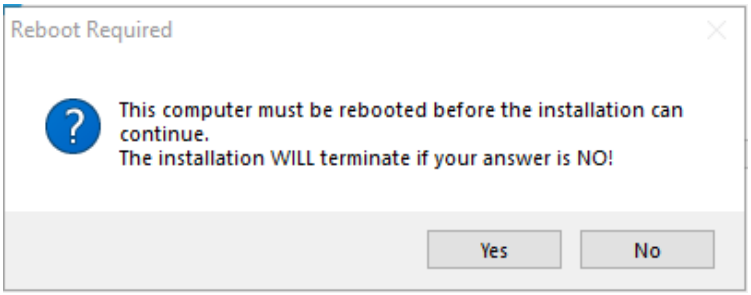
Click here: for further information on how to perform these checks on the various Windows operating systems.

4.2 Step 2. Installing Identity Access Software

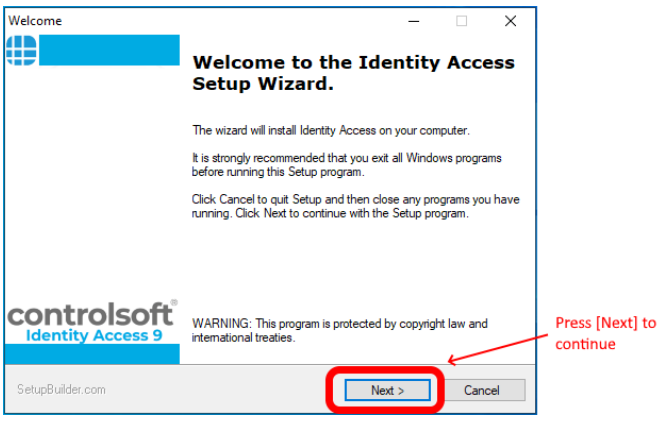
1. Download the Identity Access Software from our website at www.controlsoft.com/login

2. Navigate to your Downloads folder, and double click **Install_IdentityAccess.exe**

3. During installation, if prompted to restart the installation click **Yes**.



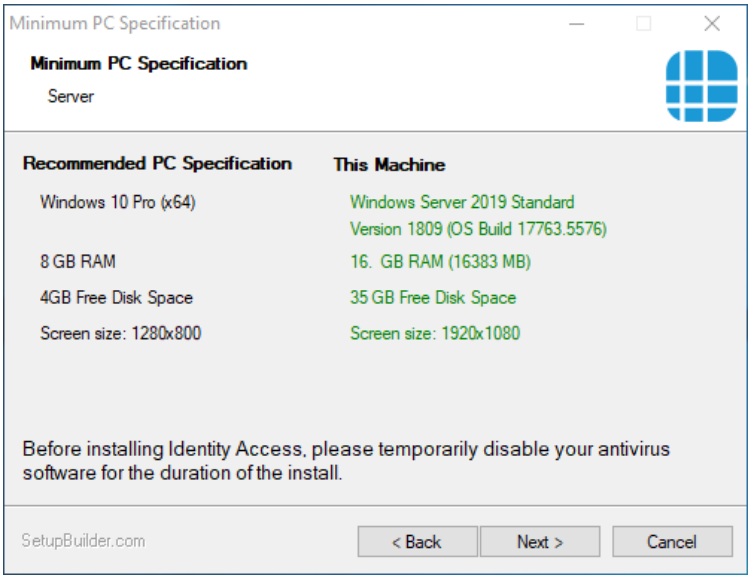
4. Once restarted the installation will restart automatically if you are logged in as an administrator. If you are providing administrator details when prompted, you must restart the installation manually from the Downloads folder.



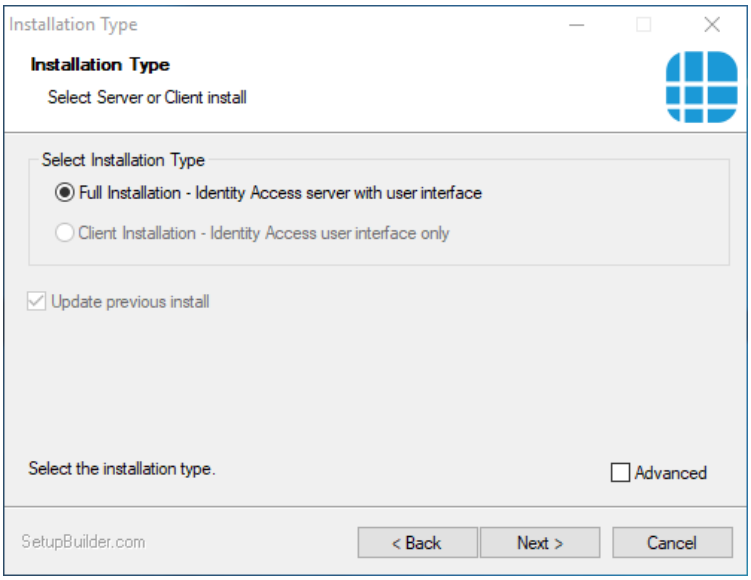
© 2026 Controlsoft Ltd

5. Continue with the installation, pressing next until you get to this screen.

NOTE: If your system does not meet our minimum specification, the non-compliant parameter will be highlighted in red in the screen below. You can continue with the installation but we are drawing to your attention that this PC is below the required specification.

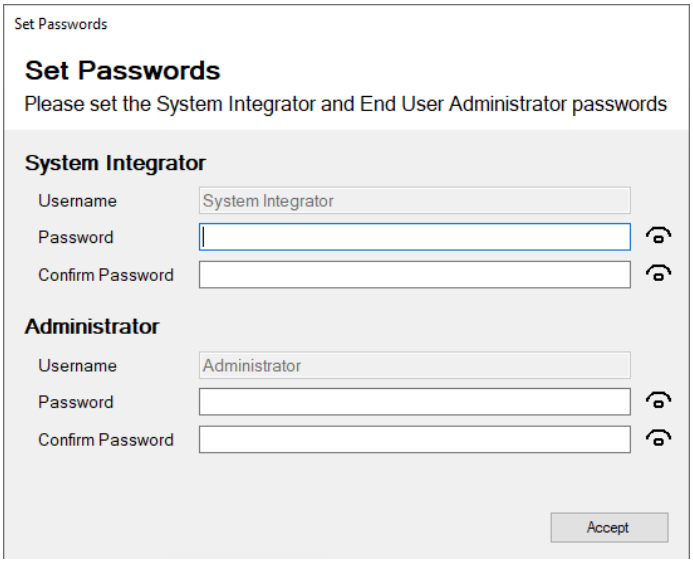


6. When prompted, select **Full Installation - Identity Access server with User Interface** and click **[Next]**



© 2026 Controlsoft Ltd

7. At the end of the installation you will be asked to fill in your System Integrator and your Administrator password.



Once the installation is finished, restart the PC and re-enable any previously disabled anti-virus.

4.3 Step 3. (Optional) Licensing Identity Access

If you requires a Professional or Enterprise license, please click here. Otherwise go to Step 4.

4.4 Step 4. Launching 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 take longer to start. Wait 2 minutes and Identity Access will connect.

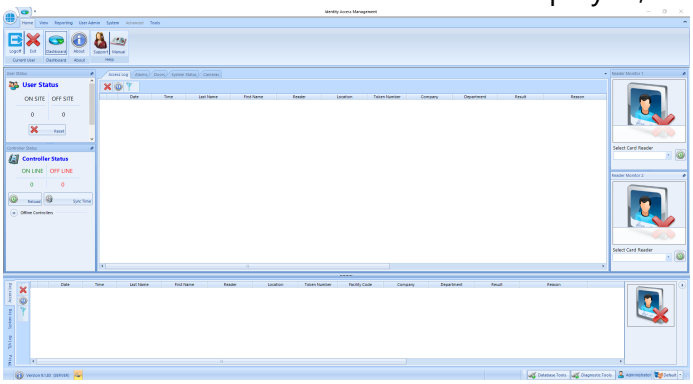


© 2026 Controlsoft Ltd

2. Select **System Integrator** and type in your password.



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



Further details can be found in the "5.3 The Dashboard" section of the Identity Access Software Guide 39

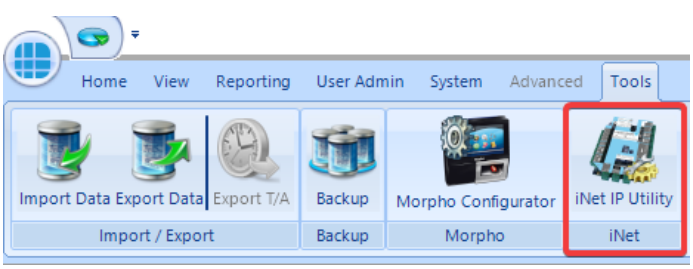
4.5 Step 5. Configure IP Controller(s)

For the PC and iNet Controller to communicate over a TCP/IP network, the PC and each iNet must be configured to a static IP Address on the same network range.

Click here if you are plugging an iNet controller directly to the PC.

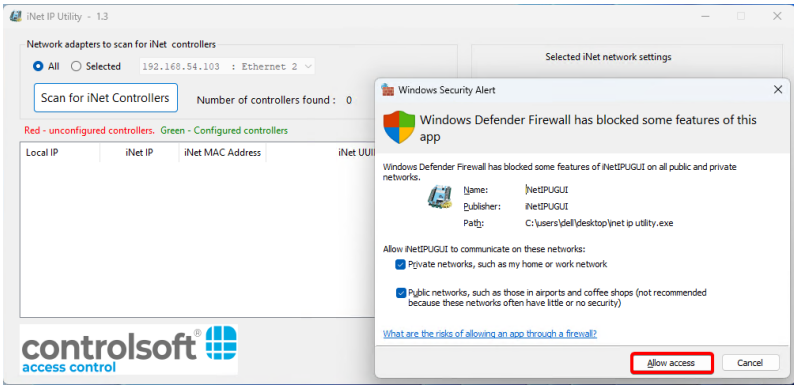
NOTE: If you are unsure what IP Address, Subnet Mask and Gateway the iNets should use, speak to IT.

1. Go to **Tools** > **iNet IP Utility**

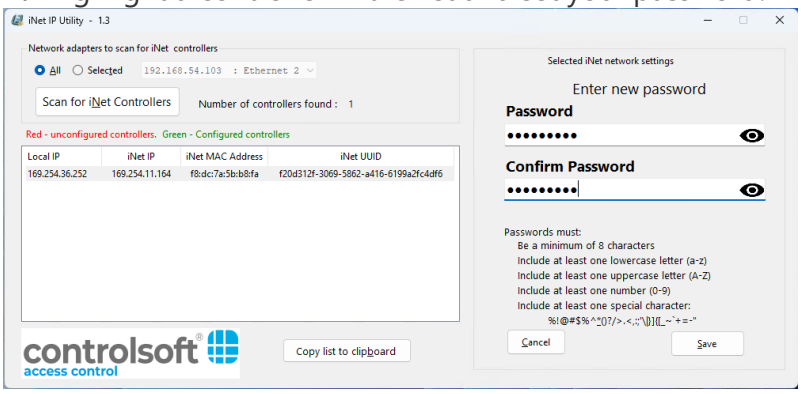


2. Press **Scan for iNet Controllers**.
3. On the "Windows Defender Firewall" notice, tick both **Private** and **Public networks** and press **Allow Access**. Then press **Scan for iNet Controllers** again.

© 2026 Controlsoft Ltd

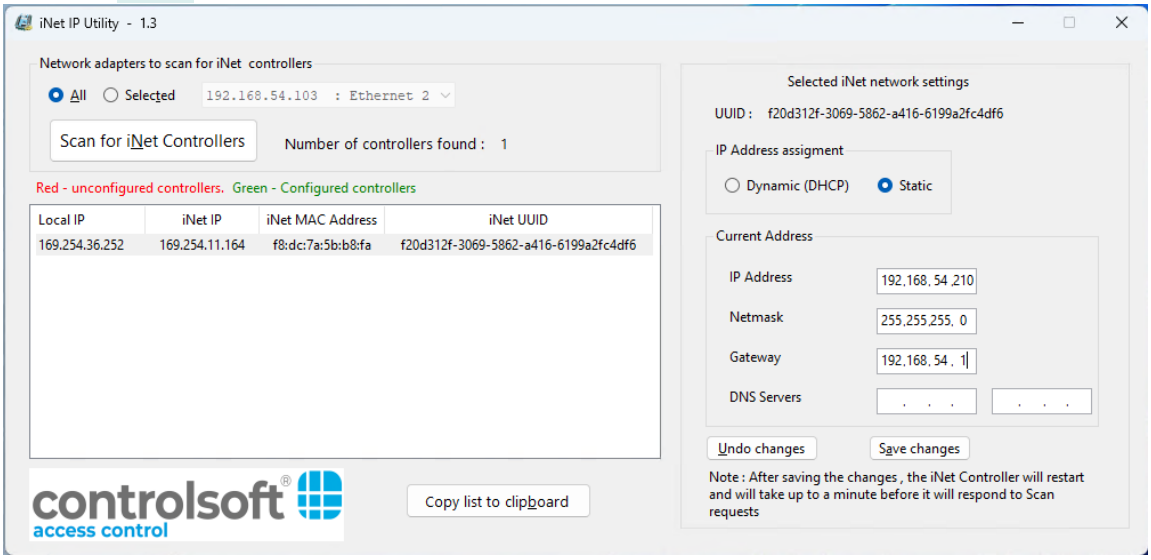


4. Highlight a controller in the list and set your password. Then click Save.



NOTE: If a message is displayed on screen saying "The iNet did not respond to the message", then the password was not inserted quick enough. Reselect the controller and type the password again.

5. Press **Static**, and fill in the Static IP Address for this controller.



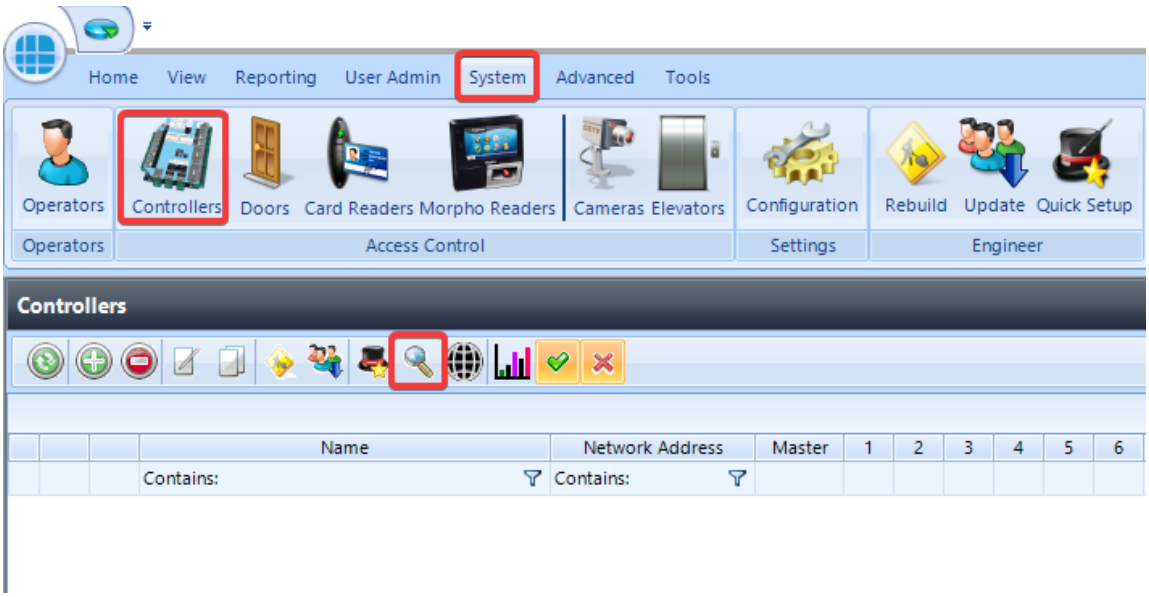
6. Press **Save Changes** and the iNet will set the IP address and automatically restart.
7. Close the iNet IP Utility.

Click Here: For further details on how to use the iNet IP Utility or how to configure it to work on Windows Server Operating systems

© 2026 Controlsoft Ltd

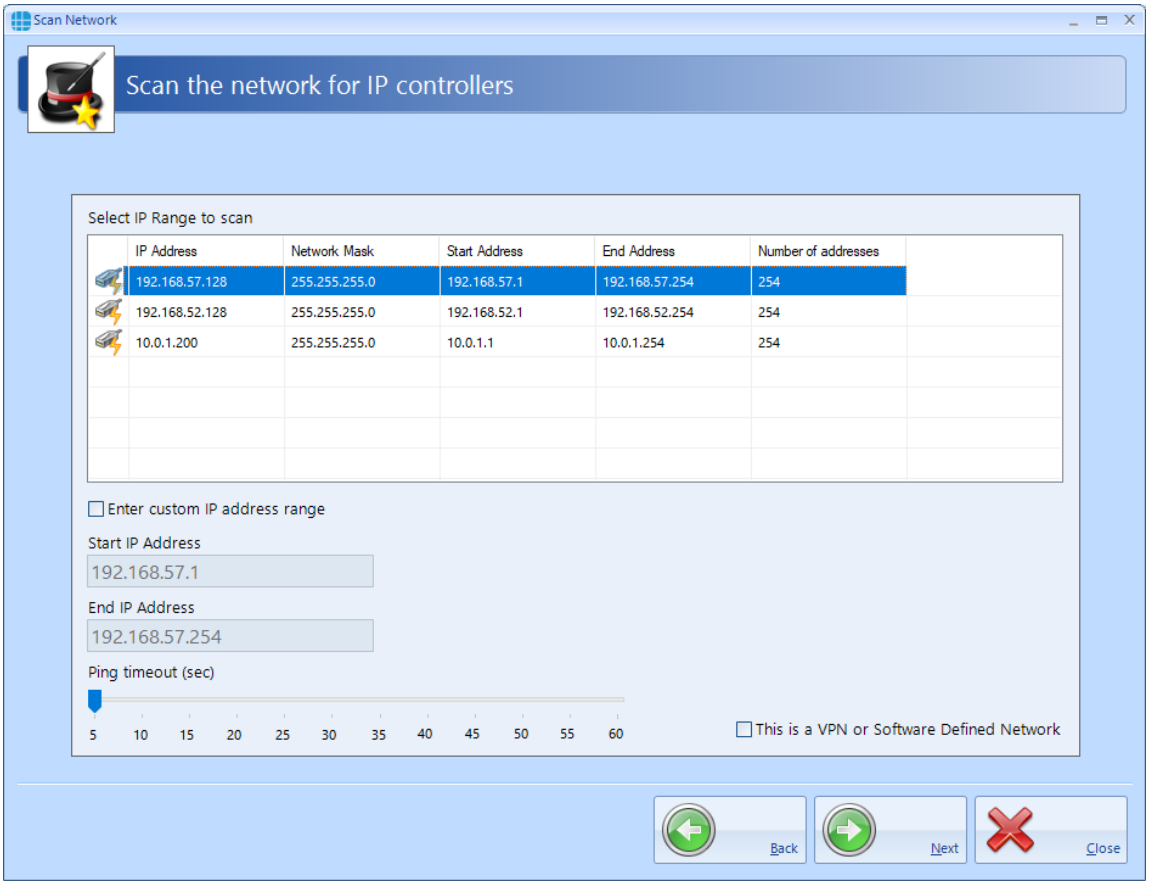
4.6 Step 6. Add IP Controller(s)

1. Within Identity Access, select **System**, then **Controllers** in the ribbon bar.



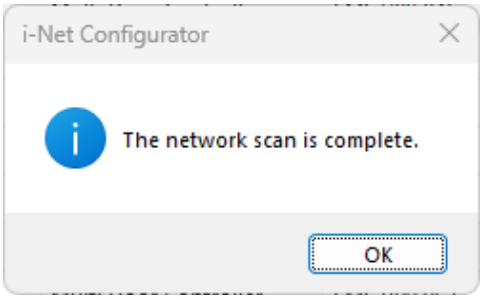
2. Click on the Scan button  then click **[Next].**

3. If there are multiple network ranges, highlight the network range which has been programmed into the iNet Controller(s) and click **[Next]**

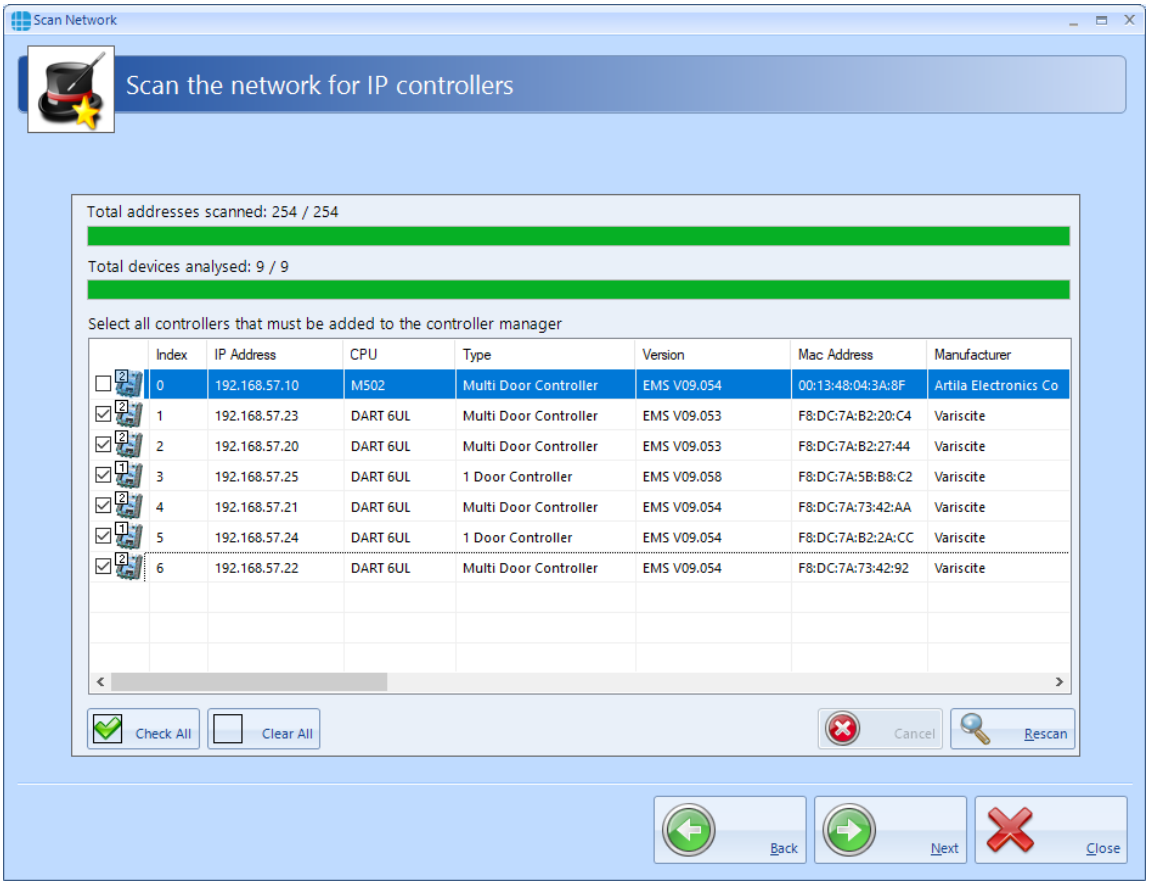


4. Click **[OK]**

© 2026 Controlsoft Ltd



5. Unselect any controller/s that you do not require by unchecking the tick box, then select **[Next]**, followed by **[Finished]**.



For information on manually creating a controller see the "7. System > Controllers" section of the Identity Access Software Guide. 61

4.7 Step 7. Add Downstream RS-485 Controllers

NOTE: This section is only applicable if **Downstream RS-485 controller** are being used. Otherwise, click here to move to Step 8. 26

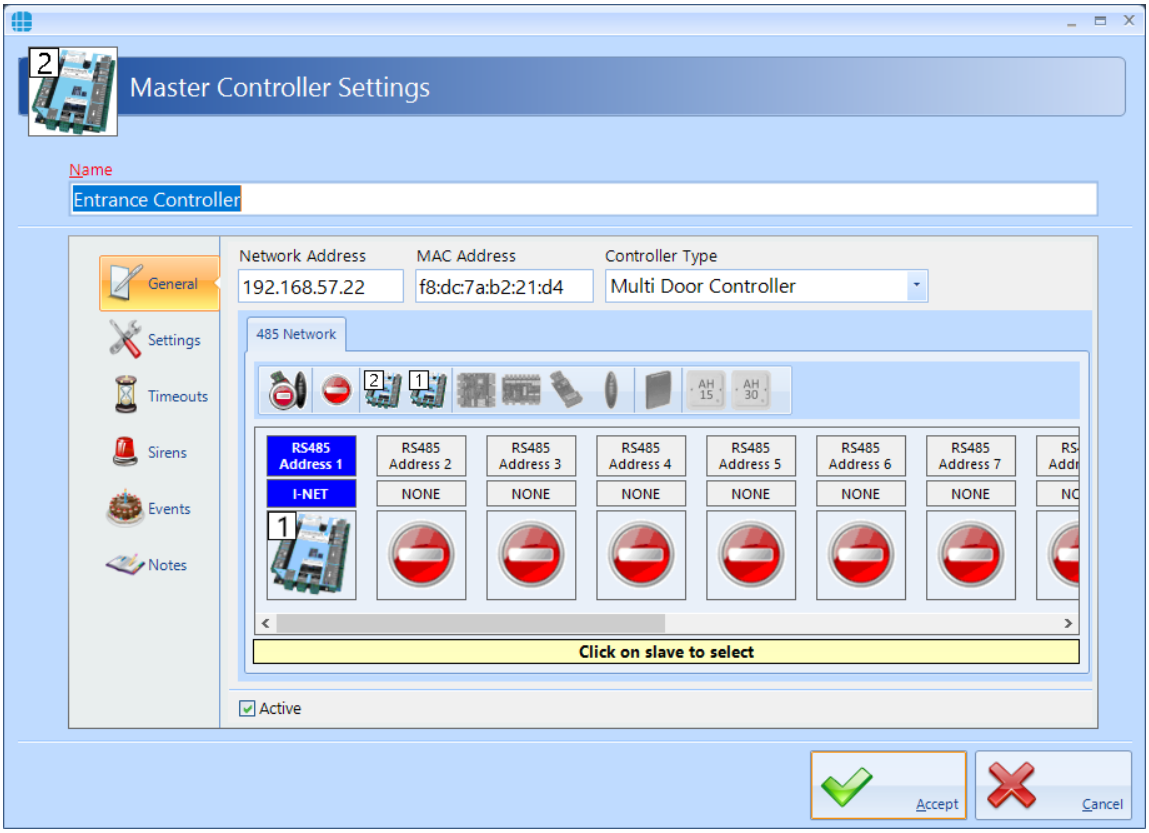
1. Double Click on the IP Controller.
2. Click the RS-485 address to be added and select the type of device to add to the RS-485 line:

 Add a 2 Door iNet to the RS-485 bus

© 2026 Controlsoft Ltd

Add a 1 Door iNet to the RS-485 bus

For other devices see the "7. System > Controllers" section of the Identity Access Software Guide 61



3. Click **[Accept]** to save the new Downstream Controllers.

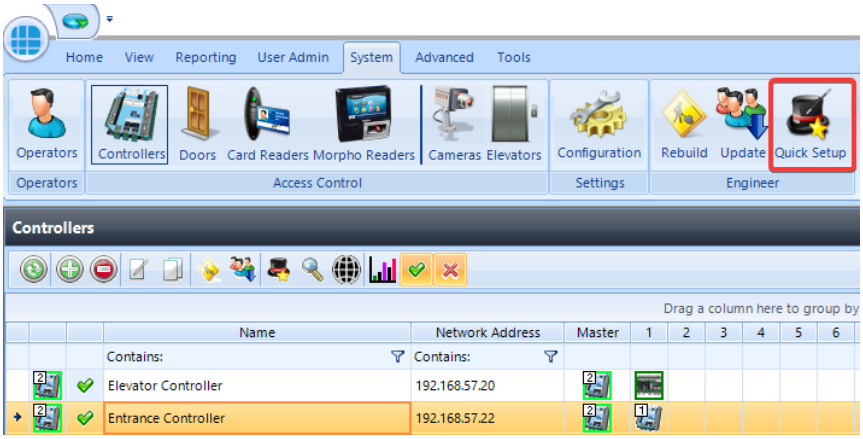
For more information on Controller Settings, see Chapter 5.1 of the Identity Access Software Guide.

© 2026 Controlsoft Ltd

4.8 Step 8. Add Doors / Readers using Door Wizard

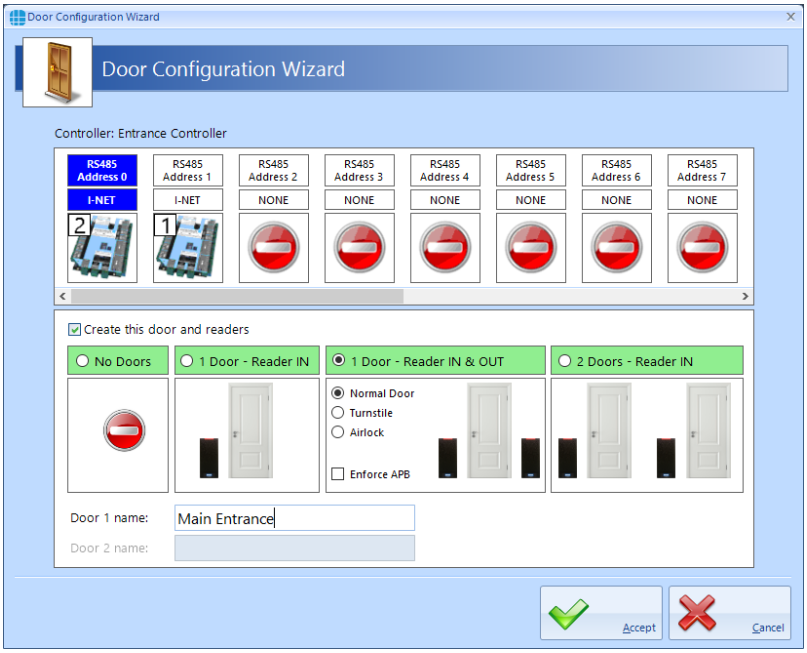
Note: The Door Wizard is designed for easy setup if using Wiegand readers, click the following links for setting up Aperio Wireless Devices or OSDP Readers

1. Highlight the IP controller and select the **Quick Setup** button.



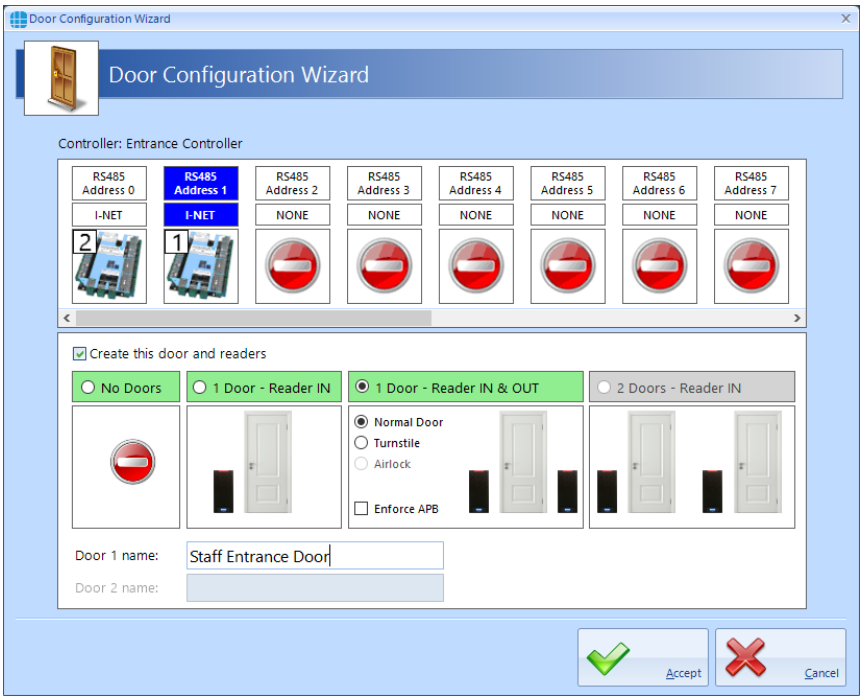
2. Select either **1 door with an IN reader**, **1 door with IN and OUT readers**, or **2 doors with IN readers** depending on your installation.

3. Enter the door name(s).

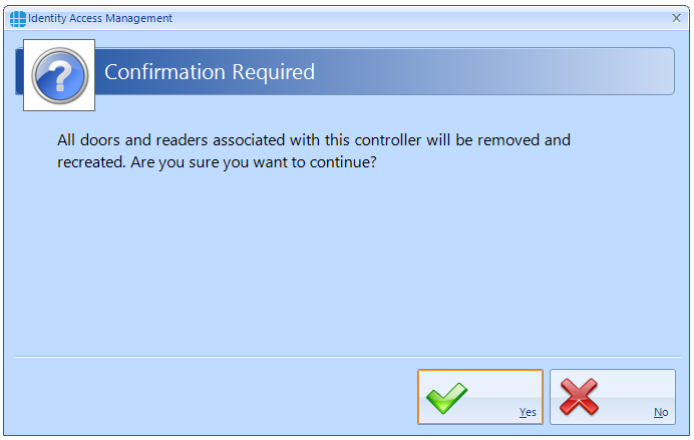


© 2026 Controlsoft Ltd

4. If you have any Downstream RS-485 controller: highlight the RS-485 address and follow the same setup procedure.



5. Click **[Accept]** and click **[Yes]** to the following message.



For information on changing Door Settings such as unlock times, see the "8. System > Doors" section of the Identity Access Software Guide. 78

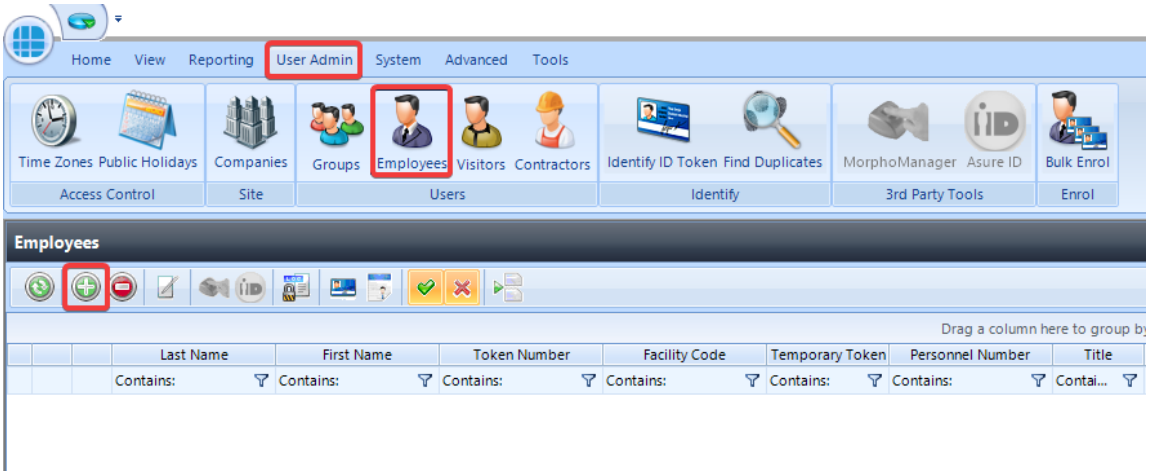
For changing Reader Settings, see the "9. System>Card Readers" section of the Identity Access Software Guide. 90

4.9 Step 9. Add Employee

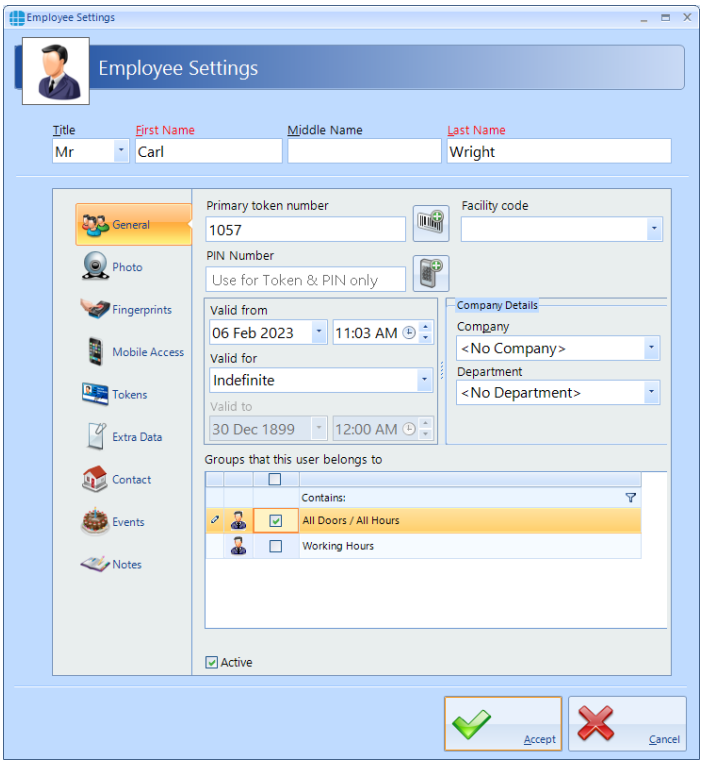
NOTE: Programming screens for Employees, Visitors and Contractors are the same.

© 2026 Controlsoft Ltd

1. Select **User Admin**, then **Employees** from the ribbon bar
2. Select 



3. Enter the **First Name** and **Last Name** of the user.
4. Enter **Primary Token Number** . This may be written on the card/keyfob or read via an USB Desktop reader.
5. If using HID cards select the **Facility Code** from the dropdown list. Add New if necessary. For further information on facility codes, see "27. Appendix D - Facility Codes" of the Identity Access Software Guide
6. Select **All Doors/All Hours** under **Groups that this user belongs to**
7. Click **Accept**



© 2026 Controlsoft Ltd

4.10 (Optional) Configure Groups (Access Levels)

Congratulations, you have now finished a basic setup. You can now test your readers with this card.

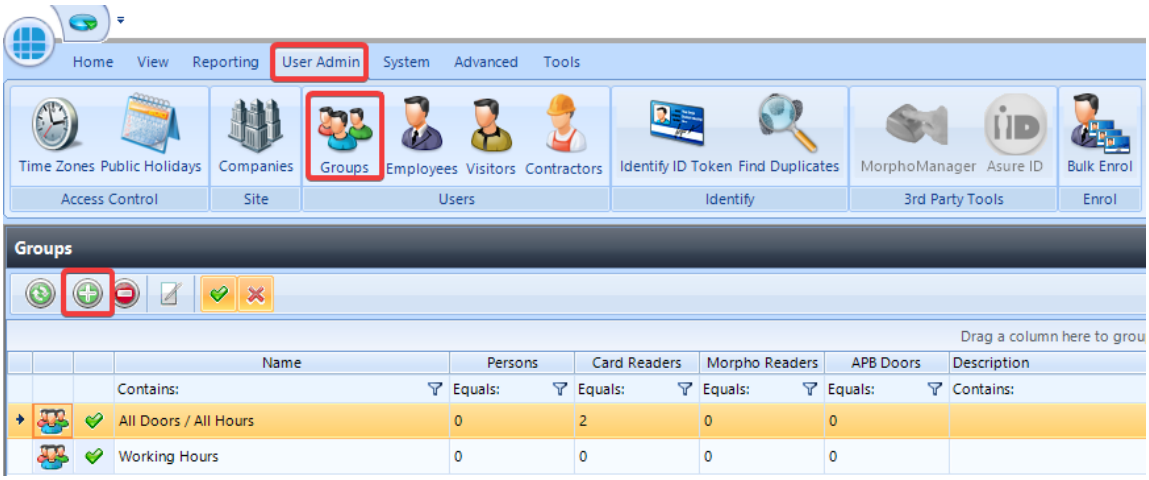
Below are the next steps to follow after a system test.

Groups are used to provided each user with their relevant access levels. It is possible to create multiple Groups. This step is optional, if further Groups are not required, click here to move onto Step 8. Configure Time Zones 113

On installation, 2 default groups are configured:

"All Doors / All Hours" is automatically assigned every door, elevator, anti-passback door and Morpho Reader to make it easier to test on initial setup. This group can be deleted but cannot be edited.

"Working Hours" is not assigned any doors automatically and has a **"Working Hours"** time zone associated to it. By default this group can only gain access from 09:00 to 17:00, however the Time Zone and access permissions to this group can be modified.

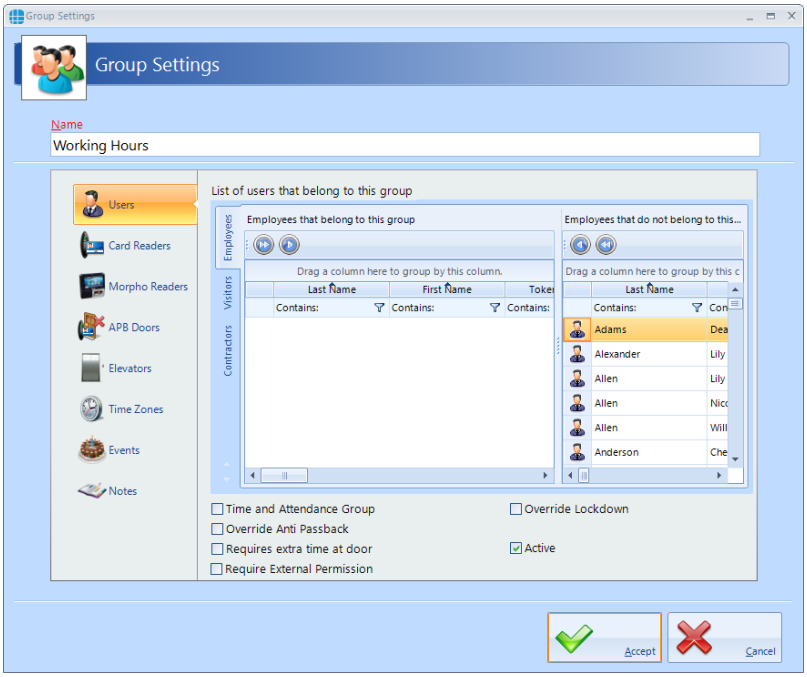


Continued on next page

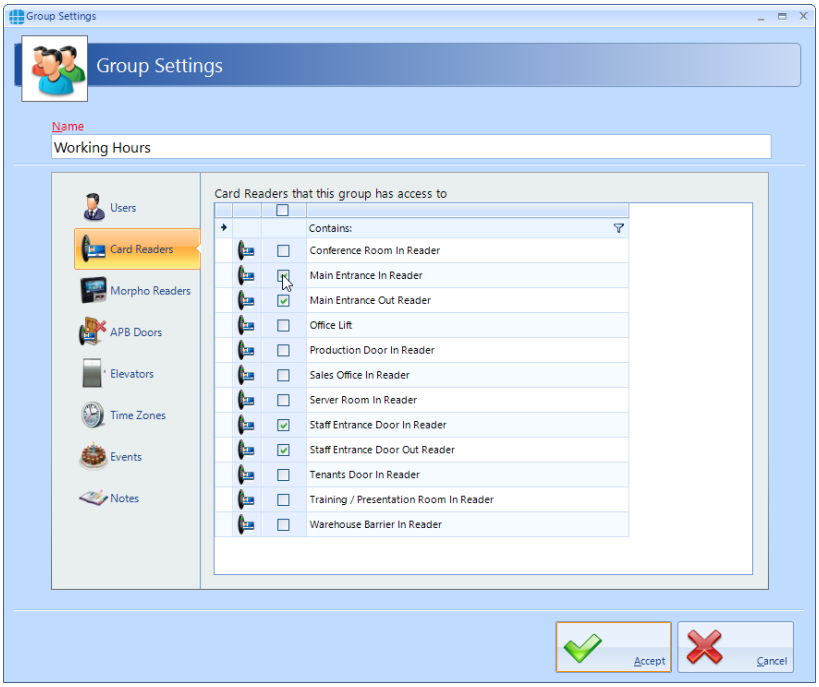
© 2026 Controlsoft Ltd

1. To create a new Group, select the **User Admin** Tab, then select **Groups** from the ribbon bar. Select the **Add** New button .

2. Give the Group a name. The Users tab can be used to assign users into this Group if they are already added to the system.



3. Select **Card Readers** in the side bar, use the tick boxes to assign this group access to specific card readers:



For more information on this please see the "13. User Admin > Groups" Section of the Software Guide. 128

© 2026 Controlsoft Ltd

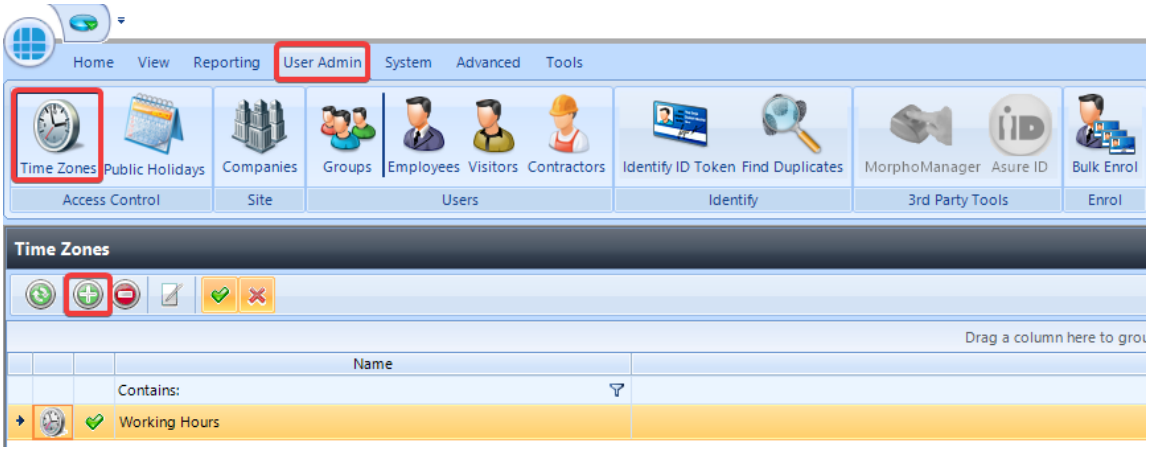
4.11 (Optional) Configure Time Zones (Access Schedules)

This step is optional, if Time Zones are not required, click here to move onto Step 9. Backups. Time Zones can be used in 2 ways:

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

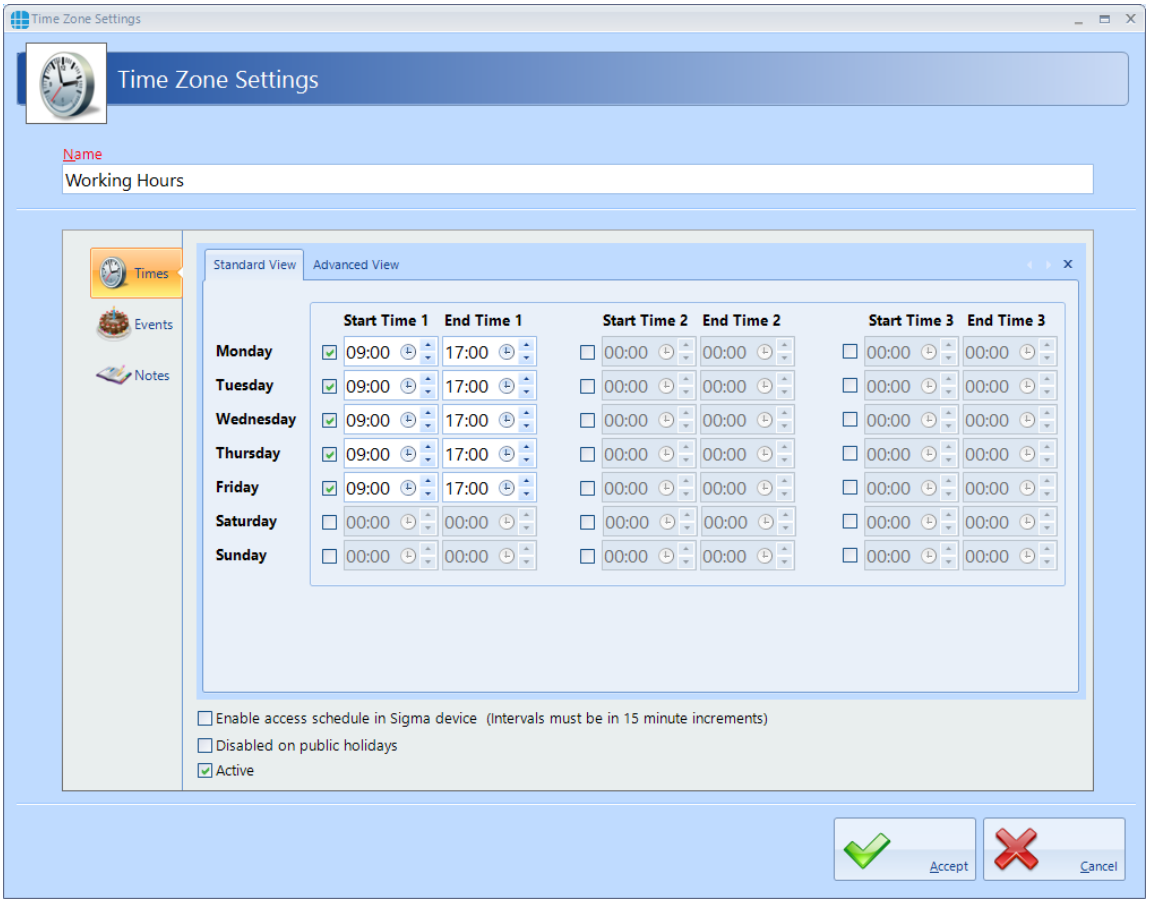
The default **"Working Hours"** time zone is assigned to the Working Hours access group. This can be edited by double clicking.

Alternatively it is possible to add a new time zone by pressing .



© 2026 Controlsoft Ltd

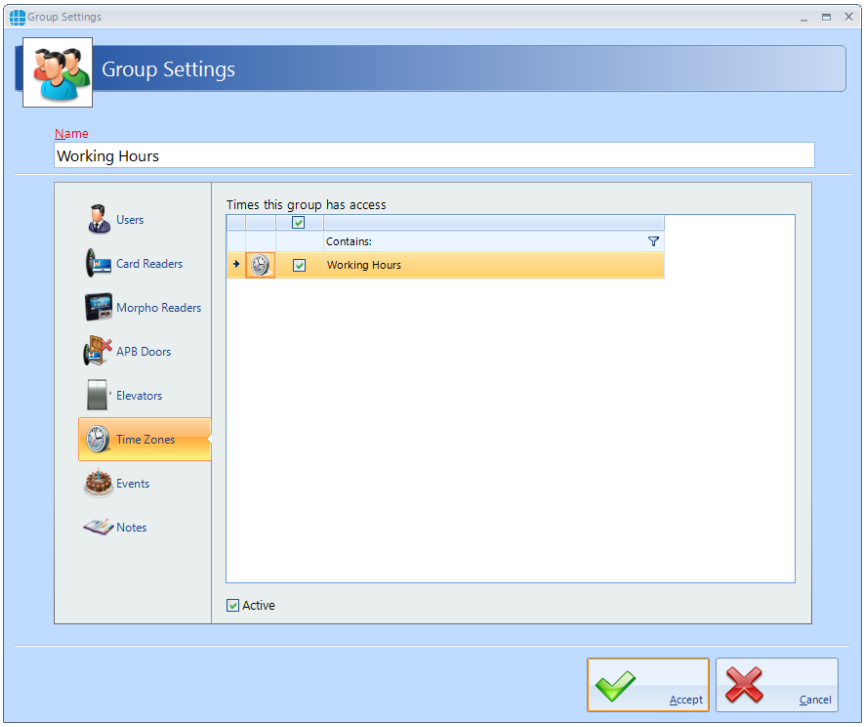
2. Select the Start and End Time for the Time Zone.



Adding a Time Zone to a Group

1. Click on the **User Admin** tab and select **Groups.** Double click the door relevant Group.
2. Select the **Time Zone** tab.
3. Click **Active** and tick the relevant Time Zone to be added to this Group.

© 2026 Controlsoft Ltd



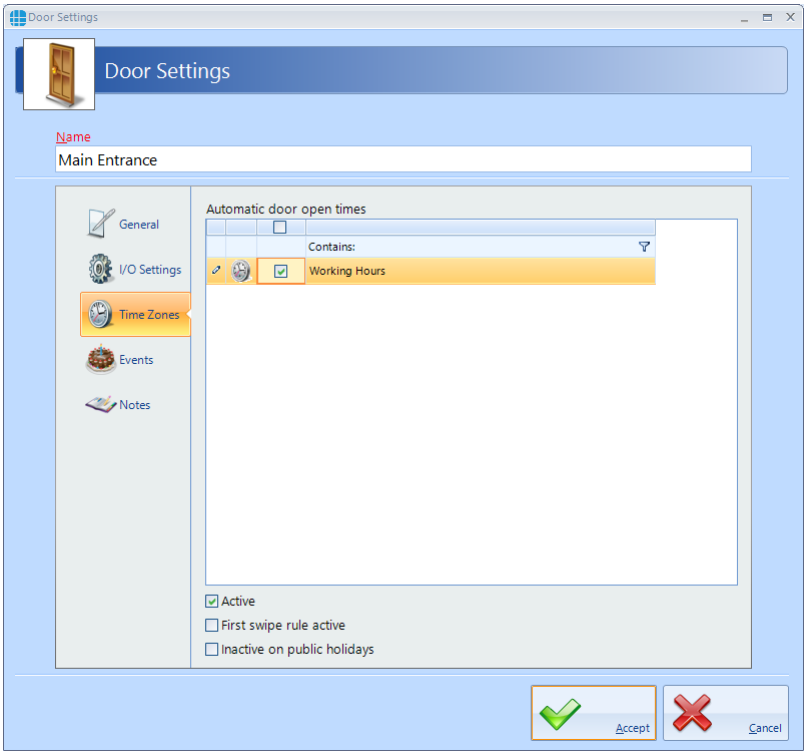
4. Press **Accept**.

NOTE: With Identity Access it is only a requirement to add a Time Zone to a Group if they require restricting. Any group with 24/7 access should not have any Time Zone restrictions applied.

Adding a Time Zone to a Door

1. Click on the **System** tab and select **Doors.** Double click the door relevant door.
2. Select the **Time Zone** tab.
3. Click **Active** and tick the relevant Time Zone to be added to this door.

© 2026 Controlsoft Ltd

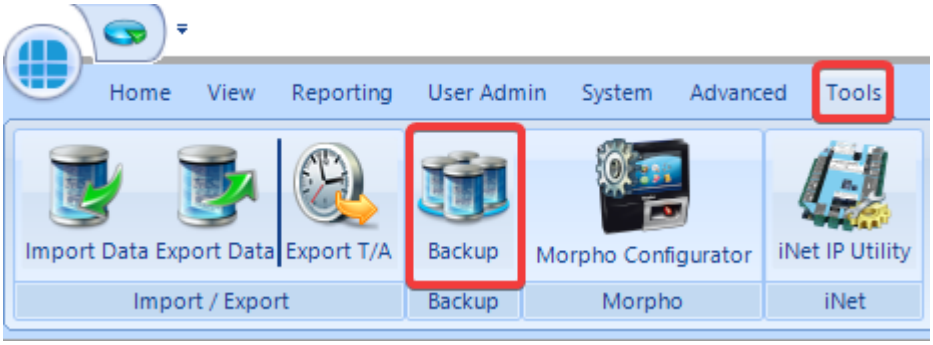


4.12 (Optional) Backups / Installing Identity Access Client

Identity Access is automatically set to backup to "C:\ProgramData\Controlsoft\IdentityAccess\Backup" daily at 13:00. By default it is setup to keep the last 7 days of backups. To adjust these settings, see the "23.14 IA Configuration > Backup" of the Identity Access Software Guide. 271

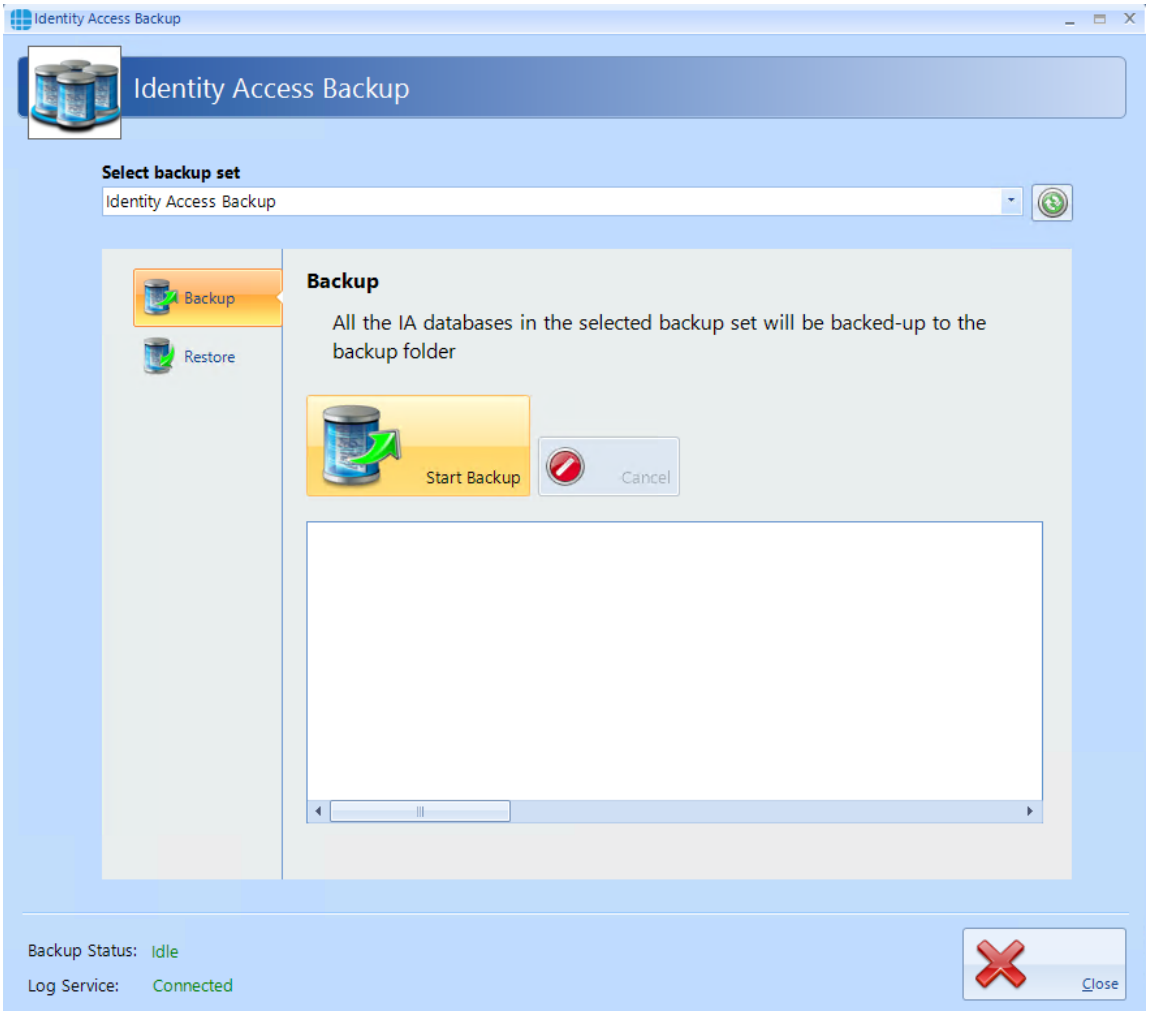
To manually backup the system:

1. Click on the **Tools** tab and select **Backup**.

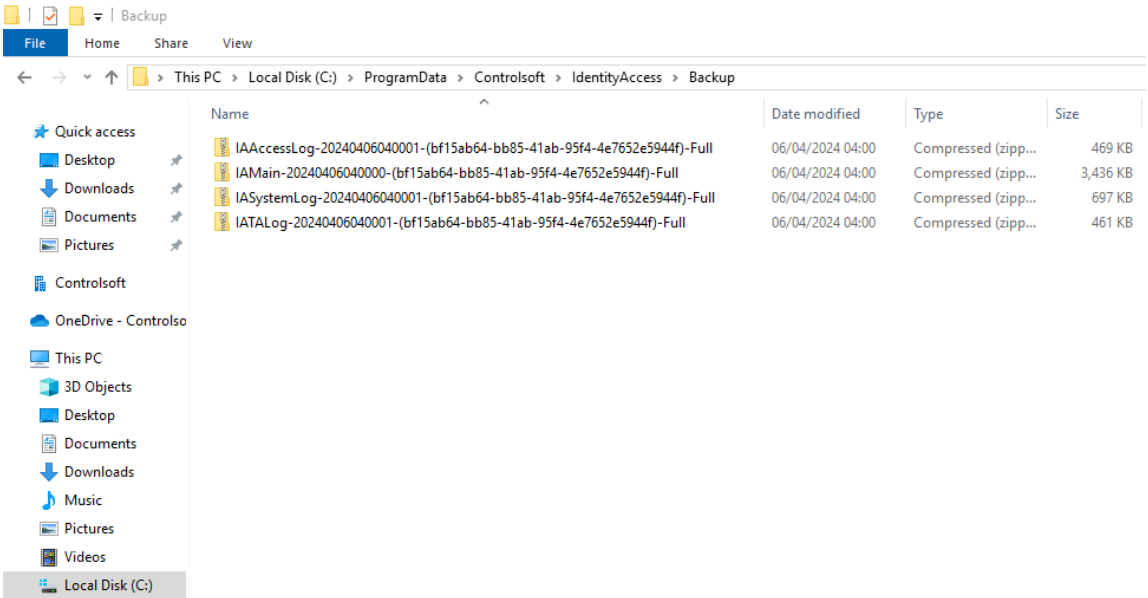


2. Select "Backup".

© 2026 Controlsoft Ltd



3. Once the Backup is completed the files can be obtained from "C:\ProgramData\Controlsoft\IdentityAccess\Backup".



© 2026 Controlsoft Ltd

Installing Identity Access Client

For further information or the setup of other functions of Identity Access, please see the Identity Access Software Guide

Identity Access can be run from a second PC using the Identity Access Client software.

Click here, for information on how to configure the Identity Access Server for a Client connection and installing the Identity Access Client.

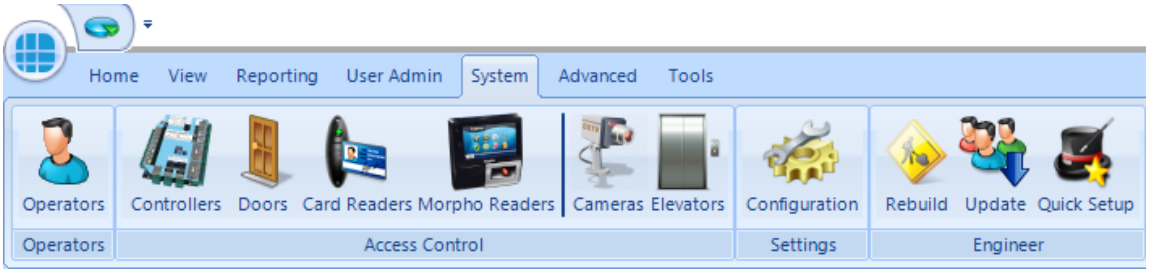
© 2026 Controlsoft Ltd

Identity Access Software Overview

5 Identity Access Software Overview

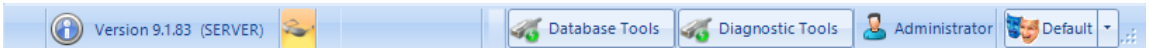
5.1 Identity Access Header and Footer

At the top of the screen, the header provides the Menu bar and the Ribbon bar:

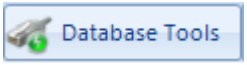


 Use this icon to quickly return to the Dashboard from anywhere in the software.

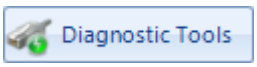
At the bottom of the screen is the footer bar:



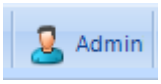
The various icons represent the following conditions:



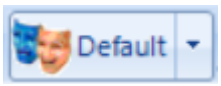
indicates the status of the connection between the Identity Access software and the Log Service. Clicking the button will bring up the Database Tools. For more information see Engineer Tools and Services 234



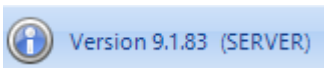
indicates the status of the connection between the Identity Access software and the Download Service. Clicking the button will bring up the Diagnostic Tools. For more information see Engineer Tools and Services 234



indicates which Operator is currently logged into the software



indicates which colour theme is selected.



The software version number and whether the install is Server or Client software is displayed in the bottom left hand corner of the screen

 shows / hides the Events Viewer window

© 2026 Controlsoft Ltd

5.2 The Option Wheel

The Option Wheel is accessible at a variety of screens throughout the Identity Access software. When options are available, right click to display the Option Wheel



Position the mouse for the required option and click to select.

NOTE: The Option Wheel is context sensitive, so may offer different options to those shown above, depending on where the Option Wheel is invoked.

5.3 The Dashboard

The **Dashboard** displays a useful summary of the status of the system. Each section is dynamically updated, without the need to press a refresh button or similar.

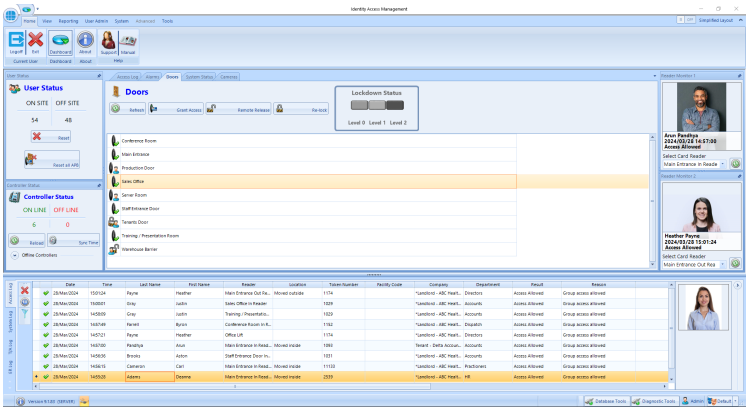
To access the Dashboard, select the **Home** tab, then select **Dashboard** (or click the dashboard icon  in the top left hand corner of the screen from anywhere in the software):

User Status: Indicates the number of users on site and off site. This section is updated as readers programmed with Location as "Inside to Outside" or "Outside to Inside" are operated (see Card Reader General) 91

Controller Status: Indicates the number of controllers online and offline. This is updated depending on whether the Download Service can communicate with each controller

Offline Controllers: Click this option to see which controllers (if any) are offline.

© 2026 Controlsoft Ltd



The central section of the dashboard is the main viewer area, where one of four windows can be viewed:

Access Log: Displays a live view access control events, as they happen. Whenever the software is closed, this viewer will be cleared. Where the event shows a green 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 an access denied event

Alarms: Displays system alarms (e.g. Door Forced Open, Door Forced, BreakGlass Activated or Fire Alarms). When an alarm condition has been investigated, it needs to be accepted by highlighting the alarm and clicking the **[Accept]** button. It is possible to configure the system so selected alarms require the operator to enter text before the alarm can be accepted. Once accepted, alarms can be removed from the list by highlighting the relevant alarm/s and click the **[Clear]** button. If the alarm condition is still active, the alarm will reappear in the Alarm Tab.

NOTE: To reduce clutter on the Alarms screen, if an alarm has not been accepted, any subsequent alarms from the same source will overwrite the original entry. Every activation of these alarms are stored in the System Log for future analysis.

Doors: Allows doors to be controlled by the Operator. To manually grant someone access through a door, highlight the relevant door in the list and click the **[Grant Access]** button. The door will then unlock for the predefined Unlock Time or Extended Unlock Time (whichever is the longer), then relock automatically. To unlock the door for a longer period, click the **[Remote Release]** button. To subsequently override the release command, simply click the **[Re-lock]** button. Using the 'Ctrl' and 'Shift' keys on the keyboard, it is possible to select multiple doors and release them all in a single command.

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

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

© 2026 Controlsoft Ltd

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

 Door Forced Closed via Operator. This symbol indicates that the door was 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 allows operators to activate "Lockdown". This feature is a security measure which operates as follows:

- Green - Lockdown is OFF
- Amber - Users are denied access at all readers if they are NOT in a group with "Override Lockdown" selected.
- Red - All users are denied access at all readers, Request to Exit buttons do not release doors, if selected (see Controller Settings 65).

To activate Lockdown, click on the Amber or Red block on the screen, or activate the relevant input (see Controller Settings 65). The only way to deactivate Lockdown, is to select the Green block on the screen.

If the Lockdown icons are grey, Lockdown is Disabled

System Status: This screen provides an overview of whether the Log Service and the Download Service are connected, whether Asure ID is licensed and available to use, and whether the HID Mobile Portal (if used) is available.

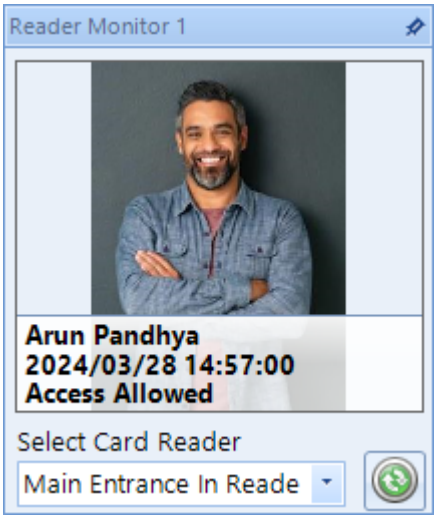
Cameras: This screen allows a single IP camera to be monitored. Choose the required camera from the dropdown list and click the **[Connect]** button.

Floorplan: This tab shows a floorplan of the building with icons to indicate the status of doors, readers, etc.

© 2026 Controlsoft Ltd

To the right of the Dashboard are two **Reader Monitors**.

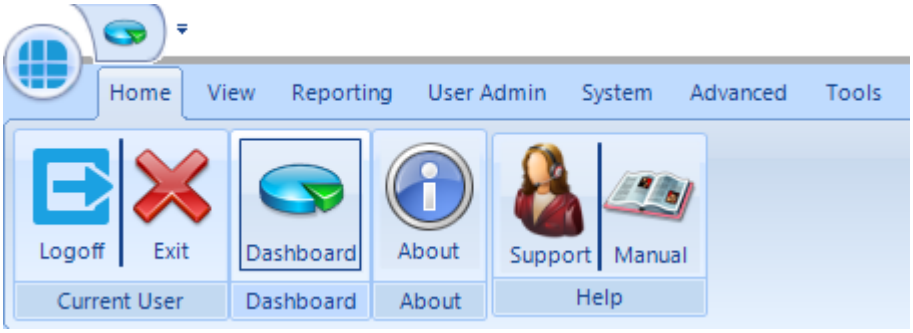
To use the Reader Monitor, select the Card Reader to be monitored. When someone accesses that reader, their photograph will be displayed in the Reader Monitor display alongside their name and date & time of access:



NOTE: It is possible to 'undock' a tab such as the Floorplan, and resize it to get a larger view on the screen. Simply click on the tab and drag it out of position, then resize the windows as required. IA can then be minimised, leaving the desired tab visible.
Before closing Identity Access, always 'redock' the window by right clicking and selecting "Tabbed Document".

5.4 Identity Access Home Tab

The **Home** tab contains 4 options:



Current User: Allows the current Operator to **Logoff** (log out and restart the program for the next Operator to log in) or **Exit** (log out and close the program)

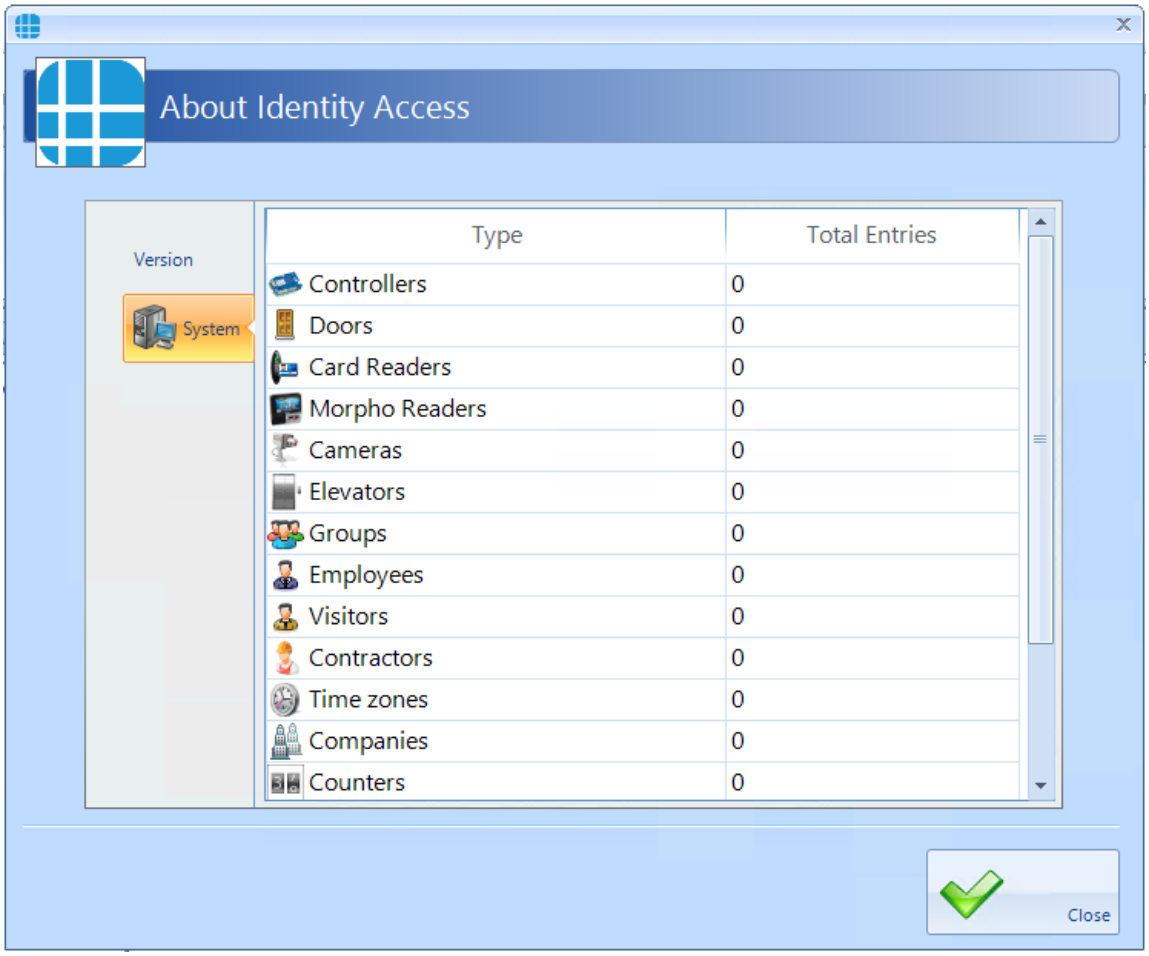
Dashboard: displays the system Dashboard (See The Dashboard) 39

© 2026 Controlsoft Ltd

About: This screen shows information about the software, such as the licence applied, version number and installation date.

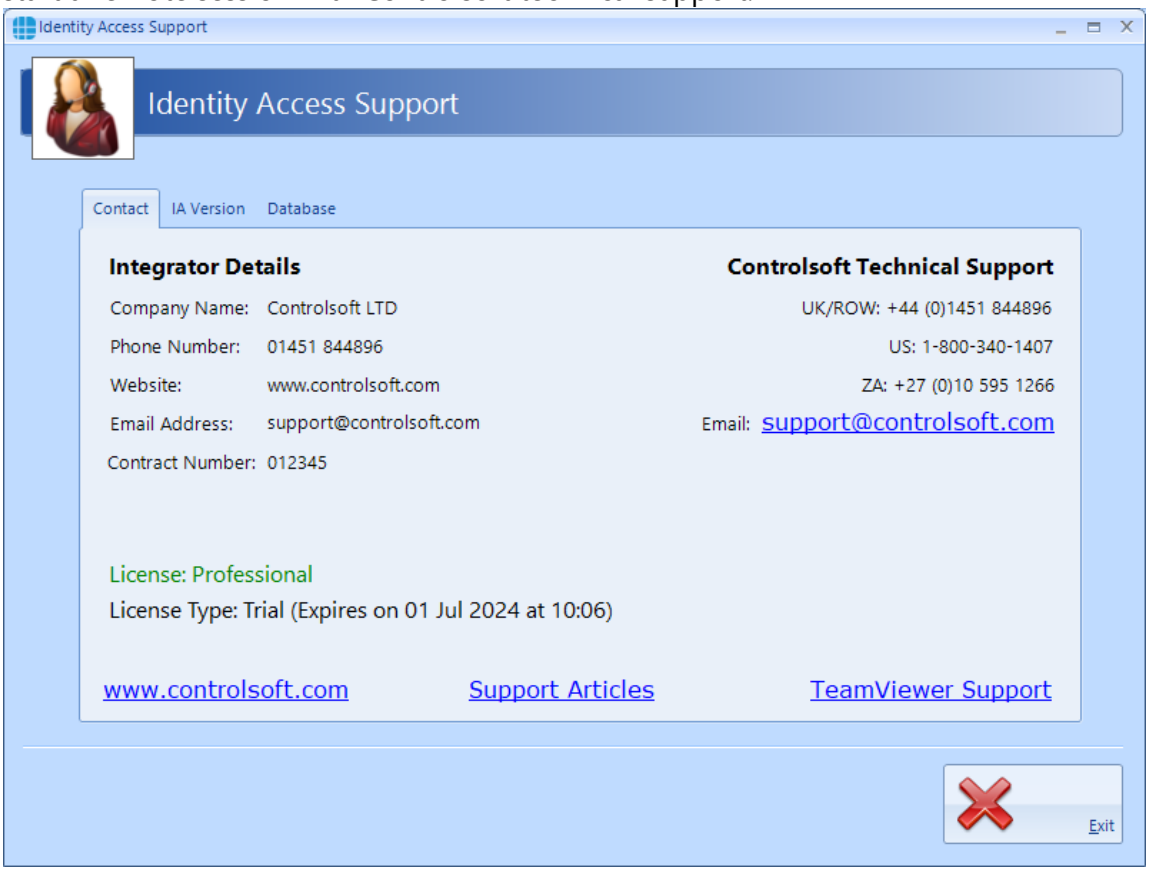


Select the **[System]** tab to view an overview of how many controllers, doors, readers etc are on the system:



© 2026 Controlsoft Ltd

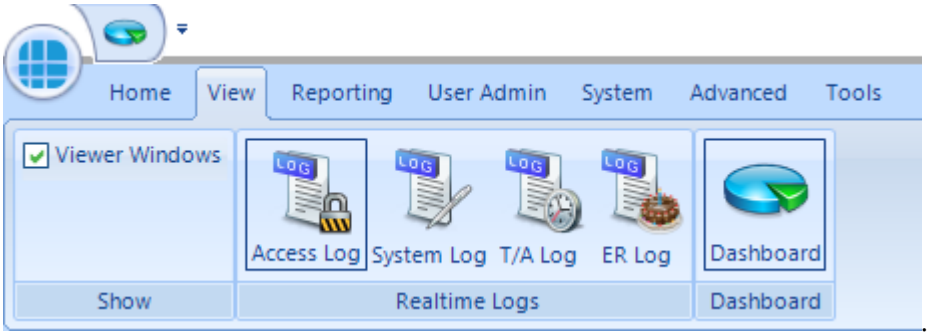
Support: This shows details of the installation including the Integrators details, version data, database statistics. It is also possible to view our extended **[Support Articles]** including Knowledge base and Application. **[Teamviewer Support]** can be used to start a remote session with Controlsoft technical support.



Manual: This option will open the Identity Access Software Guide.

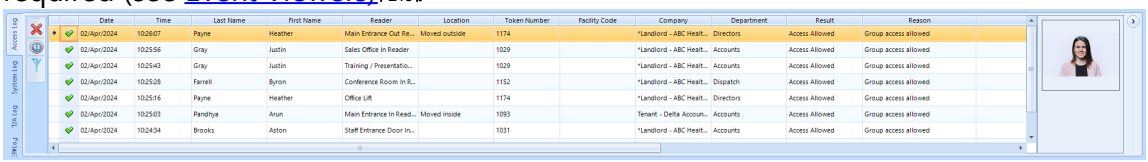
5.5 Identity Access ViewTab

The **View** tab contains 4 buttons for viewing logs and the dashboard:



© 2026 Controlsoft Ltd

Show: When the **Viewer Windows** option is selected, the lower half of the display shows Access Control events, System events, Time & Attendance events or ER Logs as required (see Event Viewers) 218:



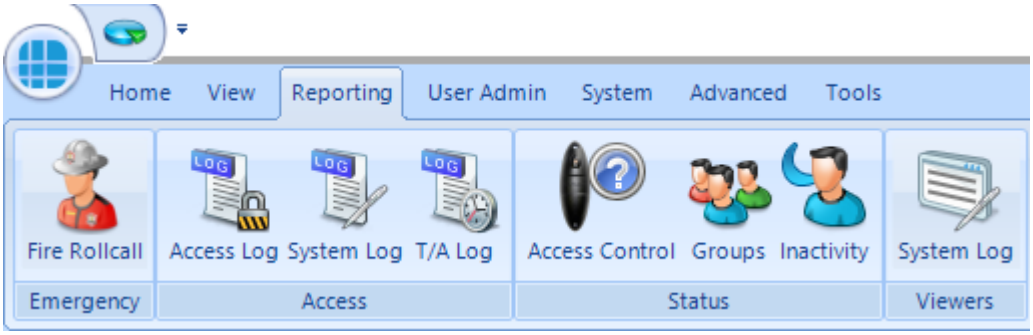
Realtime Logs: Allows the Operator to view live **Access** events, **System** events, **T/A** events or ER Logs in the Viewer window. ***NOTE: These buttons do the same as the side tabs in the viewer window.***

Dashboard: Allows the Operator to view a summary status of the system (see The Dashboard) 39

NOTE: The Dashboard can also be accessed at any time by clicking the Dashboard quick access icon  ***in the top left hand corner of the screen.***

5.6 Identity Access Reporting Tab

The **Reporting** tab is used to generate a variety of reports:



Emergency: In the event of a Fire Alarm, this icon will generate a fire roll call report, showing users who are on site. This report can be triggered from the Server or a Client machine. In addition, the server can be configured to automatically generate a Fire Roll call report when a fire alarm has been activated (see Server Configuration - Download Server 277). ***NOTE: This facility is not available in Identity Access unless a Professional or an Enterprise Features Licence is applied.***

Access: Allows the Operator to run and view reports based on **Access** events, **System** events or **T/A** events from the database.

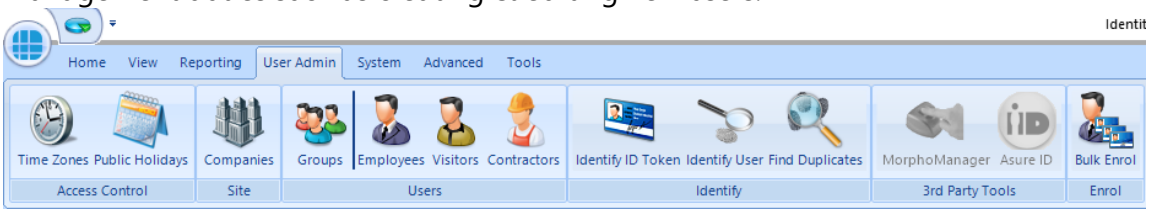
Status: Allows the Operator to run an **Access Control** report (which users have access to which readers), a **Groups** report (which users and readers are allocated to a group) or an **Inactivity** report (users who have not used their tokens for a defined period).

Viewers: Allows the Operator to view events in the System log

© 2026 Controlsoft Ltd

5.7 Identity Access User Admin Tab

The **User Admin** tab contains a number of buttons required for day to day management duties such as creating & editing new users:



Access Control: Allows **Time Zones** (times when users are allowed through defined doors) and **Public Holidays** (days when time zones are not active) to be created or edited.

Site: Allows **Companies** and Departments to be created & edited which help to create meaningful reports which filter out irrelevant data.

Users: Allows **Groups**, **Employees**, **Visitors** and **Contractors** to be created & edited.

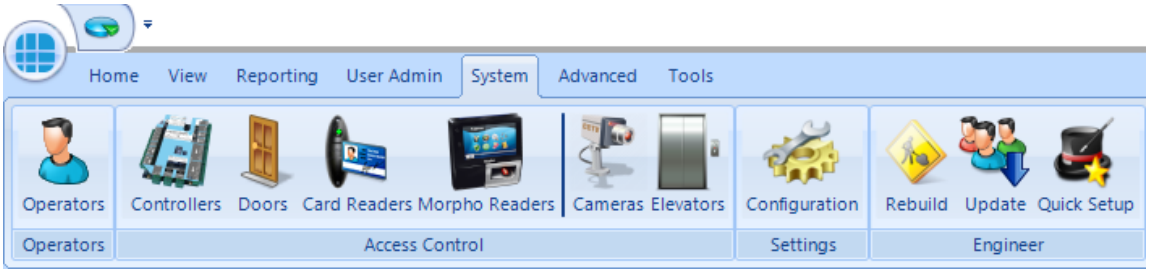
Identify: **Identify ID Token** will show who any given token belongs to, **Identify User** will display the name stored against a given fingerprint and **Find Duplicates** will search the fingerprint database looking for duplicate entries.

3rd Party Tools: Options used to run the **MorphoManager** software and **Asure ID** (HID badge printing software).

Enrol: **Bulk Enrol** provides a simple way to enrol multiple users. For more infomation see User Admin > Bulk Enrolment 172

5.8 Identity Access System Tab

The **System** tab contains buttons required to commission the Access Control system hardware:



Operators: Used to define who can log into the Identity Access software, and who has access to defined features within the software

Access Control: Used to commission the **Controllers**, **Doors**, **Card Readers**, **Morpho Readers, Cameras** and **Elevators** installed on site.

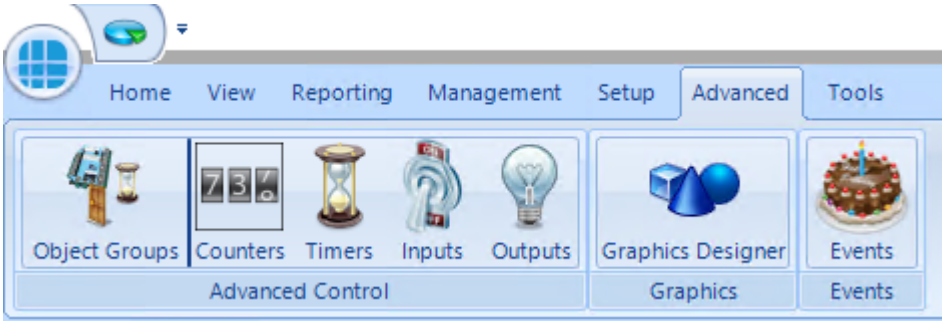
© 2026 Controlsoft Ltd

Settings: The **Configuration** option is used to launch the Identity Access Configuration utility. For further information on the IA Configuration utility, please refer to Identity Access Configuration 245

NOTE: The System tab is always accessible to Operators with Administrator rights. Other Operators will only have access to this menu if enabled in the Operator Permissions.

5.9 Identity Access Advanced Tab

The Advanced tab will only be enabled if an Enterprise Features licence is installed.



Object Groups allow various objects (Controllers, Doors, Card Readers etc) to be grouped together to allow a single command to be sent to multiple devices. By grouping objects, it is possible to simultaneously change the status of every object in the group.

Counters can be used to count the number of times an event occurs. The counter can be incremented, decremented or reset, and it is also possible to check whether the counter is less than, equal to, or greater than one of 3 programmable set points.

Timers can be used to introduce time delays in events and actions. For example: if an input activates, wait 10 seconds then activate an output.

Inputs can be defined for use with the Advanced functions.

Outputs can be defined for use with the Advanced functions.

The **Graphic Designer** allows a floorplan of the site to be imported, and objects superimposed onto the image. Objects can be IA Objects such as doors, readers or controllers or Custom Objects such as squares, circles, images or text boxes.

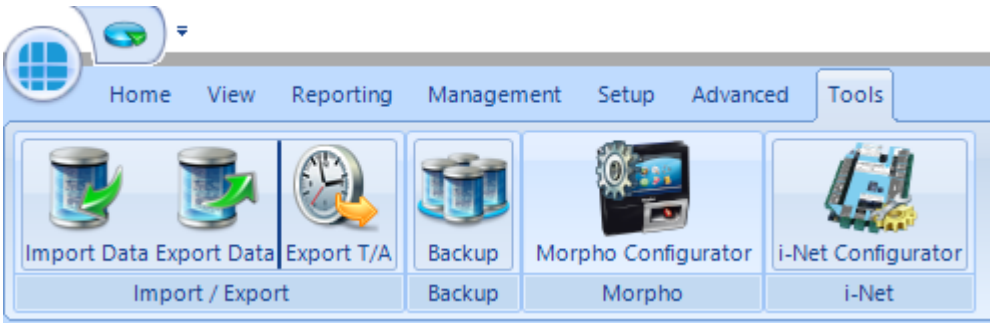
Events and Actions allows the system to react to predefined activity such as triggering a specific output when a specific input activates.

For further information on the Advanced features, see The Advanced Tab 175

© 2026 Controlsoft Ltd

5.10 Identity Access Tools Tab

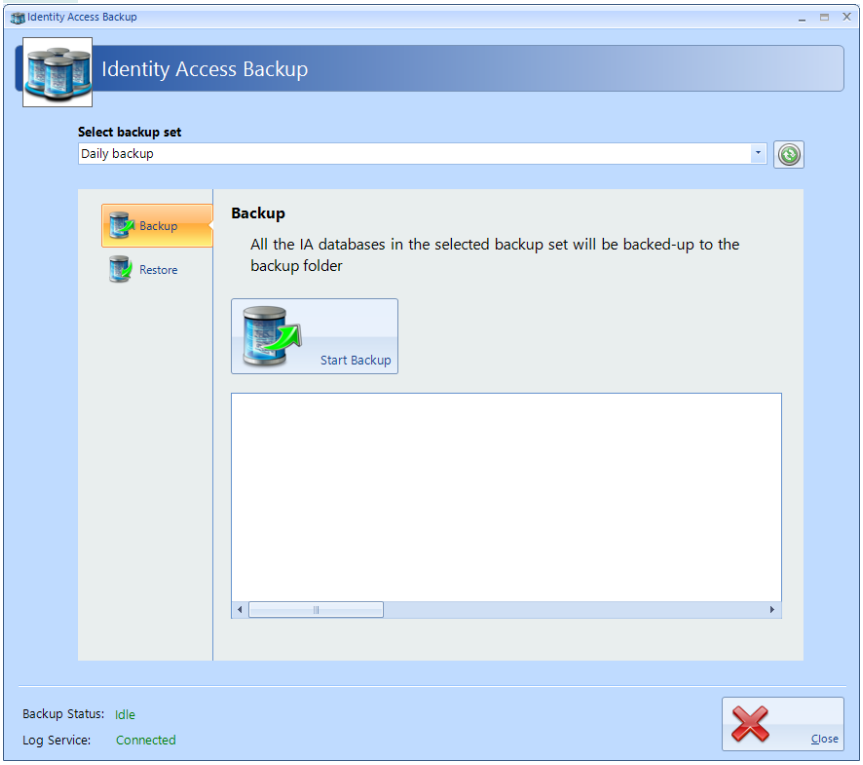
The **Tools** tab is used for importing or exporting user data



Import / Export: Used to **Import Data** and **Export Data** relating to the user database.

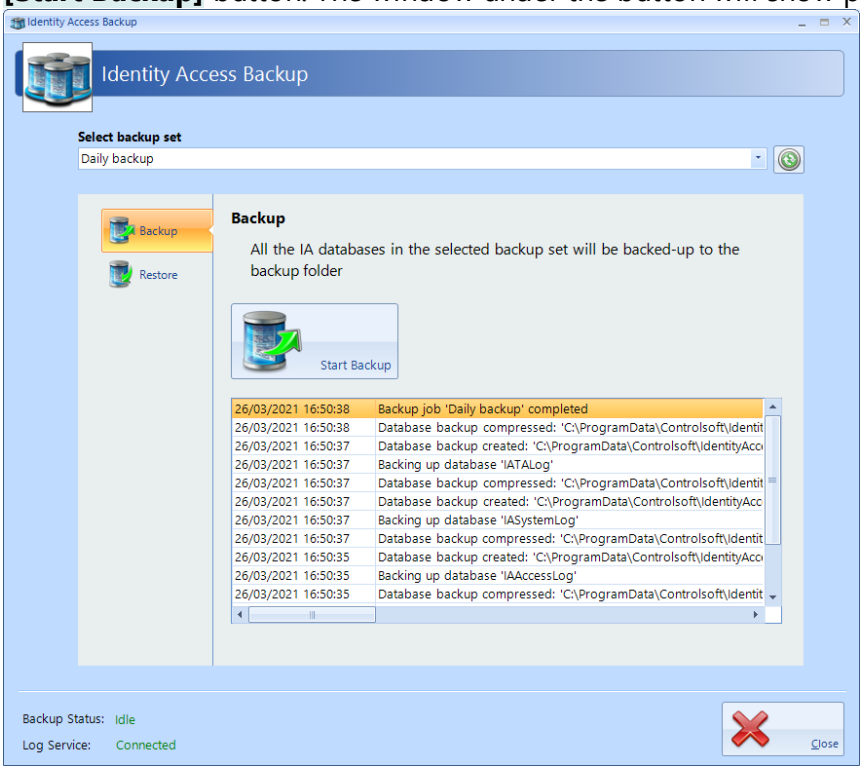
Export T/A: Exports Time & Attendance data to third party systems such as Astrow, Clockwatch and Kronos

Backup: Backups are configured within the IA Configuration utility (see IA Configuration - Backup 271) and will run automatically and/or can be initiated manually as described below. In IA User Interface, click the **Backup** button in the **Tools** menu.

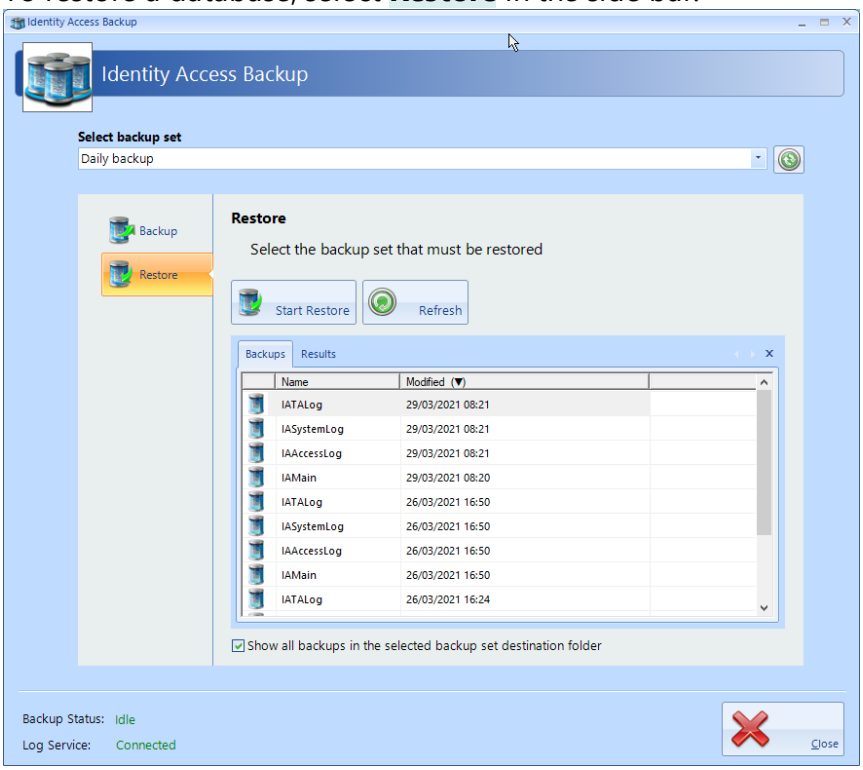


© 2026 Controlsoft Ltd

Select the required Backup Set (if more than one have been configured) and click the **[Start Backup]** button. The window under the button will show progress:

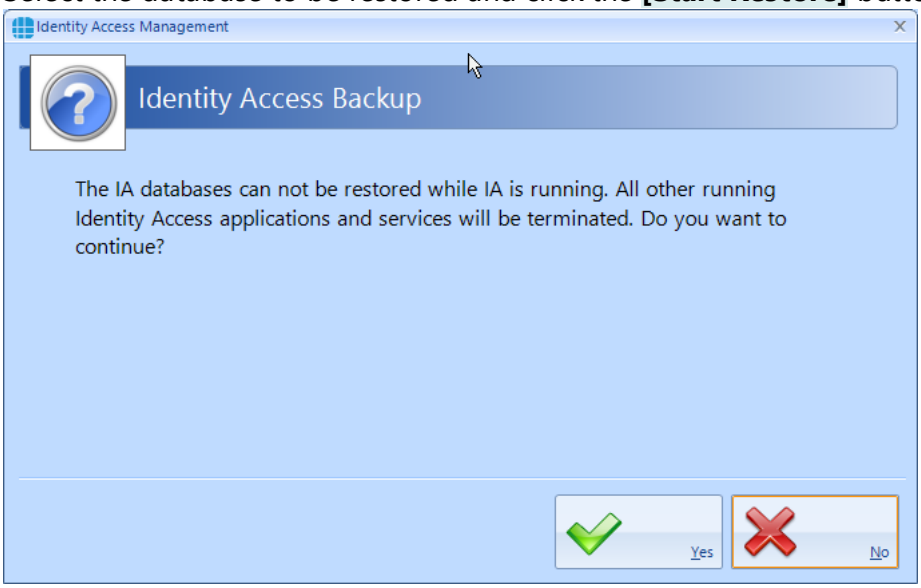


To restore a database, select **Restore** in the side bar:

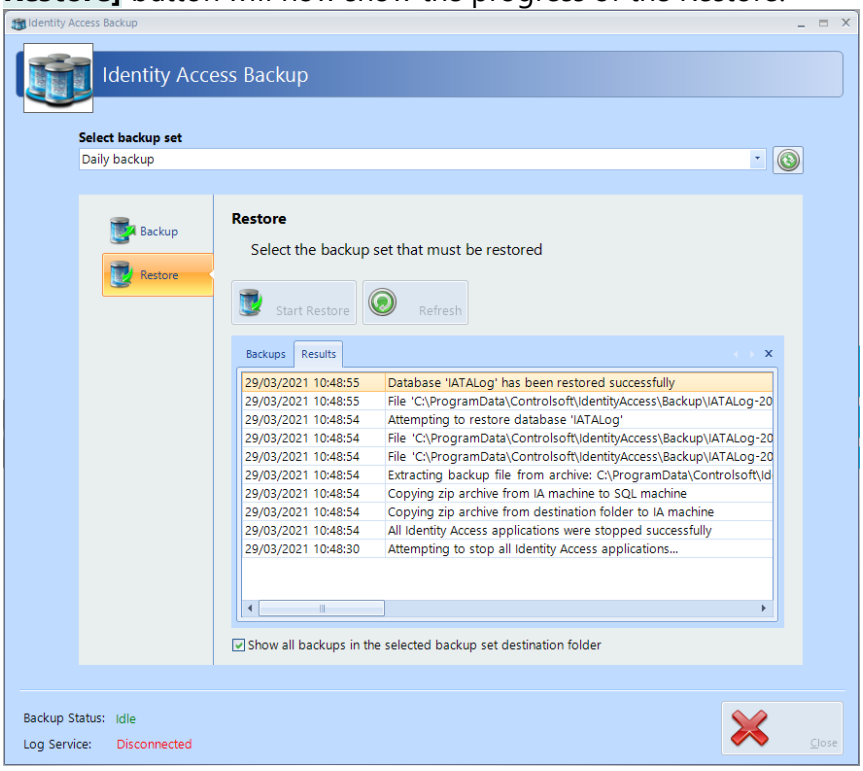


© 2026 Controlsoft Ltd

Select the database to be restored and click the **[Start Restore]** button.

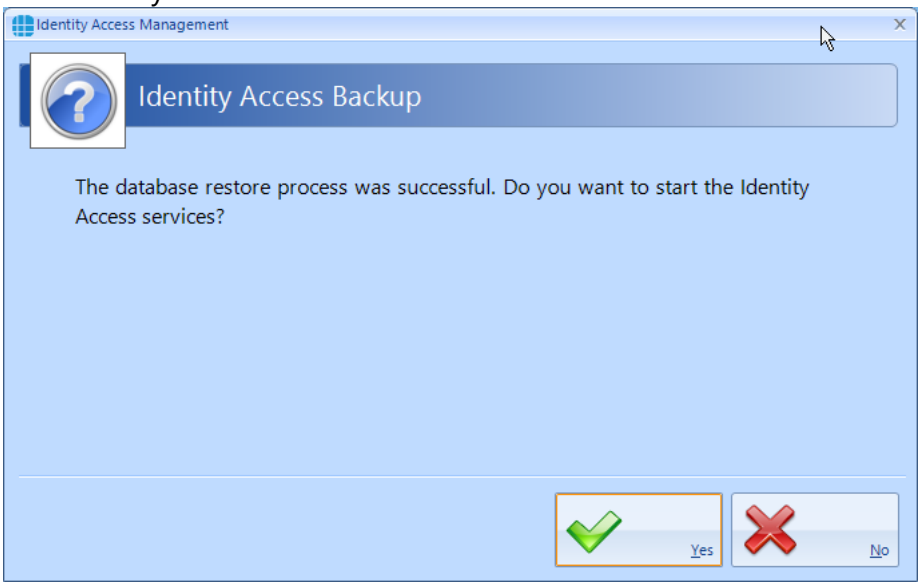


Click [Yes] to automatically close IA and continue. The window below the **[Start Restore]** button will now show the progress of the Restore:



© 2026 Controlsoft Ltd

Followed by:



Click **[Yes]** to end the Restore process and restart Identity Access.

Morpho Configurator: runs the utility to configure a Morpho fingerprint reader (see Appendix L - IA Morpho Configurator 315)

iNet IP Utility: runs the utility to configure an iNet controller (see Setting Controllers Network Addresses)

© 2026 Controlsoft Ltd

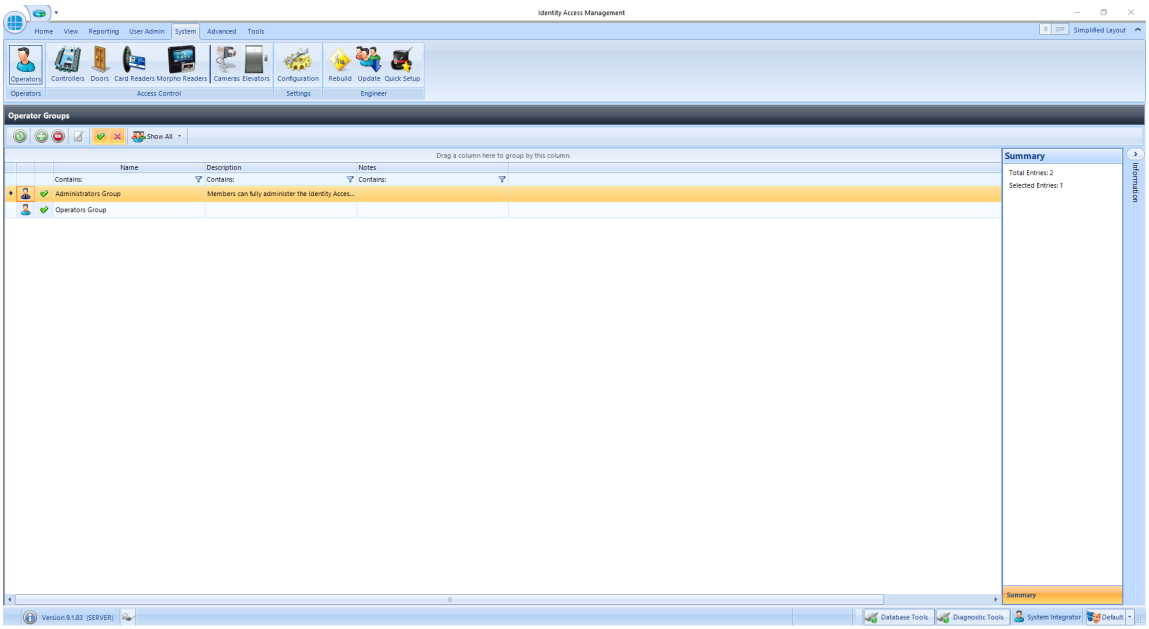
System > Operators

6 System > 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 57.

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).

Select **Operators** from the **System** tab to view the Operators window:

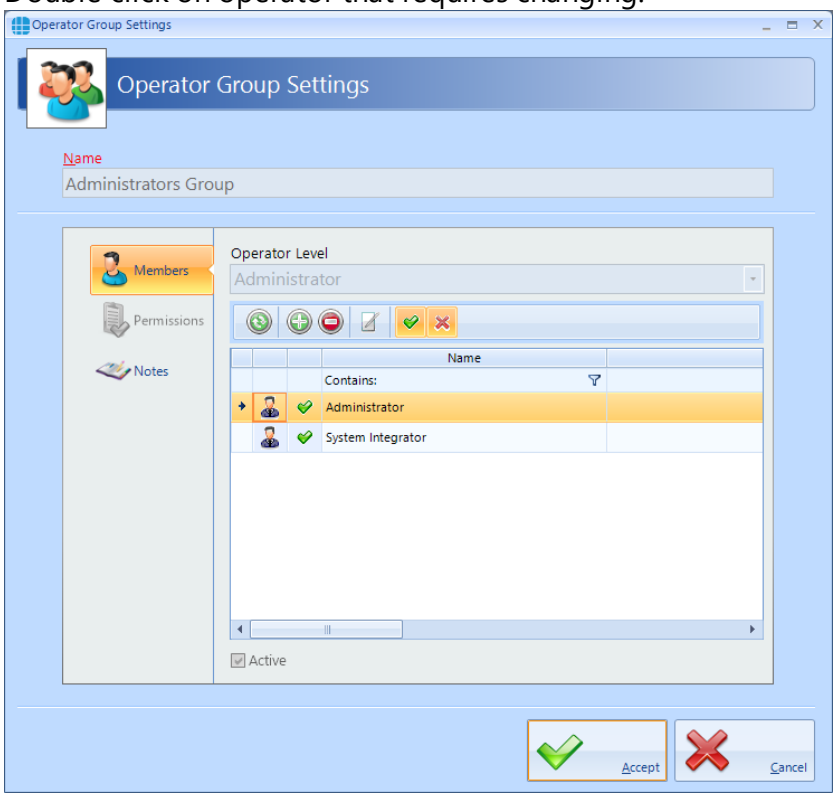


© 2026 Controlsoft Ltd

6.1 Editing the Default Operators

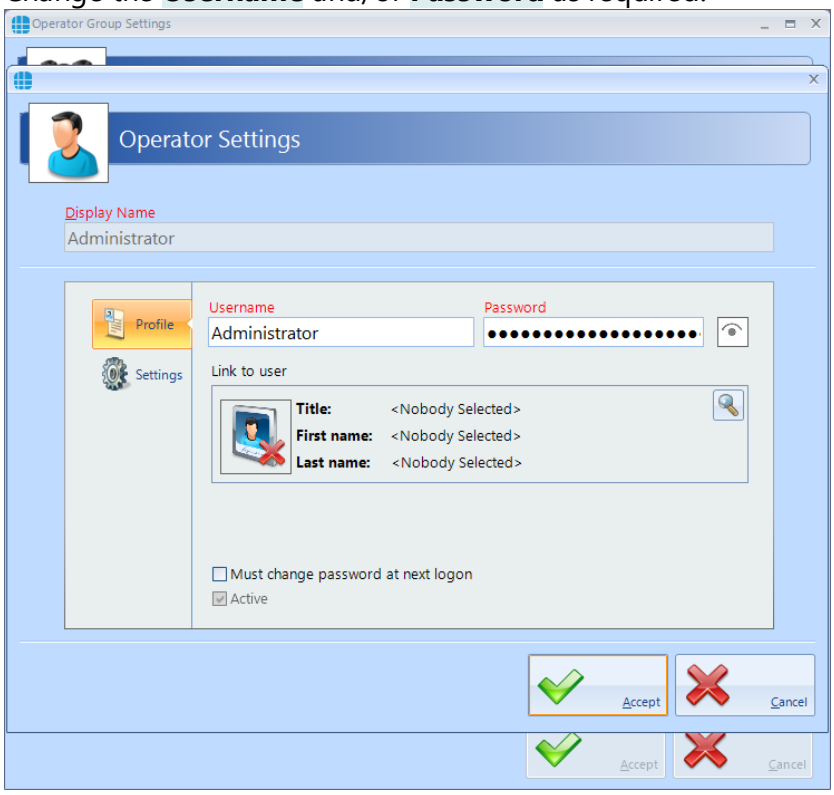
On first installation the default "Administrator" and "System Integrator" passwords are requested. To change the credentials for these operators:

1. Double click on the Administrators group.
2. Double click on operator that requires changing.



© 2026 Controlsoft Ltd

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



4. 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.

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. **NOTE**: The Administrator user cannot be unchecked.

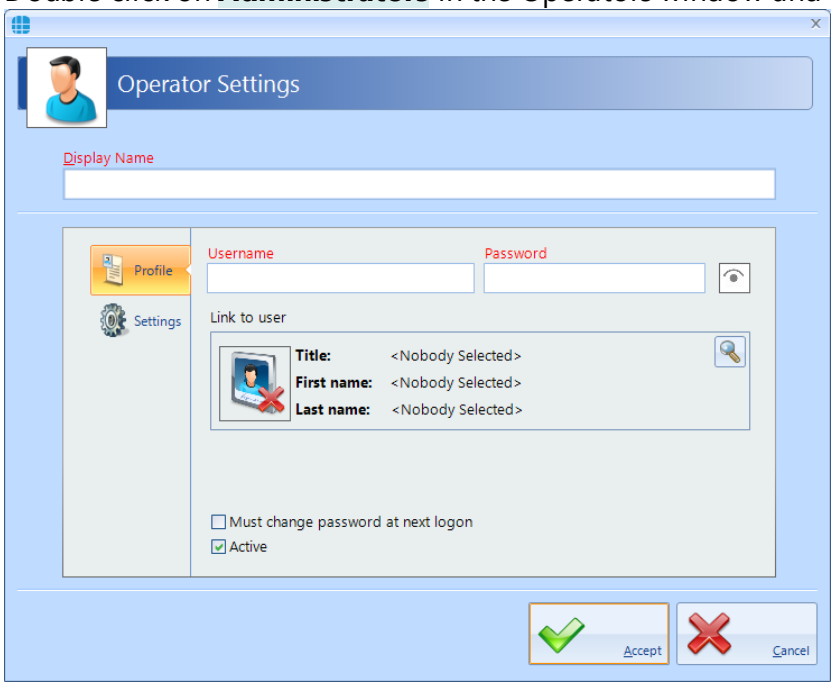
6. Click **[Accept]** when done.

© 2026 Controlsoft Ltd

6.2 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:



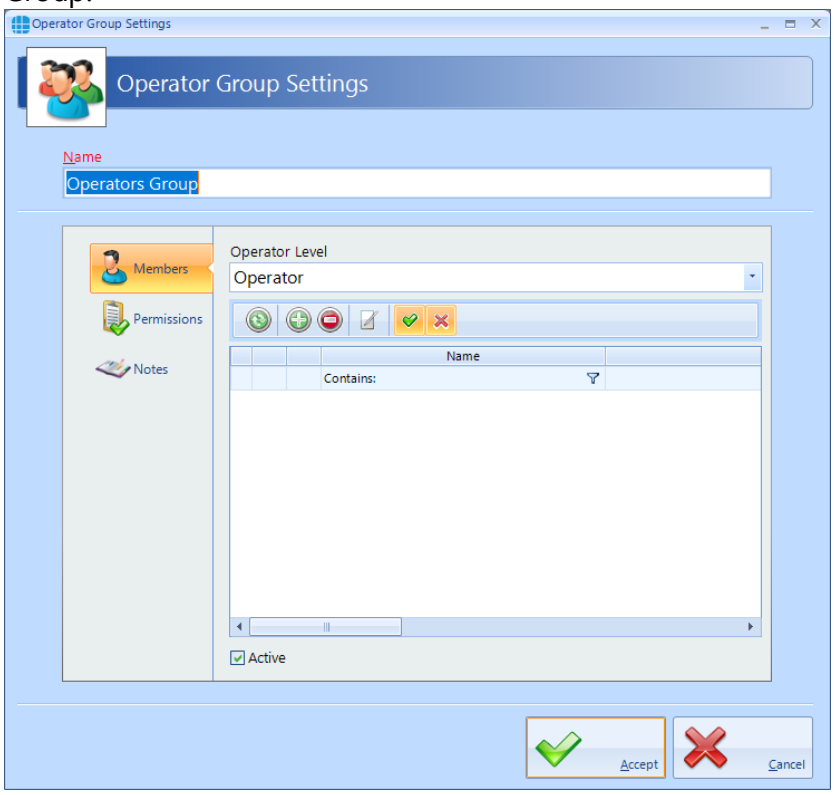
2. Enter a name for the new Administrator under **Display Name**.
3. Enter a **Username** and **Password** as required.
4. If the Operator is also a User, it is possible to use their fingerprint to log onto the Identity Access software. To link the Operator to a User, click on the magnifying glass under **Link to user** and select the User from the list that appears.
5. 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.
6. 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.
7. Click **[Accept]** when done.

© 2026 Controlsoft Ltd

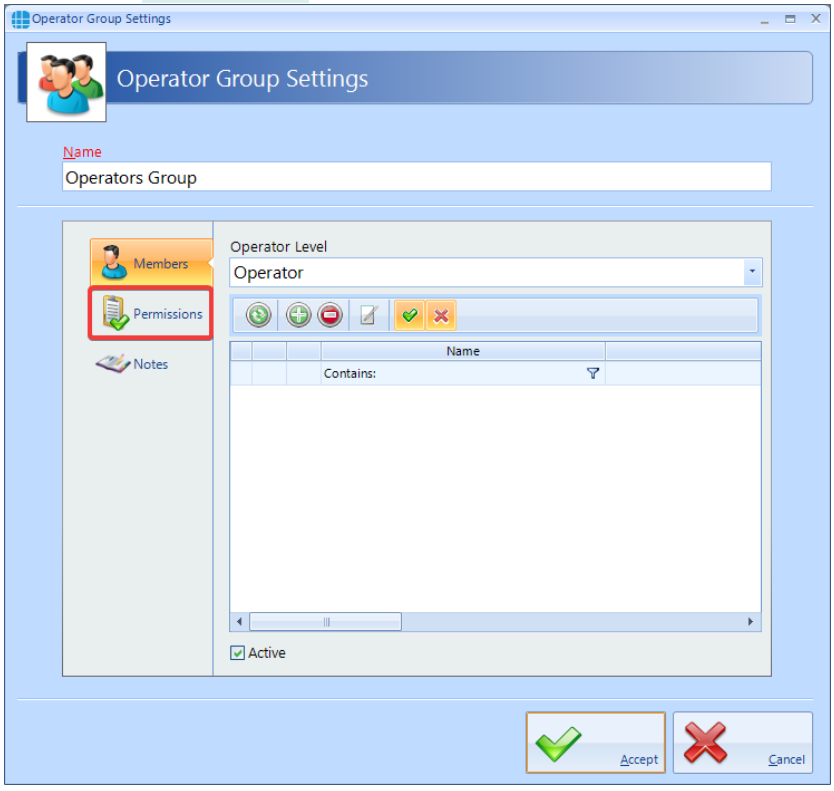
6.3 Adding an Operator

To Add a new Operator's Group to the software:

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

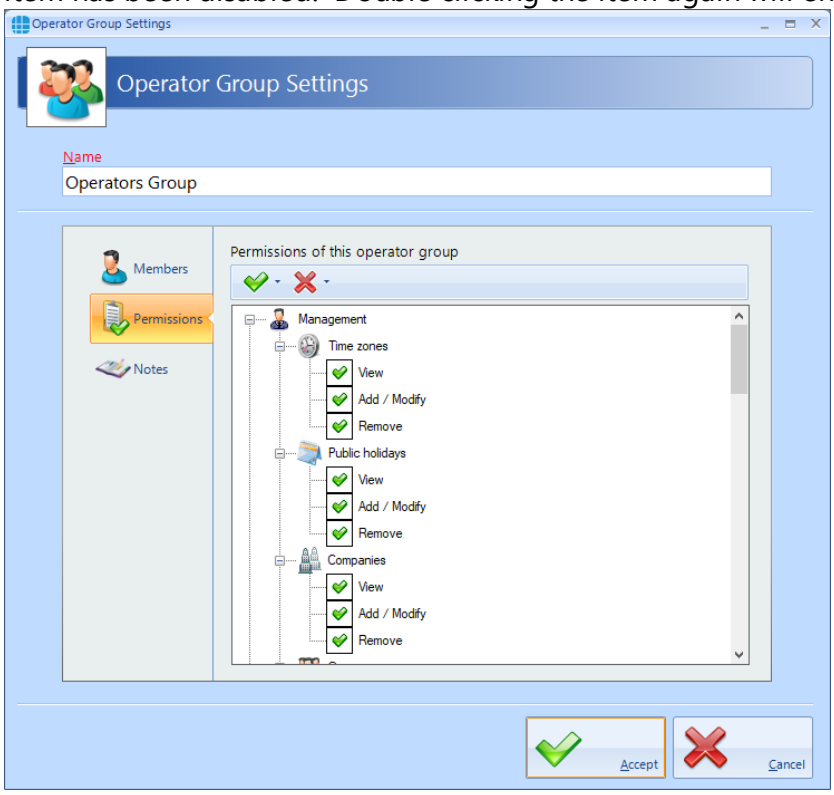


2. Select the **Permissions** tab.



© 2026 Controlsoft Ltd

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.

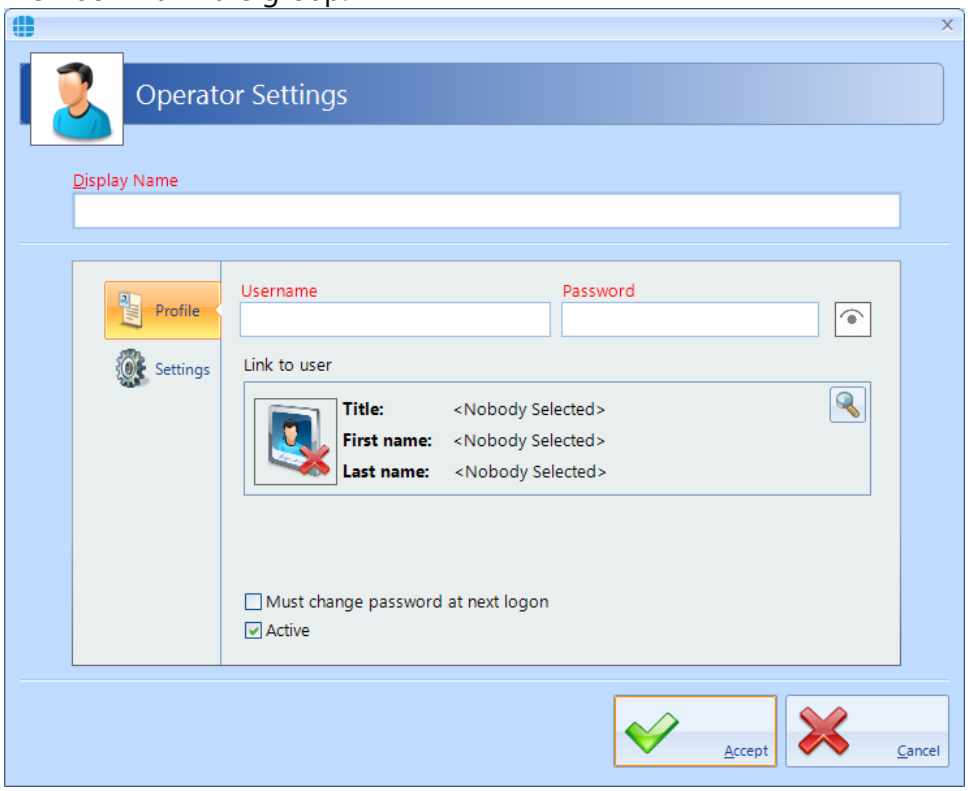


 will enable all items, selected items or all items within a permissions group

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

© 2026 Controlsoft Ltd

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**.

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. If the Operator is also a User, it is possible to use their fingerprint to log onto the Identity Access software. To link the Operator to a User, click on the magnifying glass under **Link to user** and select the User from the list which appears.

8. Tick the option **Must change password at next logon** to force the operator to enter a new password when they next log on.

9. Tick the option **Active** to make the operator active.

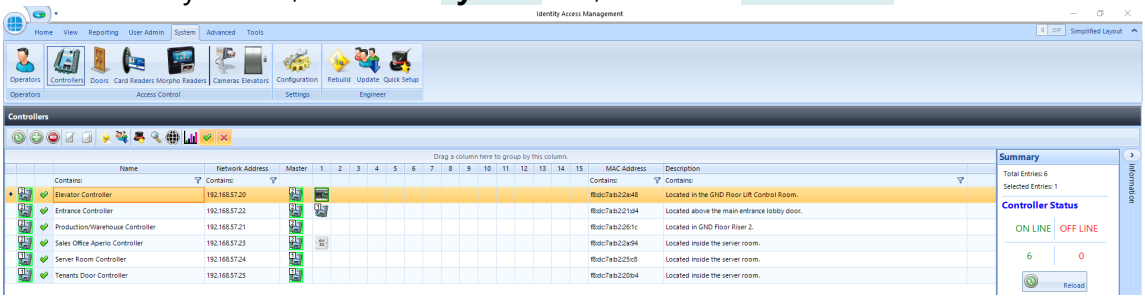
10. Click **[Accept]** when done.

© 2026 Controlsoft Ltd

System > Controllers

7 System > Controllers

Within Identity Access, select the **System** tab, then click **Controllers** in the ribbon bar.



The option buttons are:

 Refresh: Updates the list of controllers

 Add: Creates a new controller in the list

 Delete: Removes the selected controller/s from the list

 Edit: edits the selected controller

 Duplicate: Creates a new controller in the list using the selected controller as a template

 Rebuild: initiates a full download to the selected controllers

 Update: initiates an incremental download to the selected controllers

 Door Configuration Wizard: Helps configure the doors on the controller (see Step 8. Add Doors / Readers using Door Wizard 26).

 Scan: Starts the Find IP Controller Wizard. Using the Find IP Controller Wizard, simply specify the Start IP Address and Stop IP Address and Identity Access will scan for all Master iNets in that IP range (see Step 6. Add IP Controller(s) 23).

: Opens the controllers internal web page for the selected controller.

: Shows and hides the statistics for the selected controller (see Appendix M - Controller Status 318)

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

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

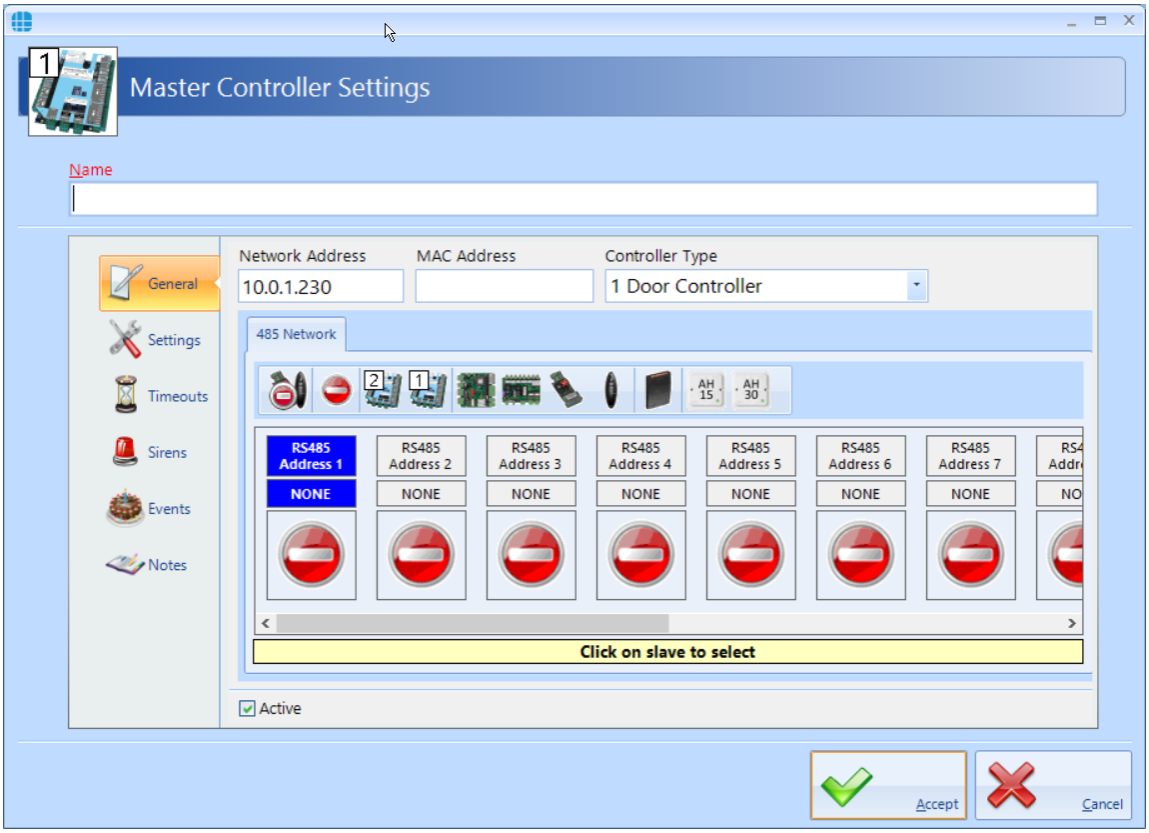
If a controller icon is surrounded by a red box, this indicates that the controller is offline

If a controller icon is shown with a red cross, this indicates that the controller has object confirmation errors. For further information on object confirmation errors see Appendix M - Controller Status 318

© 2026 Controlsoft Ltd

7.1 Controller General

The **General** tab in the **Controller Settings** window displays the basic properties of the Master Controller



Enter a **Name** to identify the controller (e.g. Ground Floor)

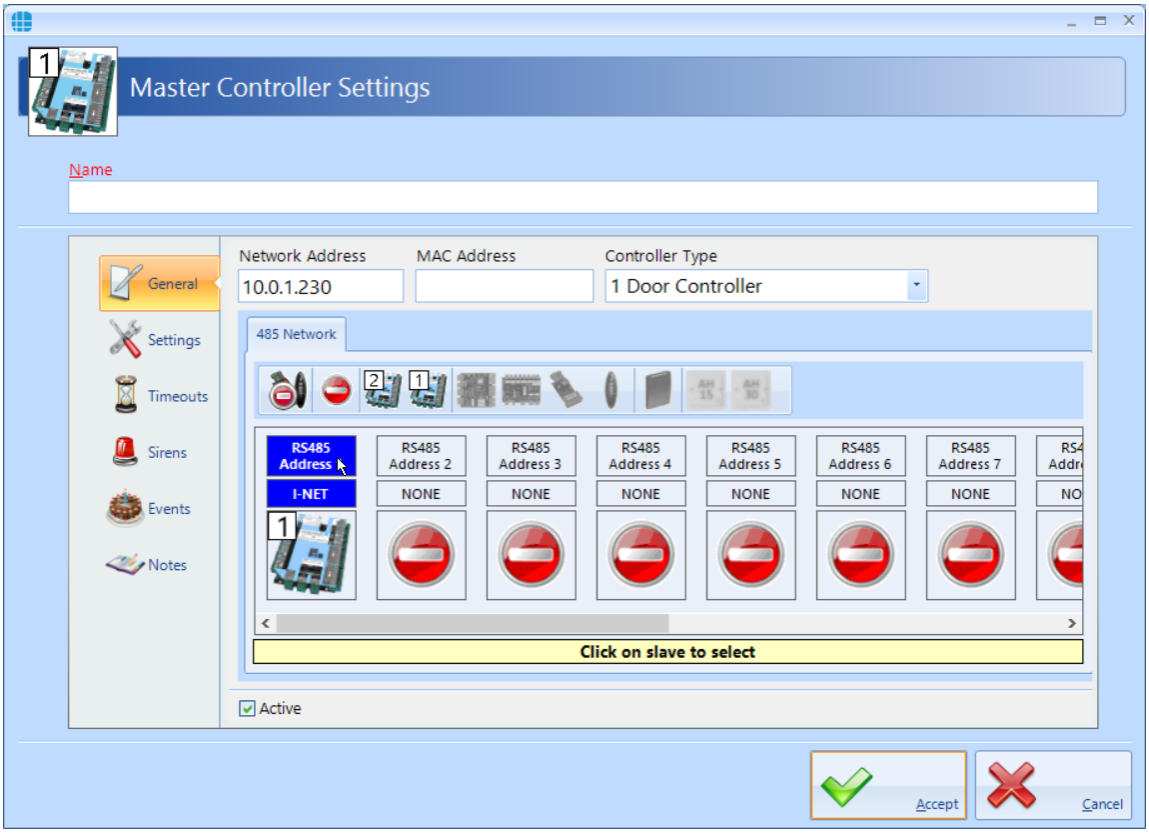
Enter the **Network Address** (IP Address) previously programmed into the controller (this will be already populated if the controller was added via the Find IP Controllers Wizard).

Entering the **MAC Address** is optional, this will be already populated if the controller was added via the Find IP Controllers Wizard.

Enter the **Controller Type** (this will be already populated if the controller was added via the Find IP Controllers Wizard).

© 2026 Controlsoft Ltd

It is then possible to define the type of expansion used on that Master Controller. For example, to add a Downstream iNet which has Address 1 on the RS485 bus, highlight **RS485 Address 1** then click on the icon for a 1 Door or 2 Door iNet.



The expansion options available are as follows:

 Removes all devices from the RS485 bus

 Removes the selected device from the RS485 bus

 Add a Downstream 2 Door iNet to the RS485 bus

 Add a Downstream 1 Door iNet to the RS485 bus

 Add an IOC IO Expander Board to the RS485 bus

 Add an AC-1100 reader to the RS485 bus

 Add an HID OSPD reader to the RS485 bus. For further information on HID OSDP readers, please refer to [Knowledge Base - HID OSDP Readers]

© 2026 Controlsoft Ltd



Add an Aperio AH15 (1:1) hub to the RS485 bus. For further information on Aperio Wireless Locks, please refer to Knowledge Base - Aperio Wireless Guide



Add an Aperio AH30 (1:8) hub to the RS485 bus. For further information on Aperio Wireless Locks, please refer to Knowledge Base - Aperio Wireless Guide

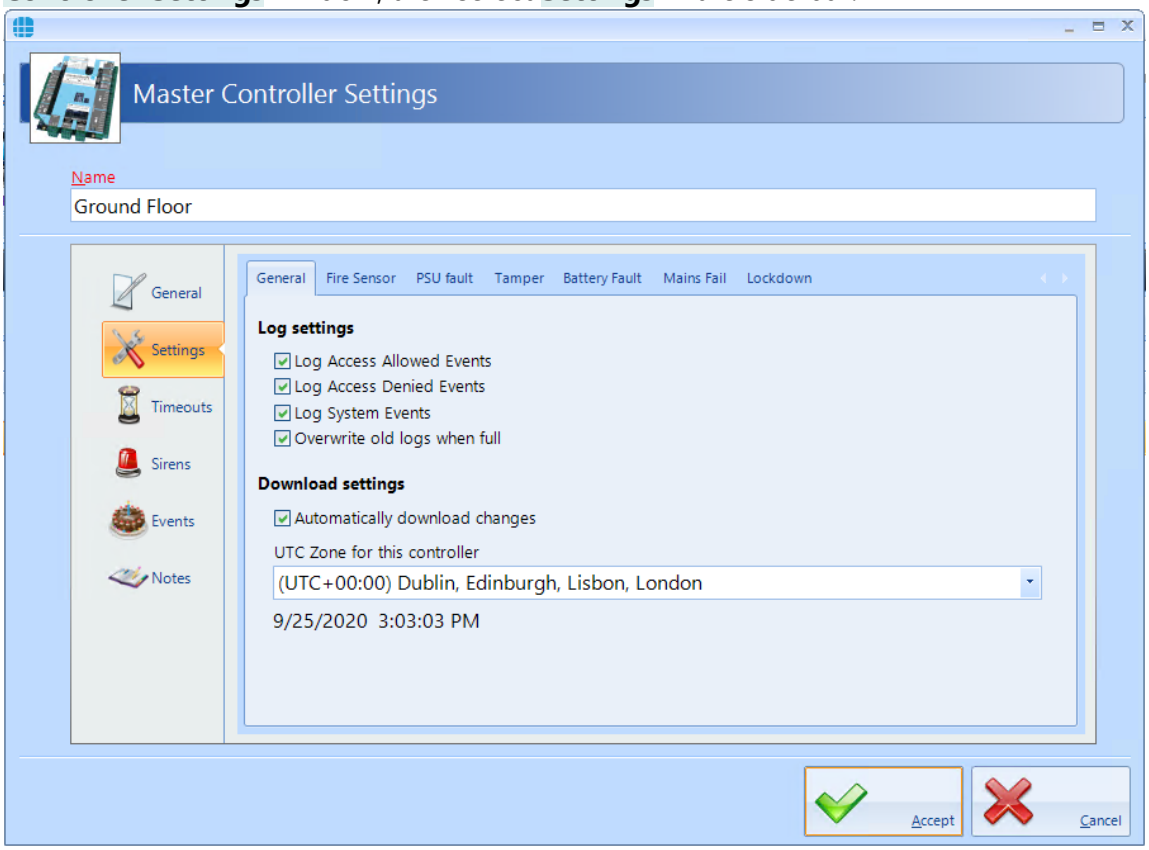
This information will then be used during the programming to define which inputs, outputs etc. are available for use. ***NOTE: Different device types cannot be combined on a single RS485 bus. Selecting a Downstream iNet greys out other types of expanders (and vice versa) reducing the possibility of configuration errors.***

When the **Active** box is ticked, data for that channel will be sent to the hardware during a Full Download.

© 2026 Controlsoft Ltd

7.2 Controller Settings

From the **Controllers** window, double click the required controller to open the **Master Controller Settings** window, then select **Settings** in the side bar.



Log Access Allowed Events, **Log Access Denied Events** and **Log System Events** ensures the controller logs all the relevant events. Only deselect these for the rare occasion that the controller is to be used as a stand-alone controller with no connected Identity Access software.

When ticked, **Overwrite old logs when full** will act as a 'cyclic buffer' with the newest event overwriting the oldest. If unticked, the controller will stop logging events when its memory is full.

Automatically download changes ensures that changes are downloaded to the controller as they happen rather than having to remember to perform a Rebuild at the and of the programming.

UTC Zone for this controller allows different controllers to operate in different international time zones.

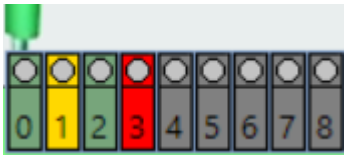
The remaining tabs allow for inputs to be programmed as Fire, Mains fail etc.

NOTE: When programming Inputs and outputs, the graphic is colour coded on the screen as follows:

- ***Green** = Input/Output is available to use (e.g. 0 and 2 in the example below)*

© 2026 Controlsoft Ltd

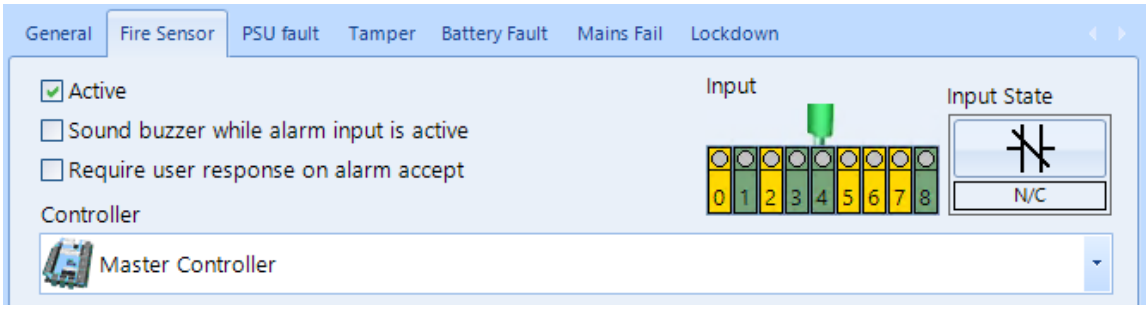
- ***Yellow** = Input/Output already programmed elsewhere (e.g. 1 in the example below)*
- ***Red** = Input/Output programmed to two different functions which needs to be resolved (e.g. 3 in the example below)*
- ***Grey** = Input/Output not present (e.g. 4, 5, 6, 7 and 8 in the example below)*



Furthermore, the 'wire' connected to the input will be green if the selection is acceptable 

or red if it is unacceptable 

Fire Sensor:



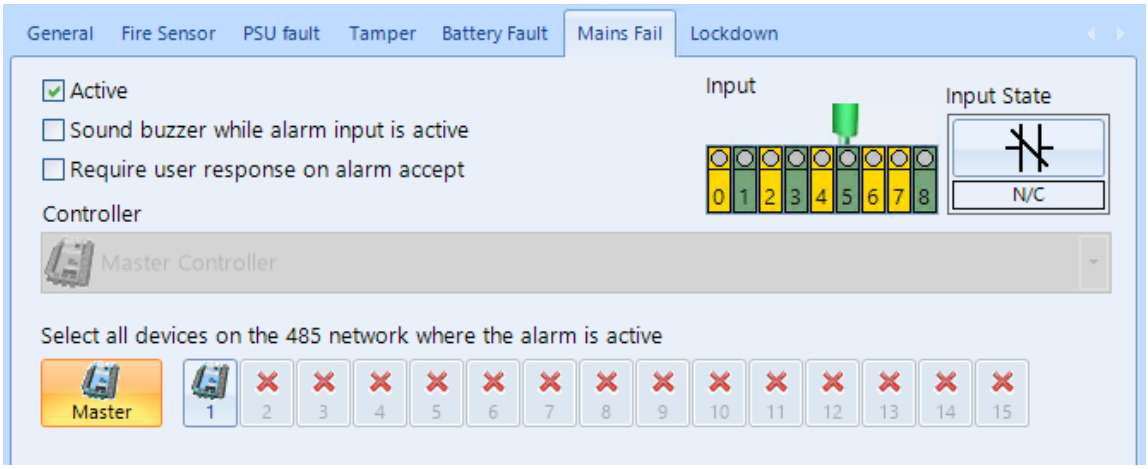
If doors on this channel are to be released during a fire alarm, tick the **Active** box, then select the **Input** the Fire Panel is connected to, and whether the Fire panel contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Sound buzzer while alarm input is active** will activate the iNet sounder during the fire alarm.

If **Require user response on alarm accept** is ticked, the operator must enter text before the fire alarm can be accepted and subsequently cleared.

Ensure that the controller is shown as Master Controller - ***NOTE: NEVER CONNECT A FIRE PANEL TO A DOWNSTREAM DEVICE***.

© 2026 Controlsoft Ltd

AC Mains Fail (Pre-cabled on 2DR-ACU):

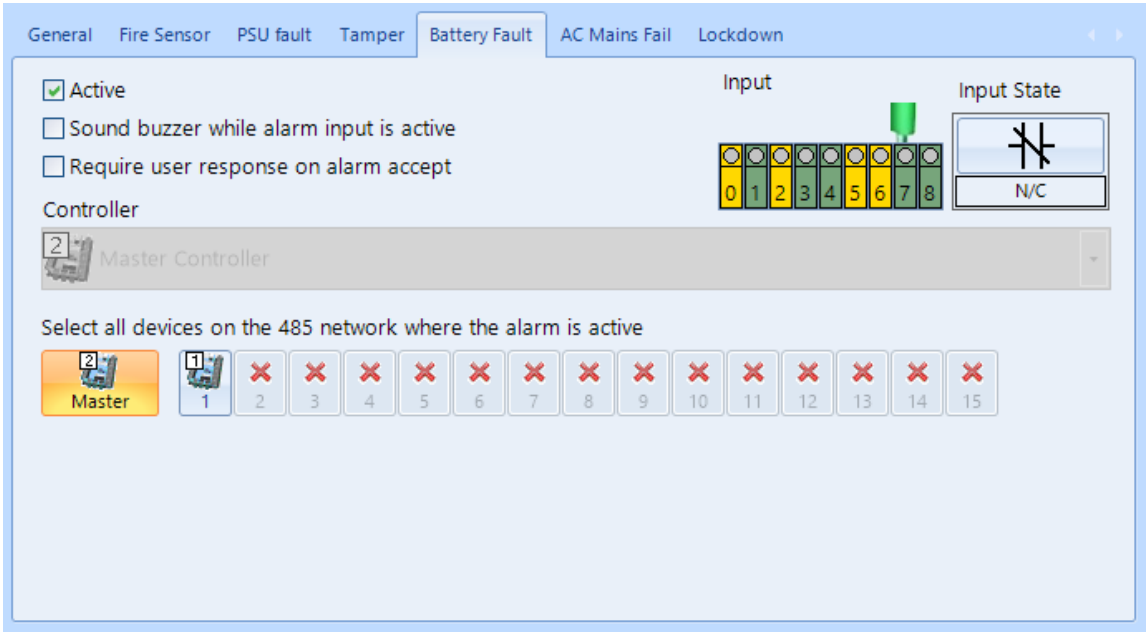


To monitor the power supply for AC Mains Fail, tick the **Active** box, then select the **Input** the AC Mains Fail signal is connected to, and whether the AC Mains Fail contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Sound buzzer while alarm input is active** will activate the iNet sounder during the fault condition.

If **Require user response on alarm accept** is ticked, the operator must enter text before the alarm can be accepted and subsequently cleared.

Select all devices on the 485 network where the alarm is active defines which devices are monitored for this fault. In the example above, the Master monitors for Mains Fail however the Downstream device does not. This is useful if you have multiple controllers per power supply/enclosure.

Battery Fault (Pre-cabled on 2DR-ACU):



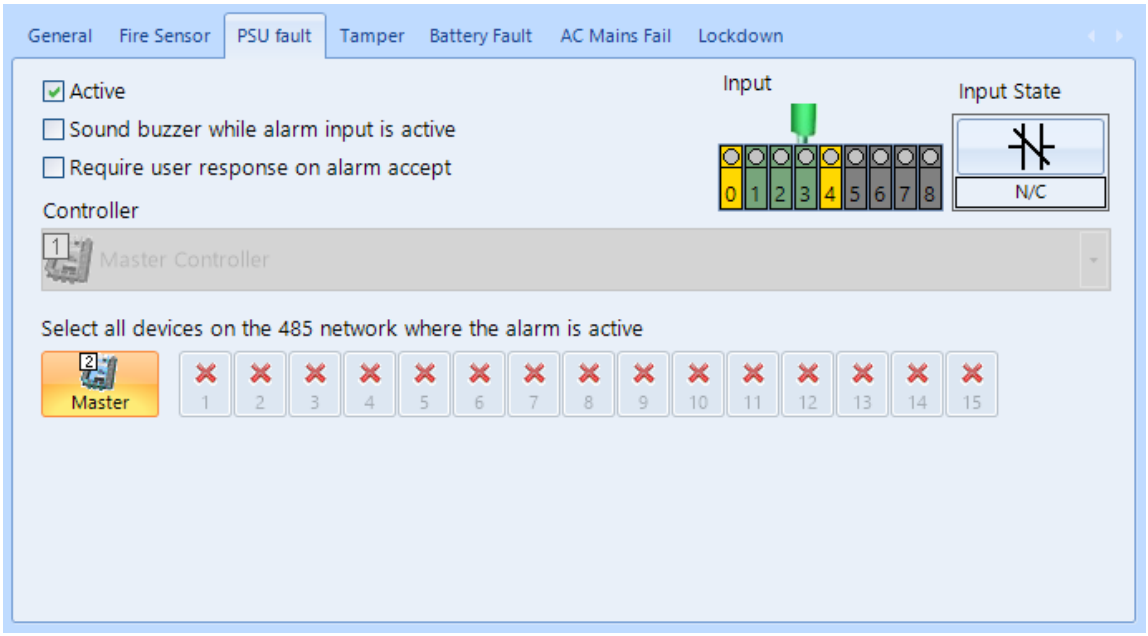
© 2026 Controlsoft Ltd

To monitor the power supply for battery fault, tick the **Active** box, then select the **Input** the battery fault signal is connected to, and whether the contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Sound buzzer while alarm input is active** will activate the iNet sounder during the fault condition.

If **Require user response on alarm accept** is ticked, the operator must enter text before the alarm can be accepted and subsequently cleared.

Select all devices on the 485 network where the alarm is active defines which devices are monitored for this fault. In the example above, the Master monitors for battery fault however the Downstream device does not. This is useful if you have multiple controllers per power supply/enclosure.

PSU Fault (Pre-cabled on 1DR-ACU):



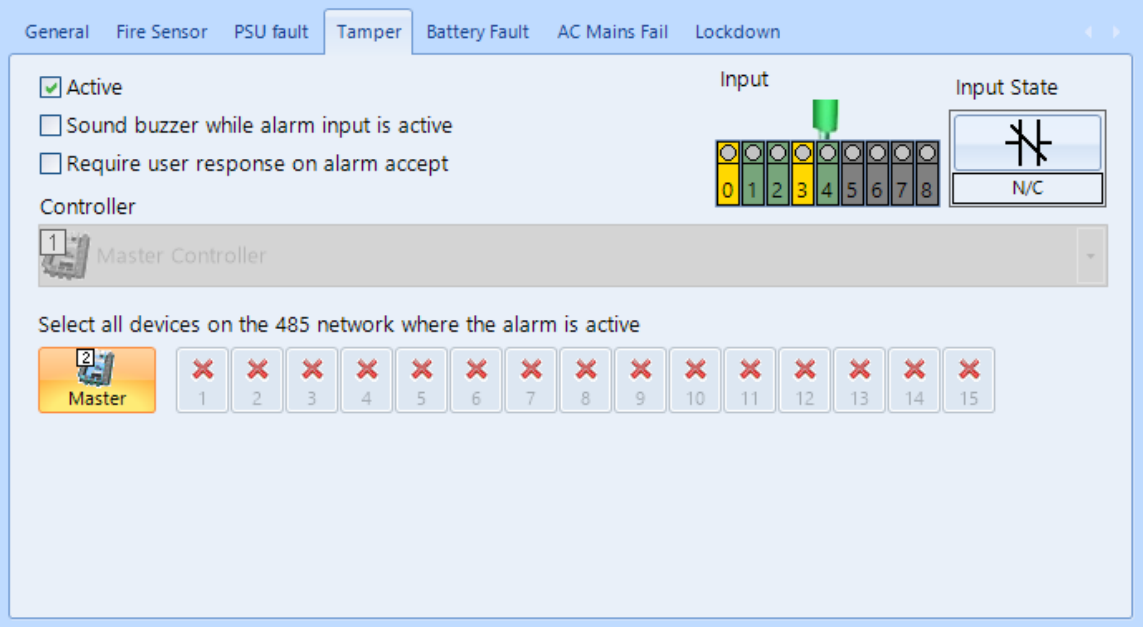
To monitor the power supply for fault, tick the **Active** box, then select the **Input** the fault signal is connected to, and whether the contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Sound buzzer while alarm input is active** will activate the iNet sounder during the fault condition.

If **Require user response on alarm accept** is ticked, the operator must enter text before the alarm can be accepted and subsequently cleared.

Select all devices on the 485 network where the alarm is active defines which devices are monitored for this fault. In the example above, the Master monitors for PSU fault however the Downstream device does not. This is useful if you have multiple controllers per power supply/enclosure.

© 2026 Controlsoft Ltd

Tamper (Pre-cabled on 1DR-ACU / 2DR-ACU):



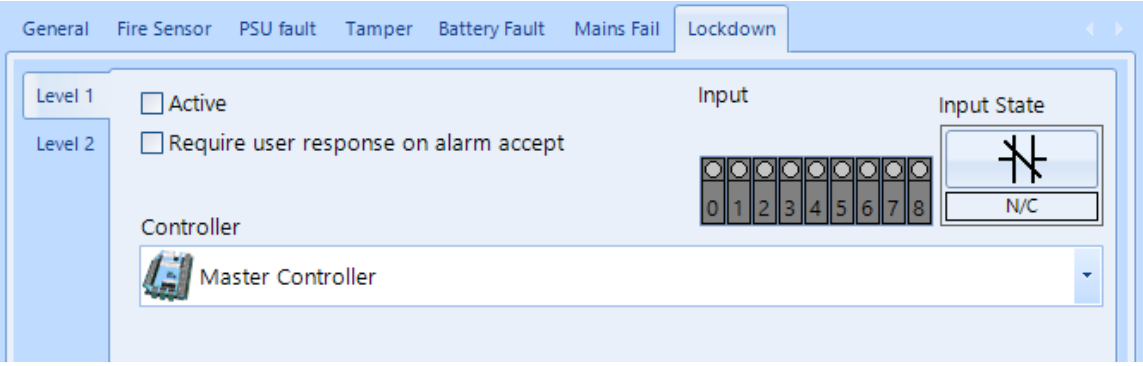
To monitor the enclosure for tamper, tick the **Active** box, then select the **Input** the tamper signal is connected to, and whether the contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Sound buzzer while alarm input is active** will activate the iNet sounder during the tamper condition.

If **Require user response on alarm accept** is ticked, the operator must enter text before the alarm can be accepted and subsequently cleared.

Select all devices on the 485 network where the alarm is active defines which devices are monitored. In the example above, the Master monitors for tamper however the Downstream device does not. This is useful if you have multiple controllers per power supply/enclosure.

Lockdown:

Click here: for full information on how to setup Lockdowns in Identity Access.

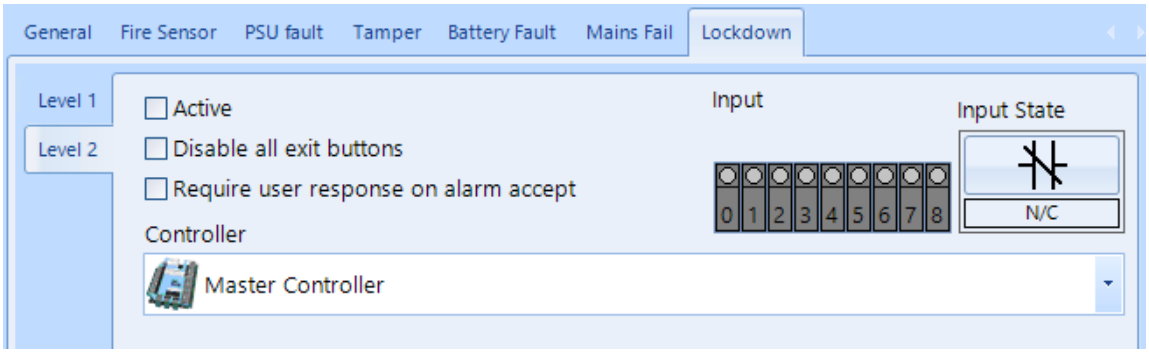


© 2026 Controlsoft Ltd

To activate Lockdown level 1 (Amber) from a push button or keyswitch, tick the **Active** box, then select the **Input** the button is connected to, and whether the button's contacts are **N/C** (Normally Closed) or **N/O** (Normally Open).

If **Require user response on alarm accept** is ticked, the operator must enter text before the Lockdown alarm can be accepted and subsequently cleared.

NOTE: If no inputs are selected for Lockdown on any controller (default), and the* Show lockdown buttons on dashboard even if no lockdown inputs are configured *is deselected (default), Lockdown will be disabled and the Lockdown icons in the Dashboard 'Doors' tab will be greyed out.



To activate Lockdown level 2 (Red) from a push button or keyswitch, tick the **Active** box, then select the **Input** the button is connected to, and whether the button's contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Disable all exit buttons** will ensure that Request to Exit buttons will not operate during Level 2 Lockdown.

If **Require user response on alarm accept** is ticked, the operator must enter text before the Lockdown alarm can be accepted and subsequently cleared.

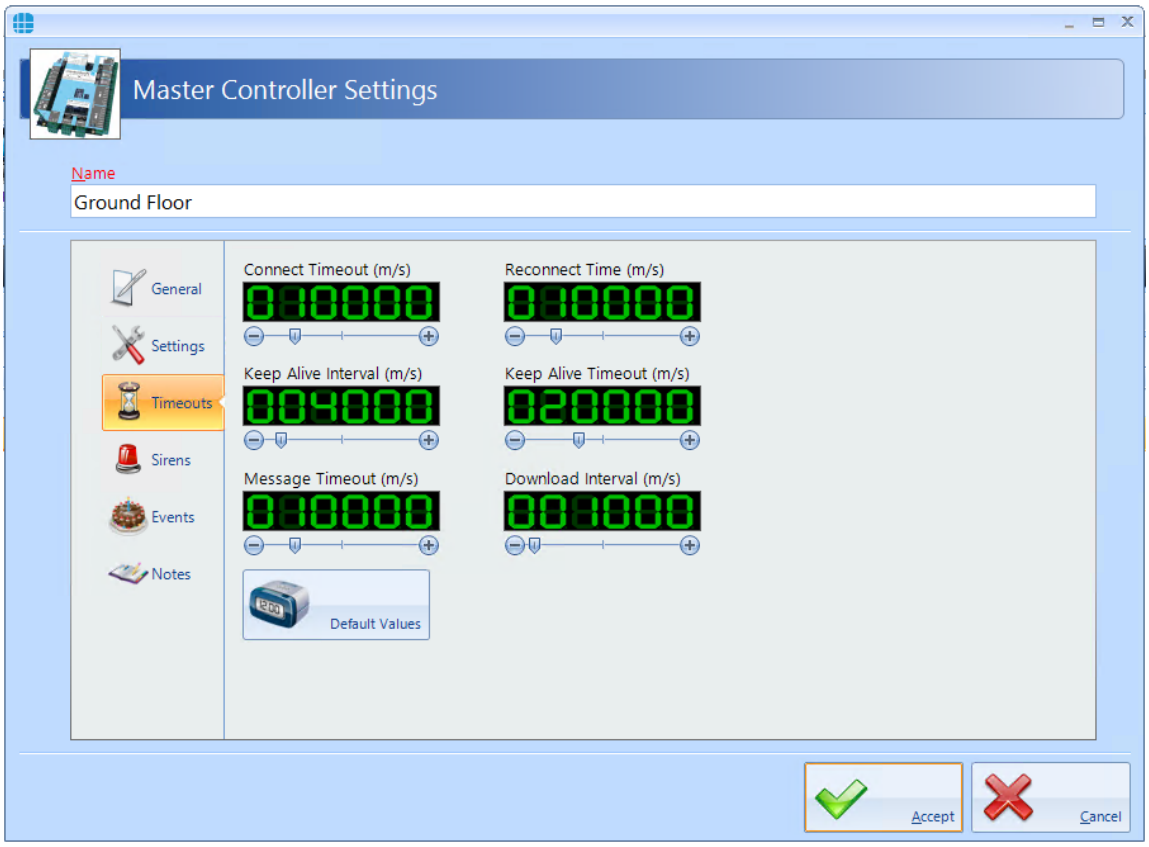
NOTE: DURING LOCKDOWN, THE ONLY WAY TO RETURN TO LEVEL 0 (GREEN) IS TO SELECT THE ON-SCREEN BUTTONS. ALWAYS ENSURE THAT ACCESS TO THE PC IS POSSIBLE DURING LOCKDOWN.

7.3 Controller Timeouts

Controlsoft recommend that all entries in the **Timeouts** tab in the side bar are left unchanged.

© 2026 Controlsoft Ltd

NOTE: Changes should only be made on advice from Controlsoft Technical Support.



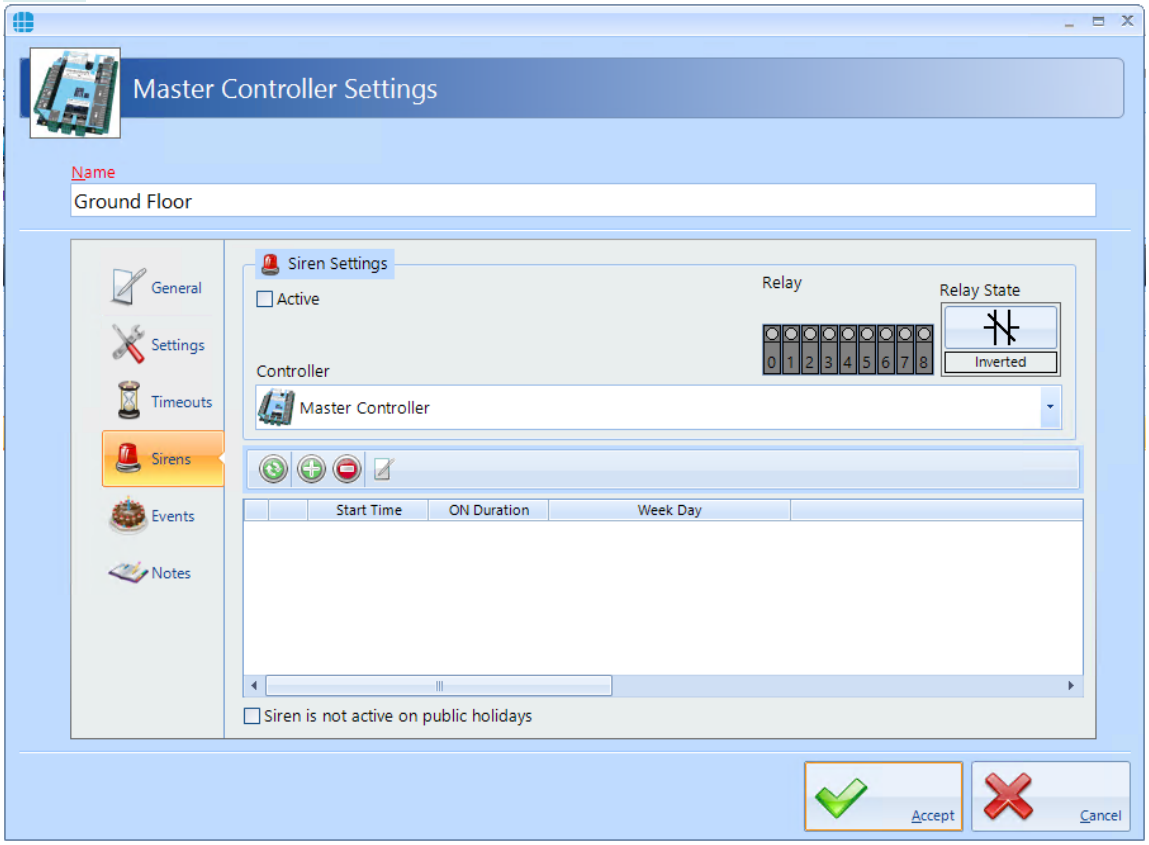
NOTE: All the timers in this window are in milliseconds.

If changes are inadvertently made, use the **[Default Values]** button to restore all timers to their correct values.

© 2026 Controlsoft Ltd

7.4 Controller Sirens

It can sometimes be useful to trigger an output at certain times of the day to activate a sounder (e.g. 'class change' bells in a school). This can be achieved simply using the **Sirens** section in the sidebar:



Tick the **Active** box under **Siren Settings** to enable the function.

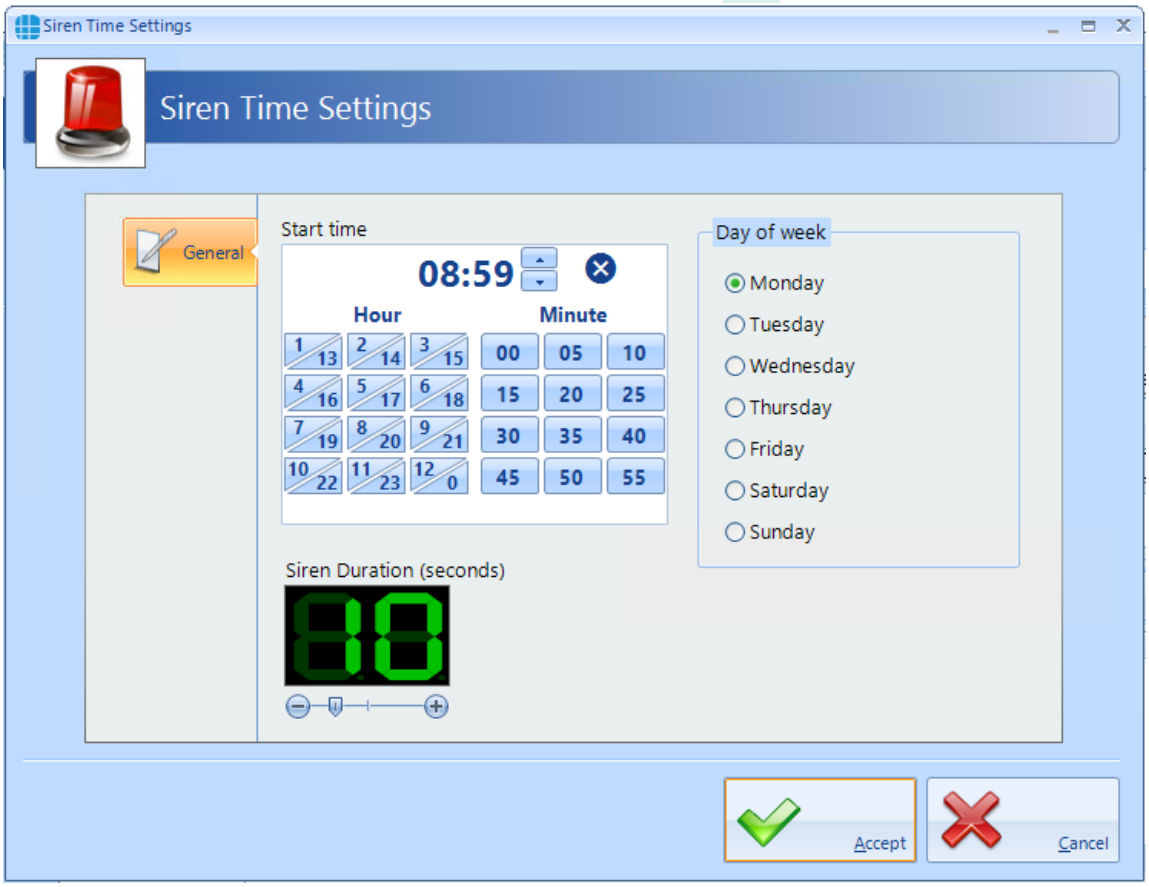
Controller defines which device will be connected to the siren, either the **Master Controller**, or **RS485 Address 1** for the device with bus address 1 etc.

Relay defines which output relay is connected to the siren (e.g Relay 3 in the example below).

Relay State defines whether the selected relay will be Normal (energises to sound the siren) or Inverted (de-energises to sound the siren)

© 2026 Controlsoft Ltd

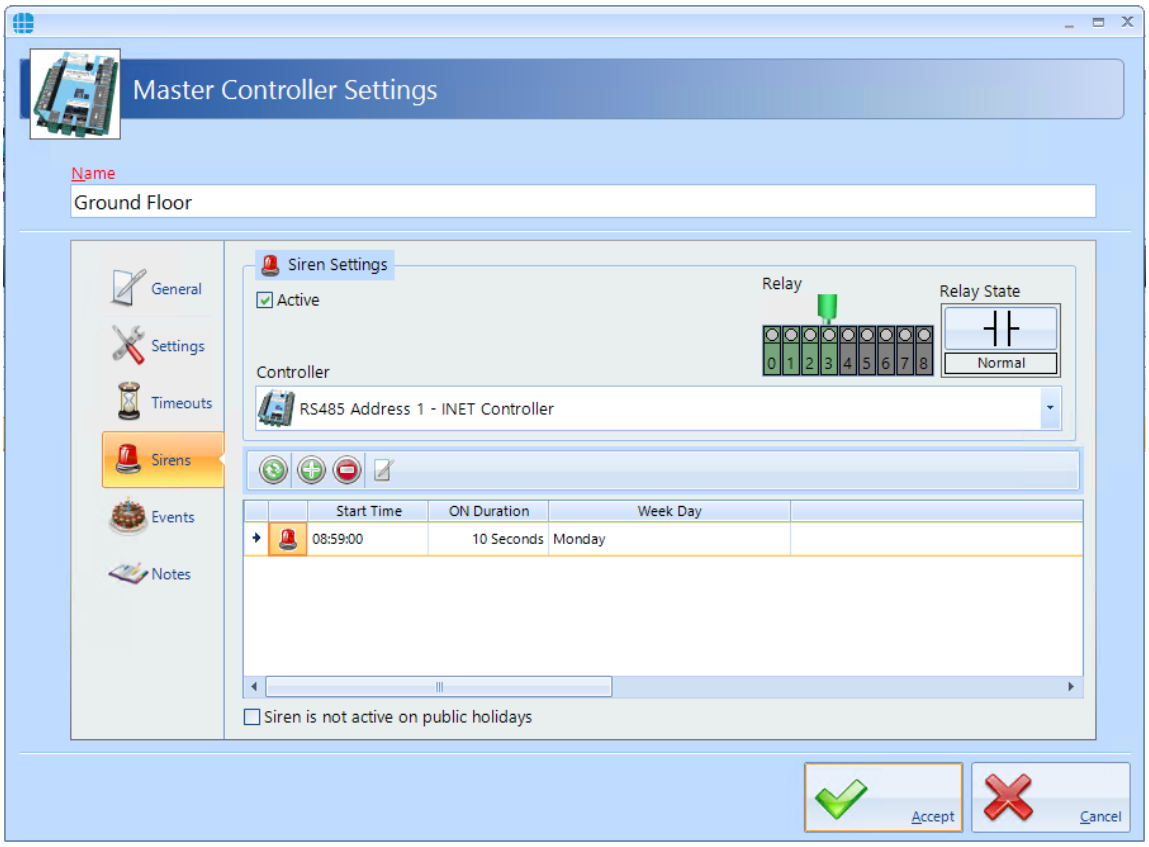
To add times that the siren is to be activated, click the **Add** button 



Select the **Start time** using the **Hour** buttons and the **Minute** buttons, or the up and down arrows. Set the **Siren Duration** and **Day of the week** as required (e.g. 8:59am for 10 seconds on Mondays).

© 2026 Controlsoft Ltd

Click **[Accept]** to update the Master Controller Properties

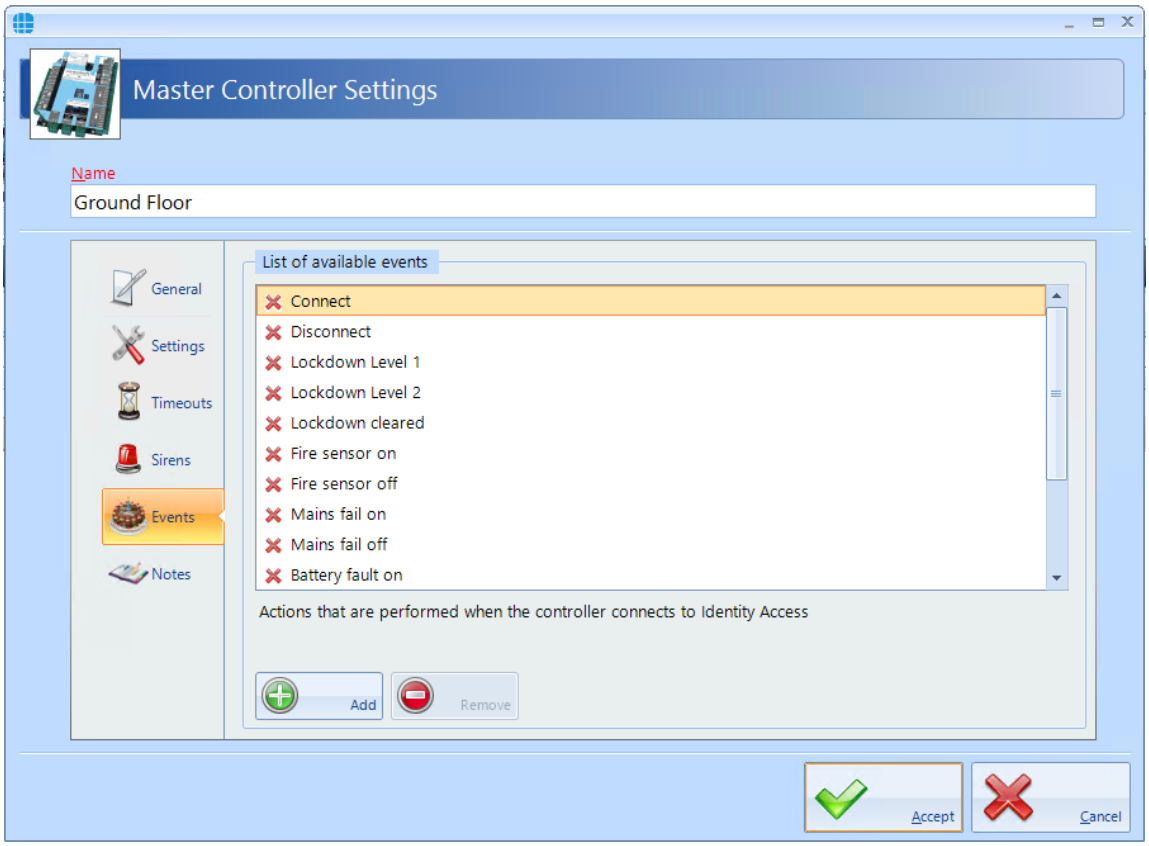


Finally, tick the box **Siren is deactivated on public holidays** if the siren is not to sound on certain days.

7.5 Controller Events

The Events tab will indicate whether any Events have been configured for the selected controller.

© 2026 Controlsoft Ltd

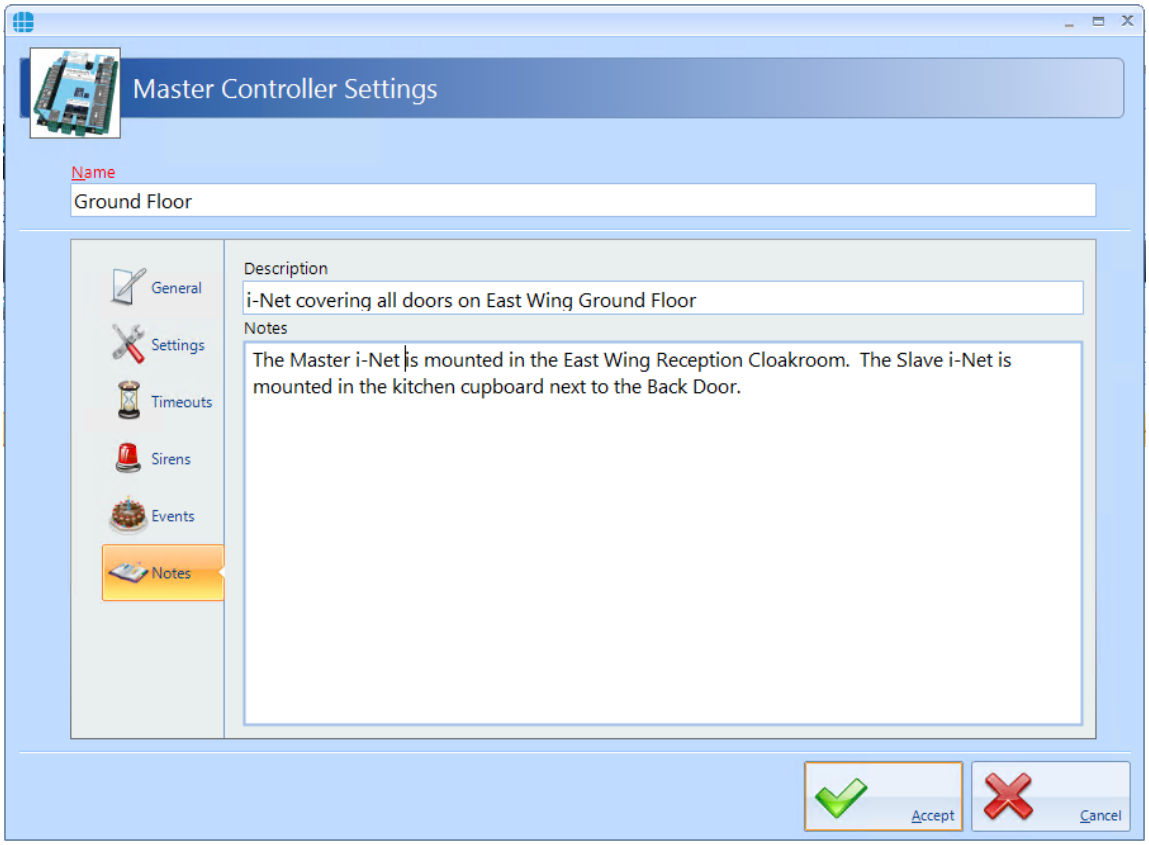


In this example, no Events have been created for the selected controller. Clicking the **[Add]** button will allow Events to be created, although this is more easily done via the **Events** button in the **Advanced** tab, where all Events and related Actions can be viewed,

© 2026 Controlsoft Ltd

7.6 Controller Notes

The Notes section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

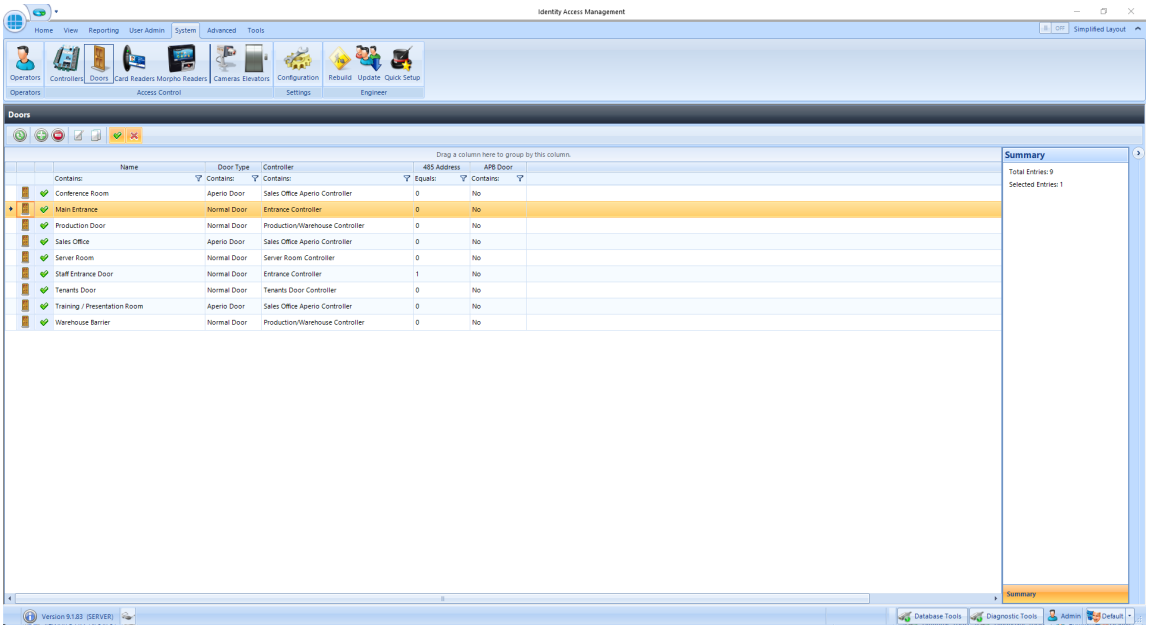


© 2026 Controlsoft Ltd

System > Doors

8 System > Doors

Doors can be configured using the **Door Configuration Wizard** (see Door Configuration Wizard), or this can be done manually. Within Identity Access, select the **System** tab, then click **Doors** in the ribbon bar.



The option buttons are:

 Refresh: Updates the list of doors

 Add: Creates a new door in the list

 Delete: Removes the selected door/s from the list

 Edit: edits the selected door

 Duplicate: Creates a new door in the list using the selected door as a template

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

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

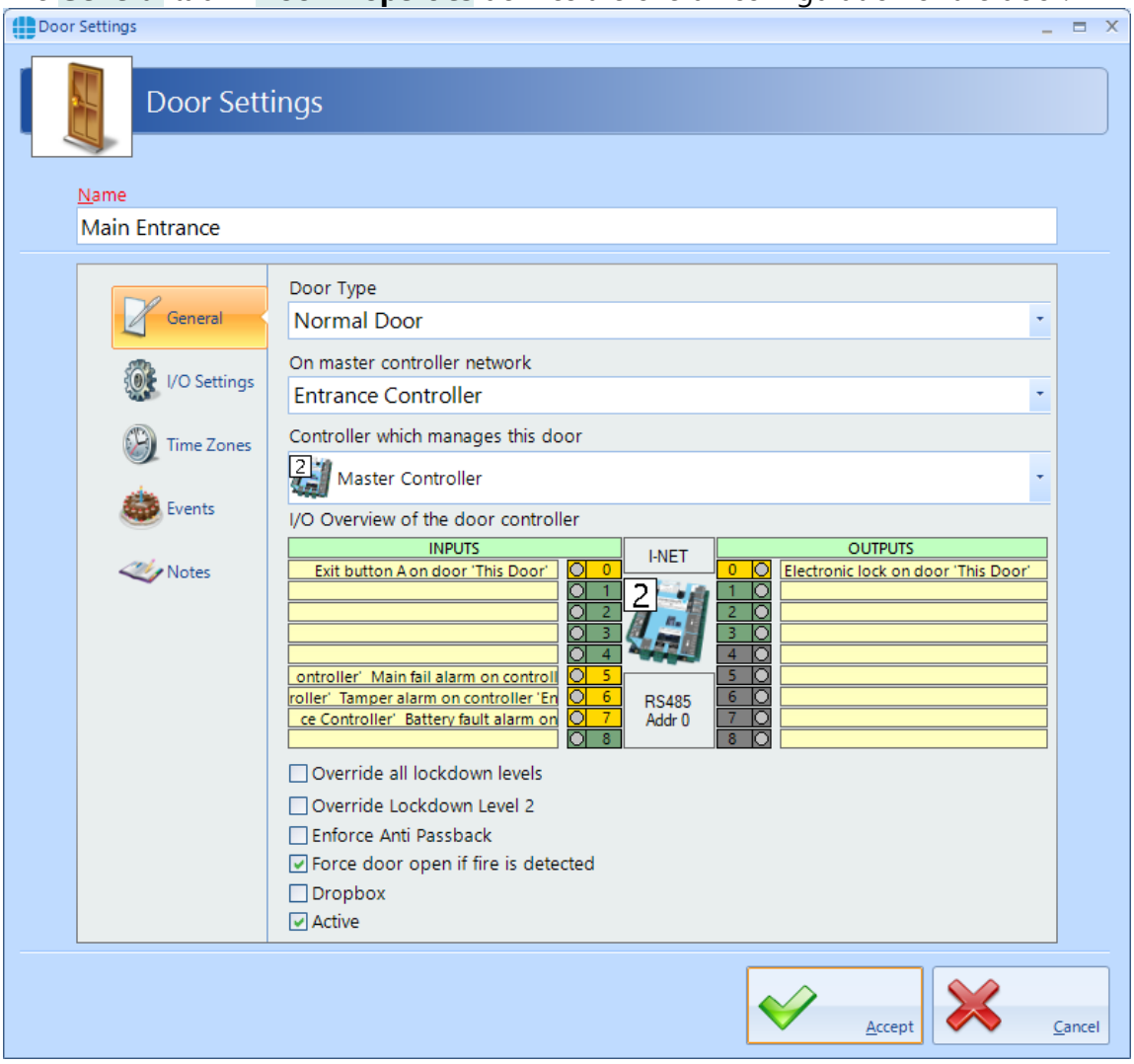
To manually create a new door, click on the **Add** button 

NOTE: Doors can be created using the Door Configuration Wizard in the Controllers screen.

© 2026 Controlsoft Ltd

8.1 Door Properties General

The **General** tab in **Door Properties** defines the overall configuration of the door.



Enter a **Name** (required) to identify the controller.

Enter the **Door Type** selectable between Normal, Turnstile, Airlock and Aperio Door. For more information on Door Types, please refer to Appendix A - Types of Door 289
For simplicity, we will describe the programming required for a Normal Door.

Select **On Master Controller Network** to be the Master Controller for the channel (e.g. Ground Floor)

The option **Controller which manages this door** is the device which is connected to the door (e.g. Master Controller or RS485 Address 1). The icon shows whether the controller is a 1 Door or 2 Door device

The **I/O Overview** of this door gives a quick overview of the inputs and outputs used for the door (not yet configured in this screenshot). NOTE: If using Aperio locks, no I/O is allocated as the functions of lock and REX are handled by the Aperio lock itself. For further information, please refer to Appendix A - Types of Door 289

© 2026 Controlsoft Ltd

The option **Override all lockdown levels** allows this door to continue to operate during Lockdown Level 1 and Level 2

The option **Override Lockdown Level 2** allows this door to continue to operate during Level 2

Select the **Enforce AntiPassBack** option if Anti-Passback is required on this door

If the door needs to be released during a fire alarm, tick **Force door open if fire is detected**.

The **Dropbox** option defines that the door operates in conjunction with a dropbox card collection device.

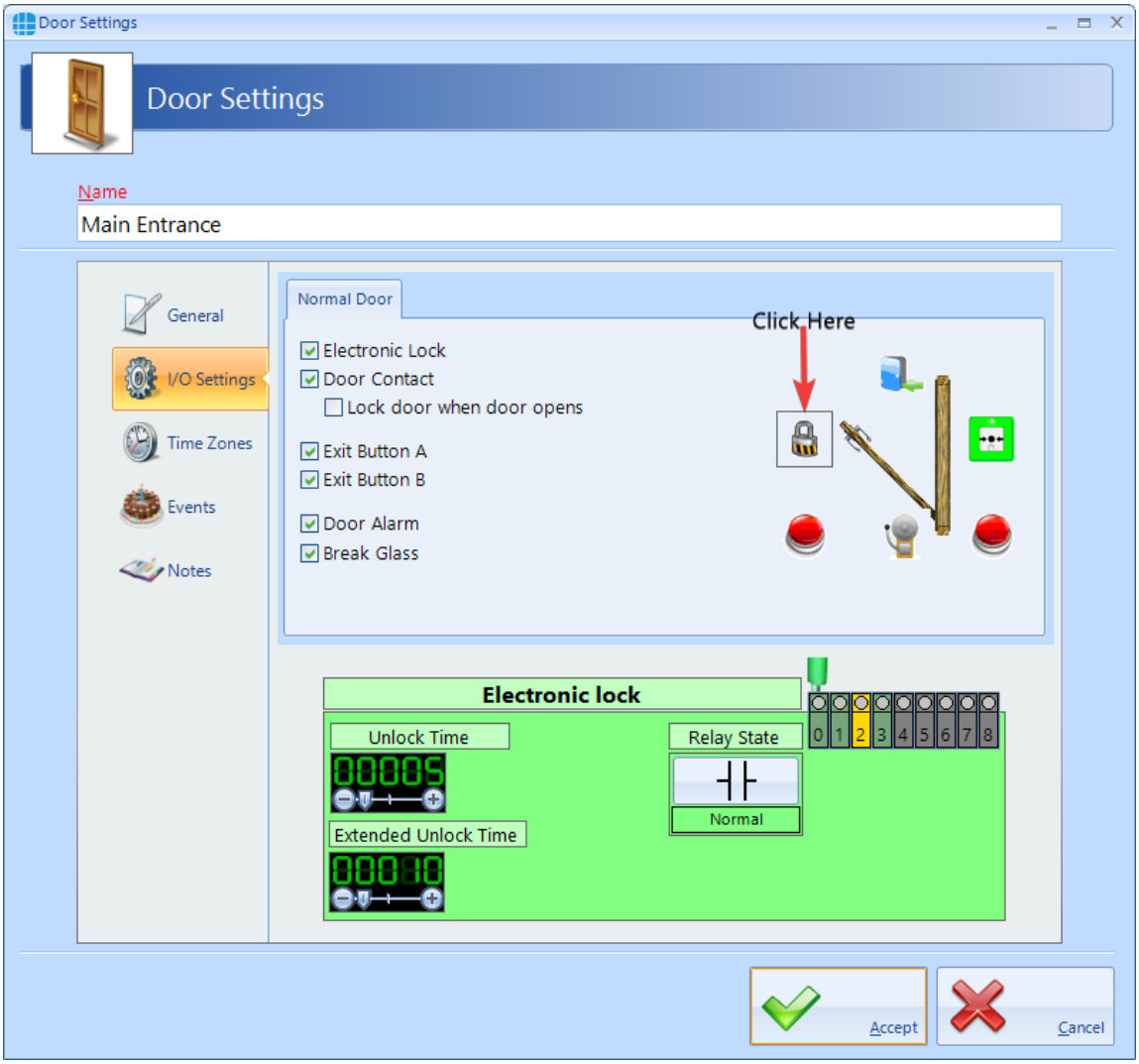
Data for this door will only be downloaded to the controller if the **Active** option is ticked. Un-ticking this option allows doors to be configured where the hardware has not yet been installed.

© 2026 Controlsoft Ltd

8.2 Door Properties I/O Settings

The **I/O Settings** tab, allows door hardware to be configured:

To configure the relay connected to the lock, tick the **Electronic Lock** option, then **click** on the lock icon:



The **Unlock Time** is the duration that the door will remain unlocked, in this instance 5 seconds. If the relay time is set to 0 seconds, the door will "latch", meaning the door will release when a valid token is presented and will re-lock when the next valid token is presented.

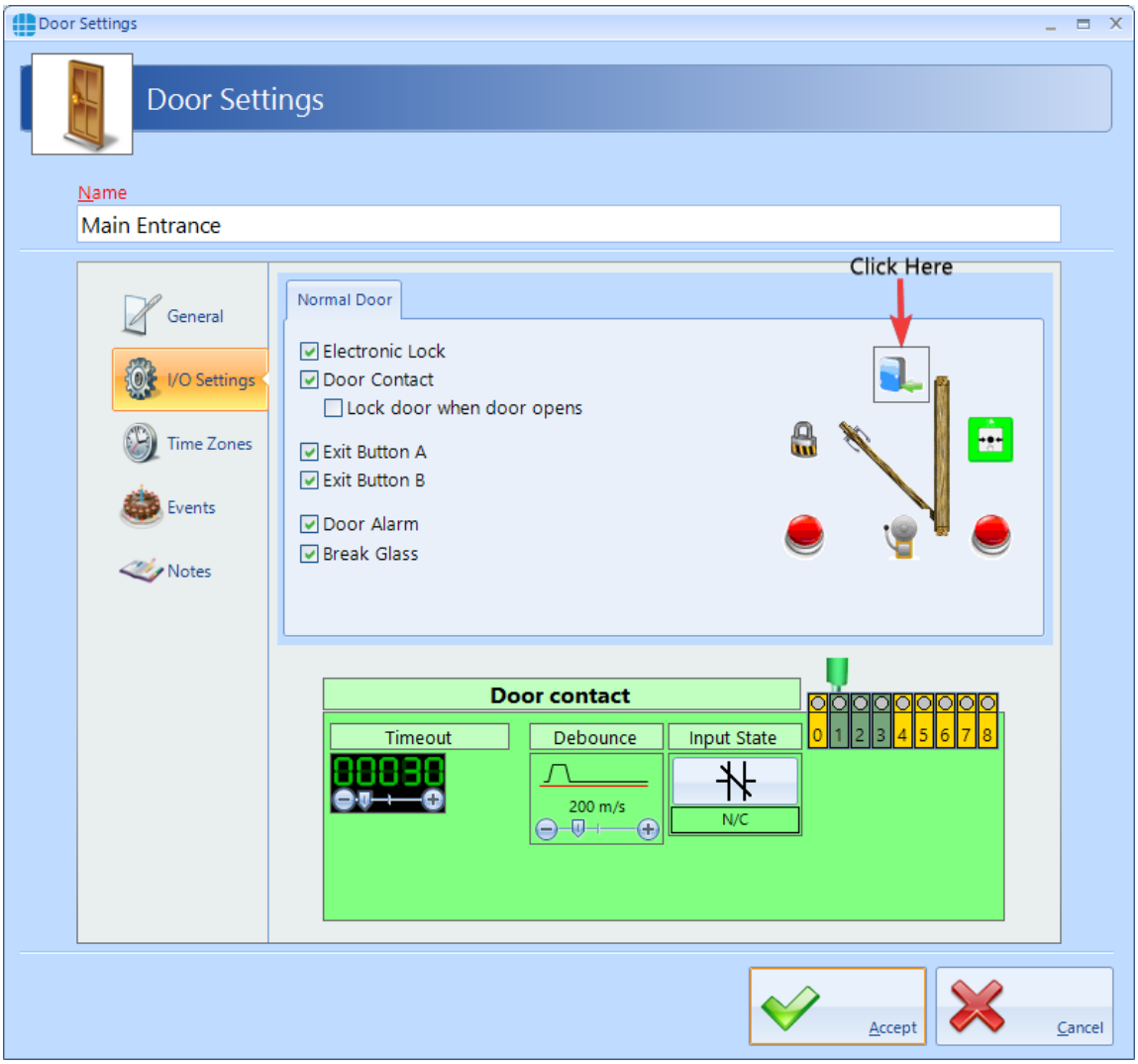
The **Extended Unlock Time** is the duration that the door will remain unlocked for users in a group selected as **Requires Extended Unlock Time.** In this example it will be set to 10 seconds.

If **Relay State** is **Normal**, the relay will be a standard Normally Open / Closed relay. Conversely, **Inverted** will energise the relay and will de-energise the relay on command.

Relay defines which relay is connected to the lock, relay 0 in this instance. If the output has been allocated to another device, the graphic will show orange.

© 2026 Controlsoft Ltd

To configure the input connected to a door contact, tick the **Door Contact** option, then click on the icon:



If the **Lock door when door opens** option is selected, the door is re-locked as soon as the door opens, overriding any remaining Unlock Time.

Timeout is the duration that the door is left open before generating a Door Held alarm (30 seconds in this instance). Maximum value being 1800 seconds (60 minutes)

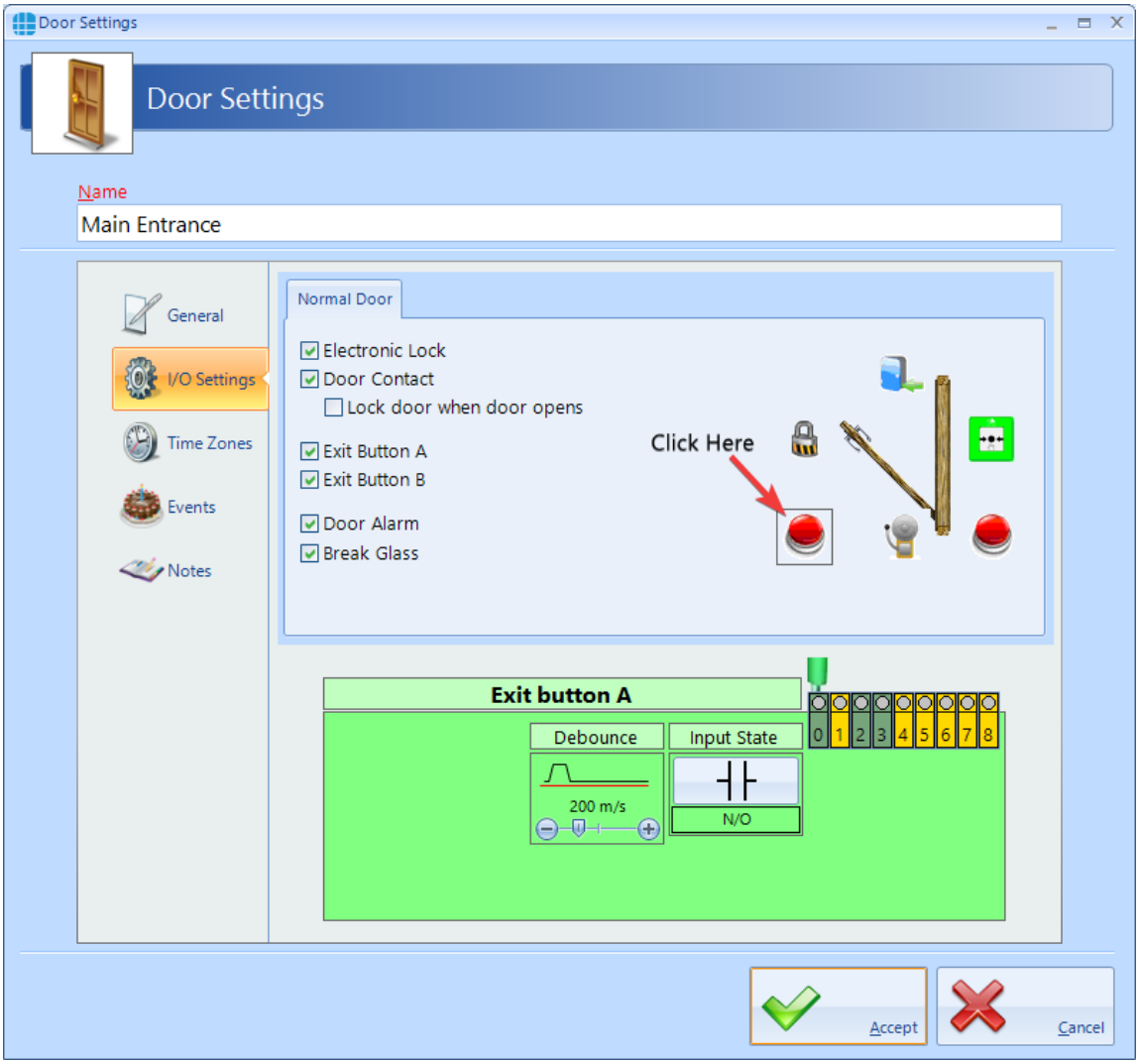
Debounce is a short delay between the door contact opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

Input State should be selected as **N/C** for a Normally Closed door contact, or **N/O** for a Normally Open door contact.

Finally, select the **Input** which is connected to the door contact. If an input has been allocated to another function, the graphic will show yellow, or red if more than one function has been allocated to the input.

© 2026 Controlsoft Ltd

To configure the input connected to a Request to Exit (REX) button, tick the **Exit Button A** option, then click on the icon:



Debounce is a short delay between the door contact opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

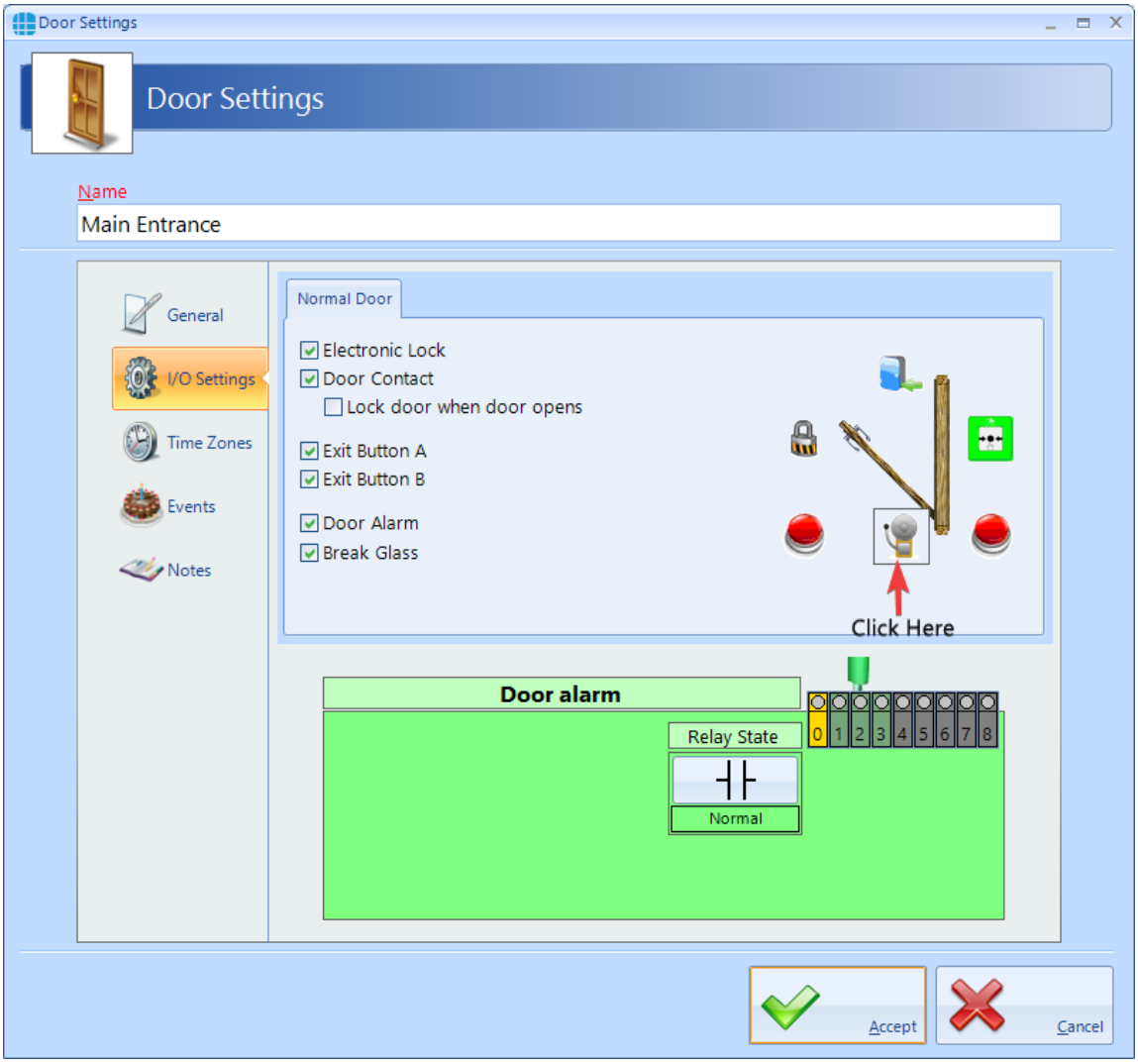
Input State should be selected as **N/C** for a Normally Closed push button, or **N/O** for a Normally Open push button.

Finally, select the **Input** which is connected to the push button. If an input has been allocated to another function, the graphic will show as yellow as shown above, or red if the input has been selected with more than one function.

NOTE: The Identity Access software can support 2 Request to Exit buttons for a single door. This can be useful in a reception area where one is fitted next to the door and another on the receptionist's desk to release the door for visitors.

© 2026 Controlsoft Ltd

To configure a door alarm relay, tick the **Door Alarm** option, then click on the icon:

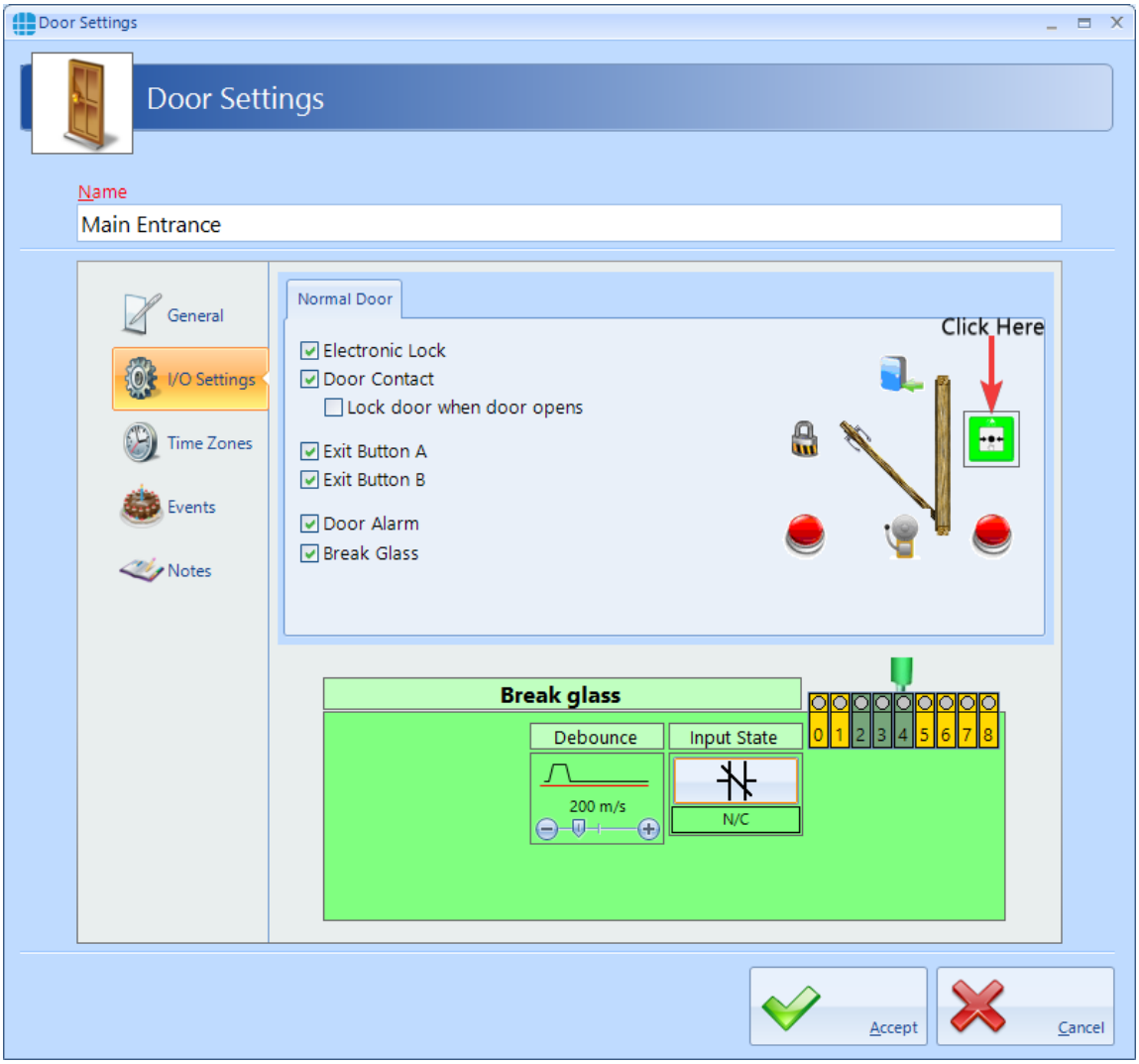


If **Relay State** is **Normal**, the relay will energise to activate the sounder. Conversely, **Inverted** will de-energise the relay to activate the sounder.

Relay defines which relay is connected to the sounder, relay 2 in this instance.

© 2026 Controlsoft Ltd

To configure a Break Glass monitoring input, tick the **Break Glass** option, then click on the icon:



Debounce is a short delay between the contacts opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

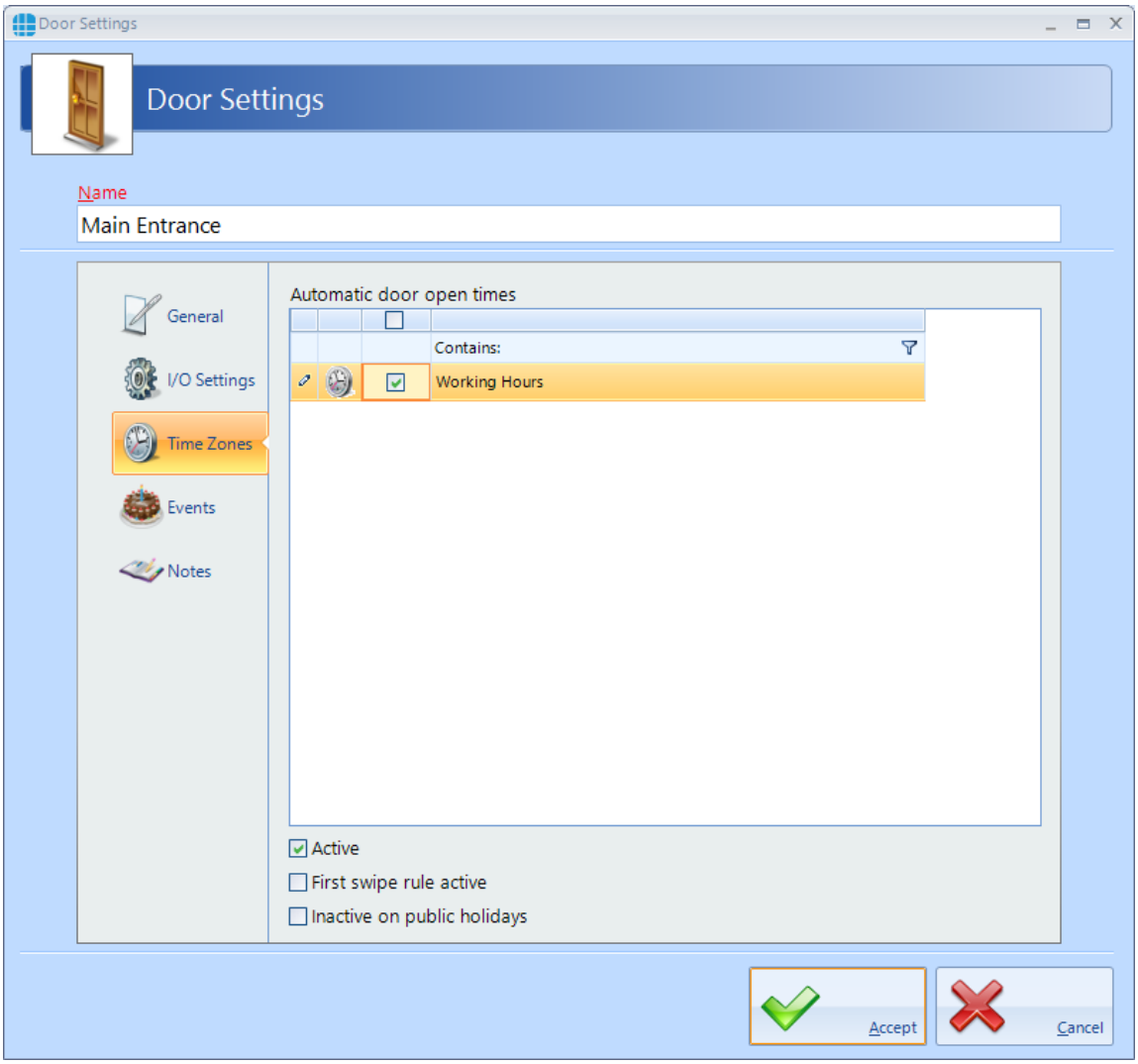
Input State should be selected as **N/C** for a Normally Closed contacts, or **N/O** for Normally Open contacts.

Finally, select the **Input** which is connected to the Break Glass.

© 2026 Controlsoft Ltd

8.3 Door Properties Time Zones

The **Time Zones** tab in the **Door Properties** windows allows the Operator to allocate a Time Zone to a door.



When a Time Zone is allocated to a door, the door will remain unlocked for the duration of that Time Zone.

When one or more Time Zones have been created, they will appear in the **Automatic door open times** window. Simply select the relevant Time Zone to allocate it to that door.

The option **Active** must be selected for the Time Zone to release the door. The door will then release automatically at the selected start time, and relock automatically and the selected end time.

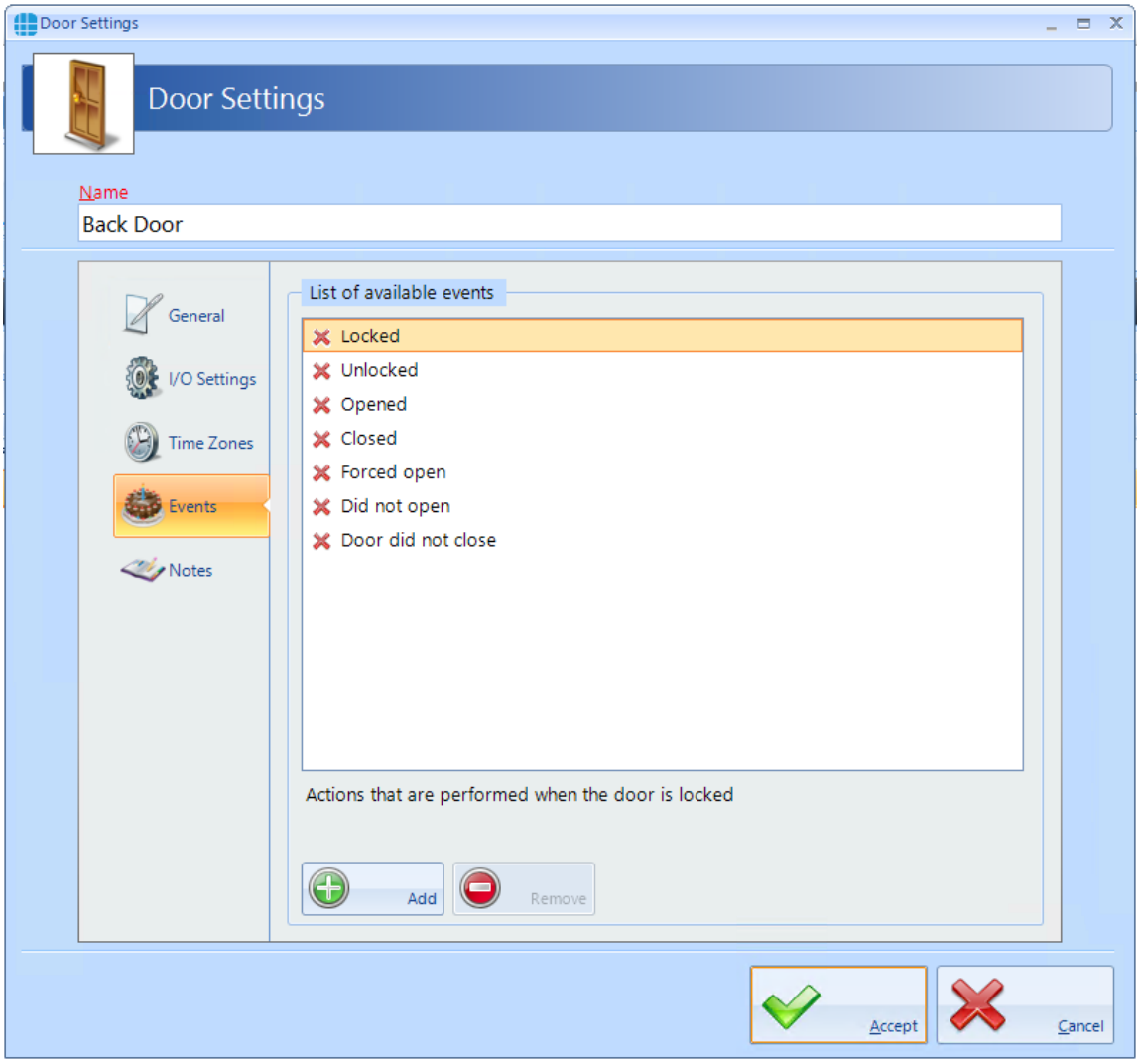
If selected, the **First swipe rule active** option will delay the door from releasing until a valid user opens the door after the start of the Time Zone.

If selected, **Inactive on public holidays** will stop the door from being unlocked by the Time Zone on predetermined days.

© 2026 Controlsoft Ltd

8.4 Door Properties Events

The Events tab will indicate whether any Events have been configured for the selected door.

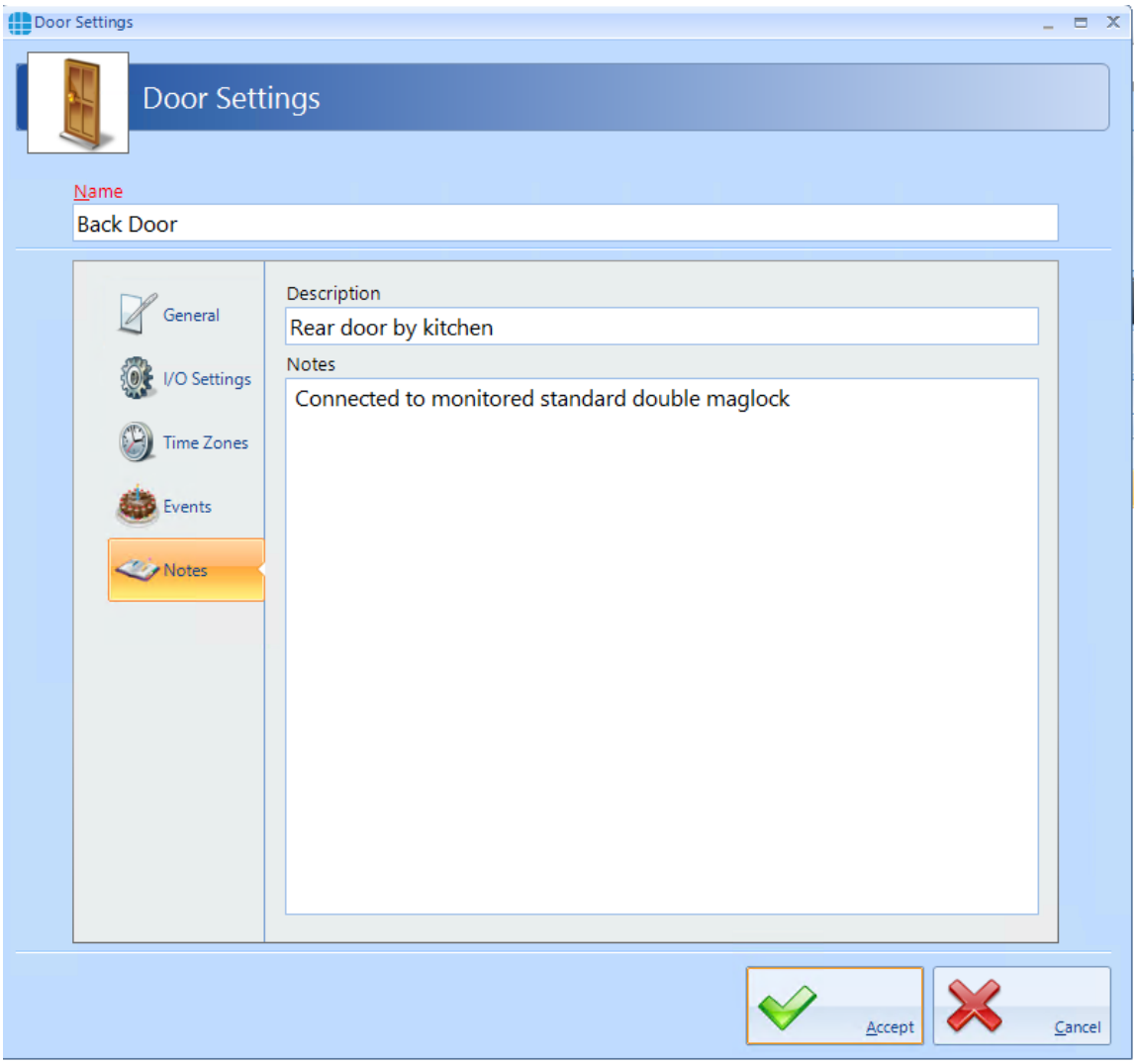


In this example, no Events have been created for the selected door. Clicking the **[Add]** button will allow Events to be created. For more information, see Events Section. 195

© 2026 Controlsoft Ltd

8.5 Door Properties Notes

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

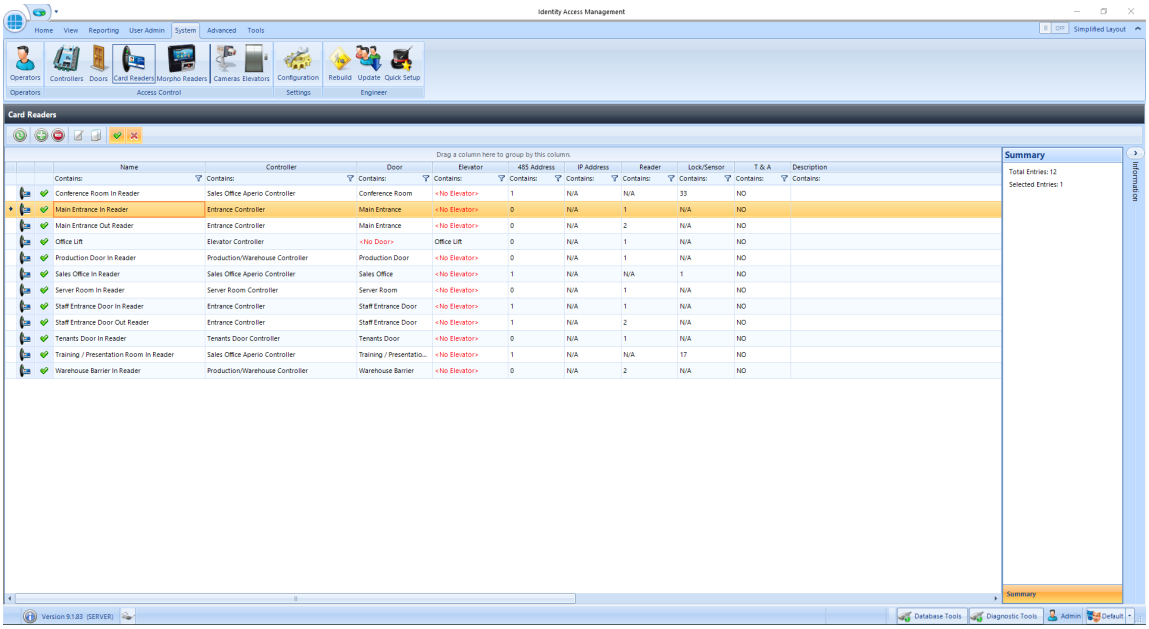


© 2026 Controlsoft Ltd

System > Card Readers

9 System > Card Readers

Within Identity Access, select the **System** tab, then click **Card Readers** in the ribbon bar.



The option buttons are:

 Refresh: Updates the list of readers

 Add: Creates a new reader in the list

 Delete: Removes the selected reader/s from the list

 Edit: edits the selected reader

 Duplicate: Creates a new reader in the list using the selected reader as a template

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

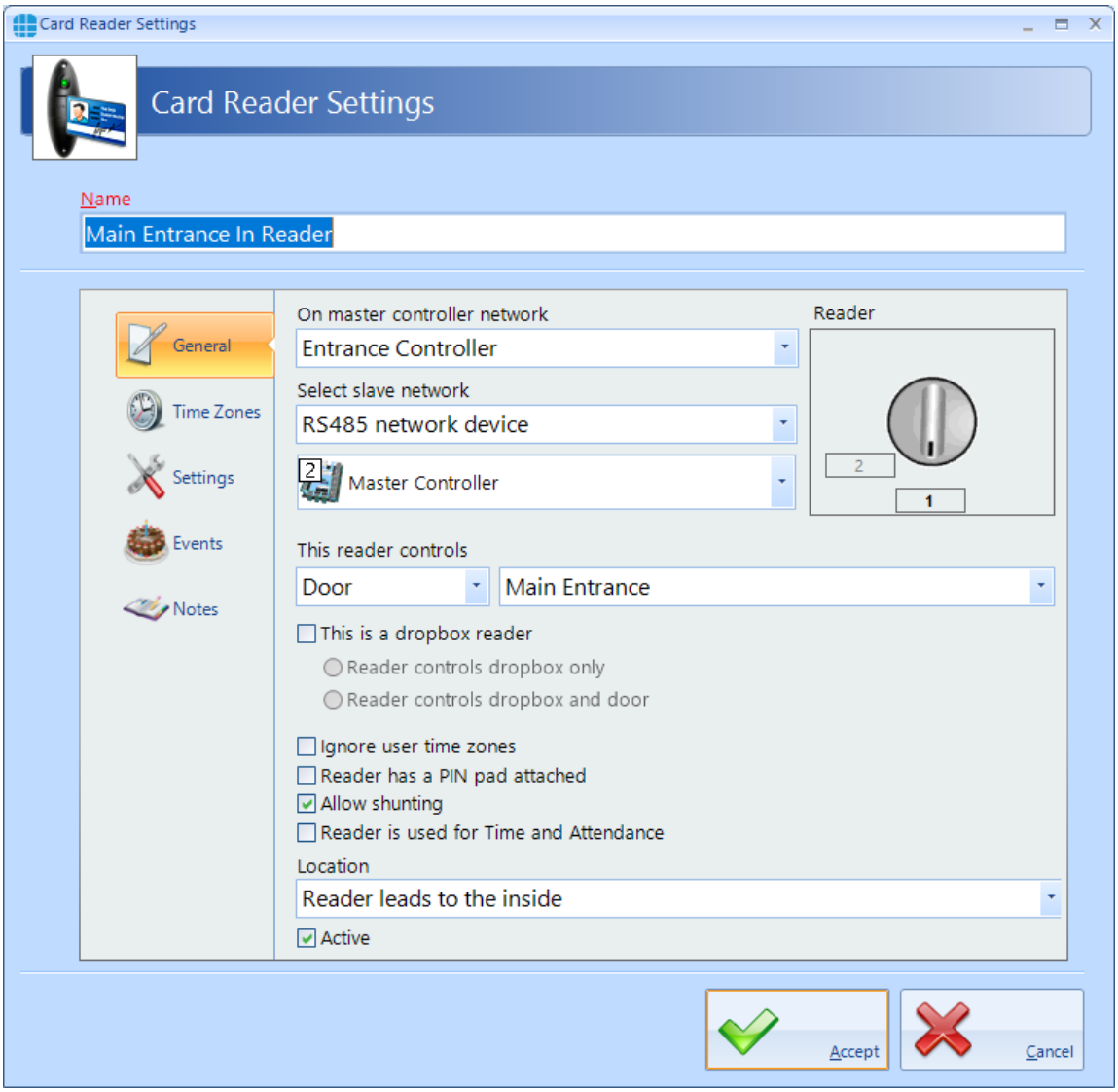
 Show/Hide Inactive: This button will show or hide Card readers not selected as Active.

To create a new reader, click on the Add button  If doors were created with the Door Configuration Wizard, the readers will have been created as well.

© 2026 Controlsoft Ltd

9.1 Card Reader General

The **General** tab in **Card Reader Properties** windows defines the overall configuration of the card reader.



Enter a **Name** for the reader

On master controller network defines which Master Controller controls the reader

Select slave network defines the connection type for the device connected to the reader. For Identity Access v9, this must be set to "RS485 network device". The dropdown box underneath is then used to select the device that the reader is physically connected to (e.g. master Controller, RS485 Address 1).

Reader is the reader port on that device that the reader is connected to

This reader controls defines what the reader controls, a door or an elevator and which door / elevator it controls.

Select **This is a dropbox reader** if the reader is used to activate a Dropbox card collector. This has options for **Reader controls dropbox only** (i.e. simply opens the

© 2026 Controlsoft Ltd

Dropbox) or **Reader controls dropbox and door** (i.e. releases the door once card has been collected)

Ignore user time zones should be ticked for OUT readers to ensure that employees can exit the area outside any relevant time zones.

Reader has a PIN pad attached must be ticked if the reader has an integral keypad and two factor authentication is required. ***NOTE: When using a keypad reader with a PIN of 4 or fewer digits, use the # key to denote then end of the PIN. Example if your PIN is 1234, enter 1234#. If your PIN is 12345, enter 12345 with no # key.***

Allow shunting speeds up the operation of the reader by not having to wait for the door to close before the reader can be used a second time.

If the card reader is to be used for Time & Attendance, select the **Reader is used for Time and Attendance** option and select **Location** as "Inside to Outside" or "Outside to Inside" as appropriate.

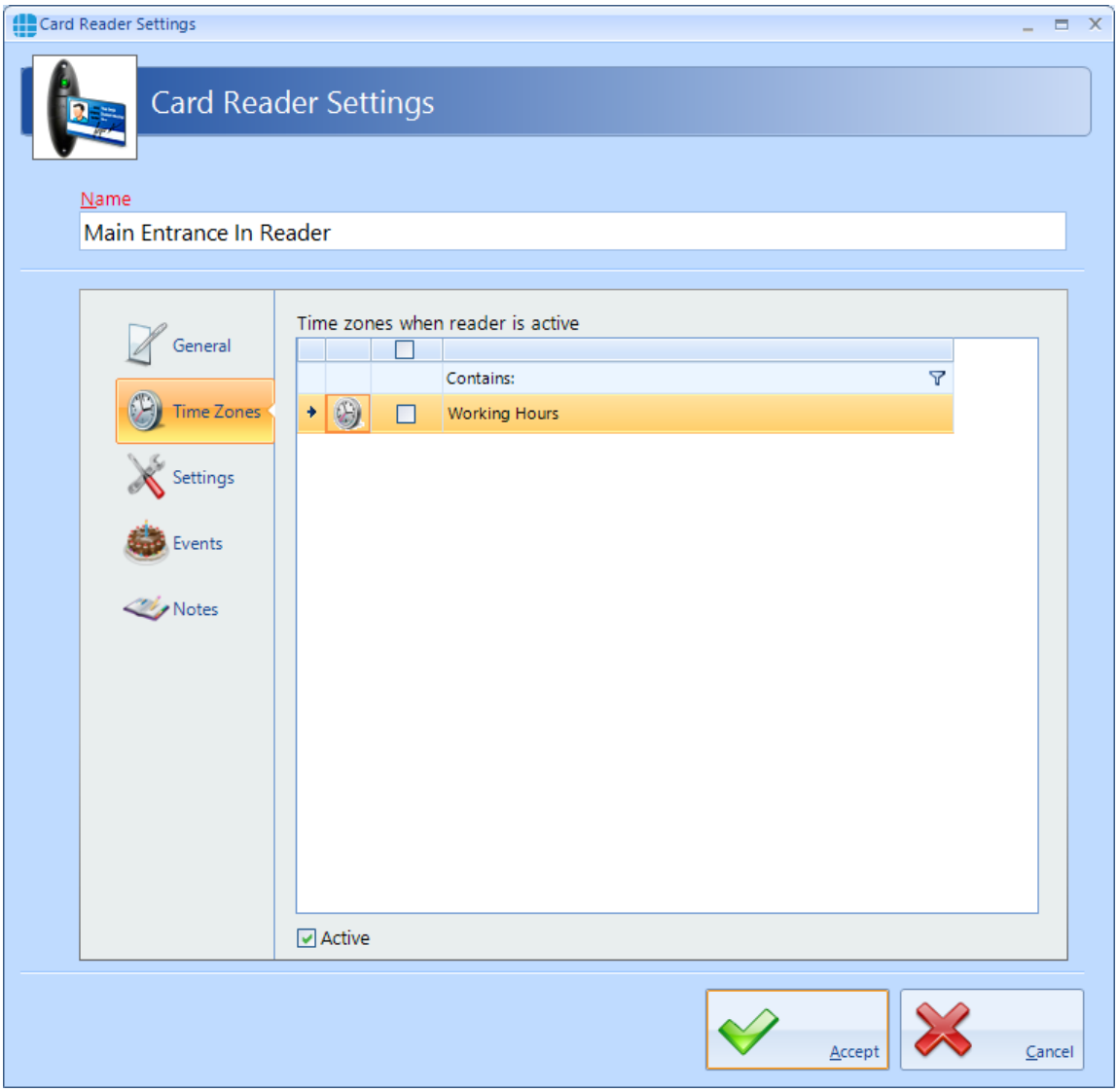
Location defines whether the reader transfers the user from being Inside to Outside, or from being Outside to Inside. This information is used to update the Dashboard, for fire roll call reports to define who is inside the building in the event of a fire alarm and for Time & Attendance.

Active must be ticked if the hardware is fitted. If this is not ticked, data for the reader will not be transmitted to the controller.

© 2026 Controlsoft Ltd

9.2 Card Reader Time Zones

The **Time Zones** tab in the **Card Reader Properties** windows allows the Operator to allocate a Time Zone to a reader.



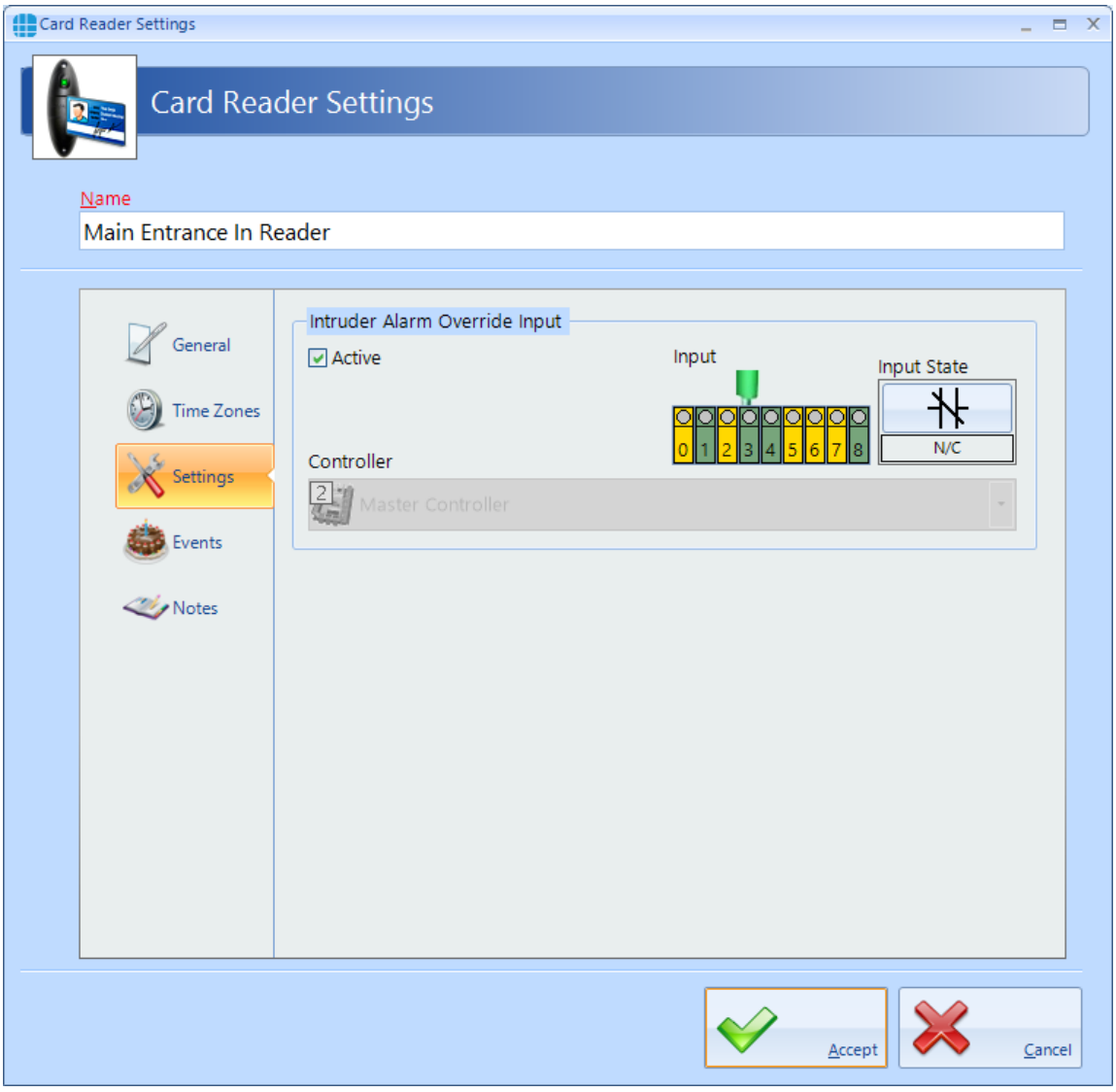
When one or more Time Zones exist, they will appear in the **Time zones when reader is active window**. Simply select the required Time Zone to allocate to the reader.

NOTE: Controlsoft do not recommend allocating a Time Zone to a card reader except in exceptional circumstances, as during the Time Zone, NOBODY would be able to access the door. It is preferable to allocate Time Zones to Users, whereby some users (e.g. Keyholders for the Intruder Alarm system) can access the door at any time in the event of an emergency.

© 2026 Controlsoft Ltd

9.3 Card Reader Settings

The **Settings** tab allows an input to be configured to disable the reader when an external contact activates (e.g. to disable a reader if the intruder alarm on the other side of the door is armed).



Select **Active** to allow the input to disable the reader

Select the appropriate **Input** connected to the external contact.

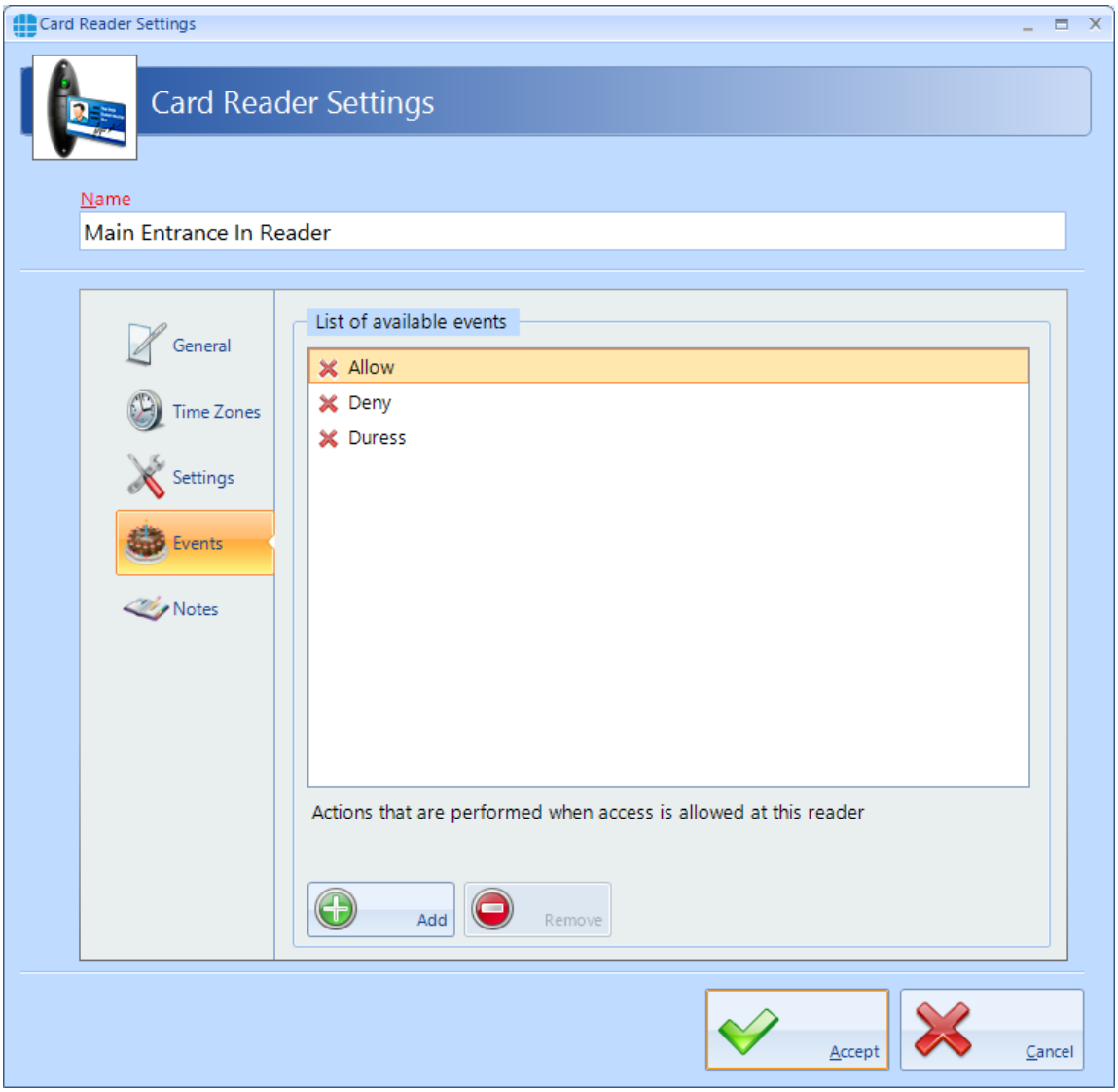
Select the **Input State** as **N/C** if the input is connected to a Normally Closed contact, or **N/O** if the input is connected to a Normally Open contact.

Controller defines which controller's input is used.

© 2026 Controlsoft Ltd

9.4 Card Reader Events

The Events tab will indicate whether any Events have been configured for the selected reader.

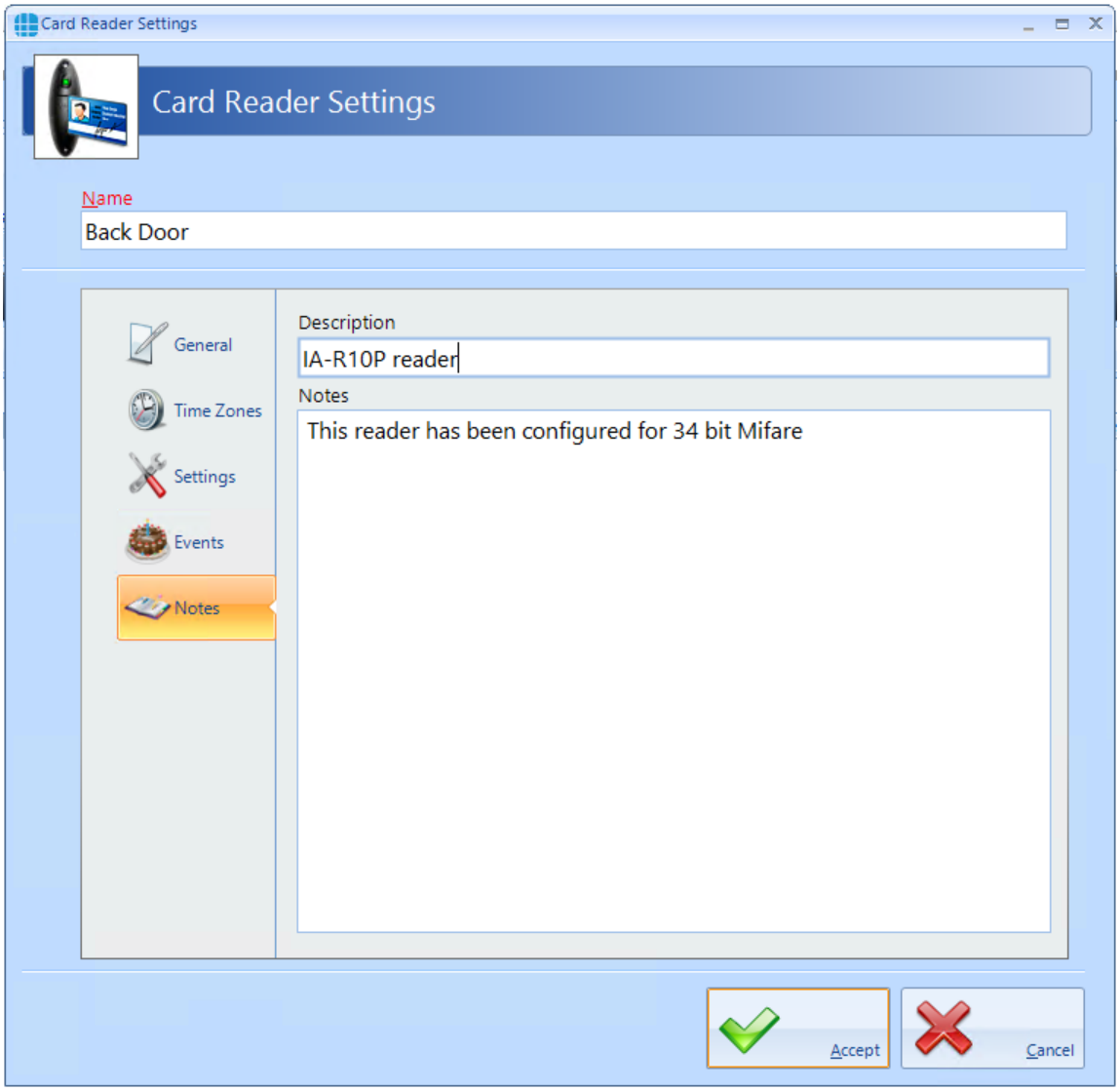


In this example, no Events have been created for the selected reader. Clicking the **[Add]** button will allow Events to be created. For more information, see Events Section. 195

© 2026 Controlsoft Ltd

9.5 Card Reader Notes

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.



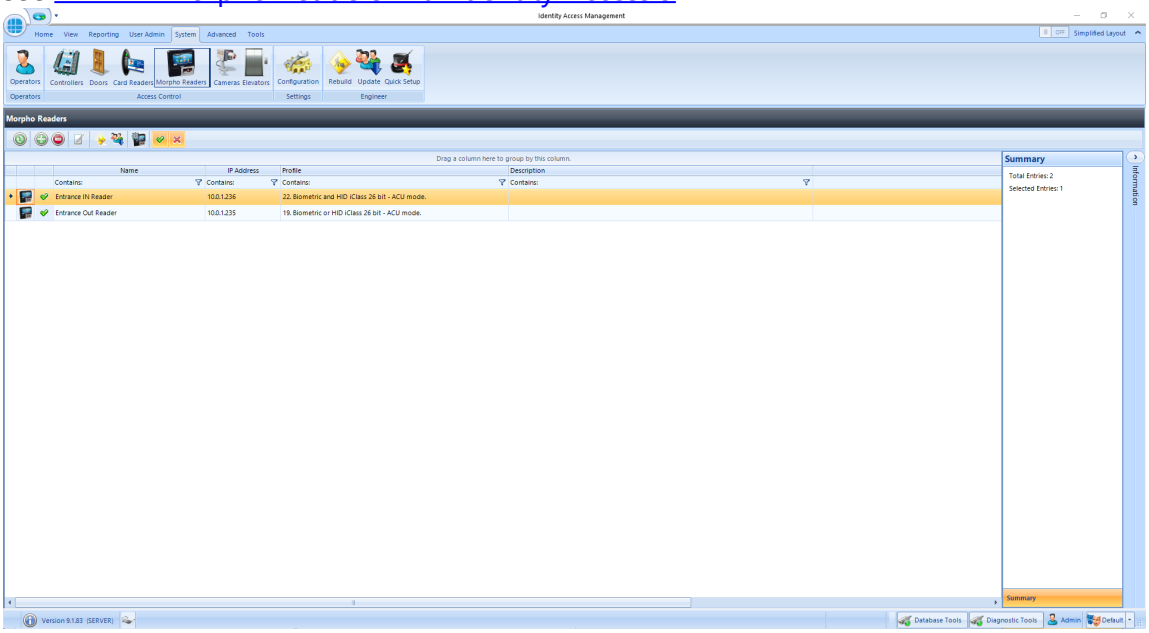
© 2026 Controlsoft Ltd

System > Morpho Readers

10 System > Morpho Readers

Within Identity Access, select the **System** tab, then click **Morpho Readers** in the ribbon bar.

For full information on how to setup Idemia Morpho readers within Identity Access, see IDEMIA Morpho Readers with Identity Access 9



The option buttons are:

 Refresh: Updates the list of readers

 Add: Creates a new reader in the list

 Delete: Removes the selected reader/s from the list

 Edit: edits the selected reader

 Rebuild: Initiates a full download to the selected Morpho readers

 Incremental Download: Initiates an Incremental Download to the selected Morpho readers

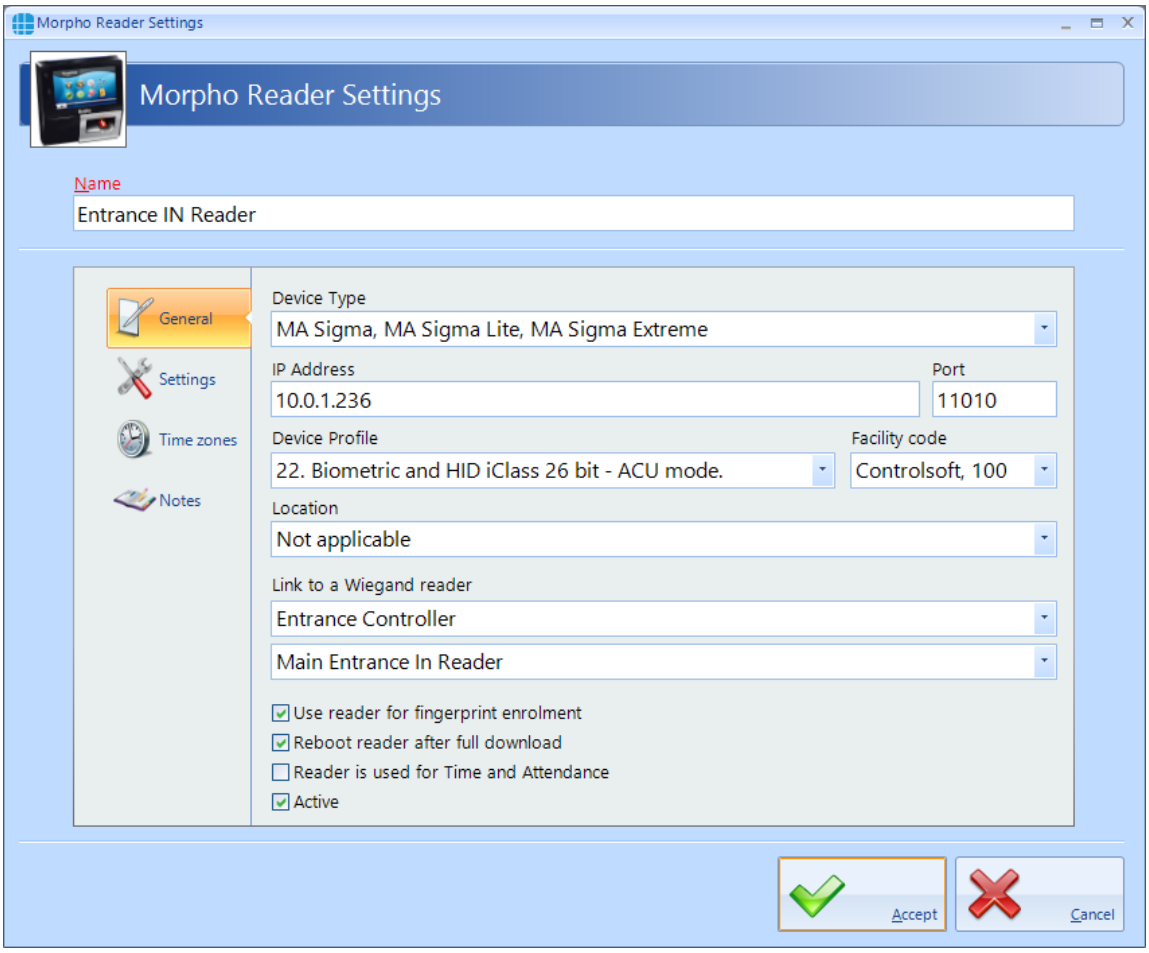
 Morpho Configurator: Opens the Morpho Configurator utility

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

© 2026 Controlsoft Ltd

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

10.1 Morpho Reader General



Enter a **Name** to identify the Morpho reader

Device Type identifies the type of Morpho reader in use, for example an MA SIGMA or J-Series

Enter the **IP Address** of the Morpho Reader and its **Port**

Select the relevant **Device Profile** from the dropdown list. Options have been provided to cover all common configurations. For custom Device Profiles, see IA Configuration - Biometrics 256

Facility Code should be set to the relevant Facility Code for that site.

© 2026 Controlsoft Ltd

Location defines whether the Morpho reader transfers the user from being **Inside to Outside**, or from being **Outside to Inside**. This information is used to update the Dashboard, for fire roll call reports to define who is inside the building in the event of a fire alarm and for Time & Attendance.

Use the **Link to a Wiegand reader** section to link the Morpho reader with a card reader on the system. If a Standalone device (i.e. without the need of an iNet access control unit) profile is selected, this section will not be displayed.

Use reader for fingerprint enrolment is used if the reader is to be used for enrolling fingerprints.

Reboot reader after full download will reboot the reader following a download.

If the Morpho reader is to be used for Time & Attendance, tick the **Reader is used for Time and Attendance** option and select the relevant **Location** option.

Active must be ticked if the hardware is fitted. If this is not ticked, data for the reader will not be transmitted to the controller.

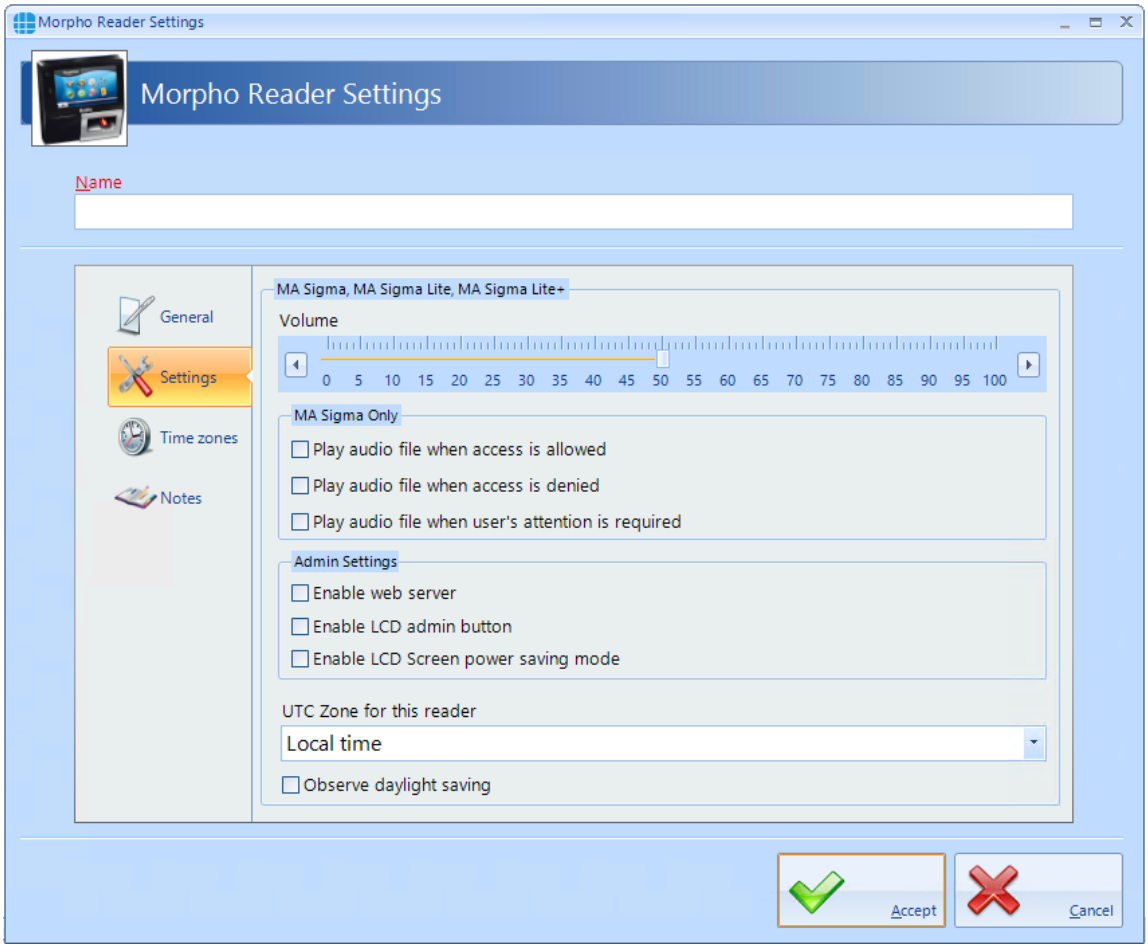
NOTE: With Identity Access v9 and later it is not necessary to edit the Default Morpho profile in the Server Configuration utility for Morpho readers to work correctly.

NOTE: Following an upgrade from Identity Access v8 or earlier, the profiles for the Morpho readers may default to "02. Biometric Only - Standalone Mode". Please ensure that you check the profile for each Morpho reader and select the appropriate profile.

© 2026 Controlsoft Ltd

10.2 Morpho Reader Settings

The **Settings** section, accessed from the side bar, allows options for the MA Sigma and MA Sigma Lite to be selected .



The **Volume** setting adjusts the volume of the selected reader

The MA Sigma allows audio files to be played under various conditions. These can be enabled or disabled by slecting **Play audio file when access is allowed**, **Play audio file when access is denied** and **Play audio file when user's attention is required**.

The **Admin Settings** enable the web server and admin screen as required

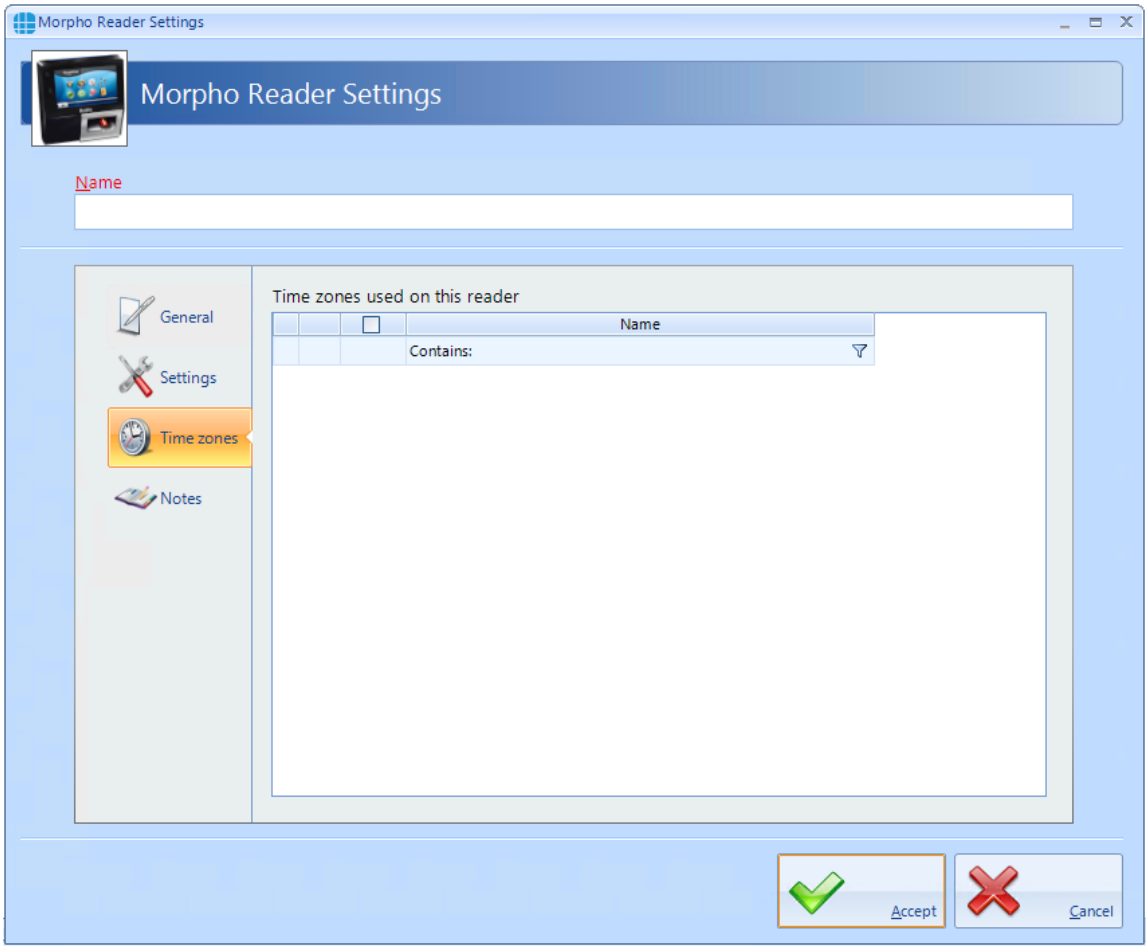
UTC Zone for this reader allows for readers to be used in different International Time Zones.

If **Observe daylight saving** is ticked, the Morpho reader will change its internal time based on daylight saving rules.

© 2026 Controlsoft Ltd

10.3 Morpho Reader Time Zones

The **Time Zones** tab allows the Operator to allocate a Time Zone to a Morpho reader.

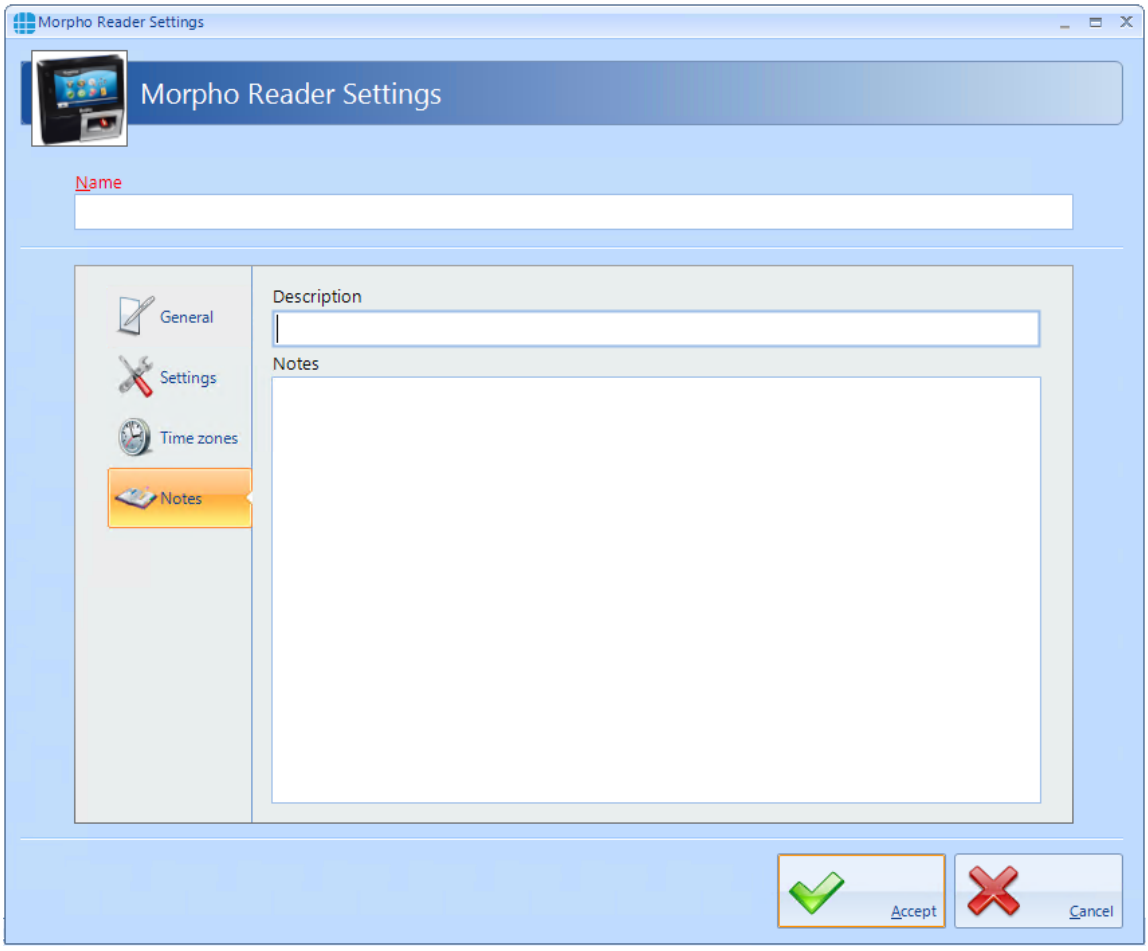


NOTE: Controlsoft do not recommend allocating a Time Zone to a Morpho reader except in exceptional circumstances, as during the Time Zone, NOBODY would be able to access the door. It is preferable to allocate Time Zones to Users, whereby some users (e.g. Keyholders for the Intruder Alarm system) can access the door at any time in the event of an emergency.

© 2026 Controlsoft Ltd

10.4 Morpho Reader Notes

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.



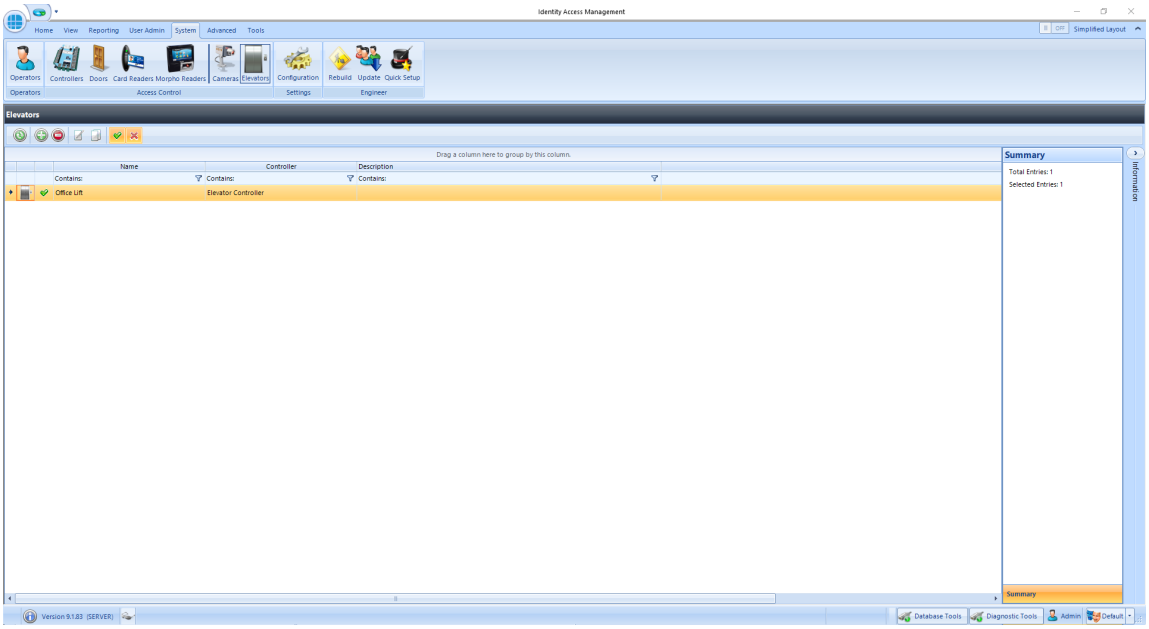
© 2026 Controlsoft Ltd

System > Elevators

11 System > Elevators

Identity Access is capable of interfacing with a Elevator Controller to provide restricted access to individual floors. The elevator must be fitted with a reader inside the cab, connected to a Master controller and I/O expanders to provide one relay output per floor. These relays are then connected to the Lift Control Unit. The maximum number of floors per Master controller is 64. For more information on setting up elevators, see Elevator Controls in Identity Access 9

Within Identity Access, select the **System** tab, then click **Elevators** in the ribbon bar.



The option buttons are:

 Refresh: Updates the list of readers

 Add: Creates a new reader in the list

 Delete: Removes the selected reader/s from the list

 Edit: edits the selected reader

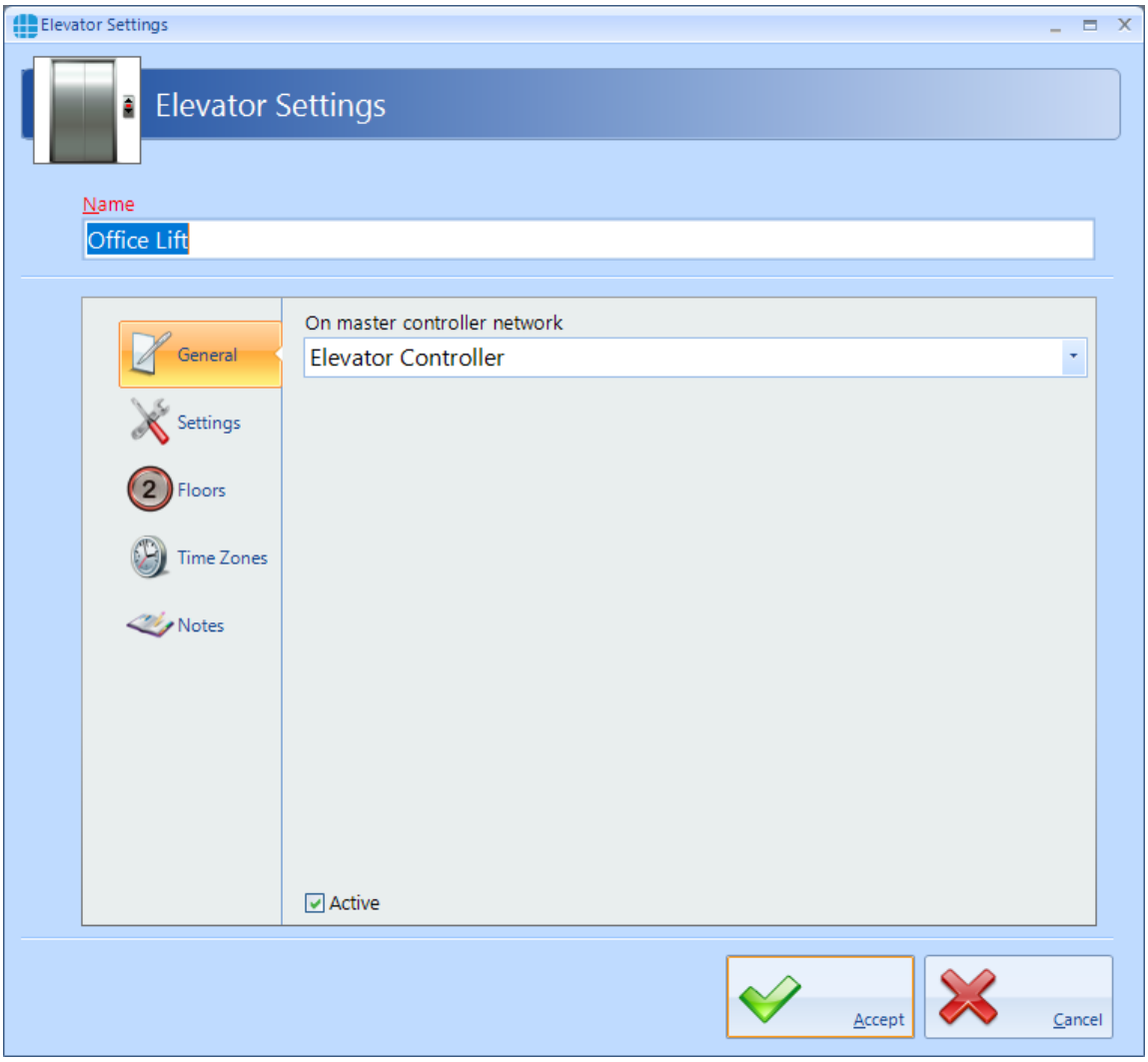
 Duplicate: Creates a new reader in the list using the selected reader as a template

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

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

© 2026 Controlsoft Ltd

11.1 Elevators General



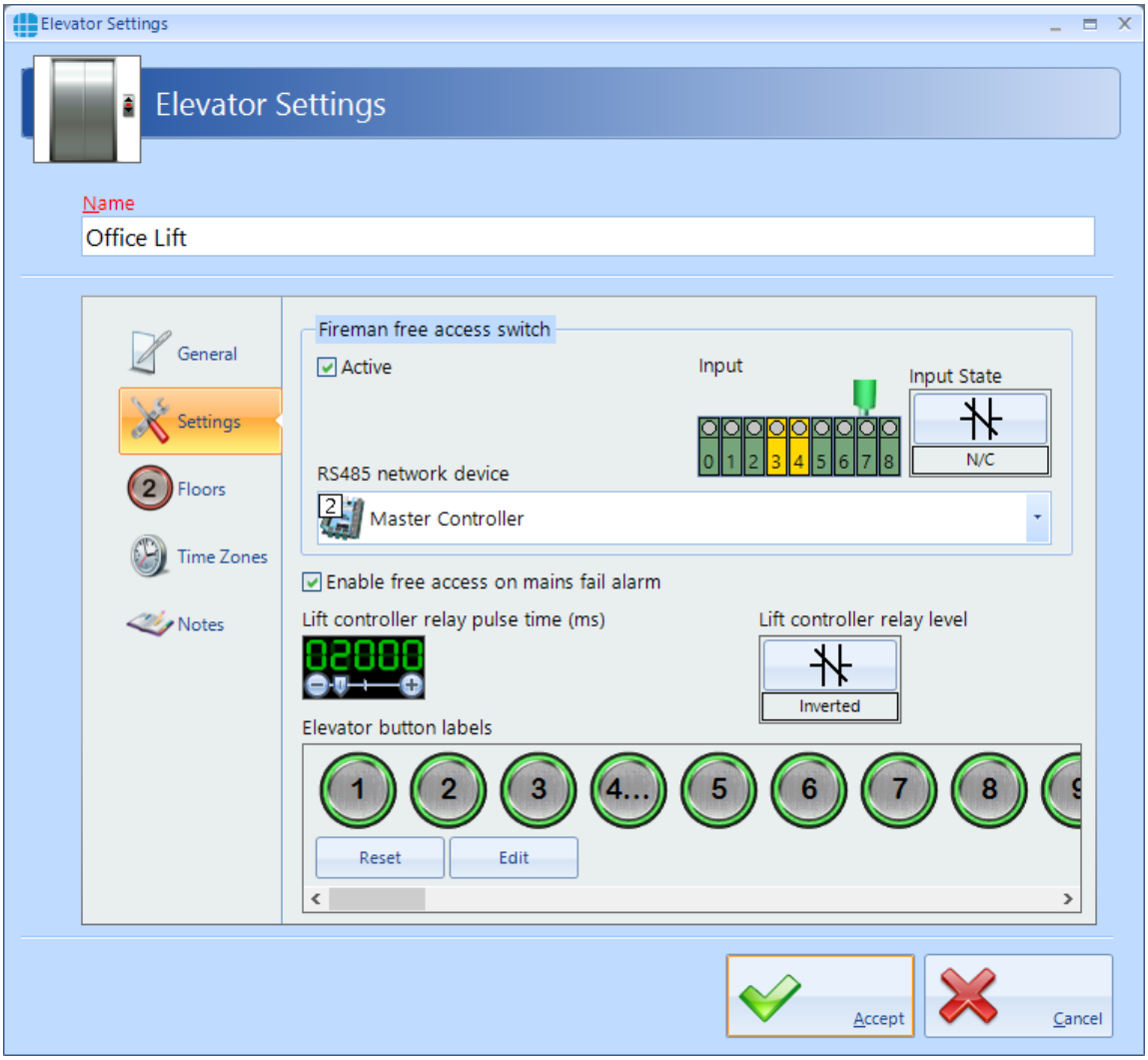
Enter a **Name** to identify the Elevator

On master controller network defines which Master Controller controls the Elevator.

© 2026 Controlsoft Ltd

11.2 Elevators Settings

The **Settings** tab, certain attributes of the Elevator to be defined:



A **Fireman's free access switch** will allow access to all floors when the switch is operated. The options available are:

- **Active** enables the switch
- **Input** defines which input the switch is connected to
- **Input State** defines whether the switch uses Normally Closed or Normally Open contacts
- **RS485 network device** defines which device the switch is physically connected to

Enable free access on mains fail alarm will allow access to all floors when the system detects a Mains Fail.

Lift controller relay pulse time (ms) defines how long the relay pulses for to activate the lift controller. ***NOTE: This timer is in milliseconds, so a value of 1000 will pulse the relay outputs for 1 second***

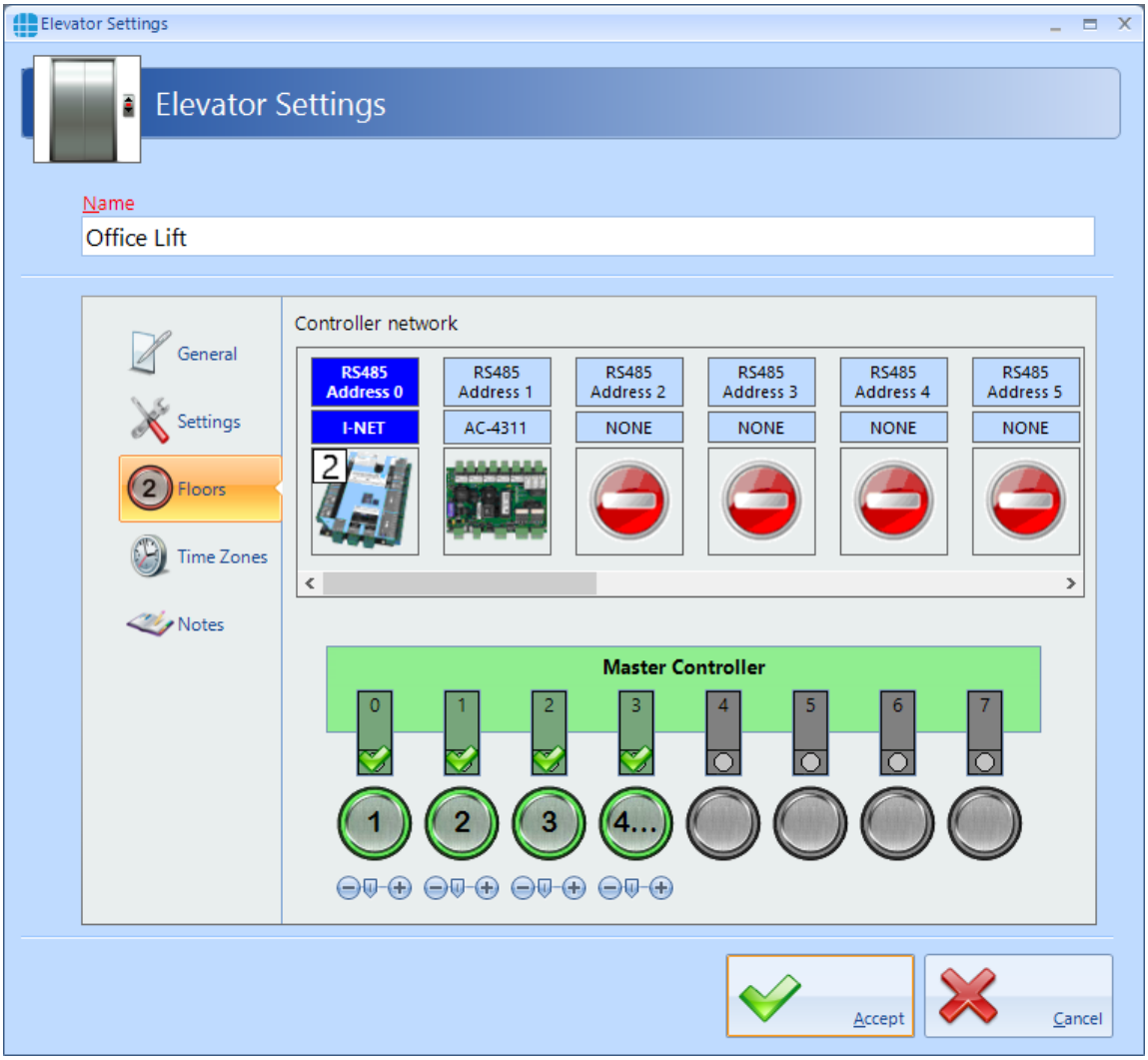
© 2026 Controlsoft Ltd

Lift controller relay level defines whether the relay outputs are Normal or Inverted

Elevator button labels allows text to be entered to make the next stage in the programming easier (e.g. change '1' to Gnd')

11.3 Elevators Floors

The **Floors** tab, defines the relay outputs are used for each floor:

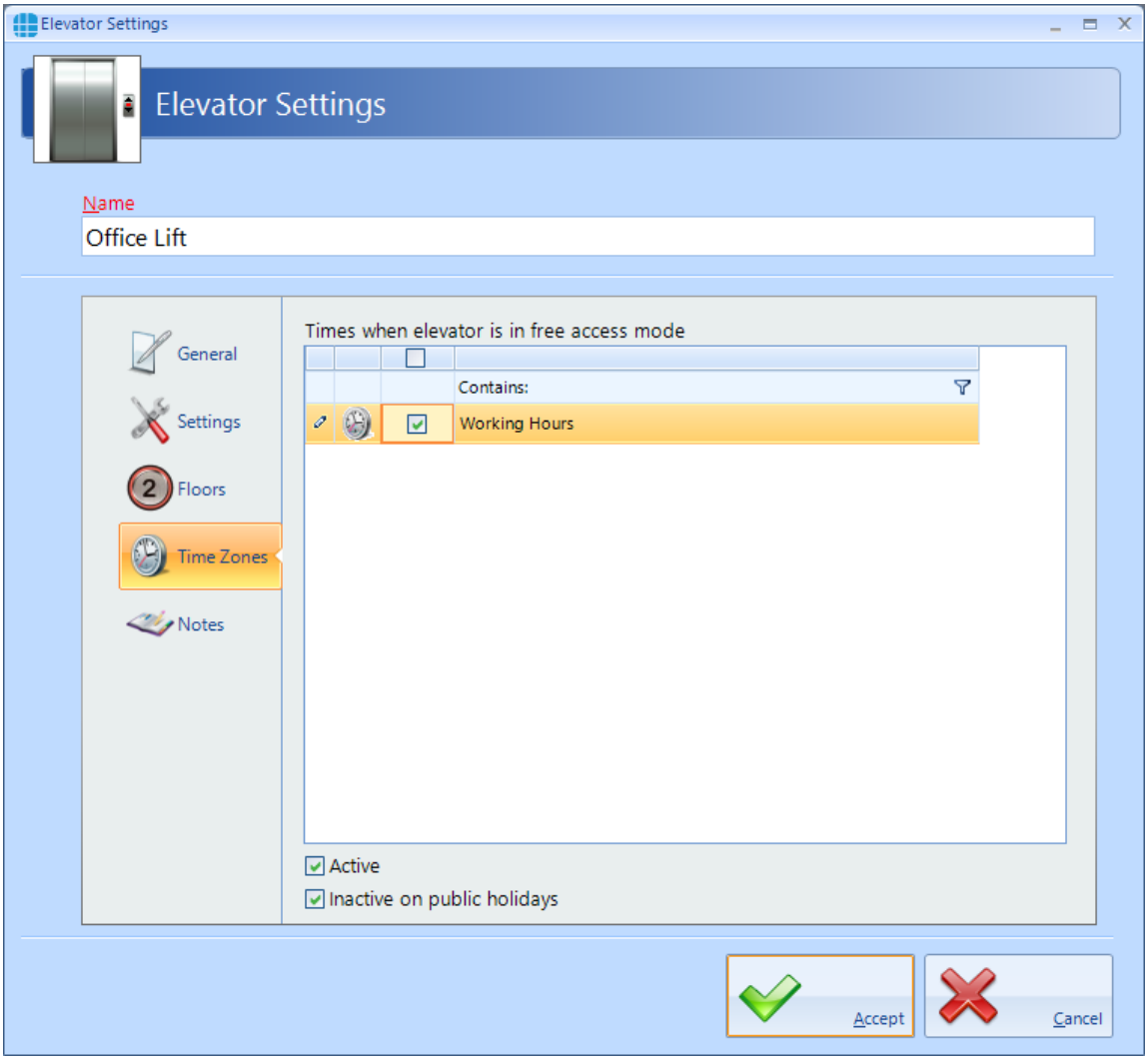


Select each output and its associated floor will be the next available floor. This can be changed if required by using the + and - symbols

11.4 Elevators Time Zones

Time Zones can be allocated to the elevator to provide free access to all floors during the time zone period.

© 2026 Controlsoft Ltd



Active must be enabled for the time zone to work.

If **Inactive on public holidays** is ticked, the elevator will not provide free access during the time zone period during any defined public holidays

© 2026 Controlsoft Ltd

System > DropBox

12 System > DropBox

A DropBox is a device usually used in conjunction with a Turnstile to collect cards when users (usually Visitors or Contractors) leave site at the end of the day. The operation is as follows:

On egress, the Visitor present their card to the DropBox reader. This then opens a flap in the DropBox to allow the visitor to deposit their card . When the internal card sensor sees the card enter the DropBox, the turnstile is activated to allow egress.

For further information on configuring DropBox, please contact Controlsoft Technical Support.

© 2026 Controlsoft Ltd

User Admin > Time Zones

13 User Admin > 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 the following ways:

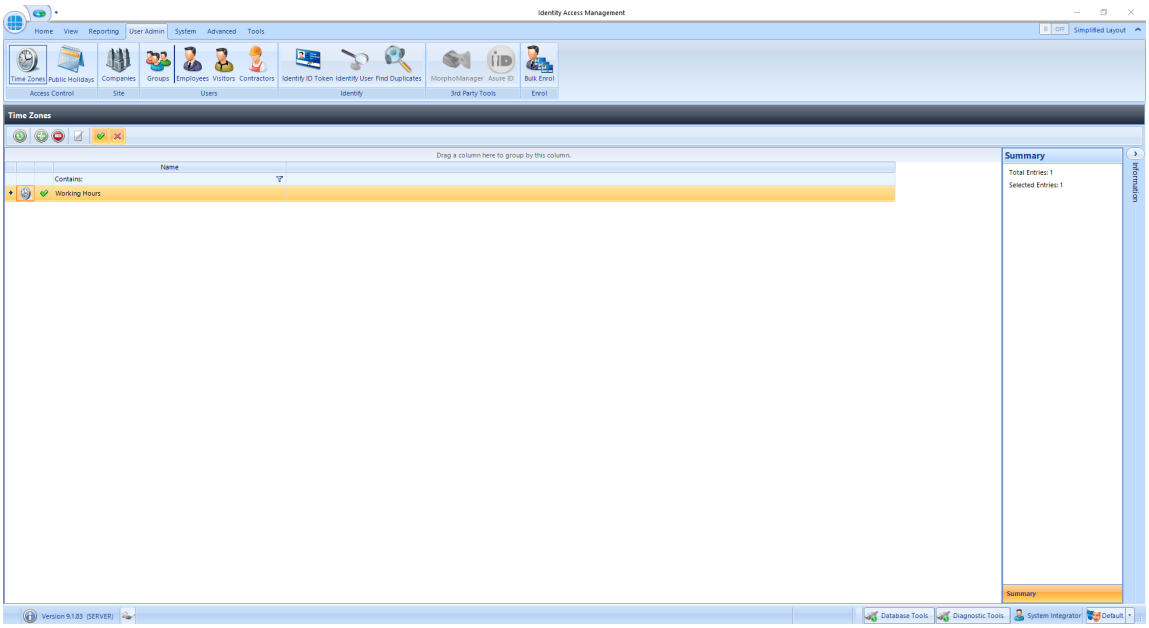
If a Time Zone is allocated to a Group, all Users in that Group will have access through the relevant doors only within the Time Zone period

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

If a Time Zone is allocated to an Elevator, the elevator is on free access within the Time Zone Period.

For general setup advise, Time Zones in the Express Commissioning section 31

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



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.

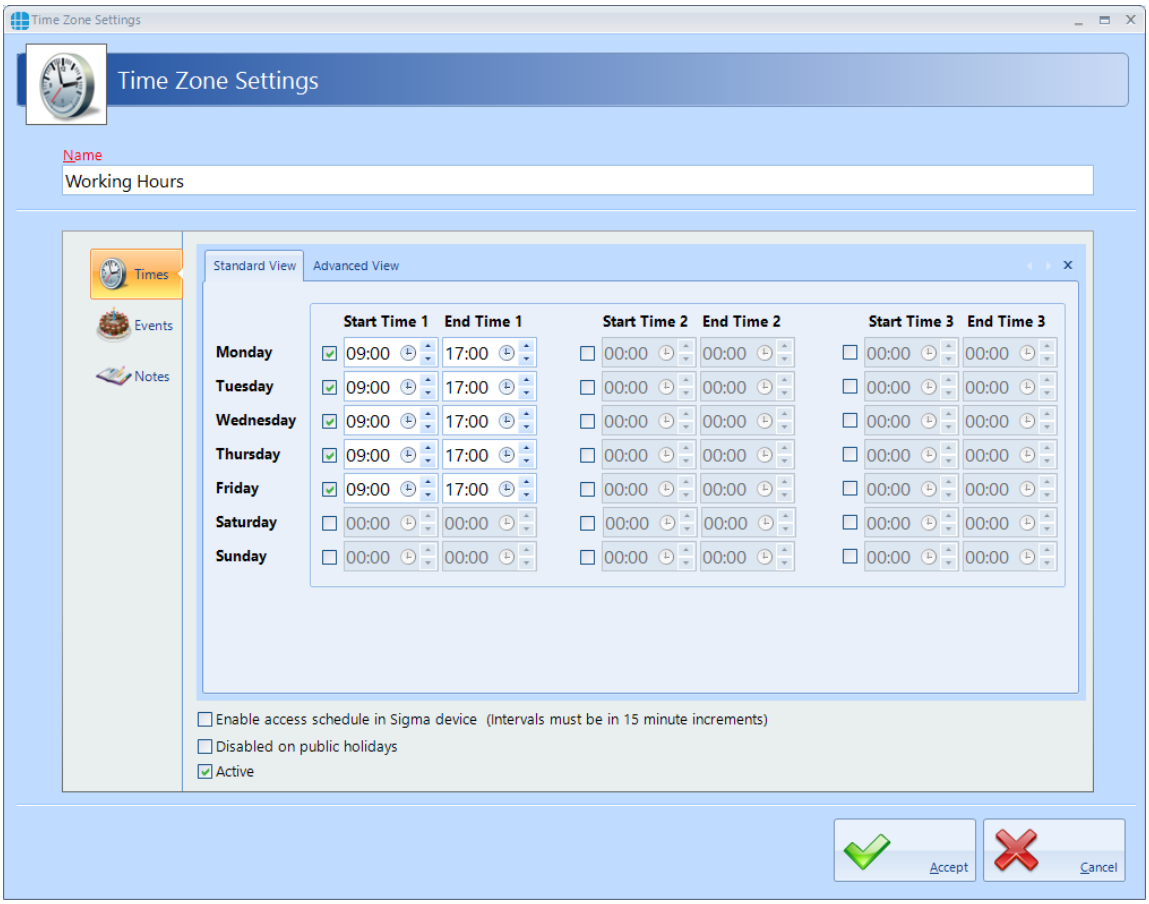
© 2026 Controlsoft Ltd

 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 

13.1 Time Zones Times

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

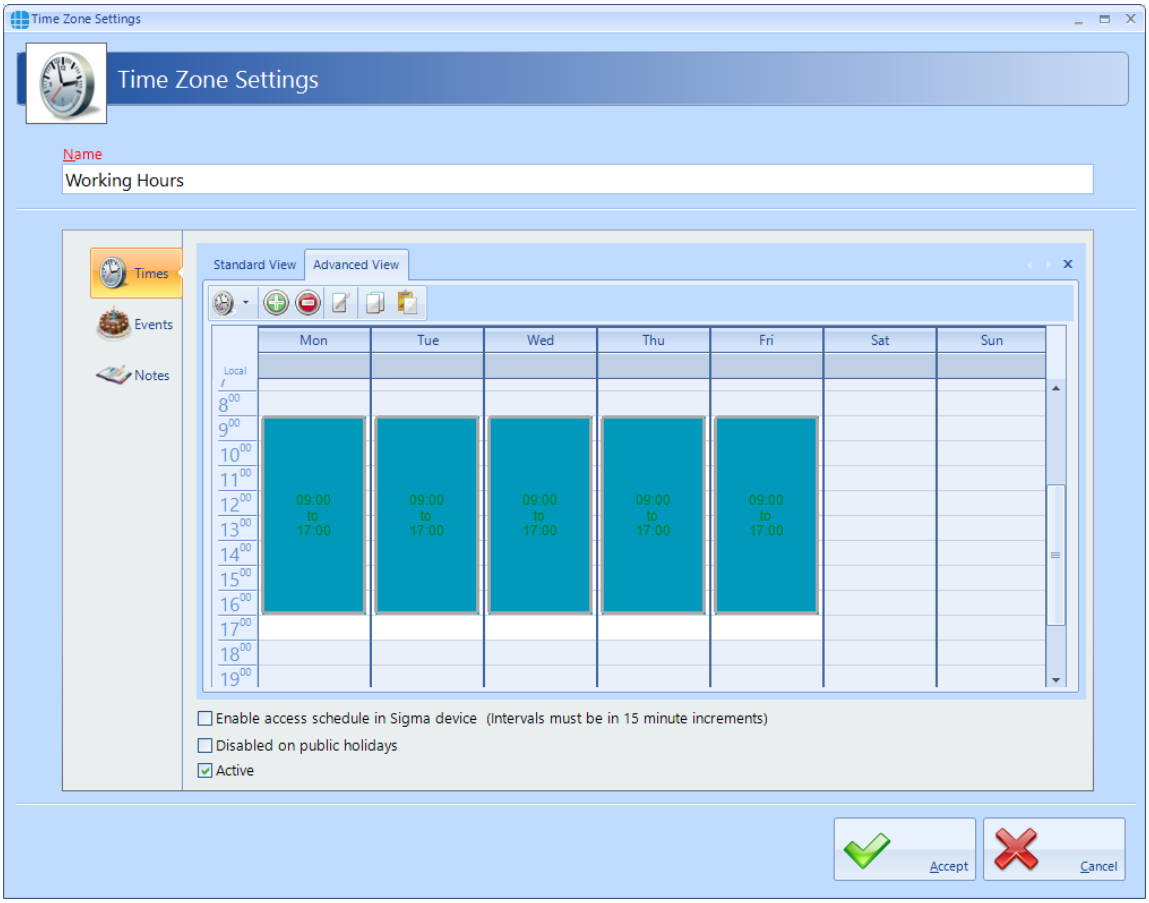


Enter a **Name** for the Time Zone

Each Time Zone can have up to 3 segments, each with its own Start Time and End Time. Time Zones can be entered with 1 minute resolution.

© 2026 Controlsoft Ltd

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

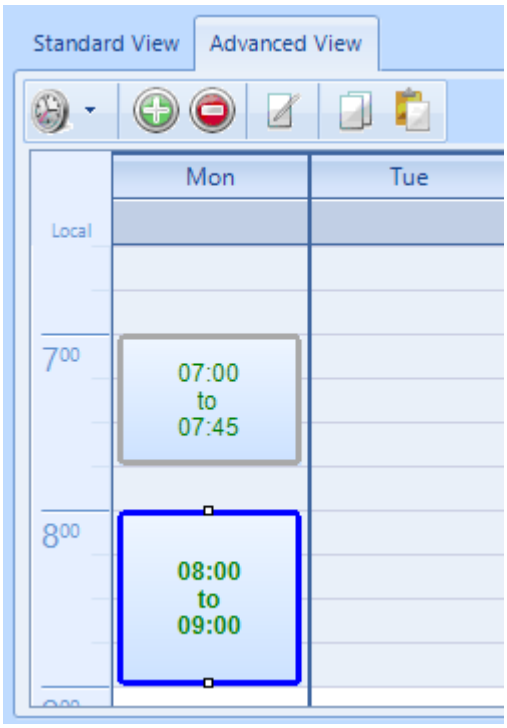


The following buttons are available in Advanced View:

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

© 2026 Controlsoft Ltd

 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

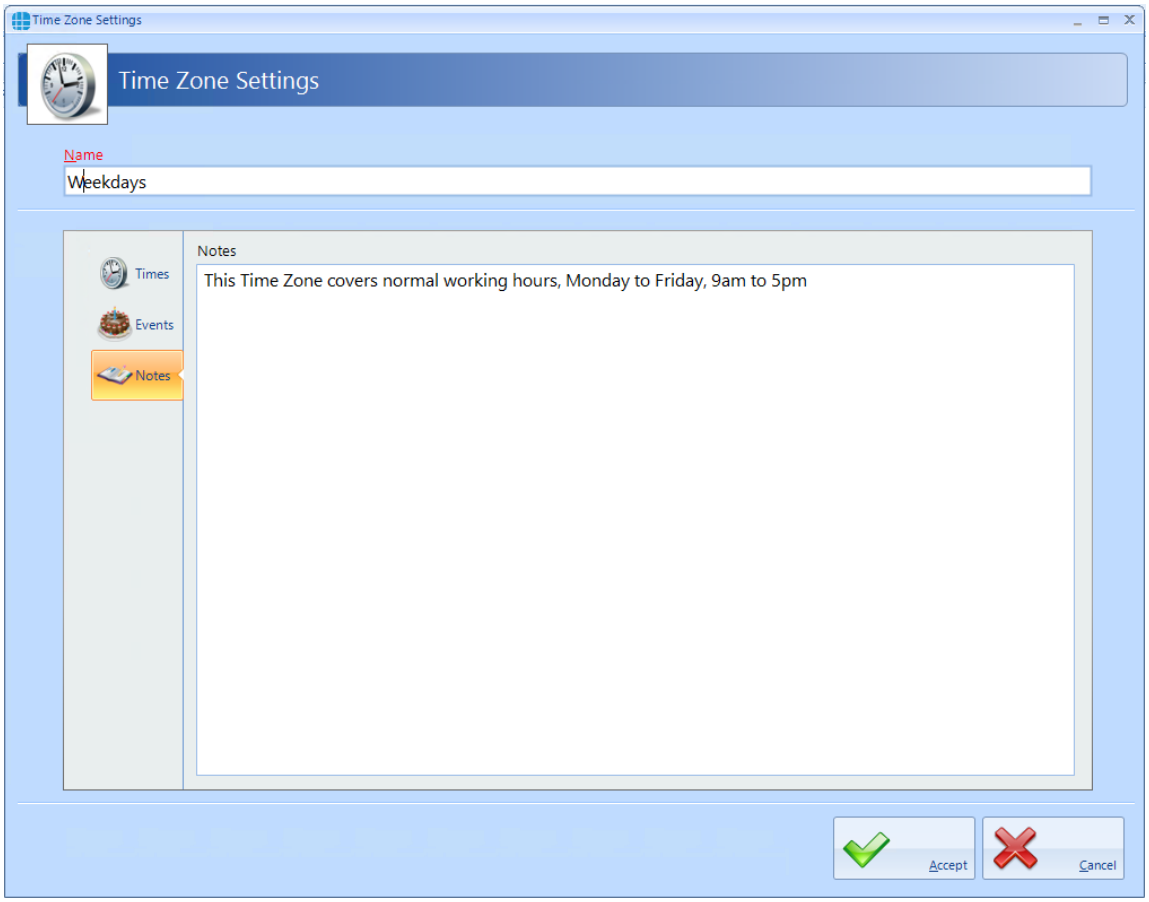
 Pastes the selected time entity

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.

he **Notes** section, accessed from the side bar, provides a text field which could provide information help a Service Engineer during their first visit to understand the function of the Time Zone.

© 2026 Controlsoft Ltd



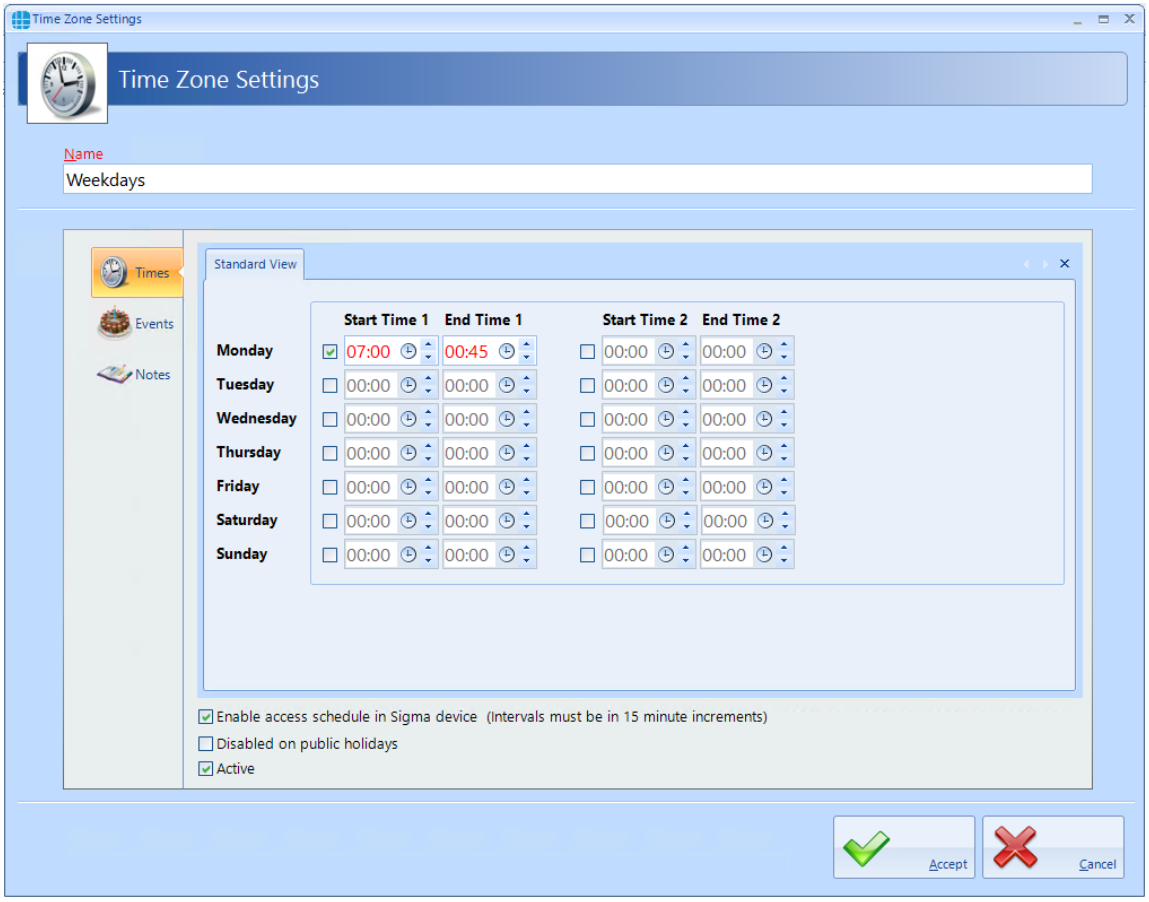
NOTE: Remember to associate Time Zones with the relevant Users / Doors, otherwise they will not be operational.

The iNet controller can support up to 63 Time Zones when fitted with the latest firmware. iNets fitted with firmware version 98.33.21.9 or older can only support 16 Time Zones.

© 2026 Controlsoft Ltd

13.2 Time Zones for Morpho Readers

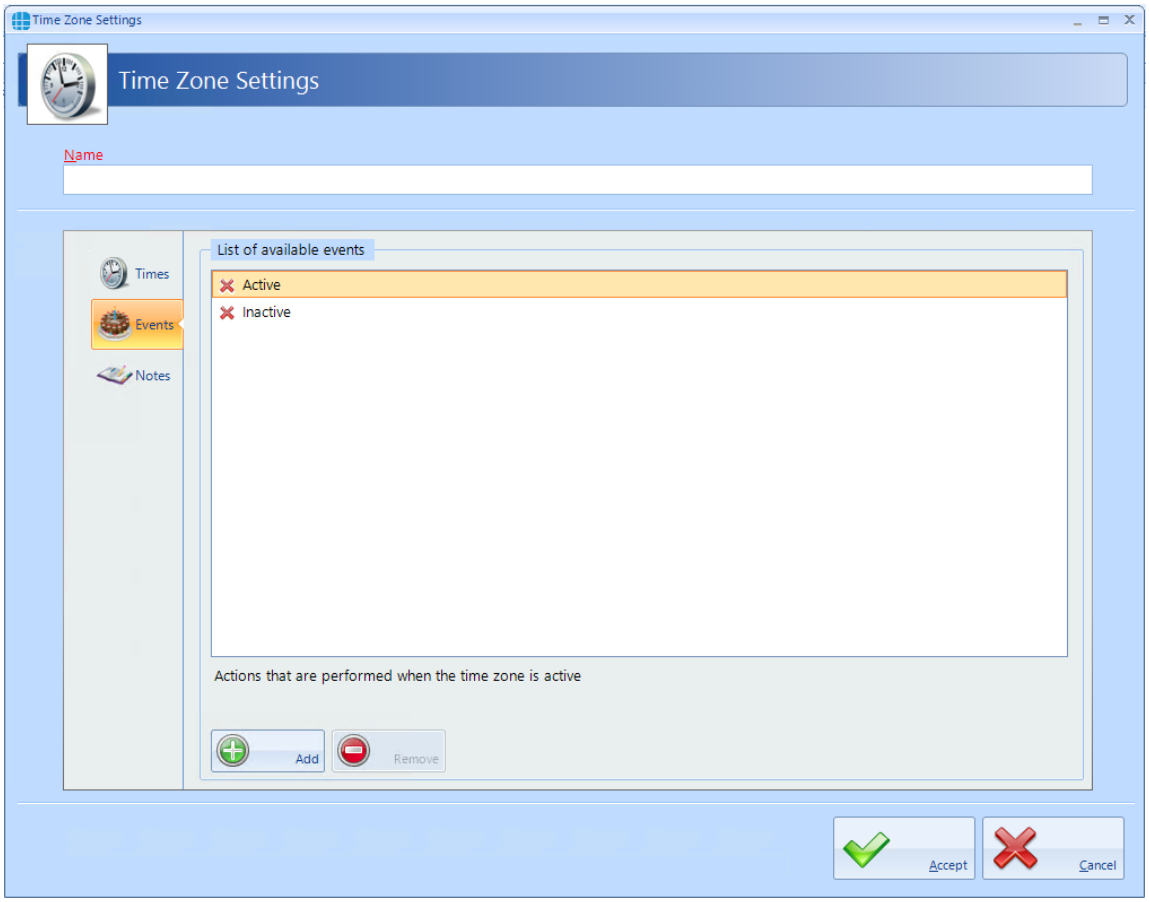
If using Time Zones with Morpho Readers, ensure that the option **Enable access schedule in Sigma device** is enabled. Morpho can only support 2 Start Times and 2 End Times per Time Zone as shown below:



13.3 Time Zones Events

Events section, accessed from the side bar, will indicate whether any Events have been configured for the selected time zone

© 2026 Controlsoft Ltd



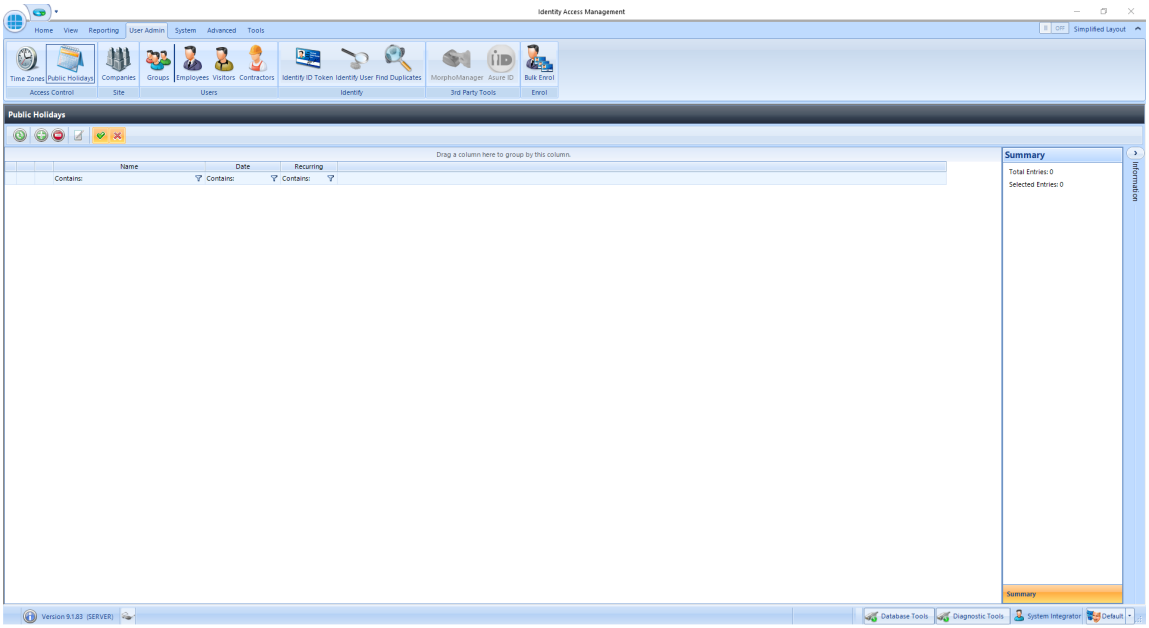
In this example, no Events have been created for the selected time zone. Clicking the **[Add]** button will allow Events to be created. For more information, see Events Section. 195

© 2026 Controlsoft Ltd

User Admin > Public Holidays

14 User Admin > Public Holidays

To configure a Public Holiday, select the **User Admin** tab, then select **Public Holiday** in the ribbon bar. To create a new Public Holiday, click the **Add** New button 

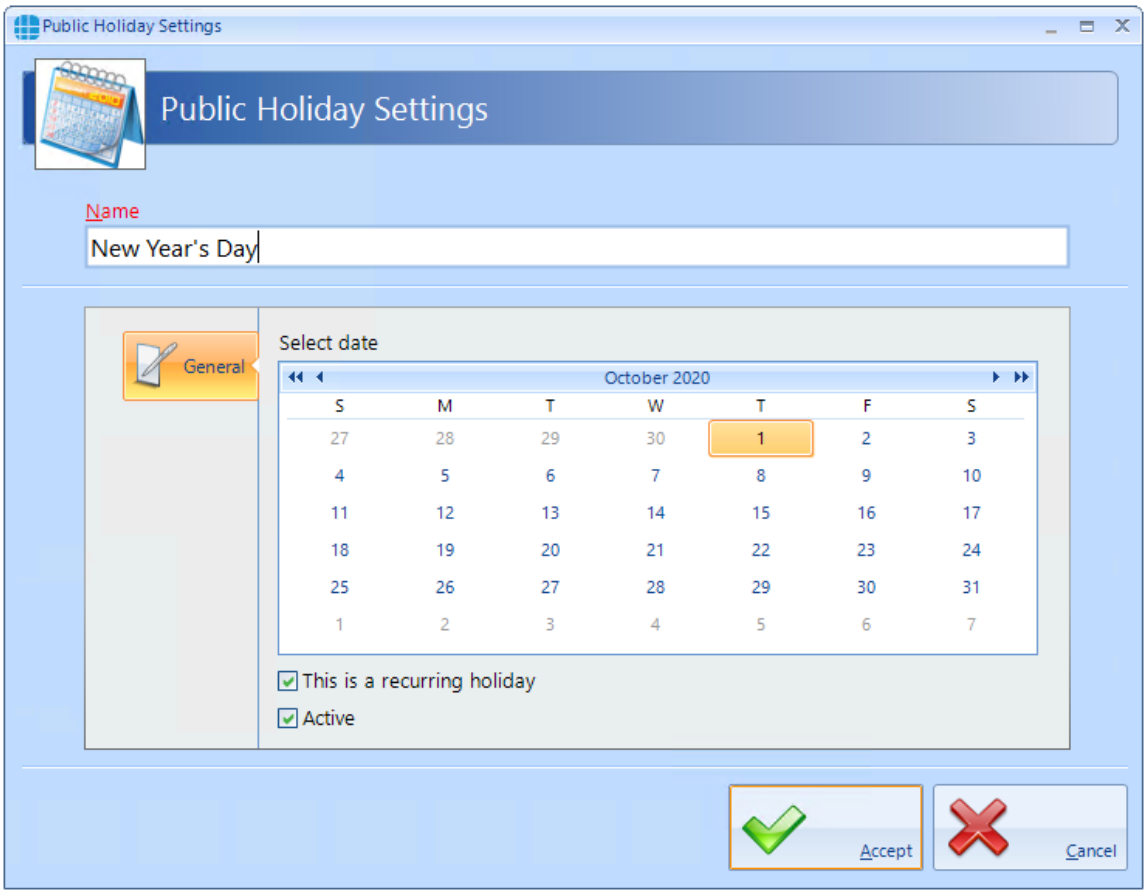


Enter a **Name** for the Public Holiday

Select date of the Public Holiday from the calendar

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

© 2026 Controlsoft Ltd



Click **[Accept]** when done.

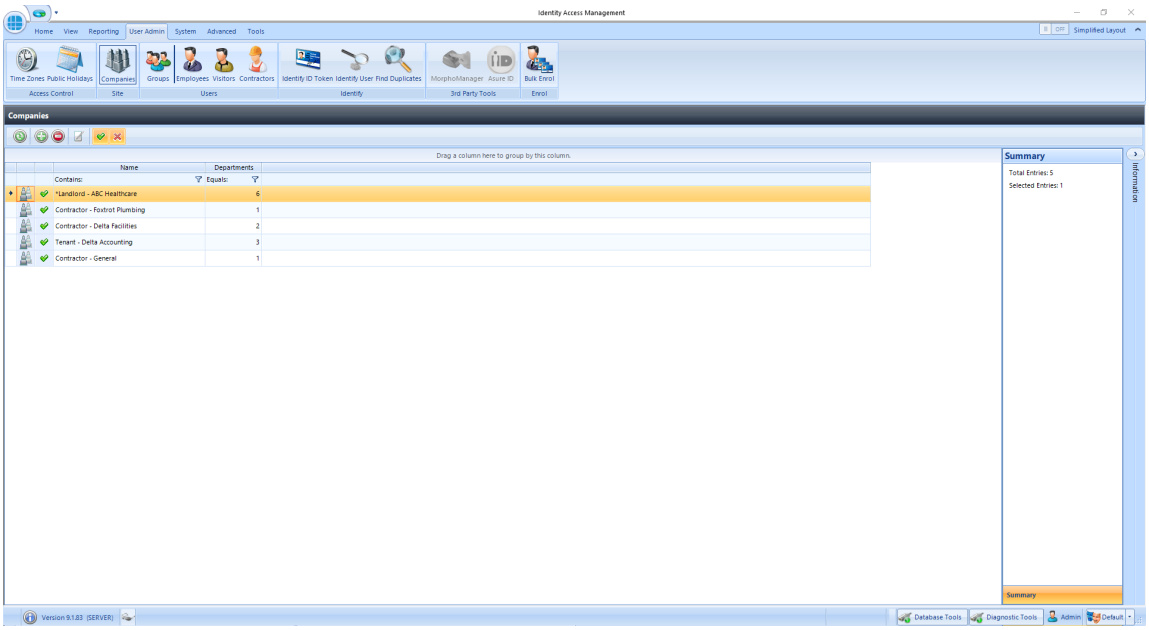
© 2026 Controlsoft Ltd

User Admin > Companies and Departments

15 User Admin > 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:



 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.

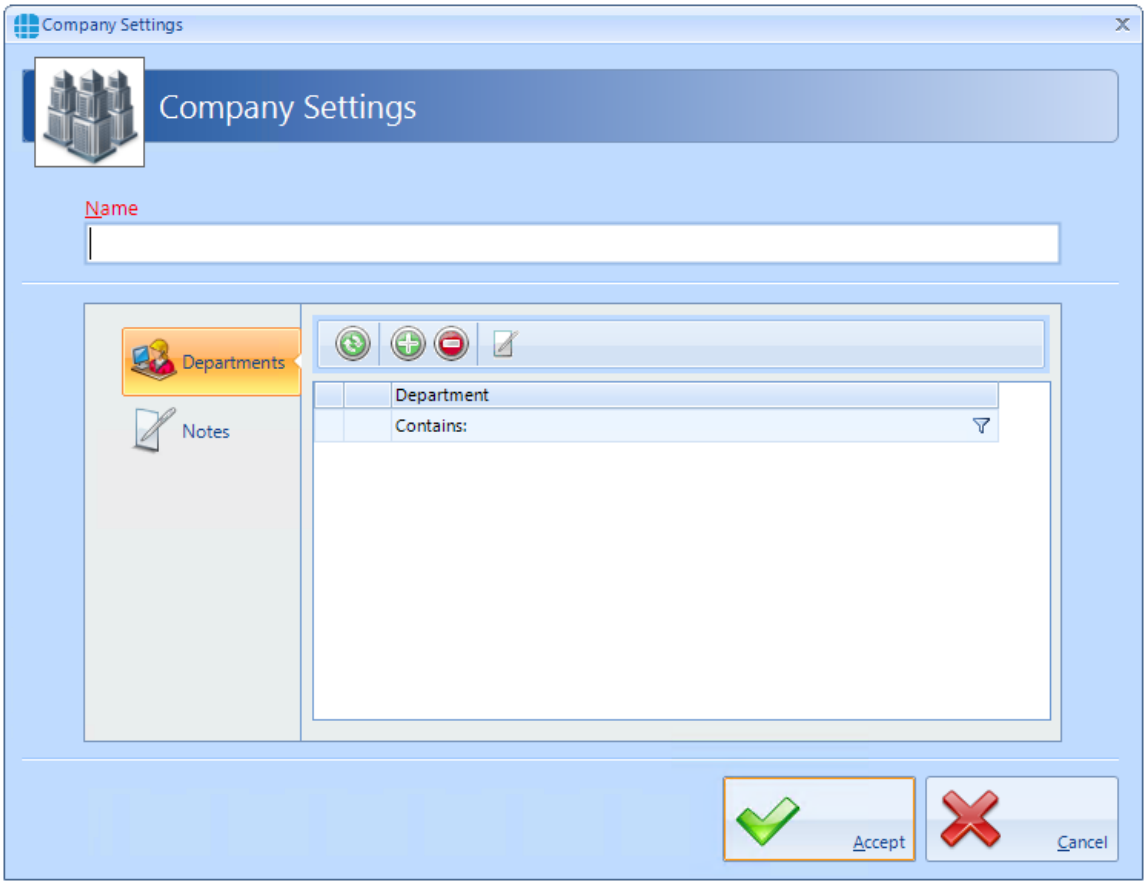
 Show/Hide Inactive: This button will show or hide Companies / Departments not selected as Active.

NOTE: When allocating a User to a Company / Department, simply choose the relevant option from the pull-down lists (see User General) 141

© 2026 Controlsoft Ltd

15.1 Creating Companies and Departments

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



.

 Refresh: Updates the list of Departments

 Add: Creates a new Department in the list

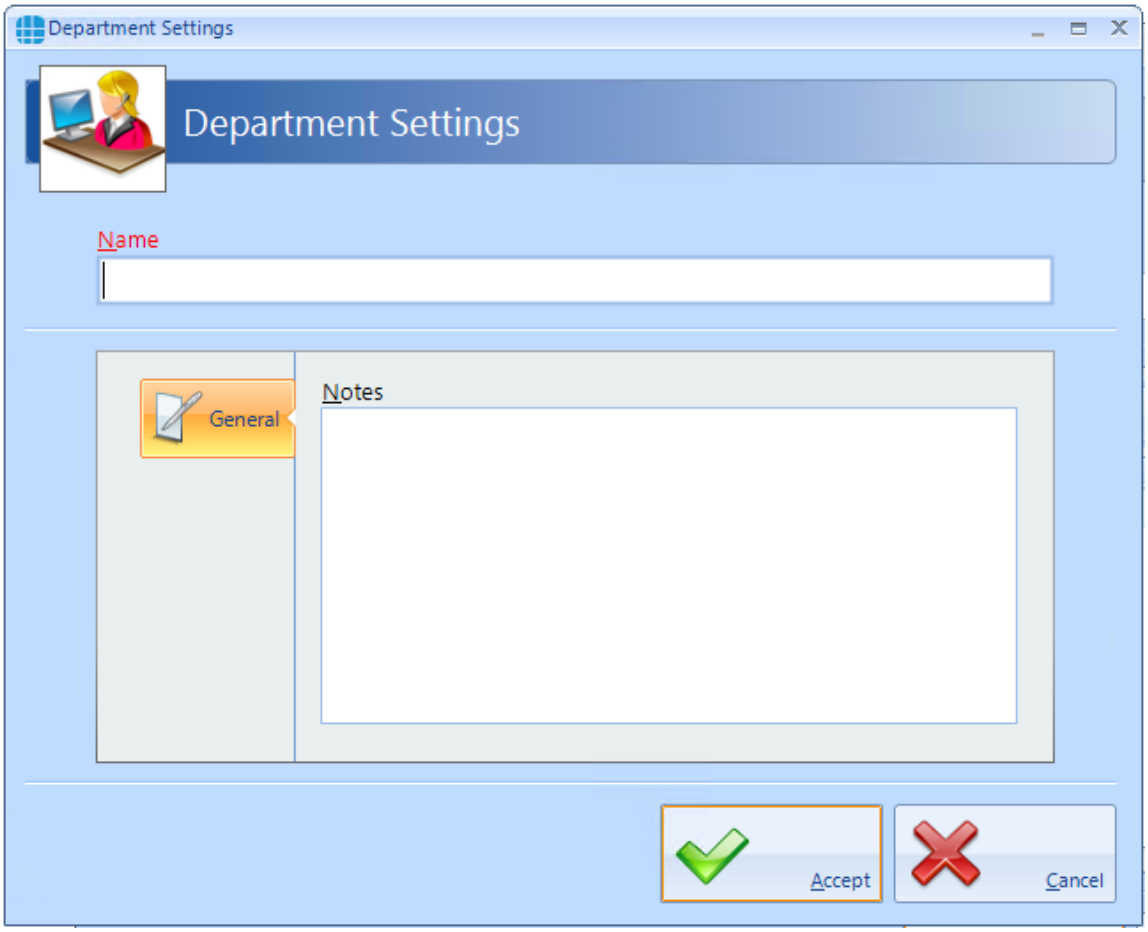
 Delete: Removes the selected Department/s from the list

 Edit: Edits the selected Department

Name: Add a name for the new Company

© 2026 Controlsoft Ltd

Click the Add button  to create a Department for the Company



Name: Add a name for the new Department

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

NOTE: The system supports multiple Companies and each Company can support multiple Departments.

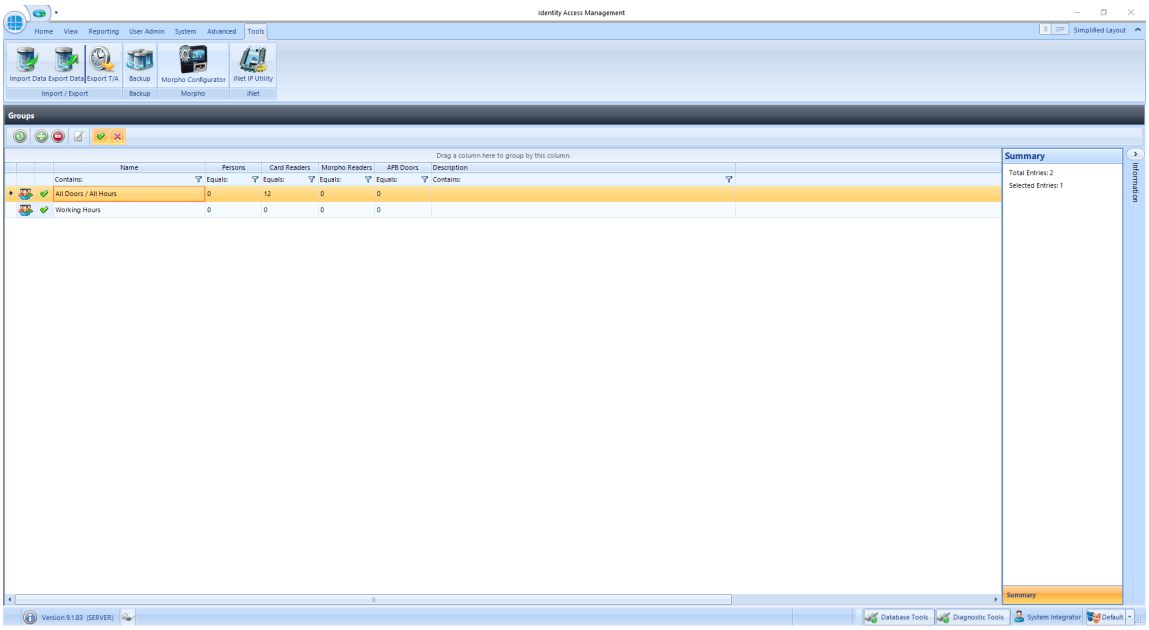
© 2026 Controlsoft Ltd

User Admin > Groups

16 User Admin > Groups

Groups are useful for speeding up the process of adding users to the system. Each Group is allocated combinations of Readers and Time Zones, so each new user is simply allocated to the relevant Group.

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



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.

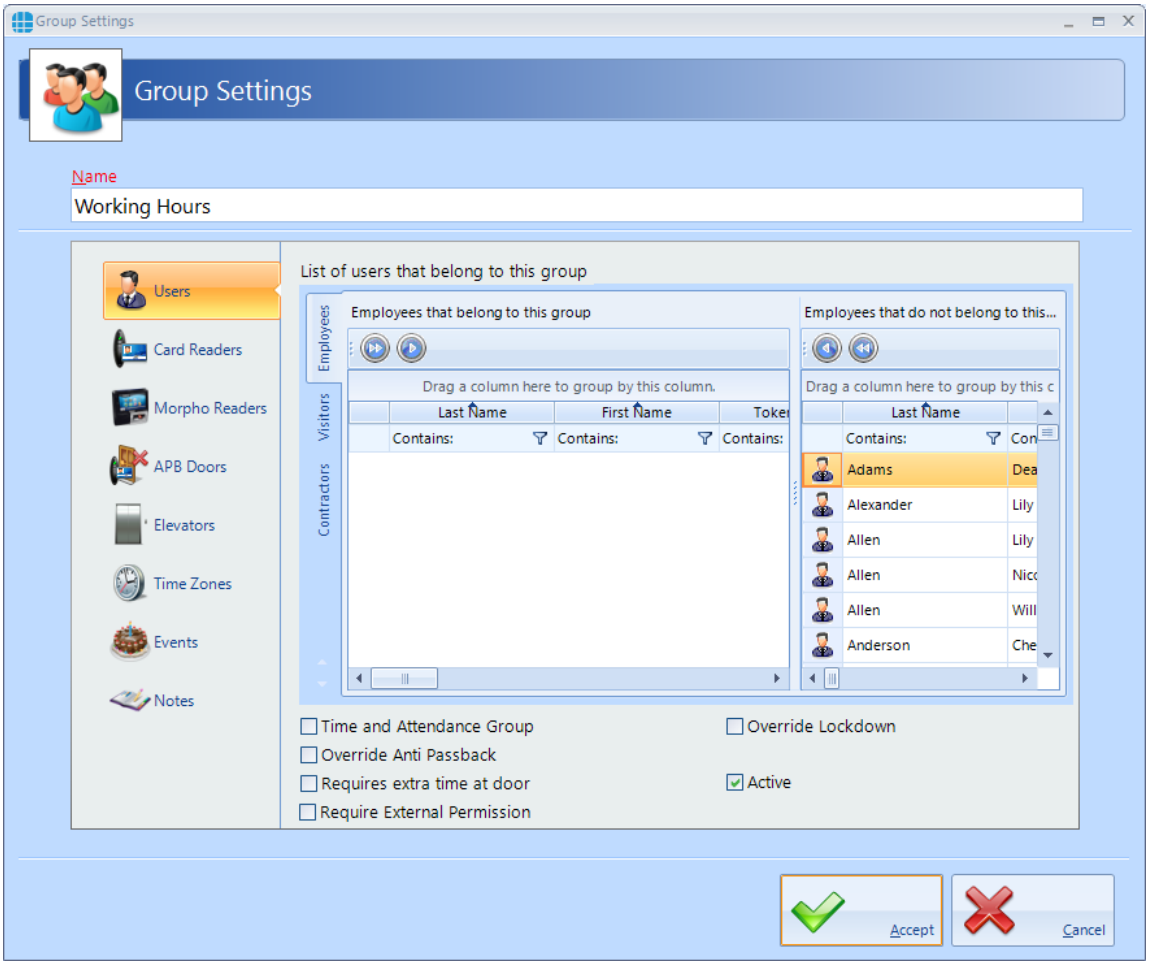
 Show/Hide Inactive: This button will show or hide Groups not selected as Active.

Select the **Add** New button 

© 2026 Controlsoft Ltd

16.1 Groups Properties Users

The Group Properties window is used to configure the group.



Enter a **Name** for the Group

Employees that belong to this group displays all users who are currently allocated to the group.

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

To allocate or de-allocate users to the Group, simply select one or more users and click or to move them between the windows. Alternately, click or to move all users between the windows.

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

Tick **Overide 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 for members of this group

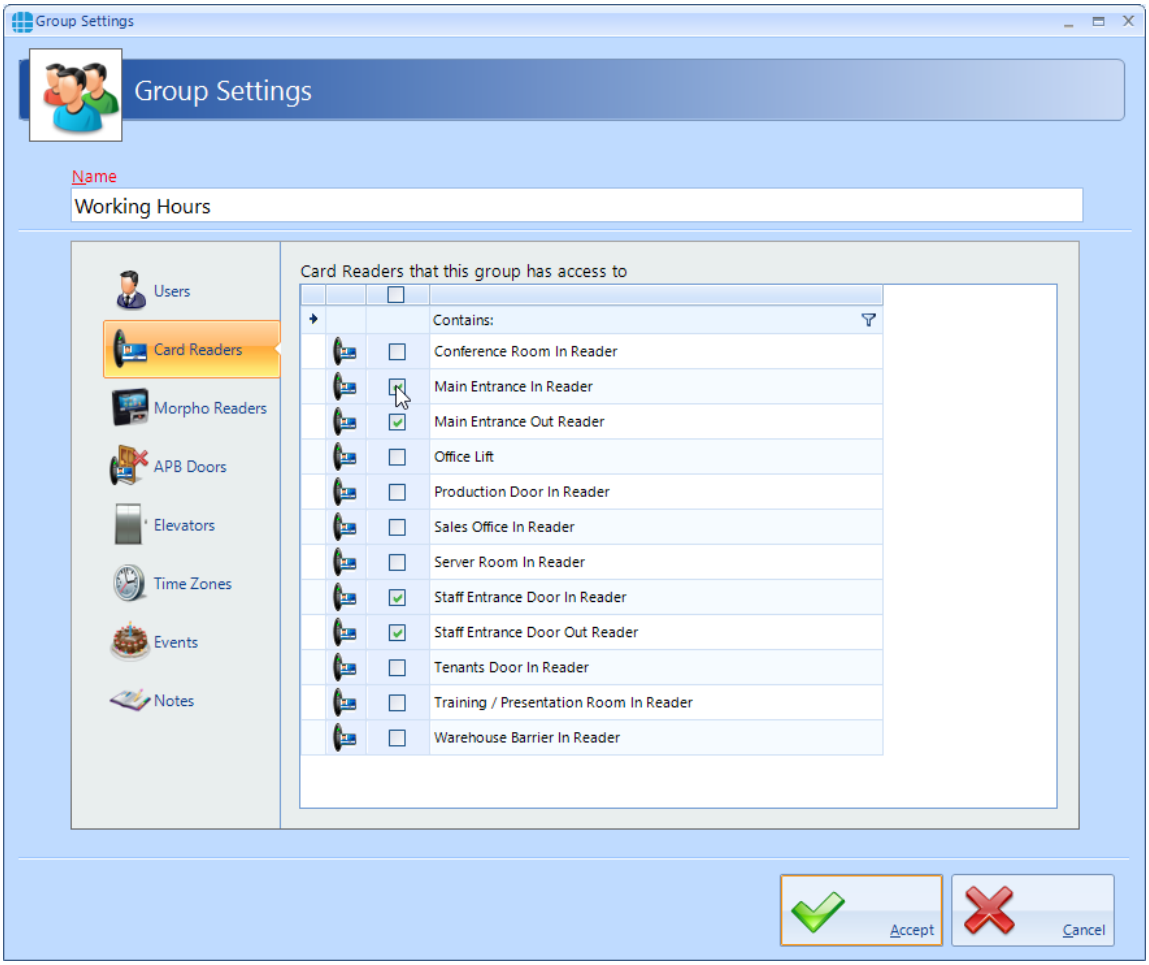
© 2026 Controlsoft Ltd

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.

16.2 Groups Properties Card Readers

Select **Card Readers** in the side bar:

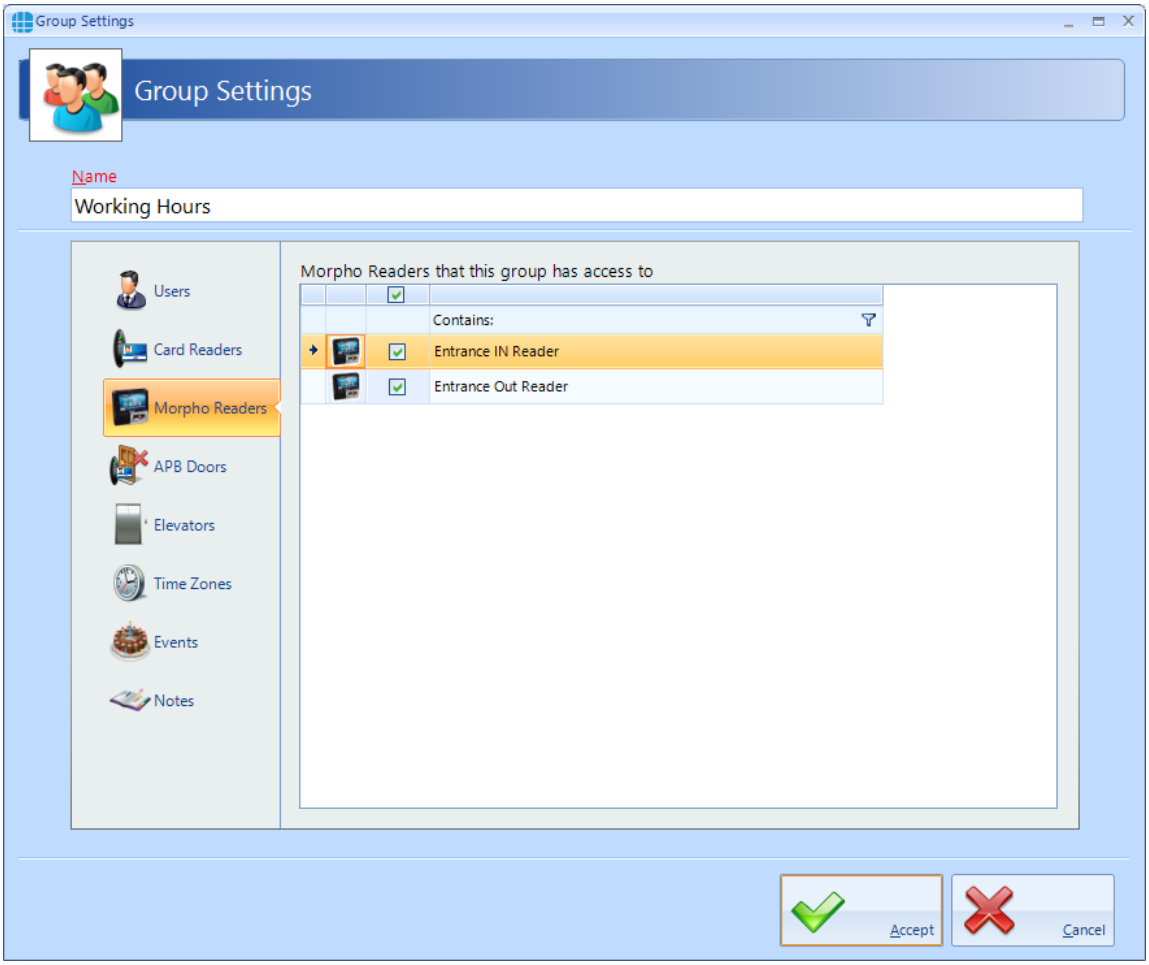


Select one or more card readers or Aperio locks that members of this Group will have access to. To select all readers, tick the **All** box (highlighted above).

© 2026 Controlsoft Ltd

16.3 Groups Properties Morpho Readers

Select **Morpho Readers** in the side bar:

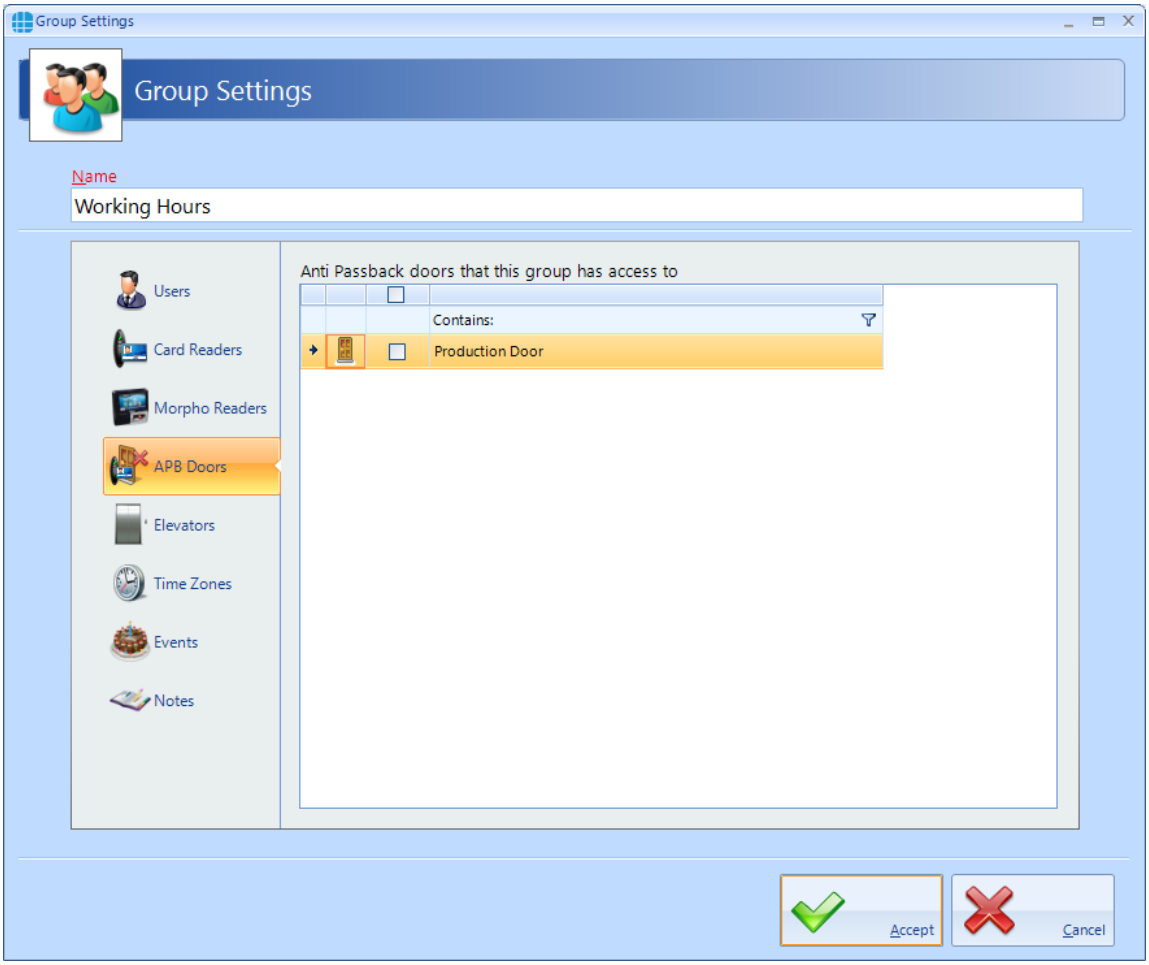


Select one or more Morpho readers that members of this Group will have access to. To select all readers, tick the **All** box (highlighted above).

© 2026 Controlsoft Ltd

16.4 Groups Properties APB Doors

Select **APB Doors** in the side bar:

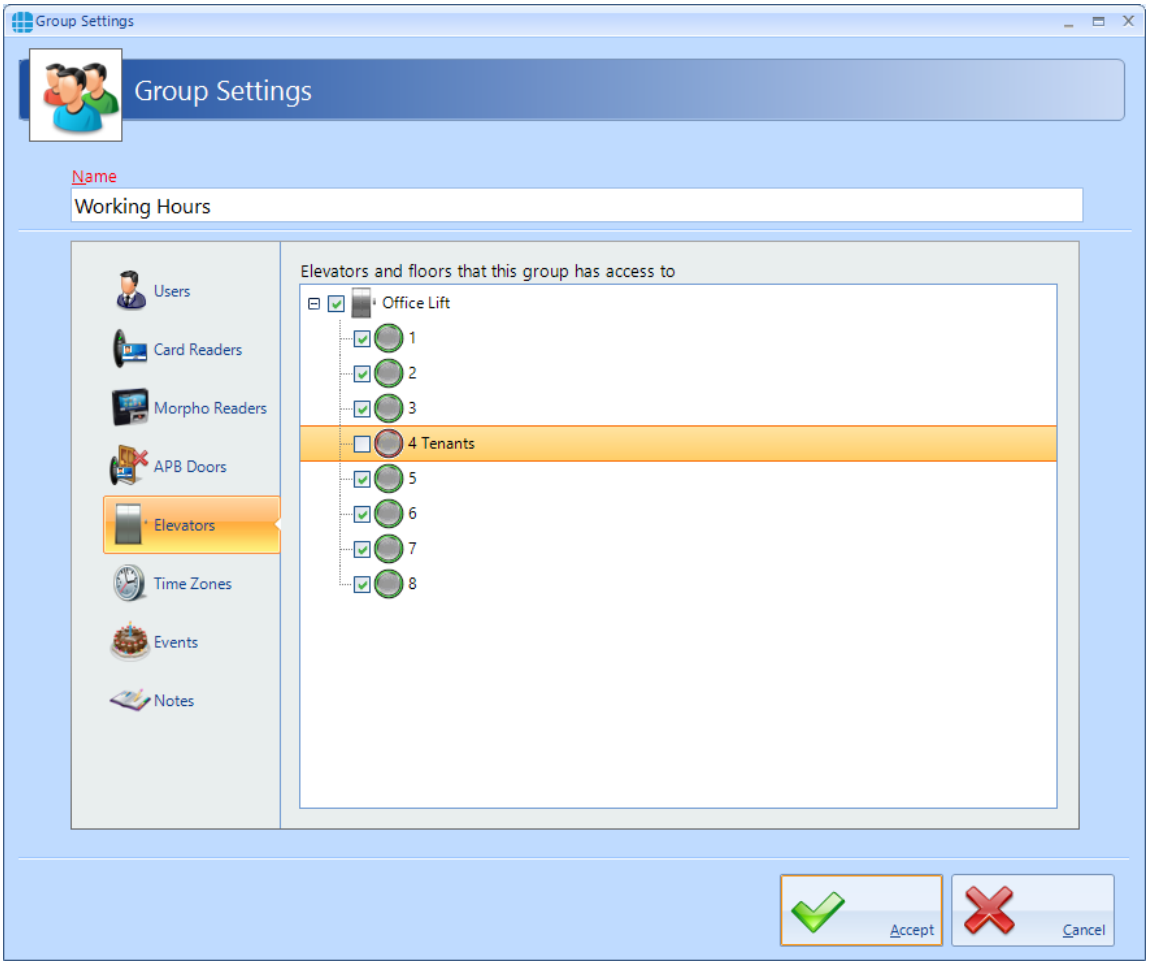


Select one or more AntiPassBack Doors where members of this Group will be subject to AntiPassBack. To select all APB doors, tick the **All** box (highlighted above).

© 2026 Controlsoft Ltd

16.5 Group Properties Elevators

Select the **Elevators** tab to define which floors are accessible to users in this group:

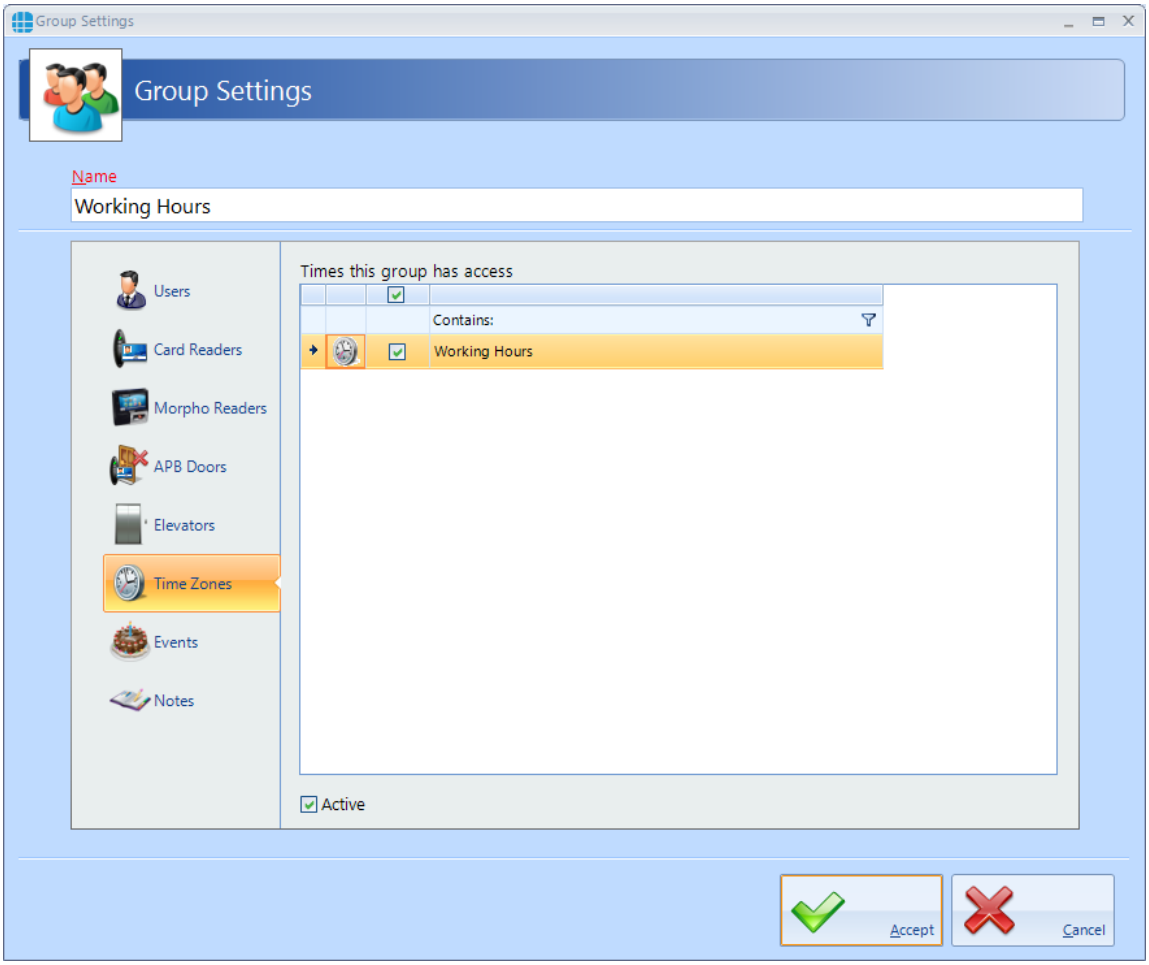


Tick the elevator and all the floors to be accessible to these users.

© 2026 Controlsoft Ltd

16.6 Groups Properties Time Zones

Select **Time Zones** in the side bar:

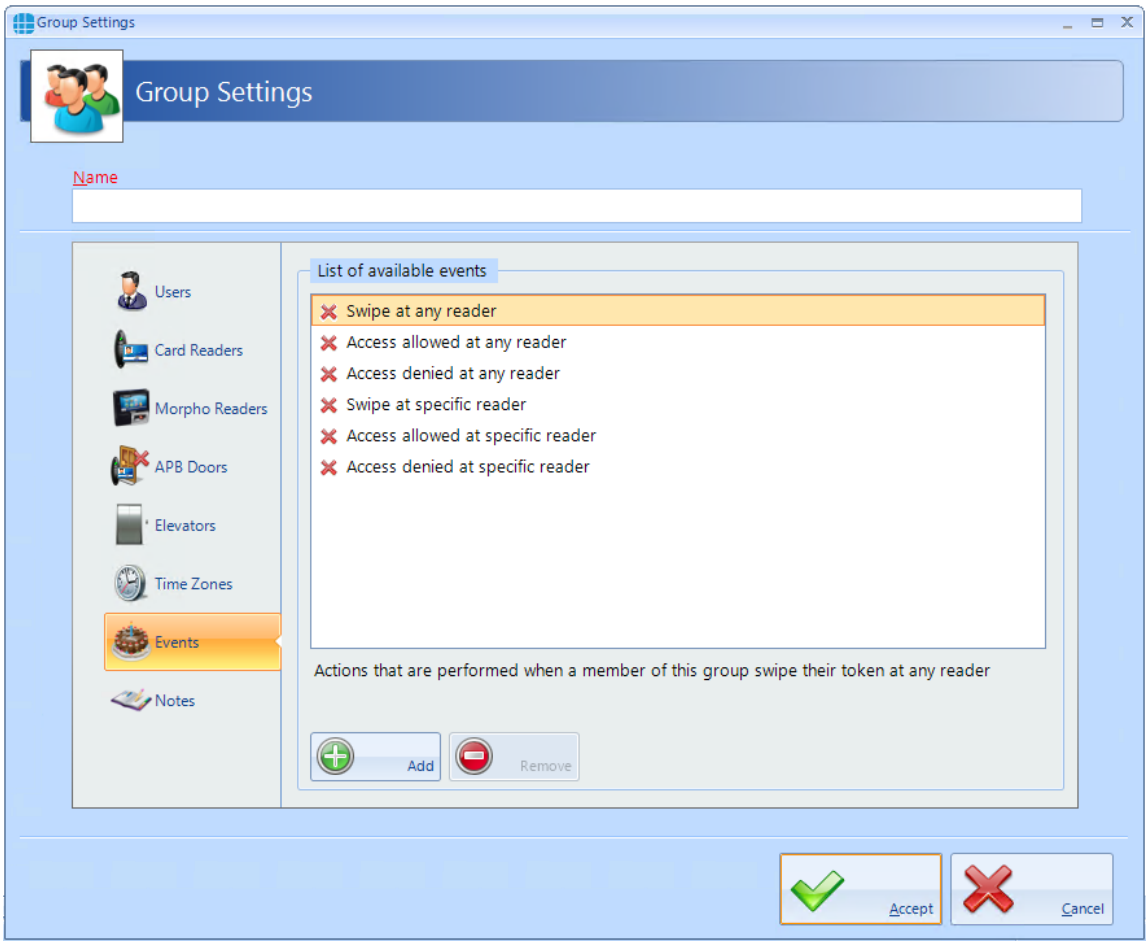


Select the Time Zone that members of this Group will be constrained by. ***NOTE: For additional flexibility, multiple Time Zones can be allocated a single group.***

16.7 Group Properties Events

The Events tab will indicate whether any Events have been configured for the selected group.

© 2026 Controlsoft Ltd



In this example, no Events have been created for the selected group. Clicking the **[Add]** button will allow Events to be created. For more information, see Events Section. 195

16.8 Allocating Users to Groups

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

1. From within the User Properties 141 Window.

2. From within the Group Properties 130 Window.

© 2026 Controlsoft Ltd

Enrolment Readers

17 Enrolment Readers

The type of Enrolment reader required will depend on the type of cards used on site. The options are:

IA-DTR. This is an Omnikey 5427G2, pre-configured to read Controlsoft 47 bit iCLASS and HID Proximity cards and fobs

OMN-1051. This is an Omnikey 5427G2, pre-configured to read Controlsoft Proximity 26-bit cards and fobs

OMN-1052. This is an Omnikey 5427G2, pre-configured to read MIFARE 32-bit and 34-bit cards and fobs

© 2026 Controlsoft Ltd

User Admin > Employees / Visitors / Contractors

18 User Admin > Employees / Visitors / Contractors

"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, for example:

Employees may have very flexible access to the premises for long periods of time.

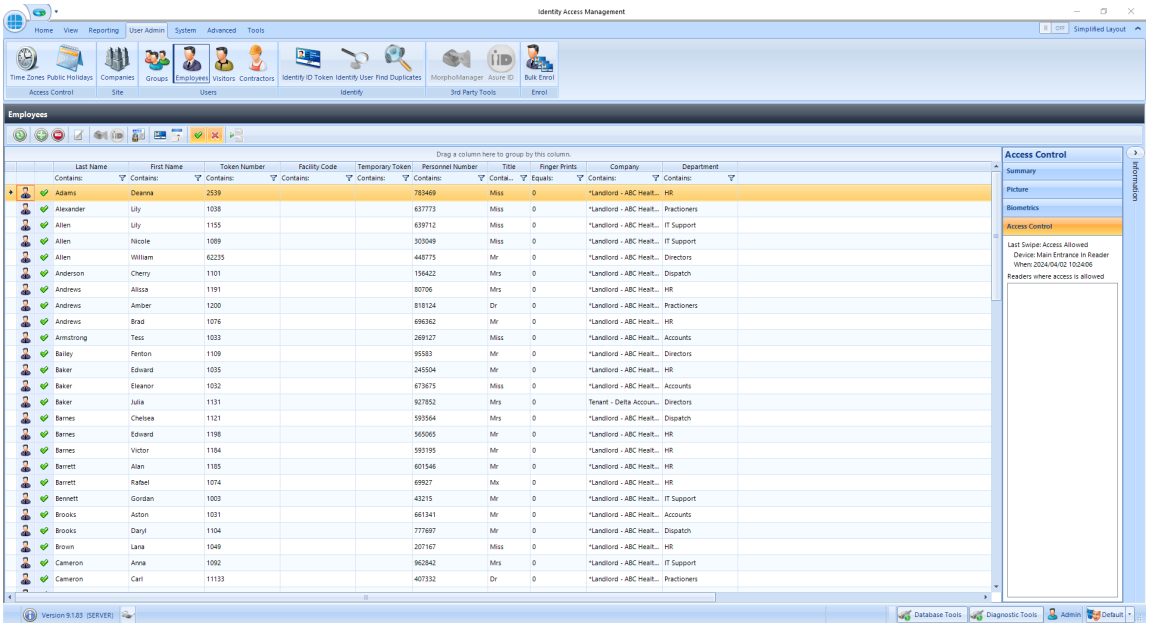
Visitors may have limited access to the premises and may be heavily managed on a day to day basis.

Contractors may have flexible access to the premises but only for short periods of time.

Furthermore, separating Employees, Visitors and Contractors makes reporting on each criteria easier and more flexible.

NOTE: Programming screens for Employees, Visitors and Contractors are the same. Programming screens for Visitors and Contractors are not shown for brevity.

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



The option icons are as follows:

 Refresh: Updates the list of Users

 Add: Creates a new User to the list

© 2026 Controlsoft Ltd

 Delete: Removes the selected User/s from the list

 Edit: edits the selected User

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



Print: Prints a card for the selected user. This icon will be greyed out if Asure ID is not installed.

 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.

For Visitors, two additional buttons are available:

 Re-activate Visitor: If a Visitor token is set to deactivate at the End of Day, simply selecting that visitor the next day and clicking this button will reactivate the token until the end of the current day.

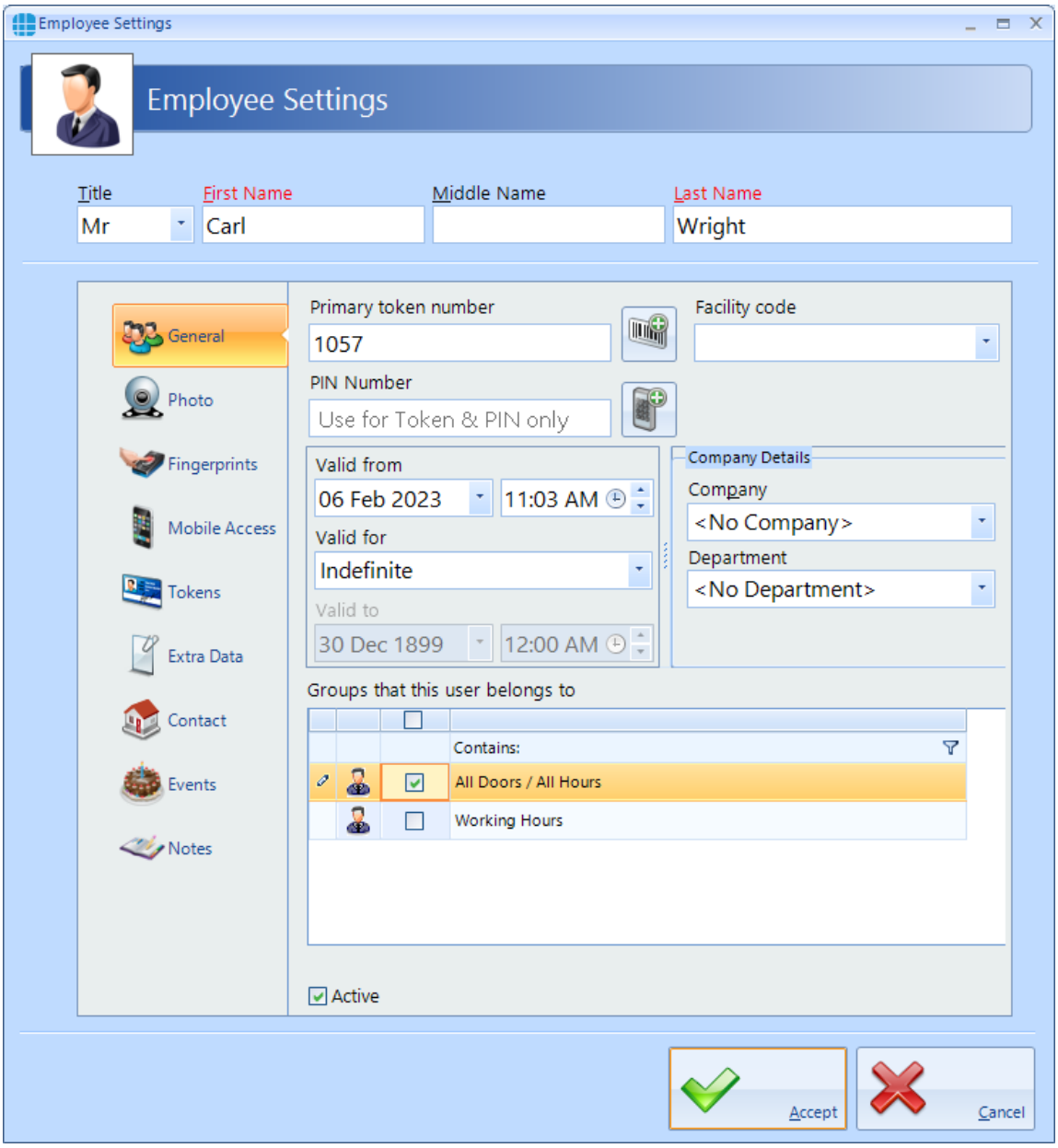
 Show Expired Visitors: Filters the display to show visitors whose tokens have expired and can be re-activated.

NOTE: Any changes made to Users (Employees, Visitors and Contractors) will automatically be downloaded to the Controllers / Biometric Readers, it will not be necessary to perform a "Rebuild"

© 2026 Controlsoft Ltd

18.1 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).

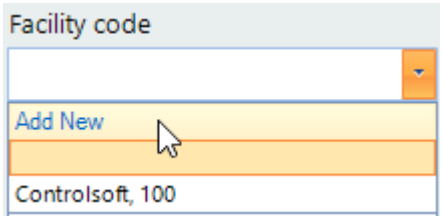
Enter the **Primary Token Number** of the card allocated to this user. This may be written on the card, read via an Enrolment reader, or may be a sequential number in systems using fingerprint only. If enabled, pressing the icon to the right of the Token Number field will automatically generate the next available 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). This ensures that another card with the same number (1036928) but a different Facility Code will not be granted access. ***NOTE: If Facility***

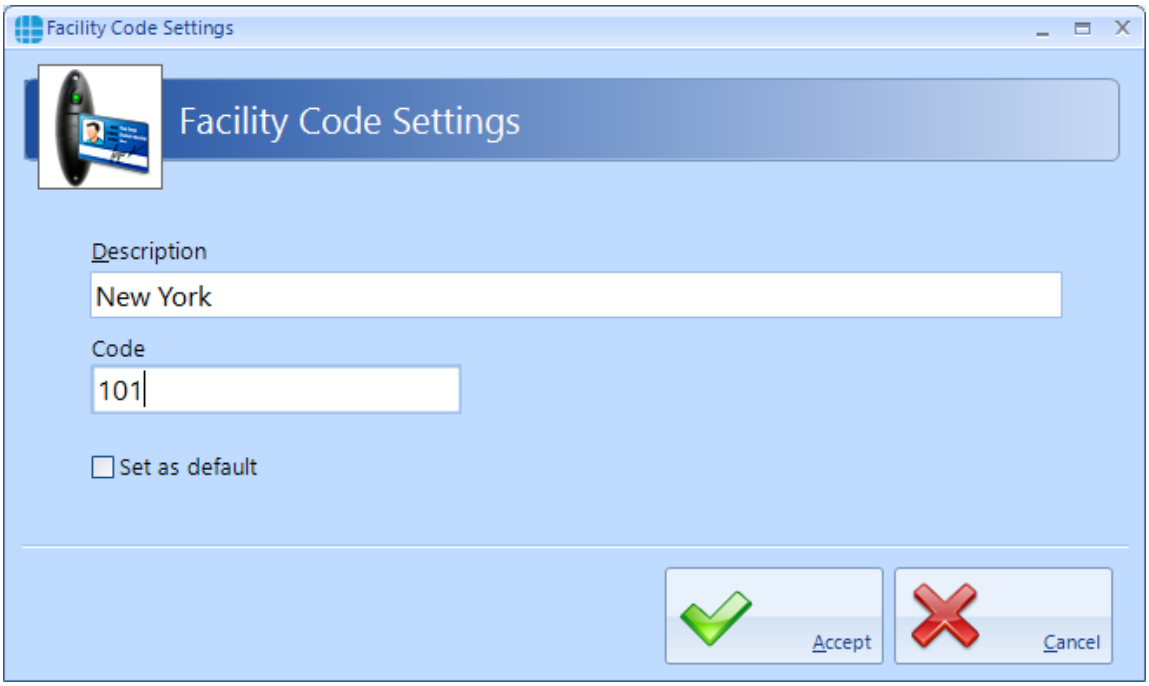
© 2026 Controlsoft Ltd

Codes are not enabled in the IA Configuration utility (see IA Configuration - Cards & Readers 247***, this field will be greyed out.***

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



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**.



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 must 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 IA 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.

Groups that this user belongs to lists all the available Groups within the system. To allocate the user to one or more groups, simple tick the boxes for the groups.

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

© 2026 Controlsoft Ltd

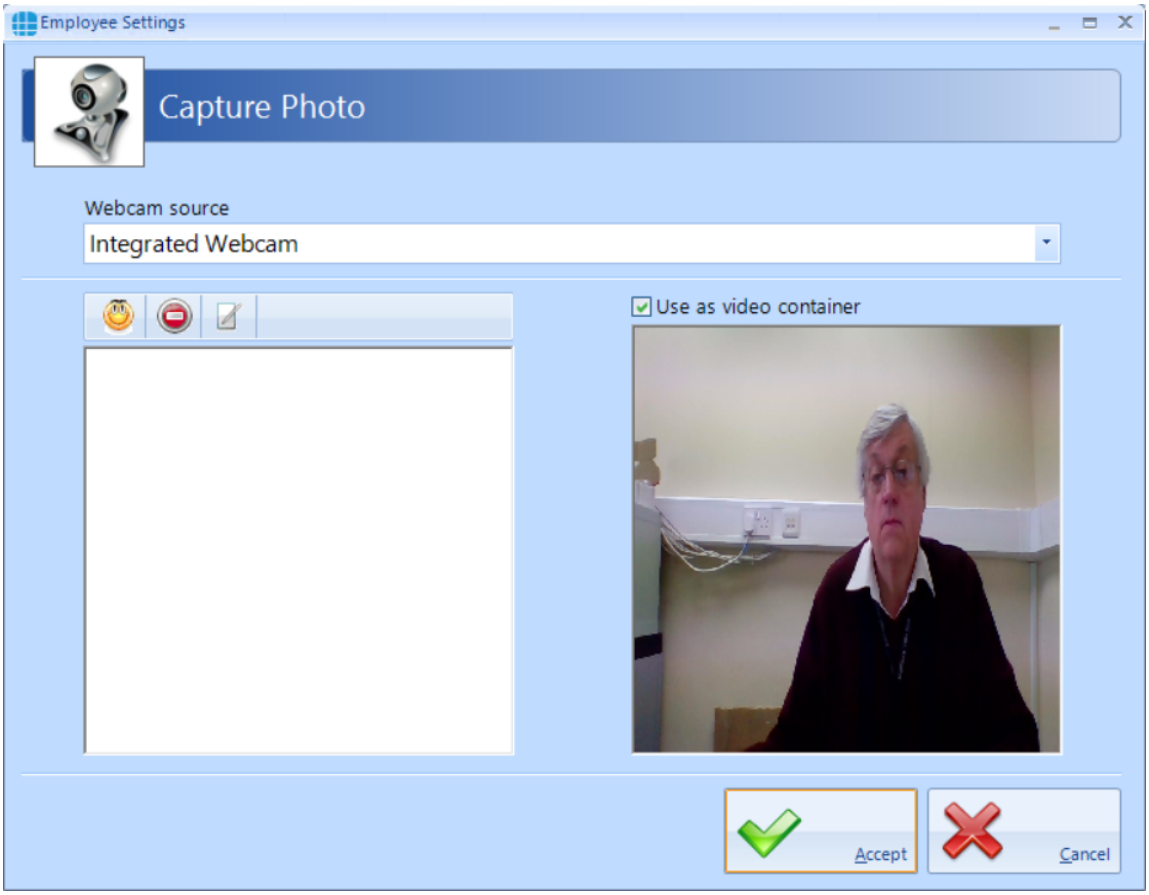
18.2 User Photo

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.

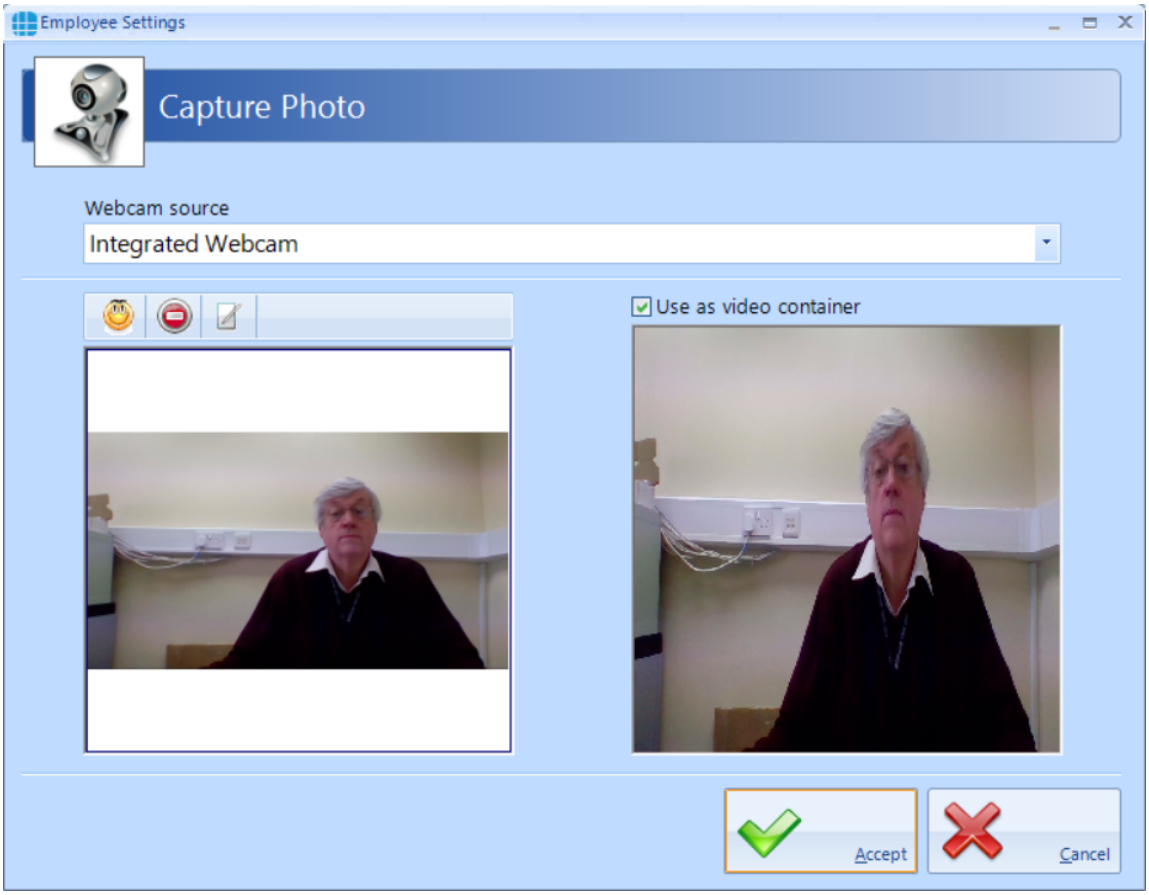


Select the import icon  to import a previously saved image, or the camera icon  to capture a photo from a webcam:

© 2026 Controlsoft Ltd

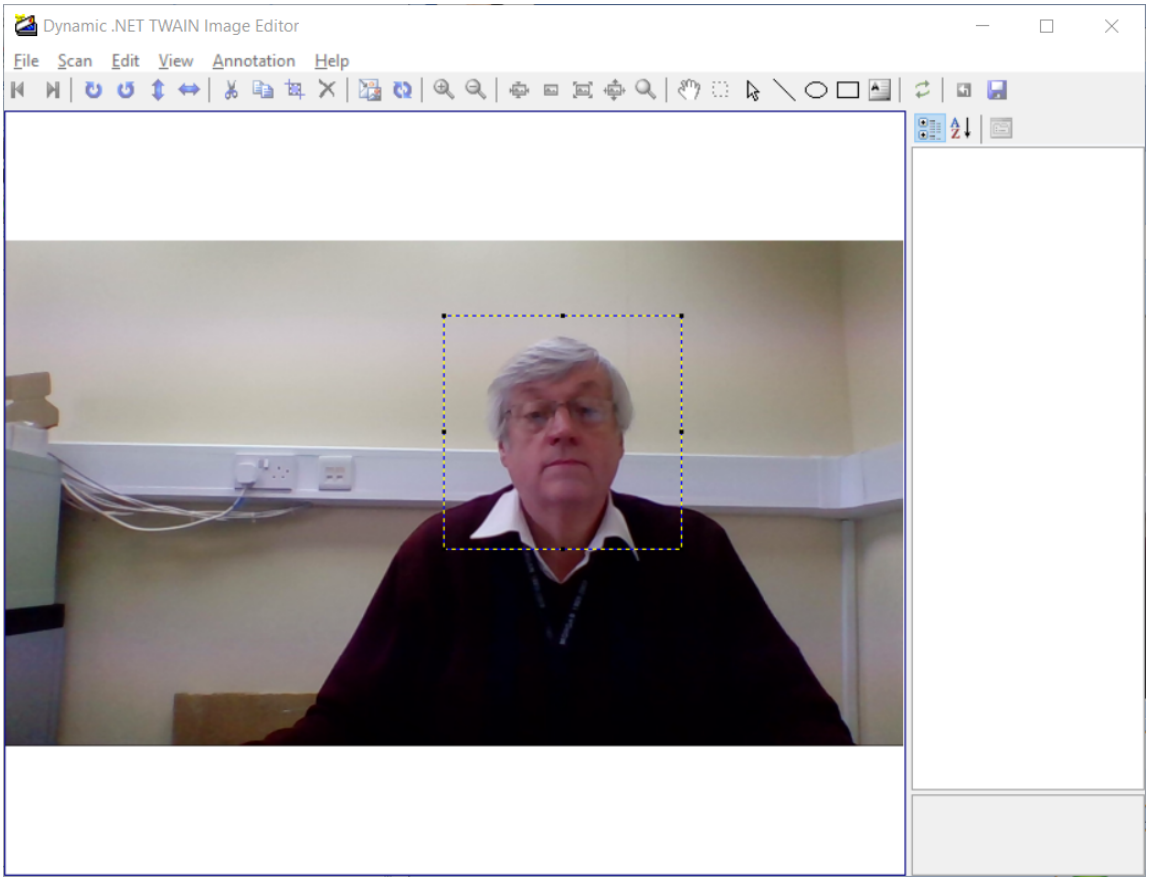


The left hand window shows a live display from the webcam. When the "Yellow Face" is clicked, a snapshot is taken and displayed in the left hand window:



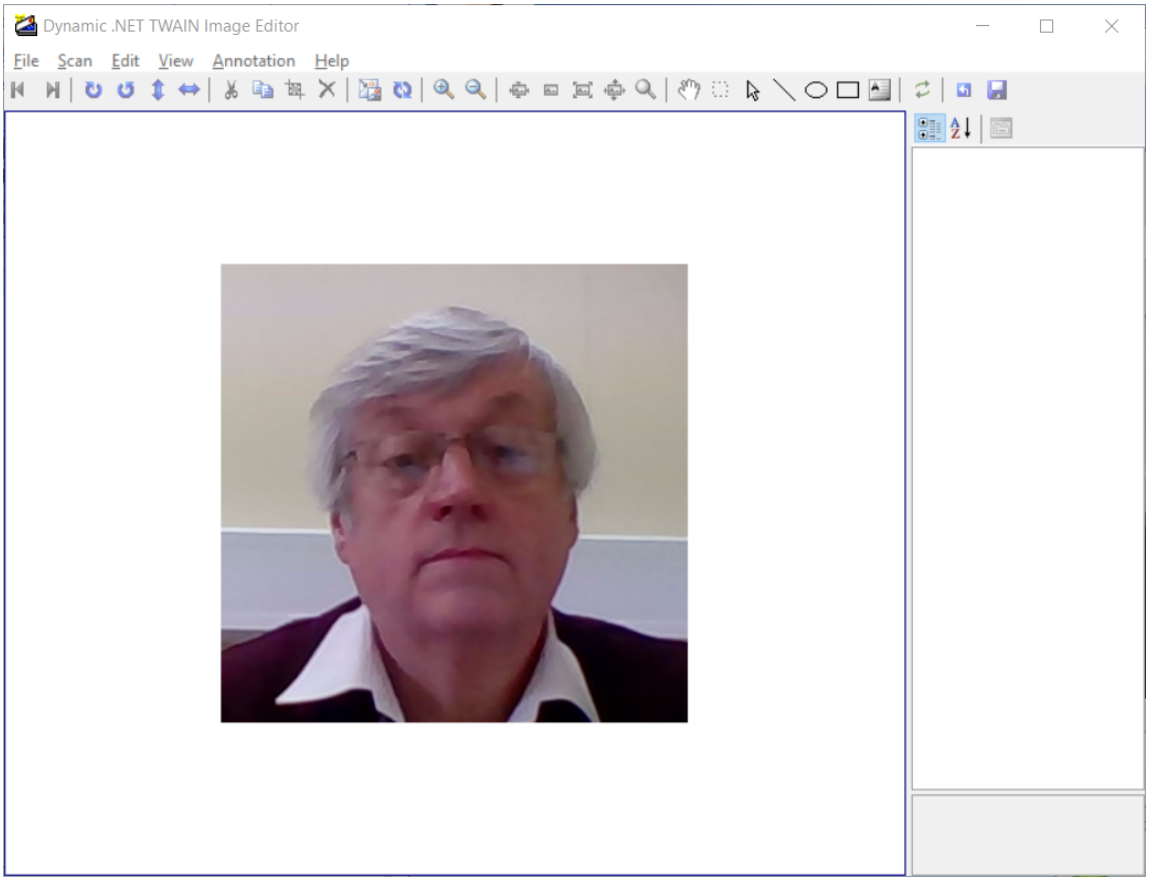
© 2026 Controlsoft Ltd

It is possible to capture multiple images, then scroll up and down to select the best image to use. To optimise the image, it is possible to zoom in on the main area of interest by clicking the edit button 



Draw a marquee around the area of interest and click the Crop button 

© 2026 Controlsoft Ltd

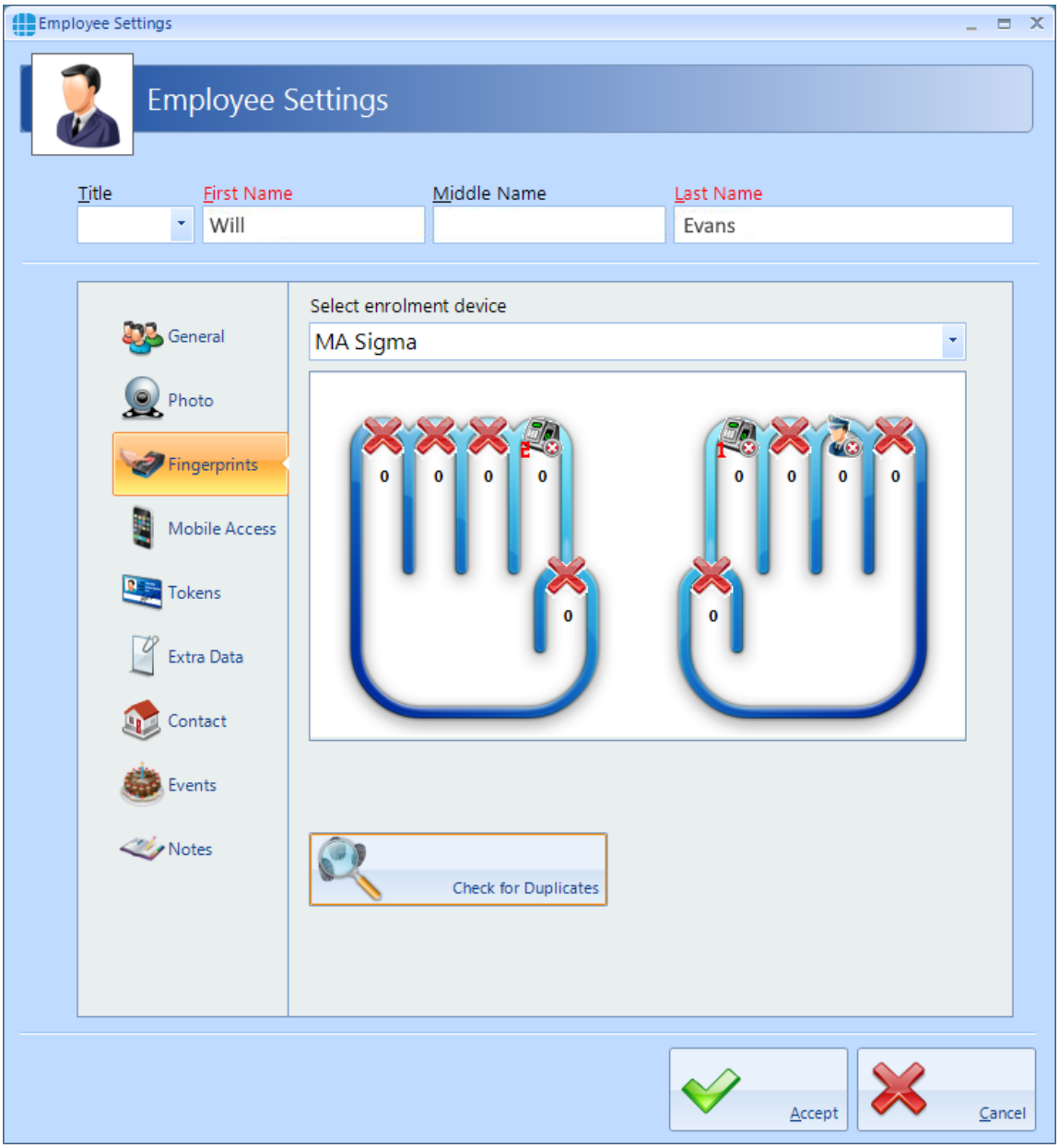


Close the window and click **[Yes]** to save the image. Finally, click **[Accept]**.

© 2026 Controlsoft Ltd

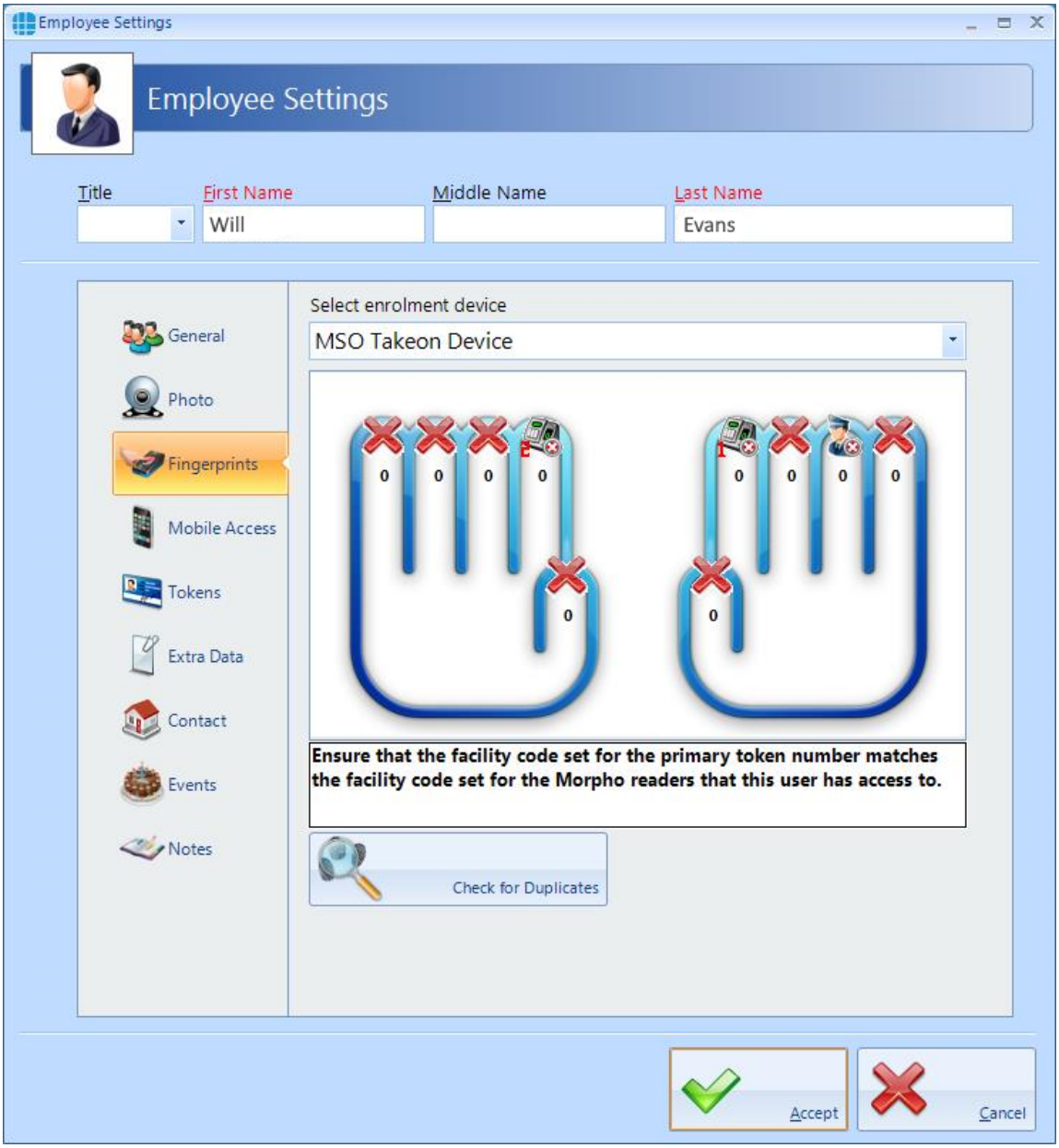
18.3 User Fingerprints

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

© 2026 Controlsoft Ltd



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

© 2026 Controlsoft Ltd



.

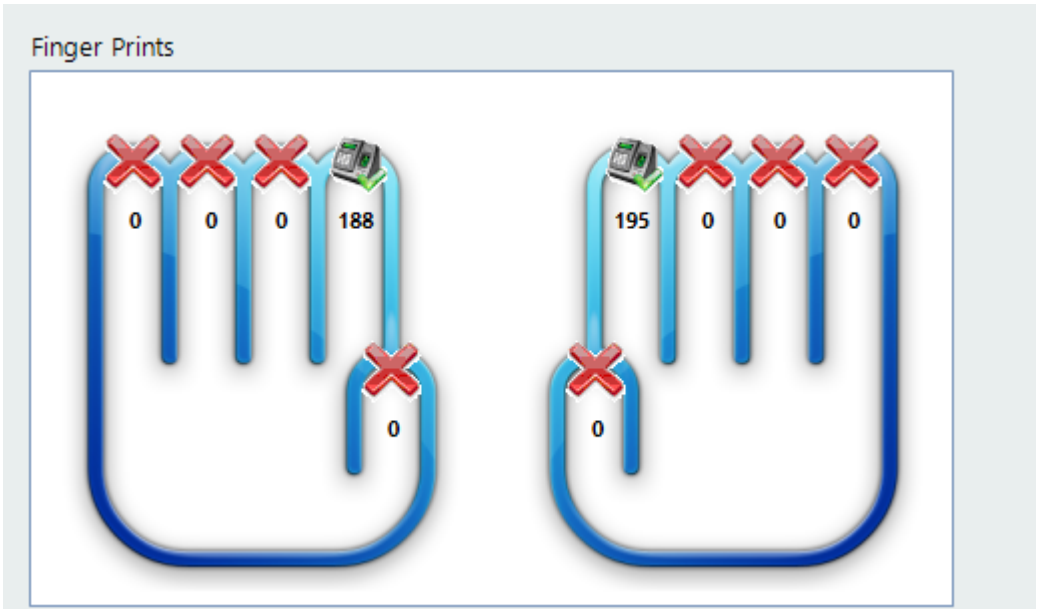
© 2026 Controlsoft Ltd

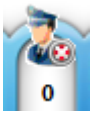
Place the selected finger on the enrolment reader 3 times, following the on-screen instructions where necessary.



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.



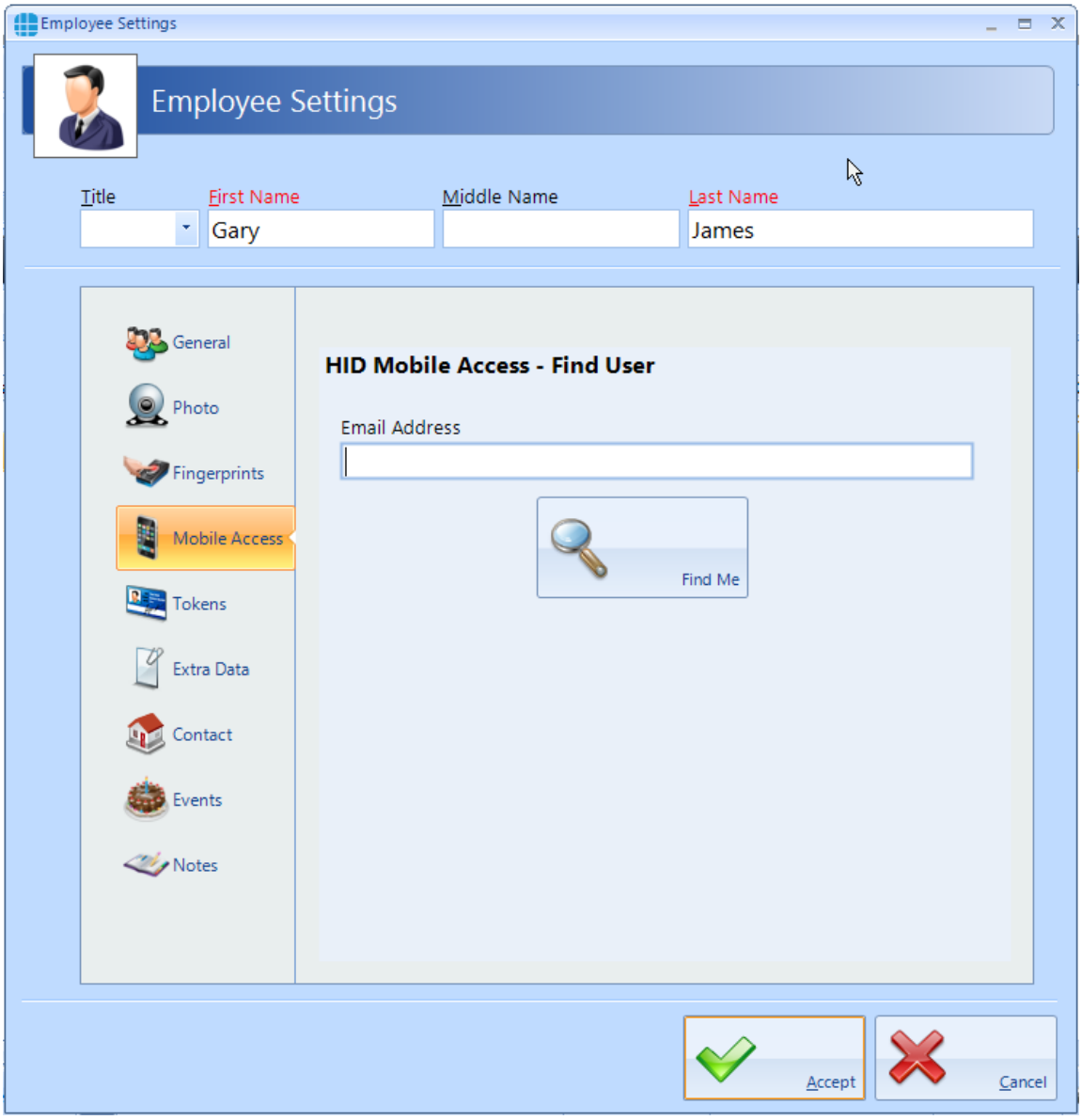
NOTE: If enrolling a Duress Fingerprint 

the system will automatically update the relevant token number into the appropriate Secondary Token field.

© 2026 Controlsoft Ltd

18.4 User Mobile Access

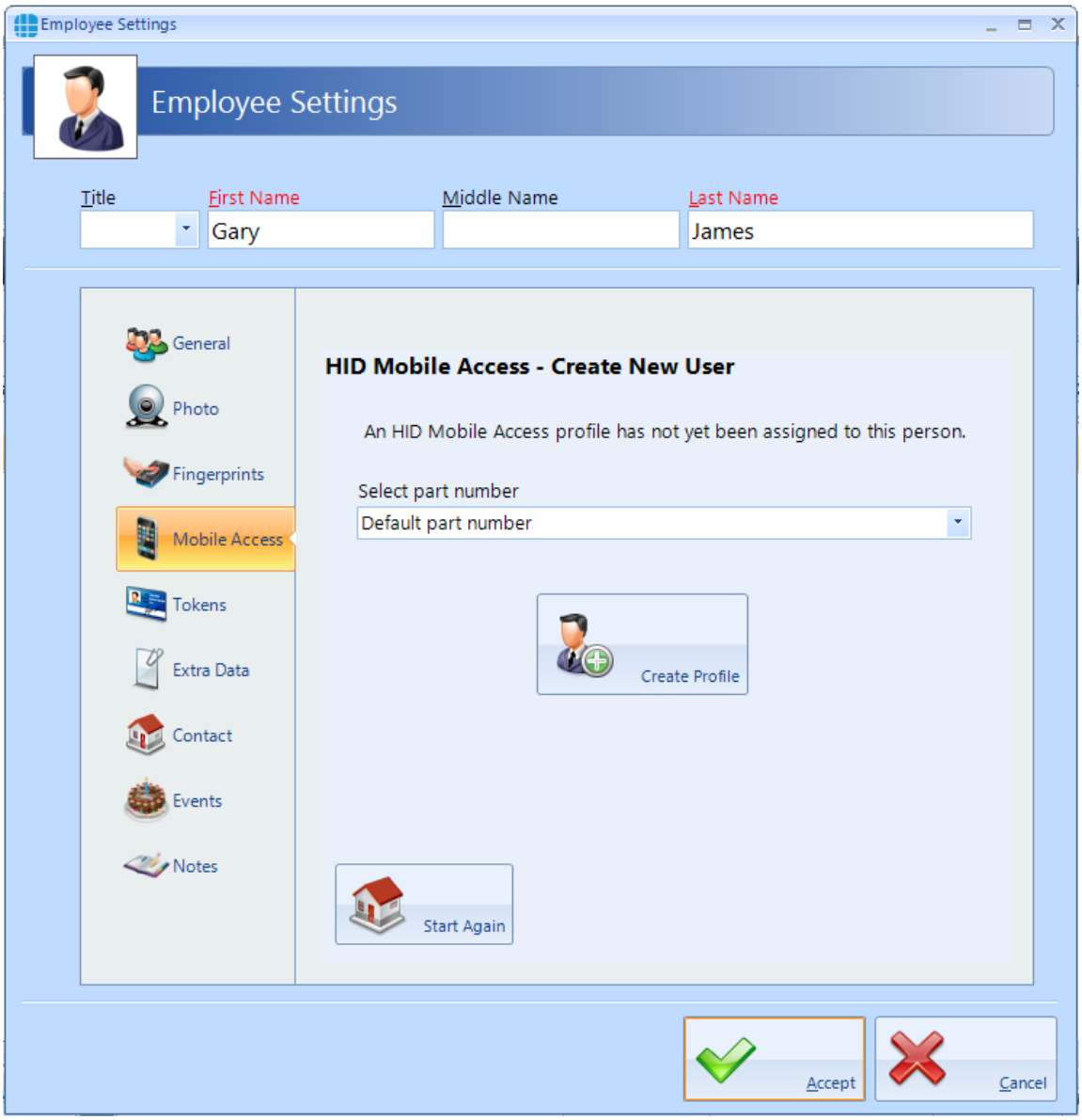
If you have a Mobile Access account, you can easily allocate mobile credentials directly from within the Identity Access software.



Enter the employee's email address (this field will be already filled in if the email address has previously been entered in the Contact section) and click the **[Find Me]** button.

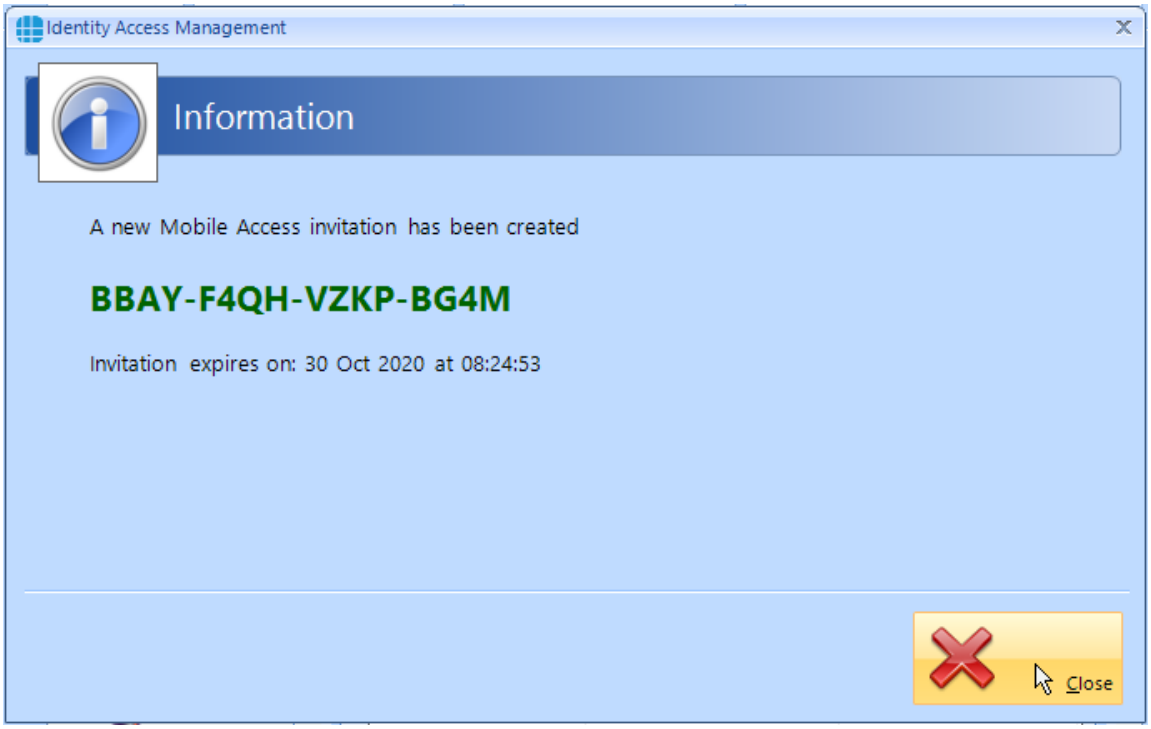
If the employee has never been issued with a Mobile Access credential, the following screen will be displayed

© 2026 Controlsoft Ltd



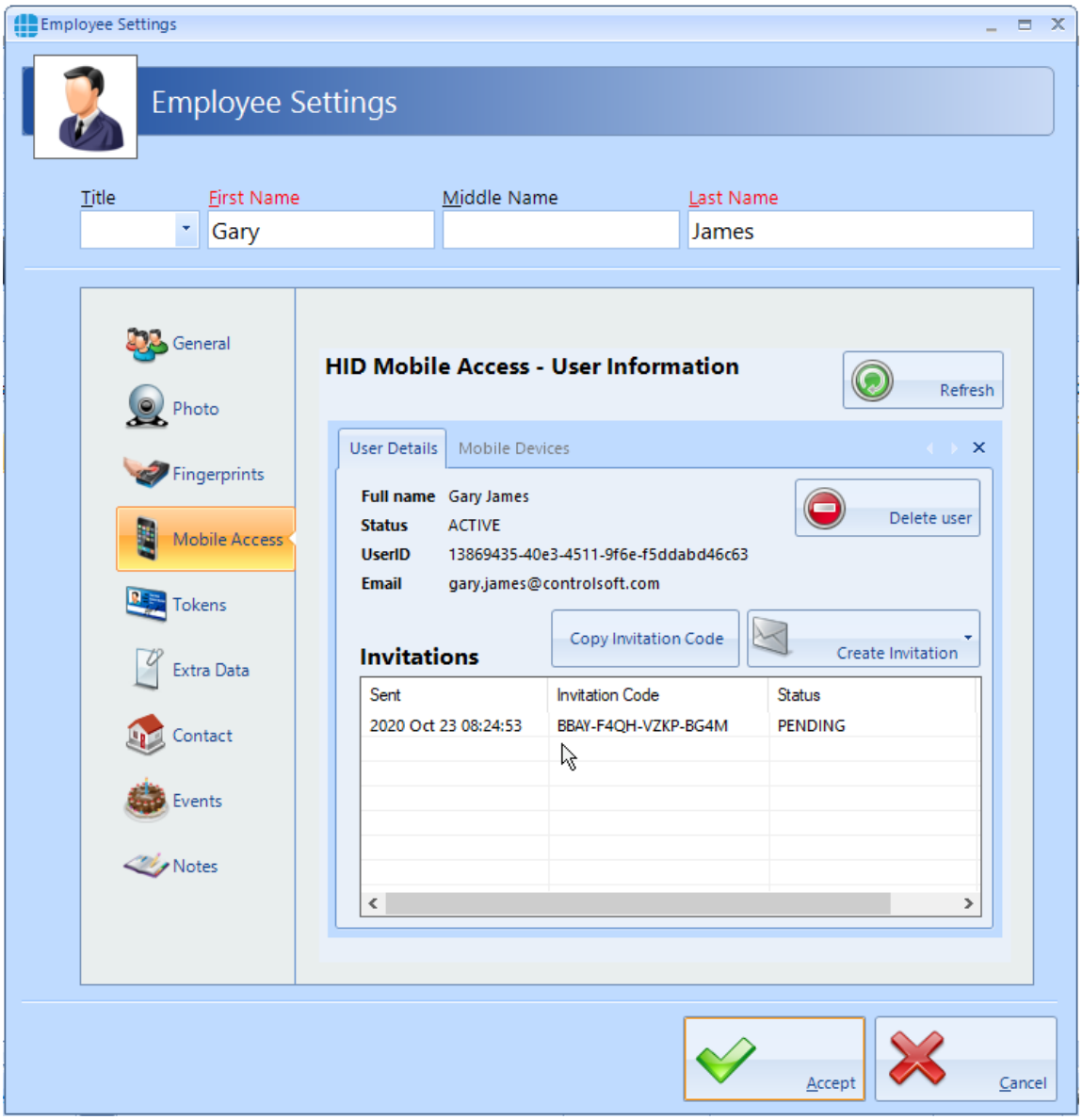
Leave the part number as **Default part number** and click on the **[Create Profile]** button. Once the system has created the profile for this employee, the invitation code will automatically be emailed to that employee (assuming that the option is selected in the IA Configuration utility, see IA Configuration - HID Mobile Access 255)

© 2026 Controlsoft Ltd



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

© 2026 Controlsoft Ltd



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.

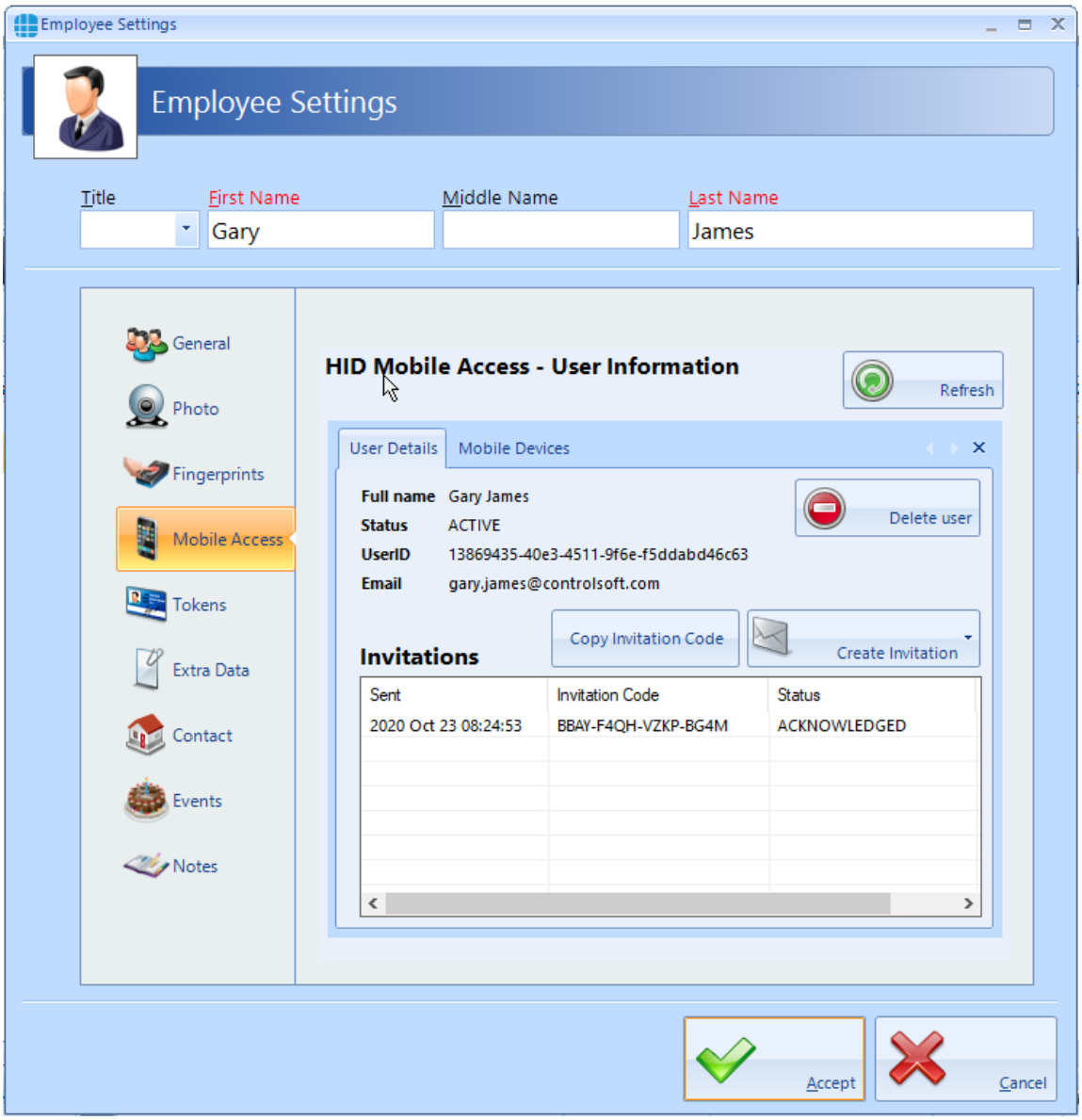
Open the app and select "**Start using the services**"

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

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

© 2026 Controlsoft Ltd

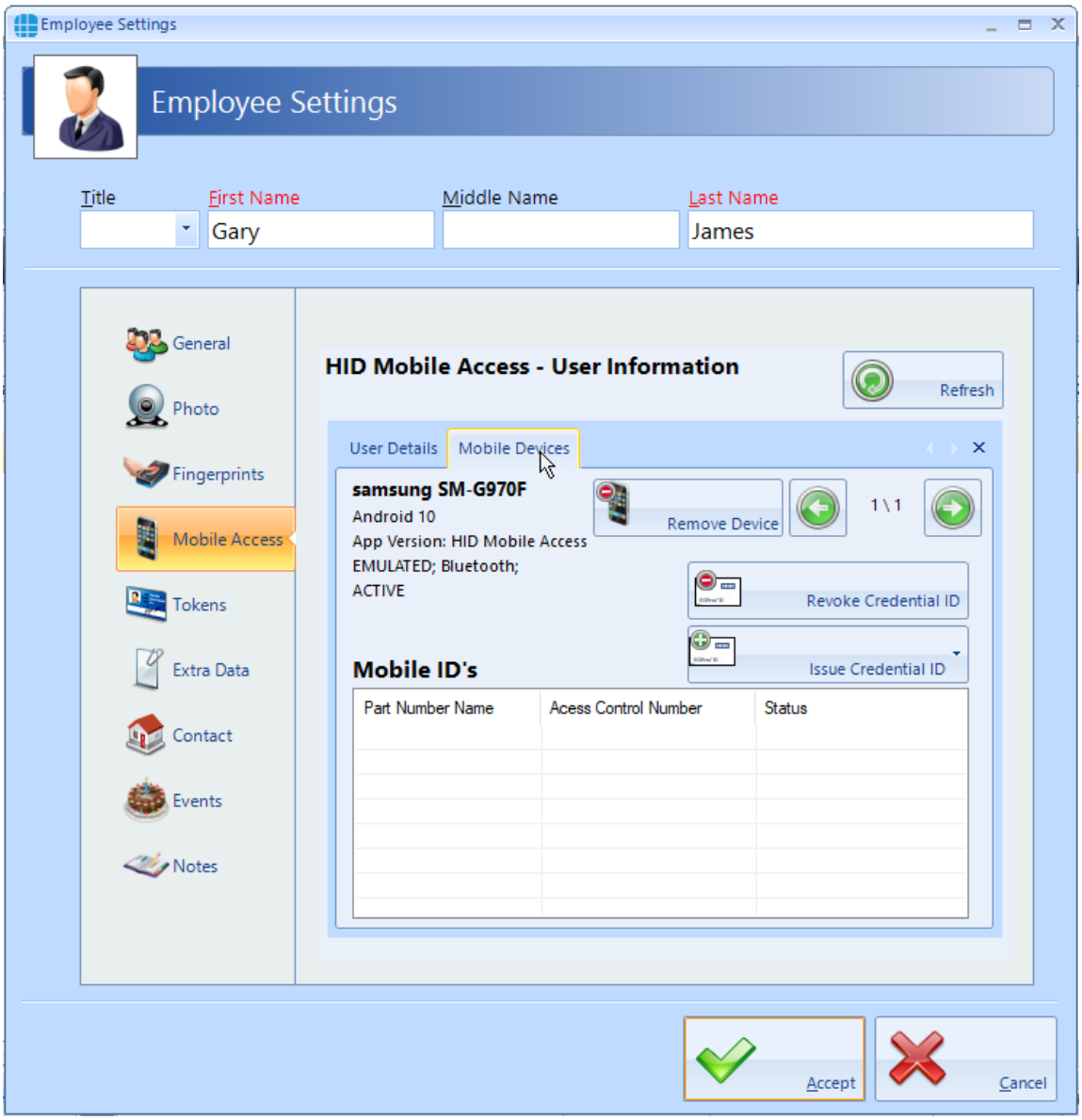


The Invitation Status is now showing as **ACKNOWLEDGED**.

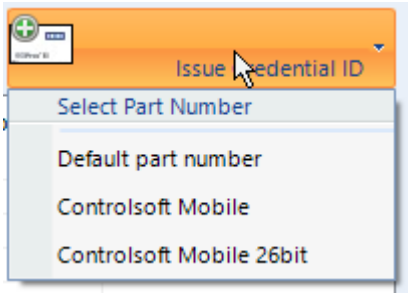
NOTE: An option exists in the IA Configuration utility called "Issue Mobile Credential ID with invitation" (see IA Configuration - HID Mobile Access 255). If this option has been selected, the invitation Status will now show as ISSUED and the next few instructions can be ignored.

Select the **Mobile Devices** tab

© 2026 Controlsoft Ltd

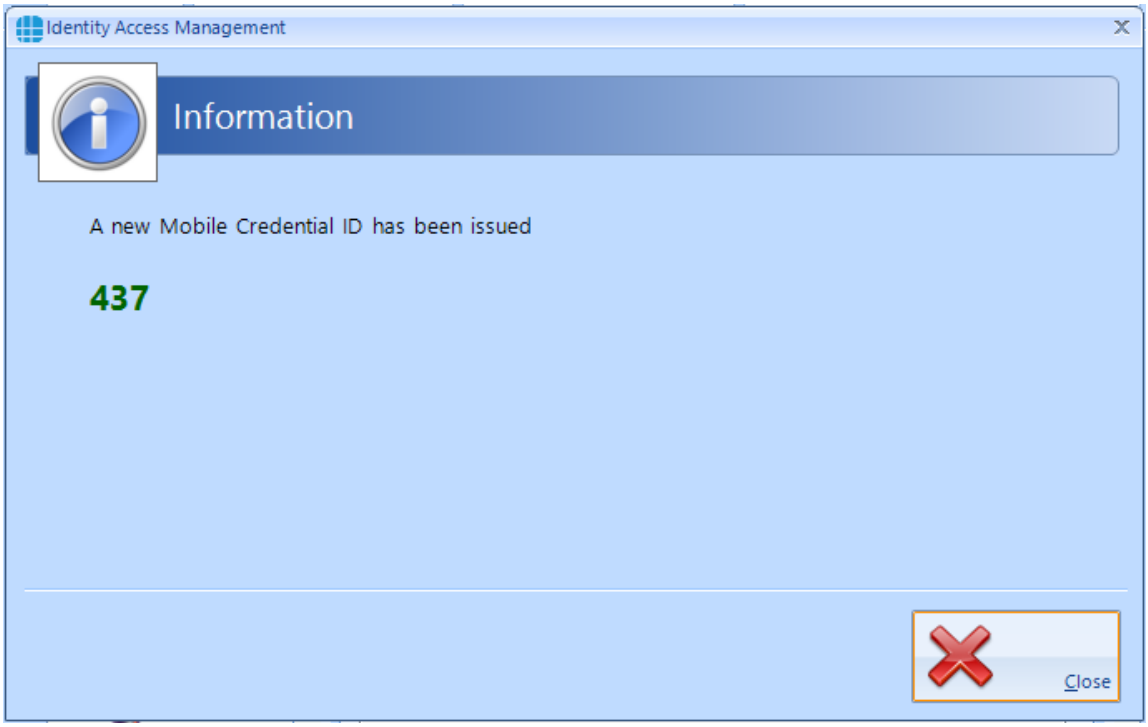


Now click the **[Issue Credential ID]** button and select the type of credential required, either **Default part number** or a specific type if different credentials are available.



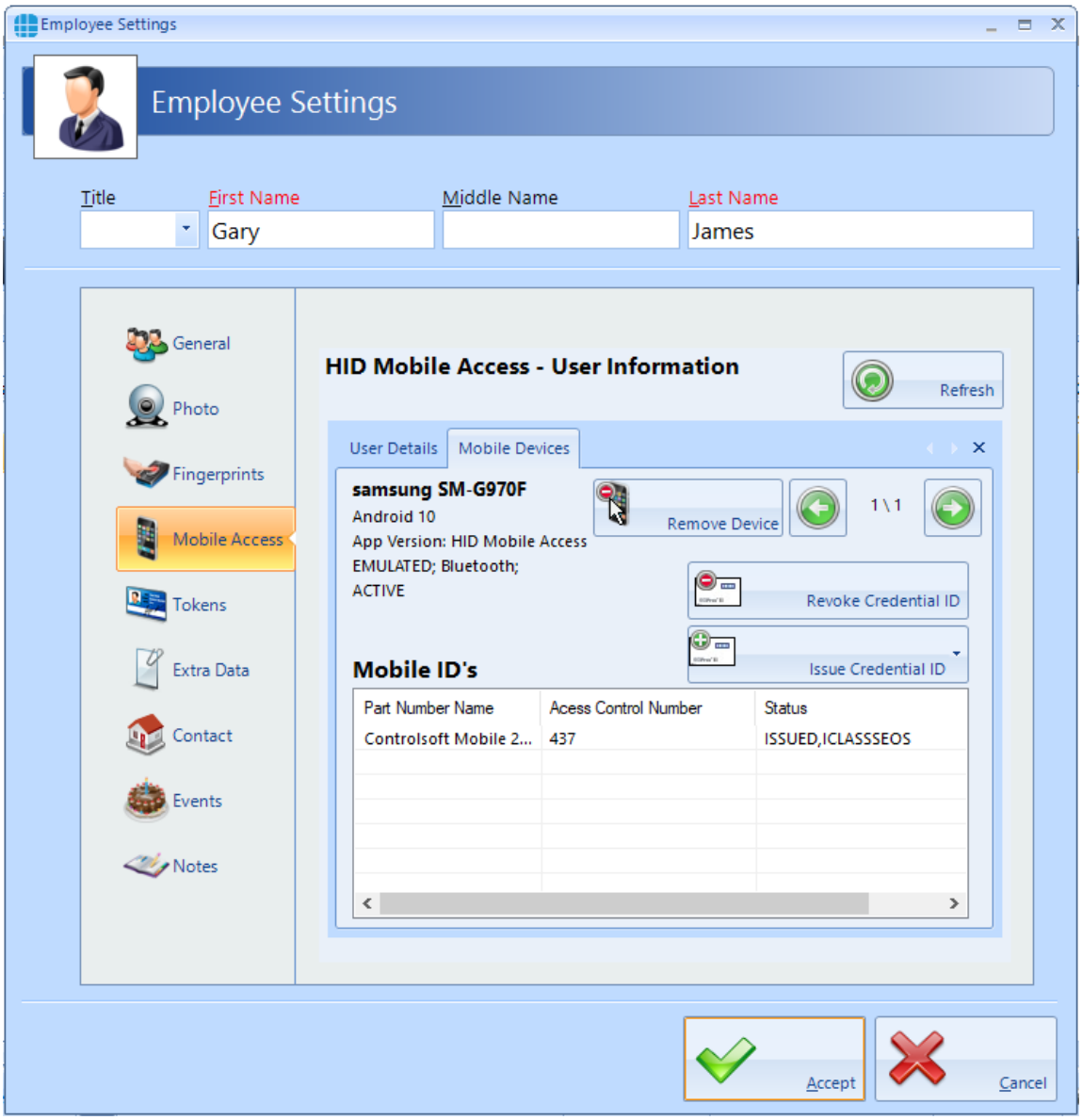
An information box will now show the credential number issued

© 2026 Controlsoft Ltd



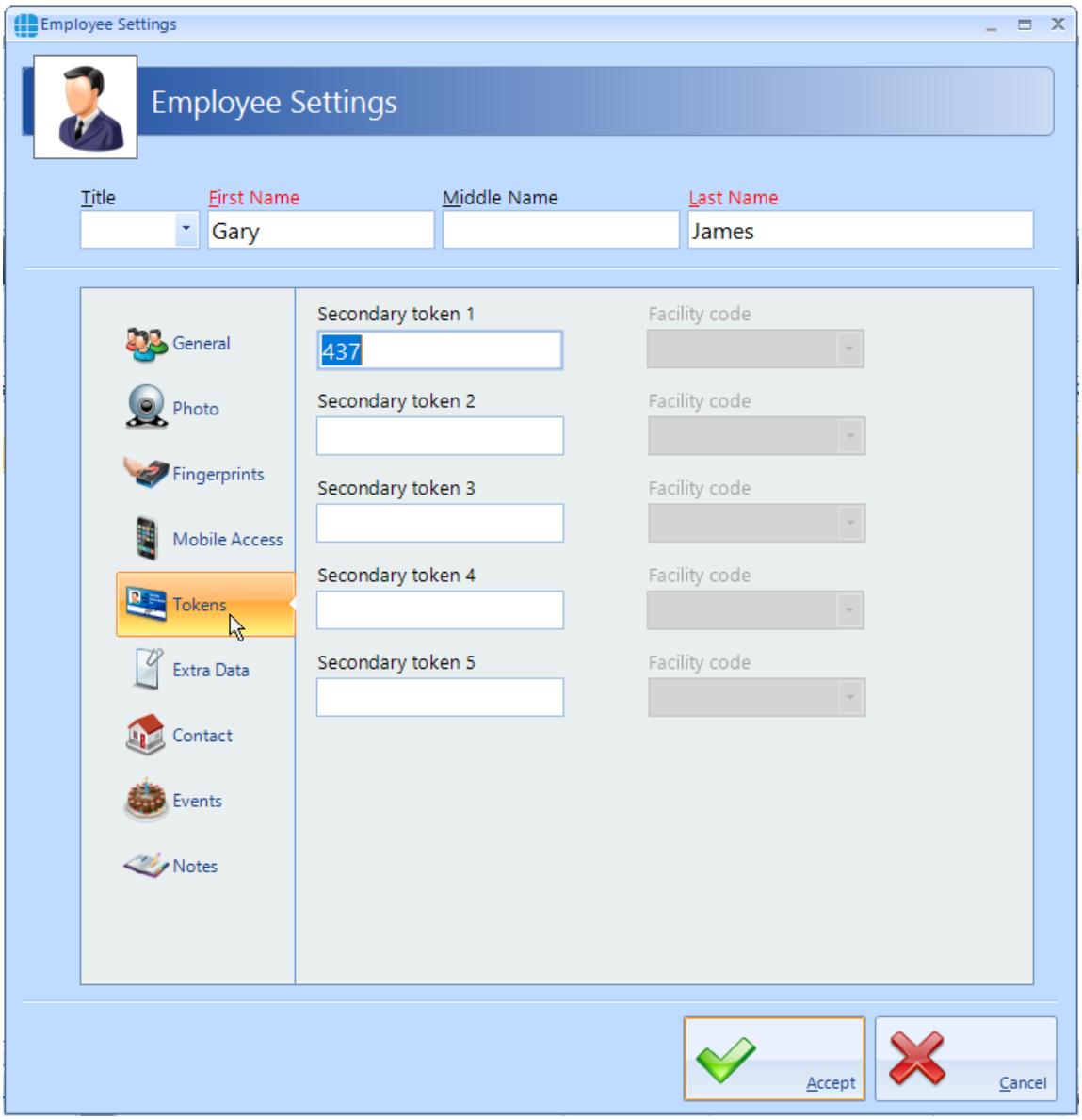
Click **[Close]** and the screen will be updated showing the status of credential 437 as **ISSUED**.

© 2026 Controlsoft Ltd



Finally check that the credential has been allocated to the employee. In this screenshot below, it has been allocated to Secondary Token 1, although this can be configured in the IA Configuration utility (see IA Configuration - HID Mobile Access 255)

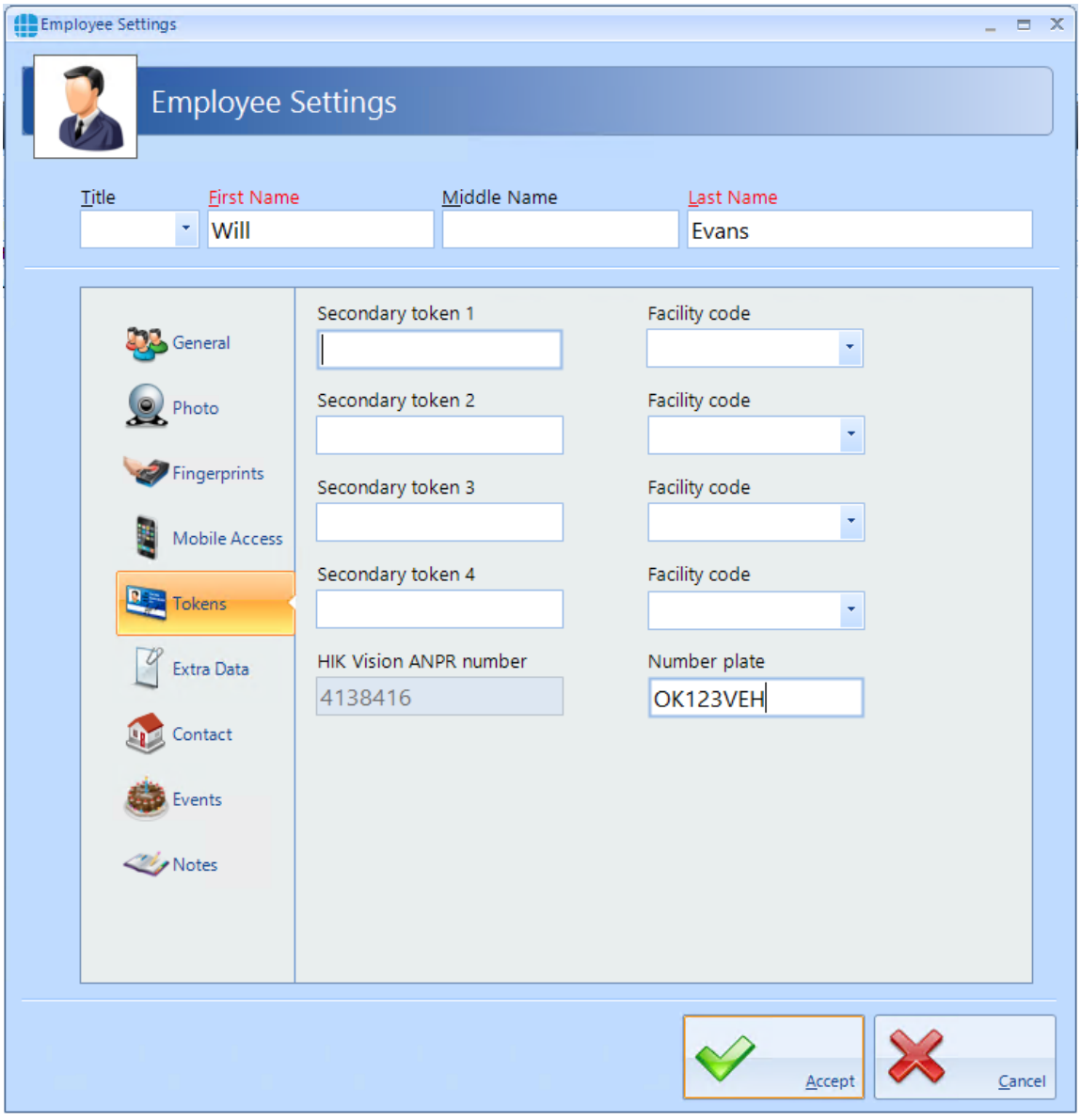
© 2026 Controlsoft Ltd



© 2026 Controlsoft Ltd

18.5 User 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 and their Facility Code 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 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" (see IA Configuration - Cards & Readers 247).

If Duress is enable in IA Configuration, other fields will be renamed accordingly.

If the Use HIK Vision ANPR option is enabled in the IA Configuration utility (see IA Configuration - Cards & Readers 247), then **Secondary Token 5** will automatically be renamed to **HIK Vision ANPR number** as in the above screenshot. This field will be

© 2026 Controlsoft Ltd

filled in automatically when a vehicle number plate is entered into the **Number plate** field.

NOTE: The ANPR number plate must be unique

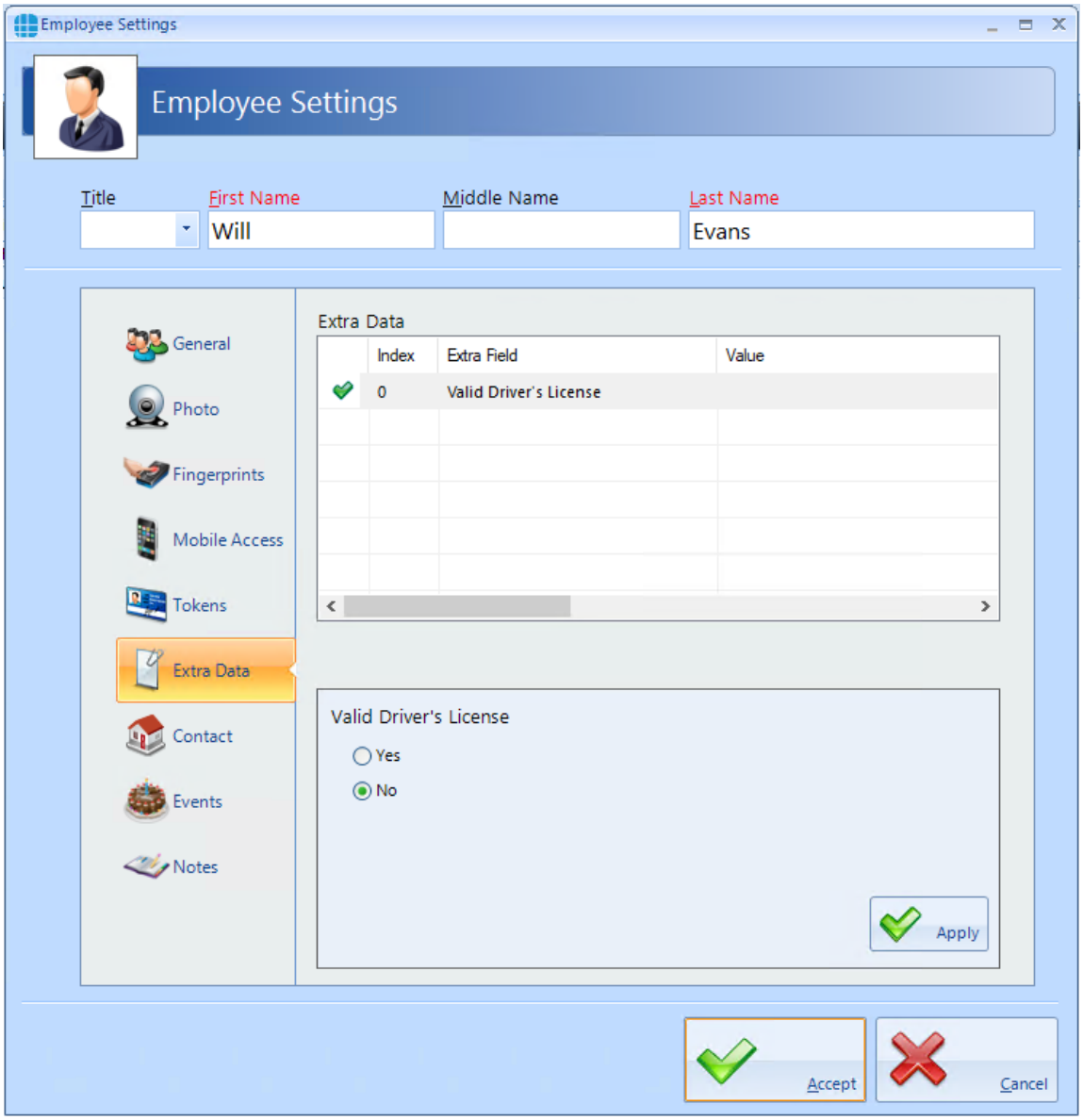
18.6 User Extra Data

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 licence, store the expiry date of the licence or even store a scan of the licence itself.

The Extra Fields are configured within the IA Configuration software (see IA Configuration - Extra Fields 262).

© 2026 Controlsoft Ltd

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



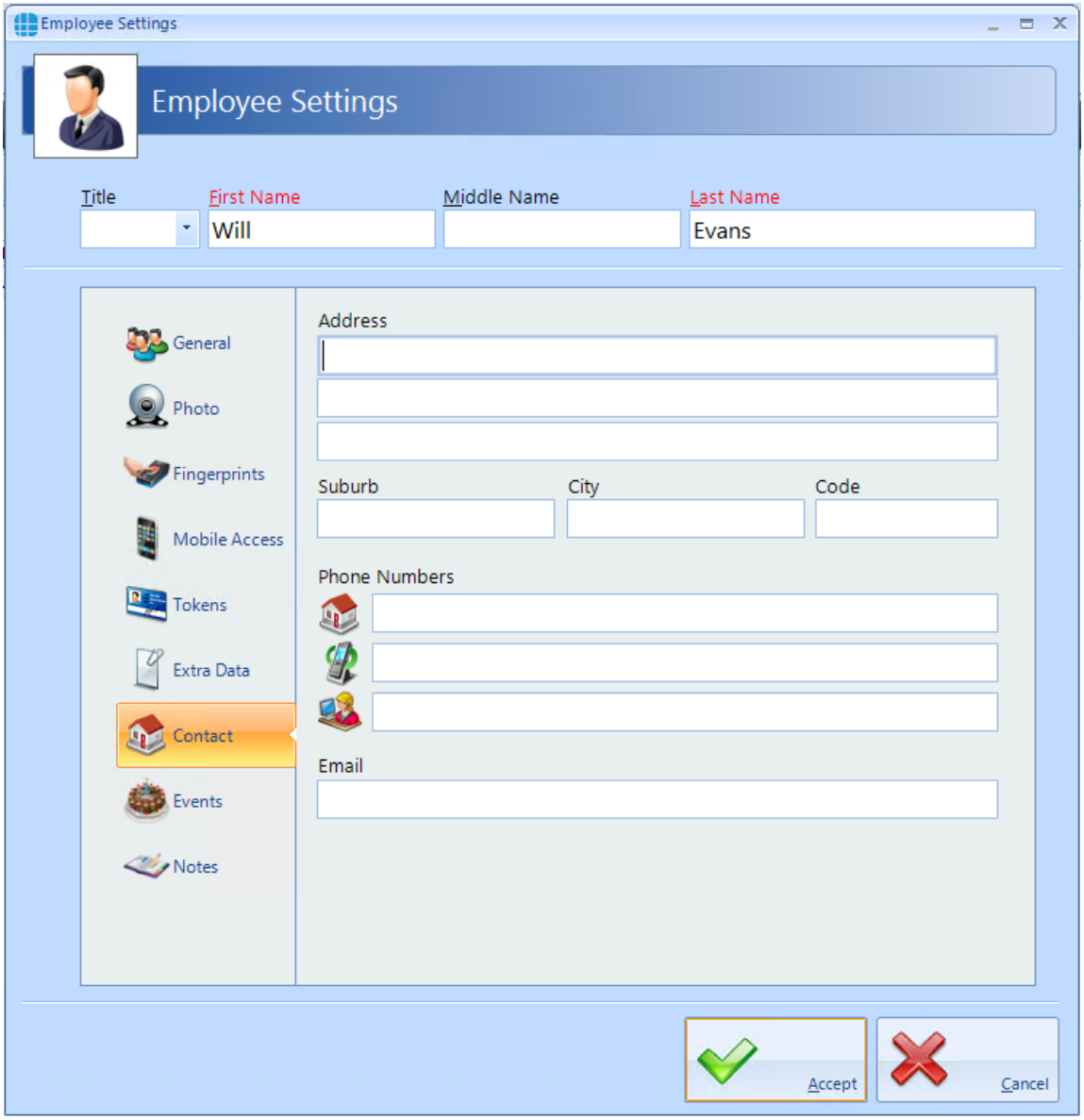
In this instance, the Extra Data Field has been configured to record whether the user has a valid driver's license. Simply select **Yes** or **No** as appropriate, followed by **[Apply]** and **[Accept]**.

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

© 2026 Controlsoft Ltd

18.7 User Contact

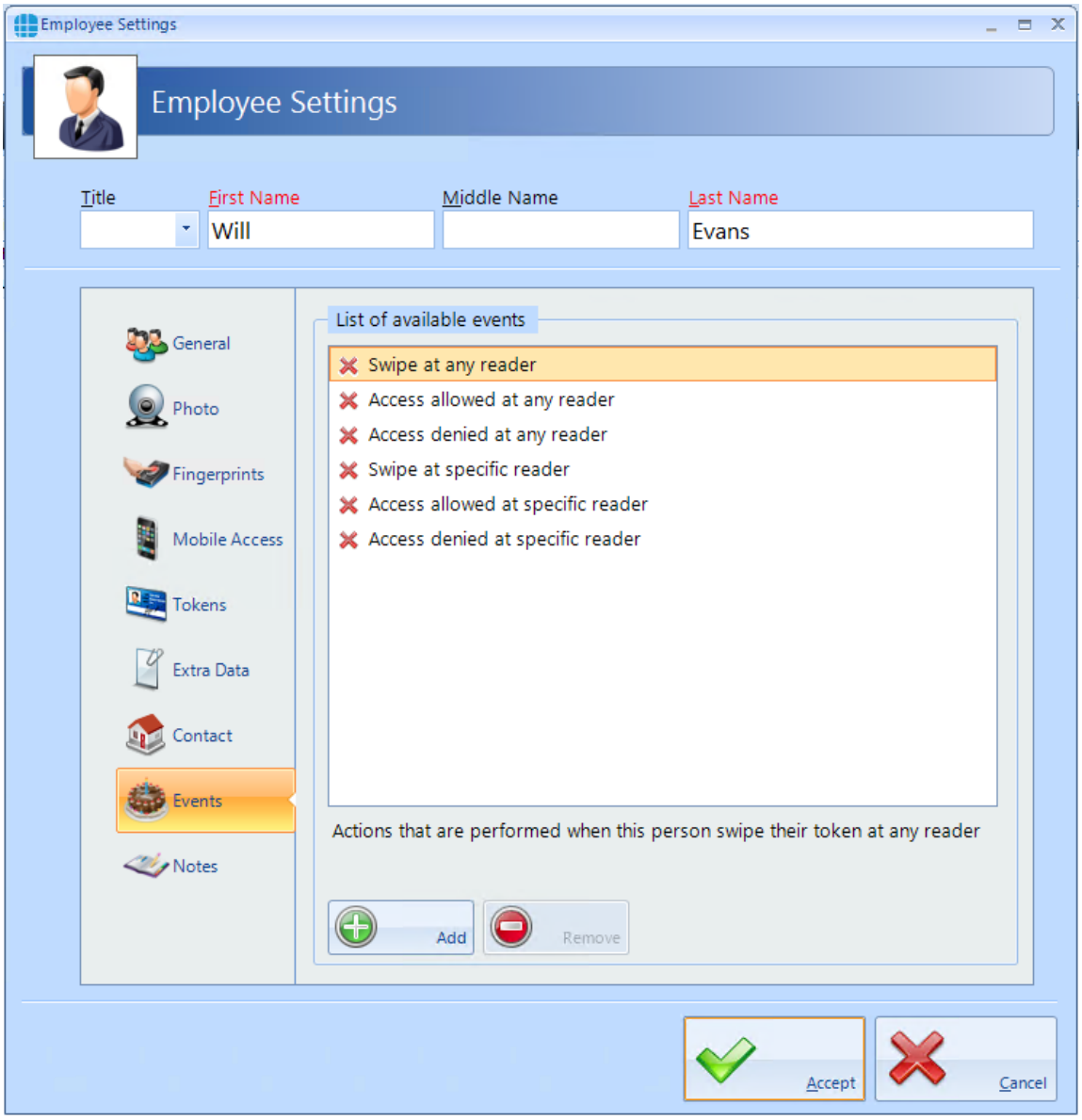
The Contact Details in this tab are not mandatory, but can be recorded if required:



18.8 User Events

The Events tab will indicate whether any Events have been configured for the selected user.

© 2026 Controlsoft Ltd

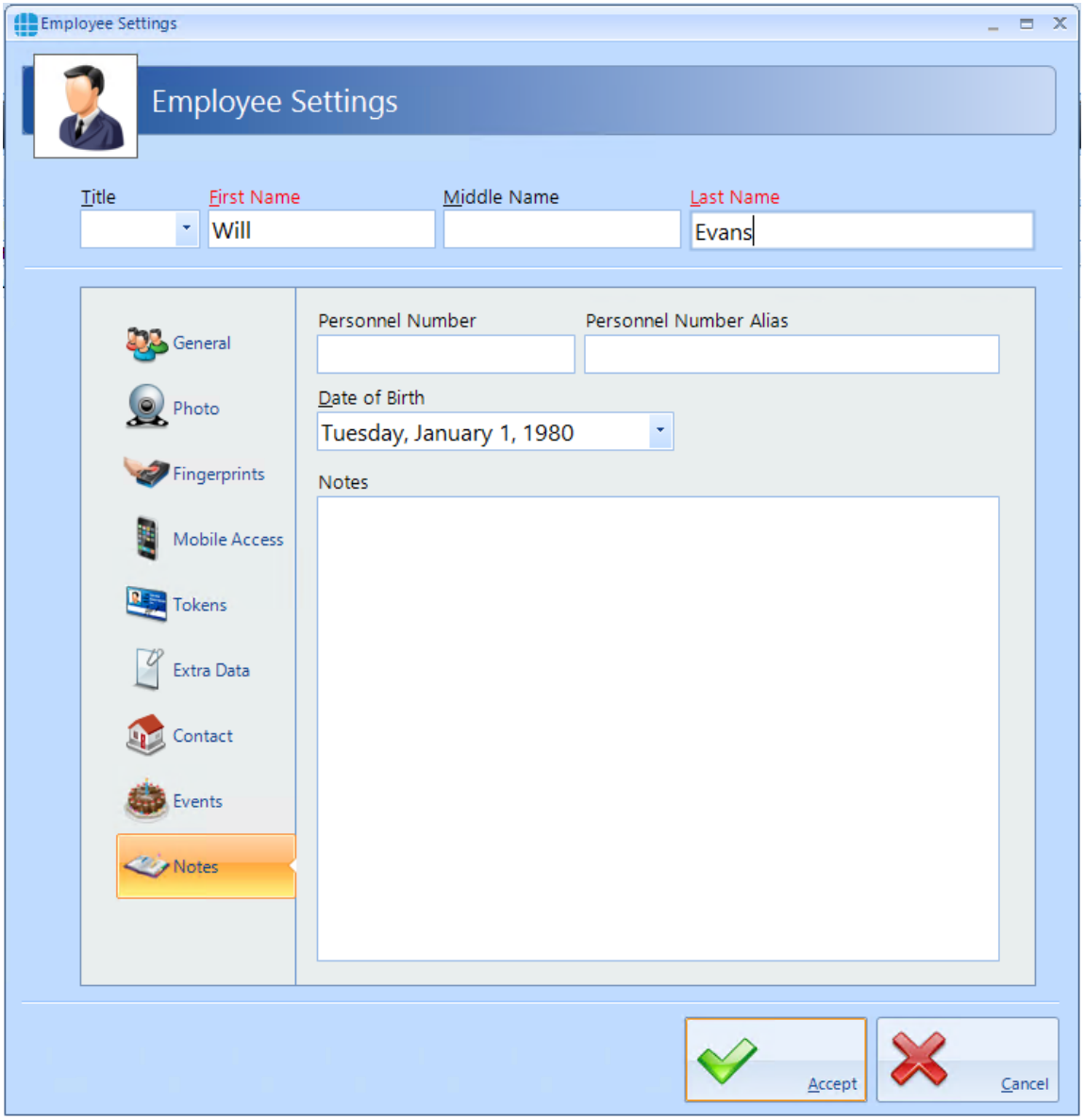


In this example, no Events have been created for the selected user. Clicking the **[Add]** button will allow Events to be created, although this is more easily done via the **Events** button in the **Advanced** tab, where all Events and related Actions can be viewed.

© 2026 Controlsoft Ltd

18.9 User Notes

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



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

 is used to automatically assign a Personnel number. This is useful if using the database for membership data. To set the parameters for the automatic assignment, see IA Configuration - Cards and Readers.

18.10 Importing Users

It is possible to import multiple users into Identity Access from another Controlsoft application (Controlsoft Lite, Controlsoft Pro or CWBio), or any other application capable of exporting its user database to a **.csv** file.

© 2026 Controlsoft Ltd

When importing from a Controlsoft application, Identity Access knows the data layout, so it is only necessary to point to the database.

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 to start the Import Wizard, then click **[Next]**

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, then click **[Open]**. Select **Delete old data before importing new data** if required. Click **[Next]**.

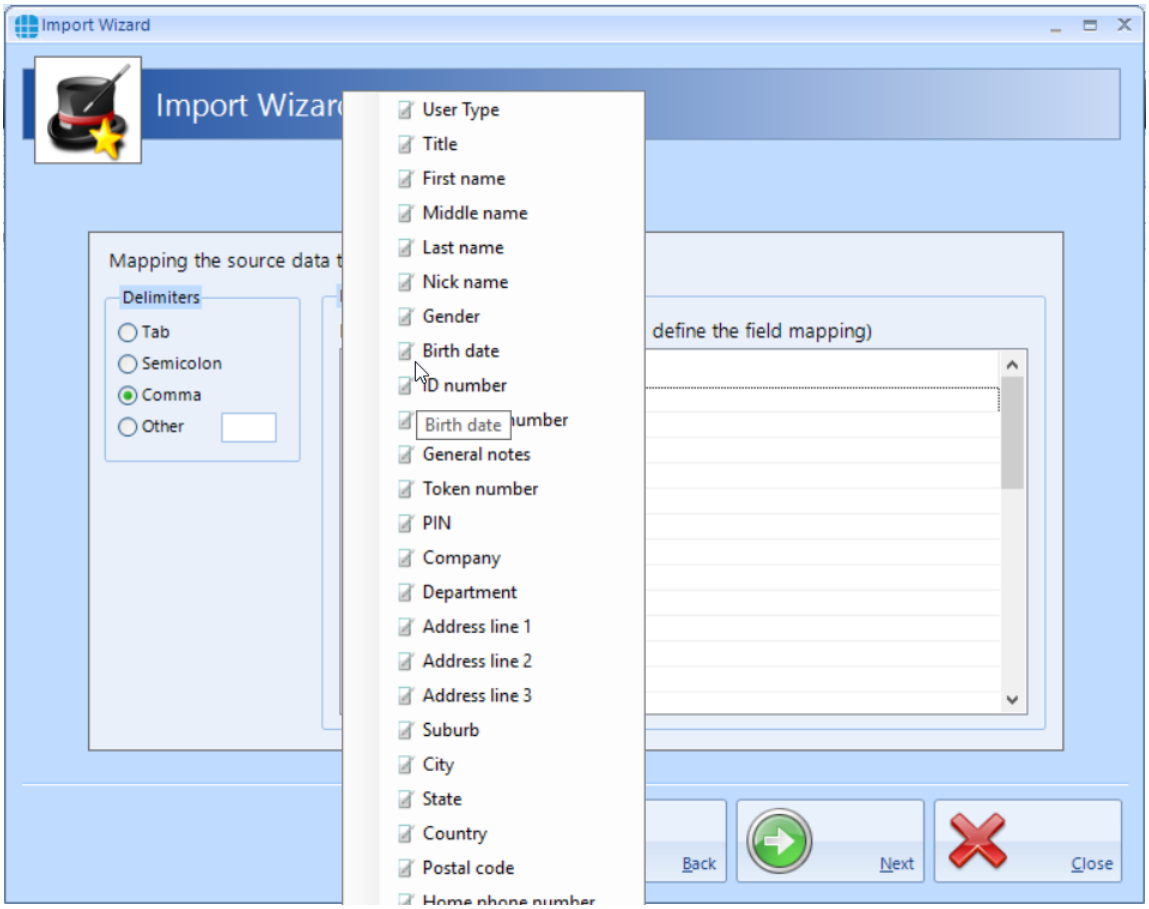
Select Destination should be set to define the types of user being imported (Employee, Visitor or Contractor). Select **Ignore duplicate names** to avoid duplicate entries. Click **[Next]**
NOTE: While this will stop a User appearing in the list twice, it will also stop a new User from being imported if they have the same name as an existing User. To avoid this, always ensure that each user has a unique name (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]**

© 2026 Controlsoft Ltd

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:



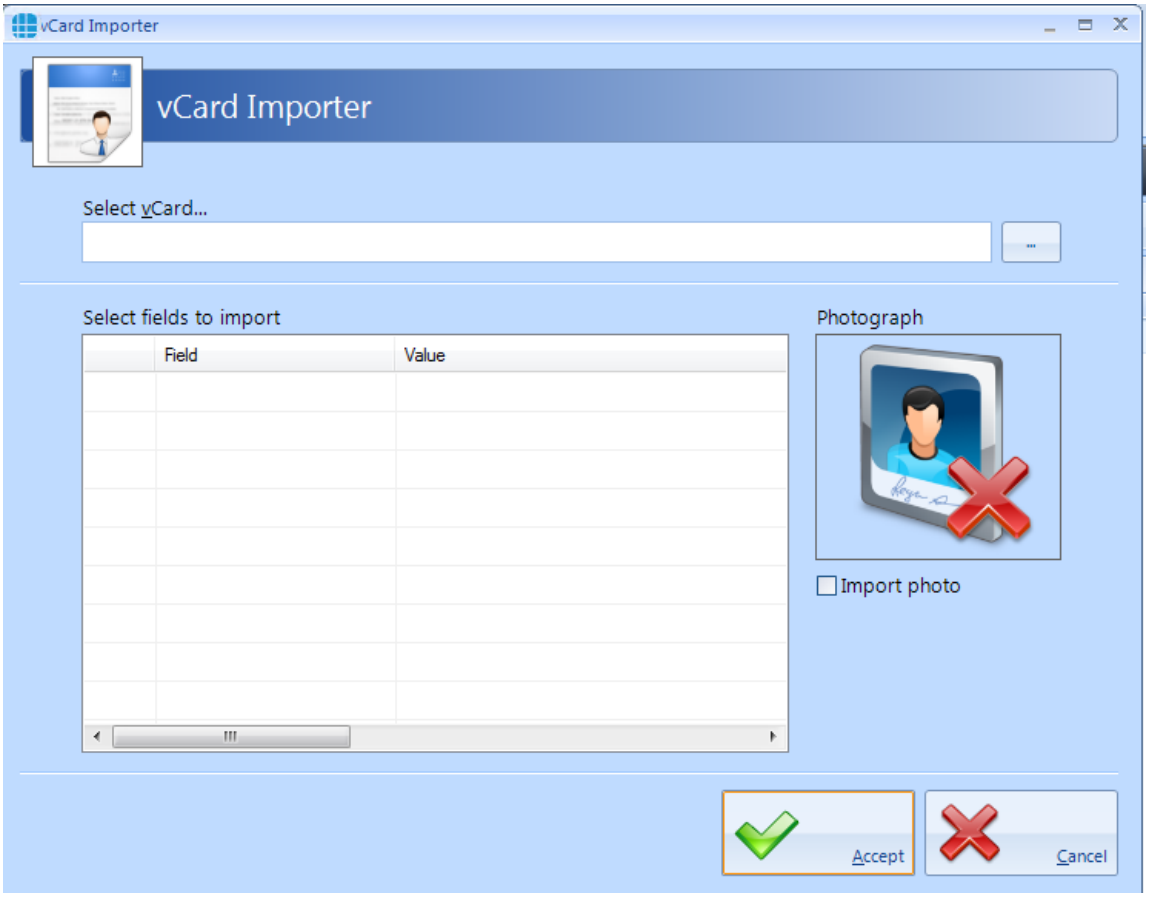
When complete, click **[Next]**, followed by **[Import]** to start the import process and **[Close]** when the import is complete.

Identity Access also has the facility to import a user via a "vCard" which can be created from some email clients such as Microsoft Outlook. To import a vCard, select

Employees from the Management tab, then select the **Import** icon 

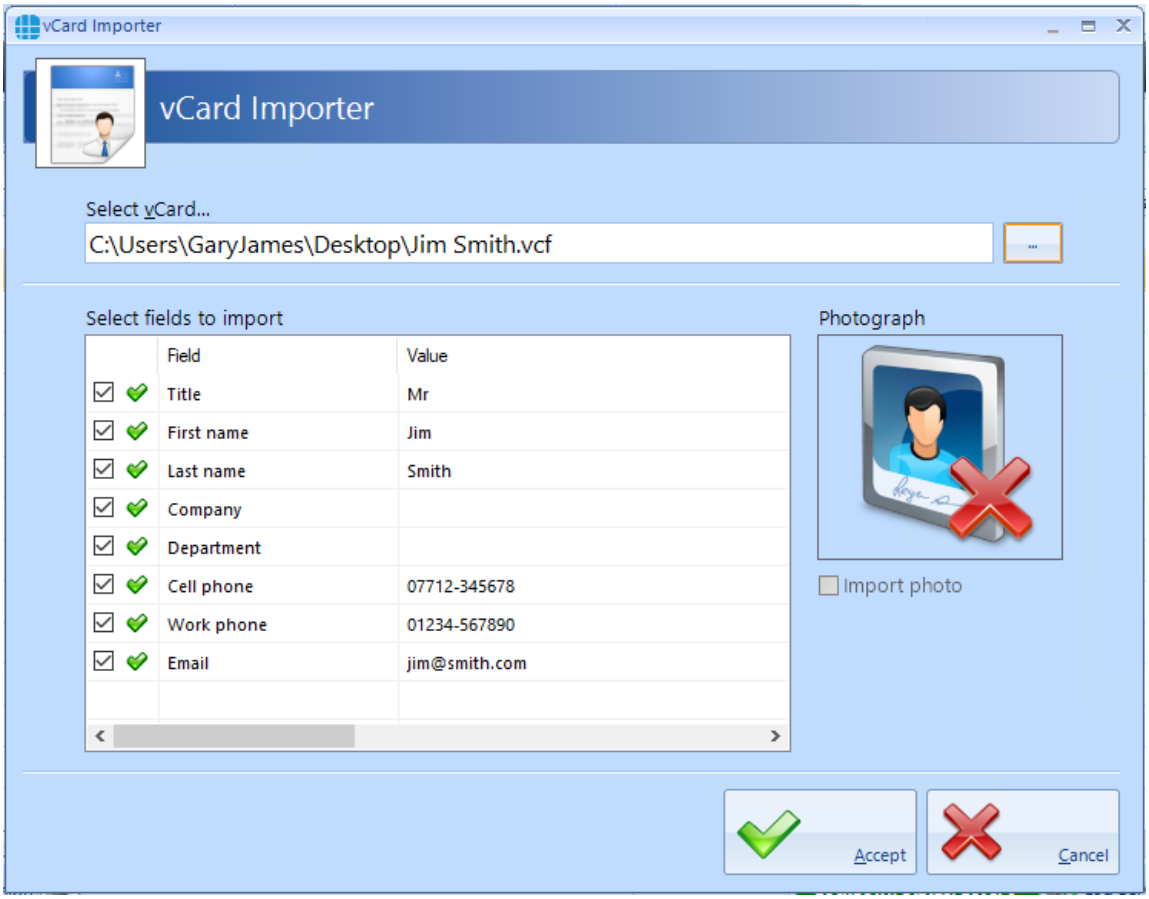
© 2026 Controlsoft Ltd

NOTE: it is not possible to import vCards for Visitors or Contractors.



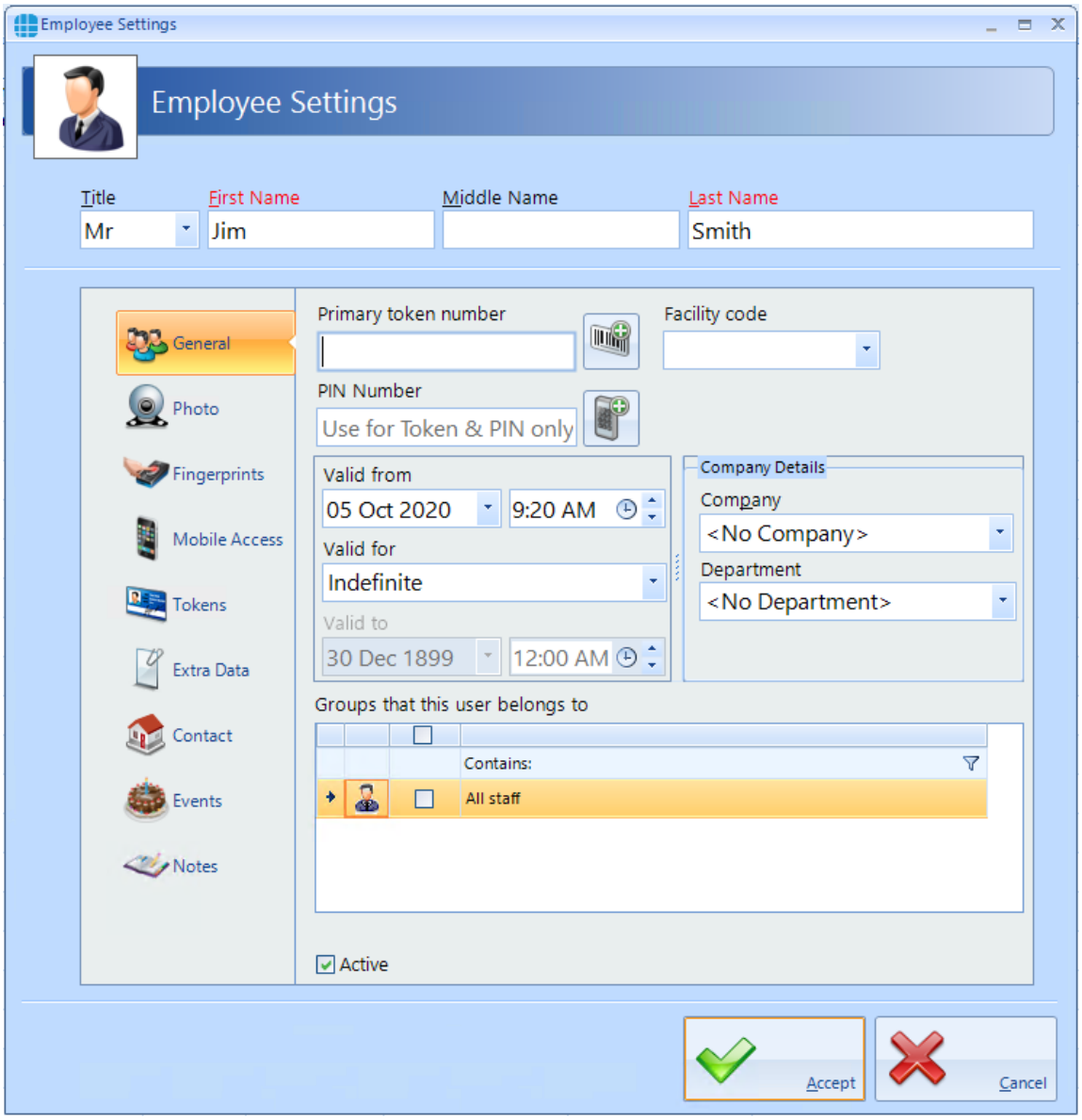
Use the **[...]** button against **Select vCard** option to browse to the vCard and click **[Open]**.

© 2026 Controlsoft Ltd



Once imported, the Employee Settings screen automatically opens for that user.

© 2026 Controlsoft Ltd



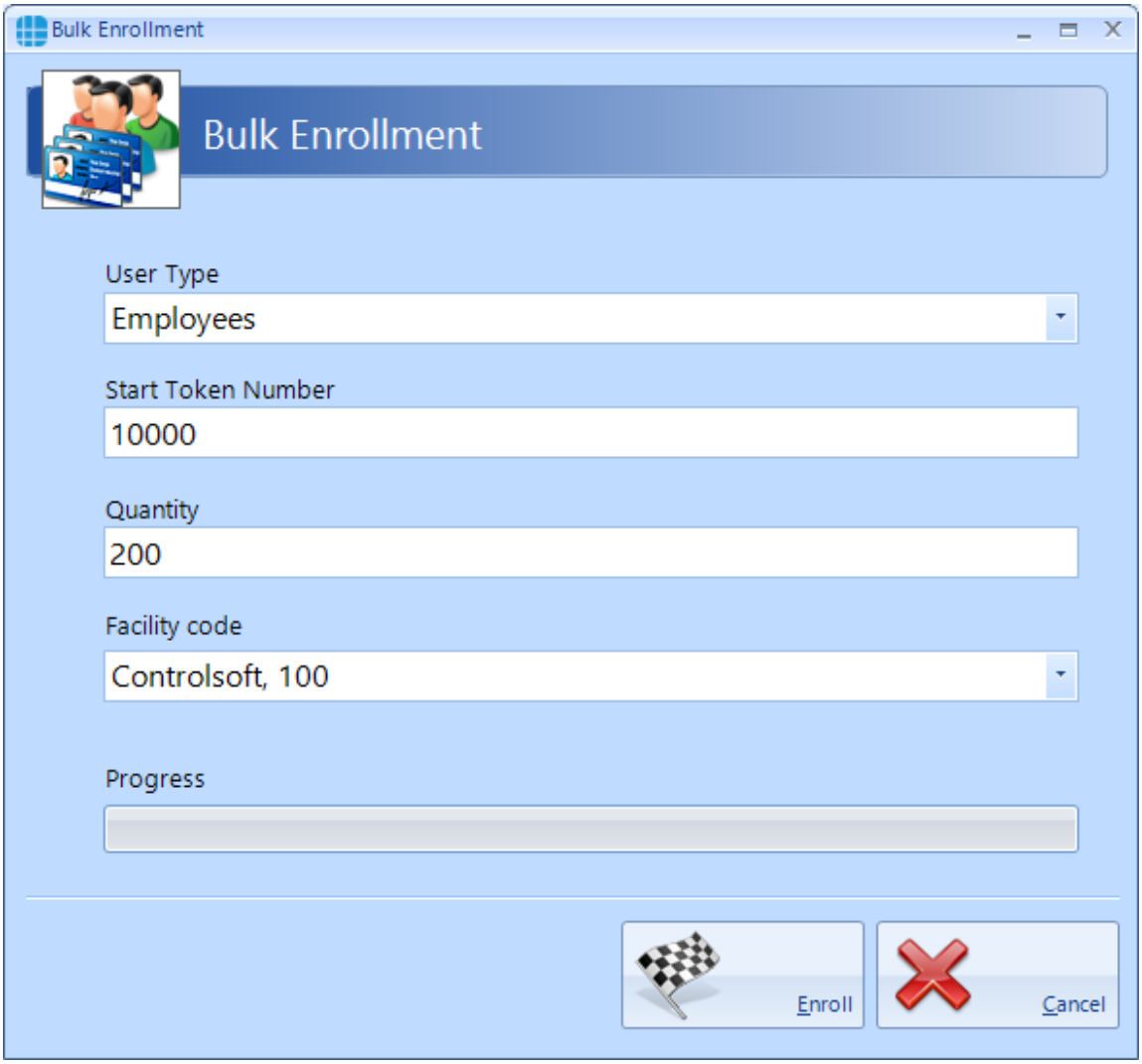
© 2026 Controlsoft Ltd

User Admin > Bulk Enrolment

19 User Admin > Bulk Enrolment

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:



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

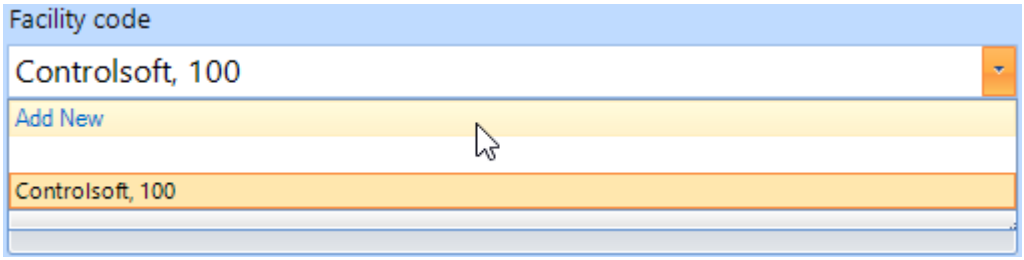
Enter the **Start Token Number**

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

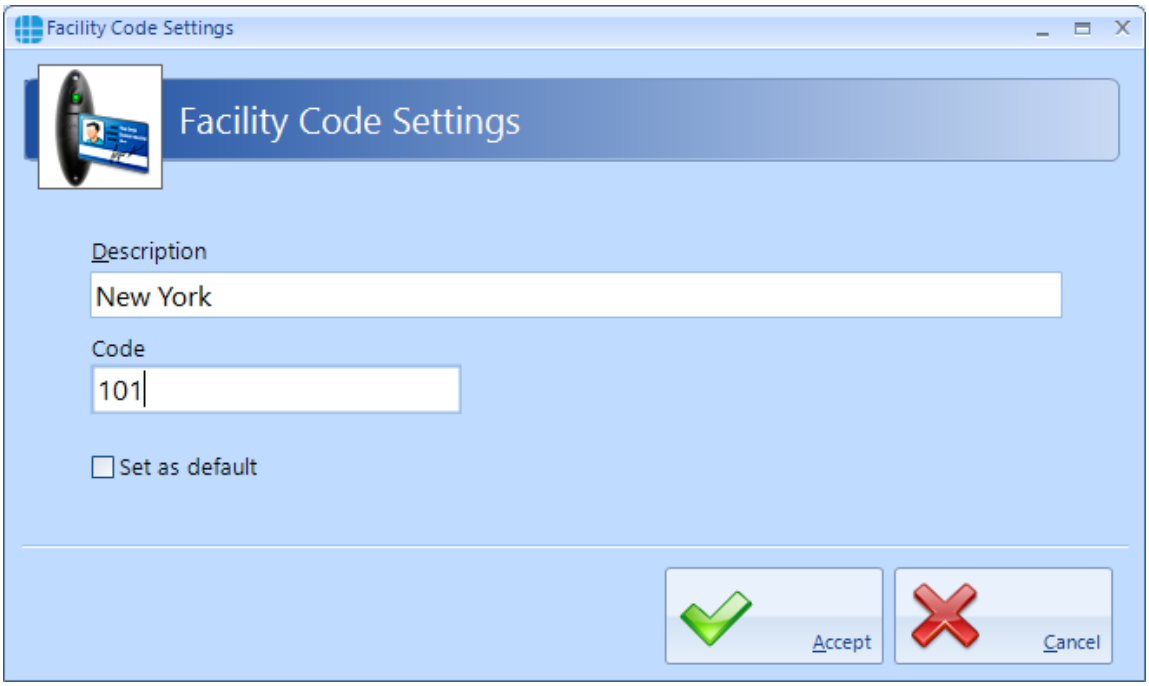
Select or Add a new **Facility Code.**

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

© 2026 Controlsoft Ltd



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**.



© 2026 Controlsoft Ltd

Advanced Tab

20 Advanced Tab

The "Advanced" tab introduced in v9 software provides a variety of new and exciting options to further enhance the flexibility of the Identity Access system. These Advanced features require an Identity Access licence as described below:

Professional Features Licence for Medium Systems (Part No. IA-PRO) Enables all Advanced features, limited to 64 doors & readers

Enterprise Features Licence for Large Systems (Part No. IA-ENT) Enables all Advanced features and not limited in size

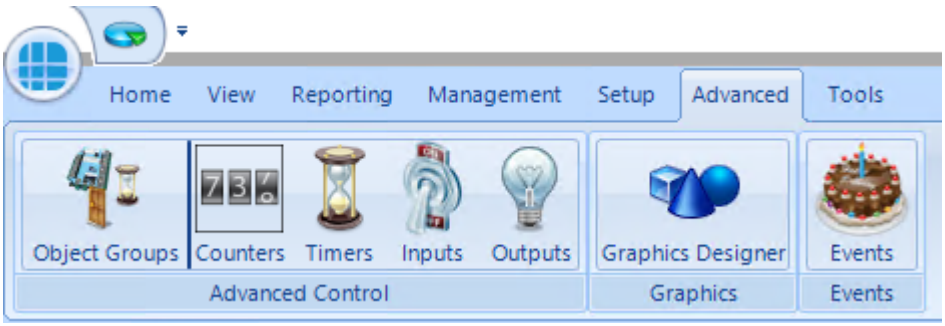
The type of Licence applied will be indicated in the About screen in the Home tab:



The Advanced features allow you to program inputs and outputs of controllers across the network for custom features. Object groups allow control of multiple controllers with a single command e.g. your Main building controllers and a secondary building's controller which may be geographically separate. The graphics designer allows you to see events such as doors being opened in a graphical plan of your environment. And finally, Events – simple "If / Then" type programming using the Events wizard – e.g. a battery failure on a controller can generate an email alert.

Click on the **Advanced** tab to view the options available:

© 2026 Controlsoft Ltd



Object Groups: Object Groups allow various objects to be grouped together to allow a single command to be sent to multiple devices.

Counters: Counters can be used to count the number of times an event occurs.

Timers: Timers can be used to introduce time delays in events and actions.

Inputs: It is possible to define an input for use with the Advanced functions.

Outputs: It is possible to define an output for use with the Advanced functions.

Graphics Designer: The Graphic Designer allows a floor plan of the site to be created, with interactive icons on the floor plan to represent doors, readers, outputs etc.

Events: Events and Actions increases the flexibility by allowing the system to react to predefined activity such as triggering a specific output when a specific input activates.

20.1 Advanced > Object Groups

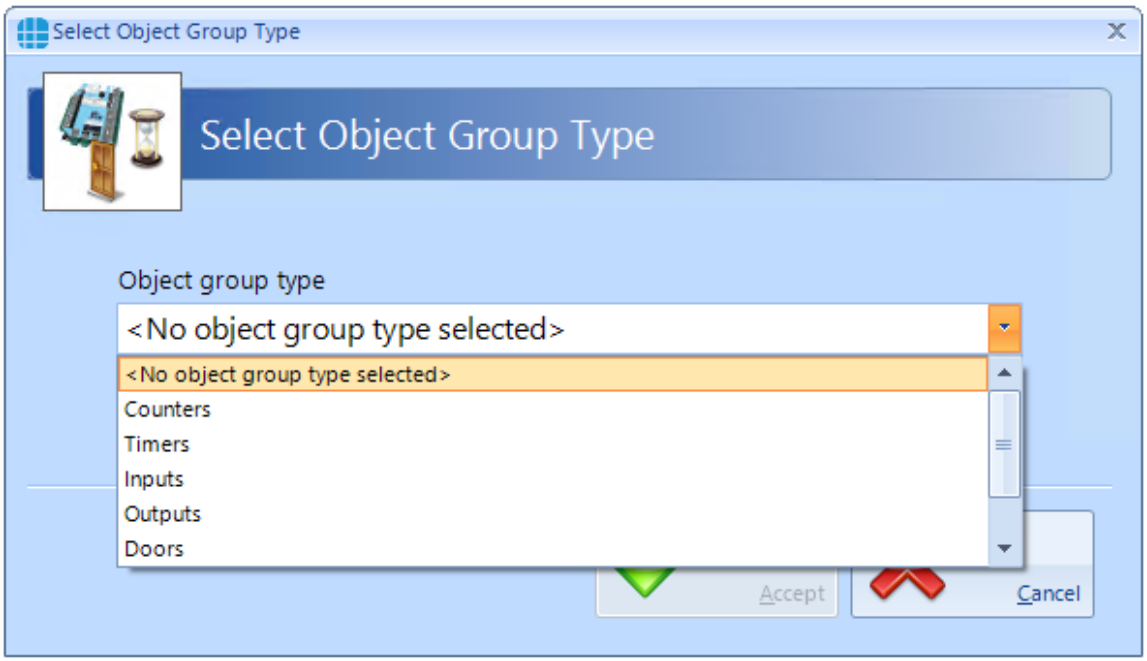
Object Groups allow various objects to be grouped together to allow a single command to be sent to multiple devices. Objects that can be grouped include Controllers, Doors, Card Readers, Counters, Timers, Inputs or Outputs.

By grouping objects, it is possible to simultaneously change the status of every object in the group. Typical examples for this feature would be:

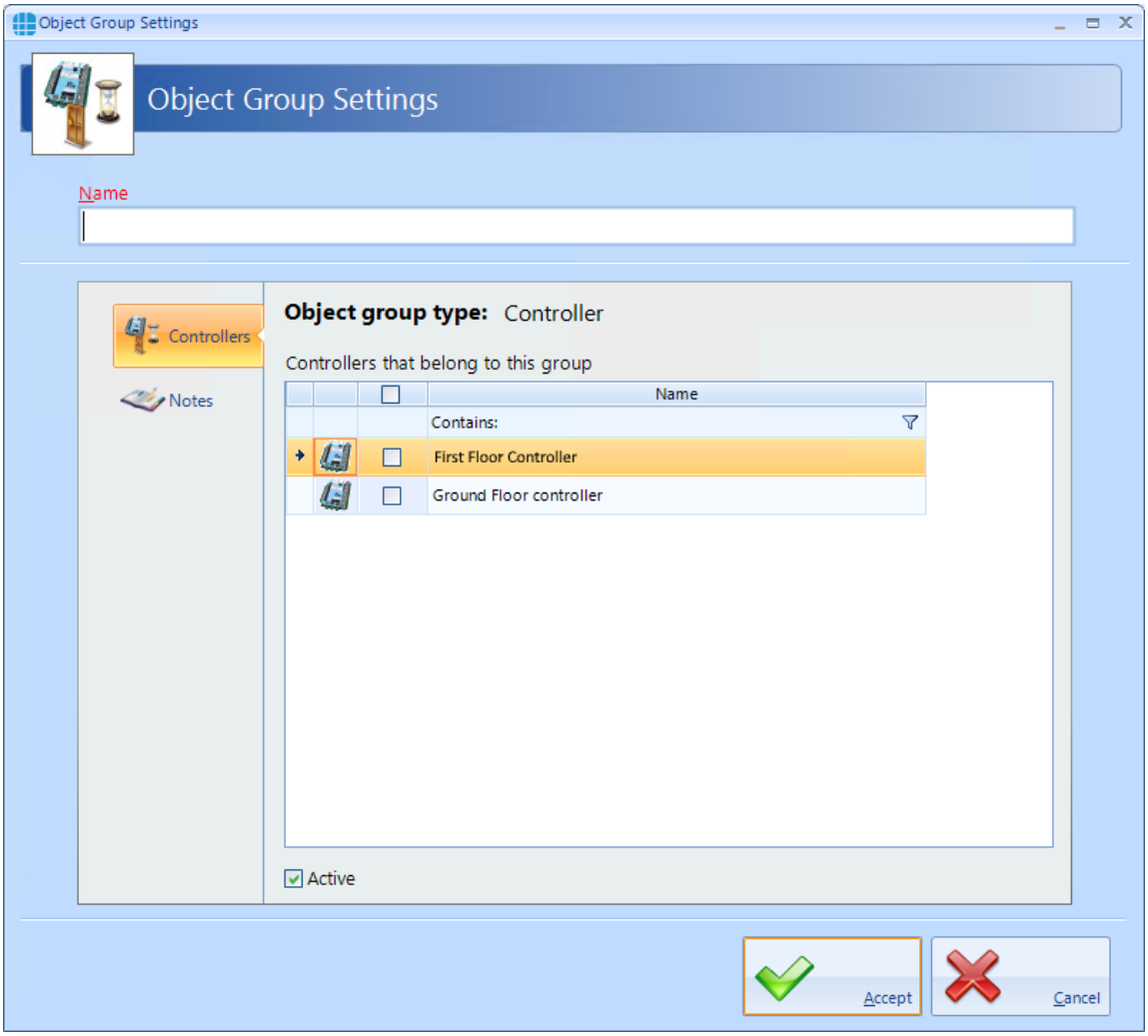
- To detect a fire alarm for a specific controller in the main building, then trigger a fire alarm to all other controllers in the same building, but not in any of the outbuildings.
- To reset all the counters in a group
- Disable all card readers in a group

To create an Object Group, select the **Advanced** tab, click on the **Object Group** button in the ribbon bar and click the **Add** button 

© 2026 Controlsoft Ltd



Enter the object group type (controllers in this example) and press **[Accept]**



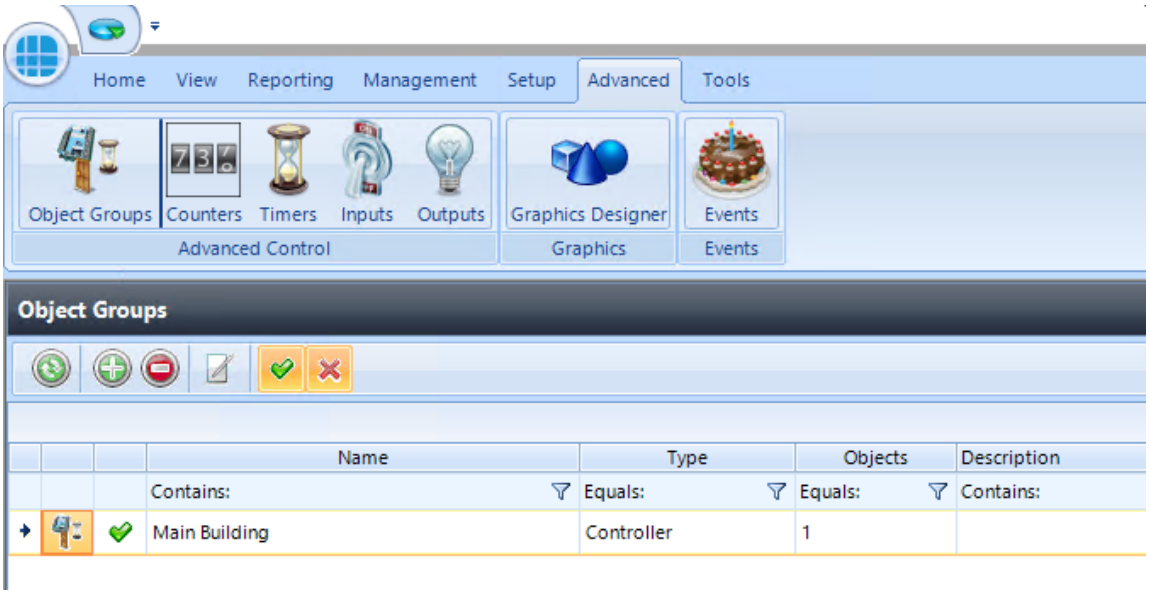
Name: Enter a meaningful name for the Object Group

© 2026 Controlsoft Ltd

Controllers that belong to this group: Select the controllers which will be included in the group

Ensure that the **Active** option is selected for the Object Group to work.

Press **[Accept]** to save the object group which will then be displayed in the Object Groups window



20.2 Advanced > Counters

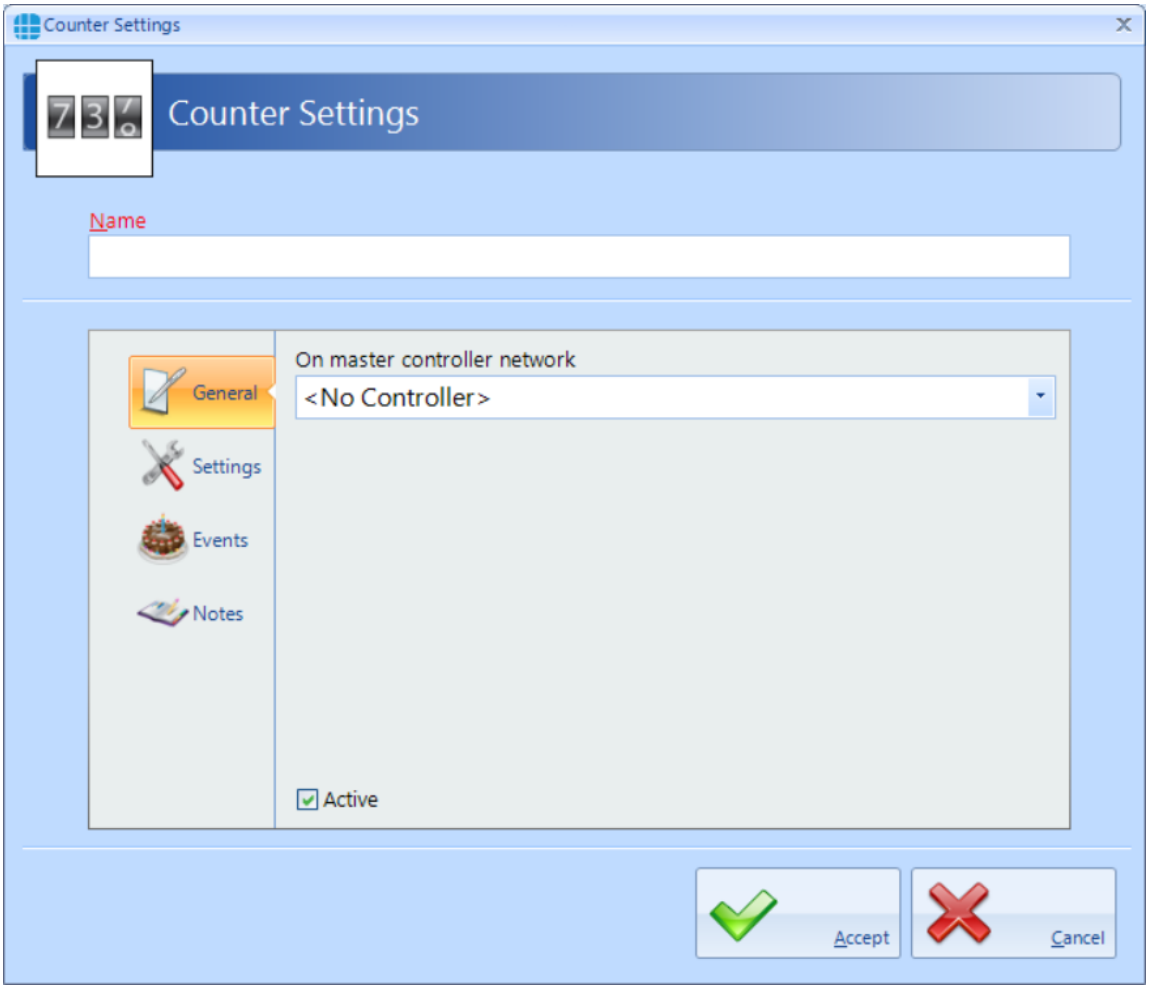
Counters can be used to count the number of times events occur. The counter can be incremented, decremented or reset, and it is also possible to check whether the counter is less than, equal to, or greater than one of 3 programmable set points.

Example: to limit the number of people in an area, create a counter with initial value = 0 and threshold = 10 then create following Events and Actions

- For Event "entry reader = grant access", Action = "increment counter"
- For Event "exit reader = grant access", Action = "decrement counter"
- For Event "counter = threshold", Action = "disable entry reader"
- For Event "counter < threshold", Action = "enable entry reader"

To create a counter, select the **Advanced** tab, click on the **Counter** button in the ribbon bar and click the **Add** button 

© 2026 Controlsoft Ltd



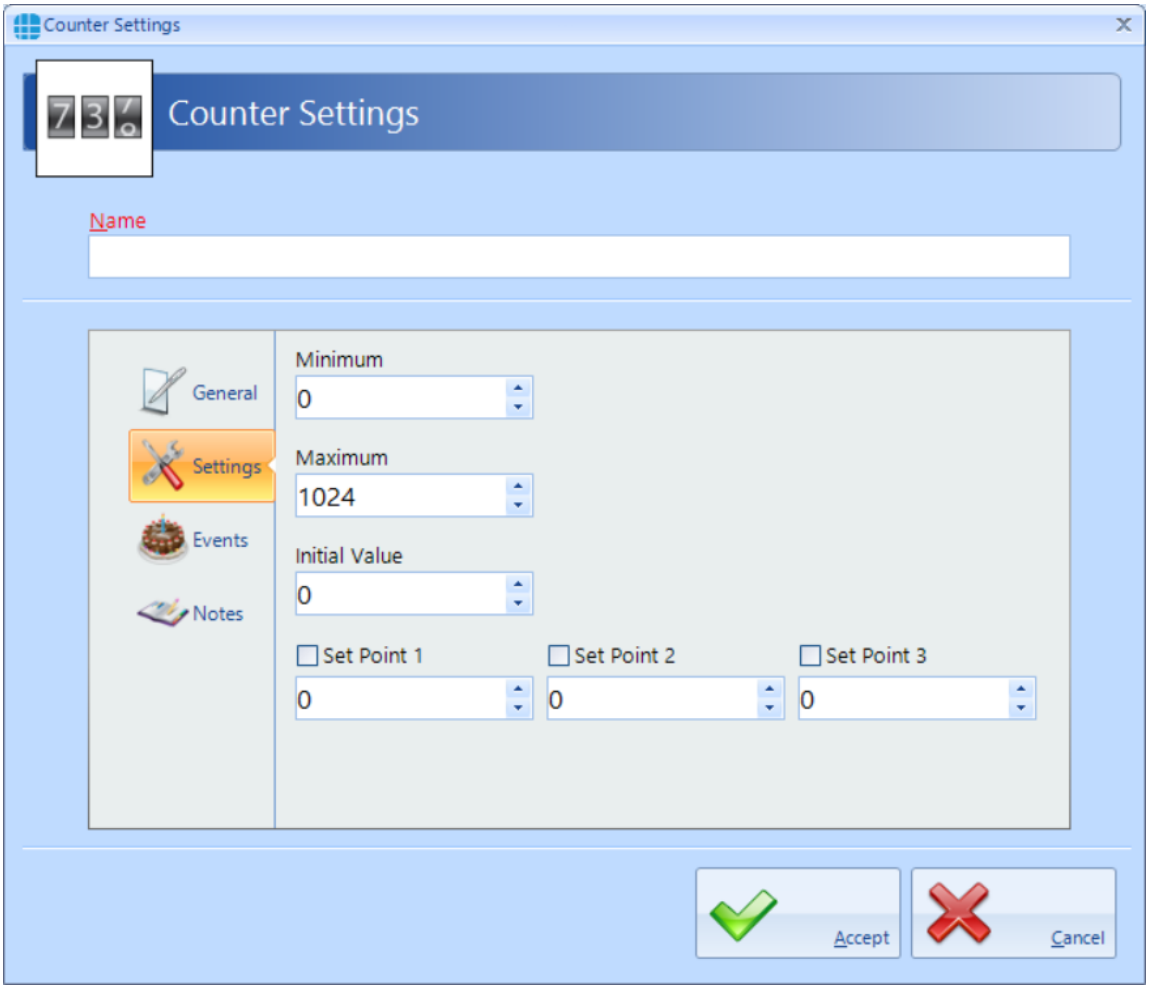
Name: Enter a meaningful name for the counter

On master controller network: Select the master controller that will run the counter. It does not matter which Master controller is used for the counter so we recommend allocating multiple counters to different master controllers to "share the workload"

Ensure that the **Active** option is selected for the counter to work

Next, select the **Settings** tab

© 2026 Controlsoft Ltd



Minimum: enter the minimum permitted value for the counter. If the counter is at the minimum value and is decremented, no change will occur.

Maximum: enter the maximum permitted value for the counter. If the counter is at the maximum value and is incremented, no change will occur

Initial Value: This is the value that the counter will be set to when the counter is reset

Set Points: Up to 3 set points can be configured which will allow analysis of the state of the counter within the Events & Actions programming

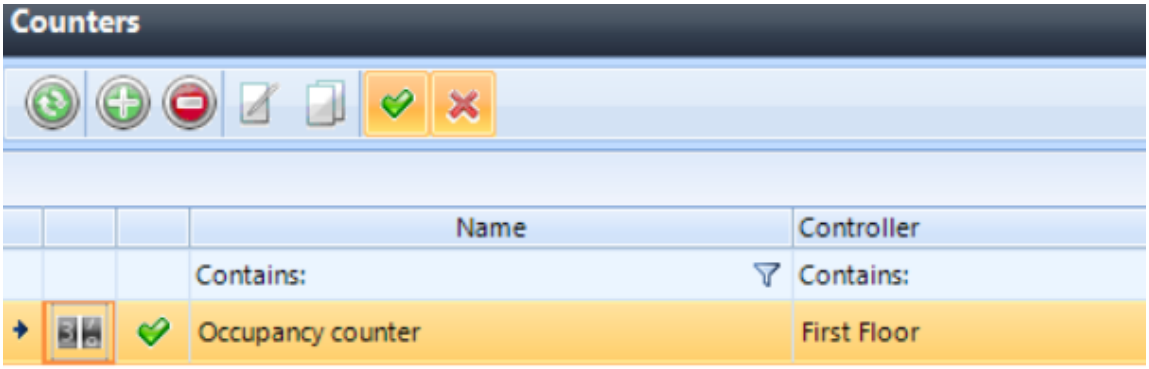
NOTE: The maximum value for any counter is 2,147,483,647

The **Events** tab in the side bar will indicate whether any Events have been configured for the selected Counter.

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

Press the **[Accept]** button to save the counter which will then be visible in the Counters screen:

© 2026 Controlsoft Ltd

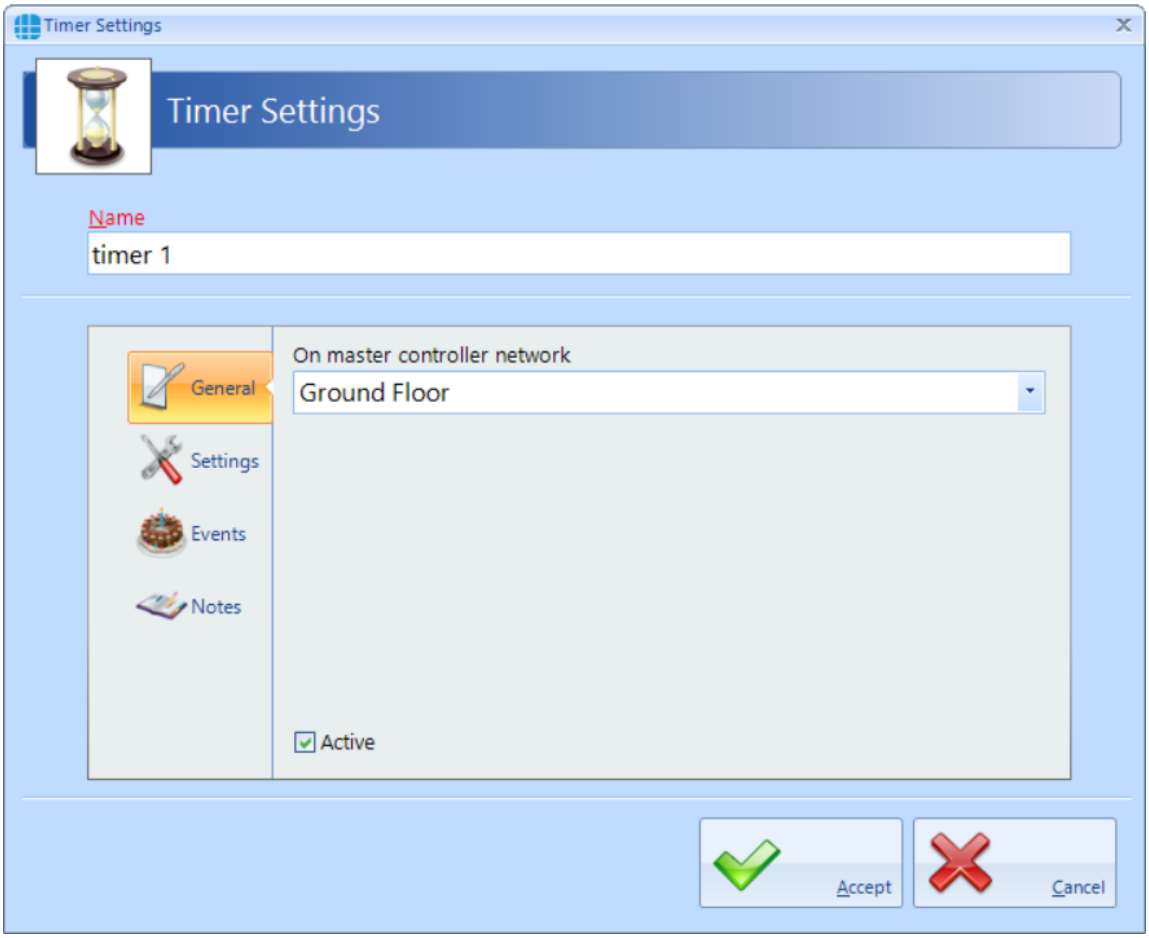


20.3 Advanced > Timers

Timers can be used to introduce time delays in events and actions. For example:

If an input activates, wait 10 seconds then activate an output. A timer can have a maximum value of 2,147,483,647 milliseconds (24 days)

To create a timer, select the **Advanced** tab, select **Timers** from the ribbon bar and click the **Add** button .



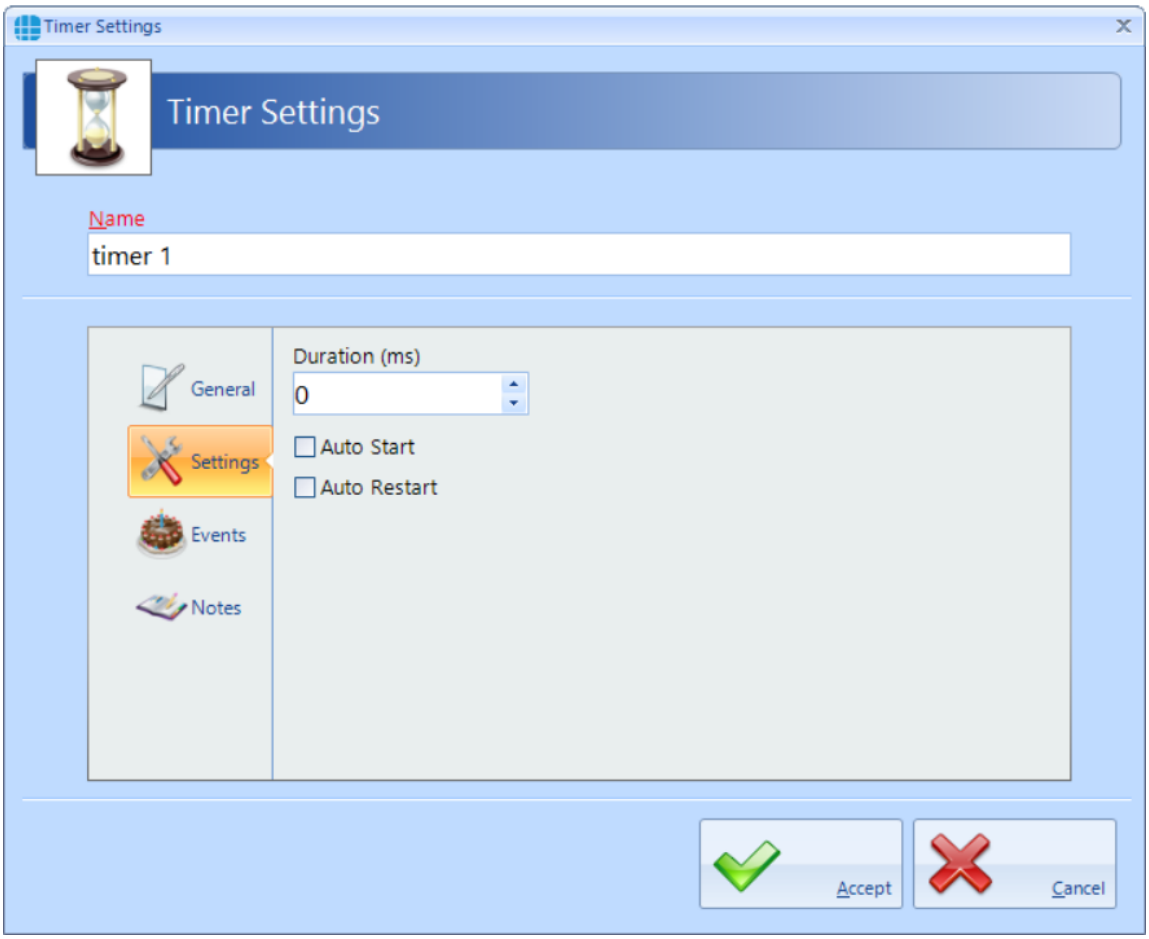
© 2026 Controlsoft Ltd

Name: Enter a meaningful name for the timer

On master controller network: Select the master controller that will run the timer. It does not matter which Master controller is used for the timer so we recommend allocating multiple timers to different master controllers to "share the workload"

Ensure that the **Active** option is selected for the timer to work

Next, select the **Settings** tab



Duration: Enter the duration period for the timer. NOTE: this time is in milliseconds so for a 5 second timer, you must enter 5000.

Auto start: If selected, the timer will start automatically when the controller powers up

Auto Restart: If selected, the timer will restart automatically when it expires

The **Events** tab in the side bar will indicate whether any Events have been configured for the selected Timer.

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

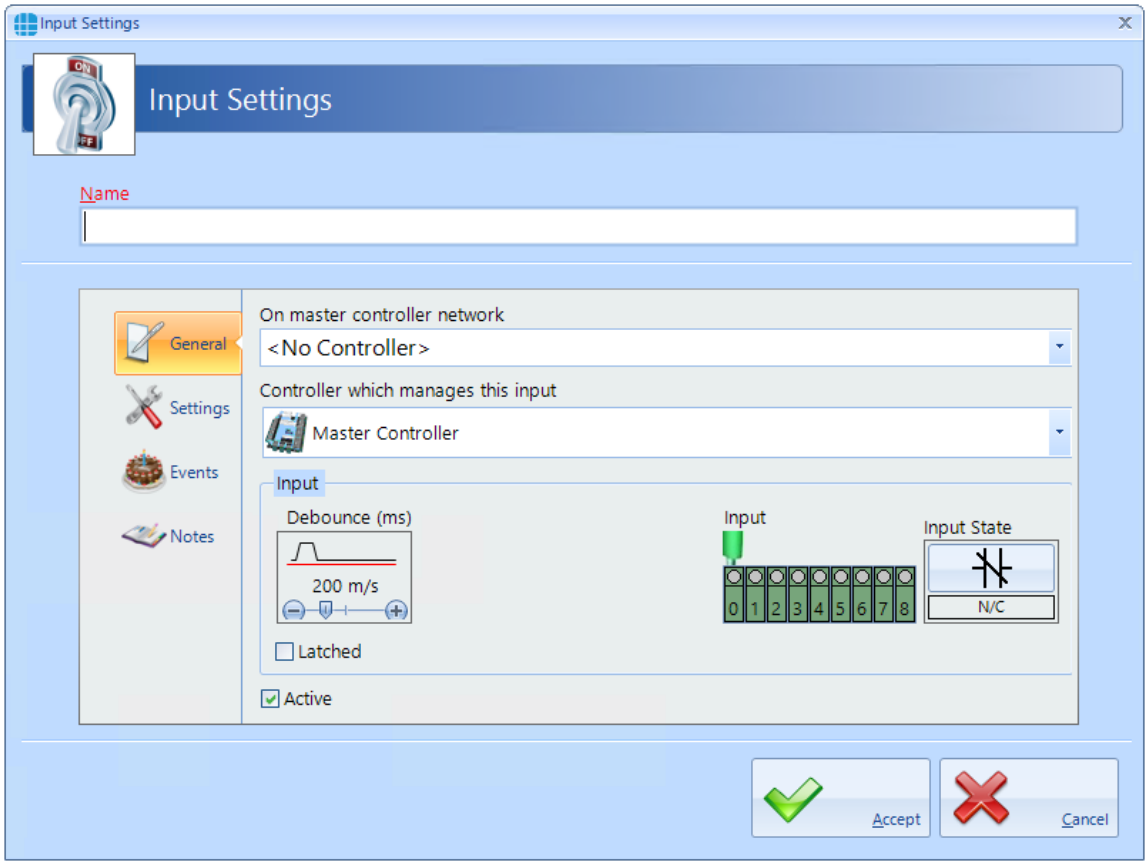
Press the **[Accept]** button to save the timer which will then be visible in the Timers screen:

© 2026 Controlsoft Ltd



20.4 Advanced > Inputs

It is possible to define an input for use with the Advanced functions. From the "**Advanced**" tab, select "**Inputs**" from the ribbon bar, then press the "**Add**" button 



Name: Give the input a meaningful name

On master controller network: Define which master controller relates to the input

Controller which manages this input: Define whether the input is on the master controller or specify which Downstream device it relates to.

Debounce: Defines the Debounce time for the input

Input: Defines which physical input is to be used

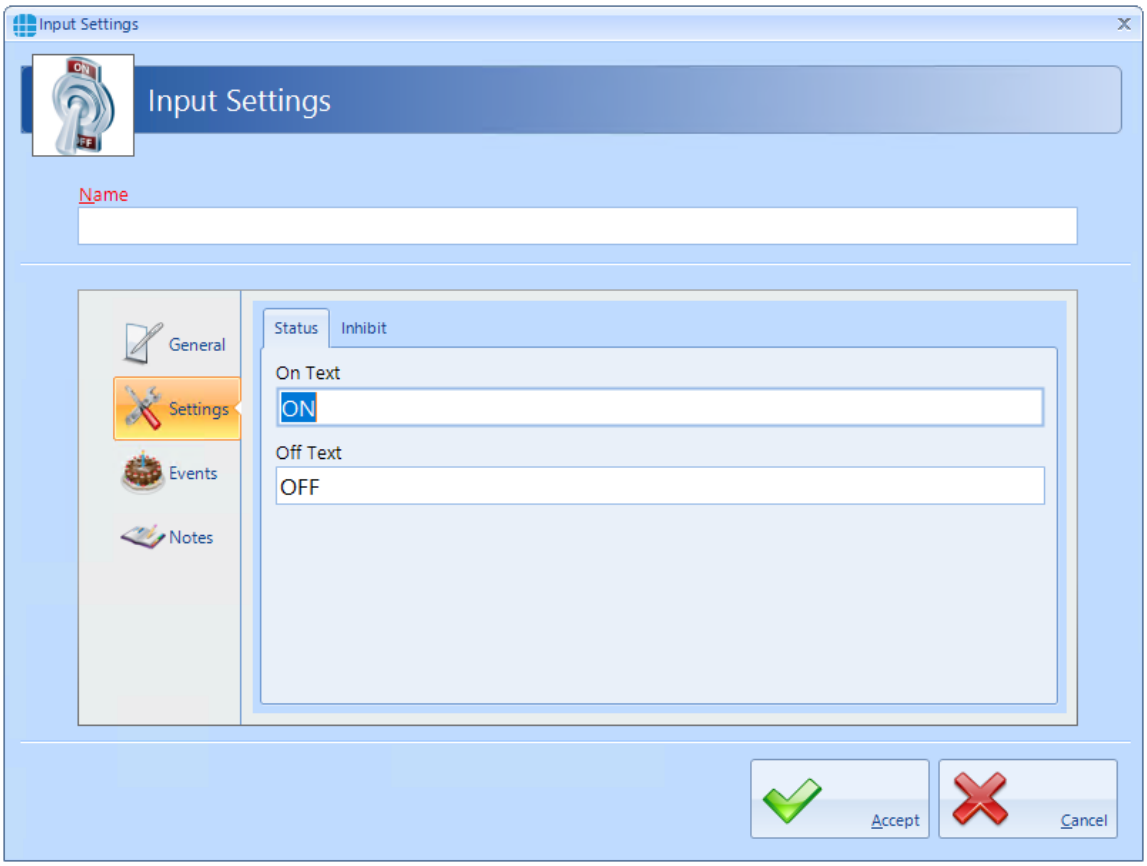
© 2026 Controlsoft Ltd

Input State: Defines whether the input is connected to normally open or normally closed contacts

Latched: It is possible to latch the state of the input until the latch is removed by an Action.

Ensure that "**Active**" is selected for the input to work.

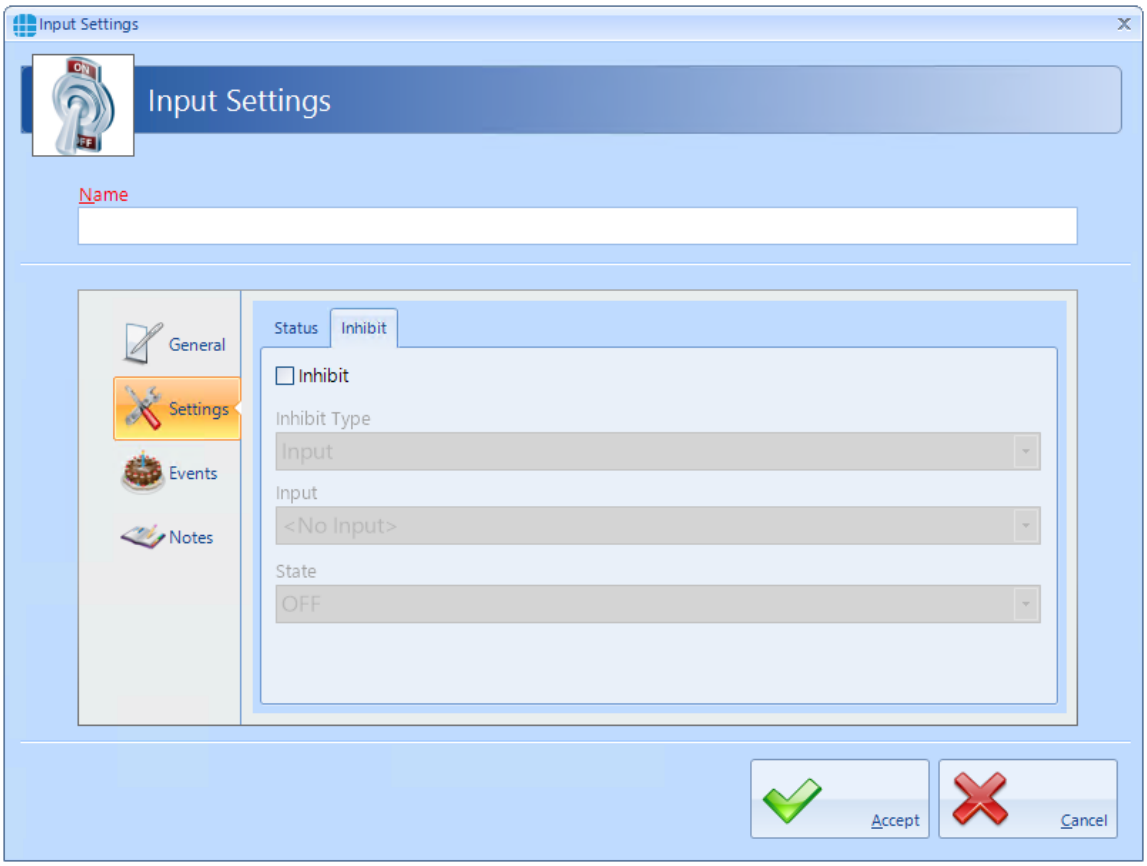
Next, select "**Settings**" in the side bar



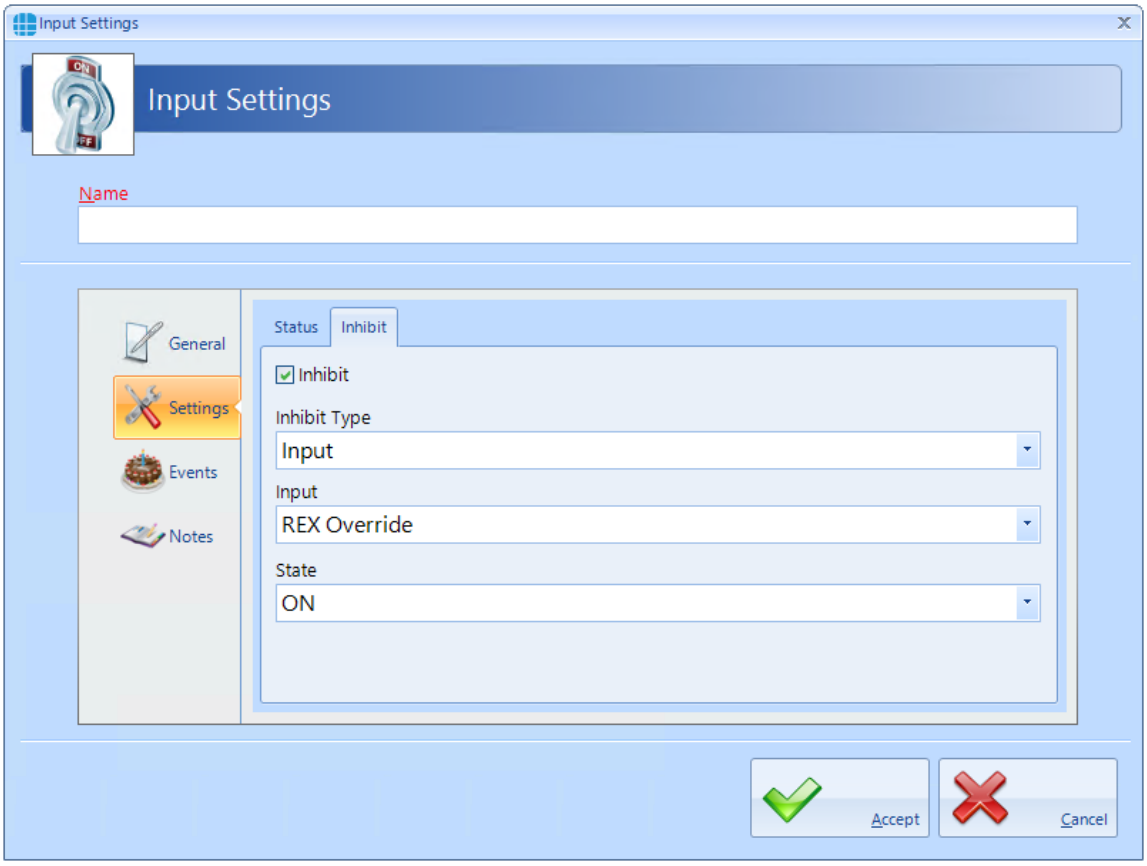
"**On Text**" and "**Off Text**" allows a label to be entered for the input to define the required status to react to (e.g. if the input is to be used to monitor a temperature sensor, it may make subsequent programming easier to refer to Hot and Cold rather than On and Off)

Select the "**Inhibit**" tab

© 2026 Controlsoft Ltd



When the "**Inhibit**" option is selected, this input will be inhibited when the specified input or output is in the specified state. For example, this input can be disabled when a different input called "REX Override" in on:



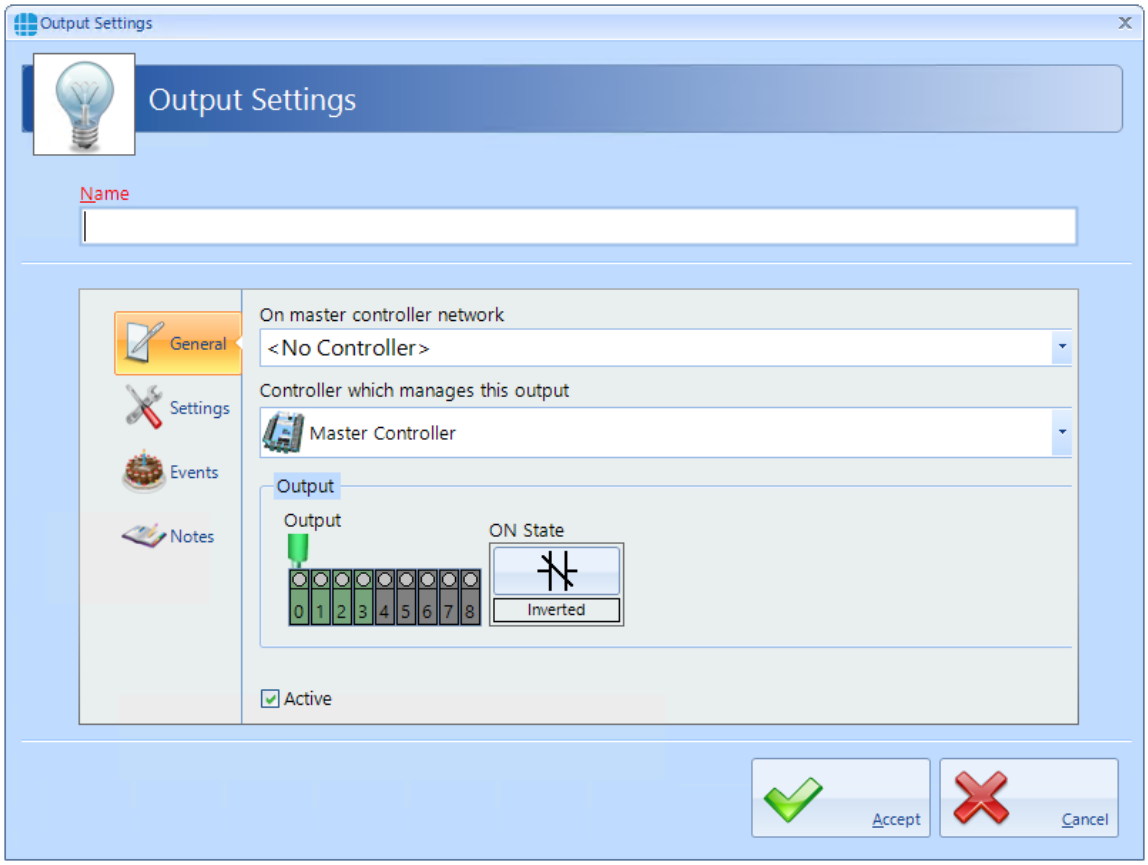
© 2026 Controlsoft Ltd

The **Events** tab in the side bar will indicate whether any Events have been configured for the selected Input.

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

20.5 Advanced > Outputs

It is possible to define an output for use with the Advanced functions. From the "**Advanced**" tab, select "**Outputs**" from the ribbon bar, then press the "**Add**" button 



Name: Give the output a meaningful name

On master controller network: Define which master controller relates to the output

Controller which manages this output: Define whether the output is on the master controller or specify which Downstream device it relates to.

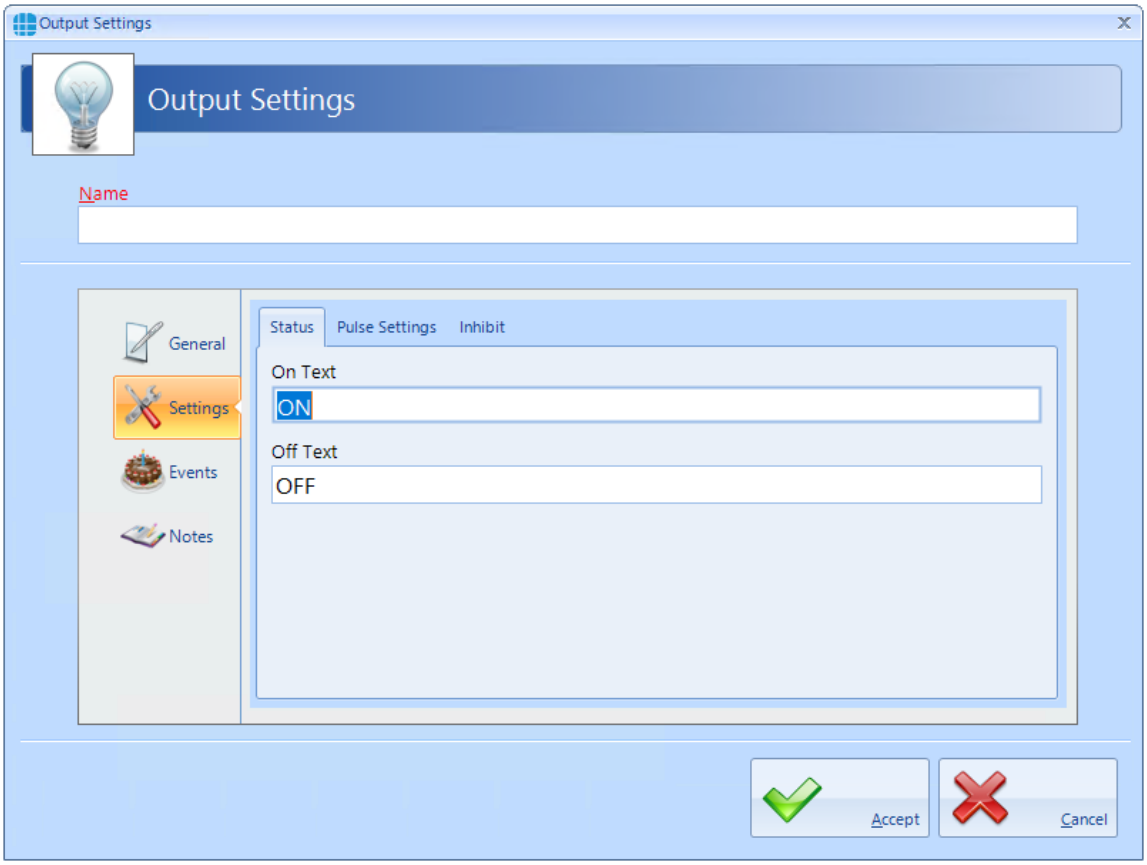
Output: Defines which output physical is to be used

ON State: Defines whether the relay is Normal (i.e. normally de-energised) or "Inverted" (i.e. normally energised)

Ensure that "**Active**" is selected for the output to work.

© 2026 Controlsoft Ltd

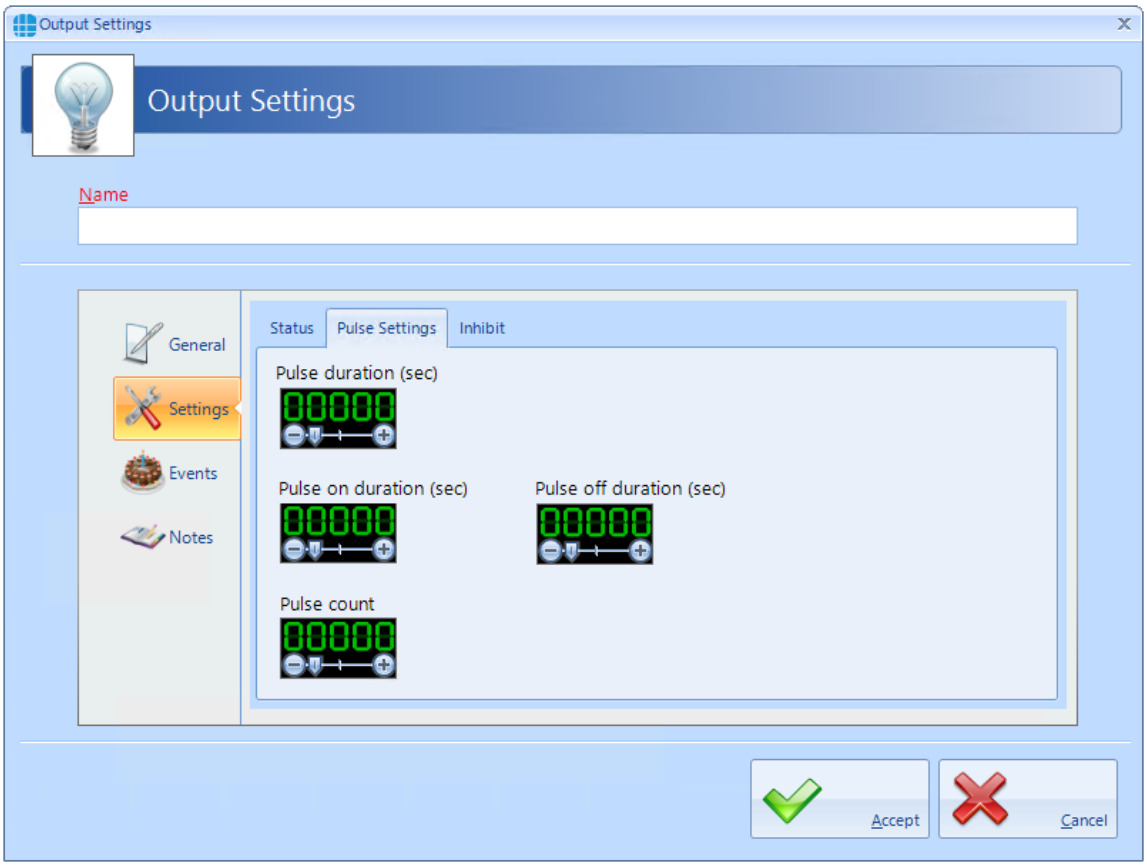
Next, select "**Settings**" in the side bar



On Text and **Off Text** allows a label for the output to be changed when defining the required status to react to (e.g. if the output is connected to a heating element, it may make subsequent programming easier to refer to Hotter and Colder rather than On and Off)

Select the "**Pulse Settings**" tab:

© 2026 Controlsoft Ltd

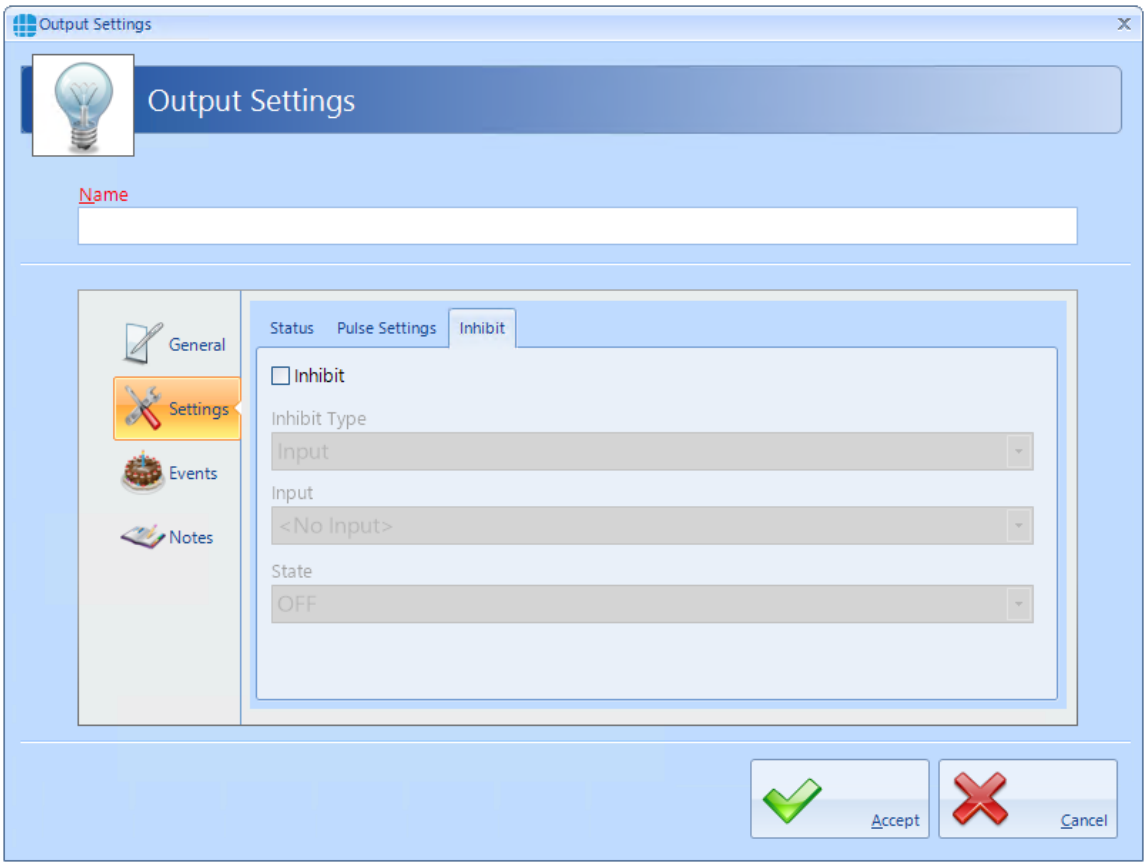


Within the Events & Actions programming, it is not only possible to turn an output on or off in response to the event, it is also possible to pulse the output, the pulse width defined by the "**Pulse duration**" setting. Furthermore, the output can be programmed to give a pulse train which is a number of pulses defined by "**Pulse count**", each pulse with an on duration defined by "**Pulse on duration**" and the off duration defined by "**Pulse off duration**"

NOTE: The maximum duration permissible for any of the pulses is 60 seconds. The maximum number of pulses in the pulse count is 8,192.

Select the "**Inhibit**" tab:

© 2026 Controlsoft Ltd



When the "**Inhibit**" option is selected, this output will be inhibited when the specified input or output is in the specified state.

The **Events** tab in the side bar will indicate whether any Events have been configured for the selected Output.

The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

20.6 Advanced > Graphics Designer

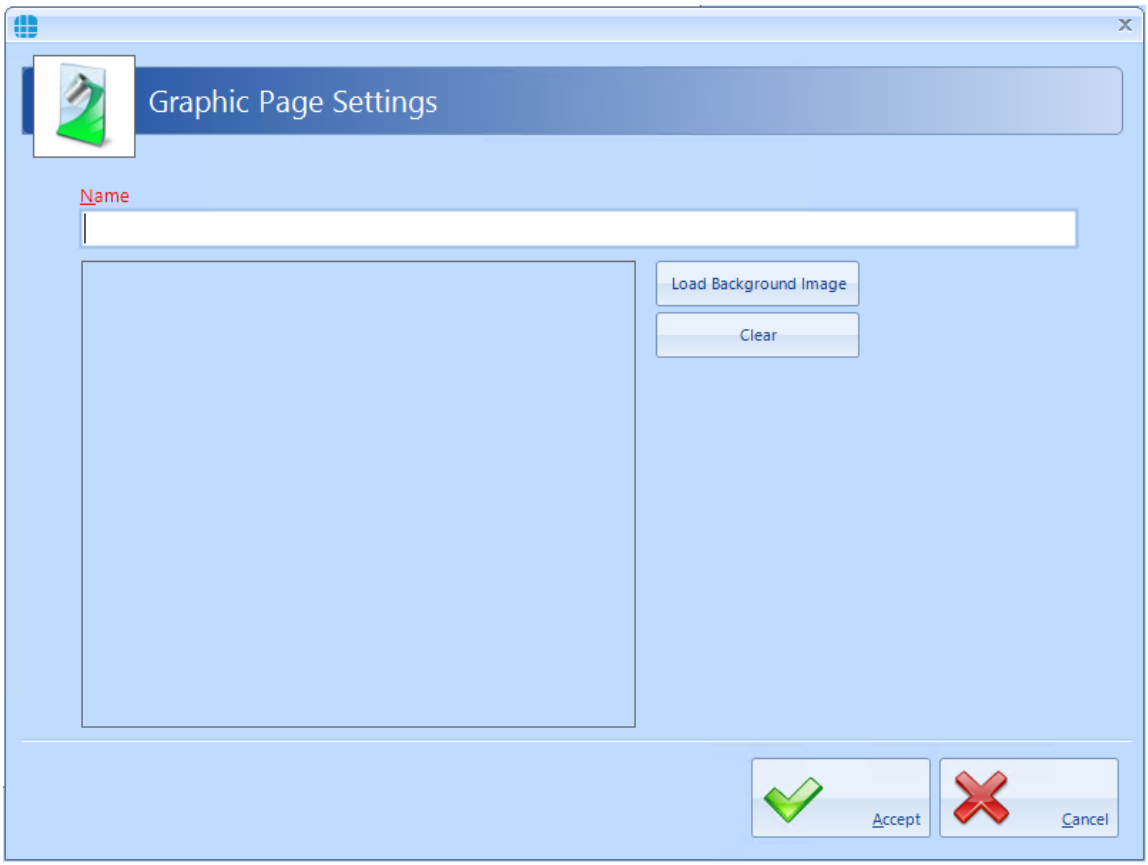
The Graphic Designer allows a floorplan of the site to be imported. This image can be in many popular formats, such as jpg, png or bmp. Multiple images can be imported to provide floorplans for a building's Ground Floor, First Floor etc.

Once a page has been imported, objects can be superimposed onto the image. Objects can be IA Objects such as doors, readers or controllers or Custom Objects such as squares, circles, images or text boxes. IA Objects have predefined states (for example a door can be open, closed, locked, unlocked, held open or forced open) whereas states for Custom Object can be created as required.

Actions can be created to change the state of any object on any page in response to an event.

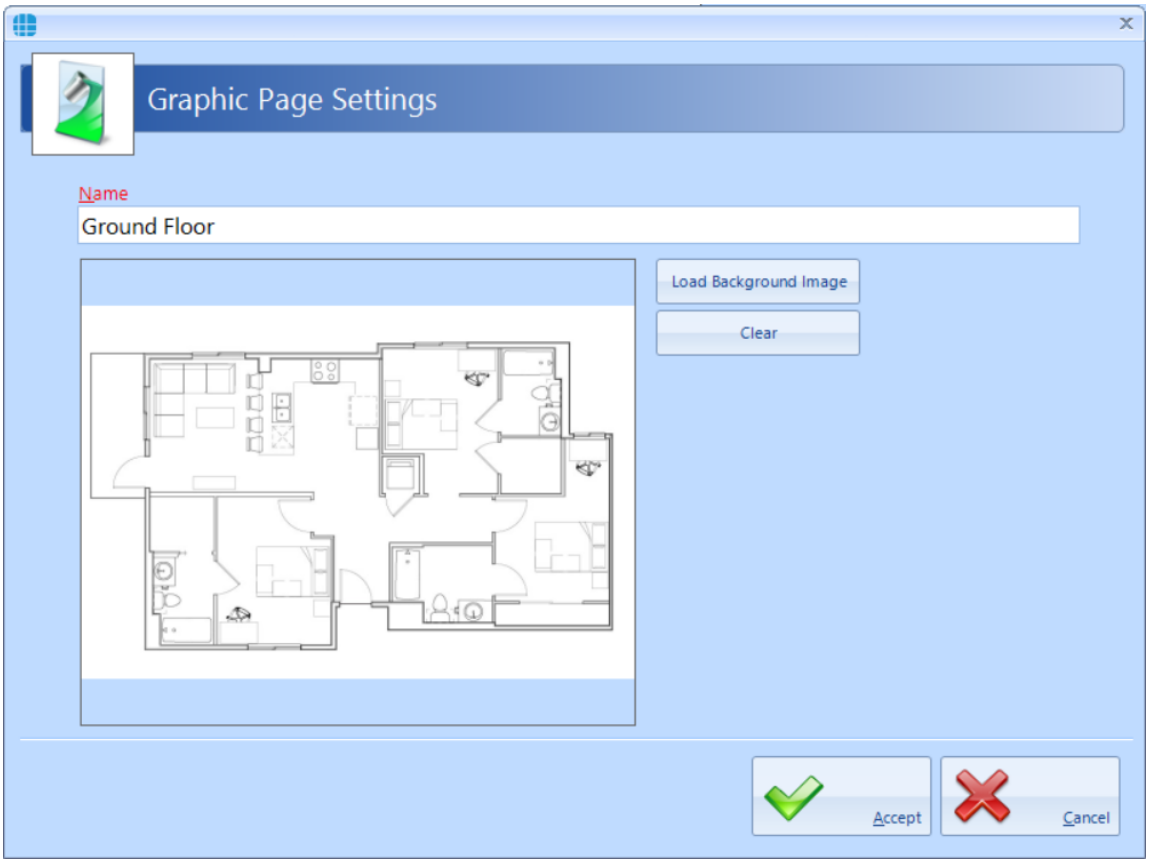
© 2026 Controlsoft Ltd

To import an image, select the **Advanced** menu, then click on **Graphic Designer** in the ribbon bar and click the **Add** button 



Enter a meaningful name for the page, click on the **[Load Background Image]** button, browse to the required image and click **[Open]**

© 2026 Controlsoft Ltd



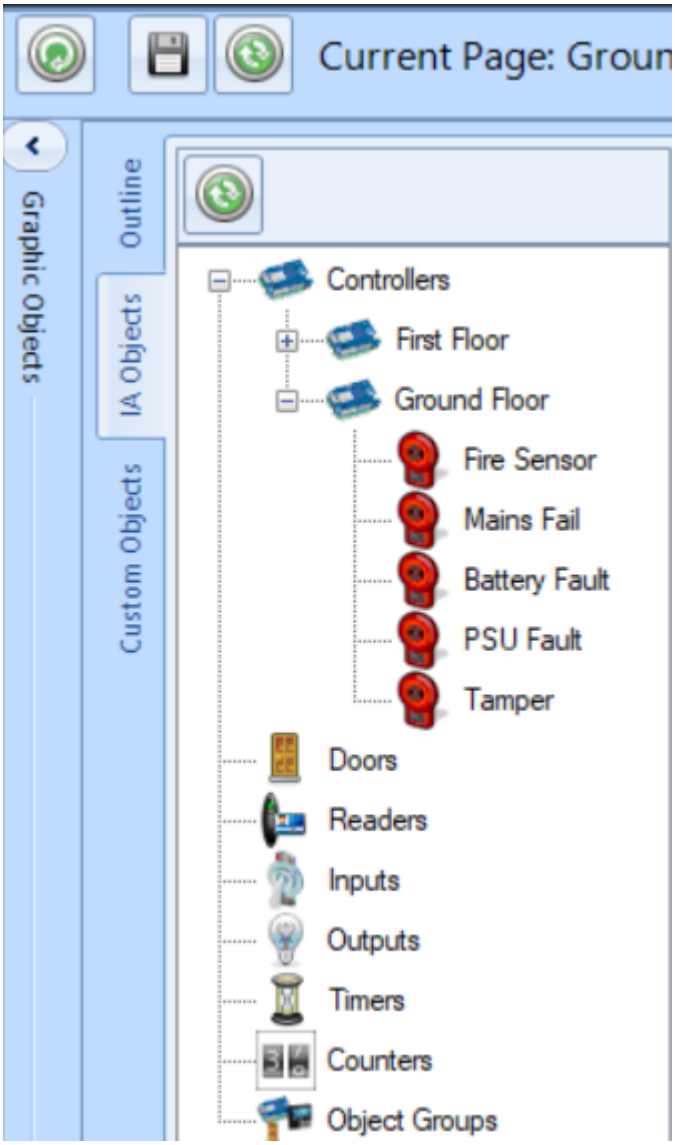
Click **[Accept]** and repeat to create all the required pages.

Next, we will add objects to a page.

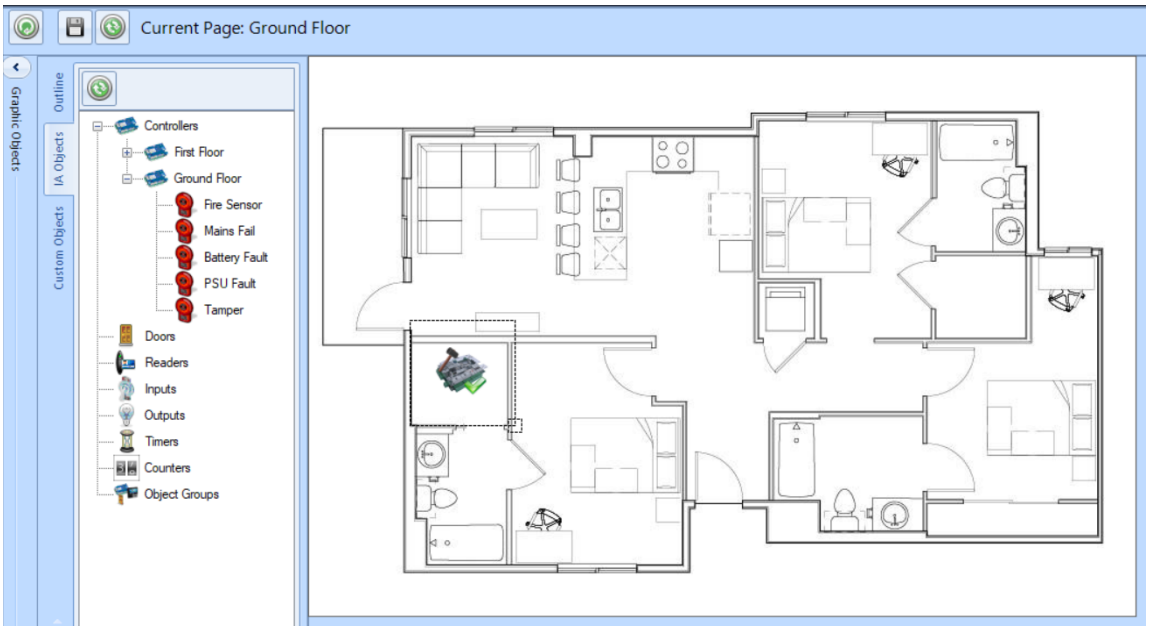
IA Objects

Select the required page so the floorplan is visible, then select the **IA Objects** tab. A list will appear showing all the controllers, doors, readers, inputs and outputs that have been created.

© 2026 Controlsoft Ltd



Select the required object and drag it onto the image, positioning it as required.



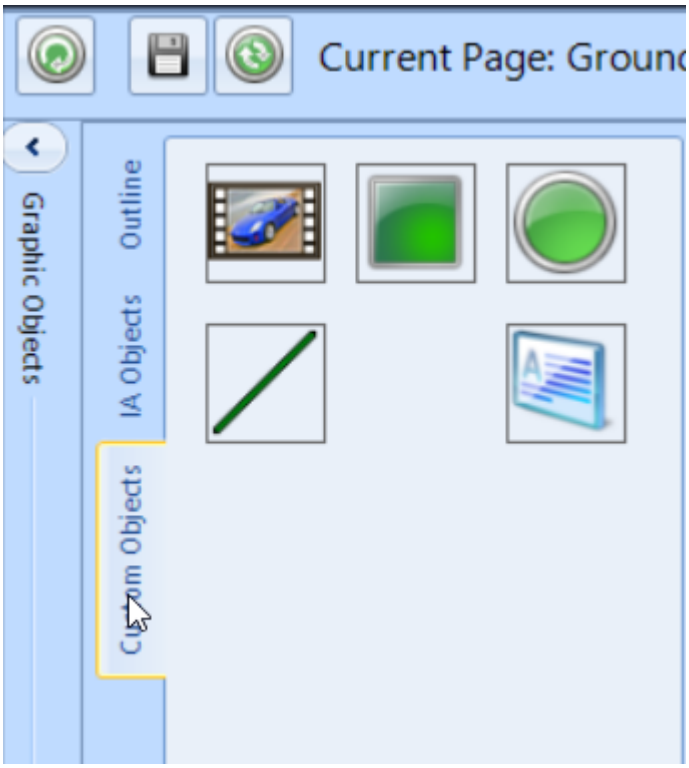
© 2026 Controlsoft Ltd

With IA Object, all the Events and Actions required to support this object are created automatically.

Place other objects onto the image as required, and click the **[Save]** button when done.

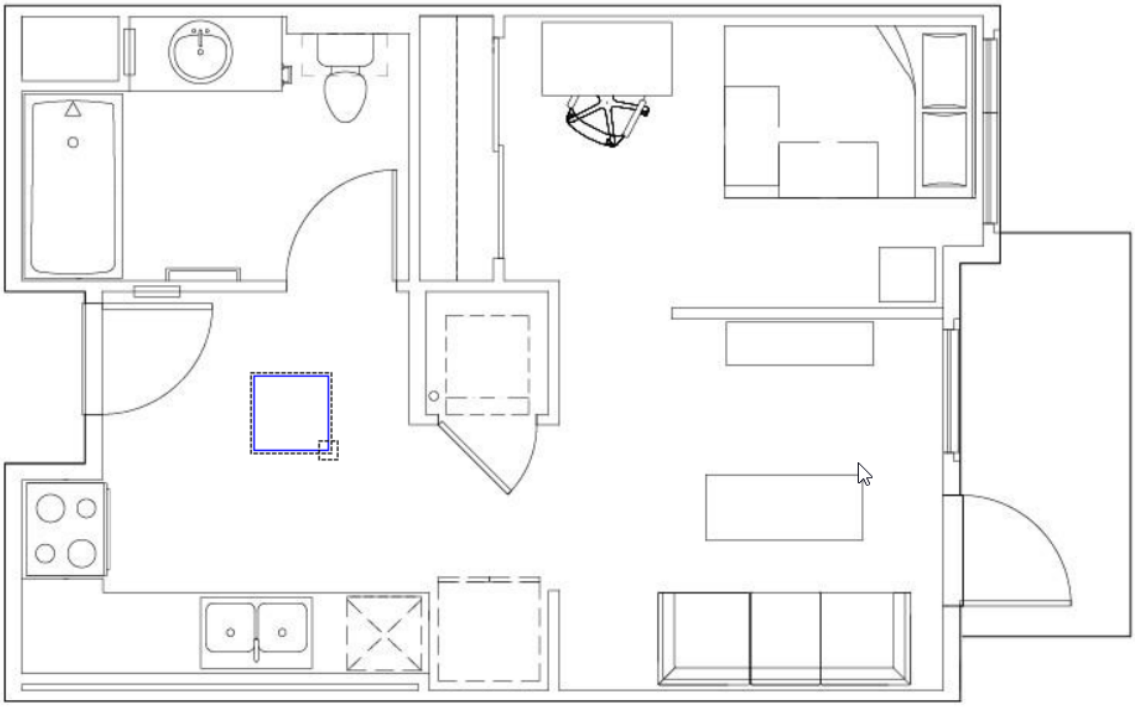
Custom Objects

Select the required page so the floorplan is visible, then select the **Custom Objects** tab. A list will appear showing the object types available. These include Image, Oblong, Ellipse, Line and Textbox

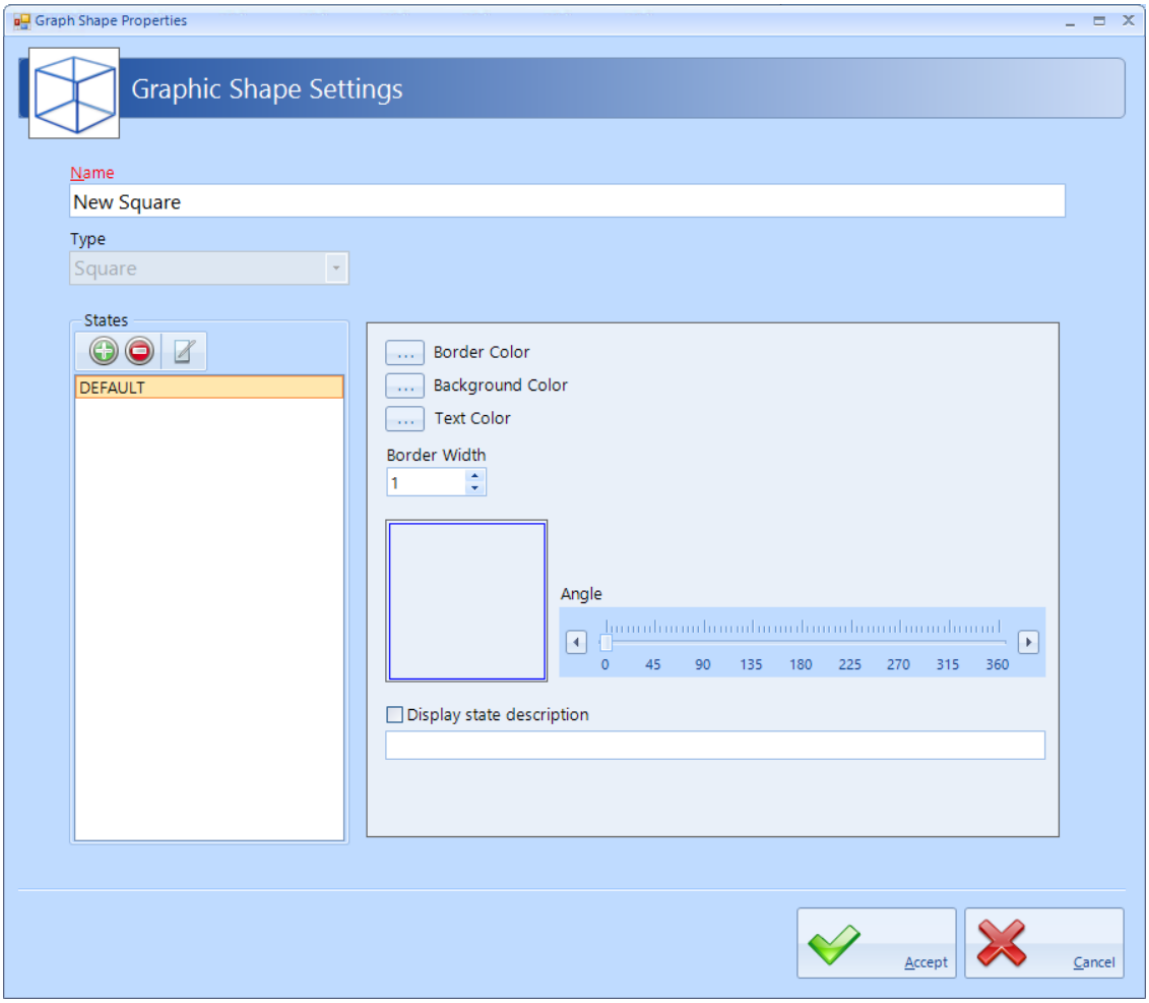


Select the required object and drag it onto the image, positioning it as required.

© 2026 Controlsoft Ltd



Select the placed object and click the **Edit** button in the **Outline** tab



Name: Give the object a meaningful name

© 2026 Controlsoft Ltd

It is now possible to edit the object to change its border colour, background colour, border width and angle of the object

To add another state, press the **Add** button and enter a name and description for the new state, then configure the object for this state as described above

A typical example for this feature could be to add an oblong inside the building outline which is green when the Intruder Alarm system is disarmed and red when it is armed.

20.7 Advanced > Events

Events and Actions allows the system to react to predefined activity such as triggering a specific output when a specific input activates. The decision-making for these actions is made in the controller, thus the software does not need to be active. To achieve this, every master controller communicates with every other master controller over the LAN connection. Events are broadcasted which allows each controller to decide whether it need to perform a resultant action.

Select "**Events**" from the "**Advanced**" ribbon bar, then press the "**Add**" button .



Now use the wizard to create the Event to be detected by clicking the **[Next]** button

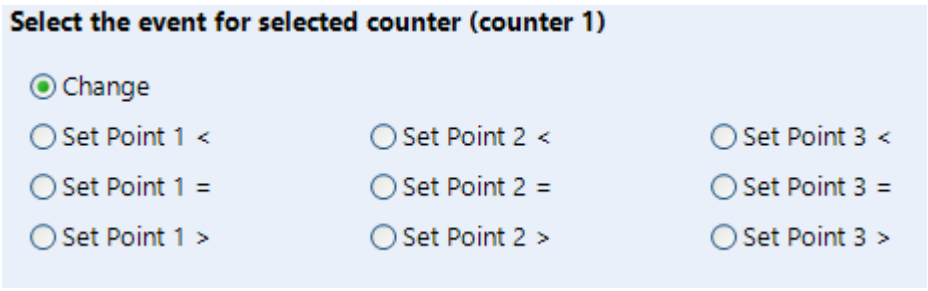
© 2026 Controlsoft Ltd



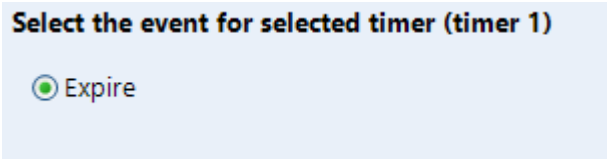
The Event can derive from a controller or, if the software is running, it can be derived from the PC.

Controller events: detectable controller events includes

Counters:

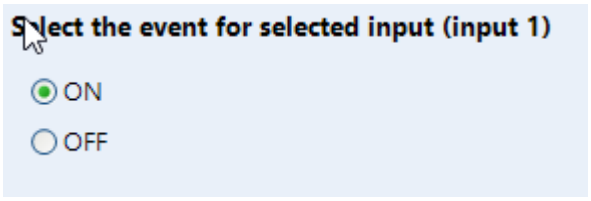


Timers:

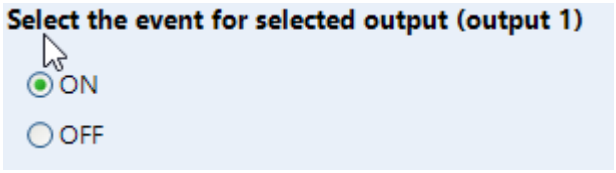


Inputs:

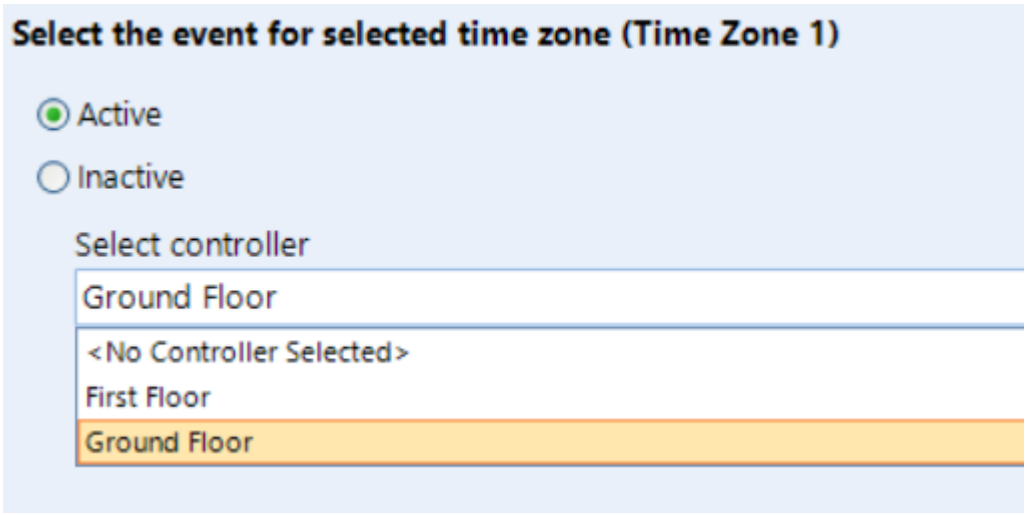
© 2026 Controlsoft Ltd



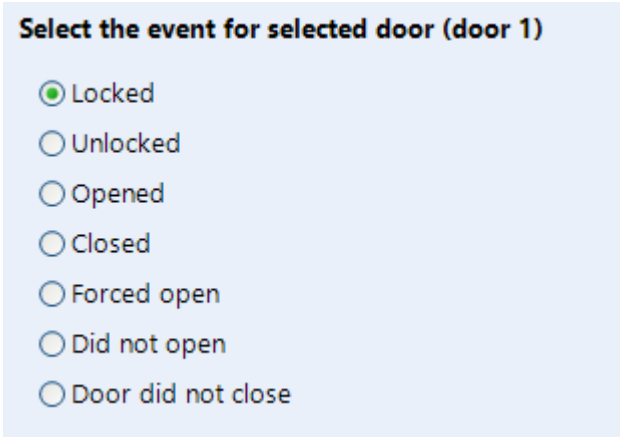
Outputs:



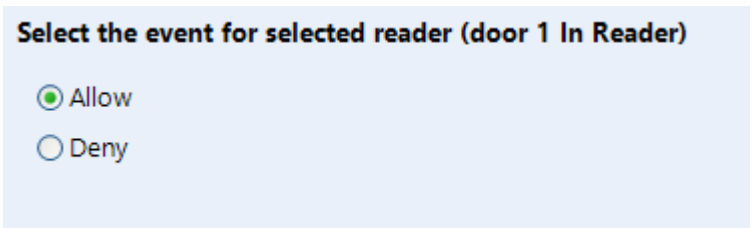
Time Zones:



Doors:

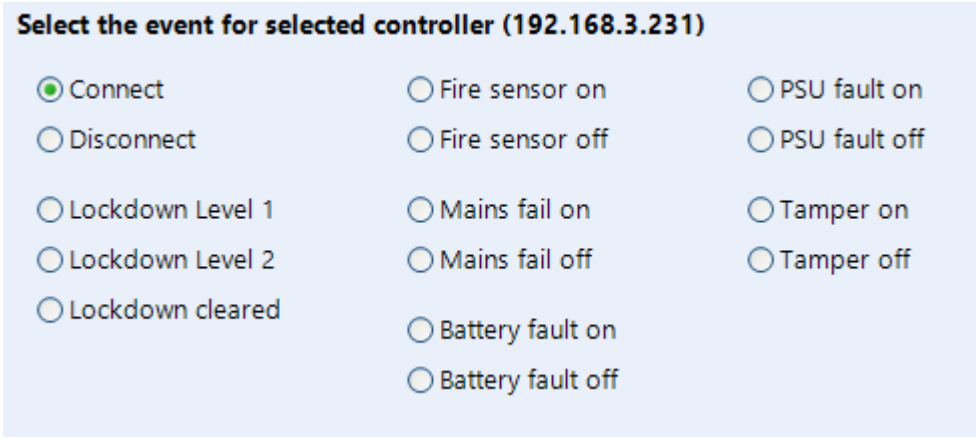


Card Readers:

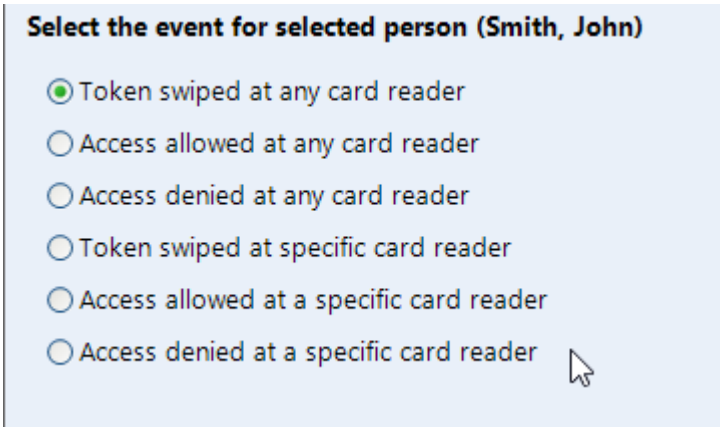


© 2026 Controlsoft Ltd

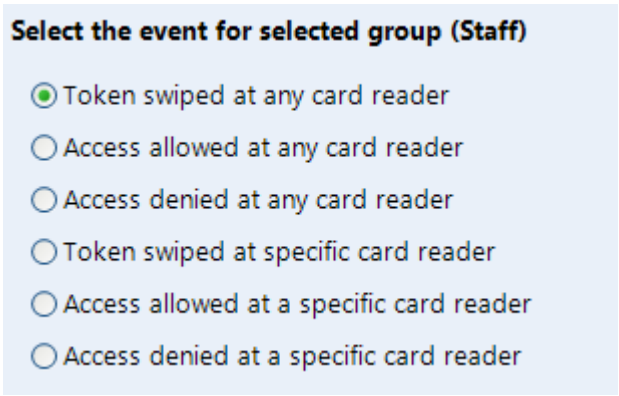
Controllers:



Persons:



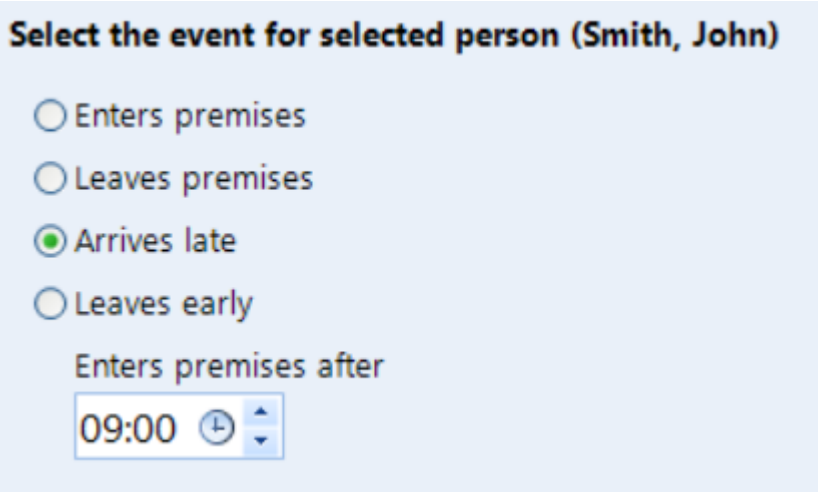
Groups:



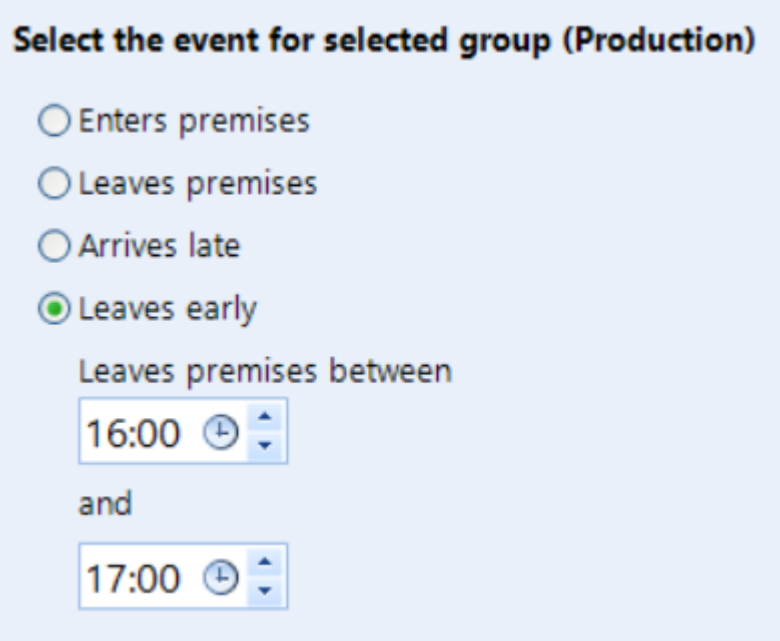
PC Events

Access Log – Person:

© 2026 Controlsoft Ltd



Access Log – Group:

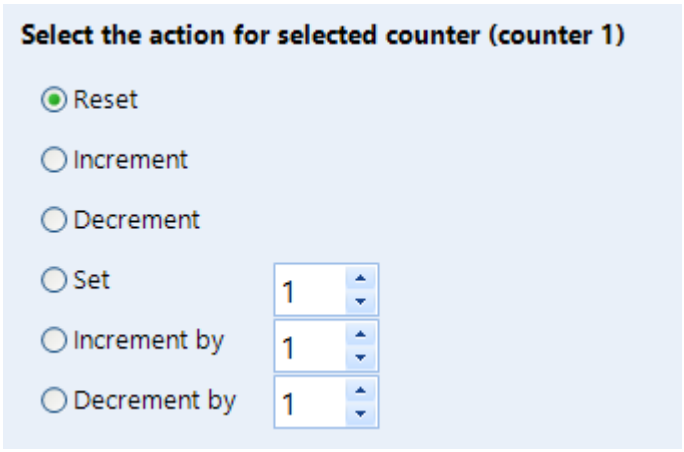


Once the event has been defined, the resultant Actions can include

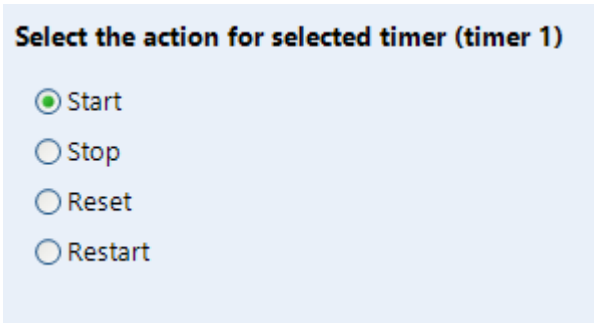
Controller actions:

Counters:

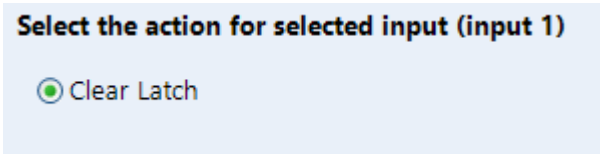
© 2026 Controlsoft Ltd



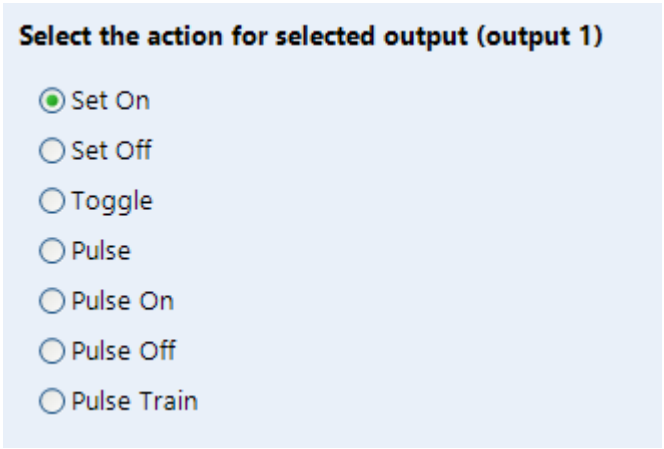
Timers:



Inputs:

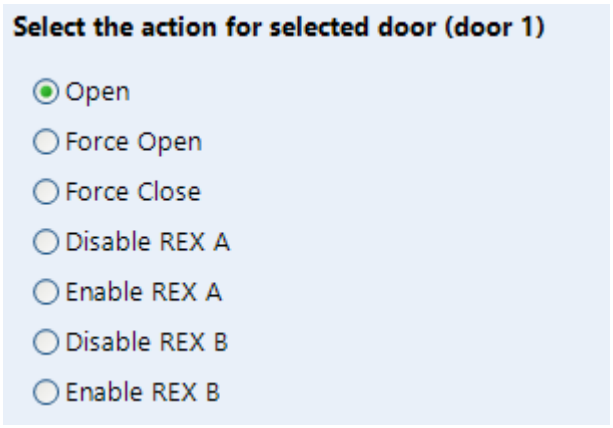


Outputs:

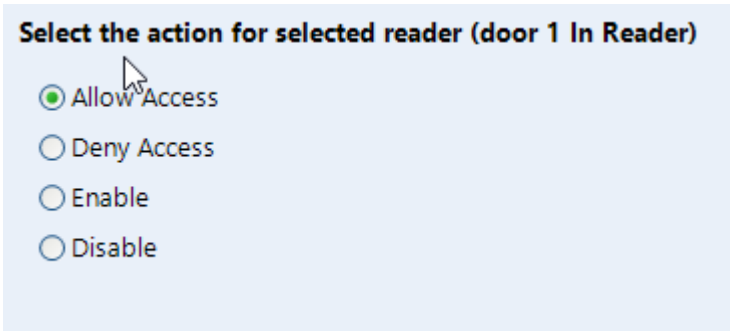


Doors:

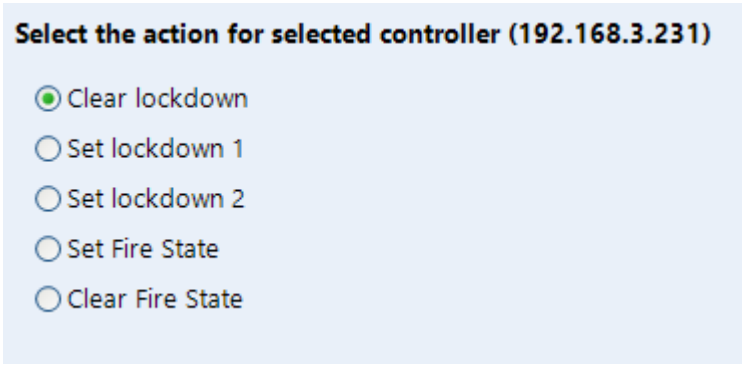
© 2026 Controlsoft Ltd



Card Readers:



Controllers:



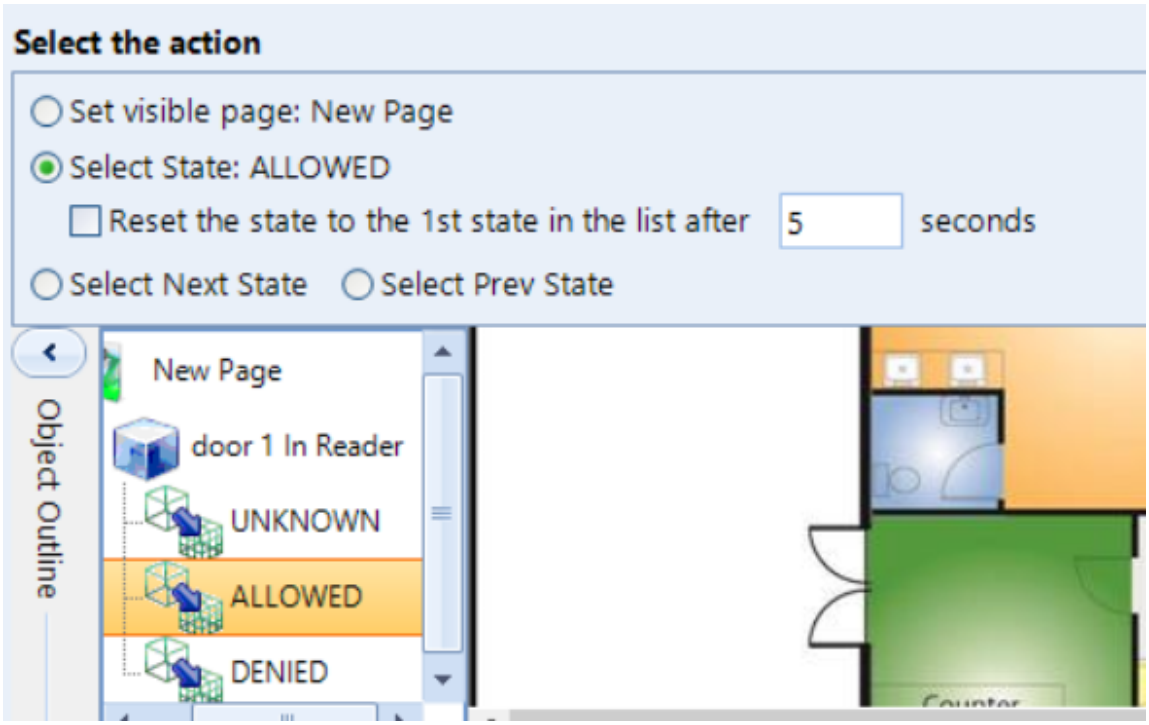
Object group:

The options available will depend on the type of objects in the group (Controllers, Card Readers etc) as described above.

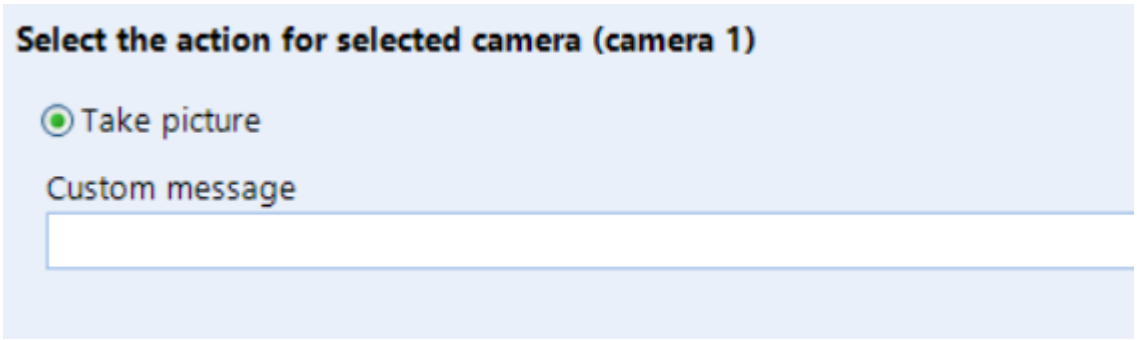
PC actions

Graphic objects:

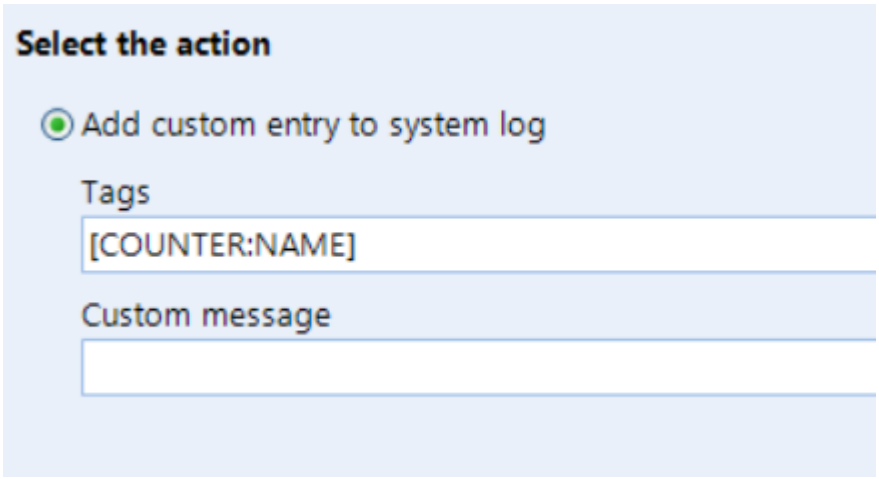
© 2026 Controlsoft Ltd



Camera:

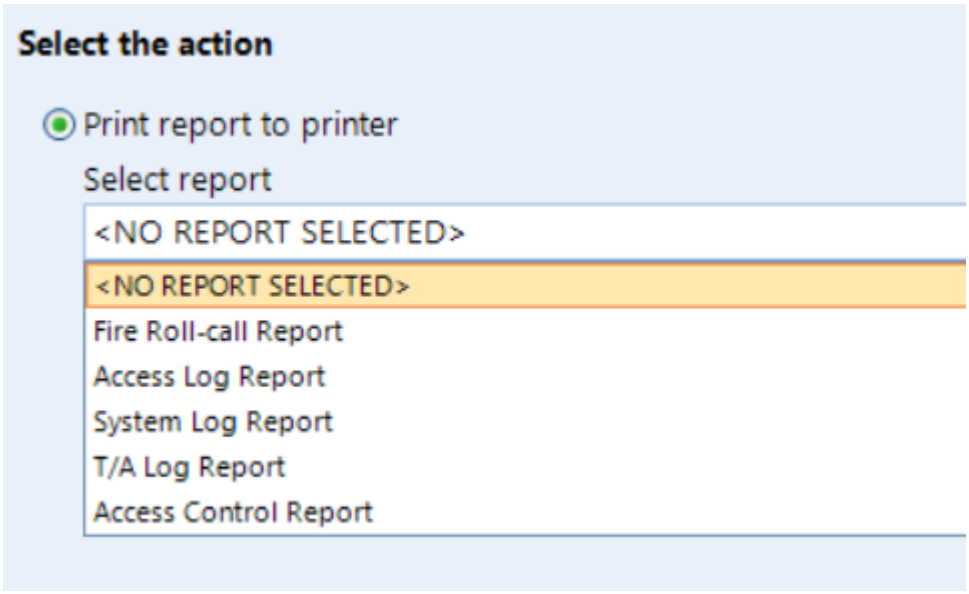


System Log:

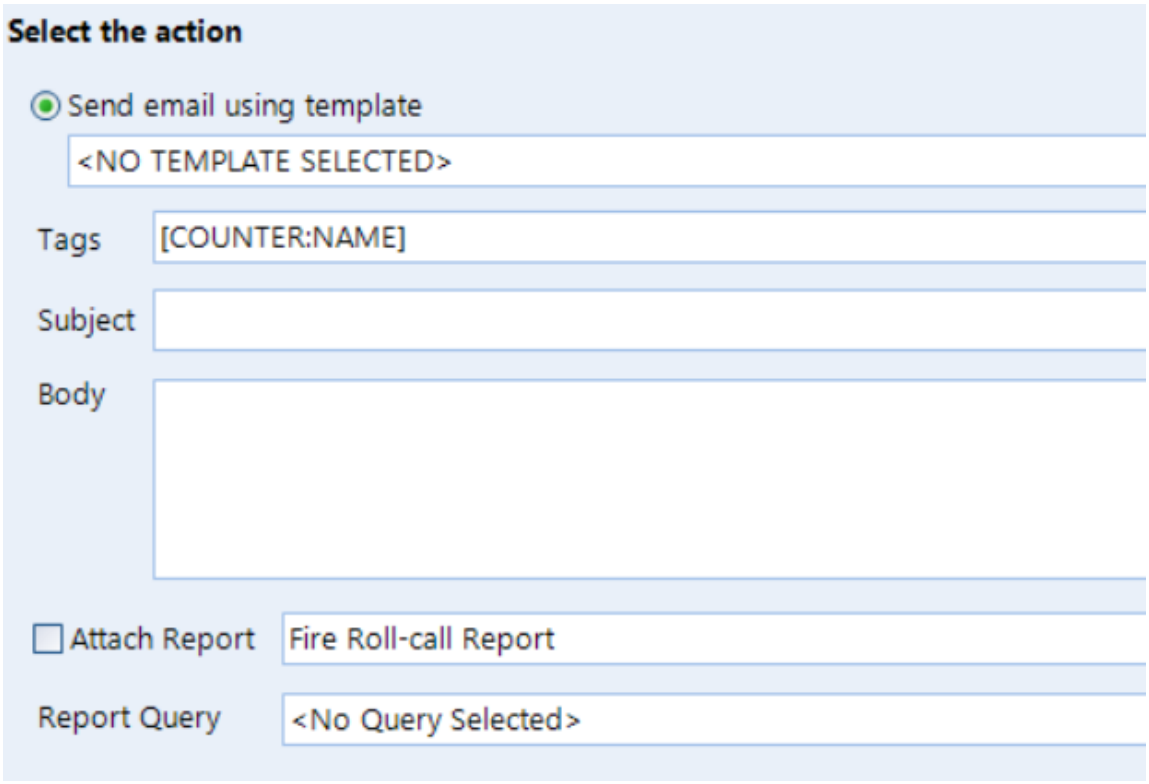


Report:

© 2026 Controlsoft Ltd

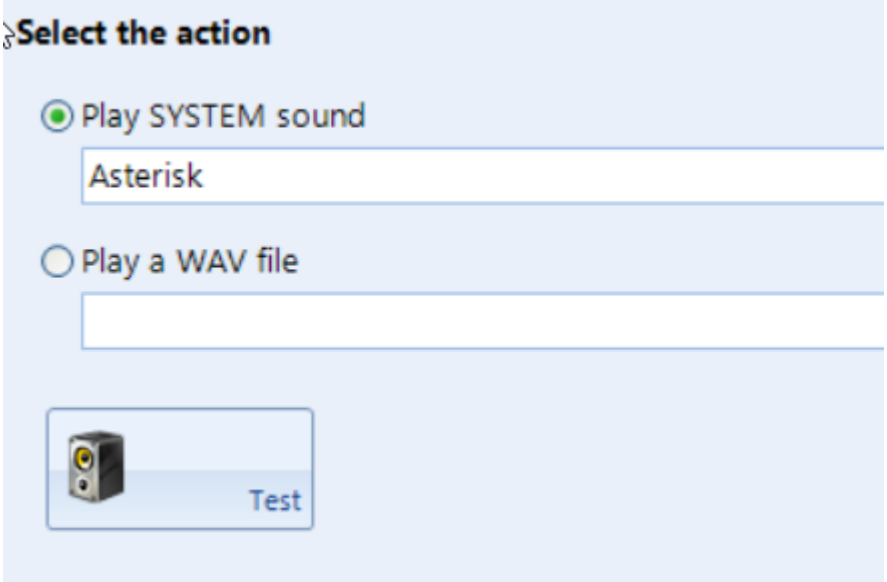


Email:



Sound:

© 2026 Controlsoft Ltd



NOTE: the Events wizard allows multiple Actions for each event.

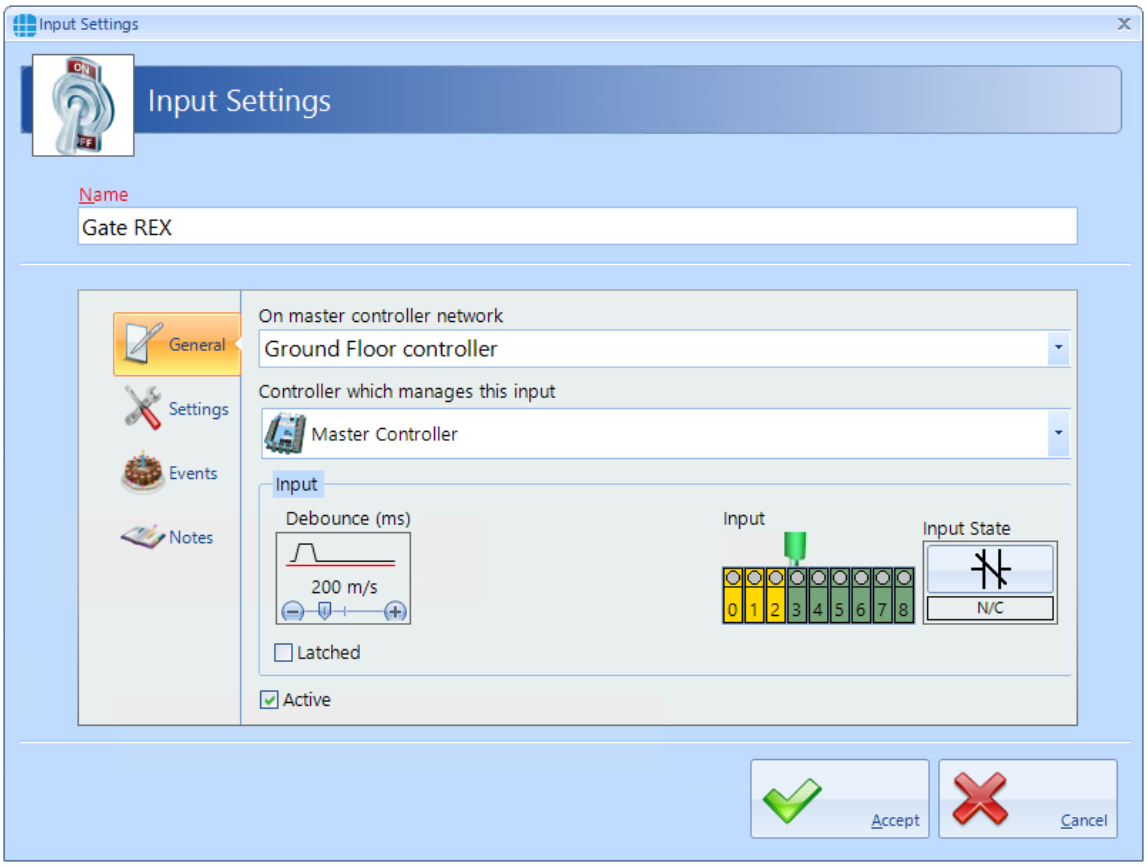
20.8 Typical Examples of Events & Actions

EXAMPLES:

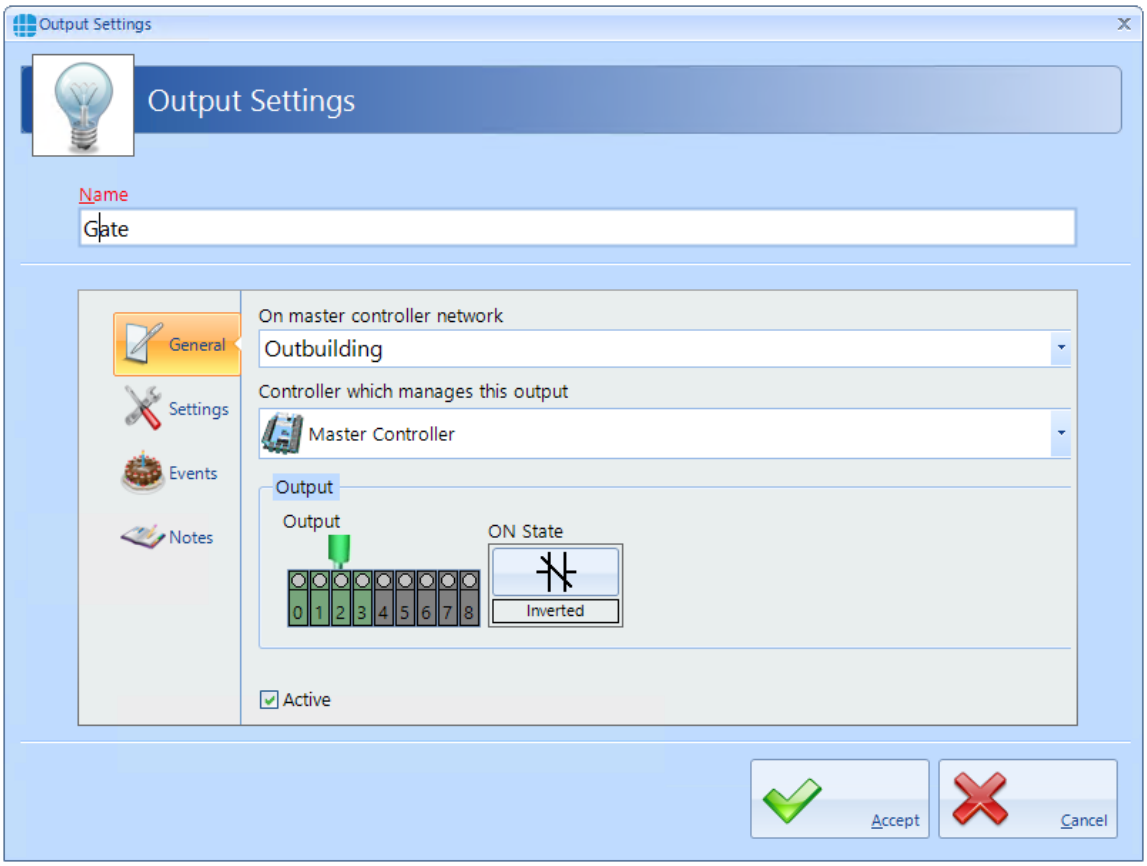
Example 1: A security guard needs to press a pushbutton on a controller in the security office to release a gate which is connected to a different controller.

Create an input called “Gate REX” on “Ground Floor” controller

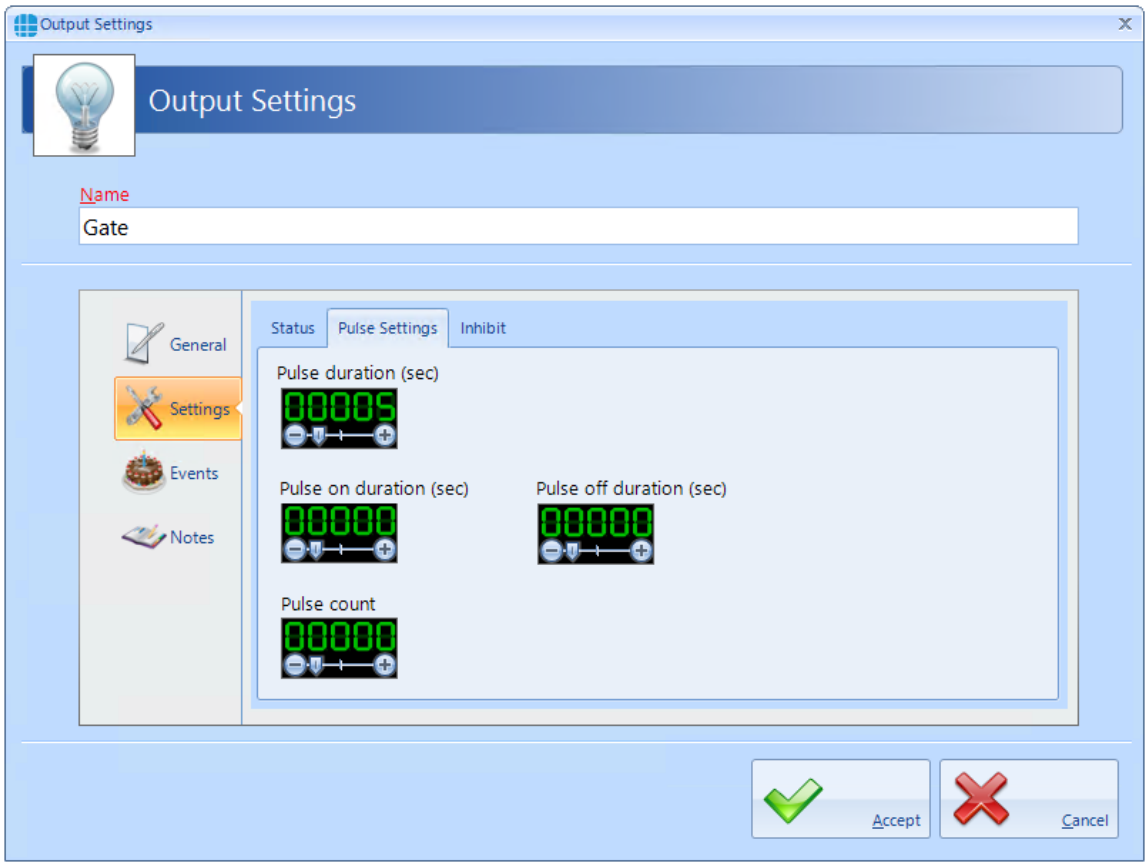
© 2026 Controlsoft Ltd



Create an output called "Gate" on "Outbuilding" controller with a pulse duration of 5 seconds



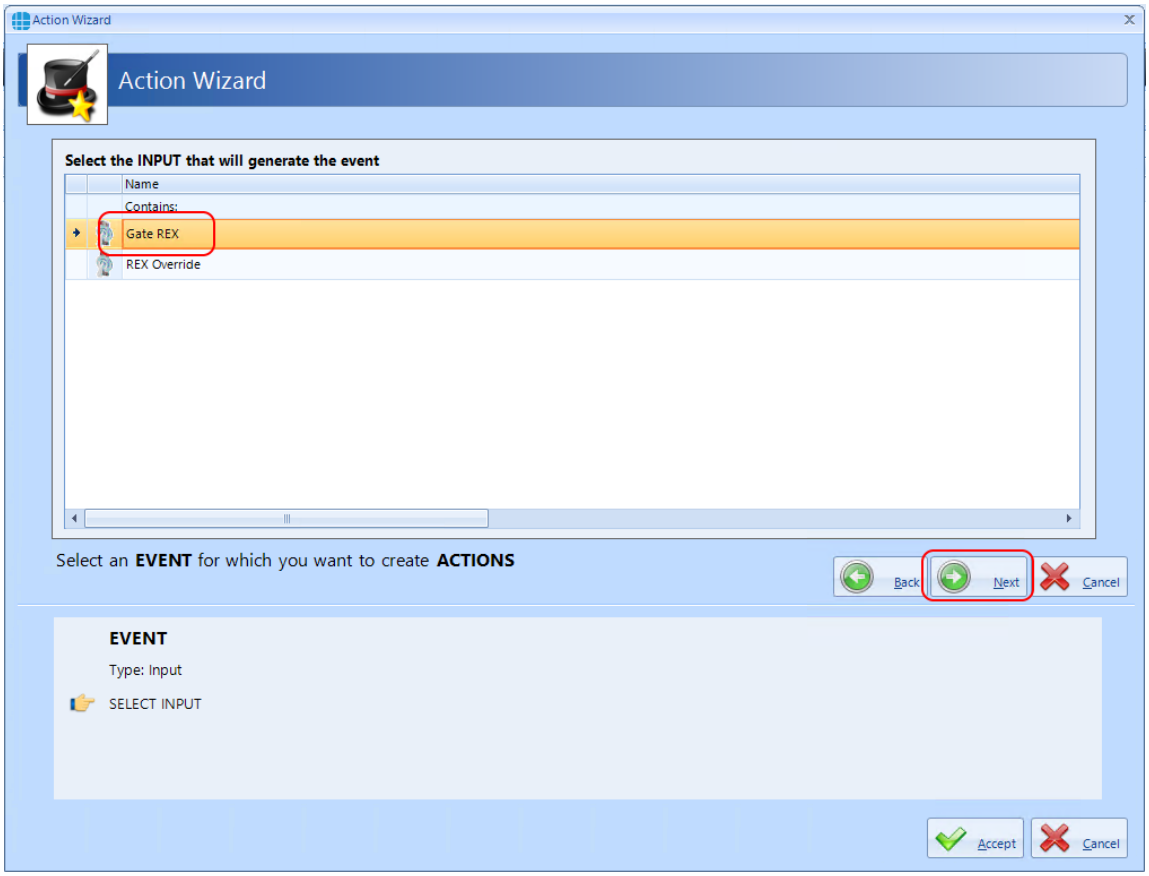
© 2026 Controlsoft Ltd



Create an event to detect that "Gate REX" has been pressed, then create the action to pulse the "Gate" output.

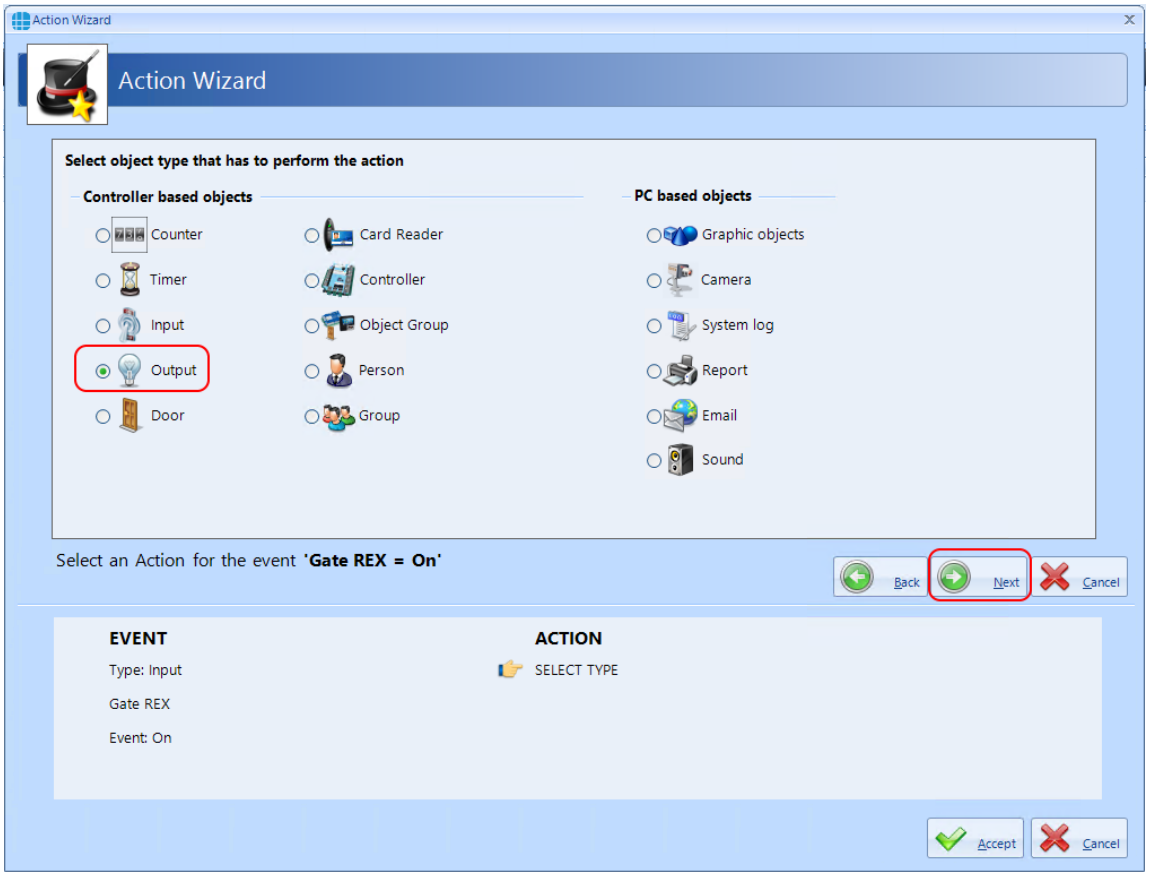


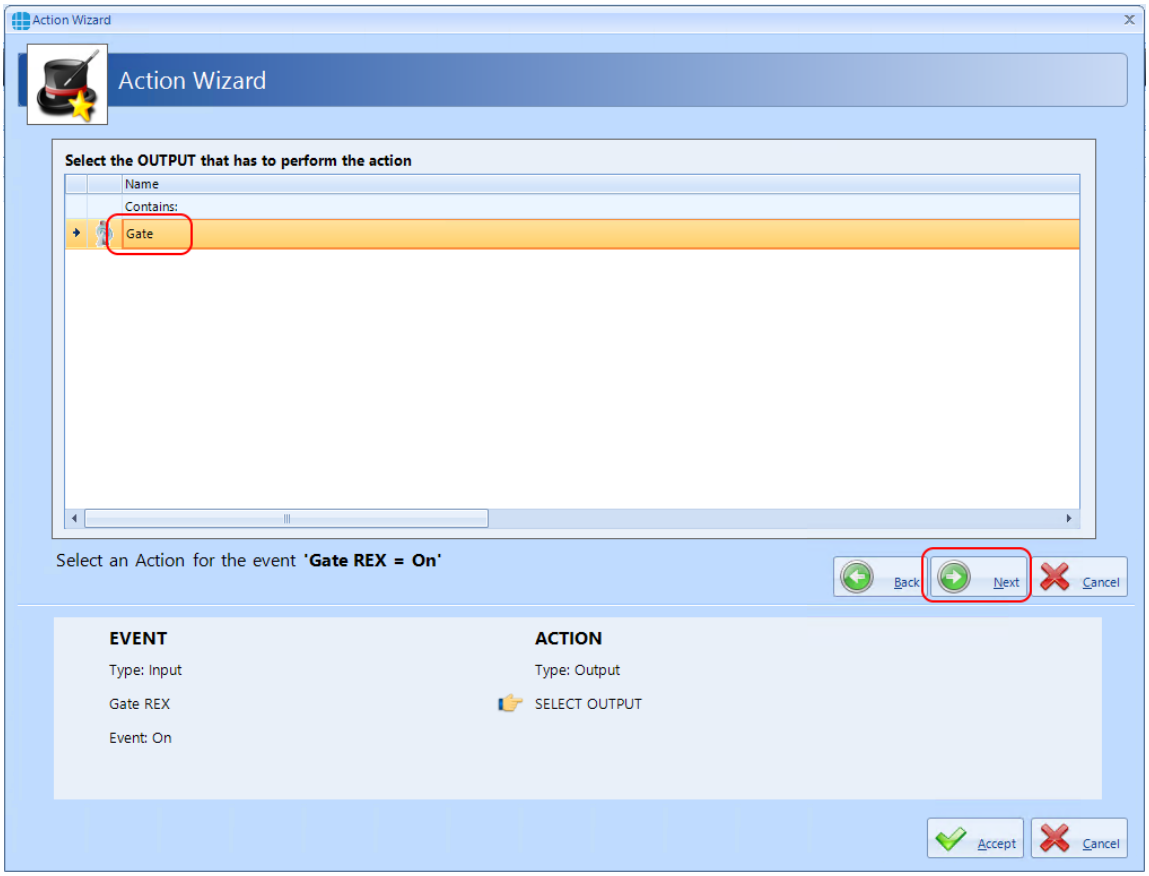
© 2026 Controlsoft Ltd



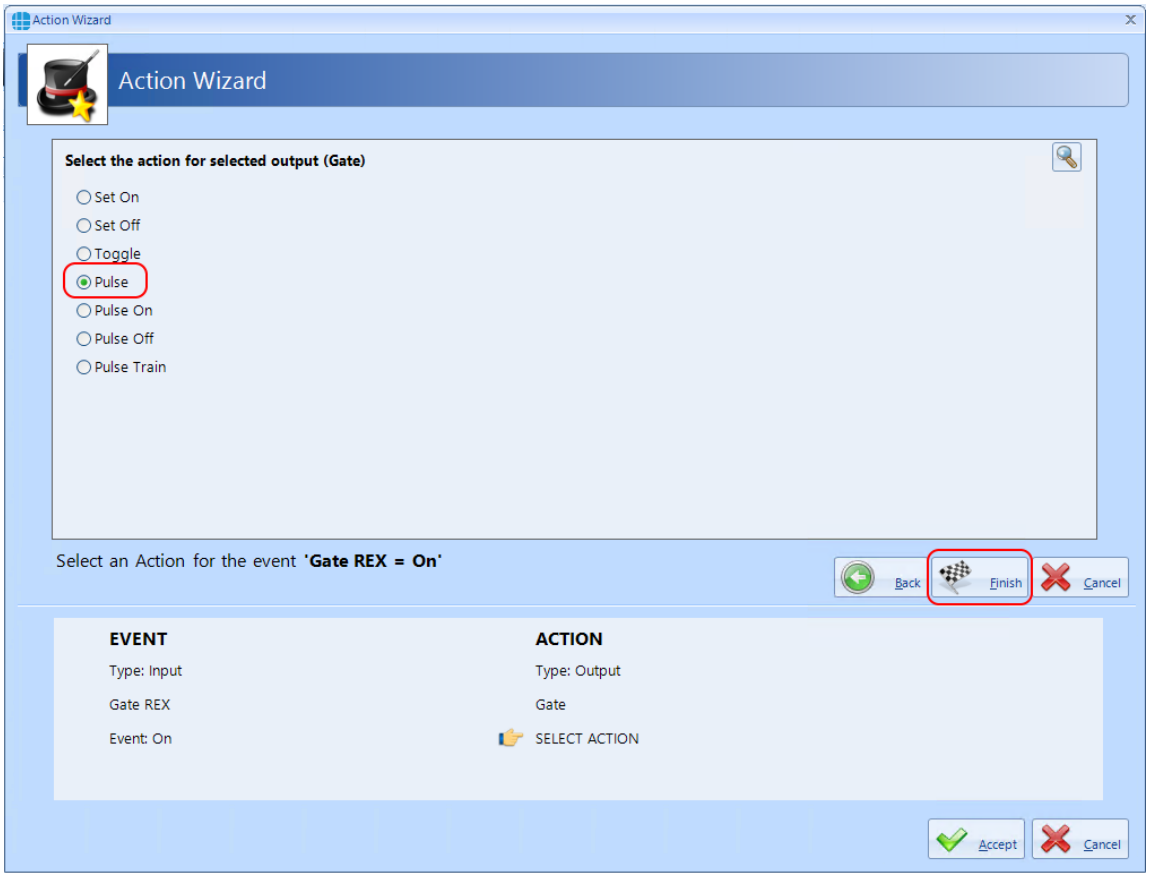


© 2026 Controlsoft Ltd

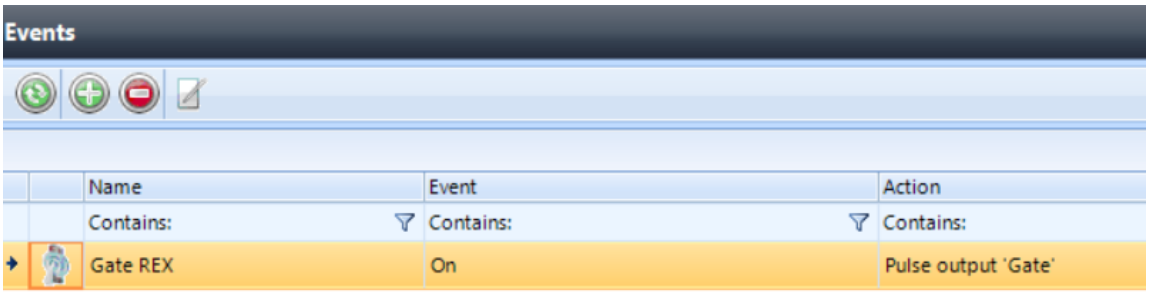




© 2026 Controlsoft Ltd

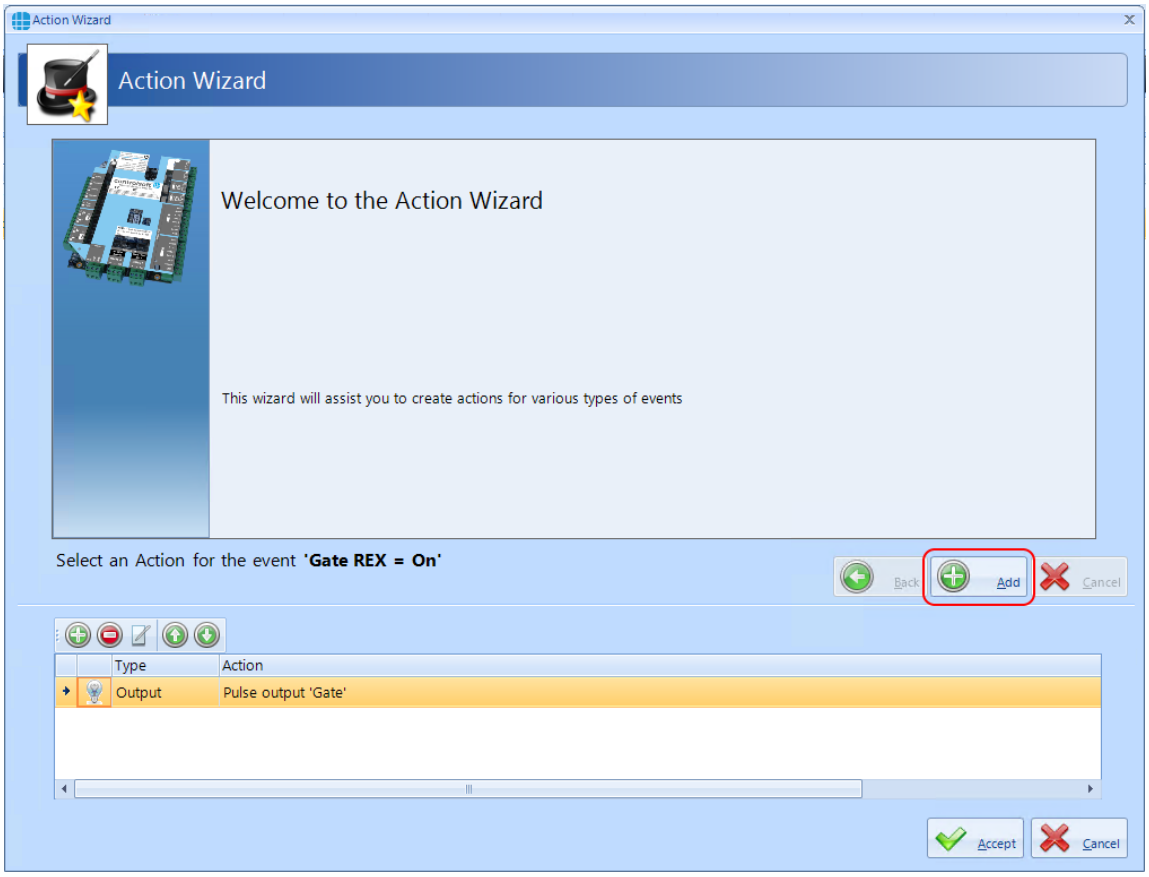


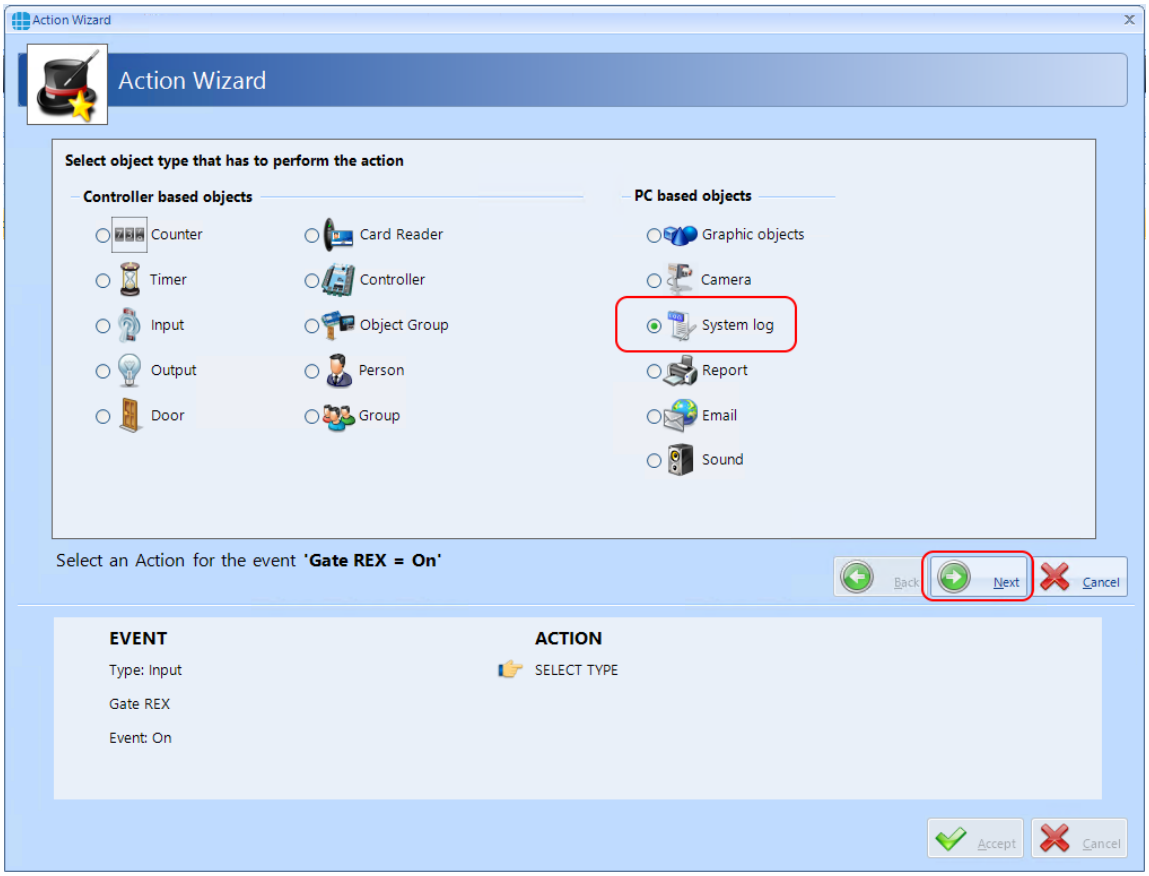
Press **[Finish]** followed by **[Accept]** to view the final result:



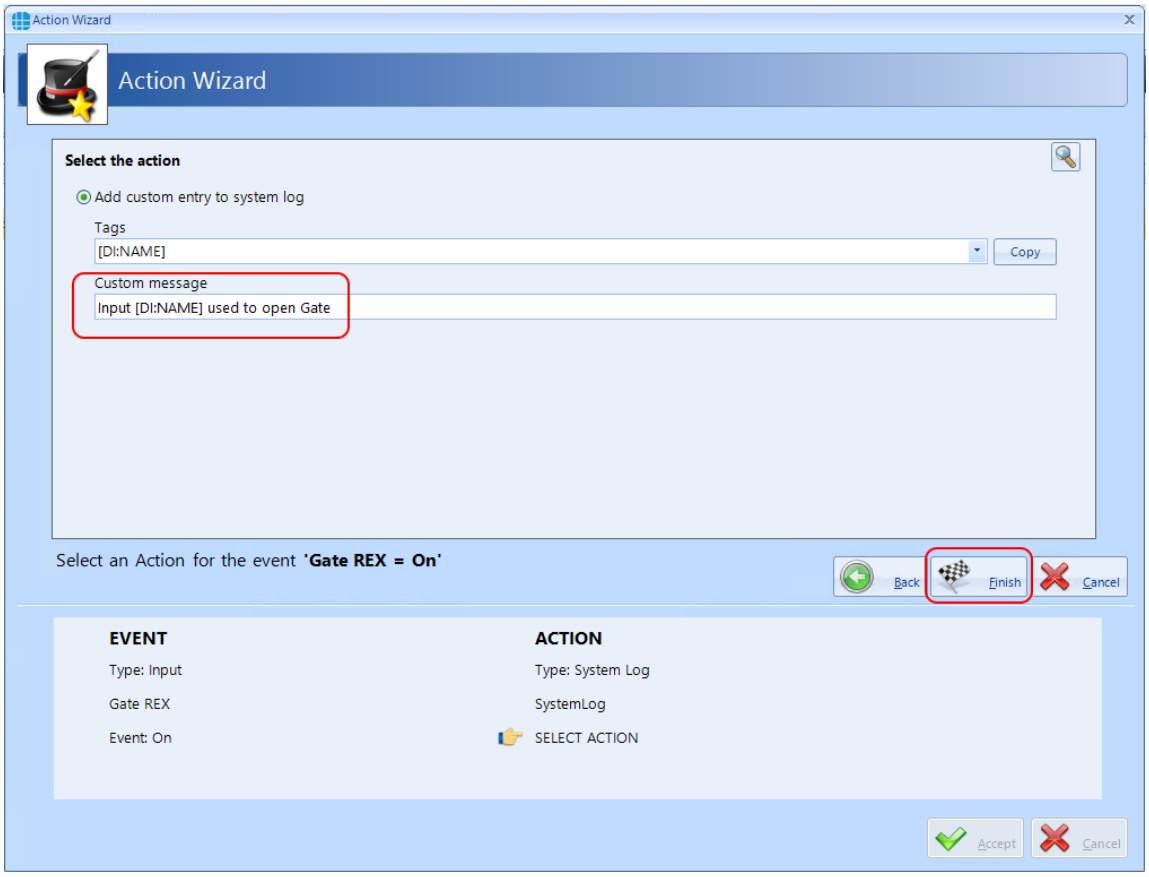
NOTE: It is possible to add more than 1 Action per event. For example, to create an entry in the System log when the Gate has been released, simply open the event and select the **[Add]** button, then create the additional Action:

© 2026 Controlsoft Ltd

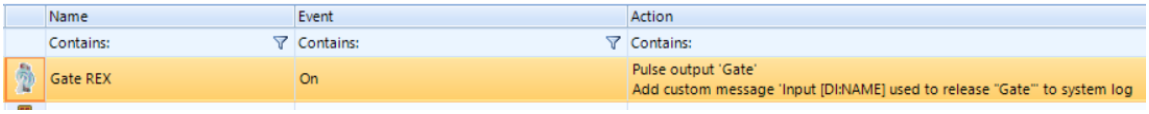




© 2026 Controlsoft Ltd



Press **[Finish]** followed by **[Accept]** to view the final result showing the 2 actions against the one event

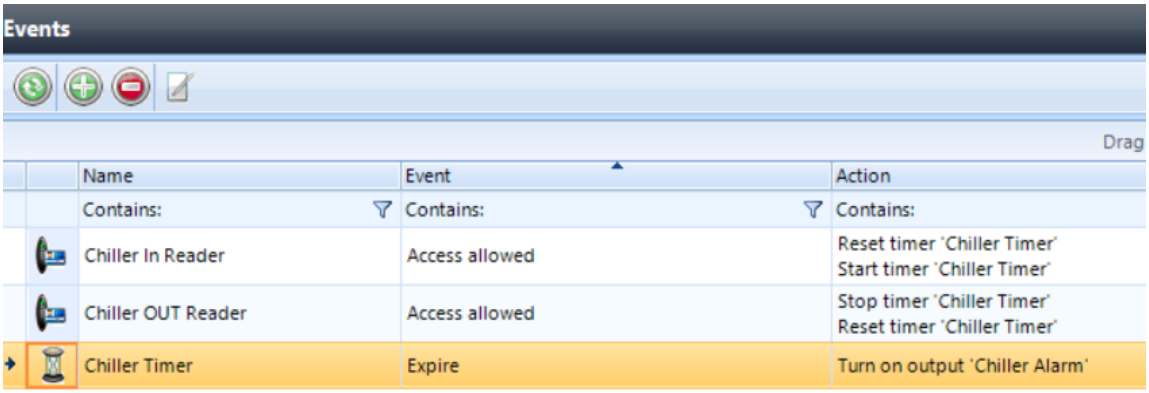


EXAMPLE 2: Sound an alarm if someone has been in the walk-in food chiller for more than 5 minutes.

Create a timer called Chiller Timer with value = 300,000mS (5 minutes)

Create an output called Chiller Alarm, which is connected to a sounder

Create the following Events and Actions:



© 2026 Controlsoft Ltd

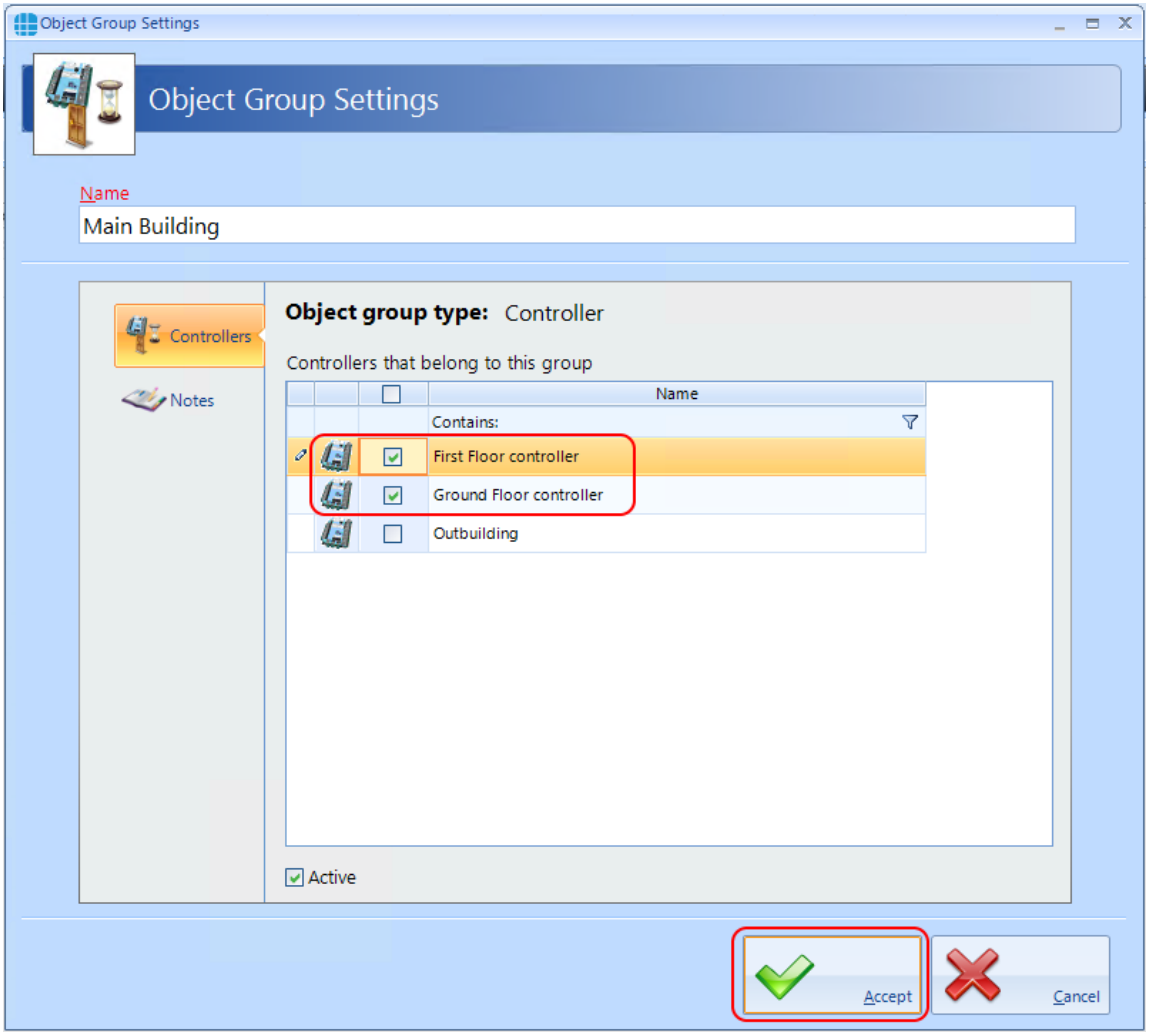
When someone is granted access into the chiller, the timer resets and starts to run (if the alarm is sounding, someone else entering the chiller will reset the timer which will silence the alarm)

When someone leaves the chiller, the timer stops and resets (if the alarm is sounding, resetting the timer on exit will silence the alarm)

If the timer expires, sound the alarm.

EXAMPLE 3: Detect a fire alarm from a controller connected to the main building fire alarm, then trigger a fire alarm on all other controllers in the same building, but not in the outbuildings.

Create an object group called 'Main Building' containing 'Ground Floor' and 'First Floor' controllers but NOT 'Outbuilding'

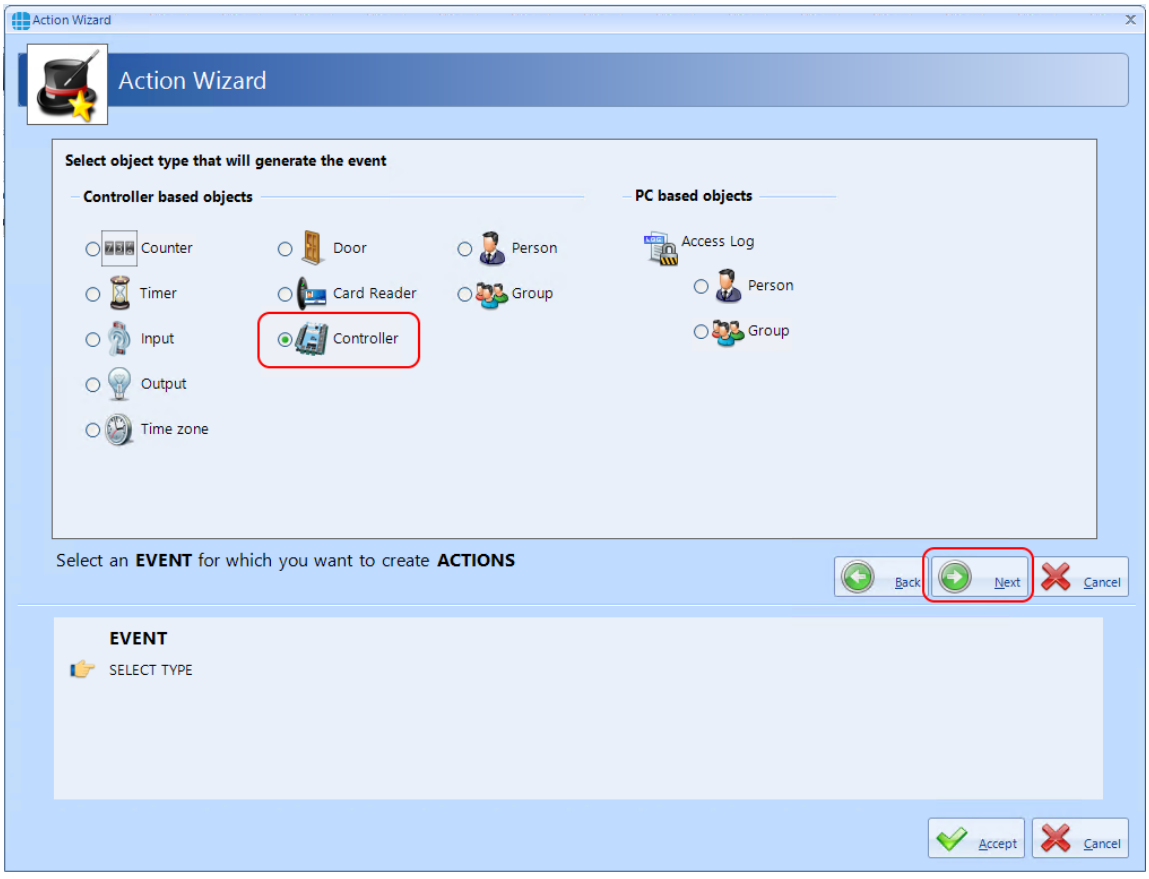


Create Events & Actions

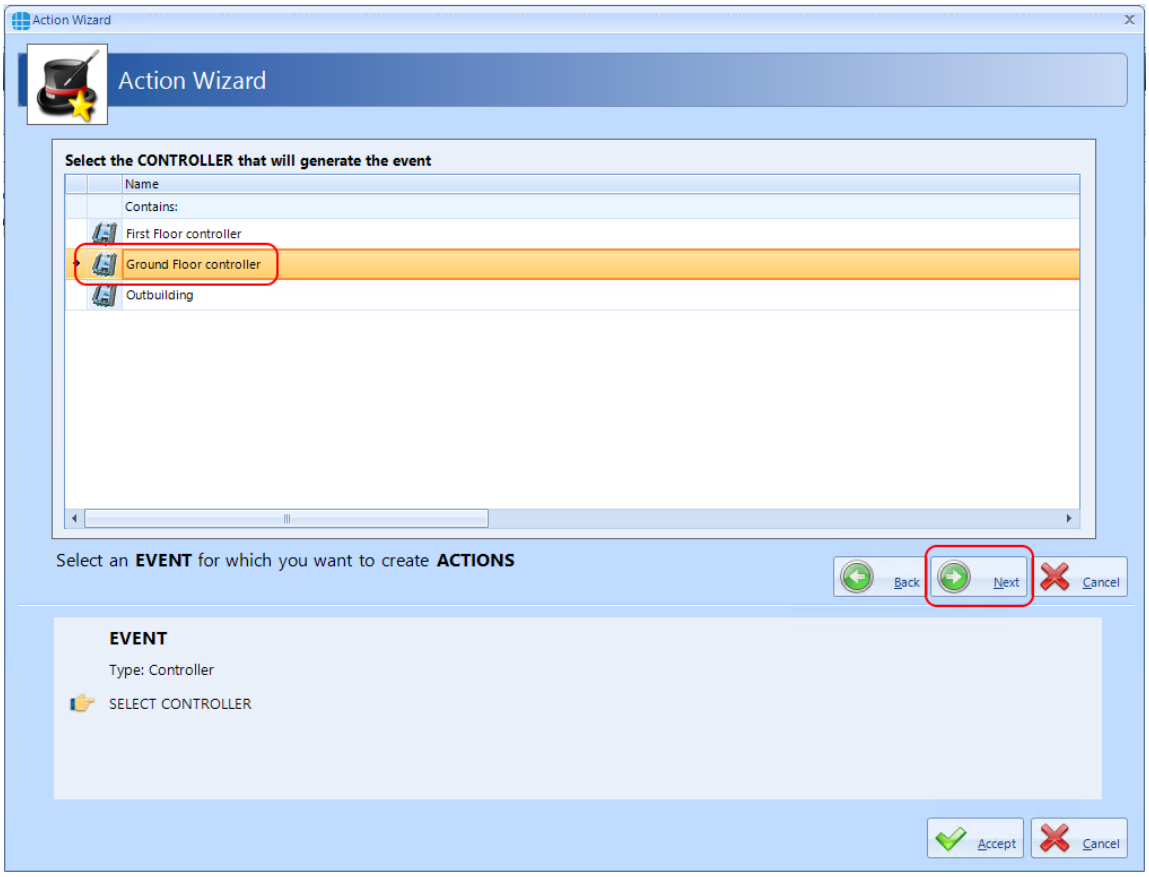
If 'Ground Floor' fire = on, set fire for 'Main Building'

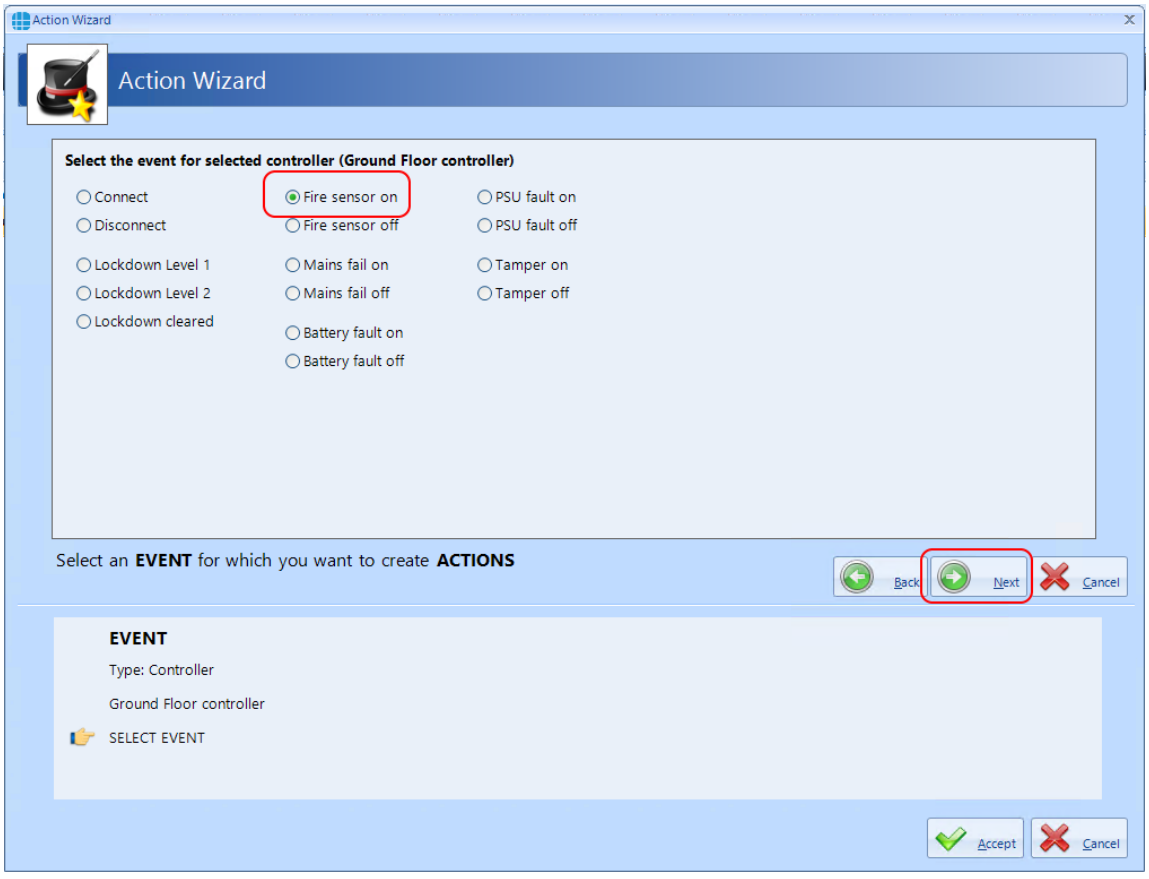
© 2026 Controlsoft Ltd



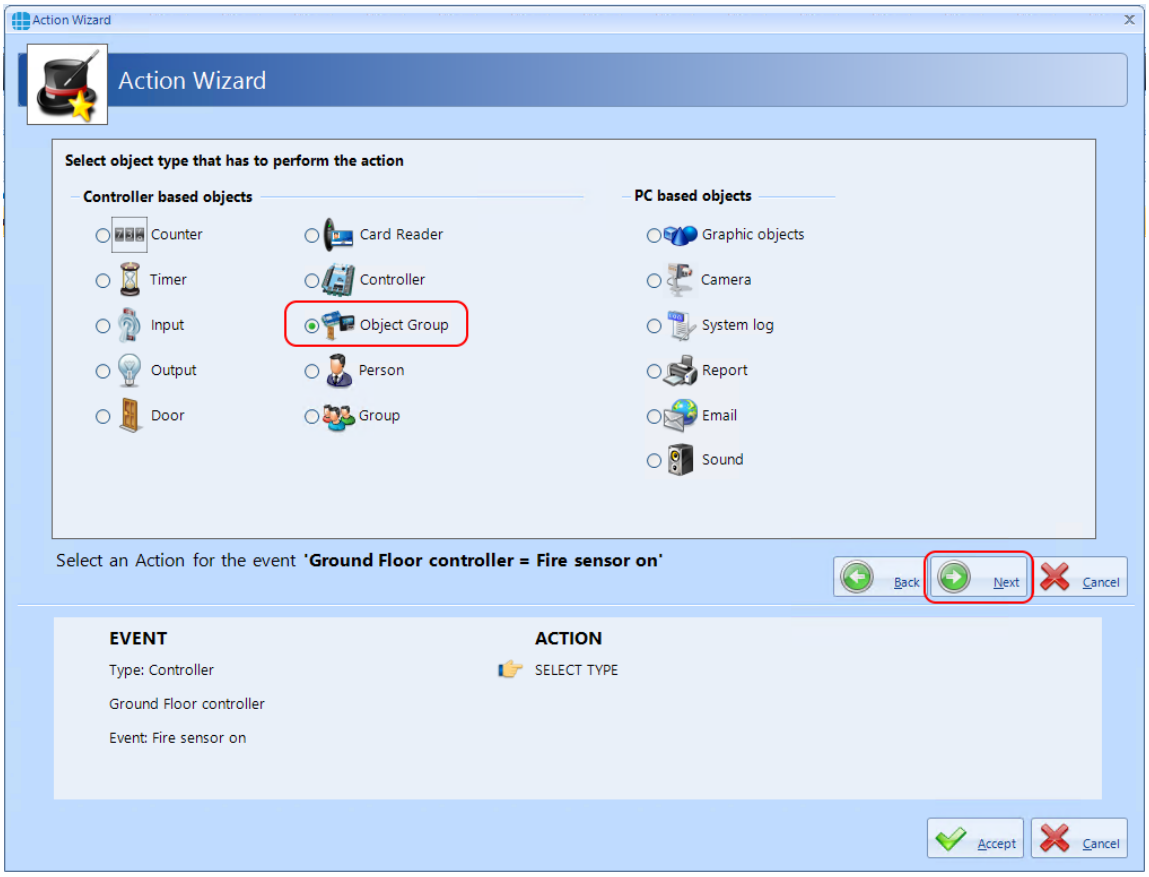


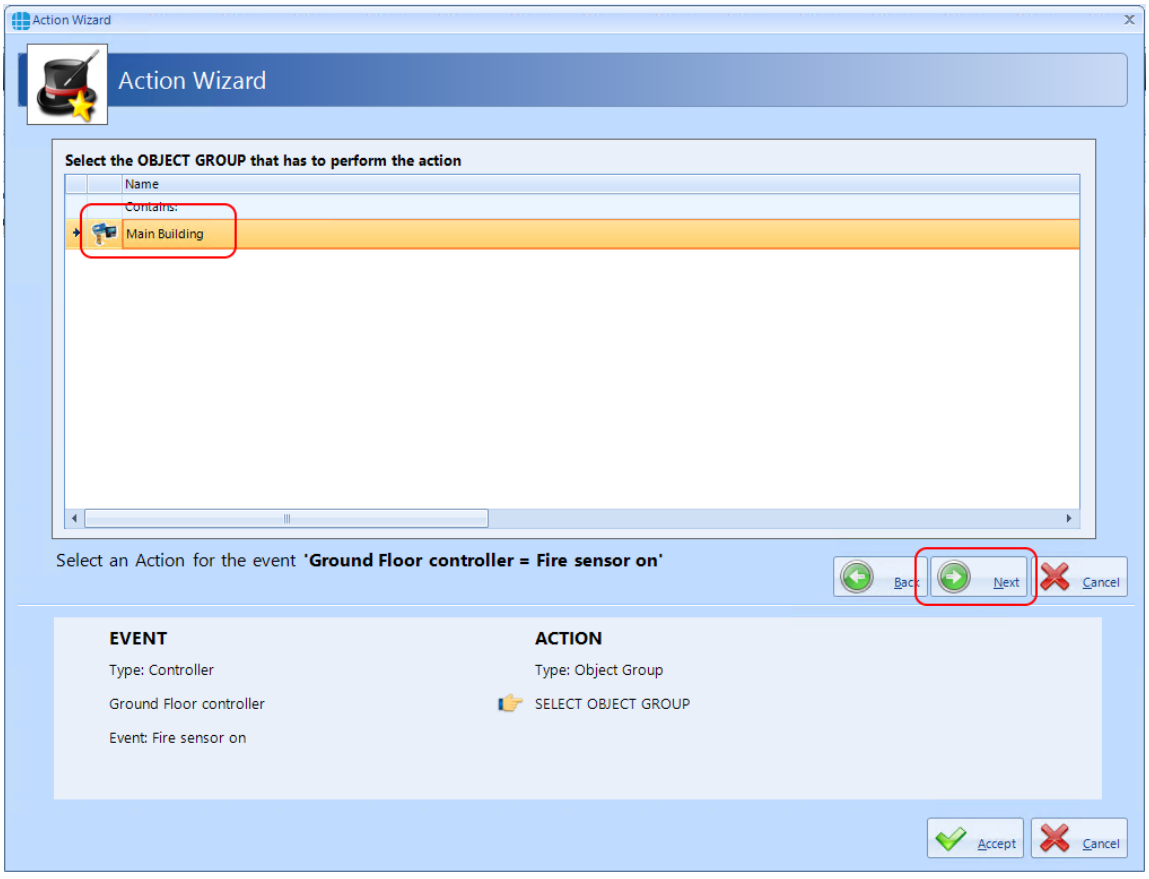
© 2026 Controlsoft Ltd



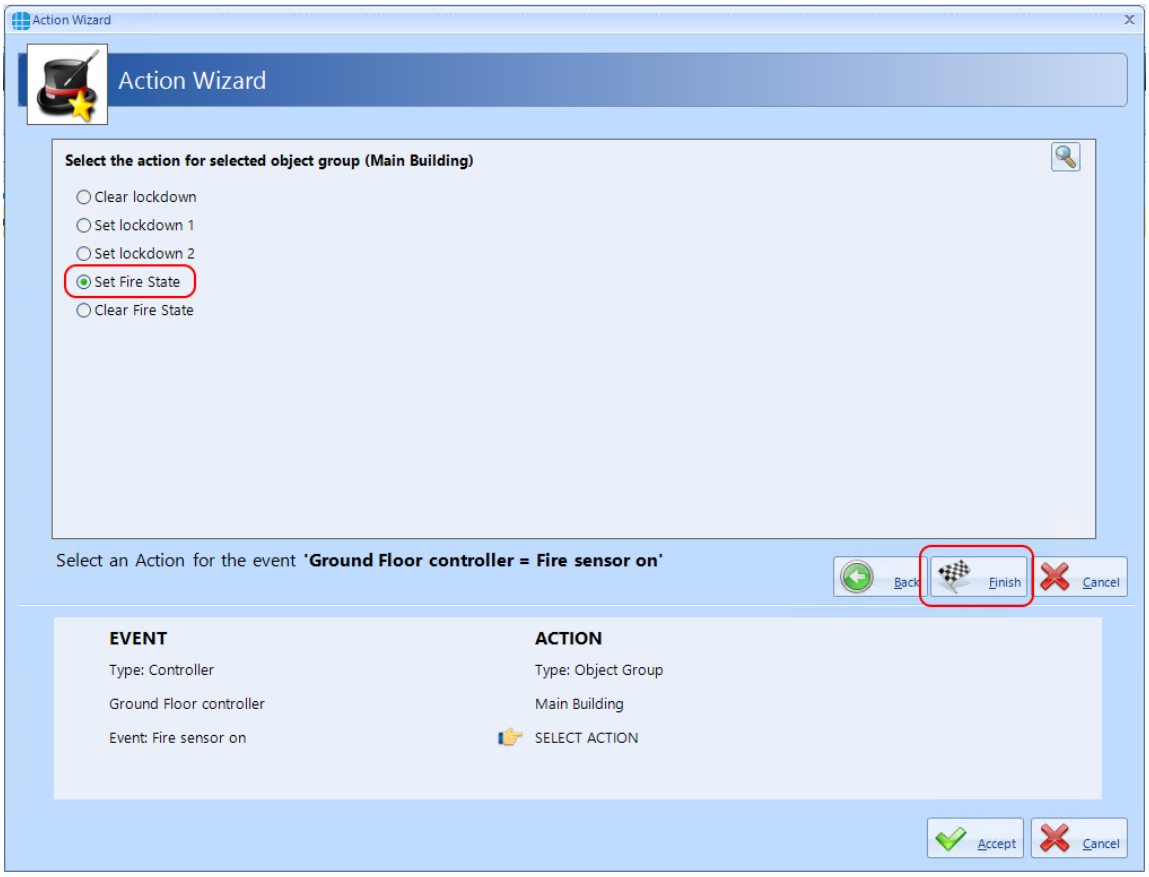


© 2026 Controlsoft Ltd





© 2026 Controlsoft Ltd



Repeat above for: If 'Ground Floor' fire = off, reset fire for 'Main Building'



© 2026 Controlsoft Ltd

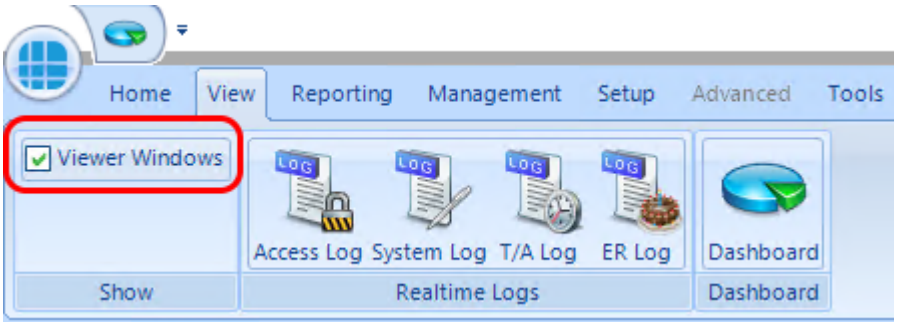
Event Viewers and Reports

21 Event Viewers and Reports

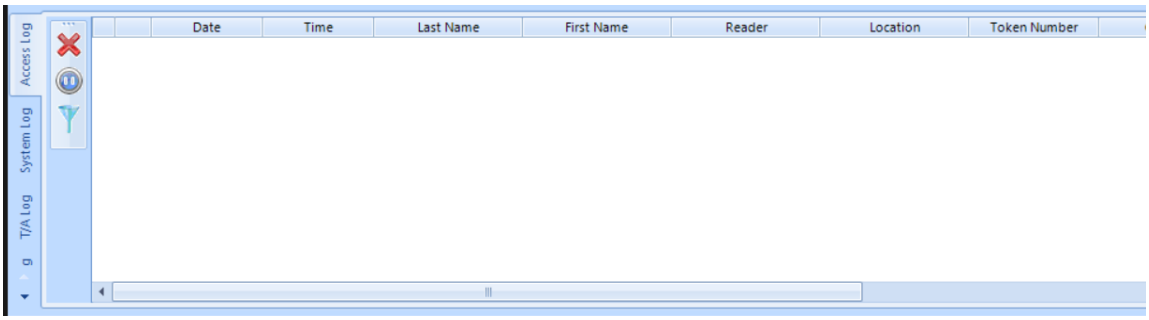
The Event Viewer in Identity Access software is a powerful tool for analysing system activity.

21.1 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. ***NOTE: This does not delete the events from the database.***

 Pause/Run: Pause will stop the display from updating, Run will restart the display updates. ***NOTE: Any events received while paused will not be displayed but will be entered into the database.***

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

© 2026 Controlsoft Ltd

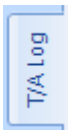
The information to be displayed is controlled by the 4 tabs below the Viewer Window:



Displays events from the Access Log.



Displays events from the System Log.



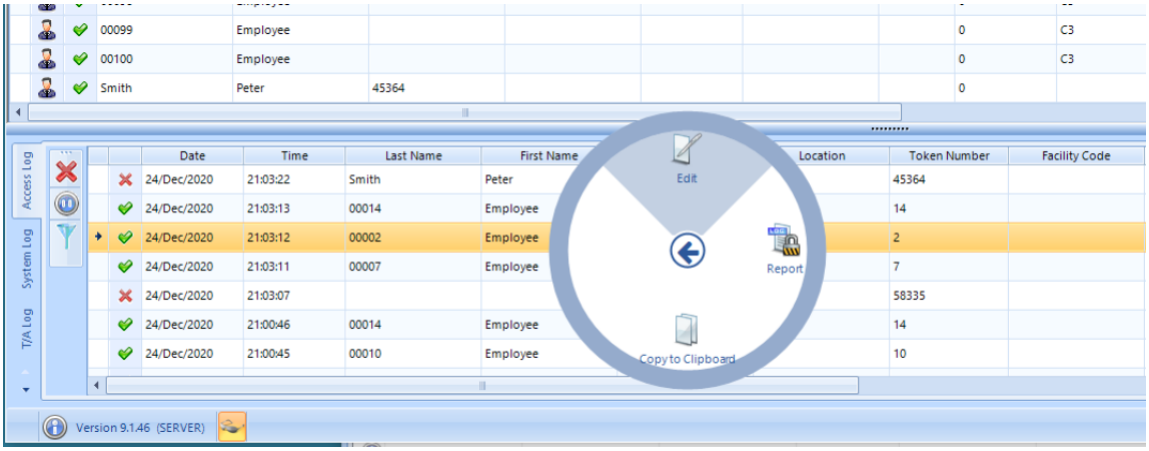
Displays events from the Time & Attendance Log



Displays Events and Actions from each controller.

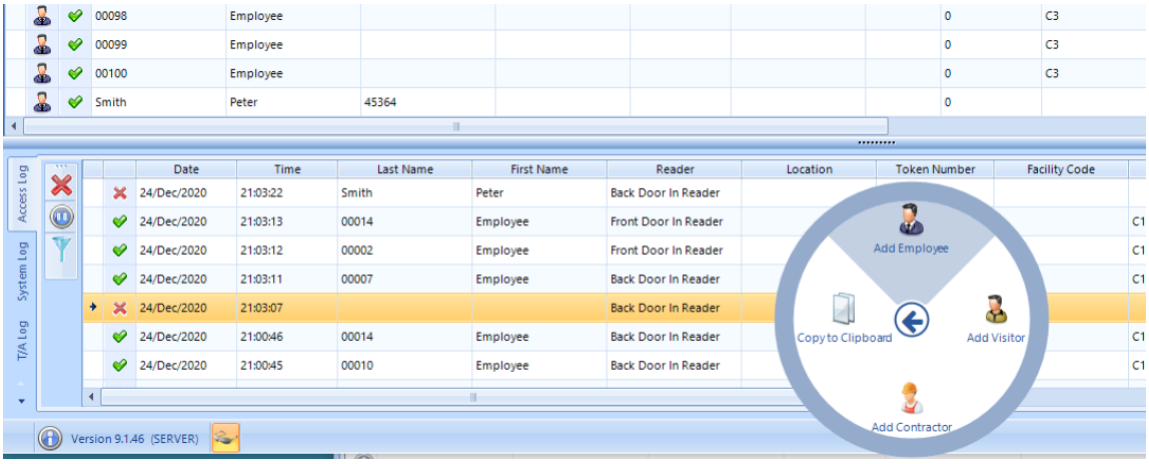
NOTE: The size of the viewer window can be adjusted simply by dragging the top of the window up or down.

If an access allowed or access denied event for a user that exists in the database is right clicked, the option wheel provides an option to edit that user:



If an access denied event for a user that does not exist in the database is right clicked, the option wheel provides an option to add that user as an Employee, Visitor or Contractor:

© 2026 Controlsoft Ltd



21.2 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.**

If the Fire Rollcall option is enabled to automatically run the Fire Roll Call Report, then on activation of a fire alarm event on the master controller the report will automatically be printed to the default printer (see IA Configuration - Reports 246).

If users are allocated to Companies and Departments, the Fire Roll Call report will print all the users in the building from the first company/department followed by a page break, then all the users in the building from the second company/department etc.

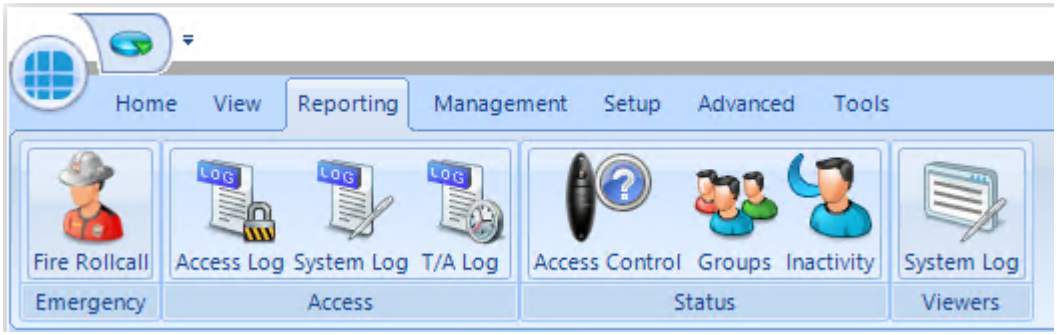
NOTE: The Fire Rollcall report is NOT available in Identity Access unless an Identity Access Professional or Enterprise licence is applied.

21.3 Access Control Reports

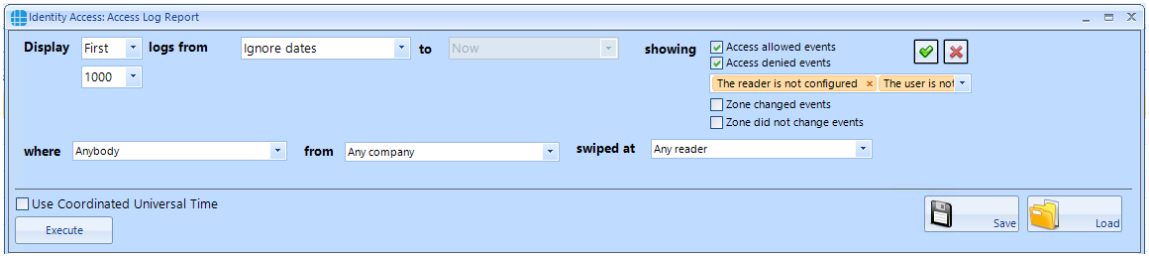
An Access Control report is a record of when people have used their token at a reader, providing an audit trail of when someone entered or exited areas of the premises.

© 2026 Controlsoft Ltd

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



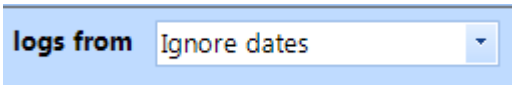
This then runs the Identity Access: Access Log Report form as shown below:



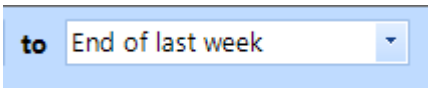
The options on generating the report are as follows:



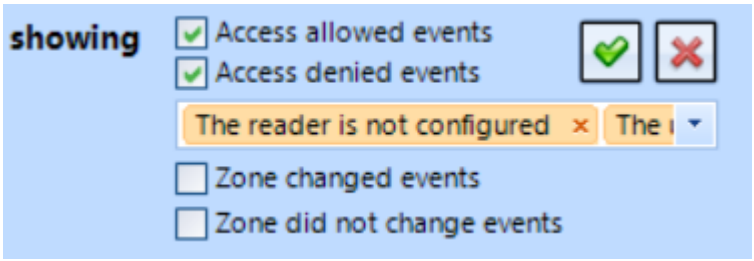
defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.



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

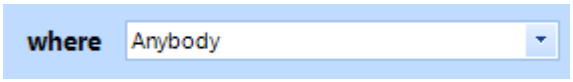


defines the date that the report ends (Example today or end of last month)

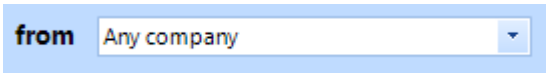


defines which events are to be reported on, Access Allowed and/or Access Denied and any combination of events from the drop down list . The Tick selects all events in the dropdown list and the Cross deselects all events in the dropdown list. When AntiPassBack is enabled for a door, the system will also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

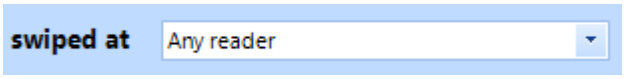
© 2026 Controlsoft Ltd



defines which user/s to report on

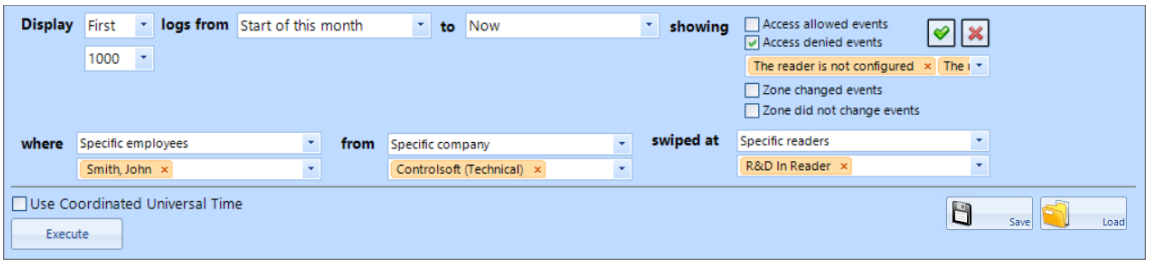


defines which Companies and Departments to report on

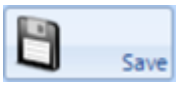


defines which reader/s to report on.

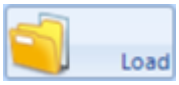
As an example, to generate a report to see if John Smith tried to get into R&D this month, the configuration would look like:



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 **Management** and **Employee** / **Visitor** / **Contractor** (depending on who you wish to run your report on).

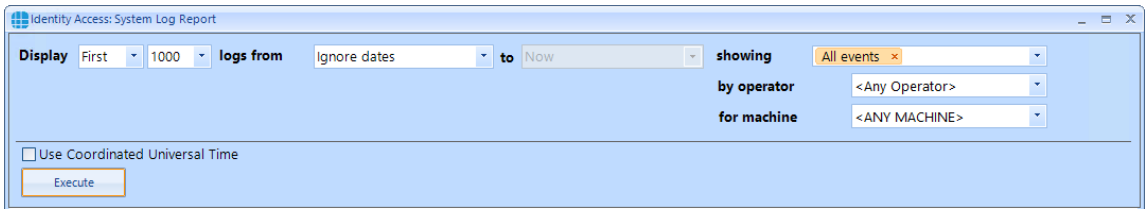
Highlight the user by left clicking their entry and click the  icon. This will automatically generate a report for this specific person. To run a report on several people it is possible to hold down the [Ctrl] key and highlight multiple entries, then click the  icon.

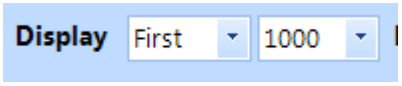
21.4 System Log Reports

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.**

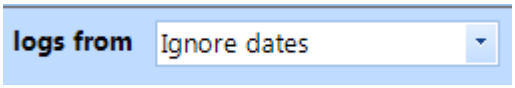
© 2026 Controlsoft Ltd

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

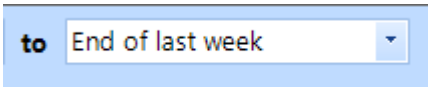




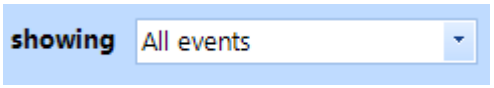
defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.



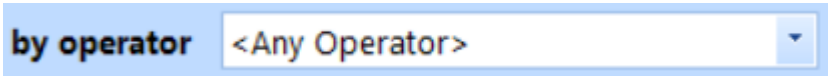
defines the date that the report starts (Example ignore dates, start of last month or 1st January 2016)



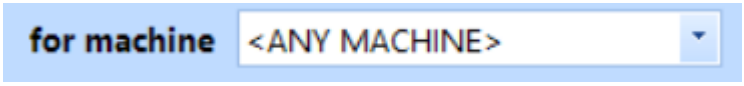
defines the date that the report ends (Example today or end of last month)



defines which events are to be reported on, such as startup & shutdowns, iNet events or which Operators have logged on.



defines which Operator to report on



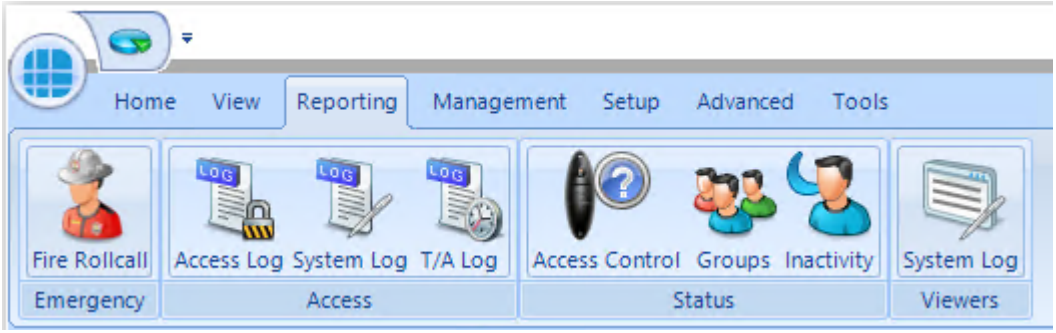
defines which Client machine to report on.

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

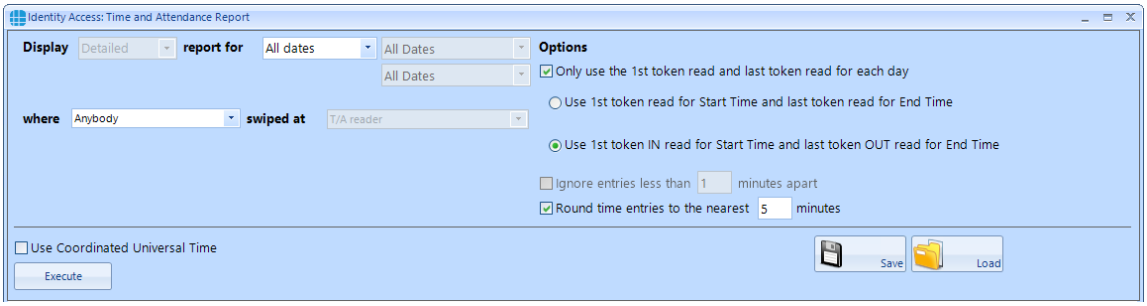
21.5 Time & Attendance Report

A Time & Attendance (T/A) report (sometimes called a Timesheet Report) will list each transaction when users 'clock in' and 'clock out' to provide a total number of hours that the user spent on site that day. To run a T/A Report, select **Reporting** and **T/A Log**

© 2026 Controlsoft Ltd



The T&A reporting screen is as follows:



The options available when generating a report are as follows:

Display: This option is greyed out in this version

report for: Allows the report to be run between certain dates. Some predefined options are available such as "Today", "This week", "Last week", "This month" etc. Custom dates and times can also be entered for maximum flexibility.

where: The report can be further refined by selecting one or more users to include in the report

swiped at: This field is preselected as "T/A reader" and cannot be edited in this version



Allows the current query to be saved for later use



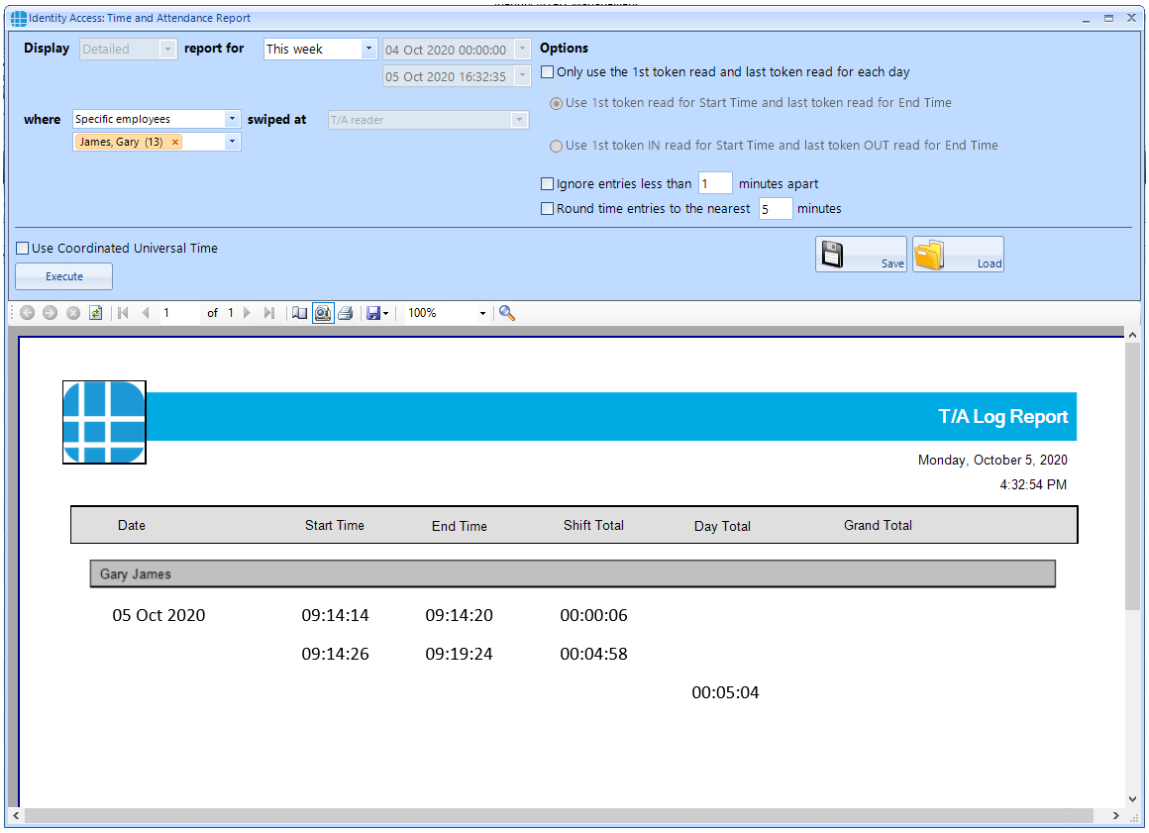
Opens a saved query

Options: The options allow the Time and Attendance data to be viewed in different ways. To show how these options work, consider the following data from the Access Log:

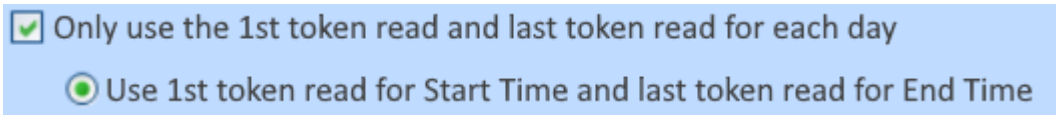
Date	Time	User	Location	Company	Reason
05/10/2020	08:00:10	Gary James	front door Out Reader		Group access allowed
05/10/2020	09:14:14	Gary James	front door In Reader		Group access allowed
05/10/2020	09:14:20	Gary James	front door Out Reader		Group access allowed
05/10/2020	09:14:26	Gary James	front door In Reader		Group access allowed
05/10/2020	09:19:24	Gary James	front door Out Reader		Group access allowed
05/10/2020	09:19:33	Gary James	front door In Reader		Group access allowed
05/10/2020	09:19:42	Gary James	front door In Reader		Group access allowed

© 2026 Controlsoft Ltd

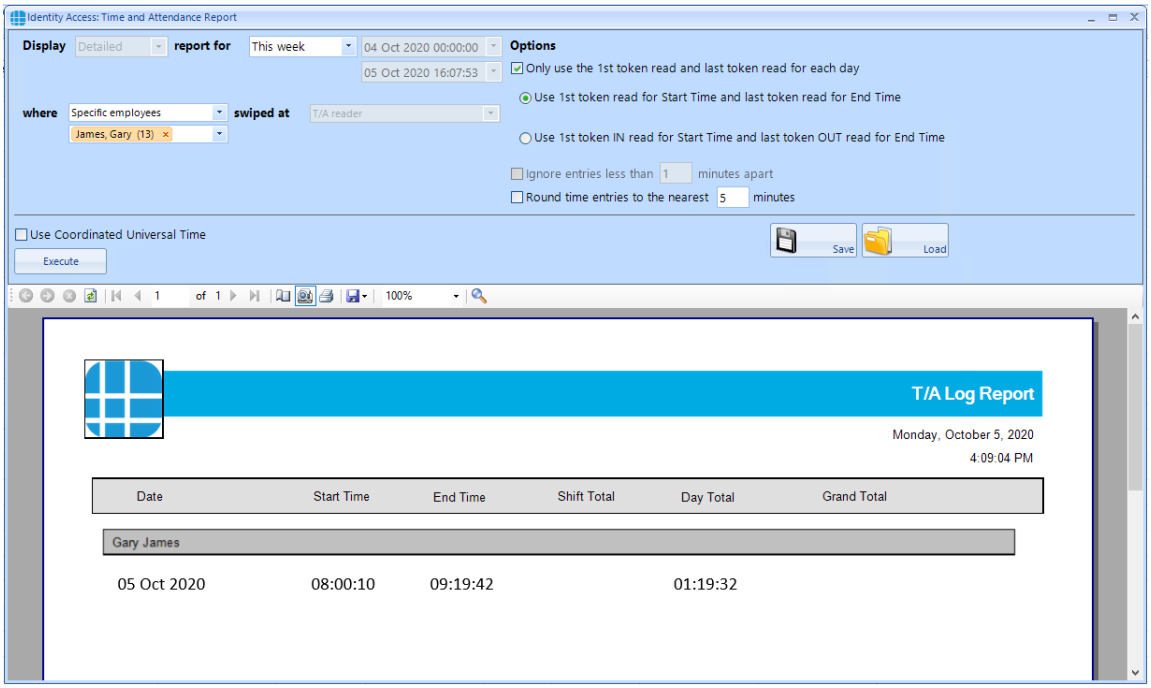
If we run a T&A report with no options selected, we get the following report:



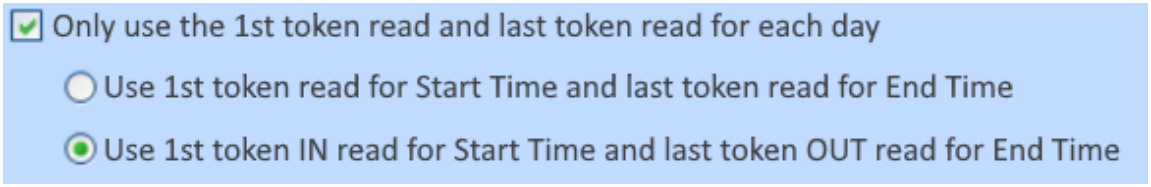
The first OUT time is ignored as it has no associated IN time. The report then shows the IN, OUT, IN and OUT activations. The final 2 IN times are also ignored as there are no associated OUT times.



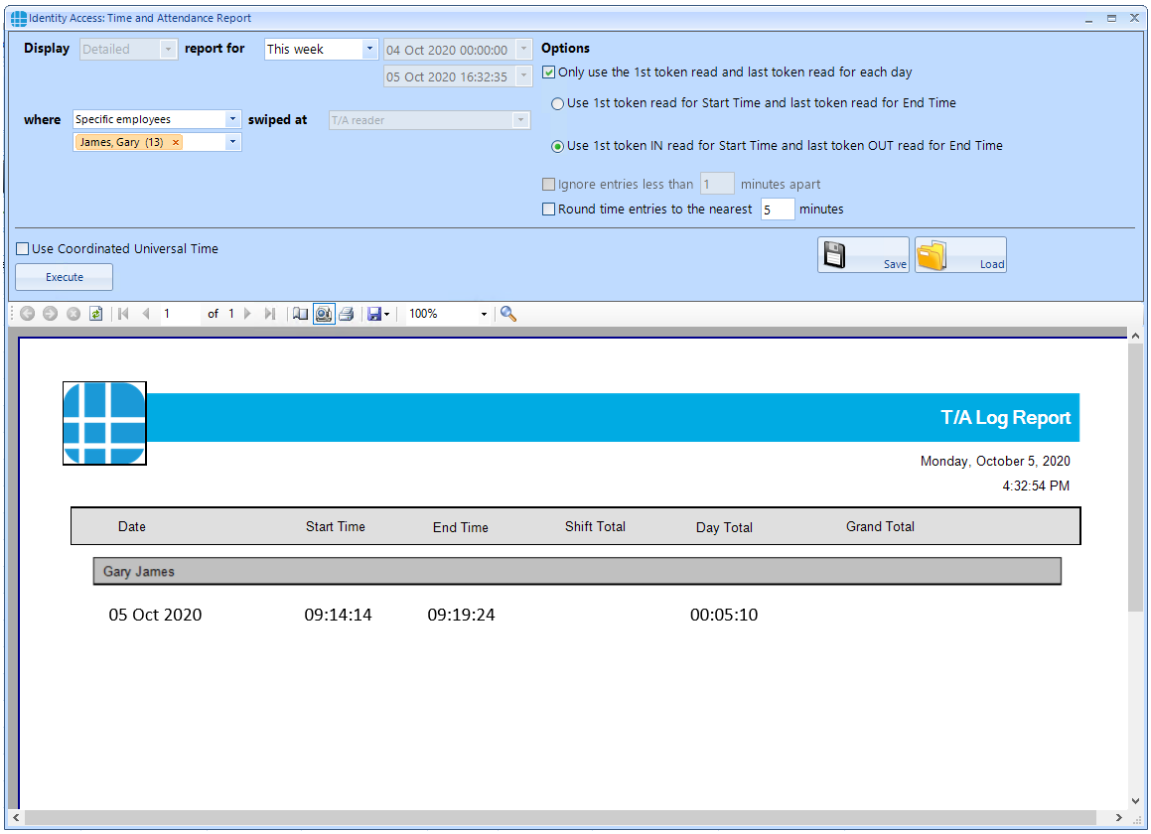
If we enable this option, the report will use the first and last transaction for that day:

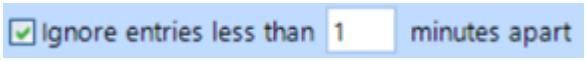


© 2026 Controlsoft Ltd

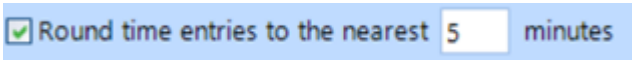


If we enable this option, the report will use the first transaction at an IN reader, and the last transaction at an OUT reader for that day:



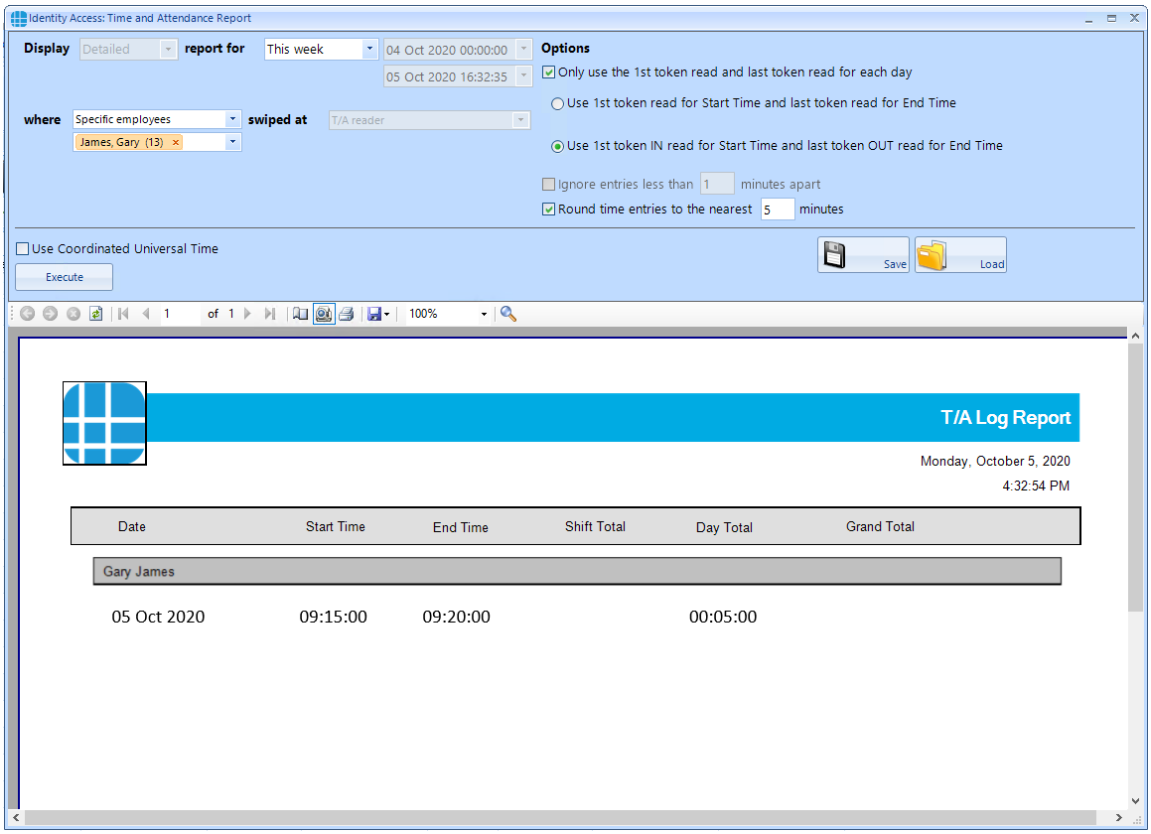


If the time between 2 transactions is less that the specified time, neither transaction will be included in the report.



This option will round the times up or down, such as :

© 2026 Controlsoft Ltd

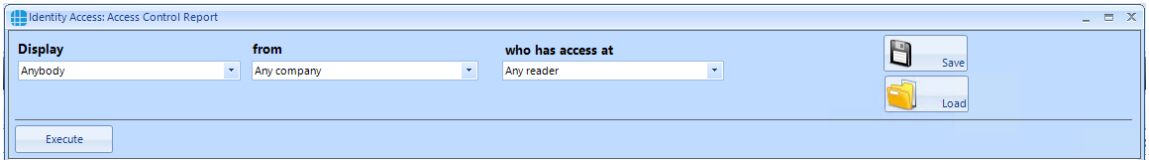


21.6 Access Control Status Report

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:



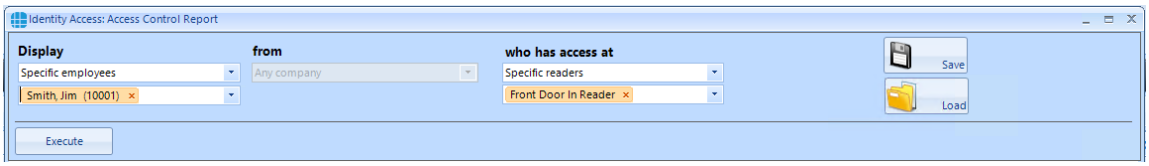
Display - selects specific users to report on

from - selects specific Companies and Departments to report on

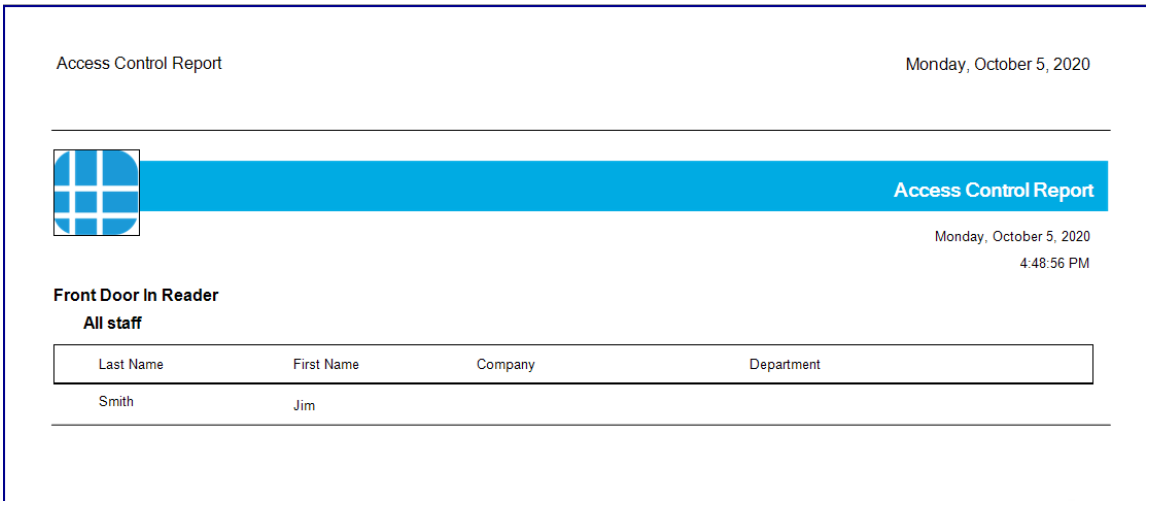
who has access at - selects the readers to report on

© 2026 Controlsoft Ltd

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



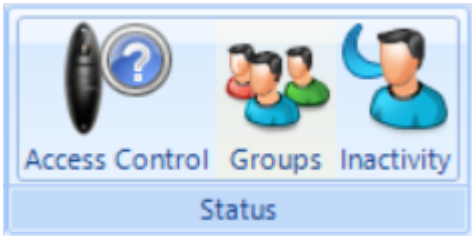
Clicking **[Execute]** would then generate the following report:



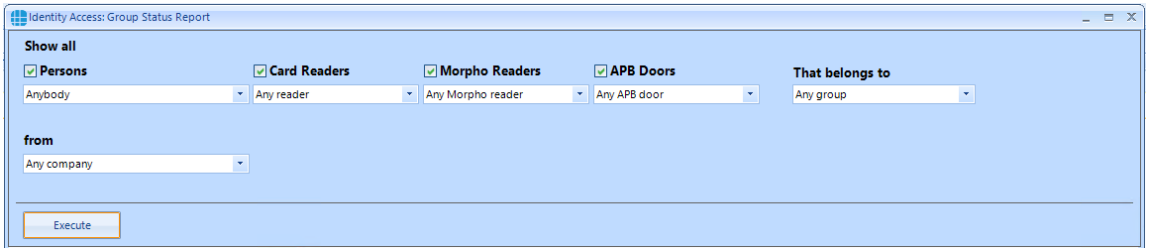
This report shows that the reader called "Front Door In Reader" is accessible by the group "All staff" which includes the user "Jim Smith"

21.7 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



© 2026 Controlsoft Ltd

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

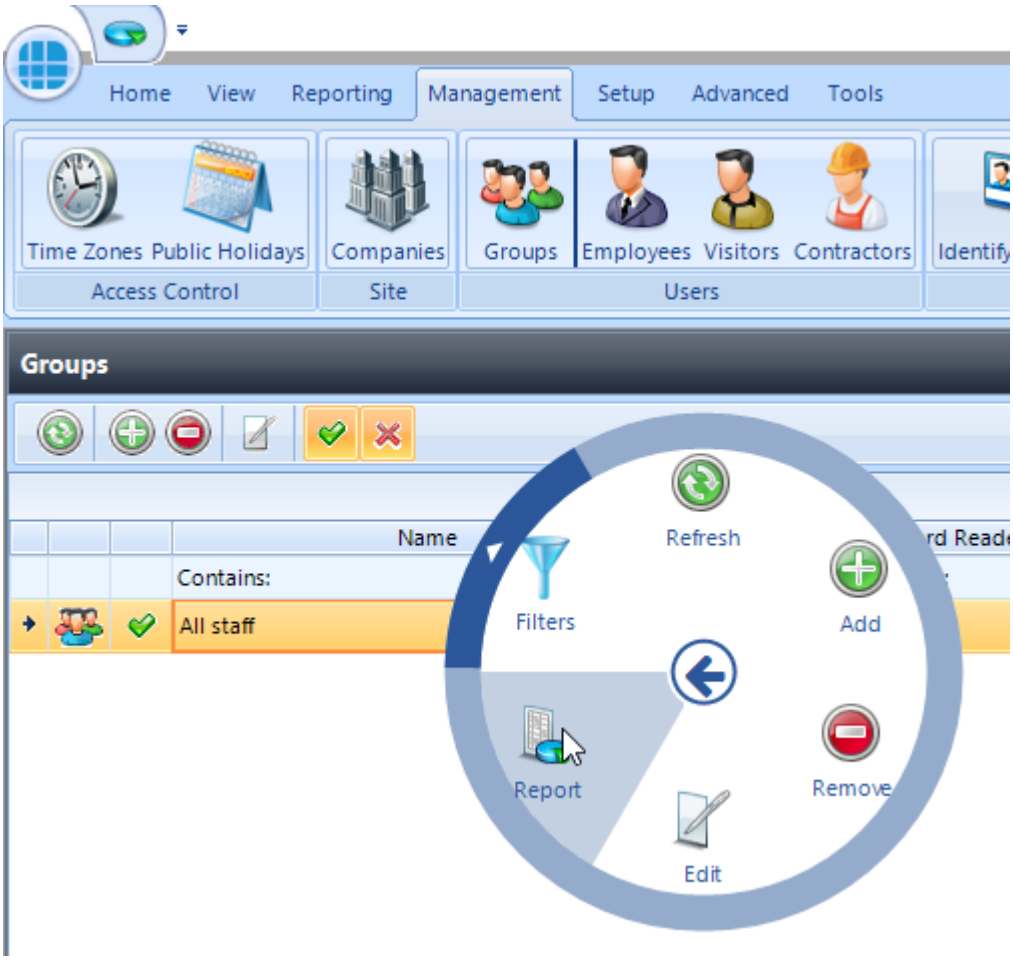
APB Doors - choose any combination of AntiPassBack doors to include in the report

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

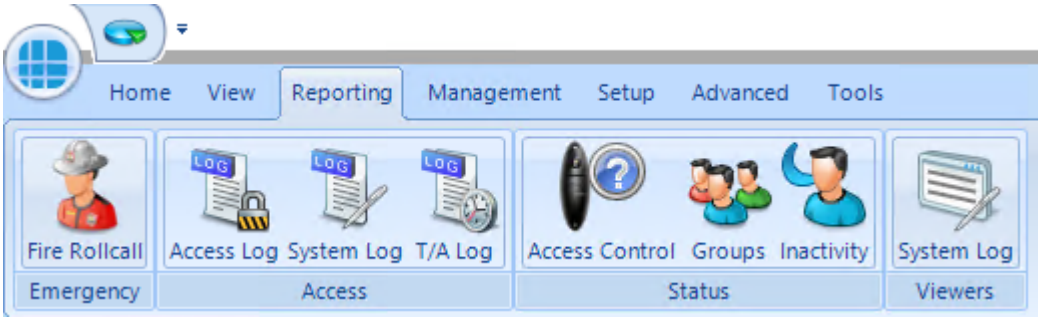


21.8 Inactivity Report

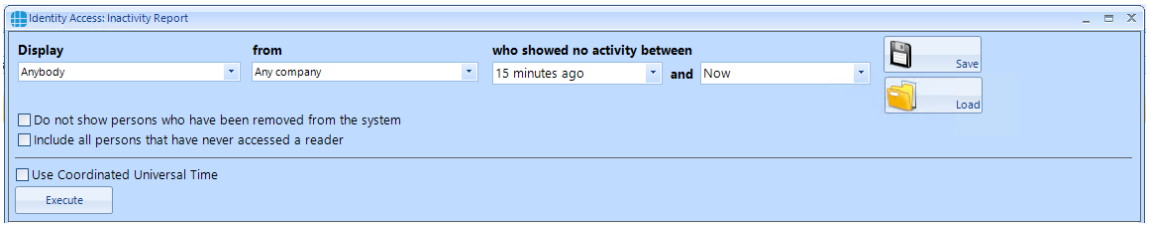
The Inactivity report is used to identify users who are no longer using the system, to allow an operator to effectively manage the user database.

© 2026 Controlsoft Ltd

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

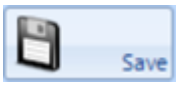
from - selects specific Companies and Departments to report on

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

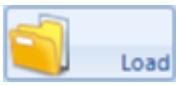
Do not show persons who have been removed from the system will exclude any users who have already been deleted.

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

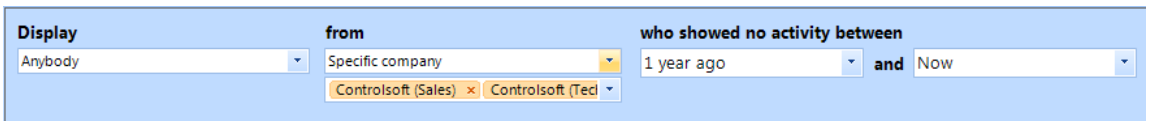


saves the current query for later use



loads a saved query

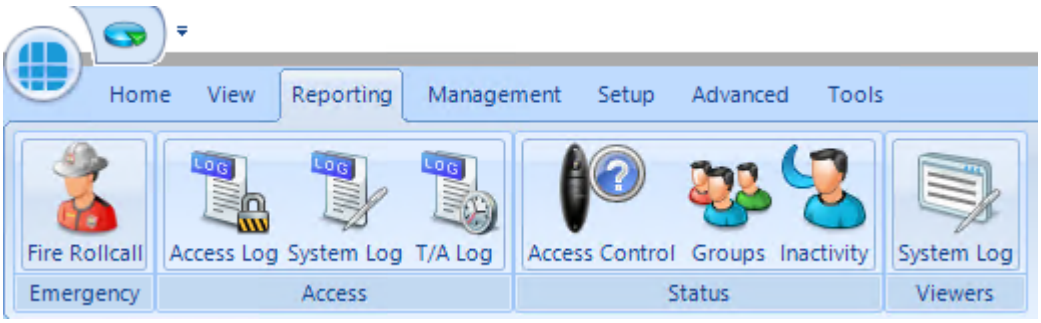
EXAMPLE: to report inactivity on anyone in Controlsoft Sales or Technical within the past year, the report configuration would look as follows:



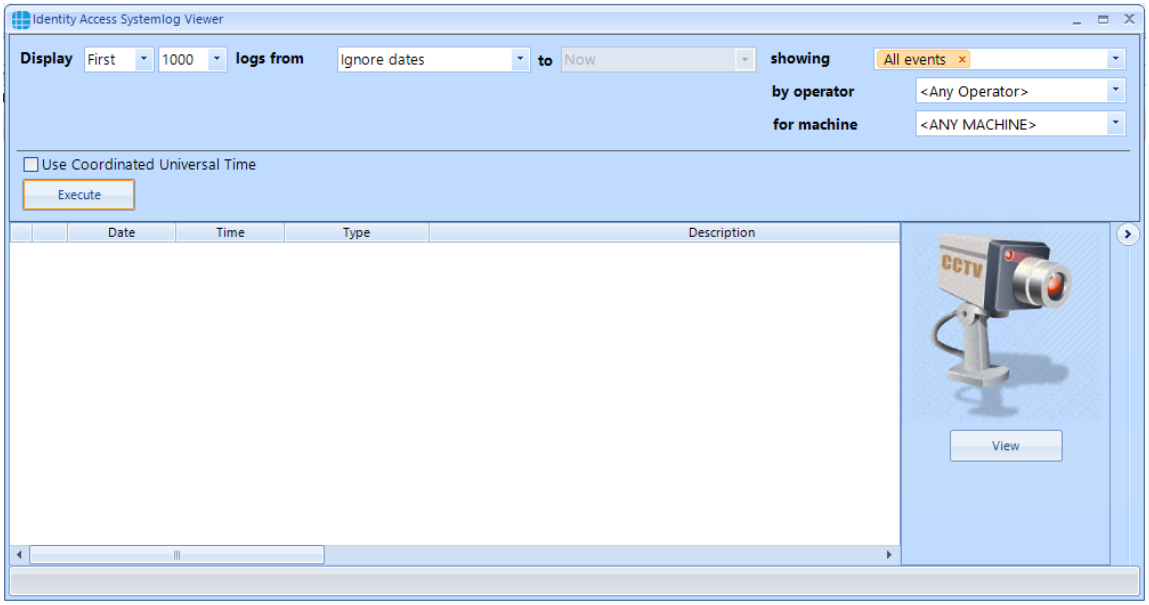
© 2026 Controlsoft Ltd

21.9 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)

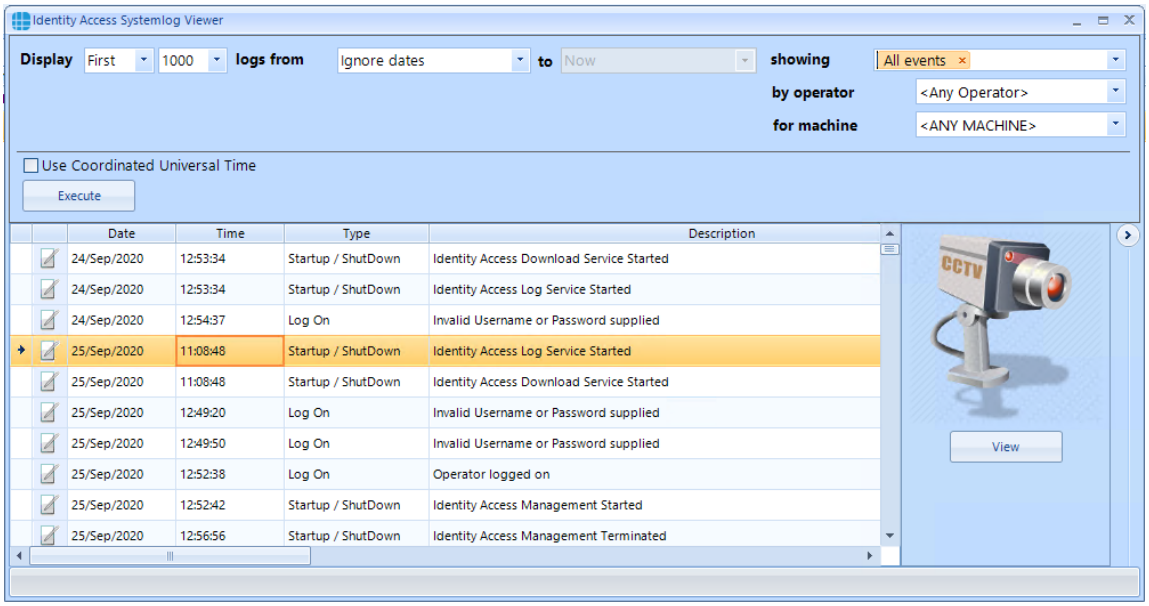
showing - which events are to be reported on, any combination of events from the drop down list .

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

© 2026 Controlsoft Ltd



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

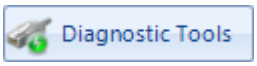
© 2026 Controlsoft Ltd

Engineer Tools and Services

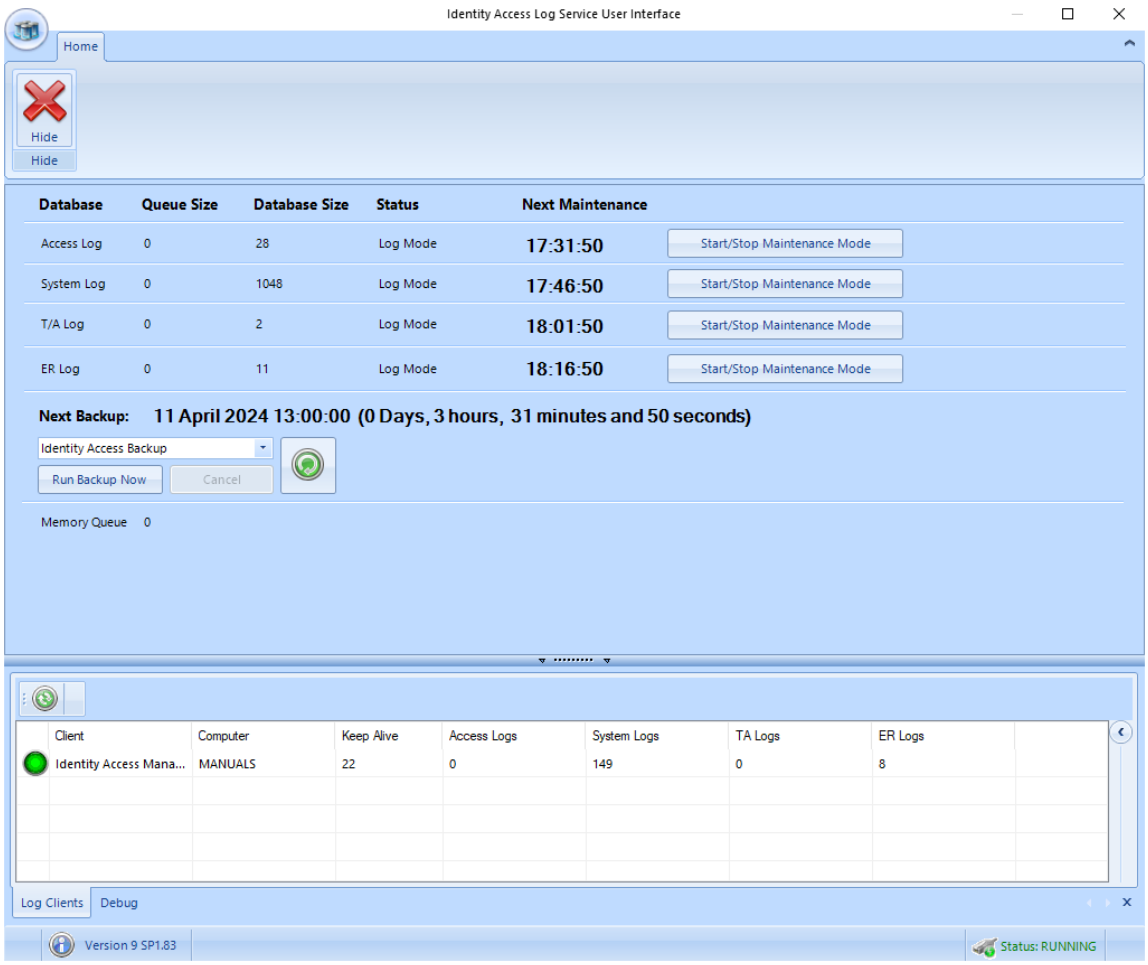
22 Engineer Tools and Services

22.1 Database Tools (Log Service)

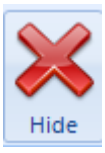
To load the Database Tools, log in to Identity Access as an administrator and select the **Database Tools** option in the lower right corner. This will load the **Log Service** user interface.



The **Log Service** reads events from Log Buffers and stores them in the SQL database.



The option buttons are:



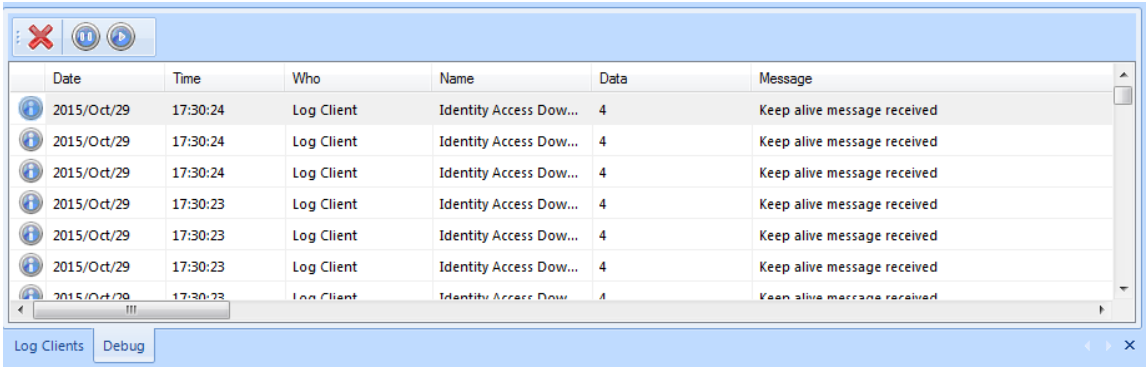
Closes the Log Server.

© 2026 Controlsoft Ltd

The upper window shows the size of the Access, System and T&A database and queues and when the next system maintenance is due. Also shown is the date and time of the next scheduled backup. The **[Run Backup Now]** button can be used to initiate a backup at any time. ***NOTE:*** All backup activity is recorded in the IA System log

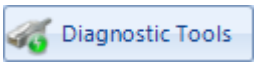
The **Log Clients** window shows devices are connected to the Log Service, in this instance the PC named MANUALS

Selecting **[Debug]** will show debug information on the communications between different software modules.



22.2 Diagnostic Tools (Download Service)

To load the Diagnostic Tools, log in to Identity Access as an administrator and select the **Diagnotic Tools** option in the lower right corner. This will load the **Download Service** user interface.

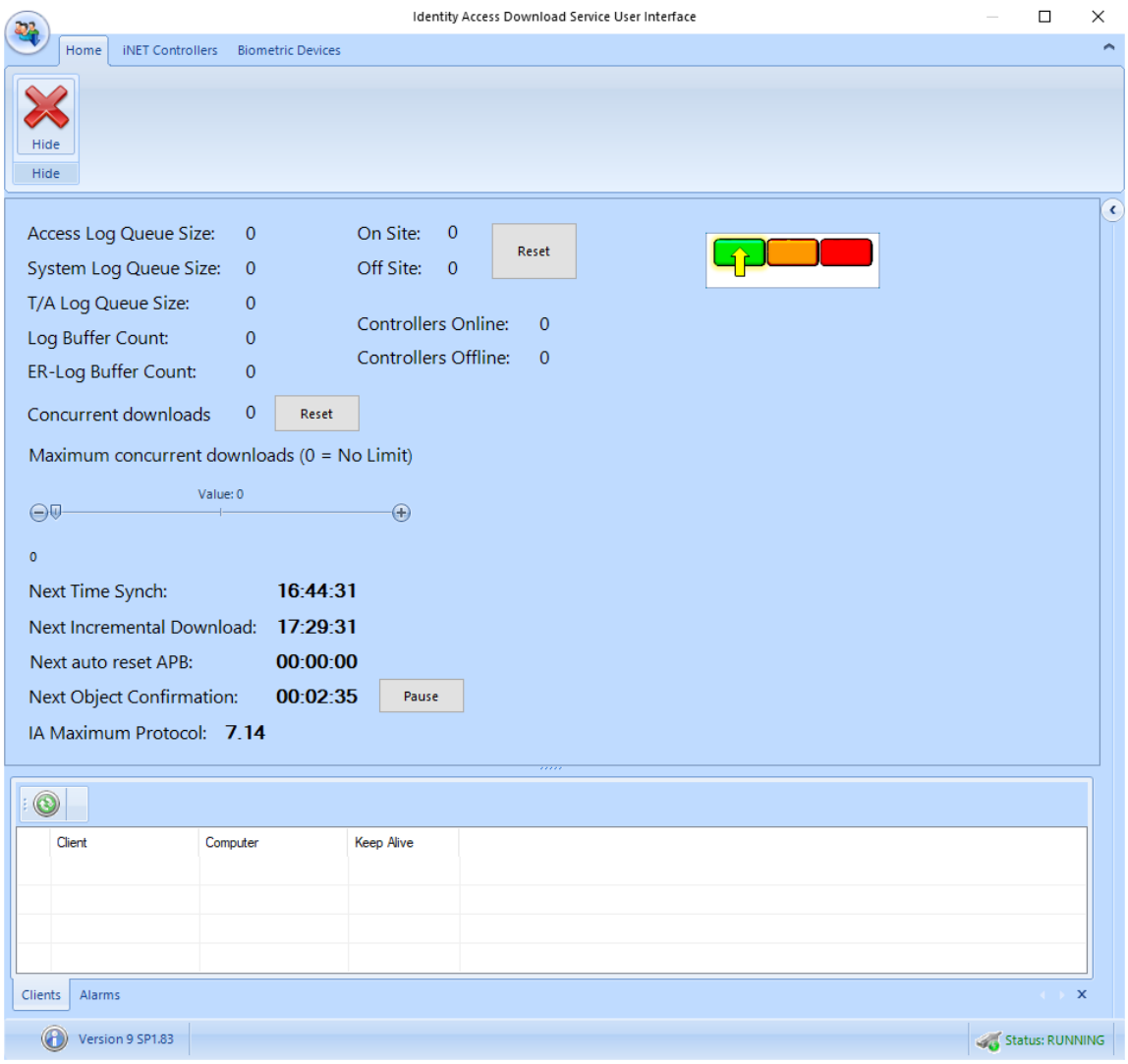


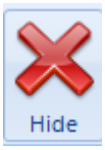
The **Download Service** handles all the communications between the Identity Access software and the network devices.

© 2026 Controlsoft Ltd

22.2.1 Home

Select the **Home** tab:





Clears the Alarms.

The upper half of the screen provides a summary of the various logs. These will increase in size if the Download Server is reading events from the controllers faster than it can write them to the Log Buffers. Maximum Concurrent Download allows a limit on the number of controllers that the Download Server can download to at any given time. This can be useful to limit the bandwidth used on the network during a Rebuild. Also shown is the time until the software next synchronises its clock with the controller clocks. This happens at 02:15 each day, but this setting can be changed in the Server Configuration utility.

In the centre of the upper half is an indication of the number of users **On Site** and **Off Site**. This is a live display, updated as users enter and leave the building. These counters can be reset to zero at any time by clicking the [Reset] button.

© 2026 Controlsoft Ltd

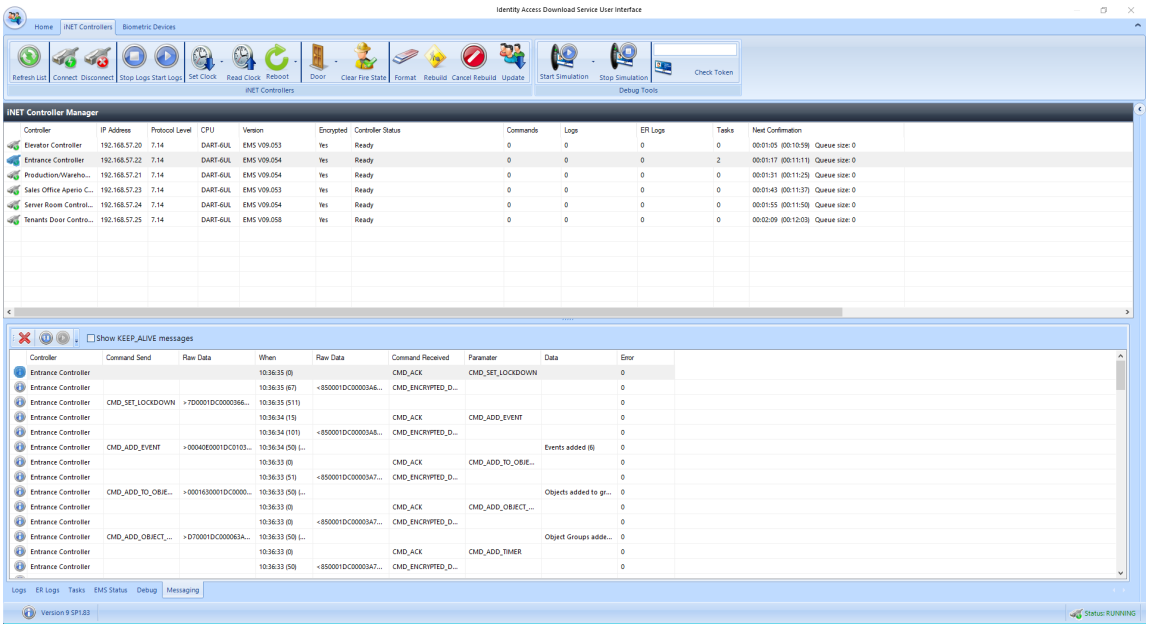
Also displayed is an indication of the number of **Controllers Online** and **Controllers Offline**.

The right hand side of the upper half shows the current Lockdown level.

The lower window has 2 tabs, **Clients**, (which shows the clients connected) and **Alarms** (which displays current system Alarms).

22.2.2 iNet Controllers

Select the **iNet Controllers** Tab**:**



The icons available are as follows:

 Refresh the list of iNet controllers



Connect or disconnect the selected controller/s in the list

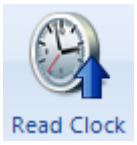


Stop and start logging events for the selected controller/s

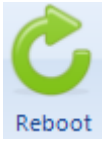


Set the clock in the selected iNet controller/s. The dropdown list allows the iNet clock to be set to **Current Time** or **Custom Time**

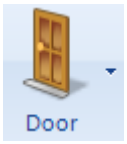
© 2026 Controlsoft Ltd



Read the clock from the selected controller/s. The time will be displayed in the Debug window.



Reboots the selected controller/s



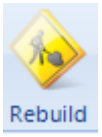
Allows a door on the selected controller to be **Granted Access** (opened for the programmed door open time), **Force Open** and **Force Closed**.



Manually clears the Fire state for the selected controller.



Clears the database in the selected controller/s



Downloads configuration data and user database to the selected controller/s



Cancels any current rebuild



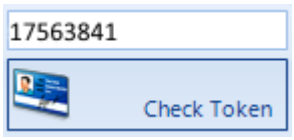
Downloads the most recent changes to the selected controller/s

If **Show Debug Tools** is enabled in the Server Configuration utility, the following options will also be visible:



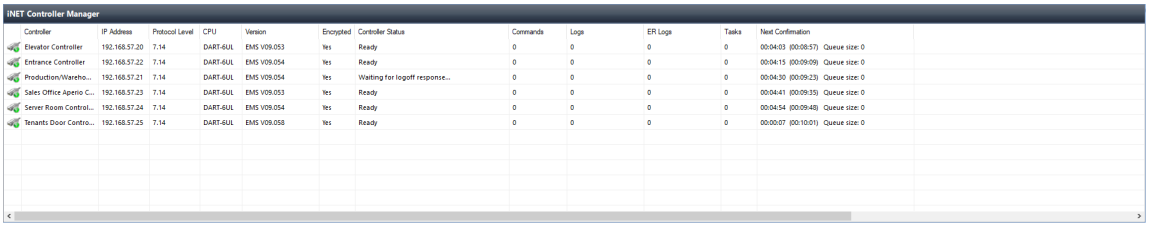
Starts and Stops "Simulation" on the selected controller/s. When starting "simulation", simply choose the frequency of event which will then be sent from each of the selected controller/s. For example, a simulation every 10 seconds from 20 controllers will generate 2 events per second.

© 2026 Controlsoft Ltd



Checks each of the selected controller/s to see if they contain the desired Token number. The results will be displayed in the Debug window.

The upper window is the iNet Controller Manager which displays the status of each of the controllers on the system:



Controller displays the name of the controller, as configured in Identity Access

IP Address displays the IP Address of the controller, as configured in Identity Access

Protocol Level is an identifier between the software and the controllers which defines commands and data transfer speeds available between the two.

CPU identifies the type of processor used on the iNet: **M501** for older (green) processor boards or **M502** for newer (blue) processor boards

Version identifies the firmware version in the controller. For IA v9 to work correctly, this must be v98.38 or higher.

Controller Status indicates whether the controller is "**Disconnected**" if the software cannot ping the controller, "Connected" if it can ping the controller but not yet communicating or "**Ready...**" when it is fully communicating.

Commands is the number of commands waiting to be sent to the controller

Logs is the number of events waiting to be read from the controller

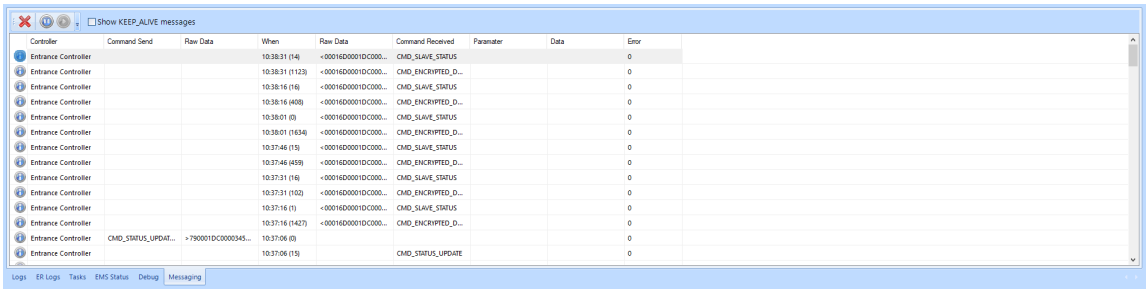
ER Logs is the number of entries from the Events and Actions log waiting to be read from that controller

Tasks is the number of tasks in the task queue for that controller.

Next Confirmation indicates when the system is due to confirm the validity of downloaded data.

© 2026 Controlsoft Ltd

The lower window will display a variety of parameters depending on the tab selected:



Logs: Displays access logs as they are received by Download Server

ER Logs: Displays the Events and Actions logs as they are received by Download Server

Tasks: Displays the Task list of commands issued to the controller awaiting completion

EMS Status: Displays the web page of the selected iNet controller (see Appendix D - iNet webpage)

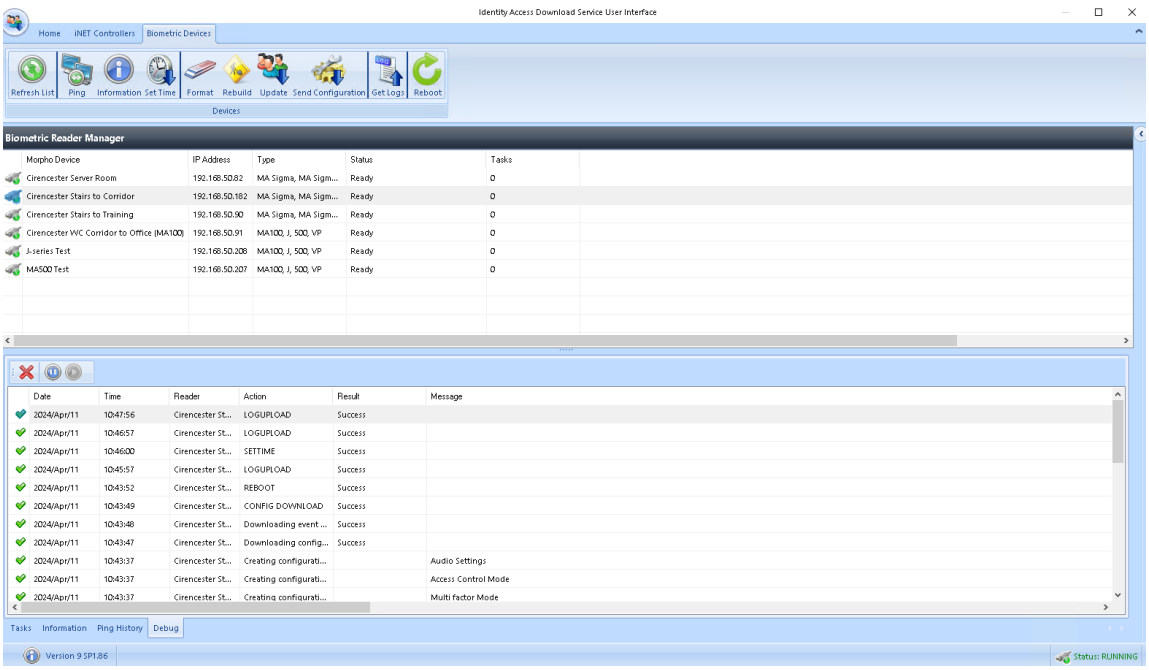
Debug: Displays commands and data being transmitted between the software and the controllers, primarily for Controlsoft use only.

Messaging: This tab displays all data sent between the software and the controller.

22.2.3 Biometric Devices

NOTE: The Biometric Devices tab is only displayed if an Identity Access Professional or Enterprise licence is installed.

Select the **Biometric Devices** Tab**:**



© 2026 Controlsoft Ltd

The icons available are as follows:

 Refreshes the screen to display the latest data



Pings the selected Morpho Reader/s to confirm availability



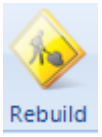
Reads configuration data from the selected Morpho Reader/s



Sets the time in the selected Morpho Reader/s to match the PC clock.



Clears the database in the selected Morpho Reader/s



Sends all configuration data and user database to the selected Morpho Reader/s



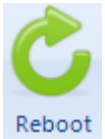
Sends most recent changes to the selected Morpho Reader/s



Sends configuration data (without the user database) to the selected Morpho Reader/s



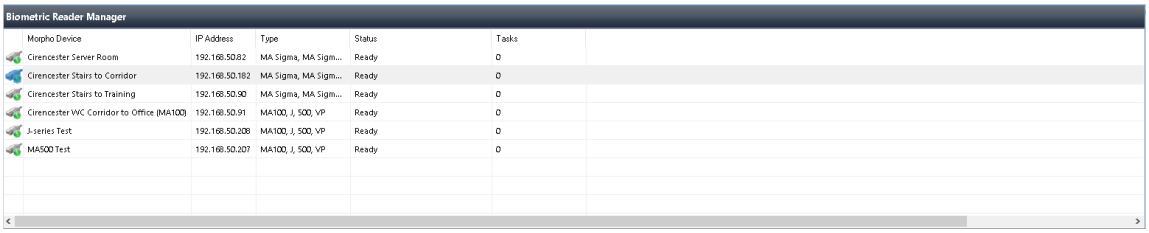
Reads event logs from the selected Morpho Reader/s



Reboots the selected Morpho Reader/s

© 2026 Controlsoft Ltd

The upper window is the Biometric Reader Manager, which displays information on each of the Biometric Readers:



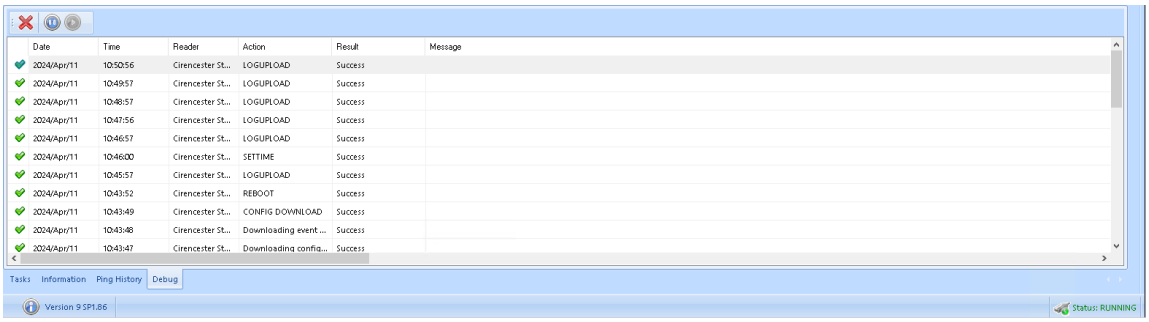
Morpho Device and **IP Address** shows the name and address of the reader as configured in Identity Access

Type shows the type of reader (e.g. MA Sigma)

Status shows the current status of the device, such as whether it is offline

Tasks shows the number of commands to be sent to the reader

The lower window will display a variety of parameters depending on the tab selected:



Tasks: Tasks waiting to be sent to the reader

Information: Displays detailed information of the device itself, such as the reader's serial number.

Ping History: The Download Server constantly pings each reader to ascertain its availability. This window will display the history of each ping to each reader.

Debug: Displays commands and data being transmitted between the software and the readers.

22.3 Service Manager

The Service Manager is a small utility which provides access to the 2 Identity Access services, the Log Service and Download Service. It also shows whether the Identity Access SQL Server instance is running.

To access the Service Manager, right click on the Identity Access Service Manager icon in the notification area and select **Show**

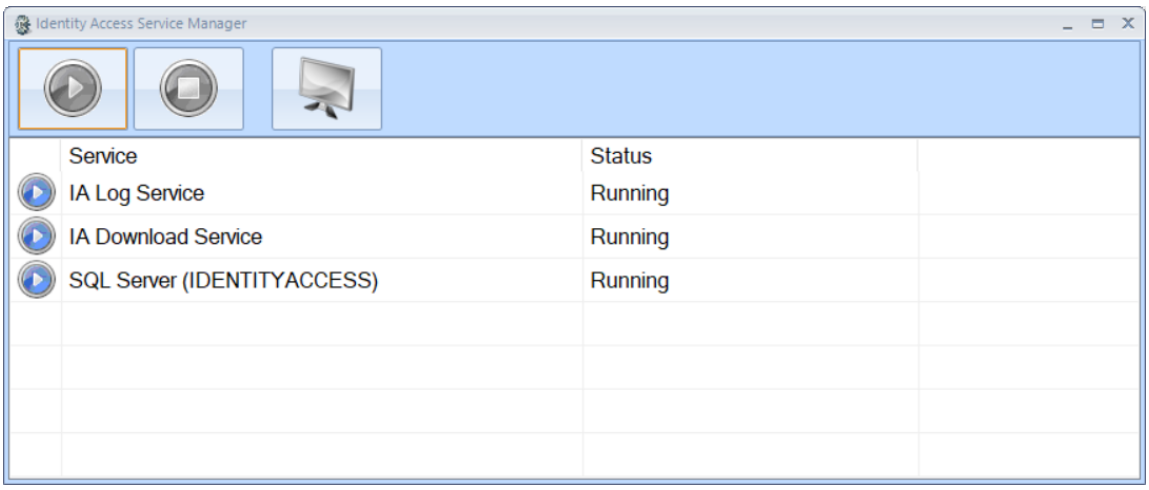
© 2026 Controlsoft Ltd



Login using administrator details.



The Service Manager will now display which services are running as shown below:

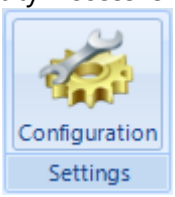


© 2026 Controlsoft Ltd

Identity Access Configuration

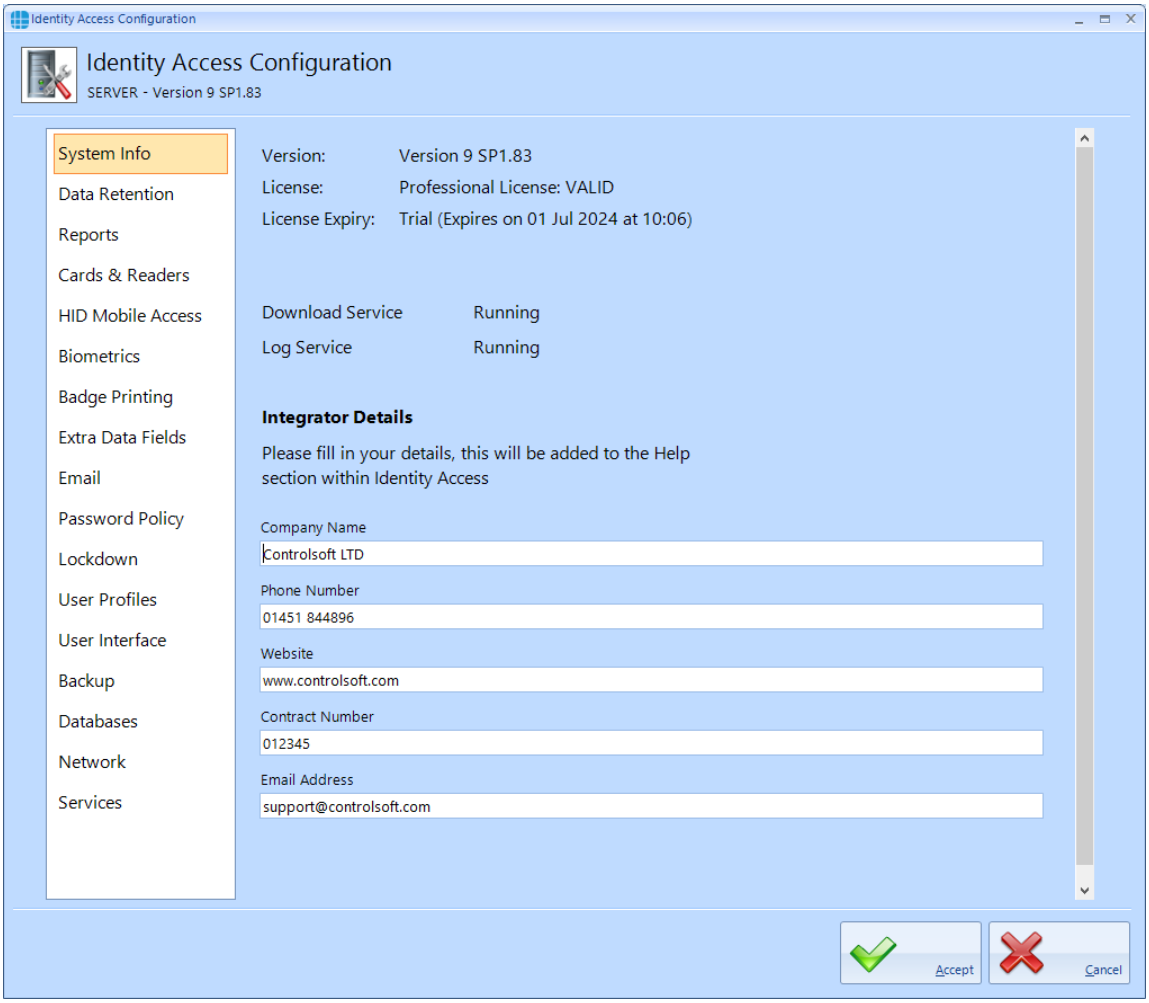
23 Identity Access Configuration

The **Identity Access Configuration** tool is used to configure certain features of the Identity Access server software.

If Identity Access is already running, simply click the Configuration icon in the **System** menu: 

23.1 IA Configuration > System Info

This screen displays basic system information as described below:



Version is the version of Identity Access installed

License is the type of license applied, either IA-Lite (i.e. no license applied), IA-PRO for a Professional license or IA-ENT for an Enterprise license.

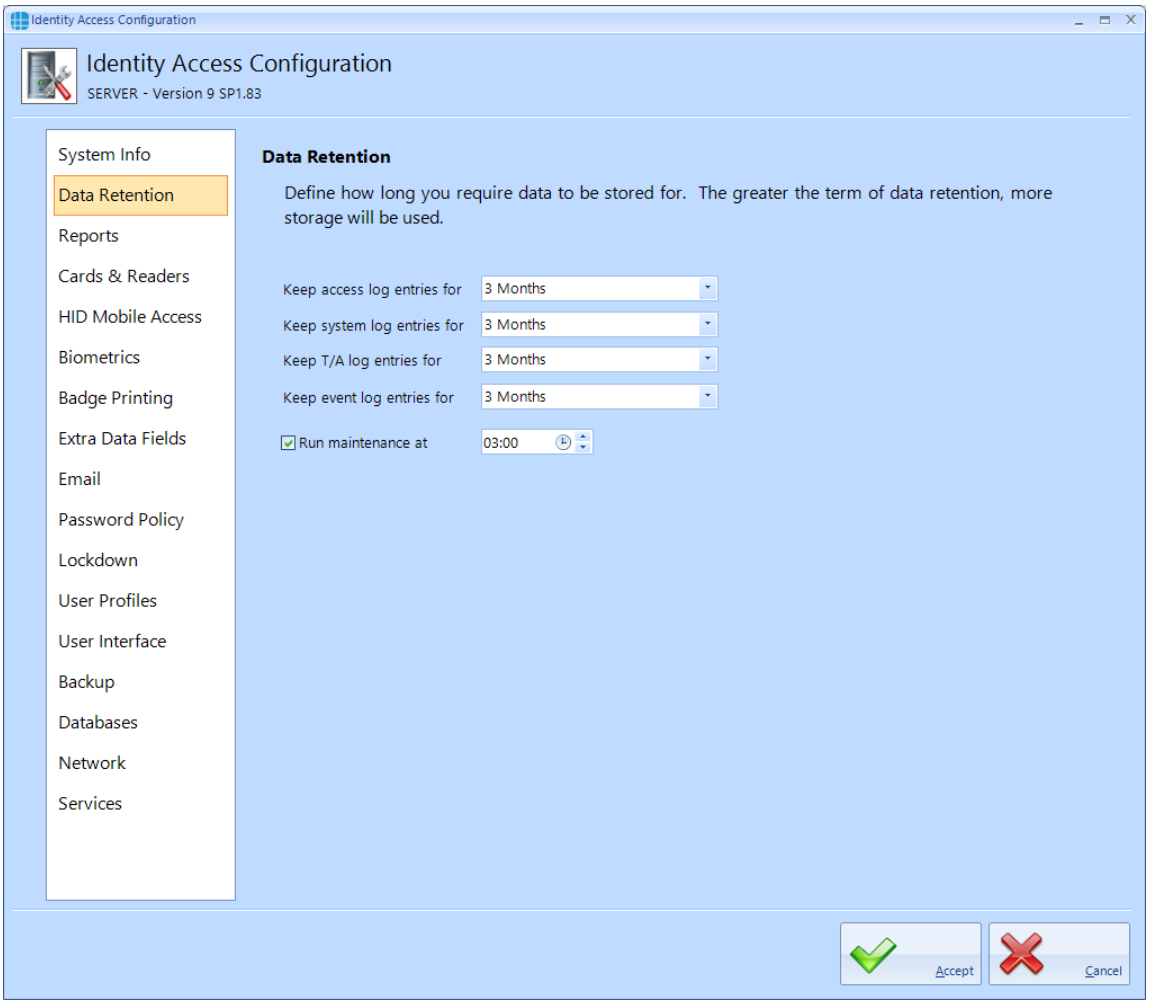
License Expiry is the date when the Identity Access software will expire.

© 2026 Controlsoft Ltd

The **Integrator Details** section is used to fill in the contact details for the System Integrator i.e. the installation / maintenance company. These are viewable from within the **Home** tab and select **Support** in the ribbon bar.

23.2 IA Configuration > Data Retention

Using this option, we can define how long data is kept in the SQL database before being purged.



Each of the databases can be independently saved for 1 day, 1 week, 2 weeks, 1 month, 2 months, 3 months, 6 months, 1 year, 2 years, 3 years, 4 years, 5 years or indefinite

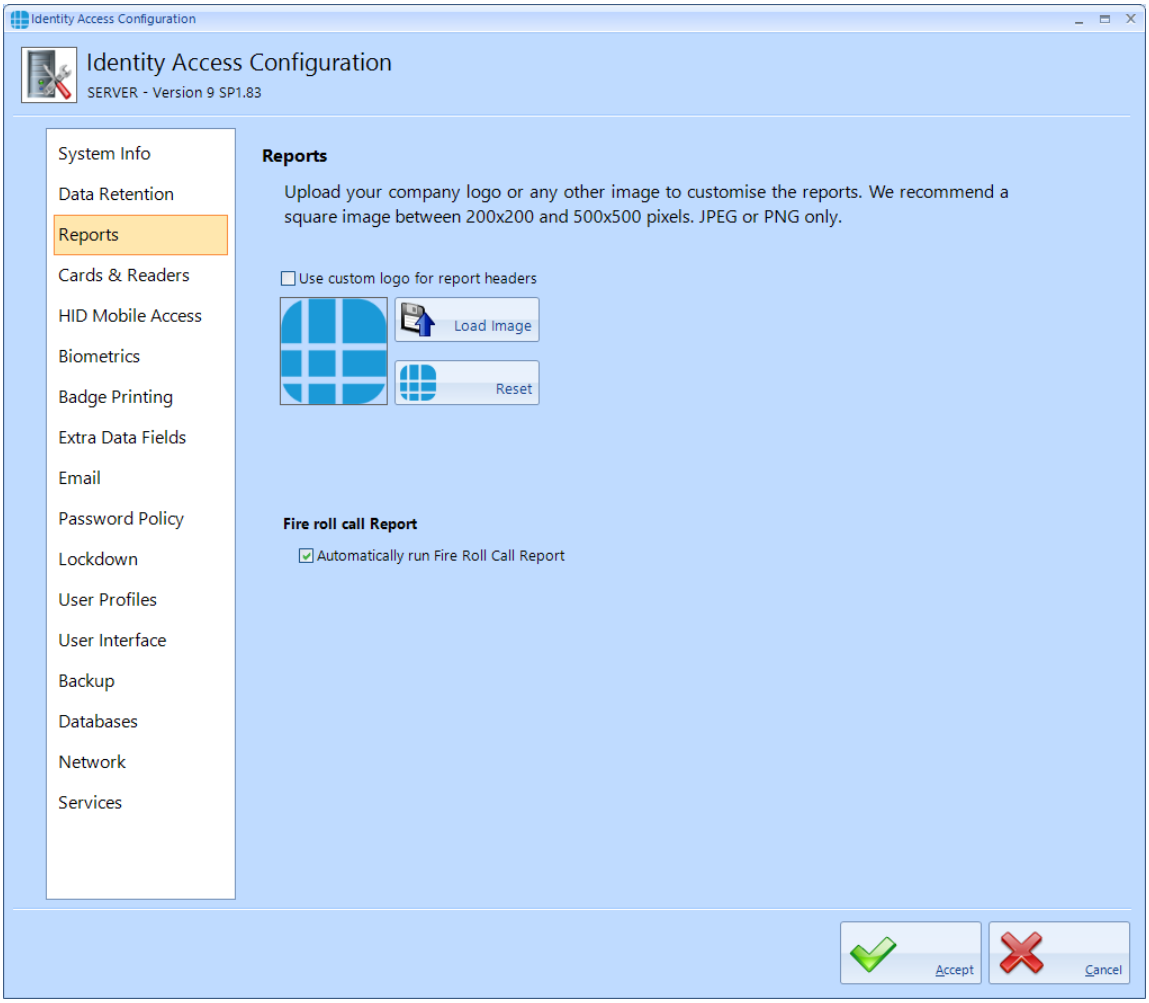
Run Maintenance defines the time of day when the database purge will occur.

NOTE: The longer data is retained, the larger the databases will become, which may affect performance.

23.3 IA Configuration > Reports

Identity Access reports can be configured with a custom logo at the top of each page.

© 2026 Controlsoft Ltd



Use custom logo for report headers - tick this option to use a custom logo, then click on [Load Image] and browse for the required logo.

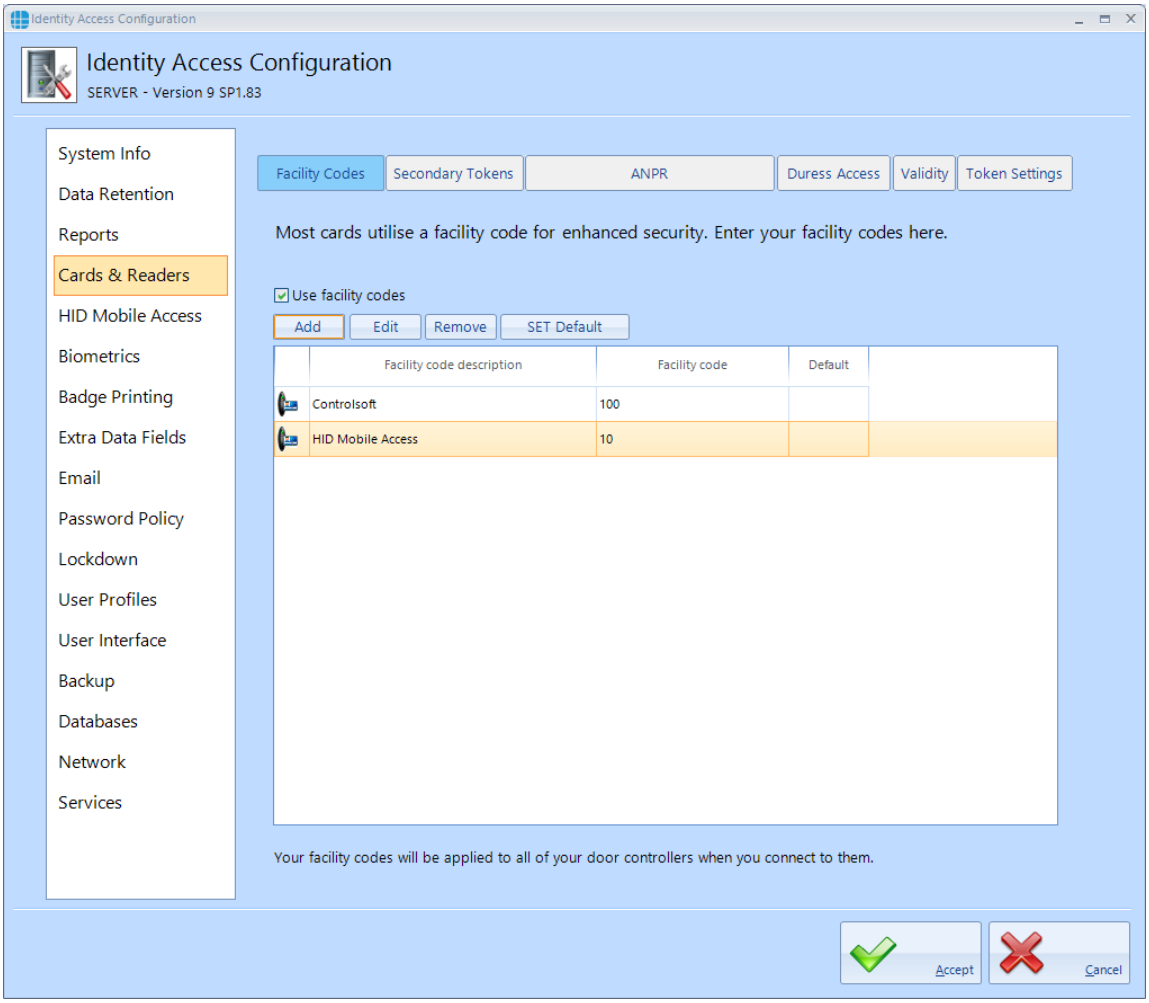
Automatically run Fire Roll Call Report - untick this option if you do not want reports automatically printed when is fire alarm condition is detected.

23.4 IA Configuration > Cards & Readers

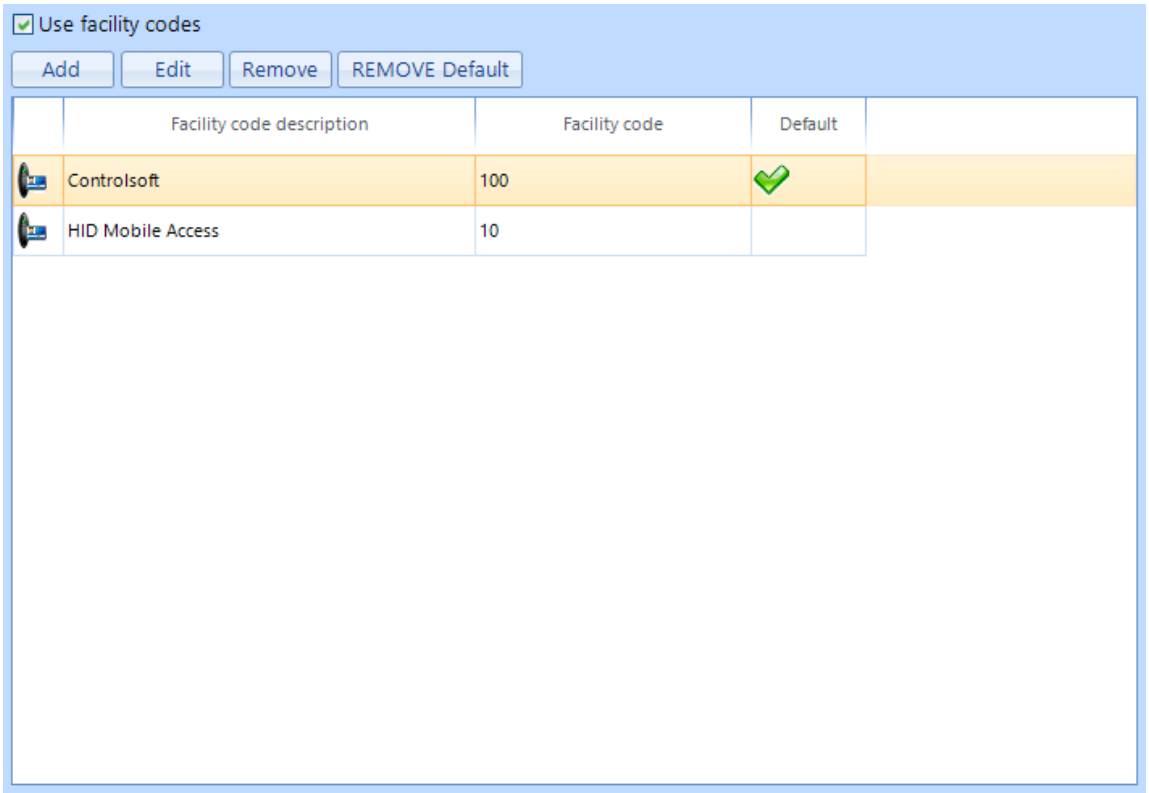
Several options can be configured within the Cards & Readers tab as described below:

Facility Codes

© 2026 Controlsoft Ltd



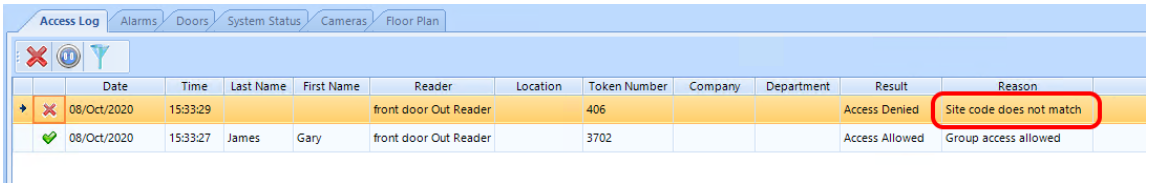
If the access control system uses Facility codes, tick the option **Use facility codes** , then click the [Add] button to enter the relevant Facility Codes in use. For example:



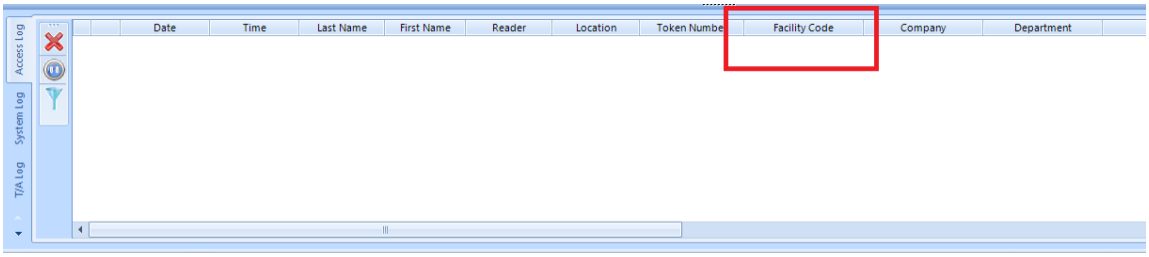
© 2026 Controlsoft Ltd

When creating Users, the relevant Facility Code is then allocated to the user (see User General 141).

NOTE: if a card with an incorrect Facility Code is presented to a reader, access will be denied, and the Dashboard will show the Reason as Site code does not match as in the example below:



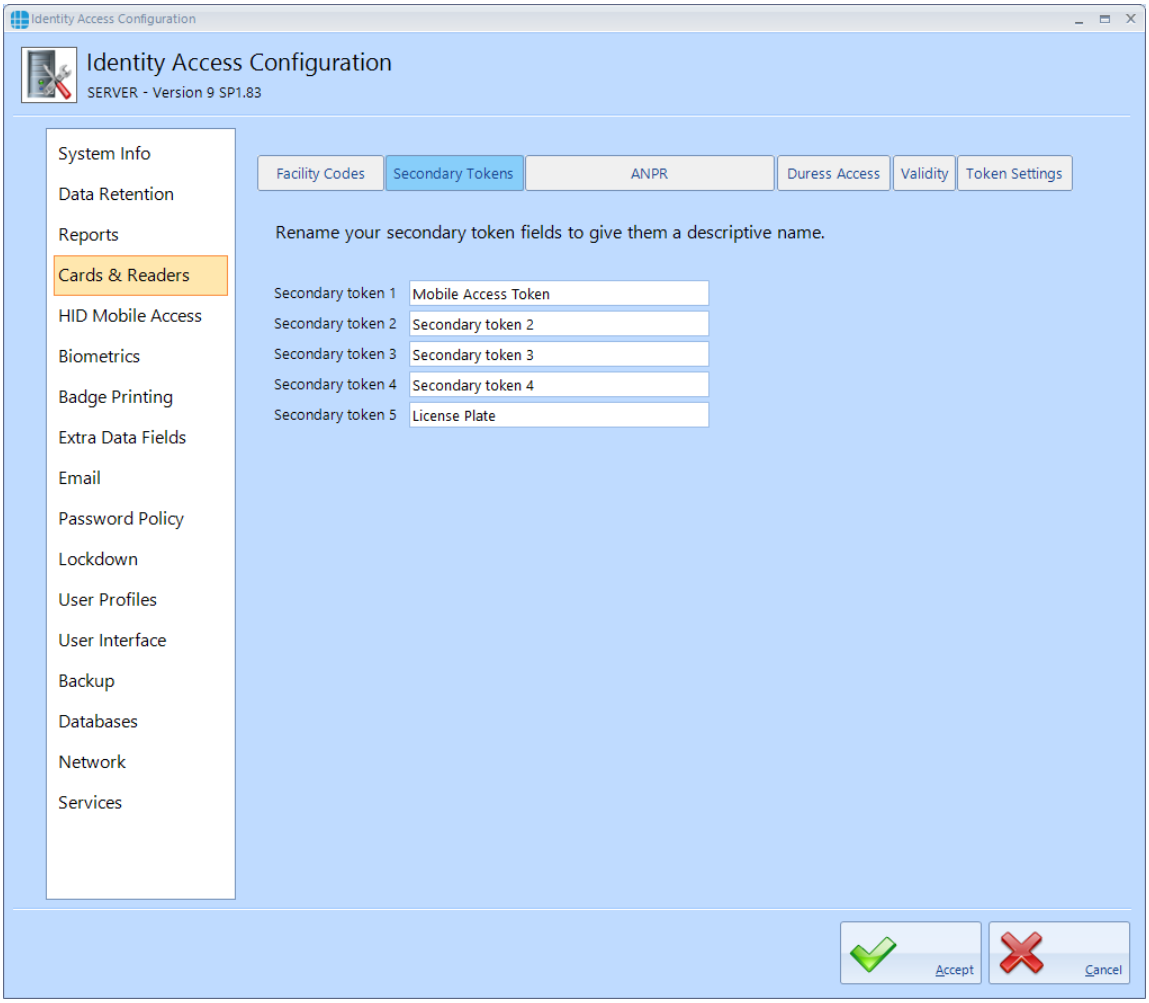
To determine the Facility Code on the card, check the activity in the Access Log viewer:



Secondary Tokens

The titles of the secondary token fields in the IA User Interface can be defined.

© 2026 Controlsoft Ltd

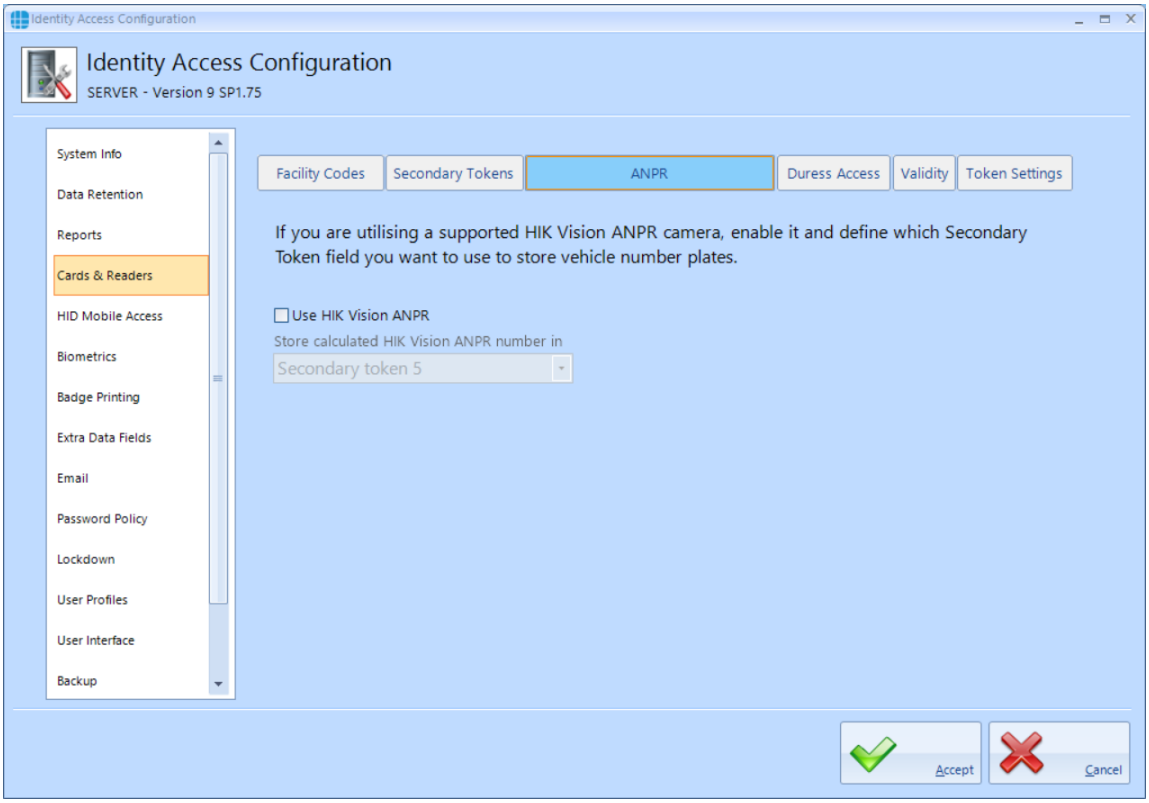


Enter text strings against each field as appropriate to the system.

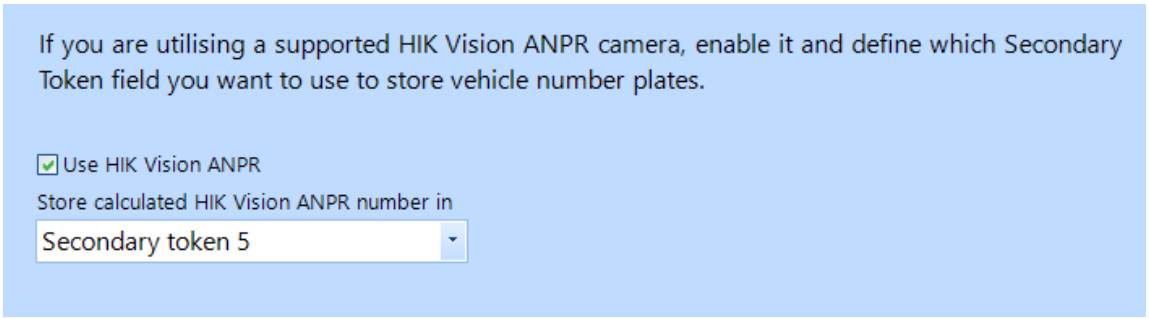
Automatic Number Plate Recognition / Automatic License Plate Recognition (ANPR / ALPR)

The Identity Access software is compatible with license plate cameras using Wiegand output (SHA-1), and is capable of calculating the relevant token number from the Number Plate entered.

© 2026 Controlsoft Ltd



Select the **Use HIK Vision ANPR** option and define which Secondary Token field will be used to enter number plates, for example:

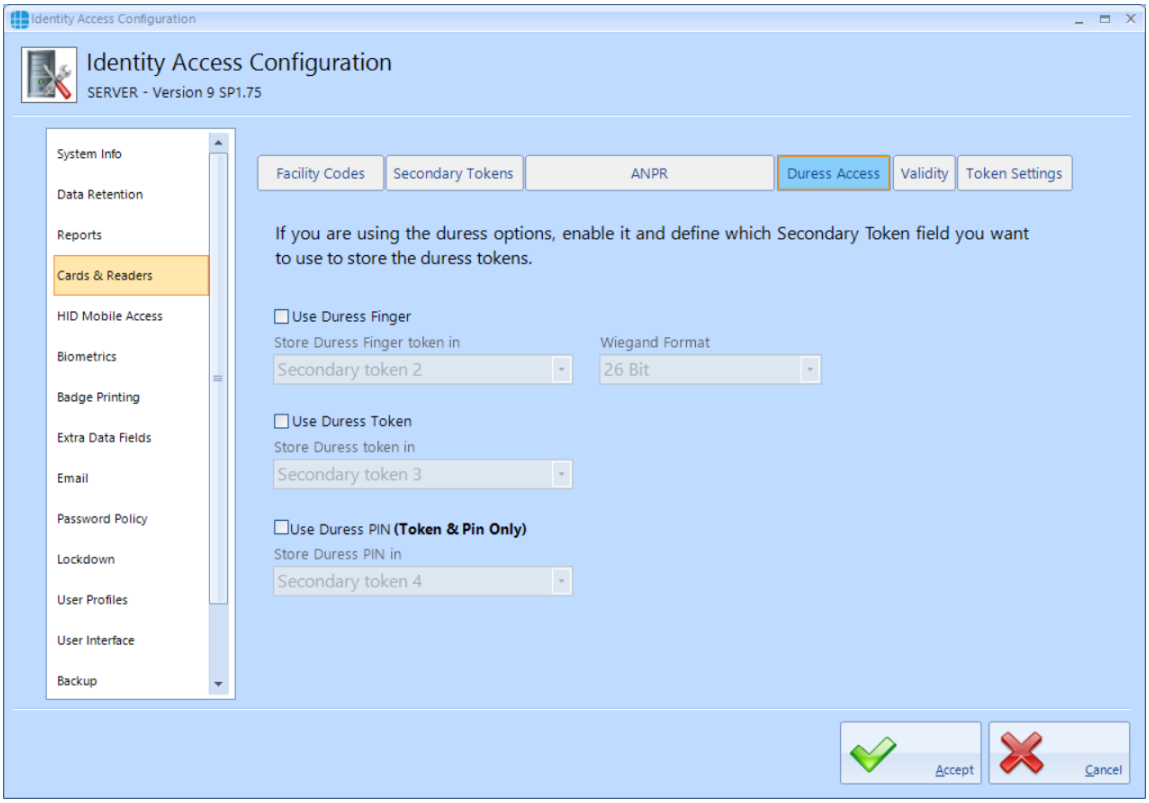


NOTE: The Wiegand output of the HIK Vision ANPR camera must be connected to an iNet controller with "Site Codes" disabled.

Duress Access

Identity Access software now allows duress options, which will generate an alarm condition in the dashboard.

© 2026 Controlsoft Ltd



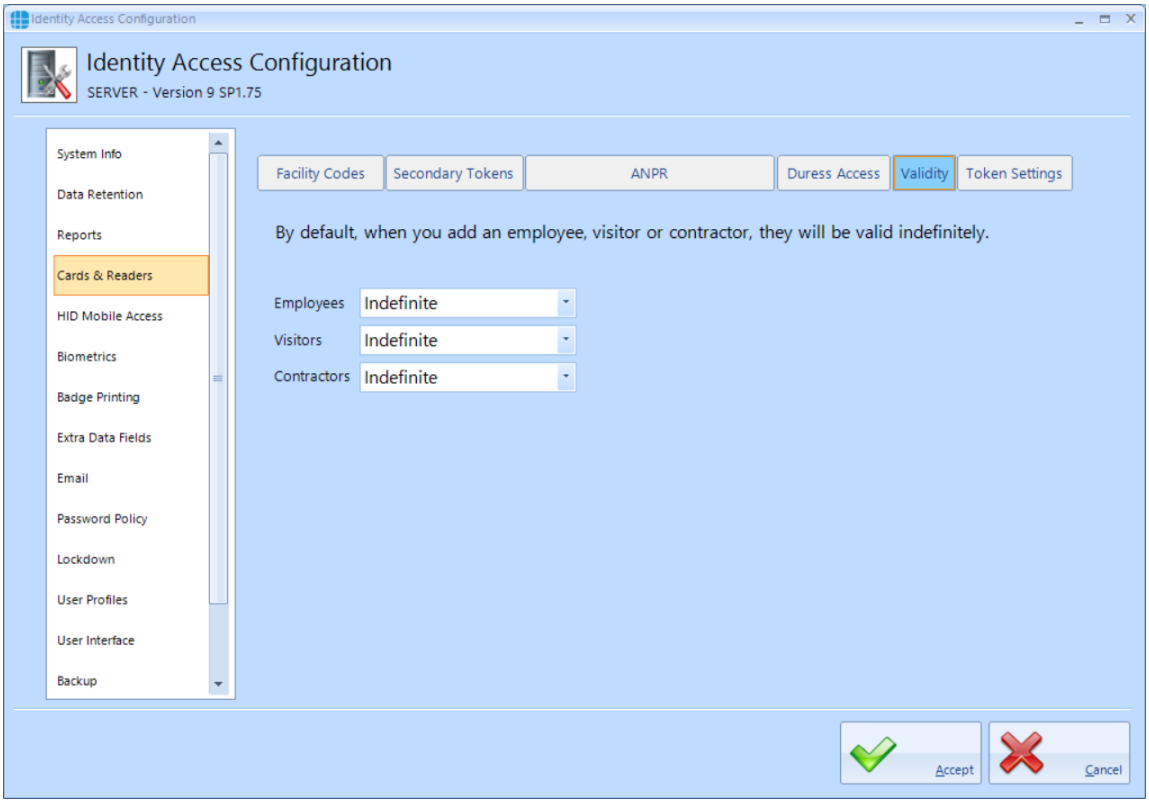
If using duress finger with Morpho fingerprint readers, ensure that the **Use Duress Finger** option is ticked, and select which secondary token field will be used to hold the relevant token number.

If a duress token is to be used, ensure that the **Use Duress Token** option is ticked, and select which secondary token field will be used to hold the relevant token number.

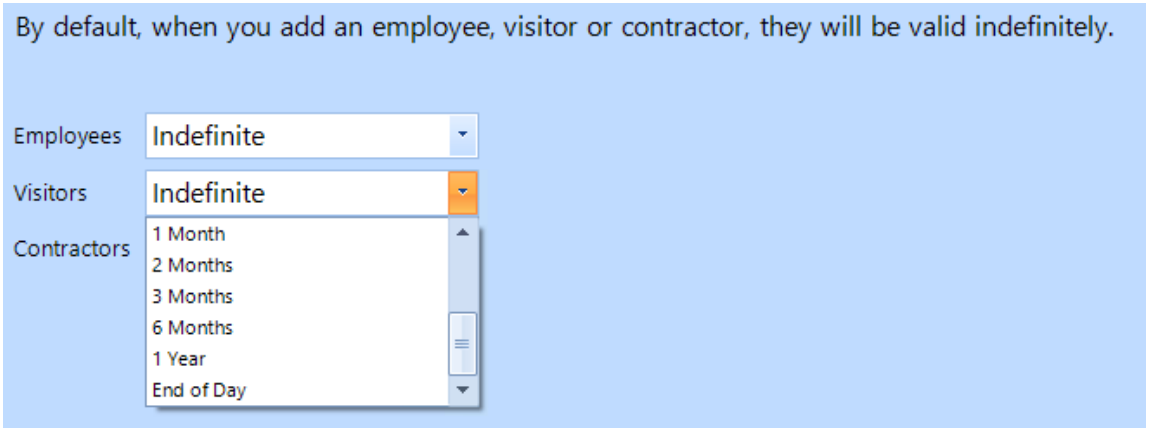
If one or more card readers have the **Reader has a PinPad attached** option selected , ensure that the **Use Duress PIN** option is ticked, and select which secondary token field will be used to hold the relevant PIN.

Validity

© 2026 Controlsoft Ltd

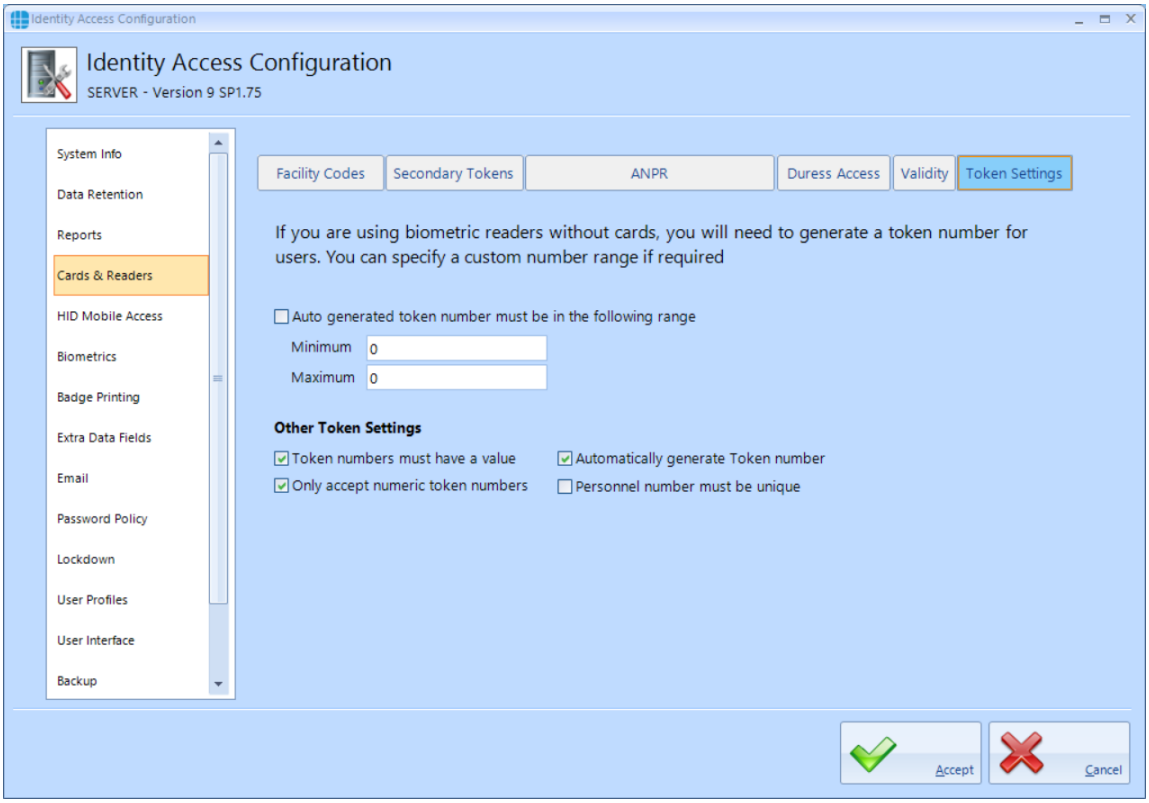


Employees, Visitors and Contractors can be given different default values for how long then they can be used until they are automatically invalidated. This could be useful, for example, for Employees to have a default validity period of Indefinite, whereas Visitors' tokens expire at the End of Day:



Token Settings

© 2026 Controlsoft Ltd



Auto generated token numbers must be in the following range - If using biometric readers with no token, IA can automatically generate the next available token number with the click of a button. These will normally start with 1 and increase sequentially. This option can be used to ensure that the automatically generated number starts at a given number, as shown above.

Token numbers must have a value - this option defines whether users can be created without a token number, which will then need to be added at a later date

Only accept numeric token numbers - this should only be deselected under certain conditions, for example if the system uses hexadecimal token numbers.

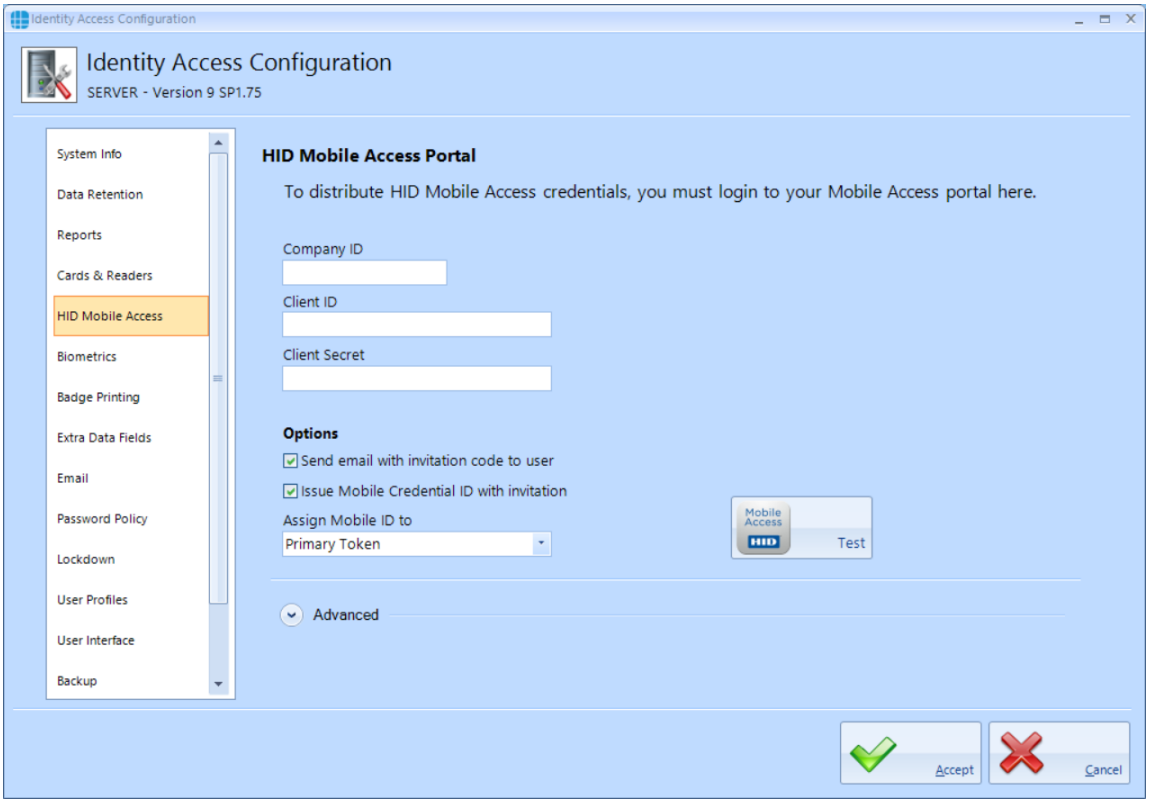
Automatically generate token number - this option enables the button in the IA User Interface to automatically generate token numbers.

If **Personnel number must be unique** is ticked, an Employee / Visitor / Contractor Personnel number cannot be duplicated

© 2026 Controlsoft Ltd

23.5 IA Configuration > HID Mobile Access

The **HID Mobile Access** screen needs to be configured if HID Mobile Access credentials are to be issued directly from the Identity Access software. The strings to be entered into the **Company ID**, **Client ID** and **Client Secret** fields will differ for each customer For further information, see Application Note: HID Mobile Access with Identity Access 9



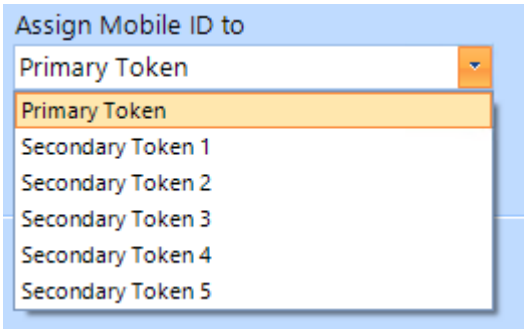
The above data strings will be provided by your vendor.

Send email with invitation code to user - when ticked, the system will automatically generate an email to the user with the invitation code to download and activate the Mobile Access token.

Issue Mobile Credential ID with invitation - When ticked, IA will issue the credential with the invitation code when simplifies the process. Controlsoft recommend that this is selected unless the customer has more than one credential type (e.g. H10301 and Controlsoft 47-bit). in this scenario, leave this option unticked and select the required credential type once the invitation code has been accepted.

The **Assign Mobile ID to** option allows a mobile credential to be allocated to a specific token field such as the Primary Token or Secondary Token 1, for example:

© 2026 Controlsoft Ltd

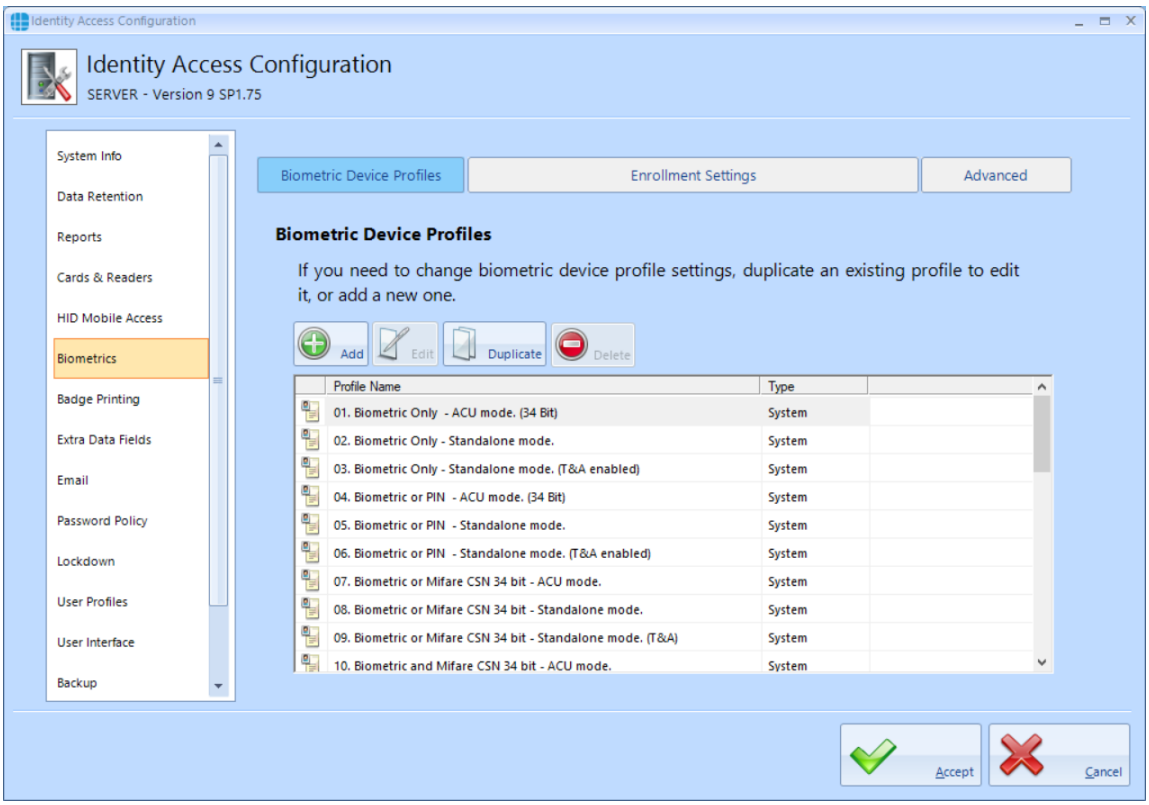


The **Advanced** options allows access to the URL strings for contacting the HID Mobile Portal. The strings must not be changed unless instructed to do so by Controlsoft Technical Support.

Once all the data is entered, click the **[Test]** button to test the connection to the credential server. If the test is successful, click **[Accept]**.

23.6 IA Configuration > Biometrics

The **Biometrics** screen allows configuration of Morpho fingerprint readers:



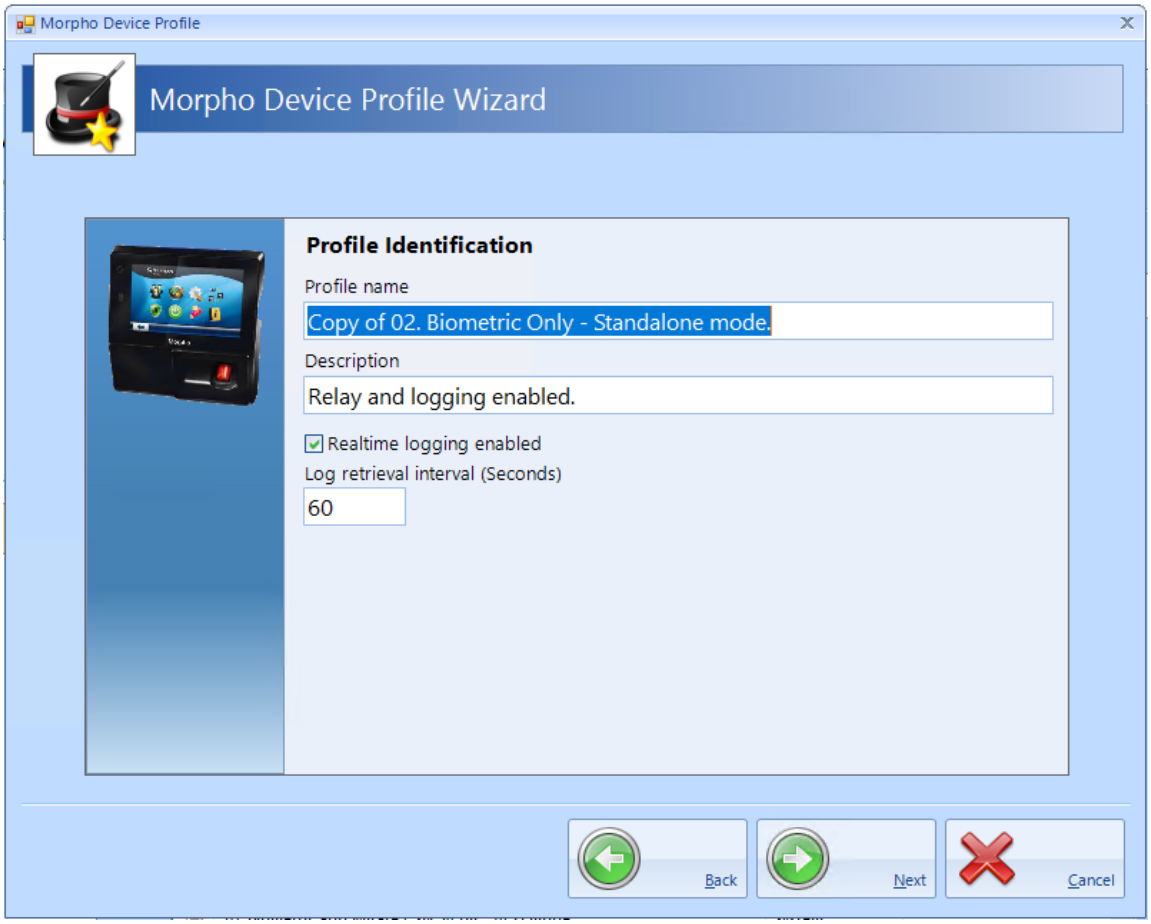
In Identity Access version 9, profiles are pre-configured for a variety of reader operating modes, significantly reducing the time required to set up Morpho readers.

NOTE: These profiles cannot be edited, but can be copied using the [Duplicate] button and the copy can then be edited.

© 2026 Controlsoft Ltd

Biometric Device Profiles

To create a new profile, click on the **[Add]** button. Alternatively, if you simply wish to edit an existing profile, select the required profile and click the **[Duplicate]** button.



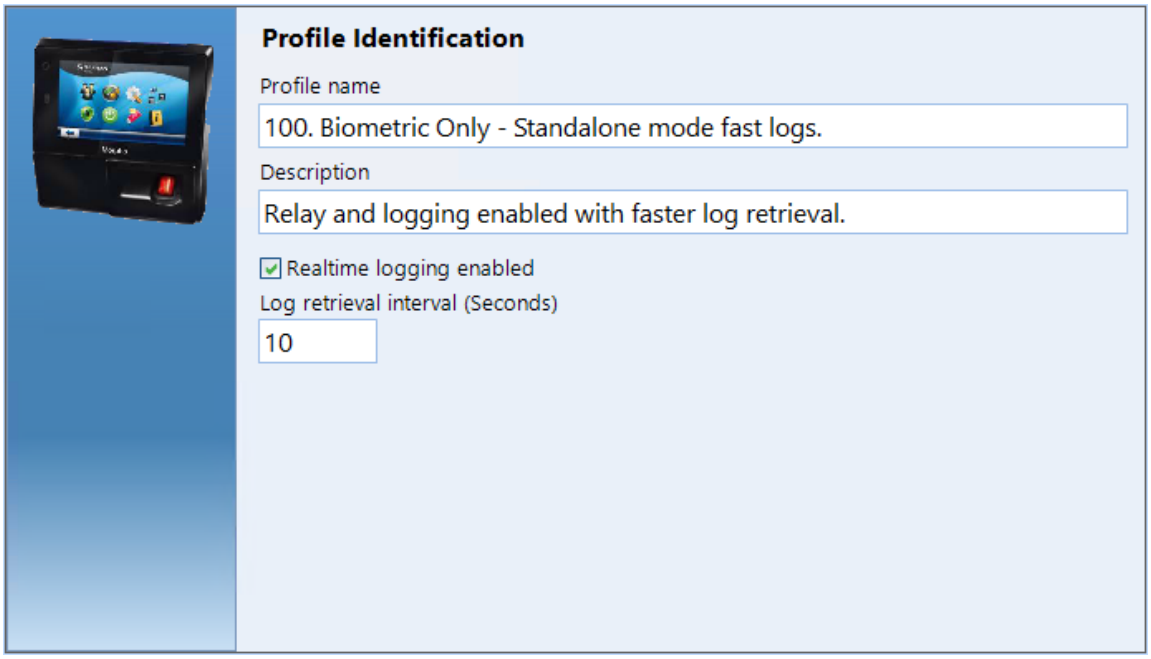
Profile name - Rename the profile as appropriate

Description - amend the description to easily identify the purpose of the profile

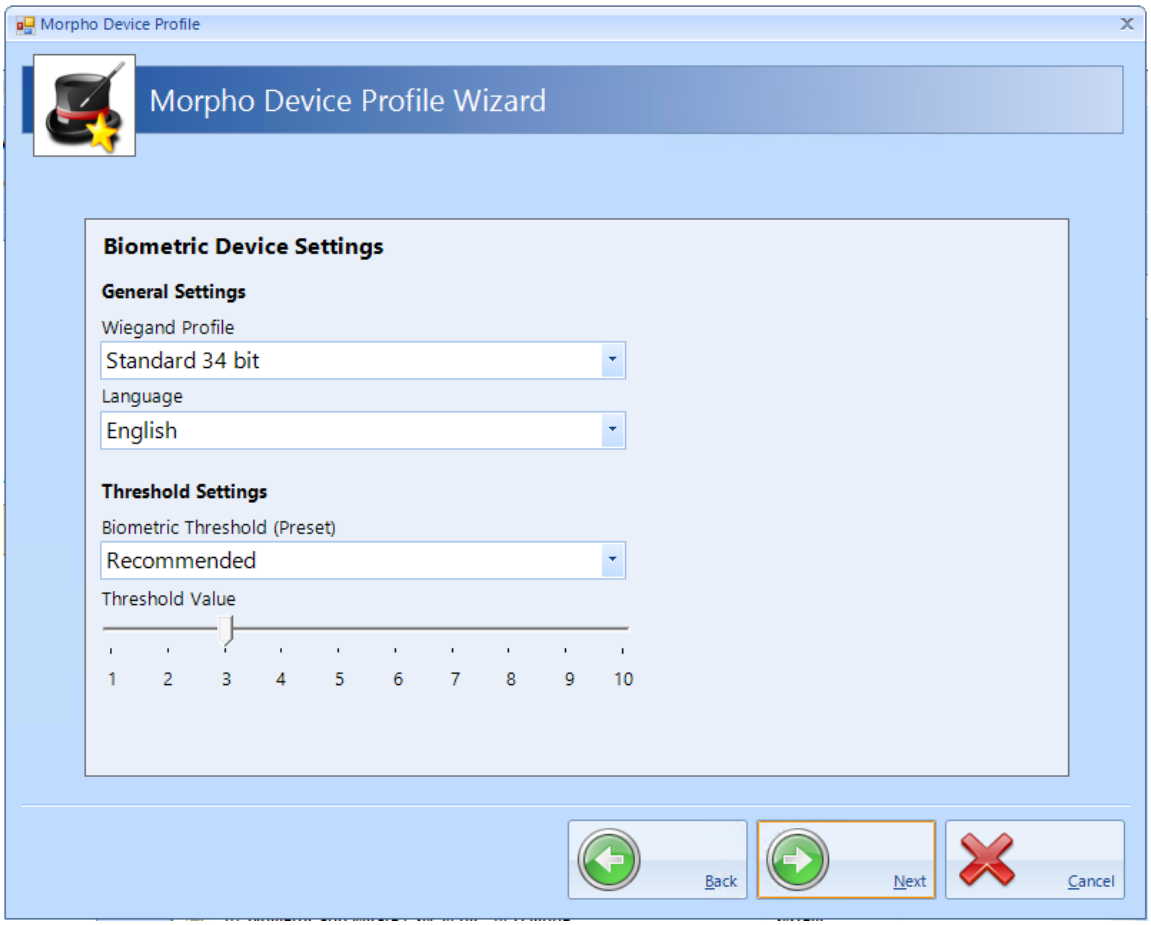
Realtime logging enabled - if this option is ticked, reader logs will be uploaded to IA

Log retrieval interval - define how frequently logs are uploaded

© 2026 Controlsoft Ltd



Click **[Next]**



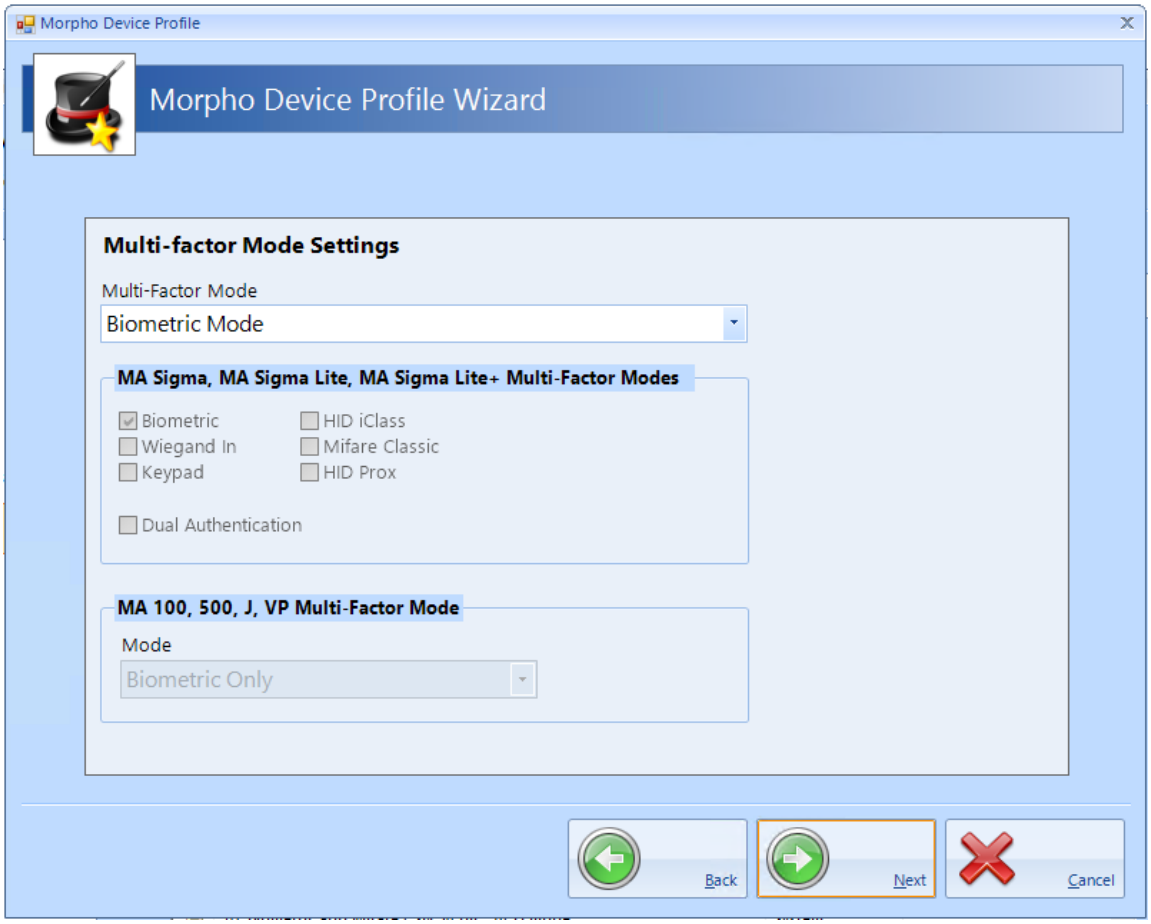
The default **Wiegand Profile** is Standard 26 bit. For any other profiles (example Controlsoft 47 bit) please contact Controlsoft Technical Support

Select the **Language** to be used (example English, Spanish, French).

© 2026 Controlsoft Ltd

The default **Threshold Settings** is Recommended. We advise that this is not changed unless advised by Controlsoft Technical Support

Click **[Next]** to continue



Multi-factor Mode should be set to Biometric Mode for fingerprint only, or changed to Custom for fingerprint and card

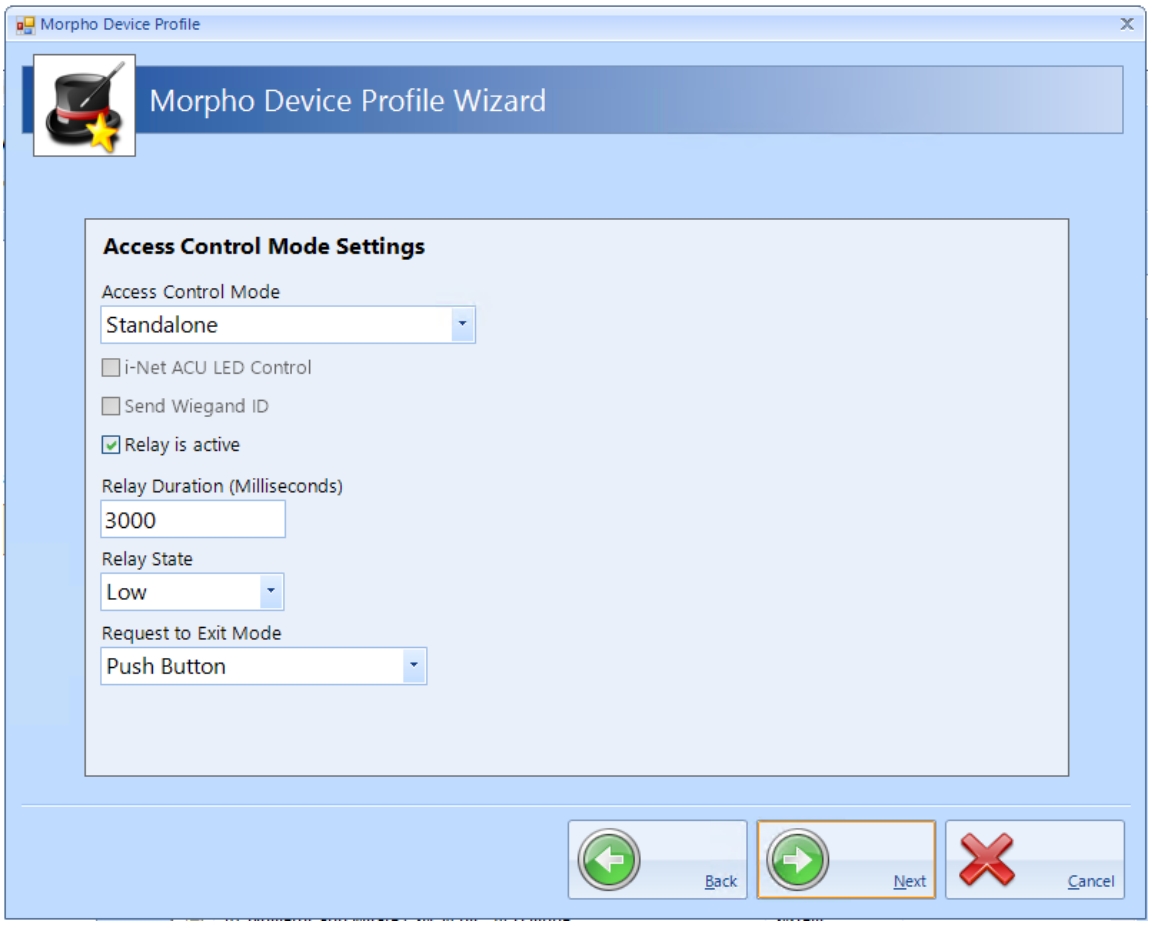
When Multi-factor Mode is set to Custom, Smart Card Mode can be selected as Smart card or Device

If the fingerprint reader is an MA100, MA500, J-Series or VP reader, the MA100,500,J,VP Multi-Factor Mode can be selected between Biometric Only (fingerprint only), Weigand in (a card reader connected to the fingerprint reader), Keypad (PIN), HID iClass, MIFARE or DESfire.

If the fingerprint reader is an MA Sigma, MA Sigma Lite or MA Sigma Lite+, the Multi-Factor Modes can be selected as Biometric, Proximity Card, Wiegand in, Keypad, HID iClass, MIFARE Classic / DESfire / DESfire EV1

Click **[Next]** to continue

© 2026 Controlsoft Ltd



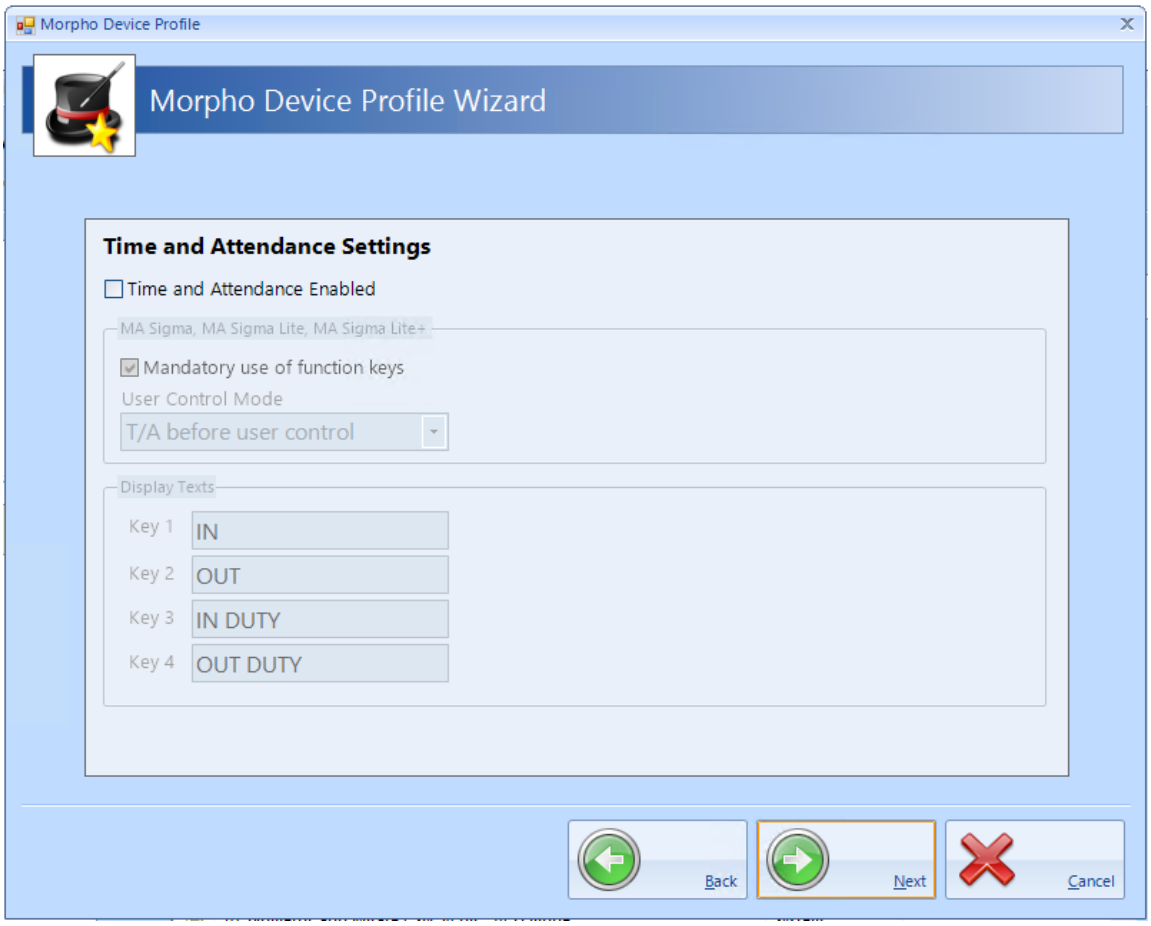
The **Access Control Mode** should be set to **None** if MorphoManager is used, **iNet ACU** if connected to an iNet or **Standalone** if no iNet controller is used.

If Standalone is selected, **Relay Duration** defines how long the door control relay will activate (3000 for 3 seconds). Select **Request to Exit Mode** as Push Button for REX operation.

NOTE: The Relay Duration is in milliseconds, for 3 seconds, enter 3000

Click **[Next]** to continue

© 2026 Controlsoft Ltd



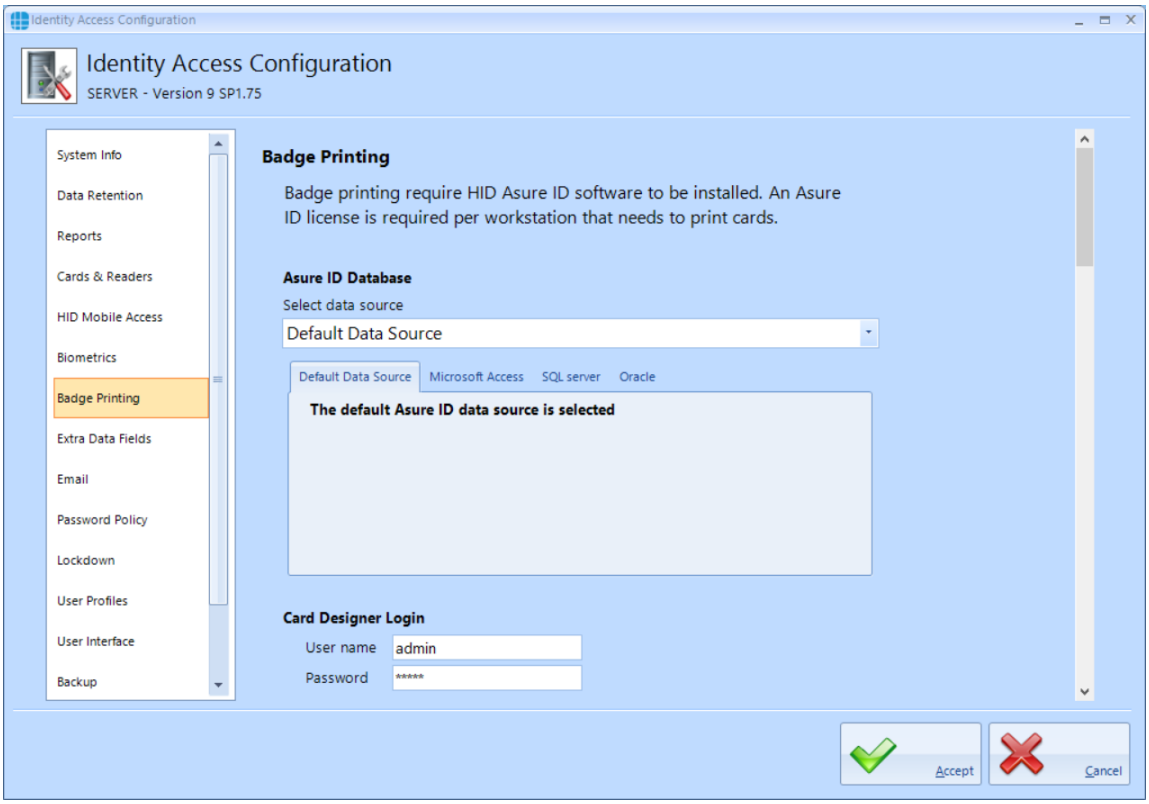
Time and Attendance should only be enabled when used with MorphoManager. When using Identity Access, the iNet will manage Time & Attendance.

Click **[Next]** followed by **[Finish]**

© 2026 Controlsoft Ltd

23.7 IA Configuration > Badge Printing

If you installed HID Asure ID software, the default configuration is suitable for most applications.



For use with Identity Access, leave the data source as **Default Data Source**

The **Card Designer Login** of **admin** and **admin** is the default credentials for Asure ID. If you change these credentials in Asure ID, you will need to change these fields as well.

The **Card Designer Field Mapping** fields are preconfigured for use with Identity Access and should only be changed if requested by Controlsoft Technical Support.

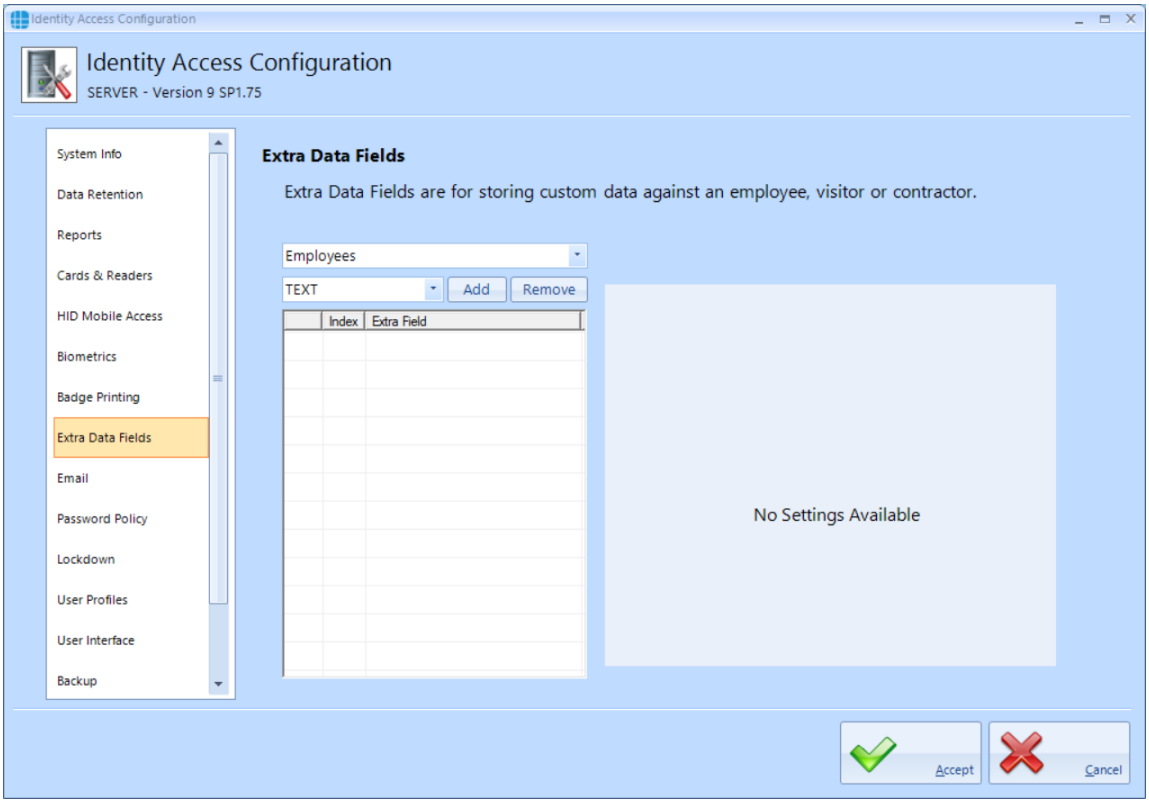
Asure ID requires a separate licence (part number IA-AID). Enter the licence key supplied by your vendor under **Register copy of Asure ID** together with your details to register the software.

23.8 IA Configuration > Extra Data Fields

The **Extra Fields** tab is used to configure Extra Data Fields within the Identity Access software.

© 2026 Controlsoft Ltd

Extra Fields are extremely flexible and very simple to generate. For example, to create an Extra Field to indicate whether an Employee has a valid driver's licence, first select Employees, then select **CHECK** for a check box from the dropdown list.

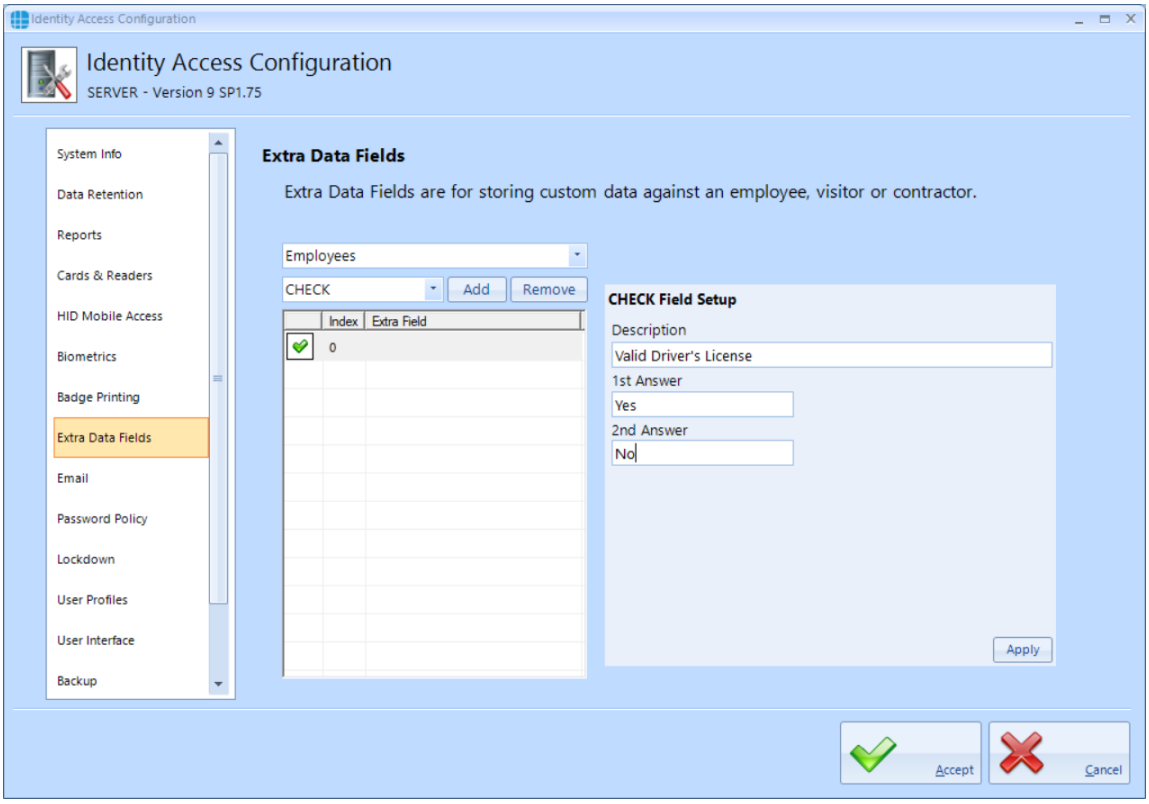


Click **[Add]**, then fill in the details under **CHECK Field Setup**, in this instance,

- **Description** = "Valid Driver's Licence"
- **1st Answer** = "Yes"
- **2nd Answer** = "No"

© 2026 Controlsoft Ltd

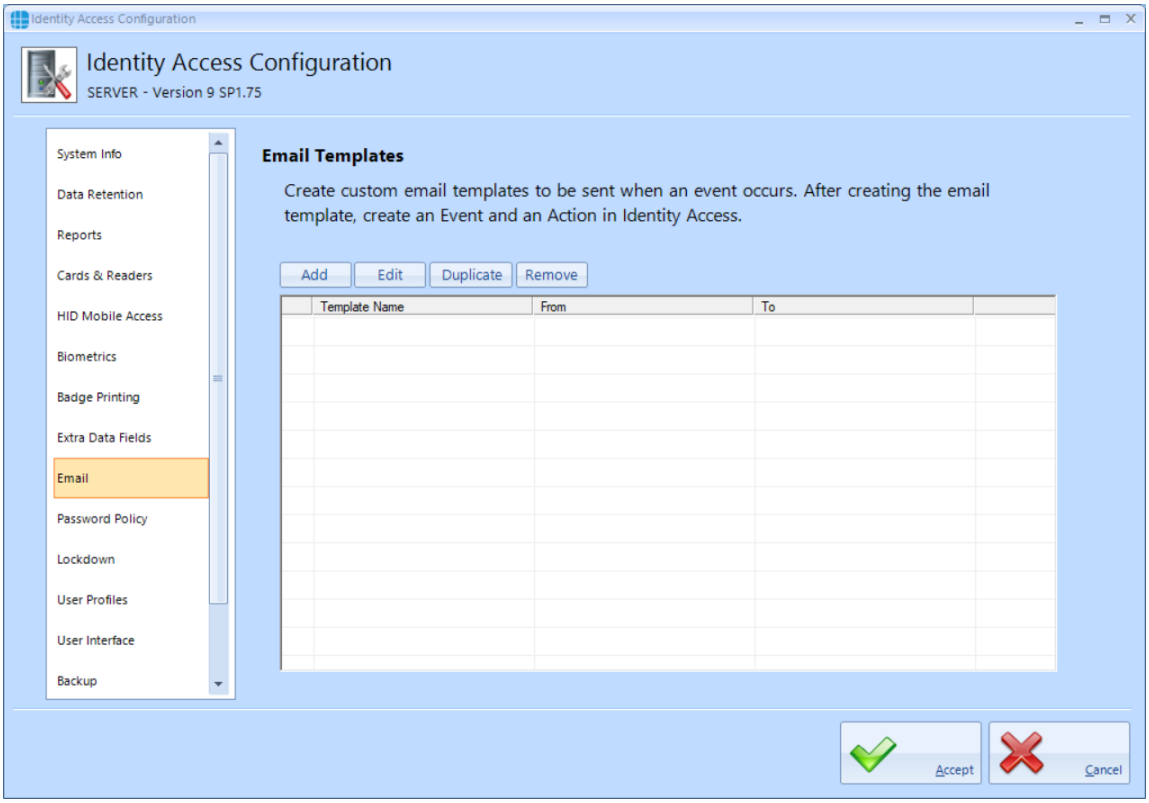
Click **[Apply]**.



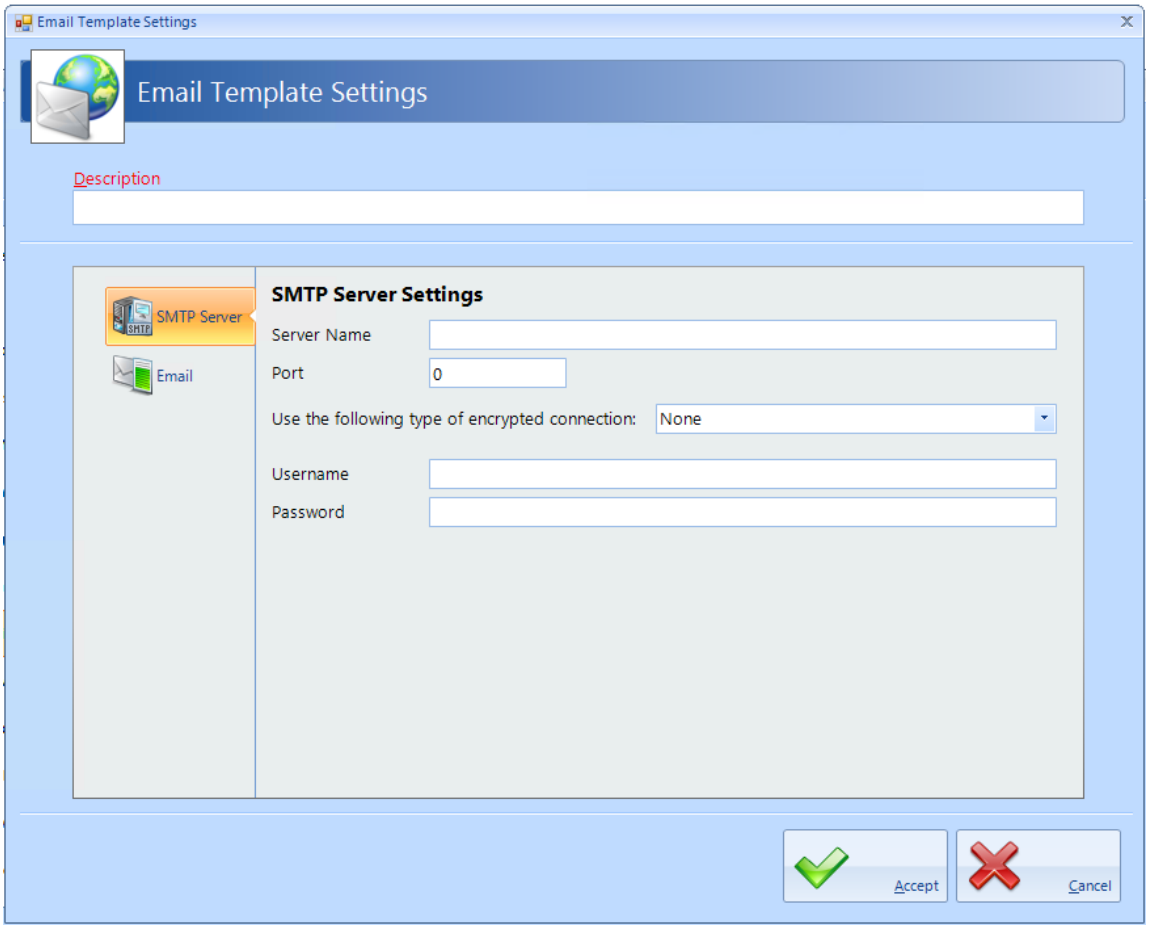
23.9 IA Configuration > Email

Email Templates can be created to allow emails to be sent whe generating Mobile Access Credentials, or as an Action following a defined Event.

© 2026 Controlsoft Ltd



To create an Email template, click the **[Add]** button and enter the following information:

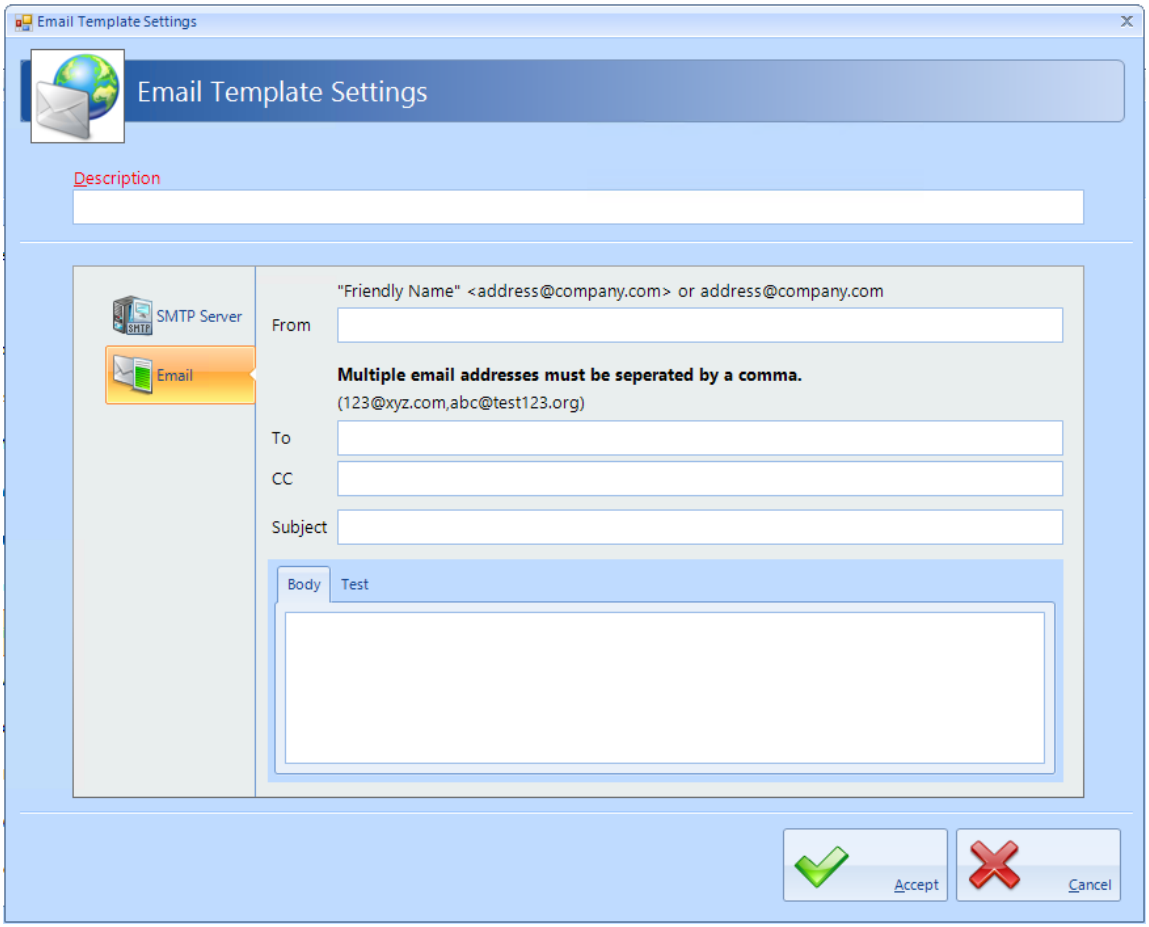


Description: add a meaningful name for the template.

© 2026 Controlsoft Ltd

SMTP Server Settings: Enter the SMTP Server Name, Port number, encryption method, Username and Password for your email account.

Click on **[Email]** in the side tab.



From: The email address of the sender

To: The email address of the recipient

CC: The email address of anyone else to be copied into the email

NOTE: It is possible to enter multiple email addresses in the To and CC fields, simply separate them with a comma as shown on the screen.

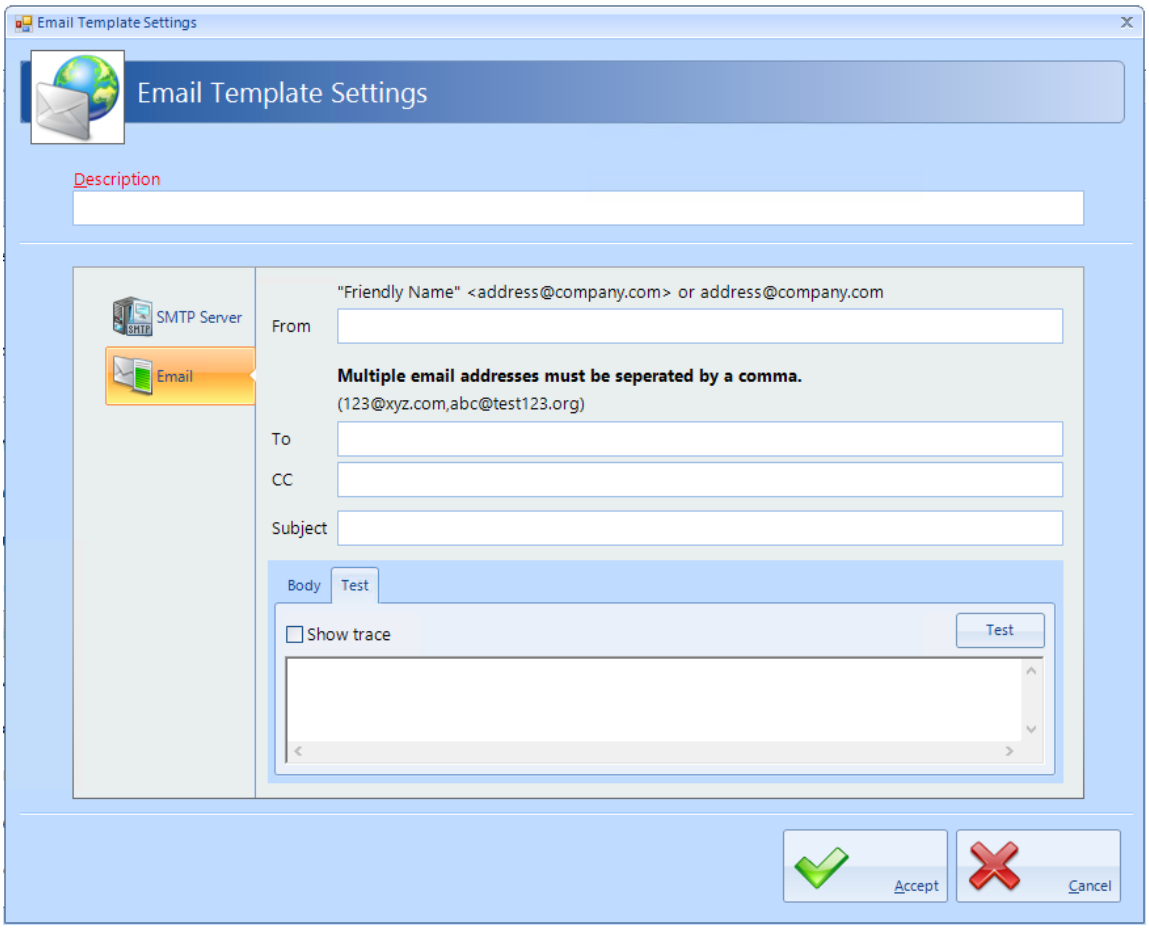
Subject: A meaningful subject so that the email can be recognised as important by the recipient

Body: The main body of the email

NOTE: The Subject and Body can be edited when creating the email action to ensure that it is relevant to the event detected.

To test the email, click the **[Test]** tab:

© 2026 Controlsoft Ltd

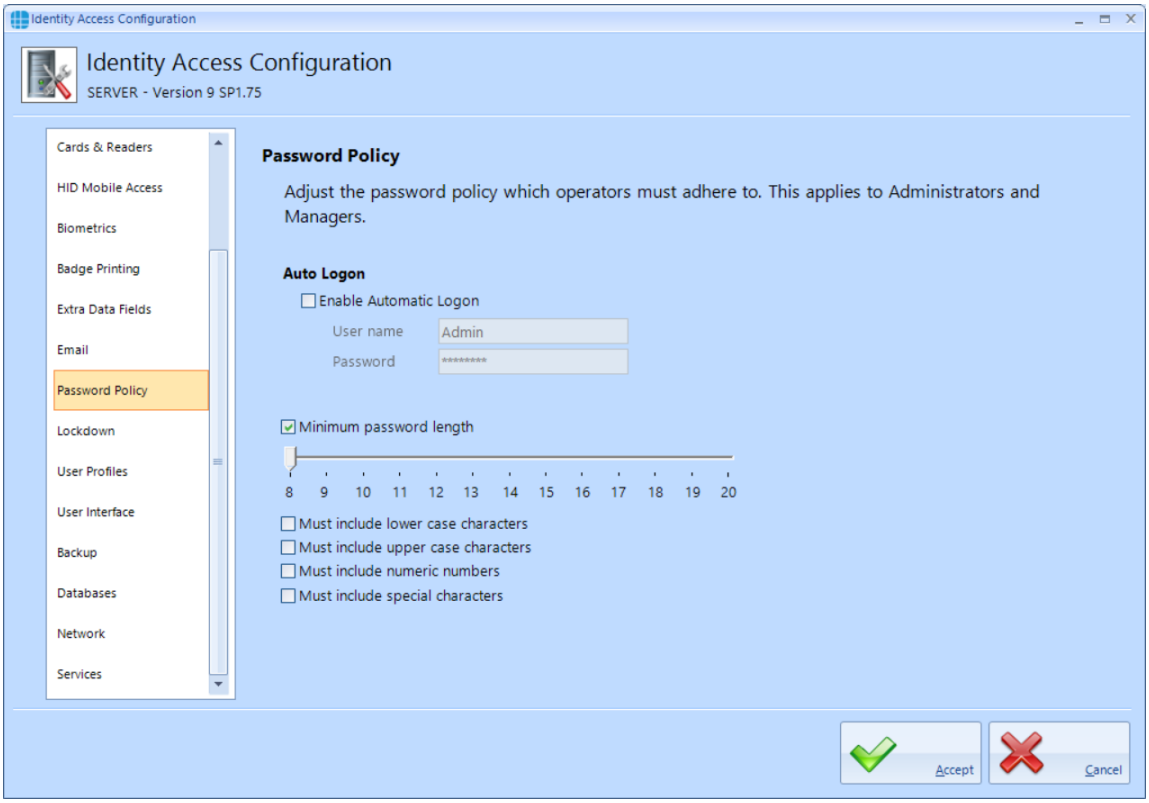


Click the **[Test]** button to send a test email. the display will indicate whether the test was successful.

23.10 IA Configuration > Password Policy

The Operators tab defines the level of security required when operators log into the system.

© 2026 Controlsoft Ltd



Auto Logon - It is possible for Identity Access to automatically logon with specific account credentials by ticking **Enable Automatic Logon** box and entering the username and password for an authorised operator. This can be useful when installing and configuring a system to make it simpler to repeatedly start the software but this is not recommended in normal use as it effectively removes the password security of the system.

The remaining options enforces constraints on the strength of Operator passwords

Minimum Password length - The minimum password length can be adjusted between 8 and 20 characters.

Must include lower case characters - The password must include at least 1 lower case character (e.g. a, b, c)

Must include upper case characters - The password must include at least 1 upper case character (e.g. A, B, C)

Must include numeric characters - The password must include at least 1 numeric character (e.g. 1, 2, 3)

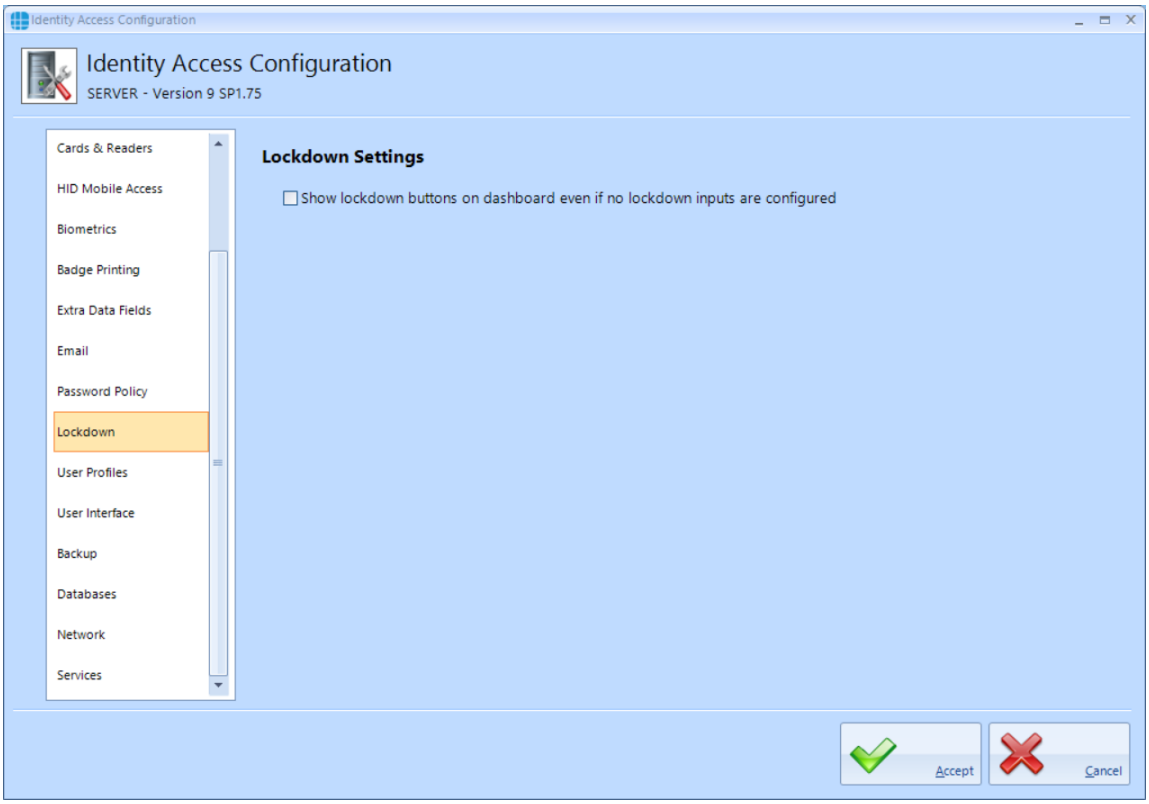
Must include special characters - The password must include at least 1 special character (e.g. !, @, >)

The screen above shows the default settings, at least 8 characters and need not include lower case, upper case, numeric or special characters.

© 2026 Controlsoft Ltd

23.11 IA Configuration > Lockdown

The Lockdown tab defines whether Lockdown buttons are always displayed in the IA User Interface

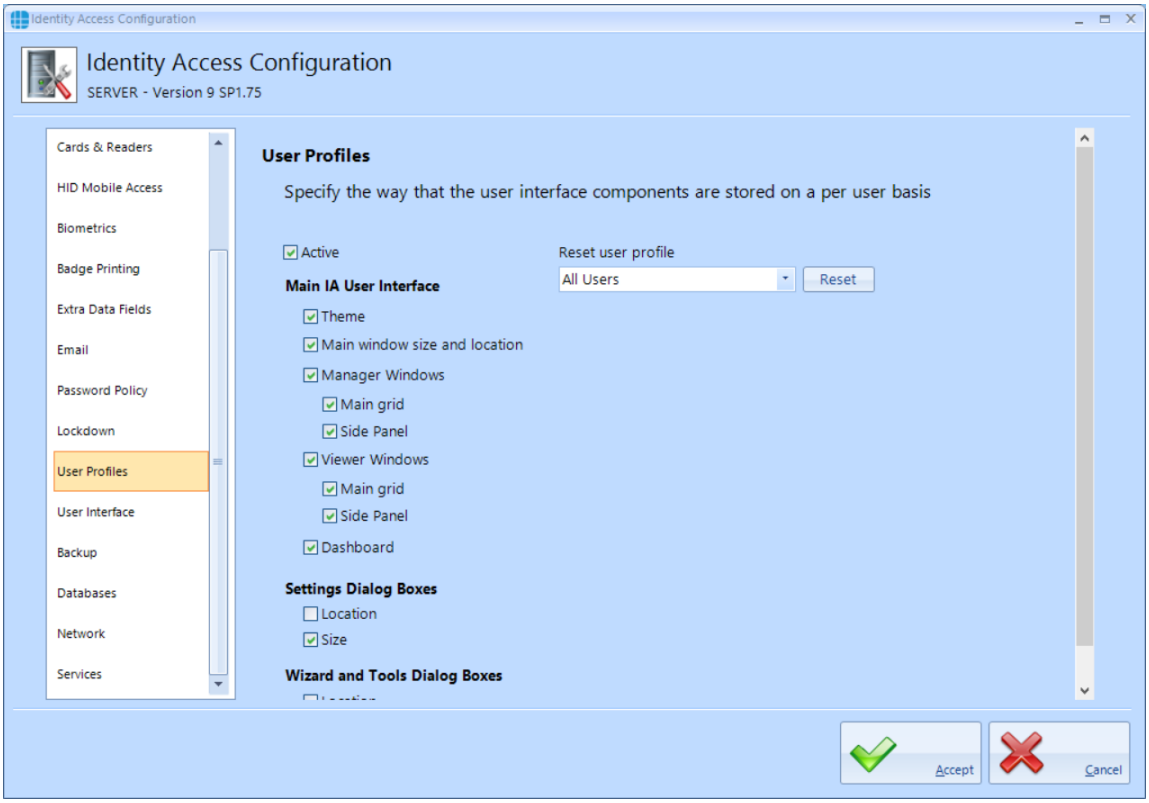


NOTE: Lockdown is only available when an IA-PRO or IA-ENT license has been applied.

23.12 IA Configuration > User Profiles

The User Profiles tab defines whether the size and positions of screens are remembered per operator. If selected, changes to screen location and size made by one operator does not affect the layout shown to other operators.

© 2026 Controlsoft Ltd



Active - ensure this option is ticked to enable user profiles

Reset User Profiles - reset operator profiles, either for everyone or by operator group.

Main IA User Interface - define which elements of the software can be adjusted by operator

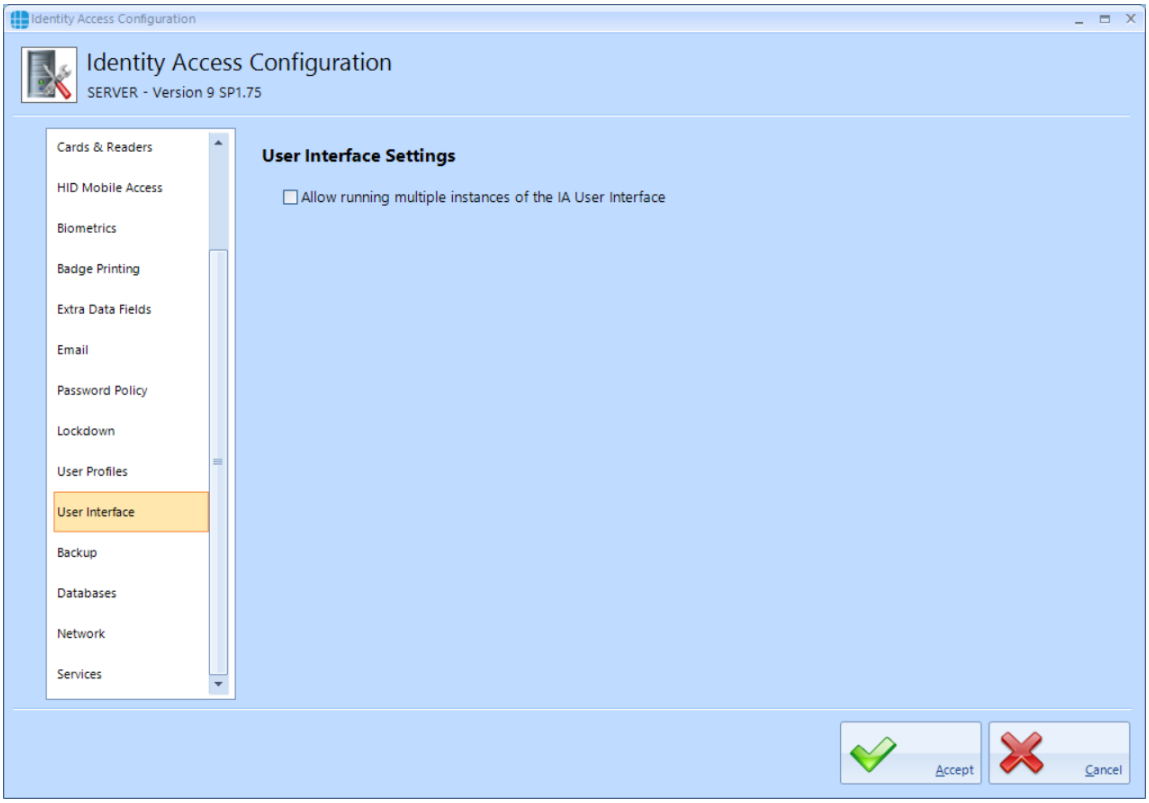
Settings Dialog Boxes - define whether **Location** and/or **Size** can be adjusted per operator

Wizard and Tools Dialog Boxes - define whether **Location** and/or **Size** can be adjusted per operator

23.13 IA Configuration > User Interface

The User Interface tab defines whether multiple instances of Identity Access can be run simultaneously.

© 2026 Controlsoft Ltd

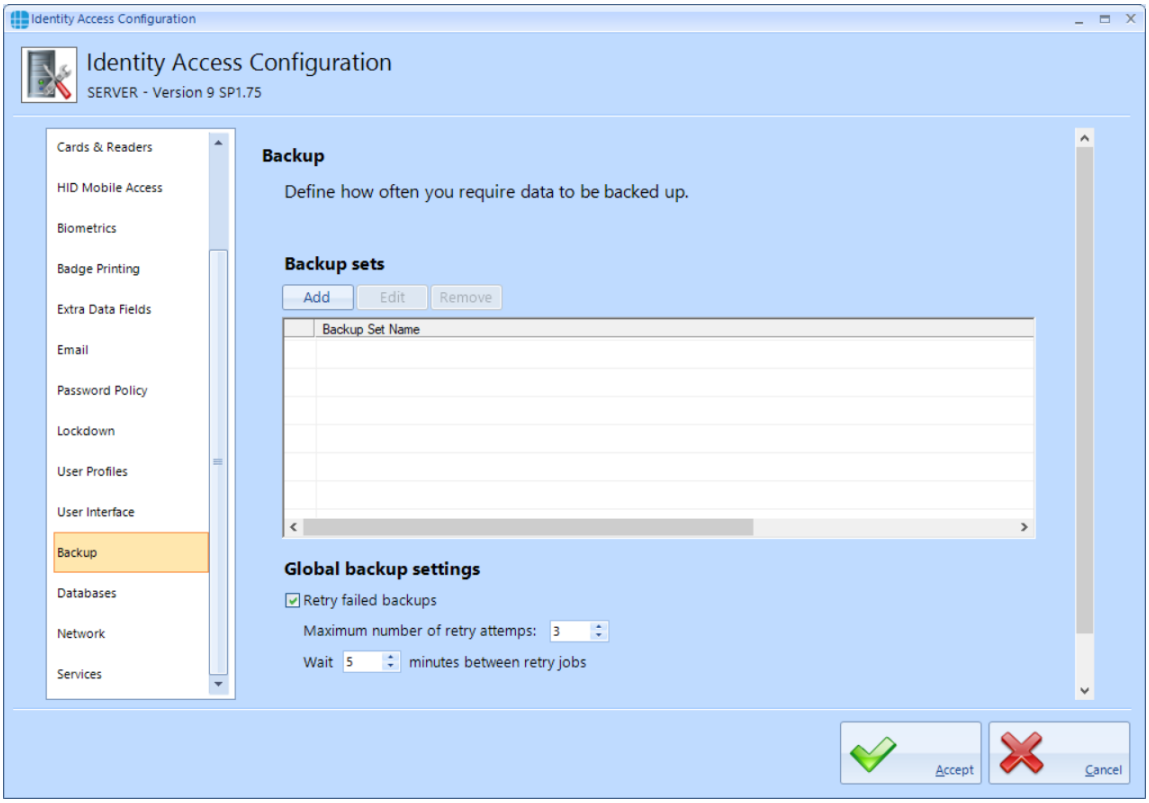


Allow running multiple instances of the IA User Interface - tick this option if you want to run an instance for each Operator

23.14 IA Configuration > Backup

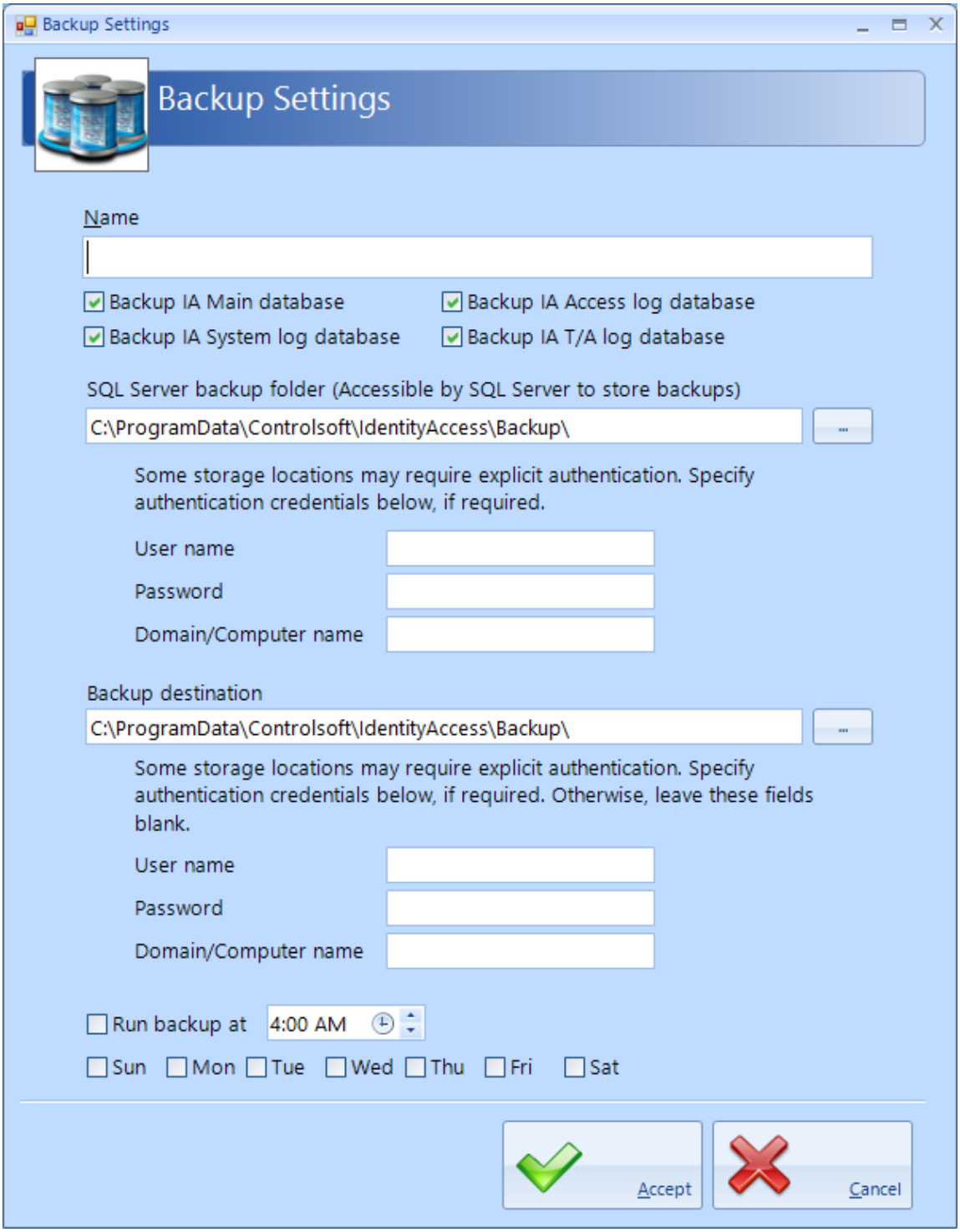
The **Backup** tab defines one or more Backup Sets to define which databases are backed up, the destination folder and the frequency of the backup.

© 2026 Controlsoft Ltd



Backup Sets allows us to define one or backup definitions. Click the **[Add]** button

© 2026 Controlsoft Ltd



Name - Give the backup set a name, then define which database files are to be backed up.

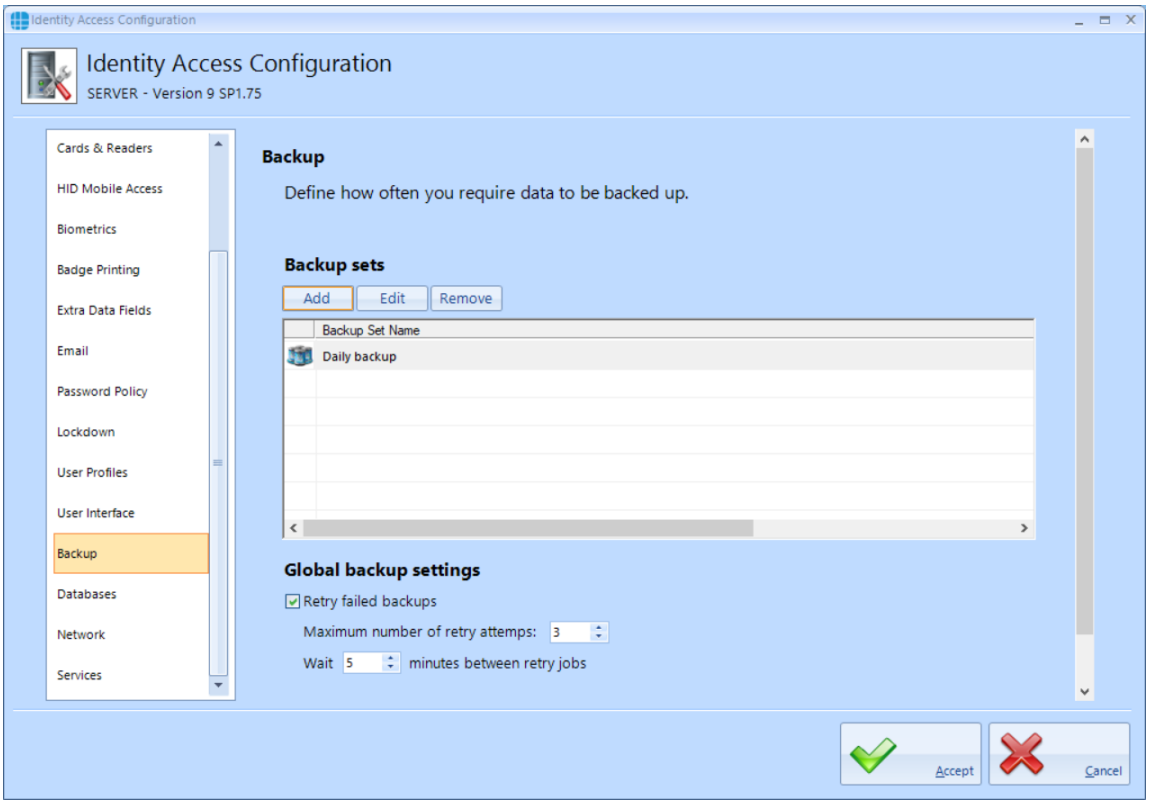
SQL Server backup folder - If the SQL Service is installed on the same PC as Identity Access this section can be ignored. If the SQL Service is installed on a different PC as Identity Access, define the relevant details to communicate with the SQL Service

Backup Destination - Define the folder where the backup are to be saved and, if needed, the relevant details to ensure that IA can communicate with the destination device. ***NOTE:*** Never save backups to the same device that runs the IA Server

© 2026 Controlsoft Ltd

software, always backup to physically different device such as a Network Storage Device.

Run backup at - Define the time and which days to perform the backup.



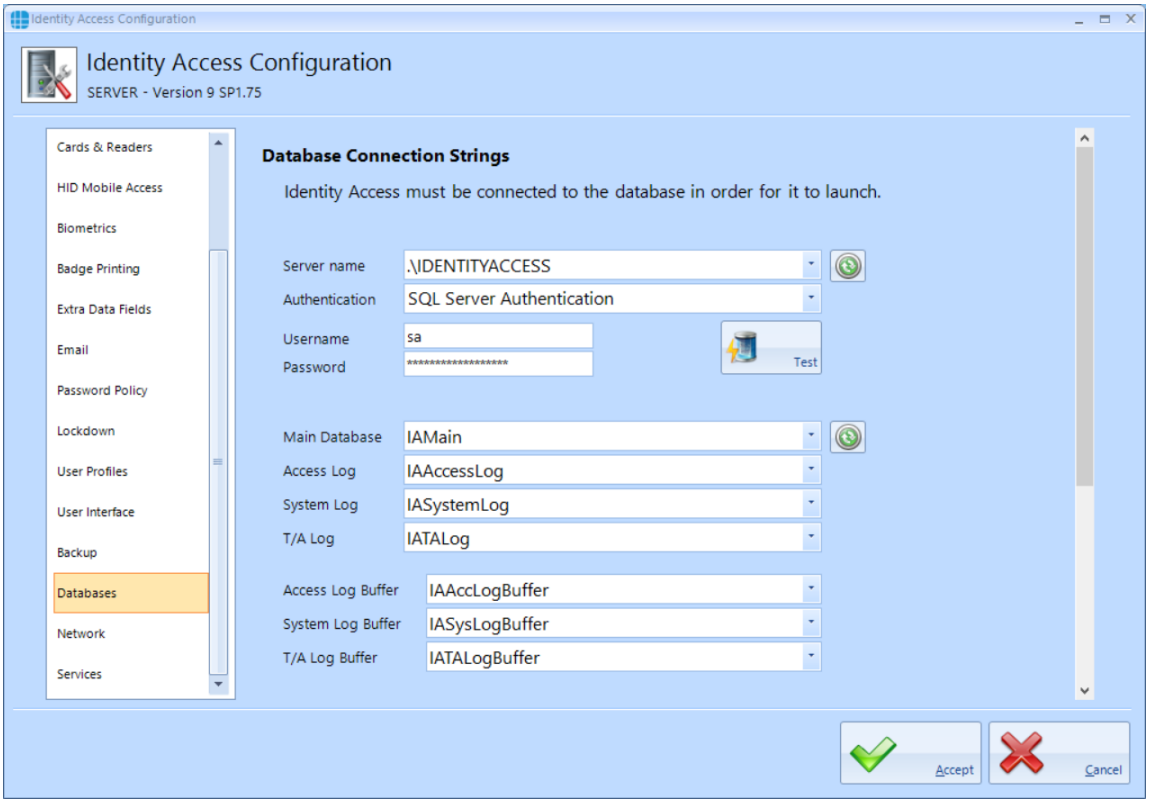
Retry failed backups - Define how many attempts should be made to backup the database before giving up and delay between each attempt.

Automatically delete old backups - to reduce storage requirements on the backup device, you can limit the number of backup files saved.

© 2026 Controlsoft Ltd

23.15 IA Configuration > Databases

The **Databases** tab is used to point to where the SQL database is installed

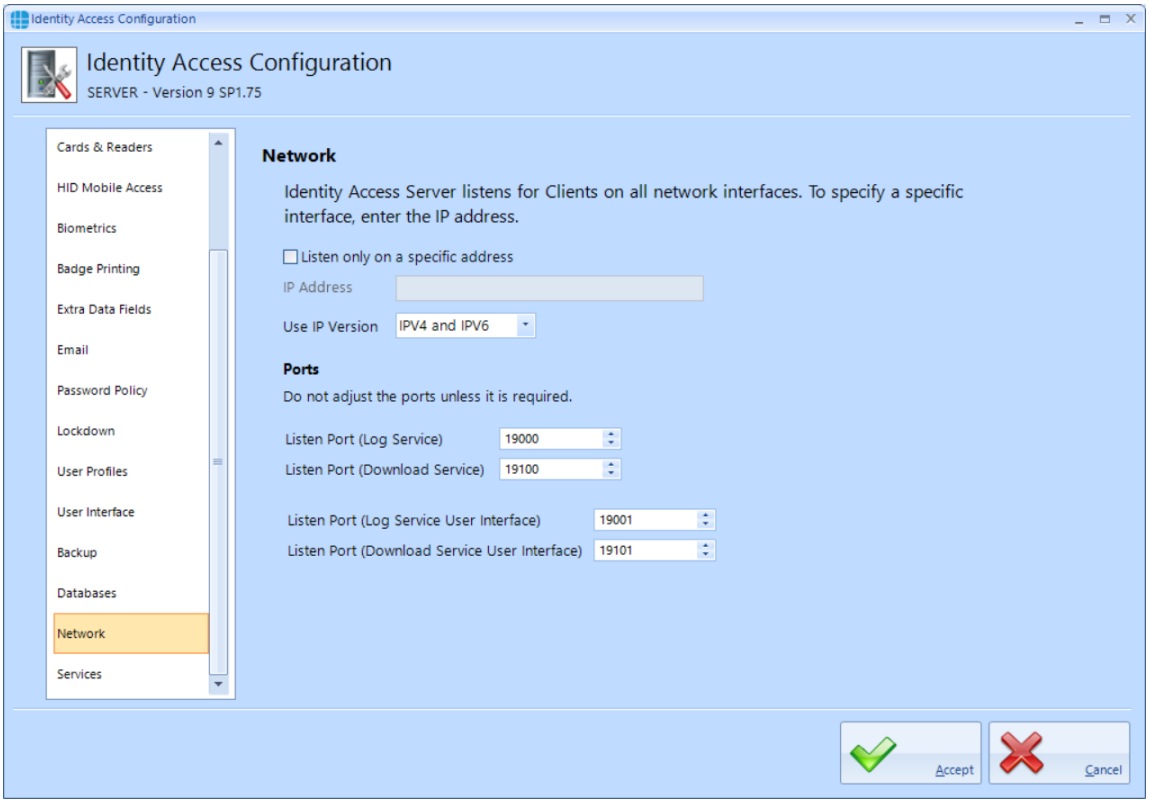


NOTE: DO NOT change these strings unless instructed to do so by Controlsoft Technical Support.

© 2026 Controlsoft Ltd

23.16 IA Configuration > Network

The **Network** tab is used to configure the network settings.



Listen only on a specific address - with this option unticked, the Server will communicate with Clients on any of the IP Address ranges configured on the Server's network card. If the option is ticked and a specific IP Address entered for the Local Host (e.g. 192.168.0.200), only clients on the same network range (192.169.0.1 to 192.168.0.254) will be able to communicate.

Use IP Version - choose from IPV4 only, IPV6 Only or IPV4 and IPV6

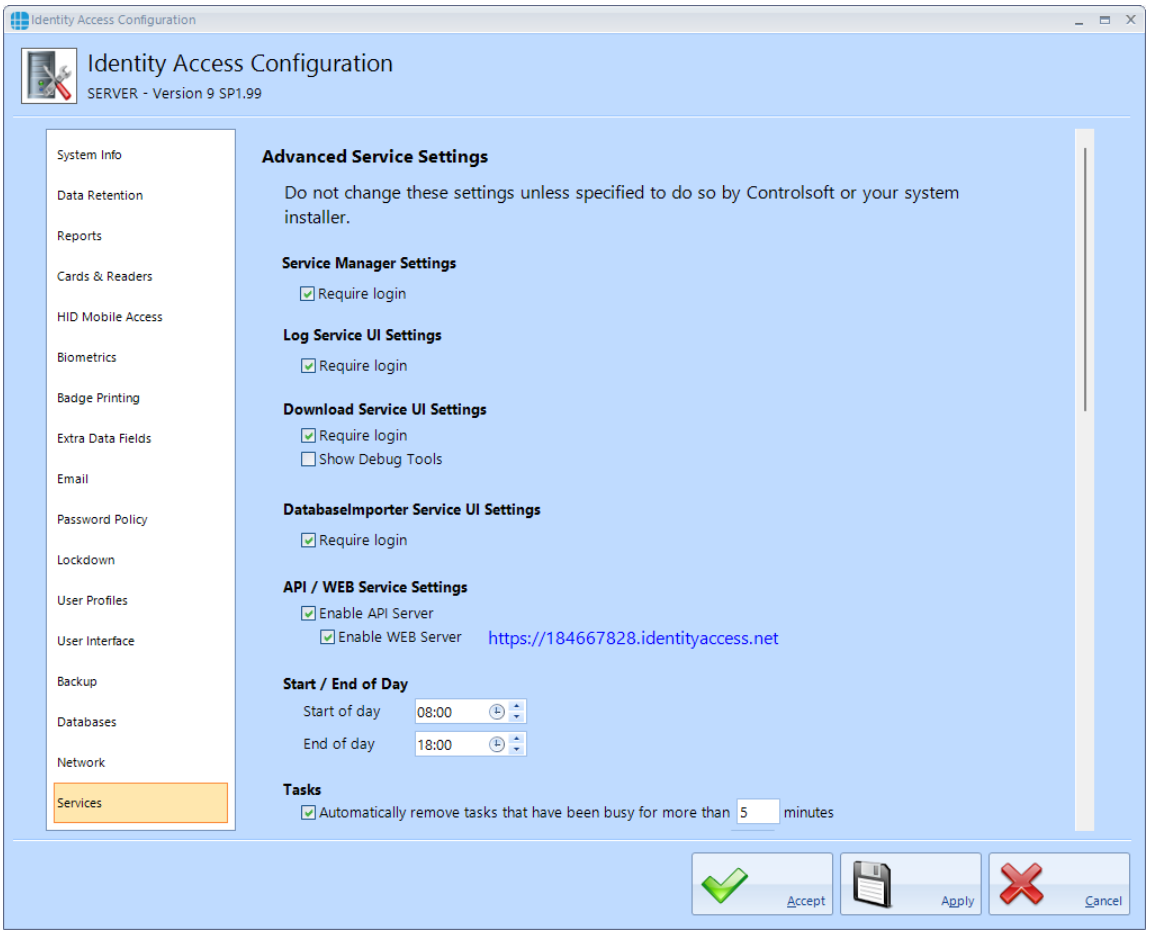
Listen Port (Log Service) and **Listen Port (Log Service User Interface)** - these are ports used for all Log Server communications

Listen Port (Download Service) and **Listen Port (Download Service User Interface)** - these are the ports used for all Download Server communications

NOTE: The above default values should not need to be changed unless requested by Controlsoft Technical Support

© 2026 Controlsoft Ltd

23.17 IA Configuration > Services



If a **Require login** options are enabled, the relevant services will require an operator's credentials to run. While unticking these can be useful when installing and configuring the software, Controlsoft strongly recommend leaving these options ticked when the installation is complete to avoid unauthorised access. When configuring Operator Permissions, selected Operator Groups can be barred from accessing these services.

The **Show Debug Tools** option will enable additional diagnostics in the Download Service user interface.

The **API/Web Service Settings** are used for enabling and disabling the Identity Access API and Identity Access Web Server which are used for access the Identity Access Web Client.

Start of day and **End of day** are used for features such as Time & Attendance and automatically invalidating cards at the end of the day.

The **Tasks** options are designed to remove tasks that have been in the queue for a long time. Controlsoft strongly recommend that these options are both selected.

The **Sync iNet Time and Date** allows flexibility in how frequently the iNet clocks are synchronised with the PC's date and time.

© 2026 Controlsoft Ltd

The timers under the **Startup** option should not be changed unless instructed to do so by Controlsoft Technical Support.

Enabling the **Perform incremental download to Morpho devices** will ensure that the Morpho fingerprint reader databases are always fully up to date.

Automatically reset Anti-Passback will reset APB at the specified time each day. This can be useful, for example, to reset APB at 2am to negate any tailgating that may occur when users leave the building each evening.

The **Objects on iNet** option defines whether data downloaded to Master and Downstream iNets is checked for integrity. Tick the box **Enable object confirmation** to enable the option. The two timers define how frequently the system checks "unconfirmed" objects (i.e. data that has not been confirmed as correctly downloaded) and "confirmed" objects (i.e. data that has been confirmed as correctly downloaded). Controlsoft recommend leaving these timers on the default settings of 5 minutes for unconfirmed objects and 30 minutes for confirmed objects. The option **Object confirmation is only active at specific times** allows a schedule to be set up which defines when data in the Master and Downstream iNets is checked.

© 2026 Controlsoft Ltd

Appendix A - Product History

24 Appendix A - Product History

v9.1.99 - Released January 2026 (Recommended minimum firmware version 9.053)

- NEW FEATURE: Identity Access Web Client. See Identity Access Web Client for further details.
- NEW FEATURE: Identity Access RESTful API For API Access
- NEW FEATURE: Identity Access Site Selector. See Identity Access Client Installation Guide for further details.
- NEW FEATURE: Online Licensing is now available. See Identity Access Licensing Guide for further details.
- Force complex password by default
- Added External Profile (With Logs) and IA-CRD 37Bit biometric device profiles
- Firewall Rules for the Identity Access ports are now automatically written on installation of Identity Access.
- Improvements to the Configuration Options table for further resilience.
- Now packaged with MSO Driver Version 4.8.4 for use with MSO1300 E4.

v9.1.90 - Released October 2024 (Recommended minimum firmware version 9.053)

- NEW FEATURE: External Authentication requests are now configurable for use with External Authentication. See Appendix K for further details.*
- External Authentication Access Allowed events are now reportable within the Access Log Report.
- External Authentication event codes have been added to the Identity Access Download Service User Interface
- ON SITE / OFF SITE now correctly reports when using External Authentication events.

*Requires firmware version 09.066.

v9.1.89 - Released August 2024 (Recommended minimum firmware version 9.064)

- NEW FEATURE: Inclusion of External Authentication requests for use with External Authentication. See Appendix K for further details.

v9.1.88 - Released May 2024 (Recommended minimum firmware version 9.054)

- NEW FEATURE: SQL Server Express 2022 now installed by default and upgraded on standard Identity Access installations.

© 2026 Controlsoft Ltd

- NEW FEATURE: AES-256 Encryption between iNet Controllers and Identity Access software.
- NEW FEATURE: Inclusion of "Bulk Enrol" feature.
- NEW FEATURE: System Integrator and Administrator Operators now setup on installation.
- NEW FEATURE: Facility Codes can now be added from within the Facility Code fields. Facility codes now enabled by default.
- NEW FEATURE: Inclusion of Automatic Personnel Numbers.
- NEW FEATURE: Inclusion of iNet IP Utility included with installation.
- NEW FEATURE: Inclusion of Rebuild, Update and Quick Setup buttons within System tab.
- NEW FEATURE: Inclusion of new Support and Manual options in the Home tab.
- NEW FEATURE: Inclusion of System Integrators details form which links to Home > Support.
- NEW FEATURE: Inclusion of Database Tools & Diagnostics Tools in Identity Access User Interface.
- NEW FEATURE: Menus are now highlighted for easier navigation.
- Backups now pre-configured to daily at 13:00.
- Latest version of MSO enrolment drivers for support with MSO-330 enrolment devices.
- "Setup" and "Management" tab name change to "System" and "User Admin".
- Inclusion of "All Door / All Hours" and "Working Hours" groups.
- "IA Configuration", "Diagnostic Tools" and "Database Tools" log in automatically when logged into Identity Access as an administrator.
- Fix for HID iClass 47 Bit - Biometric profiles not sending Wiegand data.
- Changes to Biometric profiles to allow for secondary token numbers to be used on "Biometric OR" profiles.
- Changes made to the IA Configuration Options table to prevent occasional lose of data.
- General translation fixes throughout the software.
- Hardware defaults now match the iNet 1DR and 2DR covers.
- AsureID version updated to V7.8.5.308

© 2026 Controlsoft Ltd

v9.1.75 - Released October 2022 (Recommended minimum firmware version 9.046)

- Inclusion of new 1DR and 2DR controllers
- Network Scanner added to iNet Configurator
- Fix for Sentinel issue when upgrading

v9.1.72 - Released January 2022 (Requires Firmware version 9.036 or later in all controllers)

- When using the ANPR integration, the user's Vehicle Registration is now displayed on the user overview screen.
- When adding Facility Codes in IA Configurator, it is now possible to set a default value
- Feature added to iNet Configurator to find iNets, their IP Addresses then being added to a dropdown list to access the devices
- Sentinel driver updated to v8.23
- "User Interface" tab added in IA Configuration utility to "Allow running multiple instances of the IA User Interface".

v9.1.67 - Released July 2021 (Requires Firmware version 9.032 or later in all controllers)

© 2026 Controlsoft Ltd

- Sentinel driver updated to v8.21
- Standalone Controller Configurator renamed to iNet Configurator
- Facility Code included in data import
- Column added to door manager to show whether it is an APB door
- Improved linking of Morpho reader to card reader for a given door
- If a Morpho reader is selected in a group, the appropriate card reader / APB door will be selected automatically and visa versa
- It is now possible to reset APB status for all users via the Dashboard as well as Timed Reset option
- Reset APB option added for individual users / groups via the Option Wheel
- Duress implemented for fingerprint, token and/or PIN
- Max number of doors per master controller limited to 32
- Edit button included in Employee Information screen when using the identify ID token feature
- To accommodate updated screens, recommended screen size changed to 1280x800
- Option wheel added to the access log viewer so access allowed and access denied events now allow the appropriate user to be edited, reported on or details copied to clipboard
- Access denied events for a card not allocated to a user now has an option wheel entry to add the user
- Introduction of user profiles
- Changes to IA Configurator for user profiles
- Two additional themes – Office 2013 dark and Office 2013 Light
- Addition of integrated Backup feature

v9.1.44 - Released November 2020 (requires firmware version 9.026 or later in all controllers)

- IA-STD renamed to IA-LITE
- Maximum number of doors/readers for IA-LITE limited to 12
- Maximum number of doors/readers for IA-PRO limited to 64
- New license introduced IA-ENT, unlimited number of doors

© 2026 Controlsoft Ltd

- Windows services introduced, Log Server is now Log Service and Download Server is now Download Service. Service Manager has been introduced to access the user interface for these services.
- Controller Status display added to confirm that all data on Master and Downstream iNets is correct.
- Introduction of 'Advanced' features - Object Groups, Counters & Timers, Inputs & Outputs, Graphics Designer, Events & Actions
- Compatibility added with HIKVision ANPR camera (not available with IA-LITE)
- IA Server Configuration and IA Client Configuration replaced with single utility called IA Configuration
- Lockdown no longer available in IA-LITE
- Facility Code added to user configuration to avoid issues with multiple cards with the same card number but different FACs
- AntiPassBack now supported across Master Controllers.
- Facility to allocate Temporary tokens to Visitors has been removed, but is now available to Contractors
- System log now indicates when Master and Downstream controllers connect and disconnect
- Asure ID updated to v7.8.0.262
- It is now possible to set the maximum number of concurrent downloads in the Download Service Home screen
- Facility added to remove permission for Operators to operate Lockdown
- Reliability of AntiPassBack improved by adding System Log events for 'Zone Changed' and 'Zone Not Changed' during entry and exit.
- Default I/O for Normal Doors no longer include Door Contact
- Default I/O allocation for airlocks and turnstiles amended to make better use of iNet I/O
- Default I/O allocation amended for iNet alarm inputs
- Morpho profiles added for simpler configuration
- Controller Manager now displays devices programmed onto controller's RS485 bus
- Enhanced details added to system log when users are edited
- Sentinel Licence software updated to v7.92
- Colours used for I/O Usage changed:

© 2026 Controlsoft Ltd

- Green = Input is available to use
- Yellow = Input already programmed elsewhere
- Red = Input programmed to two different functions which needs to be resolved
- Grey = Input not available

v8.0.245 - Released April 2019 (requires iNet firmware version v8.016 or later in all controllers)

- Windows 7 and Windows Server 2008 Operating Systems no longer supported
- Inclusion of Object Confirmation to check integrity of data in Master and Downstream controllers
- Operator password constraints relaxed

v8.0.229 - Released September 2018 (requires iNet firmware version v98.37.020 or later in all controllers)

- Inclusion of RS485 Aperio system
- Revised Time Zone configuration screens and improved resolution of Time Zones
- Ability to link Time Zones to Access Schedules in Morpho Sigma fingerprint readers
- Inclusion of HID OSDP readers
- Timeout for Door Held Open alarms extended to 1800 seconds (30 minutes)
- To avoid clutter on the alarms screen, any given alarm will only be displayed once, until cleared. Further activations are still logged in the System Log.

v2017.1.534 - Released August 2017 (requires firmware version v98.36.017 or later in all controllers)

- Improved communication protocols for faster data transfer
- Inclusion of Elevators
- Inclusion of Site Lockdown
- Inclusion of DropBox card collector
- First Swipe Rule for secure release of doors on Time Zone
- Simplified installation sequence
- Inclusion of camera support

© 2026 Controlsoft Ltd

- Access Control Status report
- Multiple tokens for each user
- Input type for monitoring BreakGlass
- Input types for monitoring Mains Fail, Battery Fault and PSU Fault

v2016.4 - Released January 2017. Following features and benefits included:

- Facility added to print multiple cards simultaneously
- Ability to print Visitor and Contractor cards
- Importing users from Controlsoft Pro also imports photographs
- Issuing HID Mobile credentials simplified by removing one step.
- Default for purging event logs is now 3 months (was 1 month)
- Maximum number of Time Zones increased from 16 to 63 (requires iNet firmware v98.34.21.9 or later)
- "Tag Valid From" can now be set to the nearest minute
- Supports "Latched" door operation (requires iNet firmware v98.34.21.9 or later)
- Data transfer speed increased during Uploads and Downloads (requires iNet firmware v98.34.21.9 or later)
- Morpho devices now support "External Profiles" for increased flexibility
- Issue with "Must change password at next login" resolved
- Changes can now be made to the Client Configuration and Server Configuration utility while IA User Interface is open
- Issue with the "Logoff" button now resolved
- Fire Roll Call report now runs from the IA User Interface running on a Client machine
- It is now possible to create 24 doors on an unlicenced version of IA rather than 23 in previous version.
- Issues with AntiPassBack resolved.

v2016.3 - Released October 2016. Following features included:

- Licence now transferable
- Access Reports can be filtered by Company and Department
- Increased security on Download Server and Log Server

© 2026 Controlsoft Ltd

- Inactivity reports added
- Improved stability in communications with controllers

v2016.2 - Released August 2016. Following features included:

- Licence Manager added
- Airlocks
- AntiPassBack
- Fingerprint Enrolment (a Morpho MACI licence will also be required)
- Fire Alarm Rollcall report
- Time Sheet Reports
- Turnstiles
- Integration with Asure ID (an HID licence will also be required)
- Integrated issuance of HID Mobile Access credentials
- Identity Access Express withdrawn

NOTE: To upgrade a copy of Identity Access Express to v2016.2:

1. Install Microsoft SQL Management Studio 2014 (available from www.controlsoft.com) and backup the LocalDB database
2. Uninstall Identity Access v2016.1, then install Identity Access v2016.2 (available from xxx.controlsoft.com)
3. Use Microsoft SQL Management Studio 2014 to restore the original database

v2016.1 - Initial Release

© 2026 Controlsoft Ltd

Appendix B - Types of Door

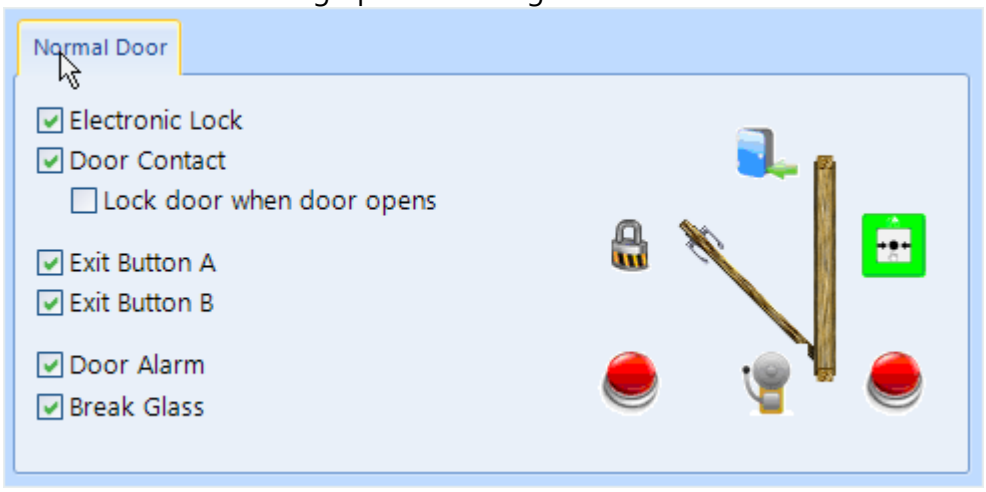
25 Appendix B - Types of Door

Within the Identity Access software, it is possible to select 4 types of door, namely Normal Door, Turnstile, Airlock and Aperio Door.

NOTE: To use Turnstiles or Airlocks, Identity Access Professional is required.

25.1 Normal Door

The term **Normal Door** refers to a standard single leaf type of door. When selected, the software shows the graphic for a single leaf door as shown below:



The components required for the door to operate are:

Electronic Lock: This is a relay output used to drive a Maglock, Strike Lock or similar. The relay output can be programmed for Normal or Inverted operation for maximum flexibility in the choice of lock type.

Door Contact: A door contact connected to an input on the controller is used to detect when the door has been opened. The input can be programmed for Normally Closed or Normally Open operation for use with any door contact.

Lock door when door opens: If this option is NOT selected, the door will be released for the full door release time. Selecting this option will truncate any remaining release time as soon as the door starts to open, so the door is secured as soon as it closes, not at the end of the release time. This is often seen as a higher security option.

Exit Button A Request to Exit (REX) button can be used to release the door from within the protected area. A REX is not required if the door uses an IN and an OUT reader. The Identity Access system support a second REX button **Exit Button B**, so in a reception area, one can be fitted at the door and another at a receptionist's desk. The input can be programmed for Normally Closed or Normally Open operation for use with any type of REX.

© 2026 Controlsoft Ltd



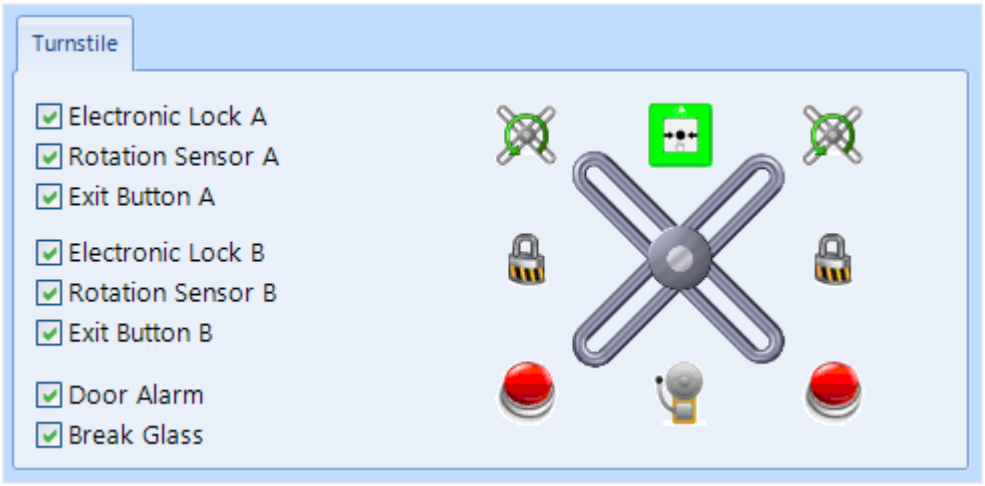
Door Alarm: This is a relay output used to drive a sounder when a Door Forced, or Door Held alarm is generated or when a breakglass has been activated. The relay output can be programmed for Normal or Inverted operation for maximum flexibility in the choice of sounder.



Break Glass: A Breakglass is used to physically remove power from the lock to provide free access. One of the internal switches is connected to an input on the controller used to detect when the breakglass has been activated. This information is then displayed on the Alarms tab on the Dashboard, and will activate the Door Alarm output (if programmed). The input can be programmed for Normally Closed or Normally Open operation for use with any breakglass.

25.2 Turnstile

The term **Turnstile** refers to a mechanism which limits access through a doorway to one person at a time. When selected, the software shows the graphic for a turnstile as shown below:



The components required for the turnstile to operate are:



Electronic Lock: This is a relay output used to allow the Turnstile to rotate. Use Electronic Lock A for anticlockwise rotation and Electronic Lock B for clockwise rotation. The relay output can be programmed for Normal or Inverted operation for maximum flexibility



Rotation Sensor: The rotation sensor is connected to an input on the controller to detect when the turnstile has rotated. Use Rotation Sensor A for anticlockwise rotation and Rotation Sensor B for clockwise rotation. The input can be programmed for Normally Closed or Normally Open operation



Exit Button: A Request to Exit button is used to release the Turnstile from within the protected area. A REX is not required if the Turnstile uses an IN and an OUT

© 2026 Controlsoft Ltd

reader. Use Exit Button A for anticlockwise rotation and Exit Button B for clockwise rotation. The input can be programmed for Normally Closed or Normally Open operation



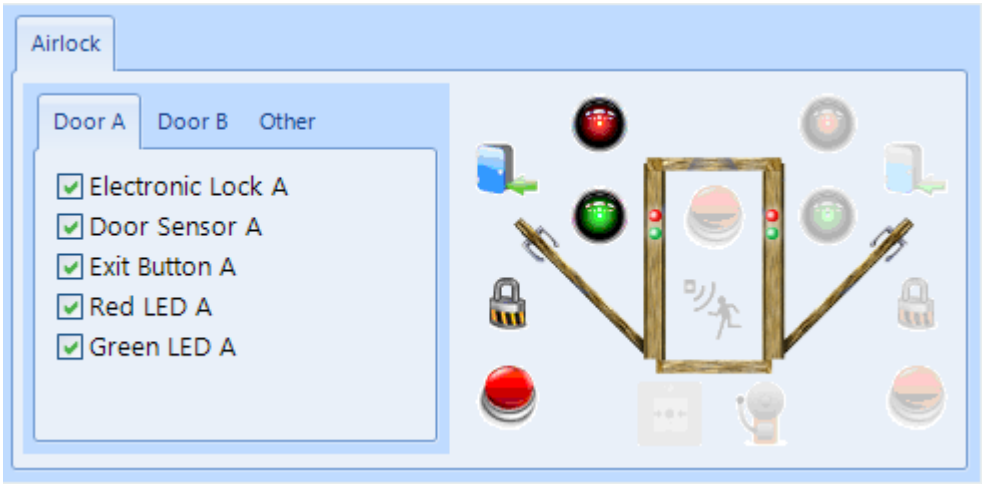
Door Alarm: This is a relay output used to drive a sounder when the turnstile has been forced. The relay output can be programmed for Normal or Inverted operation for maximum flexibility



Break Glass: A Breakglass is used to physically remove power from the lock to provide free access. One of the internal switches is connected to an input on the controller used to detect when the breakglass has been activated. This information is then displayed on the Alarms tab on the Dashboard, and will activate the Door Alarm output (if programmed). The input can be programmed for Normally Closed or Normally Open operation for use with any breakglass.

25.3 Airlock

The term **Airlock** refers to a double door configuration whereby the first door must be closed before the user can open the second door. When selected, the software shows the graphic for an Airlock as shown below:





Electronic Lock A defines the output that controls the lock



Door Sensor A defines the input that monitors the door contact which detects when the door has been opened

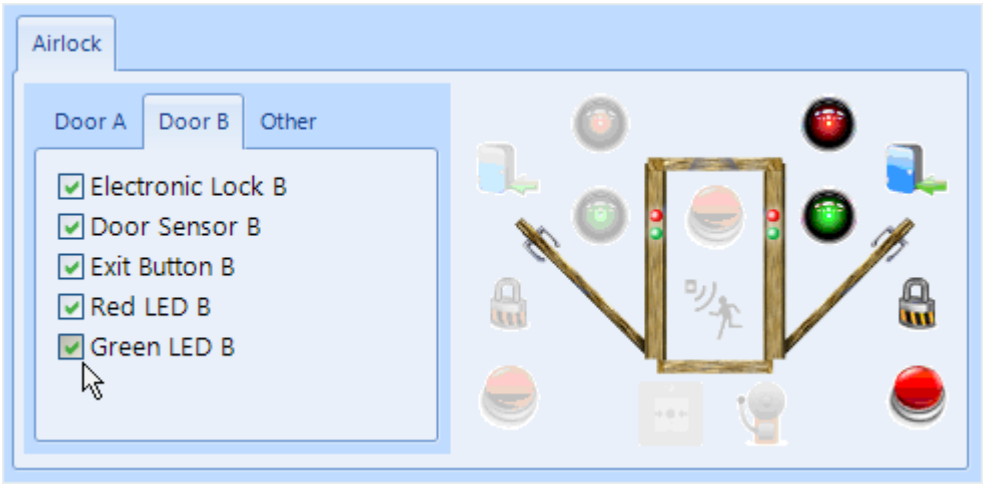


Exit Button A defines the input that monitors the Request to Exit button to release the door

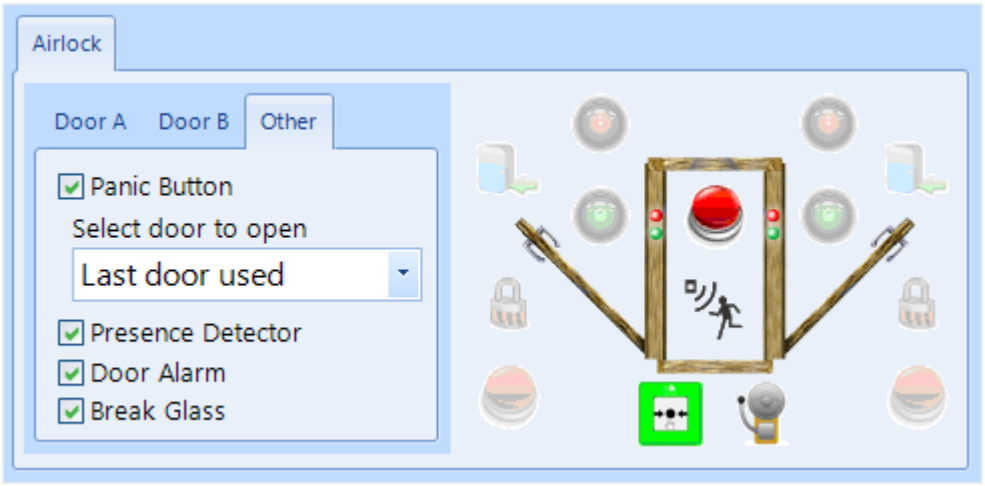
© 2026 Controlsoft Ltd

Red LED A defines the output that controls a red LED to indicate that the door is locked

Green LED A defines the output which controls a green LED to indicate that the door is unlocked



Each of the inputs and outputs for Door B are defined as per Door A



Panic Button defines which input is used to monitor an optional Panic Button for the user to activate in the event of a problem. The Panic Button can activate 'Door A' or 'Door B' or, as in the above example, the 'Last door used'.

Presence Detector defines the input that monitors a push button or movement sensor to indicate that the user is inside in the airlock, which then releases the other door.

© 2026 Controlsoft Ltd



Door Alarm defines the output which triggers in an alarm condition (Door Held Open or Door Forced)



Break Glass: A Breakglass is used to physically remove power from the lock to provide free access. One of the internal switches is connected to an input on the controller used to detect when the breakglass has been activated. This information is then displayed on the Alarms tab on the Dashboard, and will activate the Door Alarm output (if programmed). The input can be programmed for Normally Closed or Normally Open operation for use with any breakglass.

25.4 Aperio Door

Aperio locks can be used to replace existing handles and cylinders to integrate them into the Access Control system. This can provide a quick and efficient way to upgrade door handles or cylinders with mechanical locks.



NOTE: Aperio locks do not support "Out" readers, so some Identity Access functions such as Location and AntiPassBack cannot be used with Aperio locks.

For detailed instructions on how to setup Aperio Wireless devices, see Knowledge Base - Aperio Wireless Guide

© 2026 Controlsoft Ltd

Appendix C - HID Asure ID Software

26 Appendix C - HID Asure ID Software

The Controlsoft Identity Access installation includes a copy of HID Asure ID®. This is an ideal choice for organizations looking for an affordable and easy-to-use photo ID card software with direct integration with the Controlsoft Identity Access database.

Asure ID Enterprise has additional features like compound data fields, batch printing, conditional design and print rules, and password protection.

NOTE: The copy of Asure ID supplied with Identity Access is a 30 days trial copy. To use Asure ID beyond the 30 day trial period, you will require a licence. Please contact your vendor for further details.

For detailed instructions on how to setup Asure ID, see Knowledge Base - AsureID Guide

© 2026 Controlsoft Ltd

Appendix D - Facility Codes

27 Appendix D - Facility Codes

Certain card types are encoded with a facility code. A facility code makes administration of the system simple and can help against duplicated card numbers. If a facility code is encoded to a card then the requirement is turn on facility codes within Identity Access. Below are examples of cards that do not use facility codes and some that do:

Cards without facility codes:

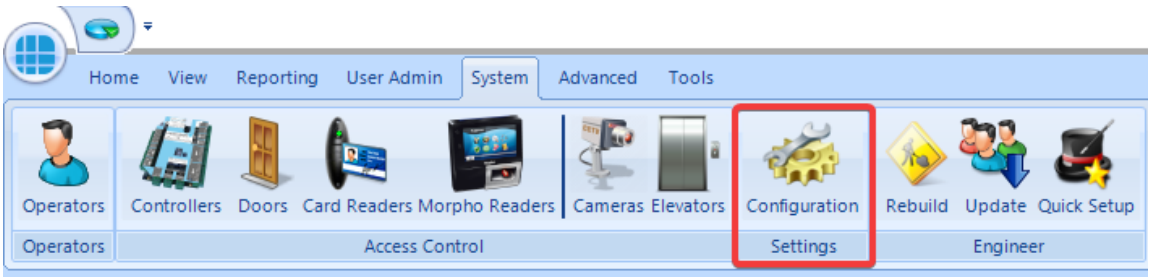
- Controlsoft Prox (Part number: AC-71***XX***)
- Mifare/Desfire reading card serial number (Part number: AC-714***X*** / AC-718***X***)
- Identity Access cards (Part Number: IA-CRD / IA-FOB / IA-MFSIO)

Cards with facility codes:

- HID iClass / Prox / SEOS cards (HID-20***XXXXXXX*** / HID-13***XXXXXXX*** / HID-50***XXXXXX*** / HID-30***XXXXXX***)
- Mifare/Desfire cards encoded with HID Secure Identity Object (Part number: AC-714***X***-SIO / AC-718***X***-SIO)

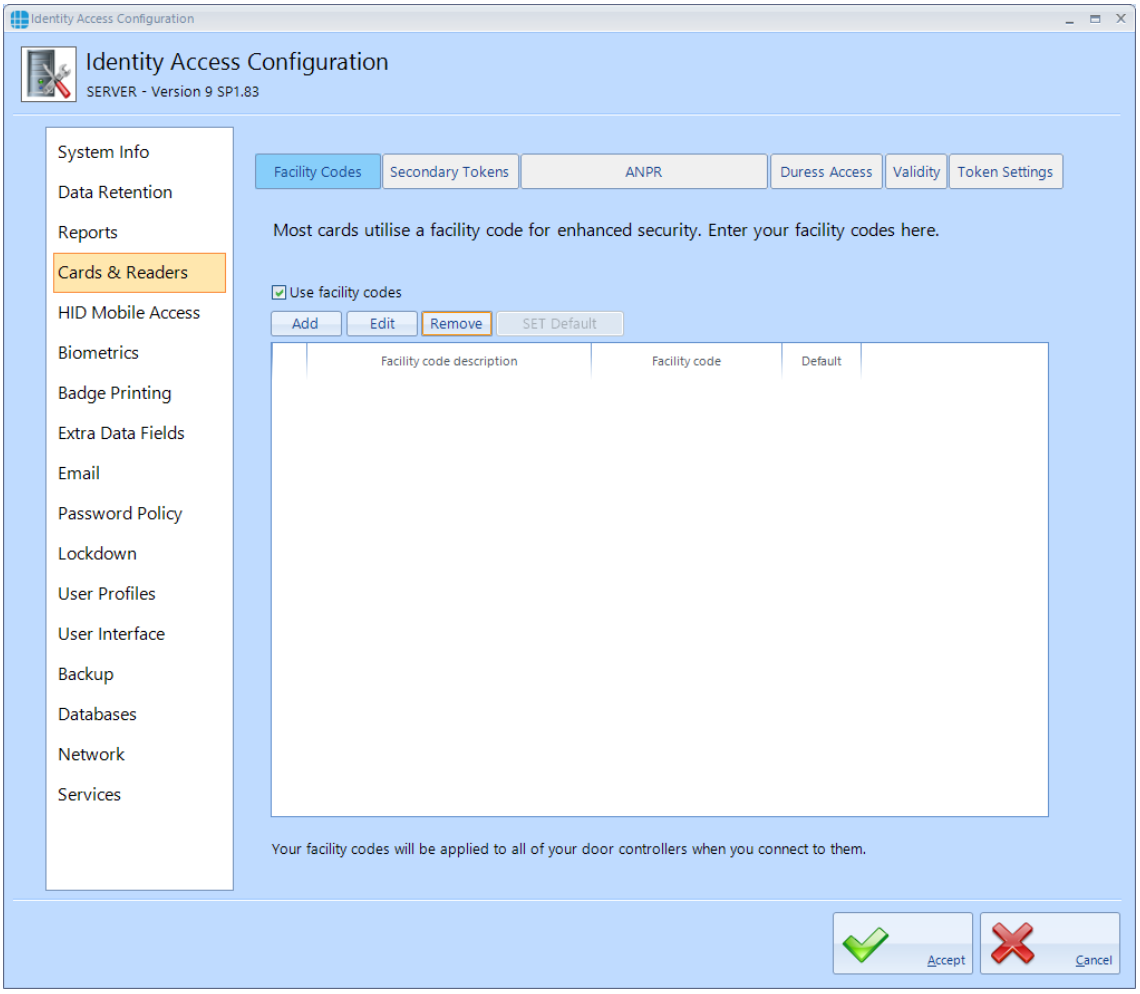
If required, to turn on Facility Codes within Identity Access:

1. Click on **System** and select **Configuration**



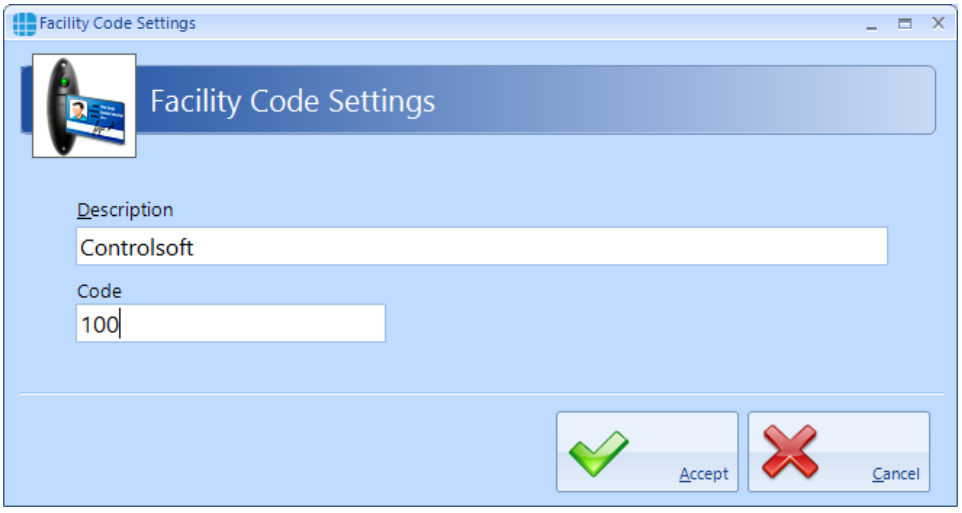
2. Select **Cards & Readers**
3. Tick **Use Facility Codes**

© 2026 Controlsoft Ltd



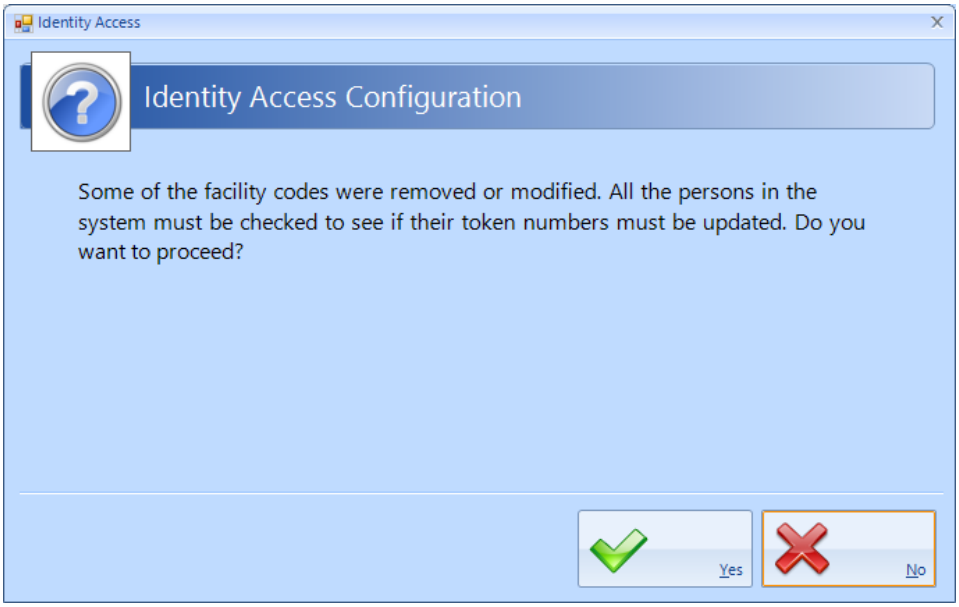
4. Click **Add** (or you will have the option to add a facility code later when adding the User)

5. Fill in a **Description** for this facility code (this can be the same value as the facility code itself) and the facility code value



6. If the following message appears: click Yes if you would like to change everyone without a facility code to have the newly added code, **OR press No if you do not want to change any currently added users.**

© 2026 Controlsoft Ltd



© 2026 Controlsoft Ltd

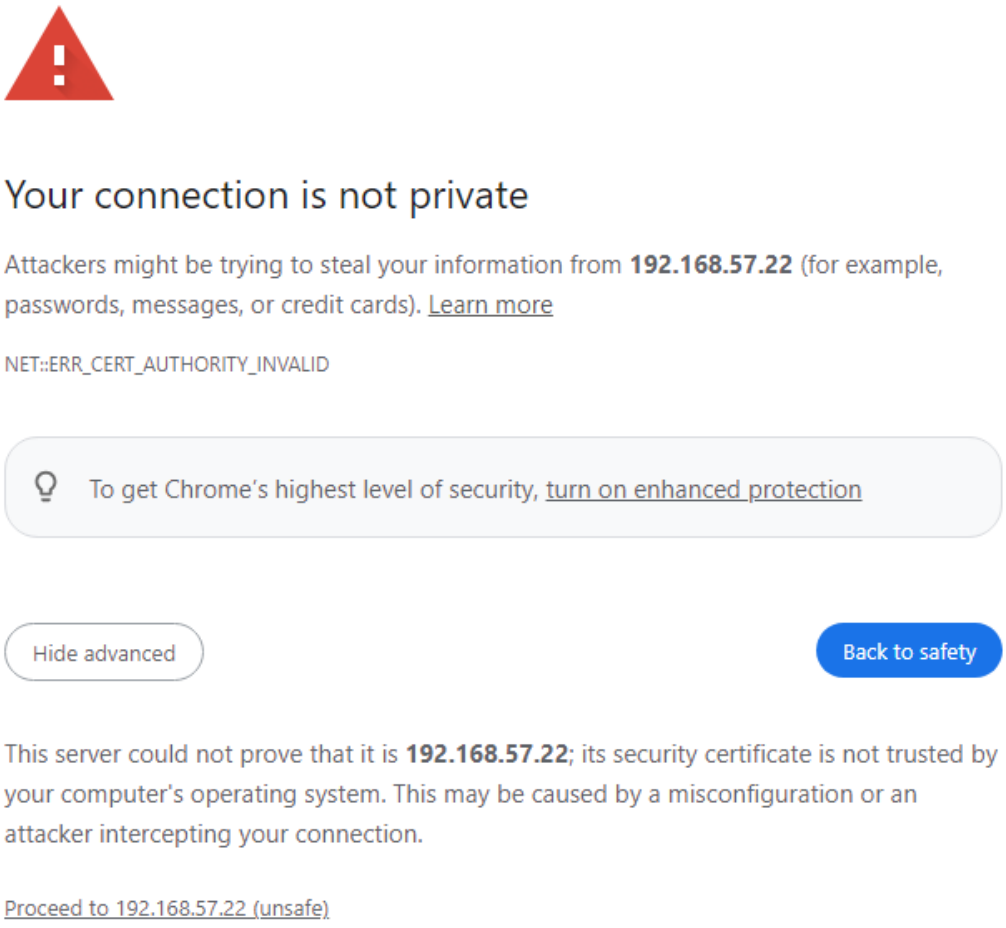
Appendix E - iNet webpage

28 Appendix E - iNet webpage

The iNet controller has a web page which provides information on the status of the controller and certain legacy controller settings can be set. The layout of the page will depend on the firmware version used. This section will show screens from firmware version 9.054.

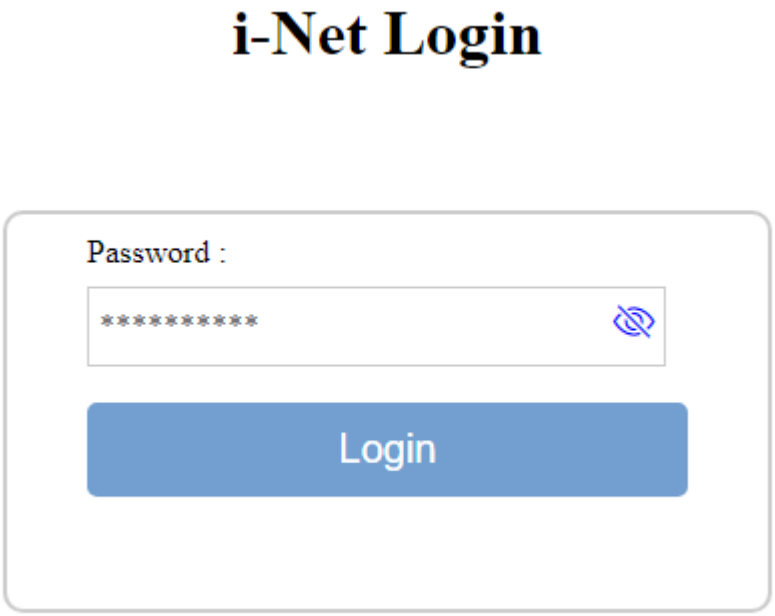
© 2026 Controlsoft Ltd

To access the webpage, go to System > Controllers. Single click the controller to highlight and click the  this will load the device within your default web browser. If you are presented with the following message, press "Advanced" and select "Proceed to XXX.XXX.XX.XX"



The landing page displays the login screen to the iNet door controller. If a password has not yet been set, this will ask you to set the password. Type in your password and select "Login".

© 2026 Controlsoft Ltd

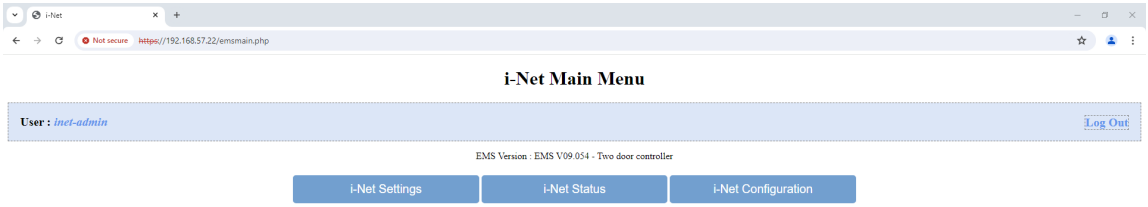


You will be presented with 3 options.

i-Net Settings - Allows you to view the internal controller settings. These are used on legacy Controlsoft installations.

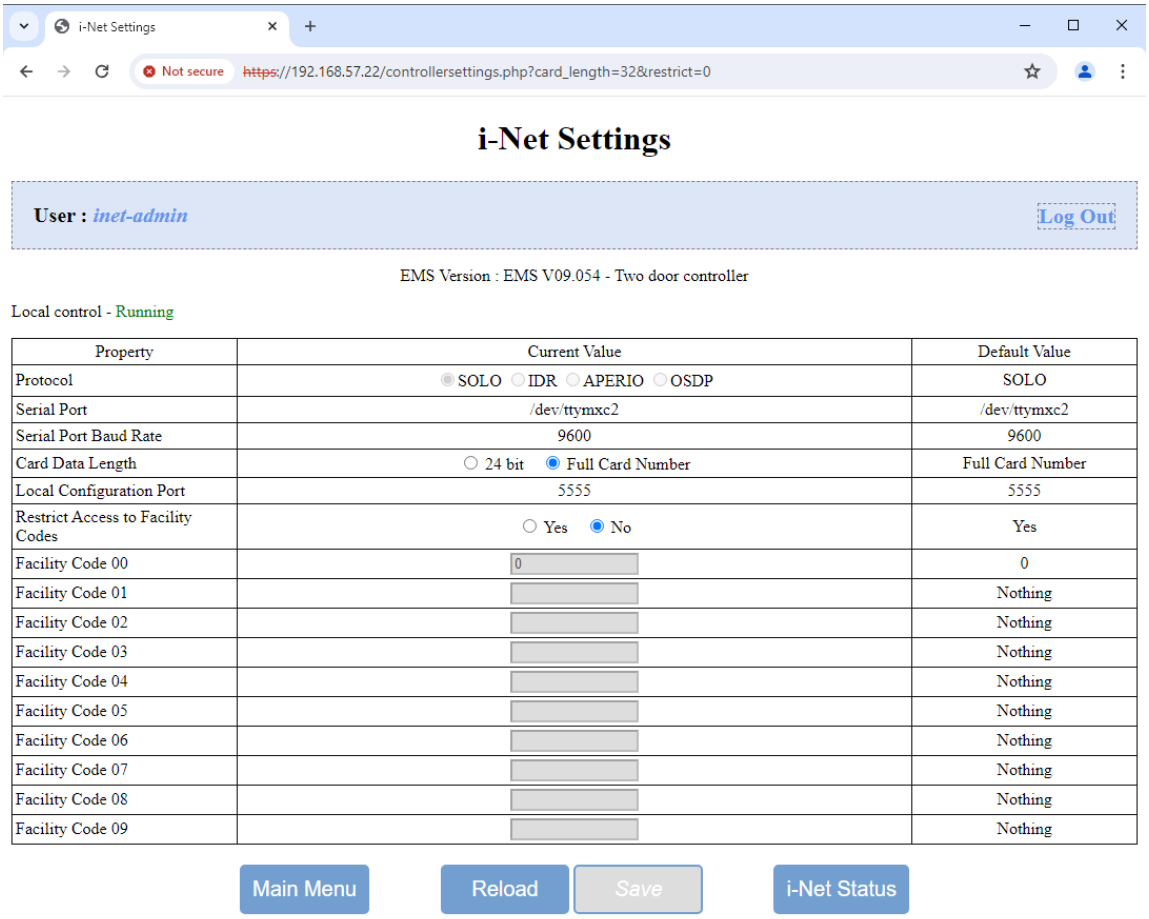
i-Net Status - Allows you to view the status of the iNet controller.

i-Net Configuration - Allows you to change the network settings / update the firmware of the iNet controller.



© 2026 Controlsoft Ltd

i-Net Settings



Protocol: The **SOLO** protocol is used for all iNets connected as Master / Downstream devices and for Master iNets connected to Expanders. **IDR** is only relevant to Controlsoft legacy equipment. The **APERIO** protocol is used with Aperio RS485 hubs and **OSDP** is used when the Master iNet is connected to HID OSPD readers

Serial Port: This must be at its default setting unless instructed otherwise by Controlsoft Technical Support

Serial Port Baud Rate: This must be at its default value, unless using the **IDR** or **OSDP** protocols. For **IDR**, the baud rate should be set to 19200. For **OSDP**, the baud rate should be set to 115200.

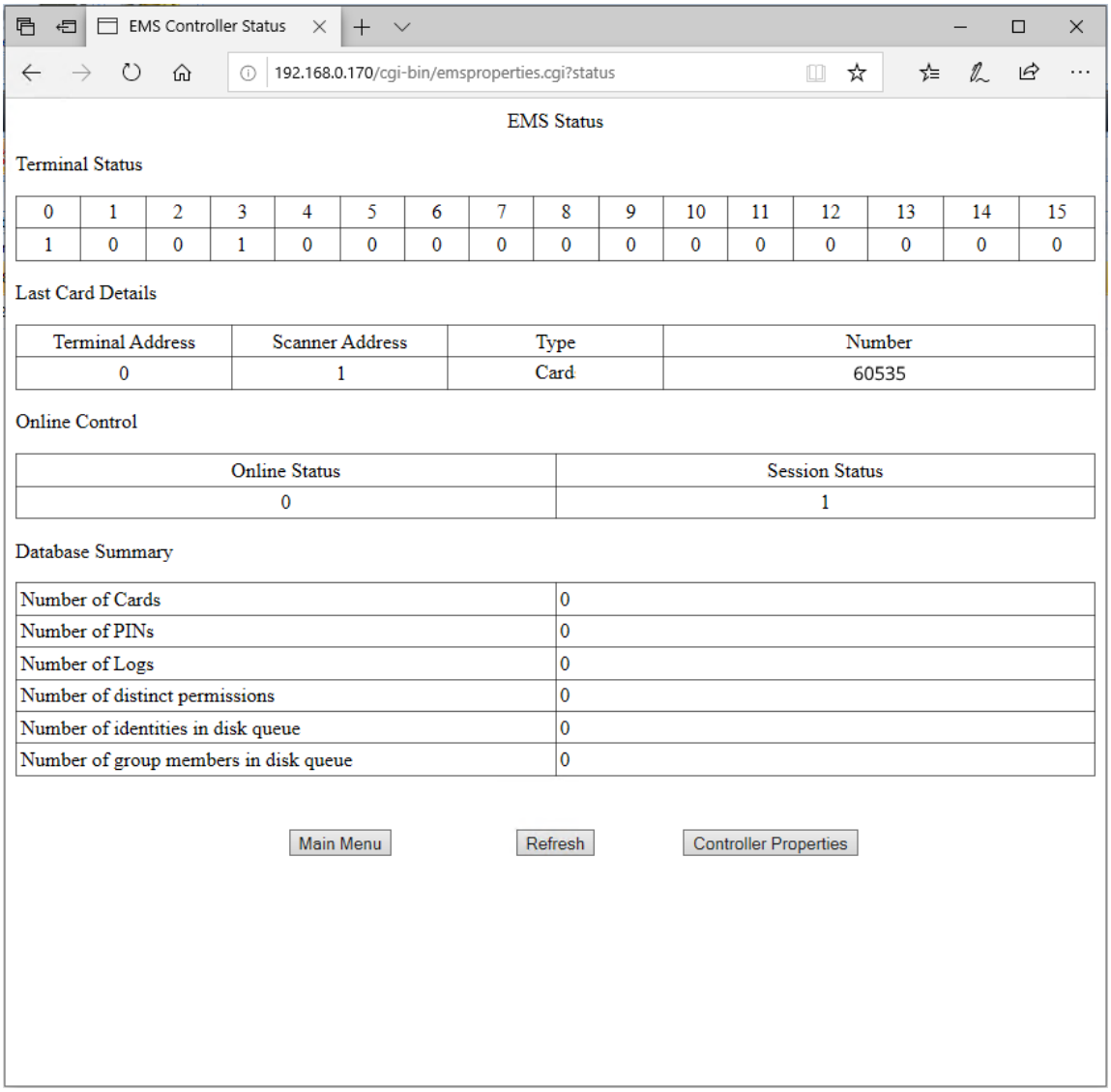
Card Data Length: **24 bit** indicates that the card number is truncated to 24 bits (plus parity). **Full Card Number** indicates that the whole card number is used (e.g. 34 bit, 47 bit, 56 bits).

Local Configuration Port: This must be at its default value unless instructed otherwise by Controlsoft Technical Support

Restrict Access to Facility Codes: This shows **Yes** if the controller is set to use site code data from the card. The following 10 fields indicate which site codes will be white listed in the controller.

© 2026 Controlsoft Ltd

i-Net Status



Terminal Status displays the devices connected to the iNet's RS485 bus. In this example, we have device address 0 (the Master iNet itself), and a device with address 1.

Last Card Details shows information on the last number read by the system. **Terminal Address** is the address of the device that read the number (0 being the Master iNet), **Scanner Address** is the Reader Port that the data came through, **Type** indicates whether the data is from a card or a PIN, **Number** indicates the card number / PIN read, **Site Code** indicates the facility code of the card that was read.

Local Control indicates whether the Controlsoft application on the iNet is Running. **Access Control Software - Session Status** will show if the iNet controller is connected to the Identity Access software.

Database Summary displays an overview of the configuration of the iNet, the **Number of Cards** and **Number of PINs**, the **Number of Logs** waiting to be uploaded and the **Number of Distinct Permissions** (if everyone has access to all

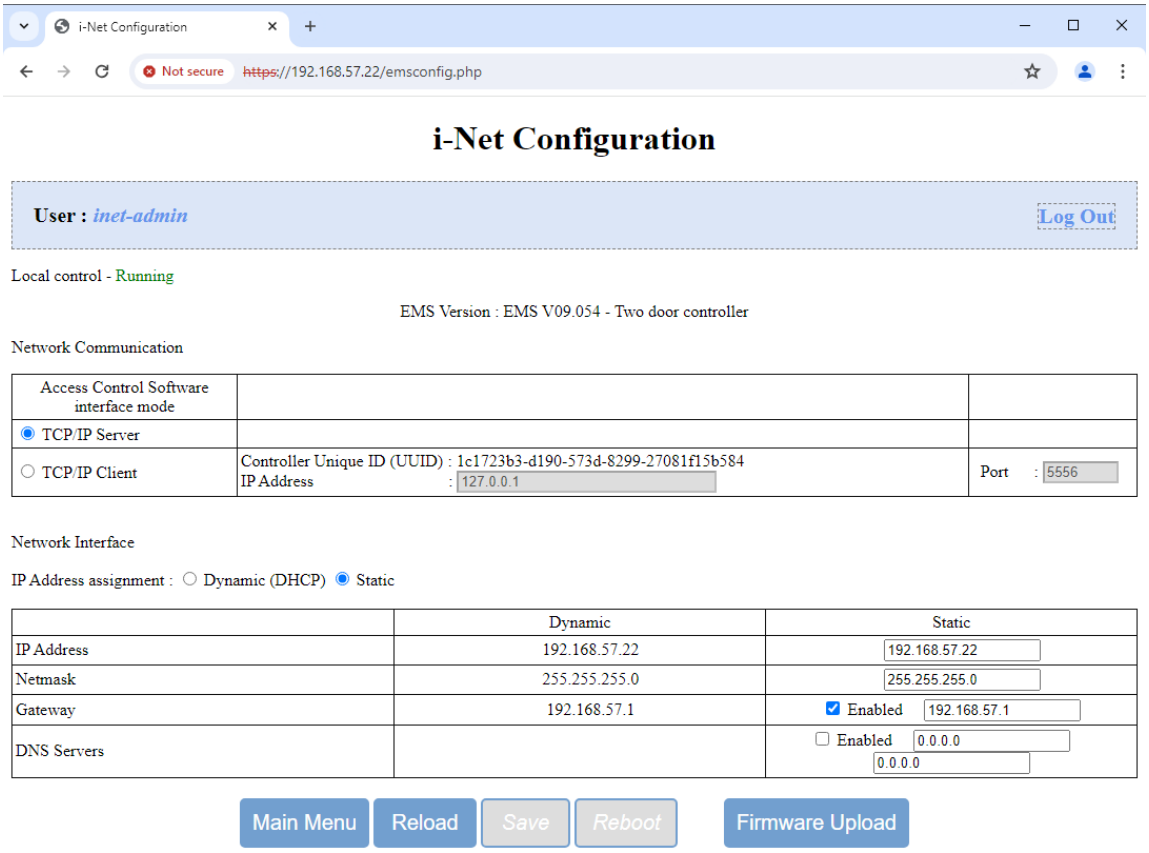
© 2026 Controlsoft Ltd

readers all the time, this is 1 distinct permission. If someone is then given access through 1 door in the mornings only, this will be a second distinct permission).

Number of identities in disk queue and **Number of group members in disk queue** relate to the number of users downloaded to the controller that have not yet been saved in the controller's database

NOTE: These displays are not live. To update the screen, simply press the [Refresh] button

i-Net Configuration



Access Control Software interface mode - this feature is not used with Identity Access V9 and should not be changed.

Network Interface allows you to manually update the controllers **IP Address**, **Netmask**, **Gateway** or **DNS Servers** settings.

Note: If Network Interface settings are changed a Save and Reboot is required for the changes to take affect.

Firmware Upload is used for updating the firmware of the iNet Controller. For more information on updating firmware see Knowledge Base: Performing iNet Controller Firmware Updates

© 2026 Controlsoft Ltd

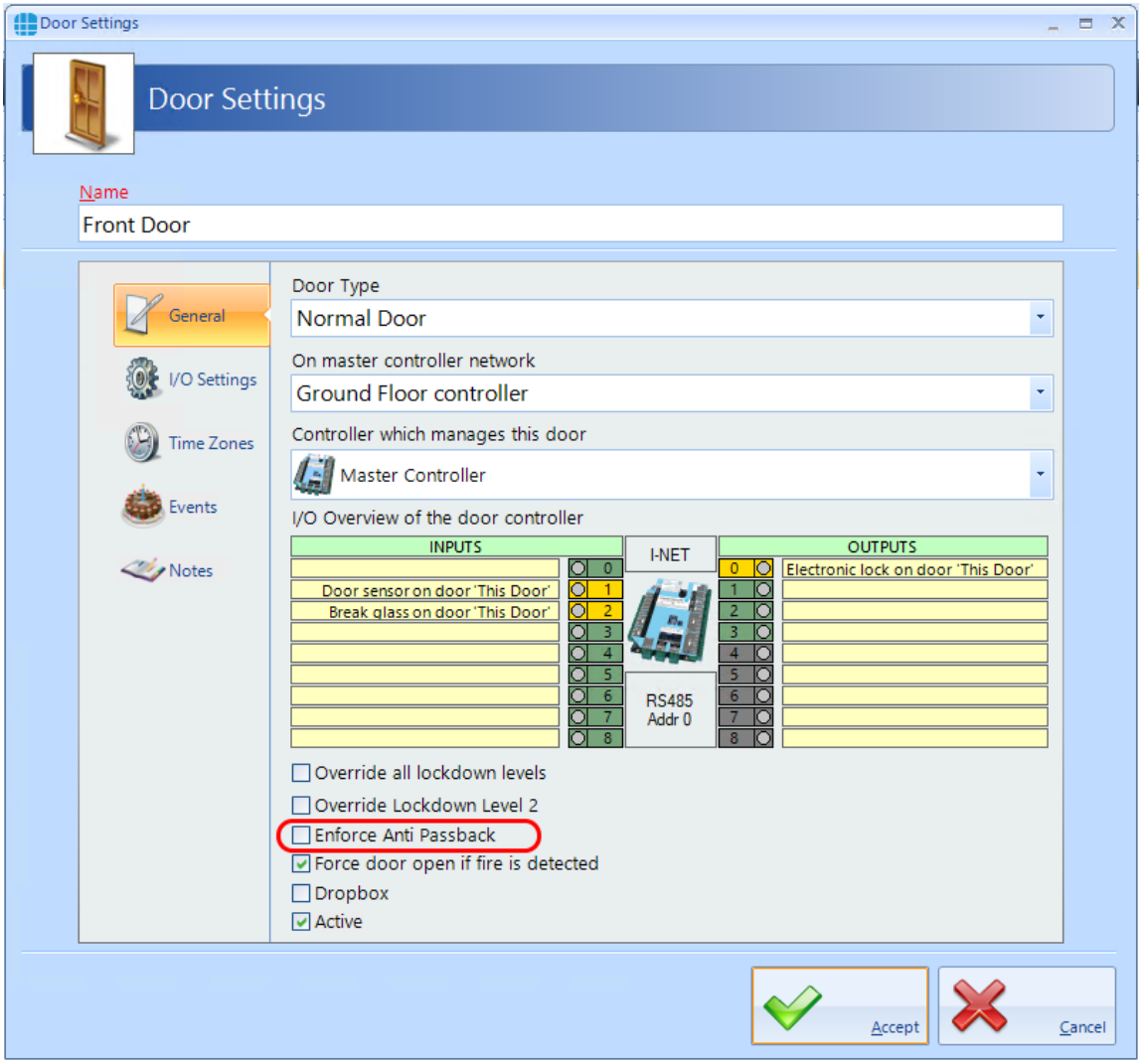
Appendix F - AntiPassBack

29 Appendix F - AntiPassBack

AntiPassBack is a feature available in Identity Access when a Professional or Enterprise Licence is installed which prevents illegal card movement when entering the building.

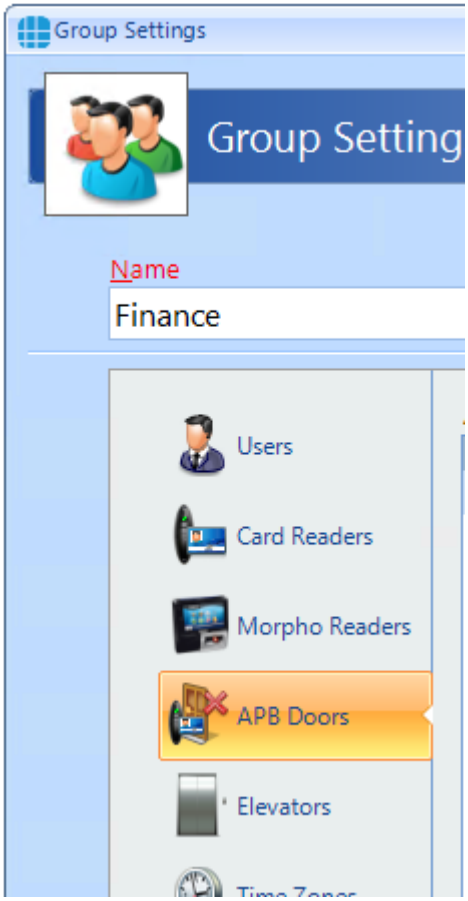
Consider the example where a token is used to move from outside to inside, then the user passes the token to someone else through an open window. When the second user attempts to use the same token to move from outside to inside, AntiPassBack will ensure that access is denied.

To use this feature, enable AntiPassBack for each external door,



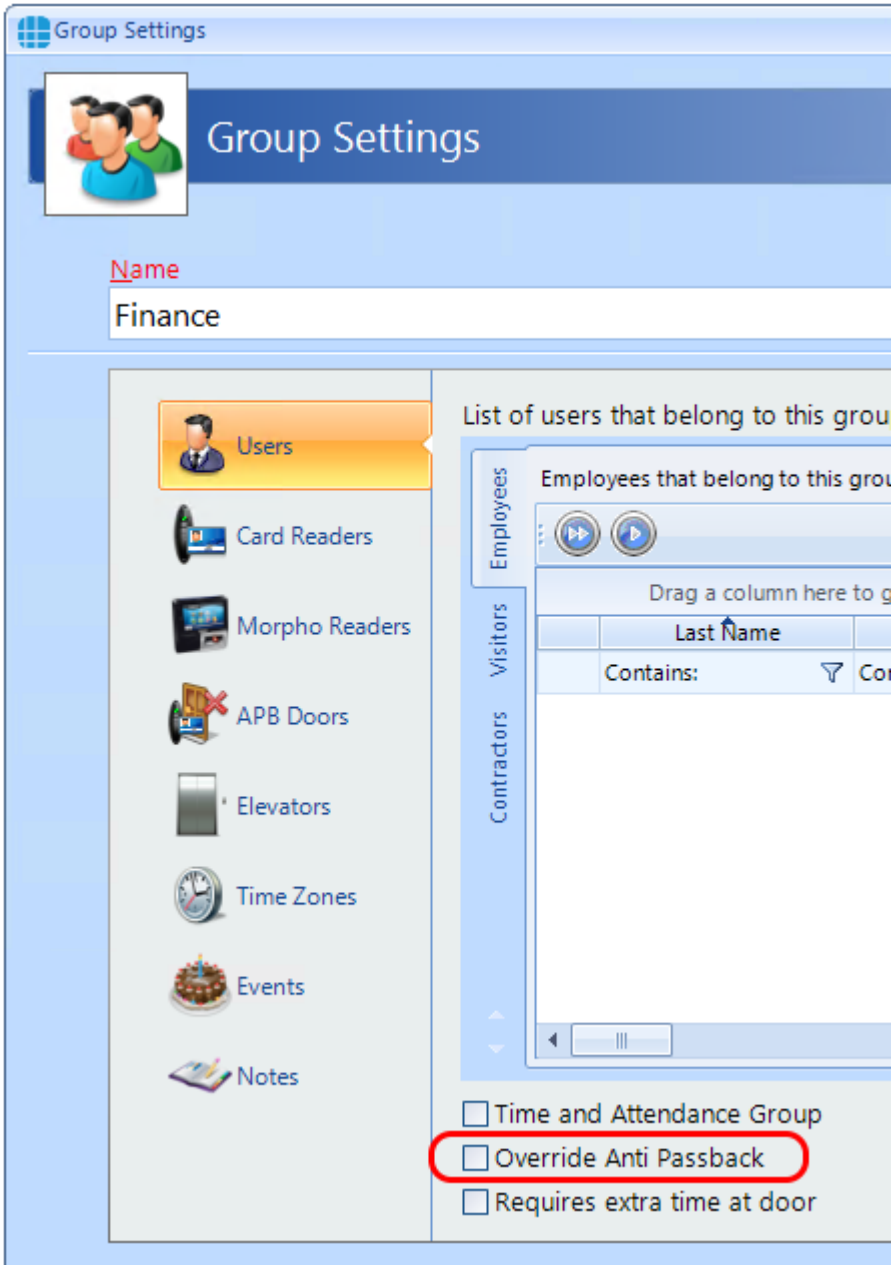
© 2026 Controlsoft Ltd

When allocating Access Rights for Groups, be sure to allocate **Card Readers** for doors without AntiPassBack, and **APB Doors** for doors with AntiPassBack



© 2026 Controlsoft Ltd

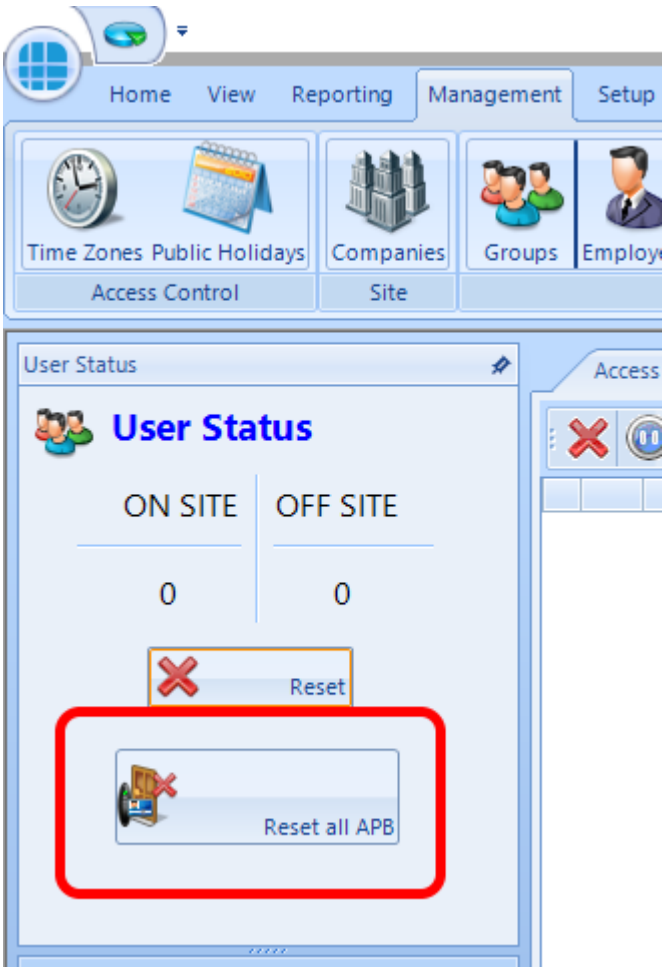
If any User Groups are to be exempt from AntiPassBack, select **Overide AntiPassback** for that Group.



If a user tailgates and finds themself in an incorrect AntiPassBack zone, it is possible to reset APB as follows:

To reset APB for ALL users - click the **Reset ALL APB** button in the dashboard:

© 2026 Controlsoft Ltd



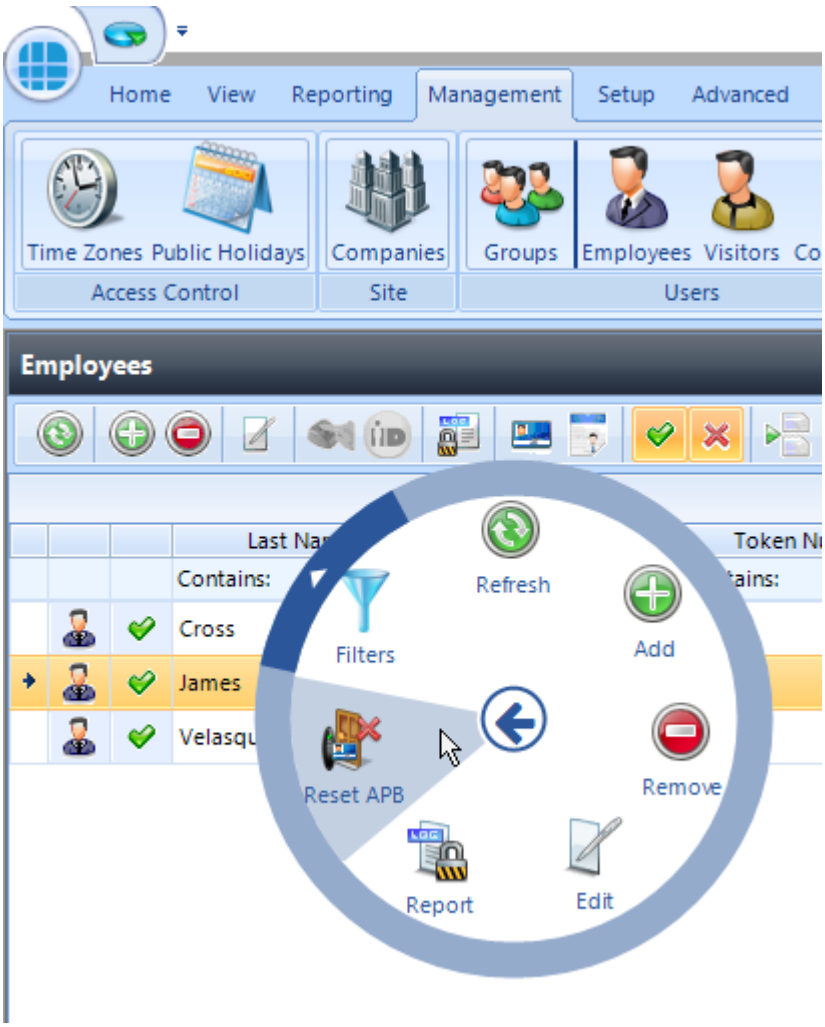
To reset APB for a group of users - select the appropriate group in the Groups manager screen and left click the mouse to display the option wheel, then select **Reset APB**:

© 2026 Controlsoft Ltd



To reset APB for an individual user - select the appropriate user in the Employee / Visitor / Contractor manager screen and left click the mouse to display the option wheel, then select **Reset APB**:

© 2026 Controlsoft Ltd



Finally, it is possible to automatically reset APB at a specific time each day. If this is selected for, say, 2am, it could prove useful to negate any tailgating while users leave the building each evening. This options is selected in the IA Configuration Services tab (see IA Configuration - Services) 277.

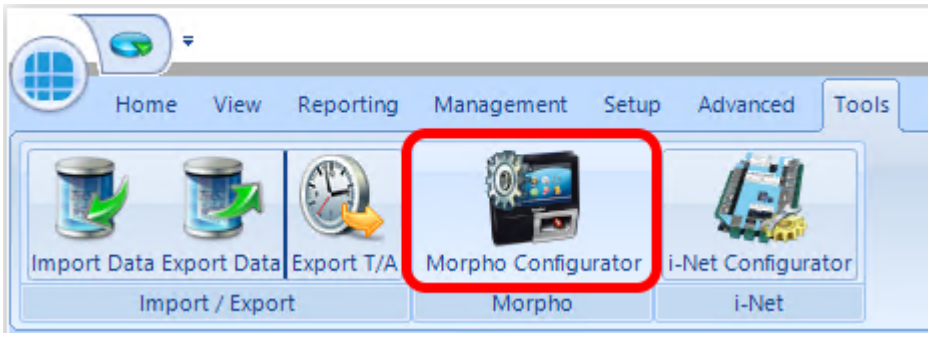
NOTE: Identity Access v9 DOES support AntiPassback across Master controllers, but ALL controllers MUST be fitted with firmware version 9.025 or later for this to work.
Older versions of Identity Access DO NOT support this feature.

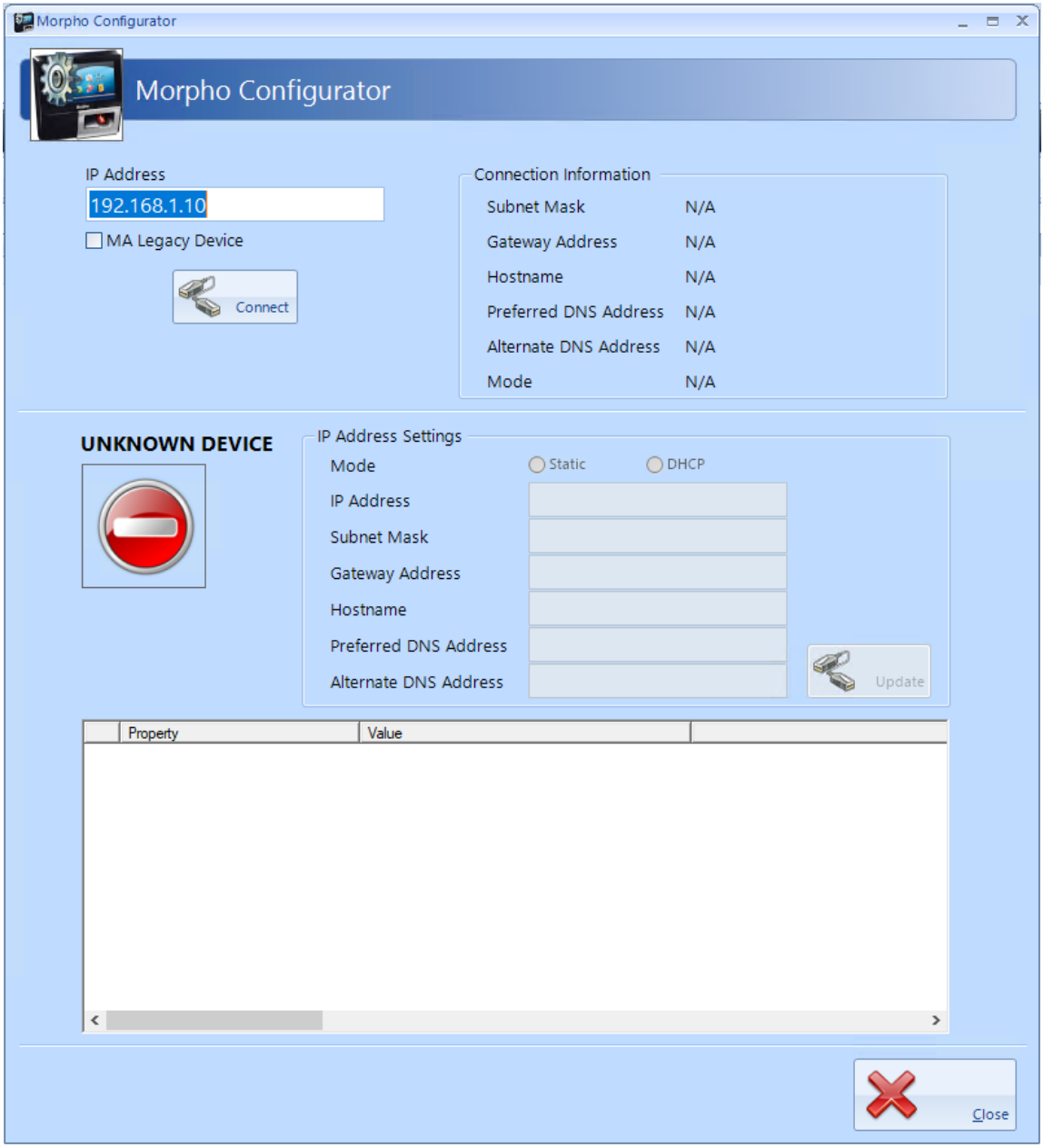
© 2026 Controlsoft Ltd

Appendix G - IA Morpho Configurator

30 Appendix G - IA Morpho Configurator

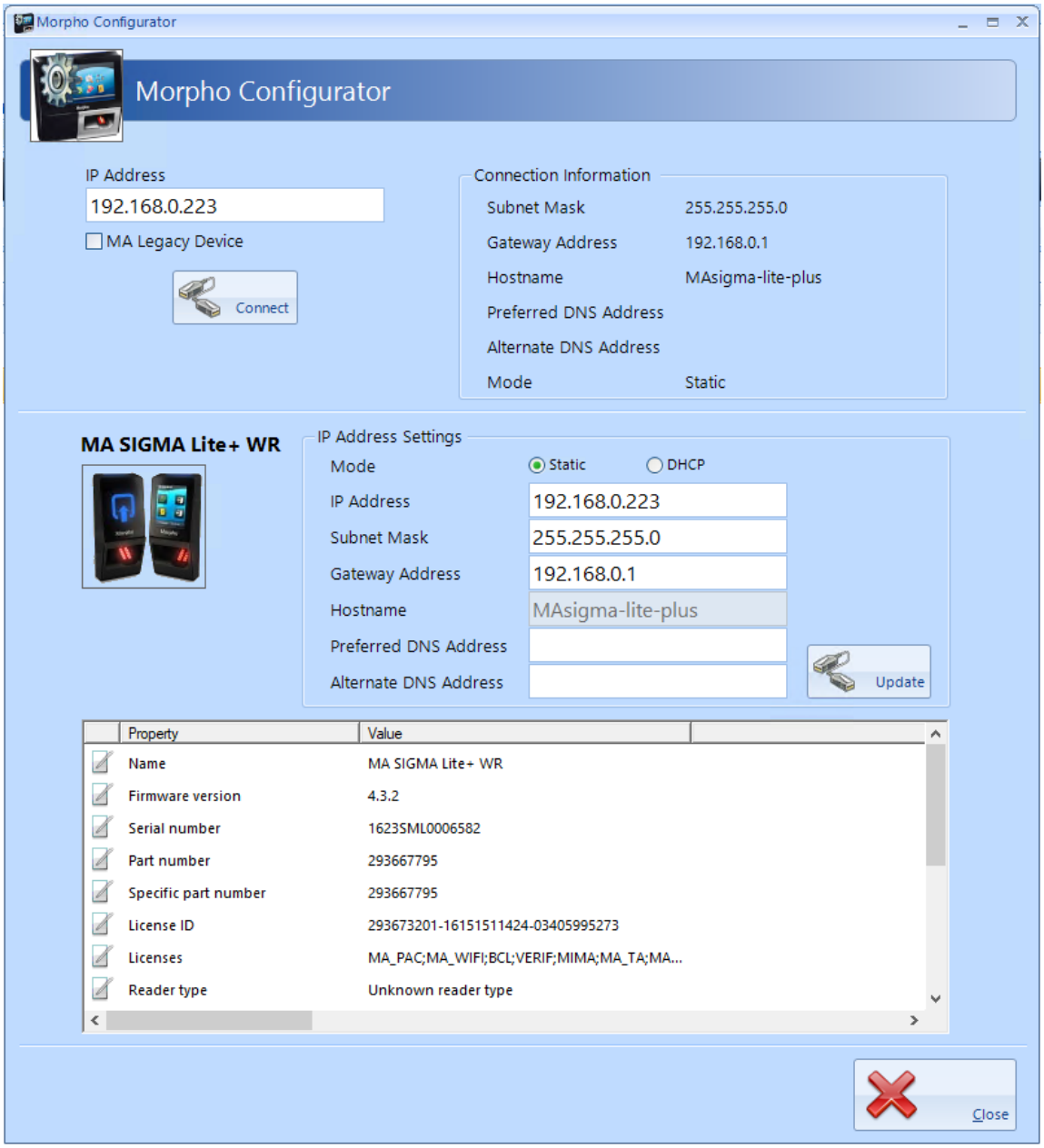
The IA Morpho Configurator is a small utility which is used to configure Morpho fingerprint readers. The utility can be run from the start menu by selecting **Start** > **Controlsoft** > **IA Morpho Configurator**, or from within Identity Access by selecting **Tools** followed by the **Morpho Configurator** button in the ribbon bar





© 2026 Controlsoft Ltd

Enter the **IP Address** of the fingerprint reader and click the **[Connect]** button



Connection Information provides details of the connection to the reader

IP Address Settings allows for changes to be made to the connection to the reader. Simply enter the required changes and click **[Update]**

The final window displays details of the reader itself, whether it has an integral reader, the firmware version, serial number etc.

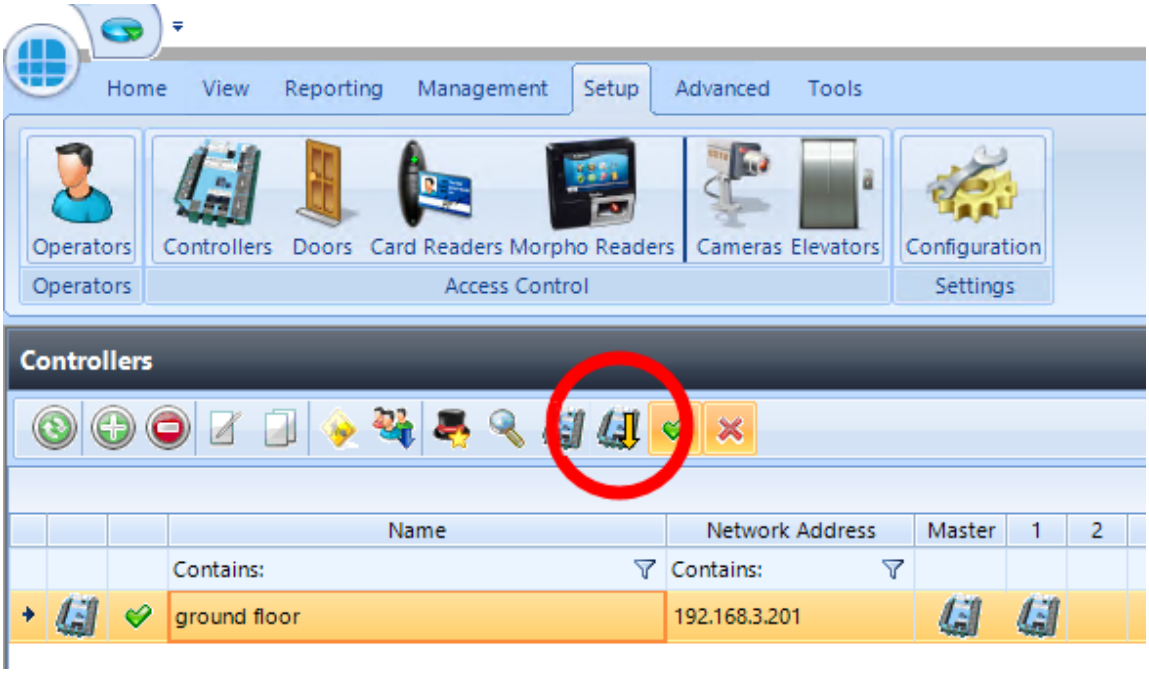
NOTE: The first four digits of the serial number is a manufacturing date code, in this example 1623 gives a manufacture date of 2016, week 23

© 2026 Controlsoft Ltd

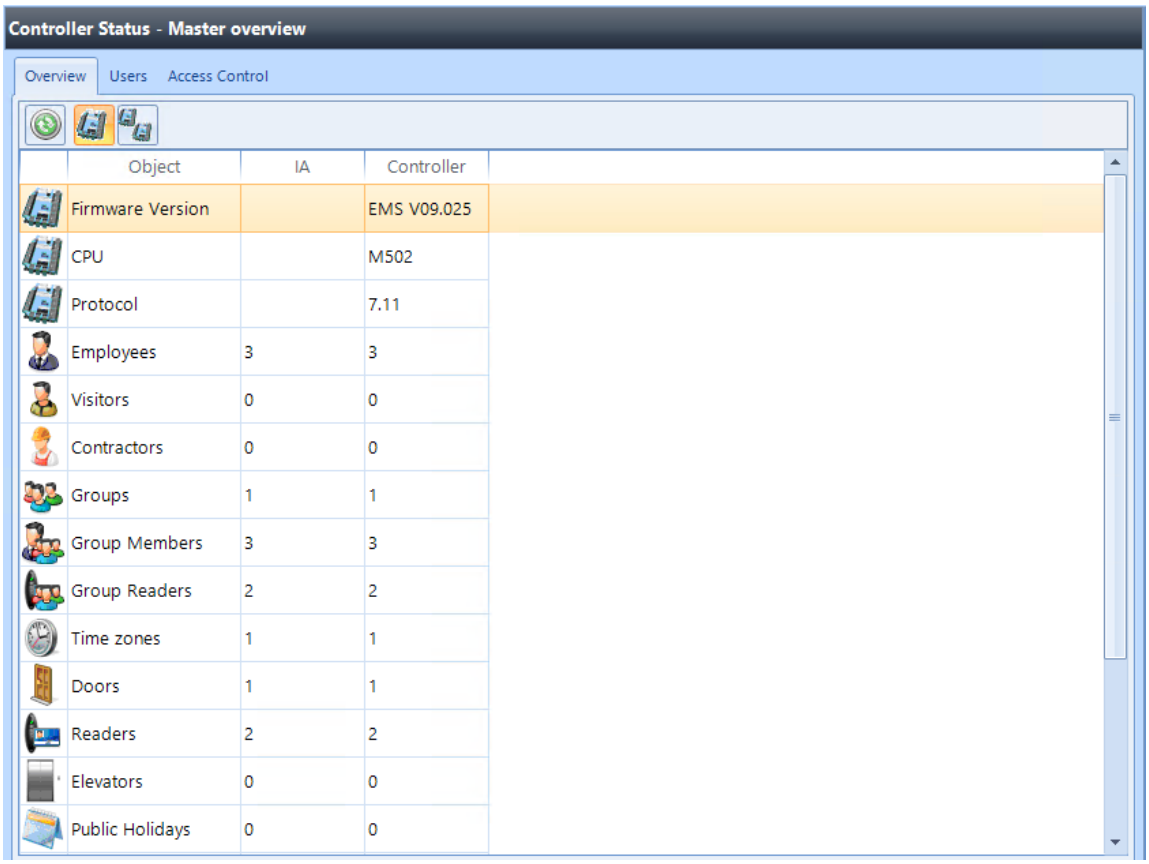
Appendix H - Controller Status

31 Appendix H - Controller Status

The Controllers status screen gives an overview of whether configuration data has been successfully transmitted to the Master and to the Downstream controllers. To access the Controller Status, select **Controllers** in the **System** menu, select the required controller and click the **Controller Status** button:



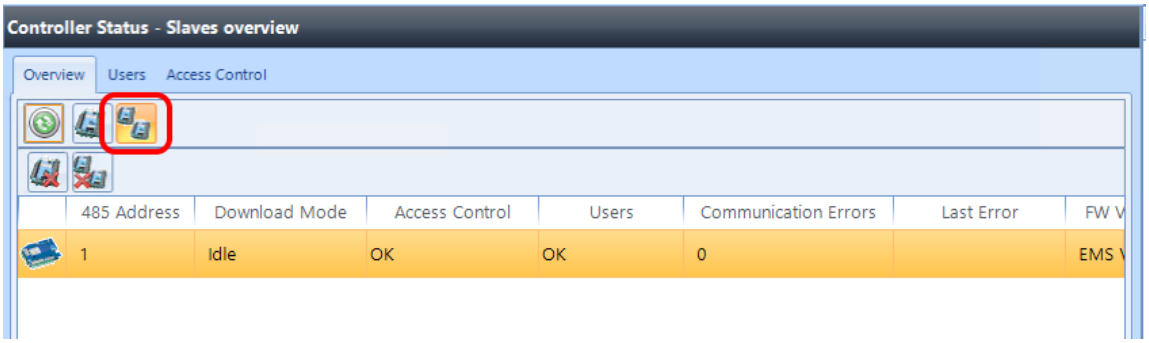
The Controller Status window will now appear on the left-hand side of the screen. Select the **Overview** tab then the **Master Controller** button:



© 2026 Controlsoft Ltd

The Master Overview screen shows the current configuration in the Identity Access database, and the same information in the Master Controller database. As can be seen from the above example, all data has been correctly downloaded.

The **Downstream Overview** button will display a list of the downstream controllers on the system and a number of status parameters:



RS485 Address – the address of each downstream controller on the bus

Download Mode – 'Idle' indicates that the downstream controller is fully operational. If the Master controller cannot communicate with the downstream controller, this status will show as 'Not Connected'

Access Control – 'OK' indicates that all access control configuration data has been correctly downloaded

Users – 'OK' indicates that all users have been correctly downloaded

Communication errors – this is a count of all communication errors between the Master and the downstream controller

Last error – the time and date of the last communication error

FW Version – this shows the firmware version in the downstream controller

FW Download Progress – when firmware is being sent to the downstream controller from the Master, this will show the progress

FW Download Started – this will show when the Master started to download firmware to the appropriate downstream controller. Knowing when the download started and the progress, it is possible to estimate the time remaining

CPU Type – this will display whether the downstream controller is fitted with an M502 processor board, or an older M501

Last Updated – this indicates when the Download Service received status data from the downstream controller

Two further buttons are available on this screen as shown below:

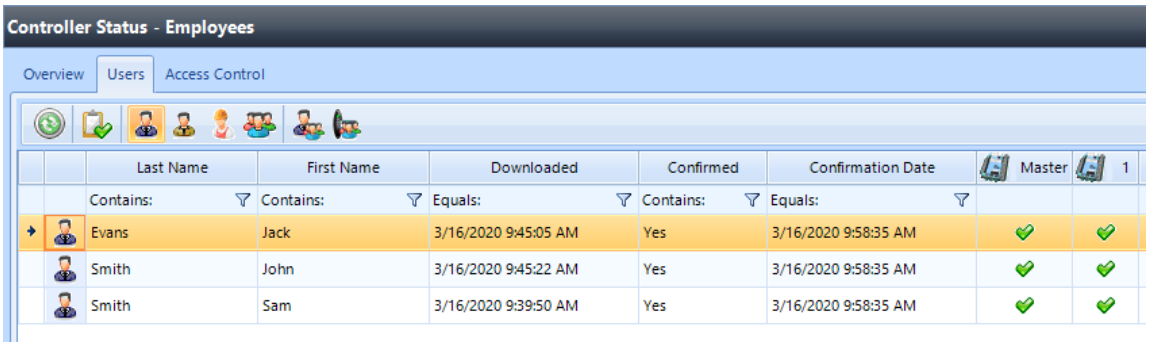
© 2026 Controlsoft Ltd



 - Clear communication errors on selected downstream controller

 - Clear communication errors on all downstream controllers

To access more detailed information on the downloaded data, click on the **Users** tab and click the refresh button :



The following information is now displayed:

The name of the employee

When the employee was downloaded

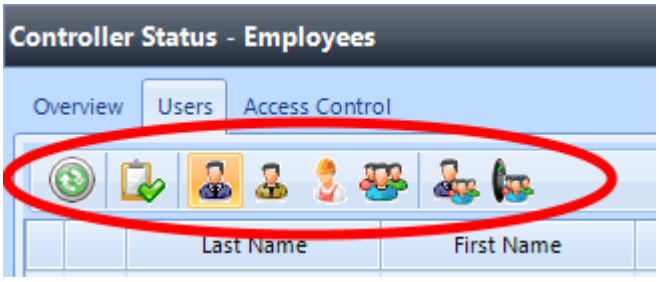
Whether the download has been confirmed as successful

When the download was confirmed as successful

Whether the employee exists in the Master and each downstream controller (users will not exist in a master/downstream controller if they have no access to any doors on that controller)

Eight buttons are provided for the following functions:

© 2026 Controlsoft Ltd



 - updates the display at any time

 - if an employee is showing as NOT Confirmed, this button will send a confirmation request to check that the employee has been successfully updated

 - displays a list of employees

 - displays a list of visitors

 - displays a list of contractors

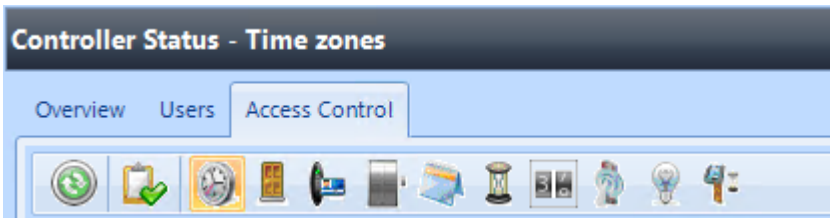
 - displays a list of groups

 - displays a list of users in each group

 - displays a list of the readers in each group

To view whether configuration data has been successfully downloaded, click on the **Access Control** tab and click the refresh button .

Twelve buttons are now available to check the downloaded status of different information:



 - updates the display at any time

 - if a door is showing as NOT Confirmed, this button will send a confirmation request to check that the door has been successfully updated

© 2026 Controlsoft Ltd

 - displays a list of time zones on the system and whether they have been successfully downloaded

 - displays a list of doors on the system and whether they have been successfully downloaded

 - displays a list of readers on the system and whether they have been successfully downloaded

 - displays a list of elevators on the system and whether they have been successfully downloaded

 - displays a list of public holidays on the system and whether they have been successfully downloaded

 - displays a list of timers on the system and whether they have been successfully downloaded

 - displays a list of counters on the system and whether they have been successfully downloaded

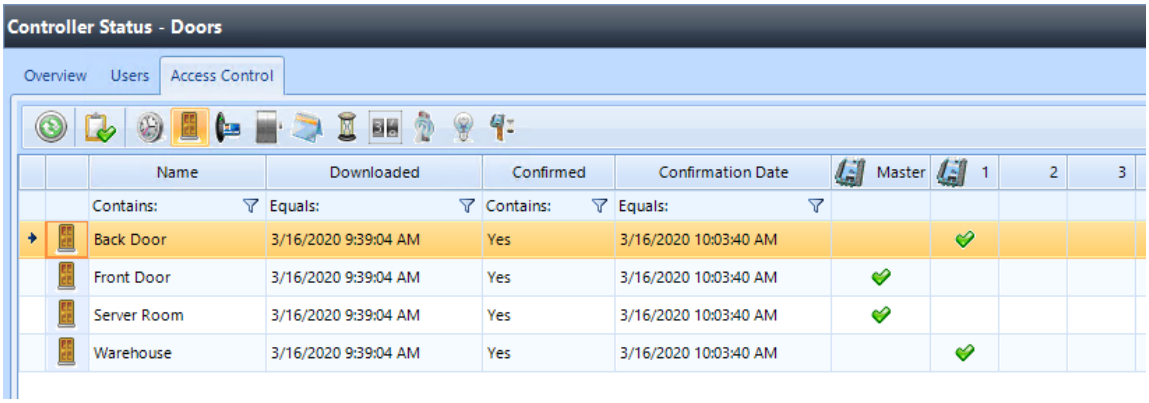
 - displays a list of inputs on the system and whether they have been successfully downloaded

 - displays a list of outputs on the system and whether they have been successfully downloaded

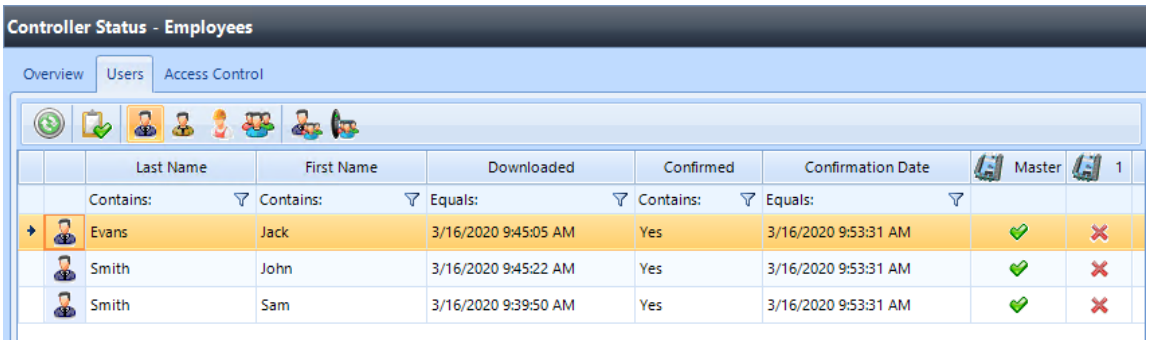
 - displays a list of object groups on the system and whether they have been successfully downloaded

The example below shows that the Front Door and the Server Room are associated with the Master controller whereas the Back Door and Warehouse are associated with downstream controller 1. The data for all 4 doors have been confirmed as successfully downloaded.

© 2026 Controlsoft Ltd



The second example below shows that the 3 users have been downloaded to the master controller, but have not been forwarded to the downstream controller



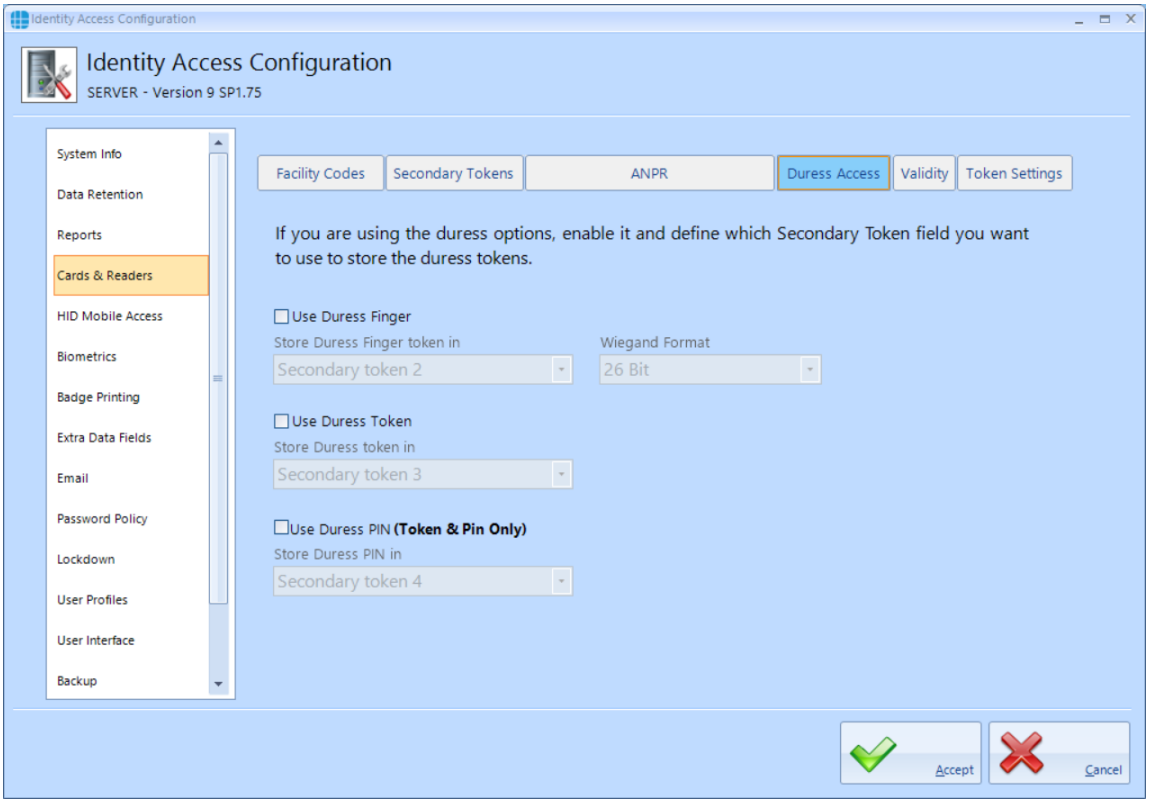
© 2026 Controlsoft Ltd

Appendix I - Duress

32 Appendix I - Duress

Duress was implemented in Identity Access 9.1.48, the operation of which is described below:

to use Duress, first enable the feature in the IA Configuration | Cards & Readers | Duress Access



For Duress via a fingerprint reader, tick the box **Use Duress Finger** and define which Secondary Token field will be used for the duress finger (the default is Secondary Token 2 but any unused field can be selected)

For Duress via an alternative token, tick the box **Use Duress Token** and define which Secondary Token field will be used for the duress finger (the default is Secondary Token 3 but any unused field can be selected)

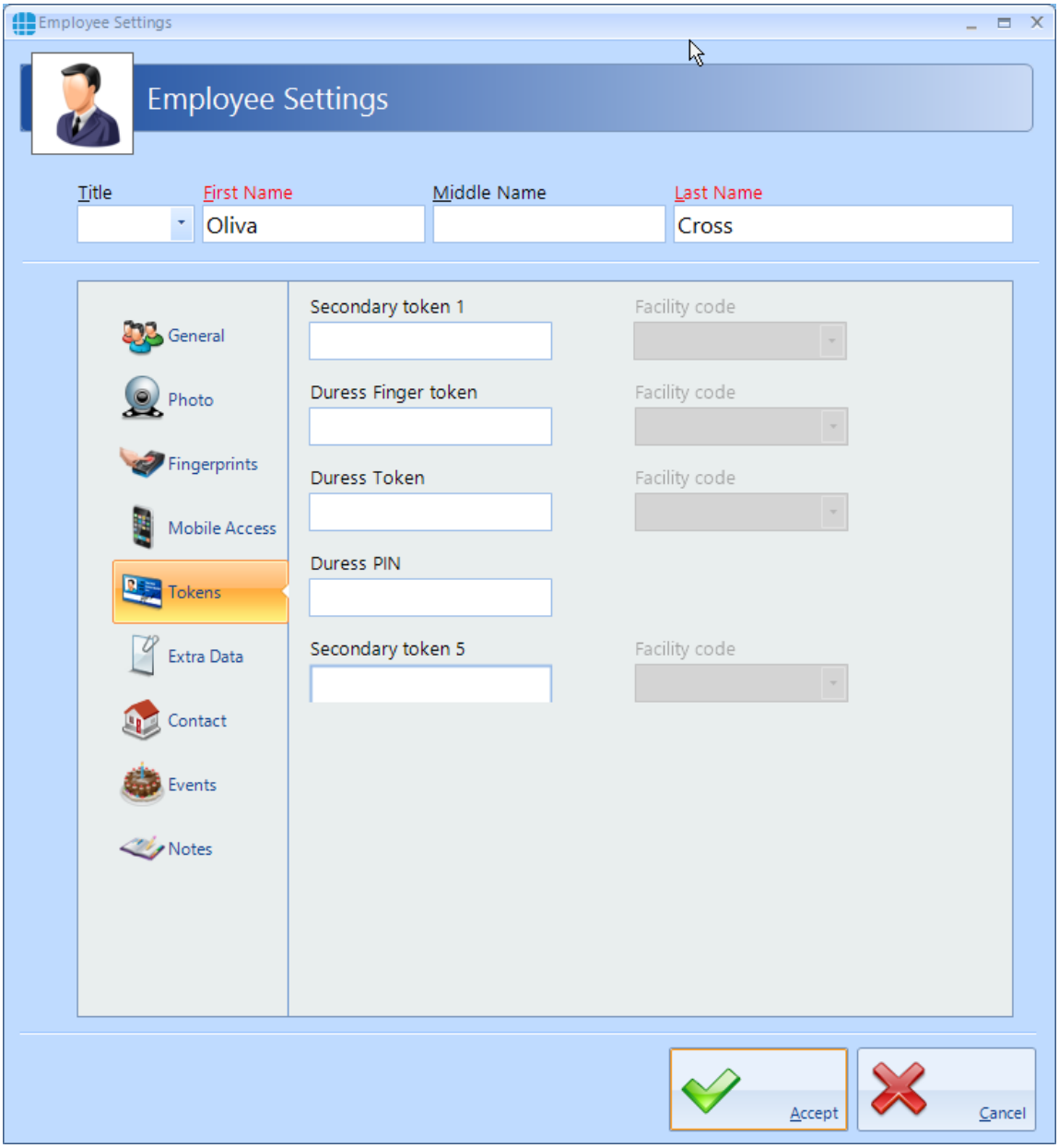
For Duress via an alternative PIN (when access via Token AND PIN is selected), tick the box **Use Duress PIN** and define which Secondary Token field will be used for the duress finger (the default is Secondary Token 4 but any unused field can be selected)

Click on **Accept** to save the changes.

NOTE: When access via Token AND PIN is selected, duress can be generated using your normal Token and the Duress PIN.

Once Duress is selected, duress information must be entered per user using the Secondary Token tab in the Employee Settings screen:

© 2026 Controlsoft Ltd



Duress Finger token will be filled in automatically when a duress finger is enrolled

Duress Token needs to be enrolled for a token to be used for duress

If one or more card readers have the **Reader has a PinPad attached** option selected , use the **Duress PIN** field to enter an alternate PIN which will generate a duress when used in conjunction with the usual token.

NOTE: Duress is only applicable to Employees, and does not work for Visitors or Contractors.

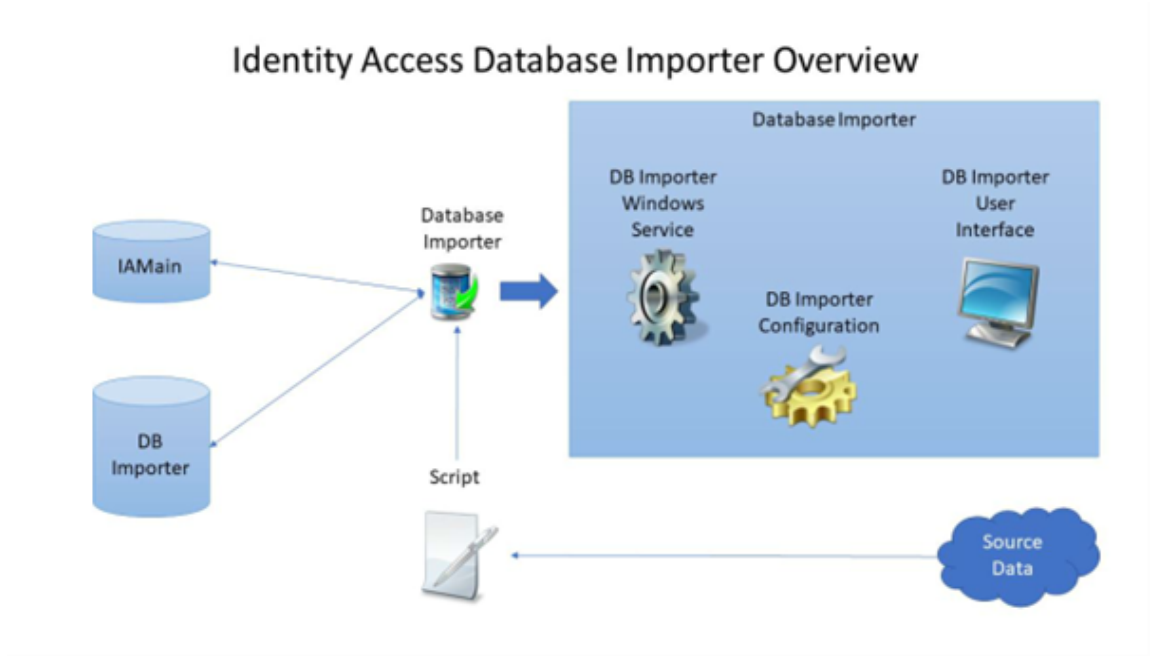
© 2026 Controlsoft Ltd

Appendix J - Database Importer

33 Appendix J - Database Importer

The Identity Access Database Importer is an application designed to import personnel data from a third-party data source into Identity Access. Employees, contractors or visitors could be created, deleted or amended in sync with the customers primary data source.

The data source is managed via a .Net script so it can be anything from a text file to a database table. The import is executed on a configurable schedule and the source data is transformed to match the requirements of Identity Access. The Identity Access Database Importer enables third party software to be the primary or a supplemental employee-manager for Identity Access.



The three main components in the import system are Identity Access, Database Importer and the Source data.

The source data can be retrieved from any data source that can be accessed using .NET, for example, CSV Files, SQL Server database, REST API's, etc – almost any DataSource that can be opened by .NET. In addition, it is possible to access data from a 3rd party application.

The Identity Access Database Importer must be installed on a machine where Identity Access (Server) is already installed. The installer will let you know if Identity Access is not installed and then terminate the installation. The source data, however, may reside on a separate machine connected to the same LAN or WAN, or even cloud storage.

The .NET script defines which data elements are read from the source data, and the system configuration defines how frequently the data is read, which can be between 1 minute (5 minute recommended) and 24 hours. This data is then used to populate the Database Importer database, which is an intermediate database, from which data is accessed by Identity Access.

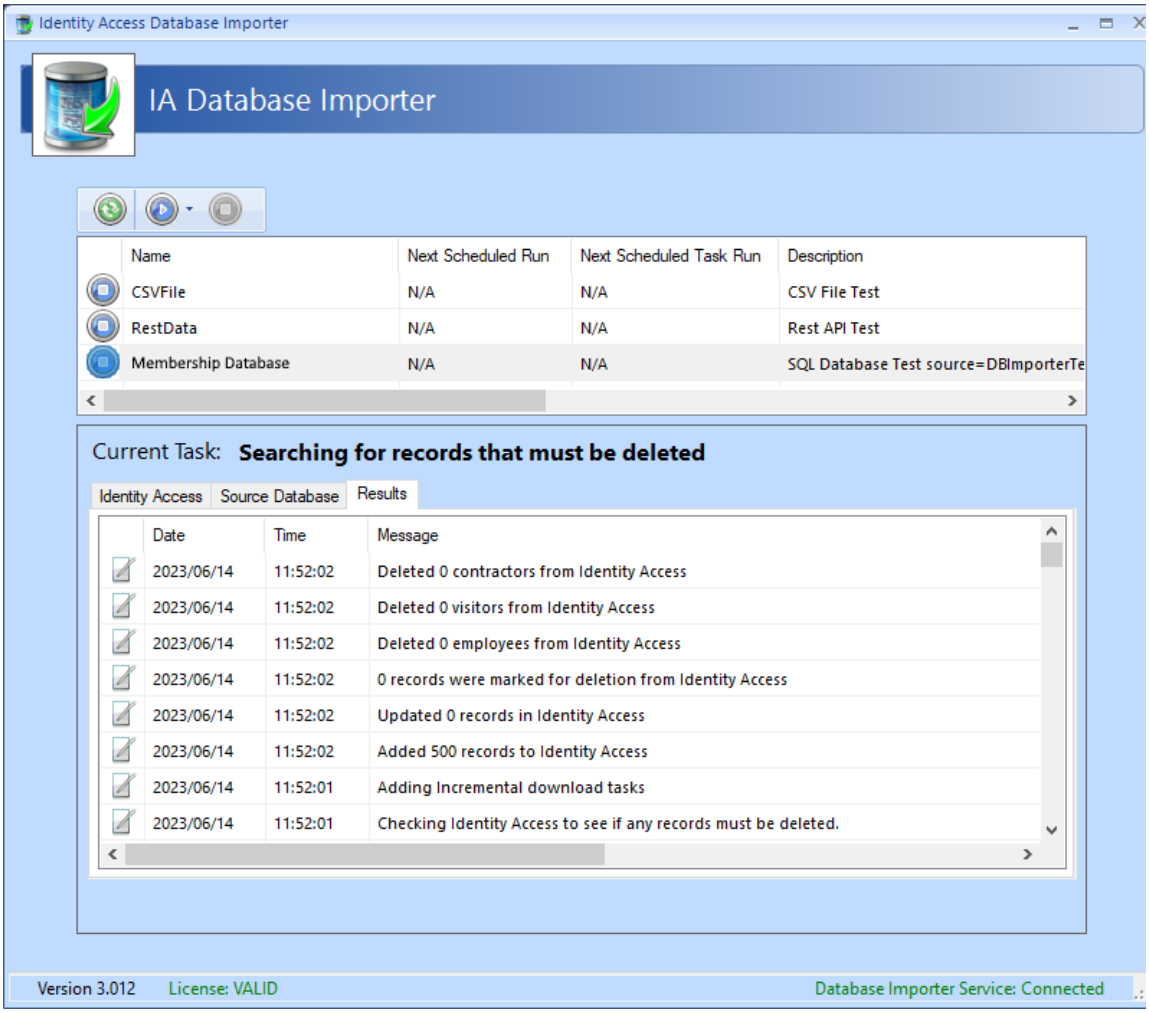
© 2026 Controlsoft Ltd

NOTE: DBimporter only requires read accesses to the source data. DBimporter never writes or changes the source data.

As well as importing user data, Database Importer can also import defined tasks. This feature, would allow, for example, an on-screen button on the source data system, to trigger an event (such as opening a specific door) on the Identity Access system, further enhancing the flexibility of the integration.

Whilst the software installation is a straightforward process, configuring the system via the .NET script can be more complex, as there are numerous options on how to access the various data elements from the valid source data formats. For example, the source data could be:

- SQL database (e.g. a membership system)
- Oracle database
- CSV File
- REST API



© 2026 Controlsoft Ltd

If you are interested in integrating Database Importer into your Identity Access system, please contact Controlsoft Technical Services on 01451-844896, or email support@controlsoft.com

33.1 Installing Database Importer

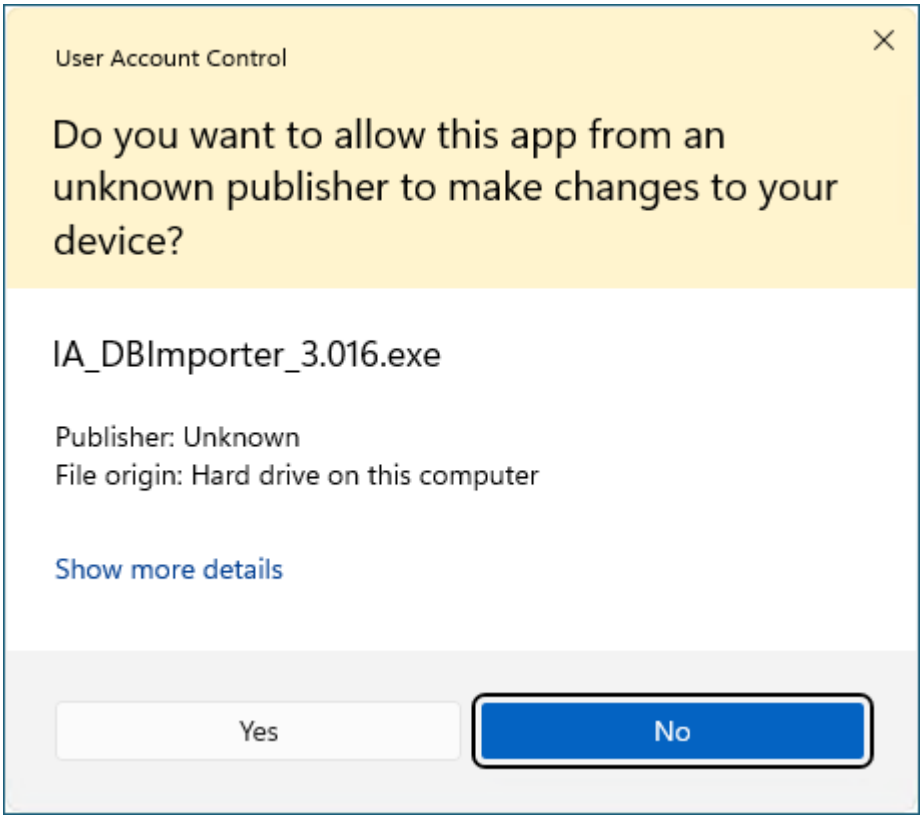
1. If you do not have a copy of Database Importer, ensure you are registered at www.controlsoft.com/login and request a copy of Database Importer from our helpdesk by emailing support@controlsoft.com from your company email account.

2. Ensure Identity Access is fully installed, as per the Identity Access - Express Commissioning Guide 18

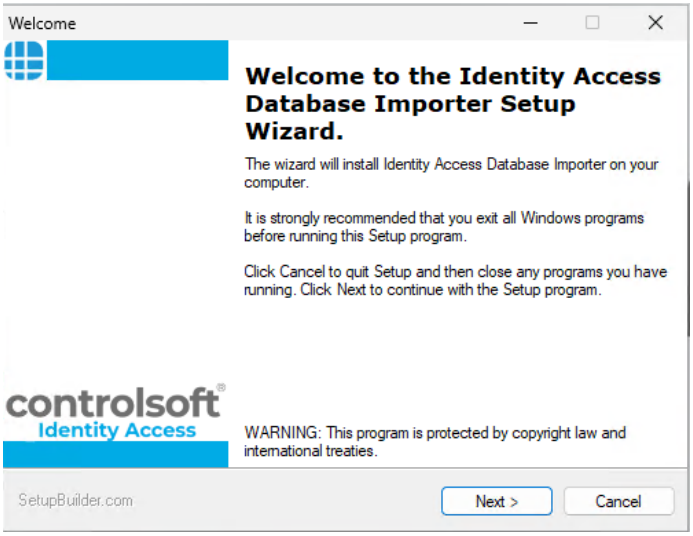
2. Place of a copy of the installation files onto the PC with Identity Access installed.

© 2026 Controlsoft Ltd

3. Double Click the installation media and click yes to the User Account Control prompt.

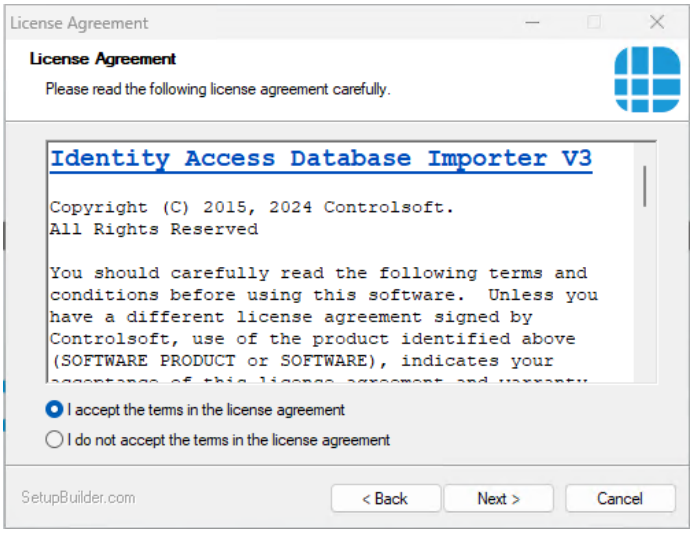


4. Click Next on the **Welcome to the Identity Access Database Importer Setup Wizard.**

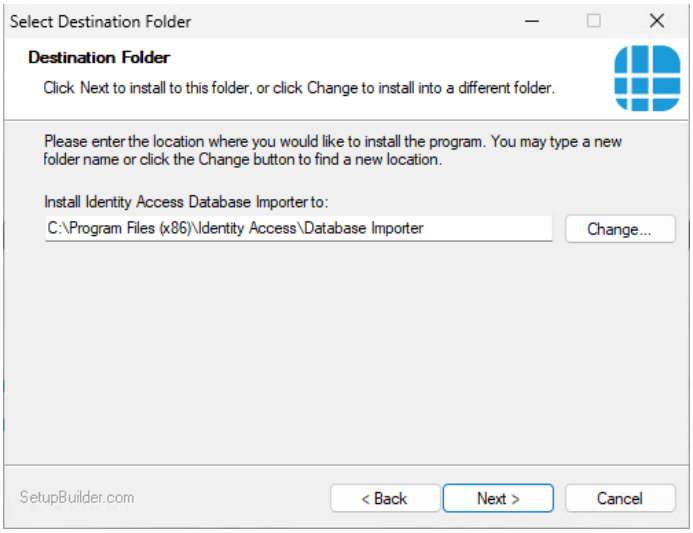


5. Read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**

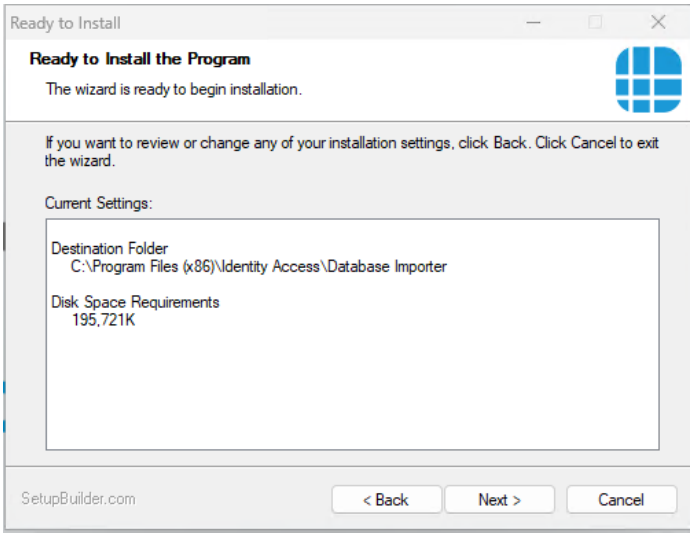
© 2026 Controlsoft Ltd



6. It is recommended to leave the installation location as default and click **Next.**

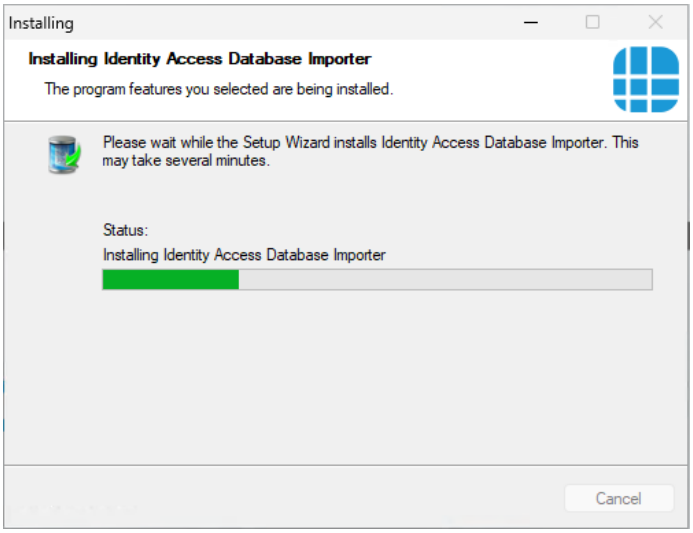


7. Review the location and size of the installation and click **Next** to start the installation.

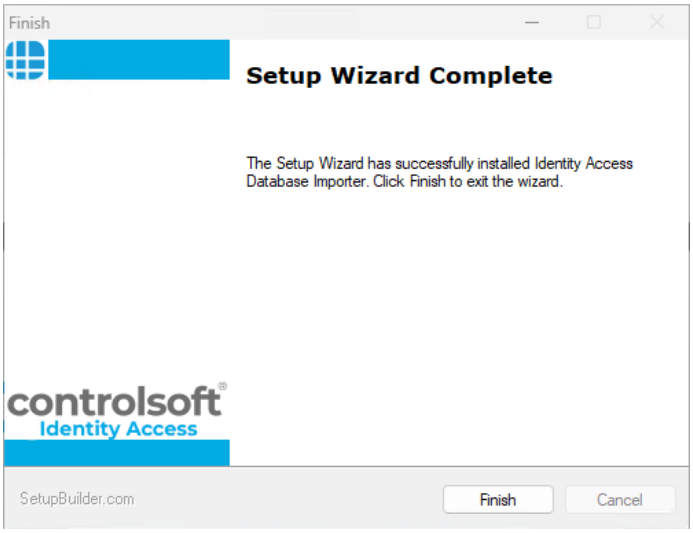


8. The Database Importer will now install.

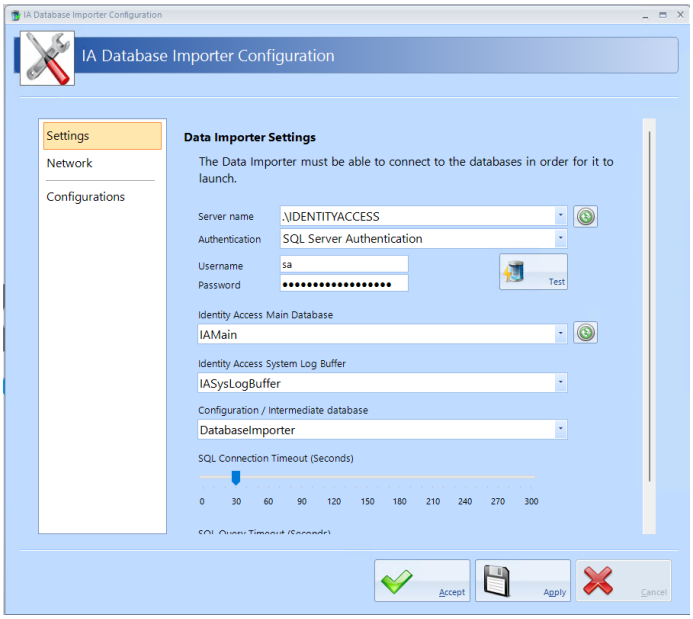
© 2026 Controlsoft Ltd



9. Once complete click Finish



10. Press the Test button to ensure Database Import Configuration has correctly connected to the Identity Access Server.



© 2026 Controlsoft Ltd

11. Press Apply and Save. Reboot the server to complete the installation process.

© 2026 Controlsoft Ltd

Appendix K - Identity Access Web Client

34 Appendix K - Identity Access Web Client

The Identity Access Web Client is a web based application suitable for desktop and mobile devices that allows for remote system management from anywhere in the world for the following features, it can also be used in place of installing Identity Access for users that do not need the full feature set:

- Adding/Editing users
- Disablement of users.
- Event Monitoring
- Open/Close and Granting Access to Doors

The Identity Access Web Client requires an Identity Access Professional or Enterprise license to be enabled.

Click here for information on how to enable and use the Identity Access Web Client.

© 2026 Controlsoft Ltd

Appendix L - Site Selector

35 Appendix L - Site Selector

Site Selector enables our partners to manage our Identity Access software as a service. The software server can be hosted either on premises or in the cloud. All access control functions are managed through a single centralized client workstation which can connect to up to 100 different sites. This enables our end users to outsource the manual tasks related to access control, like granting or revoking user permissions, monitoring alarms and running reports for various end users within the same Identity Access Client interface.

Site Selector also eliminates the need for on site PC equipment, OS licenses and IT staff time.

Click Here For more information on how to configure Site Selector

© 2026 Controlsoft Ltd

Appendix M - Licence Terms & Conditions

36 Appendix M - Licence Terms & Conditions

Identity Access Version 9

Copyright (C) 2015, 2024 Controlsoft.
All Rights Reserved

You should carefully read the following terms and conditions before using this software. Unless you have a different license agreement signed by Controlsoft, use of the product identified above (SOFTWARE PRODUCT or SOFTWARE), indicates your acceptance of this license agreement and warranty.

GRANT OF LICENSE.
1. Controlsoft grants to the user a limited, non-exclusive, non-transferable, royalty-free license to use one copy of the executable code of the SOFTWARE PRODUCT on a single CPU residing on the user's premises.

2. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

3. The user shall not rent, lease, sell, sublicense, assign, or otherwise transfer the SOFTWARE PRODUCT, including any accompanying printed materials (if any). The user may not reverse engineer, decompile or disassemble the SOFTWARE PRODUCT except to the extent that this restriction is expressly prohibited by applicable law.

4. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

DISCLAIMER OF WARRANTY
THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OF MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. Because of the various hardware and software environments into which the SOFTWARE PRODUCT may be put, NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.

ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

Appendix N - Glossary

37 Appendix N - Glossary

AC-3151 - A Reader Expander Board providing 4 inputs, 2 output relays and 2 reader ports, capable of supporting 2 doors with IN readers or 1 door with IN and OUT readers. The AC-3151 connects to the Master iNet via the RS485 343 bus.

IOC - An I/O Expander Board providing 8 inputs and 8 output relays. The IOC connects to the Master iNet via the RS485 343 bus.

Administrator - An Operator who is authorised to use all functions within the Identity Access software.

Contractor - A temporary User with a token 343 or fingerprint which allows access to the system.

Door Forced - Unauthorised opening of a door.

Door Held - Detection that a door has not closed within a defined time after access has been granted.

Download - The process of transferring configuration data from the Identity Access software to the iNets 342.

Download Service - Software which manages the communications between the Identity Access software and the controllers.

Employee - A User with a token 343 or fingerprint which allows access to the system.

Enrolment Reader - A reader that connects to the PC via USB, used to read the token number when creating new users.

Facility Code - The Facility Code option embeds a hidden number on the card as well as the card number. Controllers can then be given the ability to accept up to 10 Facility Codes. This could be useful for large systems whereby doors at Office A will only accept cards from employees from Office A, doors from Office B will only accept cards from employees from Office B but the doors at the Head Office will accept cards from all 3 sites.

Format - The process of clearing the memory in one or more controllers.

Groups - A number of Users sharing the same access rights (reader allocation, time zones etc.).

IP Address - A unique address allocated to every IP device on the network. ***NOTE: The iNet is configured as default to DHCP (it gets an IP Address from the router), but it can be reset to IP Address 10.0.1.230.***

iNet 1DR - A controller providing 5 inputs, 4 output relays and 2 reader ports, capable of supporting 2 doors with IN readers or 1 door with IN and OUT readers.

iNet 2DR - A controller providing 9 inputs, 4 output relays and 2 reader ports, capable of supporting 2 doors with IN readers or 1 door with IN and OUT readers.

© 2026 Controlsoft Ltd

Log Service - Software which manages all Access events, System events and T&A events, and stores them in the relevant database files.

MAC Address - A unique number programmed into every IP device by the manufacturer to help identify it on the network (example 0013480252D6). ***NOTE: MAC addresses for older iNets start with 001348, whereas 1DR and 2DR iNets start with F8DC7A or 540BB6***

Master iNet: An iNet controller connected to the software via an IP connection. ***NOTE: Master iNets MUST be configured with RS485 Address = 0 on the rotary switch.***

Offline Event Log - Memory in the Master controllers used to record events when communication to the Download Server is lost. Once communications has been restored, events are transferred from the Offline Event Log to the Identity Access database.

Operator - Someone who is authorised to use the Identity Access software. Operators can be assigned Administrator 342 rights to allow them full access to all software features.

Rebuild - The process of transmitting ALL configuration data and user database from the Download Server to one or more controllers.

RS485 - A proprietary bus used to connect the Master iNet to Downstream iNets or Expanders. Each device on the RS485 bus must be configured with a unique address to identify itself.

Downstream Expander - A reader expander, I/O expander or reader connected to a Master iNet 343 via an RS485 343 connection (AC-3151 342 or IOC 342).

Downstream iNet - An iNet 342 controller connected to a Master iNet 343 via an RS485 343 connection.

Time Zones - Periods that can be allocated to User Groups or doors which limit access depending on the selected period.

Token - A card or tag used at a reader to identify a User.

Turnstile - A device fitted in a doorway which restricts passage to one User at a time in a specific direction.

Update - The process of transmitting recent configuration changes and/or changes to the user database from the Download server to one or more controllers.

Upload - The process of transferring events from the iNets to the Identity Access software.

User - A collective term to include Employees, Visitors and Contractors.

Visitor - A temporary User with a token or fingerprint which allows access to the system.

© 2026 Controlsoft Ltd

© 2026 Controlsoft Ltd

Controlsoft Contact Details

38 Controlsoft Contact Details

Corporate Office:
Controlsoft Limited
Security House, 82C Chesterton Lane, Cirencester, Gloucestershire, GL7 1YD

Sales:
Tel: +44 (0)1451 844896
Email: sales@controlsoft.com

Technical:
Tel: +44 (0)1451 844896
Email: support@controlsoft.com

South Africa Office:
Controlsoft (Pty) Ltd
Block 1, Pendoring Office Park, 299 Pendoring Road, Blackheath, Randburg, 2195

Sales:
Tel: +27 (0)11 792 2778
Email: zasales@controlsoft.com

Technical:
Tel: +27 (0)10 595 1266
Email: support@controlsoft.com

US Office:
Controlsoft Access Inc
811 Boyd Ave., Suite 205, Pittsburgh, PA 15238

Sales:
Tel: +1-800-340-1407
Email: namsales@controlsoft.com

Technical:
Tel: +1-800-340-1407
Email: support@controlsoft.com

© 2026 Controlsoft Ltd