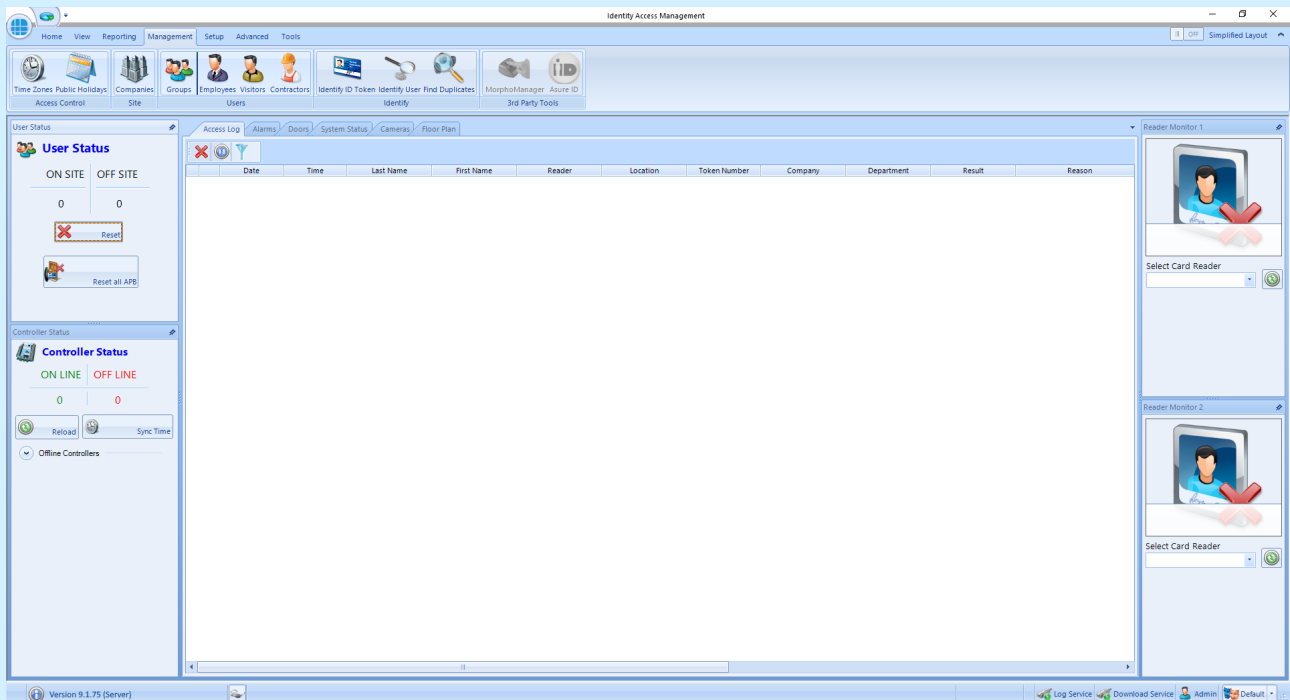


# Controlsoft Identity Access Management Software



## INSTALLATION & USER MANUAL

Version 9.1.75 © 2024 Controlsoft Ltd

<b>1. Introduction</b>	<b>7</b>
1.1 PC Specifications .....	12
1.2 Expanding Systems .....	13
1.3 Integrating with a Fire Alarm System .....	17
<b>2. Installing Identity Access Software</b>	<b>18</b>
2.1 Pre-install Checks .....	19
2.2 Installing IA Server .....	20
2.3 Advanced Option for Installing IA Server .....	25
2.4 Installing IA Client .....	30
2.5 Upgrading IA Software .....	41
2.6 Licensing the Software .....	46
2.7 Transferring a Licence .....	49
2.8 SQL Server Backup .....	51
2.9 Identity Access Configuration .....	55
2.9.1 IA Configuration - System Info .....	55
2.9.2 IA Configuration - Data Retention .....	56
2.9.3 IA Configuration - Reports .....	57
2.9.4 IA Configuration - Cards & Readers .....	58
2.9.5 IA Configuration - HID Mobile Access .....	65
2.9.6 IA Configuration - Biometrics .....	66
2.9.7 IA Configuration - Badge Printing .....	72
2.9.8 IA Configuration - Extra Data Fields .....	72
2.9.9 IA Configuration - Email .....	74
2.9.10 IA Configuration - Password Policy .....	77
2.9.11 IA Configuration - Lockdown .....	79
2.9.12 IA Configuration - User Profiles .....	79
2.9.13 IA Configuration - User Interface .....	80
2.9.14 IA Configuration - Backup .....	81
2.9.15 IA Configuration - Databases .....	84
2.9.16 IA Configuration - Network .....	85
2.9.17 IA Configuration - Services .....	86
<b>3. Preparing for IP Connection</b>	<b>88</b>
3.1 Configure the PC .....	89
3.2 Ping the i-Net Controller .....	91
3.3 Assigning a Fixed IP Address using i-Net Configurator .....	92
<b>4. Starting the Identity Access Software</b>	<b>93</b>
4.1 Identity Access Header and Footer .....	96
4.2 The Option Wheel .....	97



4.3	The Dashboard .....	98
4.4	Identity Access Home Tab .....	101
4.5	Identity Access ViewTab .....	104
4.6	Identity Access Reporting Tab .....	105
4.7	Identity Access Management Tab .....	106
4.8	Identity Access Setup Tab .....	107
4.9	Identity Access Advanced Tab .....	107
4.10	Identity Access Tools Tab .....	108
<b>5.</b>	<b>Configuring Operators</b>	<b>114</b>
5.1	Changing the Default Credentials .....	117
5.2	Adding an Administrator .....	120
5.3	Adding an Operator .....	122
<b>6.</b>	<b>Configuring the Access Control Hardware</b>	<b>128</b>
<b>7.</b>	<b>Configuring Master Controllers</b>	<b>130</b>
7.1	Find IP Controller Wizard .....	133
7.2	IP Controller Configurator .....	135
7.3	Controller General .....	136
7.4	Door Configuration Wizard .....	139
7.5	Controller Settings .....	141
7.6	Controller Timeouts .....	145
7.7	Controller Sirens .....	147
7.8	Controller Events .....	149
7.9	Controller Notes .....	151
<b>8.</b>	<b>Configuring Doors</b>	<b>152</b>
8.1	Door Properties General .....	154
8.2	Door Properties I/O Settings .....	156
8.3	Door Properties Time Zones .....	162
8.4	Door Properties Events .....	163
8.5	Door Properties Notes .....	164
<b>9.</b>	<b>Configuring Card Readers</b>	<b>165</b>
9.1	Card Reader General .....	167
9.2	Card Reader Time Zones .....	169
9.3	Card Reader Settings .....	170
9.4	Card Reader Events .....	171
9.5	Card Reader Notes .....	172

<b>10. Configuring Morpho Fingerprint Readers</b>	<b>173</b>
10.1 Morpho Reader General .....	175
10.2 Morpho Reader Settings .....	177
10.3 Morpho Reader Time Zones .....	178
10.4 Morpho Reader Notes .....	179
<b>11. Configuring Elevators</b>	<b>180</b>
<b>12. Configuring DropBox</b>	<b>186</b>
<b>13. Configure Time Zones</b>	<b>188</b>
13.1 Creating Time Zones .....	190
13.2 Time Zones for Morpho Readers .....	195
<b>14. Public Holidays</b>	<b>196</b>
14.1 Creating Public Holidays .....	198
<b>15. Companies and Departments</b>	<b>200</b>
15.1 Creating Companies and Departments .....	202
<b>16. Configuring Groups</b>	<b>204</b>
16.1 Creating Groups .....	206
16.1.1 Groups Properties Users .....	207
16.1.2 Groups Properties Card Readers .....	208
16.1.3 Groups Properties Morpho Readers .....	209
16.1.4 Groups Properties APB Doors .....	210
16.1.5 Group Properties Elevators .....	211
16.1.6 Groups Properties Time Zones .....	212
16.1.7 Group Properties Events .....	212
16.1.8 Groups Properties Notes .....	214
16.2 Allocating Users to Groups .....	214
<b>17. Enrolment Readers</b>	<b>216</b>
17.1 Omnikey 5427G2 Reader .....	217
<b>18. Users</b>	<b>219</b>
18.1 User General .....	222
18.2 User Photo .....	224
18.3 User Fingerprints .....	228
18.4 User Mobile Access .....	232
18.5 Multiple Tokens .....	240
18.6 User Extra Data .....	241

18.7	User Contact .....	243
18.8	User Events .....	243
18.9	User Notes .....	245
18.10	Importing Users .....	245
<b>19.</b>	<b>The Advanced Tab</b>	<b>251</b>
19.1	Object Groups .....	253
19.2	Counters .....	255
19.3	Timers .....	258
19.4	Inputs .....	260
19.5	Outputs .....	263
19.6	Graphics Designer .....	266
19.7	Events .....	271
19.8	Typical Examples of Events & Actions .....	280
<b>20.</b>	<b>Event Viewers and Reports</b>	<b>293</b>
20.1	Event Viewers .....	294
20.2	Fire Rollcall Report .....	296
20.3	Access Control Reports .....	297
20.4	System Log Reports .....	299
20.5	Time & Attendance Report .....	300
20.6	Access Control Status Report .....	303
20.7	Groups Status Report .....	305
20.8	Inactivity Report .....	306
20.9	System Log .....	307
<b>21.</b>	<b>Service Manager</b>	<b>310</b>
21.1	Log Service .....	312
21.2	Download Service .....	313
21.2.1	Home .....	314
21.2.2	i-Net Controllers .....	315
21.2.3	Biometric Devices .....	318
<b>22.</b>	<b>Appendix A - Types of Door</b>	<b>322</b>
22.1	Normal Door .....	324
22.2	Turnstile .....	325
22.3	Airlock .....	326
22.4	Aperio Door .....	328
<b>23.</b>	<b>Appendix B - HID Asure ID Software</b>	<b>335</b>

<b>24. Appendix C - Windows Commands</b>	<b>346</b>
<b>25. Appendix D - i-Net webpage</b>	<b>348</b>
<b>26. Appendix E - AntiPassBack</b>	<b>353</b>
<b>27. Appendix F - i-Net Configurator</b>	<b>360</b>
27.1 Upgrading iNet Firmware .....	369
<b>28. Appendix G - Product History</b>	<b>373</b>
<b>29. Appendix H - Downloading Software</b>	<b>381</b>
<b>30. Appendix I - Licence Terms &amp; Conditions</b>	<b>383</b>
<b>31. Appendix J - HID OSDP Readers</b>	<b>385</b>
<b>32. Appendix K - Adding Morpho Readers</b>	<b>388</b>
<b>33. Appendix L - IA Morpho Configurator</b>	<b>394</b>
<b>34. Appendix M - Controller Status</b>	<b>397</b>
<b>35. Appendix N - Duress</b>	<b>404</b>
<b>36. Appendix O - Database Importer</b>	<b>407</b>
<b>37. Appendix - Glossary</b>	<b>411</b>
<b>38. Controlsoft Contact Details</b>	<b>415</b>
	<b>0</b>

# Introduction

## 1 Introduction

The Identity Access (IA) Management Software Version 9 from Controlsoft© is a PC-based Access Control Management system. Information on the hardware and software for the Identity Access system is available from the "[Getting Started with Identity Access](#)" portal

The Identity Access software manages the access control database, which is downloaded to one or more Master iNet® Controllers. The Master iNet controls access through the doors, either directly or via expanders. The iNet controller(s) make the decisions as to whether access is granted or denied. There are different options to expand the number of doors on the system (see [Expanding Systems with iNet Controllers](#)<sup>13</sup>)

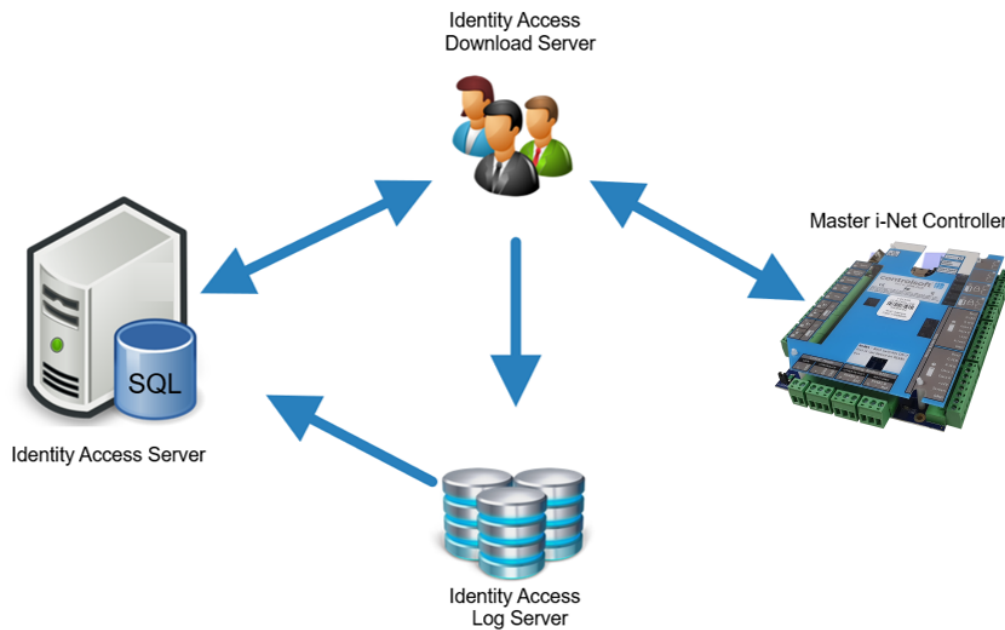
The Identity Access software is available on a flash drive by ordering the required part number shown below in green, or can be downloaded from our website [www.controlsoft.com](http://www.controlsoft.com)<sup>8</sup>.

	NO LICENCE (IA-LITE)		
		PROFESSIONAL LICENCE (Part No. IA-PRO)	
			ENTERPRISE LICENCE (Part No. IA-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 Express Database Platform	✓	✓	✓
Snow Day Rule	✓	✓	✓
Photo ID Card Printing *	✓	✓	✓
Site Lockdown	✗	✓	✓
Hikvision ANPR Integration	✗	✓	✓
Fire Alarm Roll Call Report	✗	✓	✓
Time & Attendance Reporting	✗	✓	✓
Fingerprint Enrolment	✗	✓	✓
Direct Integration with Morpho Biometric readers	✗	✓	✓
Email Notifications	✗	✓	✓
AntiPassBack	✗	✓	✓
Preconfigured Logic for Airlocks & Turnstiles	✗	✓	✓
Elevators	✗	✓	✓
Counters and Timers	✗	✓	✓
Programmable Inputs and Outputs	✗	✓	✓
Interactive Site Maps	✗	✓	✓
Events and Actions	✗	✓	✓
Annual Subscription Option	✗	SUB-PRO	SUB-ENT

\* 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:



**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.

- IAMAIN is the main database that stores the configuration data and the user database
- IAAccessLog is the Access Log database that stores all access events (i.e. who went where and when)
- IASystemLog is the System Log database that stores all system events (i.e. who logged into the software and what changes were made)
- IATALog is the T&A Log database that stores Time & Attendance information (i.e. who clocked in or out and when)



- IAAccLogBuffer, IASysLogBuffer and IATALogBuffer are temporary files that receive events from the Download Service and passes them to the Log Service.

This software is not accessible on a Client installation.

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

[IA Configuration](#)<sup>55</sup> is only used to configure the Server.

IA Morpho Configurator is used to configure the fingerprint readers

[IA Service Manager](#)<sup>311</sup> allows access to the user interface for the Download Service and the Log Service

[iNet Configurator](#)<sup>361</sup> is used to configure the iNet controllers

[Licensing Utility](#)<sup>46</sup> 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.***

Conventions used in manual:

- **On-screen text**
- [Cross reference links](#)
- **Text to be typed in**
- **Notes**

- [On-screen Buttons]

## 1.1 PC Specifications

---

### **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 Server Operating Systems:**

- Windows 10 (x64).
- Windows Server 2016.
- Windows Server 2020.

### **Recommended Identity Access Client PC Specification**

- Intel i3 processor @ 3GHZ
- 4GB RAM

- 100GB Free Disk Space
- 10/100 Network Card
- USB Port
- Screen Resolution = 1280x800 or better

**Recommended Identity Access Client Operating Systems:**

- Windows 10 (x64).

## 1.2 Expanding Systems

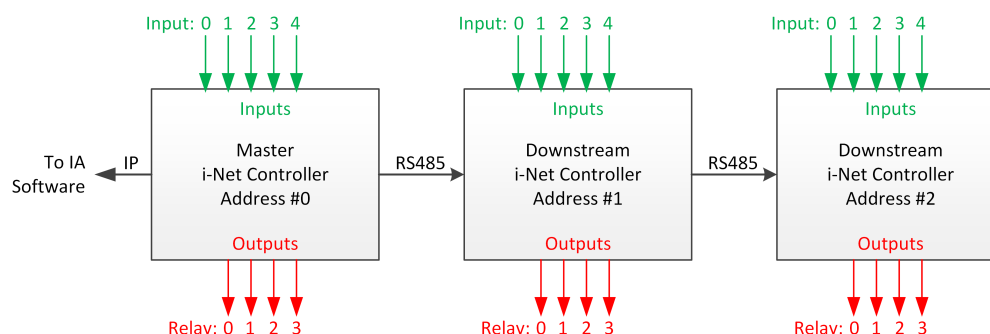
---

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. Both controllers support up to 200,000 card holders and have an offline event memory of 250,000 events. In certain markets, the older iNet Plus is still available with 9 inputs, 4 output relays, 2 Wiegand reader ports, up to 50,000 card holders and an offline event memory of 100,000 events. For further information on the hardware, please refer to the 1DR installation manual, 2DR installation manual or iNet Plus installation manual.

**Option 1 – Master iNets:**

A channel comprises of an iNet controller connected to the Identity Access software via IP. This is called the Master iNet. The system can be expanded simply by adding further Master iNets connected to the software via an IP Connection. 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 Master iNet to the SQL Database.

### Option 2 – Master and Downstream iNets:

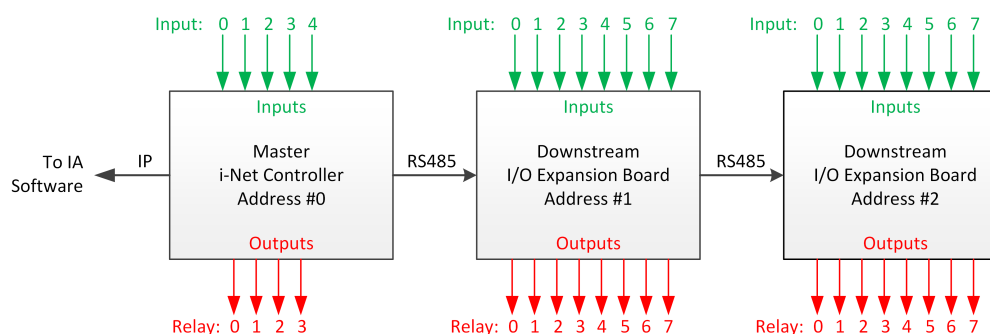


The channel comprises of an iNet controller connected to the Identity Access software via IP. This is called the Master iNet.

The other controllers are called Downstream iNets and are connected to the Master iNet via RS485.

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 hence to the SQL Database.

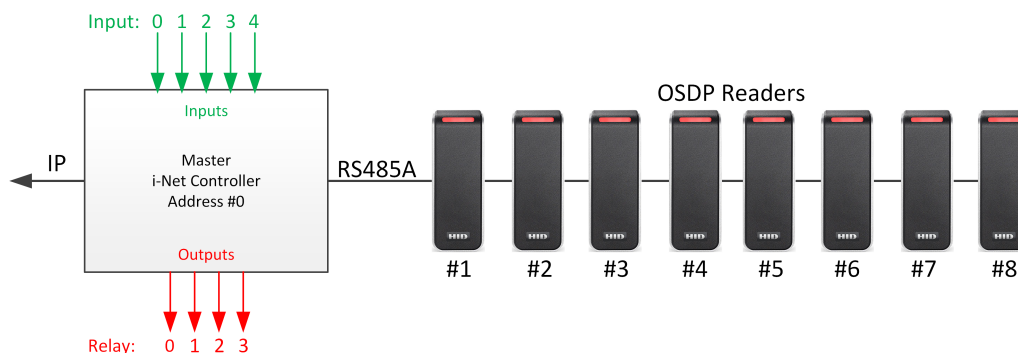
### Option 3 – Master iNet and Downstream I/O Expansion Boards



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

The other controllers are called Downstream I/O Expanders and are connected to the Master iNet via RS485.

### Option 4 – Master iNet and RS485/OSDP Readers:



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

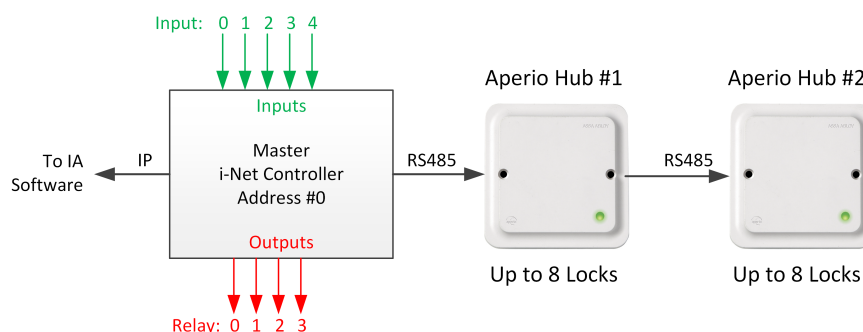
Up to 8 RS485 OSDP readers (Two Door Controllers) or up to 2 OSDP readers (One Door Controller) are then connected to the RS485 bus.

Outputs 0 to 3 (Two Door Controllers) or Output 0 (One Door Controller) are used for electronic locks for each of the door/s.

Inputs 0 to 3 are used for door contacts for each of the door/s.

Door 0 is then controlled by readers 1 (IN) and 2 (OUT). where available, door 1 is controlled by readers 3 and 4 etc.

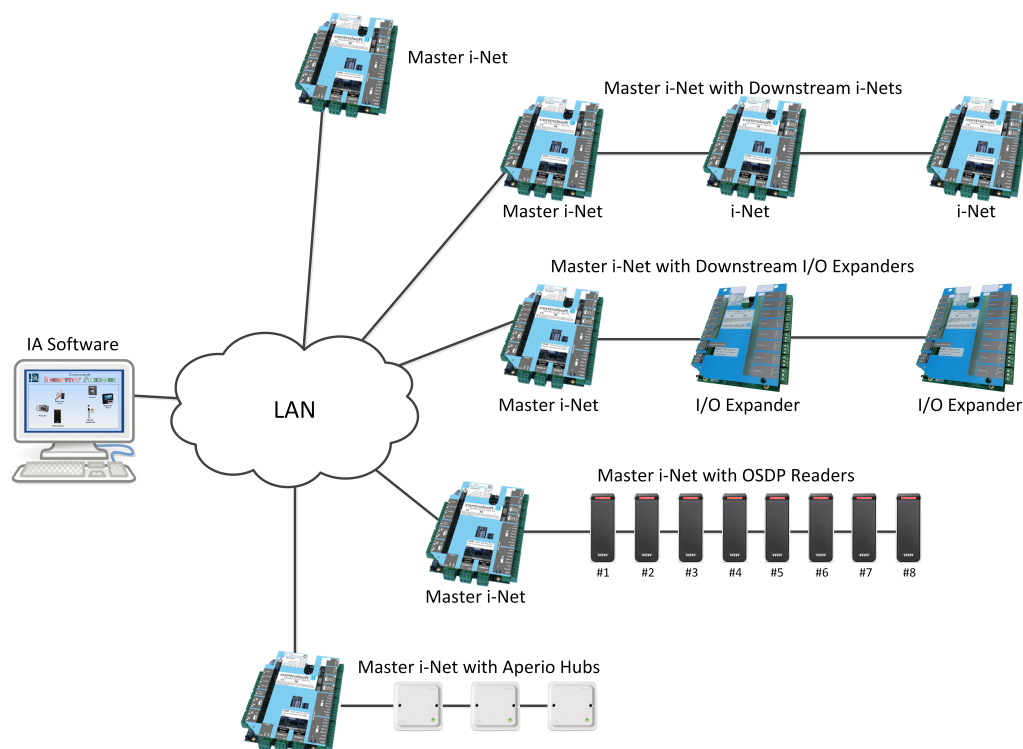
### Option 5 – Master iNet and RS485 Aperio Hubs:



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

Up to 15 RS485 Aperio Hubs are then connected to the RS485 bus, each Hub supporting up to 8 Aperio Locks up to a maximum of 32 locks per master controller.

**NOTE: It is NOT possible to combine Downstream iNets / I/O Expanders / OSDP Readers / Aperio Hubs on the same Master iNet, although a system can support multiple channels with each option:**



**NOTE: Before starting to configure the system in Identity Access, it is advisable to draw the layout of the building on a large sheet of paper, showing where all the doors are, where the controllers and readers will be situated etc. Add identifiable names, bus addresses and input & output numbers to this drawing for all the controllers, doors, readers etc. as this will make the programming much faster and will result in fewer programming errors. Where readers change the user's Location between "Inside" and "Outside", add this to the diagram to reduce confusion later.**

## 1.3 Integrating with a Fire Alarm System

It is often desirable for doors to unlock automatically in the event of a Fire. This is best achieved by the alarm relay in the fire alarm panel physically disconnecting power from the door locks. In some circumstances, it may be preferable for the fire alarm panel to provide a signal to the access control system, and the access control system then releases the relevant door/s. Controlsoft recommend that you discuss this with your local Fire Officer.

NOTE:

1. Nominate an input that will be used on the Master iNet (usually Input 4).
2. The Fire Alarm panel MUST be connected to an input on the Master iNet.
3. The output from the Fire Panel must be Voltage Free Normally Closed Contacts

Configuring the system for Fire:

Connect the relay in the Fire Alarm Panel to the required iNet input.

In Identity Access, configure the input used to monitor the fire alarm panel relay (see [Controller Settings](#)<sup>141</sup>)

Ensure that each door to be opened in the event of a fire is configured accordingly (see [Door Properties General](#)<sup>154</sup>). Simply tick the option **Force door open if fire is detected**

**NOTE: On systems using Identity Access v8 or older, a Fire Input MUST be configured on each Master iNet. With Identity Access v9 or later, it is possible to configure Events and Actions to detect a Fire condition on one master iNet and set Fire as active on any/all other Master iNets.**

# **Installing Identity Access Software**



## 2 Installing Identity Access Software

Identity Access is supplied on a flash drive by ordering the Part Numbers IA-LITE, IA-PRO or IA-ENT. IA-LITE can be downloaded from our website [www.controlsoft.com](http://www.controlsoft.com) and licenses subsequently ordered to enable the required features. The software includes Microsoft SQL Server 2014 Express x64, and is bundled with SQL Backup Master, software for various enrolment readers and HID Asure ID for card printing.

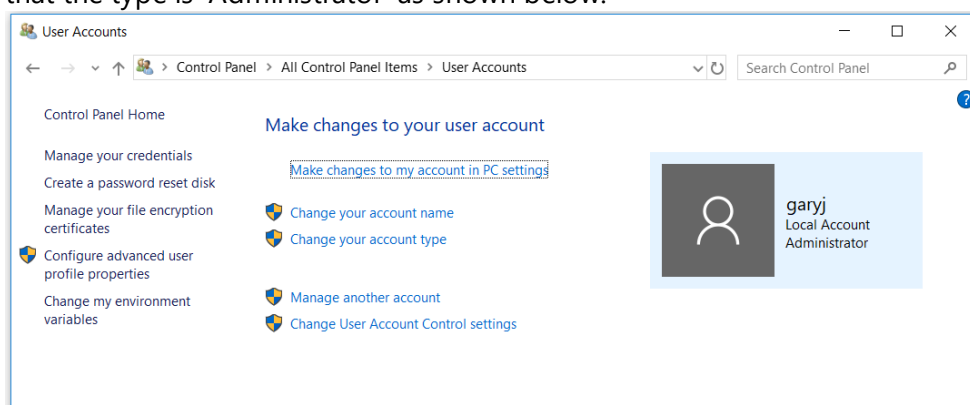
To ensure that your software installs correctly, it is important to run through the following pre-installation checks.

### 2.1 Pre-install Checks

Before installing your software (Server or Client), please temporarily disable your antivirus for the duration of the install.

Next, please ensure that you are logged into an Administrator Account. To do this:

1. Click on the **Start** Button and select **Control Panel** (see [Appendix C - Windows Commands](#) <sup>347</sup> for further assistance)
2. Select **User Accounts**
3. On the right hand side of the window the User's details will be shown, check that the type is 'Administrator' as shown below:



4. If the User Account is not an Administrator, choose another account, or contact your system administrator.


Finally, ensure that User Account Control (UAC) is set to "Never Notify", ensure that all Windows updates have been installed and temporarily disable your anti-virus software until installation is complete.

## 2.2 Installing IA Server

---

For a basic installation of Identity Access, follow the instructions below:

***NOTE: Before starting the installation, we strongly recommend that you temporarily disable your antivirus software***

If you have downloaded Identity Access from the Controlsoft website [www.controlsoft.com](http://www.controlsoft.com), please refer to [Appendix H - Downloading Software](#)  before proceeding.

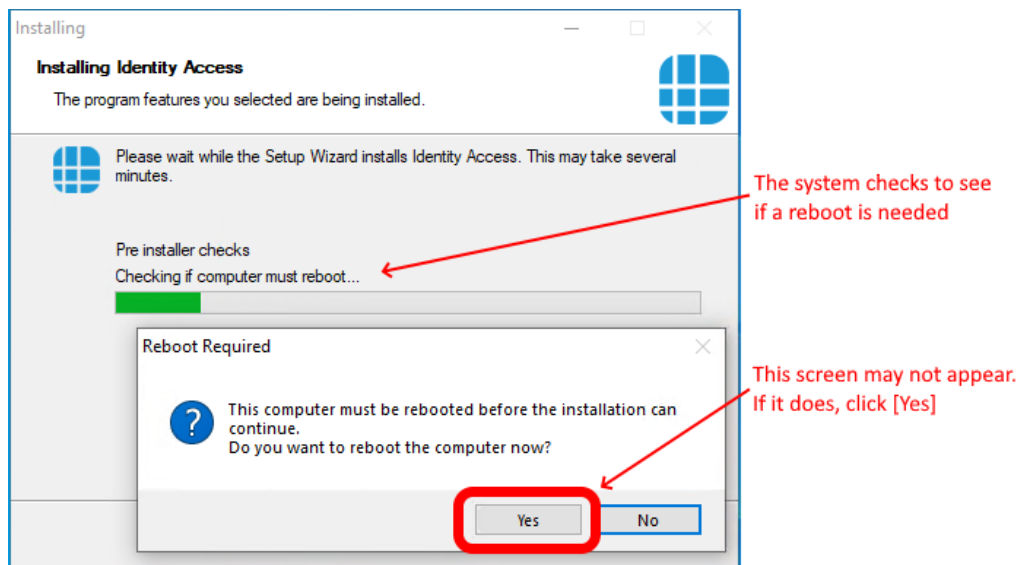
Insert the flash drive into a spare USB port and the AutoPlay screen will appear.

***NOTE: If a message box appears stating Windows protected your PC, click on More info, then [Run anyway].***

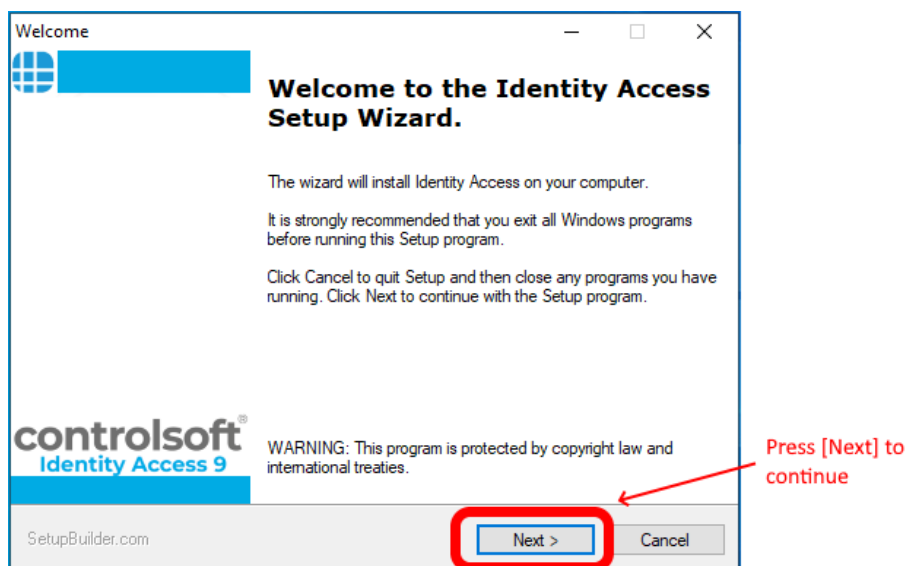
Select **Open folder to view files.**

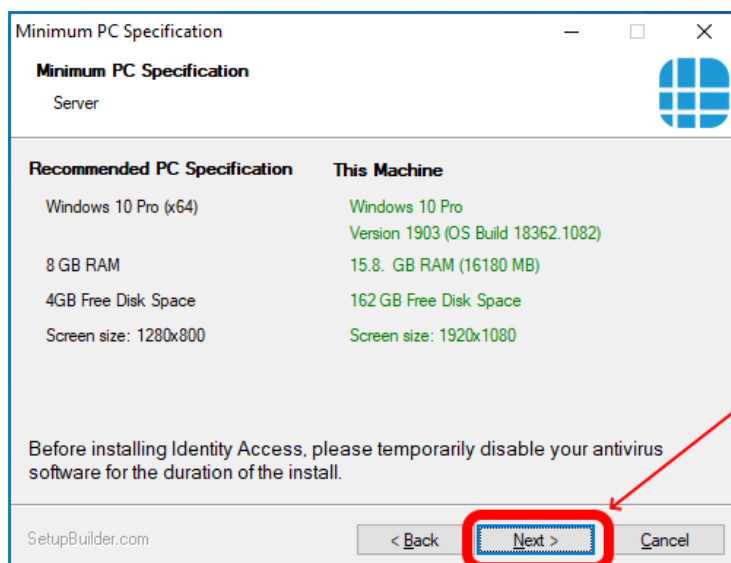
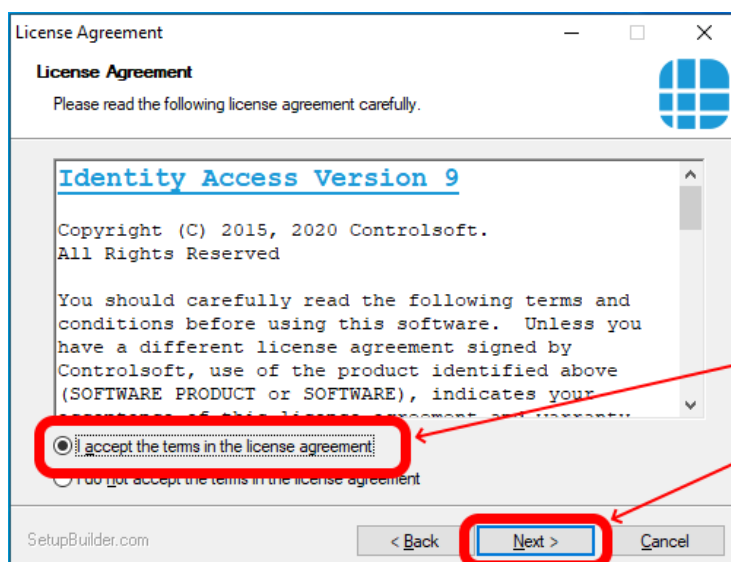
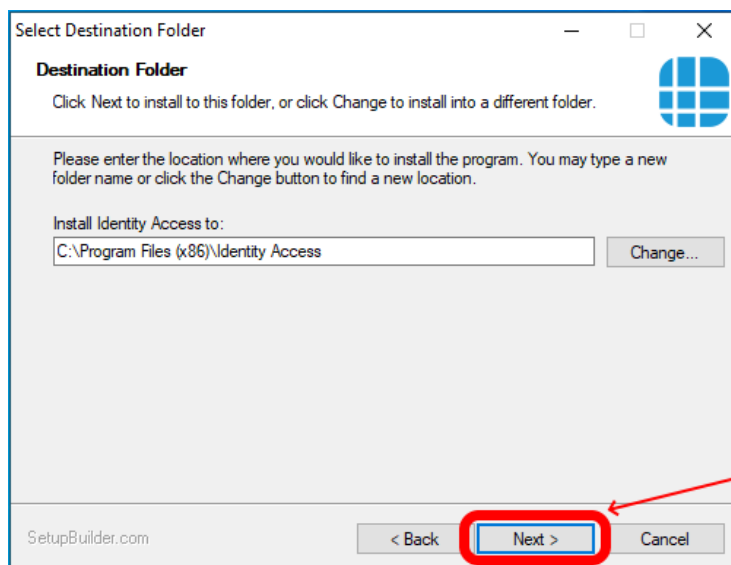
If your PC is not configured with AutoPlay, please browse to **My Computer /This PC** and double click the **IA Flash Drive** USB drive.

To start the installation, double click the file **Install\_IdentityAccess.exe**

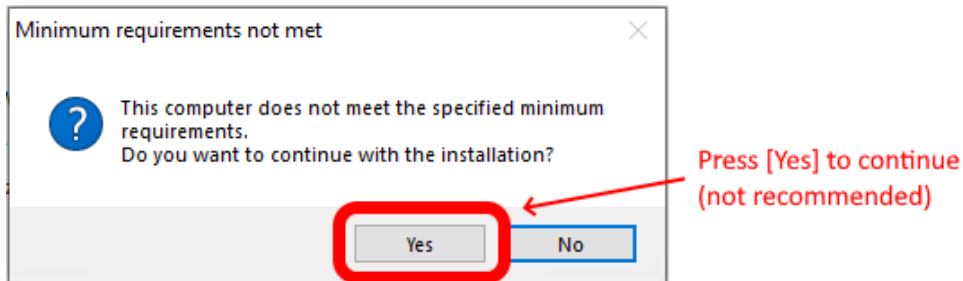


If the system reboots, the installation will recommence automatically.

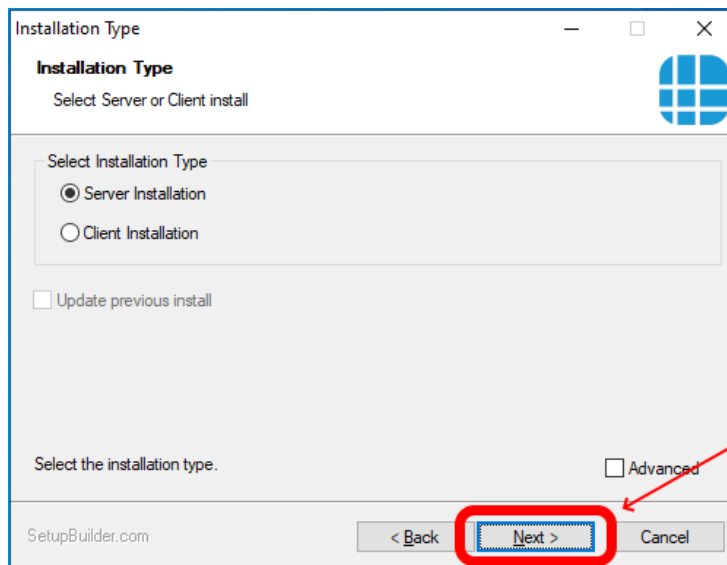




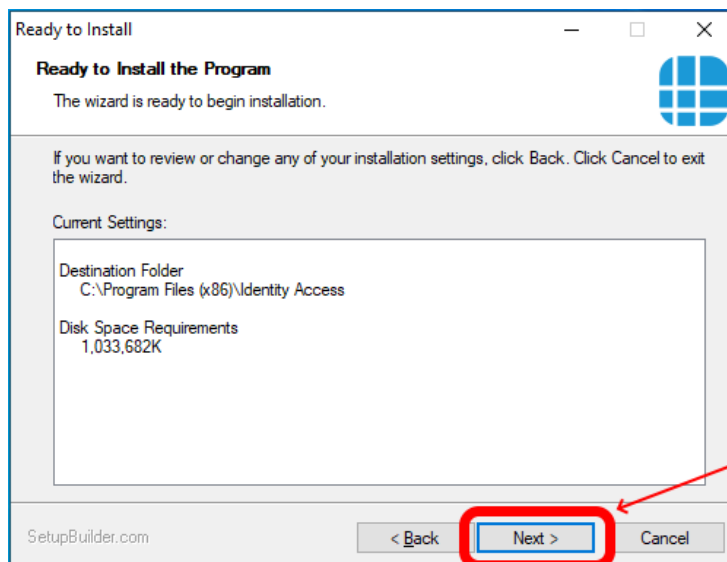
***NOTE: If your system does not meet the minimum specification, the offending parameter will be displayed in red, not green. After pressing [Next], you will be warned again.***



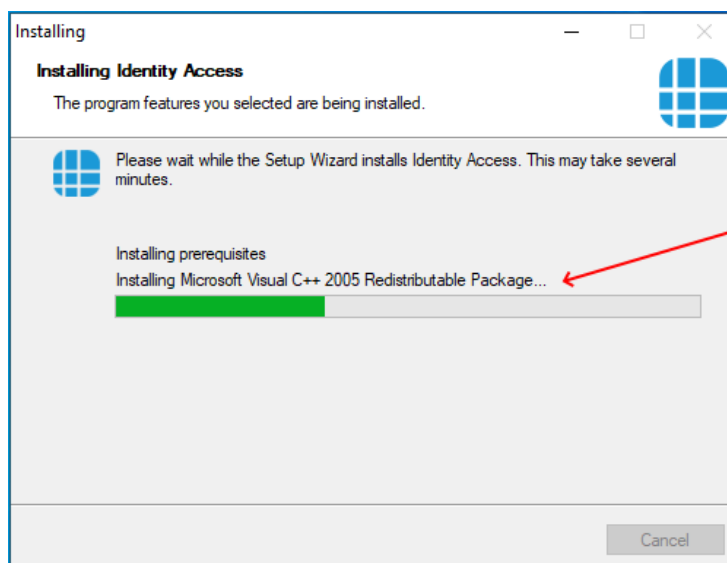
***NOTE: Controlsoft may refuse to support the system if the PC does not meet the minimum recommendations***



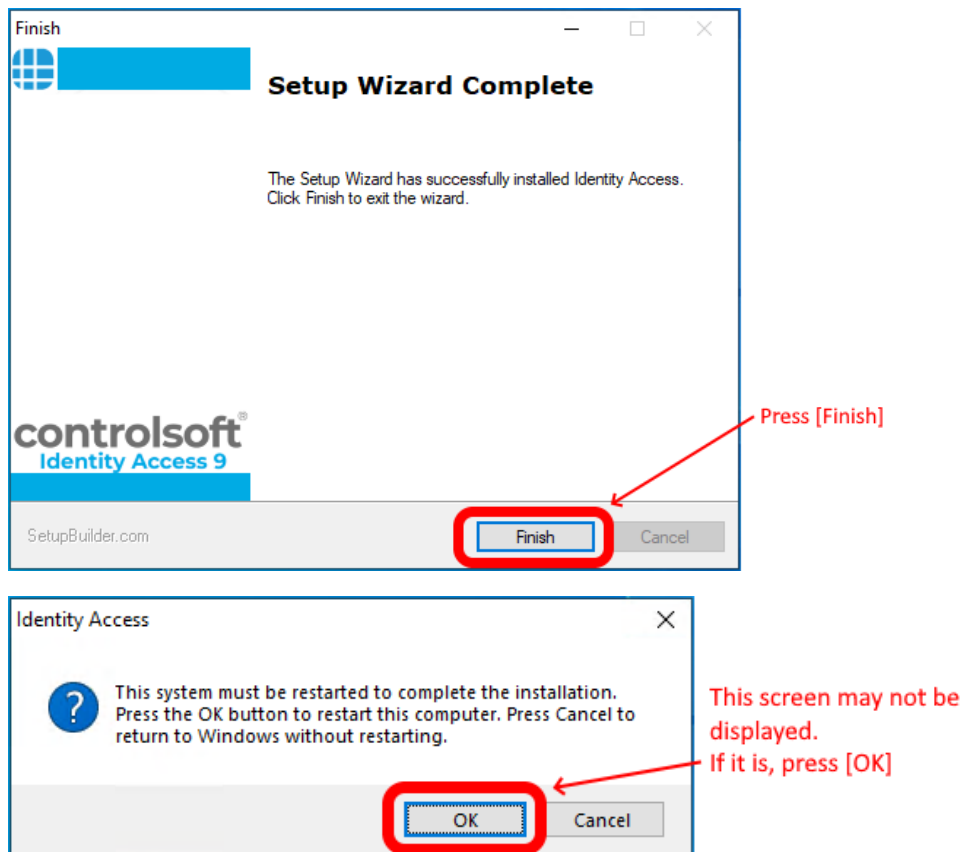
Press [Next] to install the server software



Press [Next]



Displays progress of install



Following the installation of the software, you may notice a file called InstallUtil.InstallLog. If the installation was successful, this file can be deleted.

If you experienced a problem with the install, please do not delete this file as it may be required by Controlsoft Technical Support.

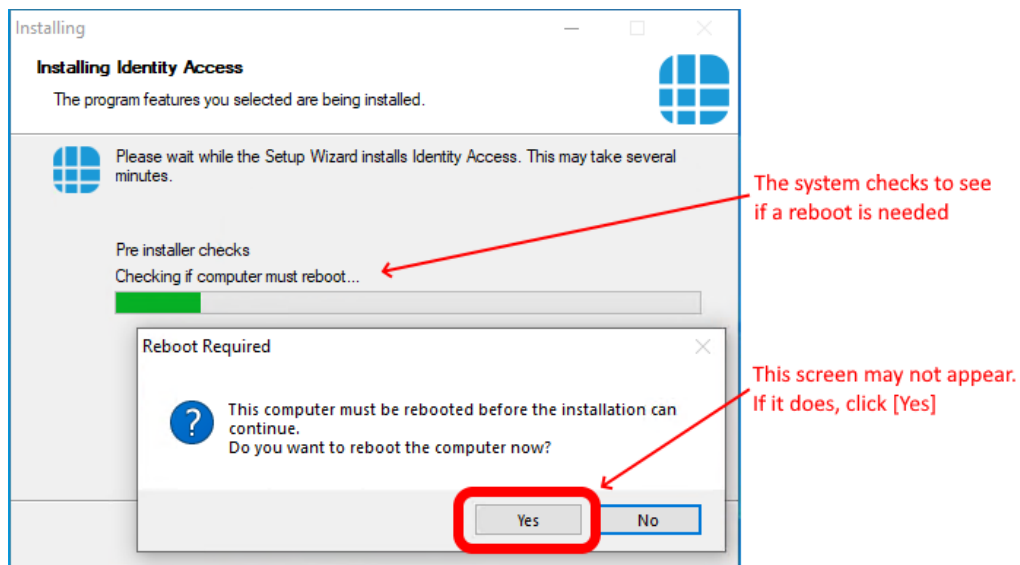
***NOTE: When all the software has been installed, you may re-enable the antivirus software.***

## 2.3 Advanced Option for Installing IA Server

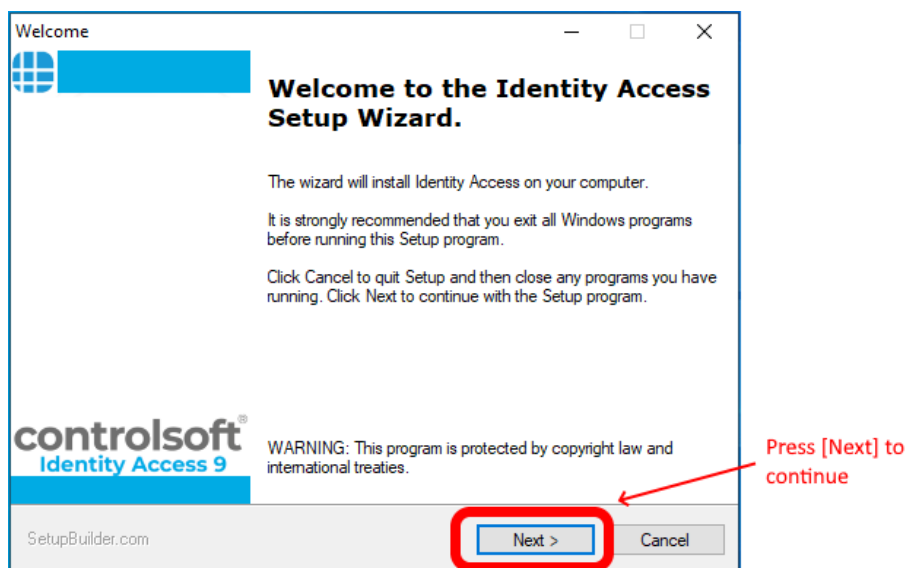
Identity Access can be installed with some Advanced options as described below.

***NOTE: Before starting the installation, we strongly recommend that you temporarily disable your antivirus software***

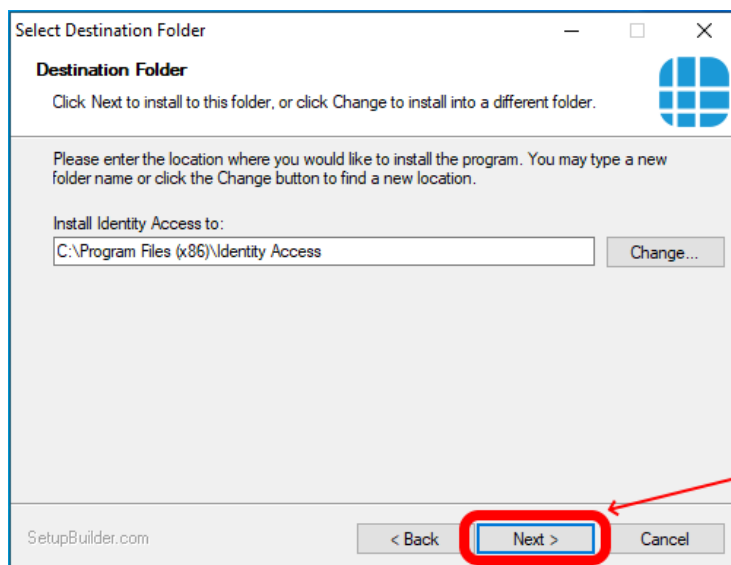
To start the installation, double click the file `Install_IdentityAccess.exe`.



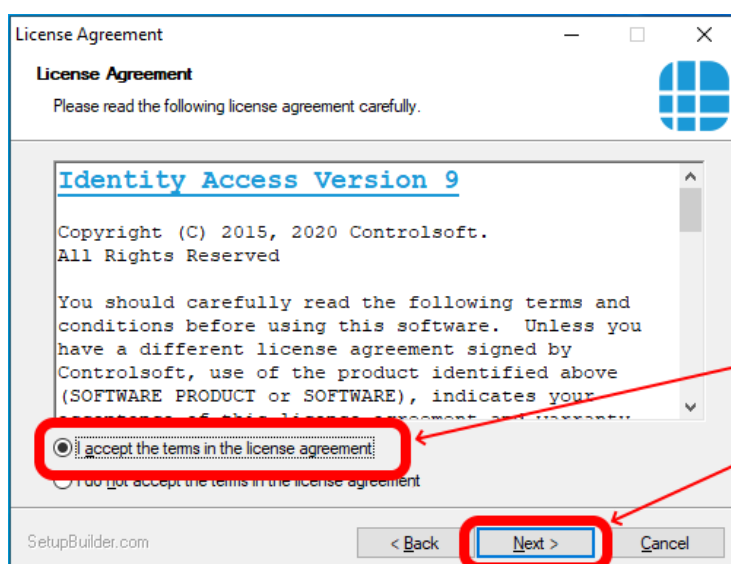
If the system reboots, the installation will recommence automatically.





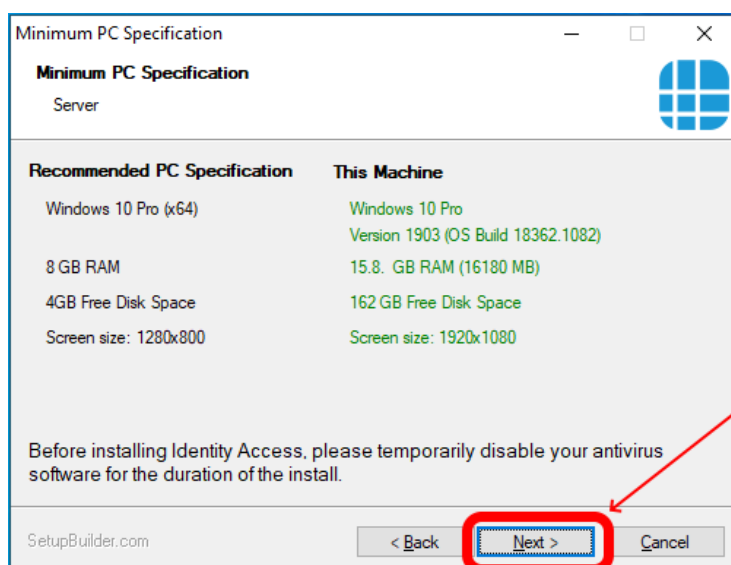


Press [Next] to continue



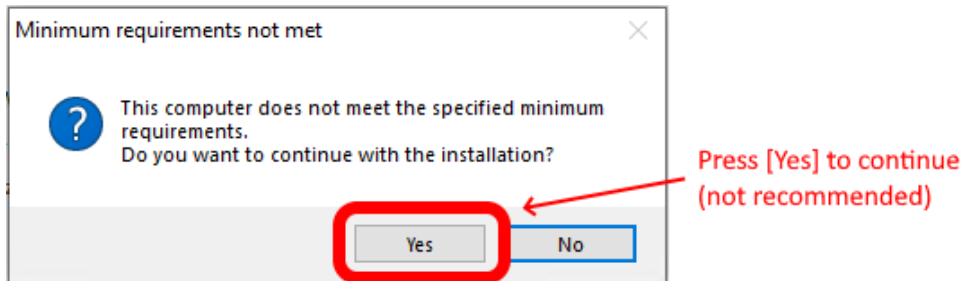
Read and accept the license

then click [Next]

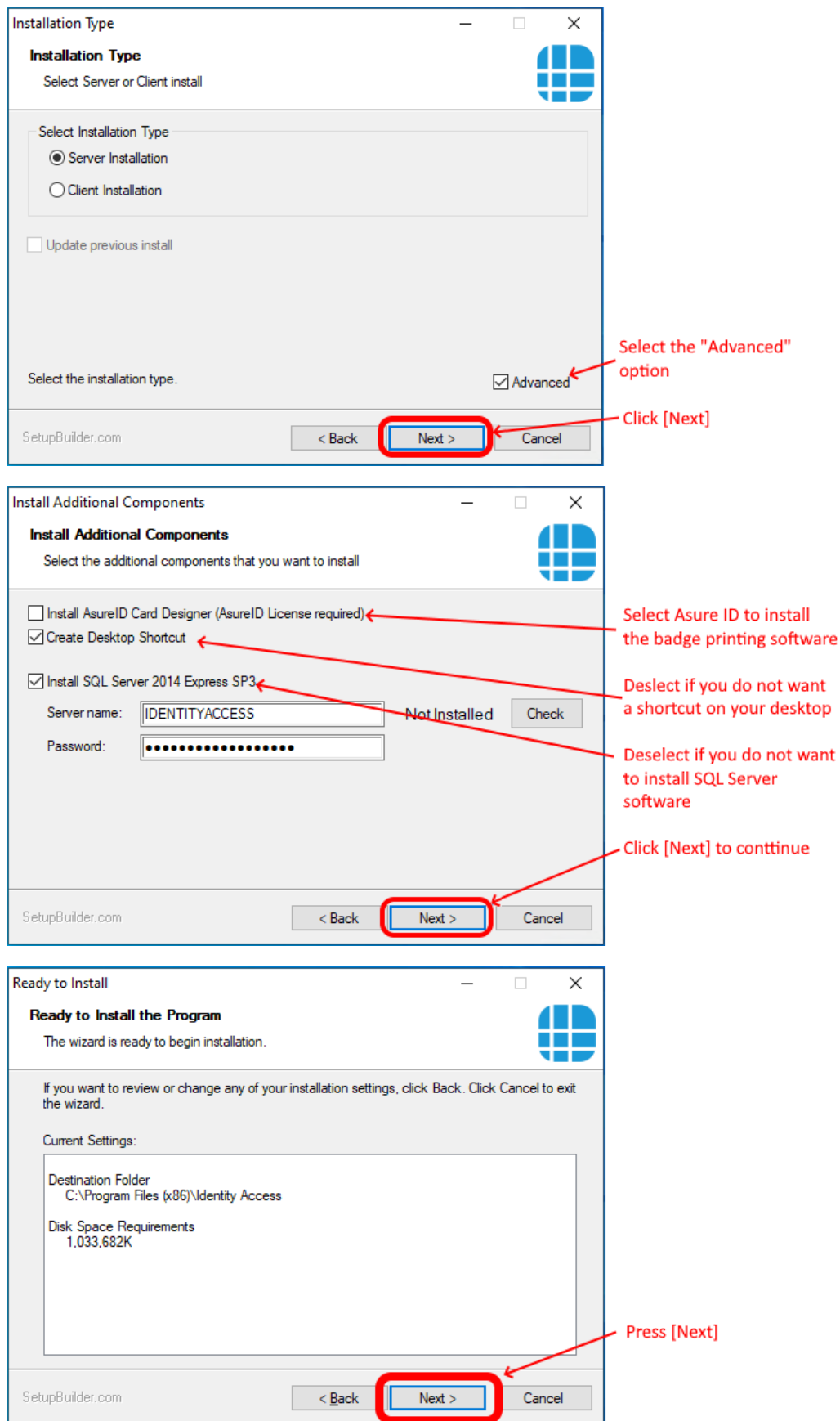


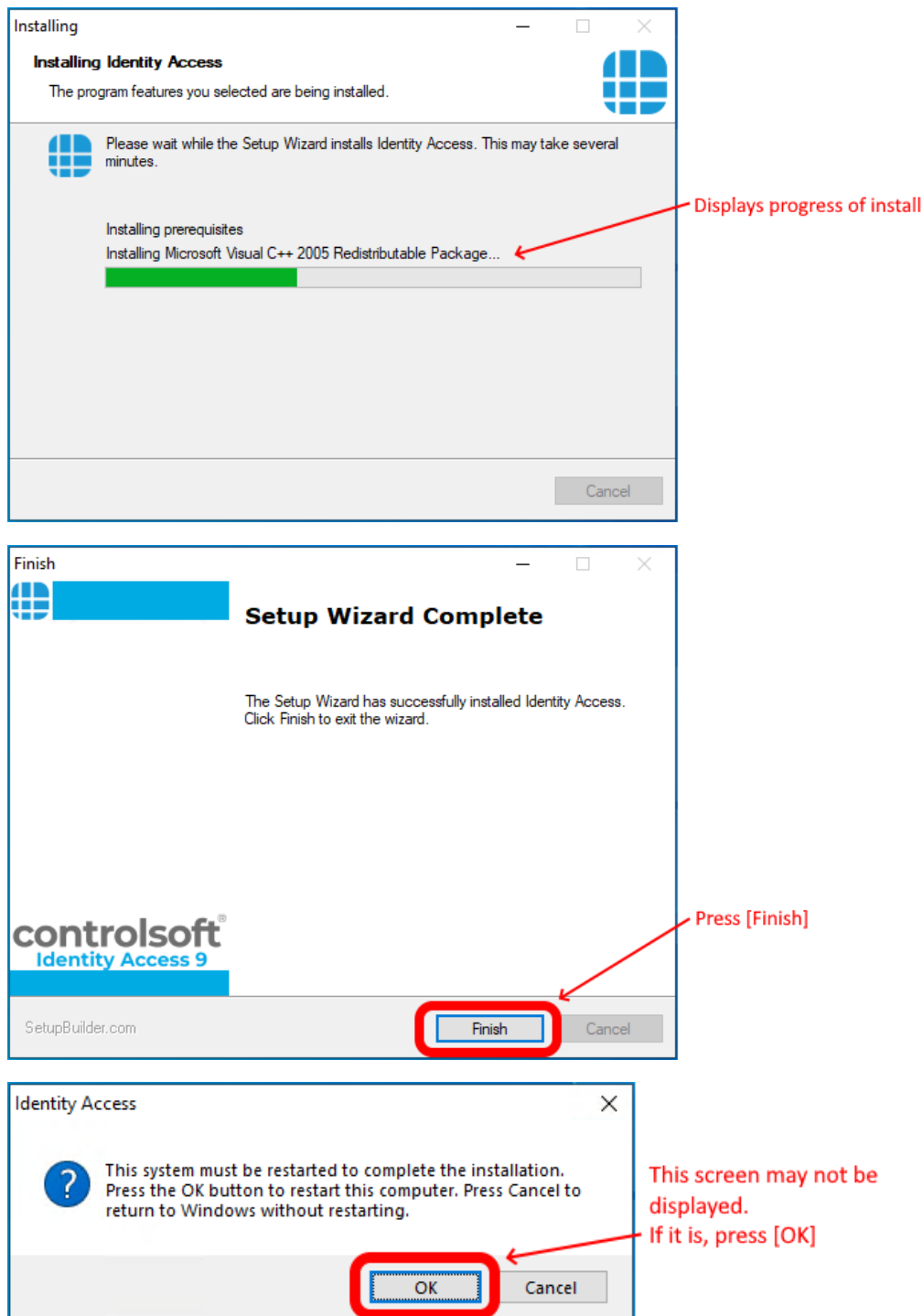
Press [Next]

**NOTE:** If your system does not meet the minimum specification, the offending parameter will be displayed in red, not green. After pressing [Next], you will be warned again.



**NOTE:** Controlsoft may refuse to support the system if the PC does not meet the minimum recommendations





**NOTE:** When all the software has been installed, you may re-enable the antivirus software.

## 2.4 Installing IA Client

Identity Access can be run from a separate computer using the Client software. This can be useful to have an operator station in the Human Resources department with a link back to the main Identity Access Server. This way a

limited amount of permissions can be applied to the operator of the Identity Access (client) software - e.g. so they can only enrol users or remove users – rather than configuring the doors/locks/controllers etc. Identity Access (client) operator can have the same permissions to administer all functions and features of the software/hardware as if running directly from the Identity Access (IA Server).

If Identity Access (Client) software is to be installed and the Microsoft windows firewall or other hardware/software providers firewall system is in use on the Identity Access (IA Server) PC then configuration to allow access to the SQL service, SQL Server Browser, Identity Access Download Service and Identity Access Log Service may be required.

The following additional Network ports should be open on the Identity Access (Server) PC.

SQL Server Access : TCP 1433

SQL Server Browser : UDP 1434

Identity Access Log Server : TCP 19000 & 19001

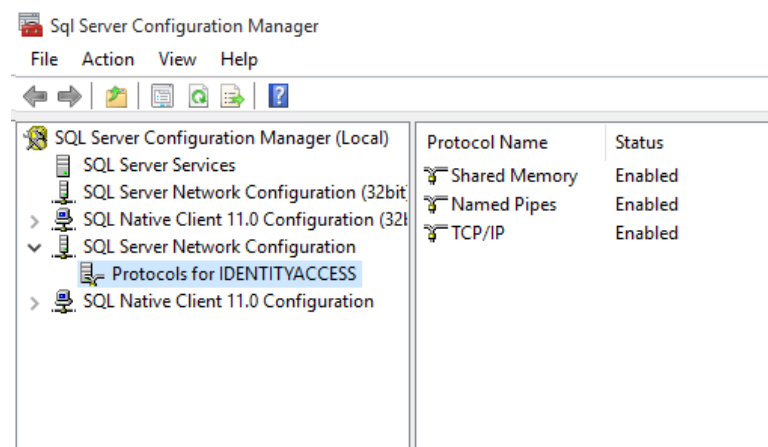
Identity Access Download Server : TCP 19100 & 19101

Configuration of Microsoft SQL Express to be available directly over TCP/IP port 1433 requires the following configuration steps – configured from the Identity Access (Server) PC –

Login to the Identity Access (Server) PC as a Administrator.

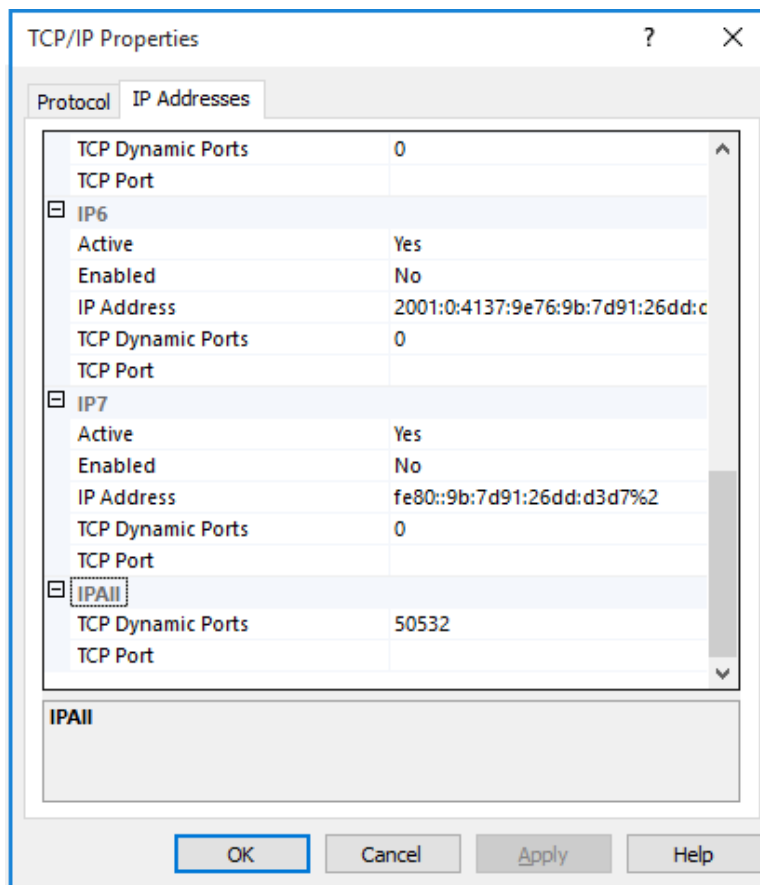
Click **Start, Microsoft SQL Server 2014** and select **SQL Server Configuration Manager**

Expand the interface until you can see the following screen:

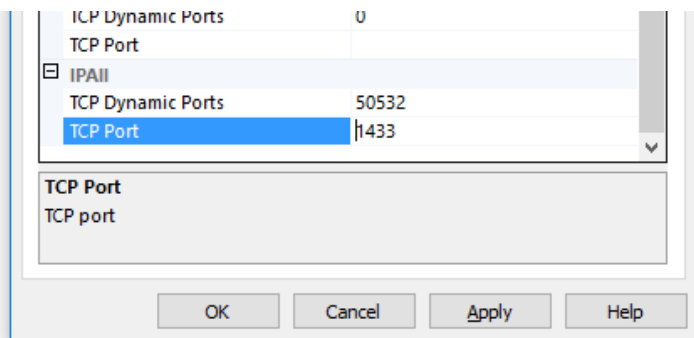


Double click on **TCP/IP** (on the right hand window) to open up the properties.

Select the **IP Addresses** tab (as below) and scroll to the bottom of the list to IPALL.



In the **TCP Port** section for **IPALL**, add the value **1433** and click **[Apply]**



You are warned that It will be necessary to restart the SQL services for changes to be applied. This can be achieved by restarting the SQL services in Windows Services, rebooting the machine or via SQL Configuration Manager -SQL Server Services.

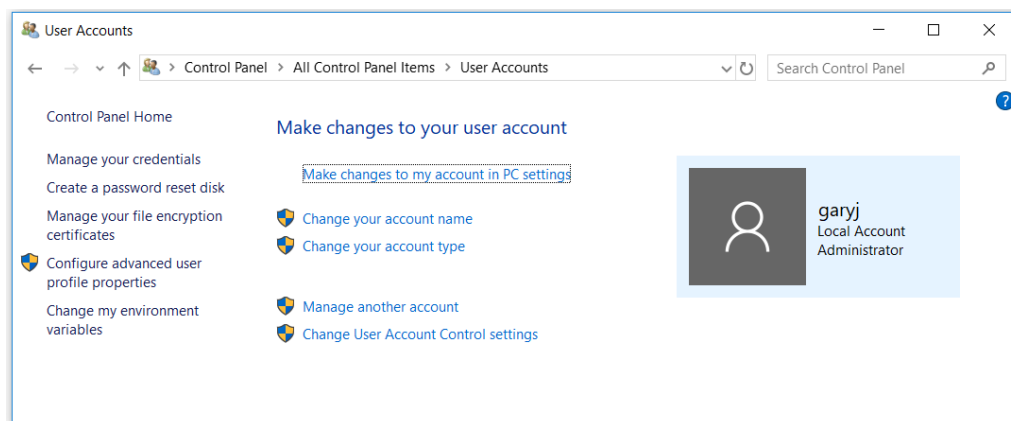
Ensure that the Server PC can ping the Client PC and visa versa.

You are now ready to start installing the Identity Access Client software.

***NOTE: Before installing your software, please temporarily disable your anti-virus for the duration of the install.***

Please ensure that you are logged into an Administrator Account. To do this:

1. Click on the **Start** Button and select **Control Panel** then select **User Accounts**.
2. On the right hand side of the window the User's details will be shown, check that the type is 'Administrator' as shown below.



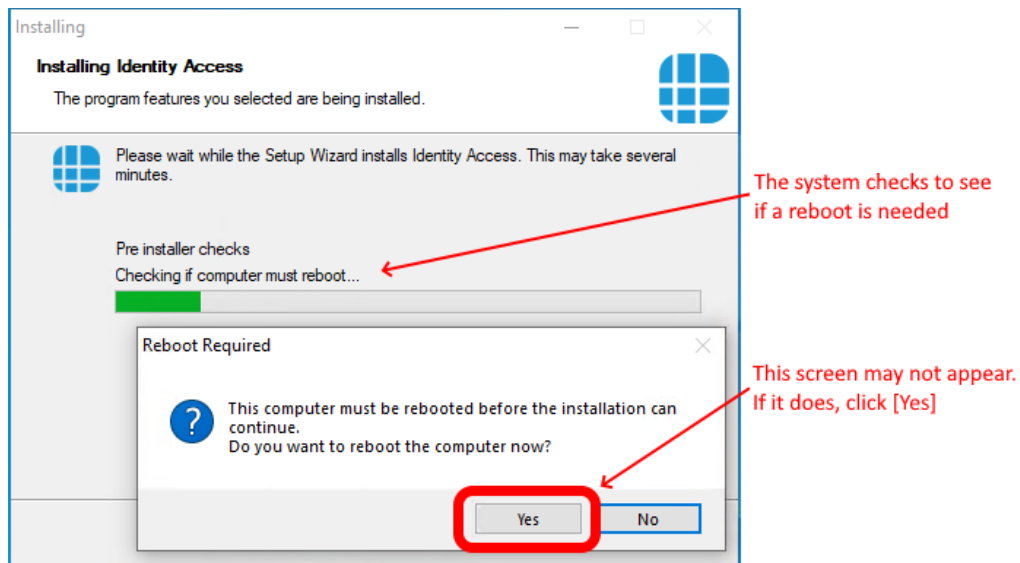
3. If the user account is not an Administrator, choose another account or contact your system administrator.

Insert the USB flash drive into a spare USB port and the AutoPlay screen will appear.

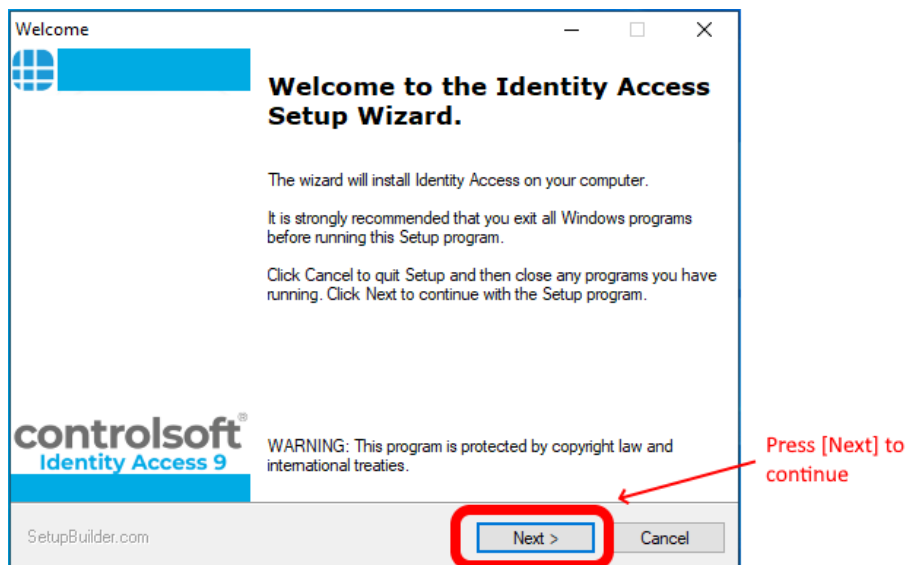
Select **Open folder to view files**.

If your PC is not configured with AutoPlay, please browse to **My Computer/This PC** and double click the IA flash drive.

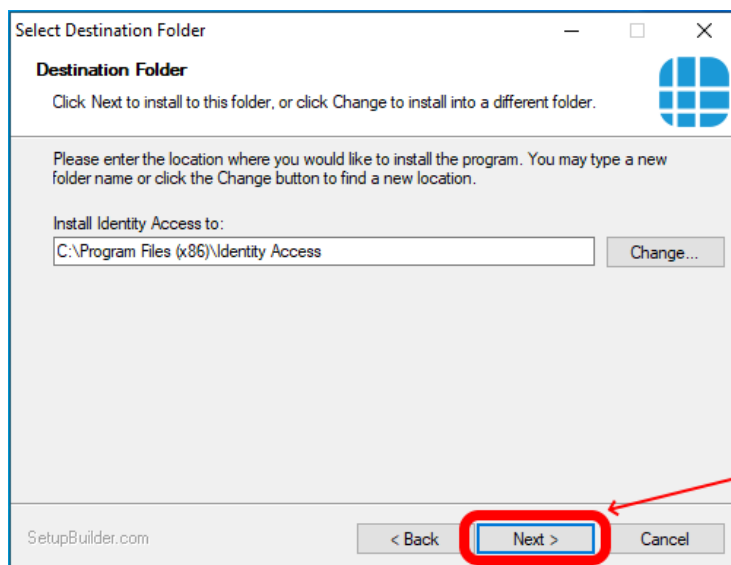
To start the installation, double click the file **Install\_IdentityAccess.exe**.



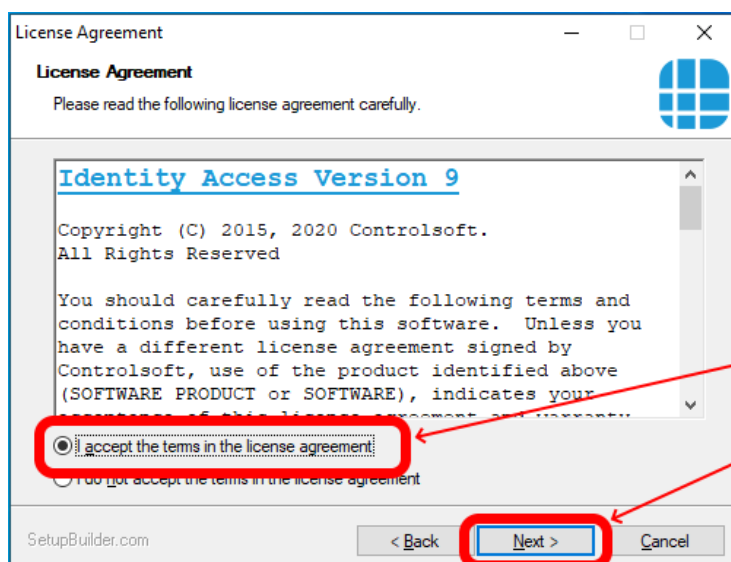
If the system reboots, the installation will recommence automatically.





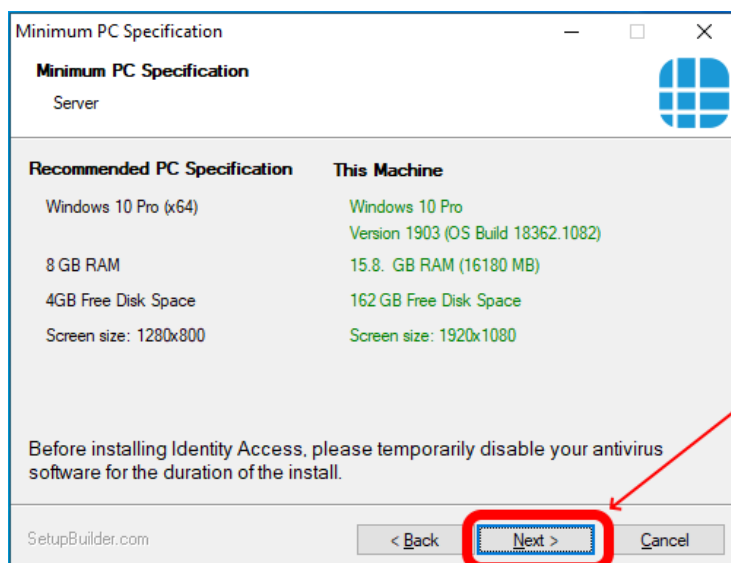


Press [Next] to continue



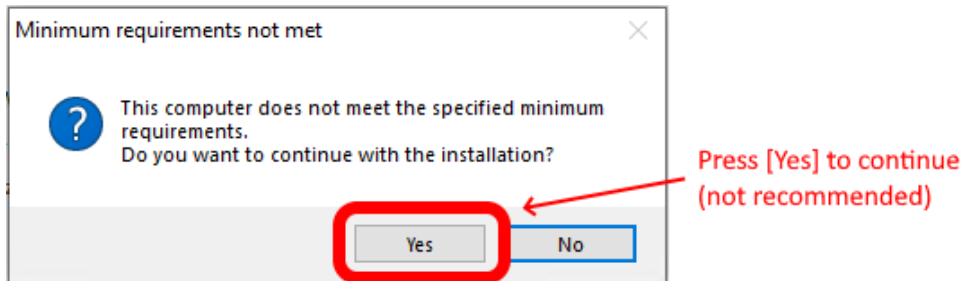
Read and accept the license

then click [Next]

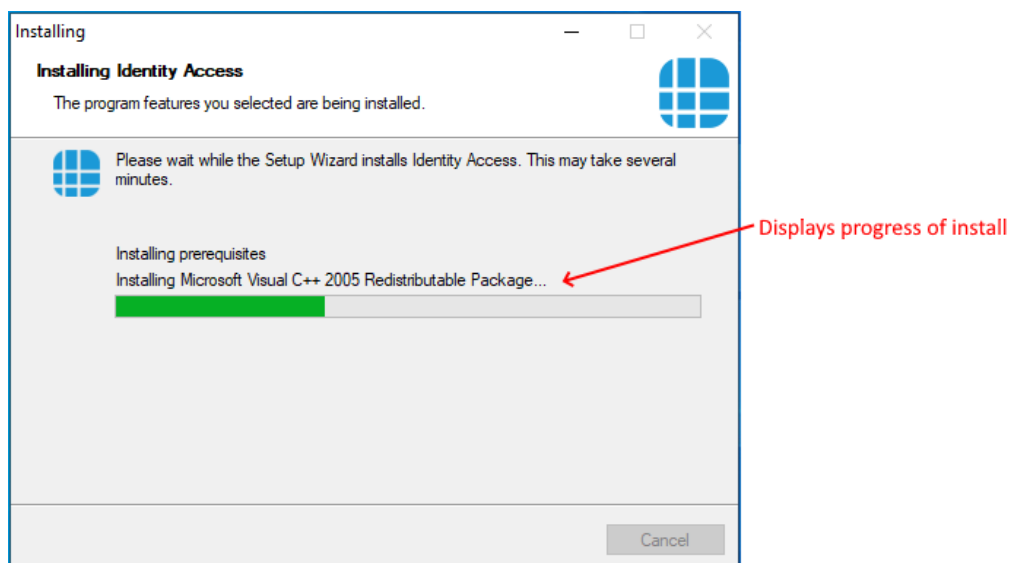
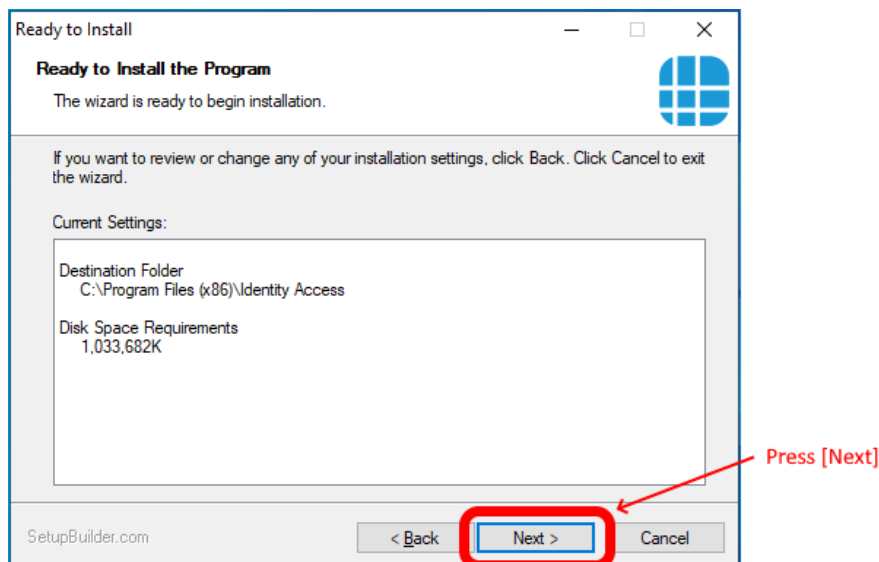
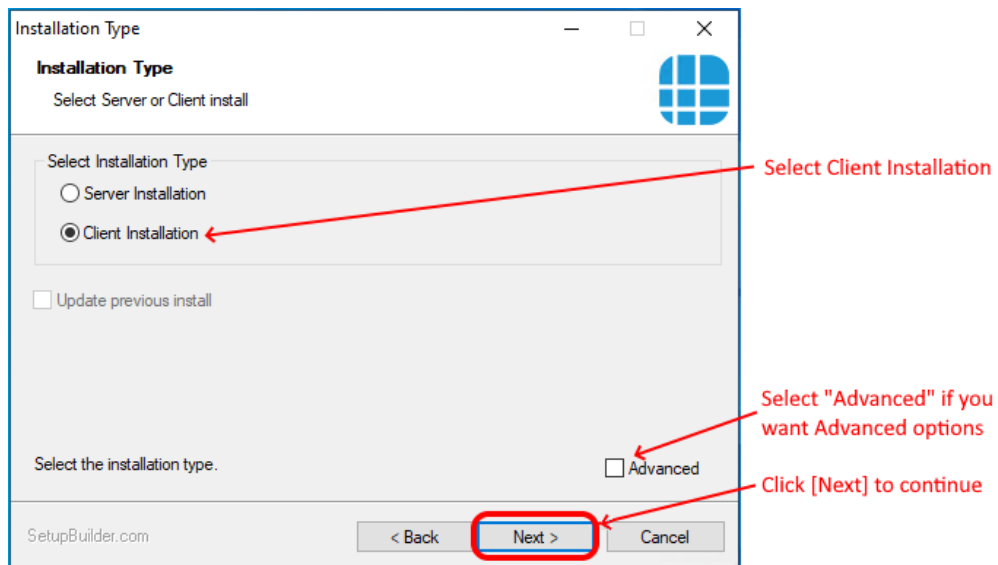


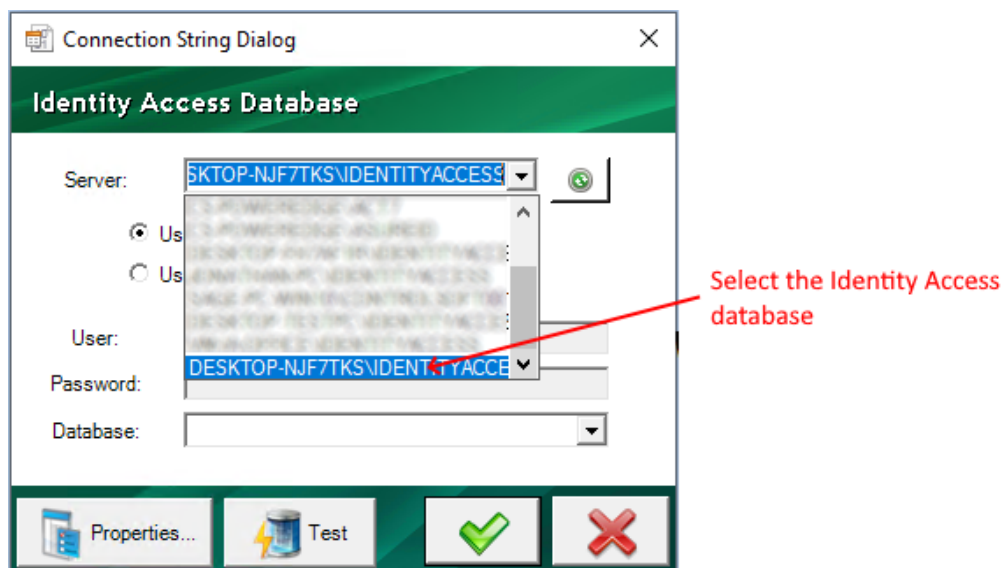
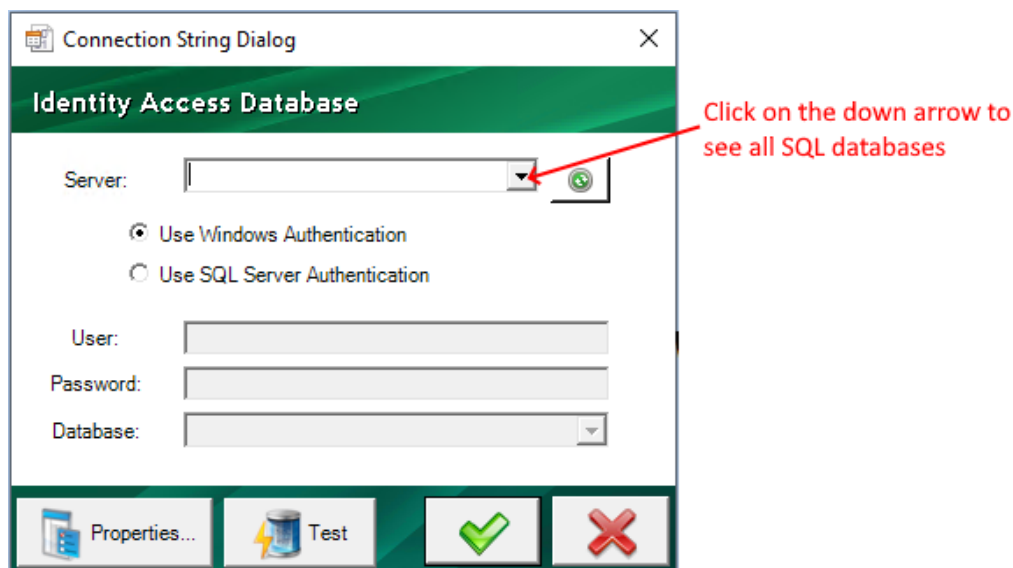
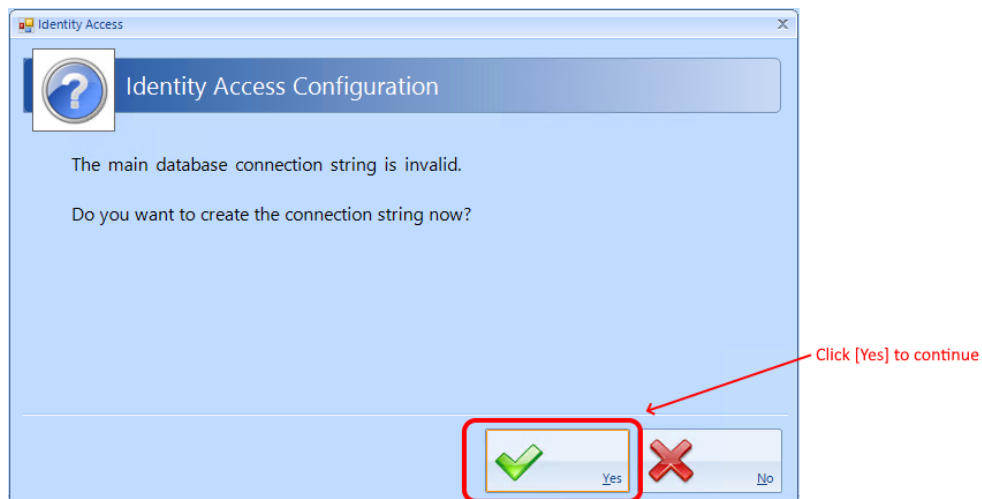
Press [Next]

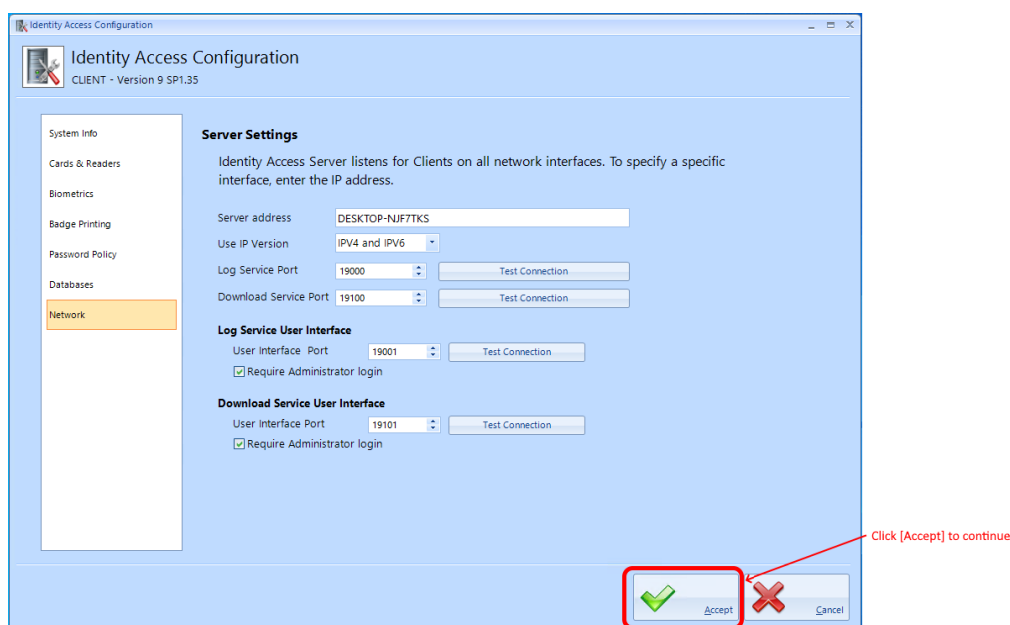
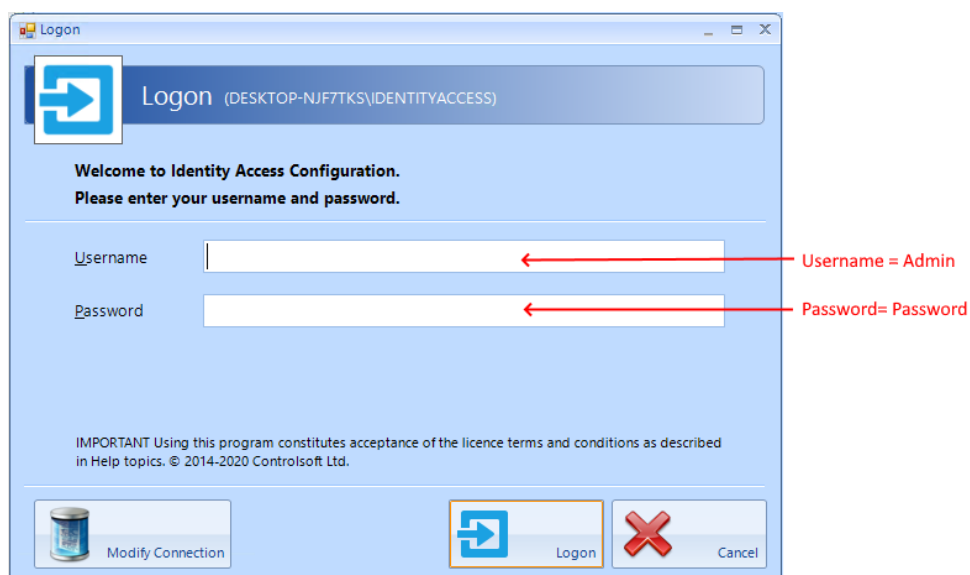
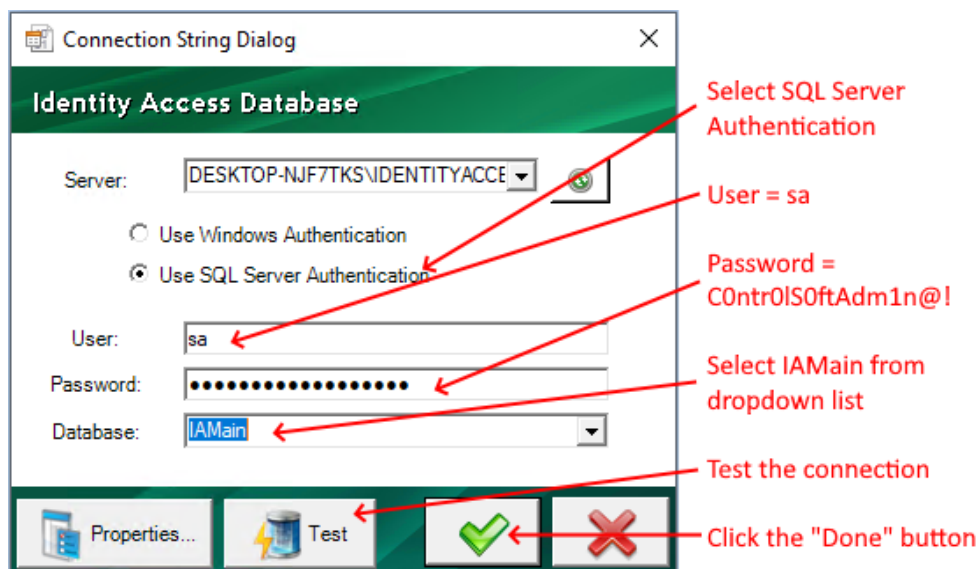
***NOTE: If your system does not meet the minimum specification, the offending parameter will be displayed in red, not green. After pressing [Next], you will be warned again.***

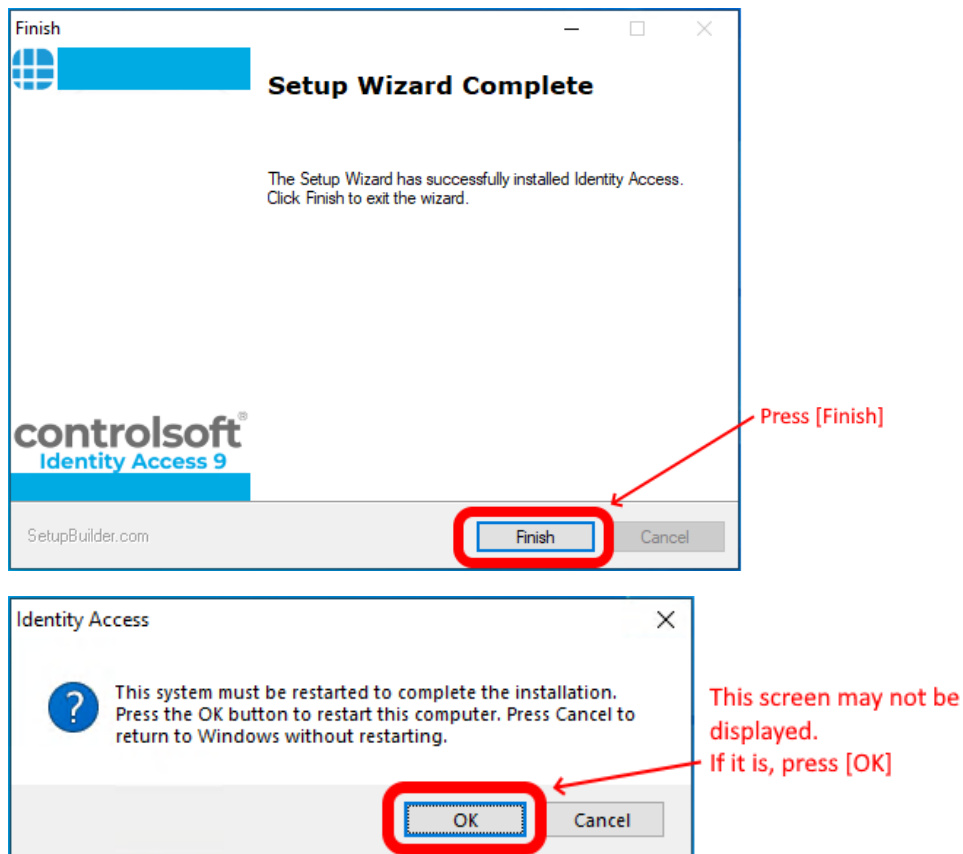


***NOTE: Controlsoft may refuse to support the system if the PC does not meet the minimum recommendations***





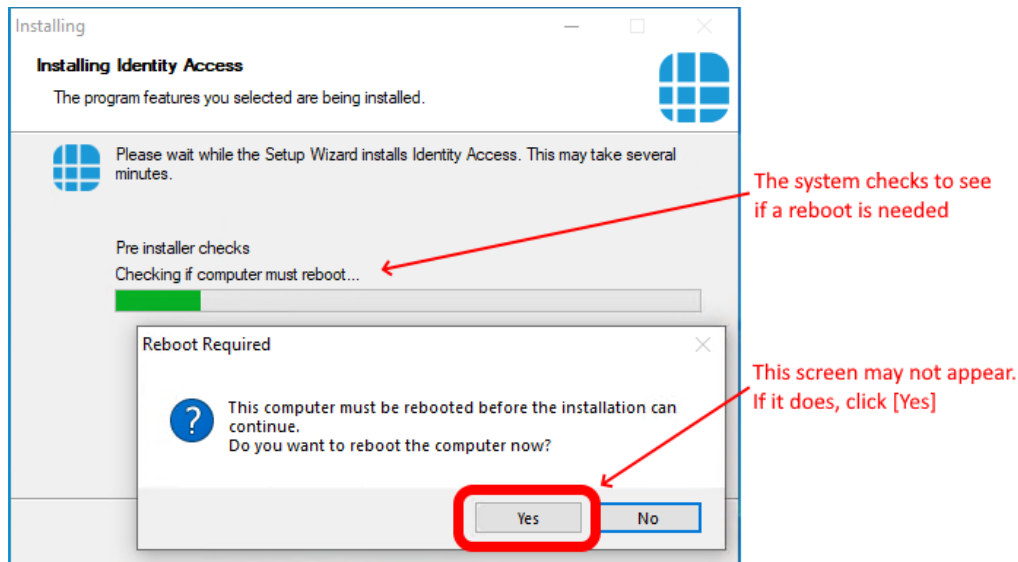




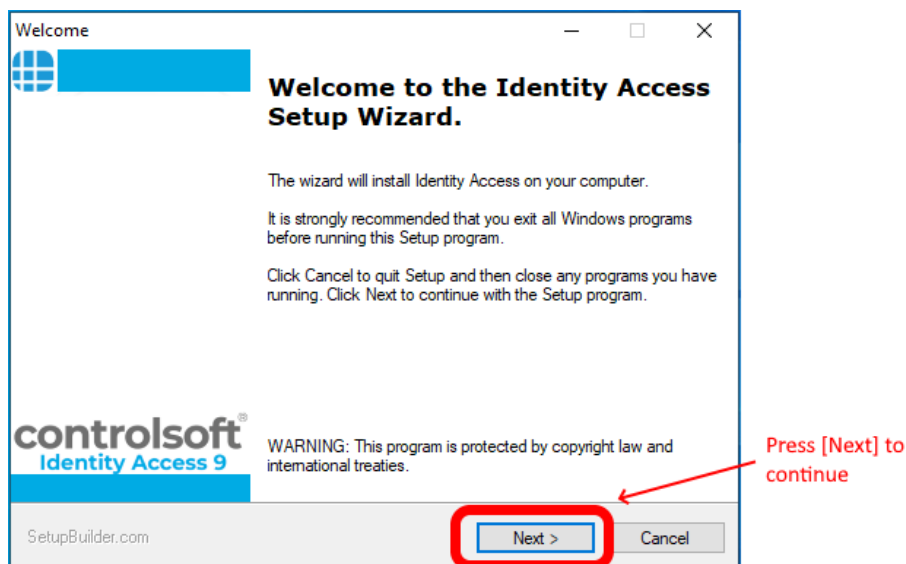
**NOTE:** When all the software has been installed, you may re-enable your antivirus software.

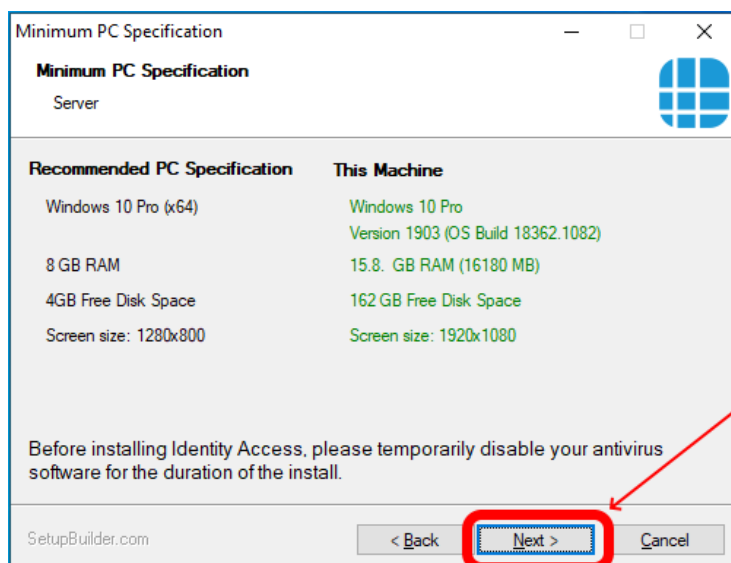
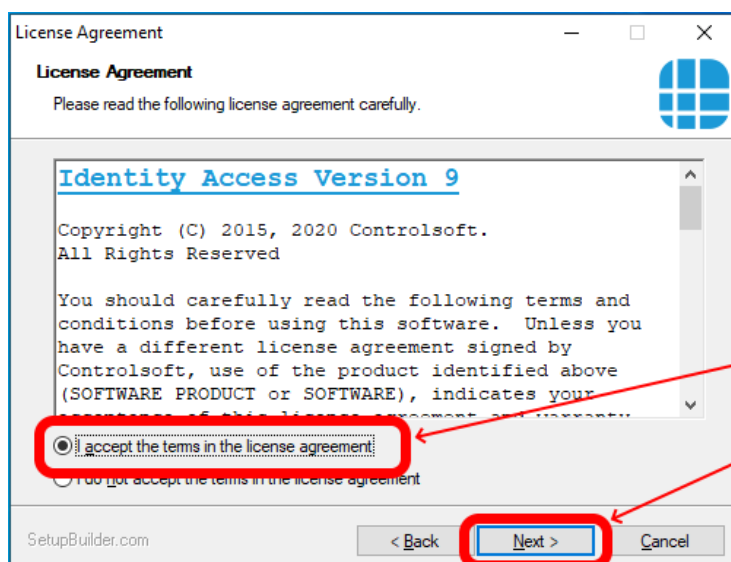
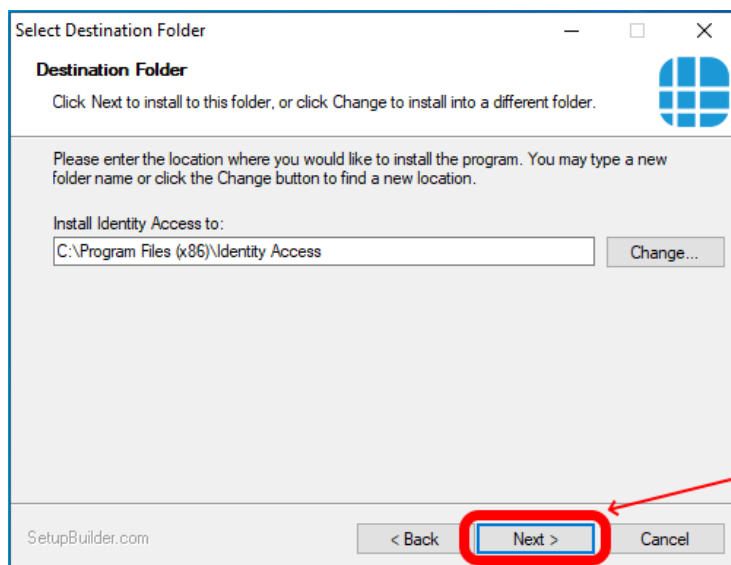
## 2.5 Upgrading IA Software

To upgrade an existing installation of Identity Access, double click the file **Install\_IdentityAccess.exe**



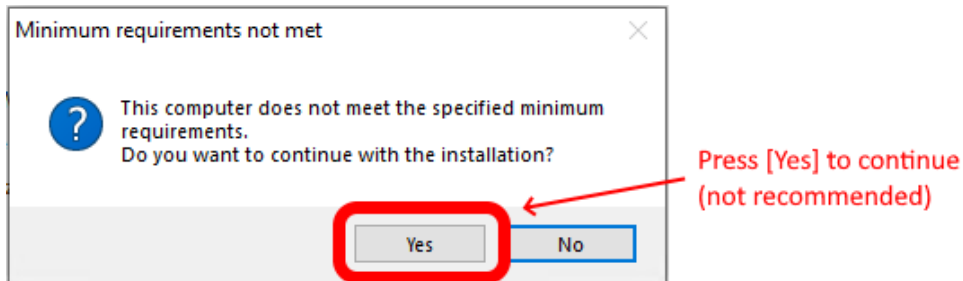
If the system reboots, the installation will recommence automatically.



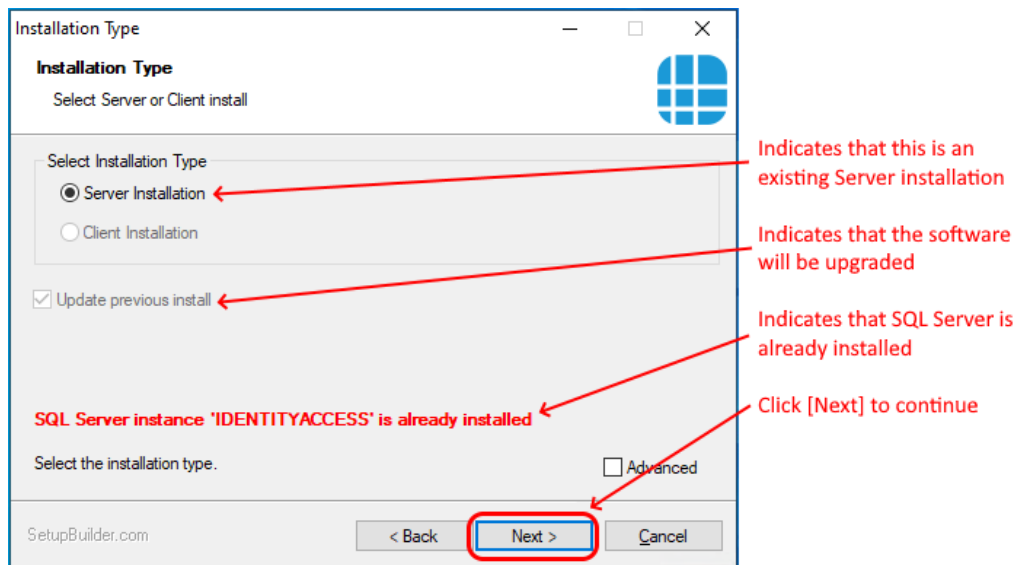




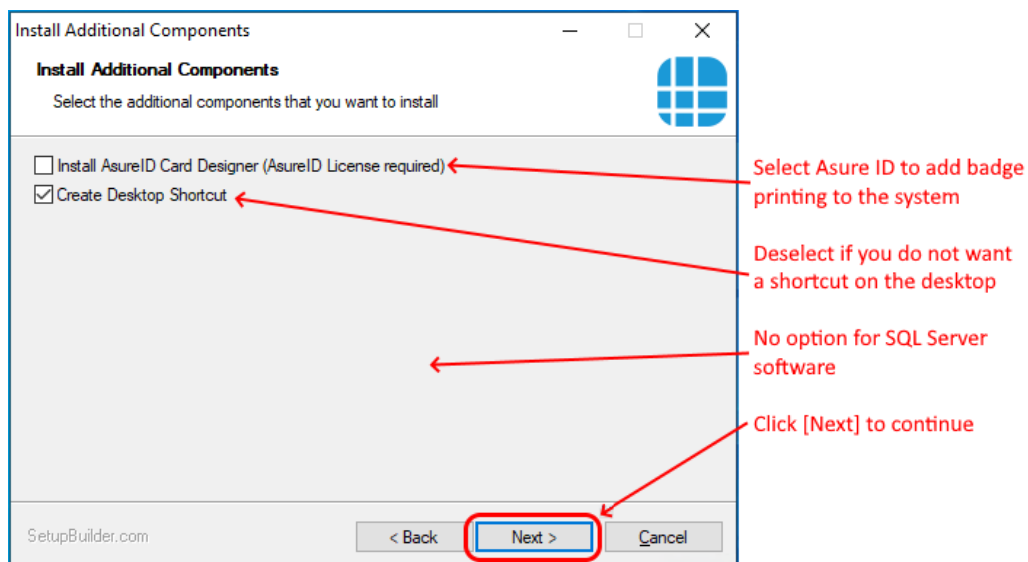
***NOTE: If your system does not meet the minimum specification, the offending parameter will be displayed in red, not green. After pressing [Next], you will be warned again.***

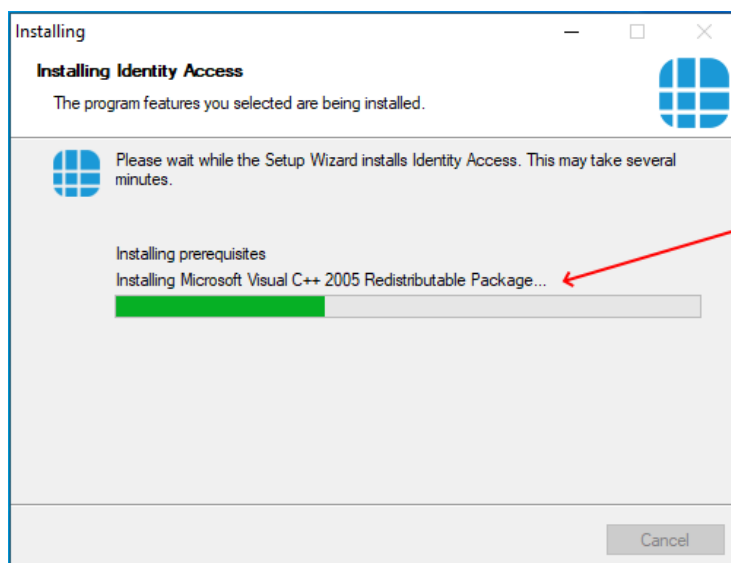
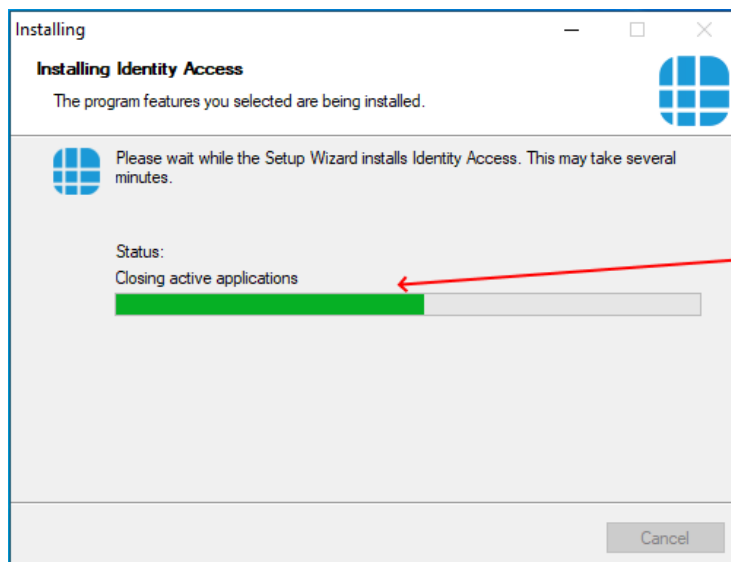
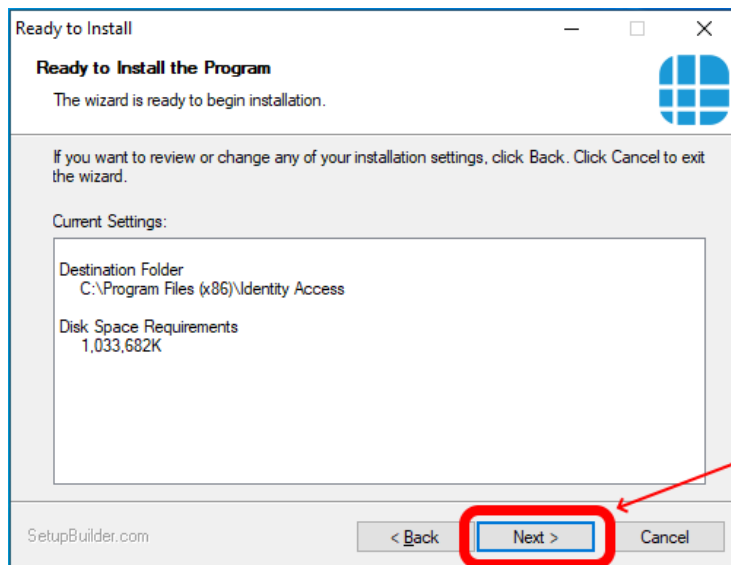


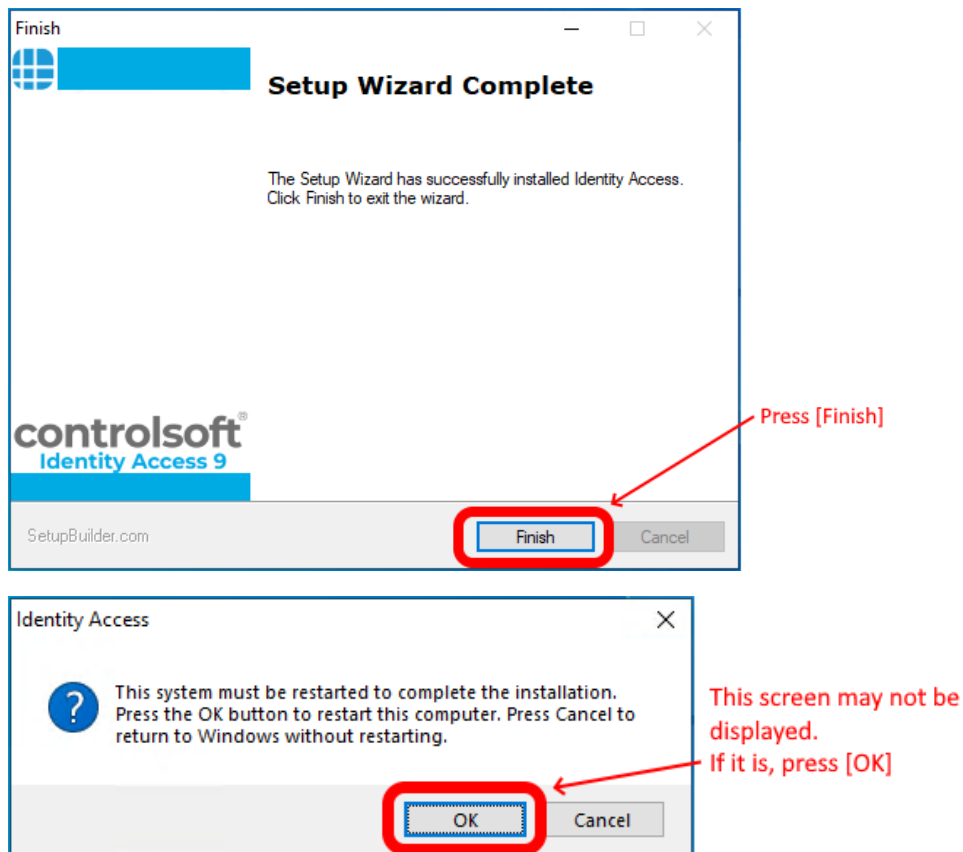
***NOTE: Controlsoft may refuse to support the system if the PC does not meet the minimum recommendations***



If advanced install options are required, select the "Advanced" option before clicking [Next]







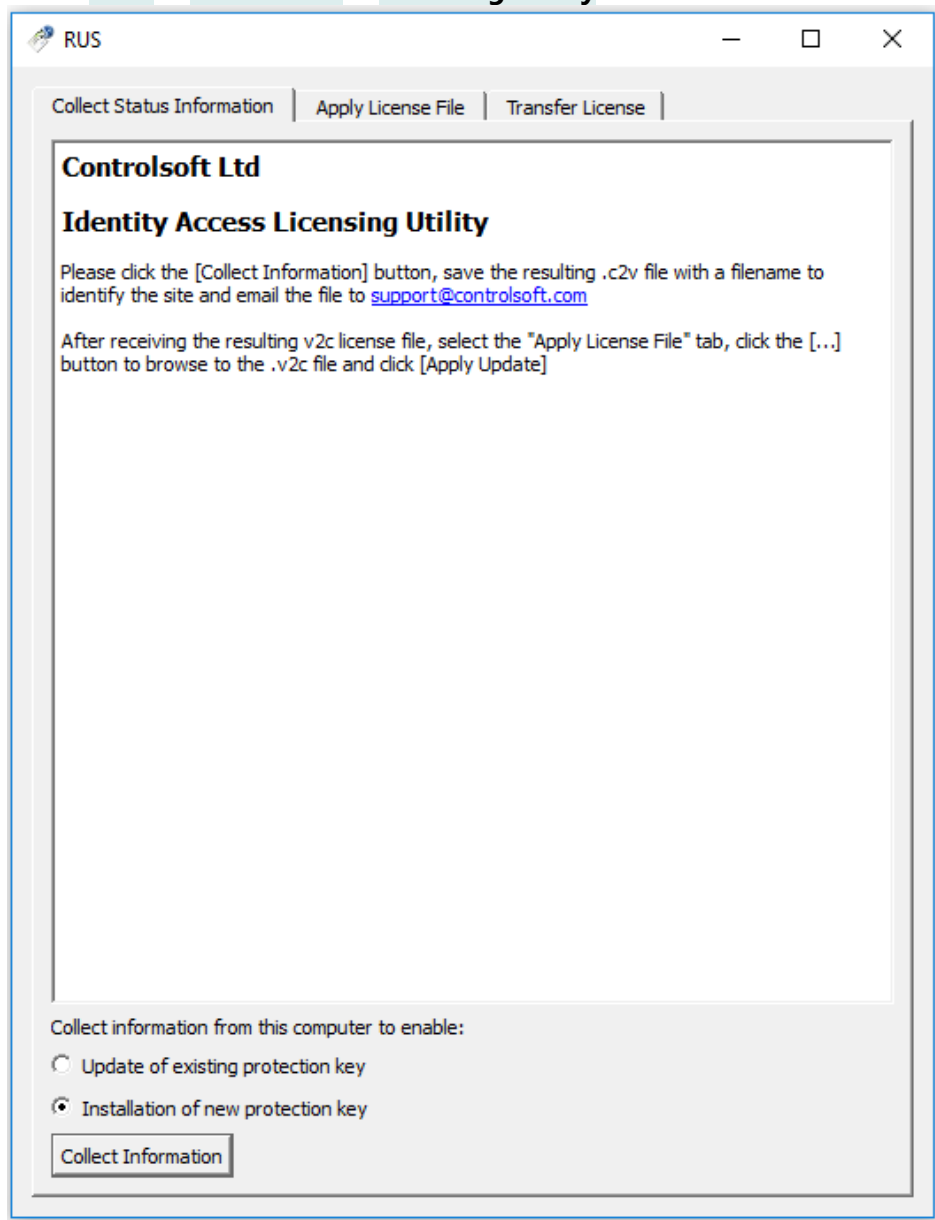
***NOTE: Following an upgrade from Identity Access v8 or earlier, the profiles for the Morpho readers may default to "02. Biometric Only - Standalone Mode". Please ensure that you check the profile for each Morpho reader and select the appropriate profile.***

## 2.6 Licensing the Software

The Identity Access software is free to use, but with certain restrictions. A licence is required to use the features as indicated in the introduction (see [Introduction](#) <sup>8</sup>).

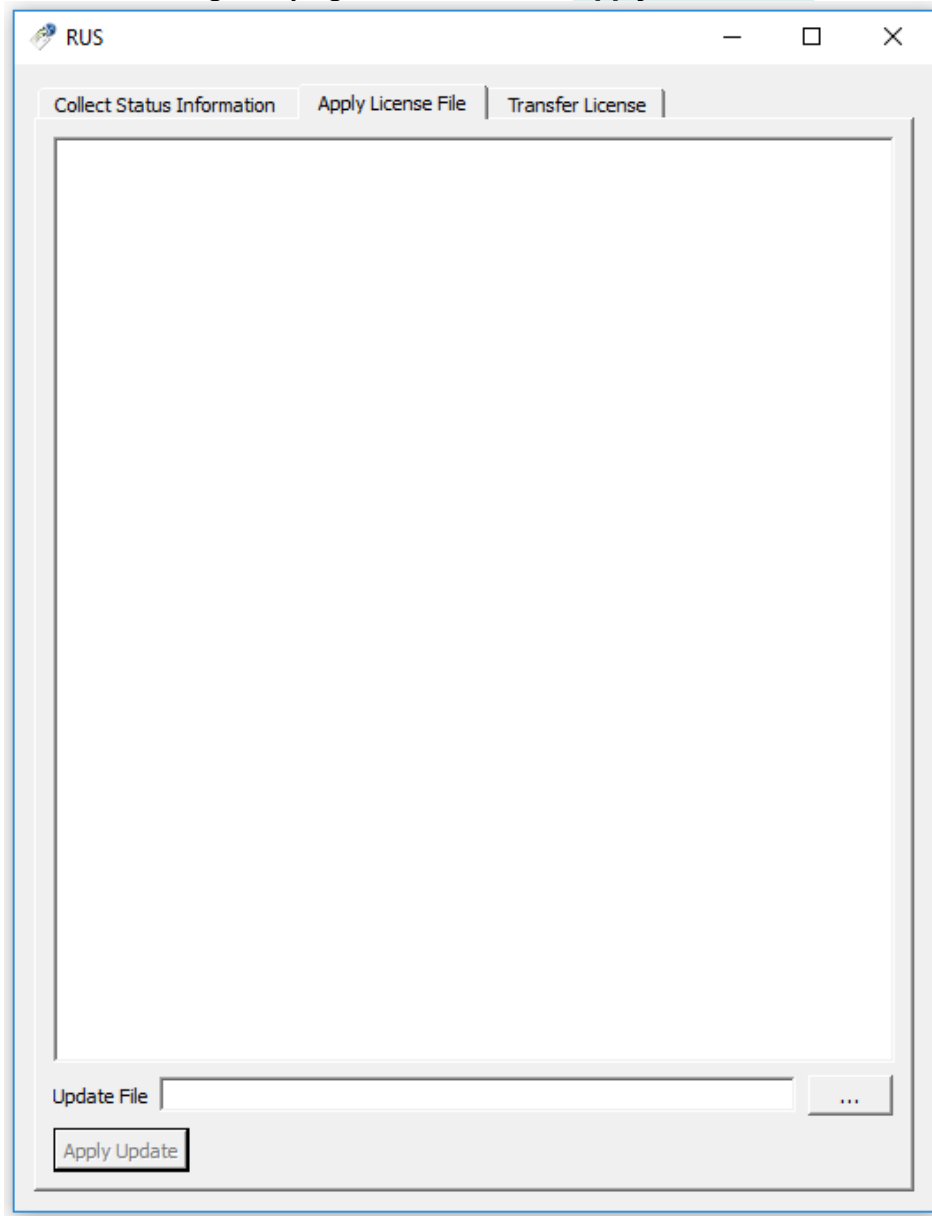
Once you have purchased your licence, follow the instructions below to apply it.

1. Select **Start** > **Controlsoft** > **Licensing Utility**

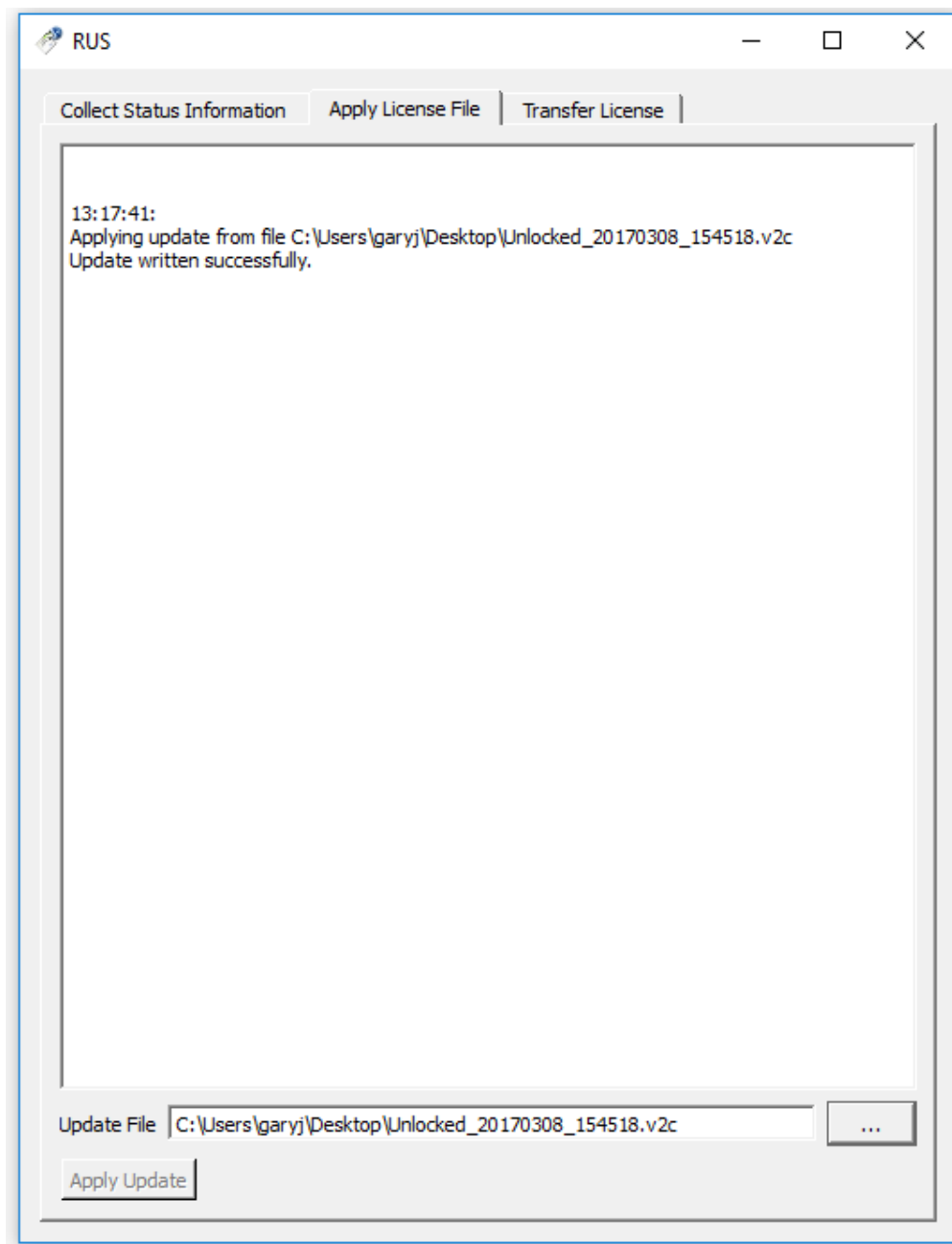


2. Ensure that **Installation of new protection key** is selected and click **[Collect Information]**
3. Save the resulting c2v file on the desktop with a name which identifies your site and email the c2v file and your Licence Number to [support@controlsoft.com](mailto:support@controlsoft.com). Controlsoft will then process the licence and email a "v2c" file back to you.
4. Save the v2c file on the desktop, and check that Identity Access, Download Service and Log Service are NOT running.

5. Run the Licensing Utility again and select the **Apply License File** tab



6. Click the [...] button, select the v2c file saved on the desktop then click the **Apply Update** button and check that the licence has been written successfully.



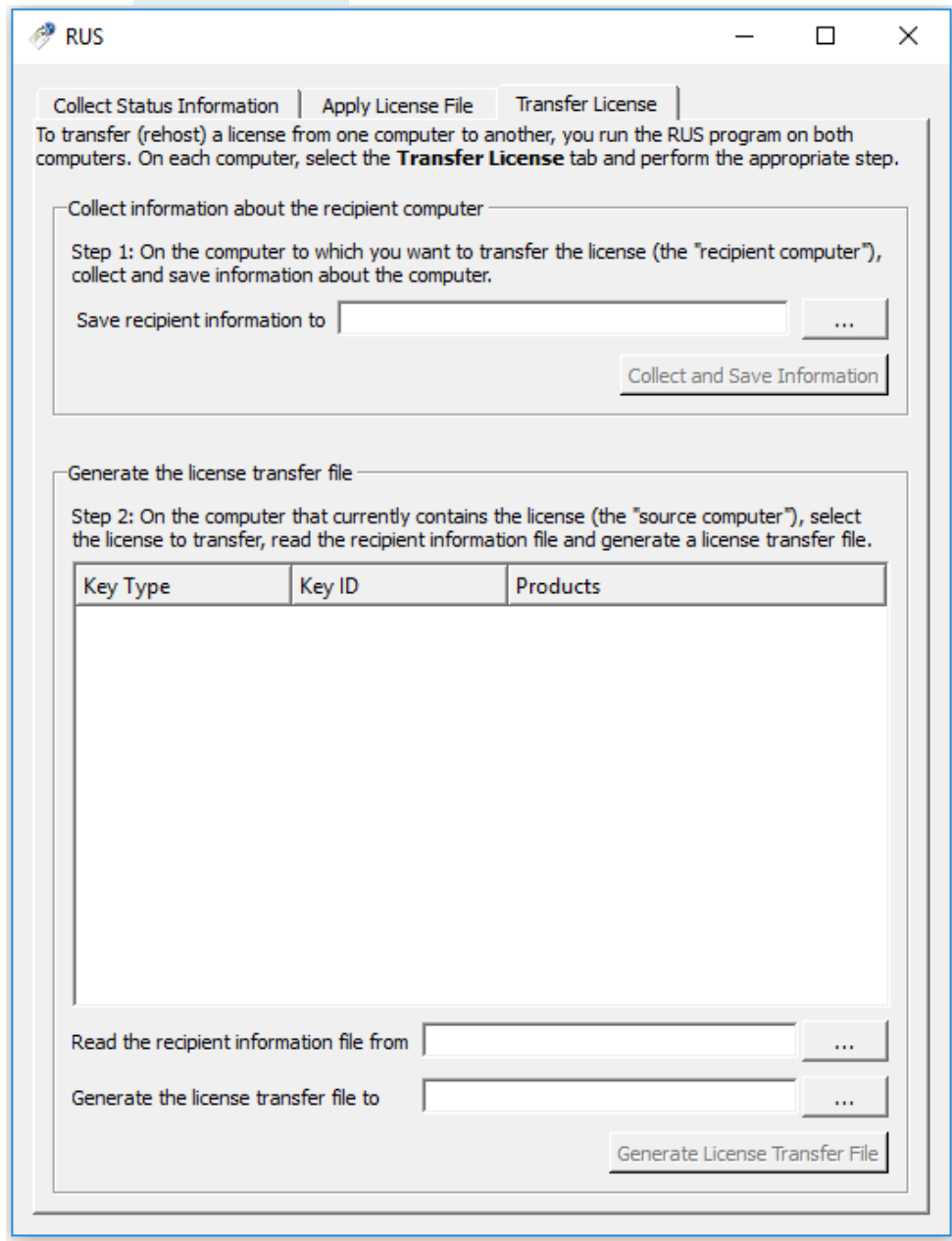
7. Start Identity Access, select **Home** in the menu bar and **About** in the ribbon bar and check that the licence is showing as **VALID**

## 2.7 Transferring a Licence

If you ever need to move a licensed copy of Identity Access software to another computer, it is possible to transfer the licence from the old machine to the new one. To do this, first install Identity Access on the new machine and run the Licensing Utility on BOTH machines:

1. Select **Start** > **Controlsoft** > **Licensing Utility**

2. Select the **Transfer License** tab on both machines



3. On the new machine, select the [...] button against "**Save recipient information to**" and enter a filename and location (e.g. on a flash drive or network drive) for the ".id" file, then select **[Collect and save Information]**.
4. On the old machine, select the [...] button against "**Read the recipient information file from**" and select the .id file on the flash drive / network drive.
5. On the old machine, select the [...] button against "**Generate the license transfer file to**" and enter a filename and location on the flash drive or network drive for the ".h2h" file



6. Select the **[Generate License Transfer File]** button and select **[Yes]** to confirm that you want to move the licence file.
7. On the new machine apply the .h2h file in the same way as applying a .v2c file as described above.

## 2.8 SQL Server Backup

---

Controlsoft Identity Access Server software (v9.1.52 and later) includes a built in Backup feature.

To configure backups, run IA Configuration (see [IA Configuration - Backup](#)<sup>[81]</sup>).

To manually initiate a backup, use the Backup button in the Tools menu in IA User Interface (see [Identity Access Tools Tab](#)<sup>[108]</sup>).

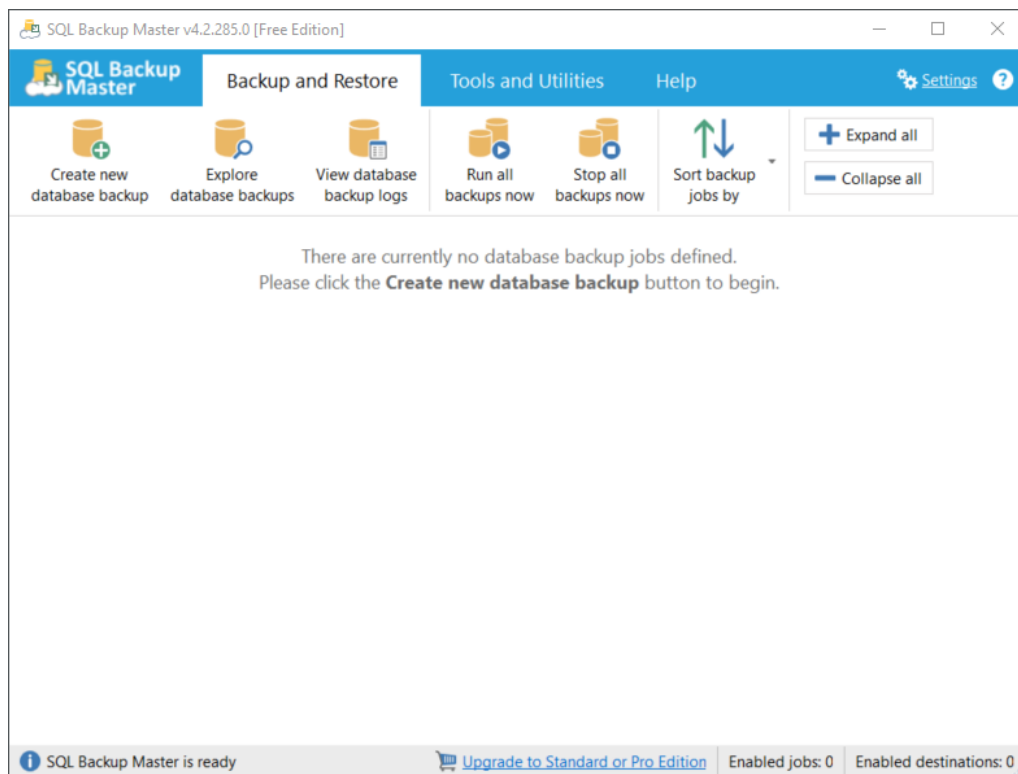
Scheduled backups are initiated by the IA Log Service (see [Log Service](#)<sup>[312]</sup>).

**Note:** Previous versions of Controlsoft Identity Access software (v9.1.44 and earlier) were supplied with a copy of a third party utility called **SQL Backup Master**. Configuration of SQL Backup Master was as follows:

- Run the Install Identity Access utility
- Open the **V9 Tools & Extras** folder followed by **SQL Backup Master**
- Run the file **sbm-setup.exe**.

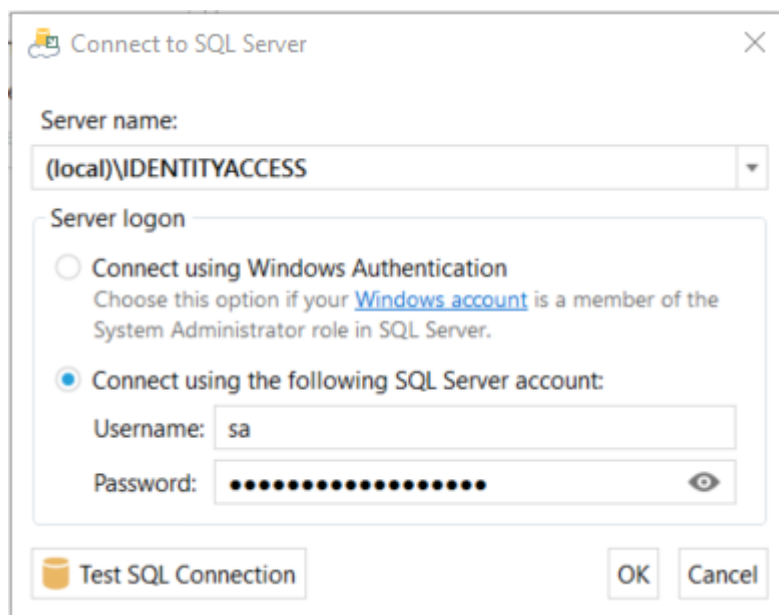
It is important that you create a backup scheme so the end users' databases are backed up regularly to an external or network drive **NOTE: Do not backup to the same drive that holds the database itself**. If the PC suffers a hard drive failure, it is much simpler and quicker to install Identity Access on a new PC or hard drive and restore the backup, rather than reprogramming all the hardware and re-enrol every user.

To create a backup scheme, Click the **Start** button, **SQL Backup Master**, then select **SQL Backup Master**



Select **Create new database backup** followed by **Choose SQL server**

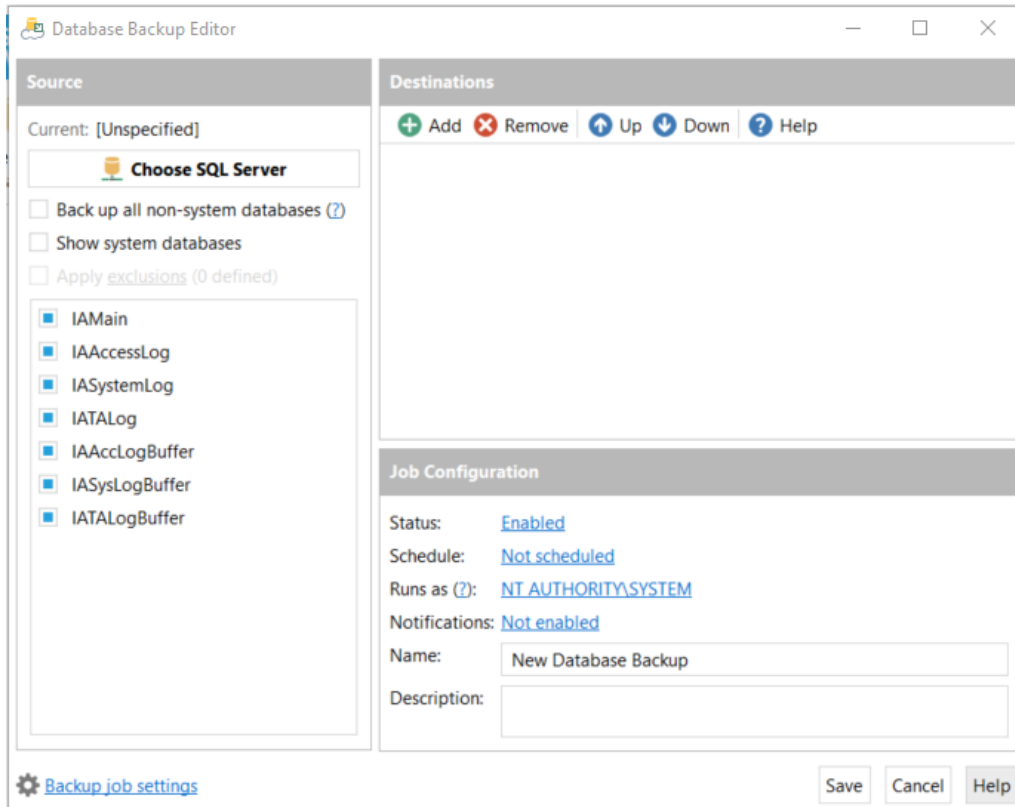
Under Server Name, choose **(local)\IDENTITYACCESS** and configure as shown below:



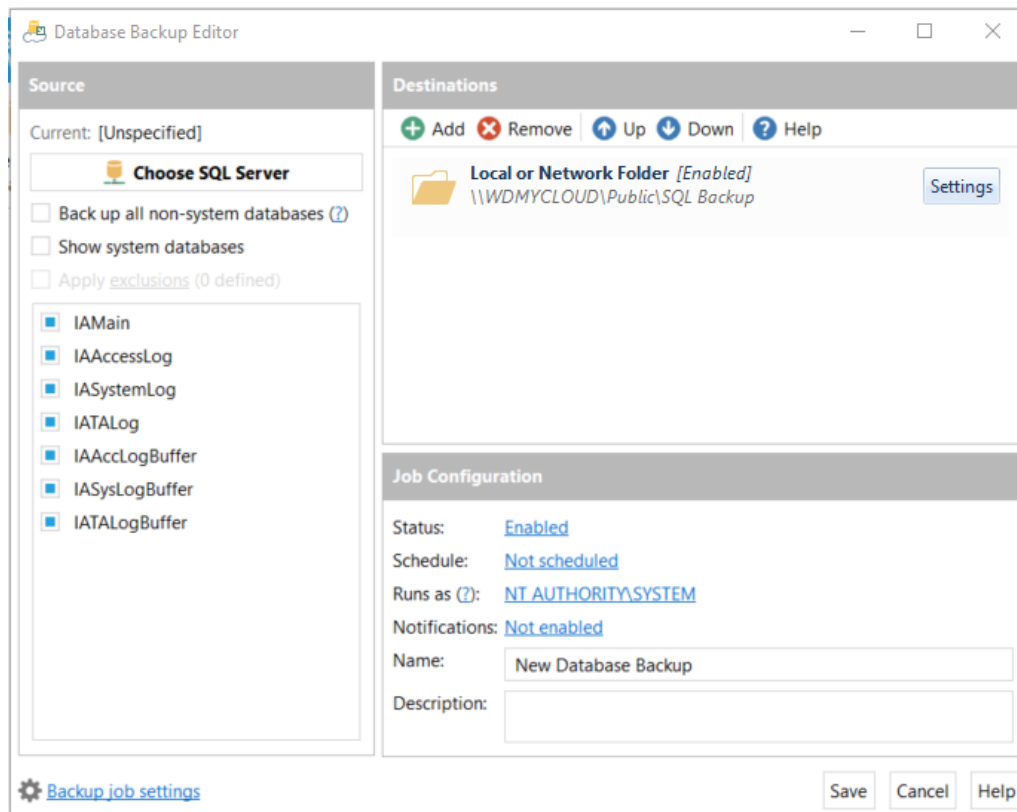
NOTE: Password is C0ntr0IS0ftAdm1n@!

Select **[Test SQL Connection]** and check that the test is successful

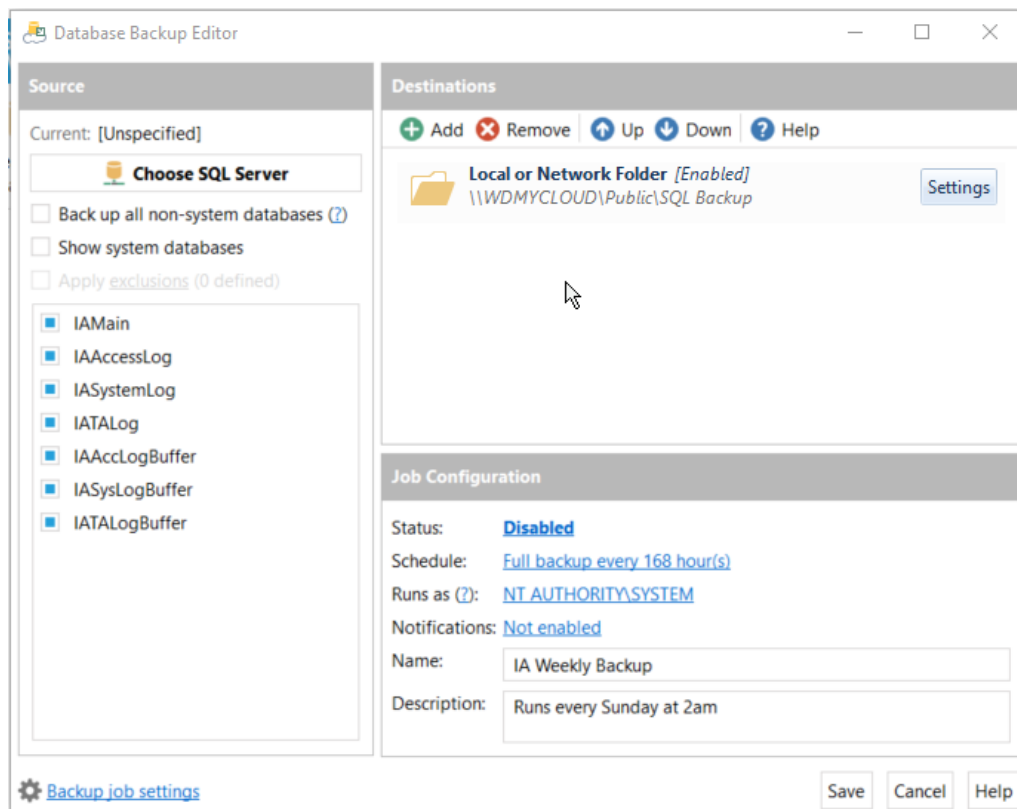
Configure the software to backup all 7 databases (Main, Access Log, System Log and Time & Attendance Log, Access Log Buffer, System Log Buffer and Time & Attendance Log Buffer):



Add a destination on a network folder:



Finally, set up a schedule for the backup and, if required, email notification:



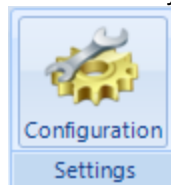
Save the profile and the customer's data will now be regularly backed up.

SQL Backup Master has its own help files, please refer to this documentation for further assistance.

## 2.9 Identity Access Configuration

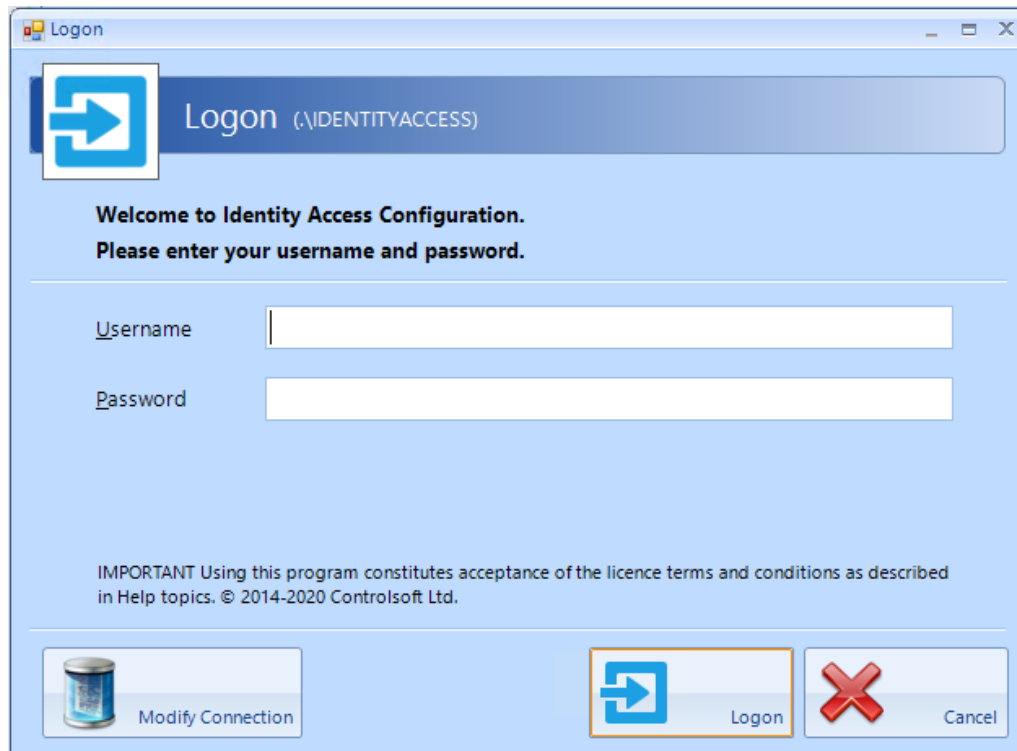
The **Identity Access Configuration** tool is used to configure certain features of the Identity Access server software, such as defining a number of system options. The tool can be found by selecting the **[Start]** button, followed by **Controlsoft** and **IA Configuration**.

If Identity Access is already running, simply click the Configuration icon in the



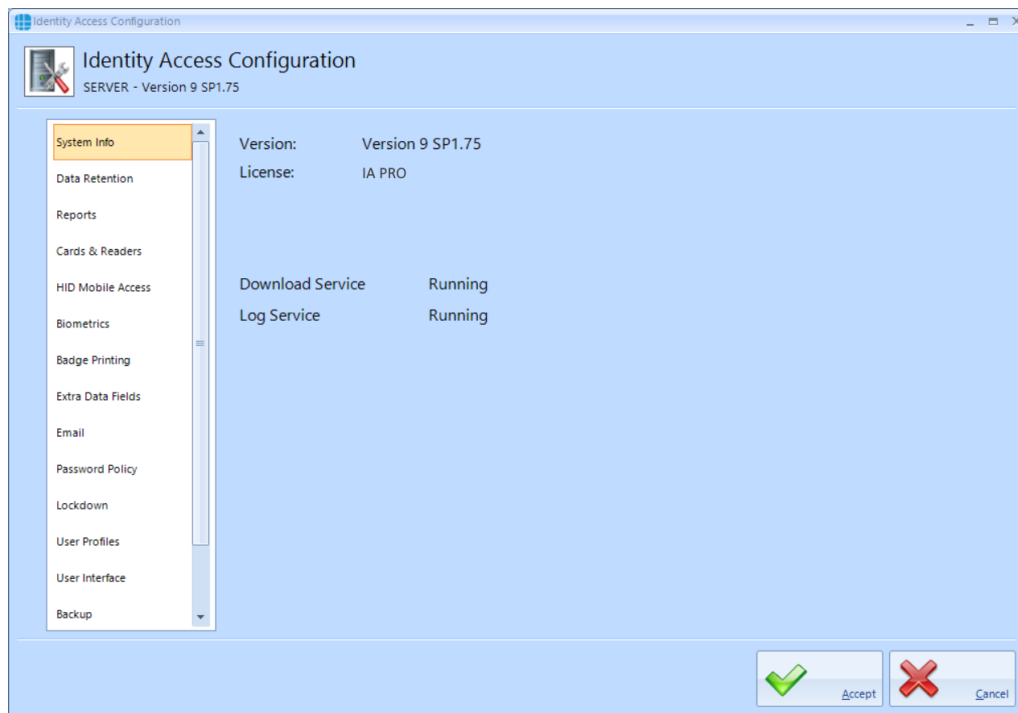
Setup menu:

When run, enter the same Username and Password as used for the Identity Access User Interface.

A screenshot of a Windows-style window titled 'Logon'. The window has a light blue background. At the top left is a blue square icon with a white right-pointing arrow. To its right, the text 'Logon (\IDENTITYACCESS)' is displayed. Below this, a message reads: 'Welcome to Identity Access Configuration. Please enter your username and password.' There are two text input fields: the first is labeled 'Username' and the second is labeled 'Password'. At the bottom of the window, there is a line of small text: 'IMPORTANT Using this program constitutes acceptance of the licence terms and conditions as described in Help topics. © 2014-2020 Controlsoft Ltd.' Below this text are three buttons: on the left, a button with a blue cylinder icon and the text 'Modify Connection'; in the center, a button with the blue arrow icon and the text 'Logon'; and on the right, a button with a red 'X' icon and the text 'Cancel'.

### 2.9.1 IA Configuration - System Info

This screen displays basic system information as described below:



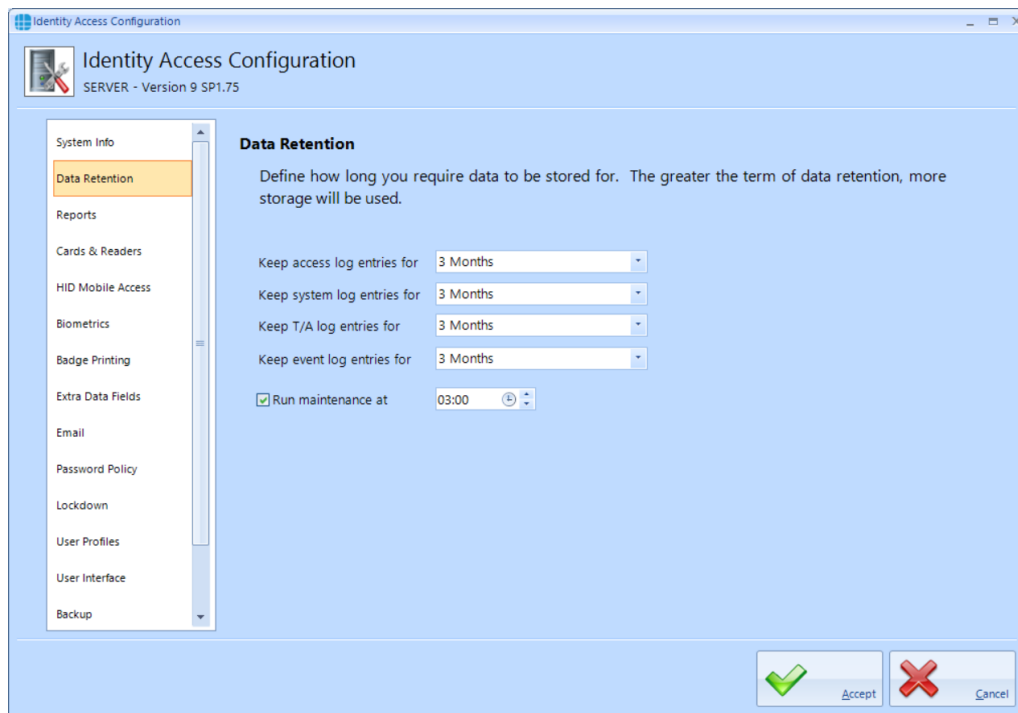
**Version** is the version of Identity Access installed

**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.

The remaining information defines whether the Download Service and Log Service are running correctly

### 2.9.2 IA Configuration - Data Retention

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



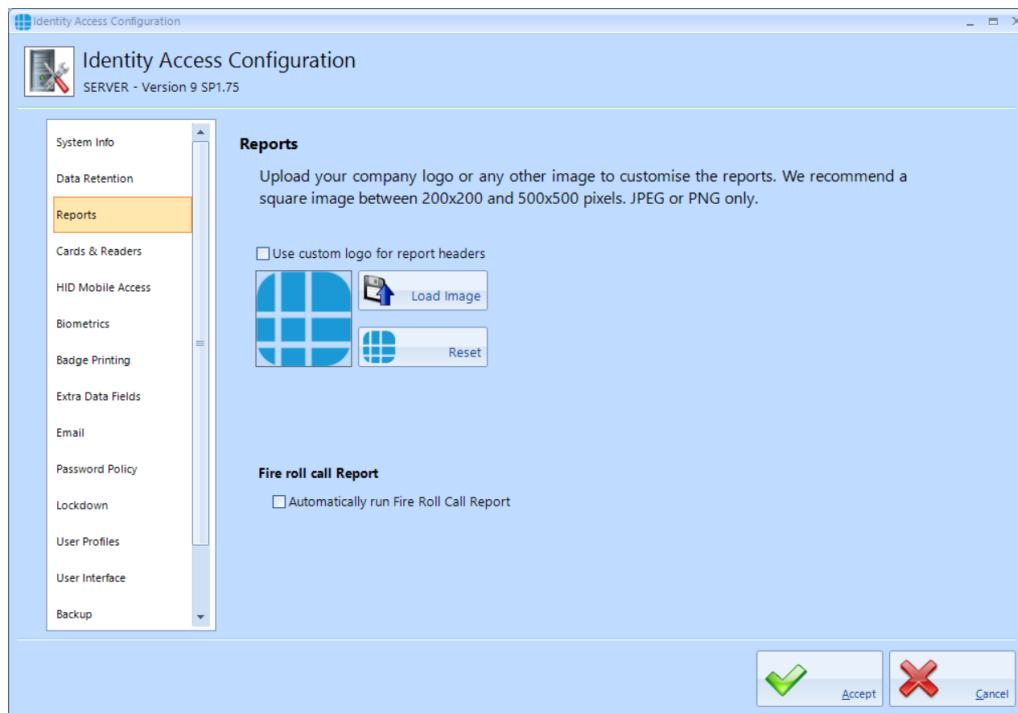
Each of the databases can be independently saved for 1 day, 1 week, 2 weeks, 1 month, 2 months, 3 months, 6 months, 1 year, 2 years, 3 years, 4 years, 5 years or indefinite

**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.***

### 2.9.3 IA Configuration - Reports

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



**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.

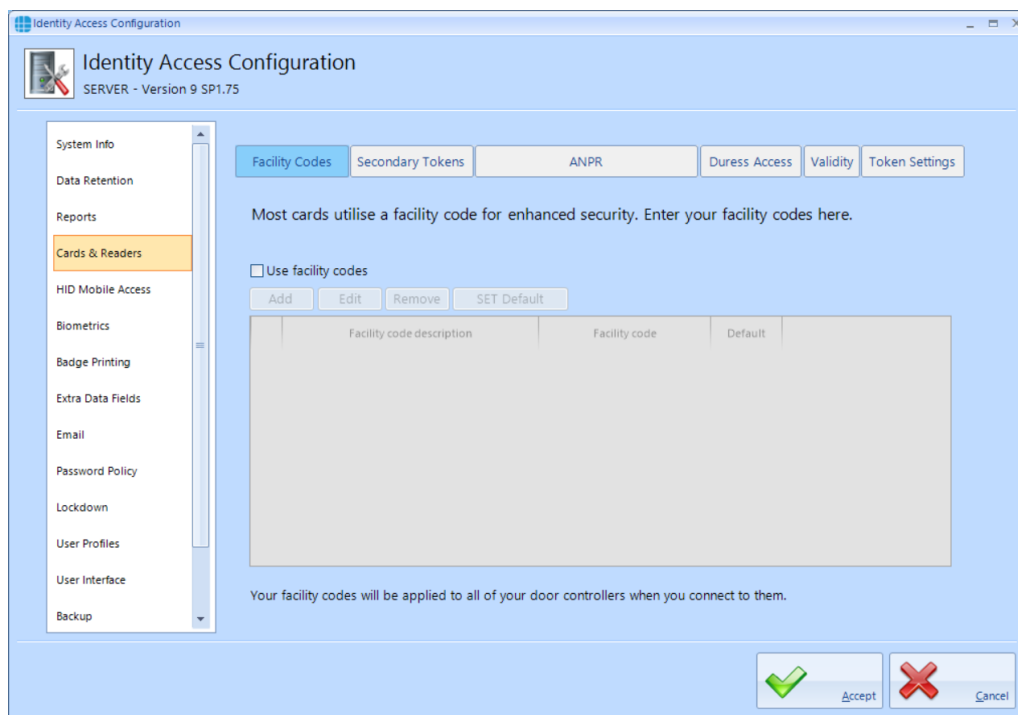
**Automatically run Fire Roll Call Report** - untick this option if you do not want reports automatically printed when is fire alarm condition is detected.

#### 2.9.4 IA Configuration - Cards & Readers

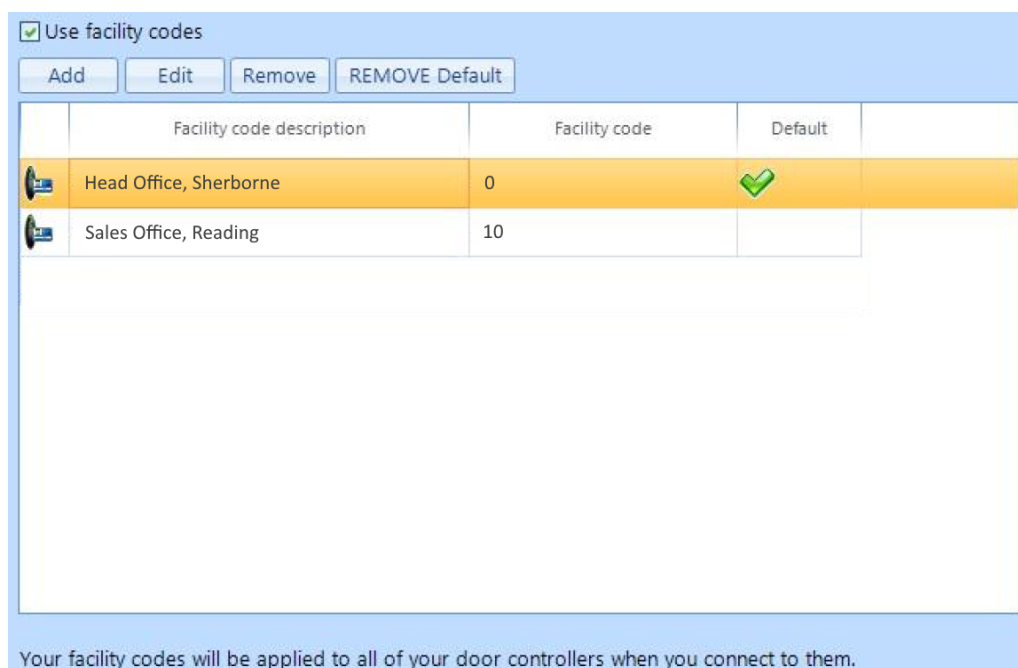
Several options can be configured within the Cards & Readers tab as described below:

##### Facility Codes





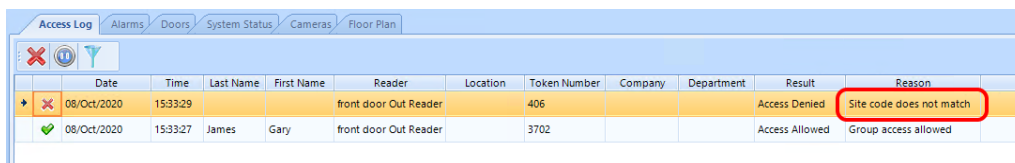
If the access control system uses Facility codes, tick the option **Use facility codes**, then click the [Add] button to enter the relevant Facility Codes in use. For example:



When creating Users, the relevant Facility Code is then allocated to the user (see [User General](#) <sup>222</sup>).

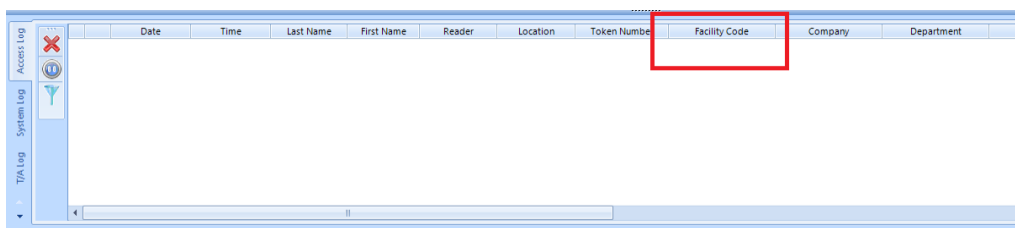
**NOTE: if a card with an incorrect Facility Code is presented to a reader, access will be denied, and the Dashboard will show**

***the Reason as Site code does not match as in the example below:***



	Date	Time	Last Name	First Name	Reader	Location	Token Number	Company	Department	Result	Reason
✖	08/Oct/2020	15:33:29			front door Out Reader		406			Access Denied	Site code does not match
✔	08/Oct/2020	15:33:27	James	Gary	front door Out Reader		3702			Access Allowed	Group access allowed

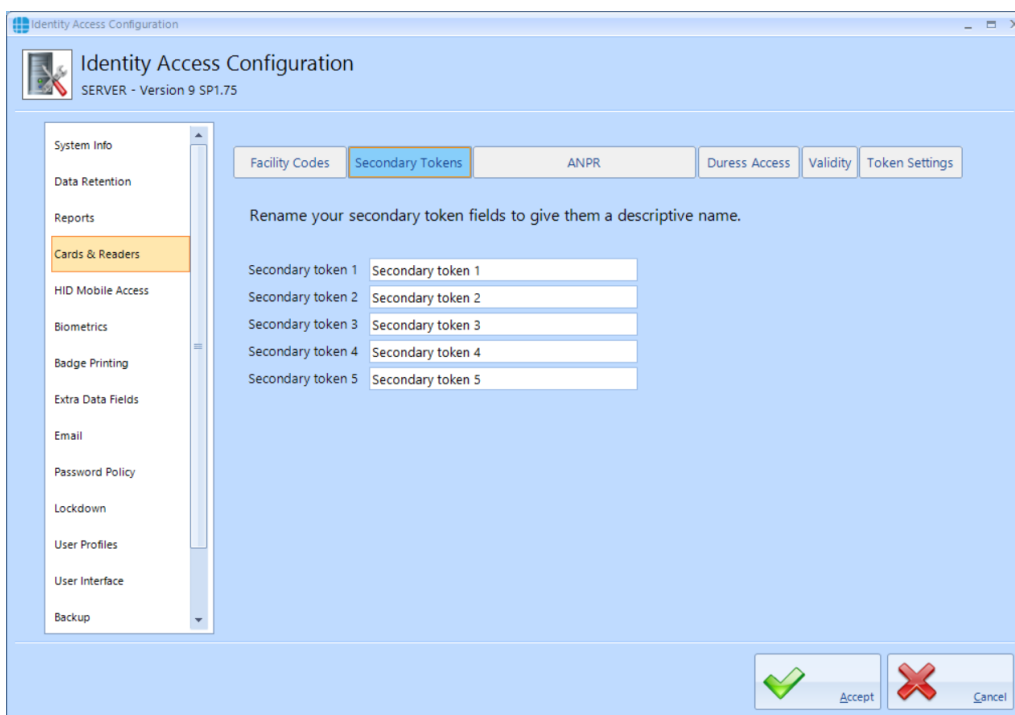
To determine the Facility Code on the card, check the activity in the Access Log viewer:



	Date	Time	Last Name	First Name	Reader	Location	Token Number	Facility Code	Company	Department
--	------	------	-----------	------------	--------	----------	--------------	---------------	---------	------------

## Secondary Tokens

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



Identity Access Configuration  
SERVER - Version 9 SP1.75

Facility Codes **Secondary Tokens** ANPR Duress Access Validity Token Settings

Rename your secondary token fields to give them a descriptive name.

Secondary token 1	Secondary token 1
Secondary token 2	Secondary token 2
Secondary token 3	Secondary token 3
Secondary token 4	Secondary token 4
Secondary token 5	Secondary token 5

Accept Cancel

Enter text strings against each field as appropriate, for example:

Rename your secondary token fields to give them a descriptive name.

Secondary token 1	Mobile Access
Secondary token 2	Secondary token 2
Secondary token 3	Secondary token 3
Secondary token 4	Secondary token 4
Secondary token 5	ANPR Number Plate

## ANPR

The Identity Access software is compatible with the HIK Vision ANPR camera, and is capable of calculating the relevant token number from the Number Plate entered.

The screenshot shows the 'Identity Access Configuration' window, version 9 SP1.75. The left sidebar contains a list of configuration categories: System Info, Data Retention, Reports, Cards & Readers (highlighted), HID Mobile Access, Biometrics, Badge Printing, Extra Data Fields, Email, Password Policy, Lockdown, User Profiles, User Interface, and Backup. The main area has several tabs: Facility Codes, Secondary Tokens, ANPR (selected), Duress Access, Validity, and Token Settings. The ANPR tab contains the following text: 'If you are utilising a supported HIK Vision ANPR camera, enable it and define which Secondary Token field you want to use to store vehicle number plates.' Below this is a checkbox labeled 'Use HIK Vision ANPR' which is currently unchecked. Underneath the checkbox is the text 'Store calculated HIK Vision ANPR number in' followed by a dropdown menu currently showing 'Secondary token 5'. At the bottom right of the window are 'Accept' and 'Cancel' buttons with green and red icons respectively.

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

If you are utilising a supported HIK Vision ANPR camera, enable it and define which Secondary Token field you want to use to store vehicle number plates.

☒ Use HIK Vision ANPR

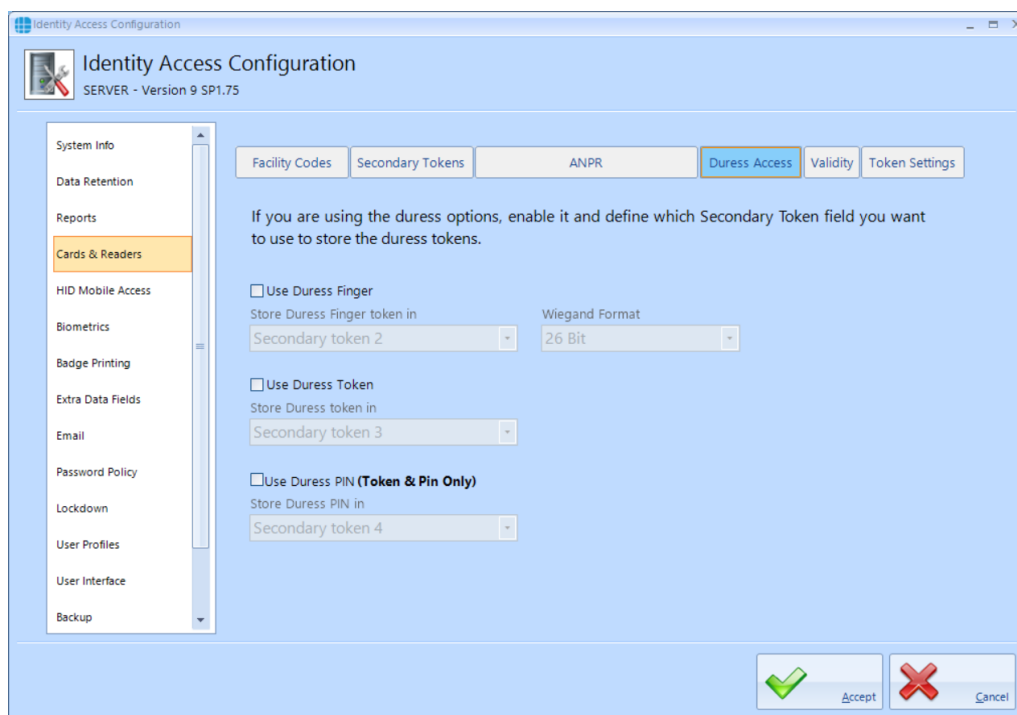
Store calculated HIK Vision ANPR number in

Secondary token 5

***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.

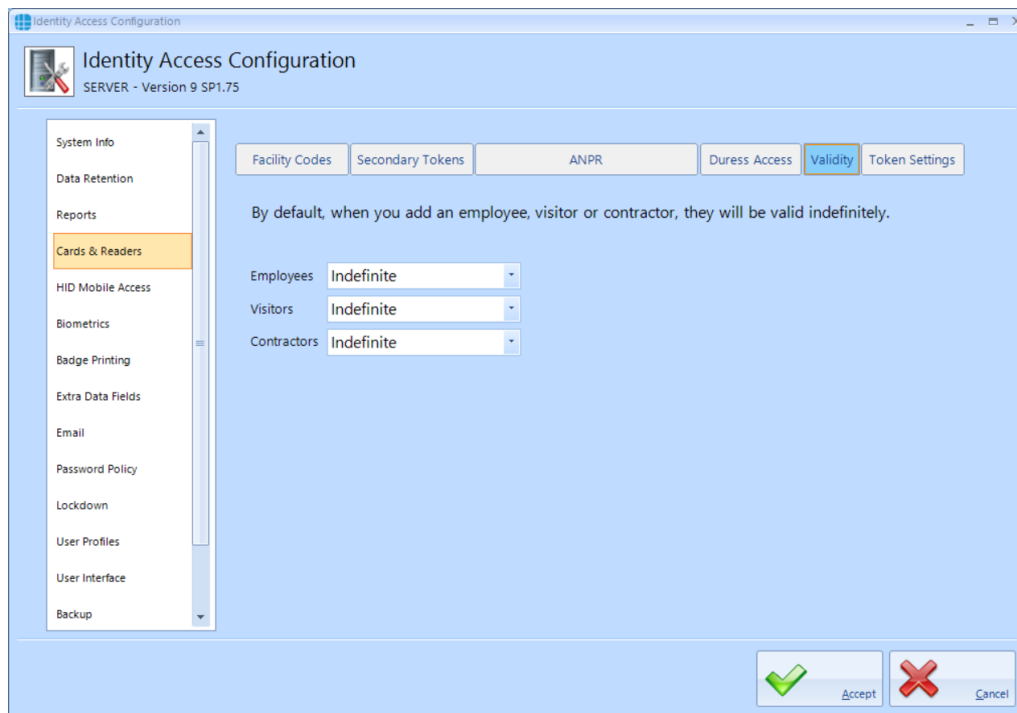


If using duress finger with Morpho fingerprint readers, ensure that the **Use Duress Finger** option is ticked, and select which secondary token field will be used to hold the relevant token number.

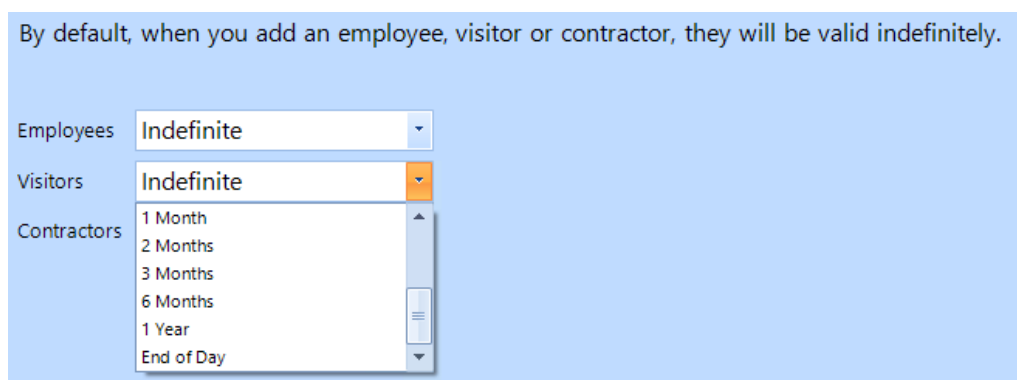
If a duress token is to be used, ensure that the **Use Duress Token** option is ticked, and select which secondary token field will be used to hold the relevant token number.

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.

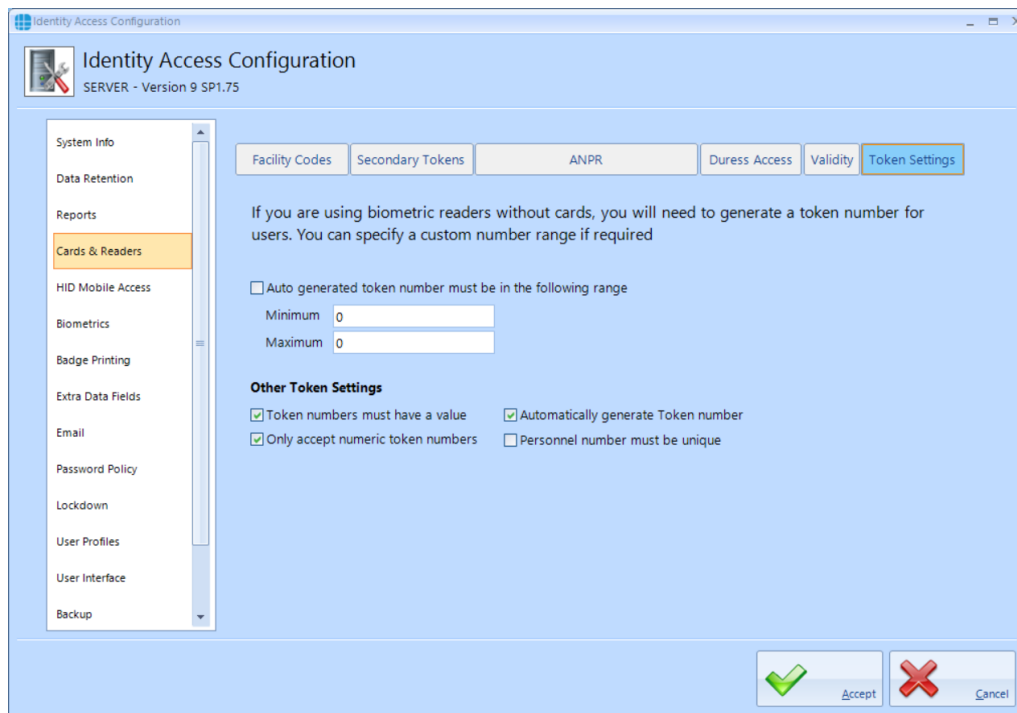
## Validity



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



**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

### 2.9.5 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, so please refer to your vendor for further information on setting up this feature.

The screenshot shows the 'Identity Access Configuration' window, version 9 SP1.75. The left sidebar contains a list of configuration categories: System Info, Data Retention, Reports, Cards & Readers, **HID Mobile Access** (highlighted), Biometrics, Badge Printing, Extra Data Fields, Email, Password Policy, Lockdown, User Profiles, User Interface, and Backup. The main area is titled 'HID Mobile Access Portal' and contains the following fields and options:

- Company ID**: A text input field.
- Client ID**: A text input field.
- Client Secret**: A text input field.
- Options**:
  - ☒ Send email with invitation code to user
  - ☒ Issue Mobile Credential ID with invitation
  - Assign Mobile ID to**: A dropdown menu currently set to 'Primary Token'.
- Advanced**: A radio button option.
- Test**: A button with a 'Mobile Access' icon.

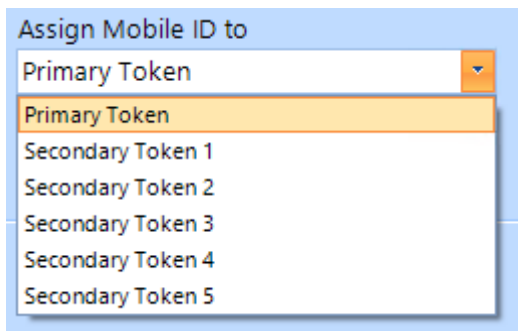
At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

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:

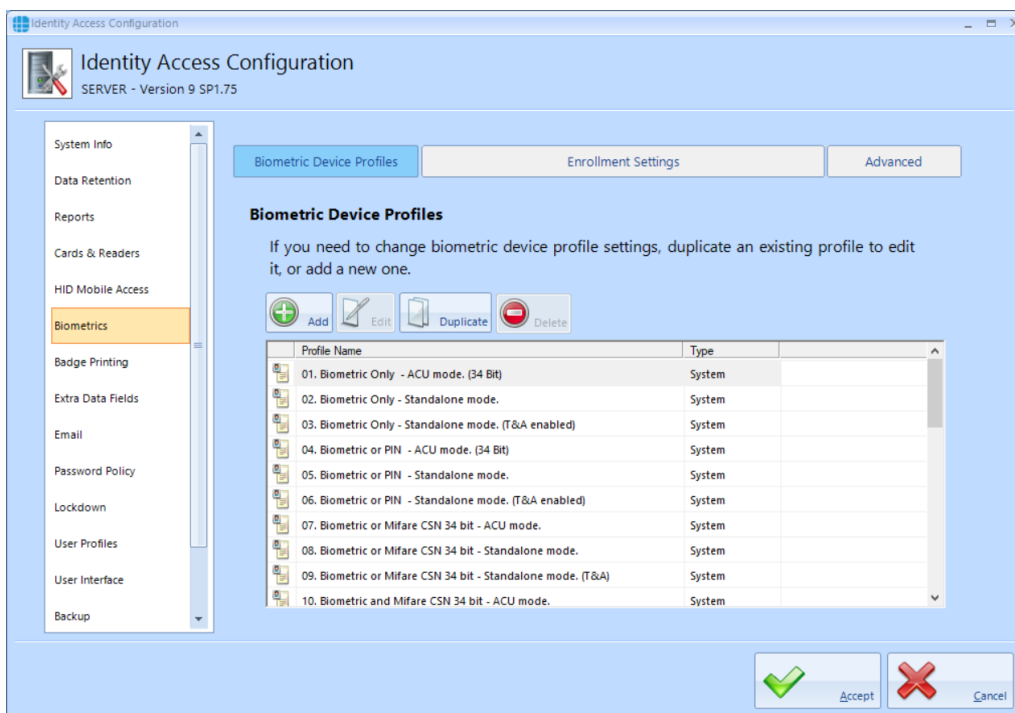


The **Advanced** options allows access to the URL strings for contacting the HID Mobile Portal. The strings must not be changed unless instructed to do so by Controlsoft Technical Support.

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]**.

## 2.9.6 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.**



### 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.

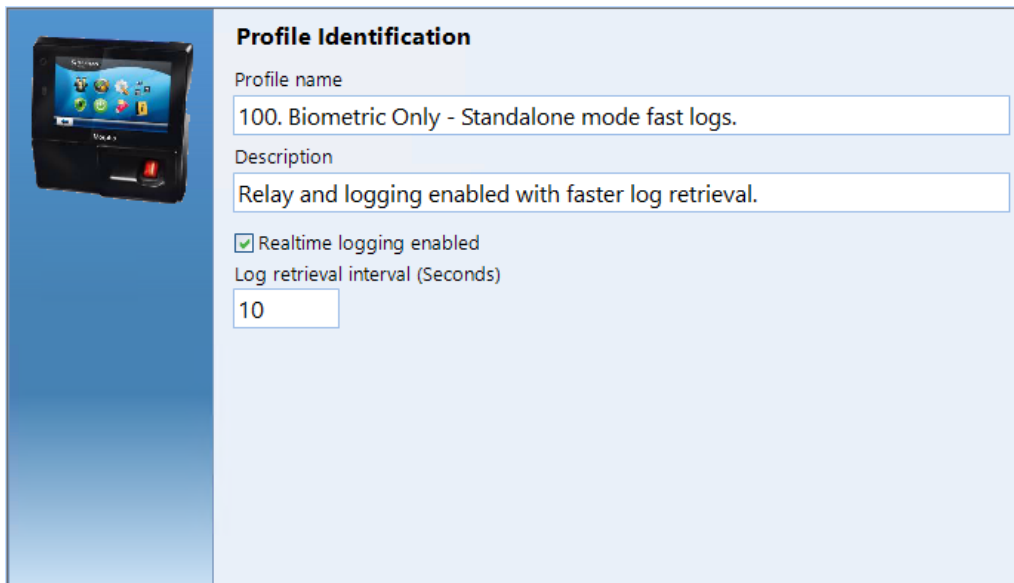


**Profile name** - Rename the profile as appropriate

**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



**Profile Identification**

Profile name  
100. Biometric Only - Standalone mode fast logs.

Description  
Relay and logging enabled with faster log retrieval.

☒ Realtime logging enabled

Log retrieval interval (Seconds)  
10

Click **[Next]**



Morpho Device Profile Wizard

**Biometric Device Settings**

**General Settings**

Wiegand Profile  
Standard 34 bit

Language  
English

**Threshold Settings**

Biometric Threshold (Preset)  
Recommended

Threshold Value  
1 2 3 4 5 6 7 8 9 10

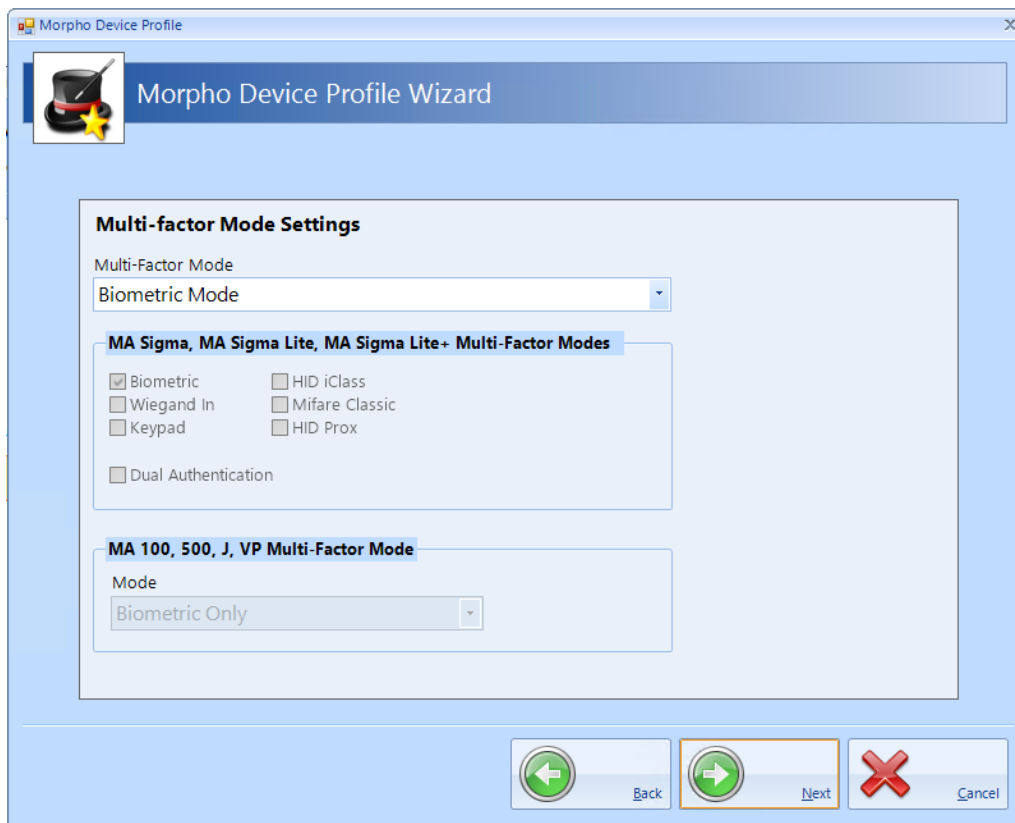
Back Next Cancel

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).

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

Click **[Next]** to continue



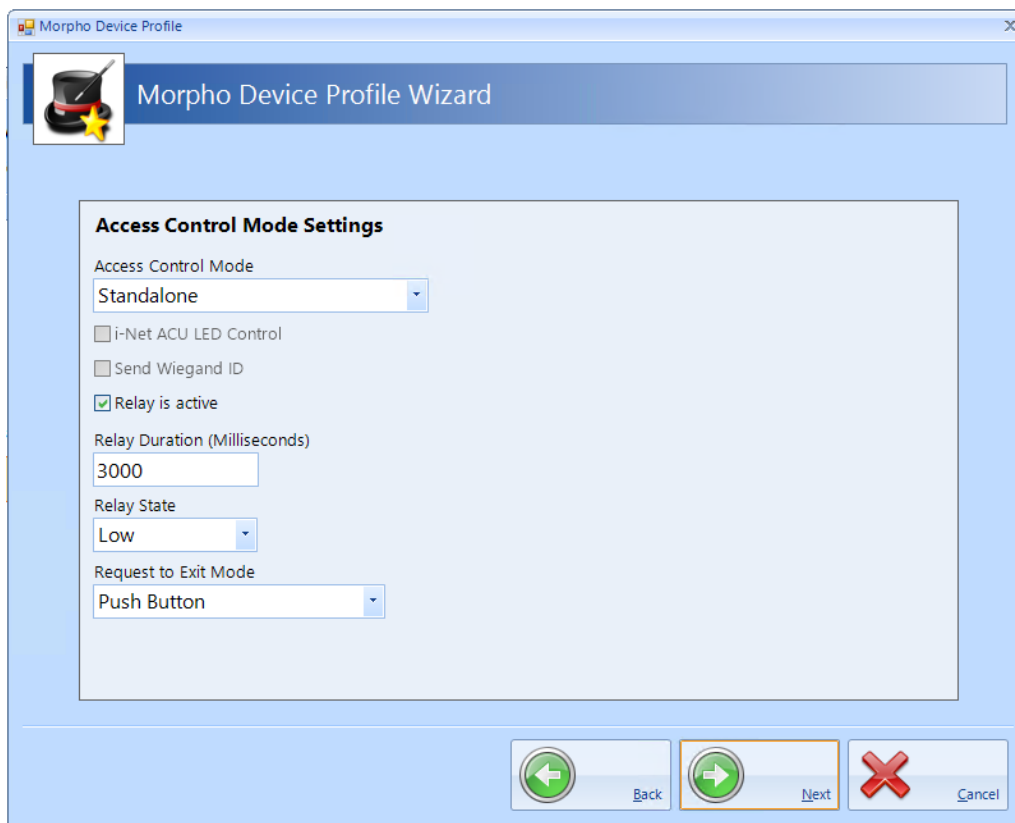
**Multi-factor Mode** should be set to Biometric Mode for fingerprint only, or changed to Custom for fingerprint and card

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), Wiegand 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

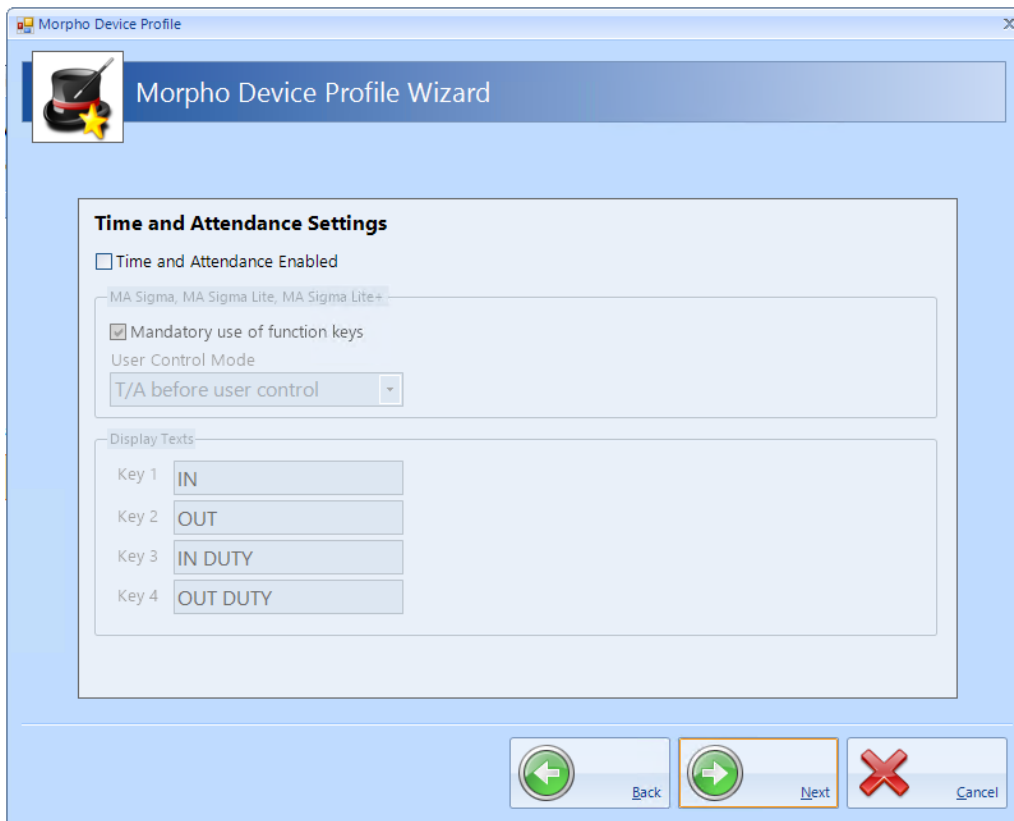


The **Access Control Mode** should be set to **None** if MorphoManager is used, **iNet ACU** if connected to an iNet or **Standalone** if no iNet controller is used.

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



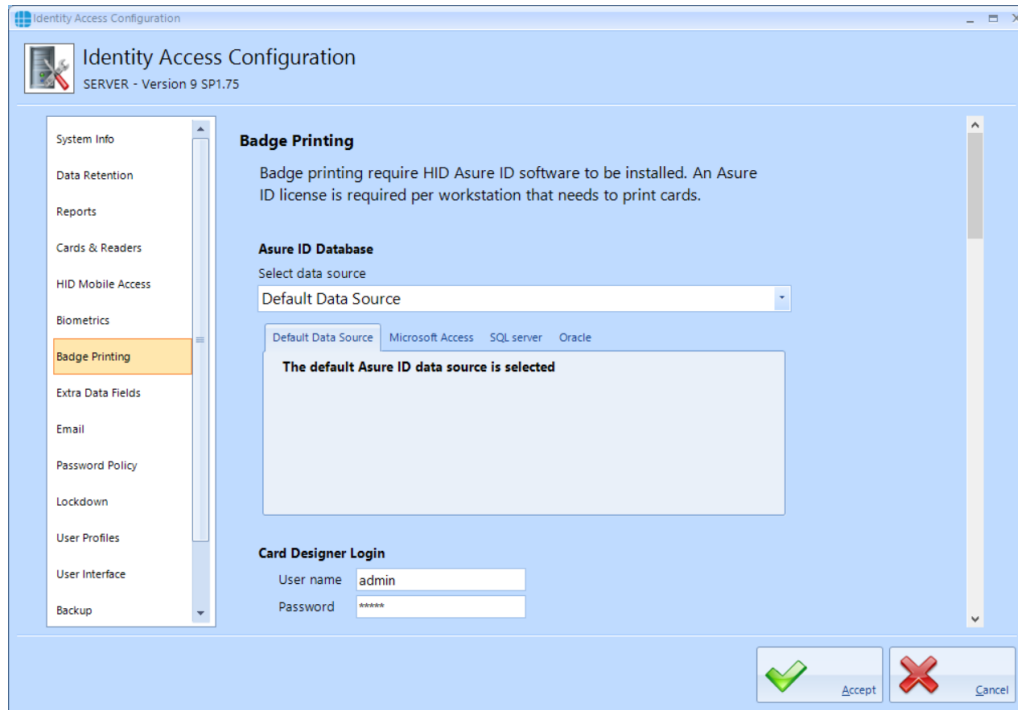
The screenshot shows the 'Morpho Device Profile Wizard' window. The title bar reads 'Morpho Device Profile'. The window has a blue header with the title 'Morpho Device Profile Wizard' and a small icon of a top hat with a star. The main content area is titled 'Time and Attendance Settings'. It contains a checkbox for 'Time and Attendance Enabled' which is currently unchecked. Below this is a text box containing 'MA Sigma, MA Sigma Lite, MA Sigma Lite+'. There is a checked checkbox for 'Mandatory use of function keys'. Below that is a 'User Control Mode' section with a dropdown menu currently set to 'T/A before user control'. At the bottom of the settings area is a 'Display Texts' section with four rows: 'Key 1' with 'IN', 'Key 2' with 'OUT', 'Key 3' with 'IN DUTY', and 'Key 4' with 'OUT DUTY'. At the bottom of the window are three buttons: 'Back' (with a left arrow icon), 'Next' (with a right arrow icon and a red border), and 'Cancel' (with a red X icon).

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]**

### 2.9.7 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.

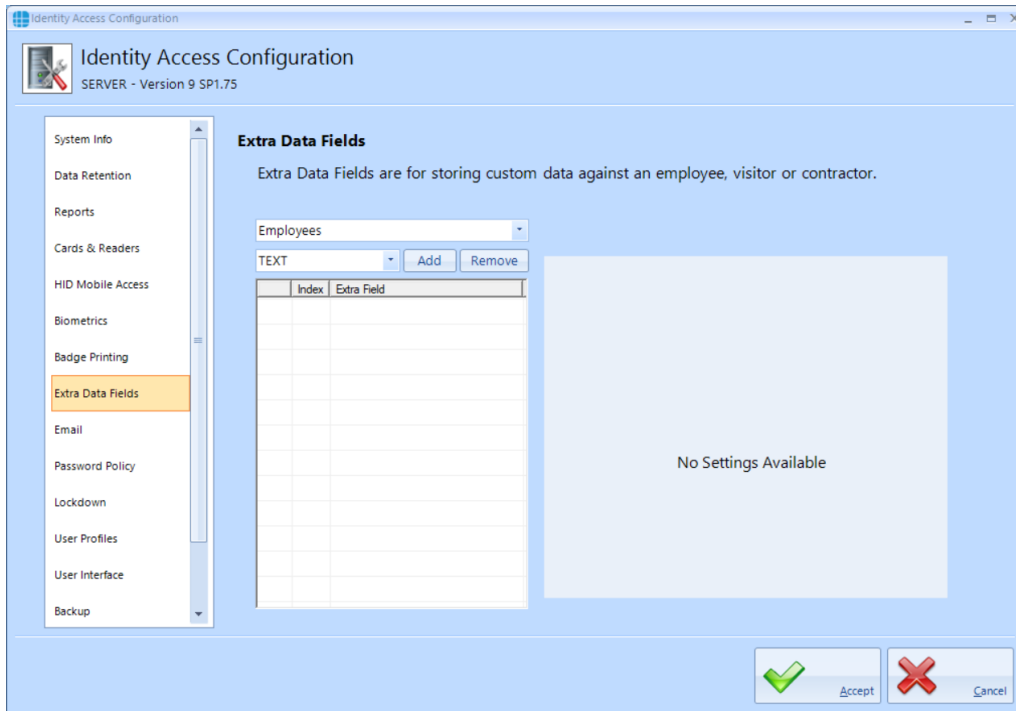
The **Card Designer Field Mapping** fields are preconfigured for use with Identity Access and should only be changed if requested by Controlsoft Technical Support.

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.

### 2.9.8 IA Configuration - Extra Data Fields

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

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"

Click **[Apply]**.

The screenshot shows the 'Identity Access Configuration' window with the 'Extra Data Fields' section selected in the left sidebar. The main area is titled 'Extra Data Fields' and includes a description: 'Extra Data Fields are for storing custom data against an employee, visitor or contractor.' Below this, there is a dropdown menu set to 'Employees' and a 'CHECK' dropdown menu. A table with columns 'Index' and 'Extra Field' is visible, showing a single row with a green checkmark in the 'Index' column and '0' in the 'Extra Field' column. To the right of the table is a 'CHECK Field Setup' panel with a 'Description' field containing 'Valid Driver's License', and two input fields for '1st Answer' (containing 'Yes') and '2nd Answer' (containing 'No'). An 'Apply' button is at the bottom right of this panel. At the bottom of the window are 'Accept' and 'Cancel' buttons with green and red icons respectively.

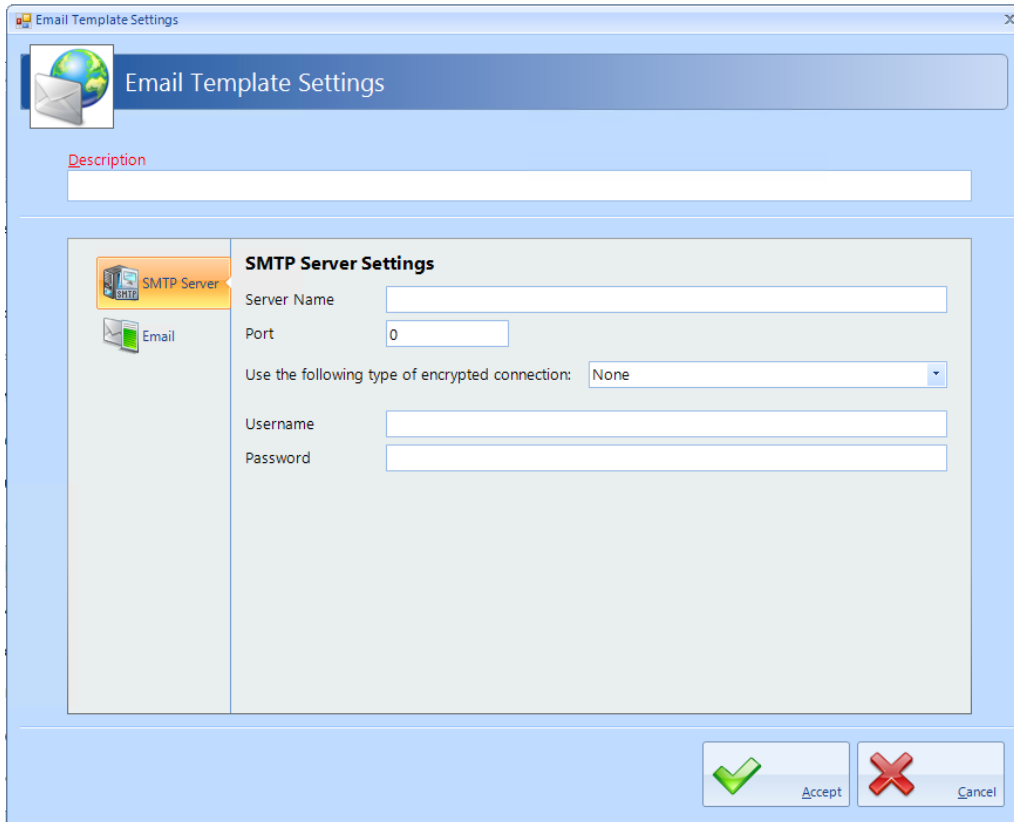
## 2.9.9 IA Configuration - Email

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

The screenshot shows the 'Identity Access Configuration' window with the 'Email' section selected in the left sidebar. The main area is titled 'Email Templates' and includes a description: 'Create custom email templates to be sent when an event occurs. After creating the email template, create an Event and an Action in Identity Access.' Below this, there are buttons for 'Add', 'Edit', 'Duplicate', and 'Remove'. A table with columns 'Template Name', 'From', and 'To' is visible, showing a single row with empty fields. At the bottom of the window are 'Accept' and 'Cancel' buttons with green and red icons respectively.



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

The image shows a software window titled "Email Template Settings". At the top, there is a blue header bar with a globe icon and the title "Email Template Settings". Below the header, there is a "Description" label followed by a text input field. The main area of the window is divided into two sections. On the left is a sidebar with two icons: "SMTP Server" (a server rack icon) and "Email" (an envelope icon). The "SMTP Server" icon is highlighted with an orange background. To the right of the sidebar, under the heading "SMTP Server Settings", there are several input fields: "Server Name" (a text box), "Port" (a text box containing the number "0"), "Use the following type of encrypted connection:" (a dropdown menu currently showing "None"), "Username" (a text box), and "Password" (a text box). At the bottom right of the window, there are two buttons: "Accept" with a green checkmark icon and "Cancel" with a red X icon.

**Description:** add a meaningful name for the template.

**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.

Email Template Settings

Description

SMTP Server

Email

"Friendly Name" <address@company.com> or address@company.com

From

Multiple email addresses must be seperated by a comma.  
(123@xyz.com,abc@test123.org)

To

CC

Subject

Body Test

Accept Cancel

**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

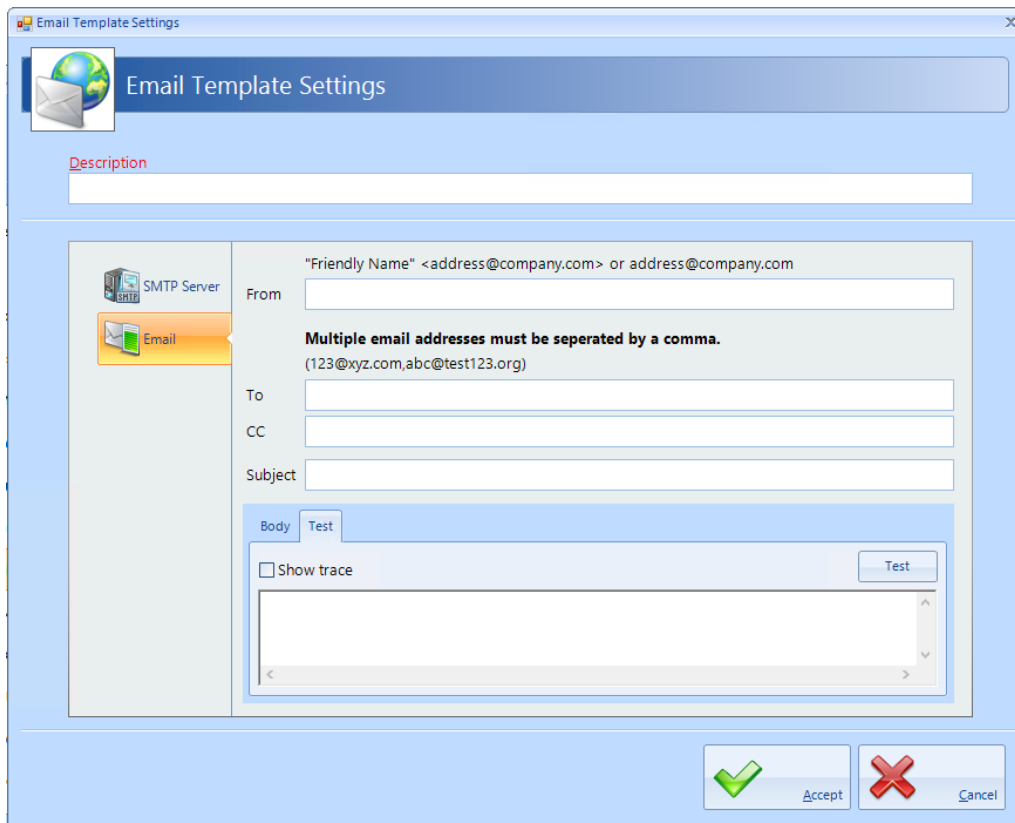
**NOTE: It is possible to enter multiple email addresses in the To and CC fields, simply separate them with a comma as shown on the screen.**

**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:

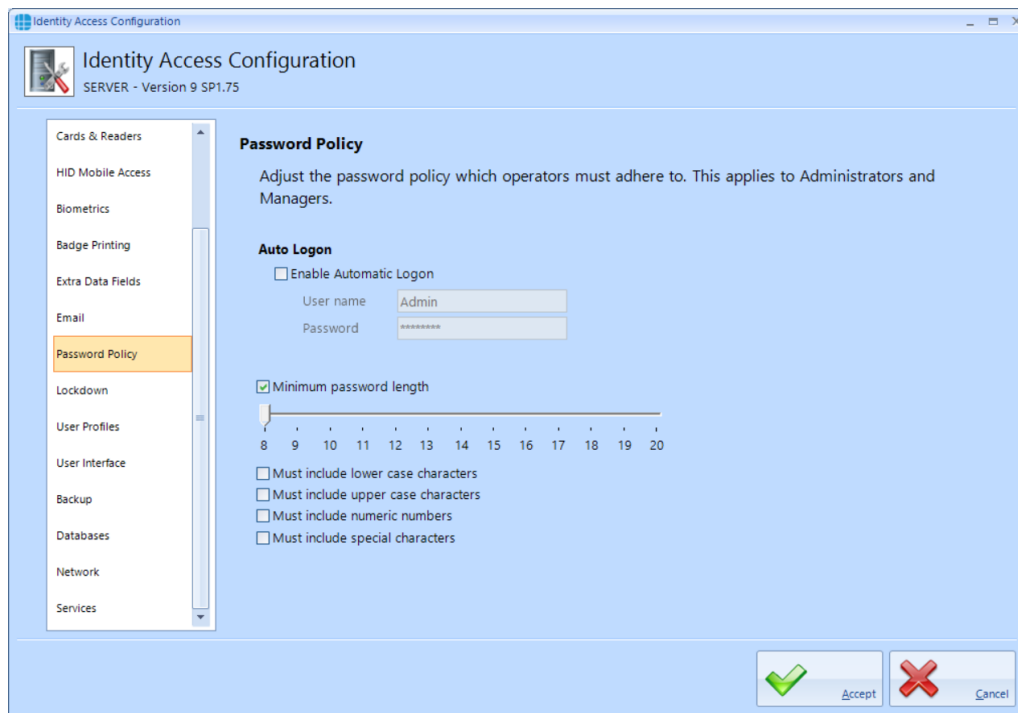


The screenshot shows the 'Email Template Settings' dialog box. It has a title bar with a close button. Below the title bar is a header area with a globe icon and the text 'Email Template Settings'. A 'Description' label is followed by a text input field. On the left, there is a sidebar with two icons: 'SMTP Server' and 'Email'. The 'Email' icon is highlighted. The main area contains the following fields: 'From' (with a placeholder 'Friendly Name' <address@company.com> or address@company.com), 'To' (with a note 'Multiple email addresses must be seperated by a comma.' and an example '(123@xyz.com,abc@test123.org)'), 'CC', and 'Subject'. Below these is a 'Body' tab and a 'Test' button. A 'Show trace' checkbox is also present. At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

Click the **[Test]** button to send a test email. the display will indicate whether the test was successful.

### 2.9.10 IA Configuration - Password Policy

The Operators tab defines the level of security required when operators log into the system.



**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)

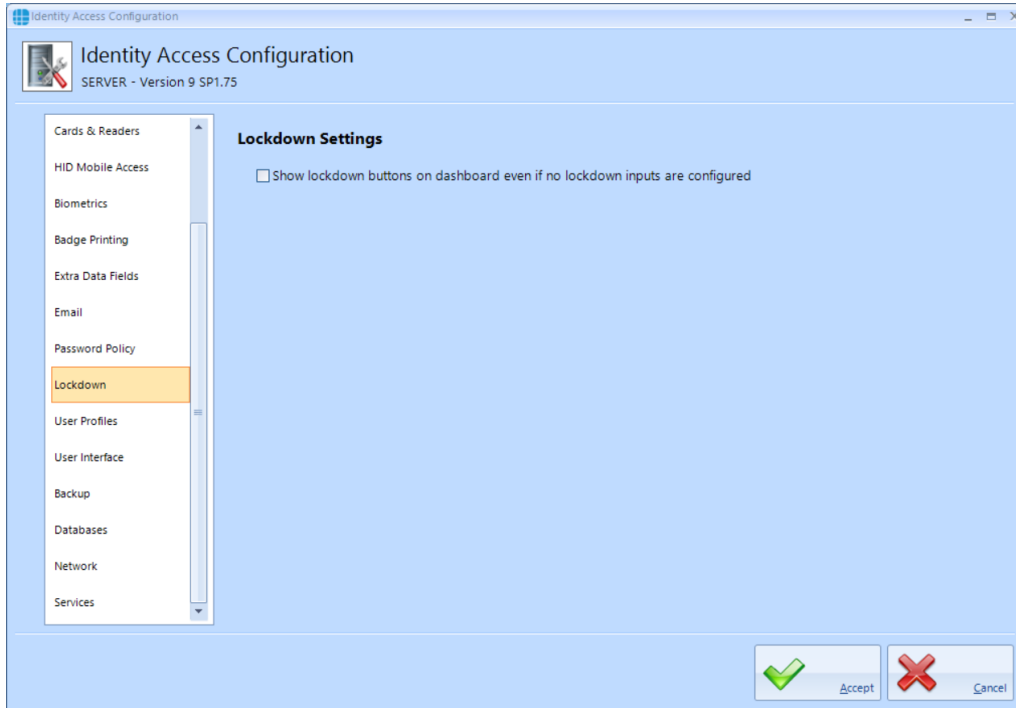
**Must include numeric characters** - The password must include at least 1 numeric character (e.g. 1, 2, 3)

**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.

### 2.9.11 IA Configuration - Lockdown

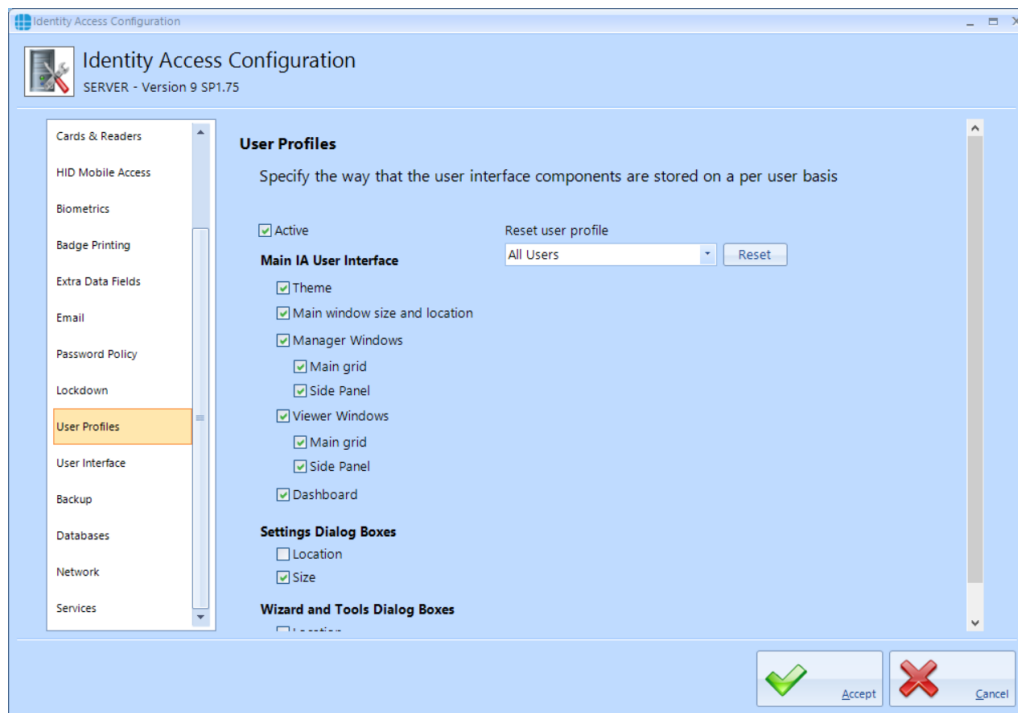
The Lockdown tab defines whether Lockdown buttons are always displayed in the IA User Interface



***NOTE: Lockdown is only available when an IA-PRO or IA-ENT license has been applied.***

### 2.9.12 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.



**Active** - ensure this option is ticked to enable user profiles

**Reset User Profiles** - reset operator profiles, either for everyone or by operator group.

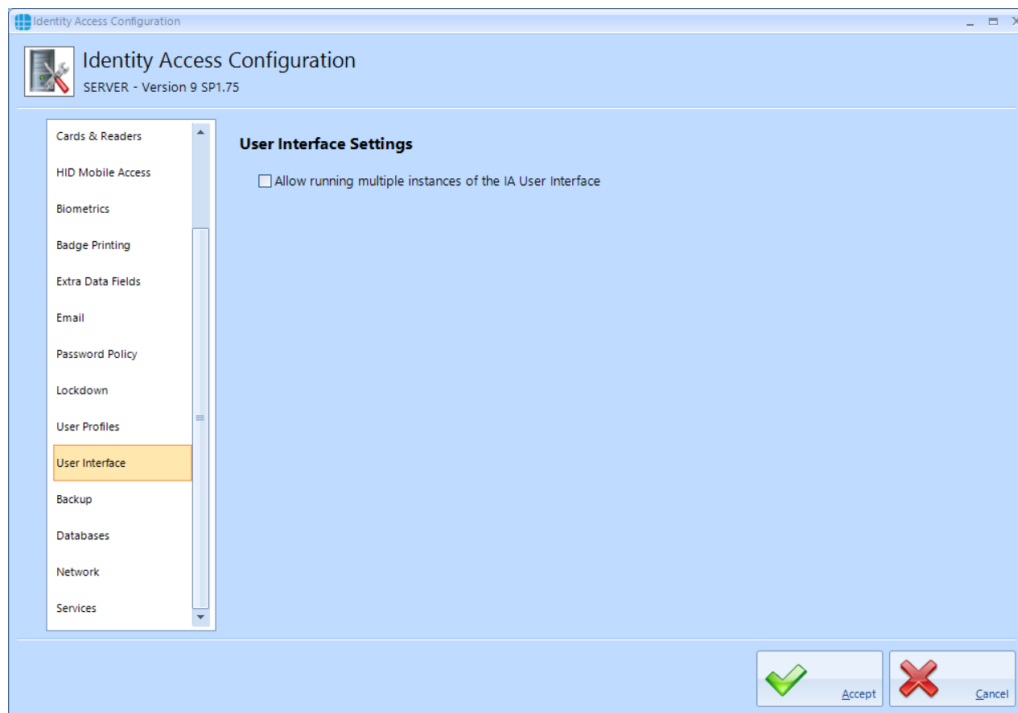
**Main IA User Interface** - define which elements of the software can be adjusted by operator

**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

### 2.9.13 IA Configuration - User Interface

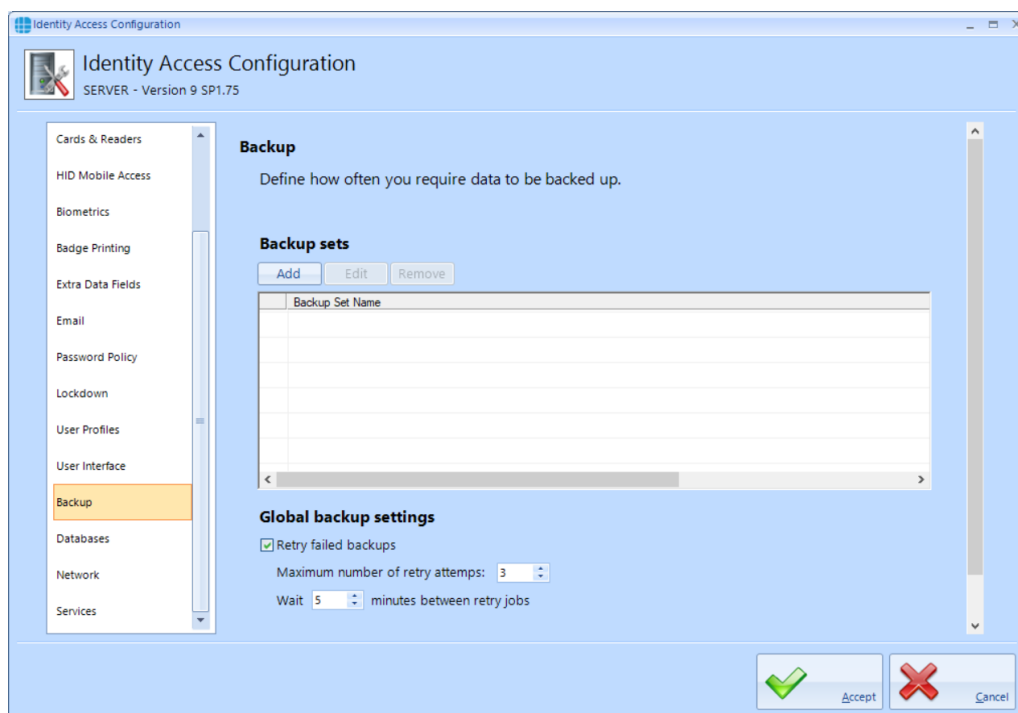
The User Interface tab defines whether multiple instances of Identity Access can be run simultaneously.



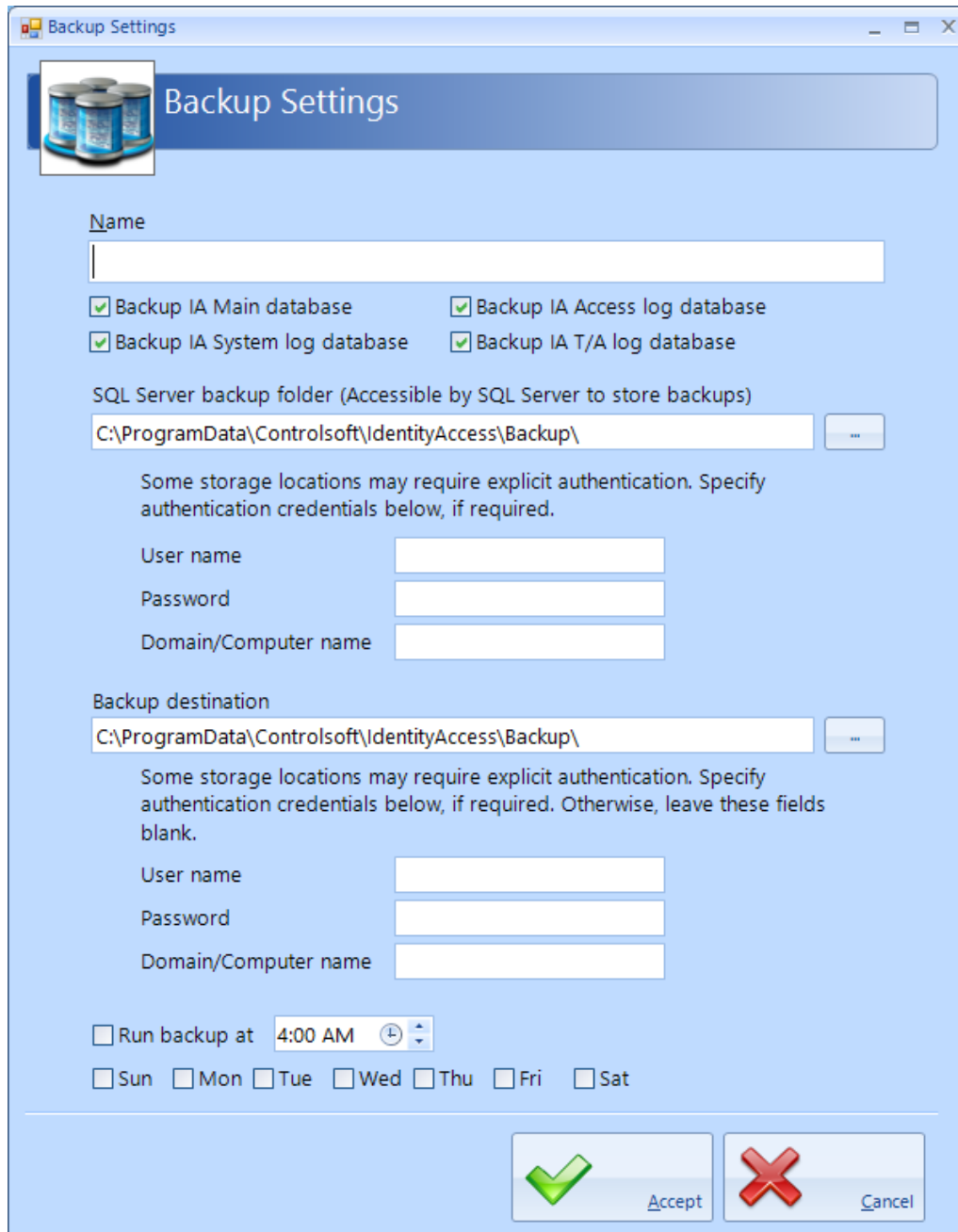
**Allow running multiple instances of the IA User Interface** - tick this option if you want to run an instance for each Operator

#### 2.9.14 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.



**Backup Sets** allows us to define one or backup definitions. Click the **[Add]** button



**Name** - Give the backup set a name, then define which database files are to be backed up.

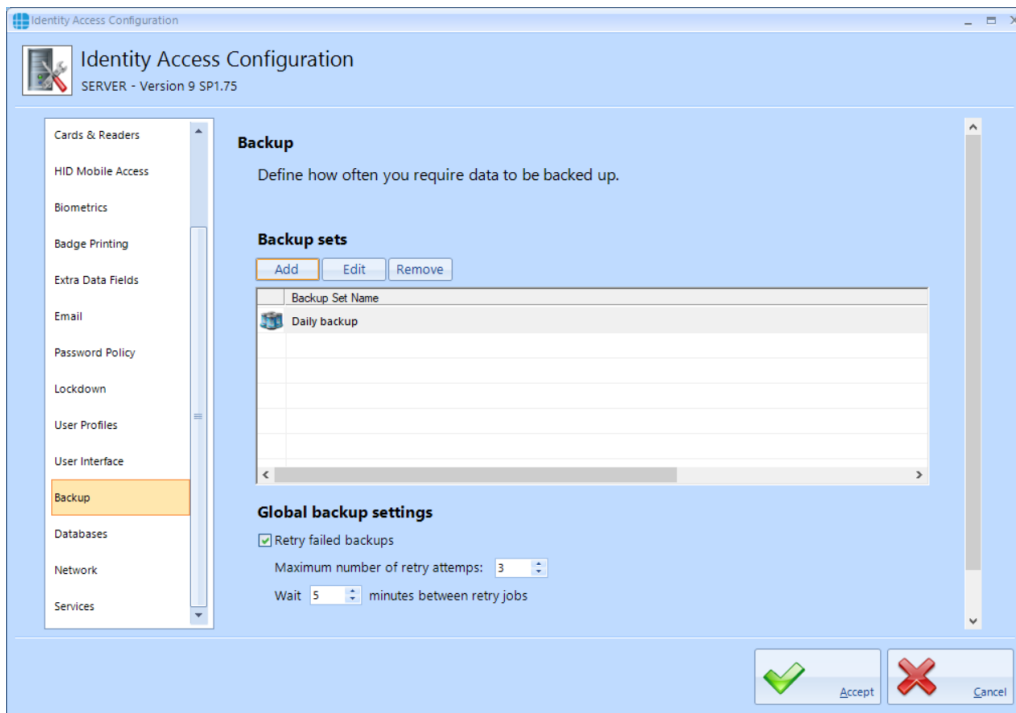
**SQL Server backup folder** - If the SQL Service is installed on the same PC as Identity Access this section can be ignored. If the SQL Service is installed on a different PC as Identity Access, define the relevant details to communicate with the SQL Service

**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 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.

### 2.9.15 IA Configuration - Databases

The **Databases** tab is used to point to where the SQL database is installed

The screenshot shows the 'Identity Access Configuration' window, version 9 SP1.75. The 'Databases' tab is selected in the left-hand navigation pane. The main area is titled 'Database Connection Strings' and contains the following fields:

- Server name: .\IDENTITYACCESS
- Authentication: SQL Server Authentication
- Username: sa
- Password: (masked with asterisks)
- Main Database: IAMain
- Access Log: IAAccessLog
- System Log: IASystemLog
- T/A Log: IATALog
- Access Log Buffer: IAAccLogBuffer
- System Log Buffer: IASysLogBuffer
- T/A Log Buffer: IATALogBuffer

At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

**NOTE: DO NOT change these strings unless instructed to do so by Controlsoft Technical Support.**

### 2.9.16 IA Configuration - Network

The **Network** tab is used to configure the network settings.

The screenshot shows the 'Identity Access Configuration' window, version 9 SP1.75. The 'Network' tab is selected in the left-hand navigation pane. The main area is titled 'Network' and contains the following settings:

- Listen only on a specific address:** An unchecked checkbox.
- IP Address:** A text input field.
- Use IP Version:** A dropdown menu currently set to 'IPV4 and IPV6'.
- Ports:** A section with the instruction 'Do not adjust the ports unless it is required.' containing four port configuration rows:
  - Listen Port (Log Service):** 19000
  - Listen Port (Download Service):** 19100
  - Listen Port (Log Service User Interface):** 19001
  - Listen Port (Download Service User Interface):** 19101

At the bottom right, there are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

**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

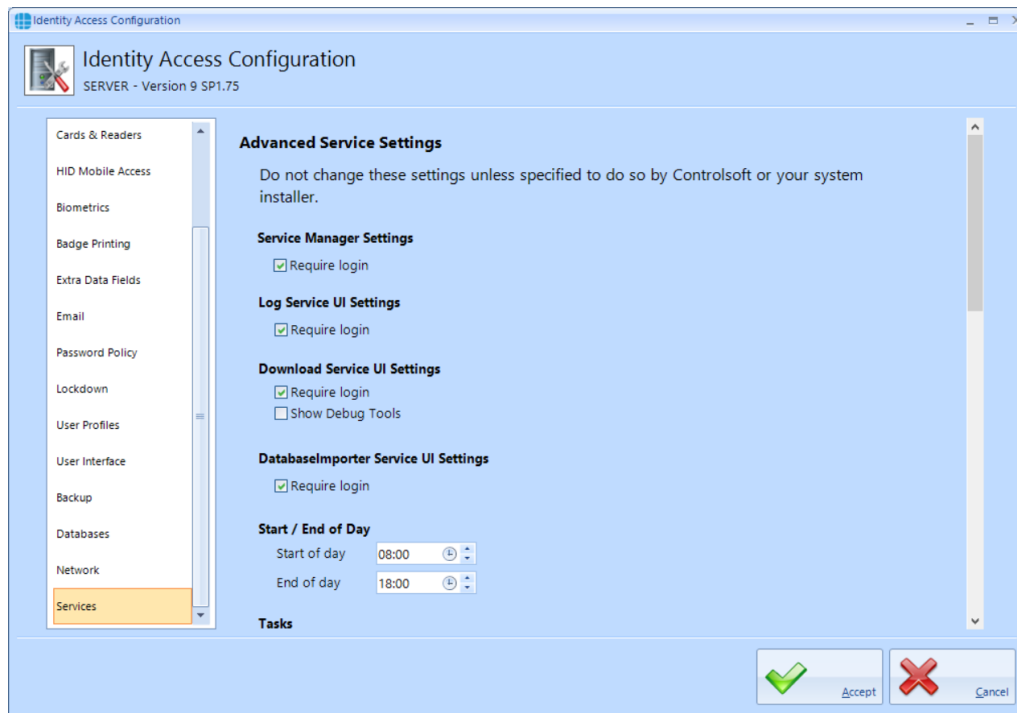
**Listen Port (Log Service)** and **Listen Port (Log Service User Interface)** - these are ports used for all Log Server communications

**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**

### 2.9.17 IA Configuration - Services

The **Download Service** tab is used to define features such as whether debug tools are shown in the Download Server and whether Fire Roll Call report is automatically printed when a fire alarm is generated.



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.

**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.

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.

# Preparing for IP Connection

### 3 Preparing for IP Connection

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

***NOTE: A default iNet Controller is configured for DHCP to enable the "Find IP Controller" wizard to detect the iNet controller. By pressing the Reset button on the iNet controller, the IP Address will change to a fixed IP Address of 10.0.1.230 (see hardware manuals for 1DR, 2DR and iNet Plus controllers)***

The procedure is to configure the PC to an IP Address on the same network segment as the iNet (e.g. 10.0.1.200), then use Controlsoft's iNet Configurator software to reconfigure each iNet to an individual IP Address on the target network (see [Assigning a Fixed IP Address to the iNet Controller](#)<sup>[92]</sup>). If you are unsure which IP Address the iNets should use, please speak to someone from the site's IT department.

When all the iNet Controllers have been configured, change the PC's IP Address back to its original settings.

***NOTE: Controlsoft strongly recommend that, once configured, you use iNet Configurator software to change the iNet to a fixed IP Address to maximise the long term reliability of the connection.***

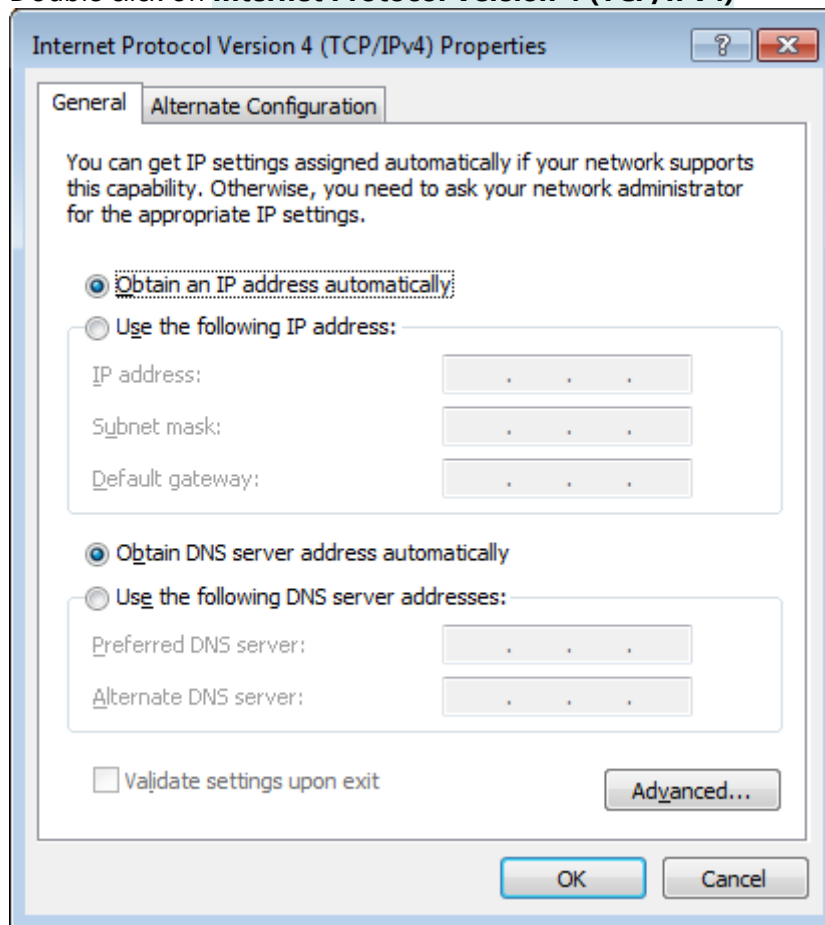
#### 3.1 Configure the PC

If the PC and the iNet controller are both on DHCP, they will communicate when both are connected to the network as the router will allocate IP Addresses. If the iNet controller has been reset to 10.0.1.230 or other fixed IP Address, the following procedure is required at the PC to ensure compatibility.

To communicate with the iNet over a TCP/IP network, the PC and iNets must be configured on the same IP range.

1. Click on the Start button and select **Control Panel** (see [Appendix C - Windows Commands](#)<sup>[347]</sup> for further assistance)
2. Select **Network and Sharing Center** then select **Change adapter settings** in the left column
3. Double click on the relevant network connection, then click on **[Properties]**

4. Double click on **Internet Protocol Version 4 (TCP/IPv4)**



5. The IP Address needs to be set to an address in the same range as the default IP Address of the iNet Controller (default = 10.0.1.230)
6. Click on **Use the following IP address** then enter the desired IP Address (e.g. 10.0.1.200).



7. Enter the Subnet Mask as 255.255.255.0

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 0 . 1 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

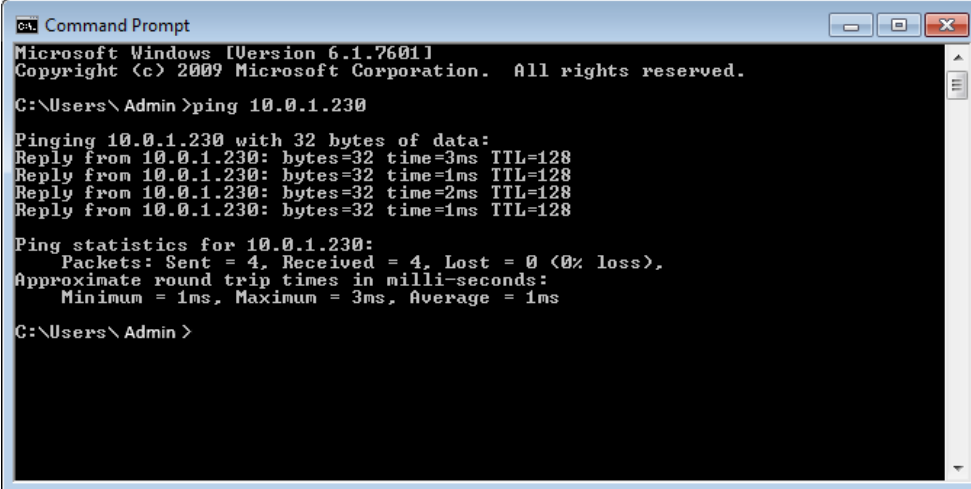
OK Cancel

8. Click on **[OK]**, **[OK]**, **[Close]**, then close the Network Connections window.

## 3.2 Ping the i-Net Controller

To confirm that you are able to communicate with an iNet Controller which is connected to the PC via IP, simply issue a 'ping' command:

1. Run the **Command Prompt** (see [Appendix C - Windows Commands](#))<sup>347</sup>, then enter the command **ping 10.0.1.230** and confirm that the iNet Controller is able to reply:



```

ca. Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.0.1.230

Pinging 10.0.1.230 with 32 bytes of data:
Reply from 10.0.1.230: bytes=32 time=3ms TTL=128
Reply from 10.0.1.230: bytes=32 time=1ms TTL=128
Reply from 10.0.1.230: bytes=32 time=2ms TTL=128
Reply from 10.0.1.230: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.1.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\Admin>
    
```

2. If the iNet controller does not respond, check the network wiring between the PC and the controller.
3. If the iNet is not new, it is possible that the IP Address is not set to the default value (10.0.1.230). To default the IP Address, press the Reset switch (see hardware manuals for 1DR, 2DR and iNet Plus controllers). Wait for the iNet Controller to reboot, then try and ping it again.

If in any doubt about IP Addresses to be used, please contact the system administrator.

## 3.3 Assigning a Fixed IP Address using i-Net Configurator

Before assigning IP Addresses to the iNet Controllers, first contact the IT department for the site and obtain IP addresses for each of the controllers installed.

***NOTE: iNet controllers MUST be configured with FIXED IP Addresses for maximum network reliability.***

Changing the iNet's fixed IP Address is done through iNet Configurator. For further information on how to use iNet Configurator, please refer to [Appendix F - iNet Configurator](#)<sup>361</sup>

# Starting the Identity Access Software

## 4 Starting the Identity Access Software

To launch the Identity Access software:

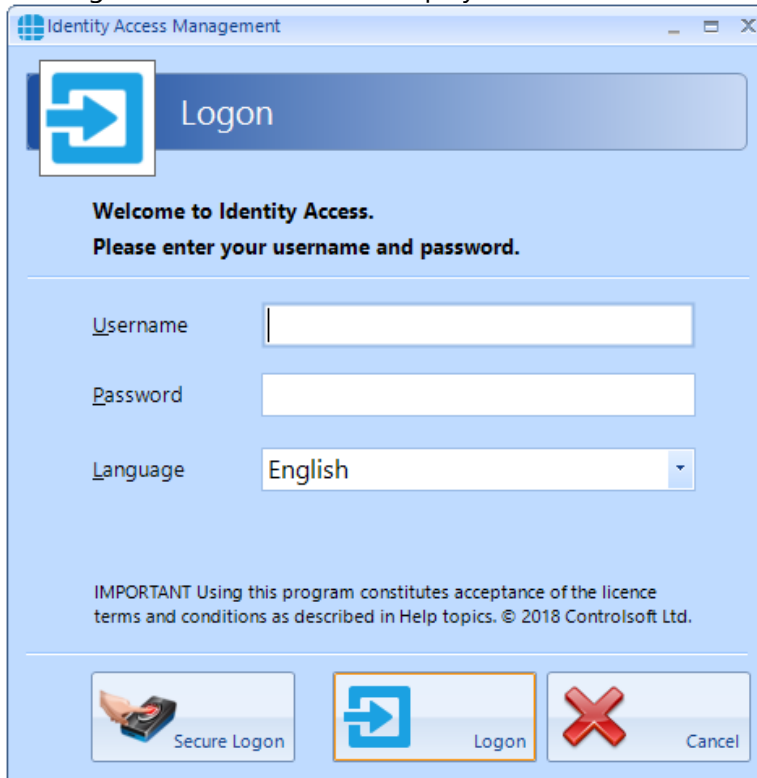
Start Identity Access as follows.

Select **Start** > **Controlsoft** > **IA User Interface**

The following splash screen will be displayed:



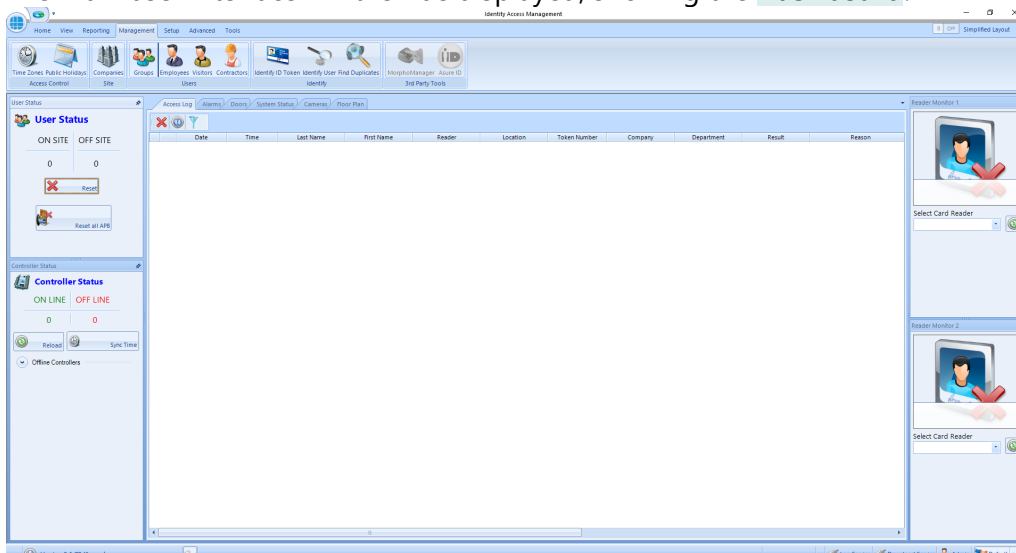
The Logon screen will then be displayed:



The screenshot shows the 'Identity Access Management' window with a 'Logon' header. Below the header, it says 'Welcome to Identity Access. Please enter your username and password.' There are three input fields: 'Username', 'Password', and 'Language' (set to 'English'). At the bottom, there are three buttons: 'Secure Logon' (with a card reader icon), 'Logon' (with a blue arrow icon), and 'Cancel' (with a red X icon). A disclaimer at the bottom states: 'IMPORTANT Using this program constitutes acceptance of the licence terms and conditions as described in Help topics. © 2018 Controlsoft Ltd.'

Enter a valid Username (default = **Admin**) and Password (default = **Password**) and click the **[Logon]** button (or press **[Enter]** on the keyboard). **NOTE: these credentials are case sensitive.**

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



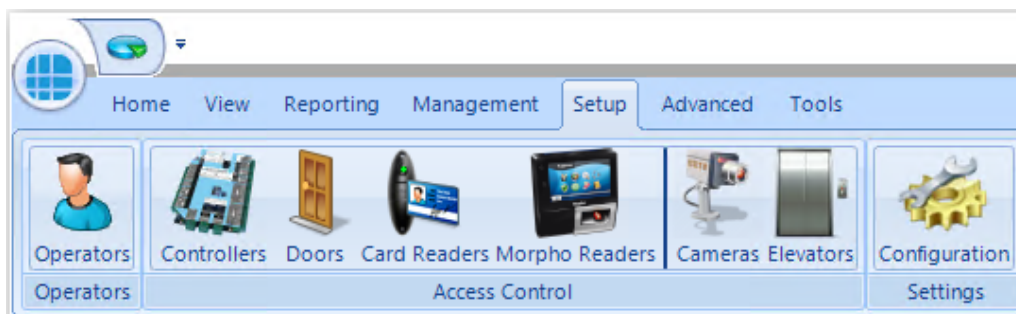
**NOTE: Screenshots used throughout this manual show screens with their default layout. The "User Profiles" feature (introduced in IA v9.1.48) allows Operators to change screen size and locations, thereby changing the overall look and feel**

***of the software. IA supports multiple operators with different personal preferences for each operator.***

The most common technique to log on to the software is to enter a Username and Password as described above. If the operator is also an Employee, it is possible to log on to the software using a fingerprint. Simply click the **[Secure Logon]** button and present a finger to the fingerprint enrolment reader.

## 4.1 Identity Access Header and Footer

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

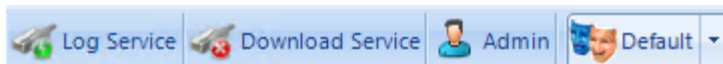


Use this icon to quickly return to the Dashboard from anywhere in the software.

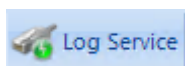
The Menu bar (Home, View etc) provides access to groups of functions from anywhere in the software.

Below the Menu bar is the Ribbon bar, which provides access to individual functions depending on which Menu bar option is selected.

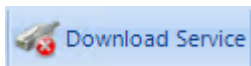
At the bottom of the screen is the footer bar:



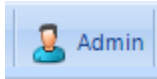
The various icons represent the following conditions:



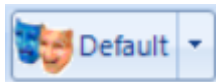
indicates the status of the connection between the Identity Access software and the Log Service (in this example, the green icon indicates that the Log Server is connected)



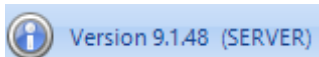
indicates the status of the connection between the Identity Access software and the Download Service (in this example, the red icon indicates that the Download Service is not connected)



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

## 4.2 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




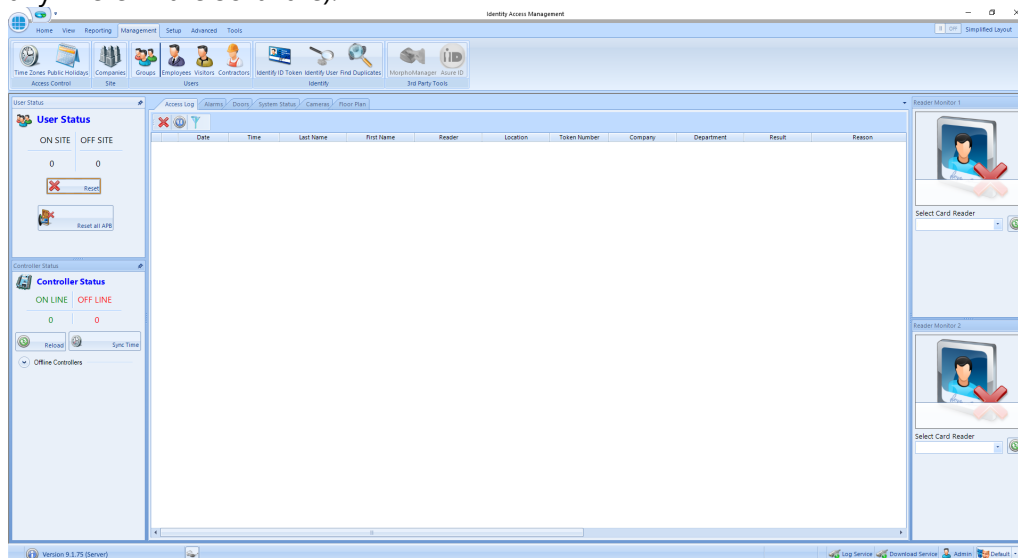
Position the mouse for the required option and click to select.

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

## 4.3 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](#))<sup>167</sup>

**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.

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.



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](#)<sup>[141]</sup>).

To activate Lockdown, click on the Amber or Red block on the screen, or activate the relevant input (see [Controller Settings](#)<sup>[141]</sup>). The only way to deactivate Lockdown, is to select the Green block on the screen.

If the Lockdown icons are grey, Lockdown is Disabled

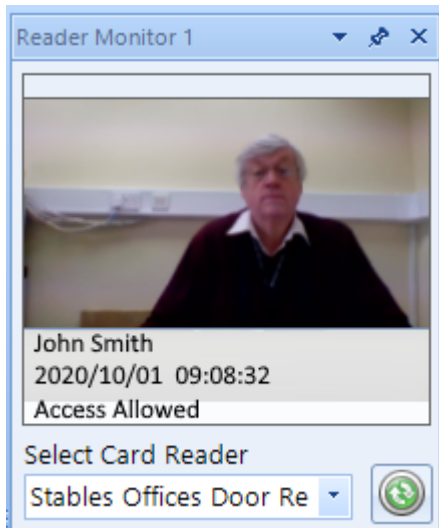
**System Status:** This screen provides an overview of whether the Log Service and the Download Service are connected, whether Azure ID is licensed and available to use, and whether the HID Mobile Portal (if used) is available.

**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.

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:

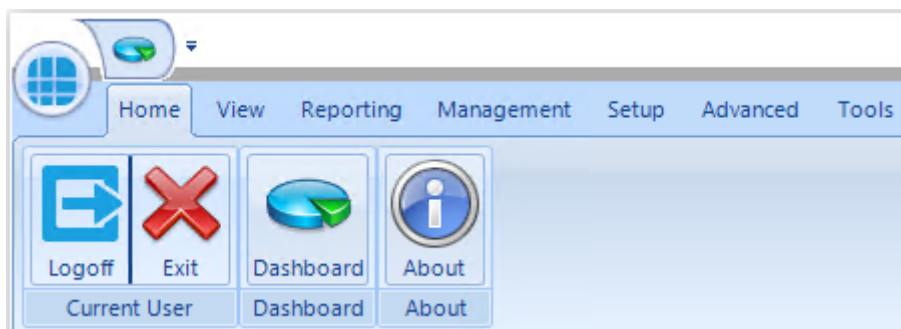


**NOTE:** It is possible to 'undock' a tab such as the Floorplan, and resize it to get a larger view on the screen. Simply click on the tab and drag it out of position, then resize the windows as required. IA can then be minimised, leaving the desired tab visible.

Before closing Identity Access, always 'redock' the window by right clicking and selecting "Tabbed Document".

## 4.4 Identity Access Home Tab

The **Home** tab contains 4 options:



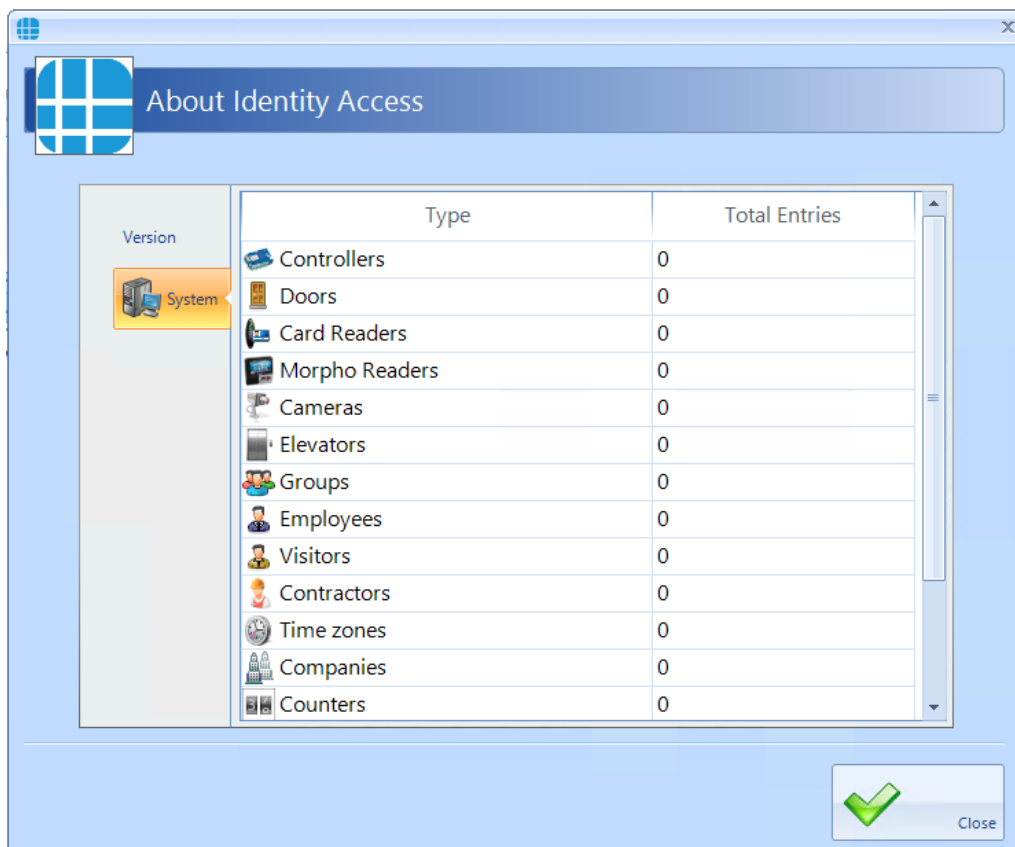
**Current User:** Allows the current Operator to **Logoff** (log out and restart the program for the next Operator to log in) or **Exit** (log out and close the program)

**Dashboard:** displays the system Dashboard (See [The Dashboard](#))

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

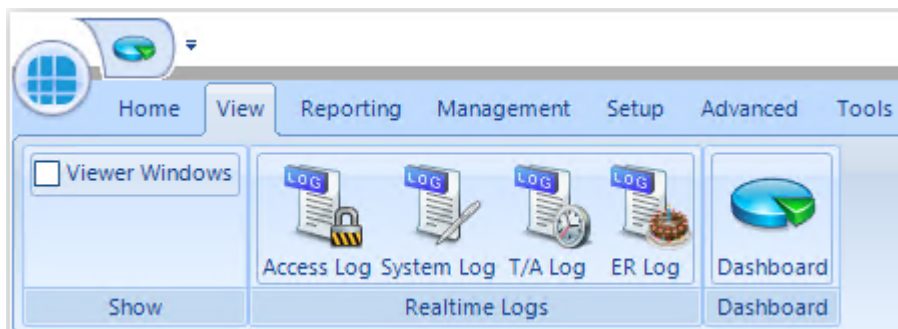


Select the **[System]** tab to view an overview of how many controllers, doors, readers etc are on the system:

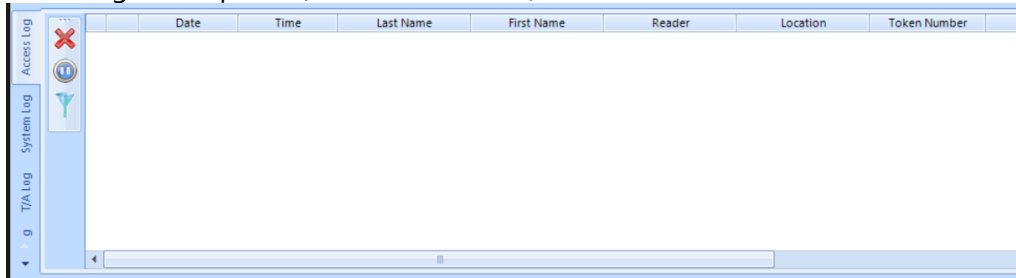


## 4.5 Identity Access ViewTab

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




**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](#))<sup>294</sup>.



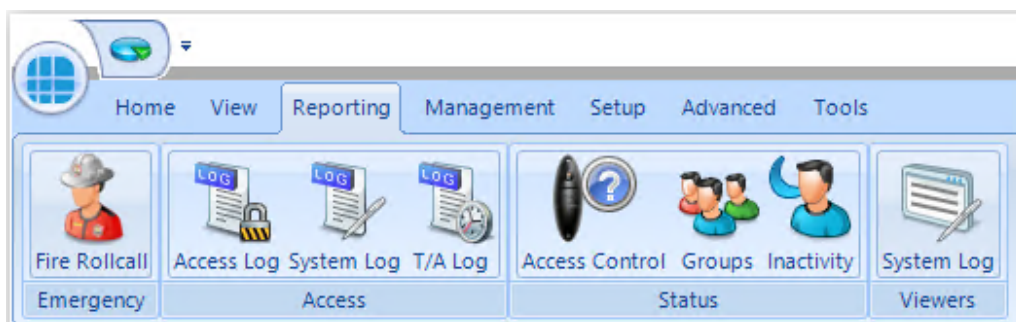
**Realtime Logs:** Allows the Operator to view live **Access** events, **System** events, **T/A** events or ER Logs in the Viewer window. **NOTE: These buttons do the same as the side tabs in the viewer window.**

**Dashboard:** Allows the Operator to view a summary status of the system (see [The Dashboard](#))<sup>98</sup>.

**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.**

## 4.6 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](#))<sup>86</sup>). **NOTE: This facility is not available in Identity Access unless a Professional or an Enterprise Features Licence is applied.**

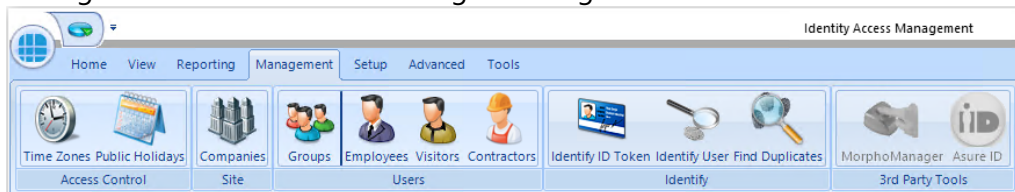
**Access:** Allows the Operator to run and view reports based on **Access** events, **System** events or **T/A** events from the database.

**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

## 4.7 Identity Access Management Tab

The **Management** 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.

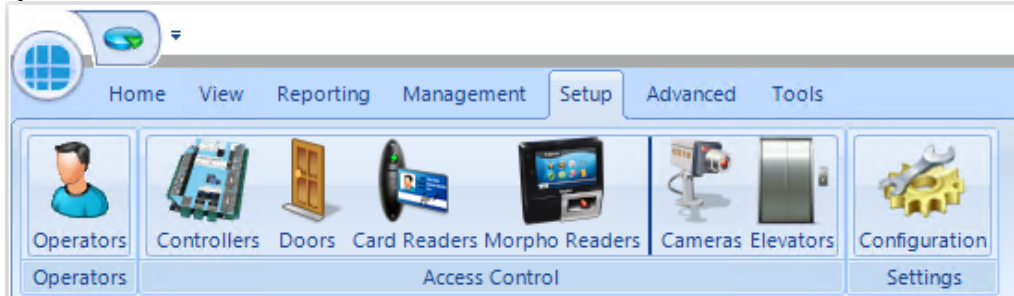
**3rd Party Tools:** Options used to run the **MorphoManager** software and **Asure ID** (HID badge printing software).

**NOTE: if Identity Access has a Professional or Enterprise licence installed, it is not necessary to use MorphoManager software as all fingerprint enrolment is handled by Identity Access itself.**



## 4.8 Identity Access Setup Tab

The **Setup** 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

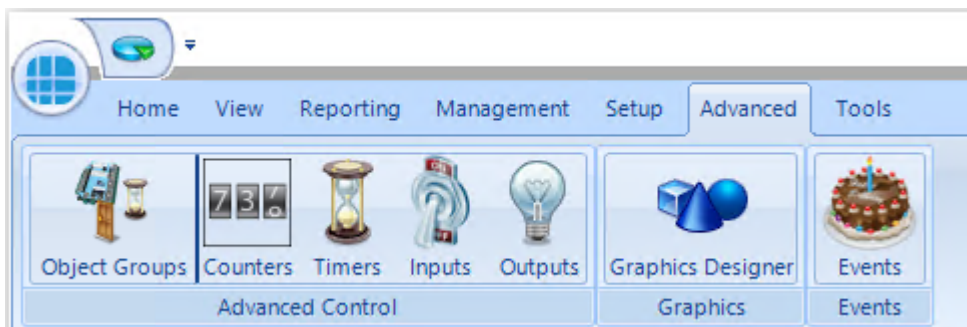
**Access Control:** Used to commission the **Controllers**, **Doors**, **Card Readers**, **Morpho Readers**, **Cameras** and **Elevators** installed on site.

**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](#)<sup>55</sup>

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

## 4.9 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.

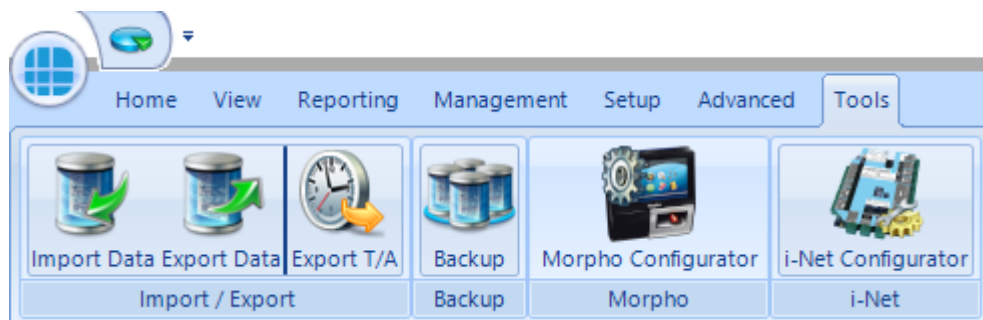
The **Graphic Designer** allows a floorplan of the site to be imported, and objects superimposed onto the image. Objects can be IA Objects such as doors, readers or controllers or Custom Objects such as squares, circles, images or text boxes.

**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](#) <sup>252</sup>

## 4.10 Identity Access Tools Tab

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

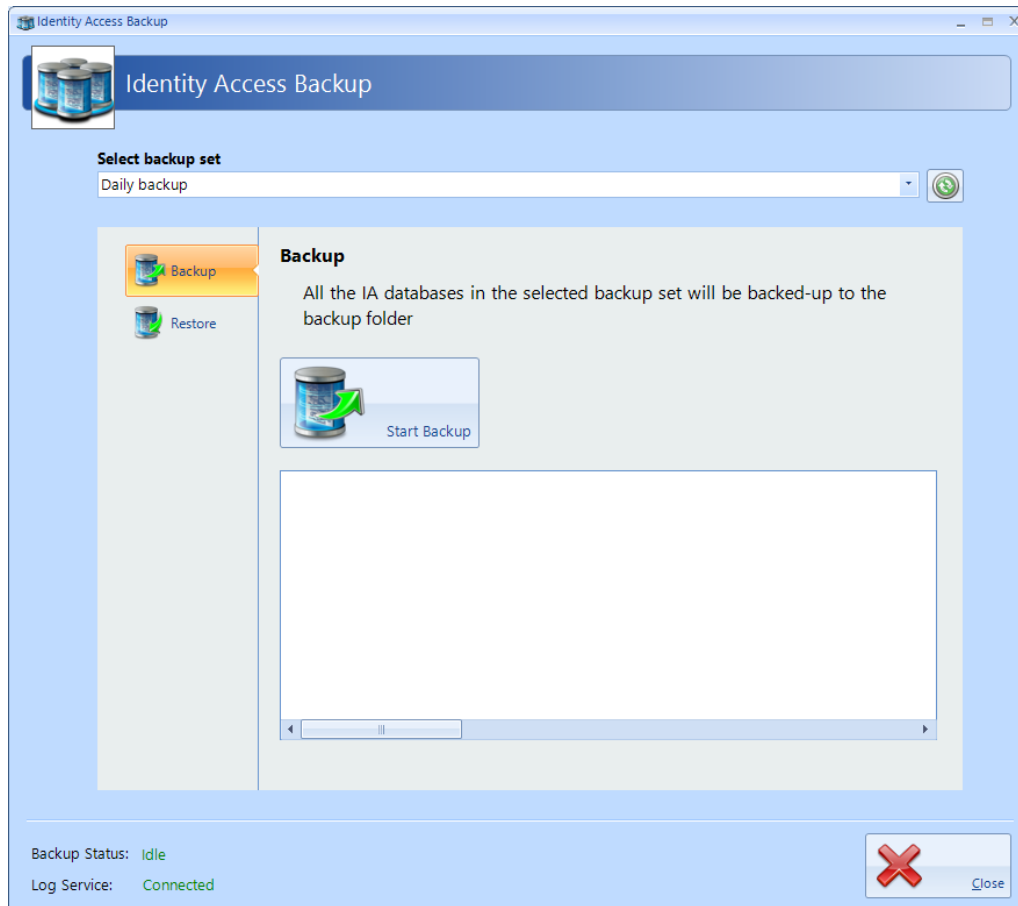


**Import / Export:** Used to **Import Data** and **Export Data** relating to the user database.

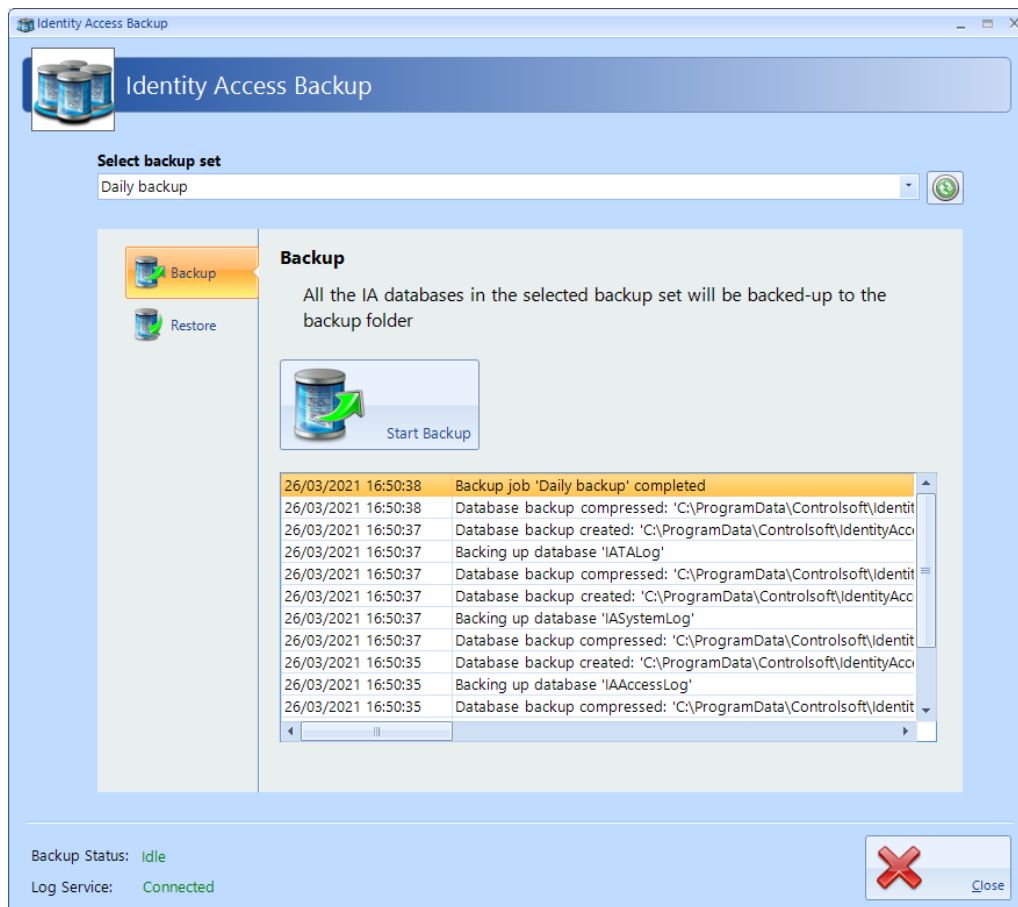
**Export T/A:** Exports Time & Attendance data to third party systems such as Astrow, Clockwatch and Kronos

**Backup:** Backups are configured within the IA Configuration utility (see [IA Configuration - Backup](#) <sup>81</sup>) and will run automatically and/or can be initiated

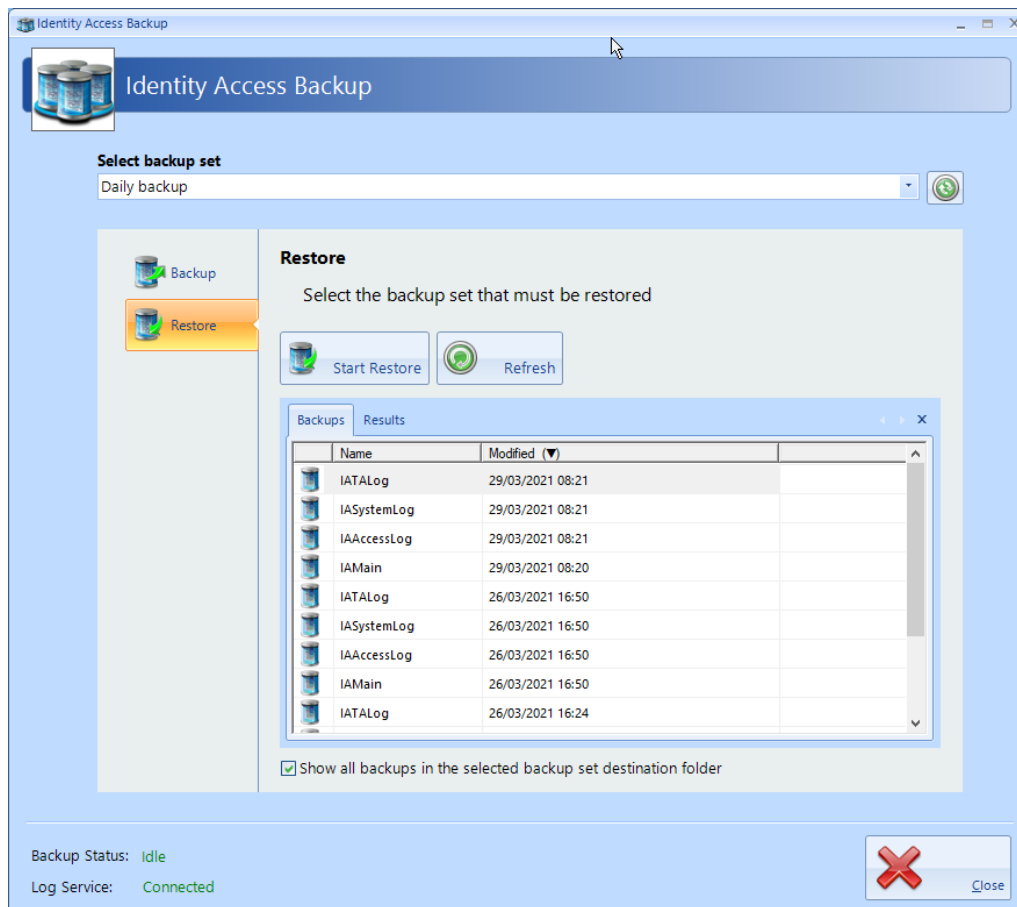
manually as described below. In IA User Interface, click the **Backup** button in the **Tools** menu.



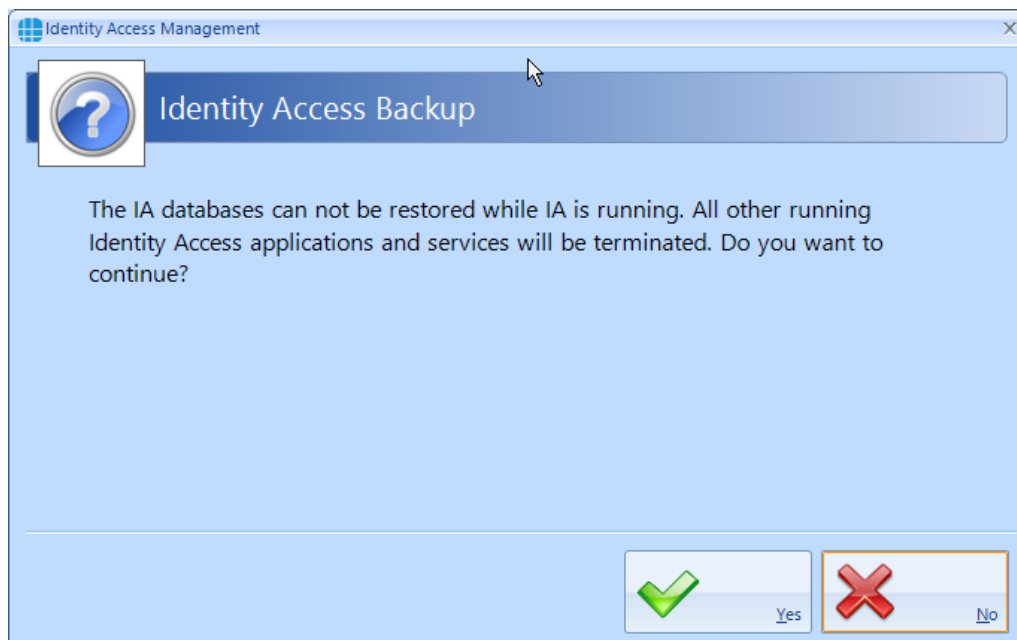
Select the required Backup Set (if more than one have been configured) and click the **[Start Backup]** button. The window under the button will show progress:



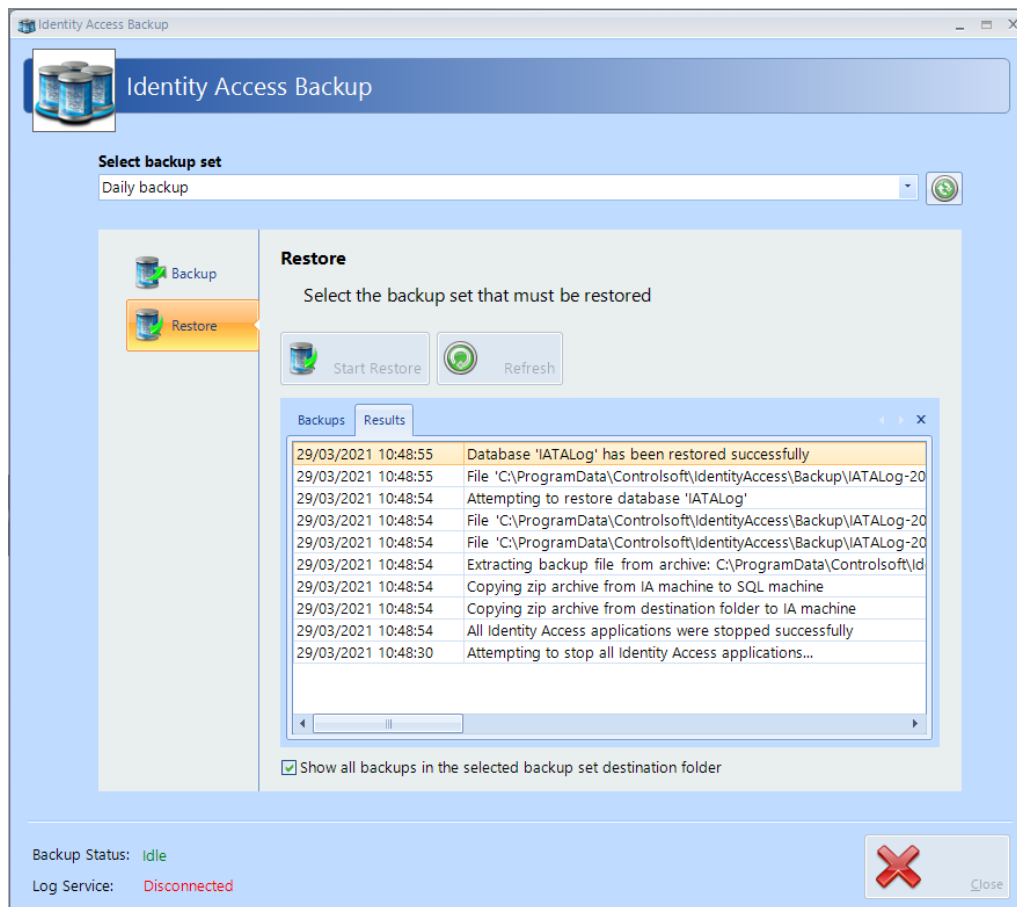
To restore a database, select **Restore** in the side bar:



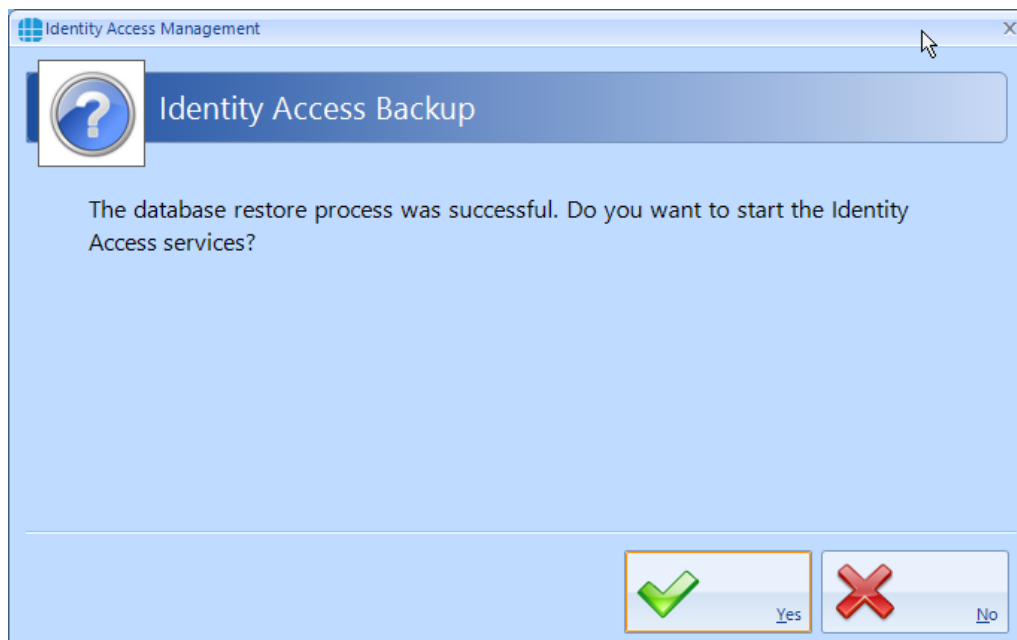
Select the database to be restored and click the **[Start Restore]** button.



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



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](#)<sup>395</sup>)

**iNet Configurator:** runs the utility to configure an iNet controller (see [Appendix F - iNet Configurator](#)<sup>361</sup>)

# Configuring Operators



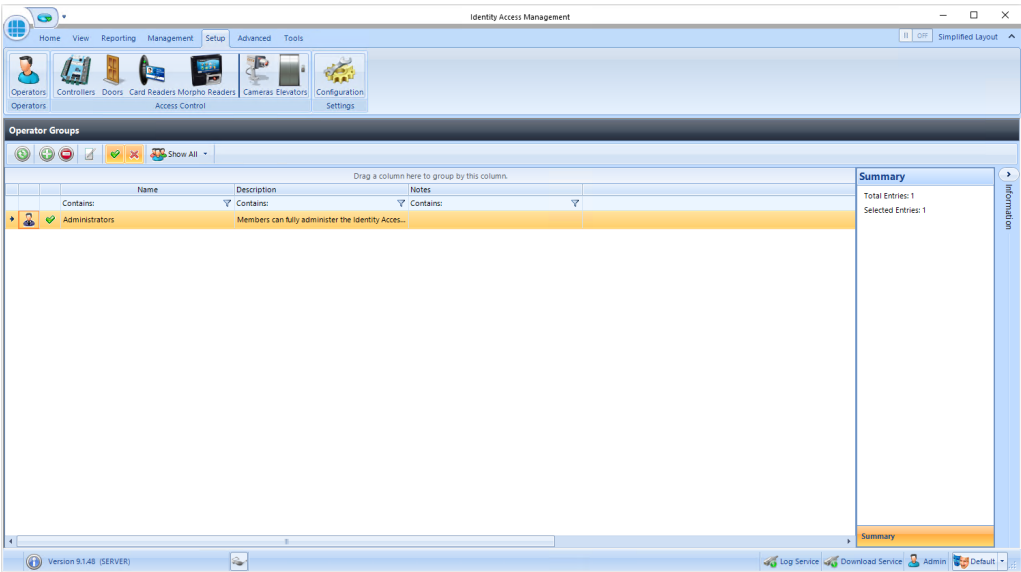
## 5 Configuring Operators

Operators are anyone authorised to access the Identity Access software. Operators can also be Users (usually Employees). If the PC is fitted with a Fingerprint Enrolment reader, operators who are also users can log into the software using their fingerprint, rather than entering a Username and Password.

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). An Operator Group may be given **Administrator** rights, and everyone in that Group will have full access to the software.

When the software is first installed, Controlsoft strongly advise that the credentials for the default Administrator is changed for security reasons. Furthermore, we recommend that the Installation Company create a new Administrator account for themselves, in case the end user forgets their password. Finally, we suggest that an operator group is created where members are restricted from functions that can affect the installed hardware.

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



When first installed, there is just one Operator group called Administrators. This Administrators group comprises one member called Admin, with Username = Admin and Password = Password (both case sensitive).

The option buttons are:



Refresh: Updates the list of operator groups



Add: Creates a new operator group in the list



Delete: Removes the selected operator group/s from the list



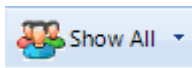
Edit: edits the selected operator groups



Show/Hide Active: This button will show or hide Operators who are Active.



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

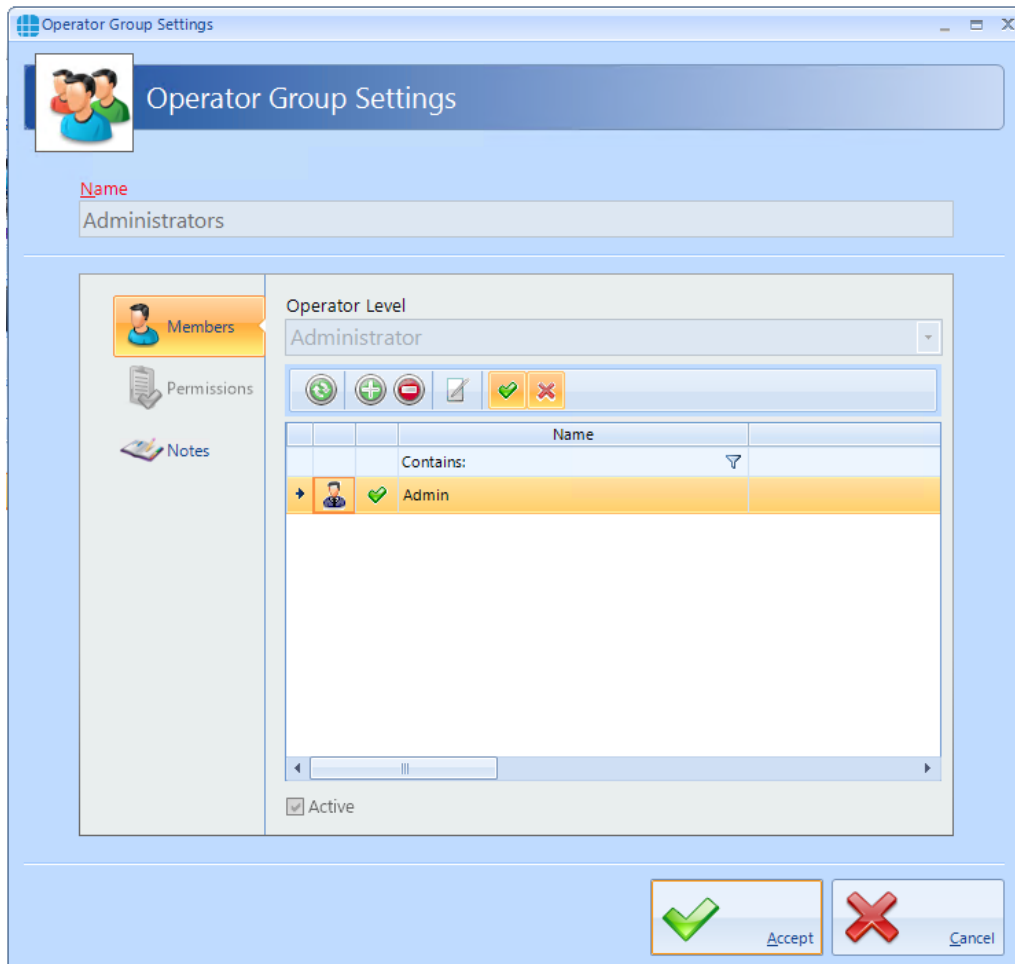


If there are many operator groups in the list, this option will either show all groups, or only Administrator groups, or only non-Administrator Operator Groups.

The **Summary** Box on the right hand side indicates how many Operator Groups exist, and how many are currently selected.

## 5.1 Changing the Default Credentials

To change the credentials for the default Operator called Admin, double click on the Administrators group



The option buttons are:



Refresh: Updates the list of members



Add: Creates a new member to the list



Delete: Removes the selected member/s from the list



Edit: edits the selected member



Show/Hide Active: This button will show or hide members who are Active.



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

To edit the member called Admin, double click the entry or click the Edit button:

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

Change the **Username** and/or **Password** as required. To check the password while entering it, click the 'eye' symbol to the right of the Password box.

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

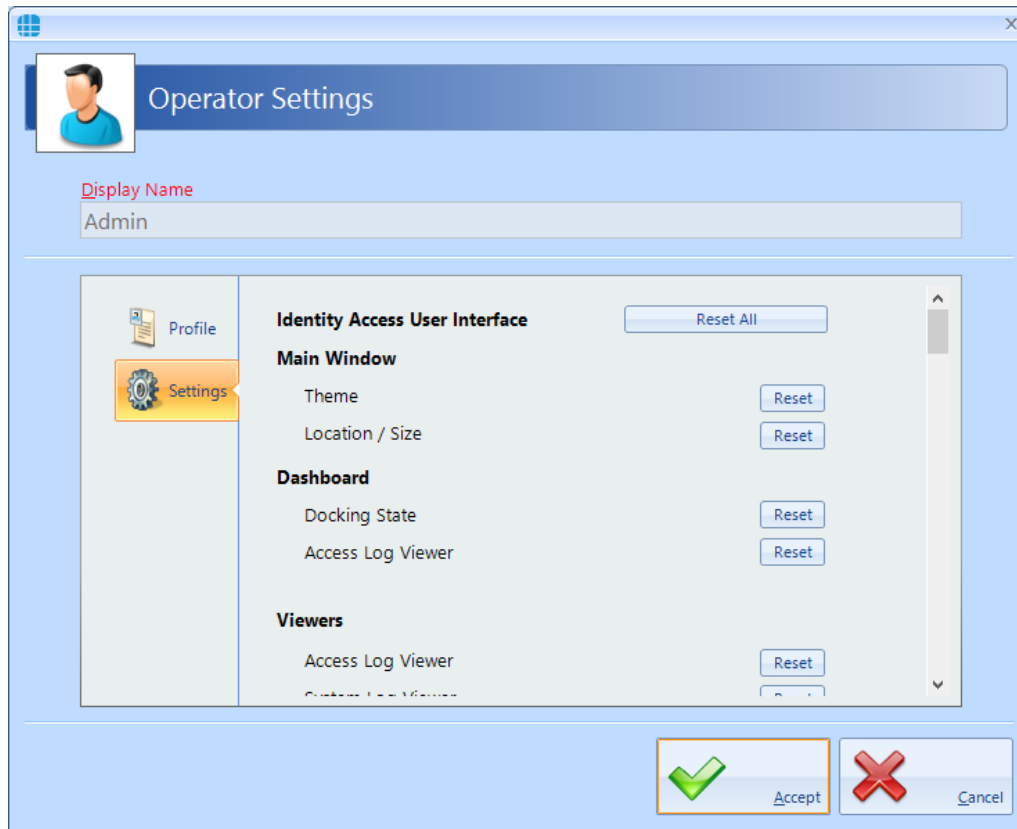
**NOTE: The default credentials are Admin and Password (both case sensitive).**

If the 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 relevant User from the list that appears.

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

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

Select the **Settings** tab in the side bar

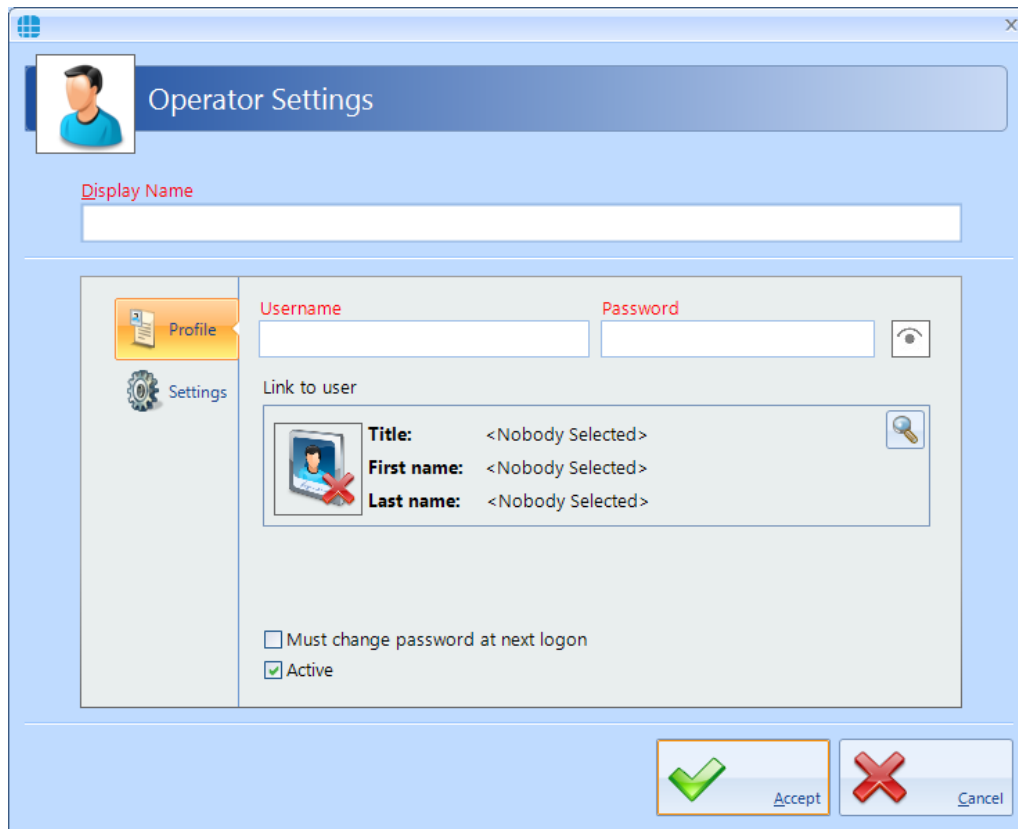


Depending on how the User Profiles are configured in the IA Configuration utility, you will have options to reset various screens, such as their size and location

Click **[Accept]** when done.

## 5.2 Adding an Administrator

To Add a new Administrator to the group, double click on **Administrators** in the Operators window and click the **Add** icon:



Enter a name for the new Administrator under **Display Name**.

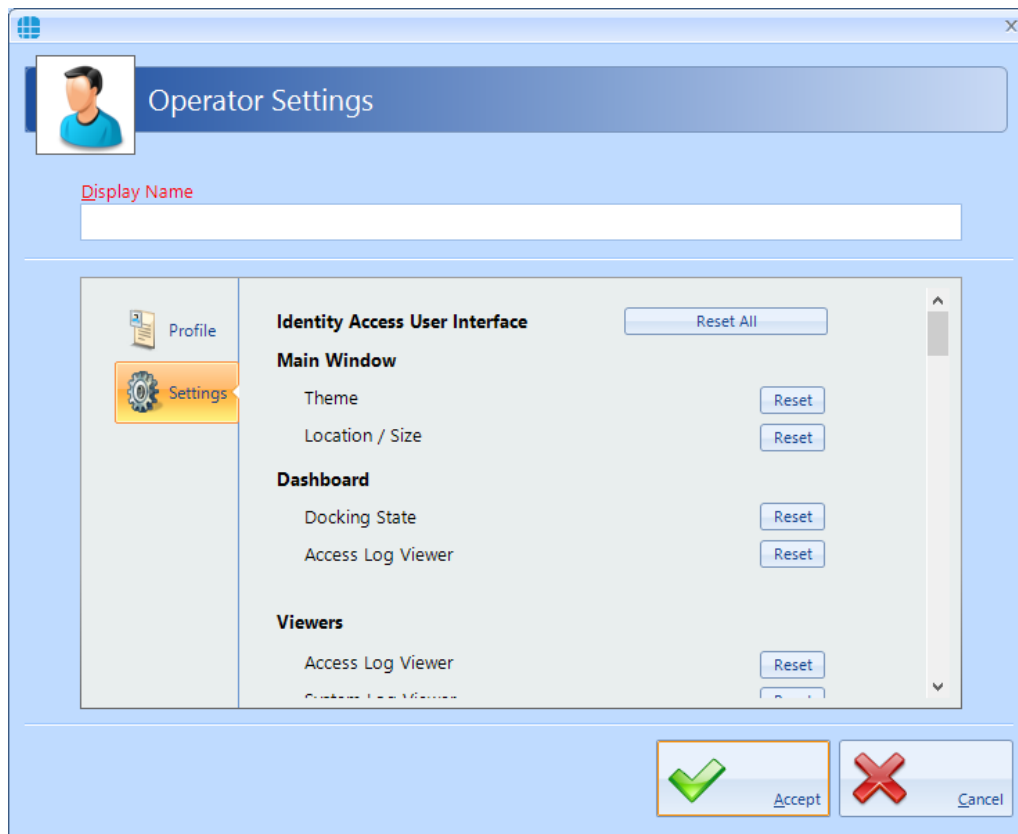
Enter a **Username** and **Password** as required. To check the password while entering it, click the 'eye' symbol to the right of the Password box. Once a Password has been entered, it can no longer be viewed.

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.

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.

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.

Select the **Settings** option in the side bar

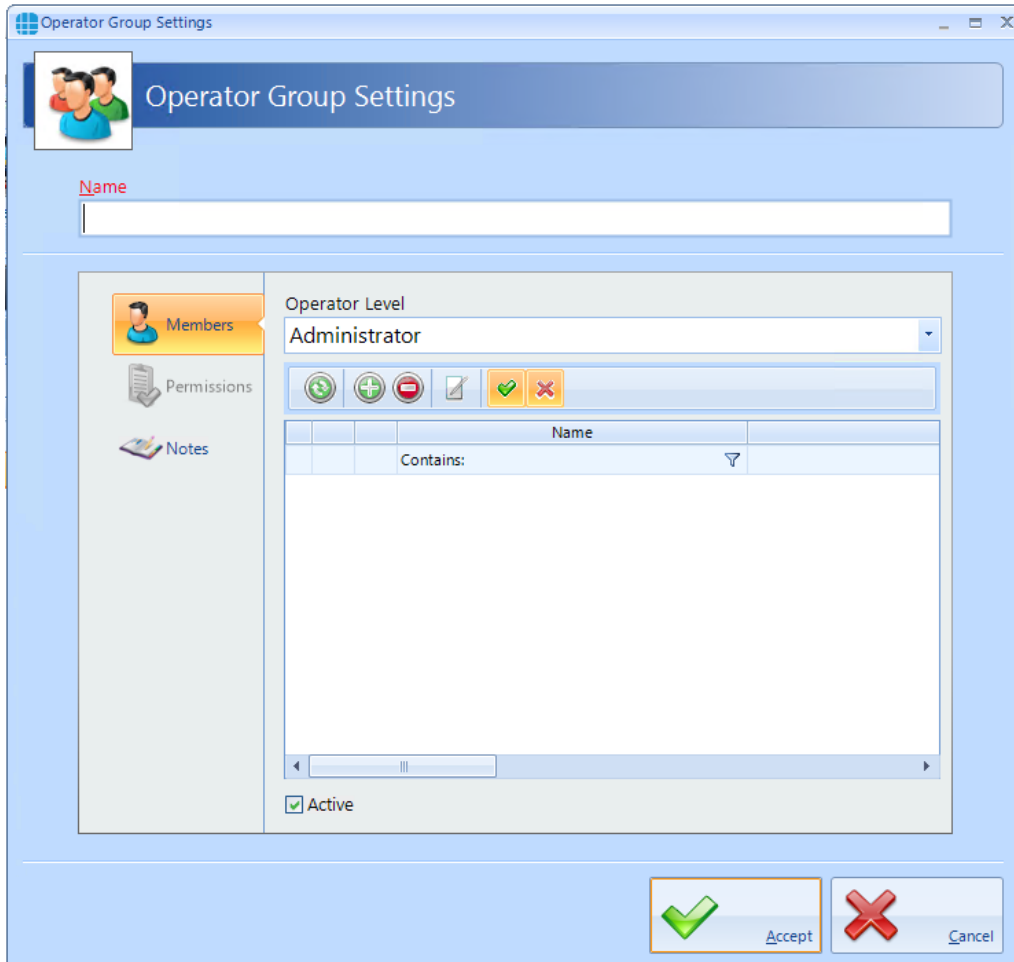


Depending on how the User Profiles are configured in the IA Configuration utility, you will have options to reset various screens, such as their size and location

Click **[Accept]** when done.

### 5.3 Adding an Operator

To Add a new Operator's Group to the software, click the **Add** icon in the **Operator Groups** window to display the **Operator Group Settings**:



The **Operator Group Settings** window is displayed. It features a sidebar with icons for **Members**, **Permissions**, and **Notes**. The main area contains a **Name** input field at the top. Below it, the **Operator Level** is set to **Administrator**. A toolbar with icons for adding, removing, and saving is present. A table with the header **Name** and a filter icon is shown, with a **Contains:** search bar. At the bottom left, there is a **Active** checkbox. At the bottom right, there are **Accept** and **Cancel** buttons.

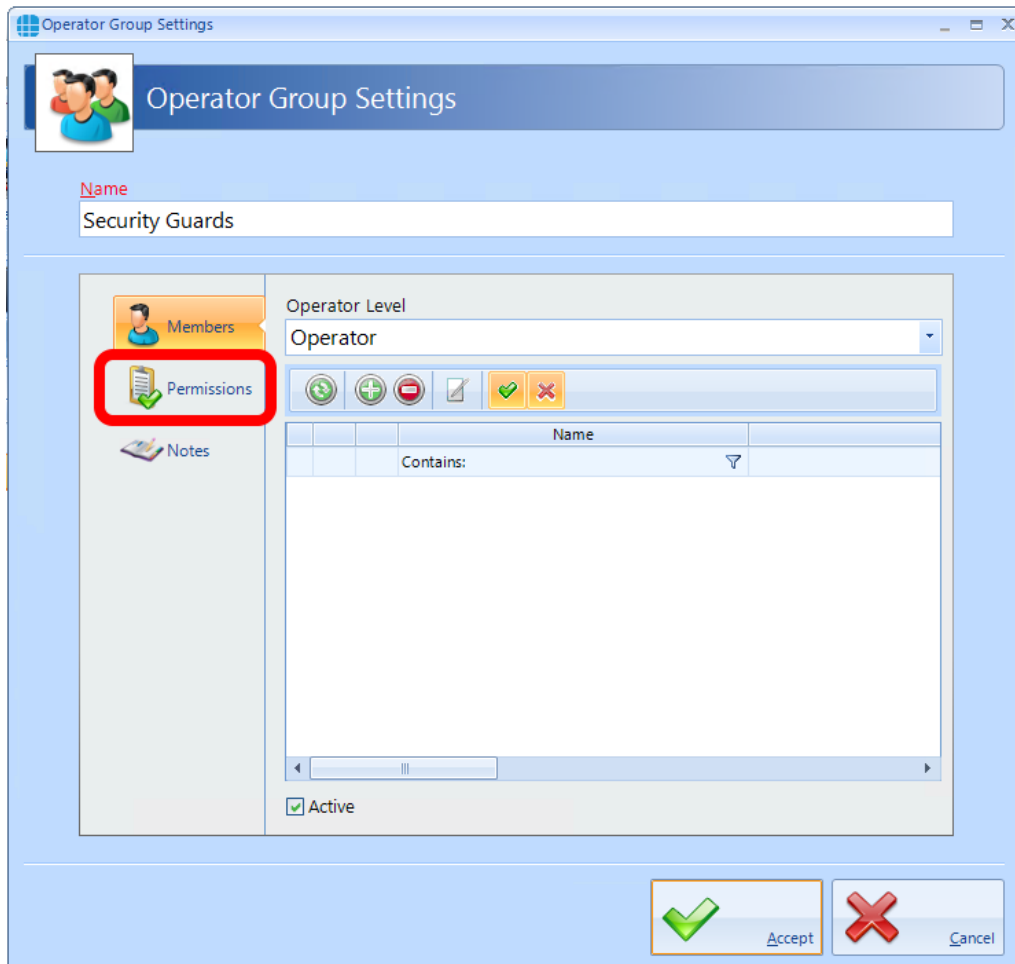
Name
Contains: <input type="text"/>

Enter a **Name** for the new Group.

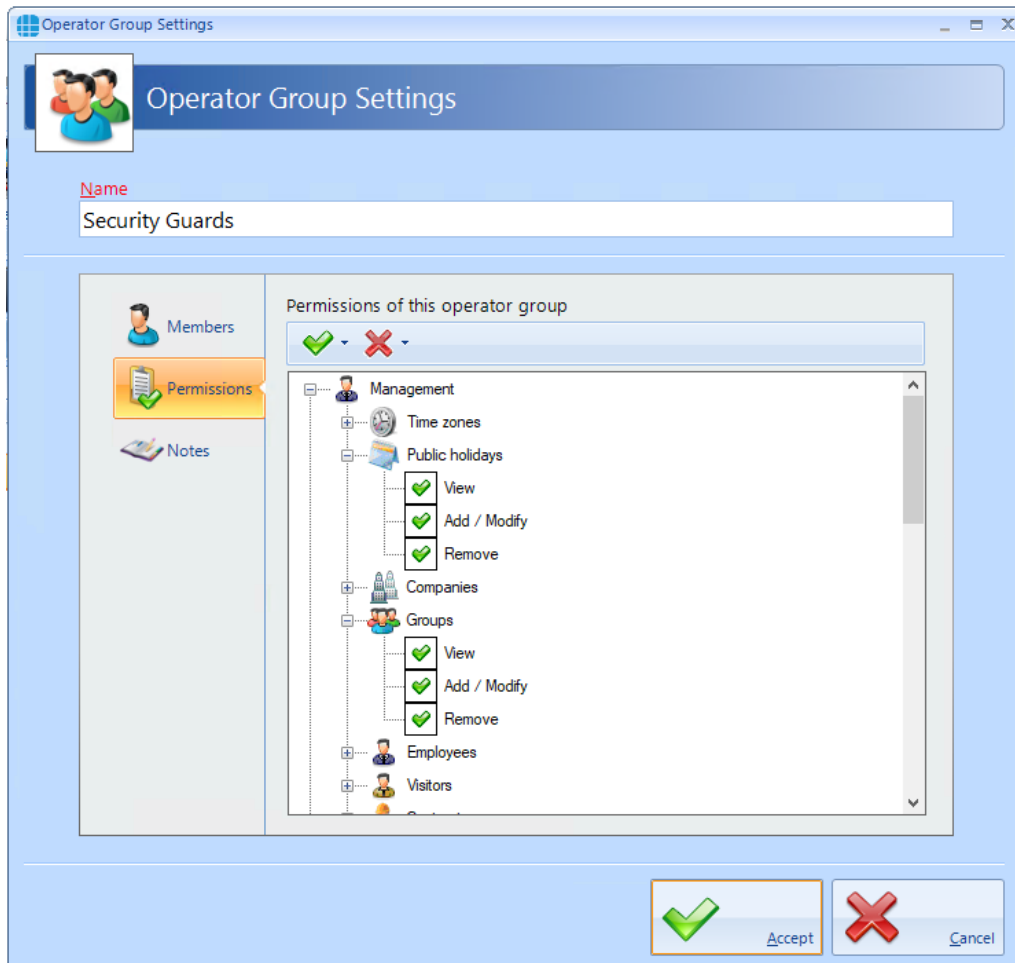
Choose the required **Operator Level** from **Administrator** (able to access all functions within the software) or **Operator** (only has access to defined functions)



If Operator is selected, the Permissions tab in the left hand side bar will no longer be greyed out allowing you to set the functions accessible to members of that group:



Select the Permissions tab:



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.

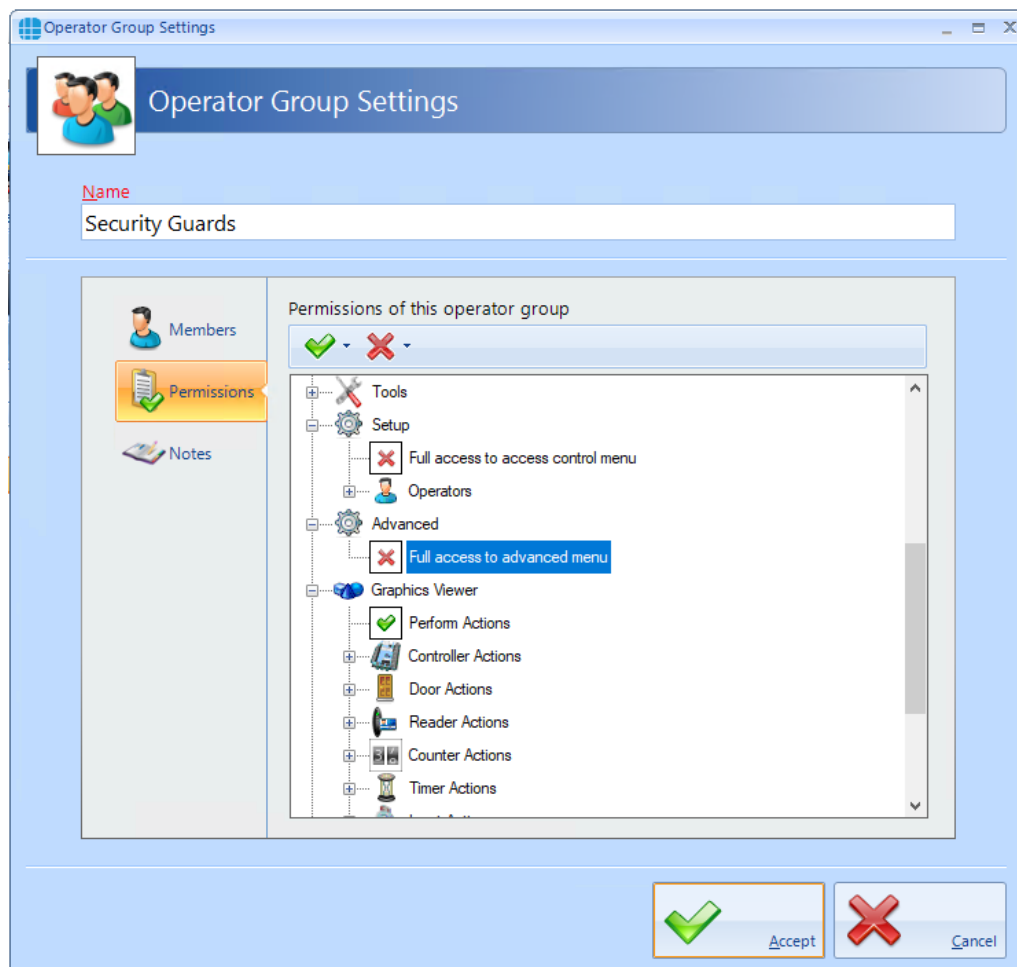



will enable all items, selected items or all items within a permissions group

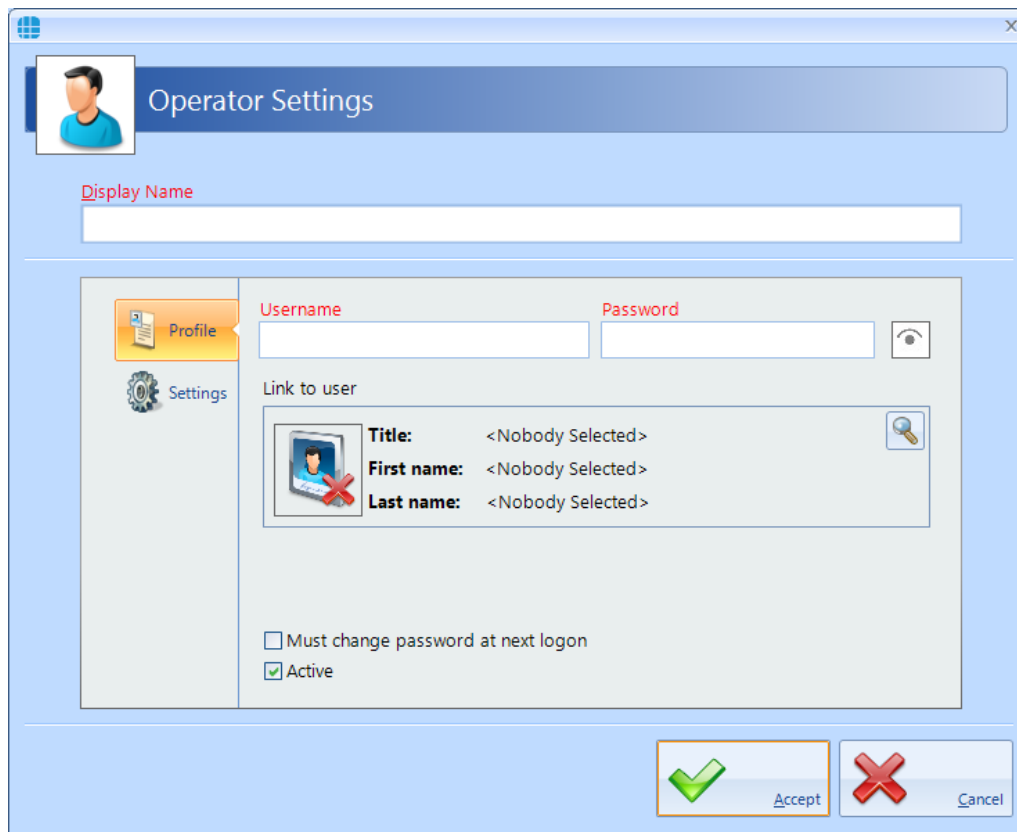


will disable all items, selected items or all items within a permissions group

For example, to prevent all members of this Operator Group from accessing the Access Control and Advanced menus, scroll to the relevant items and double click the green ticks to change it to a red cross as shown below:



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

The image shows a software window titled "Operator Settings". At the top left is a small profile icon. Below it is a text field labeled "Display Name". The main area is divided into two sections. The left section has a sidebar with "Profile" (selected) and "Settings". The right section contains fields for "Username" and "Password", with an eye icon to toggle password visibility. Below these is a "Link to user" section with a magnifying glass icon and a list showing "Title: <Nobody Selected>", "First name: <Nobody Selected>", and "Last name: <Nobody Selected>". At the bottom are two checkboxes: "Must change password at next logon" (unchecked) and "Active" (checked). At the very bottom are "Accept" and "Cancel" buttons with green and red checkmark icons respectively.

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

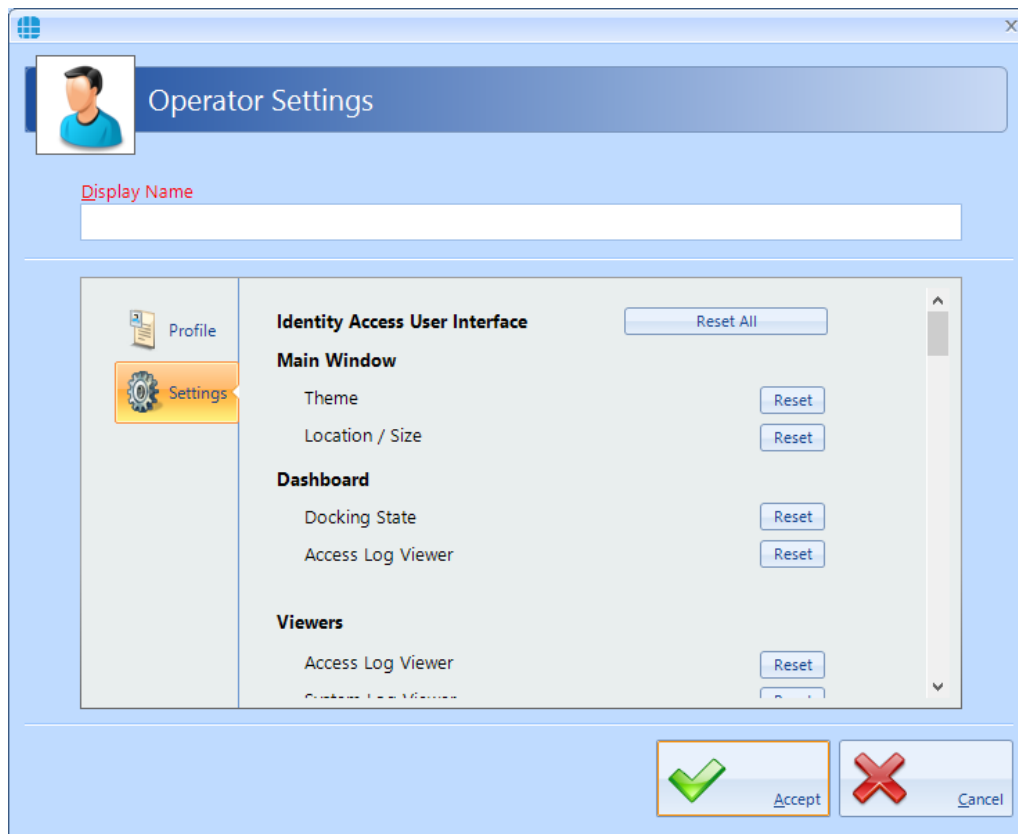
Enter a **Username** and **Password** as required. To check the password while entering it, click the 'eye' symbol to the right of the Password box. Once a Password has been entered, it can no longer be viewed.

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.

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

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

If User Profiles have been selected in the IA Configuration utility, the Settings tab in the side bar allows the size, location etc of screens to be reset.



Click **[Accept]** when done.

# **Configuring the Access Control Hardware**

## 6 Configuring the Access Control Hardware

The procedure for configuring an Access Control system in the Identity & Access software is as follows:

1. Configure the Master Controllers (Installer function)
2. Configure the Doors and link them to the relevant Master Controllers (Installer function)
3. Configure the Readers and link them to the relevant Doors (Installer function)
4. Configure Time Zones (if required) and link them to the relevant Master Controllers (Installer or End User function)
5. Configure Groups and link them to Readers and Time Zones (Installer or End User function)
6. Configure Employees, Visitors and/or Contractors and allocate them to the relevant Group/s (Installer or End User function).

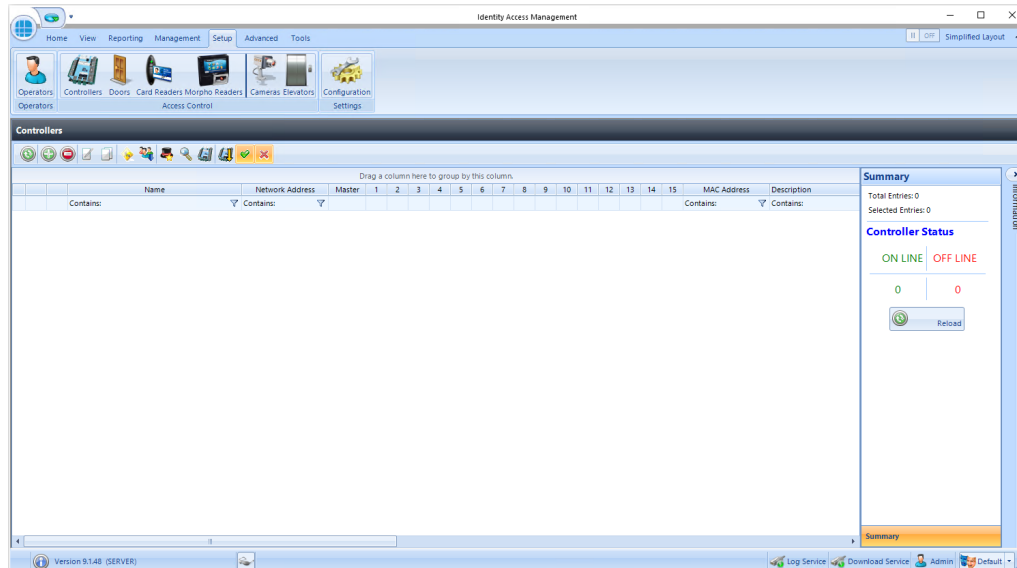
***NOTE: Before starting to configure the system in Identity Access, it is advisable to draw the layout of the building on a large sheet of paper, showing where all the doors are, where the controllers and readers will be situated etc. Add identifiable names, bus addresses and input & output numbers to this drawing for all the controllers, doors, readers etc. as this will make the programming much faster and will result in fewer programming errors. Where readers change the user's Location between "Inside" and "Outside", add this to the diagram to reduce confusion later.***

# Configuring Master Controllers



## 7 Configuring Master Controllers

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



This Controllers window shows that there are no controllers in the database. 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



Incremental Download: initiates an Incremental Download to the selected controllers



Door Configuration Wizard: Helps configure the doors on the controller (see [Door Configuration Wizard](#)<sup>139</sup>).



**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 [Find IP Controller Wizard](#)<sup>[133]</sup>).



**Configure:** This feature allows the controller's internal webpage to be configured, as per iNet Configurator. (see [IP Controller Configurator](#)<sup>[135]</sup>)



**Shows and hides the Controller Status Master Overview** (see [Appendix M - Controller Status](#)<sup>[398]</sup>)



**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.



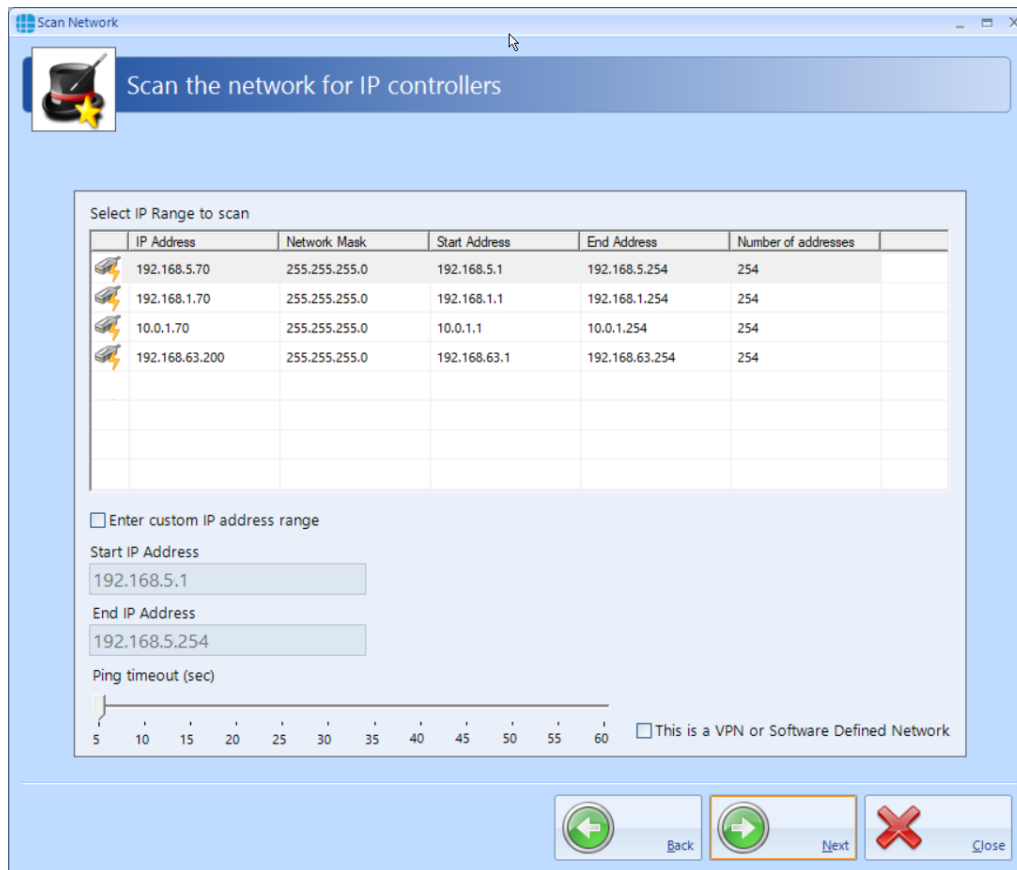
Click on the **Add** button to manually create a new Master Controller and display the **Master Controller Settings** window. The creation of controllers can be greatly simplified, however, by using the Find IP Controller Wizard:



To start the wizard, click on the Scan button then click **[Next]**

## 7.1 Find IP Controller Wizard

Firstly, select the network range from the list available, or enter a Start IP Address and Stop IP Address to define the range to be scanned:



IP Address	Network Mask	Start Address	End Address	Number of addresses
192.168.5.70	255.255.255.0	192.168.5.1	192.168.5.254	254
192.168.1.70	255.255.255.0	192.168.1.1	192.168.1.254	254
10.0.1.70	255.255.255.0	10.0.1.1	10.0.1.254	254
192.168.63.200	255.255.255.0	192.168.63.1	192.168.63.254	254

☐ Enter custom IP address range

Start IP Address  
192.168.5.1

End IP Address  
192.168.5.254

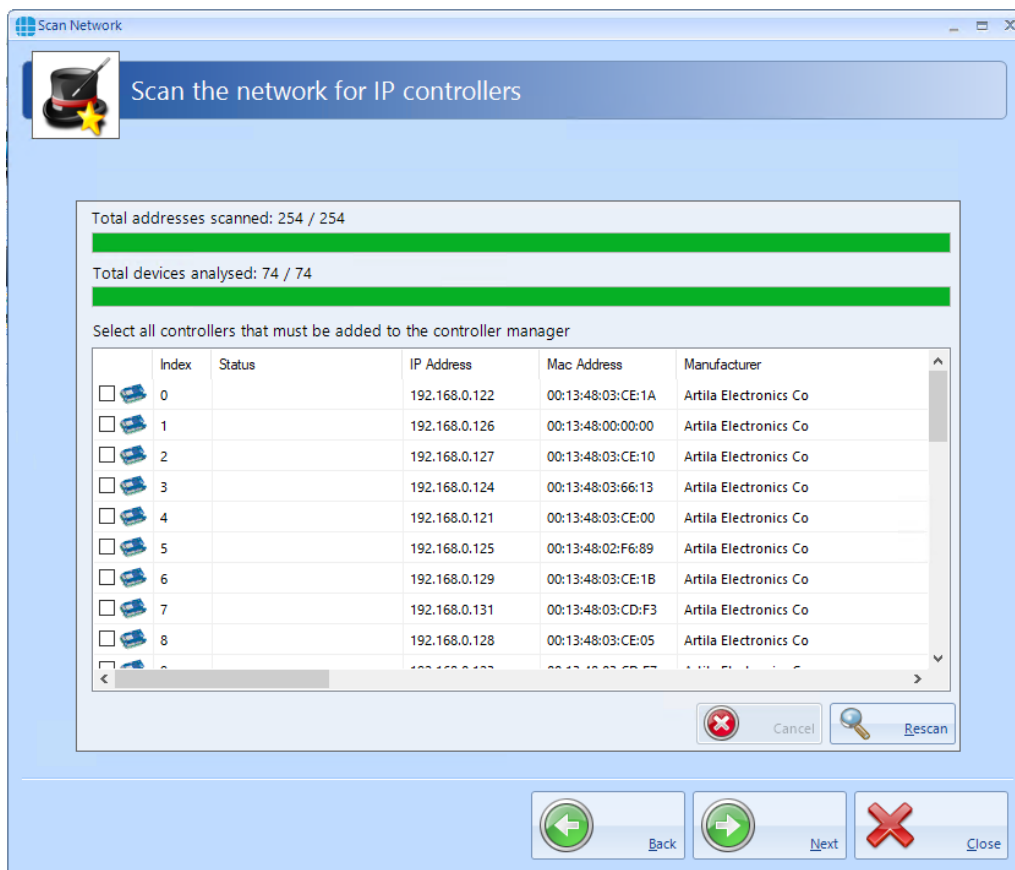
Ping timeout (sec)  
5 10 15 20 25 30 35 40 45 50 55 60

☐ This is a VPN or Software Defined Network

Back Next Close

The system will then scan the IP network for iNet controllers





Select the controller/s to be added to the system, then select **[Next]**, followed by **[Finished]**.

These controller/s will then be added to the list of available controllers in the Controllers screen. The right hand side of this screen will now show the **Controller Status** for the new controller/s as **OFFLINE** which will change to **ONLINE** after a few seconds.

## 7.2 IP Controller Configurator



The IP Controller Configurator feature allows the internal configuration options of an iNet Master Controller to be configured. The operation of this feature is the same as the iNet Configurator program available from the Controlsoft website. For further information iNet Configurator, please refer to [Appendix F - iNet Configurator](#)

## 7.3 Controller General

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

The screenshot shows the 'Master Controller Settings' window with the 'General' tab selected. The window has a sidebar with icons for General, Settings, Timeouts, Sirens, Events, and Notes. The main area contains the following fields and controls:

- Name:** A text input field.
- Network Address:** A text input field containing '10.0.1.230'.
- MAC Address:** A text input field.
- Controller Type:** A dropdown menu set to '1 Door Controller'.
- 485 Network:** A section with a header bar and a grid of RS485 addresses. The first address, 'RS485 Address 1', is highlighted in blue and labeled 'NONE'. Below the grid is a yellow bar with the text 'Click on slave to select'.
- Active:** A checkbox that is checked.
- Buttons:** 'Accept' (green checkmark) and 'Cancel' (red X) buttons at the bottom right.

RS485 Address 1	RS485 Address 2	RS485 Address 3	RS485 Address 4	RS485 Address 5	RS485 Address 6	RS485 Address 7	RS485 Address 8
NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE

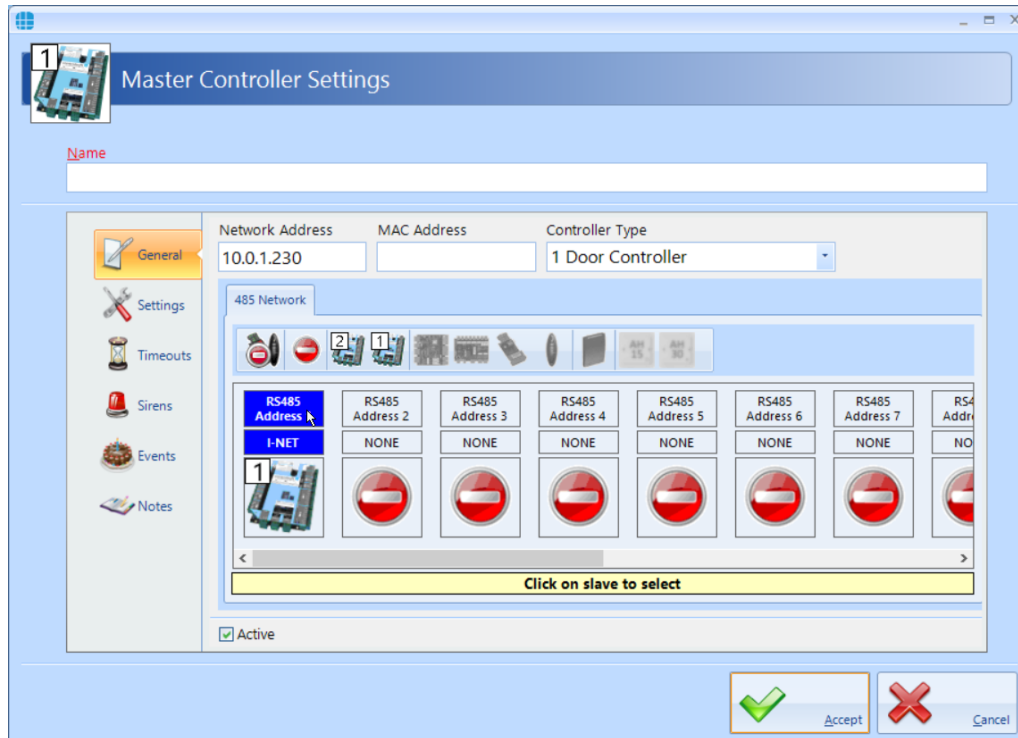
Enter a **Name** to identify the controller (e.g. Ground Floor)

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, but may help to identify the controller during a maintenance visit (this will be already populated if the controller was added via the Find IP Controllers Wizard). **NOTE: The MAC address for older iNets start with 001348 whereas the MAC address for 1DR and 2DR iNets start with F8DC7A**

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

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 AC3151 Reader Expander Board to the RS485 bus



Add an IOC IO Expander Board to the RS485 bus



Add an AC-4550 Wiegand to RS485 convertor to the RS485 bus



Add an AC-1100 reader to the RS485 bus



Add an HID OSDP reader to the RS485 bus. For further information on HID OSDP readers, please refer to [Appendix J - HID OSDP Readers](#) <sup>386</sup>



Add an Aperio AH15 (1:1) hub to the RS485 bus. For further information on Aperio Wireless Locks, please refer to [Appendix A - Types of Door](#) <sup>323</sup>

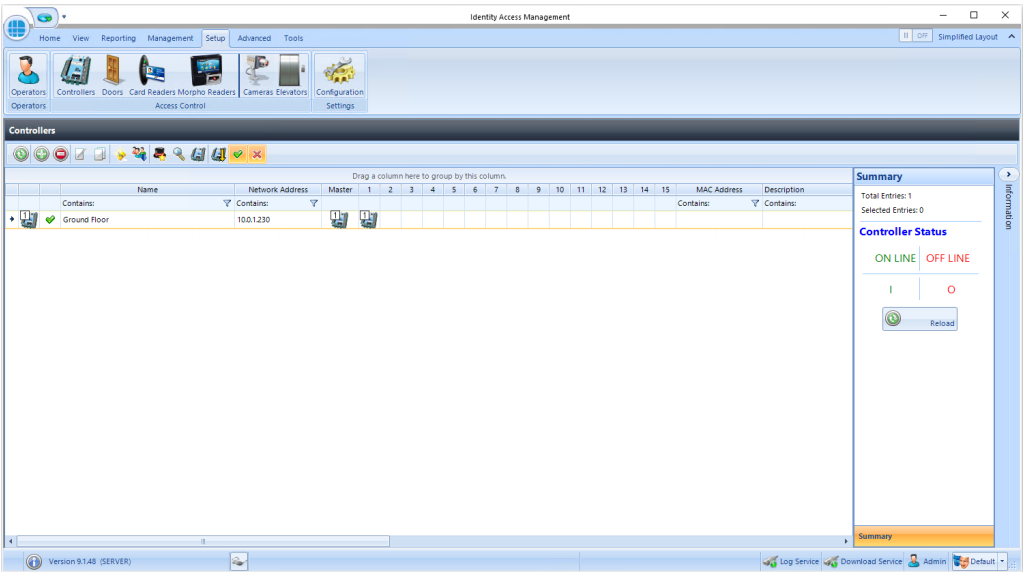


Add an Aperio AH30 (1:8) hub to the RS485 bus. For further information on Aperio Wireless Locks, please refer to [Appendix A - Types of Door](#) <sup>323</sup>

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.

Click the **[Accept]** button when finished and the new controller will be displayed in the Controllers window, complete with any devices that have been selected on the RS485 bus.



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](#)

## 7.4 Door Configuration Wizard

The Door Configuration Wizard greatly simplifies the process of setting up the doors. For the Door Configuration Wizard to work, the hardware must have been connected using default settings:

- Door 1 = Relay 0 (Lock); Input 0 (REX); Input 1 (Door Contact if used); Reader 1
- Door 2 = Relay 1 (Lock); Input 2 (REX); Input 3 (Door Contact if used); Reader 2
- Fire Alarm (if used) = Input 4

Having configured the Master Controller, activate the Door Configuration Wizard by selecting the relevant controller and clicking the Door Configuration Wizard



Door Configuration Wizard

Controller: Ground Floor

RS485 Address 0	RS485 Address 1	RS485 Address 2	RS485 Address 3	RS485 Address 4	RS485 Address 5	RS485 Address 6	RS485 Address 7
I-NET	I-NET	NONE	NONE	NONE	NONE	NONE	NONE

☒ Create this door and readers

☐ No Doors
 ☐ 1 Door - Reader IN
 ☐ 1 Door - Reader IN & OUT
 ☒ 2 Doors - Reader IN

☒ Normal Door
 ☐ Turnstile
 ☐ Airlock

☐ Enforce APB

Door 1 name:

Door 2 name:

Accept Cancel

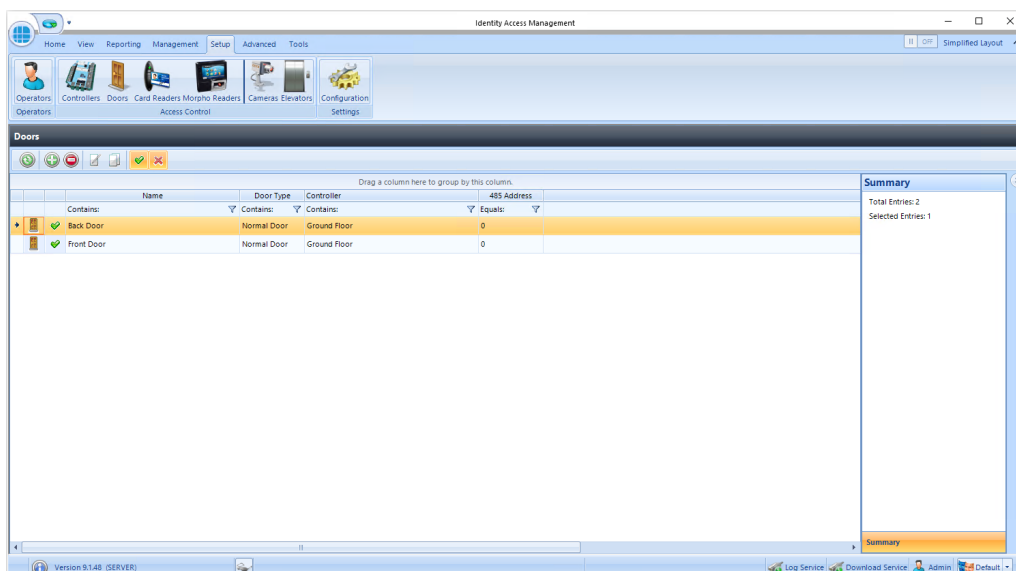
Select the Master controller then select appropriate option whether the controller is connected to 1 door with an IN reader, 1 door with IN and OUT readers, or 2 doors with IN readers (as in the above example). When the required option is selected, the tickbox **Create this door and readers** will be automatically selected.

**NOTE: The door options for Turnstile, Airlock and Enforce APB will be greyed out unless an Identity Access Professional or Enterprise Features Licence has been applied.**

**NOTE: For further information on AntiPassBack (APB), please refer to [Appendix E - AntiPassBack](#)**

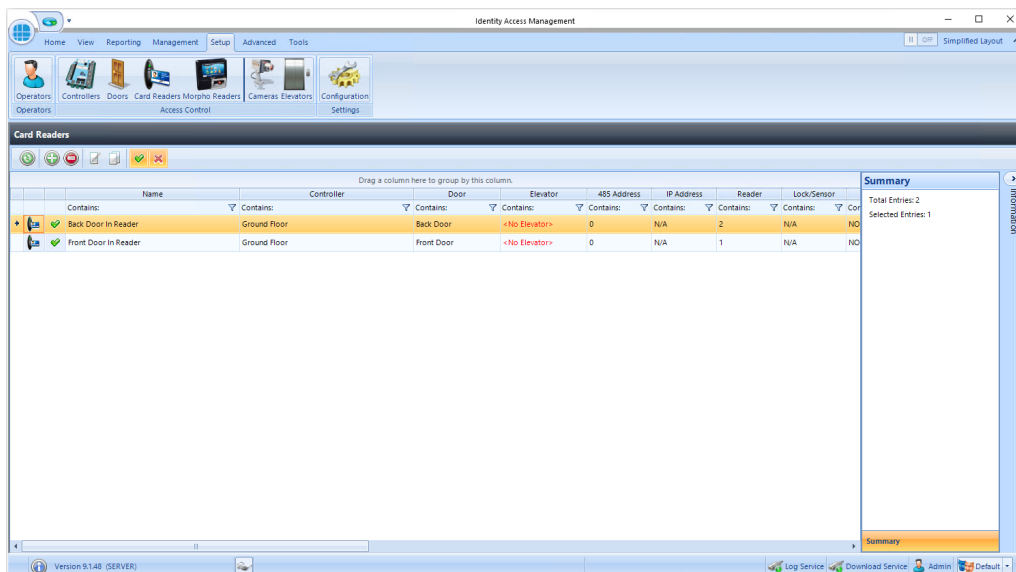
Enter name/s for the door/s to be created and click **[Accept]**.

Having created the 2 doors, selecting the **Doors** icon will then display the doors on that Master Controller as shown below:



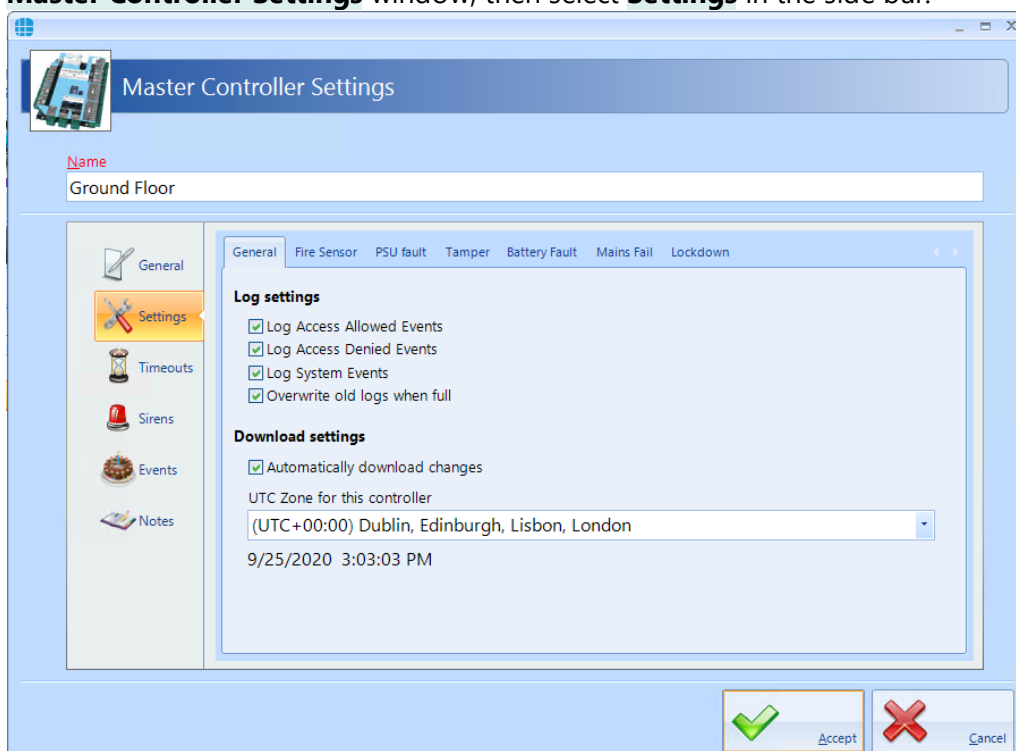
As can be seen, the Master Controller called "Ground Floor" now has 2 doors called "Front Door" and "Back Door". These names can be changed if required by editing the door properties (see [Door Properties General](#))

Checking the **Card Readers** window will also display the card readers created by the Door Configuration Wizard.



## 7.5 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.

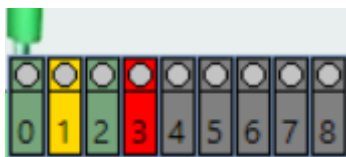
**Automatically download changes** ensures that changes are downloaded to the controller as they happen rather than having to remember to perform a Rebuild at the end of the programming.

**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)**
- **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

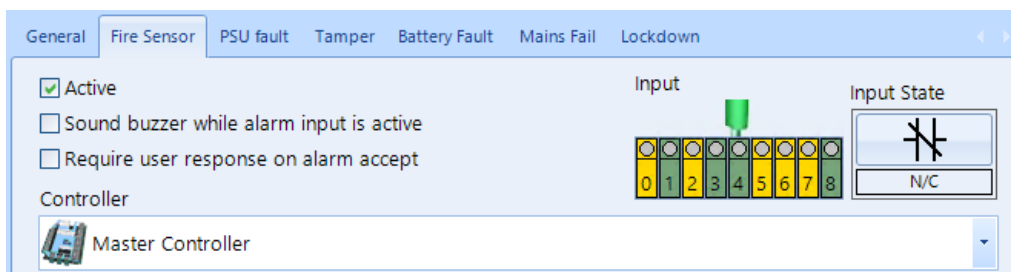


acceptable



or red if it is unacceptable

## Fire Sensor:

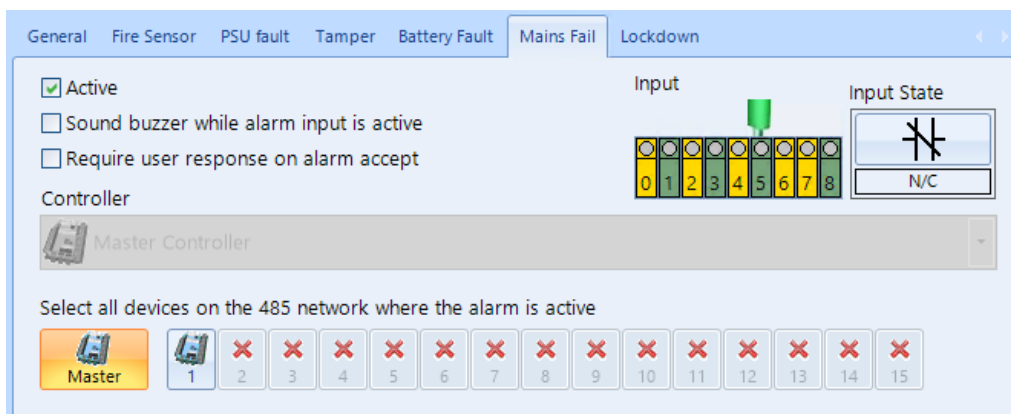


If doors on this channel are to be released during a fire alarm, tick the **Active** box, then select the **Input** the Fire Panel is connected to, and whether the Fire panel contacts are **N/C** (Normally Closed) or **N/O** (Normally Open). The option **Sound buzzer while alarm input is active** will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

## Mains Fail:



To monitor the power supply for Mains Fail, tick the **Active** box, then select the **Input** the Main Fail signal is connected to, and whether the 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 mains fail condition.

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

**Select all devices on the 485 network where the alarm is active** defines which devices are monitoring for Mains Fail. In the example above, the Master monitors for Mains Fail (e.g. IA-ACUPLUS) whereas Downstream 1 does not (e.g. IA-ACB)

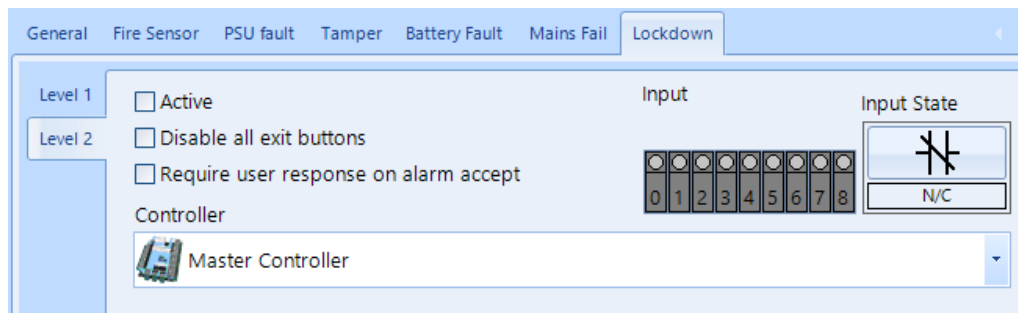
Battery Fault (Input 7), PSU Fault (not active by default) and Tamper (Input 6) can be selected as described above.

## Lockdown:

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.

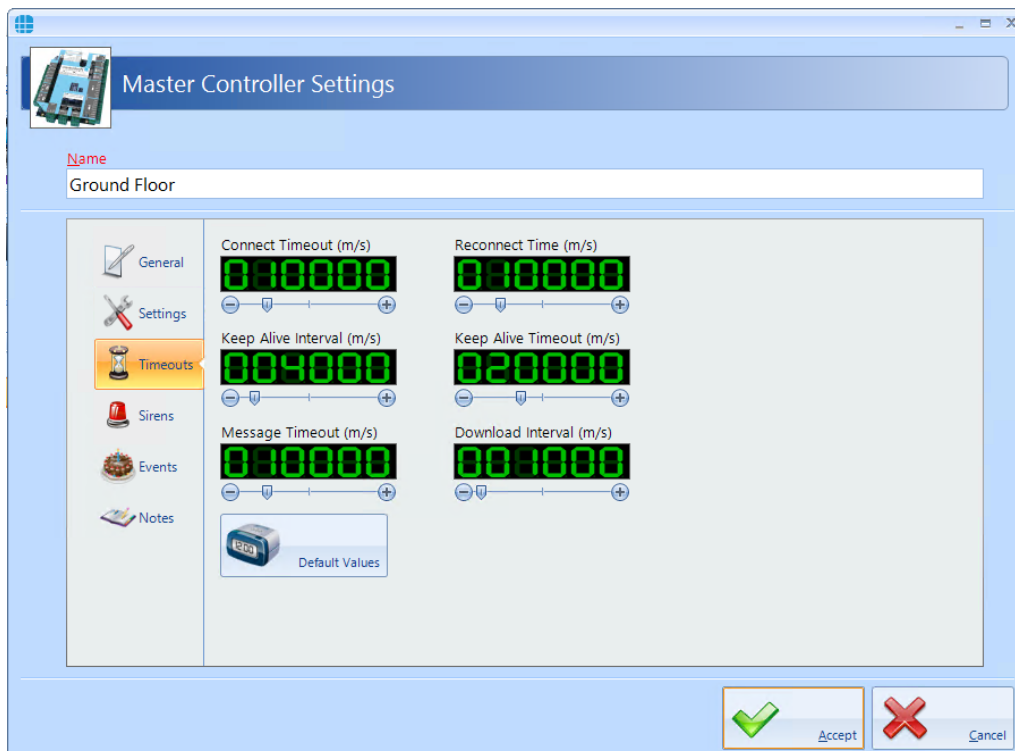
If **Require user response on alarm accept** is ticked, the operator must enter text before the Lockdown alarm can be accepted and subsequently cleared.

***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.***

## 7.6 Controller Timeouts

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

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



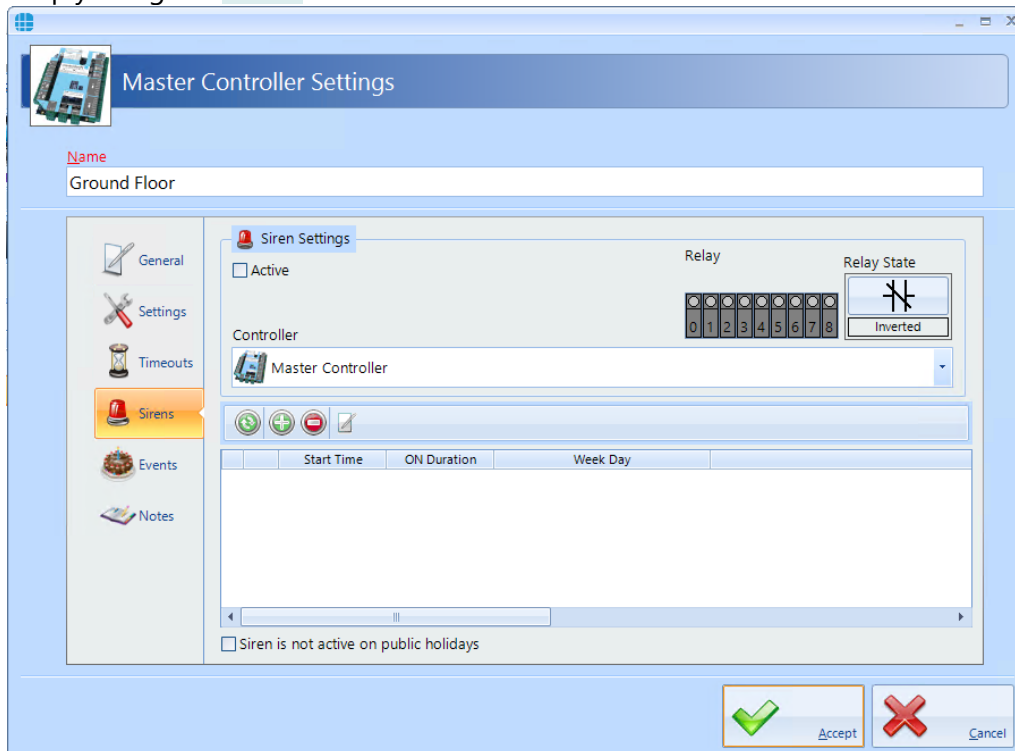
**NOTE: All the timers in this window are in milliseconds.**

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



## 7.7 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)

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



**Siren Time Settings**

**General**

**Start time**

08:59

**Hour**

1	2	3
4	5	6
7	8	9
10	11	12

**Minute**

00	05	10
15	20	25
30	35	40
45	50	55

**Day of week**

- ☒ Monday
- ☐ Tuesday
- ☐ Wednesday
- ☐ Thursday
- ☐ Friday
- ☐ Saturday
- ☐ Sunday

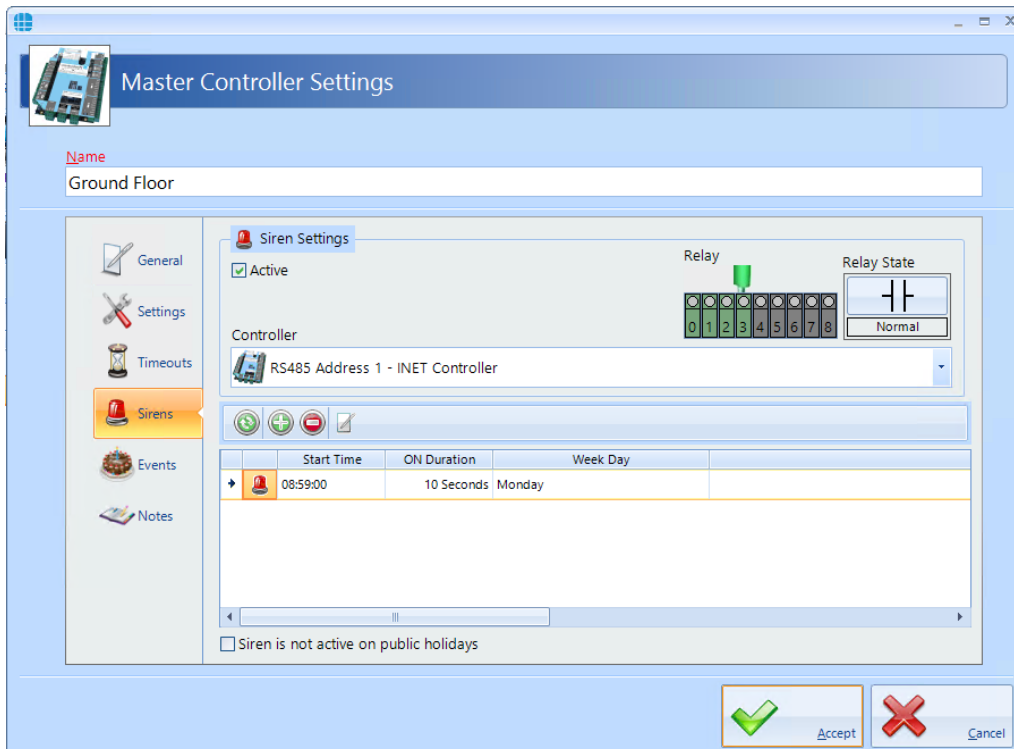
**Siren Duration (seconds)**

88

**Accept** **Cancel**

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).

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



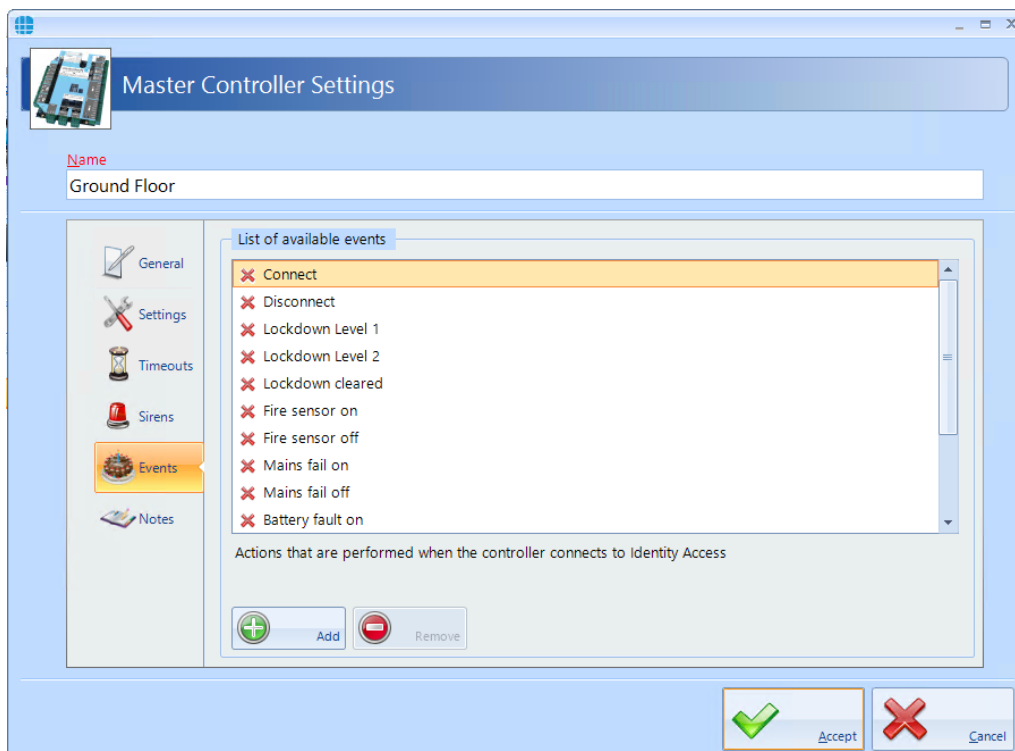
The screenshot shows the 'Master Controller Settings' window. The 'Name' field is set to 'Ground Floor'. The 'Siren Settings' tab is selected, showing a 'Relay' status of 'Active' and a 'Relay State' of 'Normal'. The 'Controller' is set to 'RS485 Address 1 - INET Controller'. A table lists siren events with columns for Start Time, ON Duration, and Week Day. The first event is at 08:59:00 for 10 seconds on Monday. A checkbox at the bottom indicates 'Siren is not active on public holidays'.

Start Time	ON Duration	Week Day
08:59:00	10 Seconds	Monday

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

## 7.8 Controller Events

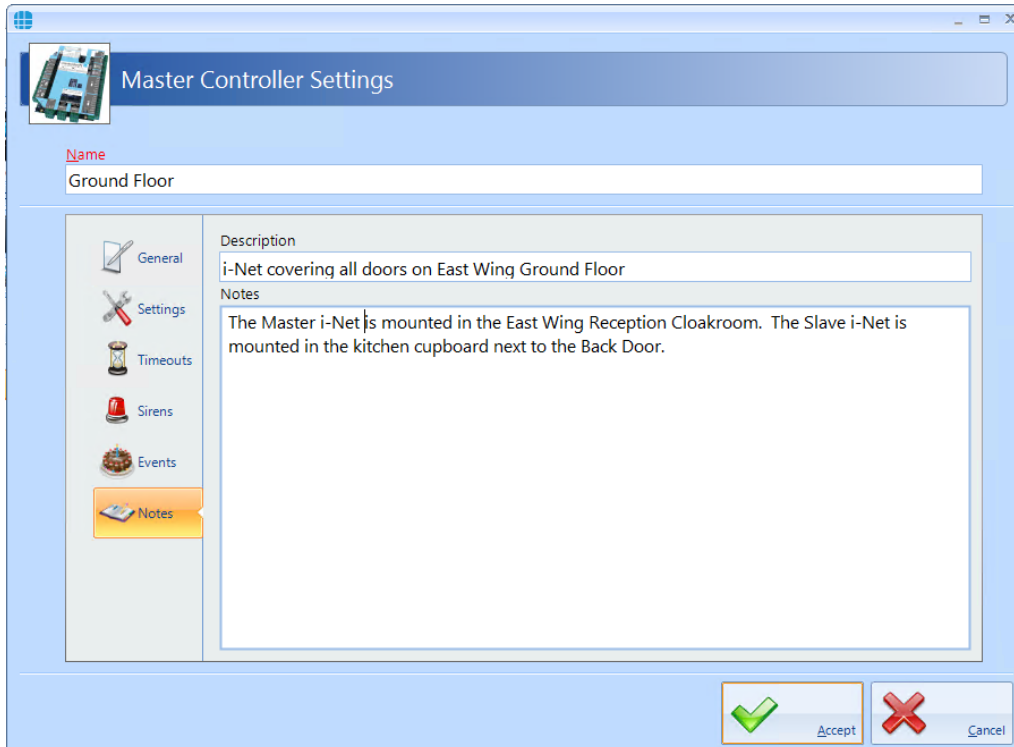
The Events tab will indicate whether any Events have been configured for the selected controller.



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,

## 7.9 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.

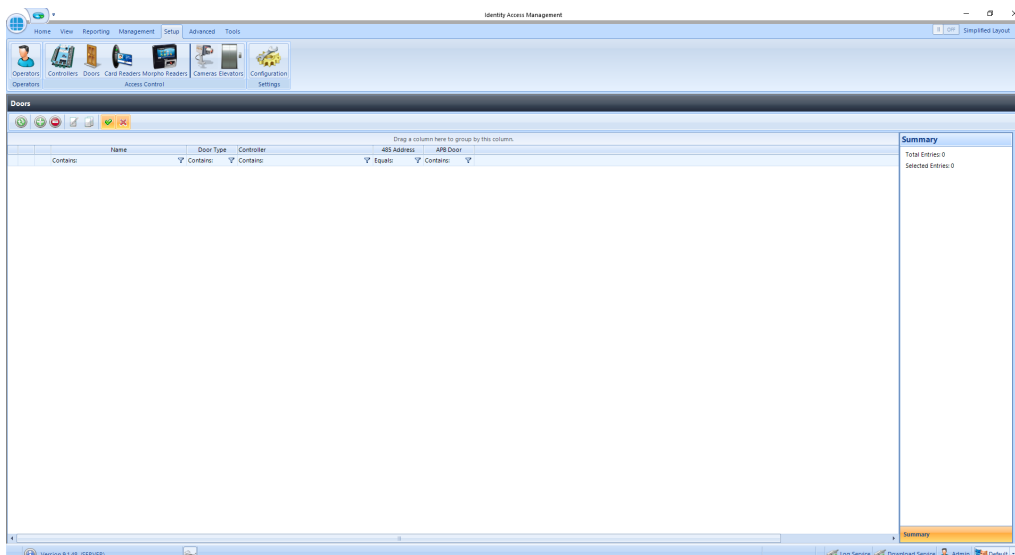


The screenshot shows the 'Master Controller Settings' window. The 'Name' field is set to 'Ground Floor'. The 'Notes' section is active, showing a 'Description' field with the text 'i-Net covering all doors on East Wing Ground Floor' and a 'Notes' text area with the text 'The Master i-Net is mounted in the East Wing Reception Cloakroom. The Slave i-Net is mounted in the kitchen cupboard next to the Back Door.' The 'Notes' section is highlighted in the side bar. At the bottom right, there are 'Accept' and 'Cancel' buttons.

# Configuring Doors

## 8 Configuring Doors

Doors can be configured using the **Door Configuration Wizard** (see [Door Configuration Wizard](#) <sup>139</sup>), or this can be done manually. Within Identity Access, select the **Setup** tab, then click **Doors** in the ribbon bar.



The Doors window above shows that there are no doors in the database. 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.**

## 8.1 Door Properties General

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

**Door Settings**

Name

**General**

**Door Type**  
Normal Door

**On master controller network**  
<No Controller>

**Controller which manages this door**  
Master Controller

**I/O Overview of the door controller**

INPUTS		I-NET	OUTPUTS	
0	<input type="checkbox"/>	1	0	Floor '1' on elevator 'test system'
1	<input type="checkbox"/>	2	1	
2	<input type="checkbox"/>	3	2	
3	<input type="checkbox"/>	4	3	
4	<input type="checkbox"/>	5	4	
5	<input type="checkbox"/>	6	5	
6	<input type="checkbox"/>	7	6	
7	<input type="checkbox"/>	8	7	
8	<input type="checkbox"/>		8	

☐ Override all lockdown levels  
☐ Override Lockdown Level 2  
☐ Enforce Anti Passback  
☐ Force door open if fire is detected  
☐ Dropbox  
☒ Active

Accept Cancel

Enter a **Name** (required) to identify the controller (e.g. Front Door)

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](#). 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](#)

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 APB 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.

When the door is configured, the **General** tab should look something like this:

The screenshot shows the 'Door Settings' window with the 'General' tab selected. The door is named 'Back Door'. The configuration includes:

- Door Type:** Normal Door
- On master controller network:** Ground Floor
- Controller which manages this door:** Master Controller
- I/O Overview of the door controller:**

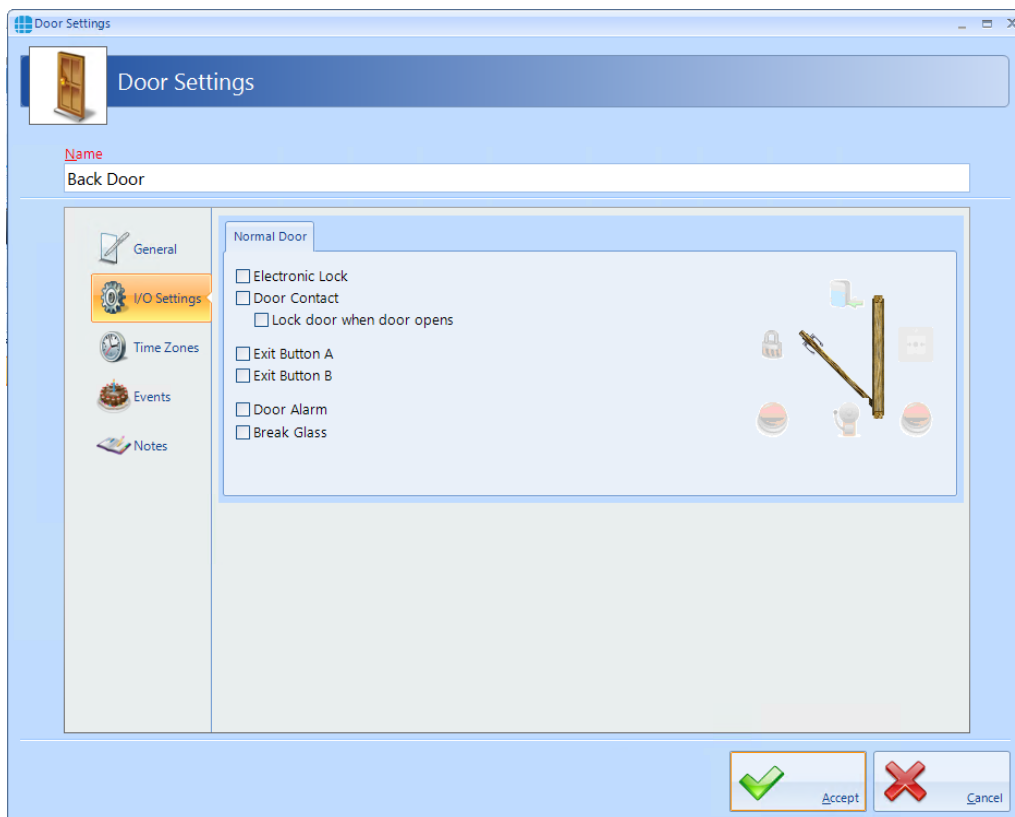
INPUTS		I-NET	OUTPUTS	
Exit button A on door 'This Door'	0	1	0	Electronic lock on door 'This Door'
Door sensor on door 'This Door'	1		1	Door alarm on door 'This Door'
Break glass on door 'This Door'	2		2	
PSU fault alarm on controller 'Ground Floor'	3		3	
Tamper alarm on controller 'Ground Floor'	4		4	
	5	RS485 Addr 0	5	
	6		6	
	7		7	
	8		8	
- Options:**
  - ☐ Override all lockdown levels
  - ☐ Override Lockdown Level 2
  - ☐ Enforce Anti Passback
  - ☐ Force door open if fire is detected
  - ☐ Dropbox
  - ☒ Active

At the bottom right, there are 'Accept' and 'Cancel' buttons.

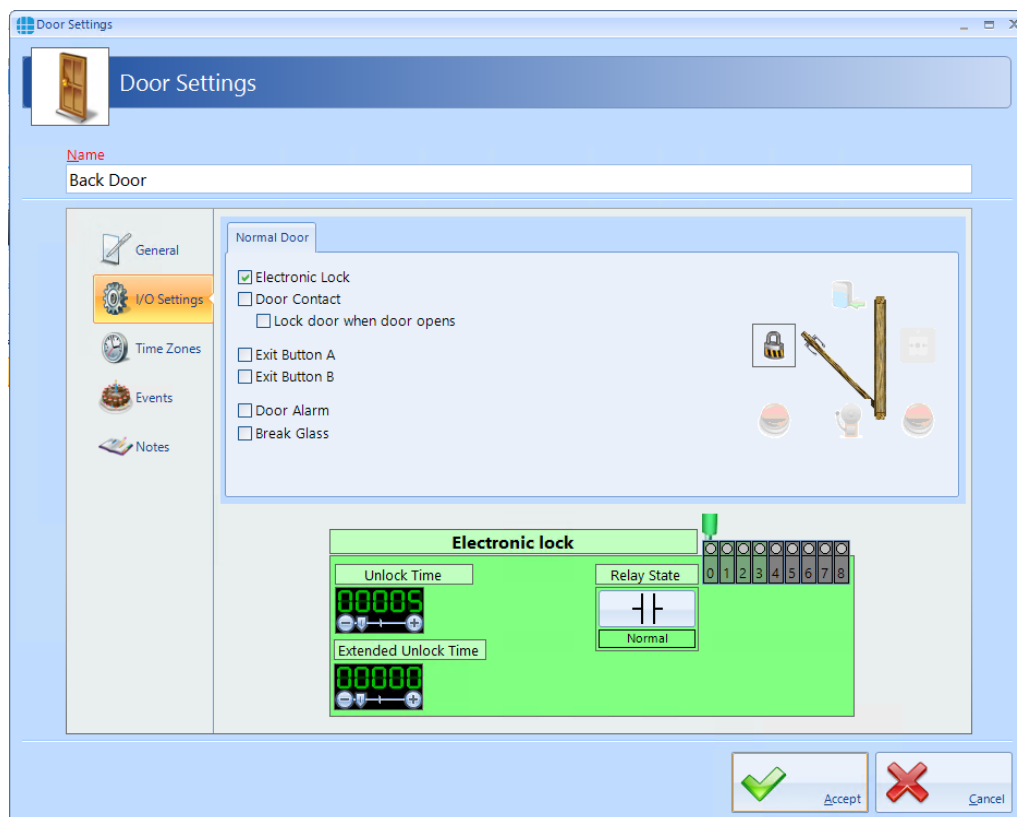
Press the **Accept** button when done.

## 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.

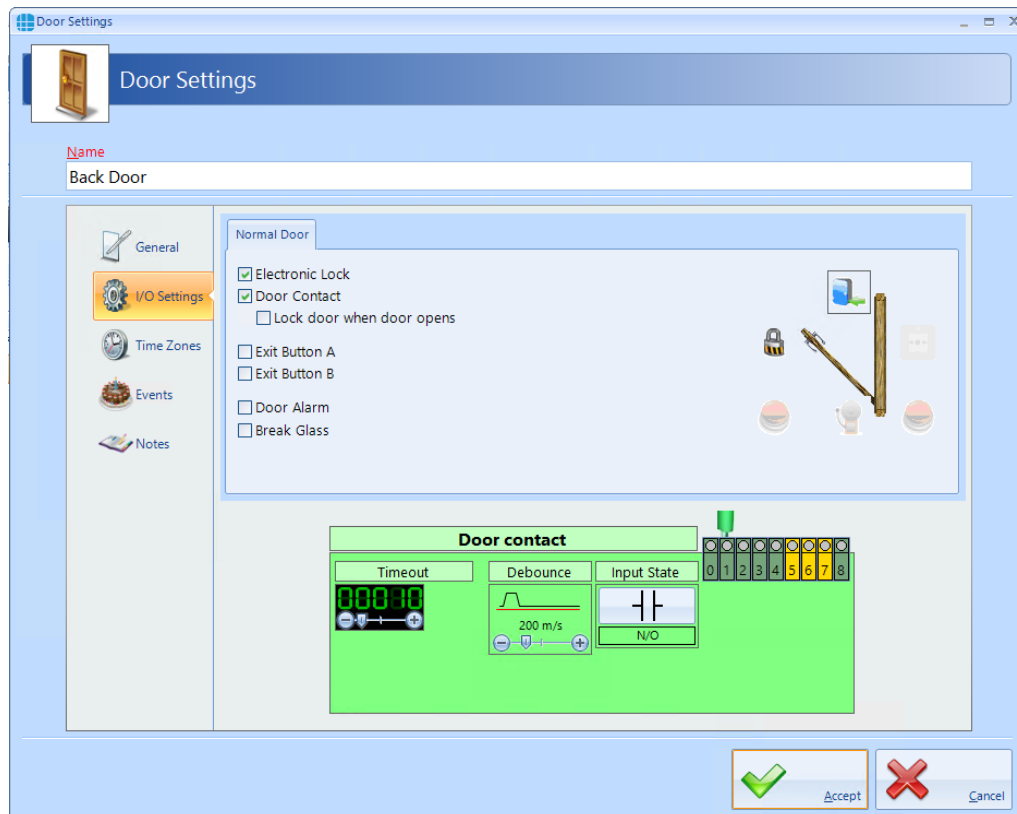
The **Extended Unlock Time** is the duration that the door will remain unlocked for users in a group selected as **Requires Extended Unlock Time**

If **Relay State** is **Normal**, the relay will energise to release the door. Conversely, **Inverted** will be normally energised and will de-energise the relay to release the door.

**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.

***NOTE: When used with iNet firmware version 98.34.21.9 or later, if the Unlock Time is set to 0 seconds, the door will "Latch". In this mode, the door will release when a valid token is presented and will relock when a valid token is next presented.***

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 (10 seconds in this instance).

**NOTE: On IA versions earlier than V8.0, the maximum Timeout value that could be selected was 60 seconds. With v8.0 and later, the maximum Timeout is 1800 seconds (60 minutes), but all controllers must be fitted with firmware version 98.37.020 or later for this Extended Timeout to work.**

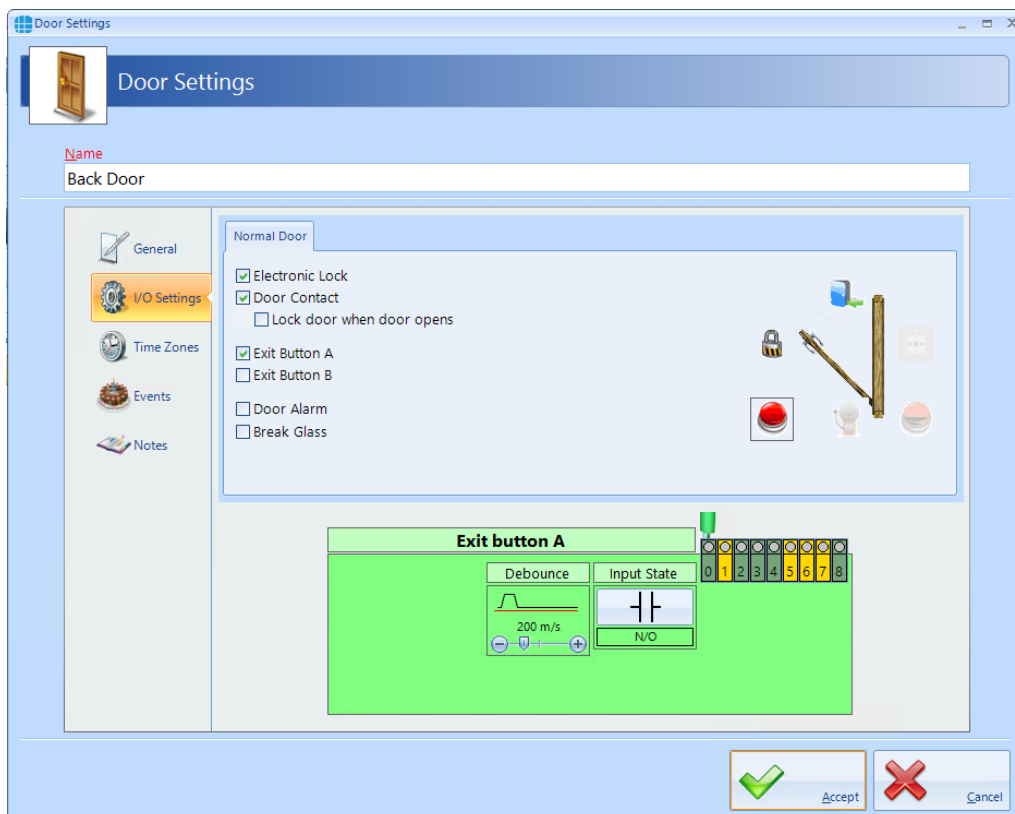
**Debounce** is a short delay between the door contact opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

**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.

**NOTE: 9 inputs are available on the configuration screen to accommodate the iNet PLUS.**

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



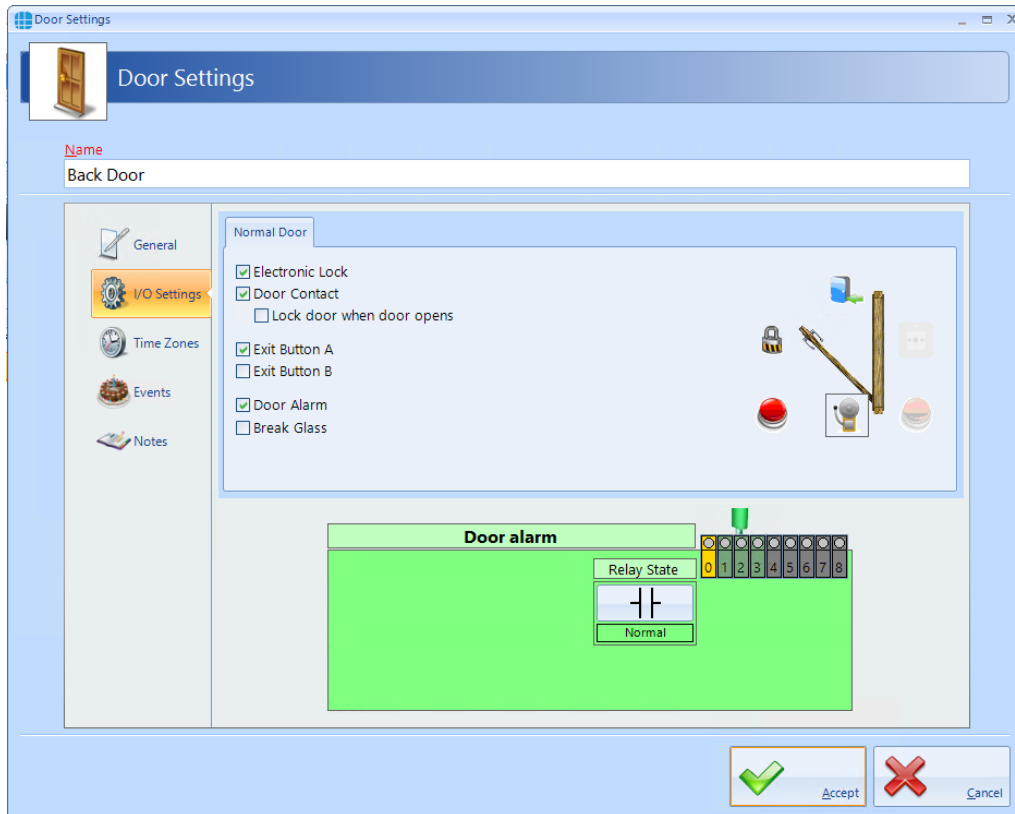
**Debounce** is a short delay between the door contact opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

**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.**

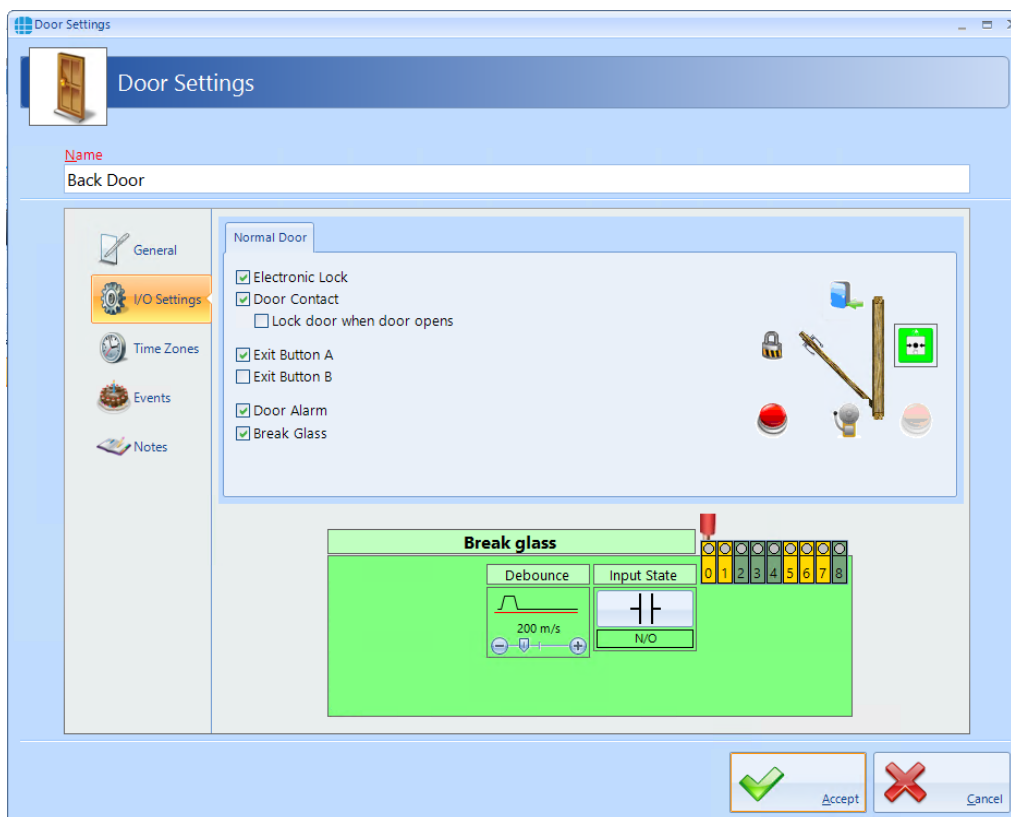
To configure a door alarm relay, tick the **Door Alarm** option, then click on the icon:



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.

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



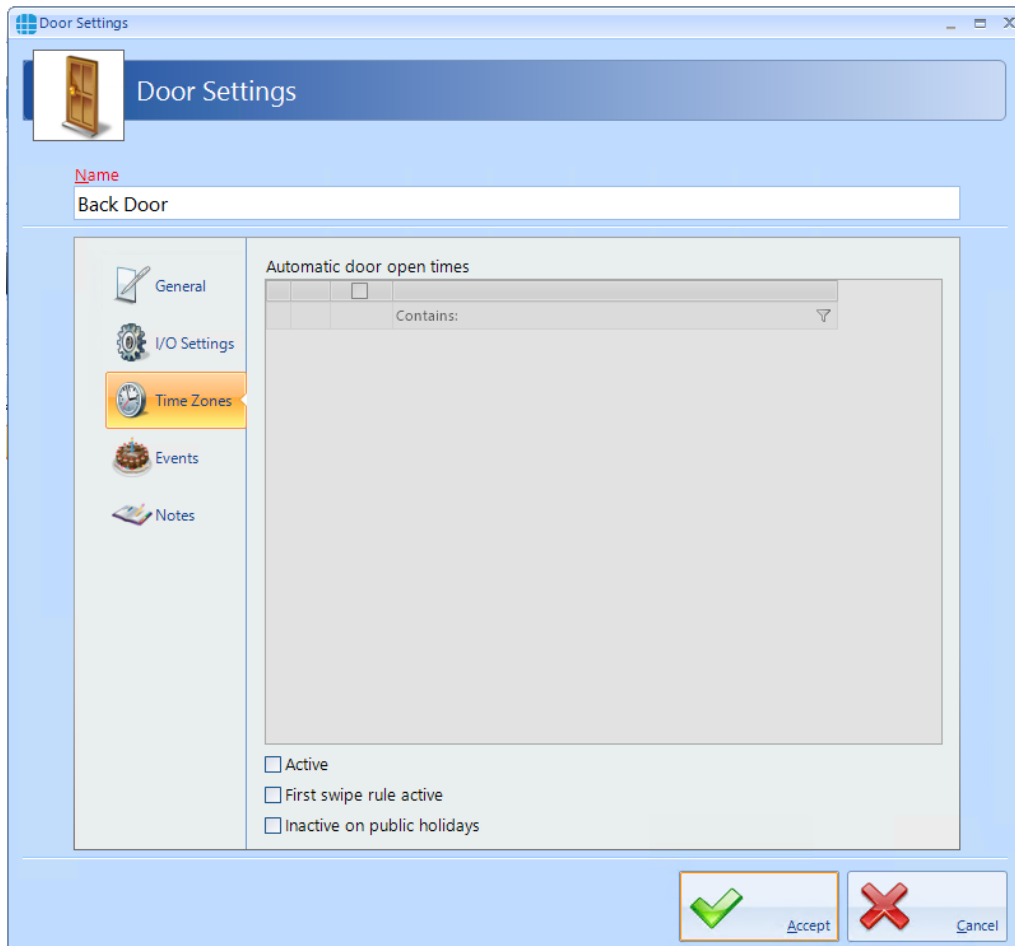
**Debounce** is a short delay between the contacts opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

**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 BreakGlass. In the example above, Input 0 is yellow as it has been allocated to another function, so the 'wire' connected to it is red showing that accepting this will cause a problem.

### 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.

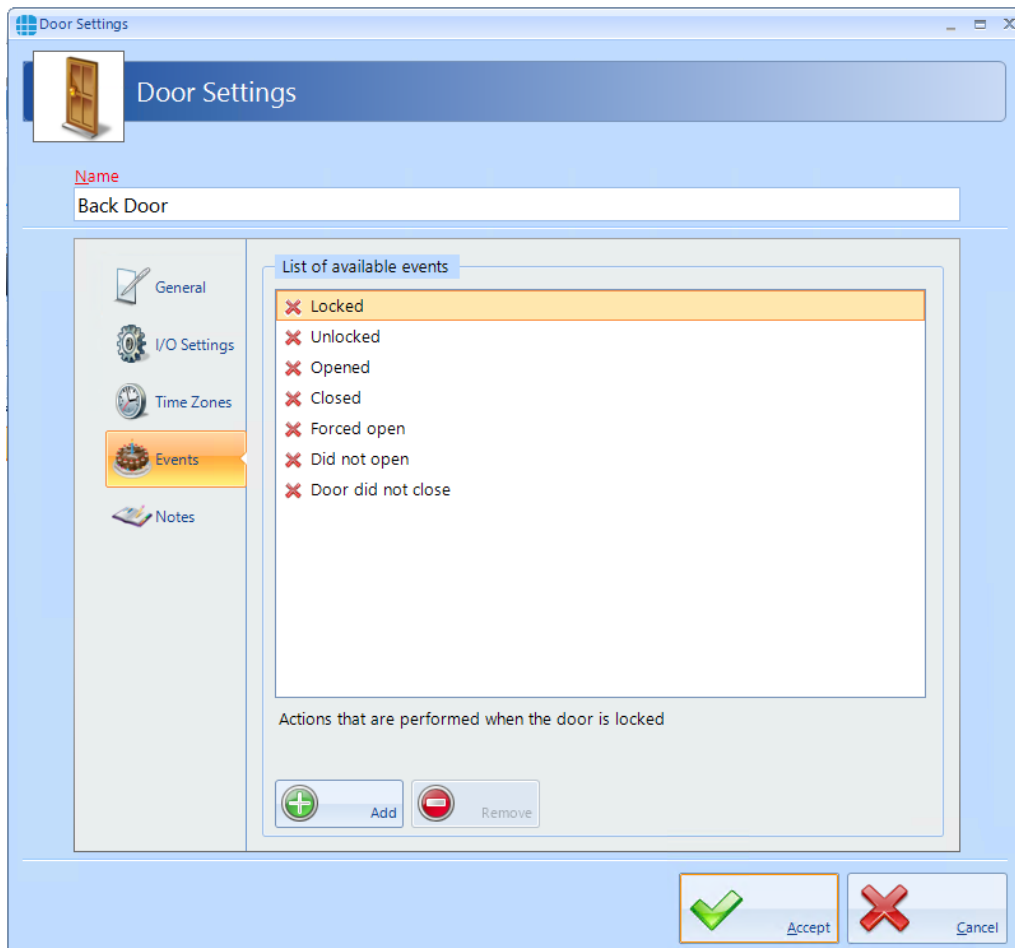
If selected, the **First swipe rule active** option will delay the door from releasing until a valid user opens the door after the start of the Time Zone.

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



## 8.4 Door Properties Events

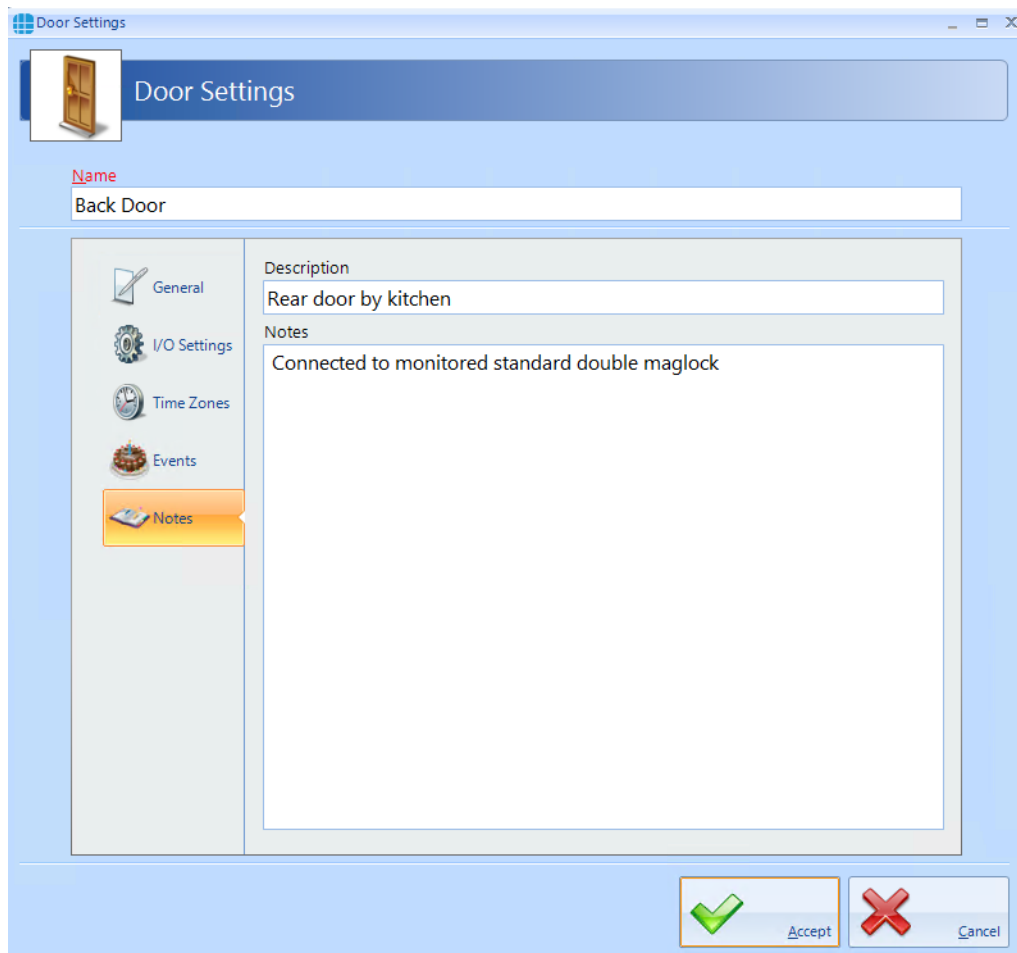
The Events tab will indicate whether any Events have been configured for the selected door.



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

## 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.

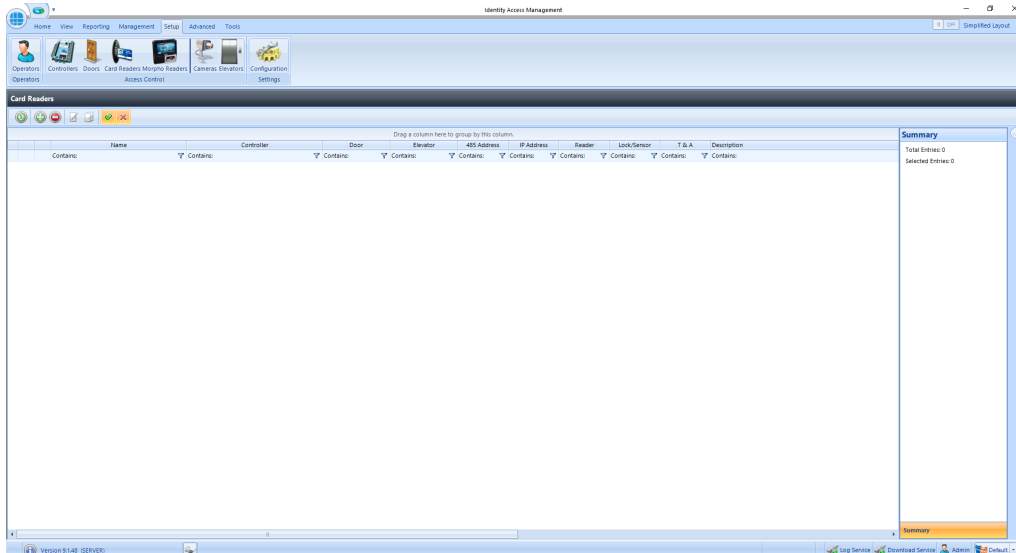


The screenshot shows the 'Door Settings' window. At the top, there is a header bar with a door icon and the title 'Door Settings'. Below the header, there is a 'Name' field containing 'Back Door'. On the left side, there is a sidebar with five icons: 'General' (pencil), 'I/O Settings' (gear), 'Time Zones' (clock), 'Events' (calendar), and 'Notes' (notepad). The 'Notes' icon is highlighted. The main area is divided into two sections: 'Description' and 'Notes'. The 'Description' field contains 'Rear door by kitchen'. The 'Notes' field contains 'Connected to monitored standard double maglock'. At the bottom right, there are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

# Configuring Card Readers

## 9 Configuring Card Readers

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



This Card Readers window shows that there are no readers in the database. 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.

## 9.1 Card Reader General

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

The screenshot shows the 'Card Reader Settings' window with the 'General' tab selected. The window has a title bar 'Card Reader Settings' and a sidebar with icons for 'General', 'Time Zones', 'Settings', 'Events', and 'Notes'. The main area contains the following fields and options:

- Name:** A text input field.
- On master controller network:** A dropdown menu set to '<No Controller>'. To its right is a 'Reader' section with a circular diagram and two numbered ports, '2' and '1'.
- Select slave network:** A dropdown menu set to 'RS485 network device'.
- Master Controller:** A dropdown menu set to 'Master Controller'.
- This reader controls:** Two dropdown menus, the first set to 'Door' and the second set to '<No Door>'. Below these are three radio button options:
  - ☐ This is a dropbox reader
    - ☐ Reader controls dropbox only
    - ☐ Reader controls dropbox and door
  - ☐ Ignore user time zones
  - ☐ Reader has a PIN pad attached
  - ☒ Allow shunting
  - ☐ Reader is used for Time and Attendance
- Location:** A dropdown menu set to 'Not applicable'.
- Active:** A checked checkbox.

At the bottom right are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

Enter a **Name** for the reader

**On master controller network** defines which Master Controller controls the reader

**Select Downstream 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 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.

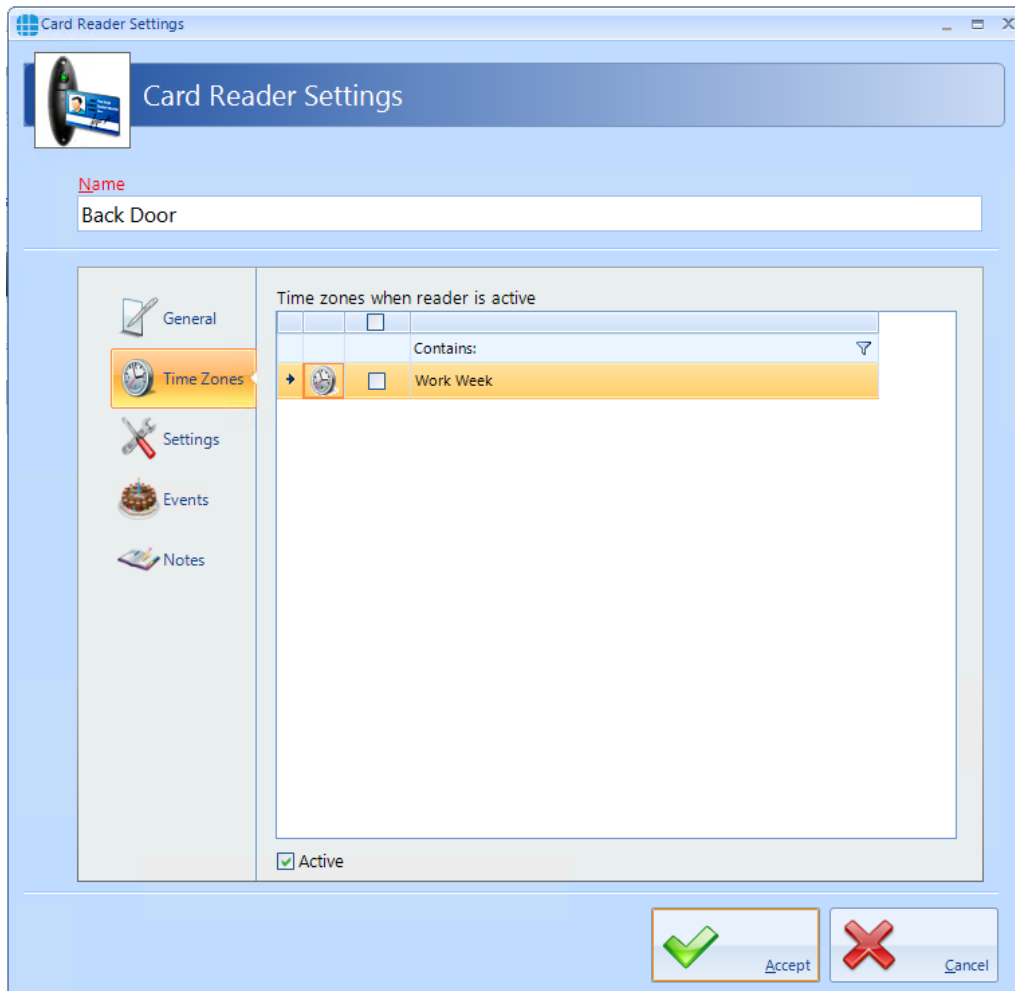
If the card reader is to be used for Time & Attendance, select the **Reader is used for Time and Attendance** option and select **Location** as "Inside to Outside" or "Outside to Inside" as appropriate.

**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.

## 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.

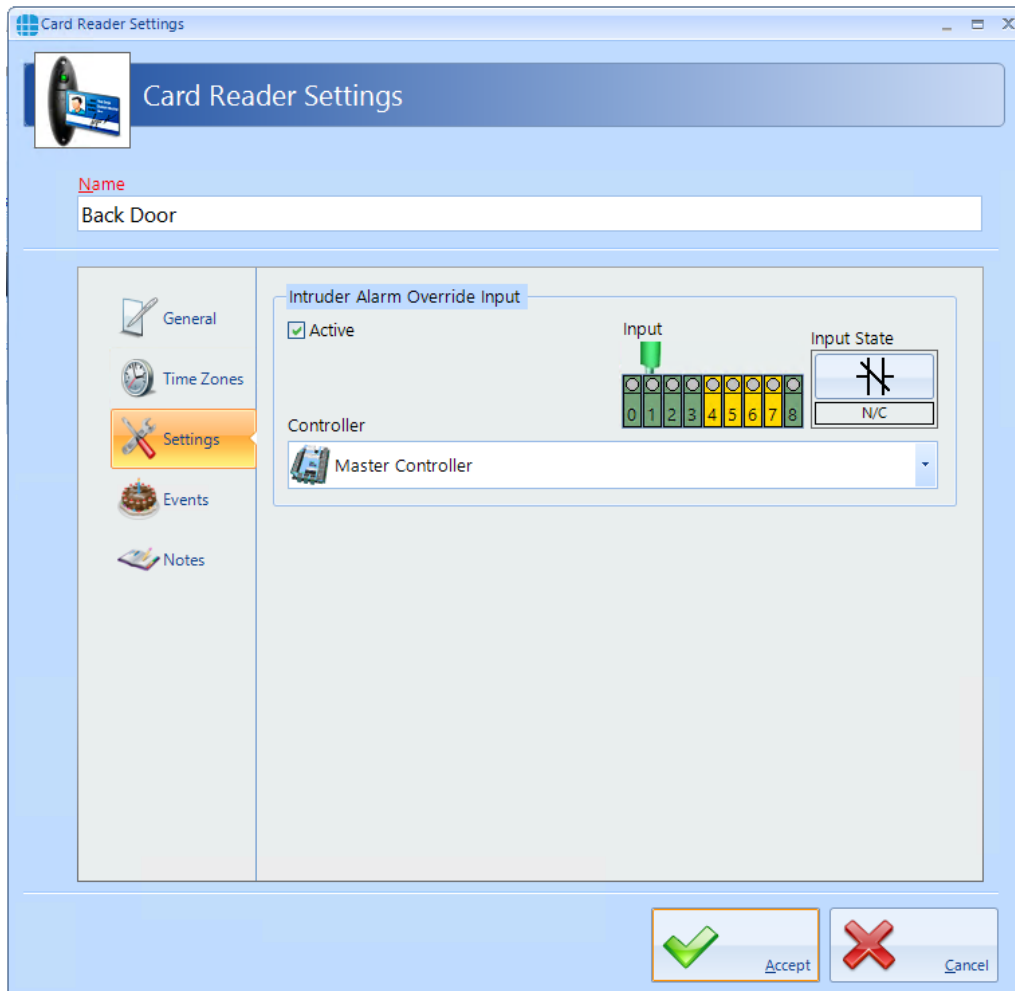


When one or more Time Zones exist, they will appear in the **Time zones when reader is active window**. Simply select the required Time Zone to allocate to the reader.

**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.**

### 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.

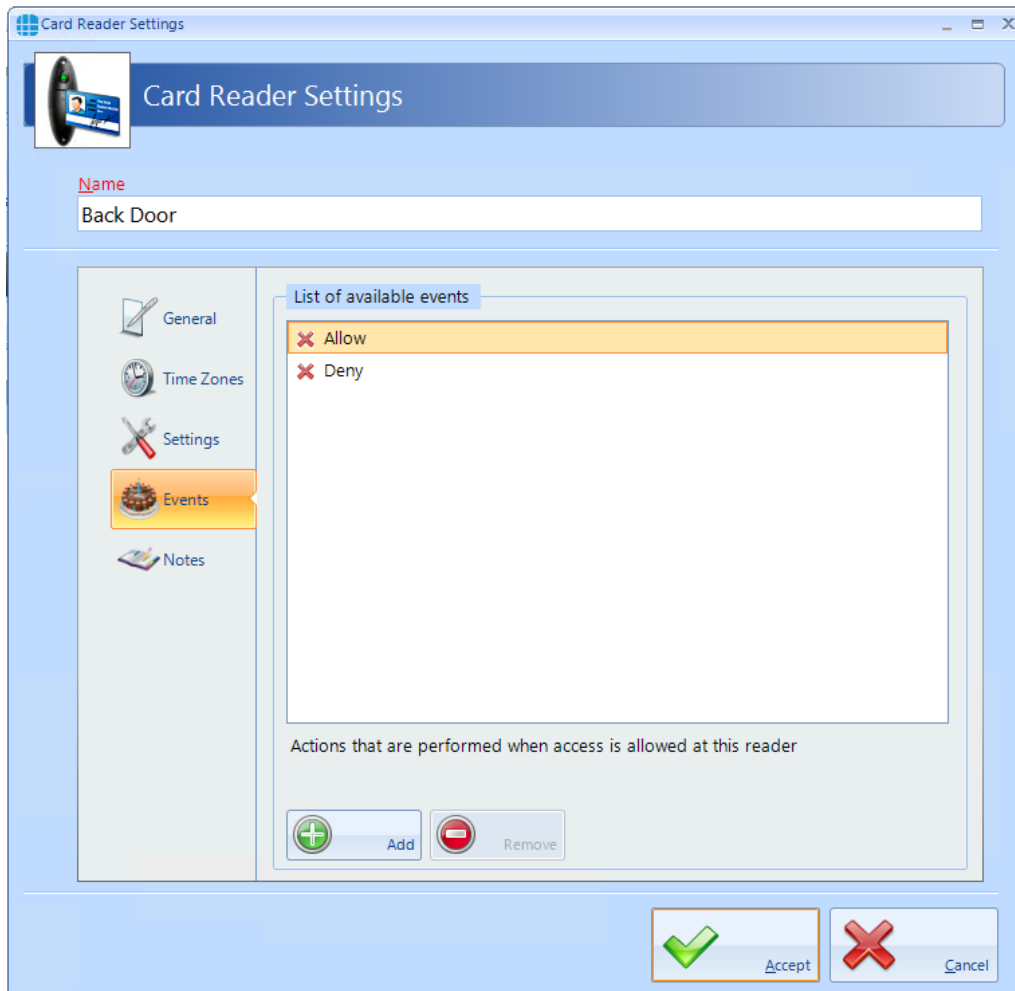
Select the **Input State** as **N/C** if the input is connected to a Normally Closed contact, or **N/O** if the input is connected to a Normally Open contact.

**Controller** defines which controller's input is used.



## 9.4 Card Reader Events

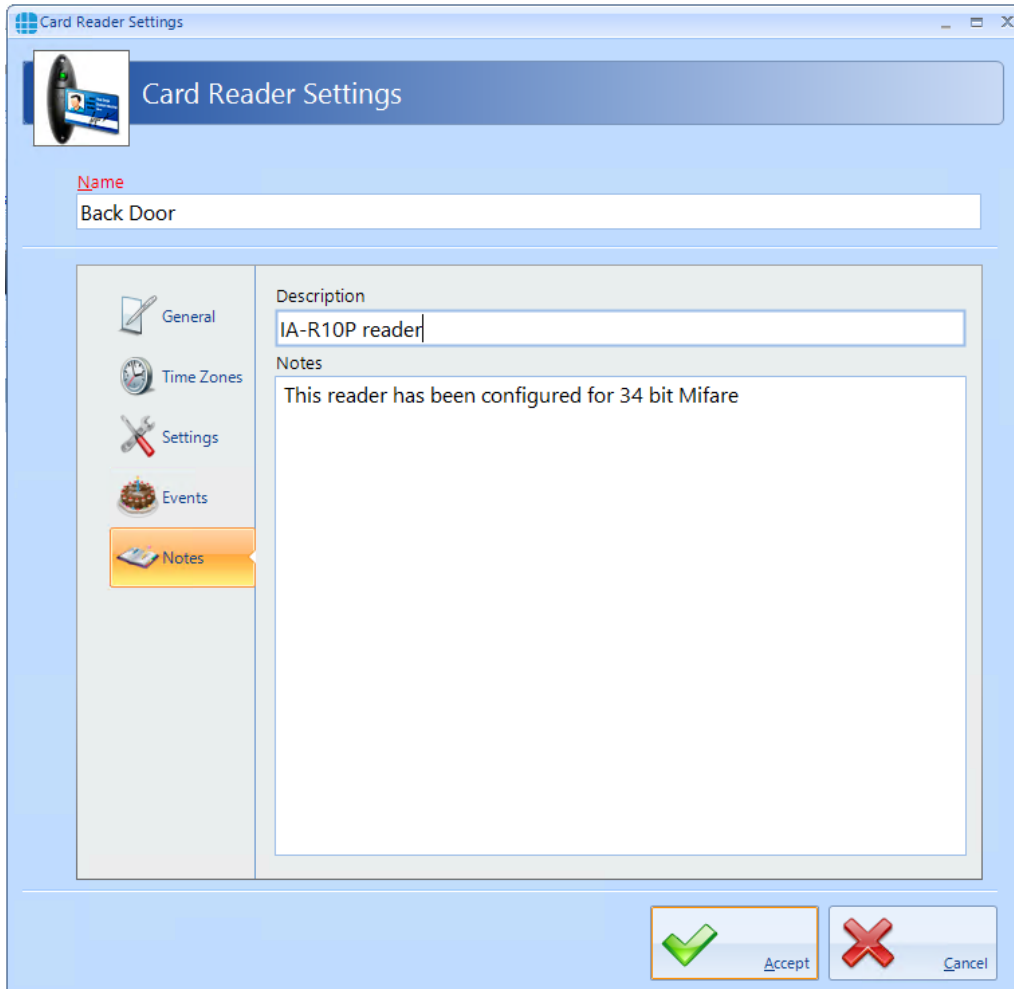
The Events tab will indicate whether any Events have been configured for the selected reader.



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

## 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.

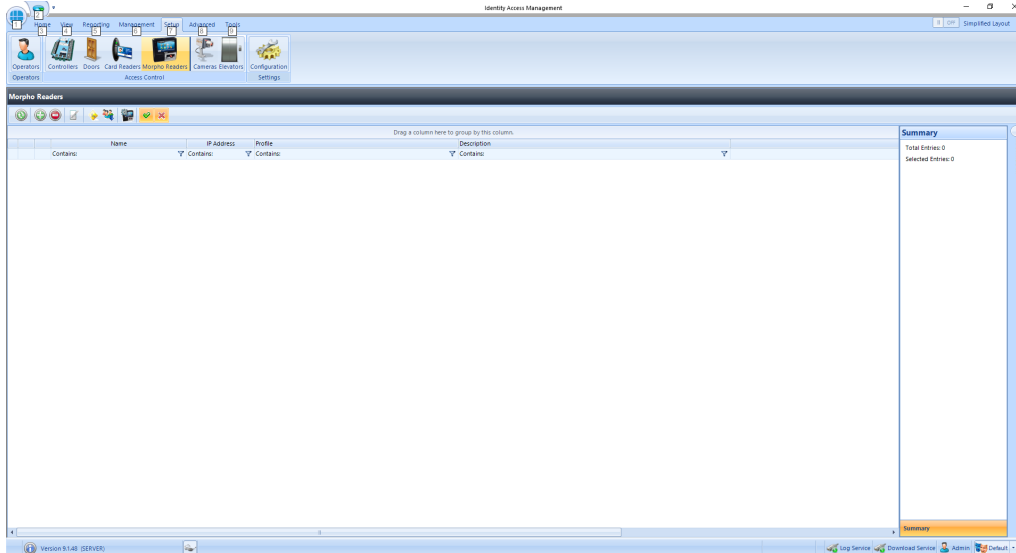


The screenshot shows the 'Card Reader Settings' window. The title bar reads 'Card Reader Settings'. Below the title bar is a header area with a card reader icon and the text 'Card Reader Settings'. The main area is divided into a left sidebar and a right content area. The sidebar contains five icons with labels: 'General' (notepad icon), 'Time Zones' (clock icon), 'Settings' (wrench icon), 'Events' (cake icon), and 'Notes' (notepad icon, which is highlighted in orange). The right content area has a 'Name' label above a text field containing 'Back Door'. Below this, there are two sections: 'Description' with a text field containing 'IA-R10P reader', and 'Notes' with a larger text area containing the text 'This reader has been configured for 34 bit Mifare'. At the bottom right of the window are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

# Configuring Morpho Fingerprint Readers

## 10 Configuring Morpho Fingerprint Readers

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



The Morpho Readers window shows that there are no readers in the database. 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.



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

To create a new Morpho reader, click on the **Add** button



## 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.

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

**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.

When used in ACU mode, the controller needs to know which Wiegand port the fingerprint reader is connected to. To achieve this, it is necessary to create a 'phantom' Card Reader which is linked to this fingerprint reader. Use the **Link to a Wiegand reader** section to define the location of the 'phantom' card reader. If a Standalone device 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, rather than using an MS-300 or MS)-1300 USB enrolment reader

**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.

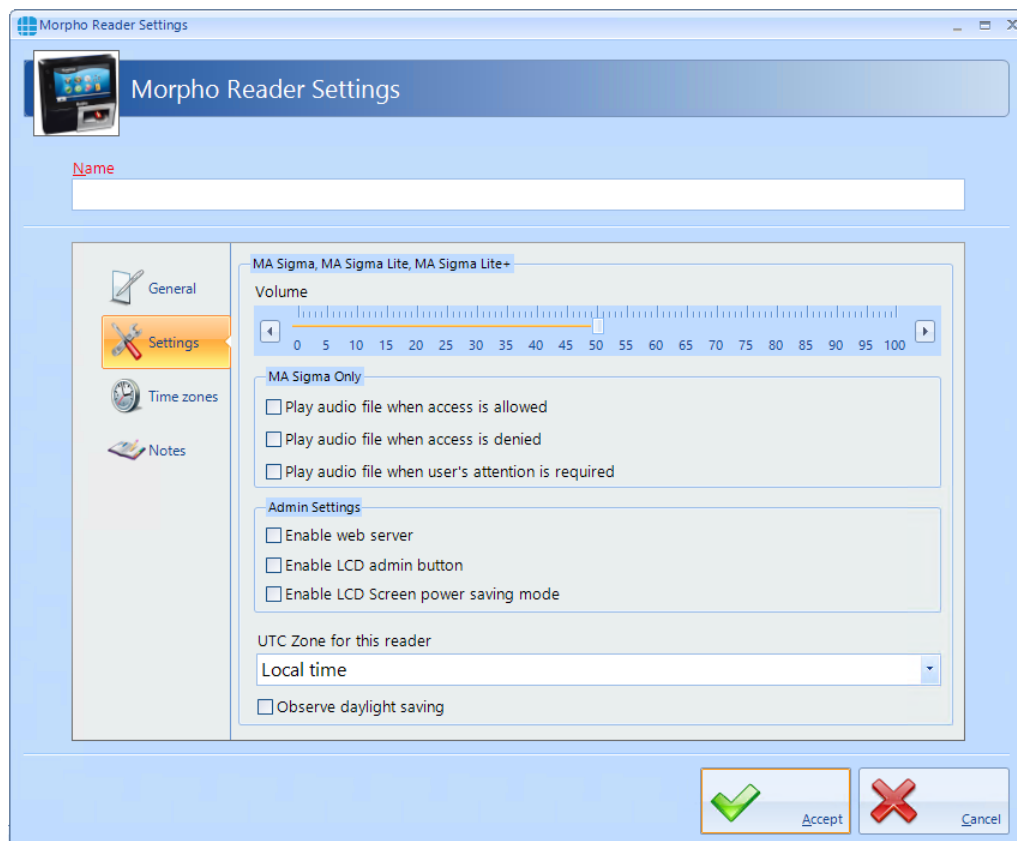
**Active** must be ticked if the hardware is fitted. If this is not ticked, data for the reader will not be transmitted to the controller.

**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.

## 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 selecting **Play audio file when access is allowed**, **Play audio file when access is denied** and **Play audio file when user's attention is required**.

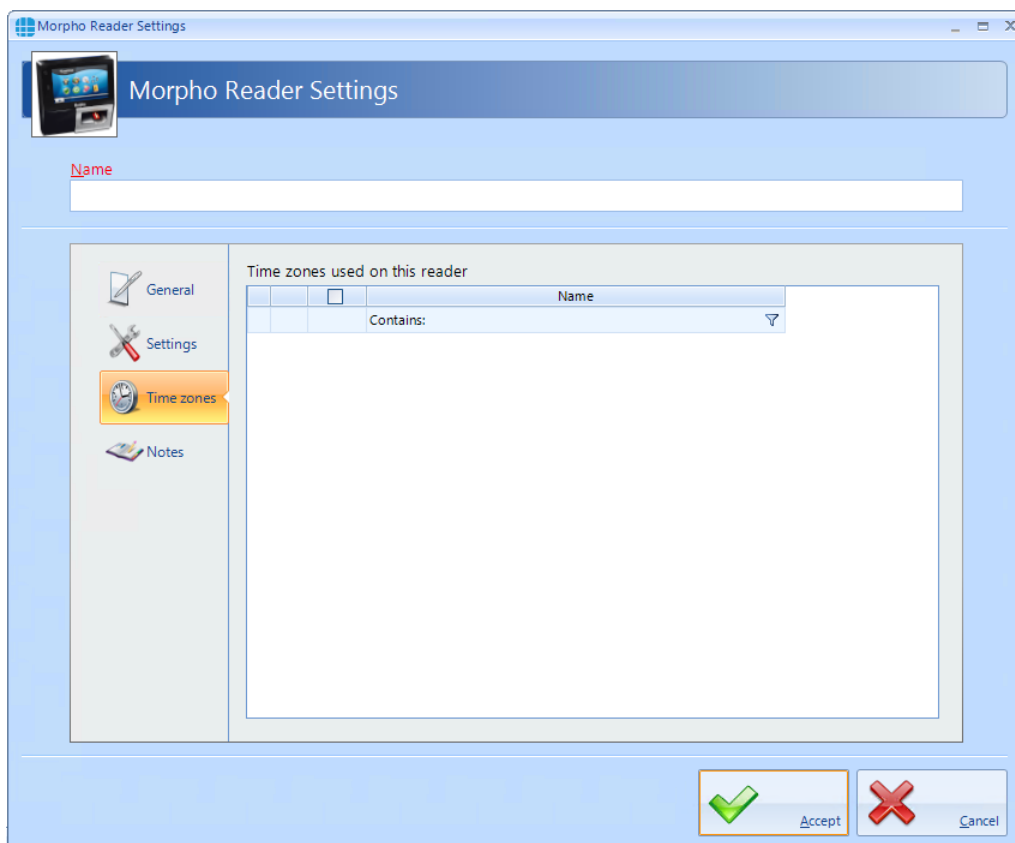
The **Admin Settings** enable the web server and admin screen as required

**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.

### 10.3 Morpho Reader Time Zones

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

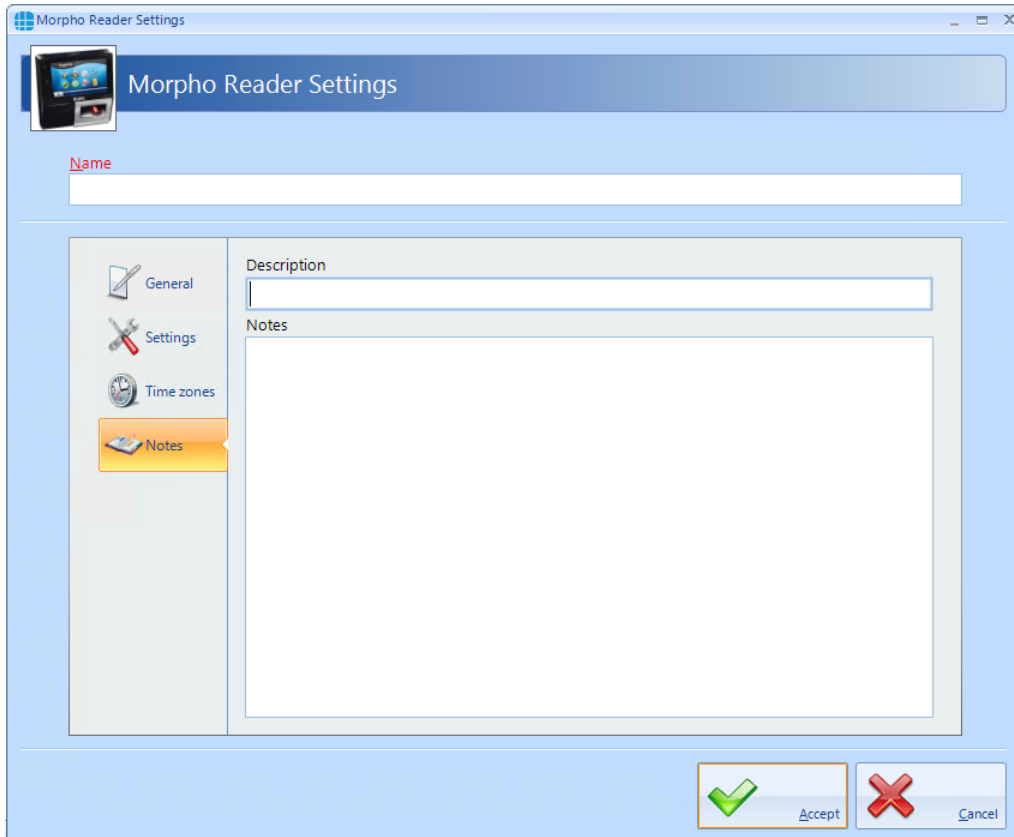


**NOTE: Controlsoft do not recommend allocating a Time Zone to a Morpho reader except in exceptional circumstances, as during the Time Zone, NOBODY would be able to access the door. It is preferable to allocate Time Zones to Users, whereby some users (e.g. Keyholders for the Intruder Alarm system) can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



## 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.



The screenshot shows the 'Morpho Reader Settings' window. The 'Notes' section is selected in the left sidebar. The main area contains a 'Name' field at the top, followed by a 'Description' text field and a larger 'Notes' text area. At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

Morpho Reader Settings

Name

General

Settings

Time zones

Notes

Description

Notes

Accept

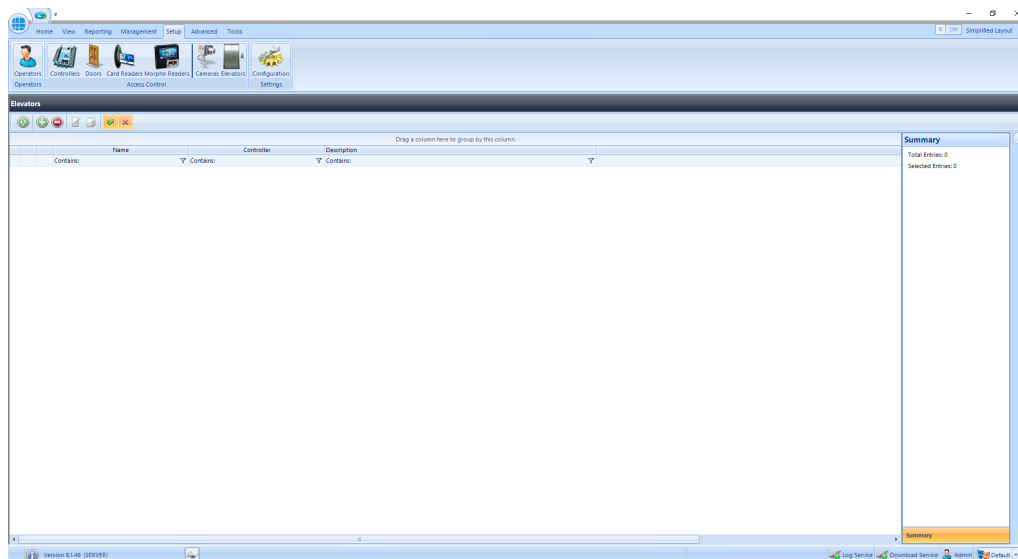
Cancel

# Configuring Elevators

## 11 Configuring 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.

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



This image shows that no elevators have yet been created.

Before creating the elevator, first create a Master controller as described previously (see [Configuring Master Controllers](#)<sup>131</sup>).

Click on the green plus symbol to add a new elevator, give it a name, link it to the required controller and ensure that the "Active" box is ticked.

The screenshot shows the 'Elevator Settings' application window. At the top, there's a header bar with the title 'Elevator Settings' and a small elevator icon. Below the header, there's a section for 'Name' with a text input field containing 'Service Elevator'. To the left of the main configuration area is a sidebar with icons for 'General' (selected), 'Settings', 'Floors' (with a '2' in a circle), 'Time Zones', and 'Notes'. The main area has a dropdown menu labeled 'On master controller network' with 'Ground Floor controller' selected. At the bottom of the main area, there's a checkbox labeled 'Active' which is checked. At the bottom right of the window, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

On the Settings tab:

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

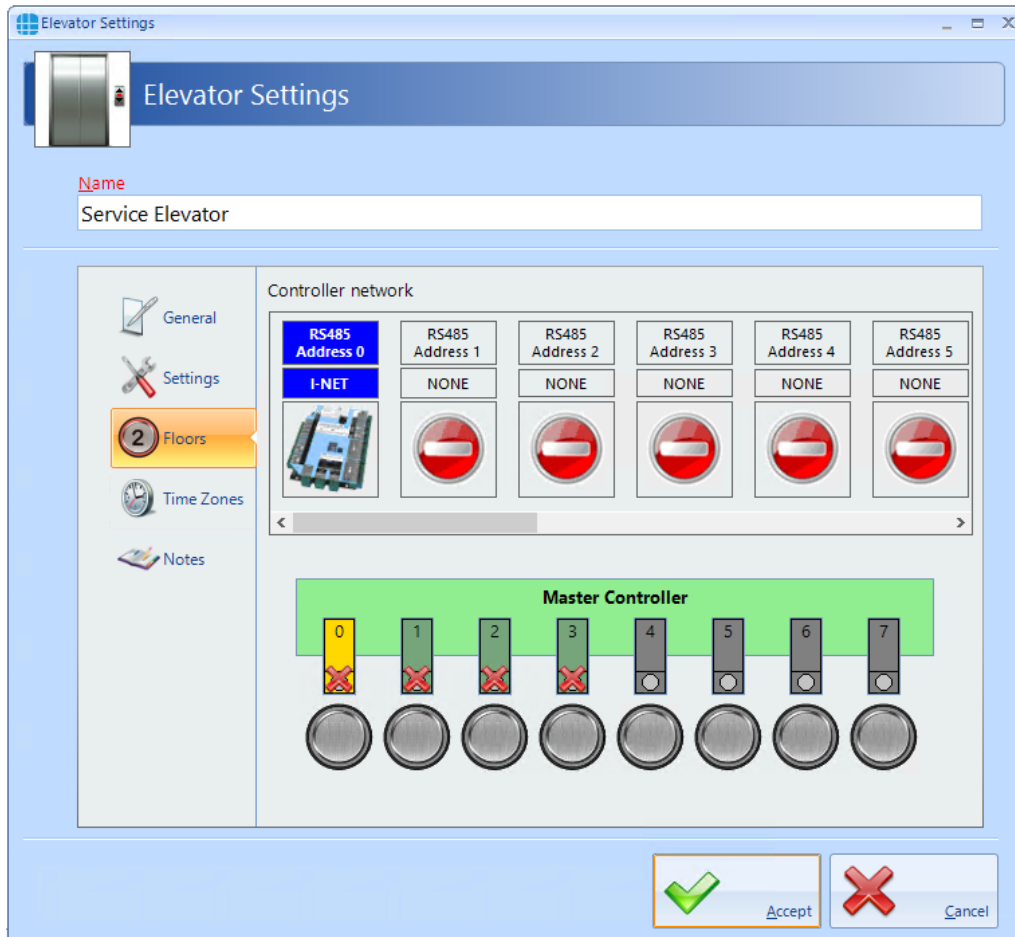
**Enable free access on mains fail alarm** will allow access to all floors when the system detects a Mains Fail.

**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**

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

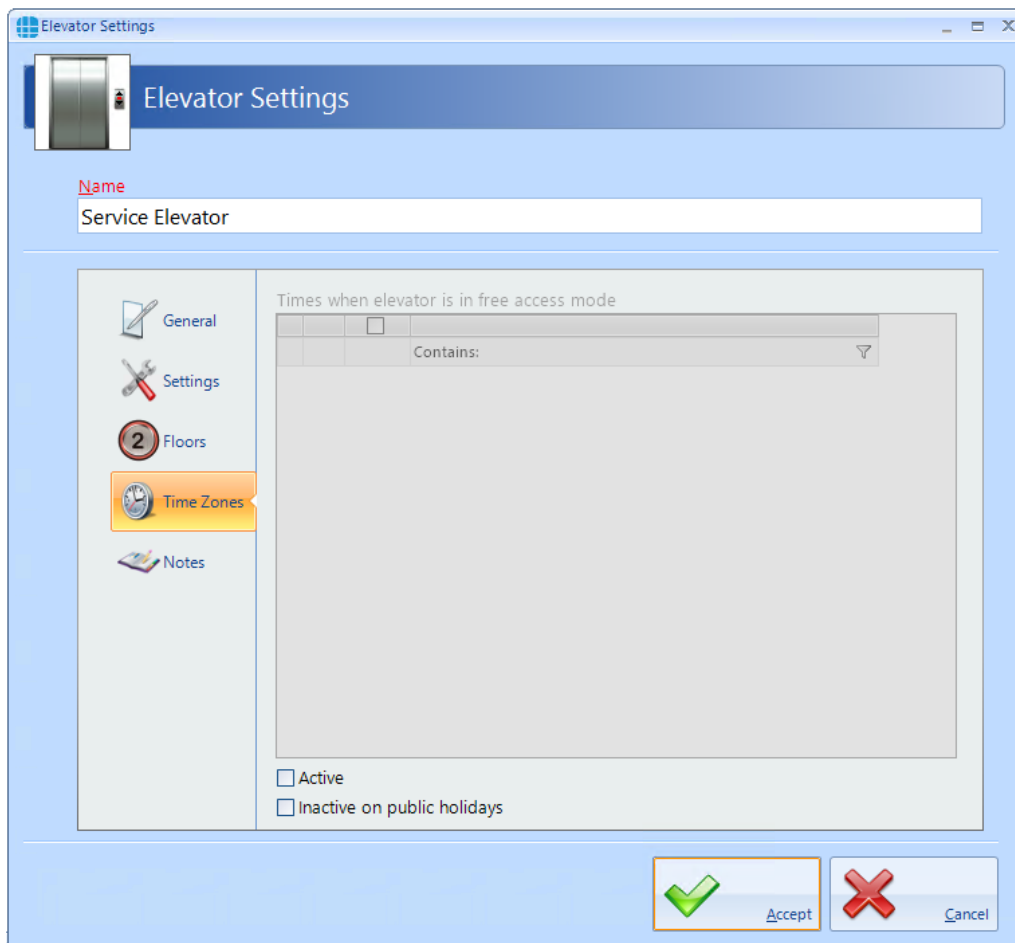
**Elevator button labels** allows text to be entered to make the next stage in the programming easier (e.g. change '1' to Gnd')

On the Floors tab:



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

On the **Time Zones** tab:



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

**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

**NOTE: It is possible to add Doors to an Elevator controller. This allows, for example, a reader to be used as a call button on the Ground Floor.**

# Configuring DropBox



## 12 Configuring 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.

# Configure Time Zones

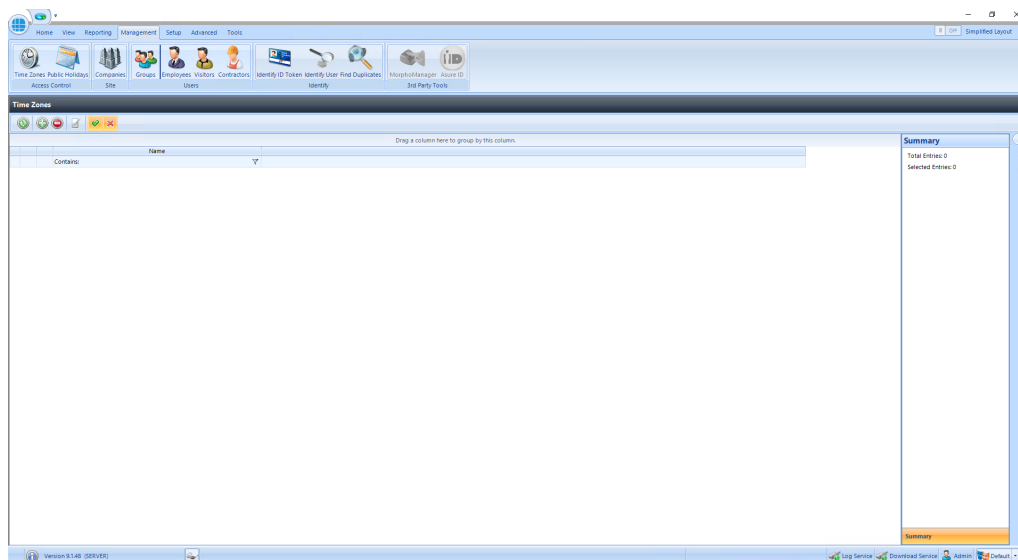
## 13 Configure Time Zones

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

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

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

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



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



Refresh: Updates the list of Time Zones



Add: Creates a new Time Zone in the list



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



Edit: edits the selected Time Zone



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



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

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



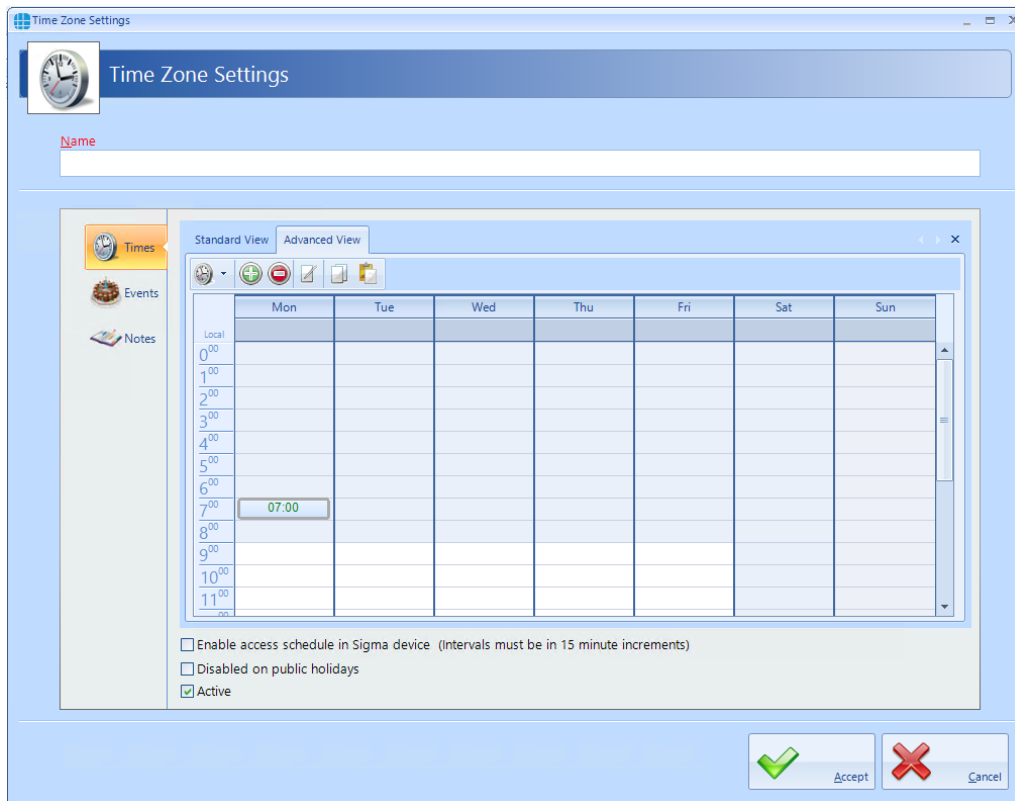
## 13.1 Creating Time Zones

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

Enter a **Name** for the Time Zone

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

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



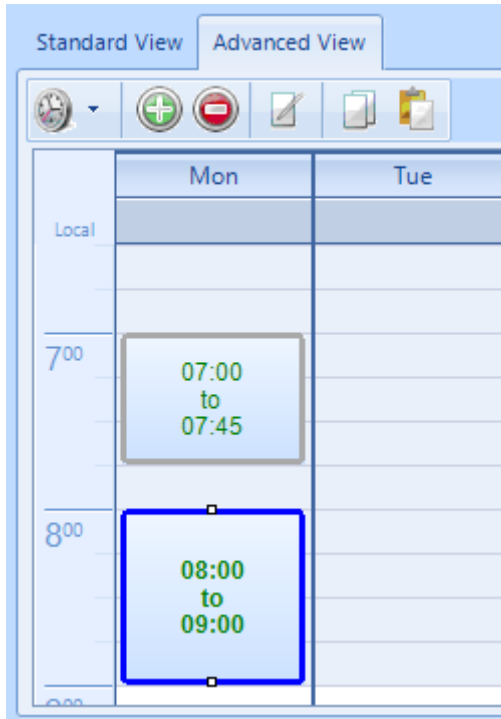
The following buttons are available in Advanced View:



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



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

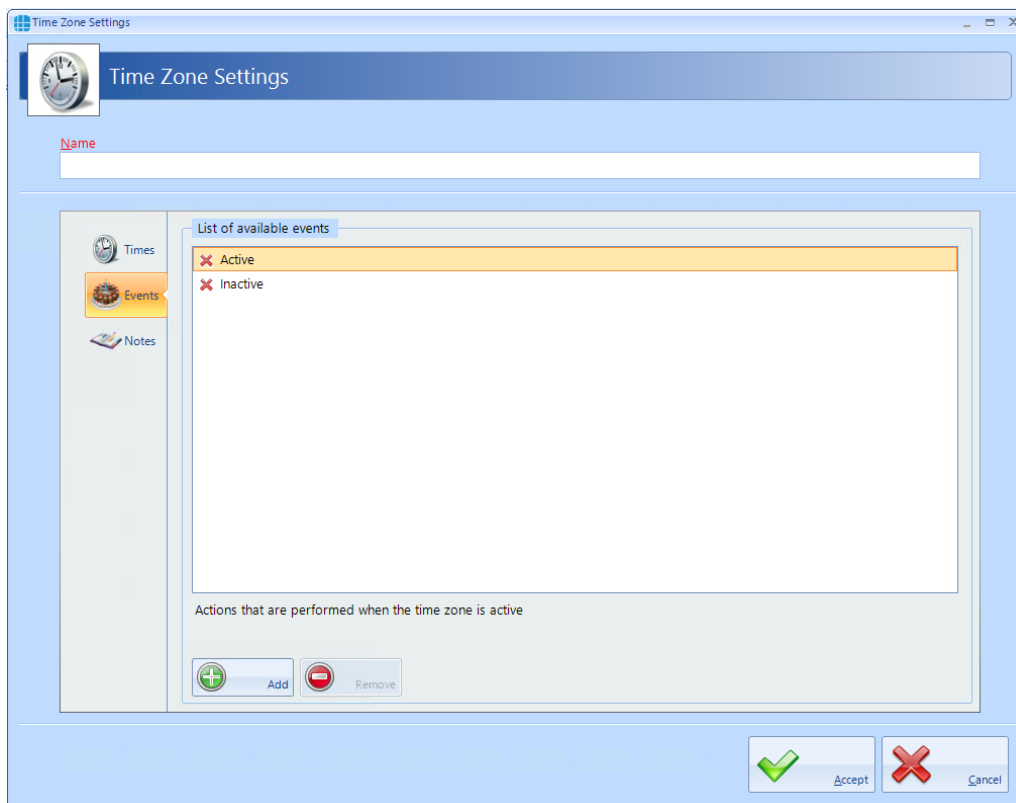


Pastes the selected time entity

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

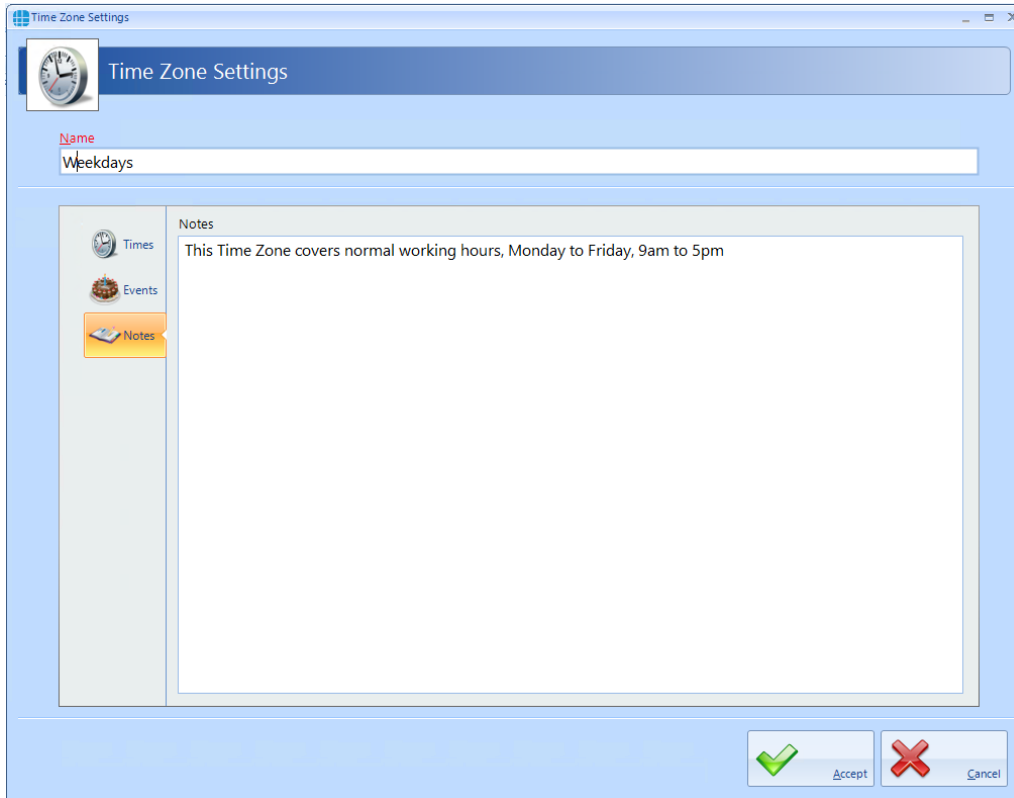
Ensure that **Active** is ticked otherwise it will not be possible to use the Time Zone.

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



In this example, no Events have been created for the selected time zone. 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.

The **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.



The screenshot shows a web-based interface for configuring time zones. The main window is titled 'Time Zone Settings'. On the left is a sidebar with three icons: a clock for 'Times', a calendar for 'Events', and a notepad for 'Notes'. The 'Notes' section is currently selected and expanded, displaying a large text area. Inside this text area, the text 'This Time Zone covers normal working hours, Monday to Friday, 9am to 5pm' is entered. Above the text area, there is a label 'Name' and a text input field containing the word 'Weekdays'. At the bottom right of the window, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

***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.



## 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:

The screenshot shows the 'Time Zone Settings' window. The 'Name' field is set to 'Weekdays'. The 'Standard View' tab is active, displaying a schedule table with two columns for 'Start Time 1' and 'End Time 1', and two columns for 'Start Time 2' and 'End Time 2'. The schedule is defined for Monday through Sunday. Monday has a checkmark in the first column, with a start time of 07:00 and an end time of 00:45. All other days have empty checkboxes and 00:00 times. Below the table, the 'Enable access schedule in Sigma device' checkbox is checked, along with 'Active'. The 'Accept' and 'Cancel' buttons are at the bottom right.

	Start Time 1	End Time 1	Start Time 2	End Time 2
Monday	<input checked="" type="checkbox"/> 07:00	00:45	<input type="checkbox"/> 00:00	00:00
Tuesday	<input type="checkbox"/> 00:00	00:00	<input type="checkbox"/> 00:00	00:00
Wednesday	<input type="checkbox"/> 00:00	00:00	<input type="checkbox"/> 00:00	00:00
Thursday	<input type="checkbox"/> 00:00	00:00	<input type="checkbox"/> 00:00	00:00
Friday	<input type="checkbox"/> 00:00	00:00	<input type="checkbox"/> 00:00	00:00
Saturday	<input type="checkbox"/> 00:00	00:00	<input type="checkbox"/> 00:00	00:00
Sunday	<input type="checkbox"/> 00:00	00:00	<input type="checkbox"/> 00:00	00:00

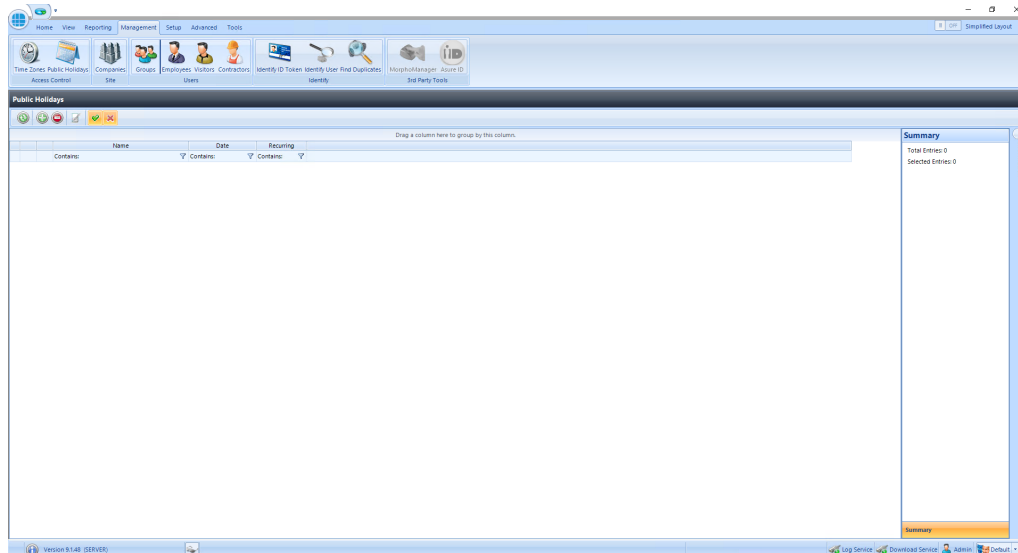
☒ Enable access schedule in Sigma device (Intervals must be in 15 minute increments)  
☐ Disabled on public holidays  
☒ Active

Accept Cancel

# Public Holidays

## 14 Public Holidays

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



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



Refresh: Updates the list of Public Holidays



Add: Creates a new Public Holiday in the list



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



Edit: edits the selected Public Holiday



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



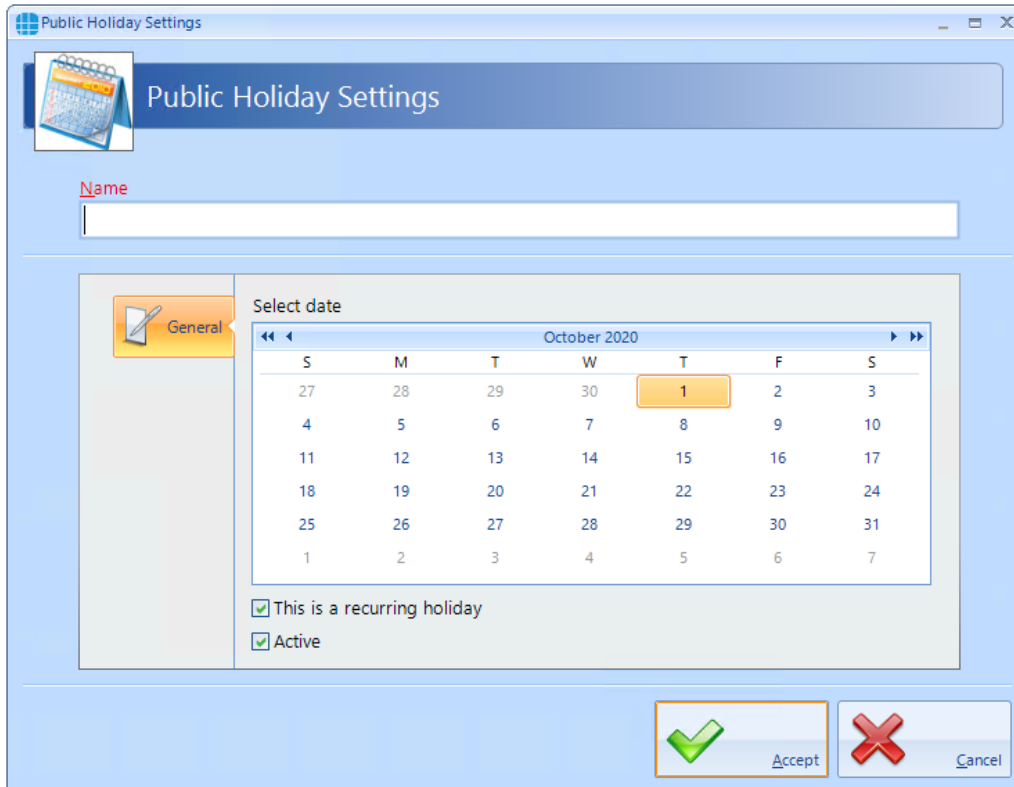
Show/Hide Inactive: This button will show or hide Operators who are not Active.

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



## 14.1 Creating Public Holidays

To configure a Public Holiday:



The image shows a 'Public Holiday Settings' dialog box. It has a title bar with the text 'Public Holiday Settings'. Below the title bar is a header area with a calendar icon and the text 'Public Holiday Settings'. Underneath is a text field labeled 'Name'. Below the 'Name' field is a 'Select date' section. This section contains a 'General' tab icon and a calendar for 'October 2020'. The calendar shows days of the week (S, M, T, W, T, F, S) and dates. The date '1' is highlighted. Below the calendar are two checkboxes: 'This is a recurring holiday' and 'Active', both of which are checked. At the bottom right of the dialog are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

Public Holiday Settings

Name

General

Select date

October 2020

S	M	T	W	T	F	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

☒ This is a recurring holiday

☒ Active

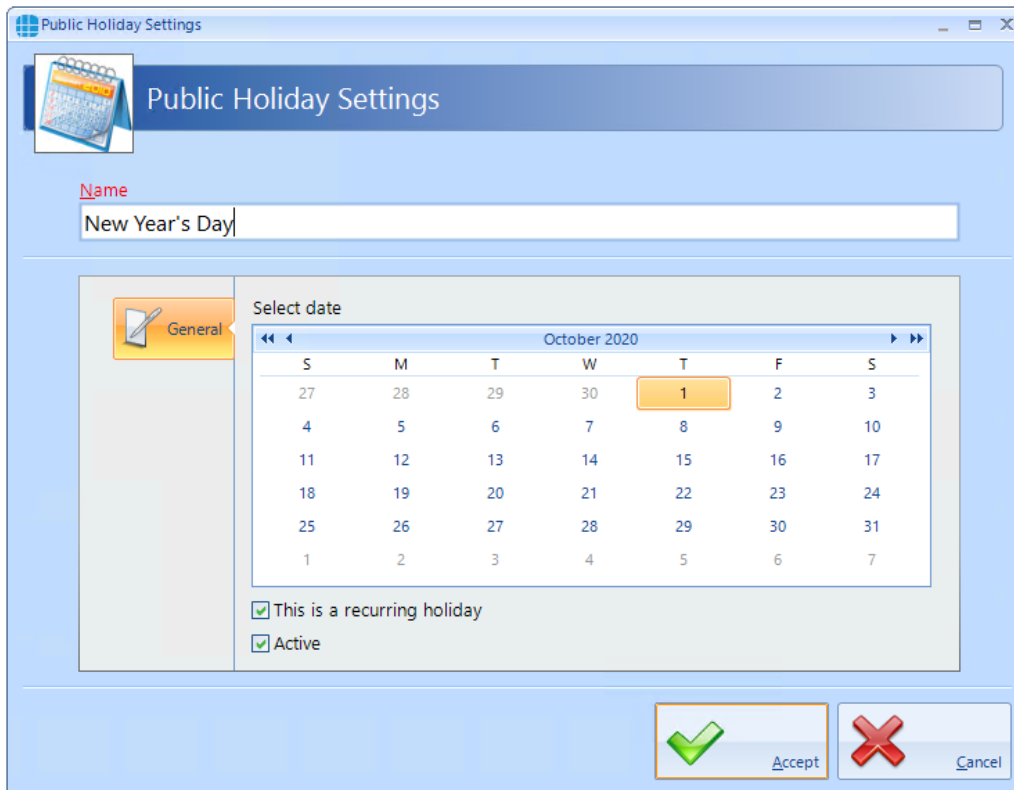
Accept Cancel

Enter a **Name** for the Public Holiday

**Select date** of the Public Holiday from the calendar

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

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



The image shows a 'Public Holiday Settings' dialog box. At the top, there's a title bar with the text 'Public Holiday Settings'. Below the title bar, there's a section with a calendar icon and the text 'Public Holiday Settings'. Underneath, there's a 'Name' label and a text input field containing 'New Year's Day'. Below the text input field, there's a 'General' tab selected, showing a 'Select date' calendar for October 2020. The calendar has a table of dates with the 1st highlighted. Below the calendar, there are two checkboxes: 'This is a recurring holiday' and 'Active', both of which are checked. At the bottom right, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

Public Holiday Settings

Name  
New Year's Day

General

Select date

October 2020

S	M	T	W	T	F	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

☒ This is a recurring holiday  
☒ Active

Accept Cancel

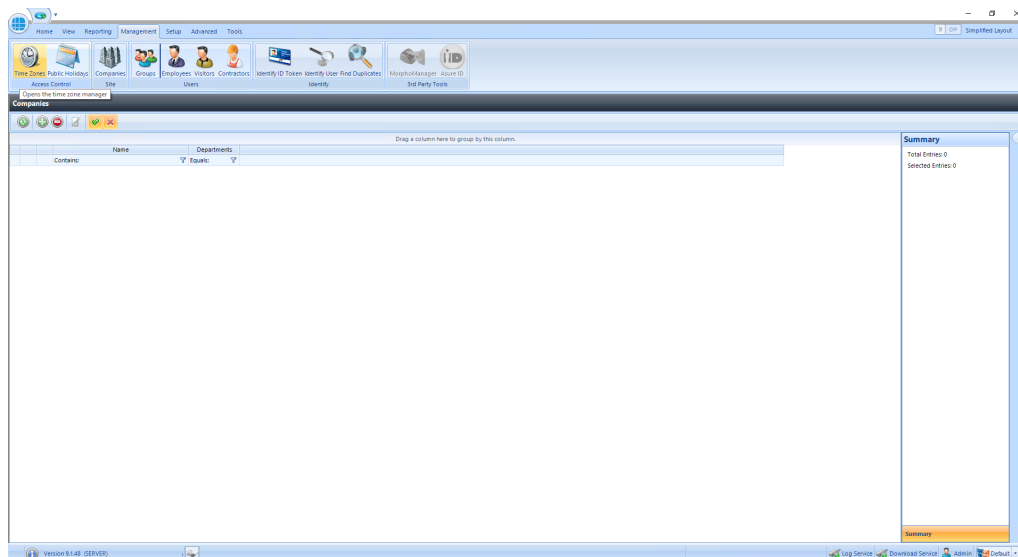
Click **Accept** when done.

# Companies and Departments

## 15 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 **Management** 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.

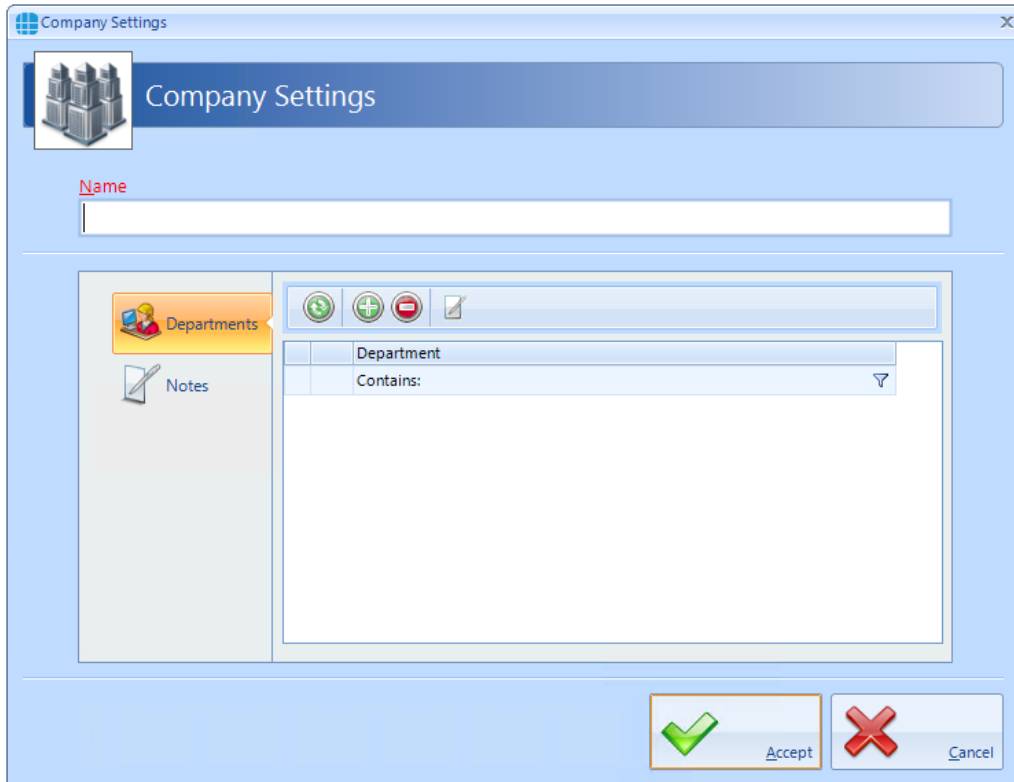


Show/Hide Inactive: This button will show or hide Companies / Departments not selected as Active.

**NOTE: When allocating a User to a Company / Department, simply choose the relevant option from the pull-down lists** (see [User General](#)) <sup>222</sup>

## 15.1 Creating Companies and Departments

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



The 'Company Settings' dialog box features a title bar with the text 'Company Settings' and a close button. Below the title bar is a 'Name' label and an empty text input field. The main area is divided into two panes: 'Departments' (highlighted with an orange tab) and 'Notes'. The 'Departments' pane contains a toolbar with four icons: a circular arrow (Refresh), a green plus sign (Add), a red minus sign (Delete), and a pencil (Edit). Below the toolbar is a table with a single header 'Department' and one row labeled 'Contains:'. The 'Notes' pane is currently empty. At the bottom right of the dialog are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).



Refresh: Updates the list of Departments



Add: Creates a new Department in the list




Delete: Removes the selected Department/s from the list

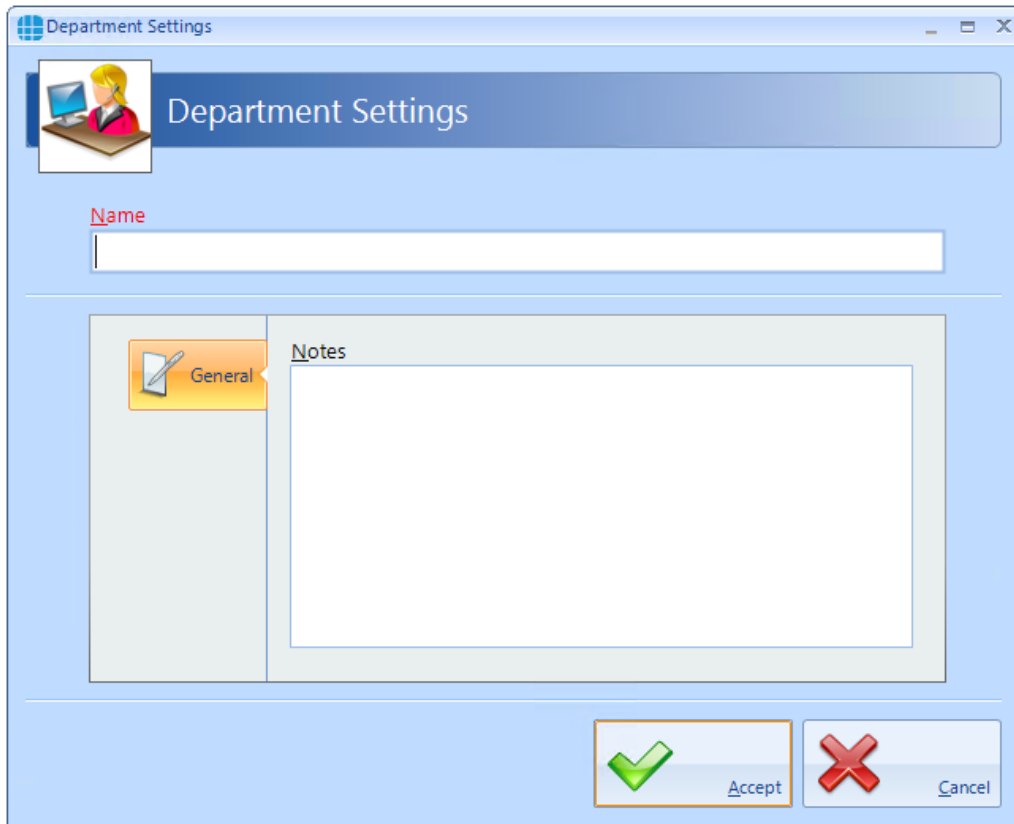


Edit: Edits the selected Department

**Name:** Add a name for the new Company



Click the Add button  to create a Department for the Company



The screenshot shows a 'Department Settings' dialog box. It features a title bar with the text 'Department Settings' and standard window controls. Below the title bar is a header area containing a user icon and the text 'Department Settings'. The main content area is divided into two sections: a 'Name' section with a text input field, and a 'Notes' section. The 'Notes' section has a 'General' tab and a large text area for entering notes. At the bottom of the dialog are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

**Name:** Add a name for the new Department

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

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

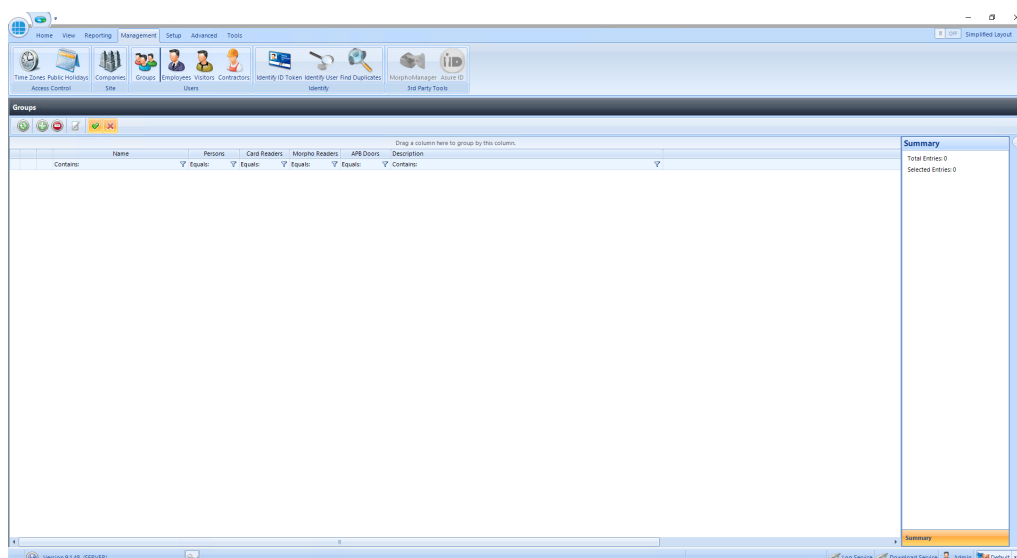
# Configuring Groups

## 16 Configuring Groups

Groups are useful for speeding up the process of adding users to the system. On older software, it was necessary to allocate combinations of Readers and Time Zones to each new user which could be a slow and error prone process.

Each Group is now 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 **Management** Tab, then select **Groups** from the ribbon bar.



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



Refresh: Updates the list of Groups



Add: Creates a new Group in the list



Delete: Removes the selected Group/s from the list



Edit: edits the selected Group



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



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

Select the **Add** New button



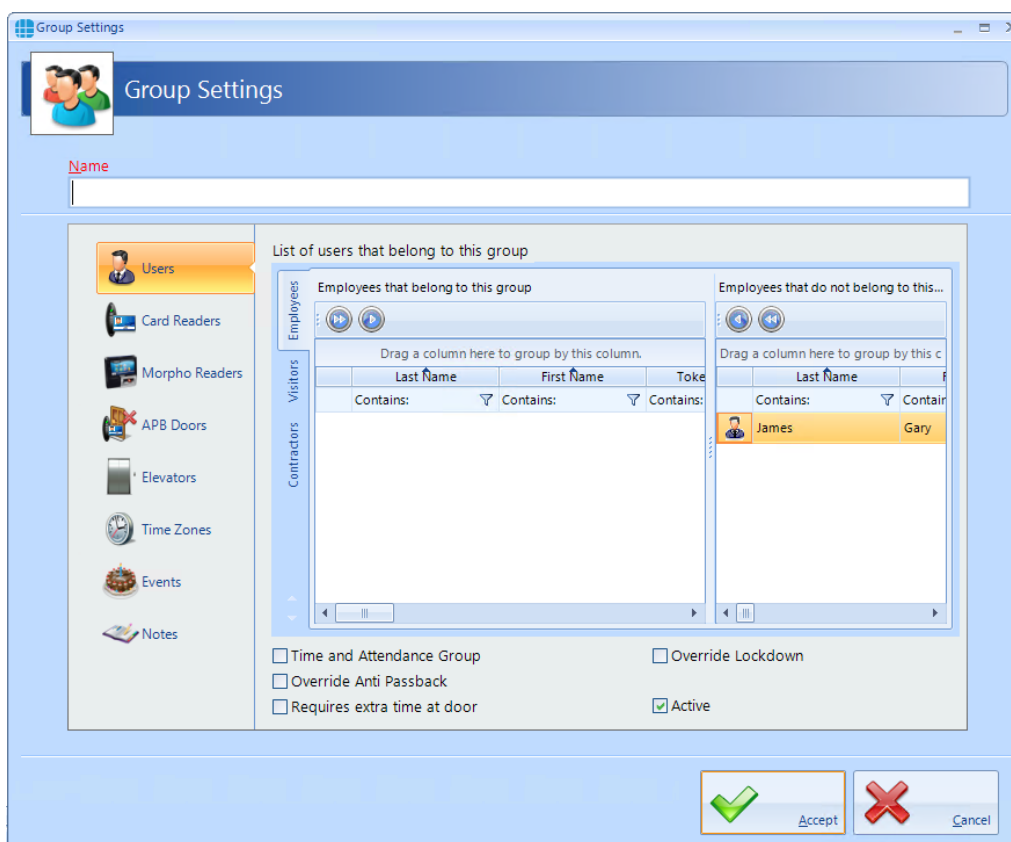
## 16.1 Creating Groups

---

To configure the Group, use the Group Properties Window:

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

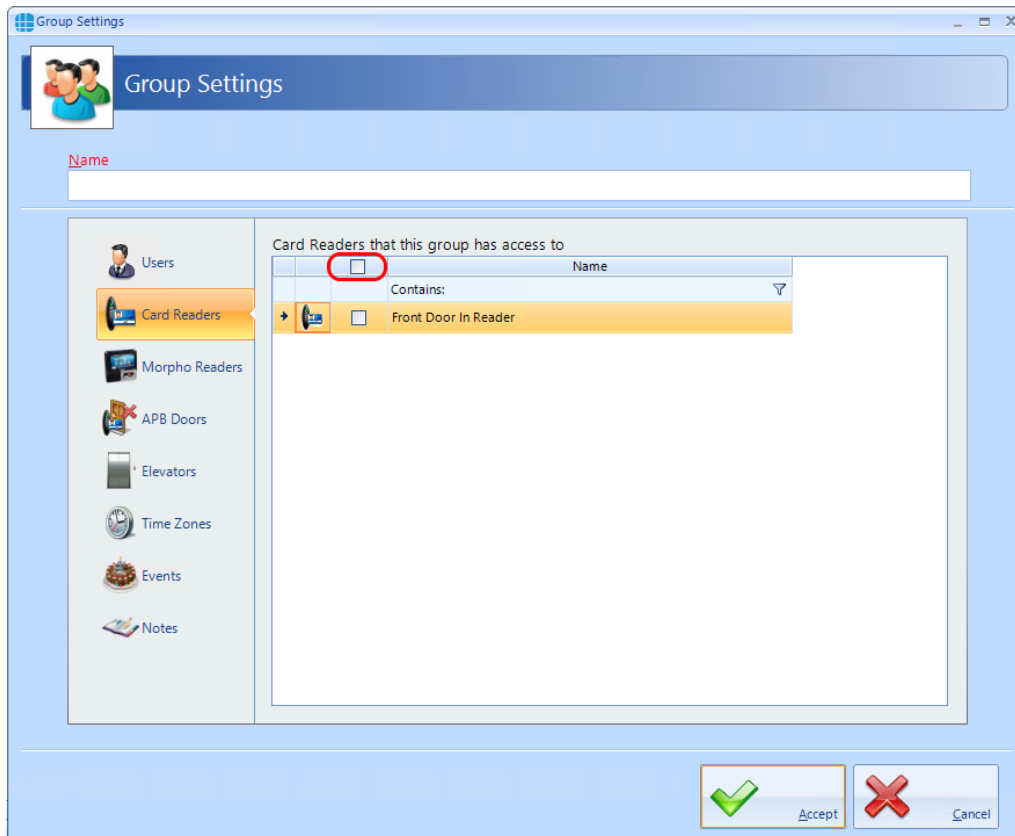
Tick **Requires extra time at door** to use the Extended Door Open Time for members of this group

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.

## 16.1.2 Groups Properties Card Readers

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

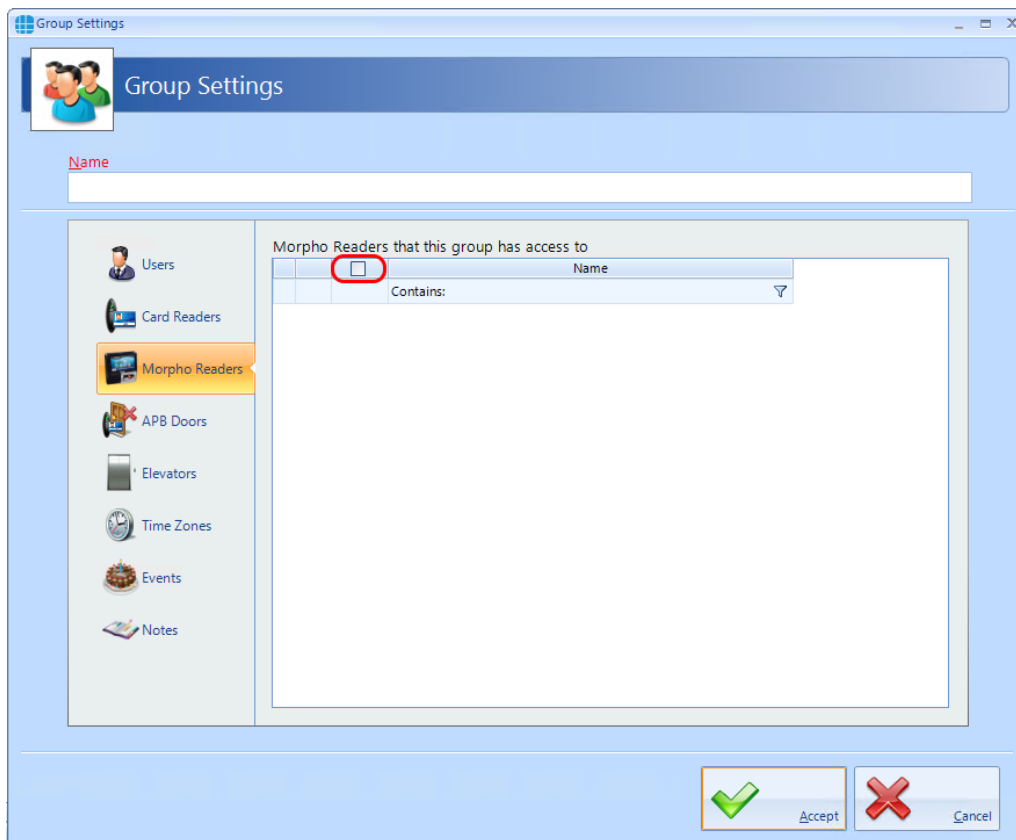


Select one or more card readers or Aperio locks that members of this Group will have access to. To select all readers, tick the **All** box (highlighted above).

**NOTE: If a card reader is linked to a Morpho fingerprint reader, selecting the card reader will automatically select the Morpho reader**

## 16.1.3 Groups Properties Morpho Readers

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

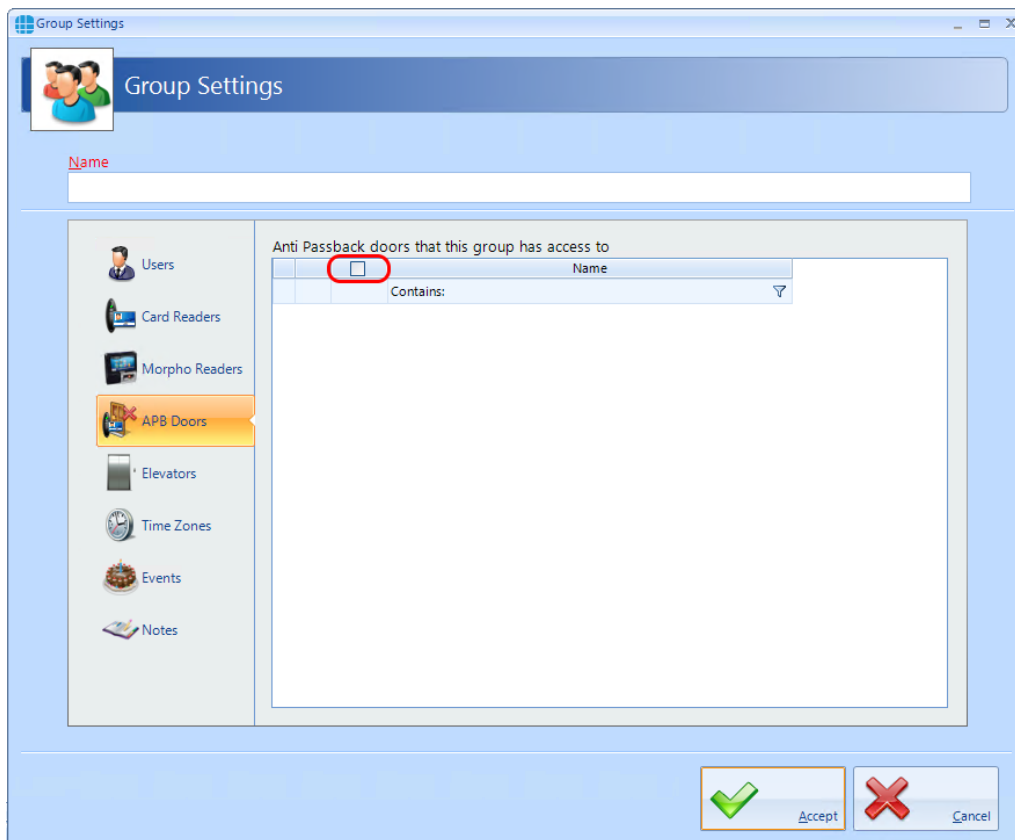


Select one or more Morpho readers that members of this Group will have access to. To select all readers, tick the **All** box (highlighted above).

NOTE: If a Morpho fingerprint reader is linked to a card reader, selecting the Morpho reader will automatically select the card reader

## 16.1.4 Groups Properties APB Doors

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

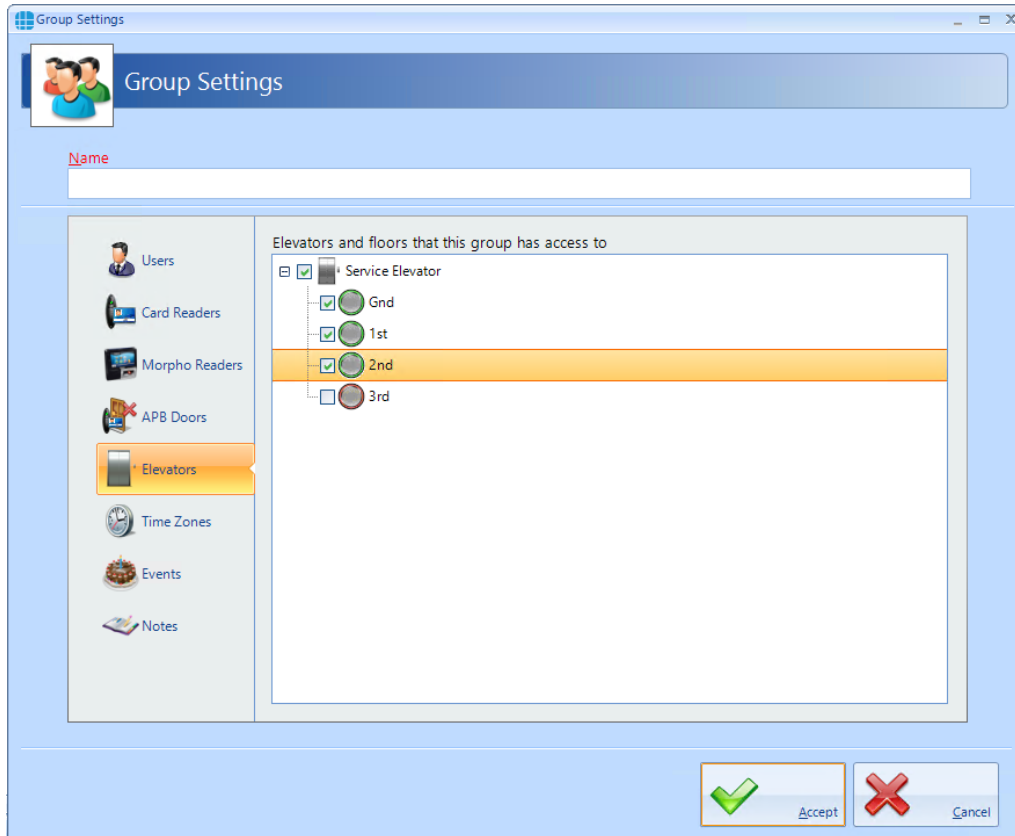


Select one or more AntiPassBack Doors where members of this Group will be subject to AntiPassBack. To select all APB doors, tick the **All** box (highlighted above).



## 16.1.5 Group Properties Elevators

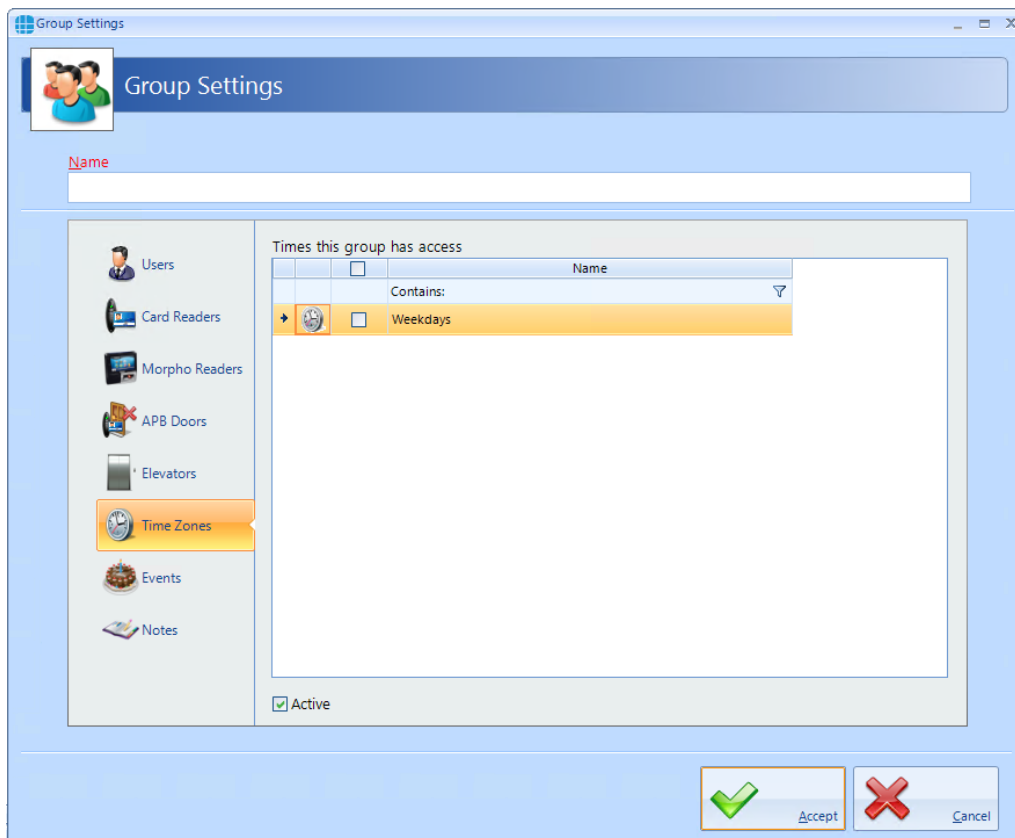
Select the **Elevators** tab to define which floors are accessible to users in this group:



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

## 16.1.6 Groups Properties Time Zones

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

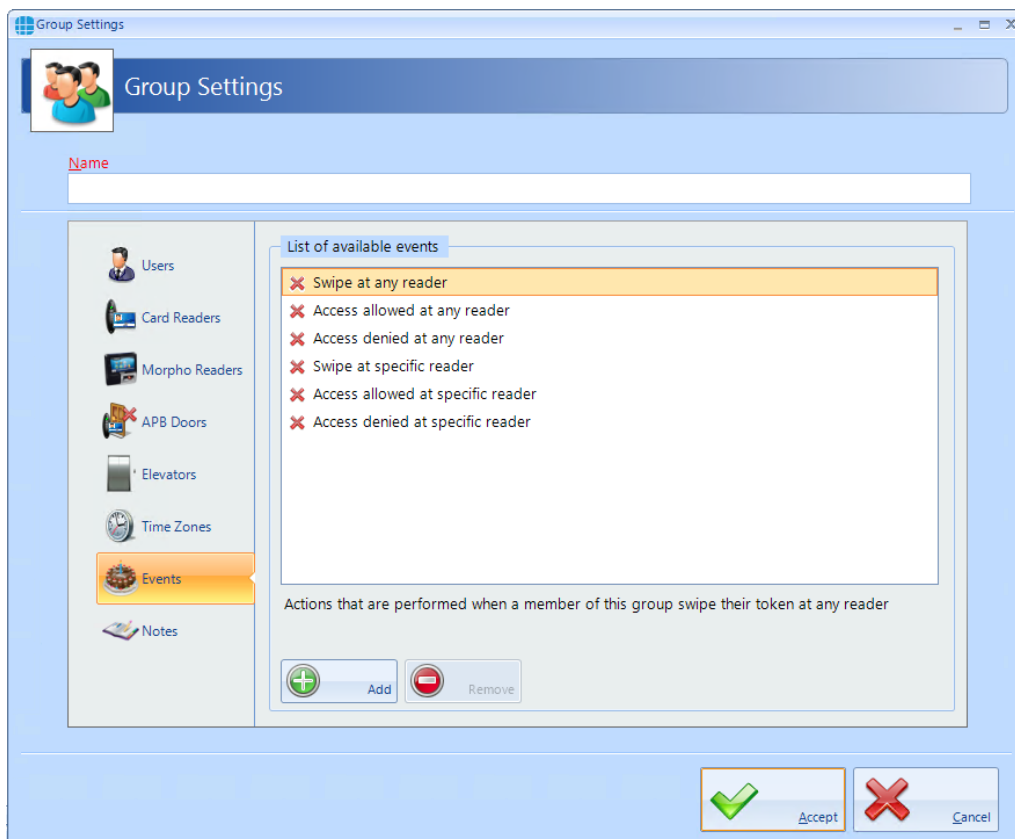


Select the Time Zone that members of this Group will be constrained by.

***NOTE: For additional flexibility, multiple Time Zones can be allocated a single group.***

## 16.1.7 Group Properties Events

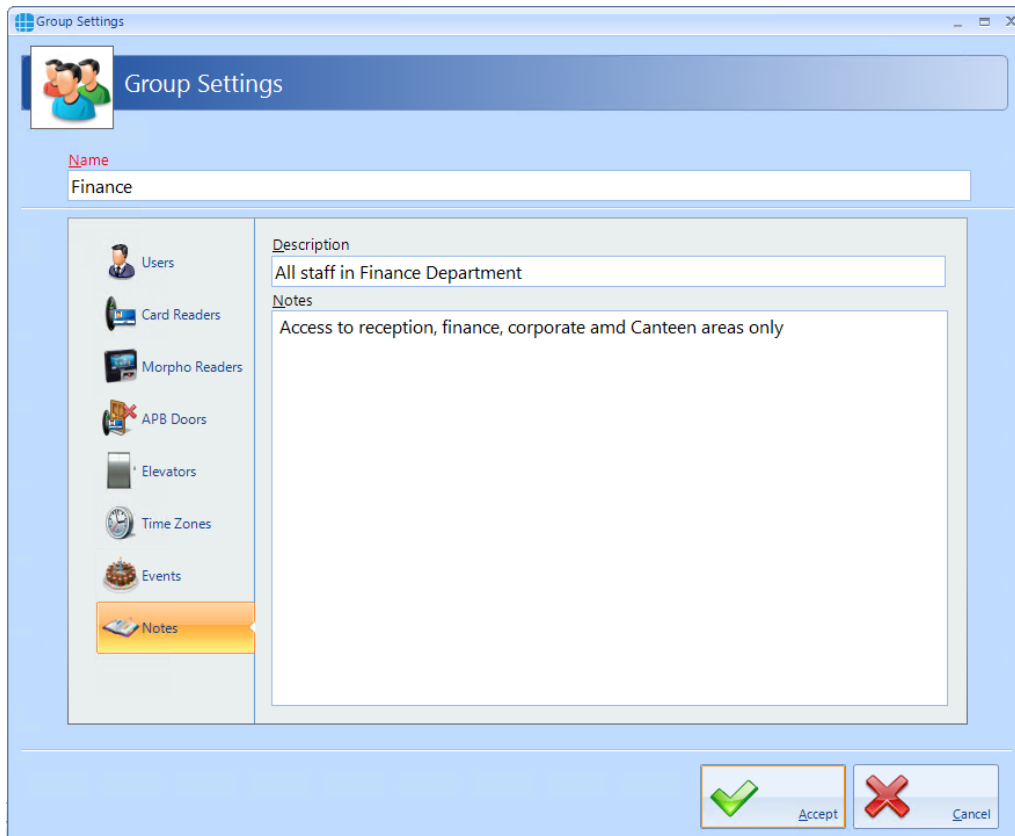
The Events tab will indicate whether any Events have been configured for the selected group.



In this example, no Events have been created for the selected group. 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.

### 16.1.8 Groups 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:



The screenshot shows the 'Group Settings' window. At the top, there's a header bar with the title 'Group Settings' and a small icon of three people. Below the header, there's a 'Name' field with the value 'Finance'. To the left of the main content area is a sidebar with several icons and labels: 'Users', 'Card Readers', 'Morpho Readers', 'APB Doors', 'Elevators', 'Time Zones', 'Events', and 'Notes'. The 'Notes' icon is highlighted in orange. The main content area is divided into two sections: 'Description' and 'Notes'. The 'Description' field contains the text 'All staff in Finance Department'. The 'Notes' field contains the text 'Access to reception, finance, corporate and Canteen areas only'. At the bottom right of the window, there are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

## 16.2 Allocating Users to Groups

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

1. From within the [User Properties](#) <sup>222</sup> Window.
2. From within the [Group Properties](#) <sup>206</sup> Window.

***NOTE: Users can be allocated to more than one Group, but please be aware that in versions prior to v2017.1 constraints exist when multiple Groups are combined:***

EXAMPLE:

Group 1 has access to Reader A from 10:00 to 11:00

Group 2 has access to Reader B from 12:00 to 13:00

A user allocated to Group 1 AND Group 2 will have access through BOTH readers from 10:00 to 11:00, AND will have access through BOTH readers from 12:00 to 13:00

***These constraints do not apply in version 8 or later.***

# Enrolment Readers

## 17 Enrolment Readers

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

**OMN-5427G2** for a variety of card types (see [Omnikey 5427G2 Reader](#)<sup>[217]</sup>)

**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

### 17.1 Omnikey 5427G2 Reader

The Omnikey 5427G2 USB Enrolment Reader is compatible with a wide range of cards or tags. Used in conjunction with Controlsoft Identity Access software, the USB Enrolment Reader offers an easy to use and cost effective solution to assigning cards or tags to employees and visitors.

Step 1: Software Installation

***NOTE: Do not insert the USB reader until the software installation is complete.***

- Browse to the **Drivers** folder and run the relevant file for your operating system (***NOTE: Use the x86 version for 32 bit Operating Systems or the x64 version for 64 bit Operating Systems.***)
- Reboot the PC if instructed to do so.

Step 2: Configure the Enrolment Reader

- Plug the Enrolment Reader into the PC's USB socket.
- Open an internet browser such as Internet Explorer, Firefox or Chrome and enter the address <http://192.168.63.99><sup>[217]</sup> to access the enrolment reader's internal webpage.
- Select the **[System Config]** tab and click on the **[Upload Config]** button. Browse to the required configuration file (e.g. Controlsoft 47 bit.cfg)

- When uploaded, select **Apply Changes**.

When installed, please refer to [User General](#)<sup>222</sup> for information on using the reader when creating or editing users.

Also, the enrolment reader can be used to log on to the Identity Access software, rather than entering a Username and Password (see [Starting the Identity Access Software](#))<sup>94</sup>.



**Users**

18 Users

"Users" is a collective term for Employees, Visitors and Contractors. These user types have been separated as they often have different requirement for Access Rights, for example:

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

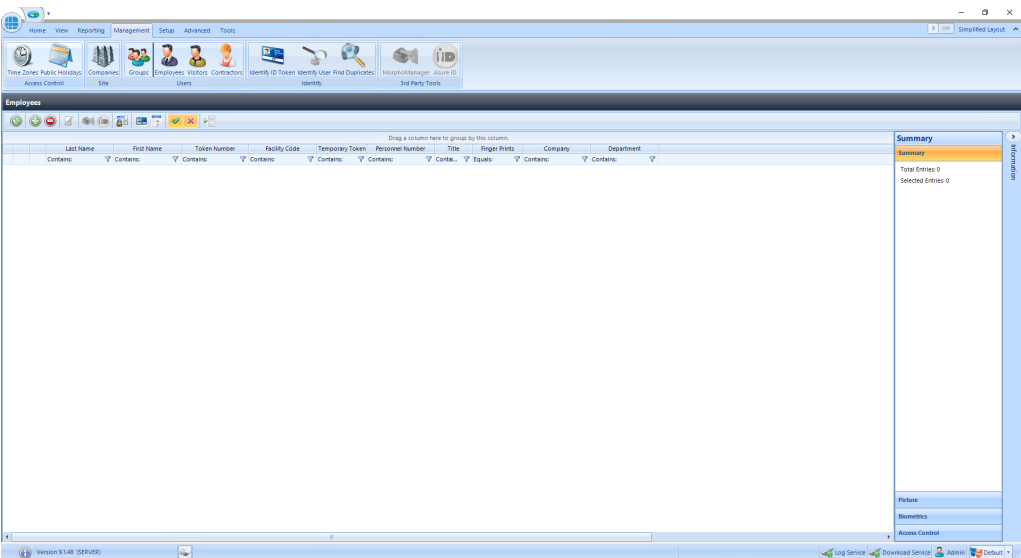
Visitors may have limited access to the premises and may be heavily managed on a day to day basis.

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 **Management** 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



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 Assure 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.

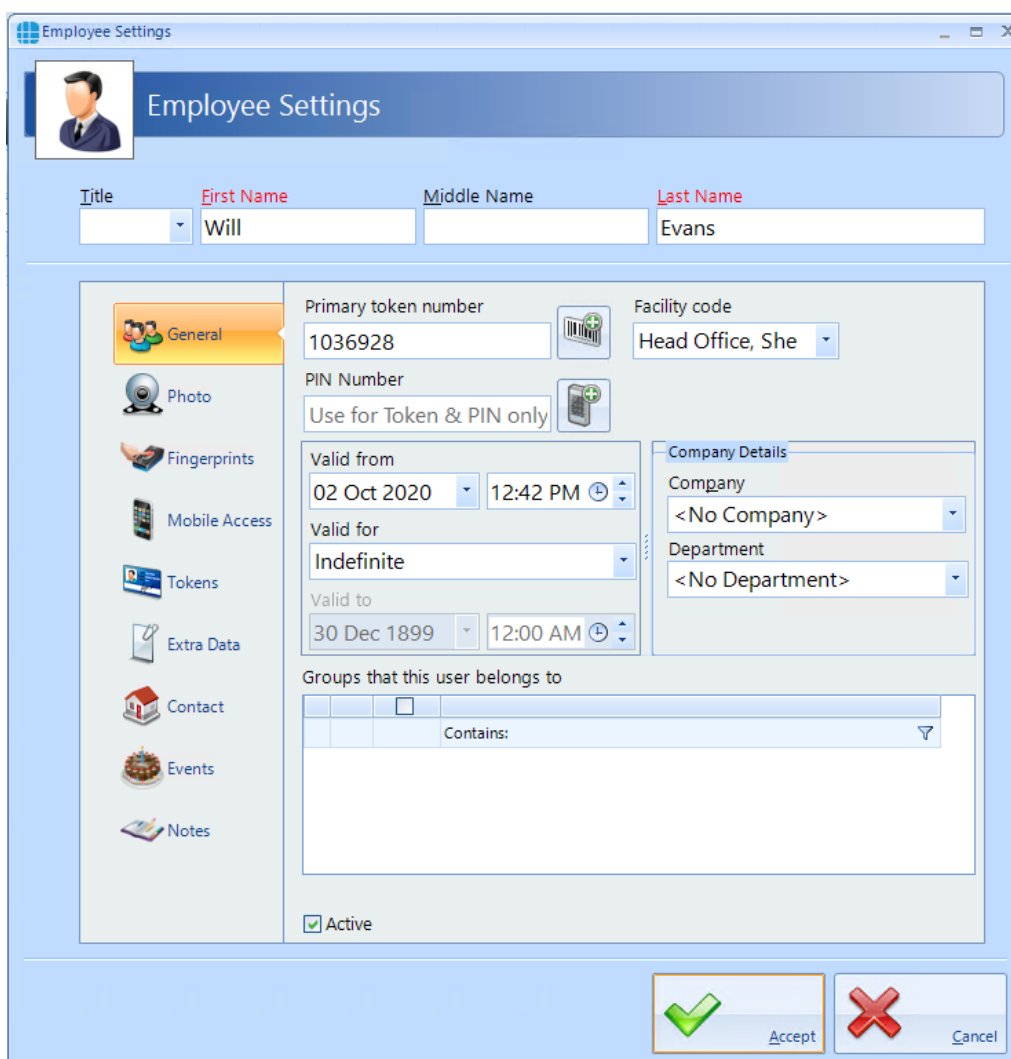


Show Expired Visitors: Filters the display to show visitors whose tokens have expired and can be re-activated.

**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"**

## 18.1 User General

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



The screenshot shows the 'Employee Settings' window. It has a title bar with the text 'Employee Settings'. Below the title bar is a header area with a user profile picture and the text 'Employee Settings'. The main area is divided into a left sidebar and a right content area. The sidebar contains icons for General, Photo, Fingerprints, Mobile Access, Tokens, Extra Data, Contact, Events, and Notes. The 'General' tab is selected. The content area contains the following fields: Title (dropdown), First Name (text box with 'Will'), Middle Name (text box), Last Name (text box with 'Evans'), Primary token number (text box with '1036928'), Facility code (dropdown with 'Head Office, She'), PIN Number (text box with 'Use for Token & PIN only'), Valid from (date and time picker with '02 Oct 2020' and '12:42 PM'), Valid for (dropdown with 'Indefinite'), Valid to (date and time picker with '30 Dec 1899' and '12:00 AM'), Company Details (Company dropdown with '<No Company>' and Department dropdown with '<No Department>'), Groups that this user belongs to (table with columns for selection and name), and an 'Active' checkbox which is checked. At the bottom right are 'Accept' and 'Cancel' buttons.

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 Codes are not enabled in the IA**

**Configuration utility (see [IA Configuration - Cards & Readers](#) <sup>58</sup>), this field will be greyed out.**

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

**NOTE: Users can be allocated to more than one Group, but please be aware that constraints exist in versions prior to v2017.1 when multiple Groups are combined:**

EXAMPLE:

Group 1 has access to Reader A from 10:00 to 11:00

Group 2 has access to Reader B from 12:00 to 13:00



A user allocated to Group 1 AND Group 2 will have access through BOTH readers from 10:00 to 11:00, AND will have access through BOTH readers from 12:00 to 13:00

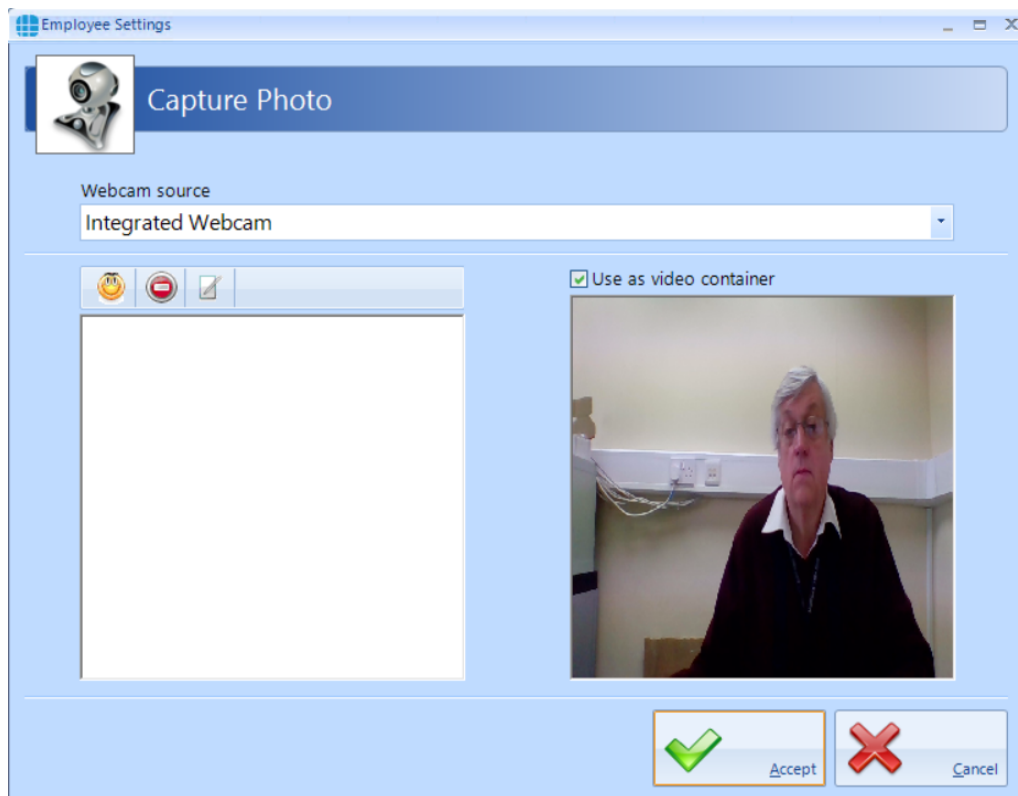
**These constraints do not apply to software v8 or later.**

## 18.2 User Photo

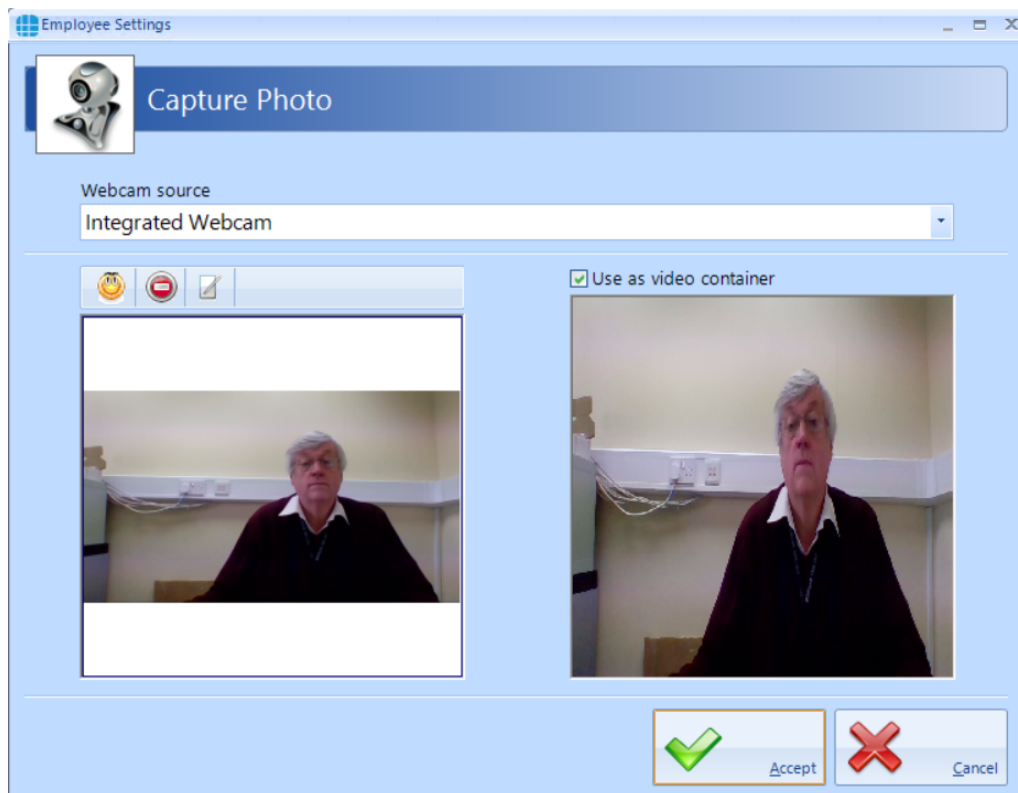
Allocating a photo to a user can be useful when identifying a lost card as it is possible to read the card and display the photo and other details of the relevant user. As standard there are two Reader Monitors located in the Dashboard to view the photos of people entering and exiting the premises.




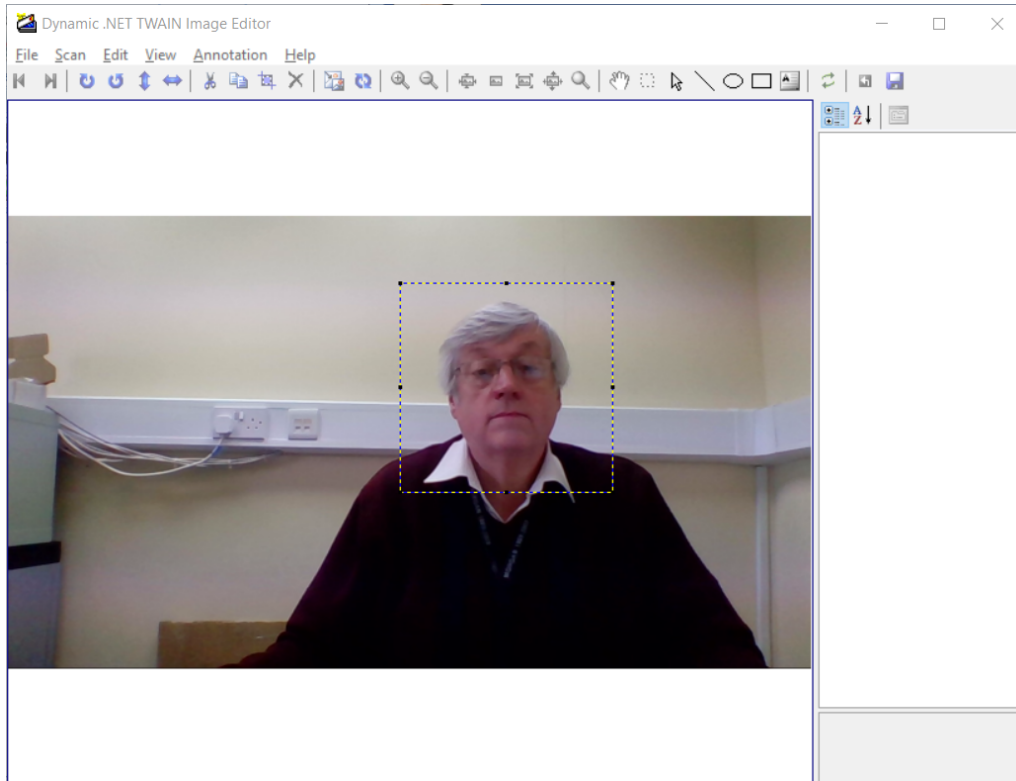
Select the import icon  to import a previously saved image, or the camera icon  to capture a photo from a webcam:




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:

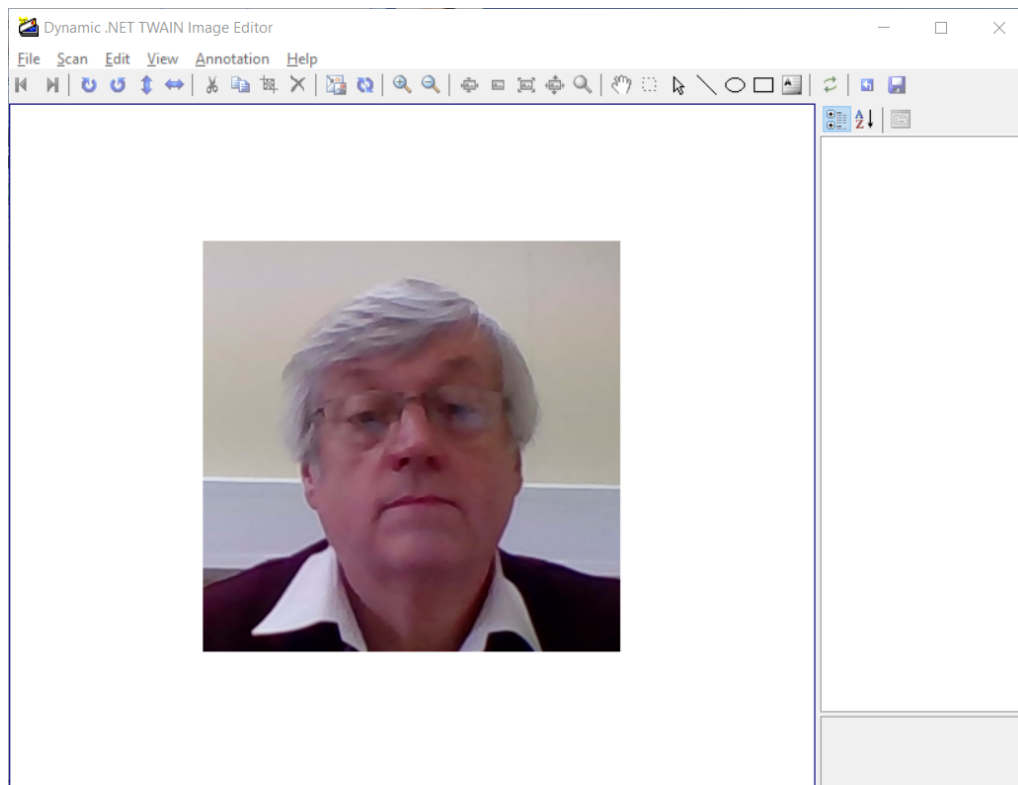


It is possible to capture multiple images, then scroll up and down to select the best image to use. To optimise the image, it is possible to zoom in on the main area of interest by clicking the edit button 



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





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

## 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.

The screenshot shows the 'Employee Settings' window. At the top, there's a header with a user icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Will'), 'Middle Name', and 'Last Name' (containing 'Evans'). A sidebar on the left contains icons for 'General', 'Photo', 'Fingerprints' (highlighted), 'Mobile Access', 'Tokens', 'Extra Data', 'Contact', 'Events', and 'Notes'. The main area is titled 'Select enrolment device' and shows a dropdown menu with 'MA Sigma' selected. Below the dropdown are two hand diagrams for fingerprint enrolment. Each hand has five fingers, each with a small icon and a '0' below it. Some icons are crossed out with a red 'X'. At the bottom of the main area is a button labeled 'Check for Duplicates'. At the very bottom of the window are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red 'X' icon).

**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**

The screenshot shows the 'Employee Settings' window for a user named Will Evans. The 'Fingerprints' tab is selected in the left-hand menu. The 'Select enrolment device' dropdown is set to 'MSO Takeon Device'. The main area displays two hand diagrams for fingerprint enrolment. Each hand has four fingers with a red 'X' and a '0' below them, indicating they are not enrolled. The thumb of each hand has a blue icon with a green checkmark and a '0' below it, indicating it is the selected finger for enrolment. A text box below the hand diagrams states: 'Ensure that the facility code set for the primary token number matches the facility code set for the Morpho readers that this user has access to.' Below this text is a button labeled 'Check for Duplicates'. At the bottom right of the window are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red 'X' icon).

Employee Settings

Title First Name Middle Name Last Name

Will Evans

General

Photo

Fingerprints

Mobile Access

Tokens

Extra Data

Contact

Events

Notes

Select enrolment device

MSO Takeon Device

0 0 0 0

0 0 0 0

0 0

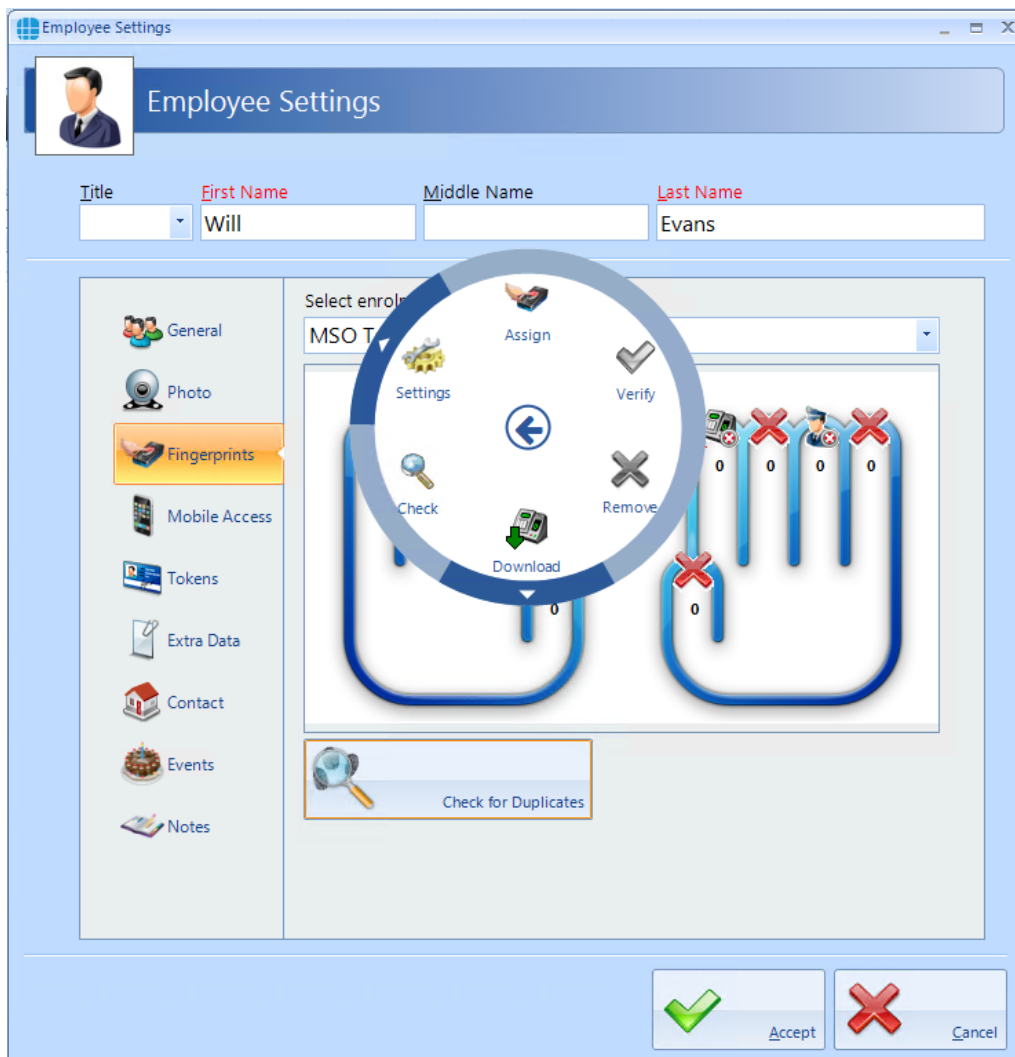
0 0

Ensure that the facility code set for the primary token number matches the facility code set for the Morpho readers that this user has access to.

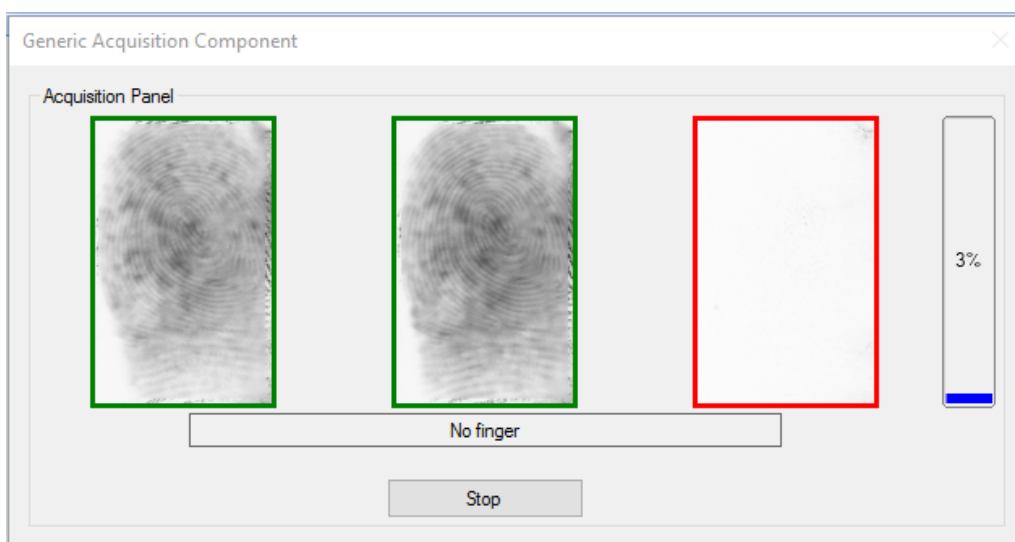
Check for Duplicates

Accept Cancel

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

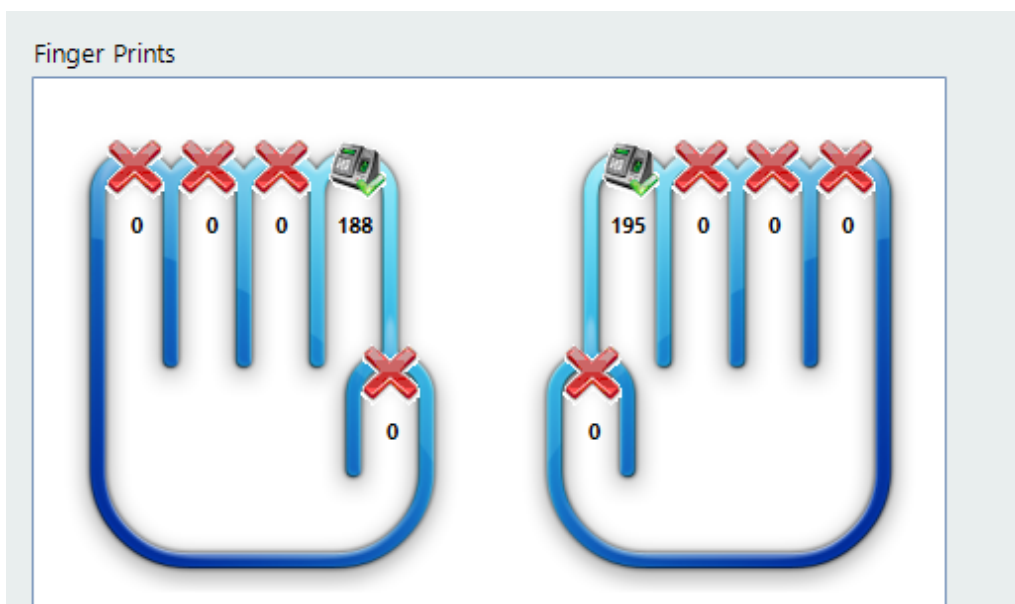


Place the selected finger on the enrolment reader 3 times, following the on-screen instructions where necessary.



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.**



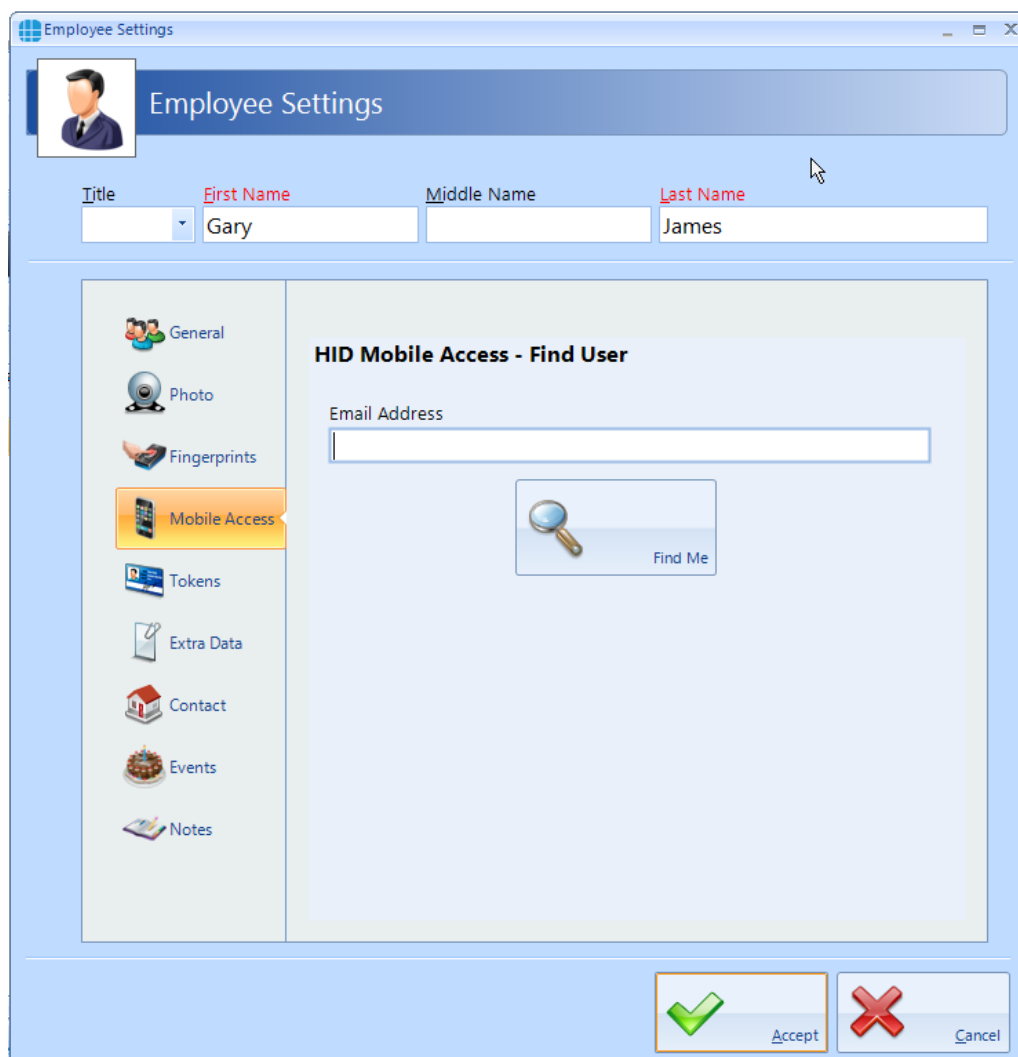
**NOTE: If enrolling a Duress Fingerprint the system will automatically update the relevant token number into the appropriate Secondary Token field.**

## 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.

Select **Management** in the tools bar, then click on the **Employees** button in the ribbon bar. Create a new employee or double click an existing employee.

Select **Mobile Access** in the side bar



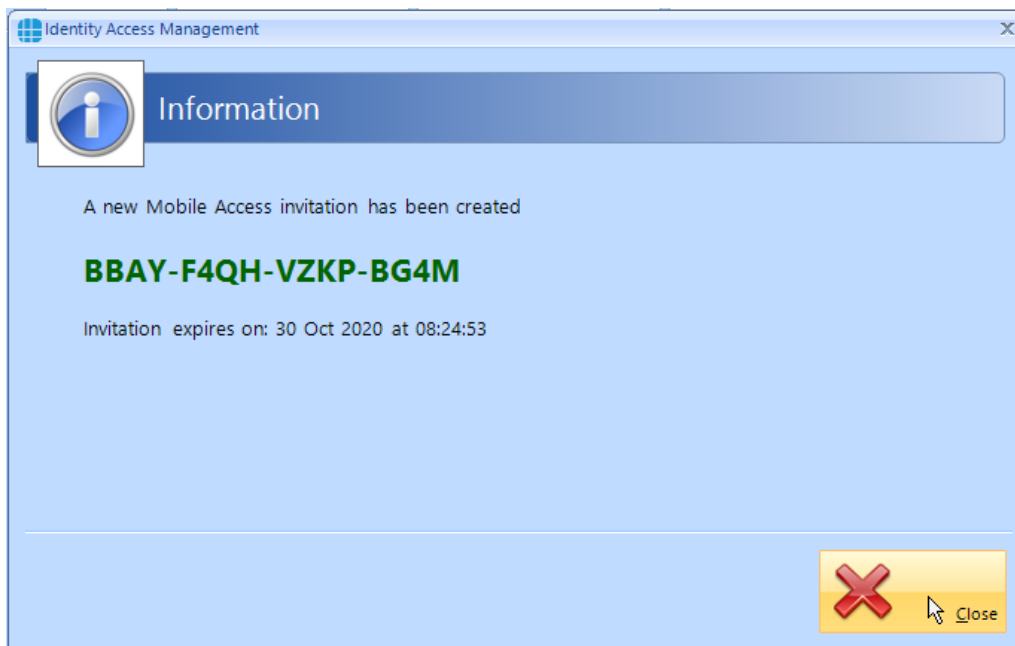
The screenshot shows the 'Employee Settings' window. At the top, there's a header bar with a user icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Gary'), 'Middle Name', and 'Last Name' (containing 'James'). On the left side, there's a vertical sidebar with icons for 'General', 'Photo', 'Fingerprints', 'Mobile Access' (which is highlighted), 'Tokens', 'Extra Data', 'Contact', 'Events', and 'Notes'. The main area of the window is titled 'HID Mobile Access - Find User'. It contains an 'Email Address' input field and a 'Find Me' button with a magnifying glass icon. At the bottom right, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

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.

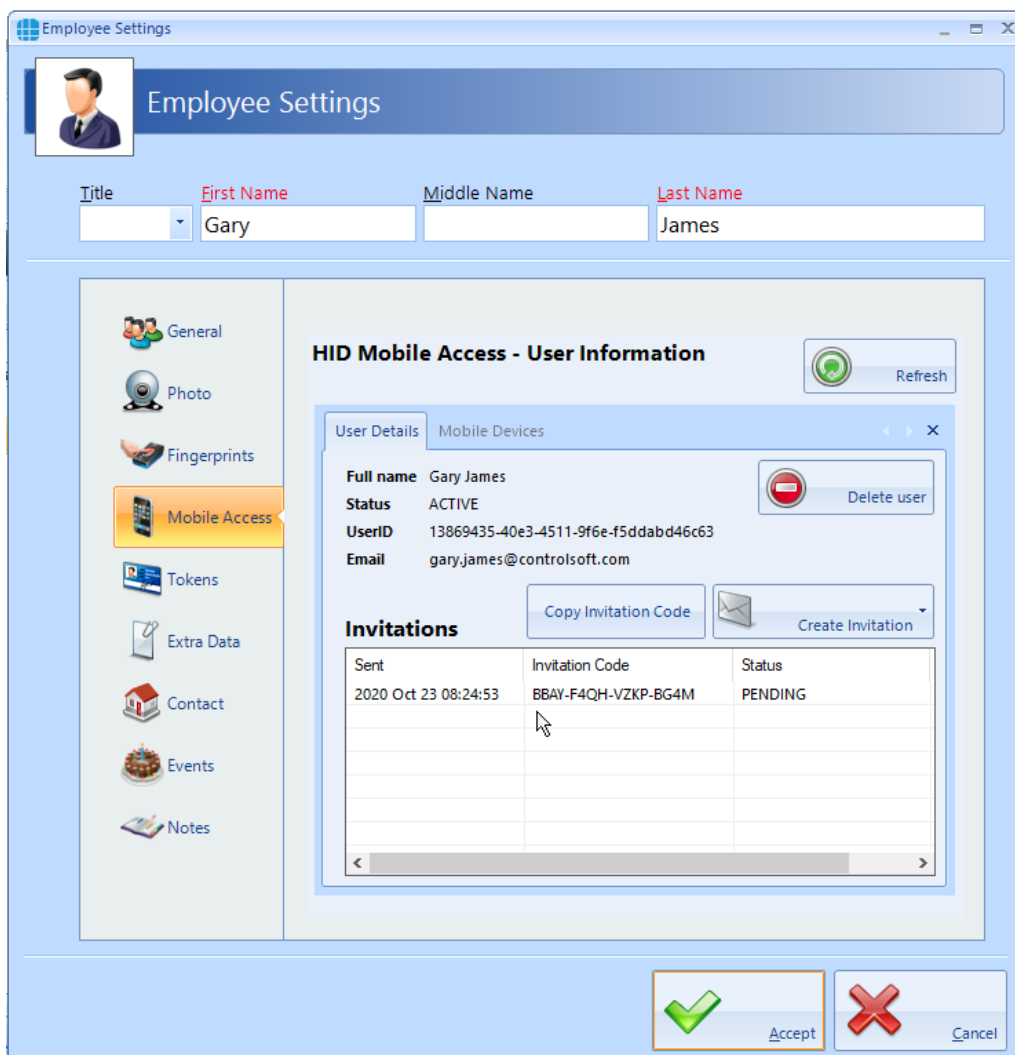
If the employee has never been issued with a Mobile Access credential, the following screen will be displayed

The screenshot shows the 'Employee Settings' window. At the top, there's a header with a user icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Gary'), 'Middle Name', and 'Last Name' (containing 'James'). The main area is divided into a left sidebar with icons for 'General', 'Photo', 'Fingerprints', 'Mobile Access' (highlighted), 'Tokens', 'Extra Data', 'Contact', 'Events', and 'Notes'. The right pane is titled 'HID Mobile Access - Create New User' and contains the text: 'An HID Mobile Access profile has not yet been assigned to this person.' Below this is a 'Select part number' section with a dropdown menu showing 'Default part number'. There are two buttons: 'Create Profile' (with a user icon and a plus sign) and 'Start Again' (with a house icon). At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmarks respectively.

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](#) <sup>65</sup>)



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





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

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

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

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

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

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

The screenshot shows the 'Employee Settings' window. On the left is a sidebar with icons for General, Photo, Fingerprints, Mobile Access (highlighted), Tokens, Extra Data, Contact, Events, and Notes. The main area is titled 'HID Mobile Access - User Information' and contains a 'Refresh' button. Below this is a 'User Details' tab showing information for Gary James: Full name, Status (ACTIVE), UserID, and Email. A 'Delete user' button is next to the details. Below the details is an 'Invitations' section with a 'Copy Invitation Code' button and a 'Create Invitation' dropdown. A table lists the invitation details:

Sent	Invitation Code	Status
2020 Oct 23 08:24:53	BBAY-F4QH-VZKP-BG4M	ACKNOWLEDGED

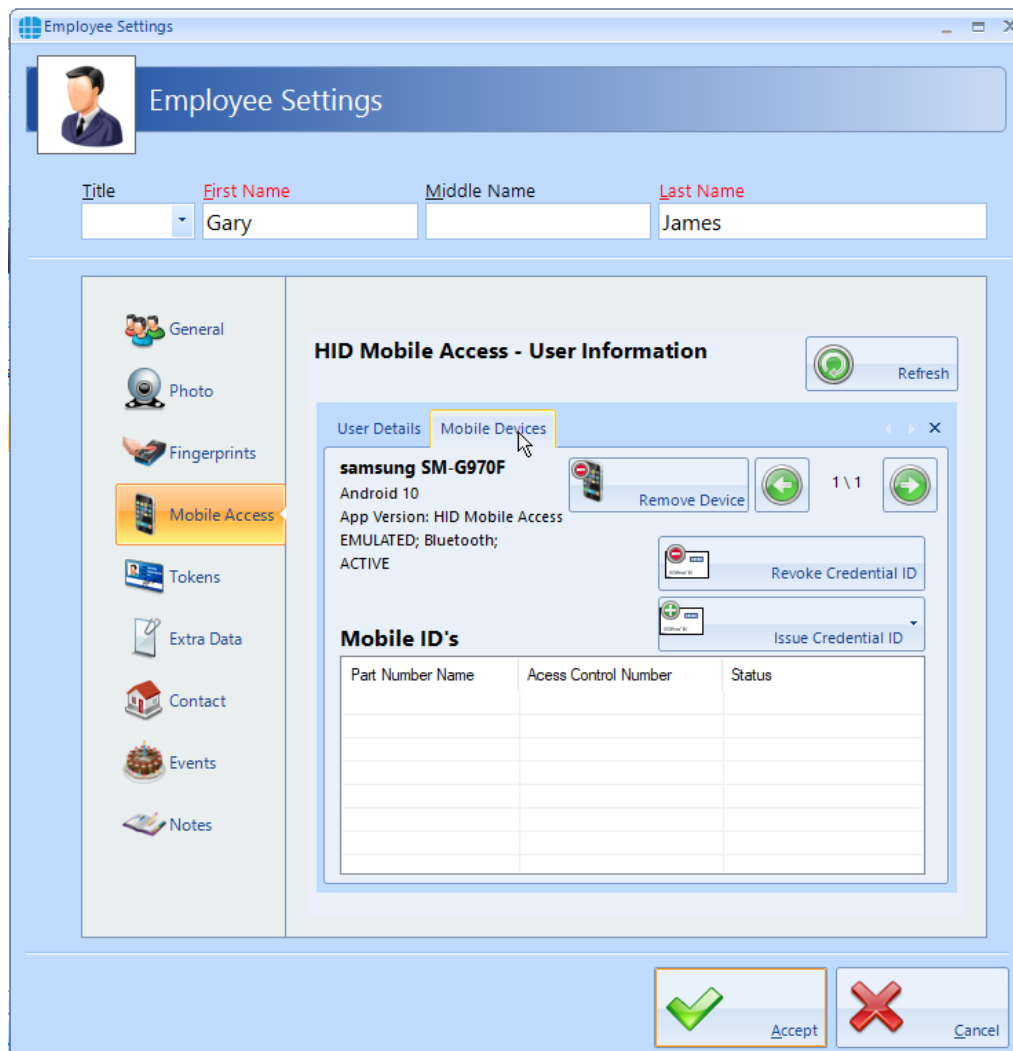
At the bottom of the window are 'Accept' and 'Cancel' buttons.

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

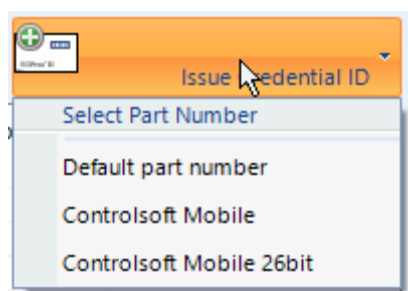
**NOTE: An option exists in the IA Configuration utility called "Issue Mobile Credential ID with invitation" (see [IA Configuration - HID Mobile Access](#)<sup>65</sup>). If this option has been**

*selected, the invitation Status will now show as **ISSUED** and the next few instructions can be ignored.*

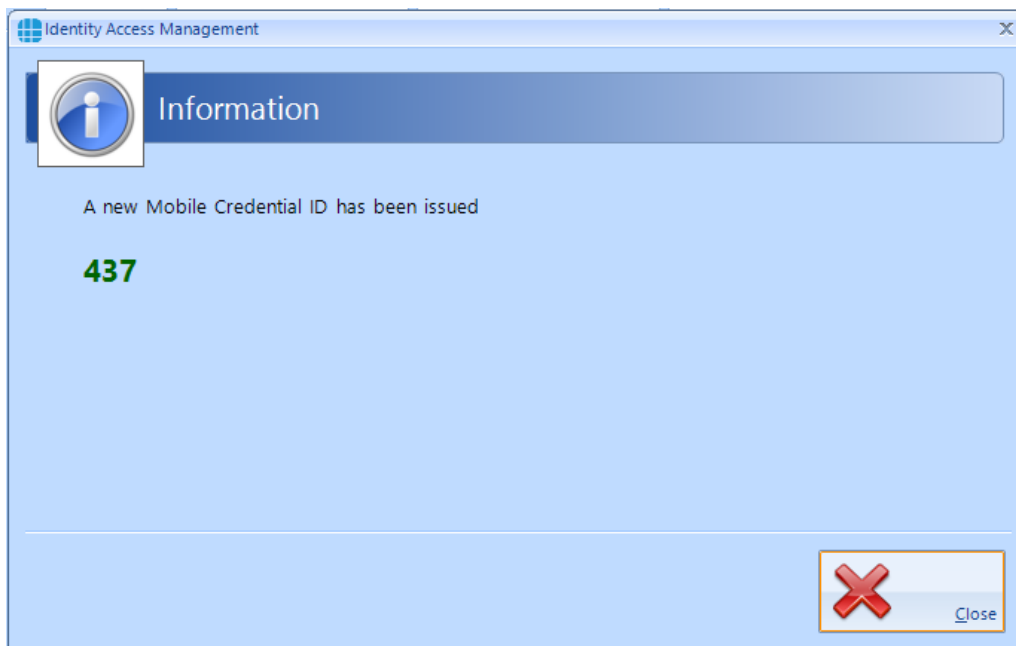
Select the **Mobile Devices** tab



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



An information box will now show the credential number issued



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


The screenshot shows the 'Employee Settings' window. The top section contains fields for 'Title', 'First Name' (Gary), 'Middle Name', and 'Last Name' (James). The left sidebar lists various settings categories: General, Photo, Fingerprints, Mobile Access (selected), Tokens, Extra Data, Contact, Events, and Notes. The main content area is titled 'HID Mobile Access - User Information' and includes a 'Refresh' button. Below this, there are tabs for 'User Details' and 'Mobile Devices'. The 'Mobile Devices' tab is active, showing details for a 'samsung SM-G970F' device, including 'Android 10', 'App Version: HID Mobile Access', 'EMULATED; Bluetooth;', and 'ACTIVE'. There are buttons for 'Remove Device', 'Revoke Credential ID', and 'Issue Credential ID'. A table titled 'Mobile ID's' lists the device's details:

Part Number Name	Access Control Number	Status
Controlsoft Mobile 2...	437	ISSUED,ICLASSEOS

At the bottom of the window, there are 'Accept' and 'Cancel' buttons.

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](#) <sup>65</sup>)

Employee Settings

 Employee Settings

Title  First Name  Middle Name  Last Name

Gary   James

General  
Photo  
Fingerprints  
Mobile Access  
**Tokens**  
Extra Data  
Contact  
Events  
Notes

Secondary token 1  
 437

Secondary token 2

Secondary token 3

Secondary token 4

Secondary token 5



Facility code

Facility code

Facility code

Facility code

Facility code

## 18.5 Multiple Tokens

Each user can be given more than 1 token to allow for multiple credential types (e.g. an Employee may have a card, a mobile credential and a windscreen tag for the car park). The **Tokens** tab allows these secondary credentials 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 screenshot shows the 'Employee Settings' window with the 'Tokens' tab selected. The 'General' tab is also visible in the sidebar. The 'Tokens' tab contains the following fields:

Token	Field	Value
Secondary token 1	Token ID	
Secondary token 1	Facility code	
Secondary token 2	Token ID	
Secondary token 2	Facility code	
Secondary token 3	Token ID	
Secondary token 3	Facility code	
Secondary token 4	Token ID	
Secondary token 4	Facility code	
HIK Vision ANPR number	ANPR number	4138416
Number plate	Number plate	OK123VEH

At the bottom right, there are two buttons: 'Accept' (with a green checkmark) and 'Cancel' (with a red X).

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](#)<sup>[58]</sup>).

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](#)<sup>[58]</sup>), then **Secondary Token 5** will automatically be renamed to **HIK Vision ANPR number** as in the above

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

***NOTE: The ANPR number plate must be unique***

## 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](#)<sup>72</sup>).

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

The screenshot shows the 'Employee Settings' window. At the top, there's a header bar with a user icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Will'), 'Middle Name', and 'Last Name' (containing 'Evans'). The main area is divided into a left sidebar with icons for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens', 'Extra Data' (highlighted), 'Contact', 'Events', and 'Notes'. The 'Extra Data' tab is active, displaying a table with columns 'Index', 'Extra Field', and 'Value'. The table contains one row with a green checkmark in the 'Index' column, '0' in the 'Extra Field' column, and 'Valid Driver's License' in the 'Value' column. Below the table, there's a section titled 'Valid Driver's License' with two radio buttons: 'Yes' and 'No'. The 'No' radio button is selected. At the bottom right of this section is a green checkmark icon and the text 'Apply'. At the very bottom of the window, there are two large buttons: a green checkmark icon with the text 'Accept' and a red 'X' icon with the text 'Cancel'.

Index	Extra Field	Value
✓ 0	Valid Driver's License	

Valid Driver's License

☐ Yes

☒ No

Apply

Accept Cancel

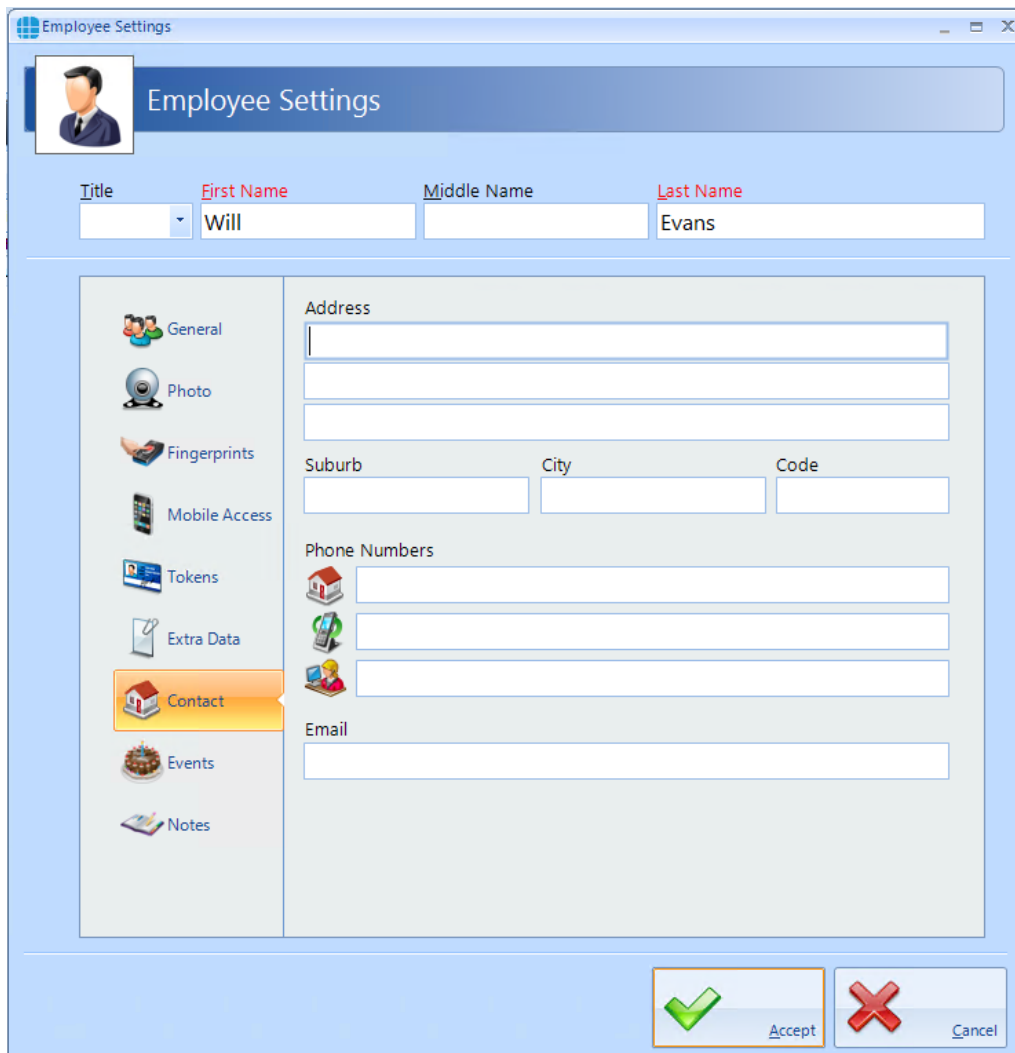
In this instance, the Extra Data Field has been configured to record whether the user has a valid driver's license. Simply select **Yes** or **No** as appropriate, followed by **[Apply]** and **[Accept]**.

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



## 18.7 User Contact

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



The screenshot shows the 'Employee Settings' window. At the top, there's a header bar with a user icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Will'), 'Middle Name', and 'Last Name' (containing 'Evans'). The main area is divided into a left sidebar with icons for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens', 'Extra Data', 'Contact' (highlighted), 'Events', and 'Notes'. The 'Contact' tab is active, showing fields for 'Address' (three stacked lines), 'Suburb', 'City', 'Code', 'Phone Numbers' (three stacked lines with house and phone icons), and 'Email' (one line). At the bottom right, there are 'Accept' and 'Cancel' buttons with green checkmark and red X icons respectively.

## 18.8 User Events

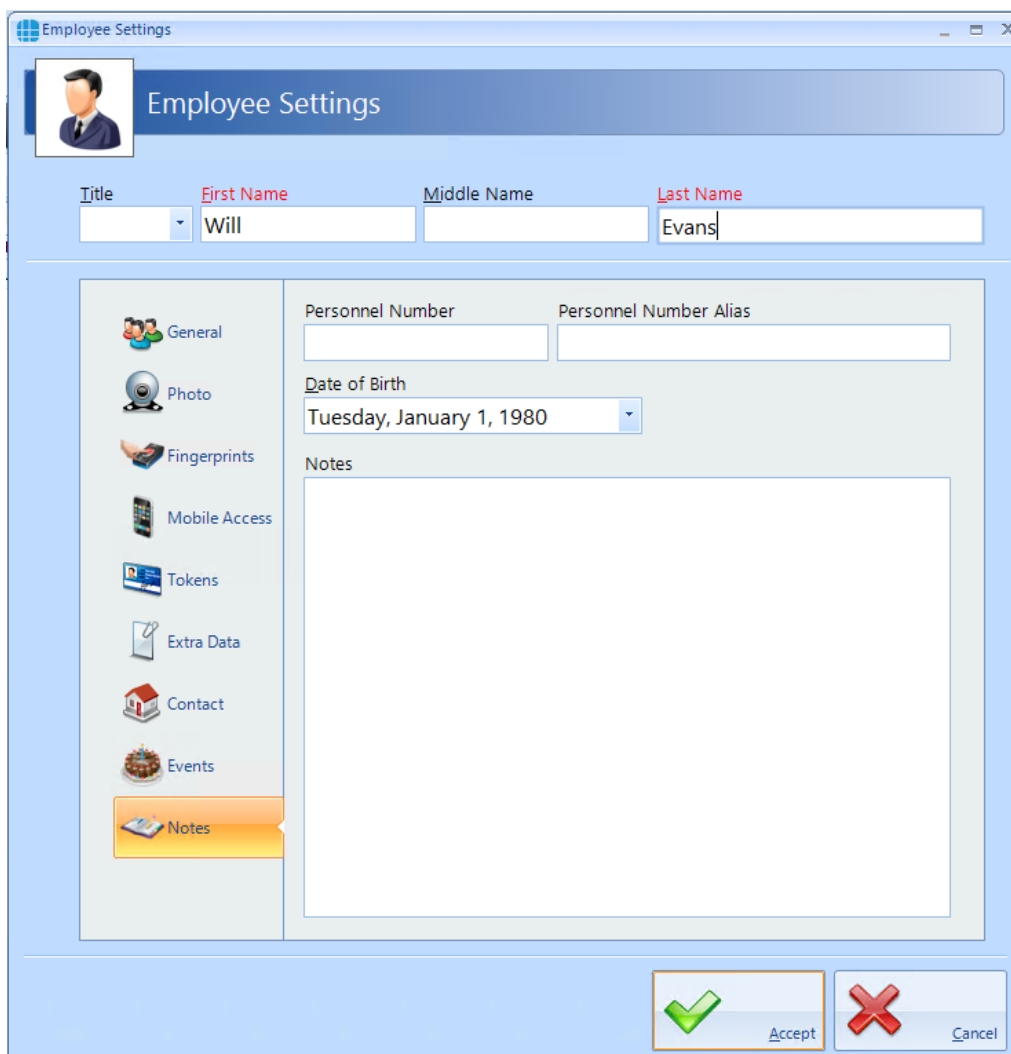
The Events tab will indicate whether any Events have been configured for the selected user.

The screenshot shows the 'Employee Settings' window. At the top, there's a header bar with a user icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Will'), 'Middle Name', and 'Last Name' (containing 'Evans'). On the left side, there's a vertical menu with icons and labels for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens', 'Extra Data', 'Contact', 'Events' (highlighted in orange), and 'Notes'. The main area of the window is titled 'List of available events' and contains a list of events, each preceded by a red 'X' icon. The events are: 'Swipe at any reader', 'Access allowed at any reader', 'Access denied at any reader', 'Swipe at specific reader', 'Access allowed at specific reader', and 'Access denied at specific reader'. Below the list, there's a text label 'Actions that are performed when this person swipe their token at any reader' and two buttons: 'Add' (with a green plus icon) and 'Remove' (with a red minus icon). At the bottom right, there are two large buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

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.

## 18.9 User Notes

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



The screenshot shows the 'Employee Settings' window with the 'Notes' tab selected. The window has a title bar 'Employee Settings' and a close button. Below the title bar is a header area with a user icon and the text 'Employee Settings'. The main area is divided into a left sidebar and a right content area. The sidebar contains icons and labels for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens', 'Extra Data', 'Contact', 'Events', and 'Notes' (which is highlighted in orange). The right content area contains the following fields: 'Title' (a dropdown menu), 'First Name' (text box with 'Will'), 'Middle Name' (text box), 'Last Name' (text box with 'Evans'), 'Personnel Number' (text box), 'Personnel Number Alias' (text box), 'Date of Birth' (calendar icon and text box with 'Tuesday, January 1, 1980'), and 'Notes' (a large text area). At the bottom right of the window are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

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

## 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.

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]**.

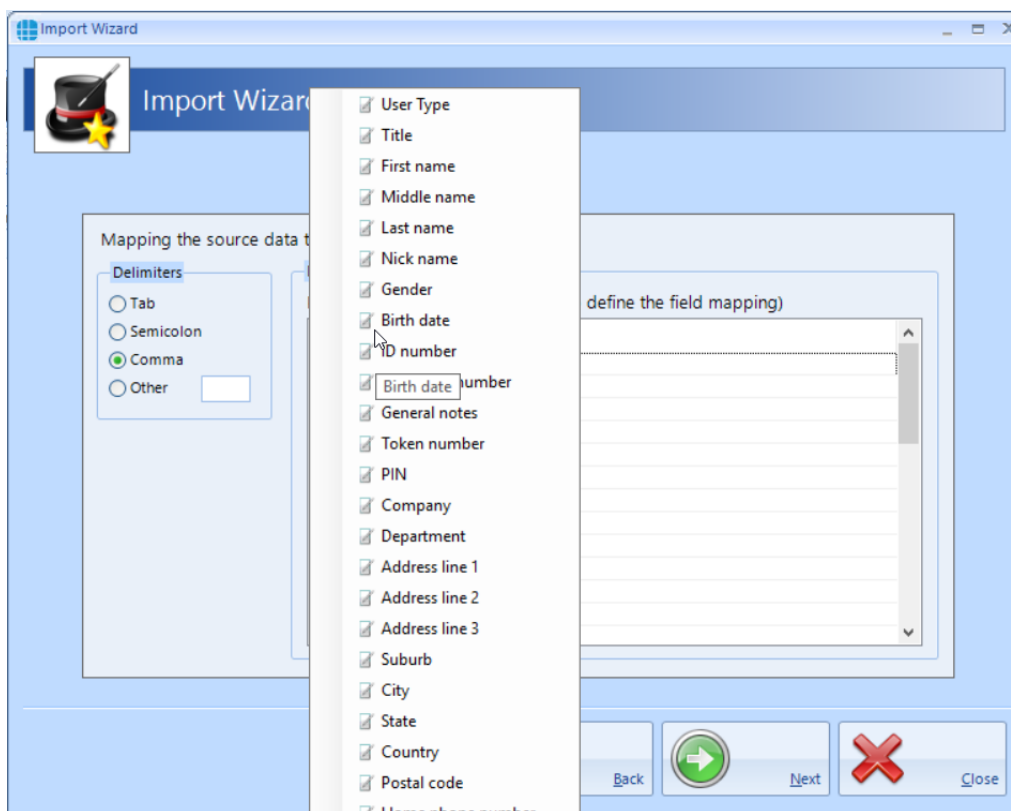
**Select Destination** should be set to define the types of user being imported (Employee, Visitor or Contractor). Select **Ignore duplicate names** to avoid duplicate entries. Click **[Next]**

***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]**

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

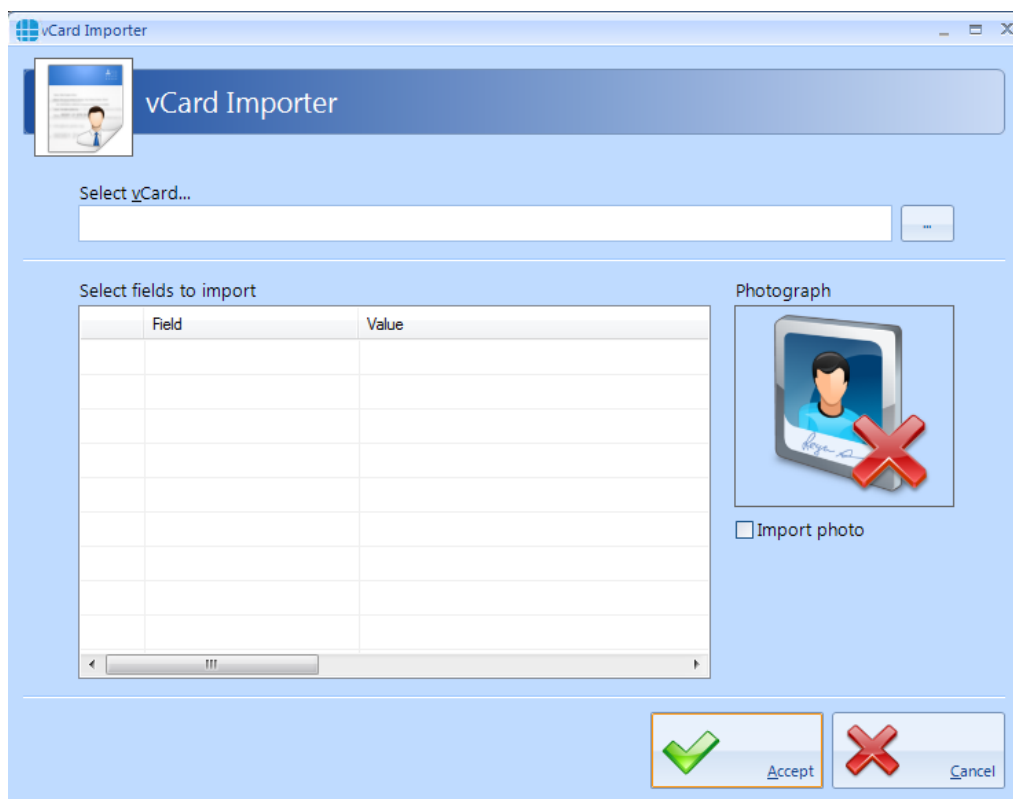
Under **Data Preview**, link each column in the .csv file to the corresponding database field. Click on each column header and select the required field from the dropdown list:



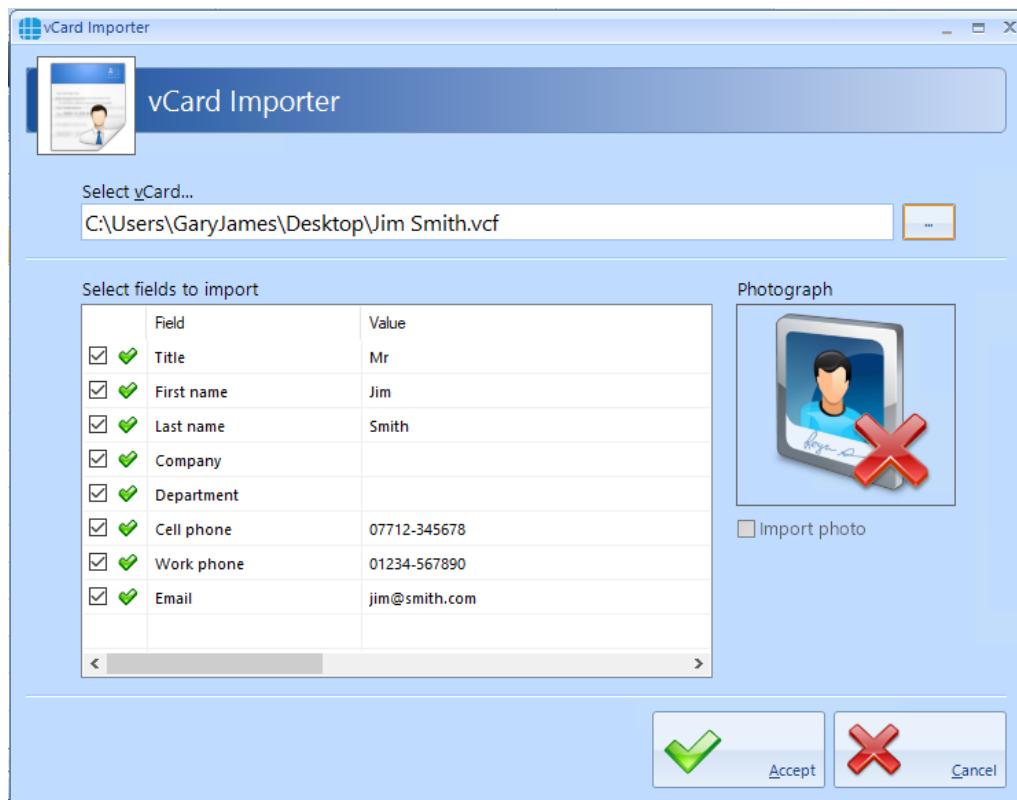
When complete, click **[Next]**, followed by **[Import]** to start the import process and **[Close]** when the import is complete.

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 

**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]**.



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

Employee Settings

 Employee Settings

Title:  First Name:  Middle Name:  Last Name:

**General**

Primary token number:  Facility code:


PIN Number:  Use for Token & PIN only: ☐

Valid from:   Valid for:  Valid to:



Company Details

Company:  Department:

Groups that this user belongs to

			Contains:
+		<input type="checkbox"/>	All staff

☒ Active



## The Advanced Tab

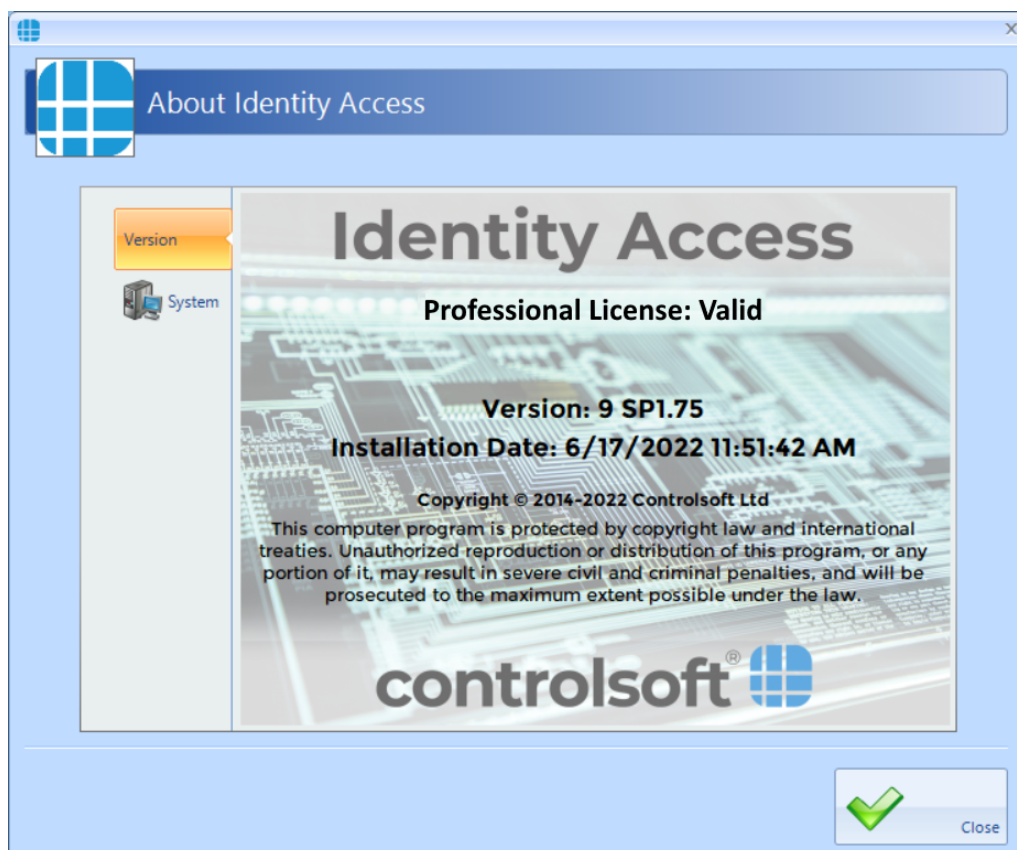
## 19 The Advanced Tab

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

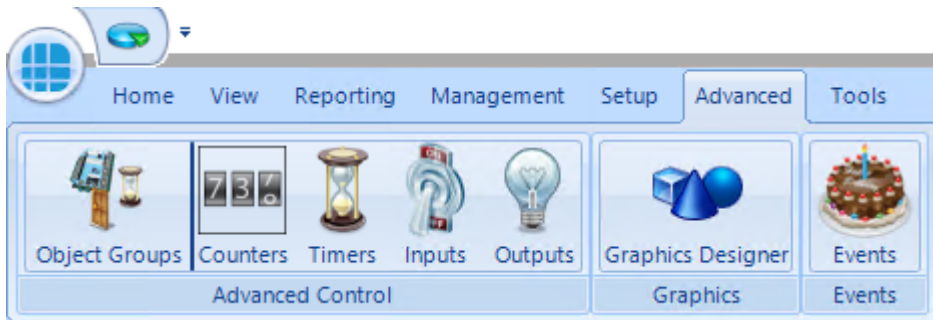
Enterprise Features Licence for Large Systems (Part No. IA-ENT) Enables all Advanced features and not limited in size

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:



**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.

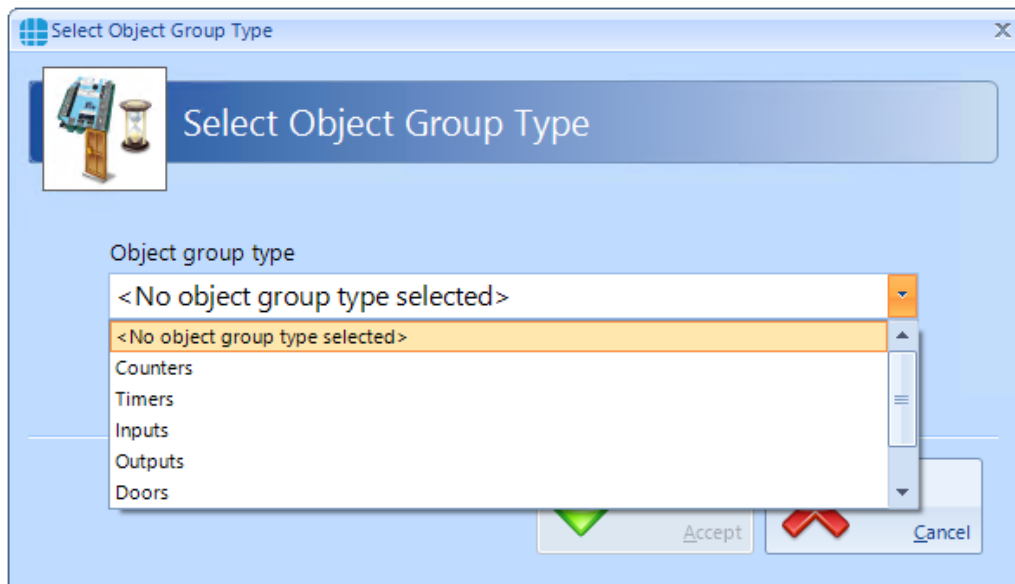
## 19.1 Object Groups

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.

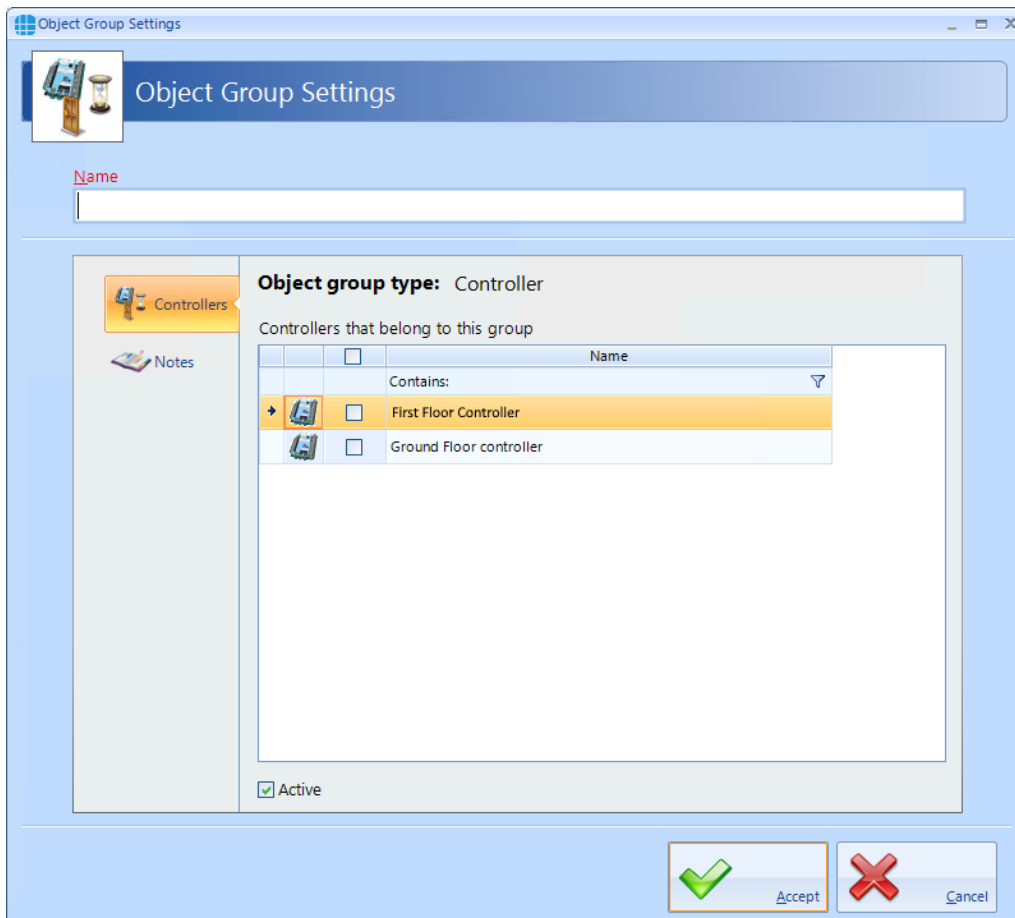
By grouping objects, it is possible to simultaneously change the status of every object in the group. Typical examples for this feature would be:

- 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 



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

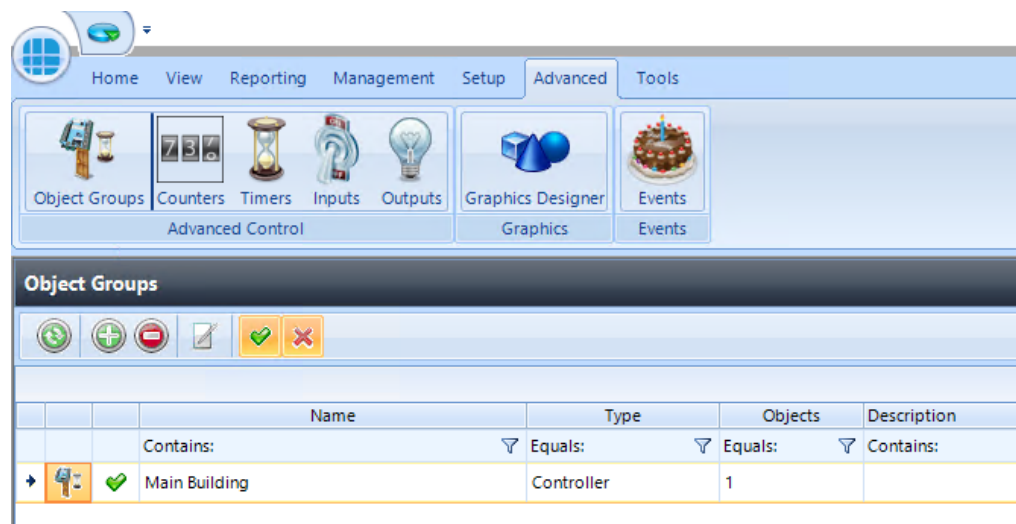


**Name:** Enter a meaningful name for the Object Group

**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



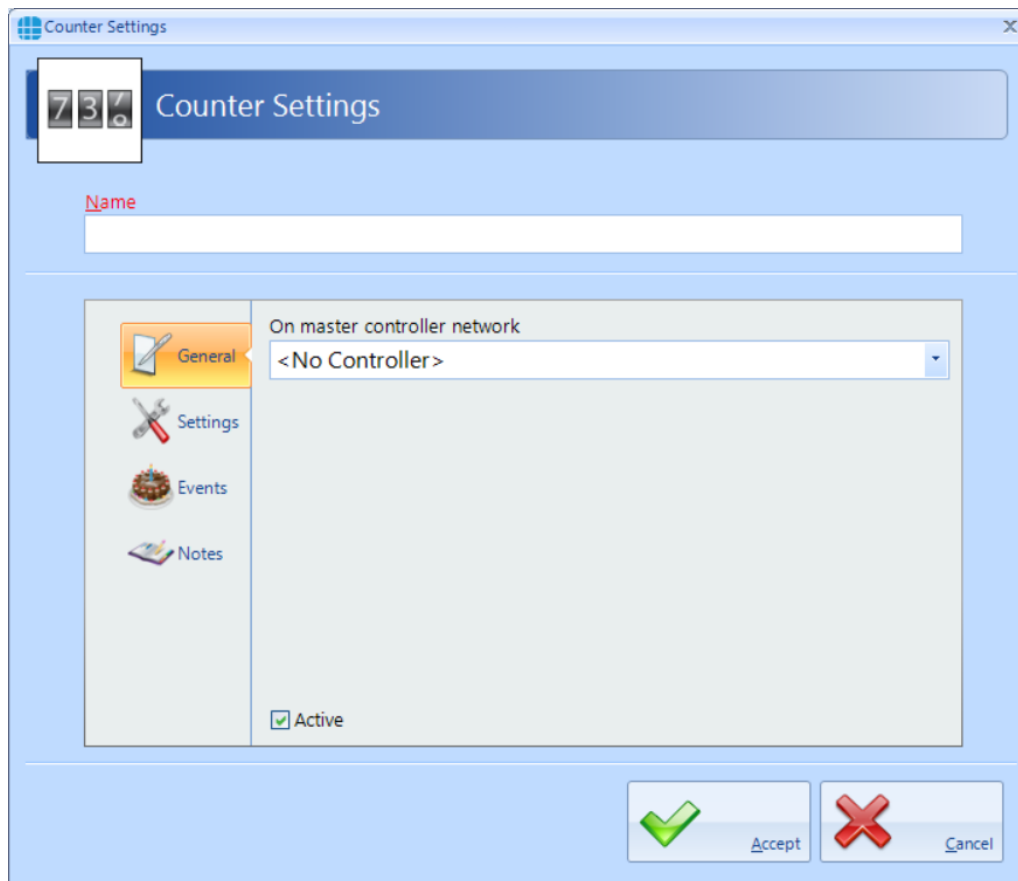
## 19.2 Counters

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

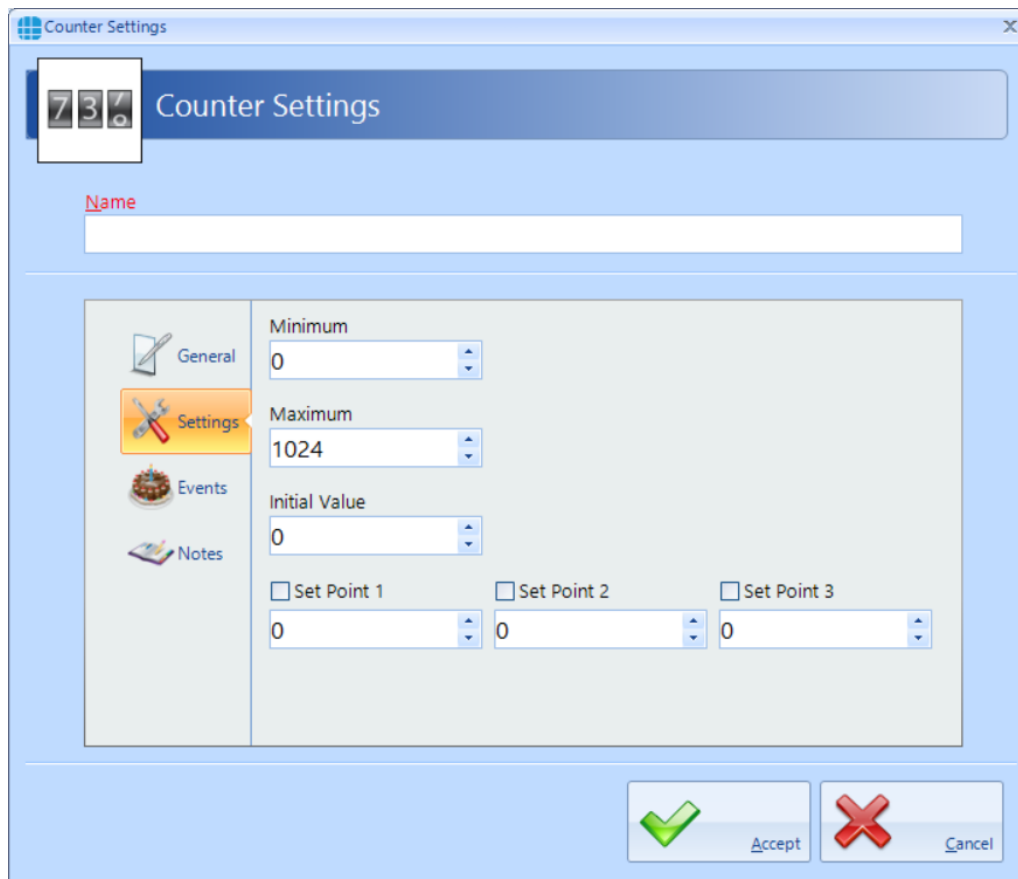


**Name:** Enter a meaningful name for the counter

**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



The image shows a 'Counter Settings' dialog box. At the top, there's a title bar with the text 'Counter Settings' and a close button. Below the title bar, there's a 'Name' label and an empty text field. The main area is divided into a left sidebar and a right content area. The sidebar has four icons: 'General' (notepad), 'Settings' (wrench and screwdriver, highlighted in orange), 'Events' (cake), and 'Notes' (book). The right content area has four sections: 'Minimum' with a spinner box set to 0, 'Maximum' with a spinner box set to 1024, 'Initial Value' with a spinner box set to 0, and 'Set Points' with three checkboxes labeled 'Set Point 1', 'Set Point 2', and 'Set Point 3', each followed by a spinner box set to 0. At the bottom right, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

**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:

Counters				
      				
			Name	Controller
			Contains:	Contains:
→			Occupancy counter	First Floor

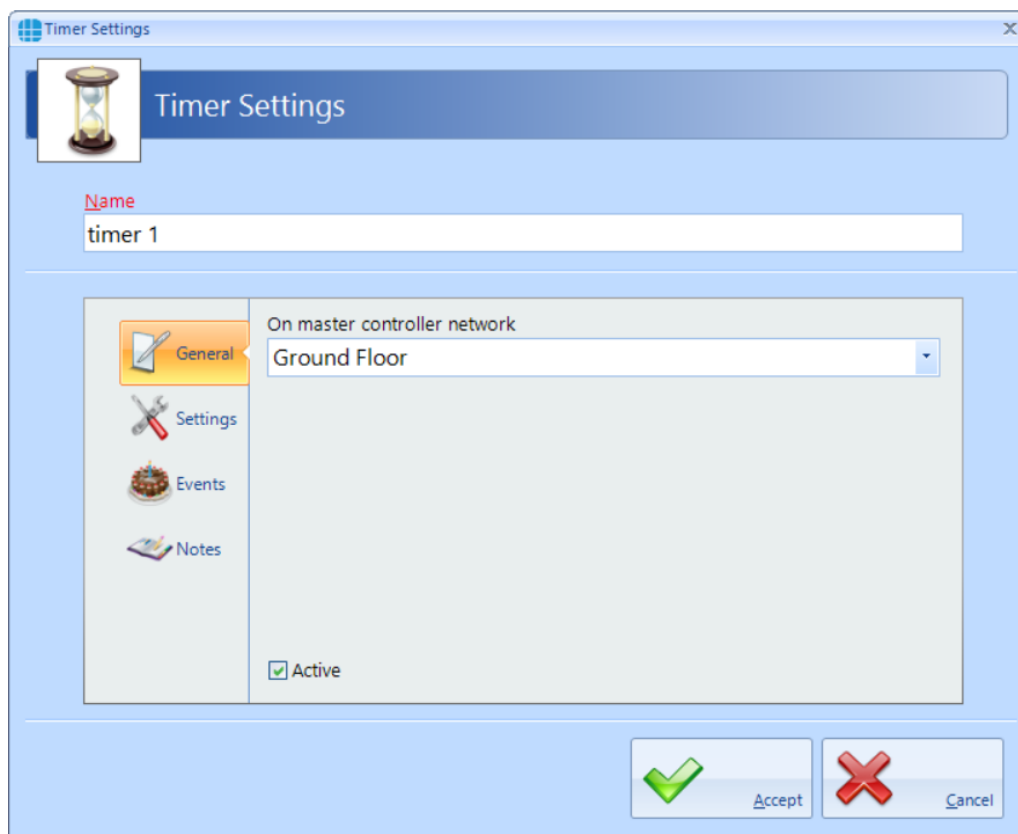
## 19.3 Timers

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 .



The **Timer Settings** dialog box is shown. It has a title bar with a close button. Below the title bar is a header area with a timer icon and the text "Timer Settings". The main area is divided into a left sidebar and a right content area. The sidebar has four tabs: **General** (selected), **Settings**, **Events**, and **Notes**. The **General** tab contains a **Name** field with the text "timer 1". Below this is a section titled "On master controller network" with a dropdown menu showing "Ground Floor". At the bottom of the sidebar is a checkbox labeled **Active** which is checked. The right content area is empty. At the bottom right of the dialog are two buttons: **Accept** (with a green checkmark icon) and **Cancel** (with a red X icon).

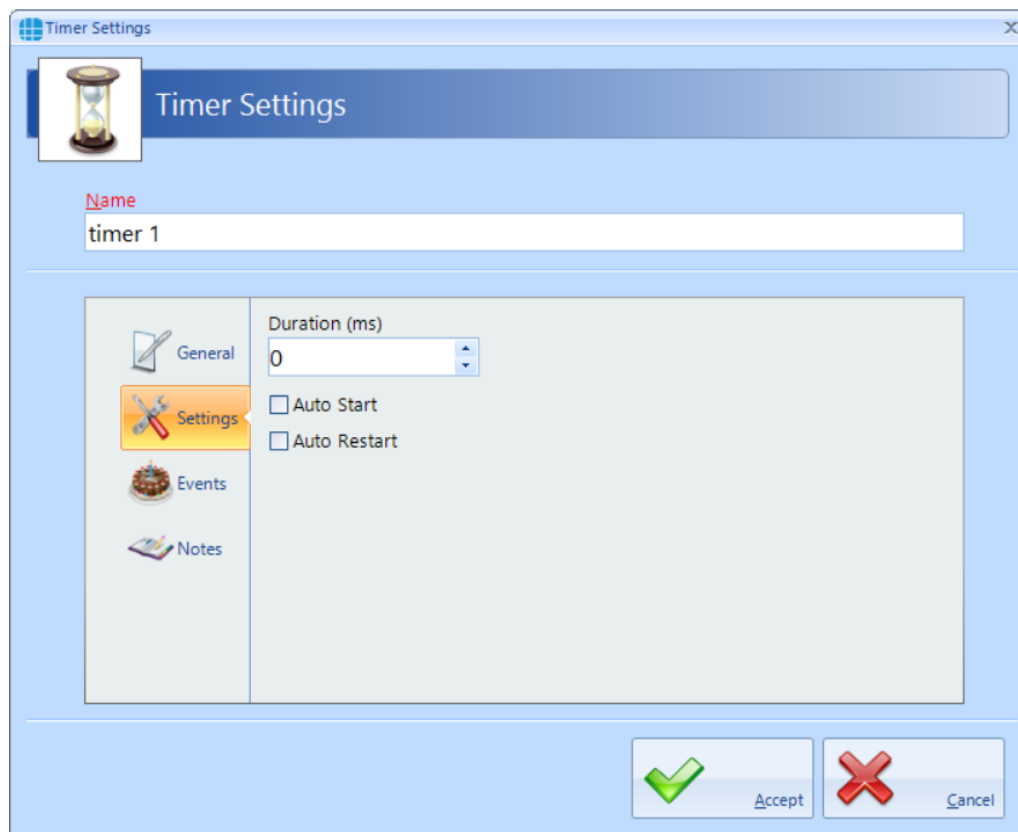
**Name:** Enter a meaningful name for the timer



**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.

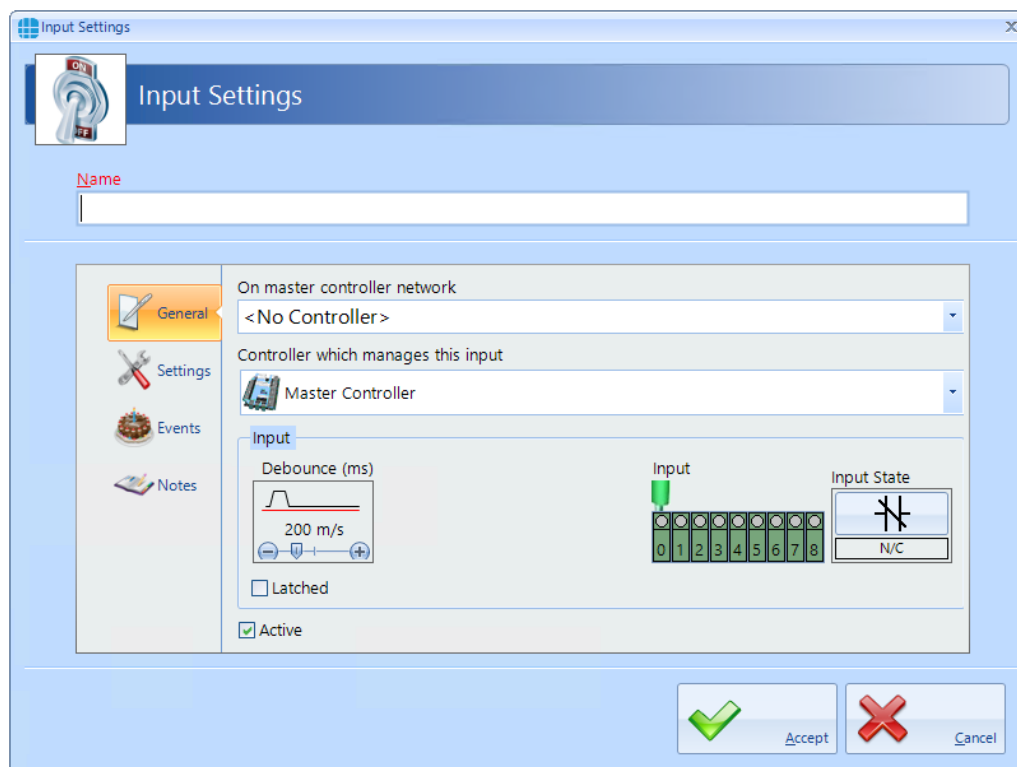
The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.

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

Timers				
Drag a column here to group by th				
	Name	Controller	Interval (ms)	
	Contains:	Contains:	Equals:	
+	timer 1	Ground Floor	5000	

## 19.4 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



The **Input Settings** dialog box is shown. It has a sidebar with icons for General (selected), Settings, Events, and Notes. The main area contains the following fields and controls:

- Name:** A text input field.
- On master controller network:** A dropdown menu currently showing "<No Controller>".
- Controller which manages this input:** A dropdown menu currently showing "Master Controller".
- Input:**
  - Debounce (ms):** A section with a graph showing a square wave, a value of "200 ms", and a checkbox for "Latched".
  - Input:** A row of 8 green circular indicators labeled 0 through 8. Indicator 0 is currently lit.
  - Input State:** A checkbox labeled "N/C" (Not Configured).
- Active:** A checked checkbox.
- Buttons:** "Accept" (green checkmark) and "Cancel" (red X).

**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

**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

The screenshot shows the 'Input Settings' window. On the left is a sidebar with icons for 'General', 'Settings' (highlighted), 'Events', and 'Notes'. The main area has a 'Name' field at the top. Below it are two tabs: 'Status' and 'Inhibit'. The 'Status' tab is selected, showing two text input fields: 'On Text' with the value 'ON' and 'Off Text' with the value 'OFF'. At the bottom right are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

**"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

The screenshot shows the 'Input Settings' dialog box with the 'Inhibit' tab selected. The 'Name' field is empty. The 'Status' tab is also visible. The 'Inhibit' section has a checkbox labeled 'Inhibit' which is currently unchecked. Below it, there are three dropdown menus: 'Inhibit Type' set to 'Input', 'Input' set to '<No Input>', and 'State' set to 'OFF'. At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

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” is on:

This screenshot shows the same 'Input Settings' dialog box, but now the 'Inhibit' checkbox is checked. The 'Inhibit Type' dropdown is set to 'Input', the 'Input' dropdown is set to 'REX Override', and the 'State' dropdown is set to 'ON'. The 'Accept' and 'Cancel' buttons are still present at the bottom right.

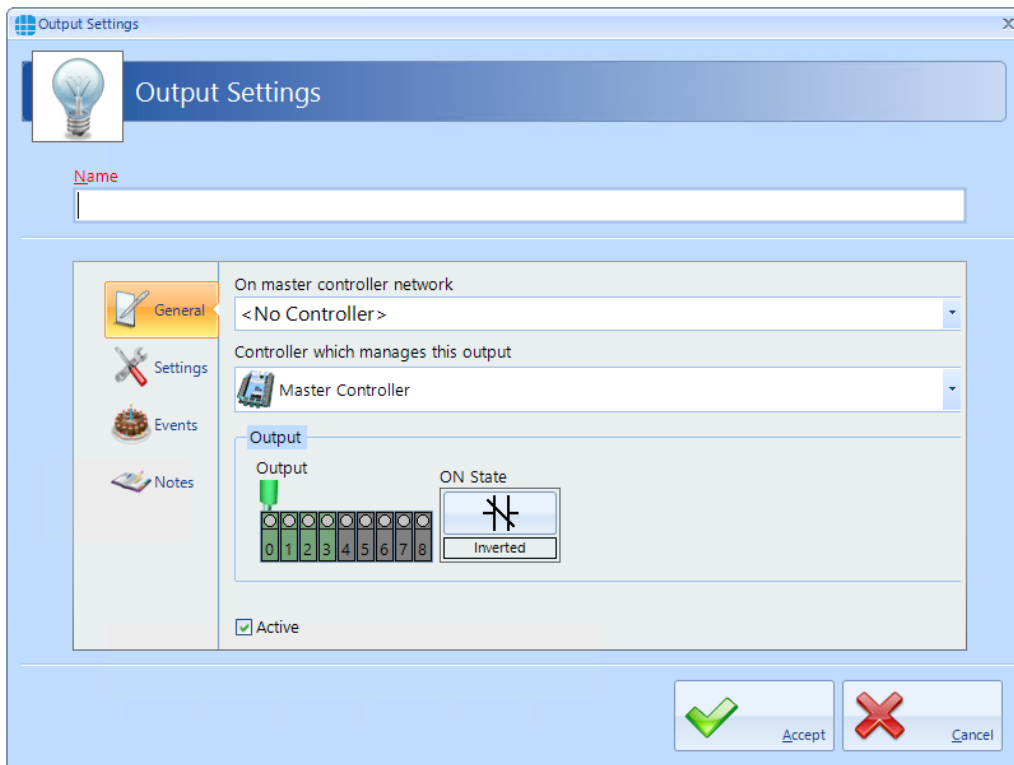
The **Events** tab in the side bar will indicate whether any Events have been configured for the selected Input.

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.

## 19.5 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

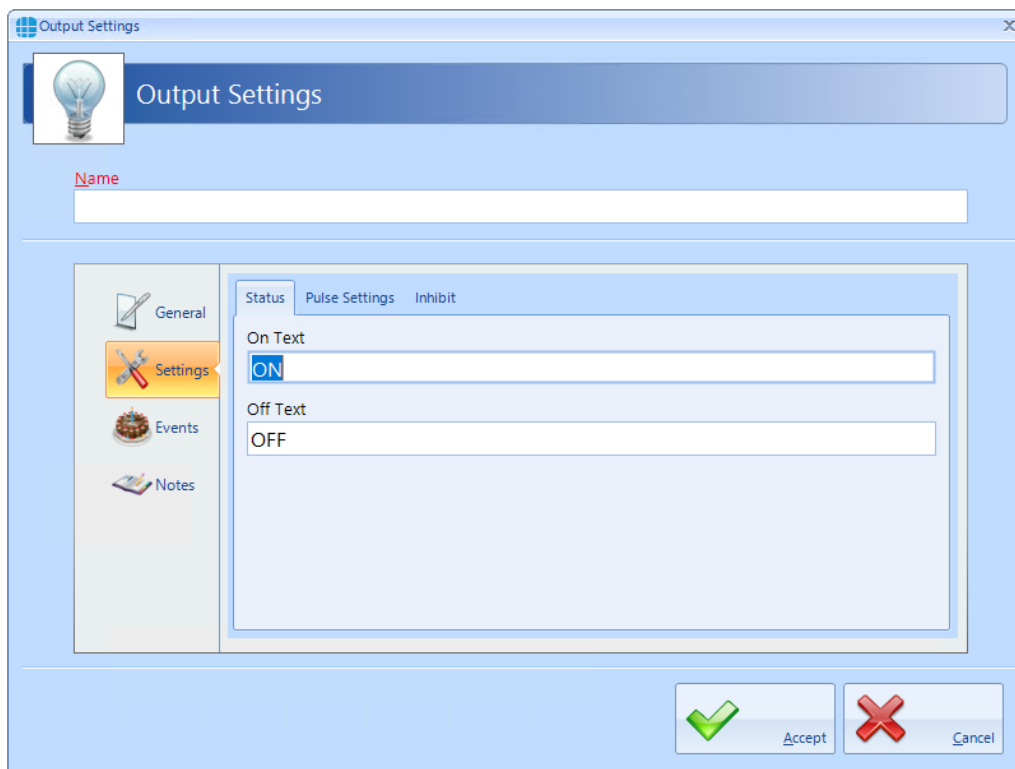
**Controller which manages this output:** Define whether the output is on the master controller or specify which Downstream device it relates to.

**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)

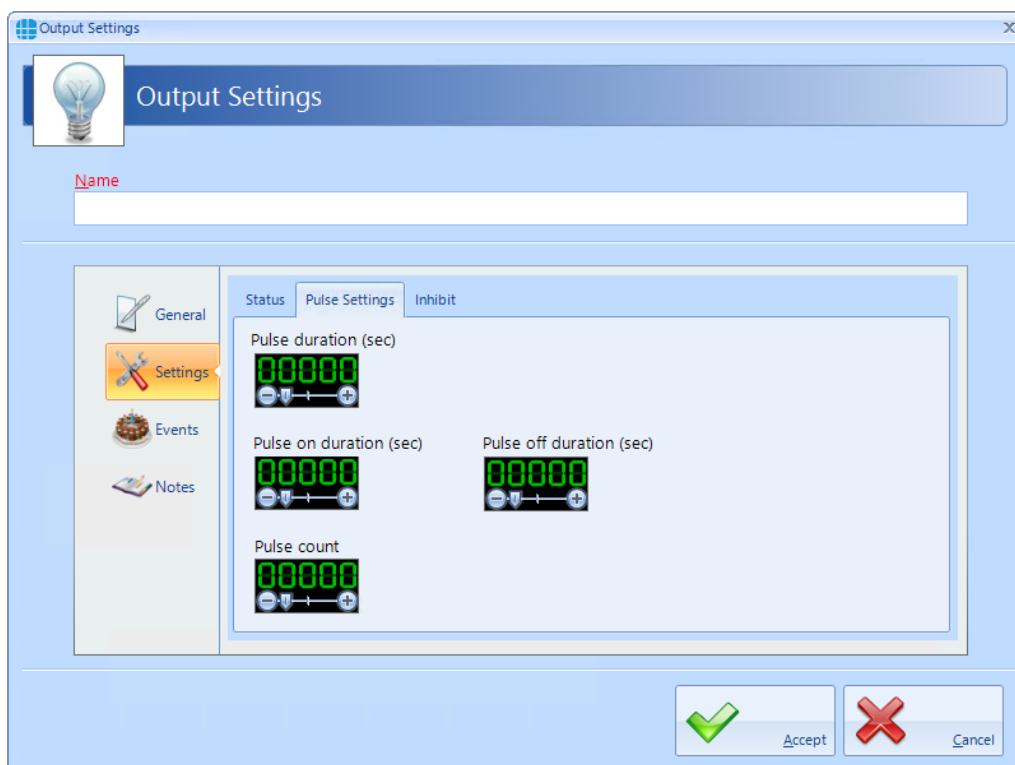
Ensure that **"Active"** is selected for the output to work.

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)

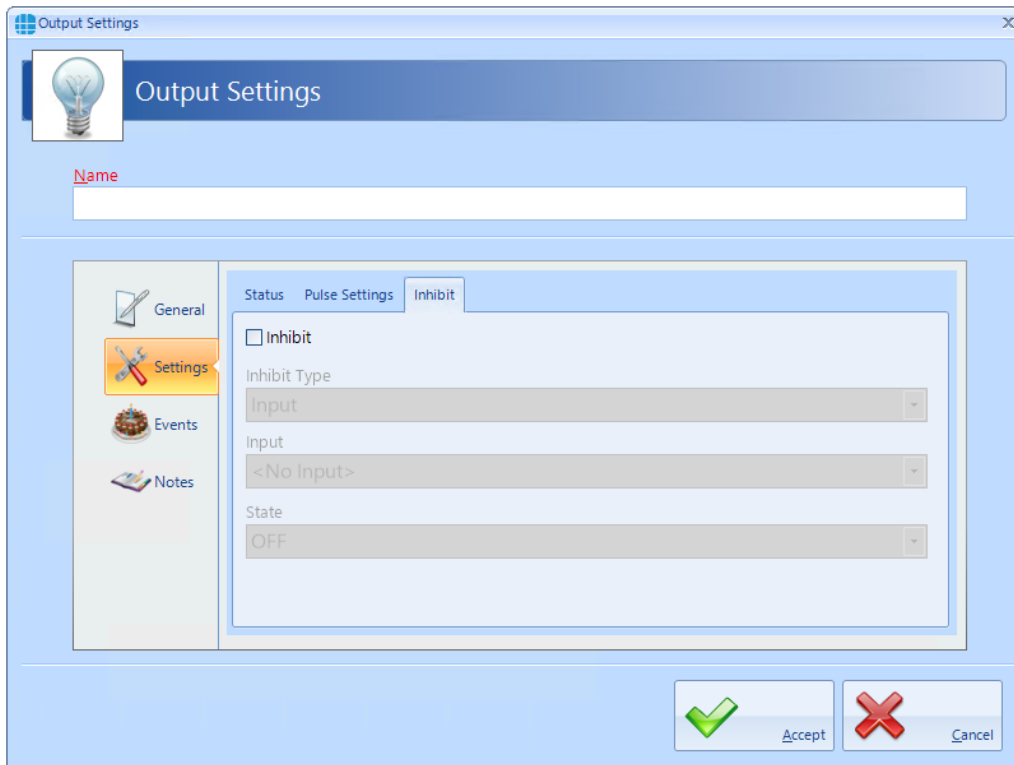
Select the "**Pulse Settings**" tab:



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:



The screenshot shows the 'Output Settings' dialog box with the 'Inhibit' tab selected. The dialog has a title bar 'Output Settings' and a close button. Below the title bar is a 'Name' field. On the left is a sidebar with icons for 'General', 'Settings', 'Events', and 'Notes'. The main area has three tabs: 'Status', 'Pulse Settings', and 'Inhibit'. The 'Inhibit' tab is active, showing an 'Inhibit' checkbox, an 'Inhibit Type' dropdown menu set to 'Input', an 'Input' dropdown menu set to '<No Input>', and a 'State' dropdown menu set to 'OFF'. At the bottom right are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

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.

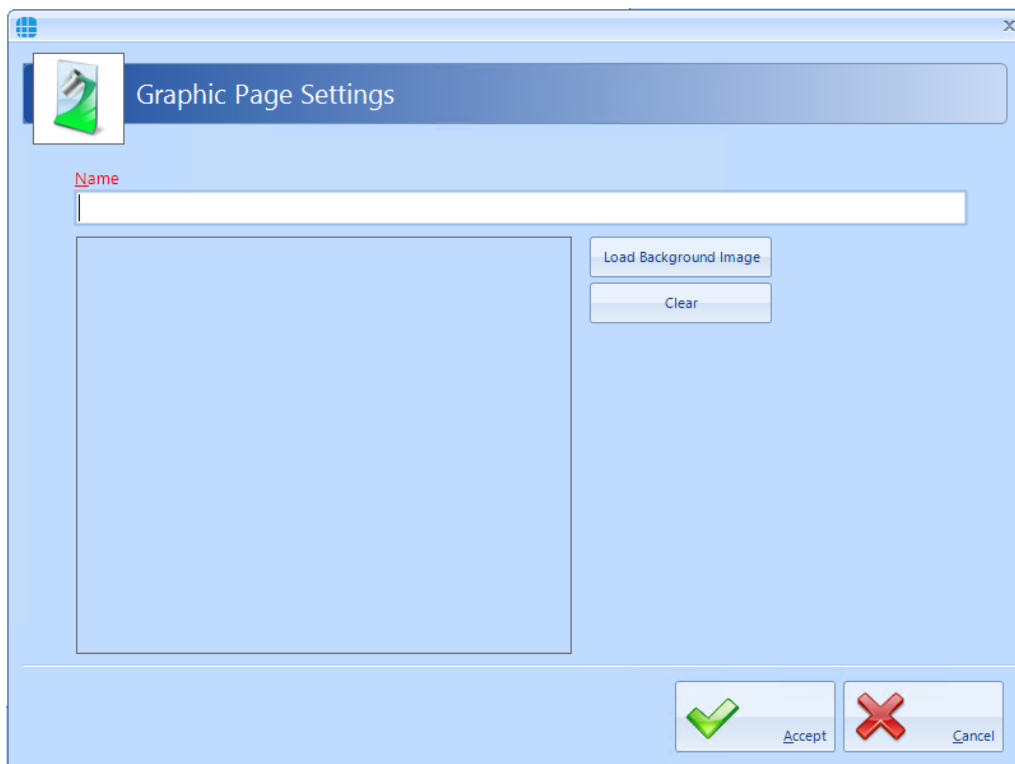
## 19.6 Graphics Designer

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.

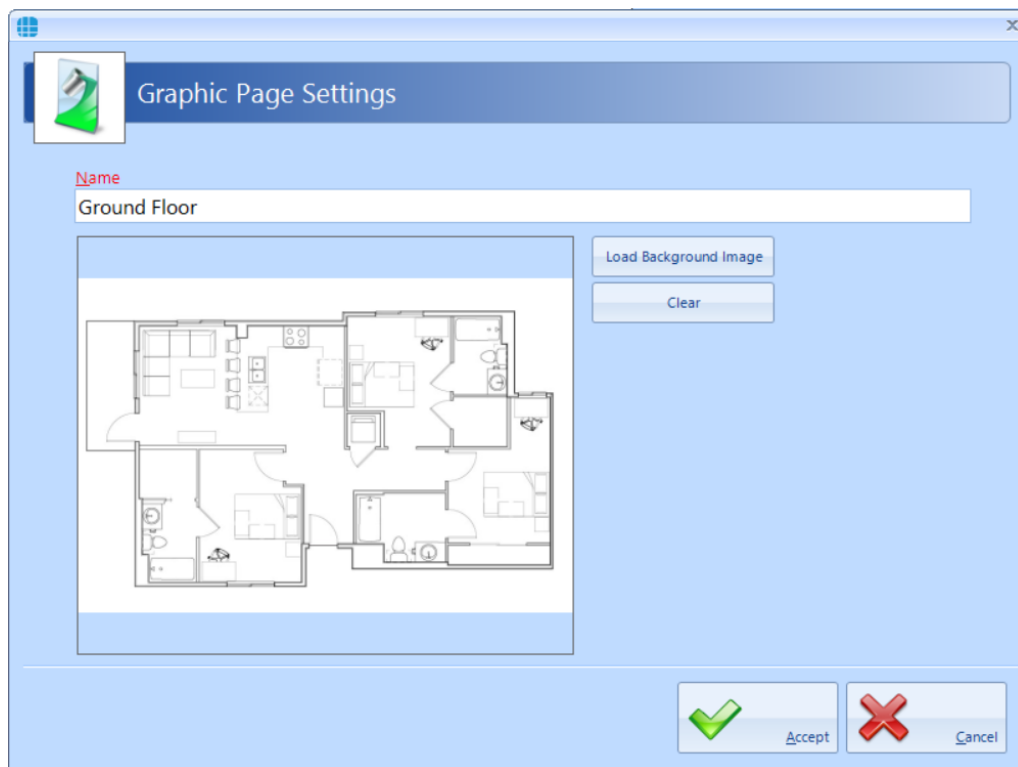
Actions can be created to change the state of any object on any page in response to an event.

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]**



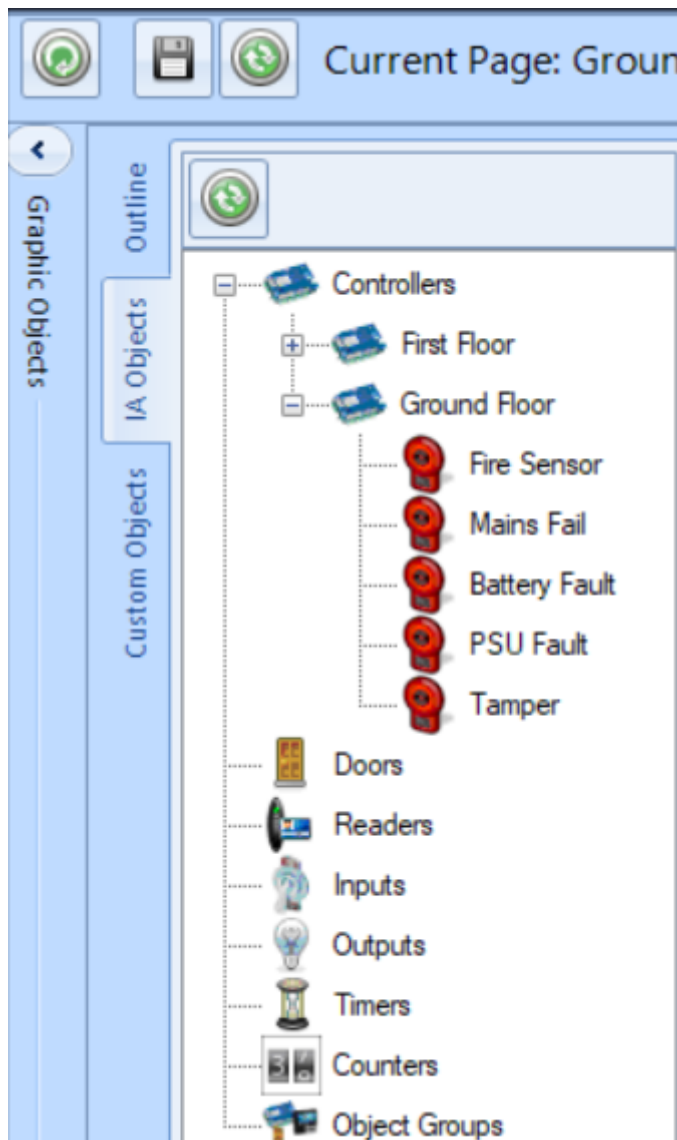


Click **Accept** and repeat to create all the required pages.

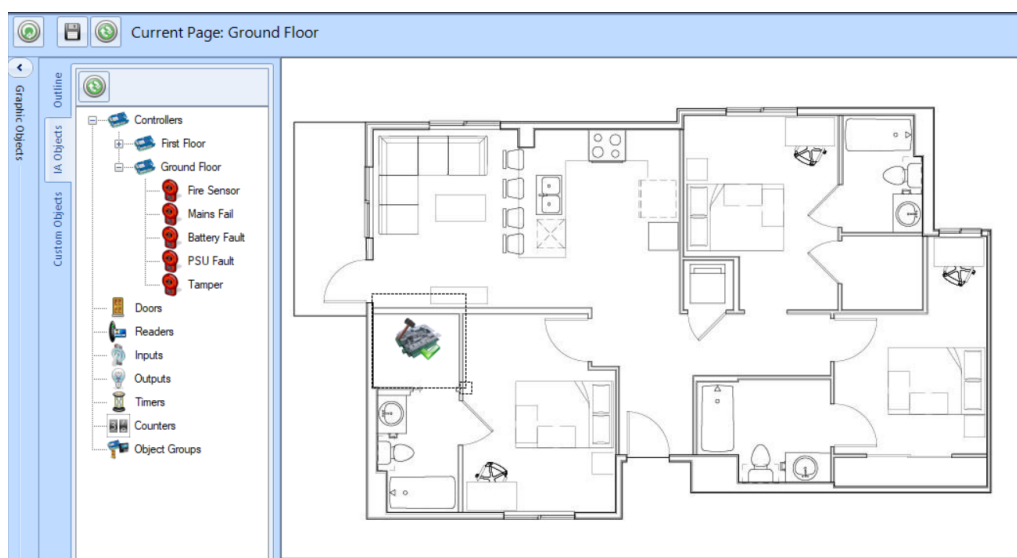
Next, we will add objects to a page.

### 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.



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

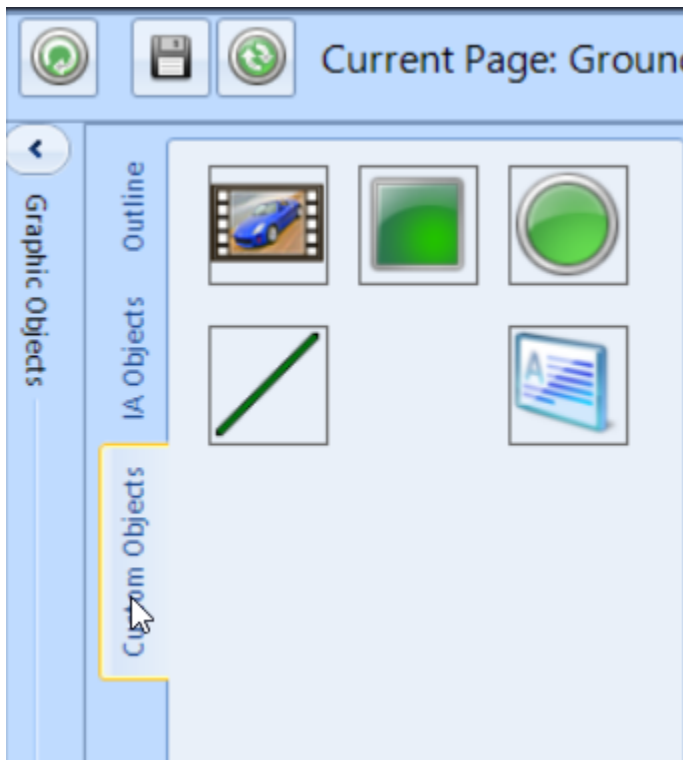


With IA Object, all the Events and Actions required to support this object are created automatically.

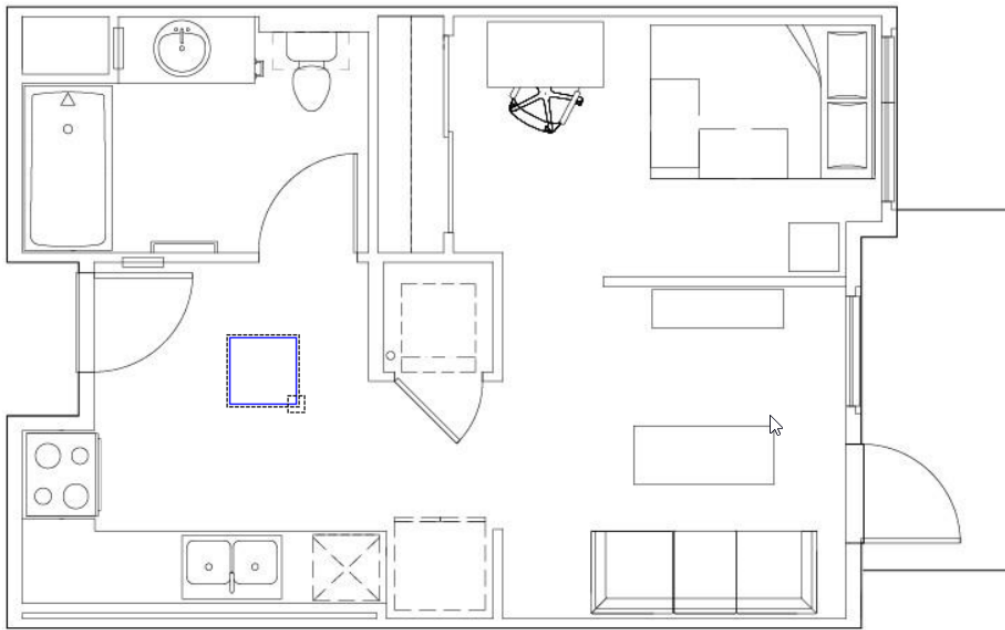
Place other objects onto the image as required, and click the **[Save]** button when done.

### Custom Objects

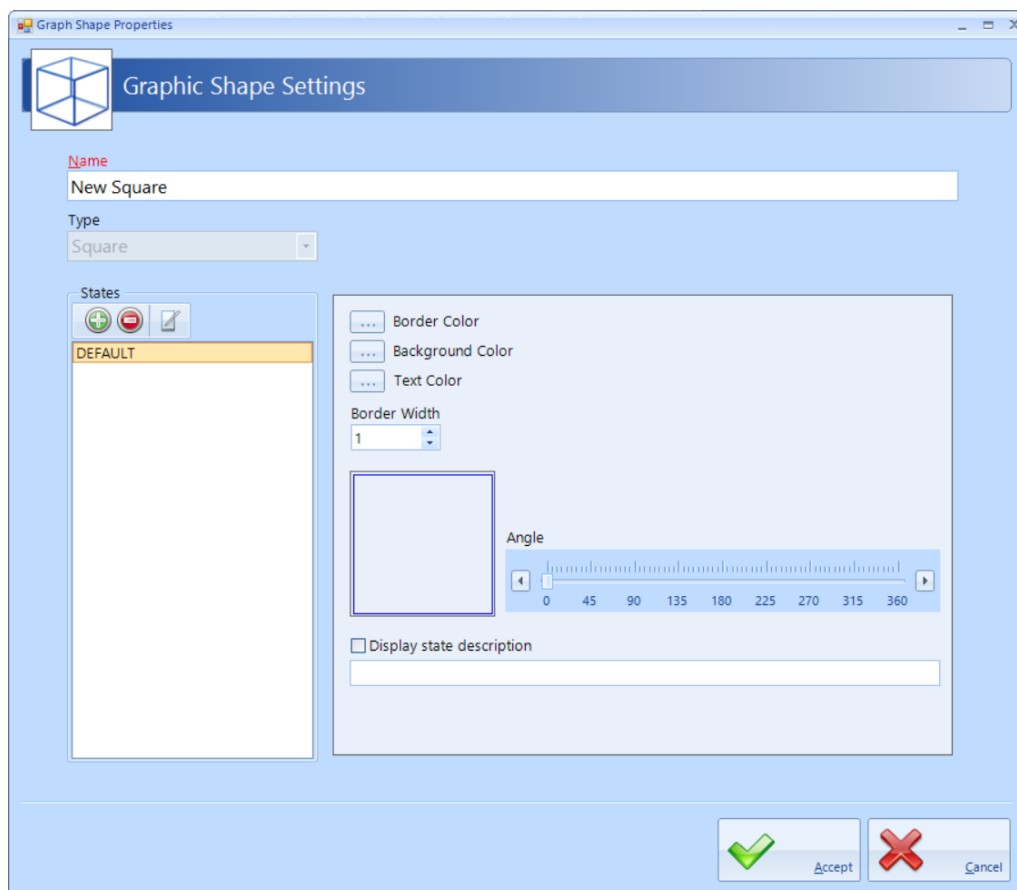
Select the required page so the floorplan is visible, then select the **Custom Objects** tab. A list will appear showing the object types available. These include Image, Oblong, Ellipse, Line and Textbox



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



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



**Name:** Give the object a meaningful name

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.

## 19.7 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

**Action Wizard**

Select object type that will generate the event

**Controller based objects**

- ☒ Counter
- ☐ Timer
- ☐ Input
- ☐ Output
- ☐ Time zone

**PC based objects**

- ☐ Access Log
- ☐ Person
- ☐ Group

Select an **EVENT** for which you want to create **ACTIONS**

**EVENT**

SELECT TYPE

Back Next Cancel

Accept Cancel

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:

**Select the event for selected counter (counter 1)**

- ☒ Change
- ☐ Set Point 1 <
- ☐ Set Point 1 =
- ☐ Set Point 1 >
- ☐ Set Point 2 <
- ☐ Set Point 2 =
- ☐ Set Point 2 >
- ☐ Set Point 3 <
- ☐ Set Point 3 =
- ☐ Set Point 3 >

Timers:

**Select the event for selected timer (timer 1)**

- ☒ Expire

Inputs:

Select the event for selected input (input 1)

- ☒ ON  
☐ OFF

Outputs:

Select the event for selected output (output 1)

- ☒ ON  
☐ OFF

Time Zones:

Select the event for selected time zone (Time Zone 1)

- ☒ Active  
☐ Inactive

Select controller

Ground Floor

< No Controller Selected >

First Floor

Ground Floor

Doors:

Select the event for selected door (door 1)

- ☒ Locked  
☐ Unlocked  
☐ Opened  
☐ Closed  
☐ Forced open  
☐ Did not open  
☐ Door did not close

Card Readers:

**Select the event for selected reader (door 1 In Reader)**

- ☒ Allow
- ☐ Deny

Controllers:

**Select the event for selected controller (192.168.3.231)**

- |  |   |                                     |
|--|---|-------------------------------------|
| <input checked="" type="radio"/> Connect | <input type="radio"/> Fire sensor on    | <input type="radio"/> PSU fault on  |
| <input type="radio"/> Disconnect         | <input type="radio"/> Fire sensor off   | <input type="radio"/> PSU fault off |
| <input type="radio"/> Lockdown Level 1   | <input type="radio"/> Mains fail on     | <input type="radio"/> Tamper on     |
| <input type="radio"/> Lockdown Level 2   | <input type="radio"/> Mains fail off    | <input type="radio"/> Tamper off    |
| <input type="radio"/> Lockdown cleared   | <input type="radio"/> Battery fault on  |                                     |
|  | <input type="radio"/> Battery fault off |                                     |

Persons:

**Select the event for selected person (Smith, John)**

- ☒ Token swiped at any card reader
- ☐ Access allowed at any card reader
- ☐ Access denied at any card reader
- ☐ Token swiped at specific card reader
- ☐ Access allowed at a specific card reader
- ☐ Access denied at a specific card reader

Groups:

**Select the event for selected group (Staff)**

- ☒ Token swiped at any card reader
- ☐ Access allowed at any card reader
- ☐ Access denied at any card reader
- ☐ Token swiped at specific card reader
- ☐ Access allowed at a specific card reader
- ☐ Access denied at a specific card reader

PC Events



Access Log – Person:

**Select the event for selected person (Smith, John)**



☐ Enters premises

☐ Leaves premises

☒ Arrives late

☐ Leaves early

Enters premises after

09:00  

Access Log – Group:

**Select the event for selected group (Production)**



☐ Enters premises

☐ Leaves premises



☐ Arrives late

☒ Leaves early

Leaves premises between

16:00  

and

17:00  

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

Controller actions:

Counters:

**Select the action for selected counter (counter 1)**

☒ Reset

☐ Increment

☐ Decrement

☐ Set

☐ Increment by

☐ Decrement by

Timers:

**Select the action for selected timer (timer 1)**

☒ Start

☐ Stop

☐ Reset

☐ Restart

Inputs:

**Select the action for selected input (input 1)**

☒ Clear Latch

Outputs:

**Select the action for selected output (output 1)**

☒ Set On

☐ Set Off

☐ Toggle

☐ Pulse

☐ Pulse On

☐ Pulse Off

☐ Pulse Train

Doors:

**Select the action for selected door (door 1)**

- ☒ Open
- ☐ Force Open
- ☐ Force Close
- ☐ Disable REX A
- ☐ Enable REX A
- ☐ Disable REX B
- ☐ Enable REX B

Card Readers:

**Select the action for selected reader (door 1 In Reader)**

- ☒ Allow Access
- ☐ Deny Access
- ☐ Enable
- ☐ Disable

Controllers:

**Select the action for selected controller (192.168.3.231)**

- ☒ Clear lockdown
- ☐ Set lockdown 1
- ☐ Set lockdown 2
- ☐ Set Fire State
- ☐ Clear Fire State

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:

**Select the action**

☐ Set visible page: New Page


☒ Select State: ALLOWED

☐ Reset the state to the 1st state in the list after  seconds

☐ Select Next State   ☐ Select Prev State

**Object Outline**

- New Page
  - door 1 In Reader
    - UNKNOWN
    - ALLOWED**
    - DENIED



Camera:

**Select the action for selected camera (camera 1)**

☒ Take picture

Custom message

System Log:

**Select the action**

☒ Add custom entry to system log

Tags

Custom message

Report:

**Select the action**

☒ Print report to printer

Select report

<NO REPORT SELECTED>

<NO REPORT SELECTED>

Fire Roll-call Report

Access Log Report

System Log Report

T/A Log Report

Access Control Report

Email:

**Select the action**

☒ Send email using template

<NO TEMPLATE SELECTED>

Tags [COUNTER:NAME]

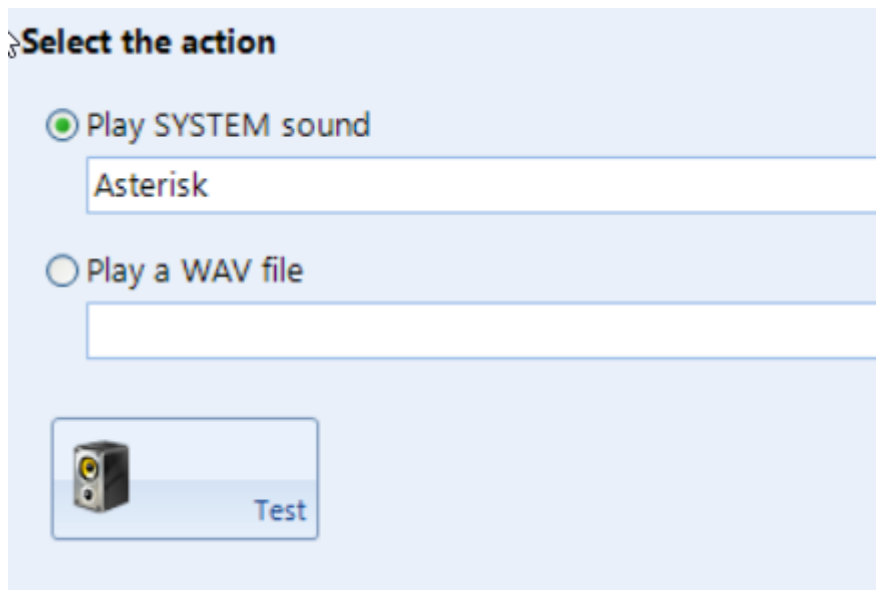
Subject

Body

☐ Attach Report Fire Roll-call Report

Report Query <No Query Selected>

Sound:




**Select the action**

☒ Play SYSTEM sound

Asterisk

☐ Play a WAV file

 Test

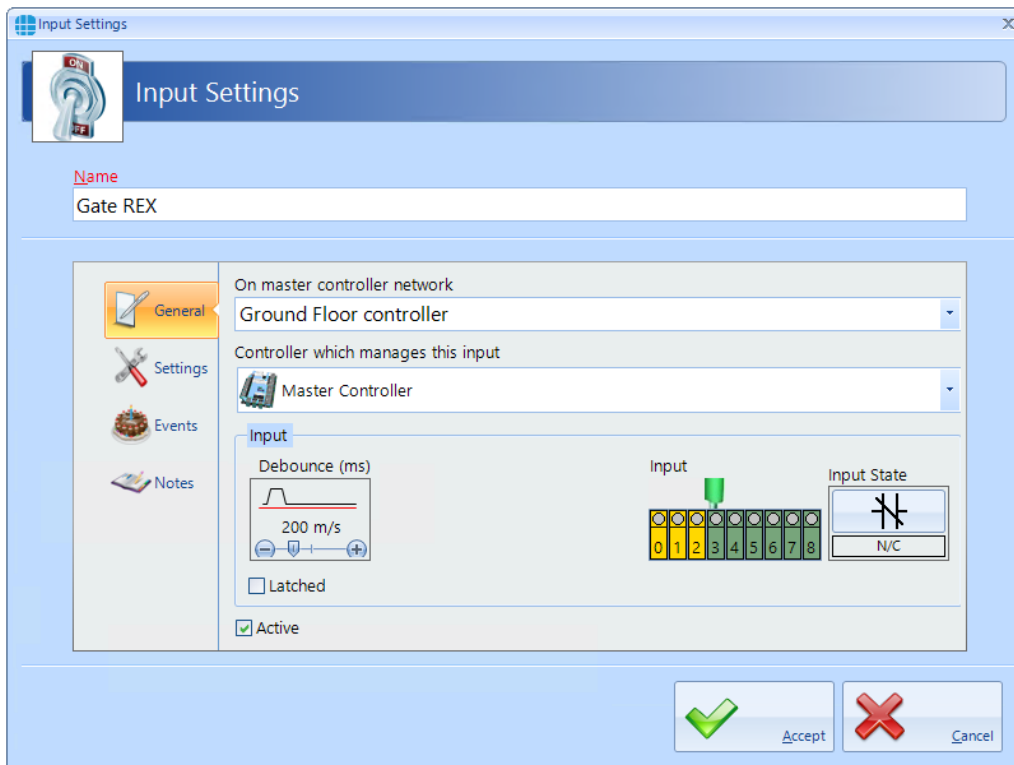
**NOTE:** the Events wizard allows multiple Actions for each event.

## 19.8 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.

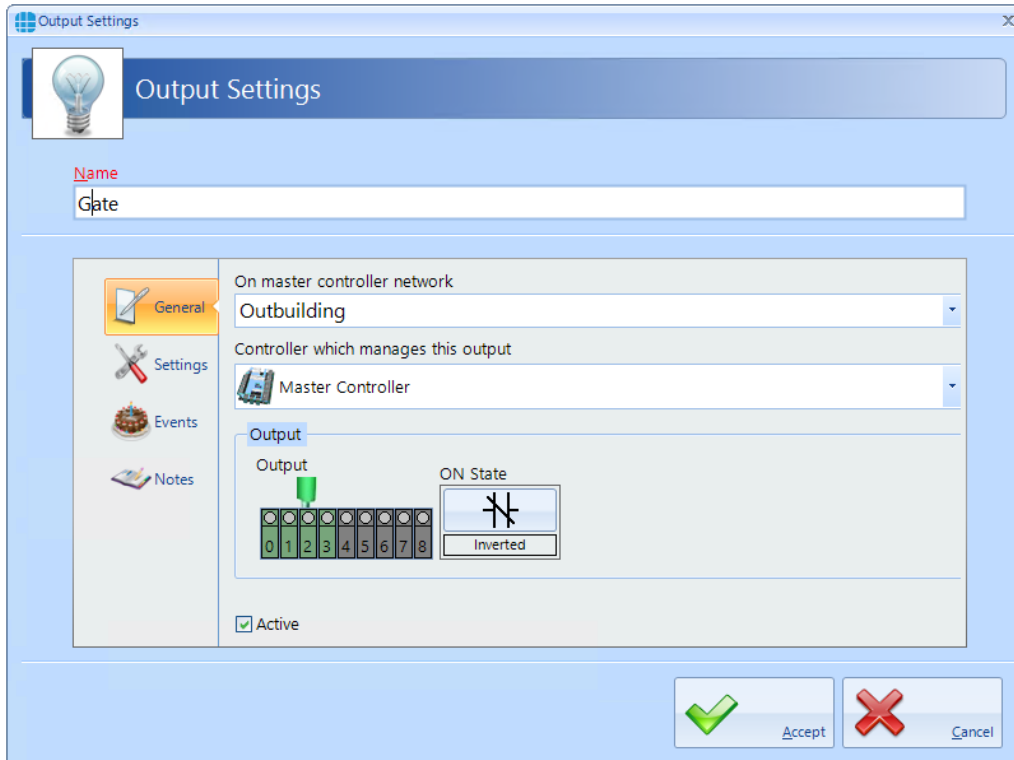
Create an input called "Gate REX" on "Ground Floor" controller



The **Input Settings** dialog box is shown. The **Name** field contains "Gate REX". The **General** tab is selected. The **On master controller network** dropdown is set to "Ground Floor controller". The **Controller which manages this input** dropdown is set to "Master Controller". The **Input** section shows a **Debounce (ms)** value of 200 m/s, a **Latched** checkbox, and an **Active** checkbox. The **Input** section also displays a visual representation of the input state, showing a green bar on the "Input" label and a green bar on the "Input State" label. The **Input State** is currently set to "N/C".

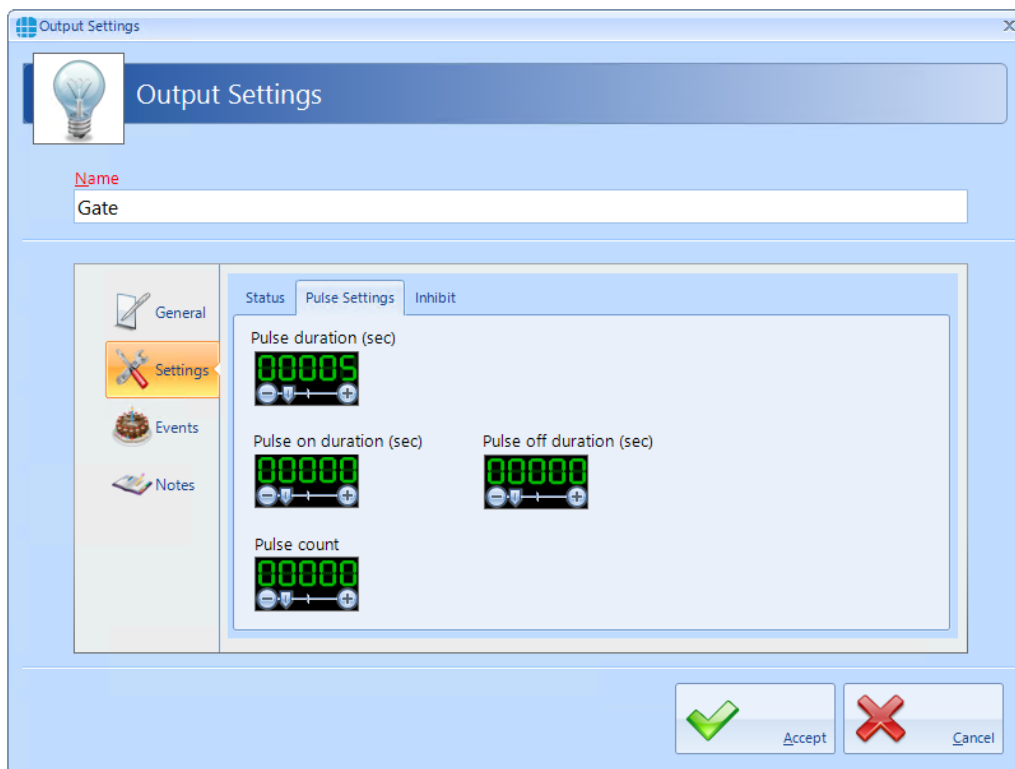
Buttons: **Accept** (green checkmark) and **Cancel** (red X).

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

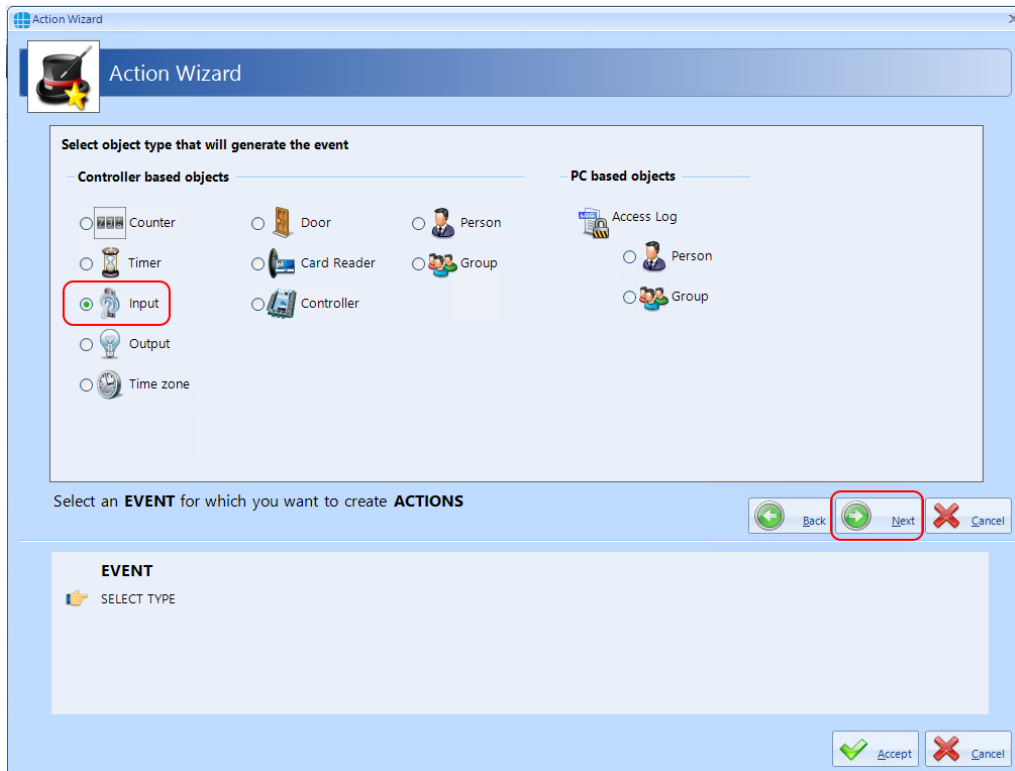


The **Output Settings** dialog box is shown. The **Name** field contains "Gate". The **General** tab is selected. The **On master controller network** dropdown is set to "Outbuilding". The **Controller which manages this output** dropdown is set to "Master Controller". The **Output** section shows a visual representation of the output state, showing a green bar on the "Output" label and a green bar on the "ON State" label. The **ON State** is currently set to "Inverted".

Buttons: **Accept** (green checkmark) and **Cancel** (red X).



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





Action Wizard

Select the INPUT that will generate the event

	Name
Contains:	
+	Gate REX
	REX Override

Select an **EVENT** for which you want to create **ACTIONS**

Back Next Cancel

**EVENT**  
Type: Input  
SELECT INPUT

Accept Cancel

Action Wizard

Select the event for selected input (Gate REX)

☒ ON  
☐ OFF

Select an **EVENT** for which you want to create **ACTIONS**

Back Next Cancel

**EVENT**  
Type: Input  
Gate REX  
SELECT EVENT

Accept Cancel

Action Wizard

Select object type that has to perform the action

**Controller based objects**

- ☐ Counter
- ☐ Timer
- ☐ Input
- ☒ Output
- ☐ Door

**PC based objects**

- ☐ Card Reader
- ☐ Controller
- ☐ Object Group
- ☐ Person
- ☐ Group
- ☐ Graphic objects
- ☐ Camera
- ☐ System log
- ☐ Report
- ☐ Email
- ☐ Sound

Select an Action for the event 'Gate REX = On'

Back Next Cancel

EVENT	ACTION
Type: Input	SELECT TYPE
Gate REX	
Event: On	

Accept Cancel

Action Wizard

Select the OUTPUT that has to perform the action

Name
Gate

Select an Action for the event 'Gate REX = On'

Back Next Cancel

EVENT	ACTION
Type: Input	Type: Output
Gate REX	SELECT OUTPUT
Event: On	

Accept Cancel

**Action Wizard**

Select the action for selected output (Gate)

- ☐ Set On
- ☐ Set Off
- ☐ Toggle
- ☒ Pulse
- ☐ Pulse On
- ☐ Pulse Off
- ☐ Pulse Train

Select an Action for the event 'Gate REX = On'

Back Finish Cancel

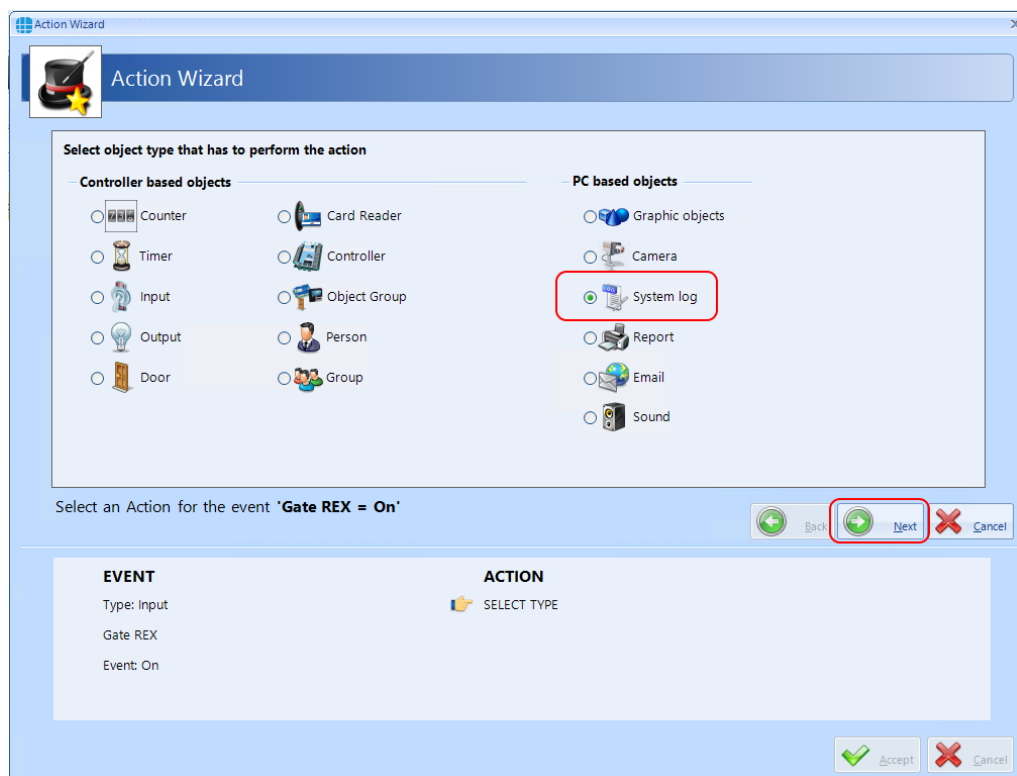
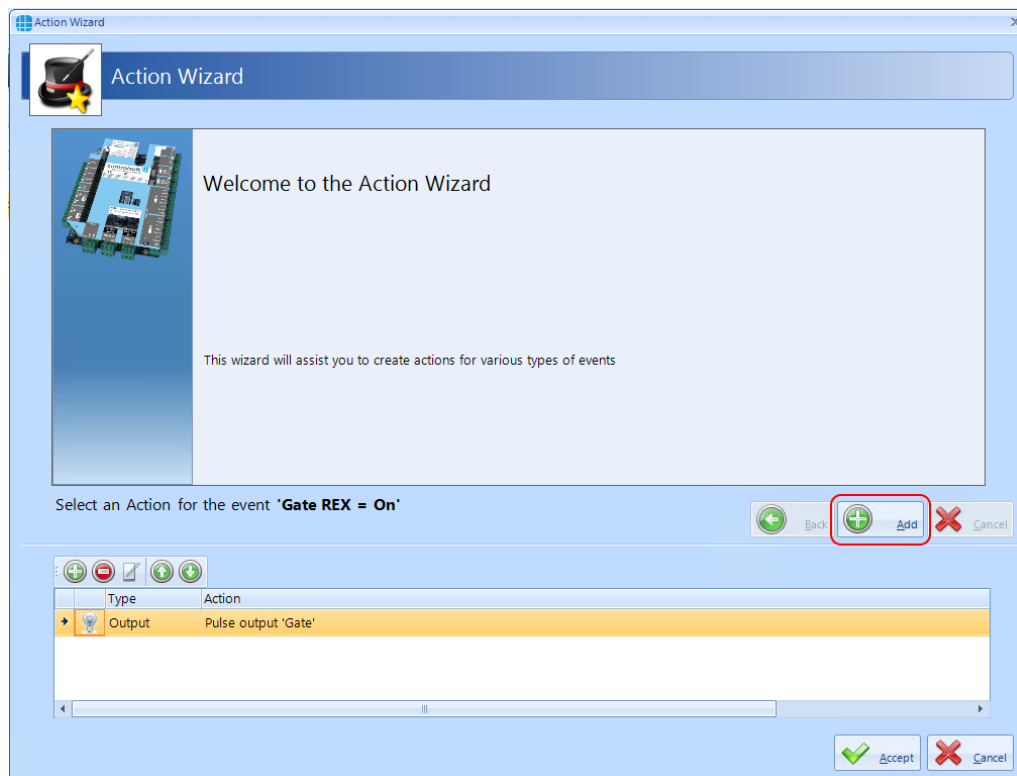
EVENT	ACTION
Type: Input	Type: Output
Gate REX	Gate
Event: On	SELECT ACTION

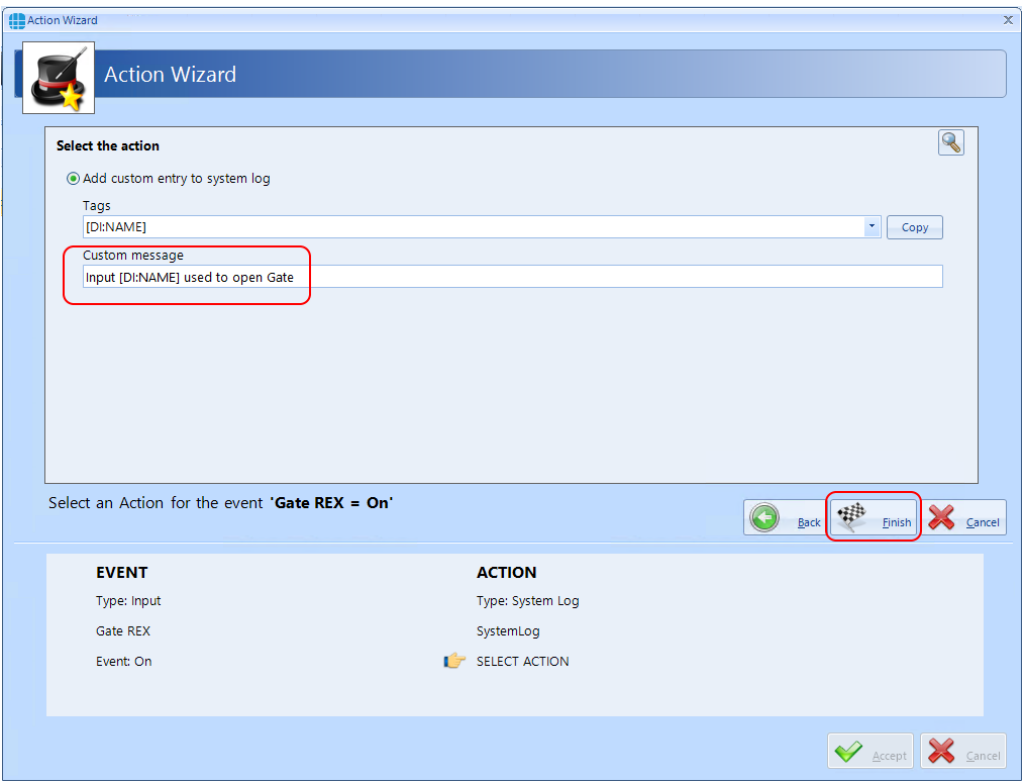
Accept Cancel

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

Events			
	Name	Event	Action
	Contains:	Contains:	Contains:
	Gate REX	On	Pulse output 'Gate'

**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:





Name	Event	Action
Contains:	Contains:	Contains:
Gate REX	On	Pulse output 'Gate' Add custom message 'Input [Di:NAME] used to release "Gate" to system log

**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:

Events			
Drag			
Name	Event	Action	
Contains:	Contains:	Contains:	
Chiller In Reader	Access allowed	Reset timer 'Chiller Timer' Start timer 'Chiller Timer'	
Chiller OUT Reader	Access allowed	Stop timer 'Chiller Timer' Reset timer 'Chiller Timer'	
Chiller Timer	Expire	Turn on output 'Chiller Alarm'	

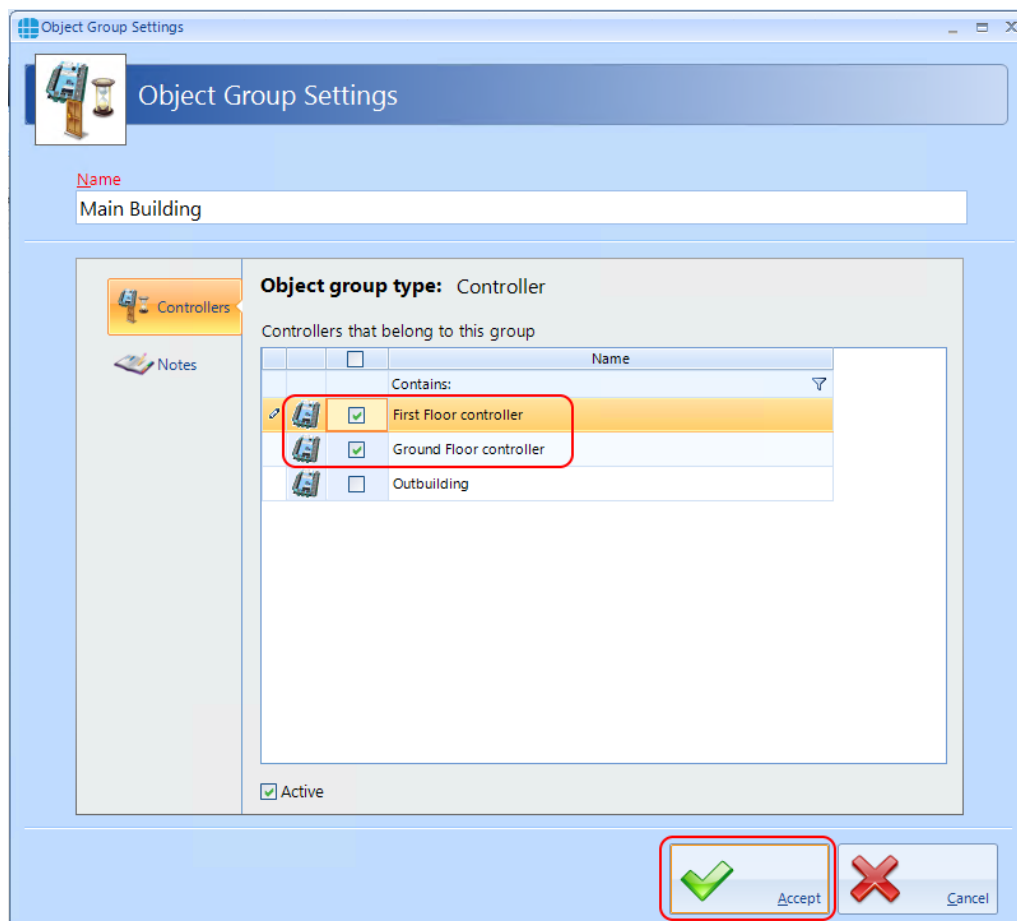
When someone is granted access into the chiller, the timer resets and starts to run (if the alarm is sounding, someone else entering the chiller will reset the timer which will silence the alarm)

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.

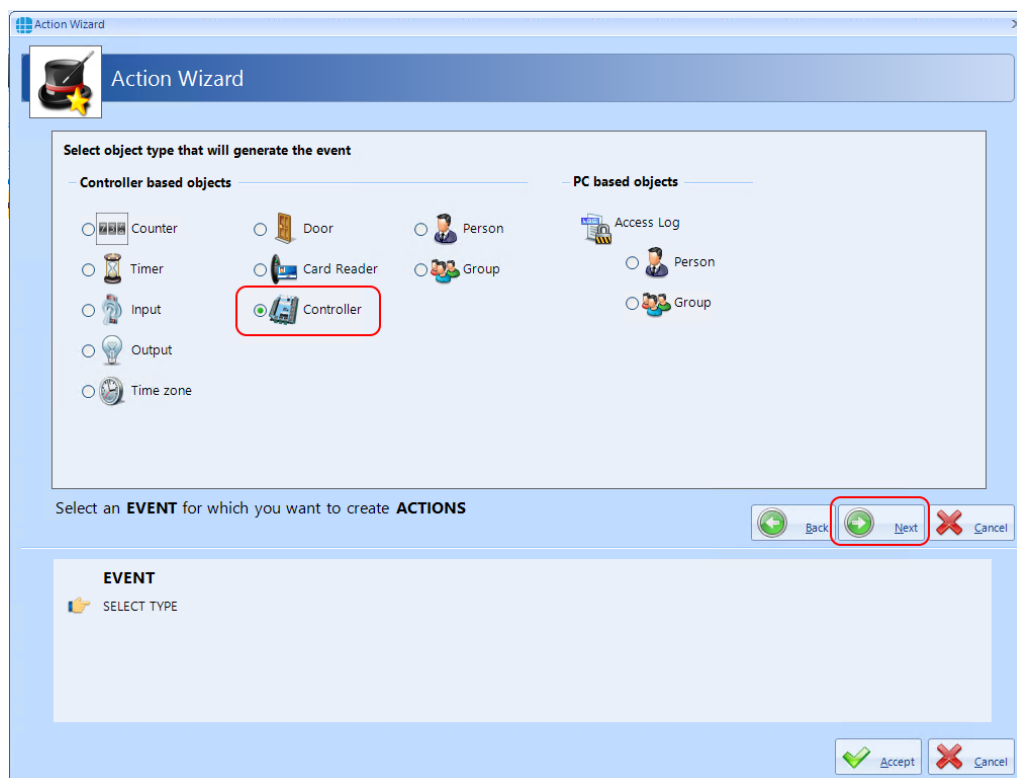
**EXAMPLE 3:** Detect a fire alarm from a controller connected to the main building fire alarm, then trigger a fire alarm on all other controllers in the same building, but not in the outbuildings.

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'



Action Wizard

Select the **CONTROLLER** that will generate the event

Name
Contains:
First Floor controller
<b>Ground Floor controller</b>
Outbuilding

Select an **EVENT** for which you want to create **ACTIONS**

Back Next Cancel

**EVENT**  
Type: Controller  
SELECT CONTROLLER

Accept Cancel

Action Wizard

Select the event for selected controller (**Ground Floor controller**)

<input type="radio"/> Connect	<input checked="" type="radio"/> Fire sensor on	<input type="radio"/> PSU fault on
<input type="radio"/> Disconnect	<input type="radio"/> Fire sensor off	<input type="radio"/> PSU fault off
<input type="radio"/> Lockdown Level 1	<input type="radio"/> Mains fail on	<input type="radio"/> Tamper on
<input type="radio"/> Lockdown Level 2	<input type="radio"/> Mains fail off	<input type="radio"/> Tamper off
<input type="radio"/> Lockdown cleared	<input type="radio"/> Battery fault on	
	<input type="radio"/> Battery fault off	

Select an **EVENT** for which you want to create **ACTIONS**

Back Next Cancel

**EVENT**  
Type: Controller  
Ground Floor controller  
SELECT EVENT

Accept Cancel



Action Wizard

Select object type that has to perform the action

**Controller based objects**

- ☐ Counter
- ☐ Timer
- ☐ Input
- ☐ Output
- ☐ Door
- ☐ Card Reader
- ☐ Controller
- ☒ Object Group
- ☐ Person
- ☐ Group

**PC based objects**

- ☐ Graphic objects
- ☐ Camera
- ☐ System log
- ☐ Report
- ☐ Email
- ☐ Sound

Select an Action for the event 'Ground Floor controller = Fire sensor on'

Back Next Cancel

EVENT	ACTION
Type: Controller	SELECT TYPE
Ground Floor controller	
Event: Fire sensor on	

Accept Cancel

Action Wizard

Select the OBJECT GROUP that has to perform the action


Name
Contains:
Main Building

Select an Action for the event 'Ground Floor controller = Fire sensor on'

Back Next Cancel

EVENT	ACTION
Type: Controller	Type: Object Group
Ground Floor controller	SELECT OBJECT GROUP
Event: Fire sensor on	

Accept Cancel



Action Wizard

Select the action for selected object group (Main Building)

☐ Clear lockdown

☐ Set lockdown 1


☐ Set lockdown 2


☒ Set Fire State

☐ Clear Fire State

Select an Action for the event 'Ground Floor controller = Fire sensor on'

Back

 Finish

 Cancel

EVENT

Type: Controller


Ground Floor controller


Event: Fire sensor on


ACTION

Type: Object Group

Main Building

 SELECT ACTION

 Accept

 Cancel

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

Events



Drag a column here to group by

	Name	Event	Action
	Contains:	Contains:	Contains:
	Ground Floor	Fire sensor on	Set the fire alarm state on object group 'Main Building'
	Ground Floor	Fire sensor off	Clear the fire alarm state on object group 'Main Building'

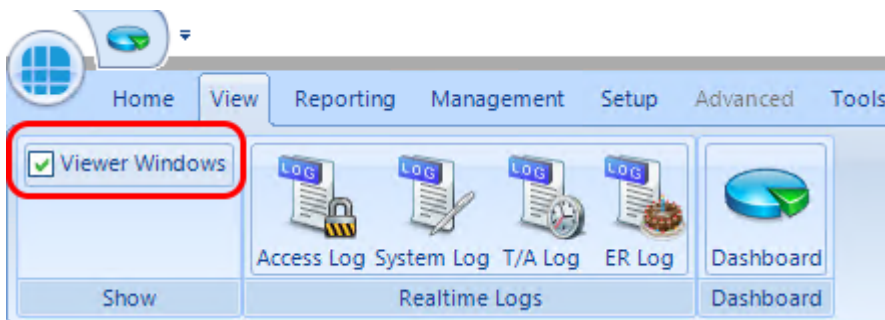
## Event Viewers and Reports

## 20 Event Viewers and Reports

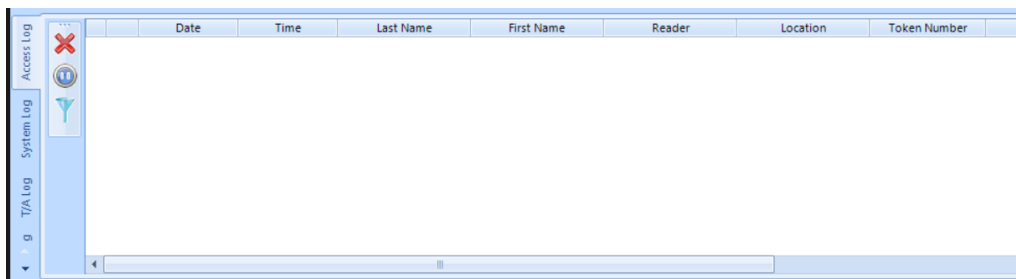
The Event Viewer in Identity Access software is a powerful tool for analysing system activity.

### 20.1 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.**

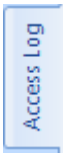


Pause/Run: Pause will stop the display from updating, Run will restart the display updates. **NOTE: Any events received while paused will not be displayed but will be entered into the database.**

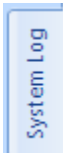


Enable filters to selectively display required information. This can be useful to display the movement of a single user through the system.

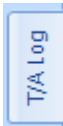
The information to be displayed is controlled by the 4 tabs below the Viewer Window:



Displays events from the Access Log.



Displays events from the System Log.



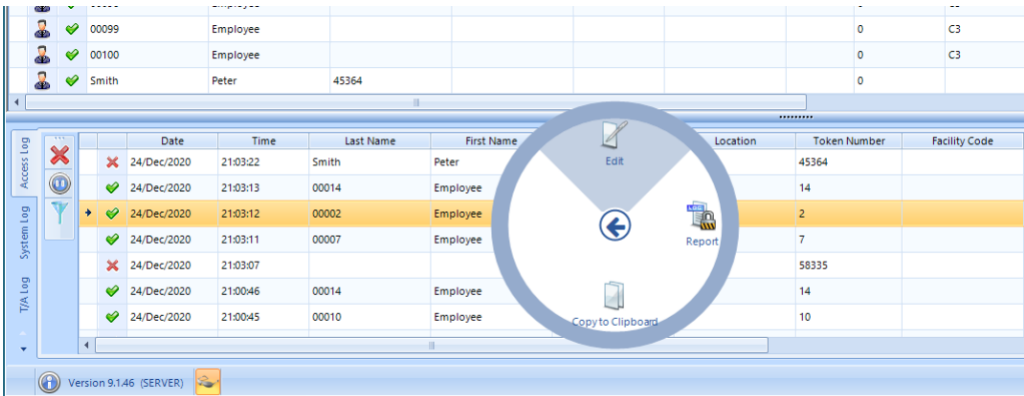
Displays events from the Time & Attendance Log



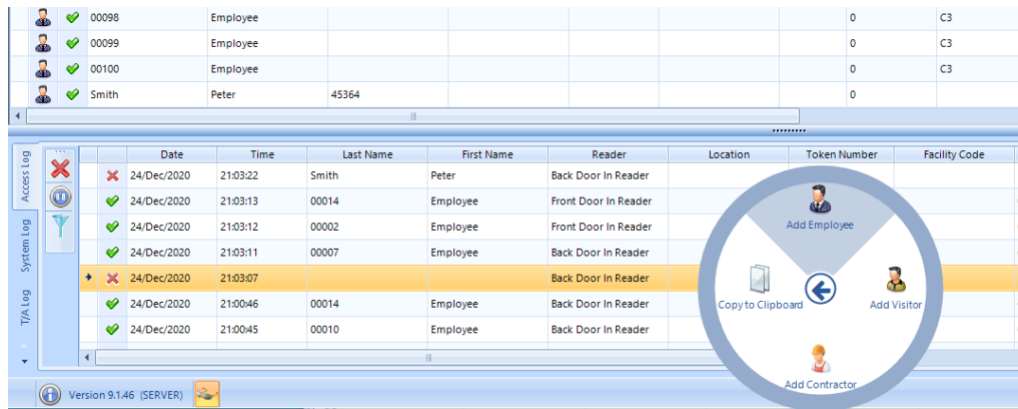
Displays Events and Actions from each controller.

***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:



## 20.2 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](#)<sup>57</sup>).

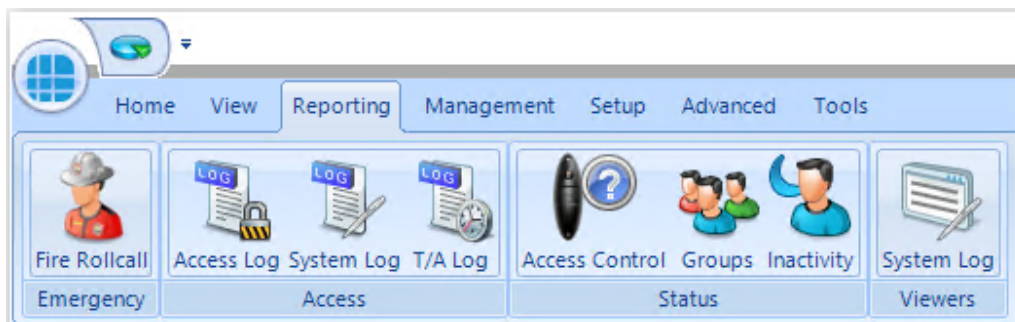
If users are allocated to Companies and Departments, the Fire Roll Call report will print all the users in the building from the first company/department followed by a page break, then all the users in the building from the second company/department etc.

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

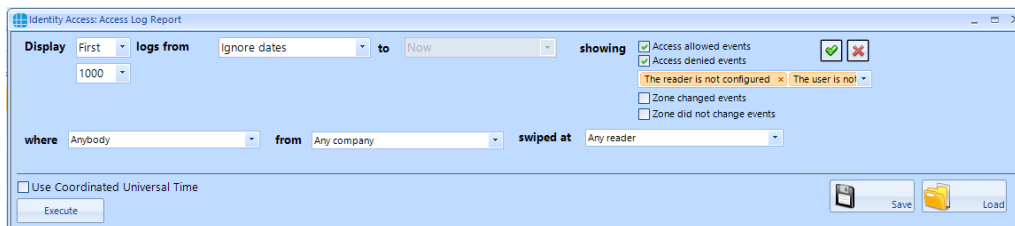
## 20.3 Access Control Reports

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.

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



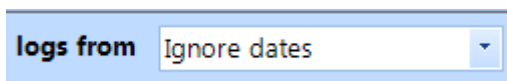
This then runs the Identity Access: Access Log Report form as shown below:



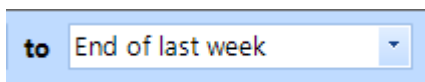
The options on generating the report are as follows:



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.

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

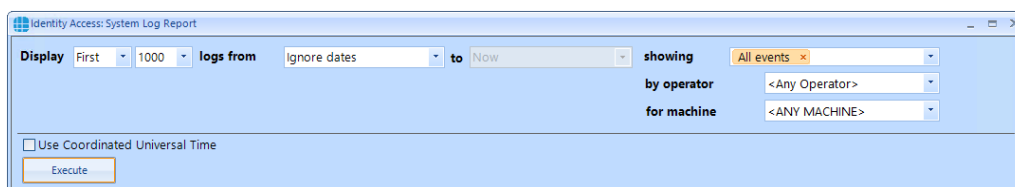


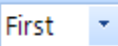
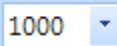
on several people it is possible to hold down the [Ctrl] key and highlight multiple entries, then click the  icon.

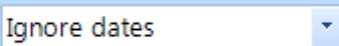
## 20.4 System Log Reports

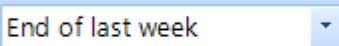
The System Log report is a record of all Identity Access system events, such as when people have logged on / off the software, when doors have been forced open or when database entries have been modified. The System Log Report menu can be accessed by selecting **Reporting** and **System Log**.

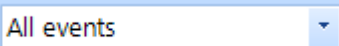
The way System Log reports are configured is similar to the Access log Reports, but with fewer options:




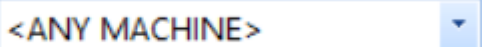
**Display**   defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.

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

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

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

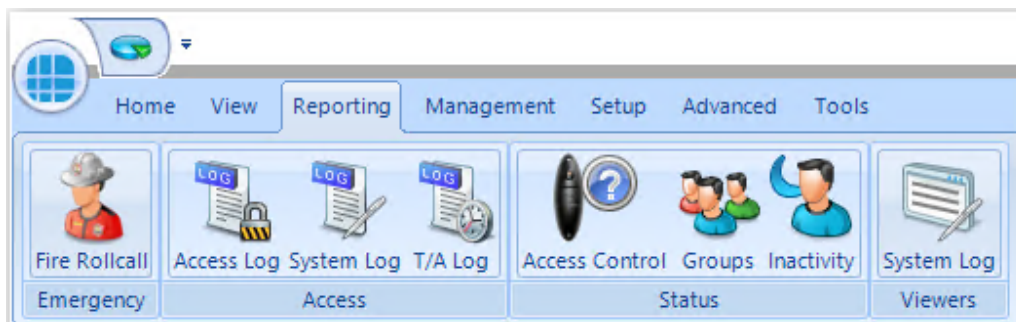
**by operator**  defines which Operator to report on

**for machine**  defines which Client machine to report on.

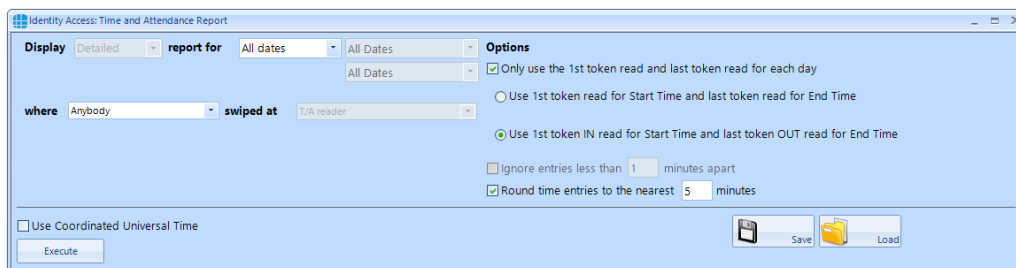
Once configured, click the **[Execute]** button to generate the report.

## 20.5 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**



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
<input type="checkbox"/>	05/10/2020	08:00:10	Gary James	front door Out Reader		Group access allowed
<input type="checkbox"/>	05/10/2020	09:14:14	Gary James	front door In Reader		Group access allowed
<input type="checkbox"/>	05/10/2020	09:14:20	Gary James	front door Out Reader		Group access allowed
<input type="checkbox"/>	05/10/2020	09:14:26	Gary James	front door In Reader		Group access allowed
<input type="checkbox"/>	05/10/2020	09:19:24	Gary James	front door Out Reader		Group access allowed
<input type="checkbox"/>	05/10/2020	09:19:33	Gary James	front door In Reader		Group access allowed
<input type="checkbox"/>	05/10/2020	09:19:42	Gary James	front door In Reader		Group access allowed

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

Identity Access: Time and Attendance Report

Display: Detailed report for: This week 04 Oct 2020 00:00:00 to 05 Oct 2020 16:32:35

Options:

- ☐ Only use the 1st token read and last token read for each day
- ☒ Use 1st token read for Start Time and last token read for End Time
- ☐ Use 1st token IN read for Start Time and last token OUT read for End Time
- ☐ Ignore entries less than 1 minutes apart
- ☐ Round time entries to the nearest 5 minutes

☐ Use Coordinated Universal Time

Execute Save Load

**T/A Log Report**

Monday, October 5, 2020 4:32:54 PM

Date	Start Time	End Time	Shift Total	Day Total	Grand Total
Gary James					
05 Oct 2020	09:14:14	09:14:20	00:00:06		
	09:14:26	09:19:24	00:04:58		
				00:05:04	

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.

- ☒ Only use the 1st token read and last token read for each day
- ☒ Use 1st token read for Start Time and last token read for End Time

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

Identity Access: Time and Attendance Report

Display: Detailed report for: This week 04 Oct 2020 00:00:00 to 05 Oct 2020 16:07:53

Options:

- ☒ Only use the 1st token read and last token read for each day
- ☐ Use 1st token read for Start Time and last token read for End Time
- ☐ Use 1st token IN read for Start Time and last token OUT read for End Time
- ☐ Ignore entries less than 1 minutes apart
- ☐ Round time entries to the nearest 5 minutes

☐ Use Coordinated Universal Time

Execute Save Load

T/A Log Report

Monday, October 5, 2020 4:09:04 PM

Date	Start Time	End Time	Shift Total	Day Total	Grand Total
Gary James					
05 Oct 2020	08:00:10	09:19:42		01:19:32	

- ☒ Only use the 1st token read and last token read for each day
- ☐ Use 1st token read for Start Time and last token read for End Time
- ☒ Use 1st token IN read for Start Time and last token OUT read for End Time

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:

Identity Access: Time and Attendance Report

Display: Detailed report for: This week 04 Oct 2020 00:00:00 to 05 Oct 2020 16:32:35

Options:

- ☐ Only use the 1st token read and last token read for each day
- ☐ Use 1st token read for Start Time and last token read for End Time
- ☒ Use 1st token IN read for Start Time and last token OUT read for End Time
- ☐ Ignore entries less than 1 minutes apart
- ☐ Round time entries to the nearest 5 minutes

☐ Use Coordinated Universal Time

Execute Save Load

T/A Log Report

Monday, October 5, 2020 4:32:54 PM

Date	Start Time	End Time	Shift Total	Day Total	Grand Total
Gary James					
05 Oct 2020	09:14:14	09:19:24		00:05:10	

☒ Ignore entries less than 1 minutes apart

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

☒ Round time entries to the nearest 5 minutes

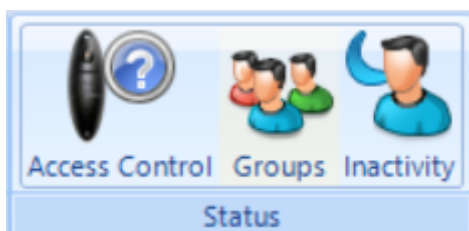
This option will round the times up or down, such as :

**T/A Log Report**  
Monday, October 5, 2020  
4:32:54 PM

Date	Start Time	End Time	Shift Total	Day Total	Grand Total
05 Oct 2020	09:15:00	09:20:00		00:05:00	

## 20.6 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:

The screenshot shows the 'Identity Access: Access Control Report' configuration window. It has three dropdown menus: 'Display' set to 'Anybody', 'from' set to 'Any company', and 'who has access at' set to 'Any reader'. There are 'Save' and 'Load' buttons on the right and an 'Execute' button at the bottom left.

**Display** - selects specific users to report on

**from** - selects specific Companies and Departments to report on

**who has access at** - selects the readers to report on

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

The screenshot shows the 'Identity Access: Access Control Report' configuration window with specific selections. The 'Display' dropdown is set to 'Specific employees' with 'Smith, Jim (10001)' selected. The 'from' dropdown is set to 'Any company'. The 'who has access at' dropdown is set to 'Specific readers' with 'Front Door In Reader' selected. There are 'Save' and 'Load' buttons on the right and an 'Execute' button at the bottom left.

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

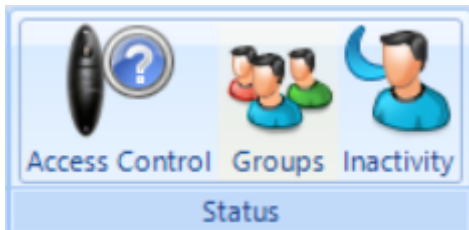
The screenshot shows the generated 'Access Control Report'. It includes a header with the title 'Access Control Report' and the date 'Monday, October 5, 2020'. Below the header is a blue bar with the title 'Access Control Report' and the date 'Monday, October 5, 2020 4:48:56 PM'. The report is titled 'Front Door In Reader' and 'All staff'. It contains a table with columns 'Last Name', 'First Name', 'Company', and 'Department'. The table has one row with the data 'Smith', 'Jim', and empty cells for 'Company' and 'Department'.

Last Name	First Name	Company	Department
Smith	Jim		

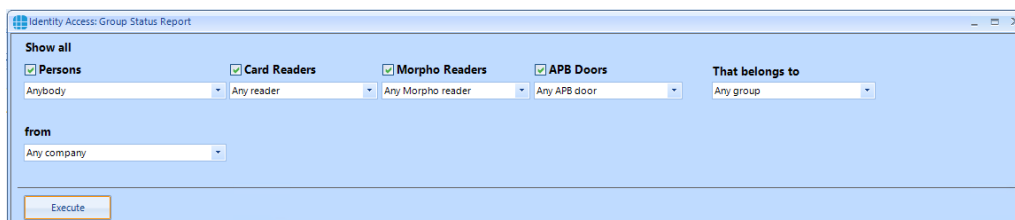
This report shows that the reader called "Front Door In Reader" is accessible by the group "All staff" which includes the user "Jim Smith"

## 20.7 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

A screenshot of a software window titled 'Identity Access: Group Status Report'. It contains several configuration options: 'Show all' with a checkbox; 'Persons' with a dropdown menu set to 'Anybody'; 'Card Readers' with a checked checkbox and a dropdown set to 'Any reader'; 'Morpho Readers' with a checked checkbox and a dropdown set to 'Any Morpho reader'; 'APB Doors' with a checked checkbox and a dropdown set to 'Any APB door'; 'That belongs to' with a dropdown set to 'Any group'; and 'from' with a dropdown set to 'Any company'. An 'Execute' button is at the bottom.

**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

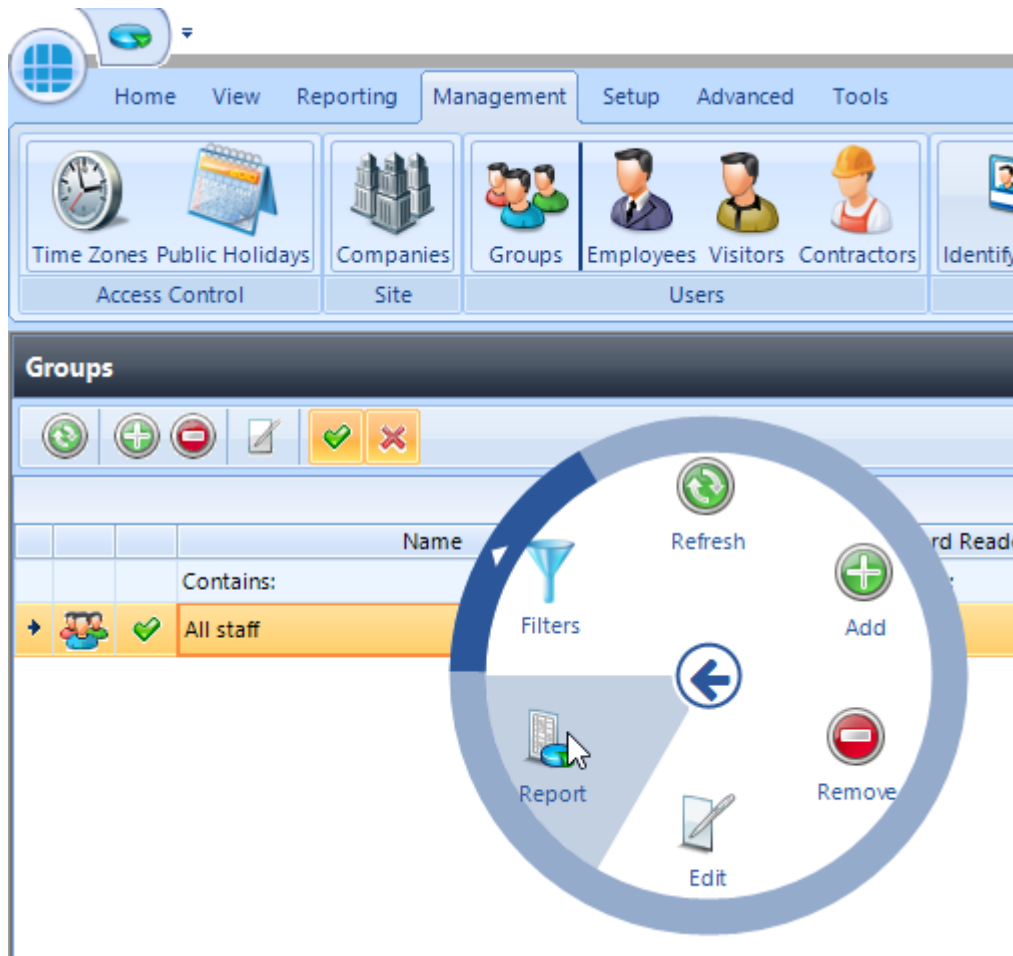
**APB Doors** - choose any combination of AntiPassBack doors to include in the report

**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.

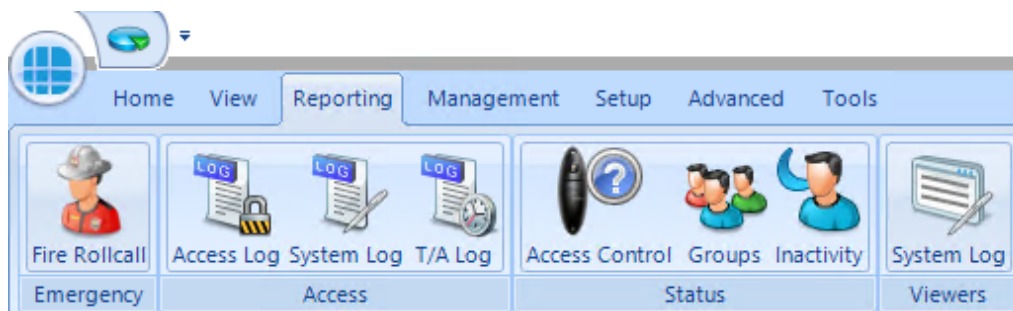
**NOTE: This report can be run for a specific Group by selecting the required Group in the Groups screen, then right click and select report from the Option Wheel**



## 20.8 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.

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

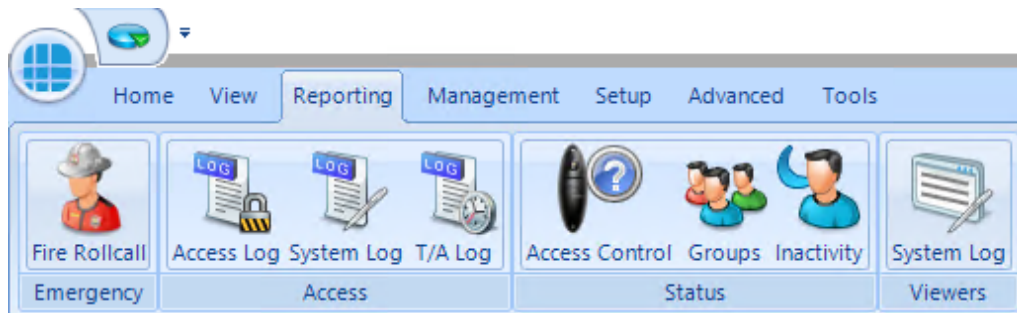


loads a saved query

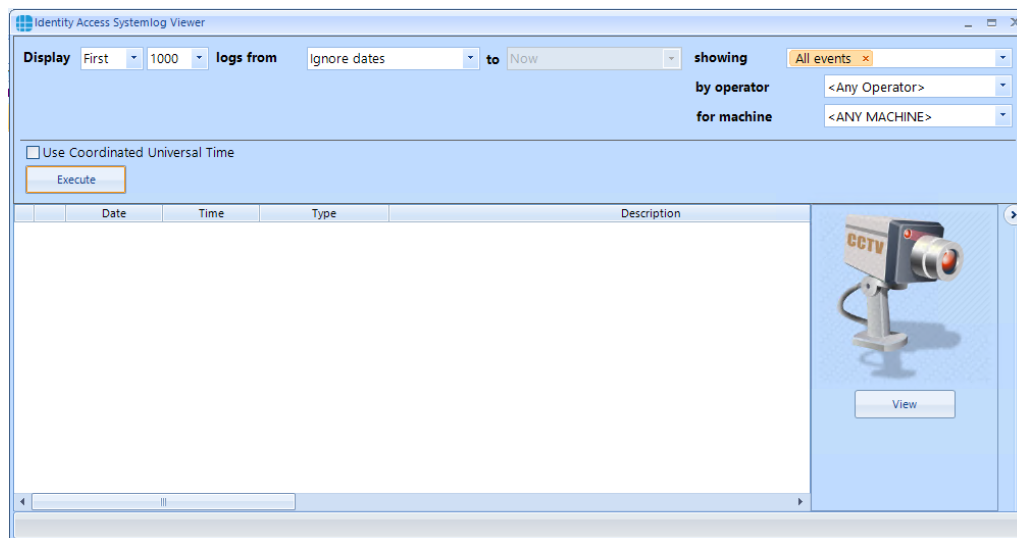
EXAMPLE: to report inactivity on anyone in Controlsoft Sales or Technical within the past year, the report configuration would look as follows:

## 20.9 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

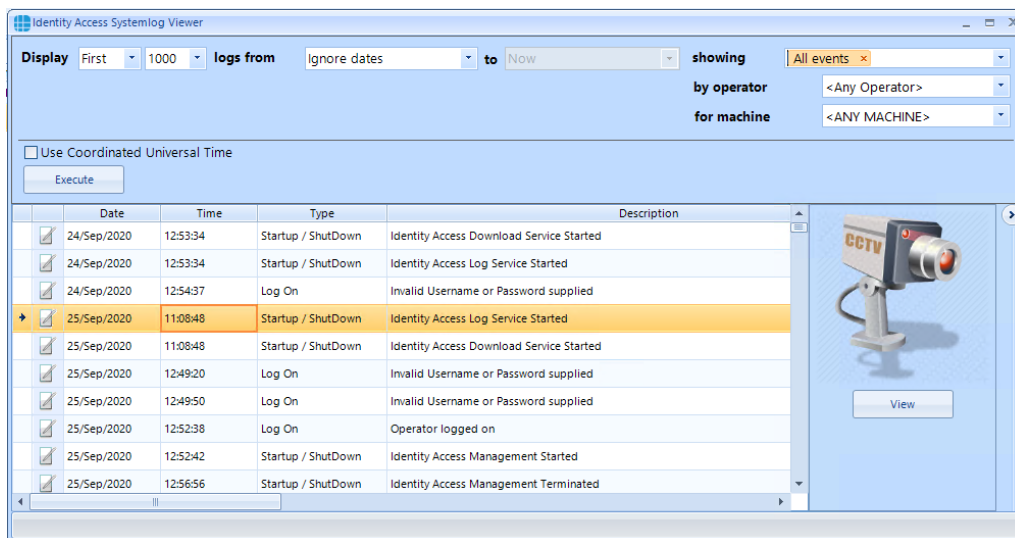
**logs from** - defines the date that the report starts (Example ignore dates, start of last month or 1st January 2020)

**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



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

# Service Manager

## 21 Service Manager

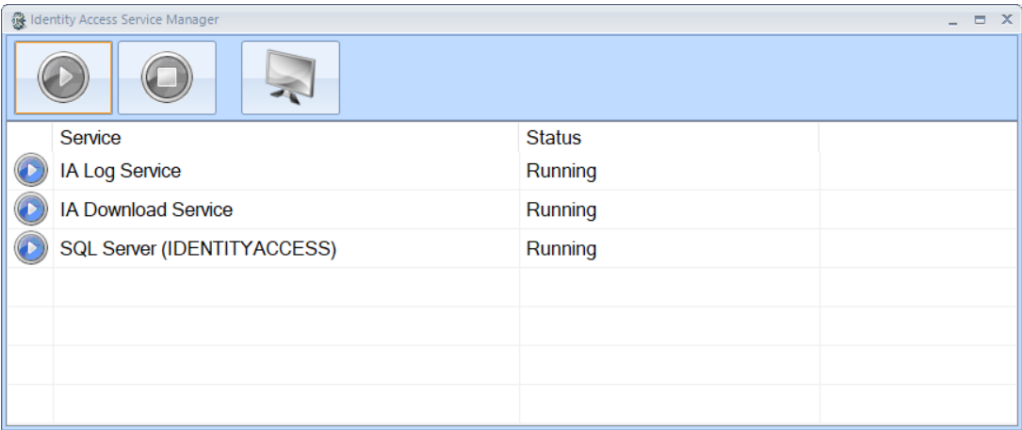
The Service Manager is a small utility which provides access to the 2 Identity Access services, the Log Service and Download Service. It also shows whether the Identity Access SQL Server instance is running.

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



Enter your username and password to access the software (Administrator users only)

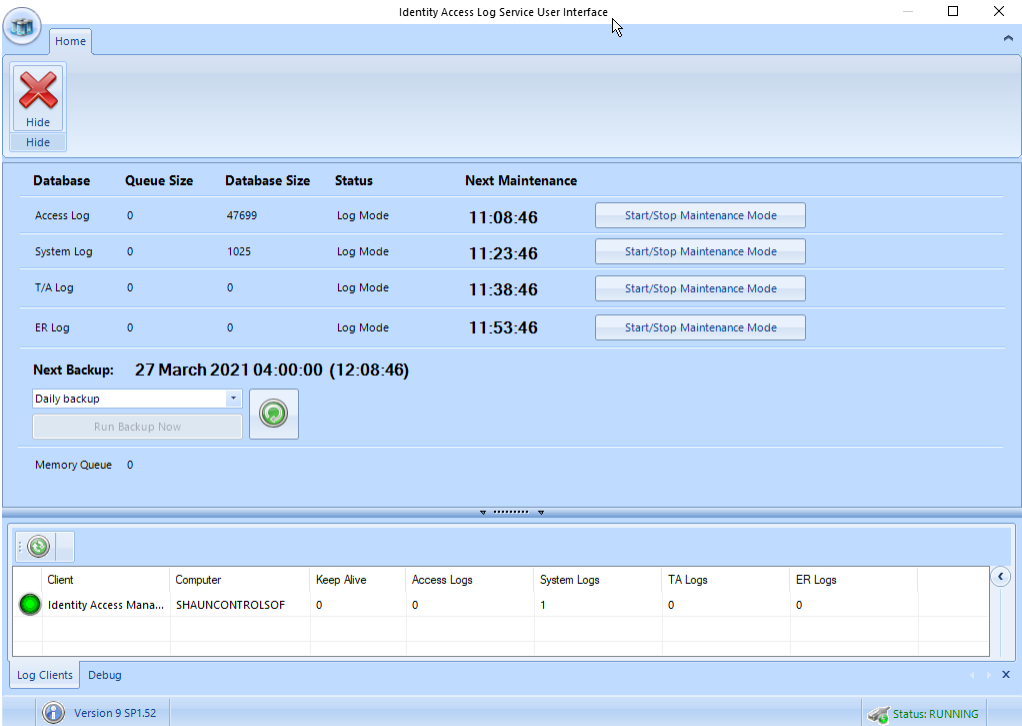
The Service Manager will now display which services are running as shown below:



21.1 Log Service

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

To run the Log Service user interface, select **IA Log Service** and press the



The option buttons are:

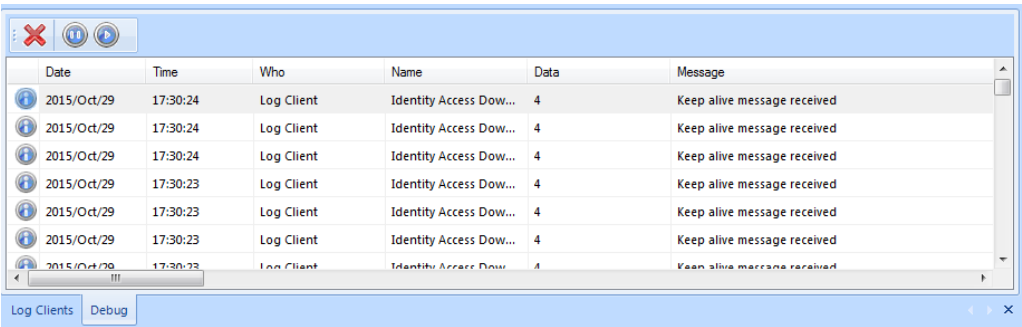


Closes the Log Server.

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 SHAUNCONTROLISO

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



Date	Time	Who	Name	Data	Message
2015/Oct/29	17:30:24	Log Client	Identity Access Dow...	4	Keep alive message received
2015/Oct/29	17:30:24	Log Client	Identity Access Dow...	4	Keep alive message received
2015/Oct/29	17:30:24	Log Client	Identity Access Dow...	4	Keep alive message received
2015/Oct/29	17:30:23	Log Client	Identity Access Dow...	4	Keep alive message received
2015/Oct/29	17:30:23	Log Client	Identity Access Dow...	4	Keep alive message received
2015/Oct/29	17:30:23	Log Client	Identity Access Dow...	4	Keep alive message received
2015/Oct/29	17:30:23	Log Client	Identity Access Dow...	4	Keep alive message received

## 21.2 Download Service

The **Download Service** handles all the communications between the Identity Access software and the Master iNets. All events from the iNet controllers are saved in the Log Buffers.

To run the Download Service, select **IA Download Service** and press the

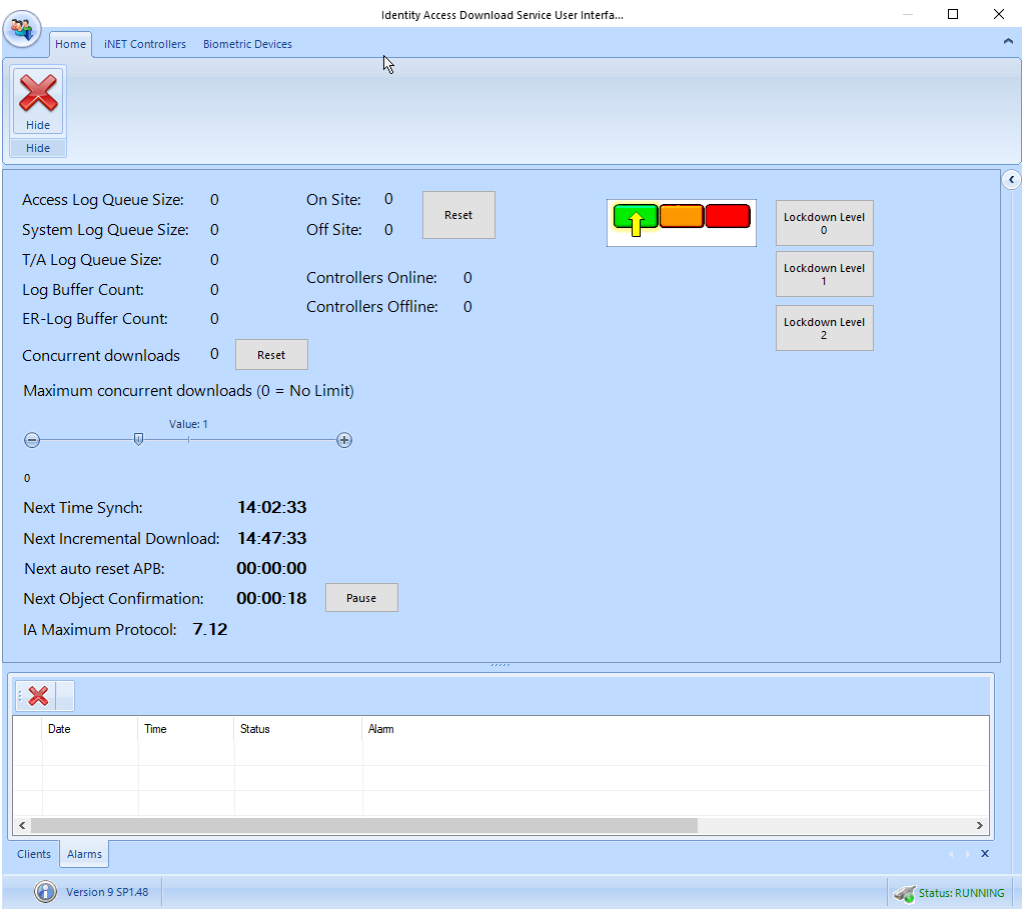


icon

The Download Service has 3 tabs, **Home**, **iNet Controllers** and **Biometric Devices**.

21.2.1 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.



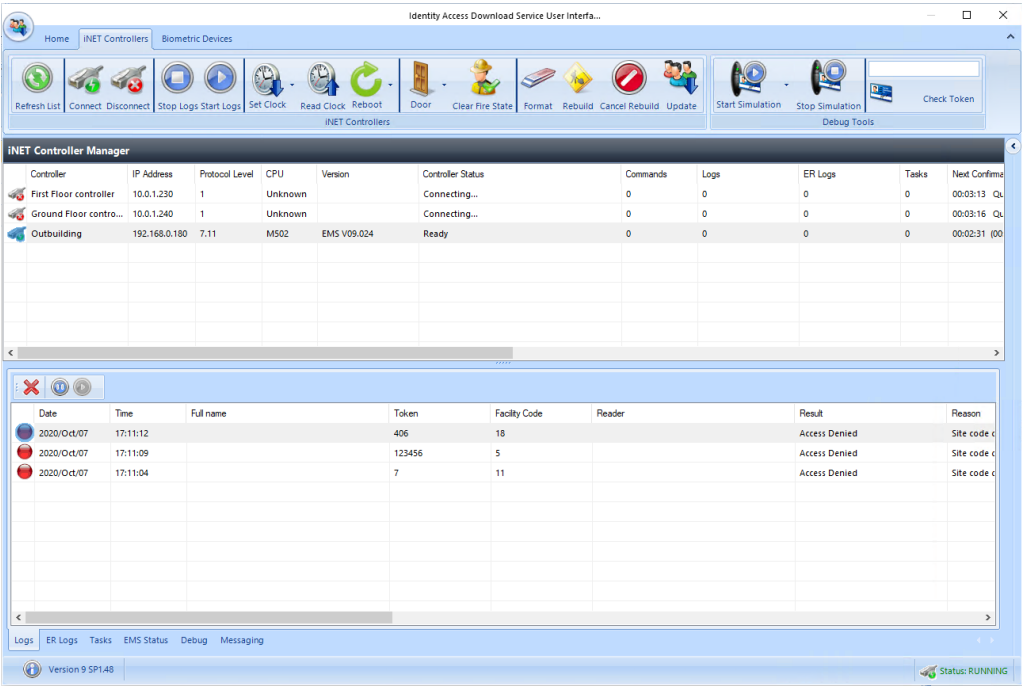
Also displayed is an indication of the number of **Controllers Online** and **Controllers Offline**.

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)

21.2.2 i-Net 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



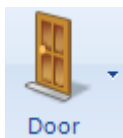
Set the clock in the selected iNet controller/s. The dropdown list allows the iNet clock to be set to **Current Time** or **Custom Time**



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



Reboots the selected controller/s



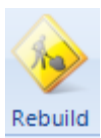
Allows a door on the selected controller to be **Granted Access** (opened for the programmed door open time), **Force Open** and **Force Closed**.



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

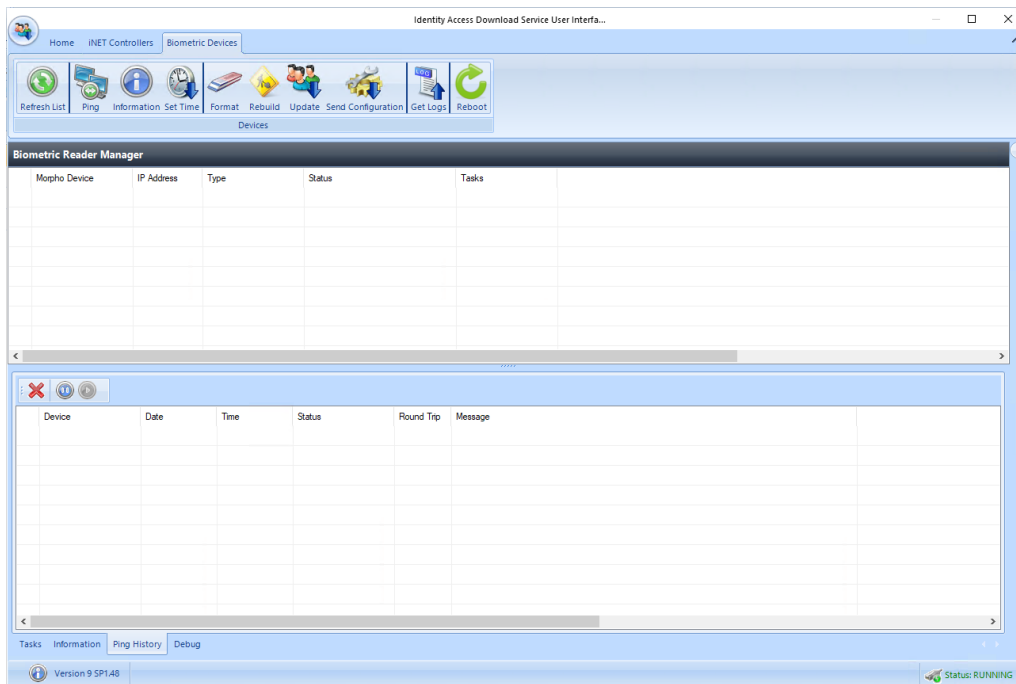


Downloads the most recent changes to the selected controller/s





Select the **Biometric Devices** Tab:



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

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

Biometric Reader Manager					
Morpho Device	IP Address	Type	Status	Tasks	

**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



## **Appendix A - Types of Door**



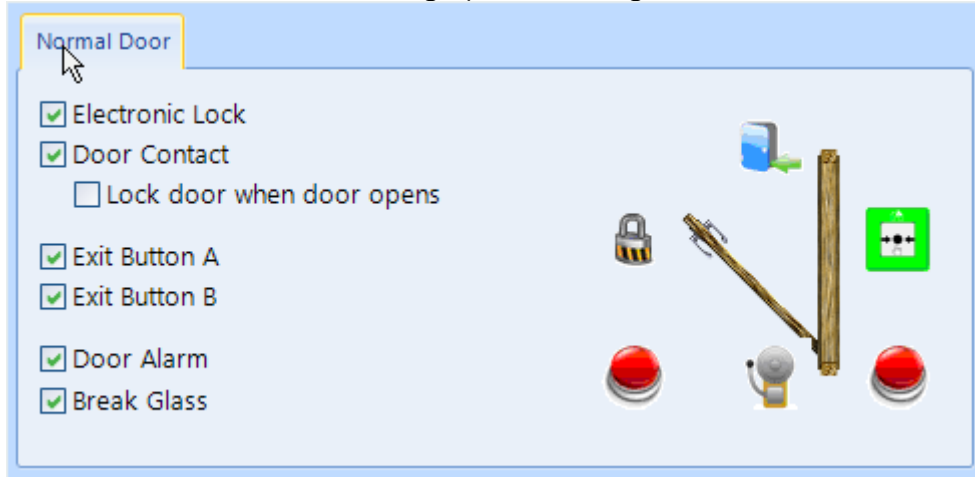
## 22 Appendix A - Types of Door

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.***

## 22.1 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.



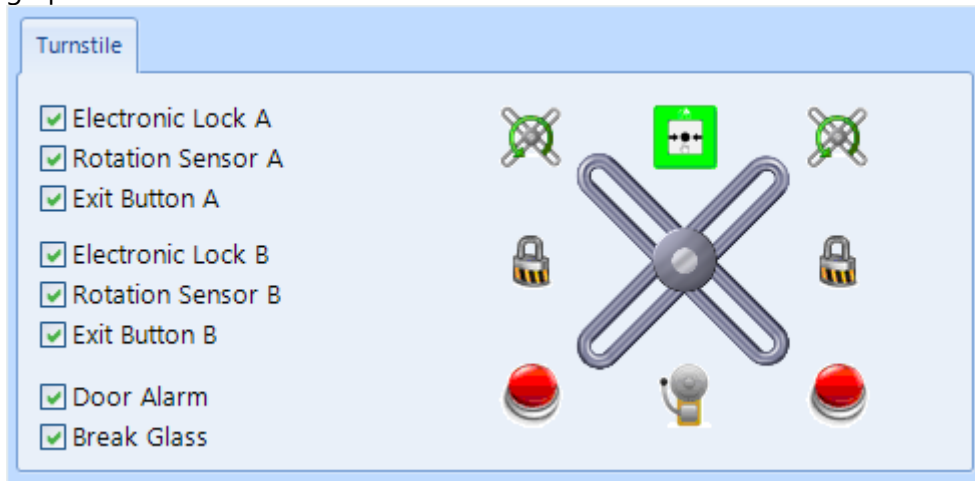
**Door Alarm:** This is a relay output used to drive a sounder when a Door Forced, or Door Held alarm is generated or when a breakglass has been activated. The relay output can be programmed for Normal or Inverted operation for maximum flexibility in the choice of sounder.



**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.

## 22.2 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 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.

## 22.3 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



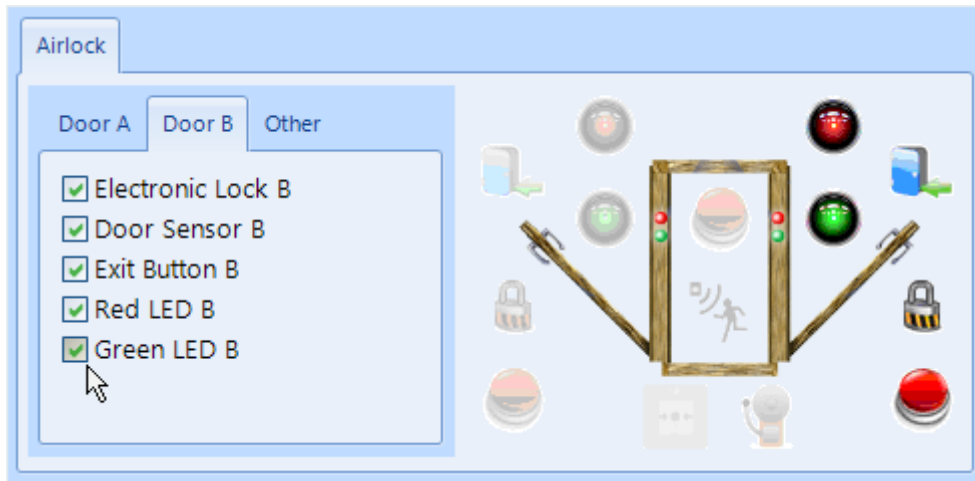
**Exit Button A** defines the input that monitors the Request to Exit button to release the door



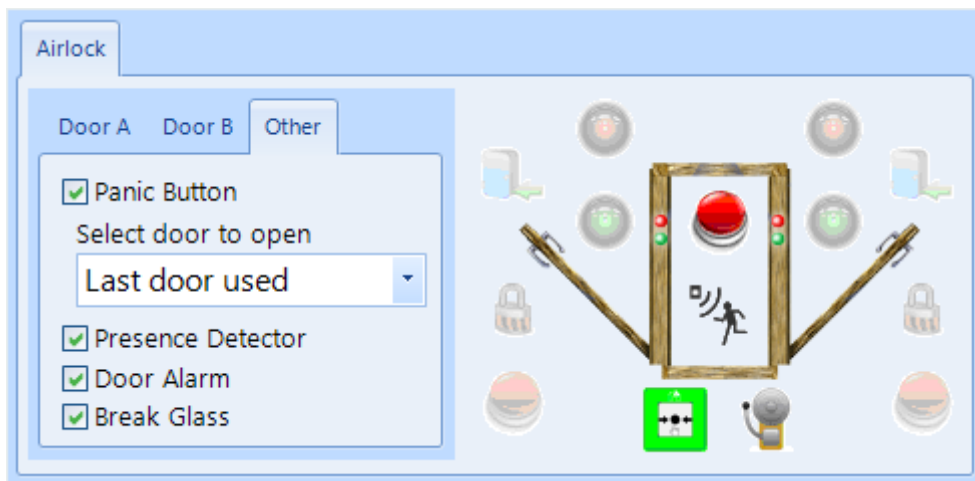
**Red LED A** defines the output that controls a red LED to indicate that the door is locked



**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.



**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.

## 22.4 Aperio Door

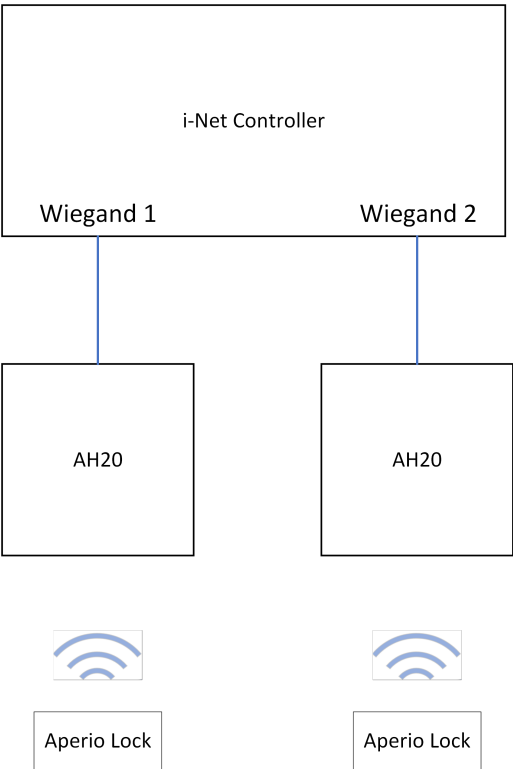
Aperio locks can be used to replace existing handles and cylinders to integrate them into the Access Control system. This can provide a quick and efficient way to upgrade door handles or cylinders with mechanical locks.



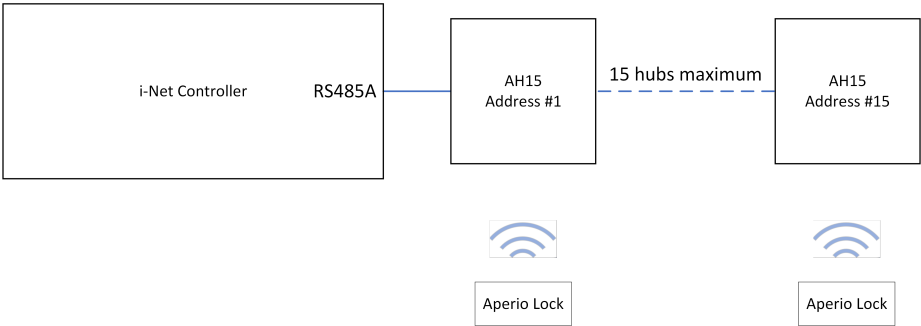
**NOTE: Aperio locks do not support "Out" readers, so some Identity Access functions such as Location and AntiPassBack cannot be used with Aperio locks.**

The controller can be connected to the locks via a Wiegand Hub or an RS485 Hub as detailed below:

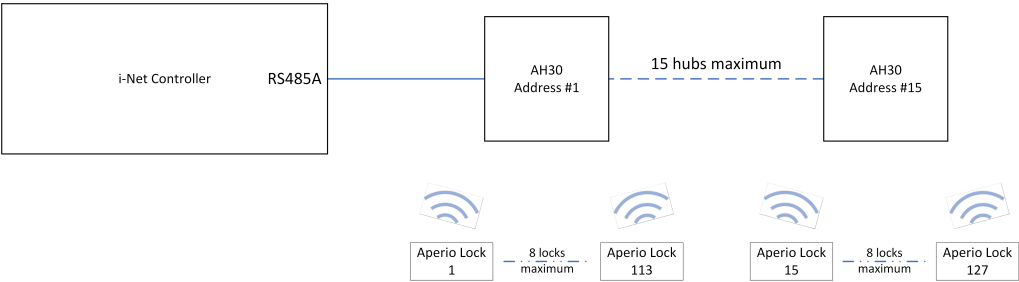
**AH20 Wiegand 1:1 Hub** - each hub can monitor a single lock, and connects the iNet controller via a standard Wiegand interface



**AH15 RS485 1:1 Hub** - each hub can monitor a single lock, with up to 15 hubs connecting to the iNet controller via an RS485 interface



**AH30 RS485 1:8 Hub** - each hub can monitor up to 8 locks, with up to 15 hubs connecting to the iNet controller via an RS485 interface



The lock addressing on the AH30 hubs may at first look confusing, but the addressing scheme is as follows:

	1st lock	2nd lock	3rd lock	4th lock	5th lock	6th lock	7th lock	8th lock
Hub #1	1	17	33	49	65	81	97	113
Hub #2	2	18	34	50	66	82	98	114
Hub #3	3	19	35	51	67	83	99	115
Hub #4	4	20	36	52	68	84	100	116
Hub #5	5	21	37	53	69	85	101	117
Hub #6	6	22	38	54	70	86	102	118
Hub #7	7	23	39	55	71	87	103	119
Hub #8	8	24	40	56	72	88	104	120
Hub #9	9	25	41	57	73	89	105	121
Hub #10	10	26	42	58	74	90	106	122
Hub #11	11	27	43	59	75	91	107	123
Hub #12	12	28	44	60	76	92	108	124
Hub #13	13	29	45	62	77	93	109	125
Hub #14	14	30	46	62	78	94	110	126
Hub #15	15	31	47	63	79	95	111	127

where "1st lock" is the first lock that was paired on the relevant hub, "2nd lock" is the second lock that was paired etc.

**NOTE 1: The iNet only supports up to 32 doors per master controller**

**NOTE 2: For compatibility with Aperio RS485 hubs, the iNet controller must be fitted with firmware version 98.37.020 or later.**

**NOTE 3: For maximum flexibility, it is possible to mix AH15 hubs and AH30 hubs on the same RS485 bus.**

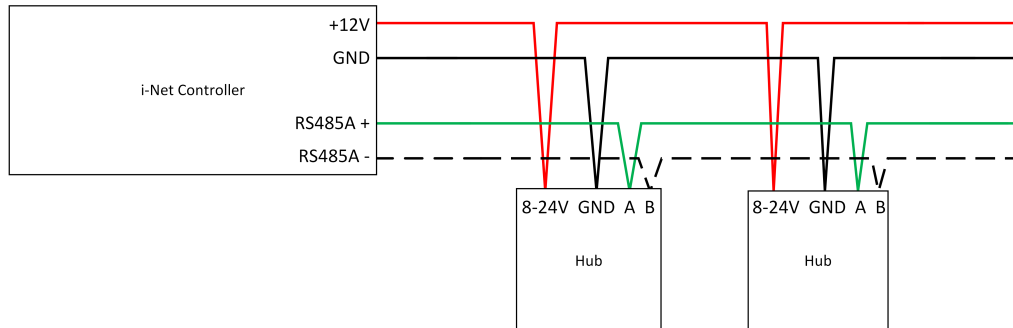
**NOTE 4: Hubs with address 0 cannot be used.**

To configure Aperio handlesets or cylinders using an RS485 hub:

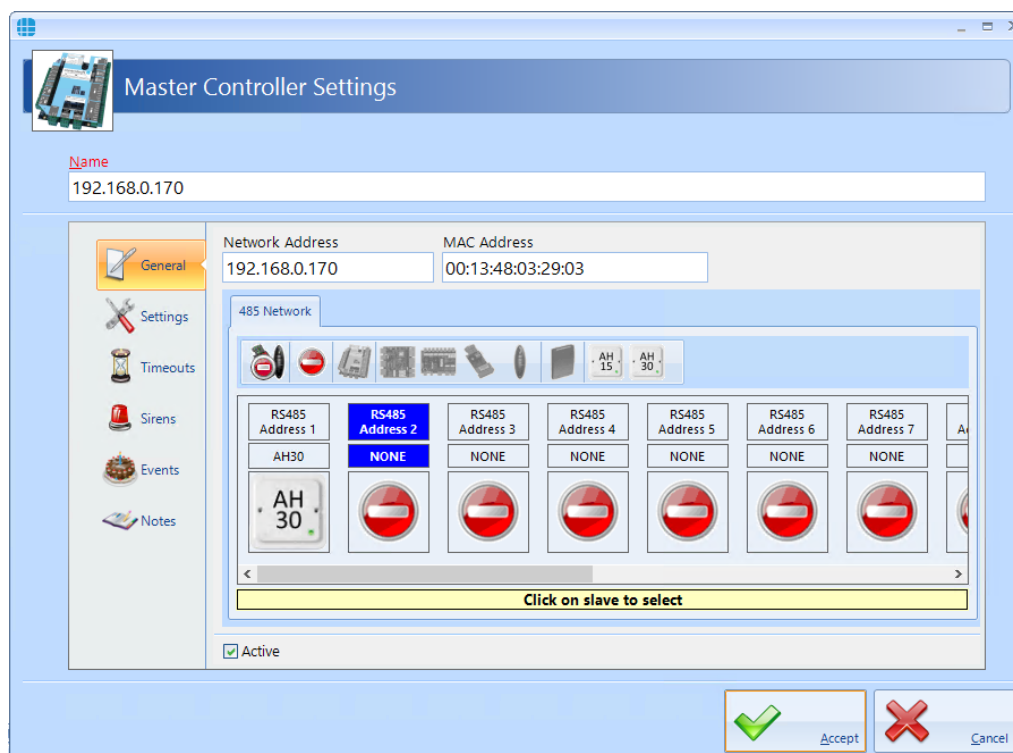
Configure the 10-way DIP switch on each hub for the desired address on the RS485 bus (please refer to documentation supplied with the hub for further information)



Connect the hub/s to the iNet RS485 Port A using Belden 8723 cable (or equivalent) with terminal "A" on the hub connected to "+" on the iNet, and terminal "B" on the hub connected to "-" on the iNet. Further hubs are connected in a "daisy-chain" manner (i.e. '+' to 'A' to 'A' etc, '-' to 'B' to 'B' etc)



Create a controller in Identity Access either manually or using the Find Controller Wizard. Edit the controller and add the relevant hub/s to the RS485 bus as indicated below:



Press **Accept** and perform a full download to the controller. The iNet will then start communicating with the hub, indicated by activity on the RS485 LEDs.

Next, pair the hub with up to 8 locks (AH30) or 1 lock (AH15 / AH20) using the Aperio Programming Application (PAPP) tool. The sequence in which locks are paired will define the reader numbers in the Card Reader Settings screen as described above.

Doors and readers can then be created in the usual manner. Creating an Aperio door on an AH30 hub is as shown below:


**Door Settings**

Name: Front Door

Door Type: Aperio Door

On master controller network: Ground Floor controller

I/O Overview of the door controller

INPUTS		I-NET	OUTPUTS	
0	<input type="checkbox"/>	 RS485 Addr 0	0	<input type="checkbox"/>
1	<input type="checkbox"/>		1	<input type="checkbox"/>
2	<input type="checkbox"/>		2	<input type="checkbox"/>
3	<input type="checkbox"/>		3	<input type="checkbox"/>
4	<input type="checkbox"/>		4	<input type="checkbox"/>
5	<input type="checkbox"/>		5	<input type="checkbox"/>
6	<input type="checkbox"/>		6	<input type="checkbox"/>
7	<input type="checkbox"/>		7	<input type="checkbox"/>
8	<input type="checkbox"/>	8	<input type="checkbox"/>	

☐ Override all lockdown levels



☐ Override Lockdown Level 2

☐ Enforce Anti Passback

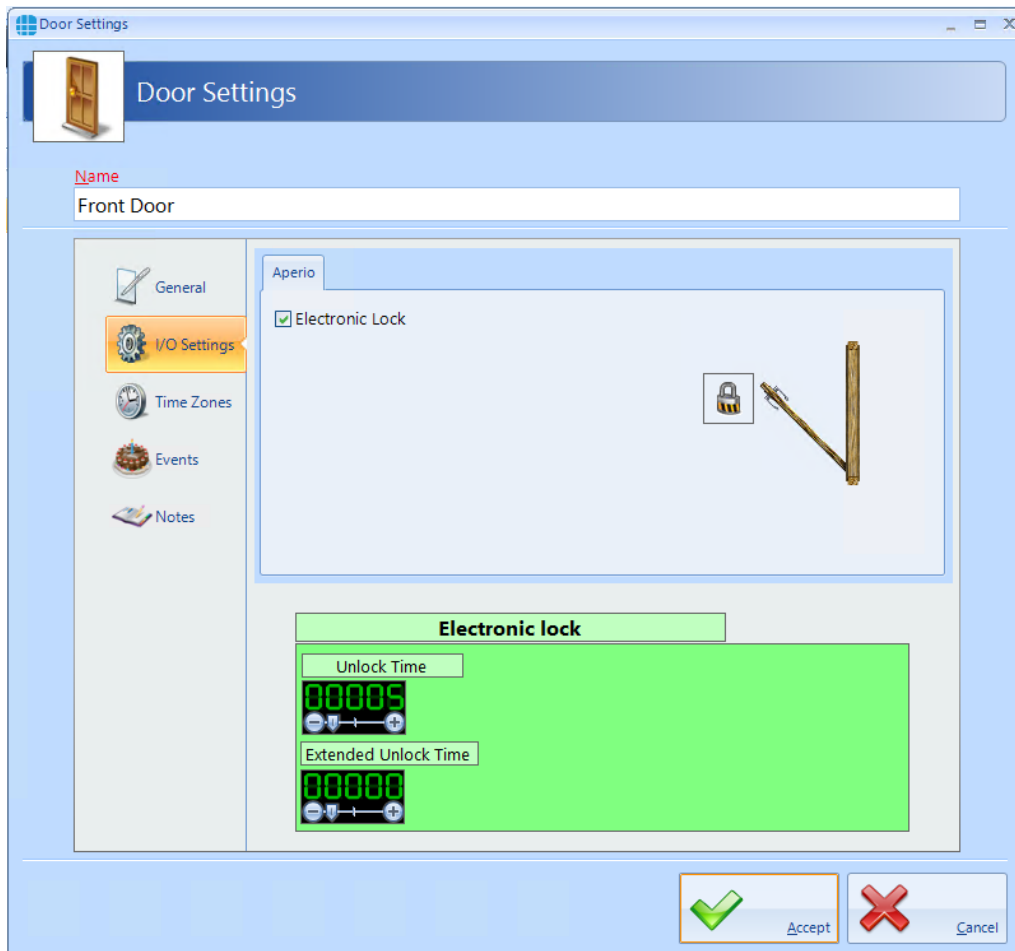
☐ Force door open if fire is detected

☐ Dropbox

☒ Active

 **Accept**  **Cancel**

To set the door open time and extended door open time, select "I/O Settings" in the side bar and click on the lock icon:



Creating an Aperio reader on an AH30 hub is as shown below:

The screenshot shows the 'Card Reader Settings' window for an AH30 hub. The window has a title bar 'Card Reader Settings' and a sidebar with icons for General, Time Zones, Settings, Events, and Notes. The 'General' tab is selected. The 'Name' field is 'Server Room'. The 'On master controller network' dropdown is '192.168.0.170'. The 'Select slave network' dropdown is 'RS485 network device'. The 'RS485 Address 1 - AH30 Hub' dropdown is 'AH 30'. The 'Lock / Sensor' section shows a dial with numbers 49, 65, 81, 33, 97, 17, 113, and a central '1'. The 'This reader controls' section has a dropdown set to 'Door' and a text field 'Server Room'. There are checkboxes for 'Reader has a PIN pad attached', 'Reader is used for Time and Attendance', and 'Active' (checked). The 'Location' dropdown is 'Not applicable'. At the bottom right are 'Accept' and 'Cancel' buttons.

Card Reader Settings

Name  
Server Room

General  
Time Zones  
Settings  
Events  
Notes

On master controller network  
192.168.0.170

Select slave network  
RS485 network device

RS485 Address 1 - AH30 Hub  
AH 30

Lock / Sensor  
65  
49 81  
33 97  
17 113  
1

This reader controls  
Door Server Room

☐ Reader has a PIN pad attached  
☐ Reader is used for Time and Attendance  
Location  
Not applicable  
☒ Active

Accept Cancel

**NOTE: If creating doors and reader with the Door Wizard, remember to ensure that the door and reader configuration screens match the above.**

## **Appendix B - HID Asure ID Software**

## 23 Appendix B - HID Asure ID Software

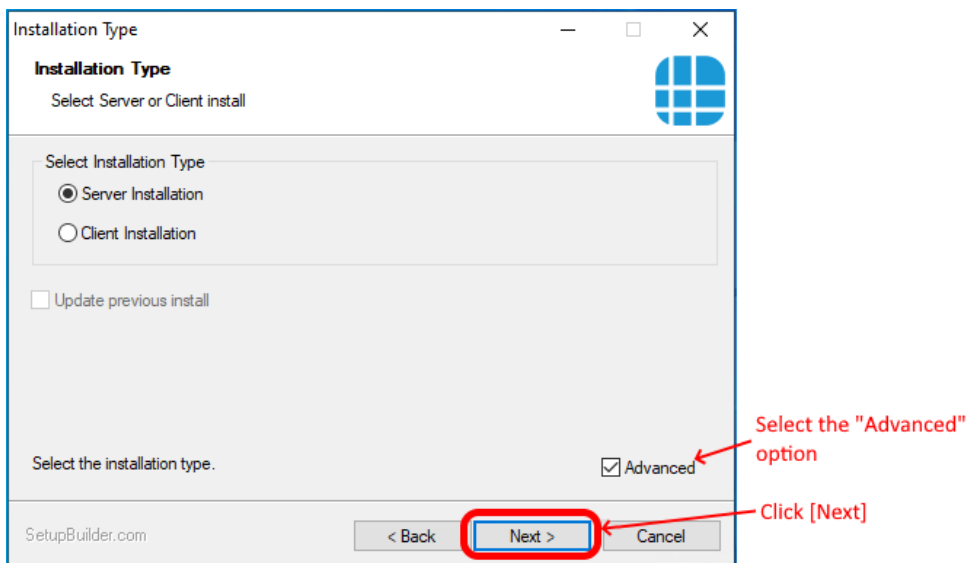
The Controlsoft Identity Access install flash drive includes a copy of HID Asure ID® 7. This is an ideal choice for organizations looking for an affordable and easy-to-use photo ID card software with direct integration with the Controlsoft Identity Access database.

Asure ID Enterprise has additional features like compound data fields, batch printing, conditional design and print rules, and password protection.

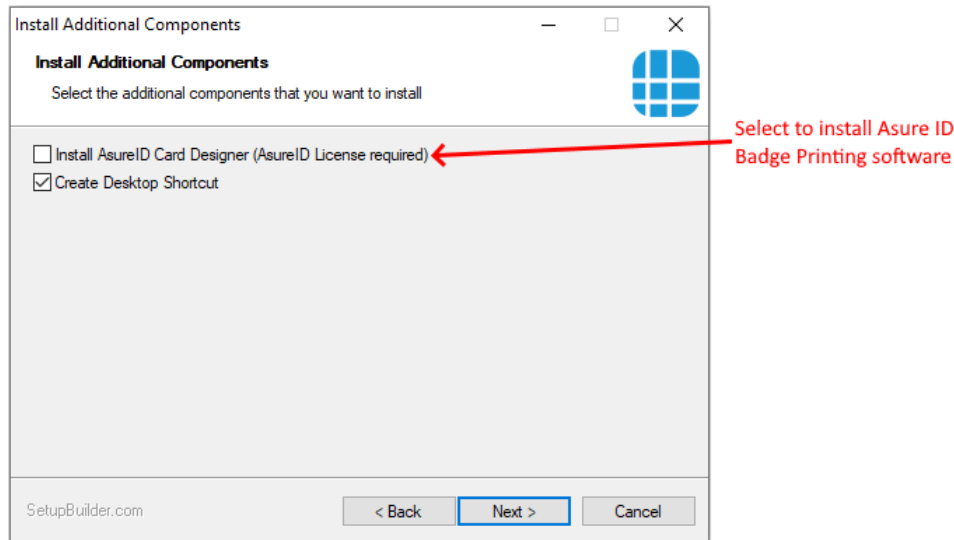
***NOTE: The copy of Asure ID supplied with Identity Access is a 30 days trial copy. To use Asure ID beyond the 30 day trial period, you will require a licence. Please contact your vendor for further details.***

To install Asure ID:

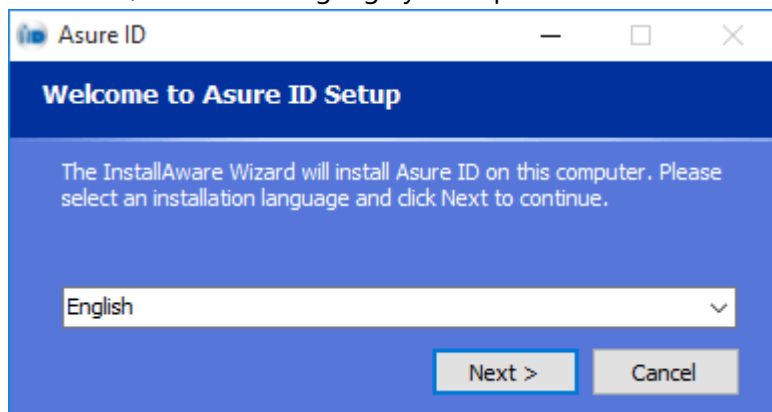
1. Install the IA software until the **Advanced** option can be seen



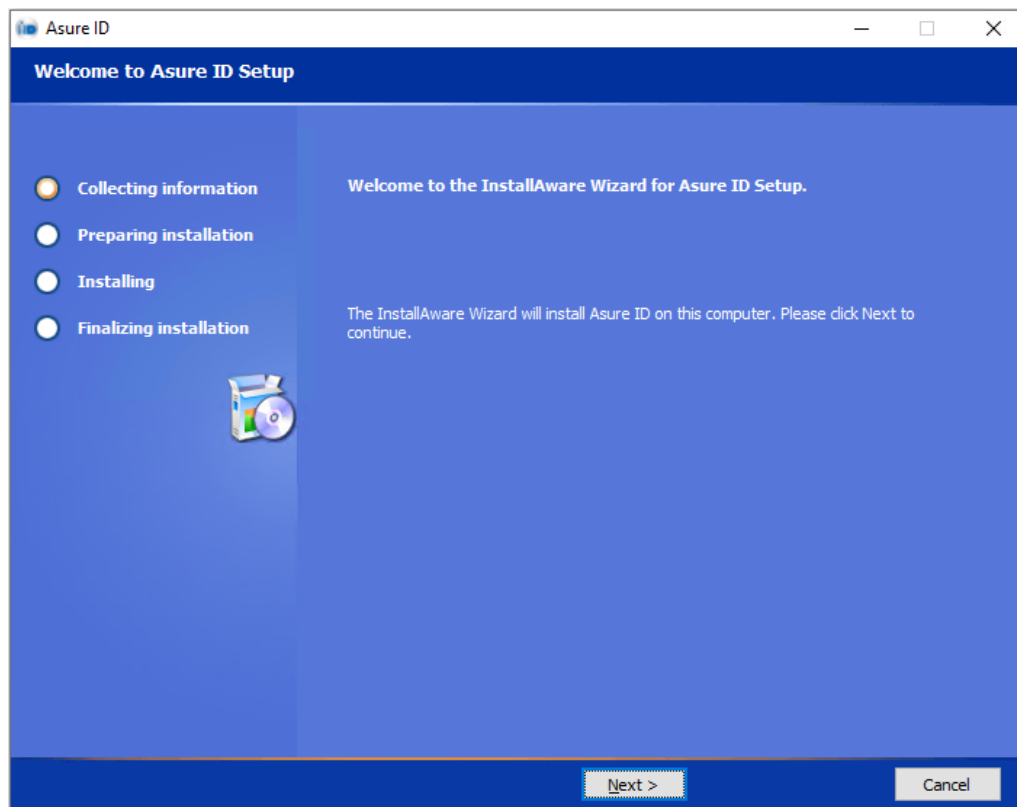
2. Tick the **Install AsureID Card Designer** box during the Controlsoft Identity Access installation:



3. During the installation of Identity Access, the AsureID setup will automatically start. First, select the Language you require:



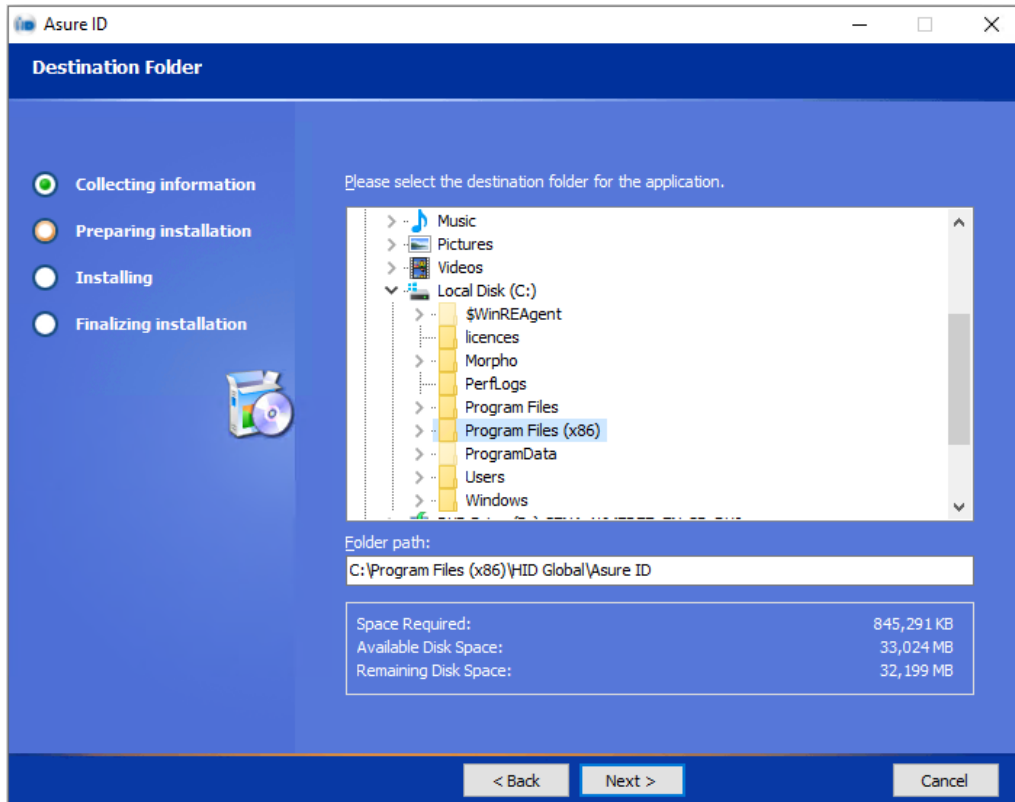
4. Click **[Next]**



5. Click **[Next]** , then read the license agreement, select **I accept the license agreement** and select **[Next]**

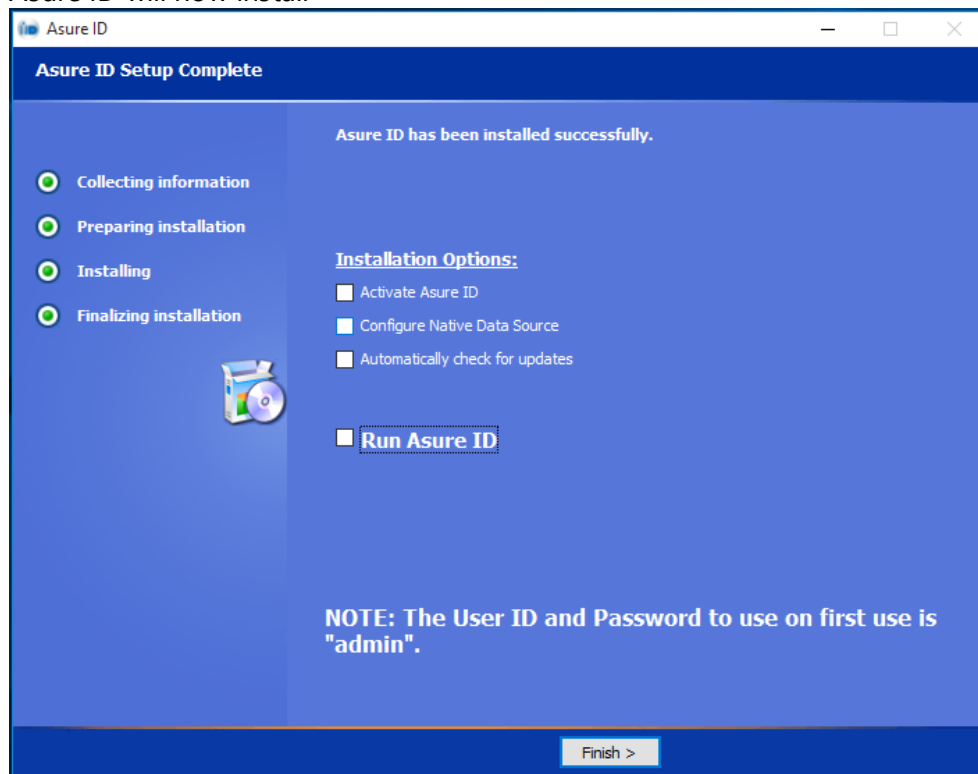


6. Select your Fargo printer from the dropdown list and click **[Next]**
7. You can now define the destination folder for the AsureID software, although we strongly recommend that you leave this as the default folder:

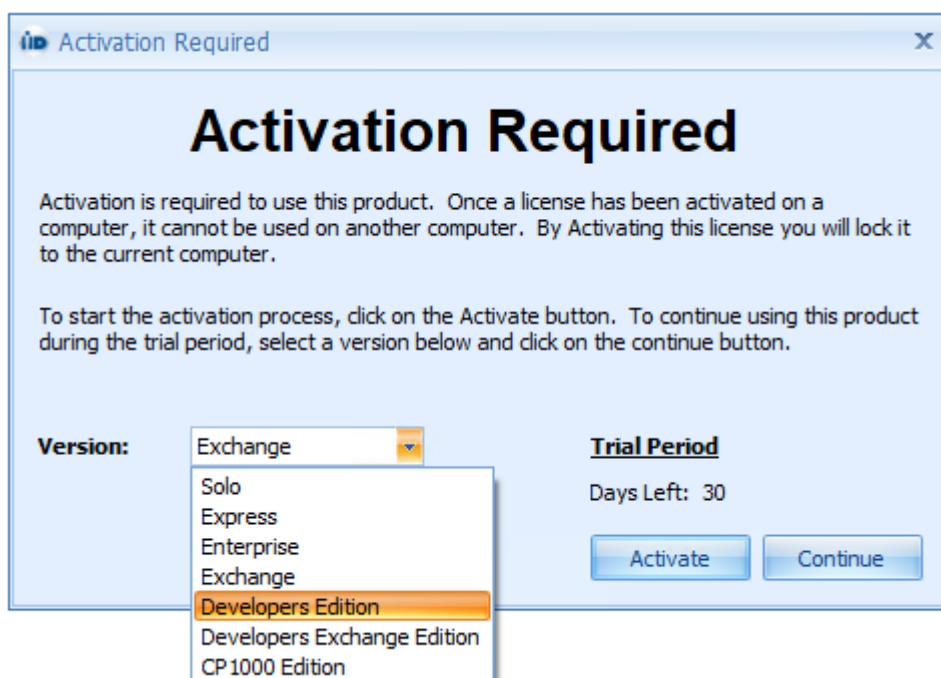


Click **[Next]** to continue

8. Asure ID will now install



9. Once the installation is complete, click **[Finish]** and the activation process will begin



10. Select **Developers Edition** and click **[Activate]**

Activate License

Activate License

First Name:

Last Name:

Email:

Company Name:

State / Province:

Country:

Printer Make / Model:

License Key:

☒ Subscribe to product newsletter

☒ Subscribe to anonymous surveys

Phone Activation Activate Online

Asure ID

System License: **None**

License Level: **Trial**

Additional Licenses:

Close

11. Enter all the required information including the license key which will have been supplied by your vendor, and click **Activate Online**.

### To configure Asure ID

Run the IA Configuration utility and log in (default credentials are Admin and Password), then select the **Asure ID** tab on the side bar.

**Database Settings** are for Advanced Users to use AsureID data on a different machine. The Default Data Source is a Microsoft Access database housed on the same PC as AsureID. It is also possible to setup the AsureID database on a SQL Server or Oracle Server.

The default **Card Designer Login** credentials are **admin** and **admin**. If this is changed within AsureID it must also be changed within the IA Client Configuration utility.

**Card Designer Field Mapping** is a list of fields that are configured to work between Controlsoft Identity Access and AsureID. The Names in this list should not be changed.

For further information, see [IA Configuration - Badge Printing](#) 

### Asure ID Card Designer

To open the Asure ID Card Designer within the Identity Access User Interface select **Management** then select the **Asure ID** button



To map a field from Identity Access, click on **Data Field** and draw a box where you want the information placed on the card. Under **Field Name** select the Field to be mapped.

The screenshot shows the 'Data Field Properties' dialog box with the following sections and settings:

- Data Field**
  - Field Name: IA\_FLName (selected from a dropdown menu showing IA\_Title, IA\_FName, IA\_MName, IA\_LName, IA\_FLName, IA\_FMLName, IA\_Company)
  - Field Type: ☒ Text, ☐ List, ☐ Date, ☐ Yes/No, ☐ Numeric
- Font**
  - Font Name: Arial
  - Font Color: Black
  - Font Height: 12
  - Font Style: ☒ B, ☒ I, ☒ U, ☒ S
- Options**
  - ☐ Word Wrap
  - ☐ Reduce To Fit
  - ☐ Laser Engrave (with 'Laser Settings' button)
- Printing**
  - ☐ Non-Printable Entry
  - ☐ Conditional (with 'Edit Condition' button)
  - ☐ Print on Fluorescing Panel
- Alignment**
  - Horizontal: ☒ Left, ☐ Center, ☐ Right
  - Vertical: ☒ Top, ☐ Middle, ☐ Bottom
  - Rotation: 0 (In degrees CCW)
- Placement**
  - Left: 28.6, Width: 50.5
  - Top: 7.2, Height: 6.3
- Border and Fill**
  - Border Color: Transparent
  - Border Width: 0
  - Fill Color: Transparent

Buttons at the bottom: OK, Cancel

EXAMPLE: To add a photo to the card, select the **Photo** icon, then draw a box where the photo is to be placed on the card. Select **IA\_Photo** as the **Field Name**

**Photo Properties**

**Image**

Field Name:

Format type:

☐ Use a Folder Data Source

☐ This is a Read-only Field

**Data Source**

Source:

Table:

Field:

**Options**

☒ Maintain Aspect Ratio

☐ Transparency

☐ ChromaKey

☐ Invert Image

☐ Laser Engrave

**Placement**

Left:  Width:

Top:  Height:

Rotation angle (CCW):

**Printing**

☐ Non-Printable Entry

☐ Conditional

☐ Print on Fluorescing Panel

☐ Mandatory Entry

**Border and Fill**

Border Color:

Border Width:

**Rounded Corners**

Width:  Height:

For further detailed information on how to use Asure ID, please refer to the HID documentation installed with the software.

Once you have completed your card design click on **File** and **Save Template**. Exit the AsureID Card Designer, then restart the Identity Access User Interface.

**Select Users and Print**

To Print a card from within Identity Access, select **Management** then Select **Employee** / **Visitor** / **Contractor** as appropriate.

Click on the User or Users you wish to print (hold down the **[Ctrl]** key to select



multiple Users) and select the Asure ID icon

Select the relevant Template for the user/s and the printer to be used



a preview of the front and back of the card can then be seen. If printing more than one card, the slider can be used to check each card individually prior to printing.

For advanced options such as multiple copies of each card tick **Show Print Dialog**.

Click **[Print]** to print the card/s.

## **Appendix C - Windows Commands**



## 24 Appendix C - Windows Commands

To access Windows **Control Panel**

**Windows 10** – Right click the **Start** button and select **Control Panel**

**Windows Server 2008** – Click the **Start** button, and select **Control Panel**

**Windows Server 2012** – Place the cursor in bottom right hand corner of the screen, select **Settings** followed by **Control Panel**

To access Windows **Command Prompt**

**Windows 10** – Right click the **Start** button, select **Run**, type `cmd` followed by **[OK]**

**Windows Server 2008** – click the **Start** button, click in the **Search programs and files** field, type `cmd` then select **cmd.exe**

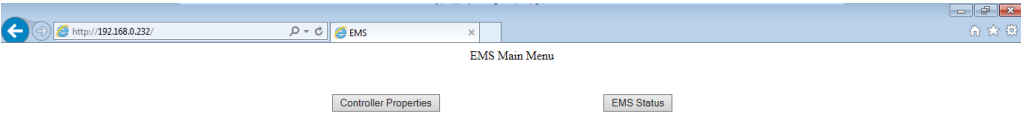
**Windows Server 2012** – Place the cursor in the bottom right hand corner of the screen, select **Search**, type `cmd` in the text field and select **Command Prompt**

## **Appendix D - i-Net webpage**

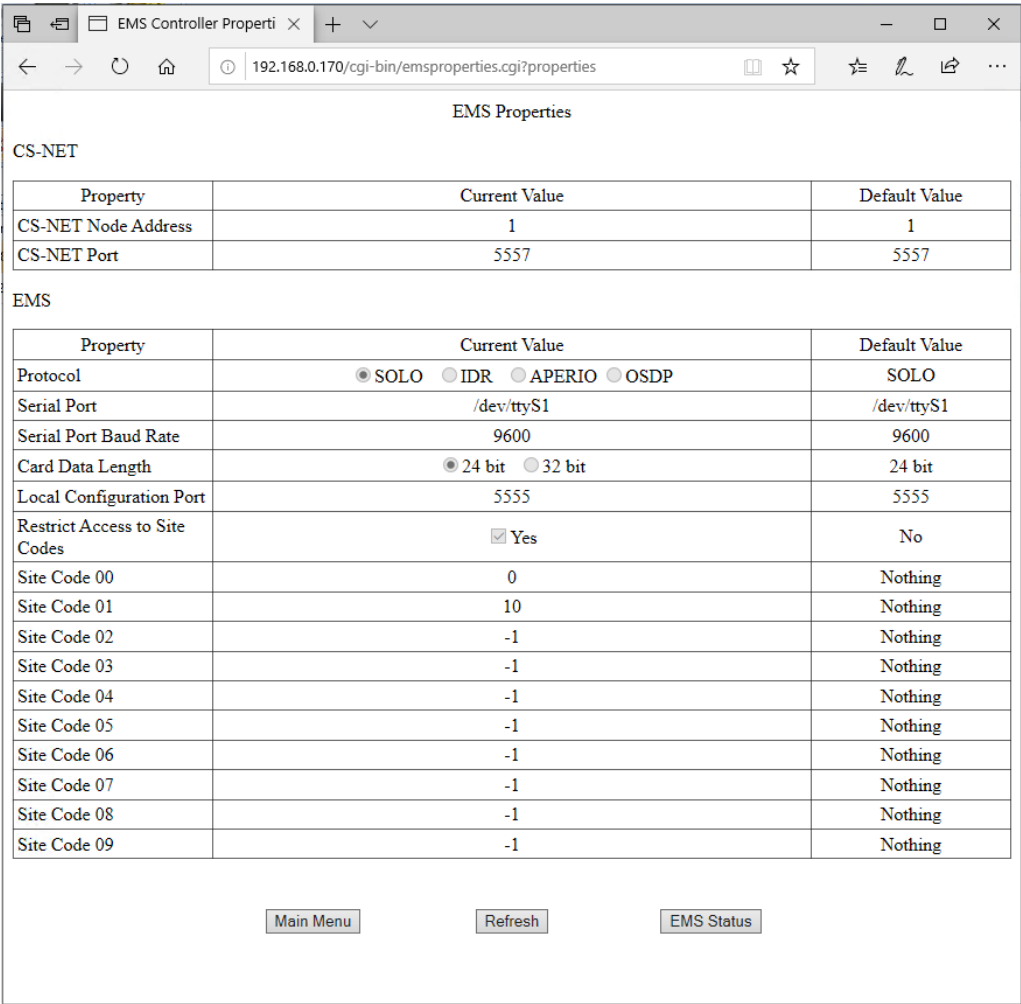
25 Appendix D - i-Net webpage

The iNet controller has a read-only webpage which provides information on the status of the controller. The layout of the page will depend on the firmware version used. This section will show screens from firmware version 9.025 (the most recent version fully compatible with Identity Access V9 software).

To access the webpage, use any browser (e.g. Internet Explorer, Firefox, Chrome) and enter the iNet's IP Address. The landing page displays the options available:



Click the **[Controller Properties]** button:



This screen displays the configuration details of the iNet **NOTE - These parameters cannot be changed in the webpage, but can be**

**changed from within the iNet Configurator software:** (see [IP Controller Configurator](#))<sup>135</sup>

**CS-NET Node Address** and **CS-NET Port**: Not required for Identity Access, these must remain at their default values

**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). **32 bit** 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 Site 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 accepted.



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***

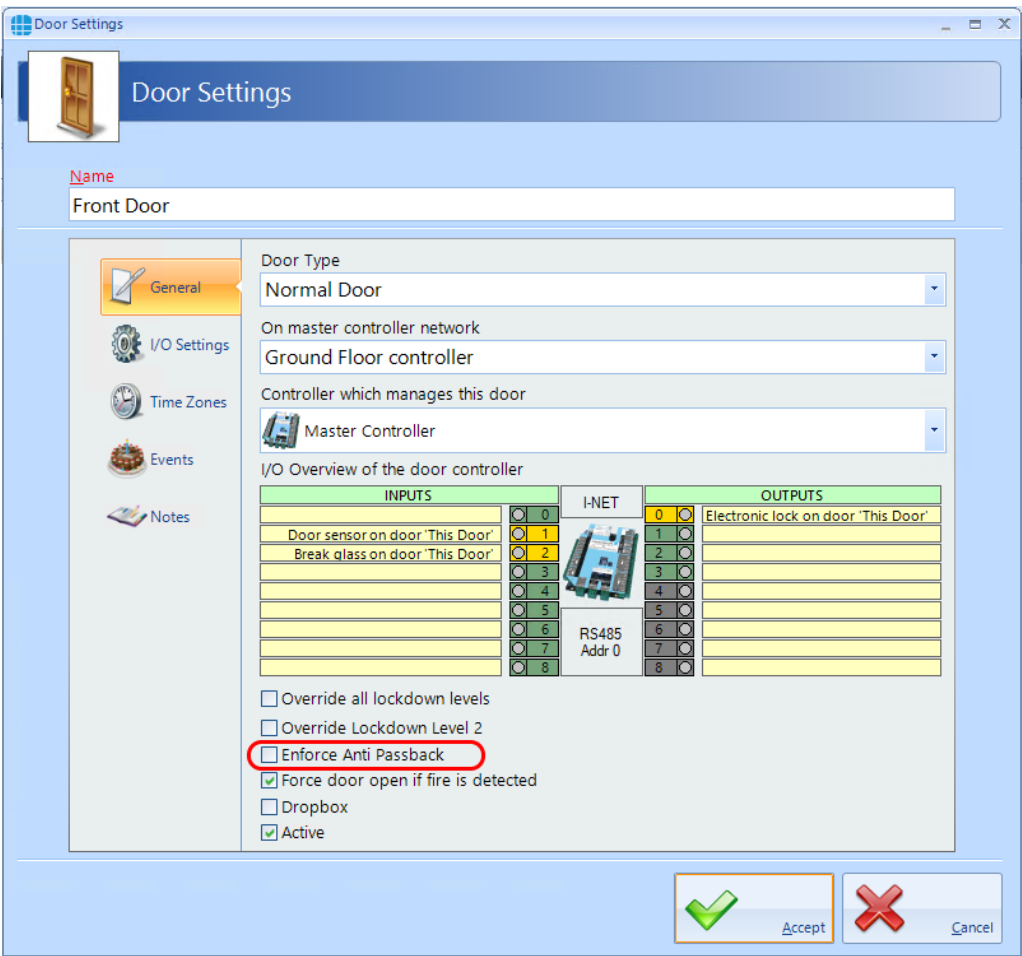
## **Appendix E - AntiPassBack**

26 Appendix E - 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.

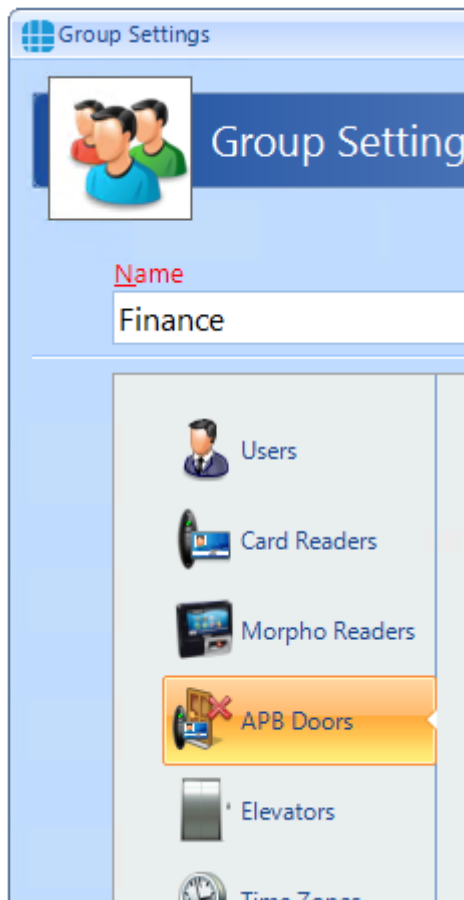
Consider the example where a token is used to move from outside to inside, then the user passes the token to someone else through an open window. When the second user attempts to use the same token to move from outside to inside, AntiPassBack will ensure that access is denied.

To use this feature, enable AntiPassBack for each external door,

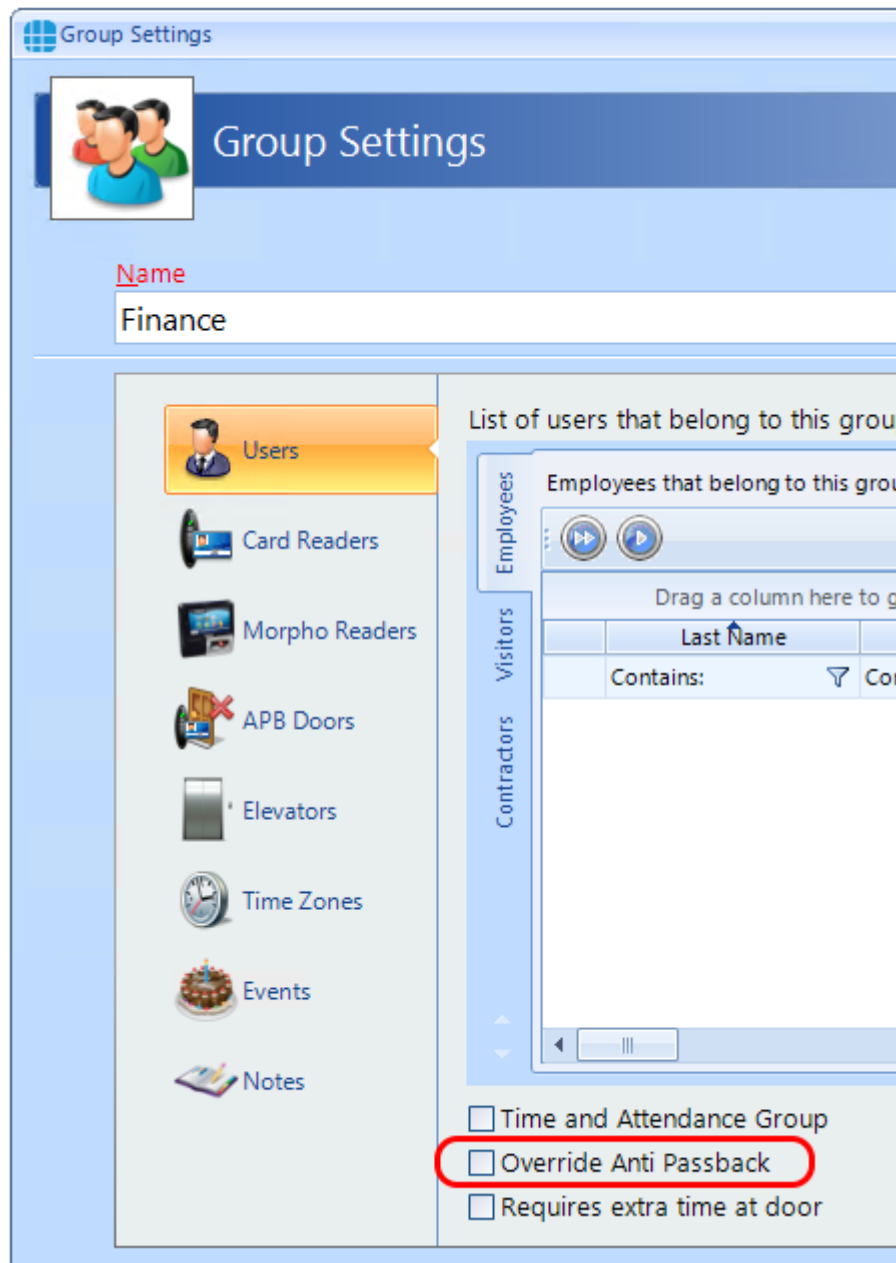




When allocating Access Rights for Groups, be sure to allocate **Card Readers** for doors without AntiPassBack, and **APB Doors** for doors with AntiPassBack

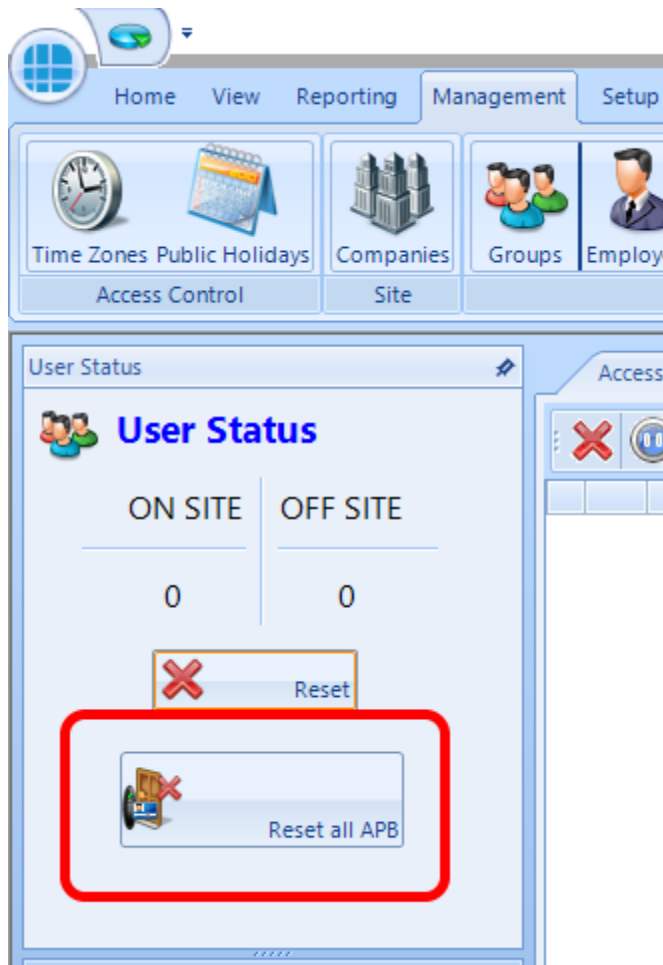


If any User Groups are to be exempt from AntiPassBack, select **Override AntiPassback** for that Group.

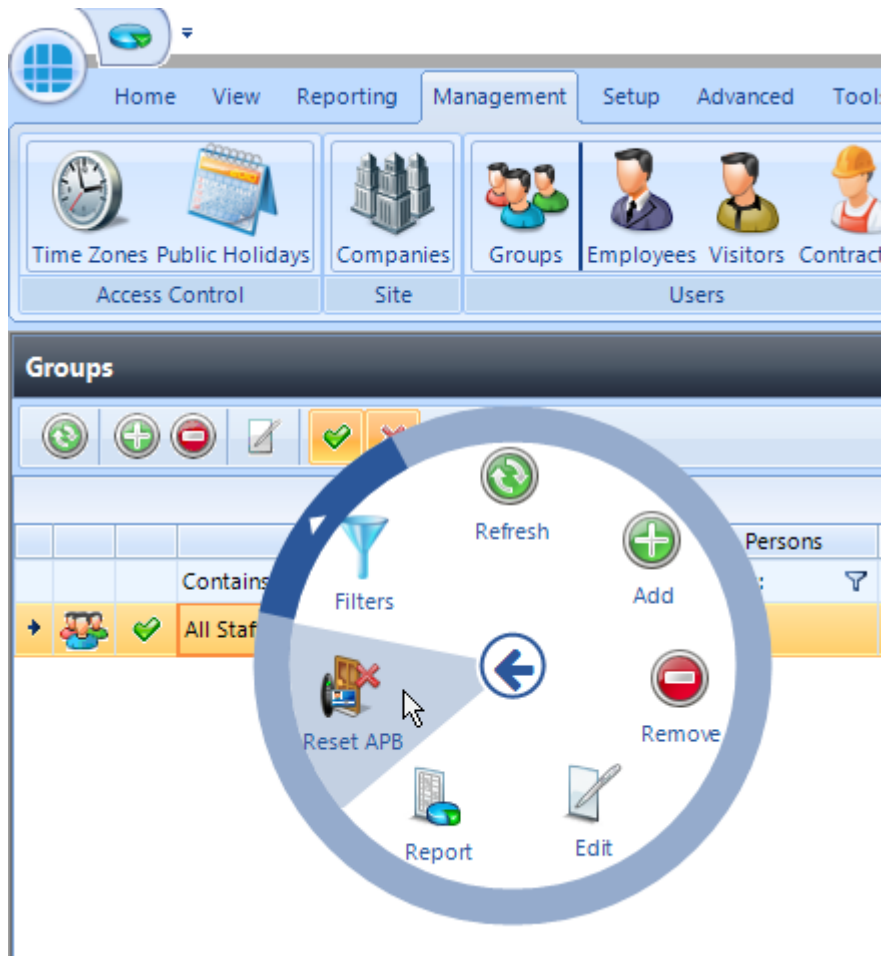


If a user tailgates and finds themselves in an incorrect AntiPassBack zone, it is possible to reset APB as follows:

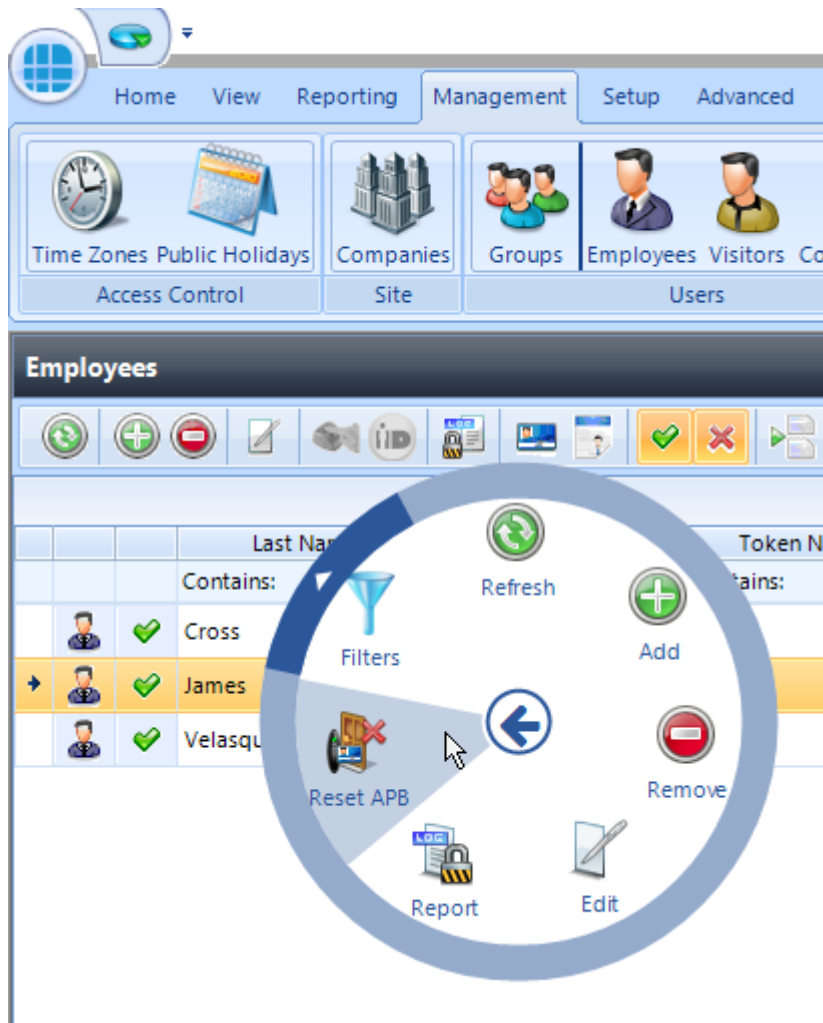
To reset APB for ALL users - click the **Reset ALL APB** button in the dashboard:



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**:



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**:



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](#))<sup>86</sup>.

***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.***

## **Appendix F - i-Net Configurator**

## 27 Appendix F - i-Net Configurator

iNet Configurator is a small utility required to configure the internal settings of the iNet controller. iNet Configurator is installed automatically with Identity Access software.

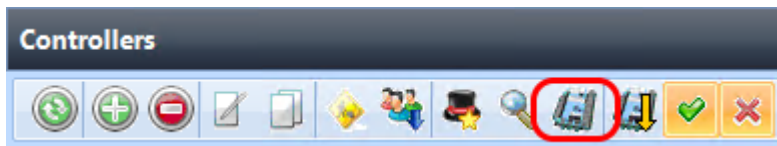
A video on how to configure an iNet controller can be found on our YouTube channel at <https://www.youtube.com/channel/UCMUTUFhnU1et7qqwHFFWKxw>

### Running iNet Configurator

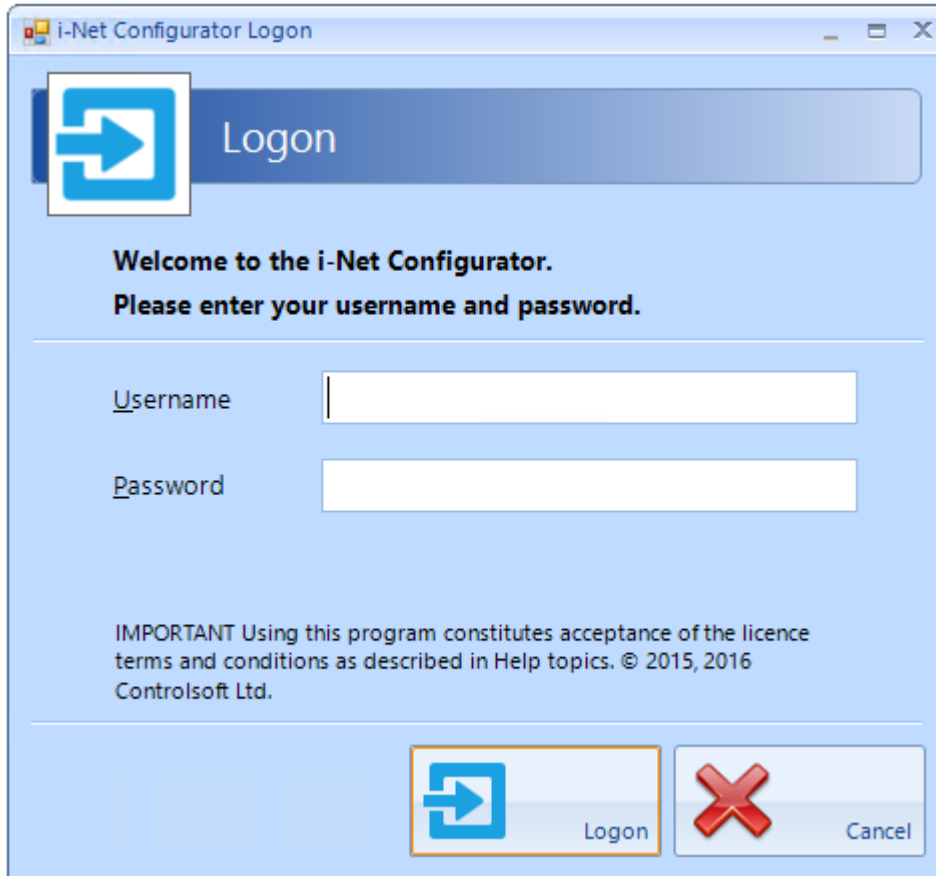
To run the iNet Configurator software, select

**Start > Controlsoft > iNet Configurator**

iNet Configurator can also be run from within IA by selecting a controller in the Controller Manager window and clicking the icon



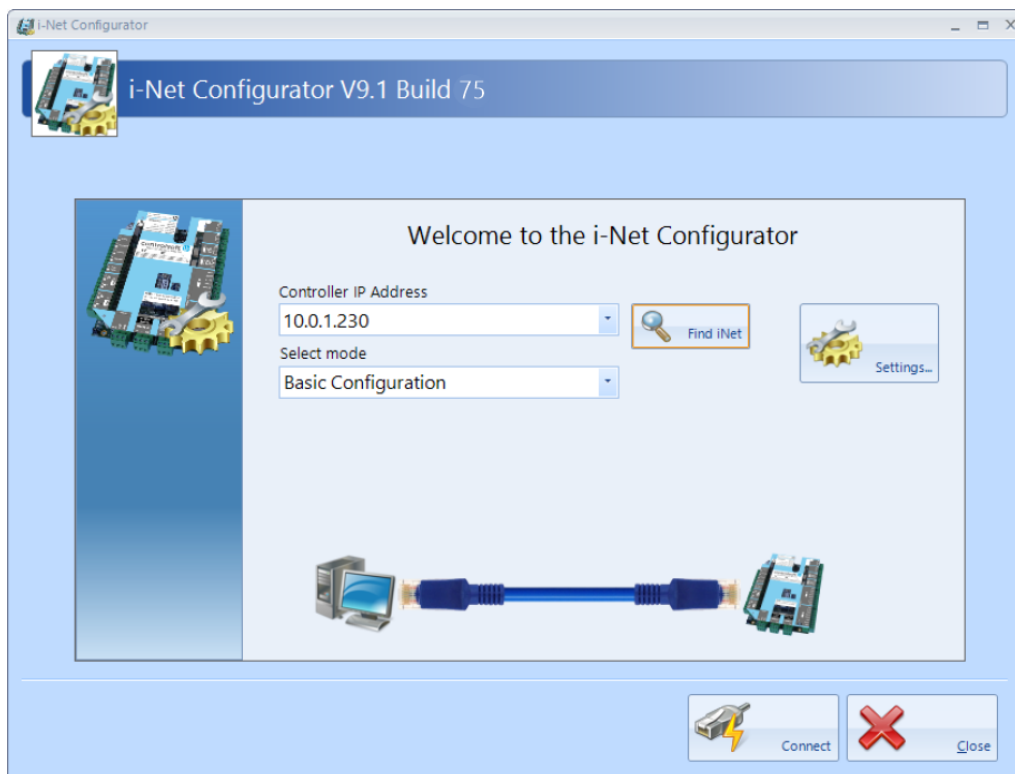
If iNet Configurator has been run as a stand alone application, the login screen will then be displayed:

The image shows a Windows-style dialog box titled "i-Net Configurator Logon". It has a blue header bar with a blue square icon containing a white right-pointing arrow. Below the header, the word "Logon" is written in a large, light blue font. The main area of the dialog is light blue and contains the text "Welcome to the i-Net Configurator. Please enter your username and password." Below this text are two input fields: "Username" and "Password". At the bottom of the dialog, there are two buttons: a "Logon" button with the same blue arrow icon and a "Cancel" button with a red "X" icon. A small disclaimer at the bottom of the dialog reads: "IMPORTANT Using this program constitutes acceptance of the licence terms and conditions as described in Help topics. © 2015, 2016 Controlsoft Ltd."

***NOTE: The default login credentials are Username = Admin, Password = Password. These login credentials are case sensitive. They are stored as part of the standalone application - it does NOT use Identity Access login credentials***

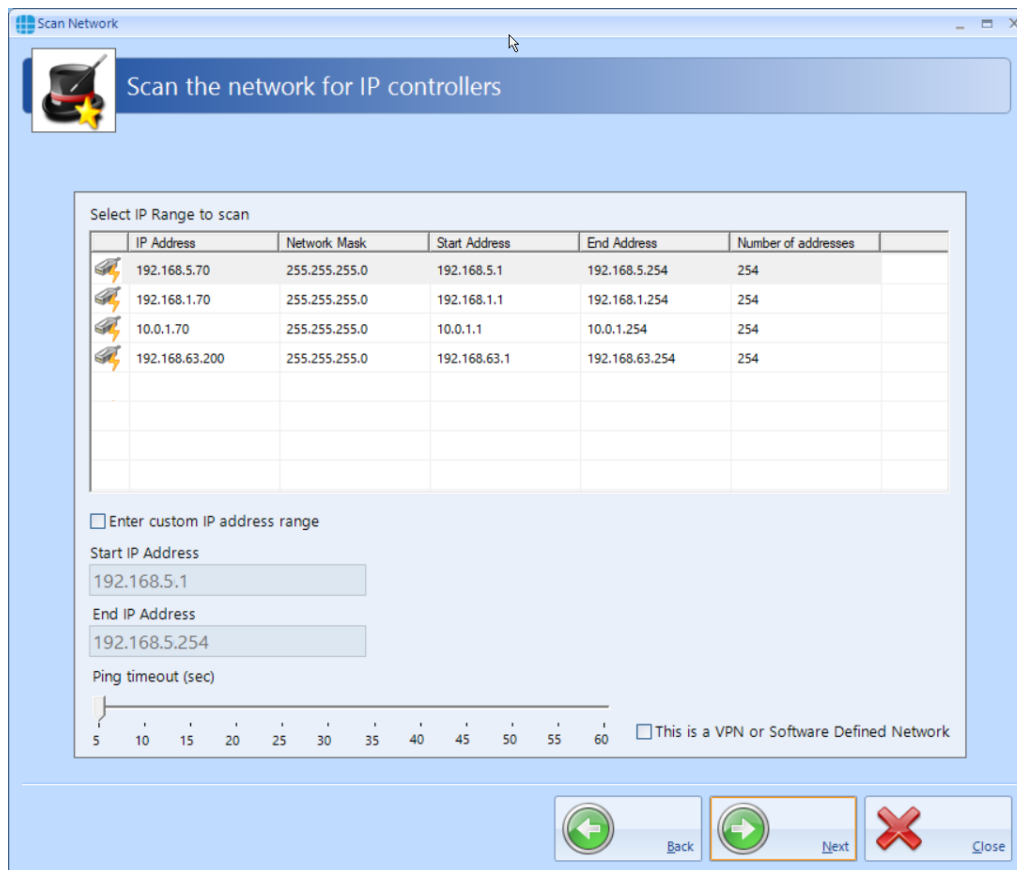
***NOTE: If iNet Configurator is run from within Identity Access, login credentials are NOT required.***





The **Controller IP Address** defaults to the iNet default of 10.0.1.230 unless iNet Configurator has been run from within Identity Access in which case this field will automatically show the IP Address of the selected controller.

The **[Find iNet]** button will search for iNets on a selected network range.



IP Address	Network Mask	Start Address	End Address	Number of addresses
192.168.5.70	255.255.255.0	192.168.5.1	192.168.5.254	254
192.168.1.70	255.255.255.0	192.168.1.1	192.168.1.254	254
10.0.1.70	255.255.255.0	10.0.1.1	10.0.1.254	254
192.168.63.200	255.255.255.0	192.168.63.1	192.168.63.254	254

☐ Enter custom IP address range

Start IP Address  
192.168.5.1

End IP Address  
192.168.5.254

Ping timeout (sec)  
5 10 15 20 25 30 35 40 45 50 55 60

☐ This is a VPN or Software Defined Network

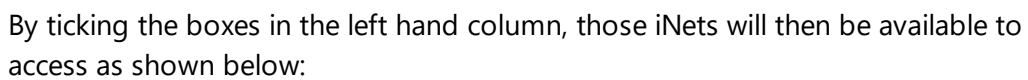
Back Next Close

Select the range to be scanned in the upper window, or if you know the address to be within a specific range of addresses, select **Enter custom IP address range** and enter the **Start** and **End** addresses.

If the controllers are connected across a VPN, select **This is a VPN or Software Defined Network**.

Click **[Next]** to start the scan

When the search is complete, the screen will display a list of iNets found.



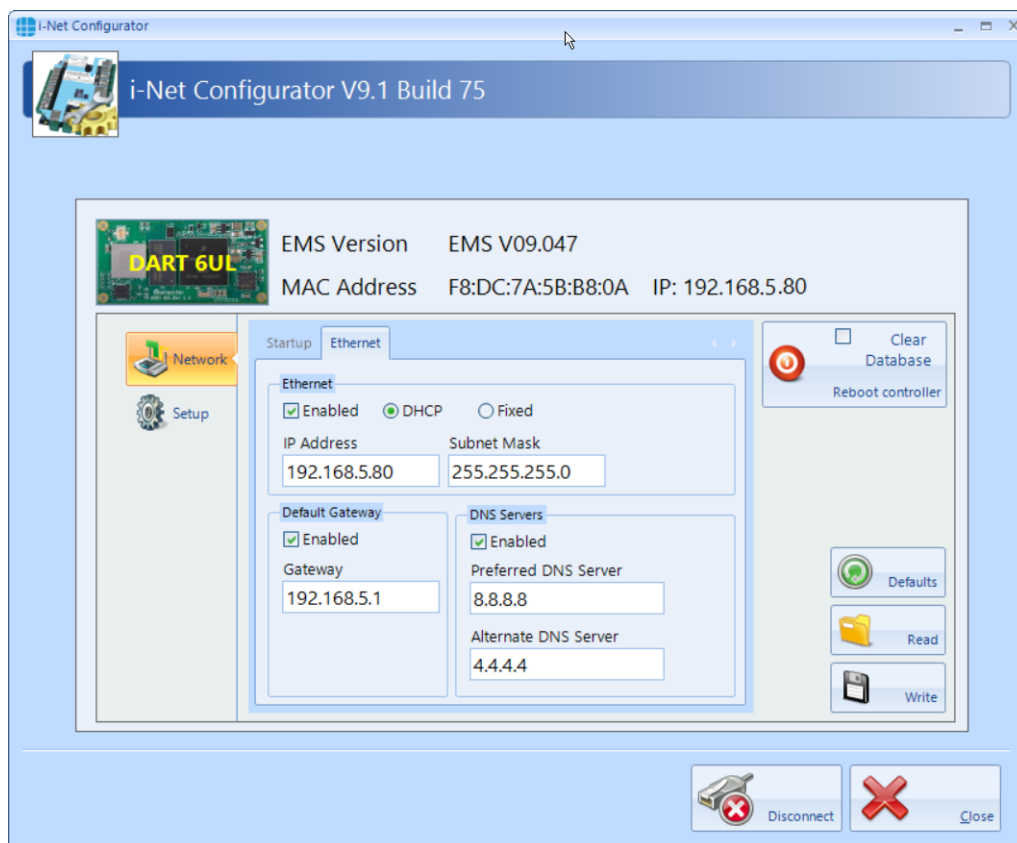
**Select mode** should be left as **Basic Configuration** unless instructed by Controlsoft Technical Support

The **[Settings]** button is used to change the login credentials for a stand alone iNet Configurator.

Click the **[Connect]** button to connect to the controller. The blue 'wire' will turn red if the software cannot connect the controller, or green if it does connect.



When connected, the following screen is displayed:



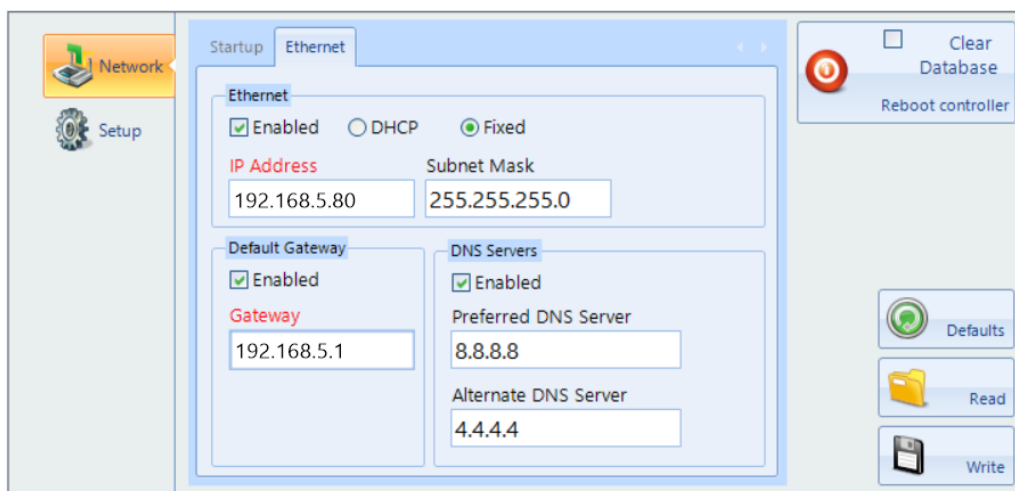
The top section of the screen shows the type of iNet in use. This will either be M501 or M502 for older iNets, or a DART 6UL for the 1DR or 2DR controllers.

This section also shows the **EMS Version** (the firmware in the iNet), as well as the iNet's **MAC Address** Address and **IP** address.

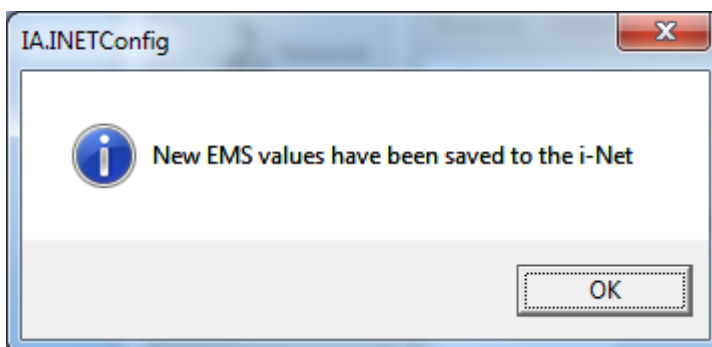
**Network** tab:

Ensure that under **Ethernet**, the option **Enabled** is ticked. From the factory, iNets are configured for **DHCP** which means that they are allocated an IP Address by the router when they power up. This makes it easy to find using Identity Access' "Find Controller" feature. **NOTE: Once found, the Ethernet setting MUST be changed to Fixed to avoid connection problems in the future.**

Enter the required **IP Address**, **Subnet Mask**, **Default Gateway** and **DNS Servers**. These are usually provided by the customer's IT Department. When a change is made, the title will change to red to indicate that the setting has been changed.

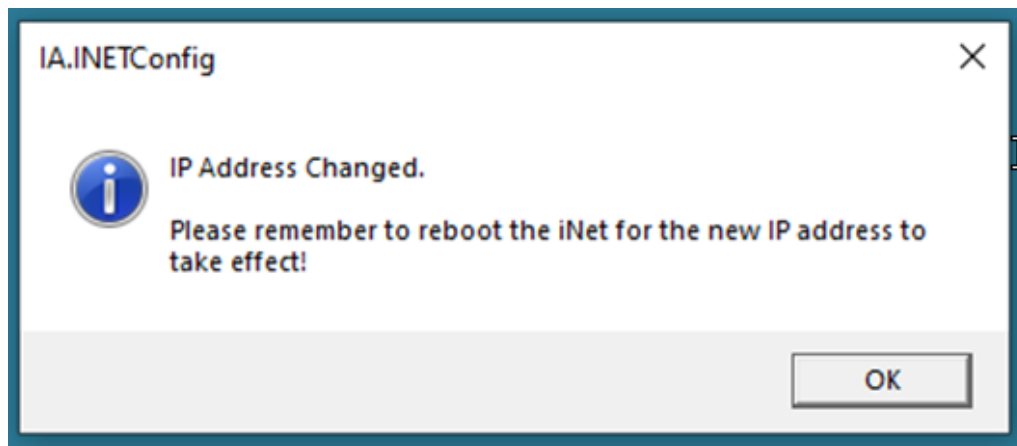


Finally, click on the **[Write]** button to write the new values to the iNet. A dialogue box will indicate that the data has been successfully written

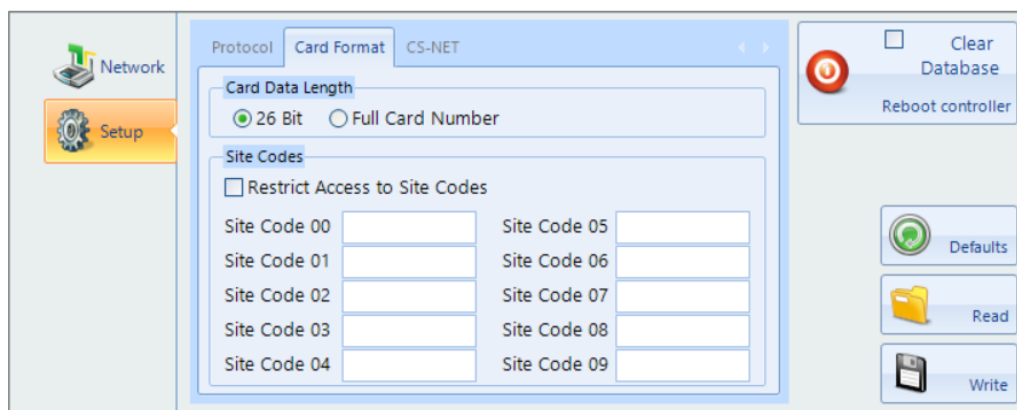


After changing the IP Address of the iNet, the controller must be rebooted to implement the new IP Address. This can be achieved by clicking the **[Reboot controller]** button. If **Clear Database** is selected, the database in the iNet will be wiped prior to the reboot.

NOTE: If you disconnect from the controller before saving the changes, a warning message will appear:



**Setup** tab:



**Card data length.** When set to **26 bit**, the data from the card will be stripped down to 24 data bits, plus 2 parity bits. When set to **Full Card Number**, the whole card number (e.g. 34-bit, 47-bit, 56-bit) will be used.

**SITE CODES:**

This feature increases the security of the system when used with HID readers and certain card formats. The card data is split into 2 parts – the site code and the card number. If the iNet controller is not configured with the same site code as used on the cards, the card number is ignored. Providing the site code in the card and in the iNet match, the card number is used to grant or deny access.

- **Restrict access to site codes** – enable this option to use site codes

- **Site code 00** to **Site Code 09** – the iNet controller can support up to 10 different site codes simultaneously. To use cards with site code 0, the iNet should be configured as follows:

The screenshot shows the 'CS-NET' configuration window in the i-Net Configurator. On the left, there are 'Network' and 'Setup' tabs. The 'Setup' tab is active, showing a 'Card Data Length' section with two radio buttons: '26 Bit' (unselected) and 'Full Card Number' (selected). Below this is a 'Site Codes' section with a checked checkbox labeled 'Restrict Access to Site Codes'. This section contains two columns of input fields for site codes, labeled 'Site Code 00' through 'Site Code 09'. The 'Site Code 00' field contains the value '0'. On the right side of the window, there are several buttons: 'Clear Database' (with a red circular icon), 'Reboot controller' (with a red circular icon), 'Defaults' (with a green circular icon), 'Read' (with a yellow folder icon), and 'Write' (with a floppy disk icon).

**NOTE: Most sites will only use one site code**

After making any changes, click the **[Write]** button to download the changes to the iNet.

Other buttons available in iNet Configurator Network and Setup tabs are:

**[Defaults]** – click this button to set all parameters to default values.

**[Read]** – click this button to read all values from the iNet controller

**[Write]** – click this button to write all values to the iNet controller

**NOTE: When changing the IP Address, the iNet controller must be rebooted after writing the settings to the iNet. This can be done by clicking the **[Reboot controller]** button.**

## 27.1 Upgrading iNet Firmware

### Upgrading iNet Firmware

**NOTE: WHEN CONNECTING A 1DR OR 2DR CONTROLLER TO AN RS485 BUS, ALL CONTROLLERS CONNECTED TO THAT BUS MUST BE UPGRADED TO FIRMWARE**

**VERSION V9.044 OR LATER.****FAILURE TO DO THIS WILL CAUSE OPERATIONAL ISSUES.**

Although iNet firmware can be upgraded over the LAN, we strongly recommend that this is done locally at the iNet controller, by plugging a LAN cable directly between your laptop and the iNet. RS485 Downstream devices can only be upgraded locally.

**Upgrading firmware on a V3 iNet with an M501 or M502 processor board**

Download the latest firmware from <https://www.controlsoft.com/downloads/>

Open the zip file (e.g. CSUpdate\_v09\_045.zip) and save the extracted folder on your hard drive.

Open the update folder and double click the update\_ems program (e.g. update\_ems\_v09\_045.bat)

When prompted, enter the IP Address of the iNet controller and press [Enter]

The iNet controller will reboot automatically when the upgrade is complete. Please ensure that once it is back online, you do a full download to the controller from the IA user interface.

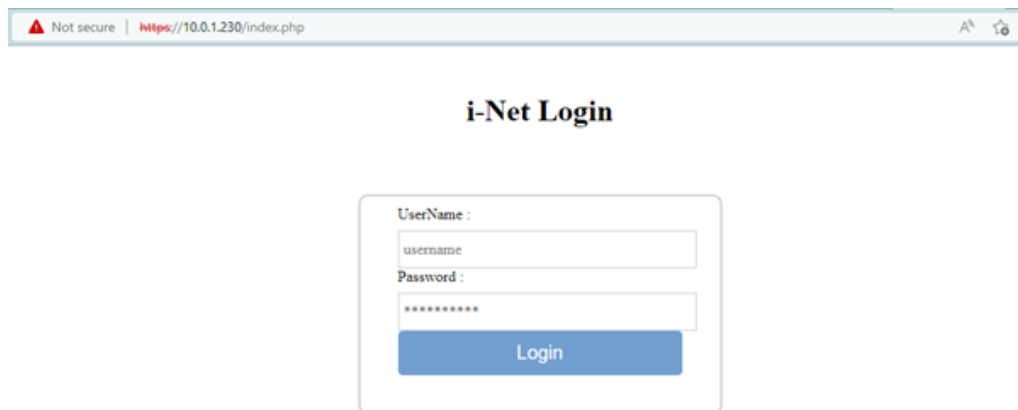
**Upgrading firmware on a 1DR or 2DR iNet**

Download the latest firmware from <https://www.controlsoft.com/downloads/>

Save the firmware file (e.g. ems\_09.045r0\_cortex7t2hf-neon.ipk) in a suitable location such as the desktop

Open a web browser and enter the IP Address of the iNet, this will display the login page for that controller.





The screenshot shows a web browser window with the address bar displaying "https://10.0.1.230/index.php". The page title is "i-Net Login". The login form contains two input fields: "UserName :" with the text "username" and "Password :" with masked characters "\*\*\*\*\*". Below the fields is a blue "Login" button.

**NOTE: When connecting to a controller for the first time, your browser may display a privacy error, just continue to the controller**

Enter the username and password for the controller. The default login details are:

Username: **inet-admin**

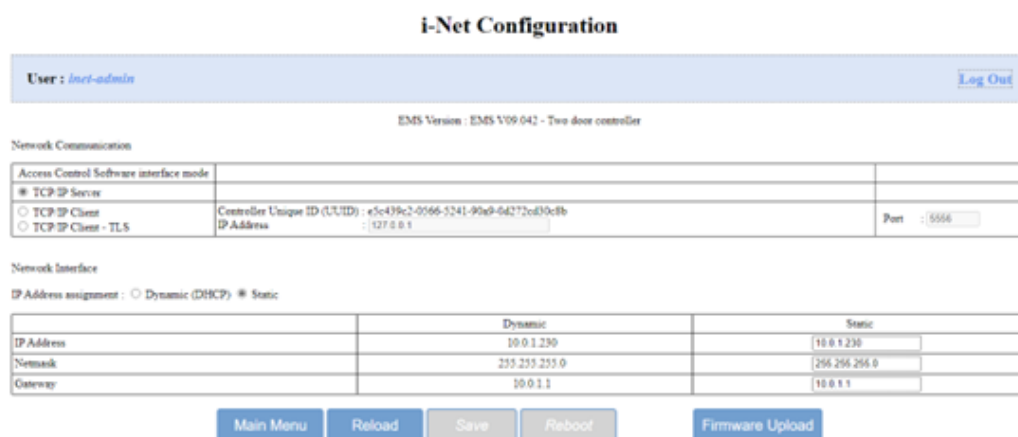
Password: **inetadm01@!**

This will display the main menu:



The screenshot shows the "i-Net Main Menu" page. At the top, it says "User: inet-admin" and "Log Out". Below this, it says "EMS Version : EMS V09.042 - Two door controller". There are three buttons: "i-Net Settings", "i-Net Status", and "i-Net Configuration".

Select **[iNet Configuration]**



The screenshot shows the "i-Net Configuration" page. At the top, it says "User: inet-admin" and "Log Out". Below this, it says "EMS Version : EMS V09.042 - Two door controller". The page is divided into two sections: "Network Communication" and "Network Interface".

**Network Communication**

Access Control Software interface mode	
<input checked="" type="radio"/> TCP/IP Server	
<input type="radio"/> TCP/IP Client	Controller Unique ID (UUID) : e5c439c2-0566-5241-90e9-04272cd30c8b
<input type="radio"/> TCP/IP Client - TLS	IP Address : 192.0.0.1 Port : 5555

**Network Interface**

IP Address assignment : ☐ Dynamic (DHCP) ☒ Static

	Dynamic	Static
IP Address	10.0.1.230	10.0.1.230
Netmask	255.255.255.0	255.255.255.0
Gateway	10.0.1.1	10.0.1.1

At the bottom, there are five buttons: "Main Menu", "Reload", "Save", "Reboot", and "Firmware Upload".

Click on **[Firmware Upload]** to display the Upload screen

**i-Net Firmware Upload**

User : *inet-admin*

Log Out

EMS Version : EMS V09.042 - Two door controller

Upload

File to upload : <a href="#">Choose File</a> No file chosen	Upload	
Note: Only .ipk format allowed to a max size of 10 MB		

Install package

	Install	
--	---------	--

[i-Net Settings](#)[i-Net Status](#)[i-Net Configuration](#)

Click on **[Choose File]**, to open file explorer.

Select the firmware file saved previously, or you can drag and drop the file over the **[Choose File]** button.

Then click **[Upload]**

Once the file has been uploaded successfully, click **[Install]**

EMS Version : EMS V09.044 - Two door controller

Upload

File to upload : <a href="#">Choose File</a> No file chosen	Upload	
Note: Only .ipk format allowed to a max size of 10 MB		

Install package

	Install	The package ems_09.044-r0_cortexa7t2hf-neon.ipk was installed successfully. Output: gpiotest: no process found met_w_led: no process found 1 ems: no process found gpiotest: no process found met_w_led: no process found 0 Upgrading ems from 09.042-r0 to 09.044 on root Configuring ems.
--	---------	---

[i-Net Settings](#)[i-Net Status](#)[i-Net Configuration](#)

The controller firmware has now been updated. Reboot the controller and when it is back online, do a full download from the IA user interface.

## **Appendix G - Product History**

## 28 Appendix G - Product History

**v9.1.75** - Released October 2022 (Requires Firmware version 9.046 or later in all controllers)

- Inclusion of new 1DR and 2DR controllers (Requires Firmware version 9.048 or later in all 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)

- 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
- 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:
  - 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
- 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 unlicensed 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
- 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](http://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](http://xxx.controlsoft.com))
3. Use Microsoft SQL Management Studio 2014 to restore the original database

**v2016.1** - Initial Release

## **Appendix H - Downloading Software**

## 29 Appendix H - Downloading Software

Identity Access software can be downloaded for free from the Controlsoft website [www.controlsoft.com](http://www.controlsoft.com)

Select "login" in the top right hand corner, then enter the username and password and click **[Submit]** to access the Client Login Area. If you do not know these login credentials, please contact Controlsoft Technical Support (contact details are on the website).

Select **See All** under **Software Downloads** to see all the downloadable files.

To make the download manageable, the files have been split into sections as described below:

**Identity Access Server and Client** - everything required for a basic Identity Access installation, including the server software, client software, SQL Express and manuals,

**Identity Access Extras** - additional files for enrolment reader, videos, iNet Configurator (standalone version), Morpho Toolbox and database backup software,

**Identity Access SQL Management Studio** - Microsoft software for advanced users to restore database backups.

Simply download and run the required zip file .

***NOTE: Always check the website periodically for new releases of Identity Access software.***

## **Appendix I - Licence Terms & Conditions**

## 30 Appendix I - Licence Terms & Conditions

### Identity Access Version 9

Copyright (C) 2015, 2020 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.

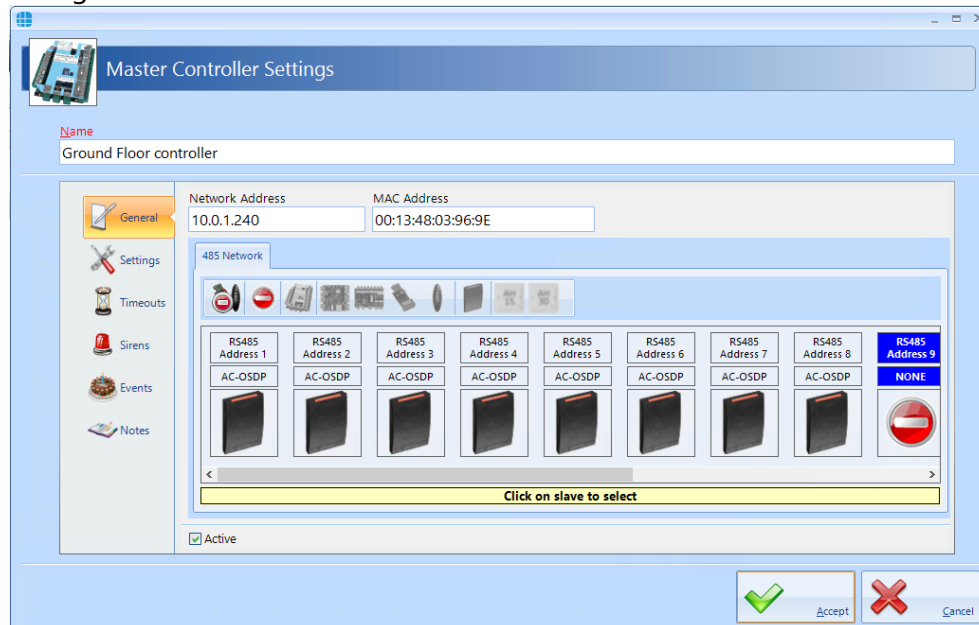
## **Appendix J - HID OSDP Readers**

## 31 Appendix J - HID OSDP Readers

OSDP (Open Supervised Device Protocol) Readers from HID are variants of the iCLASS SE, multiCLASS SE and Signo readers which communicate with the iNet controller over RS485 Port A. OSDP readers can be used with the iNet in 2 ways:

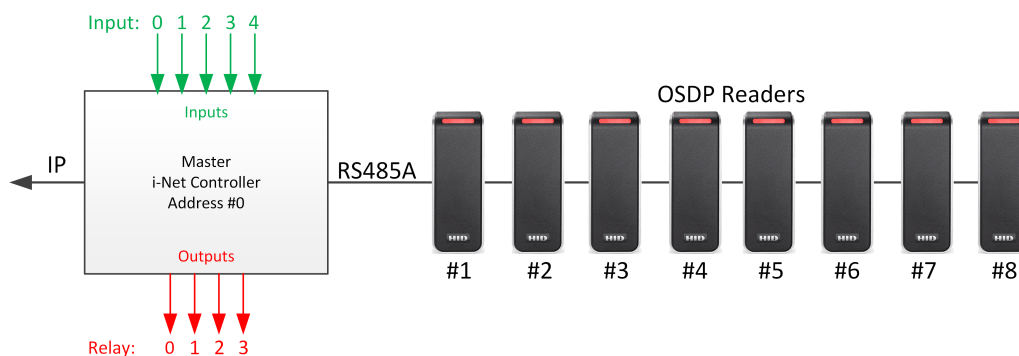
### 1. Up to 8 OSDP readers controlling 4 doors on a single iNet controller

The 8 readers are connected to the RS485 bus and the controller is configured as follows:



The system is then configured to provide the following links:

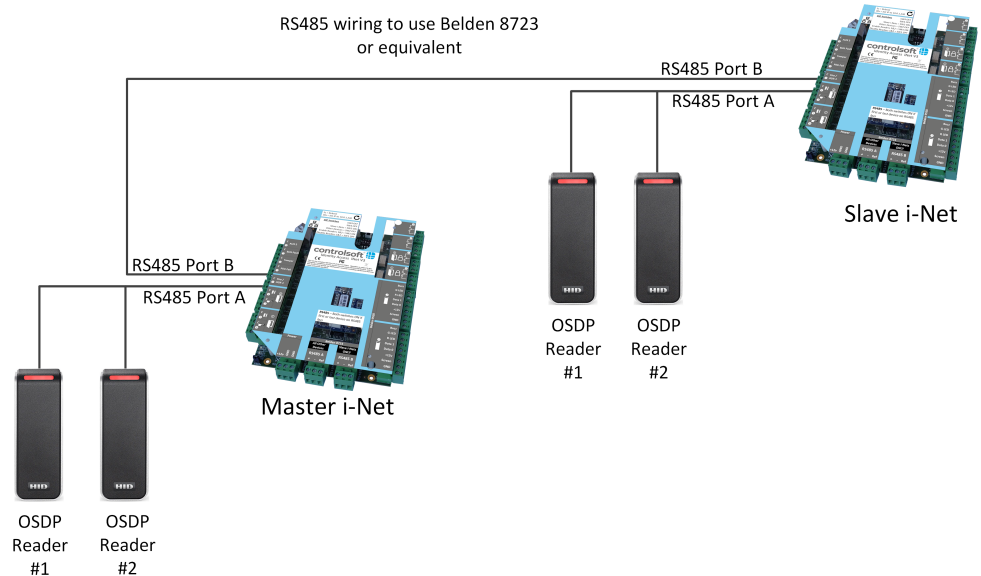
- Reader #1 is the IN reader for iNet relay 0 (Door 1)
- Reader #2 is the OUT reader for iNet relay 0 (Door 1)
- Reader #3 is the IN reader for iNet relay 1 (Door 2)
- Reader #4 is the OUT reader for iNet relay 1 (Door 2)
- Reader #5 is the IN reader for iNet relay 2 (Door 3)
- Reader #6 is the OUT reader for iNet relay 2 (Door 3)
- Reader #7 is the IN reader for iNet relay 3 (Door 4)
- Reader #8 is the OUT reader for iNet relay 3 (Door 4)



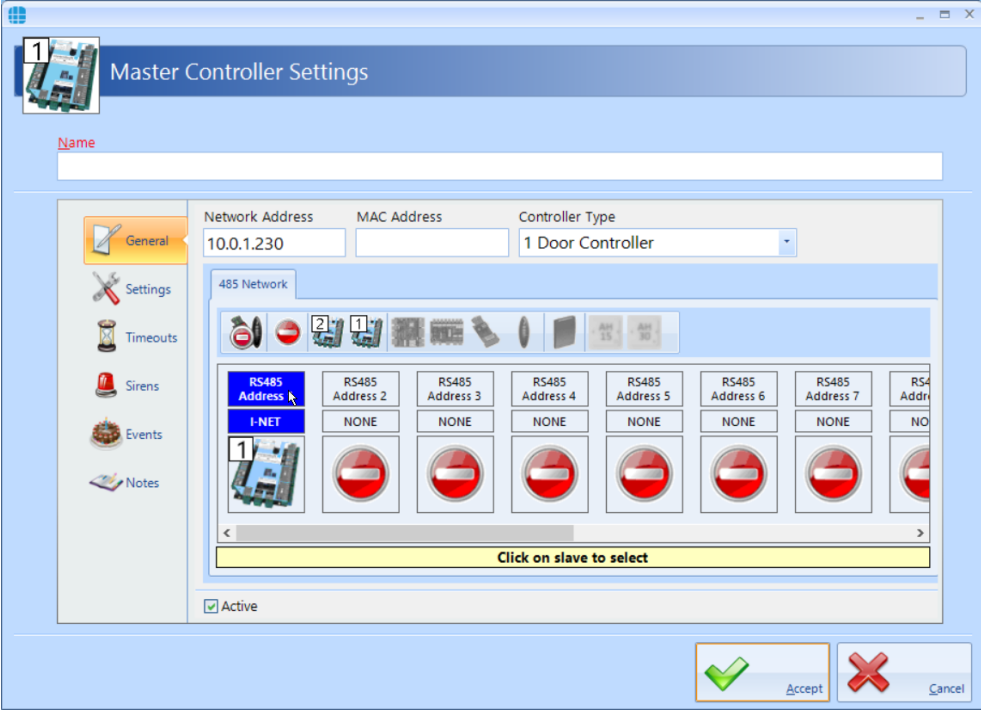


2. To replace the on-board Wiegand readers

In this configuration, the OSDP readers simply replace the on-board Wiegand readers to provide a more secure solution.



In this configuration, Downstream iNets are programmed onto the RS485 bus, NOT OSDP readers



## **Appendix K - Adding Morpho Readers**



The screenshot displays the 'Card Reader Settings' window. At the top, the title bar reads 'Card Reader Settings'. Below the title bar, there is a header area with a card reader icon and the text 'Card Reader Settings'. The main content area is divided into a left sidebar and a right pane. The sidebar contains icons for 'General' (selected), 'Time Zones', 'Settings', 'Events', and 'Notes'. The right pane is titled 'Card Reader Settings' and contains the following fields and options:

- Name:** A text field containing 'Main Entrance Card Reader'.
- On master controller network:** A dropdown menu set to 'Ground Floor controller'.
- Select slave network:** A dropdown menu set to 'RS485 network device'.
- Master Controller:** A dropdown menu set to 'Master Controller'.
- Reader:** A diagram showing a circular reader with two ports labeled '1' and '2'. Port '2' is highlighted.
- This reader controls:** A dropdown menu set to 'Door'.
- Location:** A dropdown menu set to 'Main Entrance'.
- Options:**
  - ☐ This is a dropbox reader
    - ☐ Reader controls dropbox only
    - ☐ Reader controls dropbox and door
  - ☐ Ignore user time zones
  - ☐ Reader has a PIN pad attached
  - ☒ Allow shunting
  - ☐ Reader is used for Time and Attendance
- Location:** A dropdown menu set to 'Not applicable'.
- Active:** A checkbox that is checked.

At the bottom right of the window, there are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel' (with a red X icon).

When connecting the Morpho reader, the physical Wiegand Out cabling of the Morpho Sigma Series device is connected to the Wiegand input on the iNet controller (port 2 in this example).

When programming the Morpho reader, it MUST be linked to the above card reader, which is selected under the option "Link to a Wiegand Reader" as shown below:

Morpho Reader Settings

Name  
Main Entrance

General

Device Type  
MA Sigma, MA Sigma Lite, MA Sigma Extreme

IP Address  
192.168.0.223

Port  
11010

Device Profile  
01. Biometric Only - ACU mode. (34 Bit)

Facility code

Location  
Not applicable

Link to a Wiegand reader

Ground Floor Controller

Main Entrance Card Reader

☐ Use reader for fingerprint enrolment

☐ Reboot reader after full download

☐ Reader is used for Time and Attendance

☒ Active

Accept Cancel

When choosing the Device Profile, select the relevant ACU Mode profile for the authentication level required, such as "Biometric Only – ACU Mode (34 bit)" or "Biometric and HID iCLASS 47 bit – ACU mode"

***NOTE: When creating Groups, adding a Morpho reader will automatically add the linked card reader (and visa versa).***

When used in Standalone Mode, however, the Morpho Sigma reader makes the decision whether to release the door, no iNet controller is needed.

In Standalone Mode, we only need to create a Morpho Reader on the system. Do NOT create a door or Request to Exit button within the Identity Access system as the Request to Exit button is wired directly into the Morpho Reader.



When choosing the Device Profile, select the relevant Standalone Mode profile such as "Biometric Only – Standalone Mode" or "Biometric and HID iCLASS 26 bit – Standalone mode"

The screenshot shows the 'Morpho Reader Settings' window. The 'Name' field is set to 'Main Entrance'. The 'General' tab is selected in the left sidebar. The 'Device Type' dropdown is set to 'MA Sigma, MA Sigma Lite, MA Sigma Extreme'. The 'IP Address' is '192.168.0.223' and the 'Port' is '11010'. The 'Device Profile' dropdown is set to '02. Biometric Only - Standalone mode.'. The 'Location' dropdown is set to 'Not applicable'. The 'Facility code' field is empty. At the bottom, there are four checkboxes: 'Use reader for fingerprint enrolment' (unchecked), 'Reboot reader after full download' (unchecked), 'Reader is used for Time and Attendance' (unchecked), and 'Active' (checked). At the bottom right, there are 'Accept' and 'Cancel' buttons with green and red checkmark icons respectively.

When creating Groups, simply add the Morpho reader to the relevant group/s to define the access rights at the door.

**NOTE: Morpho readers configured for PIN will use the employees token number as the PIN.**

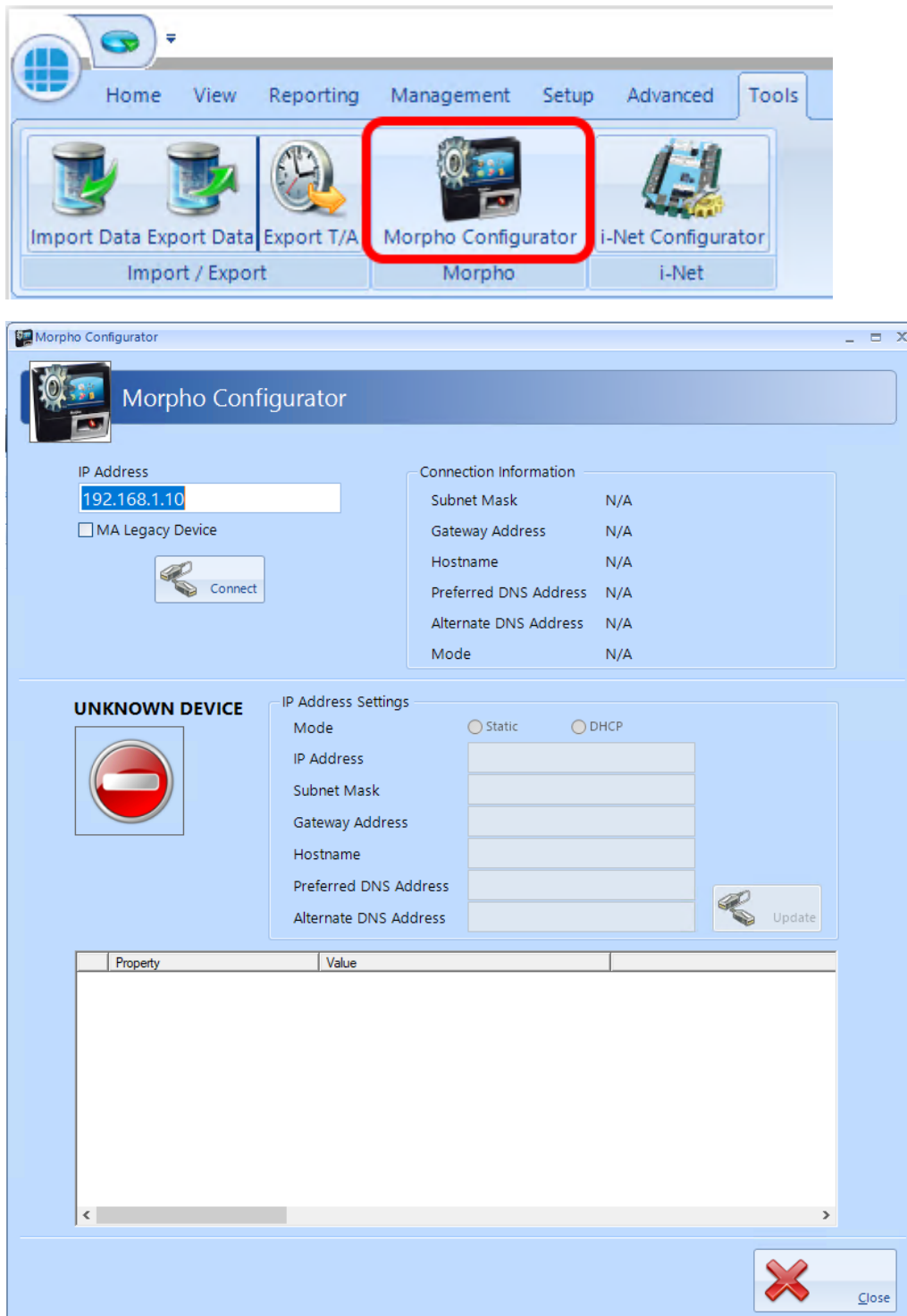


## **Appendix L - IA Morpho Configurator**



### 33 Appendix L - 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



Enter the **IP Address** of the fingerprint reader and click the **[Connect]** button

**Morpho Configurator**

IP Address: 192.168.0.223  
☐ MA Legacy Device  
 Connect

**Connection Information**

Subnet Mask: 255.255.255.0  
 Gateway Address: 192.168.0.1  
 Hostname: MAsigma-lite-plus  
 Preferred DNS Address:  
 Alternate DNS Address:  
 Mode: Static

**MA SIGMA Lite+ WR**

**IP Address Settings**

Mode: ☒ Static ☐ DHCP  
 IP Address: 192.168.0.223  
 Subnet Mask: 255.255.255.0  
 Gateway Address: 192.168.0.1  
 Hostname: MAsigma-lite-plus  
 Preferred DNS Address:  
 Alternate DNS Address:  
 Update

Property	Value
<input checked="" type="checkbox"/> Name	MA SIGMA Lite+ WR
<input checked="" type="checkbox"/> Firmware version	4.3.2
<input checked="" type="checkbox"/> Serial number	1623SML0006582
<input checked="" type="checkbox"/> Part number	293667795
<input checked="" type="checkbox"/> Specific part number	293667795
<input checked="" type="checkbox"/> License ID	293673201-16151511424-03405995273
<input checked="" type="checkbox"/> Licenses	MA_PAC;MA_WIFI;BCL;VERIF;MIMA;MA_TA;MA...
<input checked="" type="checkbox"/> Reader type	Unknown reader type

Close

**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]**

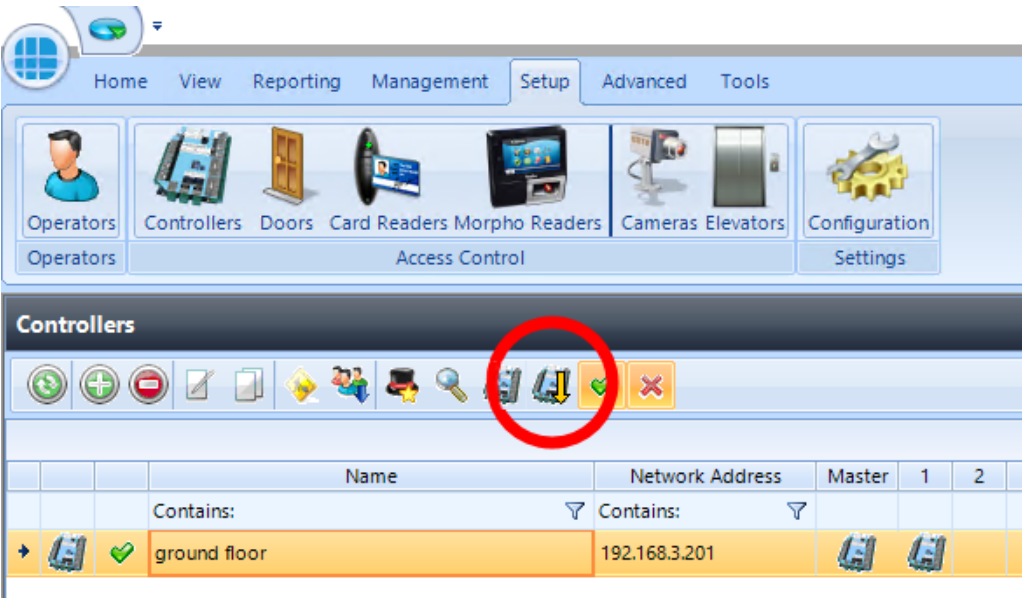
The final window displays details of the reader itself, whether it has an integral reader, the firmware version, serial number etc.

**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**

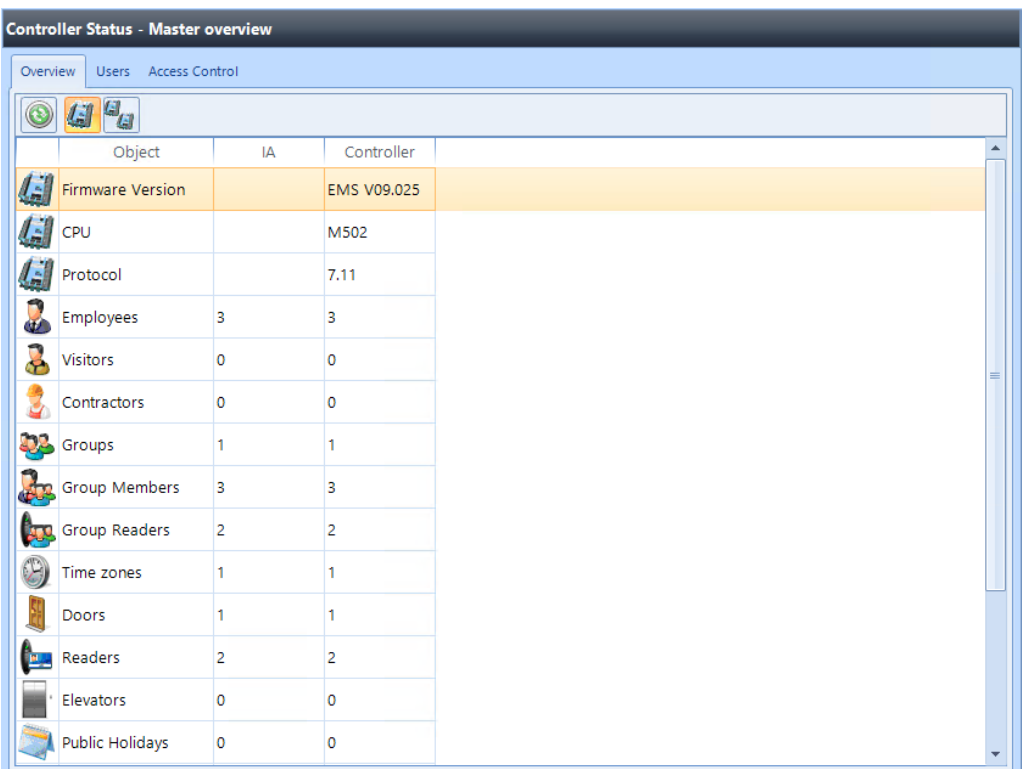
**Appendix M - Controller Status**

34 Appendix M - 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 **Setup** menu, select the required controller and click the **Controller Status** button:

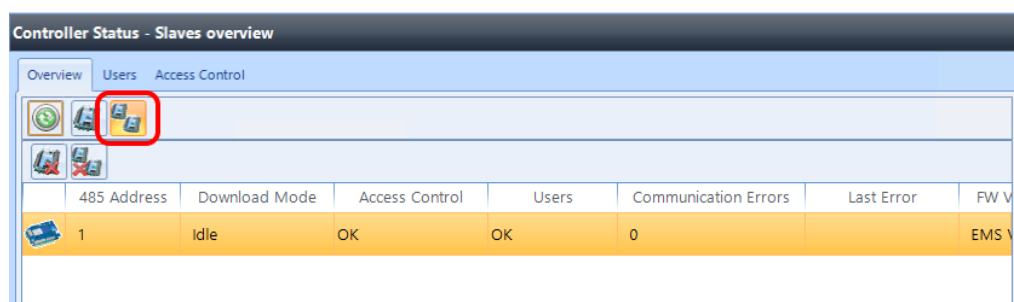


The Controller Status window will now appear on the left-hand side of the screen. Select the **Overview** tab then the **Master Controller** button:



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:



485 Address	Download Mode	Access Control	Users	Communication Errors	Last Error	FW Version
1	Idle	OK	OK	0		EMS

**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:

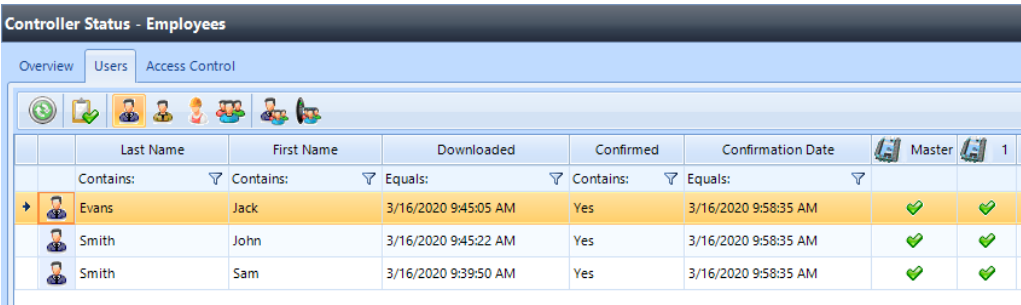


- Clear communication errors on selected downstream controller



- 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 .



	Last Name	First Name	Downloaded	Confirmed	Confirmation Date	Master	1
	Contains: ▾	Contains: ▾	Equals: ▾	Contains: ▾	Equals: ▾		
→	Evans	Jack	3/16/2020 9:45:05 AM	Yes	3/16/2020 9:58:35 AM	✓	✓
	Smith	John	3/16/2020 9:45:22 AM	Yes	3/16/2020 9:58:35 AM	✓	✓
	Smith	Sam	3/16/2020 9:39:50 AM	Yes	3/16/2020 9:58:35 AM	✓	✓

The following information is now displayed:

The name of the employee

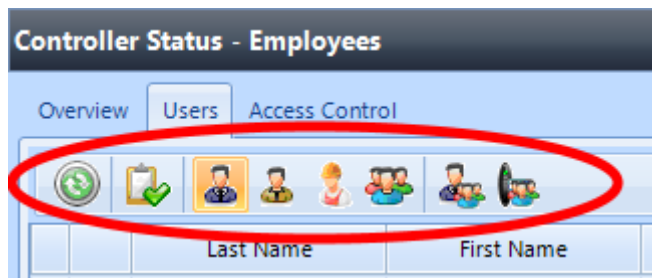
When the employee was downloaded

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:



- 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



- 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.



Controller Status - Doors									
Overview Users Access Control									
	Name	Downloaded	Confirmed	Confirmation Date	Master	1	2	3	
	Contains: ▾	Equals: ▾	Contains: ▾	Equals: ▾					
+	Back Door	3/16/2020 9:39:04 AM	Yes	3/16/2020 10:03:40 AM		✓			
	Front Door	3/16/2020 9:39:04 AM	Yes	3/16/2020 10:03:40 AM	✓				
	Server Room	3/16/2020 9:39:04 AM	Yes	3/16/2020 10:03:40 AM	✓				
	Warehouse	3/16/2020 9:39:04 AM	Yes	3/16/2020 10:03:40 AM		✓			

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

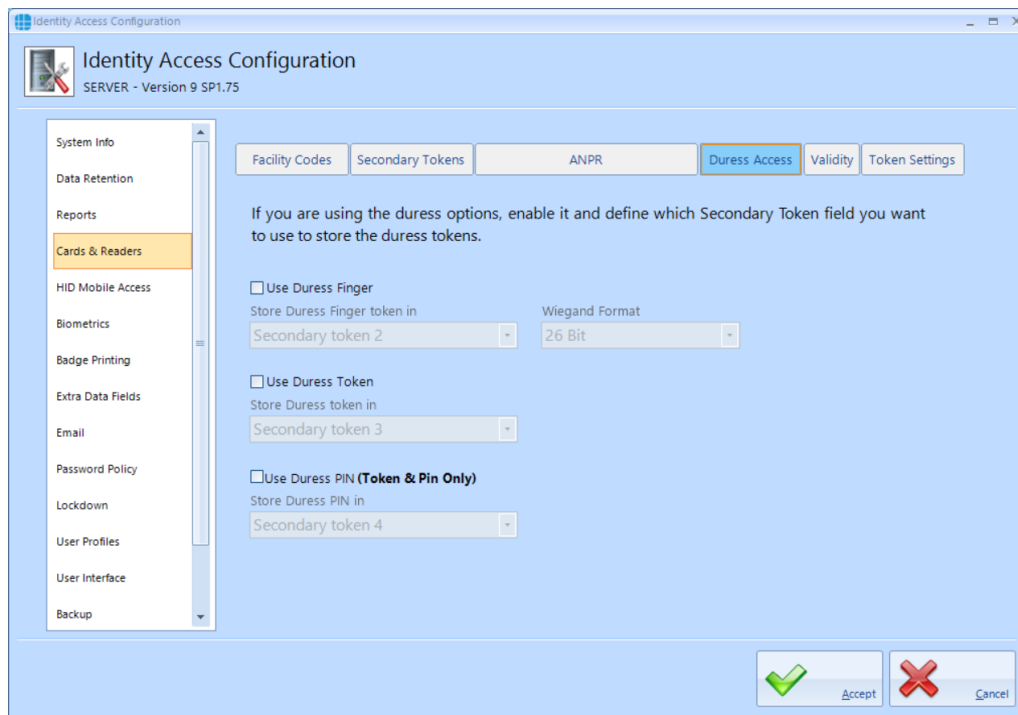
Controller Status - Employees									
Overview Users Access Control									
	Last Name	First Name	Downloaded	Confirmed	Confirmation Date	Master	1		
	Contains: ▾	Contains: ▾	Equals: ▾	Contains: ▾	Equals: ▾				
+	Evans	Jack	3/16/2020 9:45:05 AM	Yes	3/16/2020 9:53:31 AM	✓	✗		
	Smith	John	3/16/2020 9:45:22 AM	Yes	3/16/2020 9:53:31 AM	✓	✗		
	Smith	Sam	3/16/2020 9:39:50 AM	Yes	3/16/2020 9:53:31 AM	✓	✗		

## **Appendix N - Duress**

## 35 Appendix N - 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:

The screenshot shows the 'Employee Settings' window. At the top, there's a header bar with a user profile icon and the title 'Employee Settings'. Below this, there are input fields for 'Title', 'First Name' (containing 'Oliva'), 'Middle Name', and 'Last Name' (containing 'Cross'). The main area is divided into a left sidebar with icons for 'General', 'Photo', 'Fingerprints', 'Mobile Access', 'Tokens' (highlighted), 'Extra Data', 'Contact', 'Events', and 'Notes'. The 'Tokens' section is active, showing fields for 'Secondary token 1', 'Duress Finger token', 'Duress Token', 'Duress PIN', and 'Secondary token 5'. Each of these fields has a corresponding 'Facility code' dropdown menu to its right. At the bottom right, there are two buttons: 'Accept' with a green checkmark icon and 'Cancel' with a red X icon.

**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.***

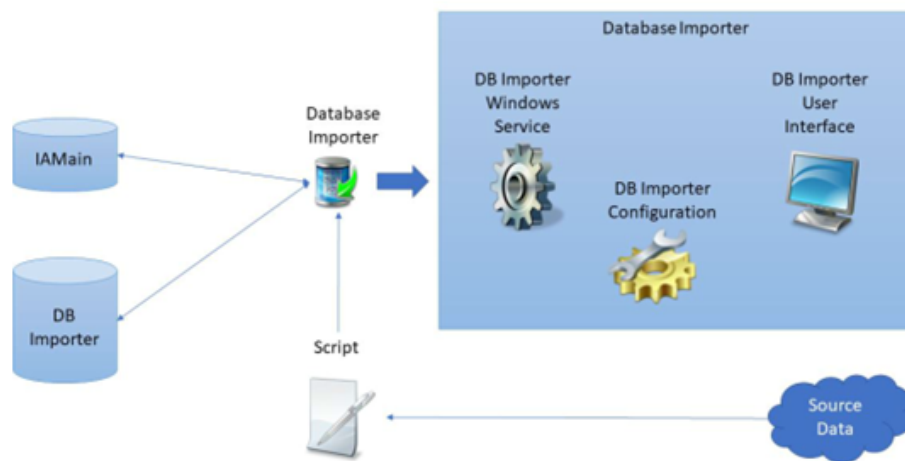
# Appendix O - Database Importer

## 36 Appendix O - 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 datasource.

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.

### Identity Access Database Importer Overview



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.

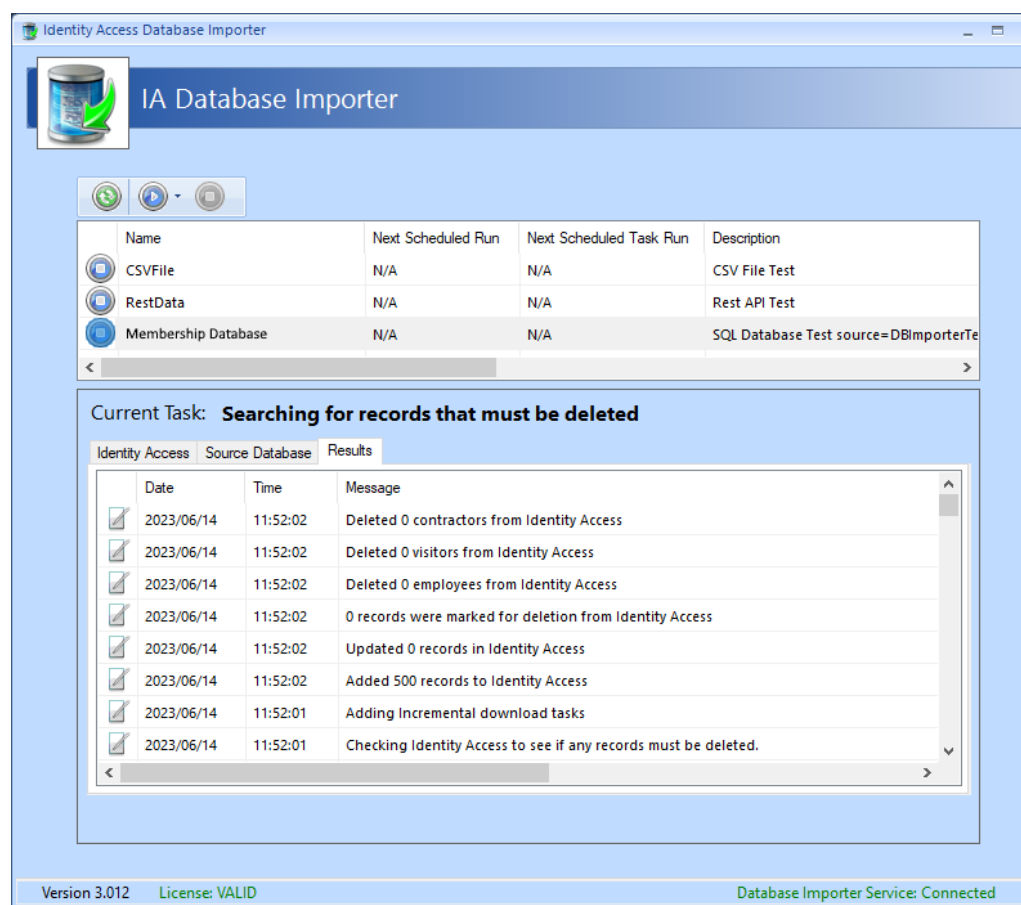
The .NET script defines which data elements are read from the source data, and the system configuration defines how frequently the data is read, which can be between 1 minute (5 minute recommended) and 24 hours. This data is then used to populate the Database Importer database, which is an intermediate database, from which data is accessed by Identity Access.

**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



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](mailto:support@controlsoft.com)



## **Appendix - Glossary**

## 37 Appendix - 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](#)<sup>[413]</sup> bus.

**IOC** - An I/O Expander Board providing 8 inputs and 8 output relays. The IOC connects to the Master iNet via the [RS485](#)<sup>[413]</sup> bus.

**Administrator** - An Operator who is authorised to use all functions within the Identity Access software.

**Contractor** - A temporary User with a [token](#)<sup>[413]</sup> 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](#)<sup>[413]</sup>.

**Download Service** - Software which manages the communications between the Identity Access software and the controllers.

**Employee** - A User with a [token](#)<sup>[413]</sup> 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** - 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 Plus** - 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.

**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**

**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](#)<sup>[412]</sup> 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](#)<sup>[413]</sup> via an [RS485](#)<sup>[413]</sup> connection ([AC-3151](#)<sup>[412]</sup> or [IOC](#)<sup>[412]</sup>).

**Downstream iNet** - An [iNet](#)<sup>[413]</sup> controller connected to a [Master iNet](#)<sup>[413]</sup> via an [RS485](#)<sup>[413]</sup> 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.

# 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](mailto:sales@controlsoft.com)

### **Technical:**

Tel: +44 (0)1451 844896

Email: [support@controlsoft.com](mailto: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](mailto:zasales@controlsoft.com)

### **Technical:**

Tel: +27 (0)10 595 1266

Email: [support@controlsoft.com](mailto: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](mailto:namsales@controlsoft.com)

### **Technical:**

Tel: +1-800-340-1407

Email: [support@controlsoft.com](mailto:support@controlsoft.com)