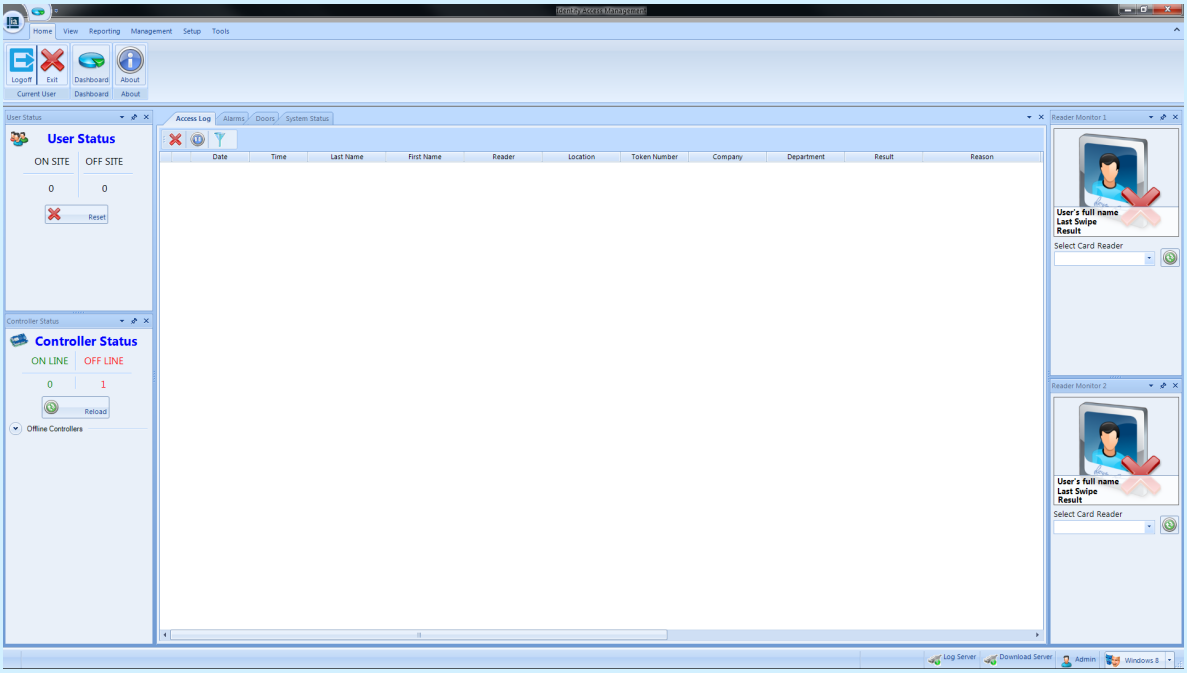
Controlsoft Identity Access Management Software



INSTALLATION & USER MANUAL

Version 2016.4 © 2017 Controlsoft Ltd

Document No: 9010-0053 Issue 6

Introduction

1 Introduction

The Identity Access (IA) Management Software v2016.2 from Controlsoft© is a PC-based Access Control Management system. The Identity Access software manages the access control database, which is downloaded to one or more Master i-Net® Controllers. The Master i-Net controls access through the doors, either directly or via expanders. The i-Net controller(s) make the decisions as to whether access is granted or denied. These are a number of ways to expand the number of doors on the system (see Expanding Systems with i-Net Controllers 12)

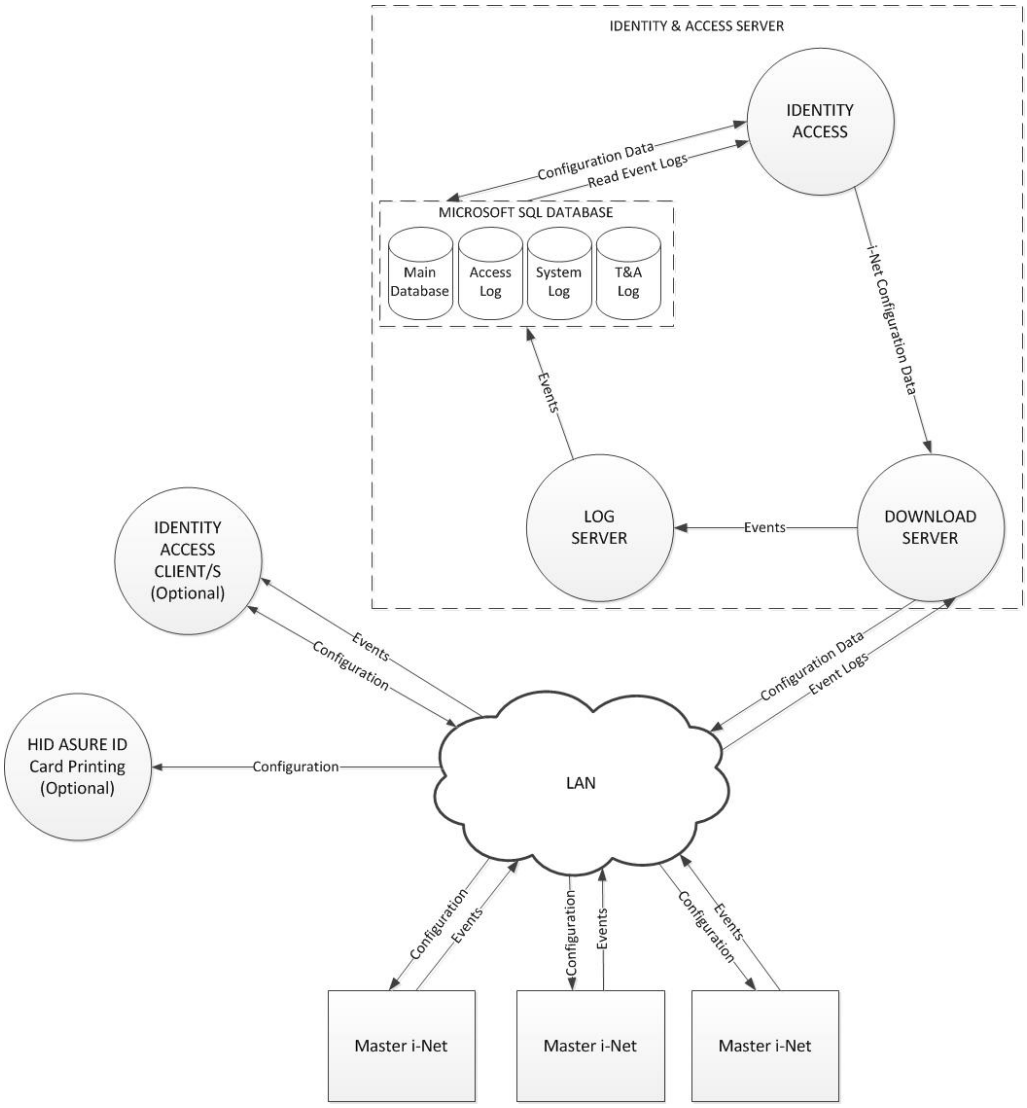
The Identity Access software is available on a flash drive by ordering part number IA-STD, or can be downloaded from our website www.controlsoft.com 8.

A license is required, part number IA-PRO, to enable the following enhanced features:

- Airlocks
- AntiPassBack
- Fingerprint Enrolment (a Morpho VERIF license will be required on the enrolment reader)
- Fire Alarm Rollcall report
- More than 24 doors
- Time Sheet Reports
- Turnstiles

Also, please note that to use Asure ID for card printing, an HID Asure ID license will also be required (Part Number IA-AID).

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



Identity Access is the main software module which handles all the user interface, from commissioning the system and saving it to the 'Main' database, to viewing events and generating reports from the 'Access', 'System' and 'T&A' logs.

Download Server communicates with the i-Nets over an IP network, sending configuration data to the controllers and receiving event logs from them.

The **Log Server** accepts events from the Download Server and saves them in the relevant SQL database.

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

- The MAIN database stores the configuration data and the user database
- The Access Log database stores all access events (i.e. who went where and when)

- The System Log database stores system events (i.e. who logged into the software and what changes were made)
- The T&A Log database stores Time & Attendance information (i.e. who clocked in or out and when)

Two further software packages are provided to configure the Server and the Client (set the database address etc). Once configured, these programs will not be required for day to day use.

Server Setup is only used to configure the Server.

Client Setup is only used to configure the Client.

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 system 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 'Main' 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

FOR IDENTITY ACCESS SERVER SOFTWARE:

Recommended PC Specification

- Intel i5 processor @ 3GHZ
- 8GB RAM
- 100GB Free Disk Space
- 10/100 Network Card
- USB Port

Performance PC Specification (more than 10,000 users)

- Intel i7 processor @ 3GHZ
- 16GB RAM
- 250GB Free Disk Space
- 10/100 Network Card
- USB Port

Operating Systems:

- Windows 7 (x64).
- Windows 8.1 (x64).
- Windows 10 (x64).
- Windows Server 2008 R2 Standard
- Windows Server 2012 R2.

If using Windows 8, please upgrade to 8.1 or Windows 10 before installing Controlsoft Identity Access

FOR IDENTITY ACCESS CLIENT SOFTWARE:

Recommended PC Specification

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

Operating Systems:

- Windows 7 (x64).
- Windows 8.1 (x64).
- Windows 10 (x64).

If using Windows 8, please upgrade to 8.1 or Windows 10 before installing Controlsoft Identity Access

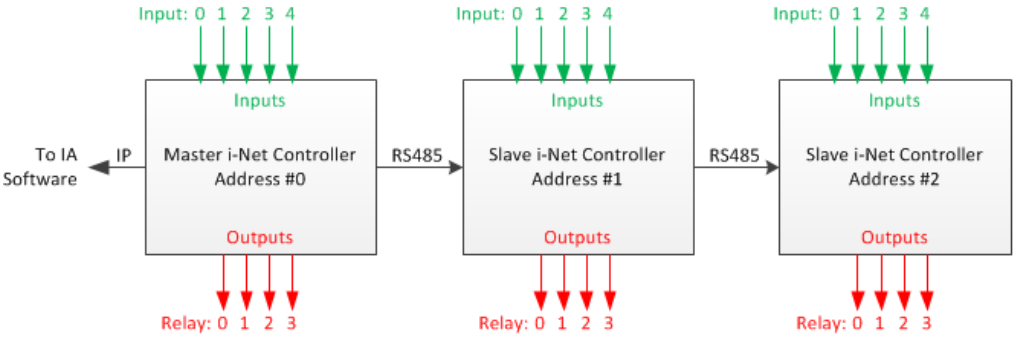
1.2 Expanding Systems

Before we start to do anything with the software, we will review how the hardware is configured and how this relates to the programming. For further information on the hardware, please refer to the installation manual for the CS-IDC-100 controllers.

Option 1 – Master i-Nets:

A channel comprises of an i-Net controller connected to the Identity Access software via IP. This is called the Master i-Net. The system can be expanded simply by adding further Master i-Nets connected to the software via an IP Connection.

Option 2 – Master and Slave i-Nets:

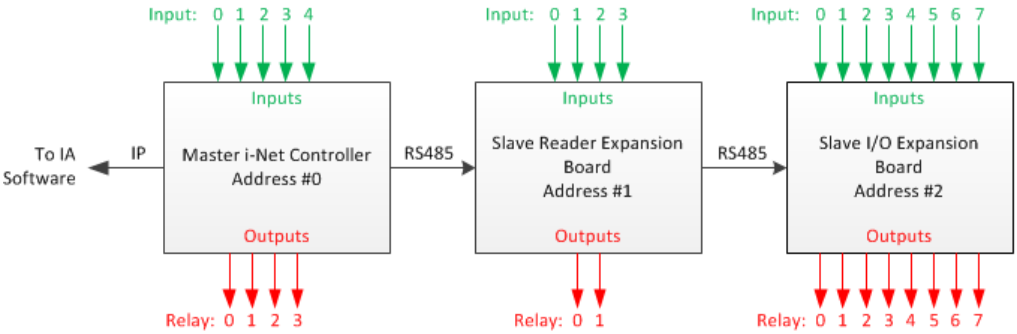


The channel comprises of an i-Net controller connected to the Identity Access software via IP. This is called the Master i-Net.

The other controllers are called Slave i-Nets and are connected to the Master i-Net via RS485.

The Master and all Slave i-nets each hold a copy of the access control database, so each Slave continues to control its doors if a fault occurs on the RS485 bus. This is Controlsoft's preferred method of expansion as it provides maximum resilience.

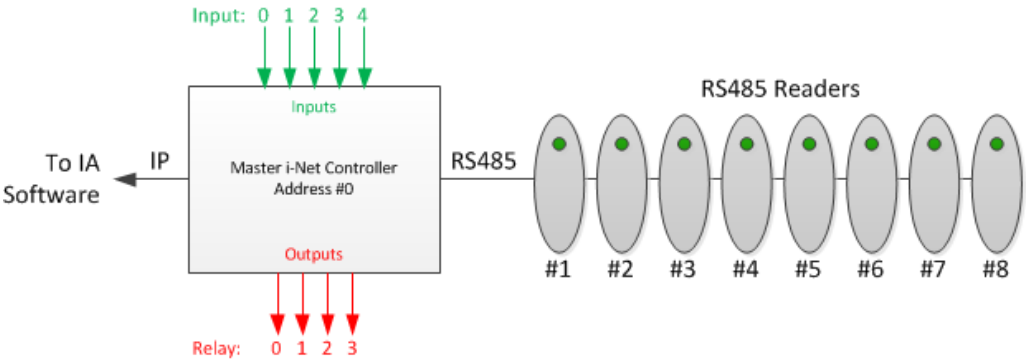
Option 3 – Master i-Net and Slave Expansion Boards



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

The other controllers are called Slave Expanders and are connected to the Master i-Net via RS485.

Option 4 – Master i-Net and RS485 Readers:



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

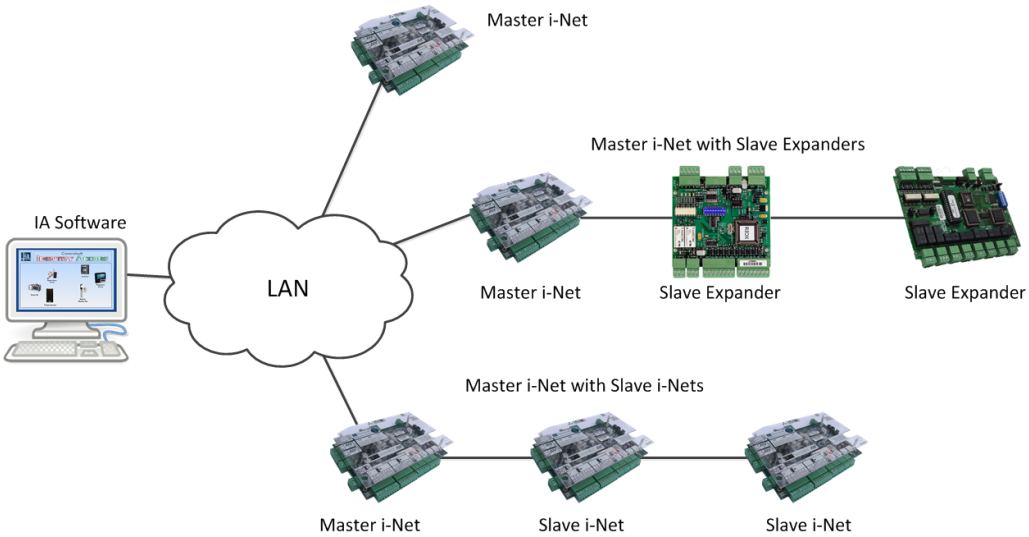
Up to 8 RS485 readers are then connected to the RS485 bus.

Outputs 0 to 3 are used for electronic locks for each of the 4 doors.

Inputs 0 to 3 are used for door contacts for each of the 4 doors.

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

NOTE: It is NOT possible to use Slave i-Nets AND Slave Expanders / Readers on the same channel, although a system can support one or more channels with Slave i-Nets and one or more channels with Slave Expanders / Readers.



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.

NOTE:

1. Nominate an input that will be used on the Master i-Net (usually Input 4).
2. The Fire Alarm panel MUST be connected to an input on each Master i-Net.
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 i-Net input.

In Identity Access, configure the input used to monitor the fire alarm panel relay (see Controller Settings) 120

Ensure that each door to be opened in the event of a fire is configured accordingly (see Door Properties General 128). Simply tick the option **Force door open if fire is detected**

Note: a Fire Input MUST be configured on each Master i-Net

Installing Identity Access Software

2 Installing Identity Access Software

Identity Access is supplied on a flash drive by ordering Part Number IA-STD, or can be downloaded from our website www.controlsoft.com. It is bundled with Microsoft SQL Server 2014 Express x64, SQL Backup Master, software for the AC-1051 & AC-1052 enrolment readers, software for the OMN-5427-CK Enrolment Reader and HID Asure ID for card printing.

A license is required, Part Number IA-PRO to enable the following Professional features:

- Airlocks
- AntiPassBack
- Fingerprint Enrolment
- Fire Alarm Rollcall Report
- More than 24 doors
- Time Sheet Reports
- Turnstiles

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

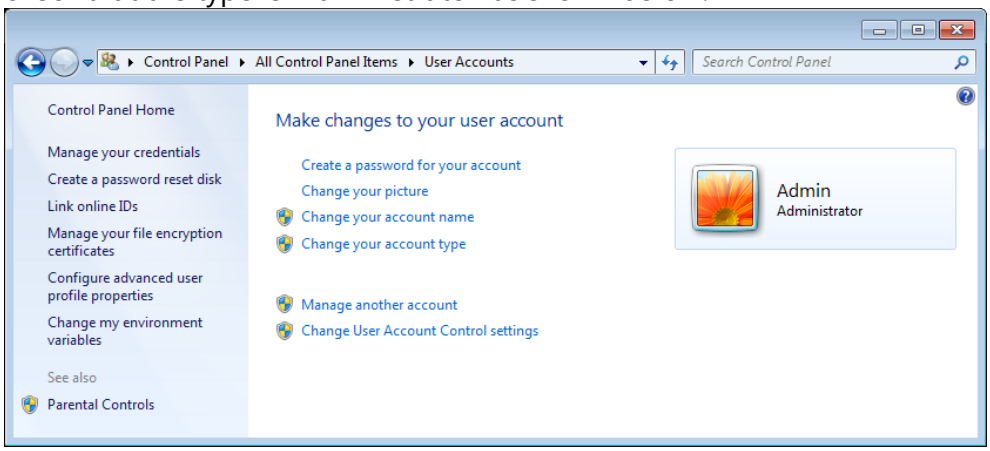
2.1 Pre-install Checks

Before installing your software, 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 222 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.

NOTE: If you have downloaded the software from the Controlsoft website DO NOT extract the files from the Downloads folder of your PC as this can cause problems with the subsequent installation. Always save the downloaded file on the root of the hard drive (C:\ ) and extract the files to the root of the hard drive (C:\ ).

2.2 Installing IA Server

To install Identity Access, follow the instructions below:

NOTE: This whole process takes roughly 15 minutes

If you have downloaded Identity Access from the Controlsoft website www.controlsoft.com, please refer to Appendix H - Downloading Software 241 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 **Install_IdentityAccess.exe**.

A launcher will appear as shown below:

Installation Type

Basic

As shown above. This installs the IA Server version which includes SQL Express 2014.

Advanced

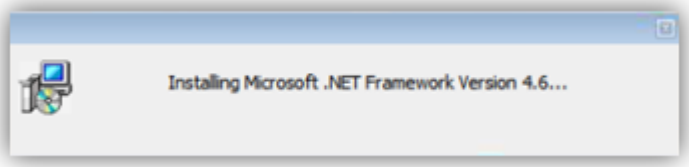
As shown below. This is for advanced users i.e. if you already have SQL Express 2014 installed or you wish to use SQL Express on another machine. The Client Only installer is also available from Advanced.

Select **View Documentation** to look through the various manuals supplied.

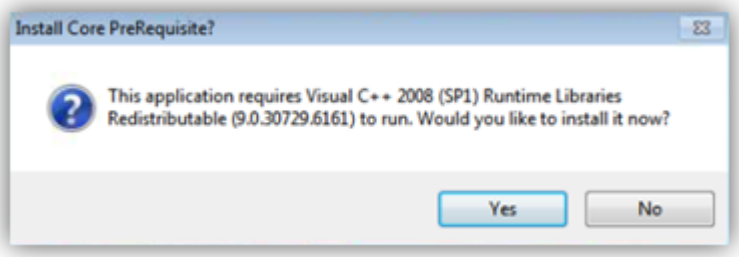
Click **Install Identity Access** and the launcher will begin by first installing Microsoft SQL Express 2014

Note: Do not close any of the windows during this process or the install will fail

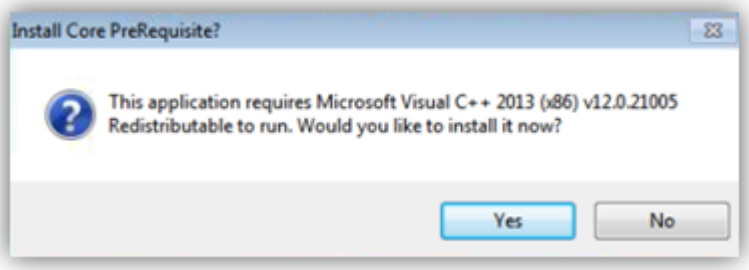
First, Dot Net 4.6 will install, please wait until this finishes.



If Prompted click **[Yes]** to install Visual C++ 2008

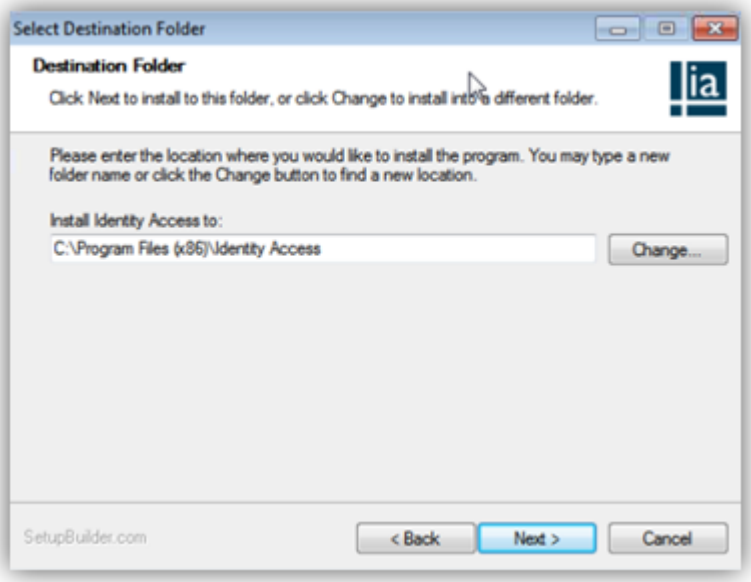


If Prompted click **[Yes]** to install Visual C++ 2013

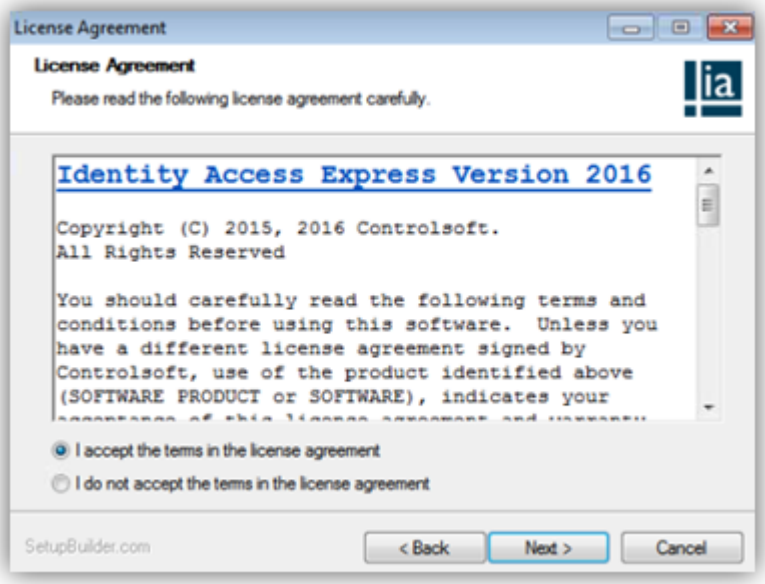


Following this, an install screen will then appear as shown below:

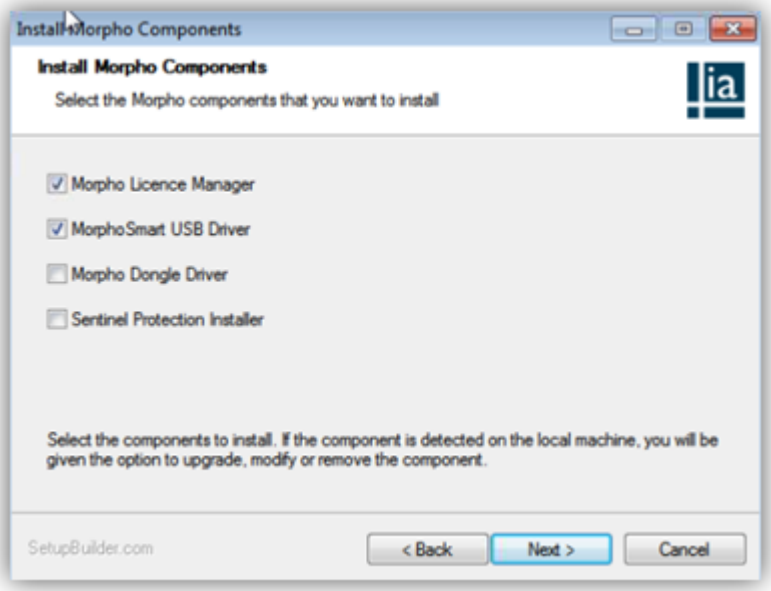
Click **[Next]**



Ensure this location is where you want to install it and then click **[Next]**

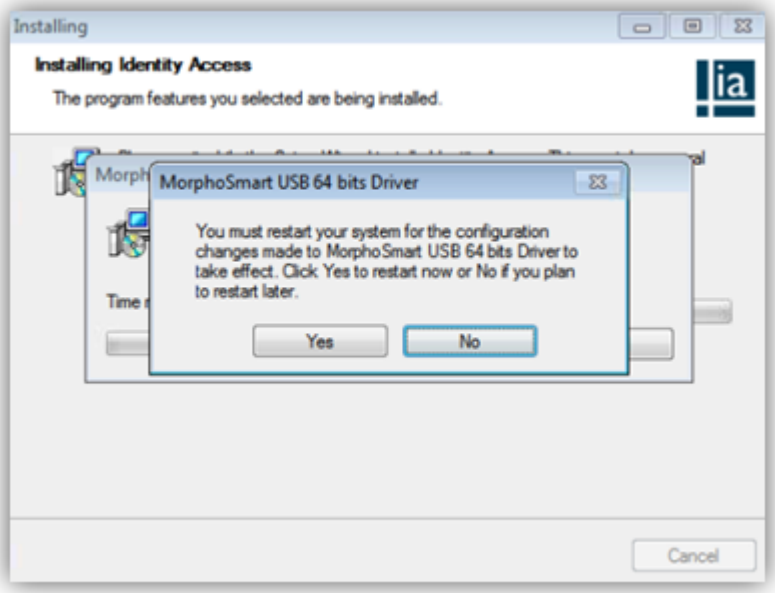


Read and accept the license agreement and press **[Next]** and then **[Next]** again



If you intend using the IA Server as a biometric enrolment station, leave Morpho License Manager and MorphoSmart USB Driver ticked.

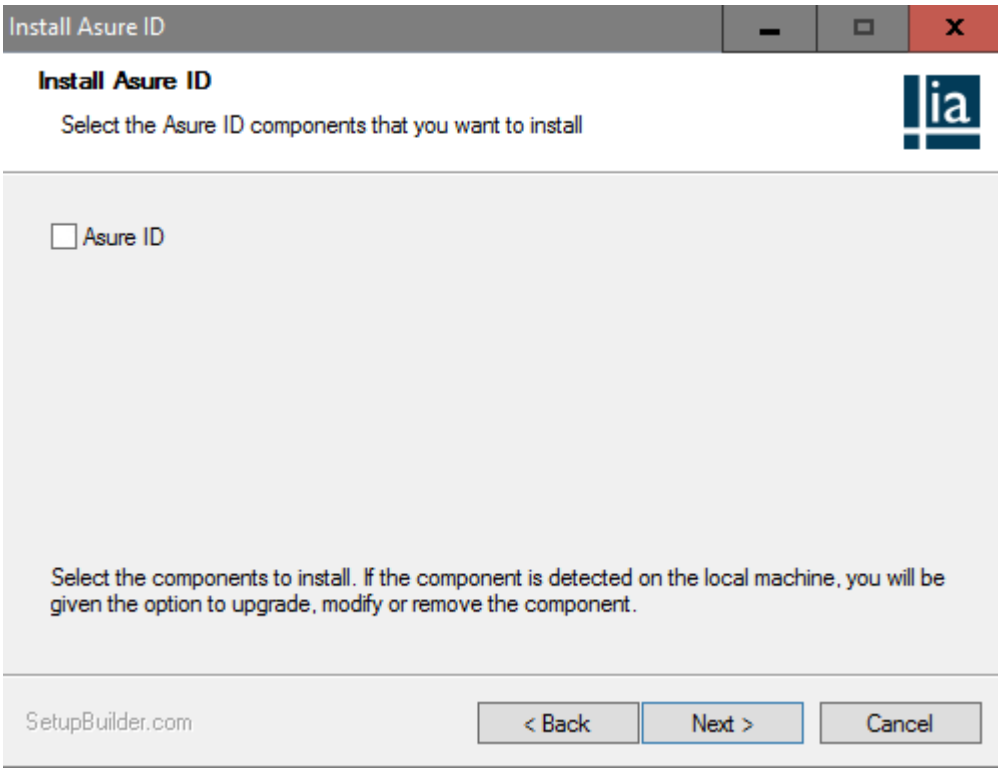
When using Morpho devices you will need a VERIF license on the Identity Access Server or Client. This comes in the form of an MSO enrolment reader.



Please select **[No]** to postpone the restart for now.

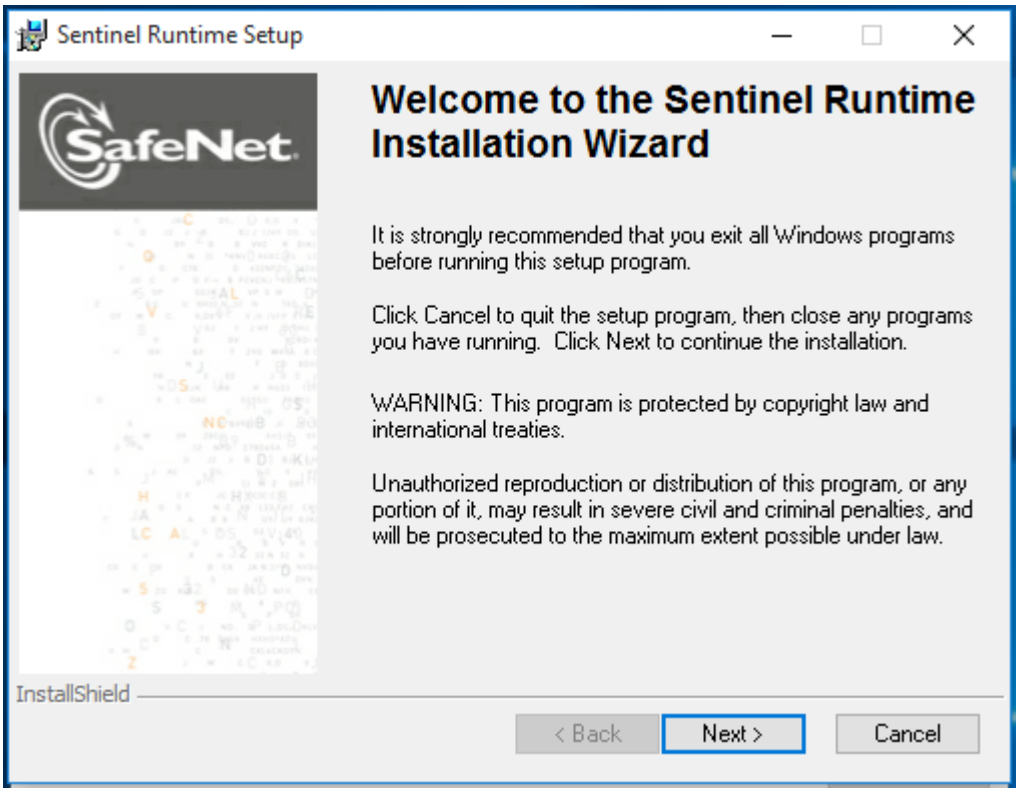
Next, decide whether IA is to be used in conjunction with HID Asure ID for card printing ***NOTE: You must have a valid HID Asure ID license***

(Part Number: IA-AID) to use this feature beyond the 30 day trial period.

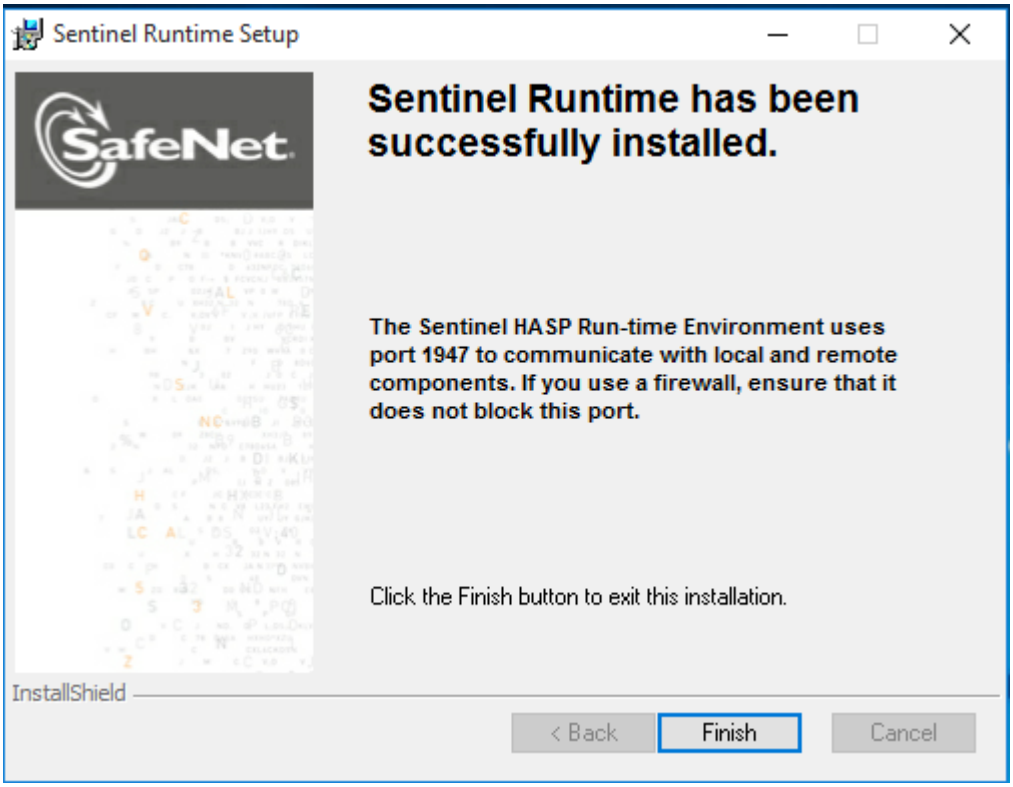


For further information on installing HID Asure ID, please refer to Appendix B - HID Asure ID Software 215

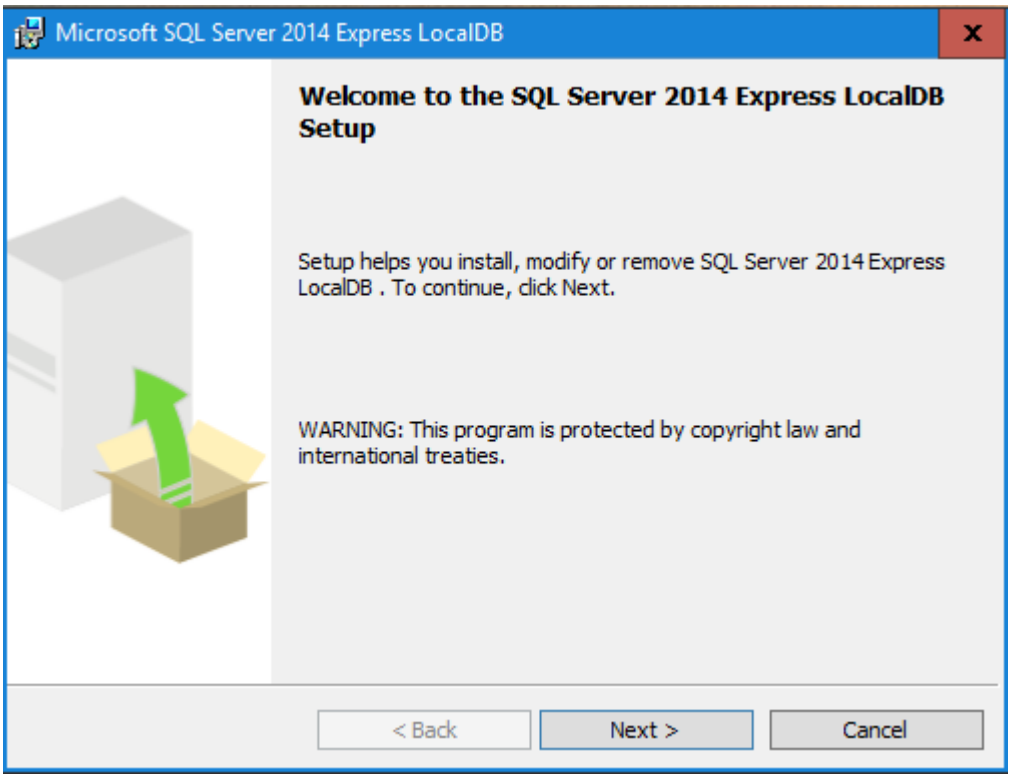
The License drivers will be installed next:



Click **[Next]**, read and accept the license agreement, then click **[Next]** and **[Next]**

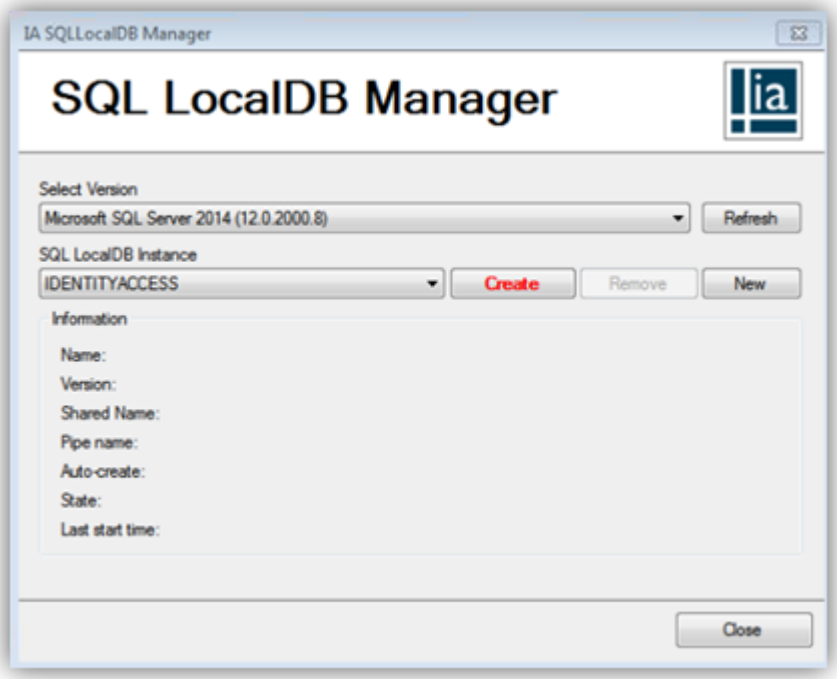


Finally, click **[Finish]** to continue the installation of the IA software

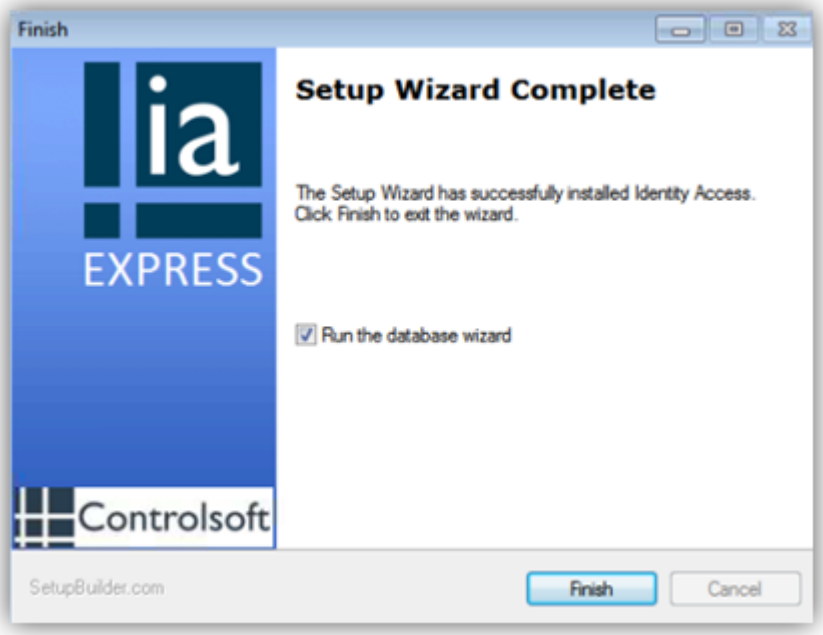


Click **[Cancel]** and then click **[Yes]**

Now click **[Finish]**



When the SQL LocalDB Manager is displayed, Click **[Close]**



Next click **[Finish]**

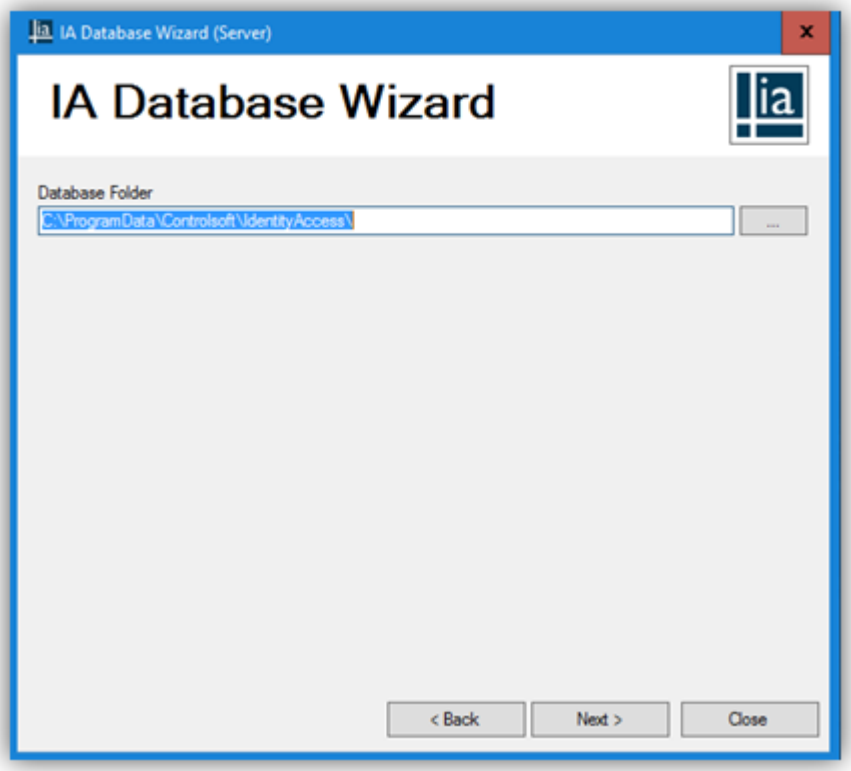
When presented with the IA Database Wizard, select the appropriate SQL Server from the drop down list or type in the PC/IP Address followed by the SQL Server Instance Name (as default the instance name is IdentityAccess) i.e.

"PC\IdentityAccess).

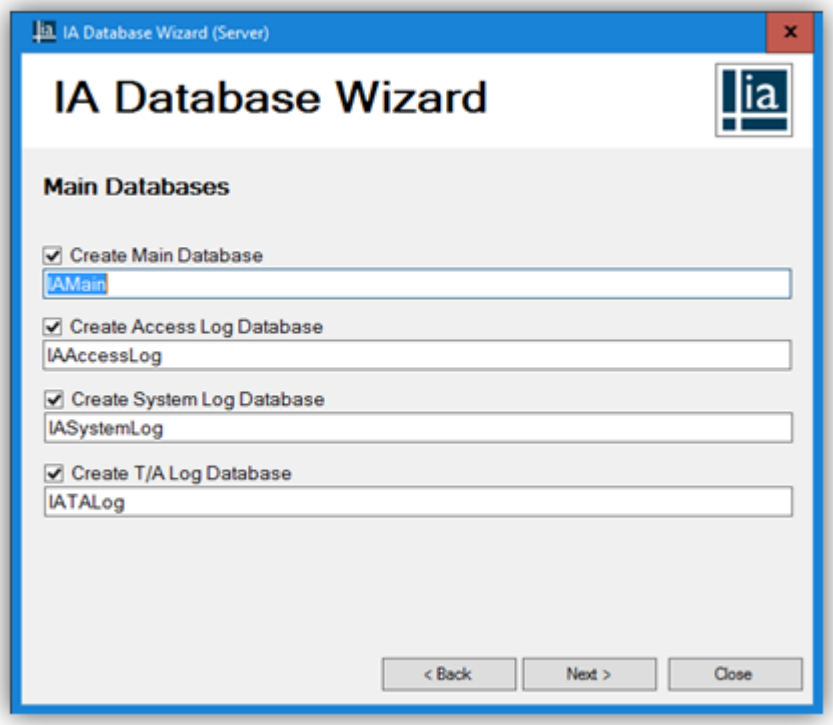
For Authentication type select **SQL Authentication** from the drop down and click **[Next]**

The next step will configure the database connection.
NOTE: Please do not close this screen while the database is being configured.

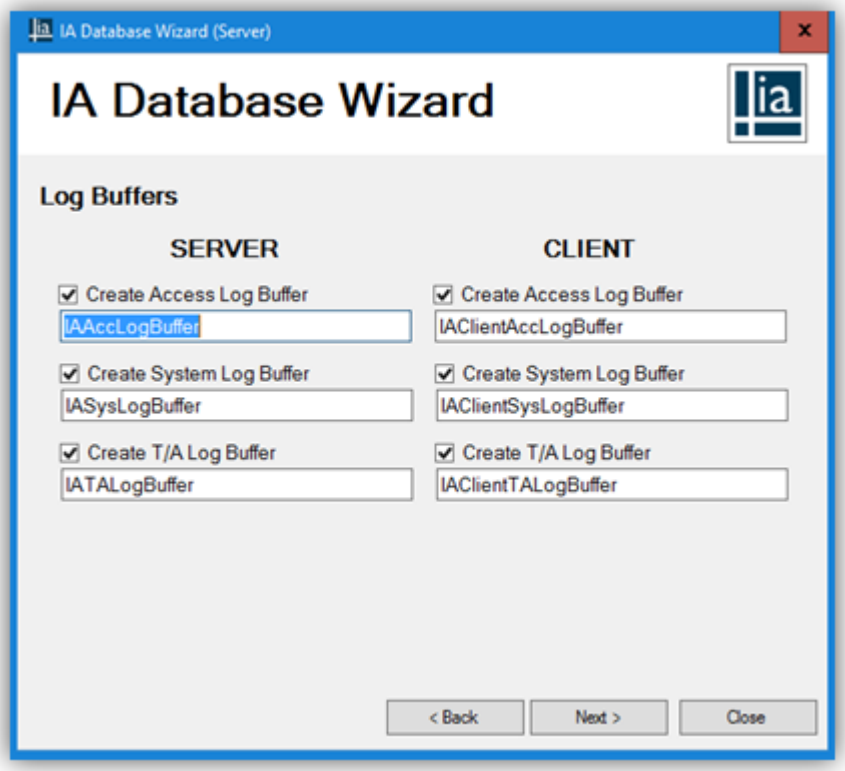
Click **[Next]**



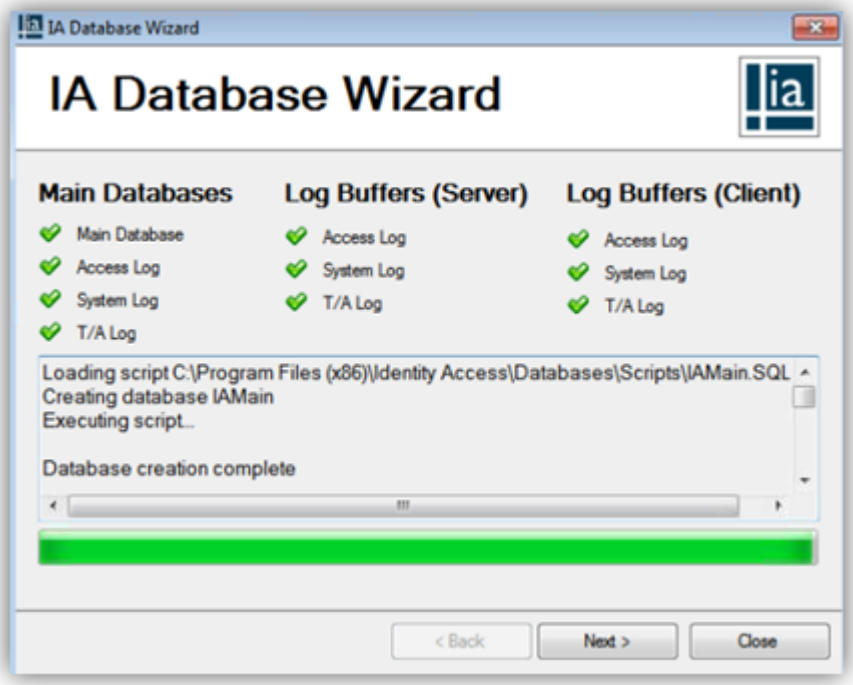
Click **[Next]** when prompted for the Database Folder



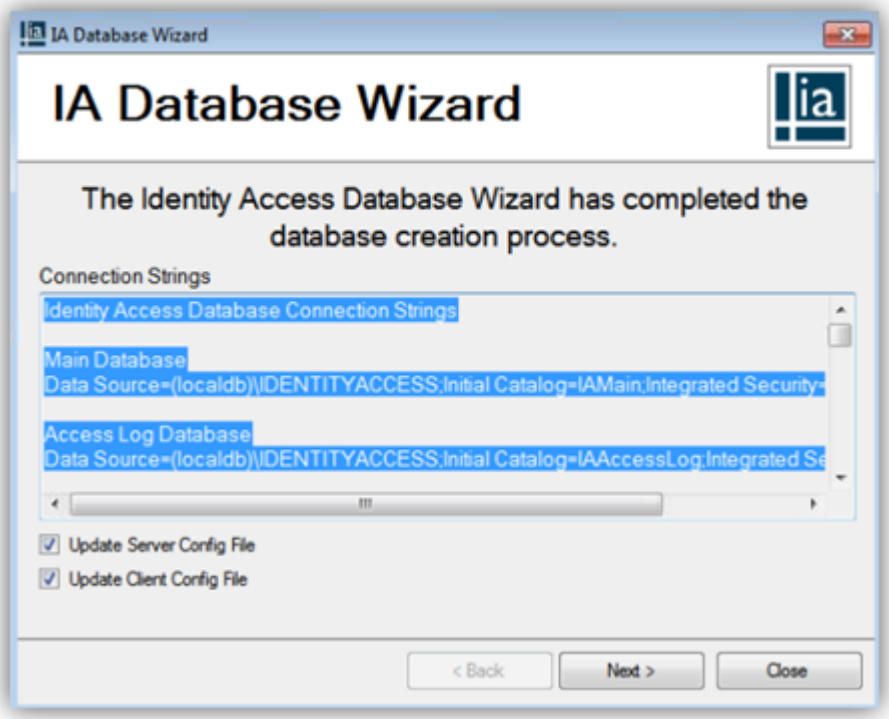
Create the Main databases by clicking **[Next]**.



Create the log buffers by clicking **[Next]** and then click **[Create]**.



The databases will now be created, click **[Next]** when complete.



Finally, click **[Next]** followed by **[Finish]**.

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

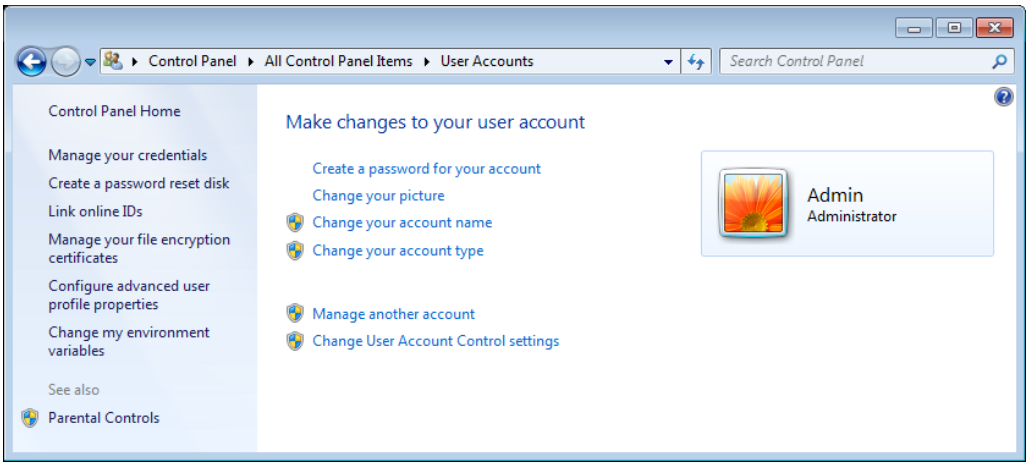
2.3 Installing IA Client

This whole process takes roughly 10 minutes.

NOTE: Before installing your software, please temporarily disable your antivirus 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 **Install_IdentityAccess.exe**.

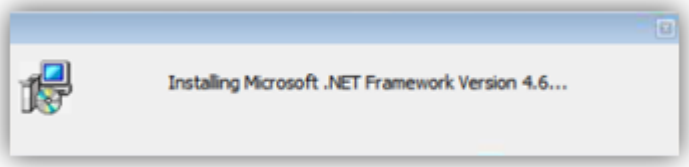
A launcher will appear as shown below:

To install a Client, first select the **Installation Type** as **Advanced**

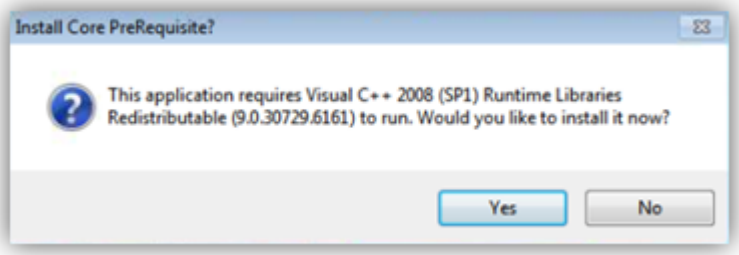
Select **View Documentation** to look through the various manuals supplied.

To start the installation, select **[Install Client Only]**.

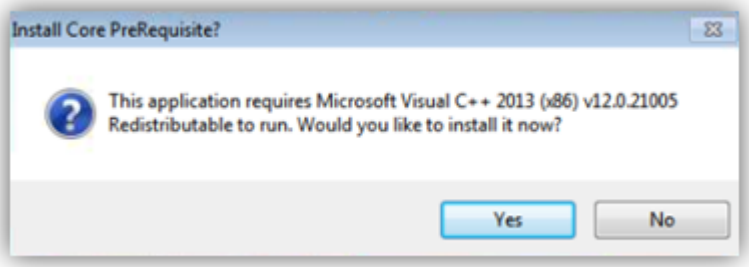
Next, Dot Net 4.6 will install, please wait until this finishes.



If prompted, Click **[Yes]** to install C++2008.

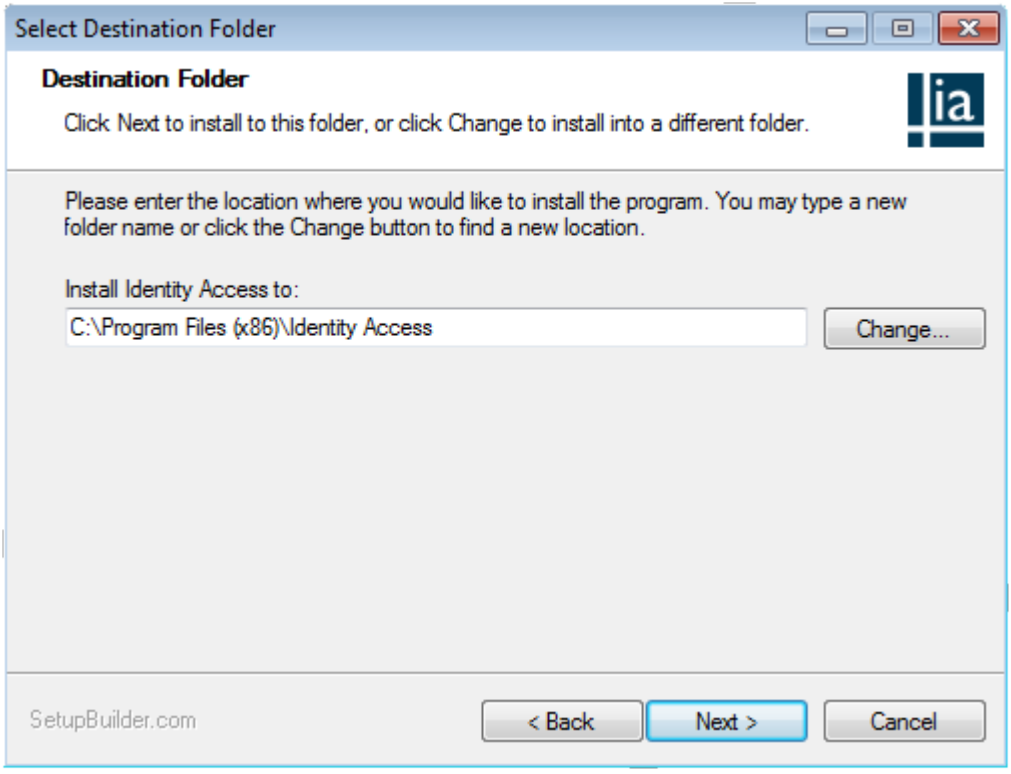


If prompted, Click **[Yes]** to install C++2013.

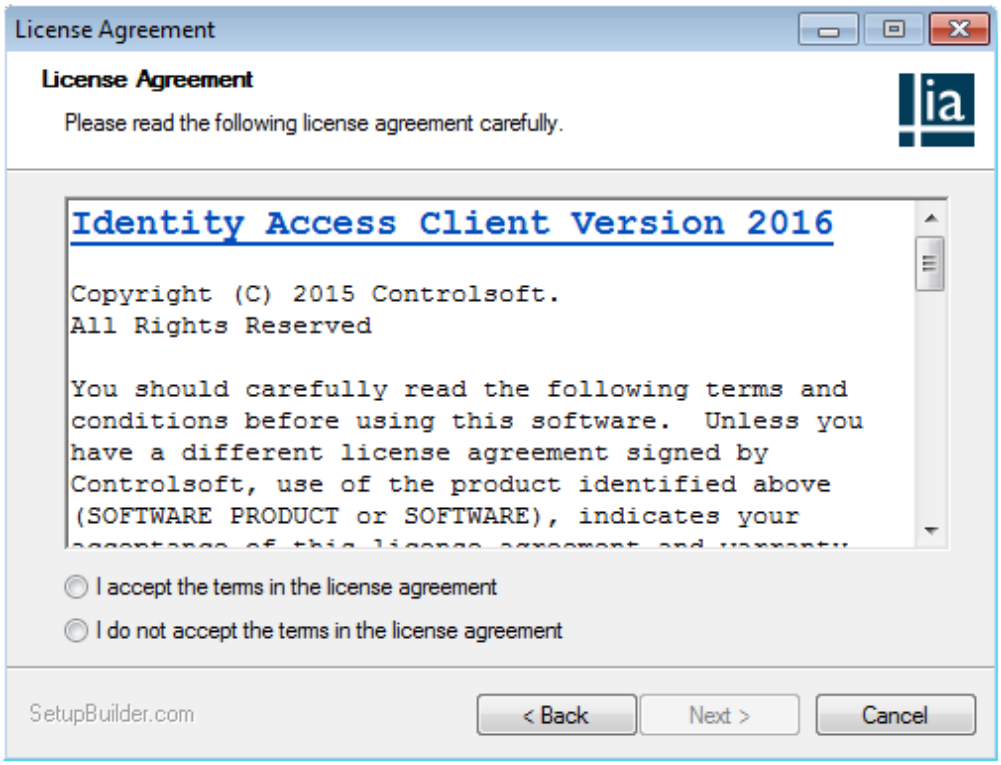


Following this an install screen will then appear as shown below:

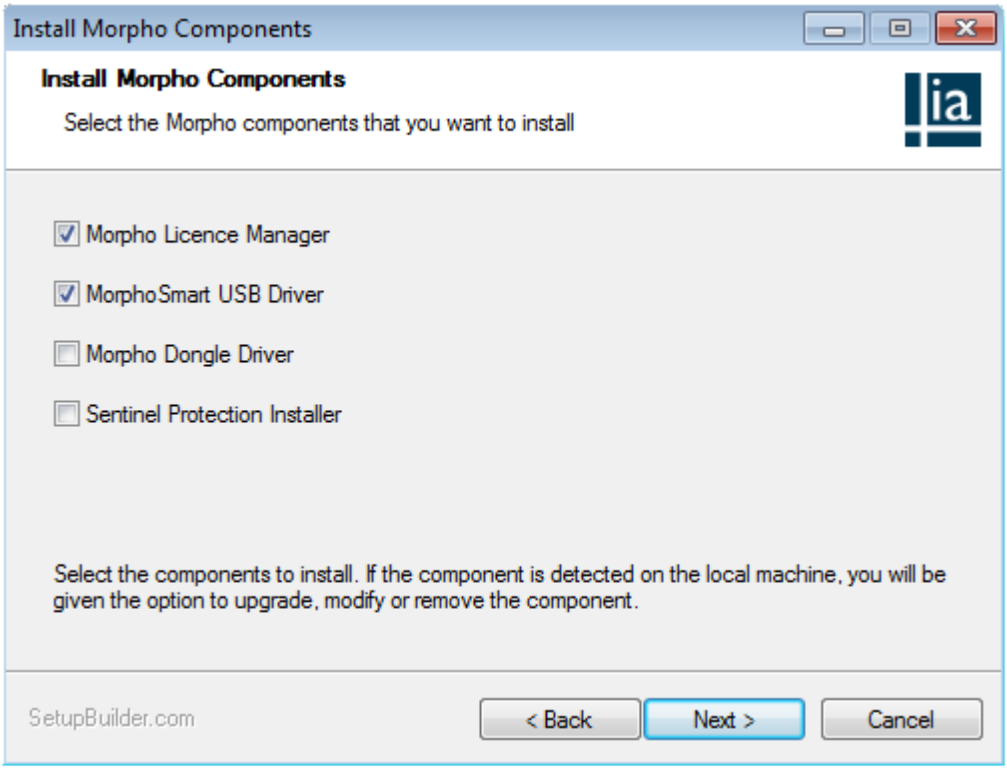
Click **[Next]**.



Ensure this location is where you want to install it and then click **[Next]**.

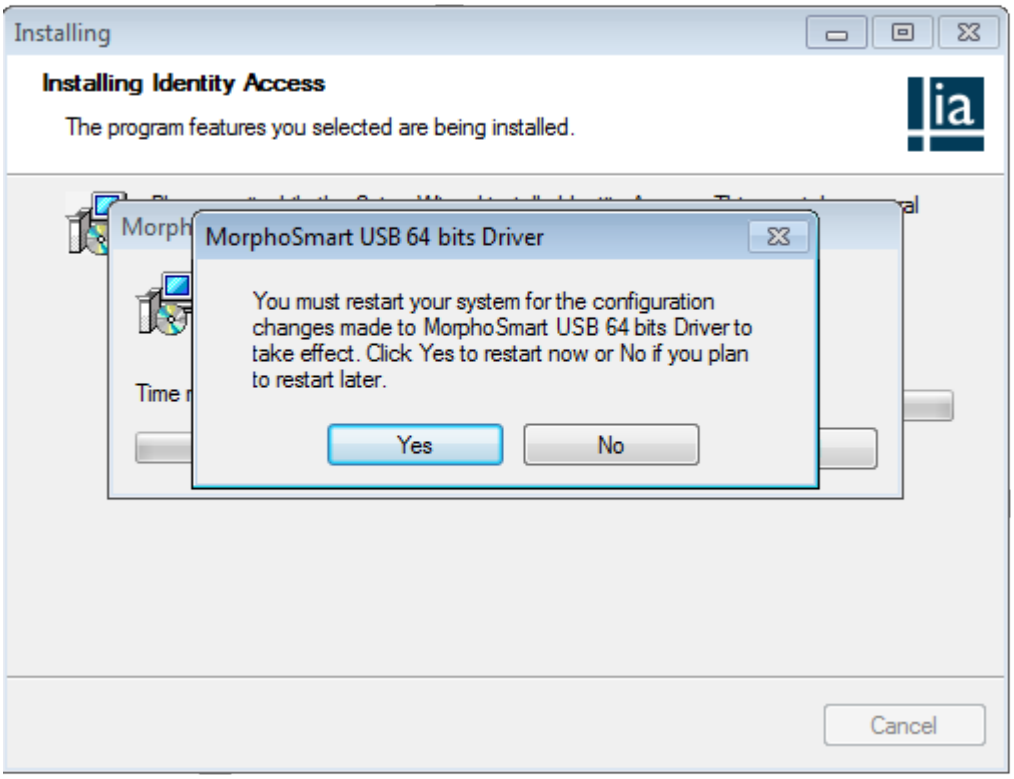


Read and accept the license agreement and press **[Next]** and then **[Next]** again.



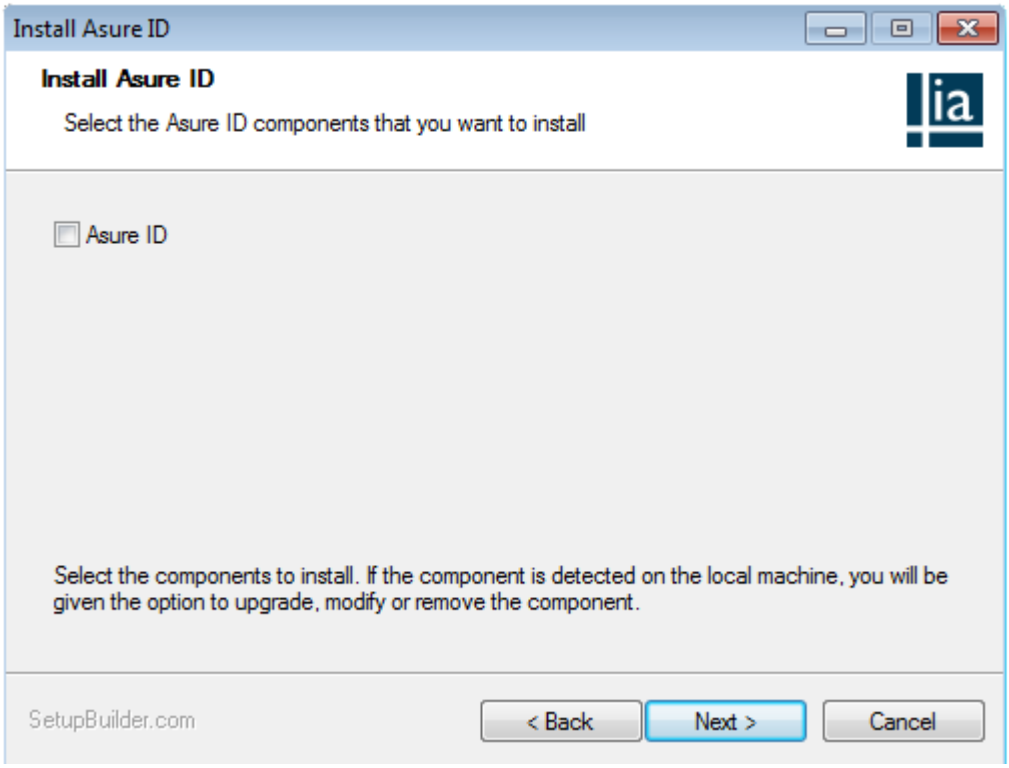
If you intend to use the IA Client as a biometrics enrolment station leave Morpho Licence Manager & Morpho Smart USB Driver ticked.

When using Morpho devices you will need a VERIF license on the Identity Access Server or Client. This comes in the form of an MSO enrolment reader.



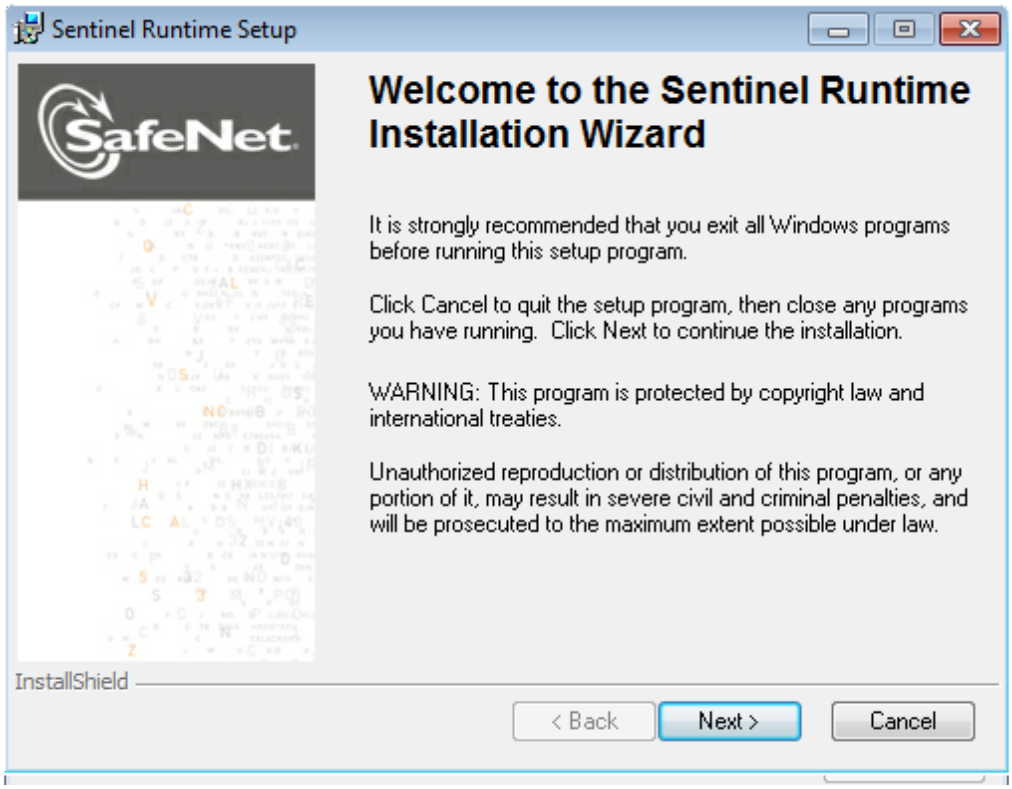
Please select **[No]** to postpone the restart for now.

Next, decide whether Asure ID is to be used in conjunction with HID Asure ID for card printing ***NOTE: You must have a valid HID Asure ID license (Part Number: IA-AID) to use this feature beyond the 30 day trial period.***

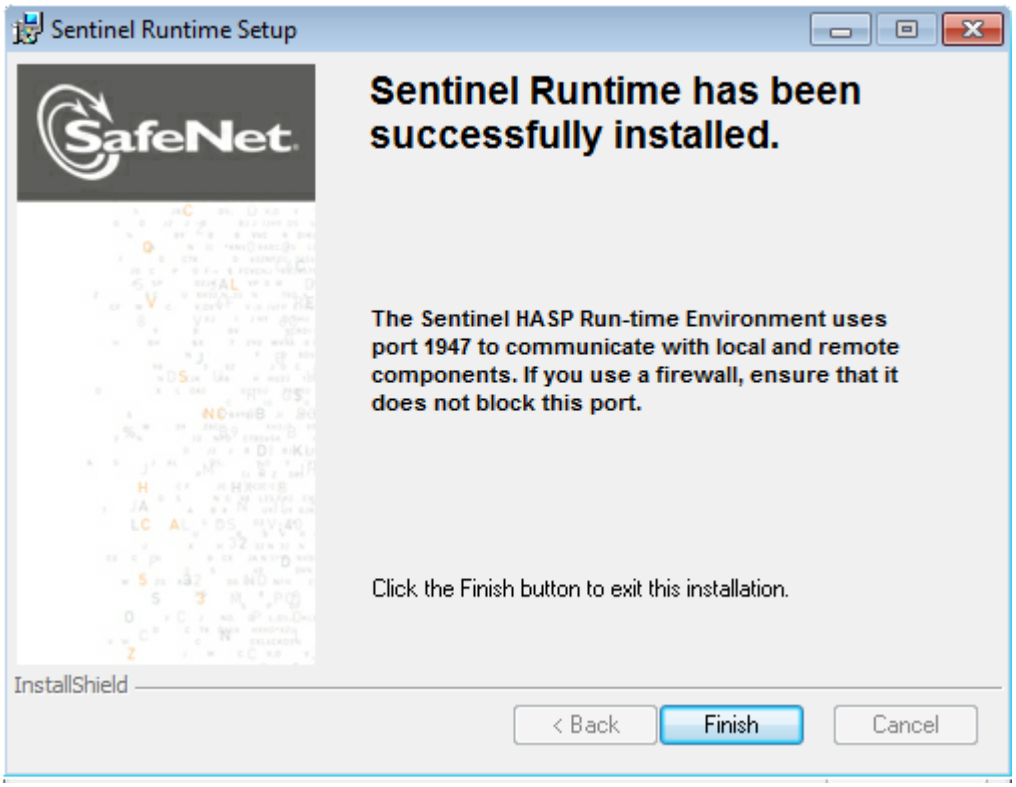


For further information on installing HID Asure ID, please refer to Appendix B - HID Asure ID Software 215.

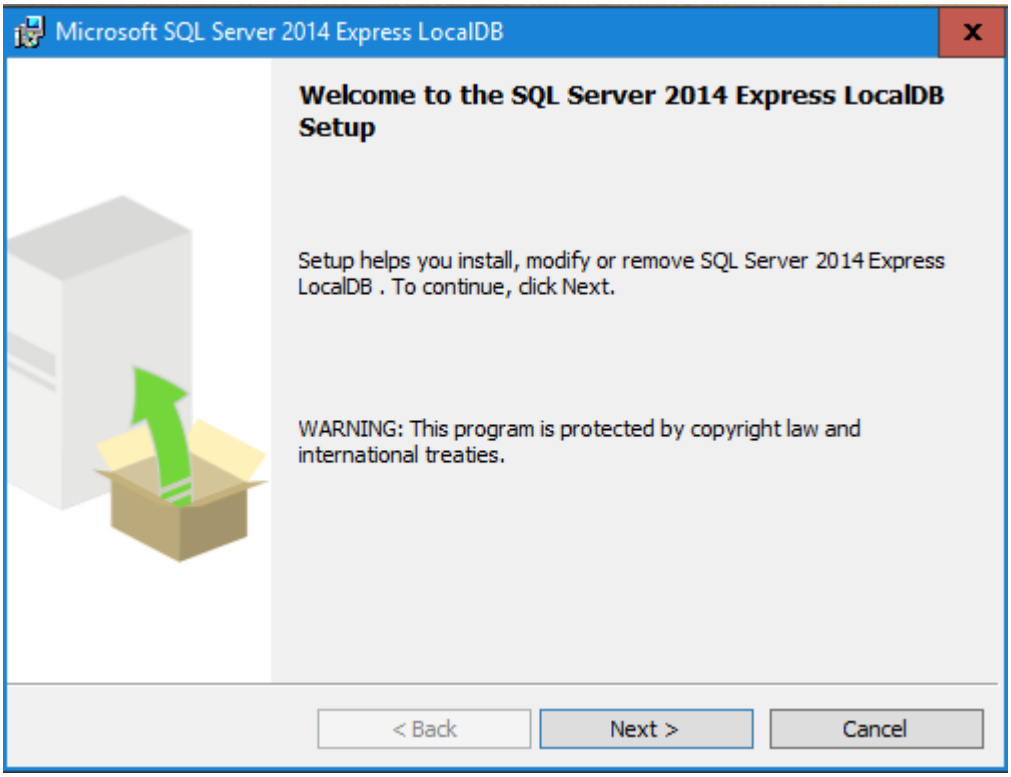
The License drivers will be installed next:



Click **[Next]**, read and accept the license agreement, then click **[Next]** and **[Next]**

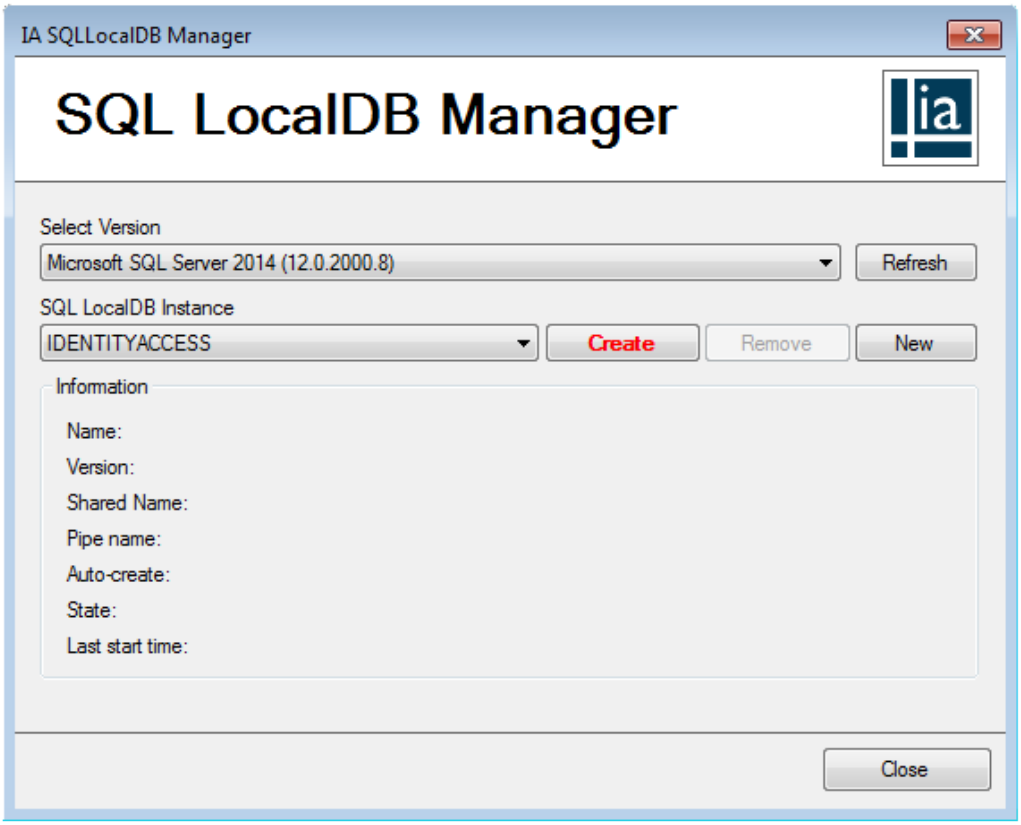


Finally, click **[Finish]** to continue the installation of the IA software



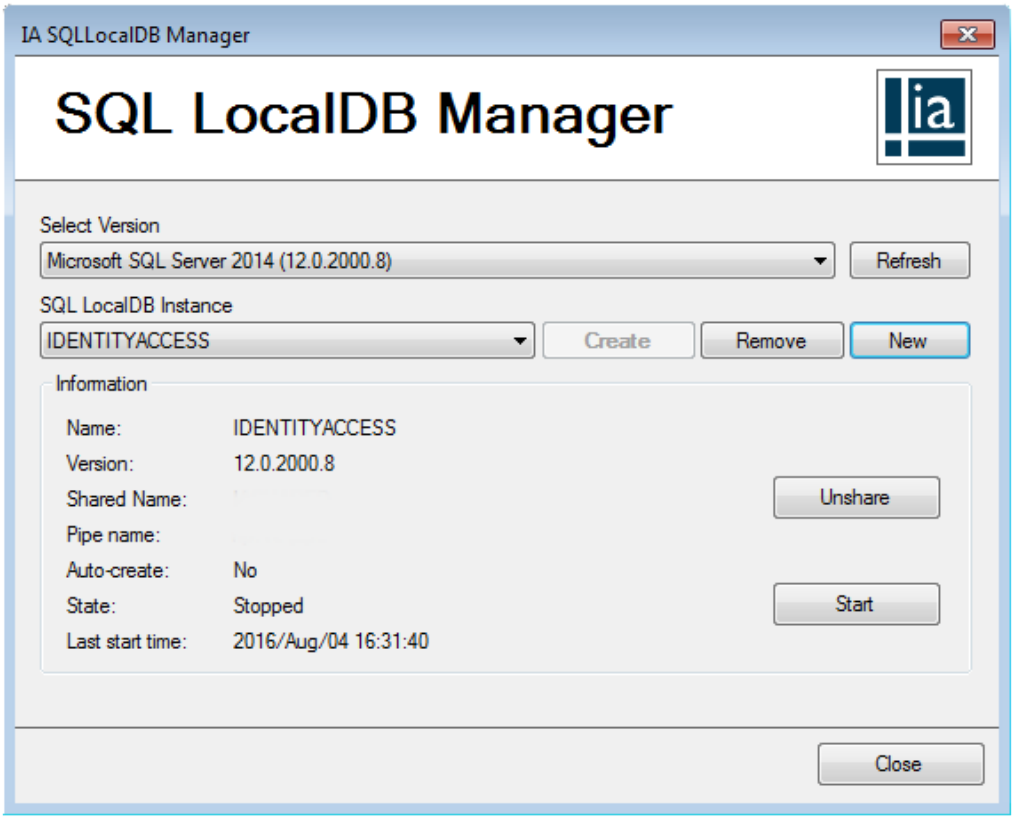
Click **[Next]**, read and accept the License Terms and then click **[Next]**.

Now click **[Install]** followed by **[Finish]**.



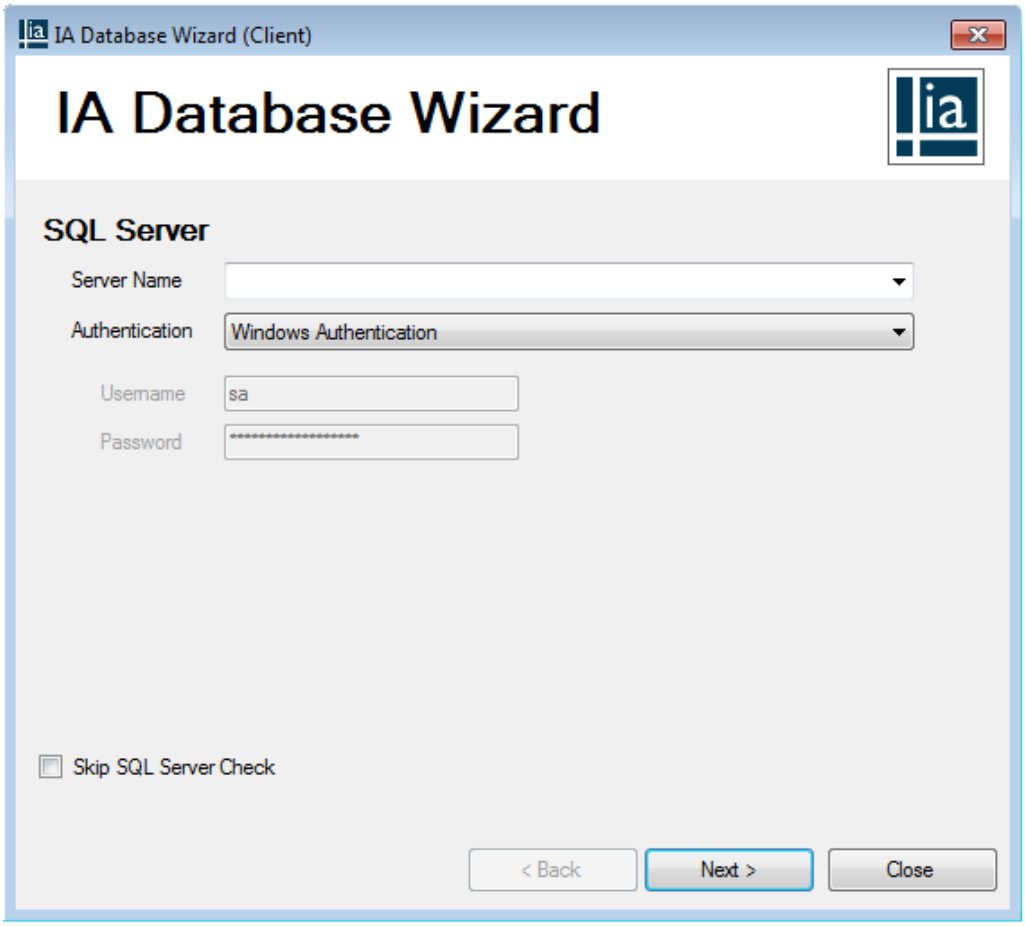
Click **[Create]** to create the LocalDB instance.

Click **[Share]** and use **IASHARED** for the name, then click **[OK]**



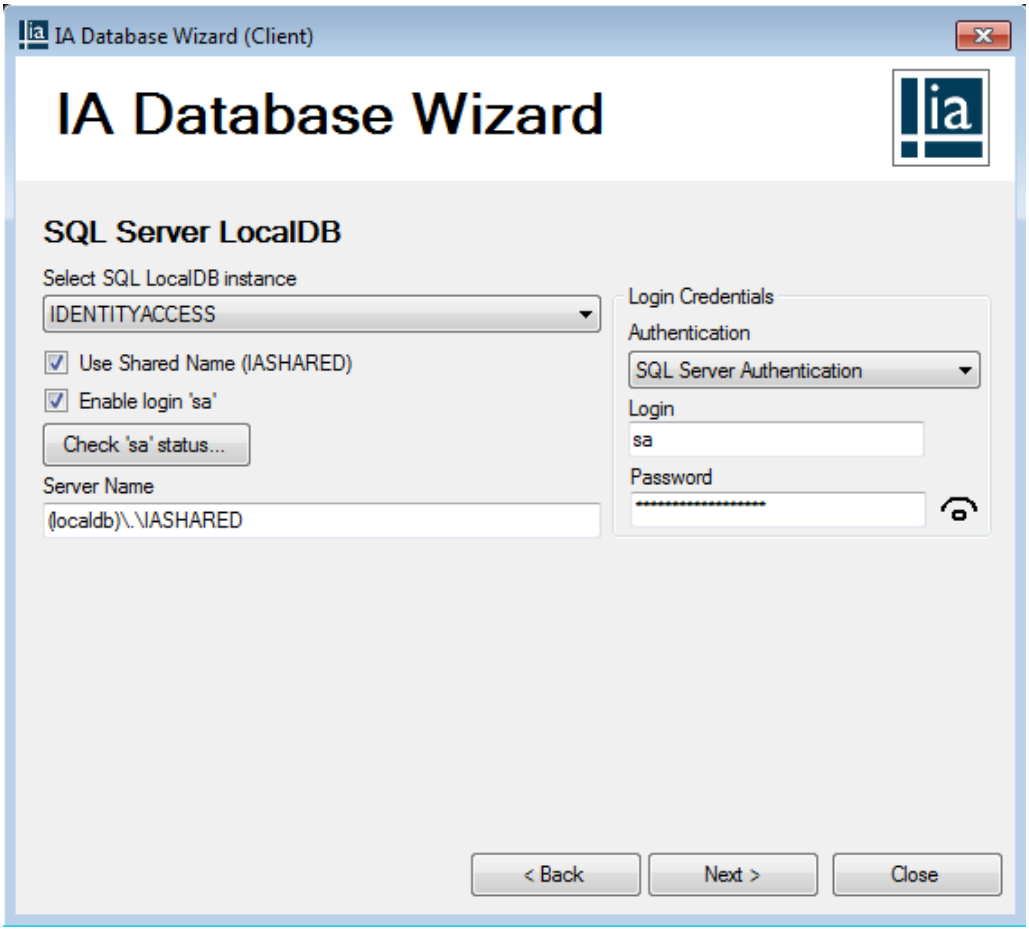
Click **[Close]**

Click **[Finish]**.



When presented with the IA Database Wizard, select the appropriate SQL Server from the drop down list or Type in the PC/IP Address followed by SQL Server Instance Name (as default the instance name is IdentityAccess) i.e. "PC\IdentityAccess)

For Authentication type select **SQL Authentication** from the drop down and click **[Next]**

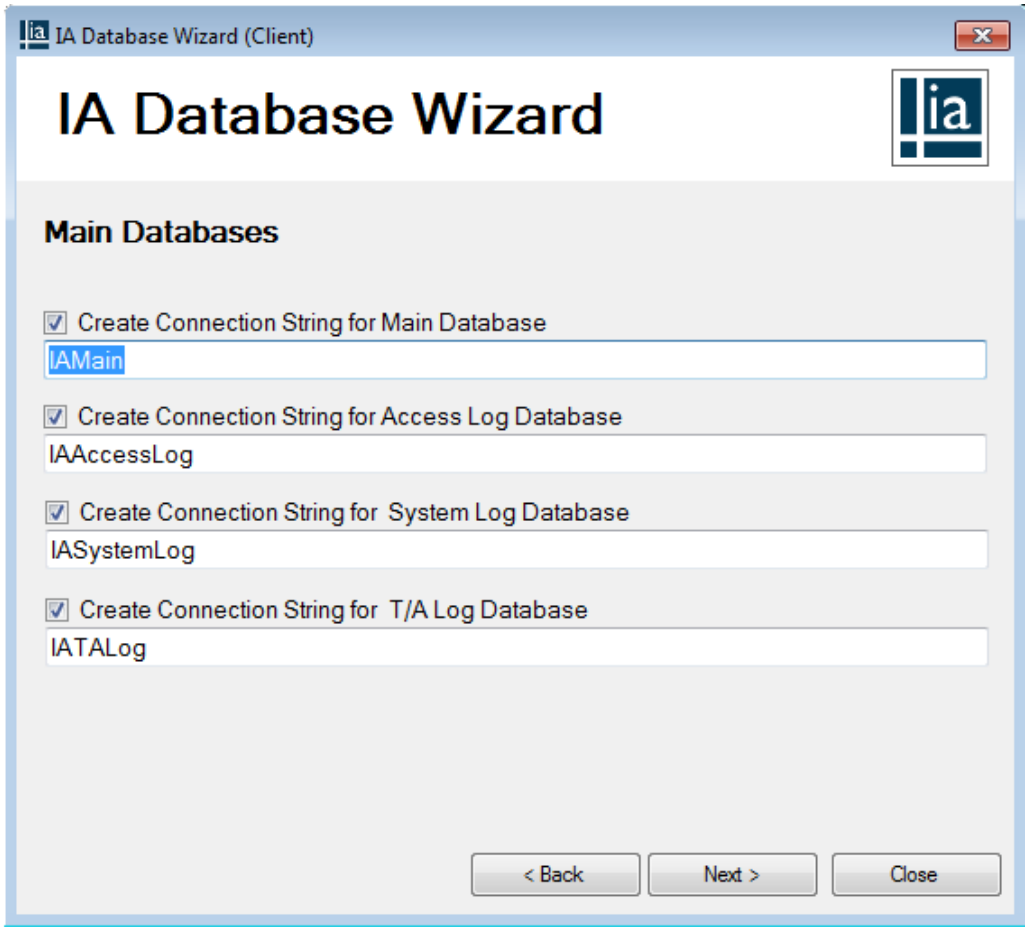


This will configure the database connection.

NOTE: Please do not close this screen while the database is being configured.

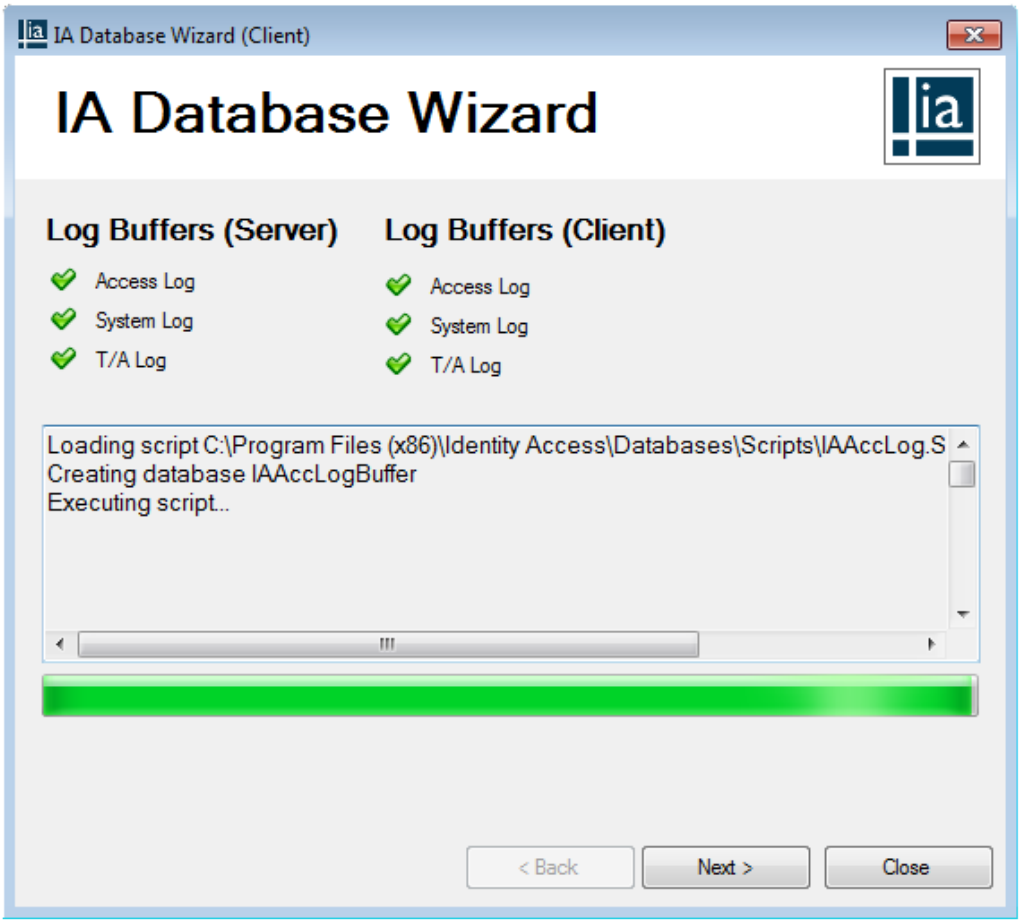
Click **[Next]**

Please click **[Next]** when prompted for the Database Folder



Create the Main databases by clicking **[Next]**.

Create the log buffers by clicking **[Next]** and then click **[Create]**.



The databases will now be created, click **[Next]** when complete.

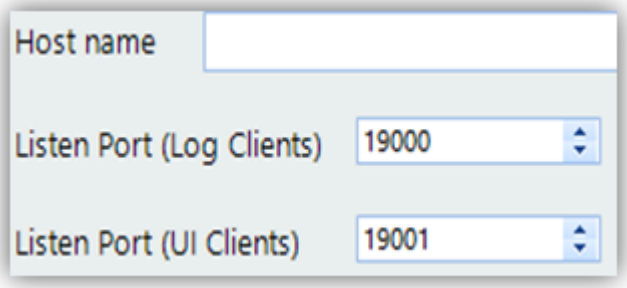
Click **[Next]** followed by **[Finish]**.

Next step is to be performed from the IA Server-

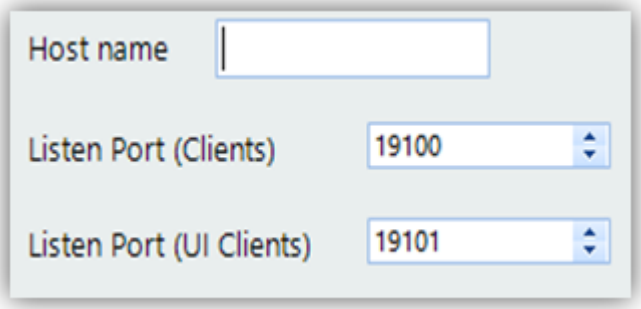
Click on the Windows Start button, **All Programs/Apps**, followed by **Controlsoft**, and open **IA Server Configuration**

Log in with Admin credentials – Default Username - **Admin** Default Password – **Password**

Select the **Log Server** menu and for the **Host name** type, change **127.0.0.1** to **the fixed IP address of the Server.**



Select the **Download Server** and for the **Host name** change **127.0.0.1** to the fixed IP address of the Server.



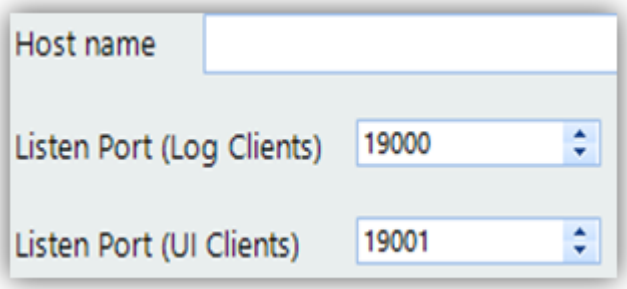
Press **[Accept]**

Now go back to the client PC and perform the following –

Click on the Windows Start button, **All Programs/Apps**, followed by **Controlsoft**, and open **IA Client Configuration**

Log in with Admin credentials – Default Username - **Admin** Default Password – **Password**

Select the **Server** menu and for the **Server name** type **the IP address of the Server**



Finally Press **Accept**

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

2.4 Licensing the Software

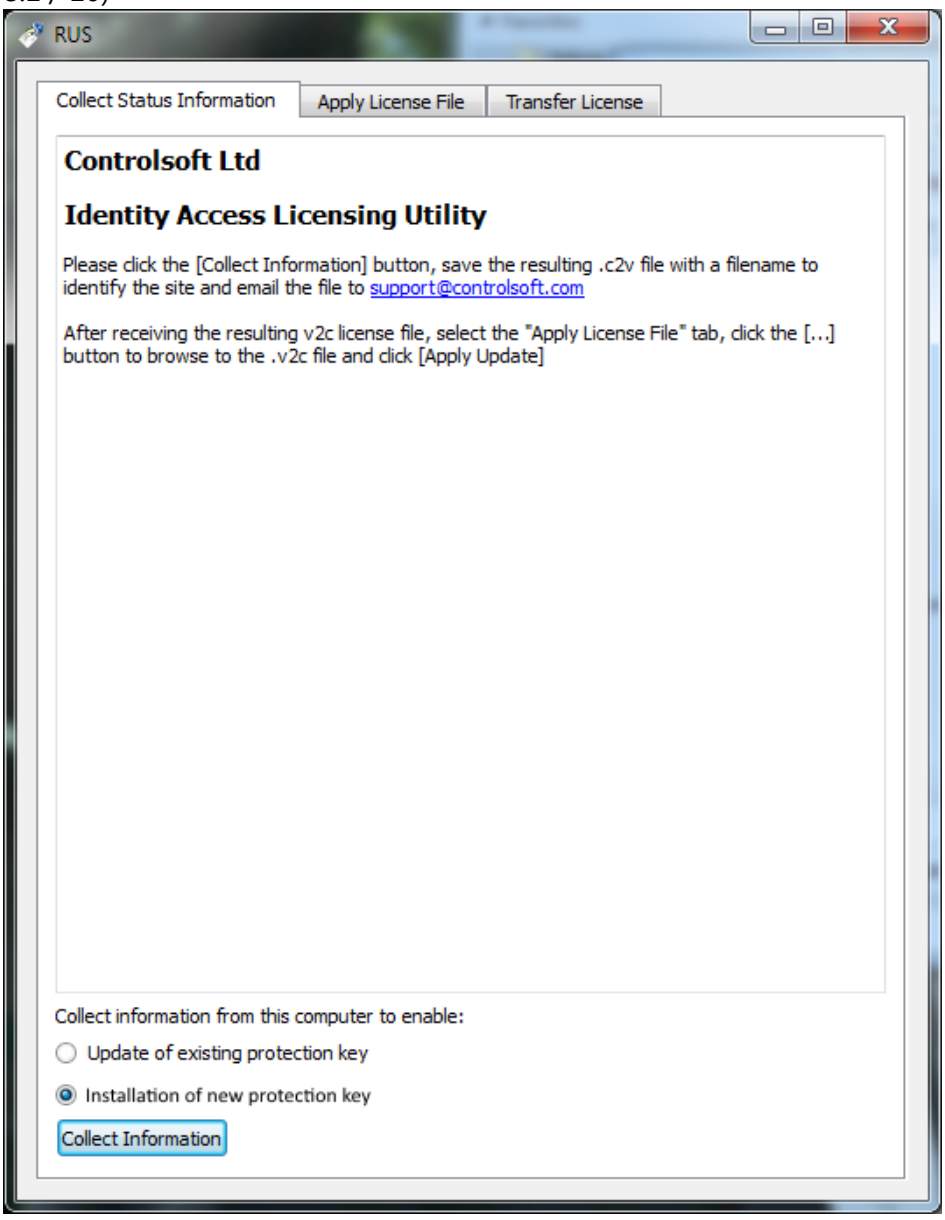
The Identity Access software does not need a license to run, unless any of the following features are to be used:

- Airlocks
- AntiPassBack
- Fingerprint Enrolment (a Morpho VERIF license will be required on the enrolment reader)
- Fire Alarm Rollcall report
- More than 24 doors
- Time Sheet Reports
- Turnstiles

Once you have purchased your license (Part Number: IA-PRO), follow the instructions below to apply it.

1. Select **Start** > **All Programs** > **Controlsoft** > **Identity Access** > **Tools** > **Licensing Utility** (for Windows 7)
   or **Start** > **All Apps** > **Controlsoft** > **Licensing Utility** (for Windows

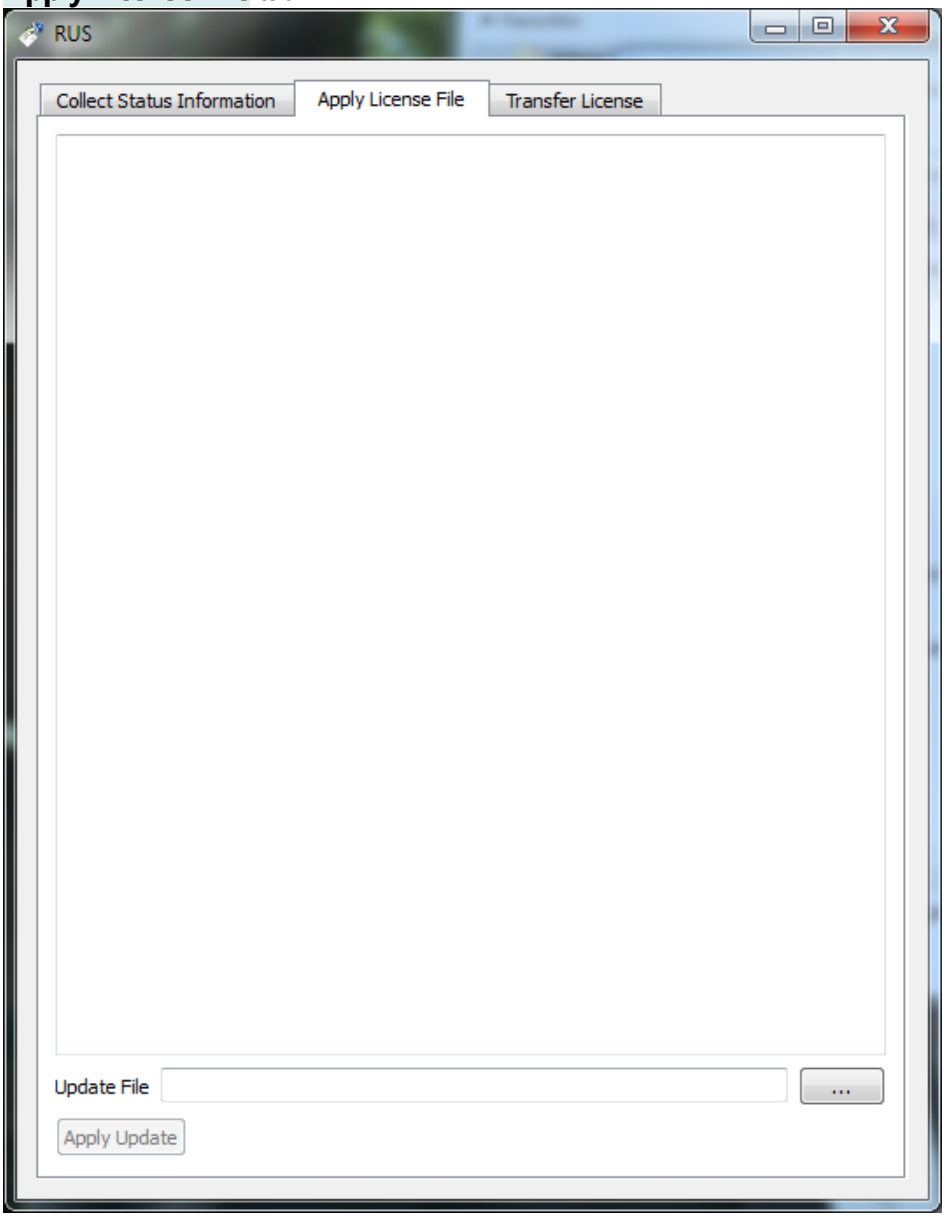
8.1 / 10)



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 Purchase Order number used to order the license to support@controlsoft.com. Controlsoft will then process the license and email a "v2c" file back to you.

4. Save the v2c file on the desktop, then run the Licensing Utility again and select the **Apply License File** tab



5. Click the **[...]** button, select the v2c file saved on the desktop then click the **[Apply License]** button and check that the license has been successfully applied.

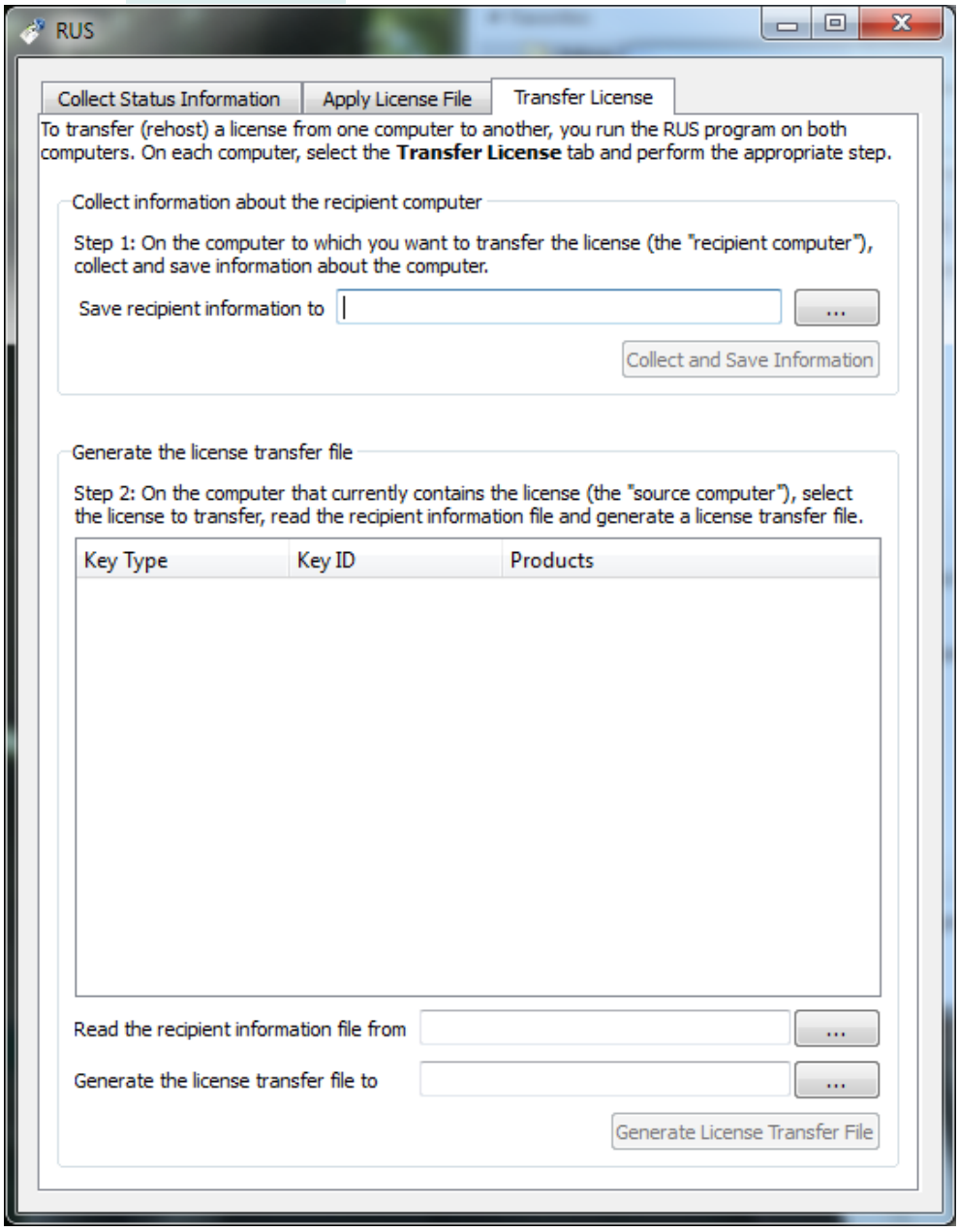
2.5 Transfering a License

If you ever need to move a licensed copy of Identity Access software to another computer, it is possible to transfer the license 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** > **All Programs** > **Controlsoft** > **Identity Access** > **Tools** > **Licensing Utility** (for Windows 7)
   or **Start** > **All Apps** > **Controlsoft** > **Licensing Utility** (for Windows 8.1 / 10)

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 license file.
7. On the new machine apply the .h2h file in the same way as applying a .v2c file as described above.

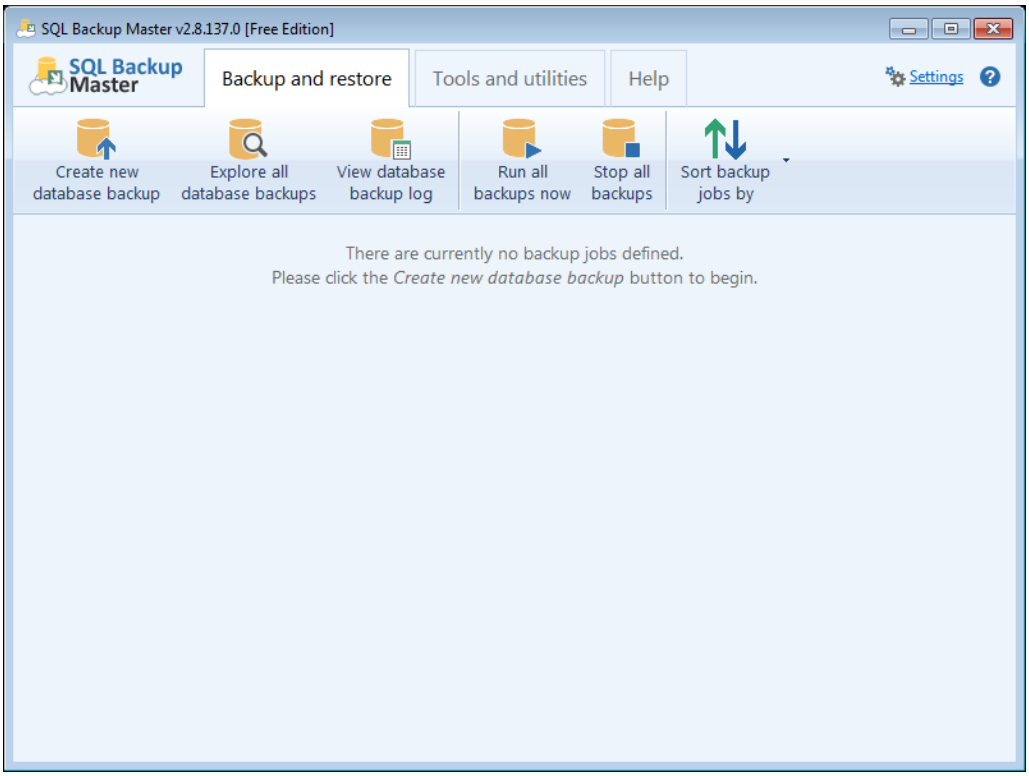
2.6 Microsoft SQL Backup

Controlsoft Identity Access Client/Server is supplied with a copy of a third party utility called **SQL Backup Master**, which is required to regularly backup the database. Installation of SQL Backup Master is simple:

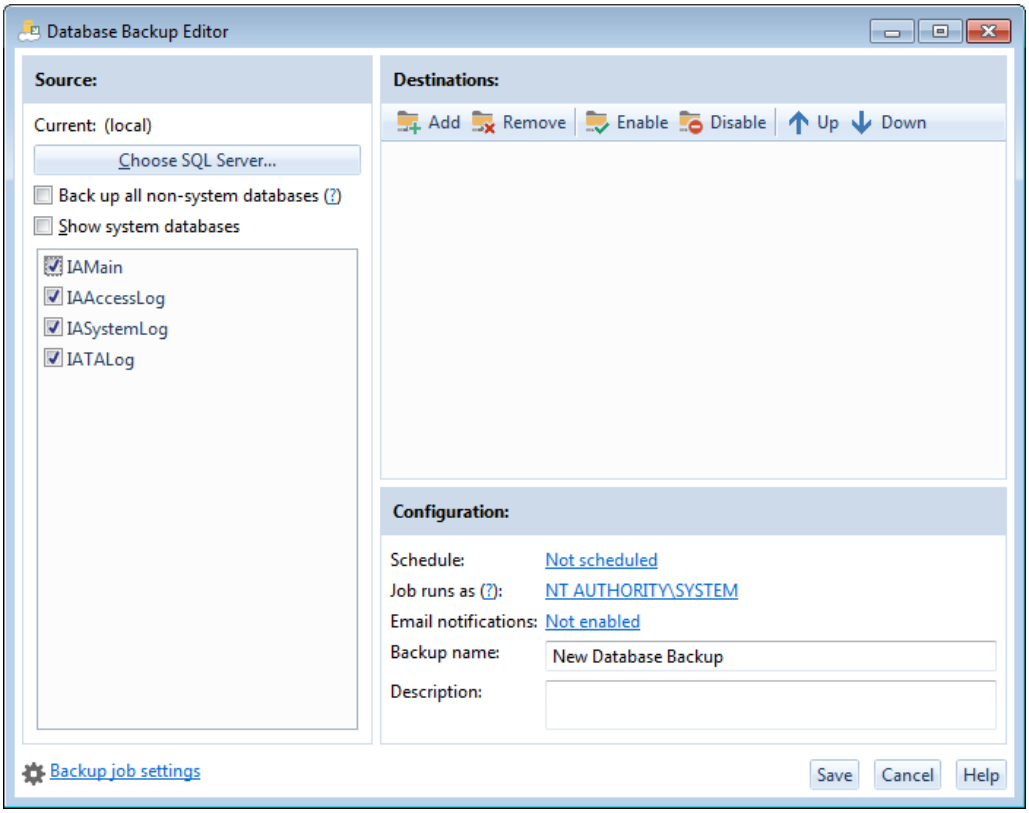
- Run the Identity Access Setup Wizard
- In the side bar, select **Extra** followed by **SQL Backup Master**
- Click on **[Install SQL Backup Master]**.

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.

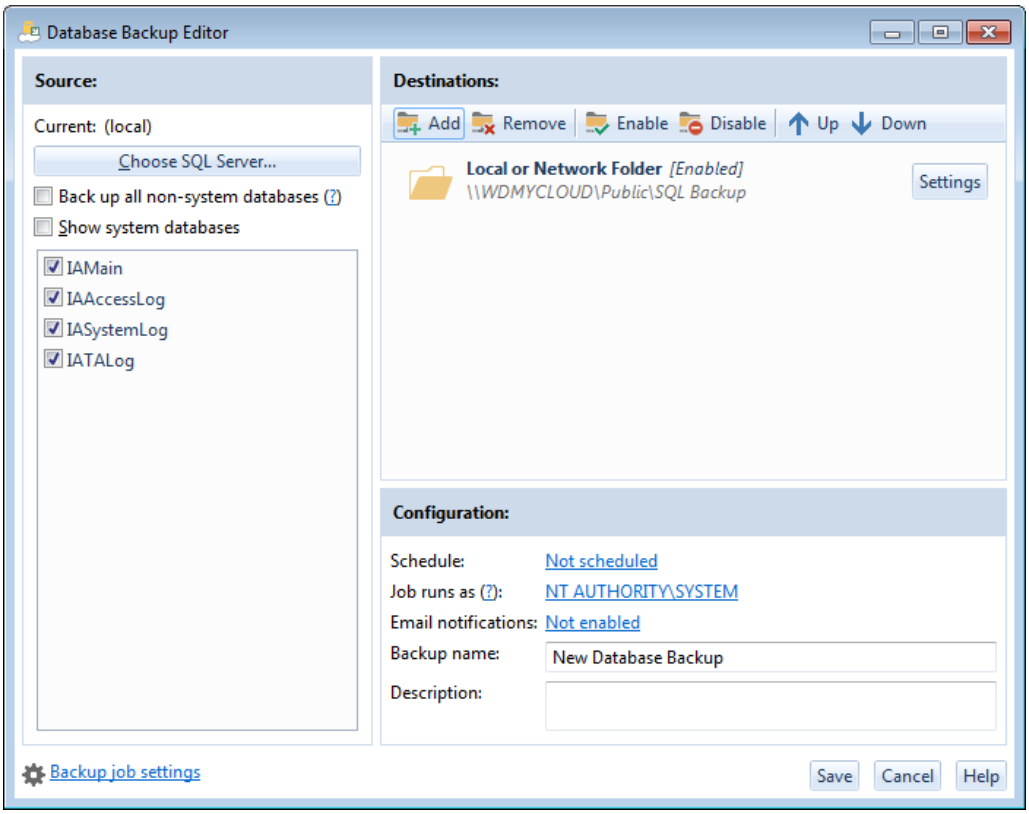
To create a backup scheme, Click the **Start** button, **All Programs**, **SQL Backup Master**, then select **SQL Backup Master**



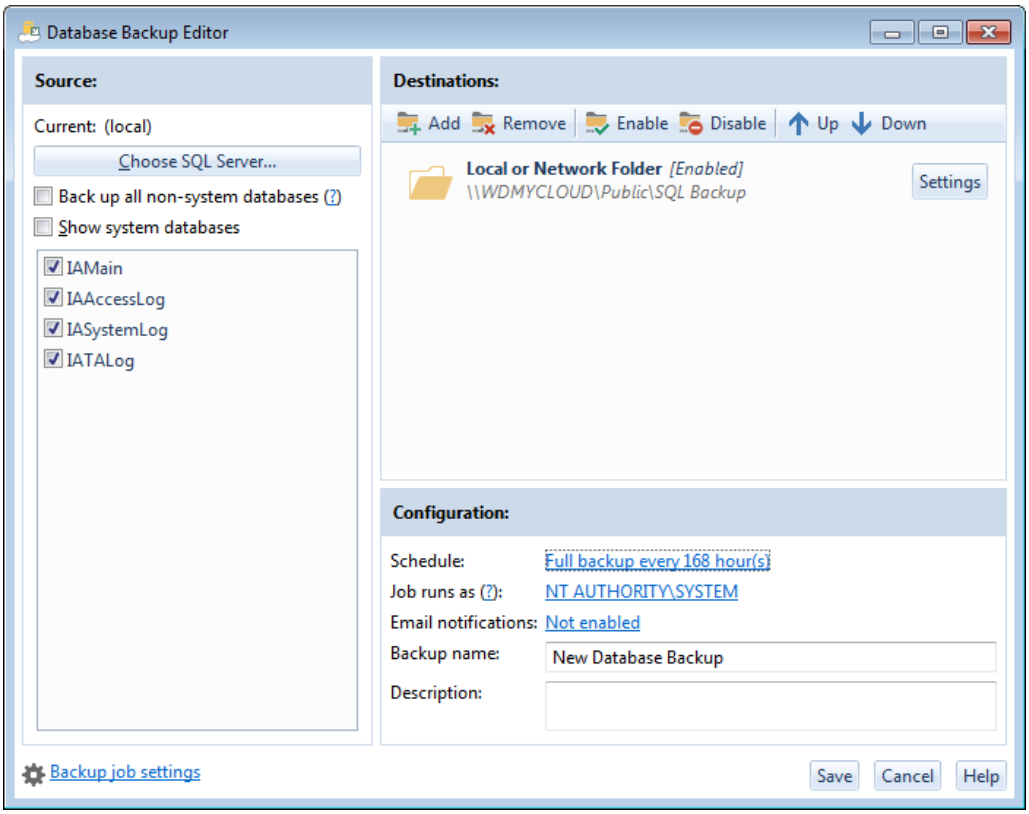
Connect to the Identity Access SQL database and configure the software to backup all 4 databases (Main, Access Log, System Log and Time & Attendance Log):



Add a destination on a network folder:



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



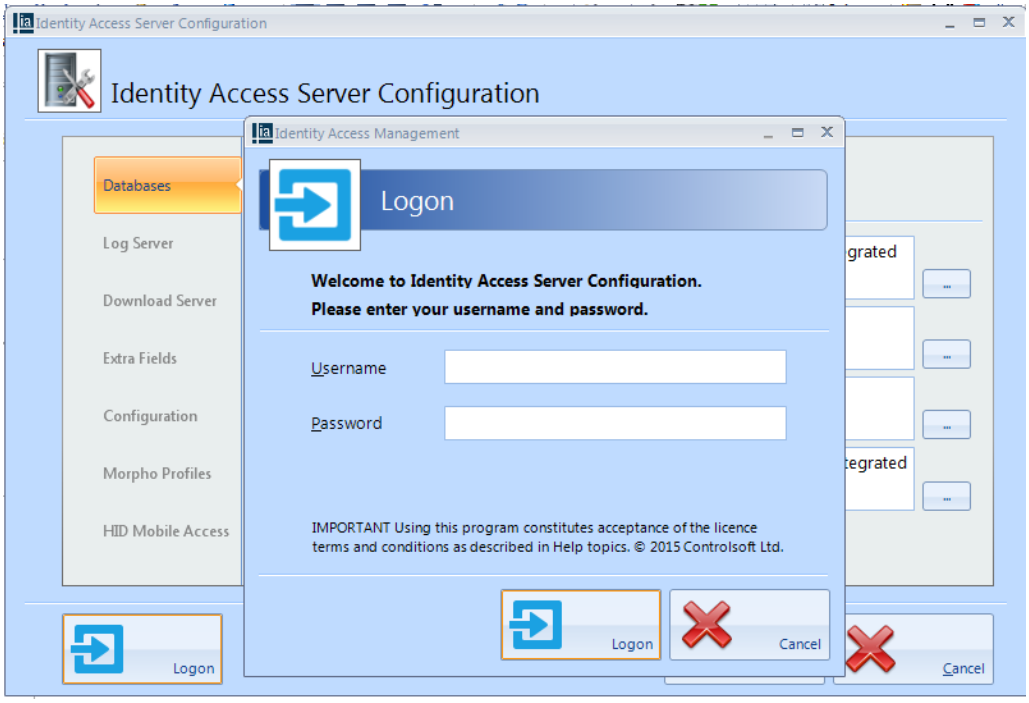
Save the profile and the customer's data will now be regularly backed up.

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

2.7 Identity Access Server Configuration

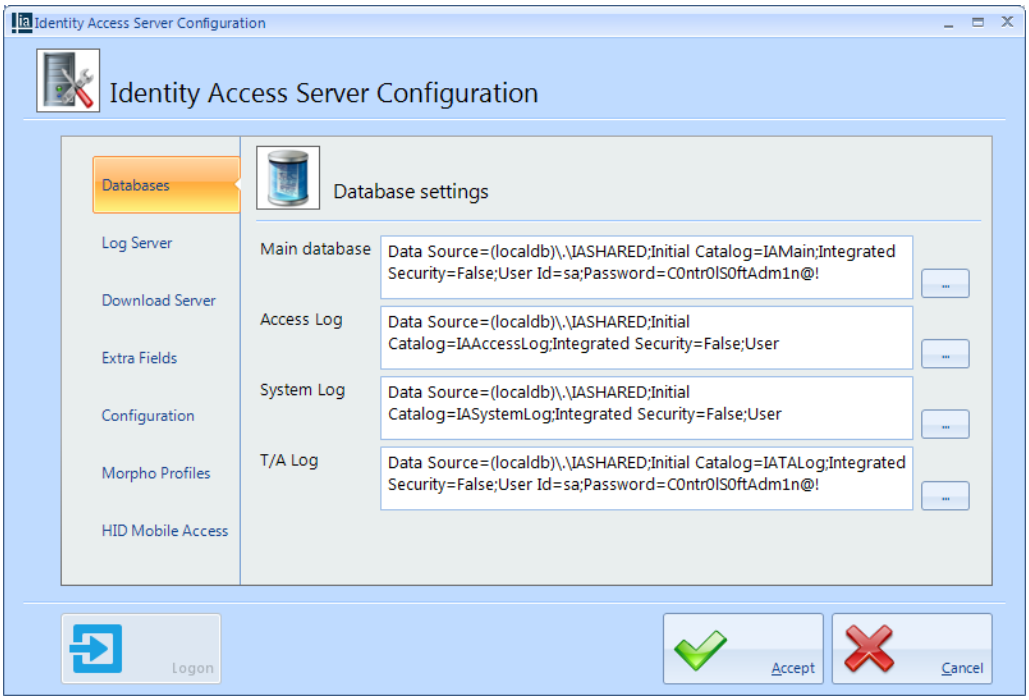
The **Identity Access Server Configuration** tool is used to configure certain features of the Identity Access server software, such as defining the connection path to the SQL database. The tool can be found by selecting the **Start** button, **All Programs**, **Controlsoft**, **Identity Access**, **Server**, **IA Server Configuration**.

First, click the **[Logon]** button and enter the same Username and Password as used for the Identity Access User Interface.



2.7.1 Server Configuration - Databases

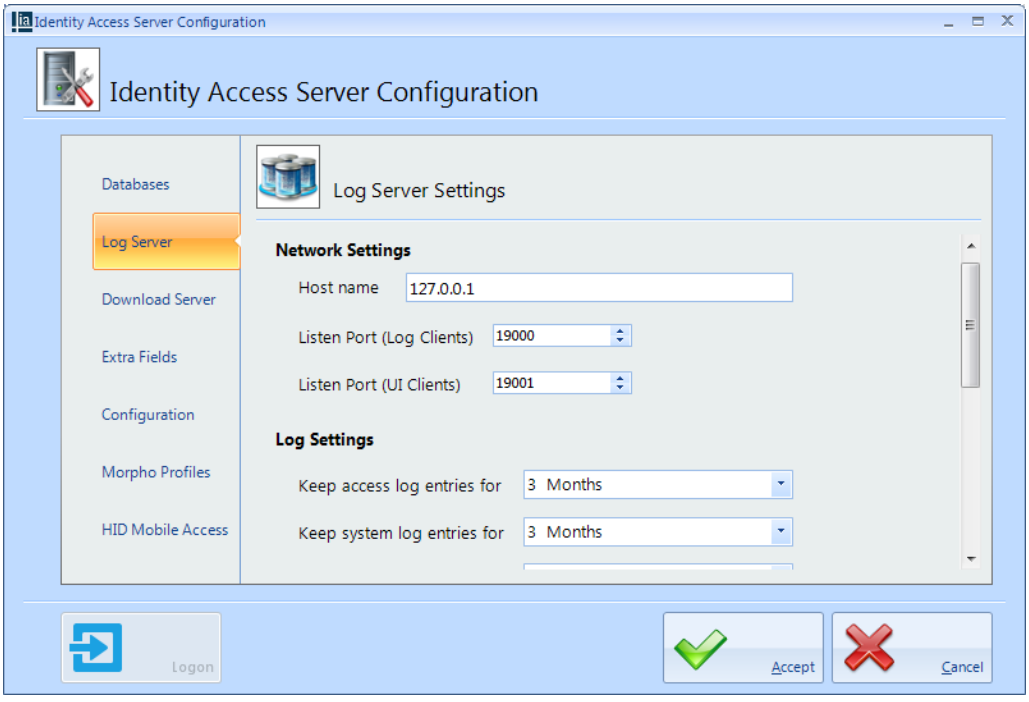
The **Databases** tab is used to point to where the SQL database is installed



NOTE: Do not change these strings unless instructed to do so by Controlsoft Technical Support.

2.7.2 Server Configuration - Log Server

The **Log Server** tab is used to point to the host name or IP Address (127.0.0.1 being the local machine) where the Log Server is installed, how long events should be stored in the database and location of the log buffers.



The **Network Settings** point to the machine that hosts the Identity Access server software (127.0.0.1 being the current machine)

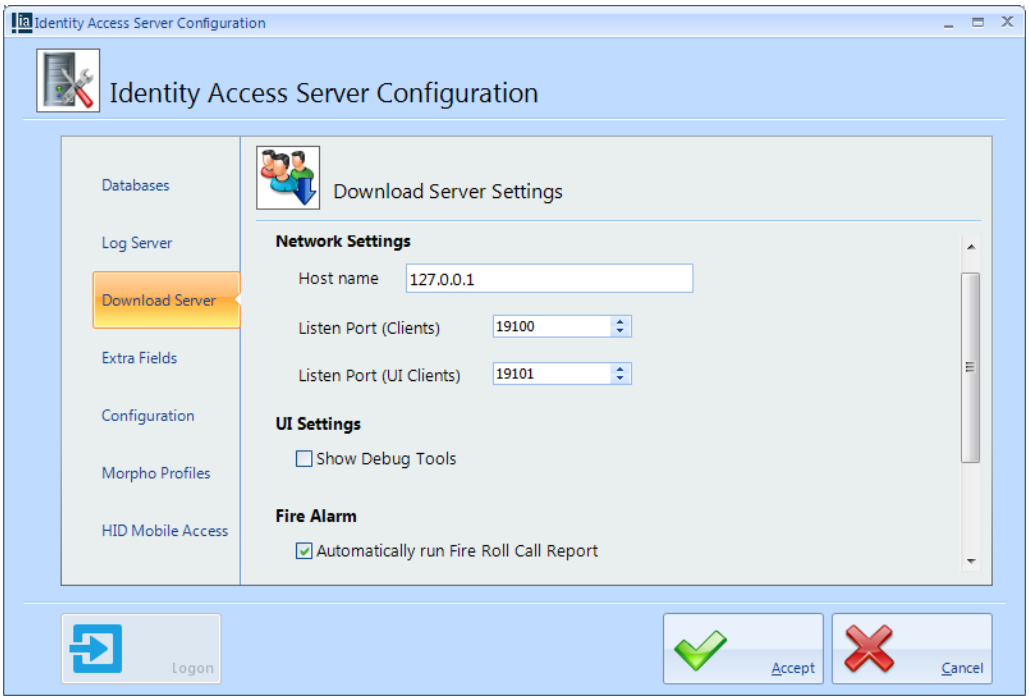
Log Settings define how long each log is maintained before 'old' events are deleted.

The **Log Buffer** strings should not be changed unless instructed to do so by Controlsoft Technical Support.

If the option **Require Administrator login** is ticked, Administrator credentials are required to use the Server Configuration utility.

2.7.3 Server Configuration - Download Server

The **Download Server** tab is used to point to the host name or IP Address (127.0.0.1 being the local machine) where the Download Server is installed. The screen also defines whether debug tools are shown in the Download Server and whether Fire Roll Call report is automatically printed when a fire alarm is generated.



The **Network Settings** point to the machine that hosts the Identity Access Download Server software (127.0.0.1 being the current machine)

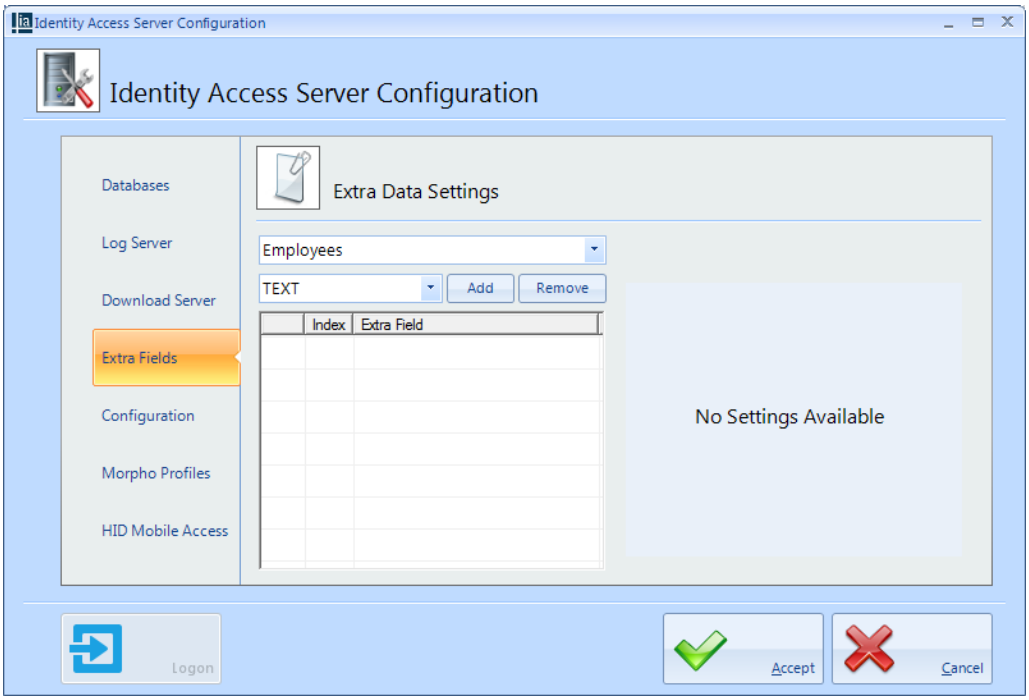
If the **UI Settings** option is enabled, the Download Server debug screen is enabled providing further diagnostics.

Enable the **Fire Alarm** option if a Fire Roll Call report is to be automatically generated at the default printer when the fire alarm system activates. ***Note: This feature requires the Professional Features License (Part Number IA-PRO) to be installed.***

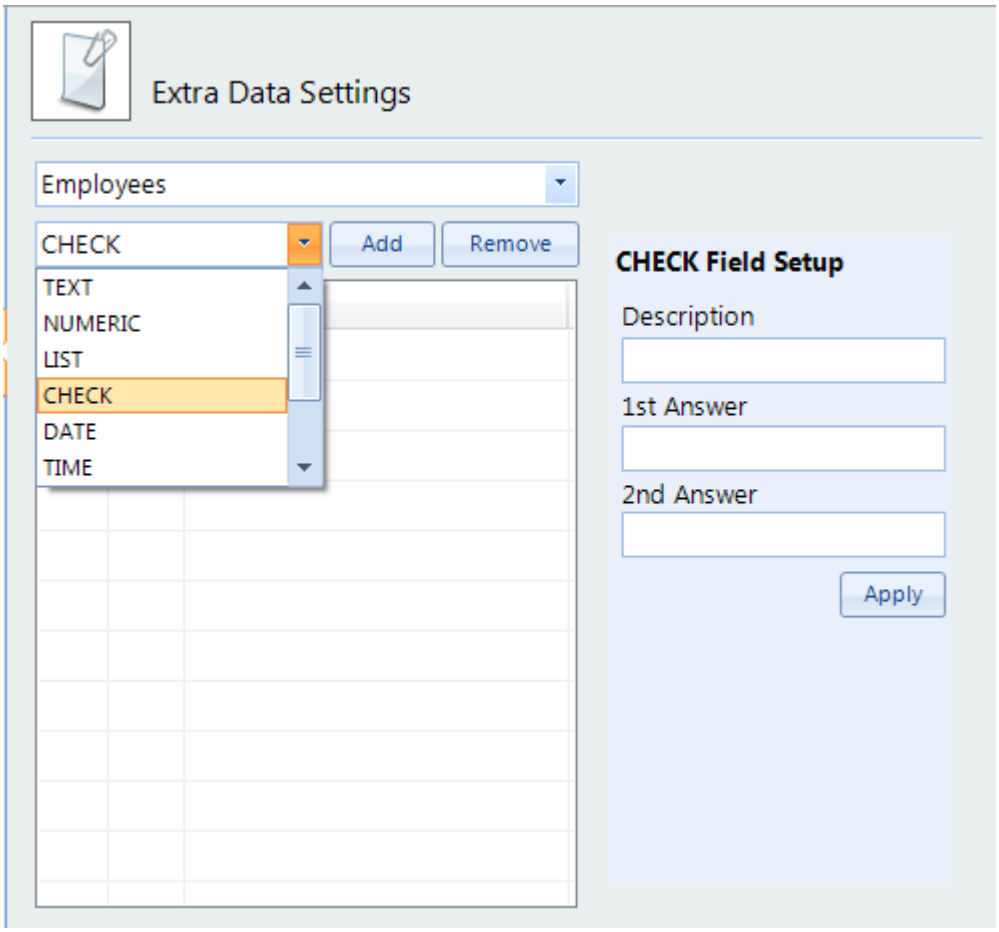
The **Tasks** option will remove tasks that have been busy for longer than the defined time.

2.7.4 Server Configuration - Extra Fields

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



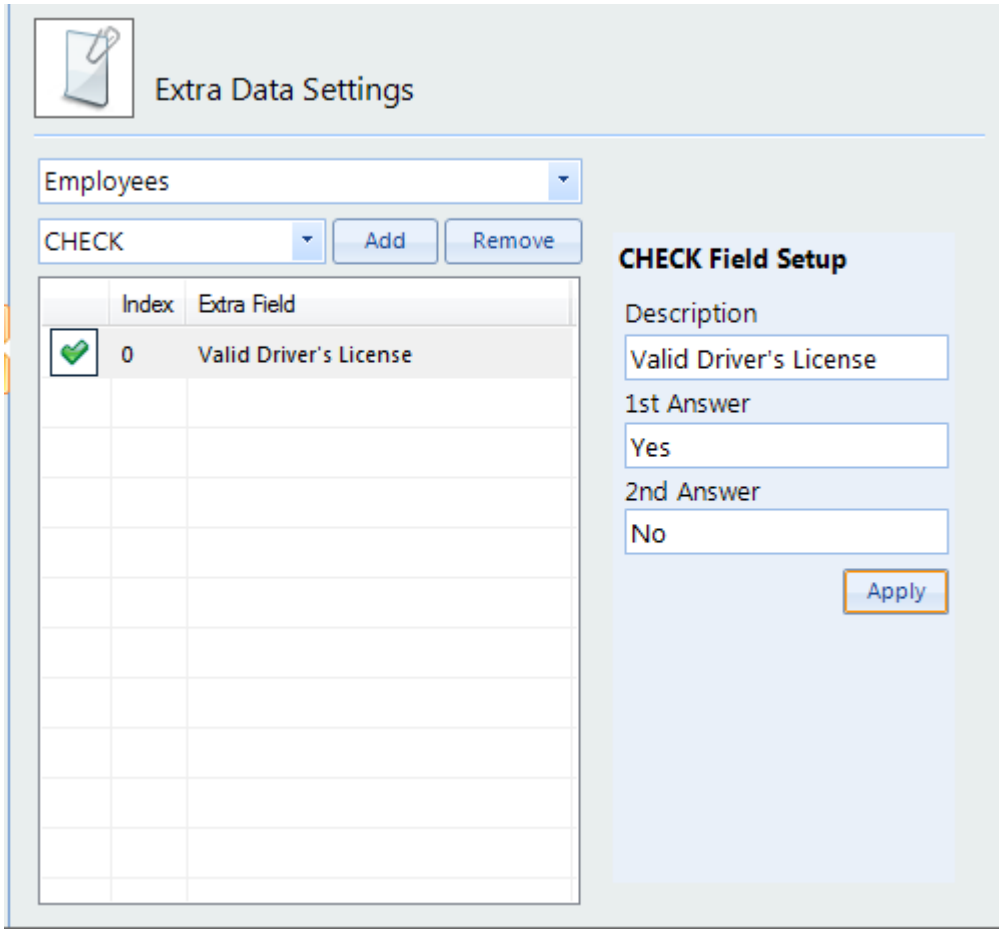
Extra Fields are extremely flexible and very simple to generate. For example, to create an Extra Field to indicate whether an Employee has a valid driver's license, first select Employees, then select **CHECK** for a check box from the dropdown list.



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

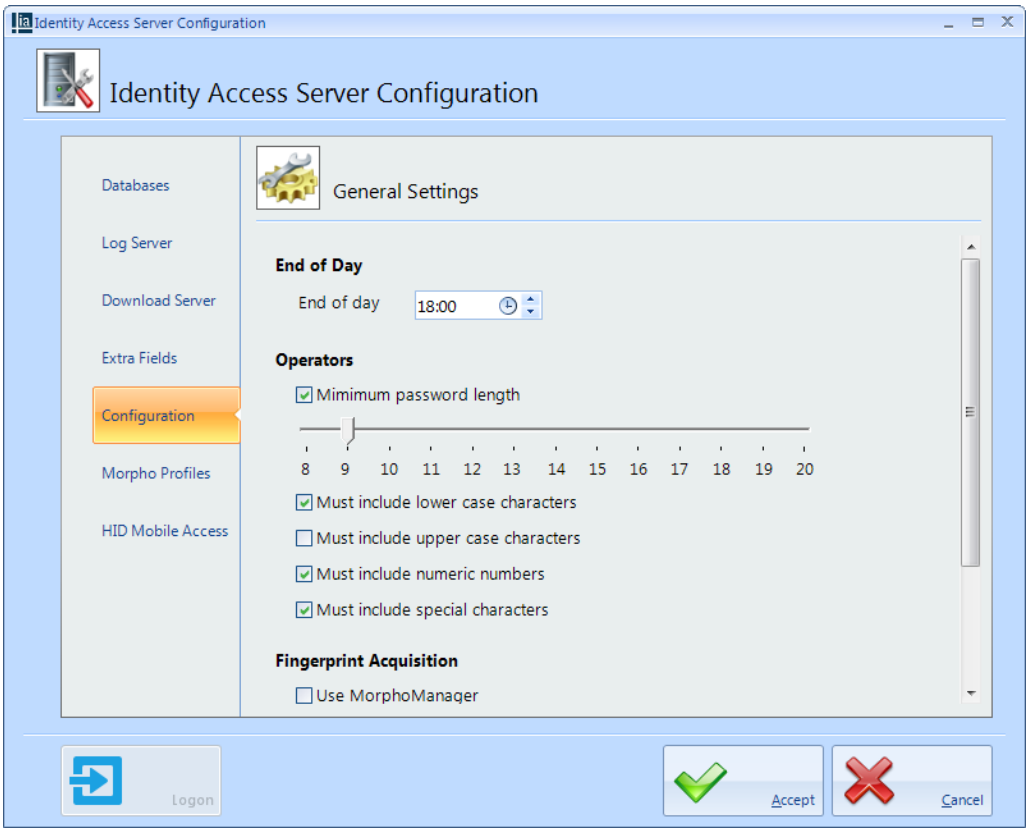
- **Description** = "Valid Driver's License"
- **1st Answer** = "Yes"
- **2nd Answer** = "No"

Click **[Apply]**.



2.7.5 Server Configuration - Configuration

The **Configuration** tab sets various parameters as described below:



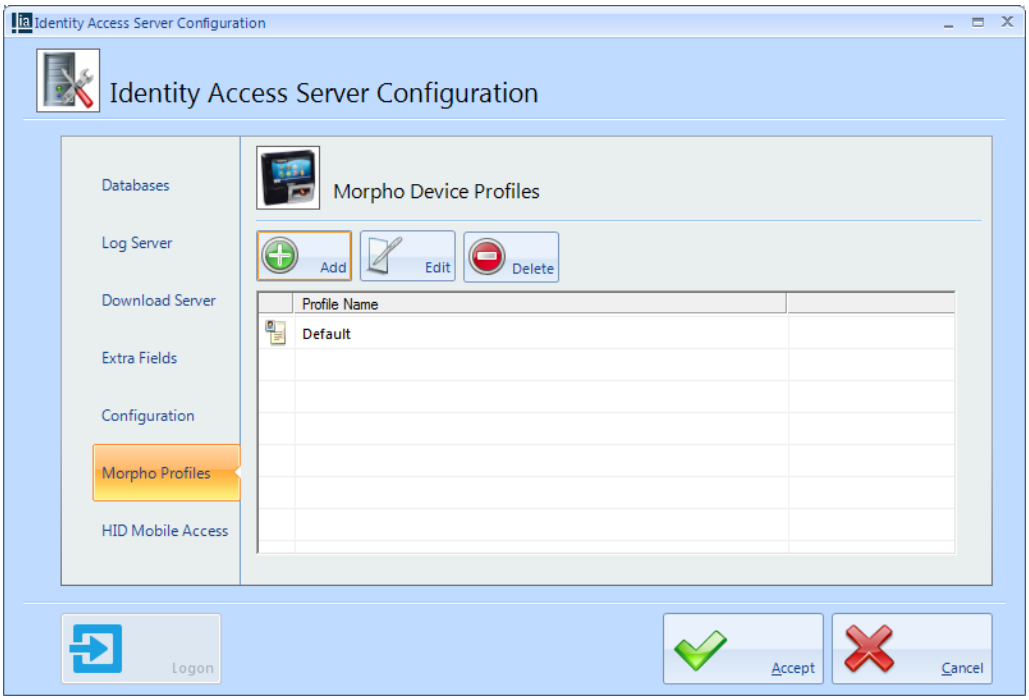
End of Day defines the time at which the IA software considers the working day complete.

The **Operators** tab enforces constraints on the strength of Operator passwords. In the example above, passwords must be at least 9 characters and must include lower case, numeric and special characters, but may also include upper case characters.

If the **Use MorphoManager** option is selected (not shown above), the **Morpho Readers** icon in the Identity Access **Setup** tab will be greyed out and it will not be possible to enrol fingerprints directly from Identity Access.

2.7.6 Server Configuration - Morpho Device Profile

The **Morpho Device Profile** screen allows configuration of Morpho fingerprint readers:



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

Tick the **Realtime logging enabled** option if Identity Access is to log events from the fingerprint reader. The default retrieval interval is 300 seconds (5 minutes)

The **Allow remote enrollment** option allows a fingerprint to be captured at a reader and the user saved in the selected group.

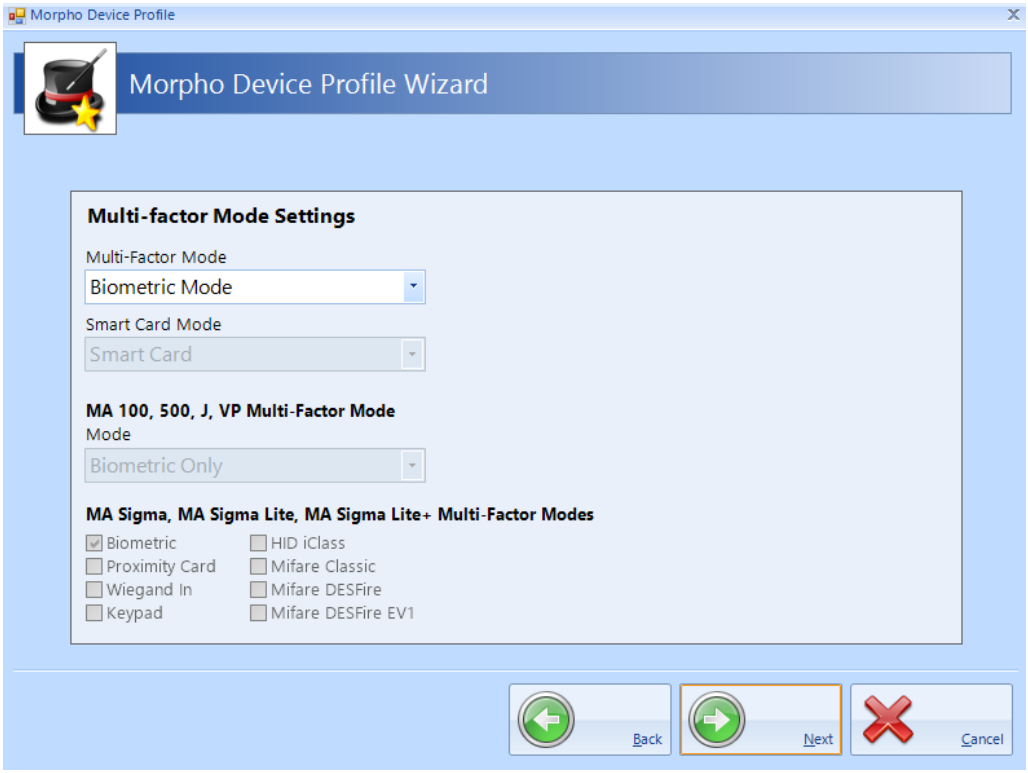
Select **[Next]** to continue

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



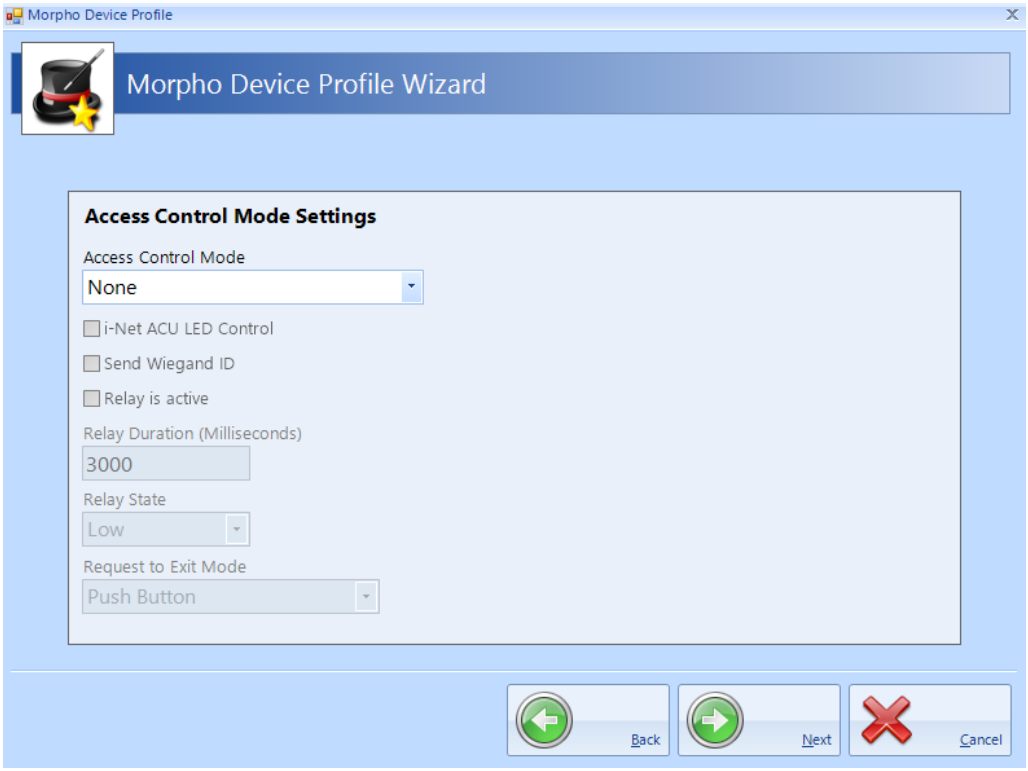
Multi-factor Mode should be set to **Biometric Mode** for fingerprint only, or changed to **Custom** for fingerprint and card

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

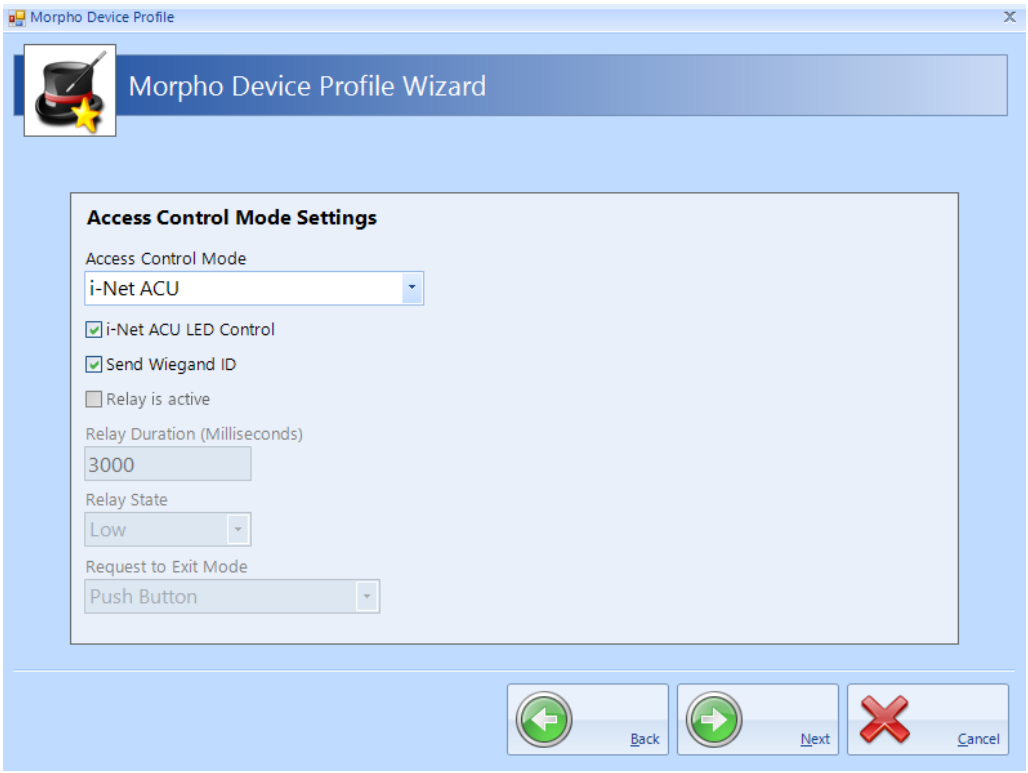
If the fingerprint reader is an MA100, MA500, J-Series or VP reader, the **MA100,500,J,VP Multi-Factor Mode** can be selected between Biometric Only (fingerprint only), Weigand in (a card reader connected to the fingerprint reader), Keypad (PIN), HID iClass, MIFARE or DESfire.

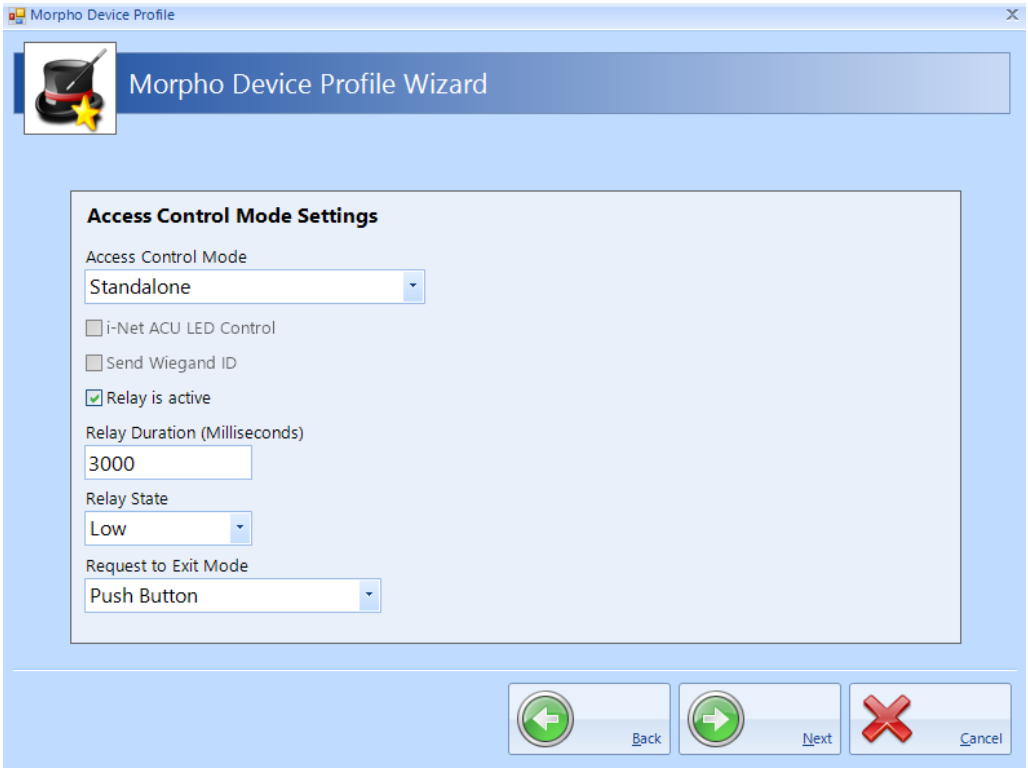
If the fingerprint reader is an MA Sigma, MA Sigma Lite or MA Sigma Lite+, the **Multi-Factor Modes** can be selected as Biometric, Proximity Card, Wiegand in, Keypad, HID iClass, MIFARE Classic / DESfire / DESfire EV1

Click **[Next]** to continue



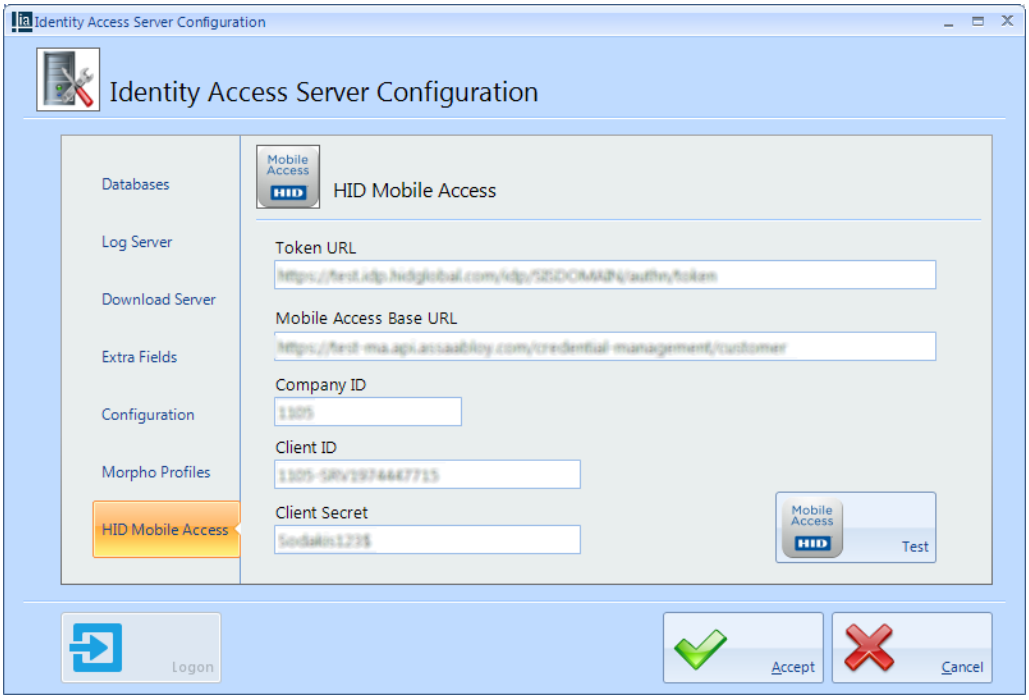
The **Access Control Mode** should be set to None if MorphoManager is used or Standalone if no i-Net controller is used.





2.7.7 Server 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 each field will differ for each customer, so please refer to your vendor for further information on setting up this feature.

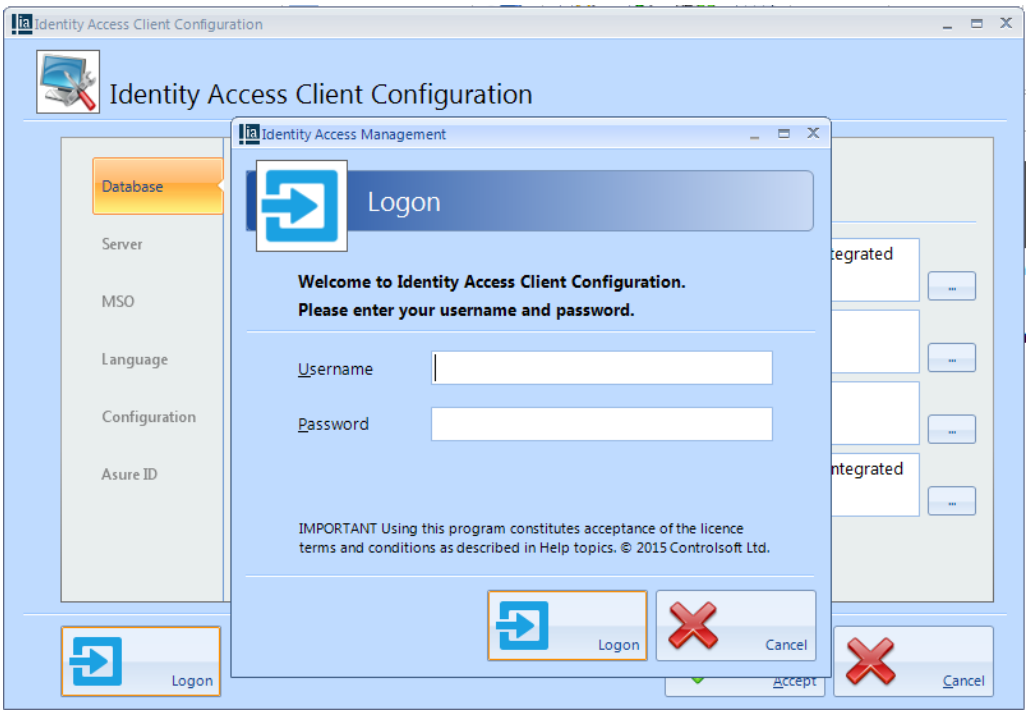


Once the strings are entered, click the **[Test]** button to test the connection to the credential server. If the test is successful, click **[Accept]**.

2.8 Identity Access Client Configuration

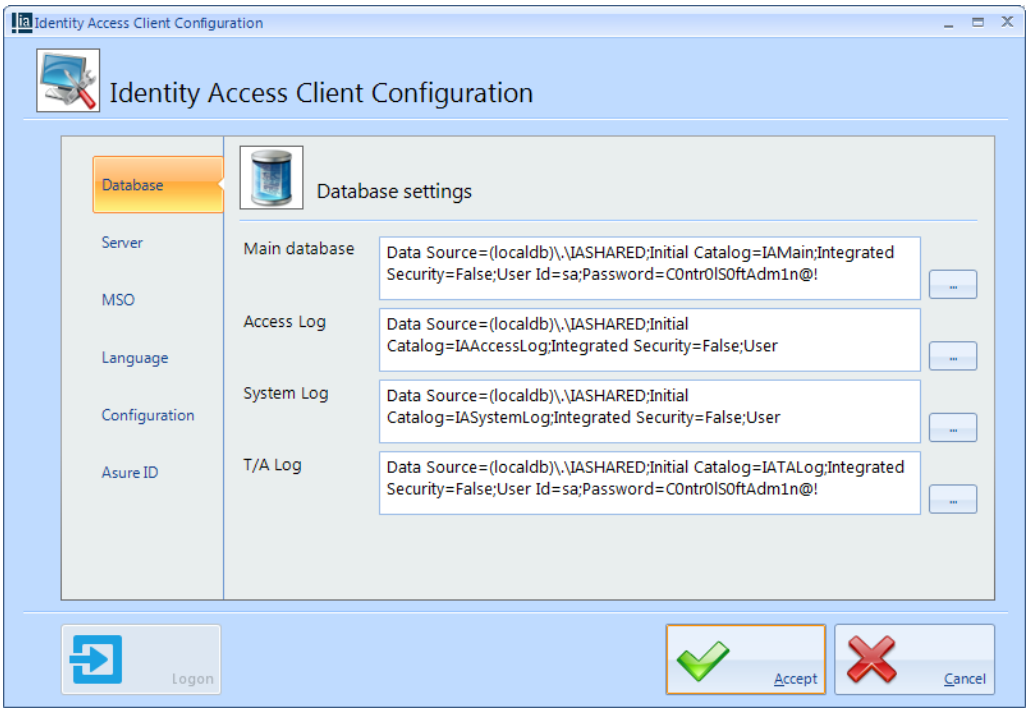
The **Identity Access Client Configuration** tool is used to configure certain features of the Identity Access client, such as defining the connection path to the SQL database. The tool can be found by selecting the **Start** button, **All Programs**, **Controlsoft**, **Identity Access**, **IA Client Configuration**.

To use the Client Configuration utility, click **[Logon]** and enter the same Username and Password as used for the Identity Access User Interface.



2.8.1 Client Configuration - Database

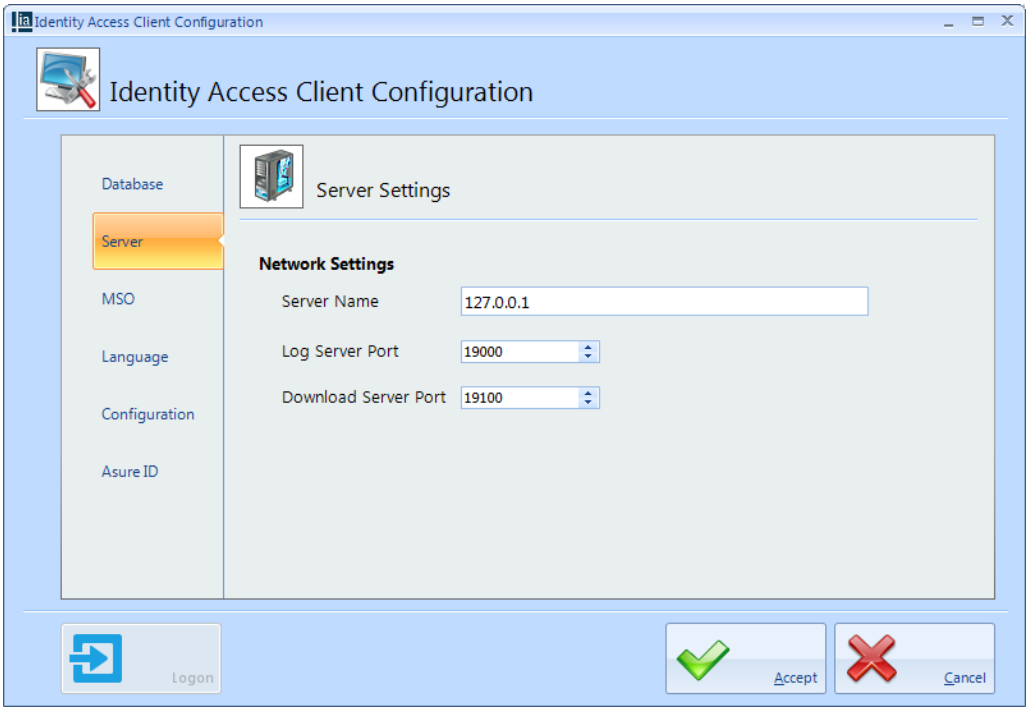
The **Database** tab is used to point to the database in use:



NOTE: Do not change these strings unless instructed to do so by Controlsoft Technical Support.

2.8.2 Client Configuration - Server

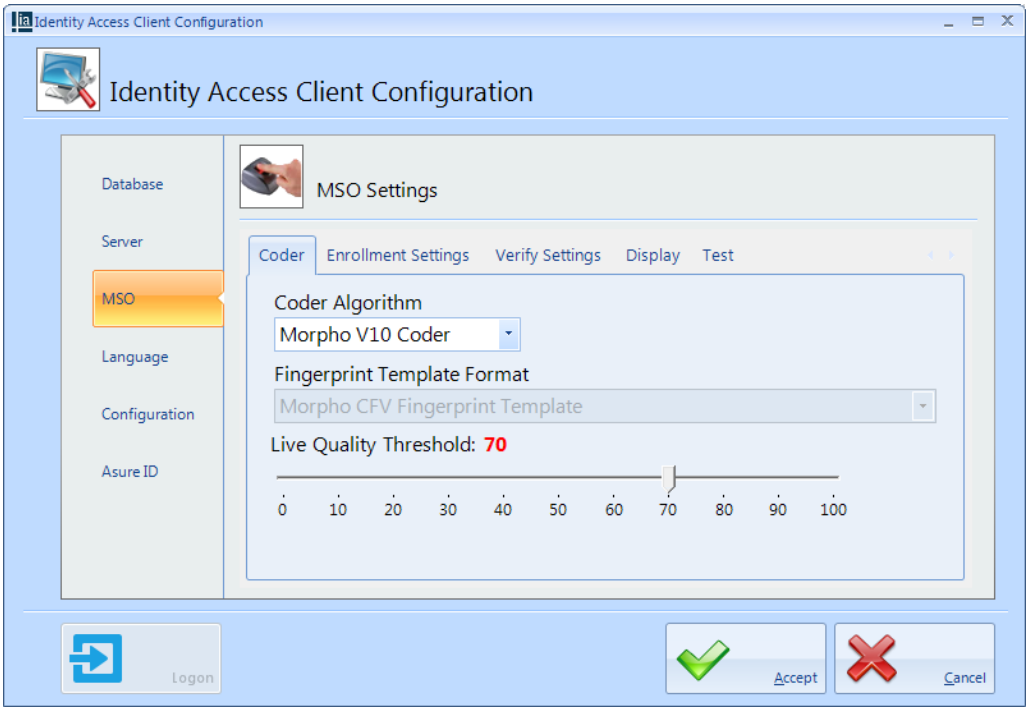
The **Server** tab points to the IP Address of the server (in this example 127.0.0.1 being the local machine):



NOTE: Do not change these parameters unless instructed to do so by Controlsoft Technical Support.

2.8.3 Client Configuration - MSO

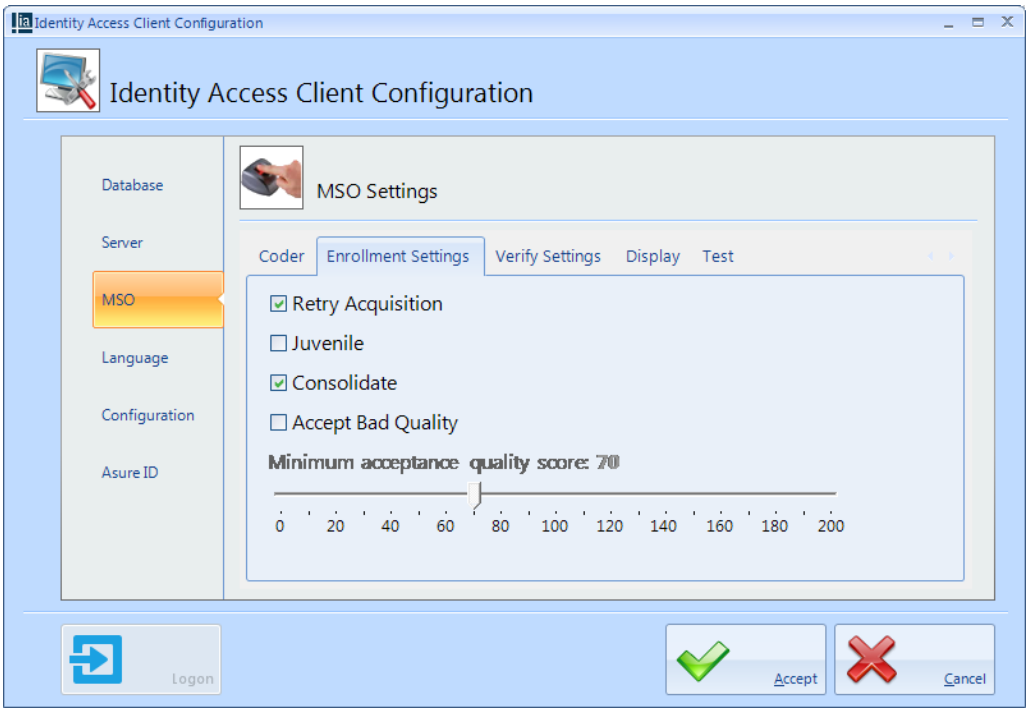
The **MSO** tab is used to configure a USB Fingerprint Enrolment reader. In general, these settings should be left as default unless instructed otherwise by Controlsoft Technical Support:



The **Coder Algorithm** will depend on the Morpho readers being used (V10 being used for the most recent readers). Please refer to the Morpho documentation for the reader in use.

The **Fingerprint Template Format** allows a specific template to be used.

The **Live Quality Threshold** defines the quality of fingerprint read during enrolment. Increasing this from the default of 70 will improve the fingerprint template, but may make it more difficult to enrol a user.



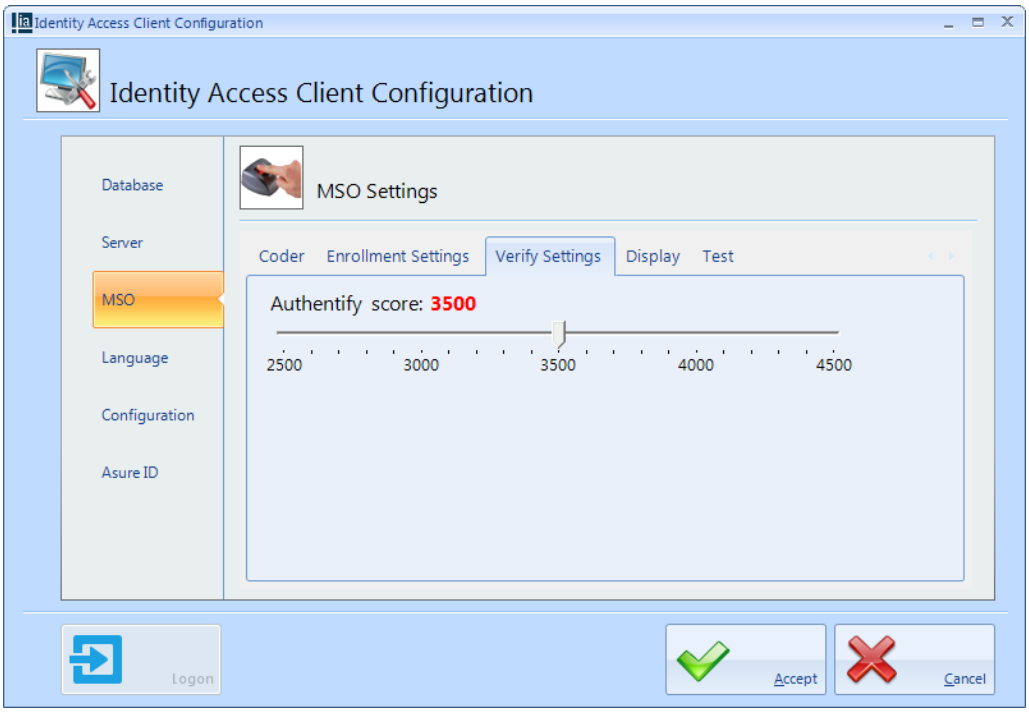
The **Retry Acquisition** allows the user to retry (or not) an acquisition even if live quality is inferior to LiveQualityThreshold.

Tick the **Juvenile** box if enrolling fingerprint images of young applicants (under 12 years old).

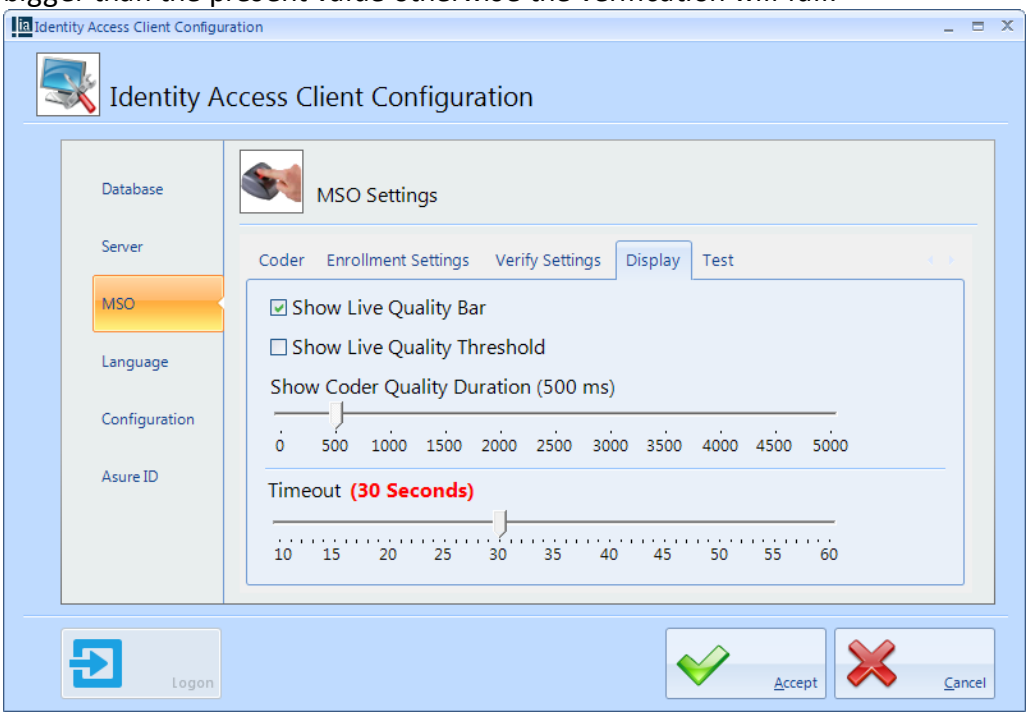
Tick the **Consolidate** option to capture each fingerprint 3 times during enrolment. If unticked, only 1 capture will be required (quicker but poorer quality).

Tick the **Accept Bad Quality** option allows the operator to accept an acquisition even if live quality is less that the **Minimum acceptance quality score**.

The **Minimum acceptance quality score** defines the quality of the image required before the system will enrol a fingerprint.



When you verify your fingerprint the resulting **Authetify Score** value must be bigger than the present value otherwise the verification will fail.

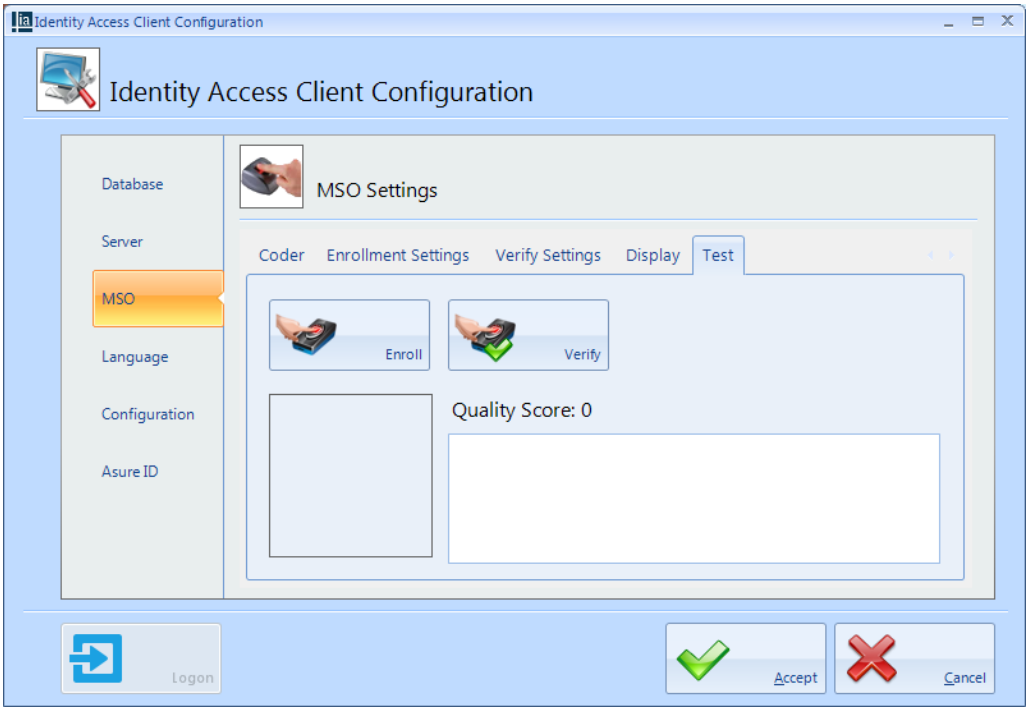


If **Show Live Quality Bar** is enabled, Identity Access will display the quality of the fingerprint during enrolment

If **Show Live Quality Threshold** is enabled, Identity Access will display during enrolment this as a reminder of the minimum acceptable quality level.

Show Coder Quality Duration indicates the duration which the coder quality is shown before closing the acquisition window. Simply move the slider to adjust this setting.

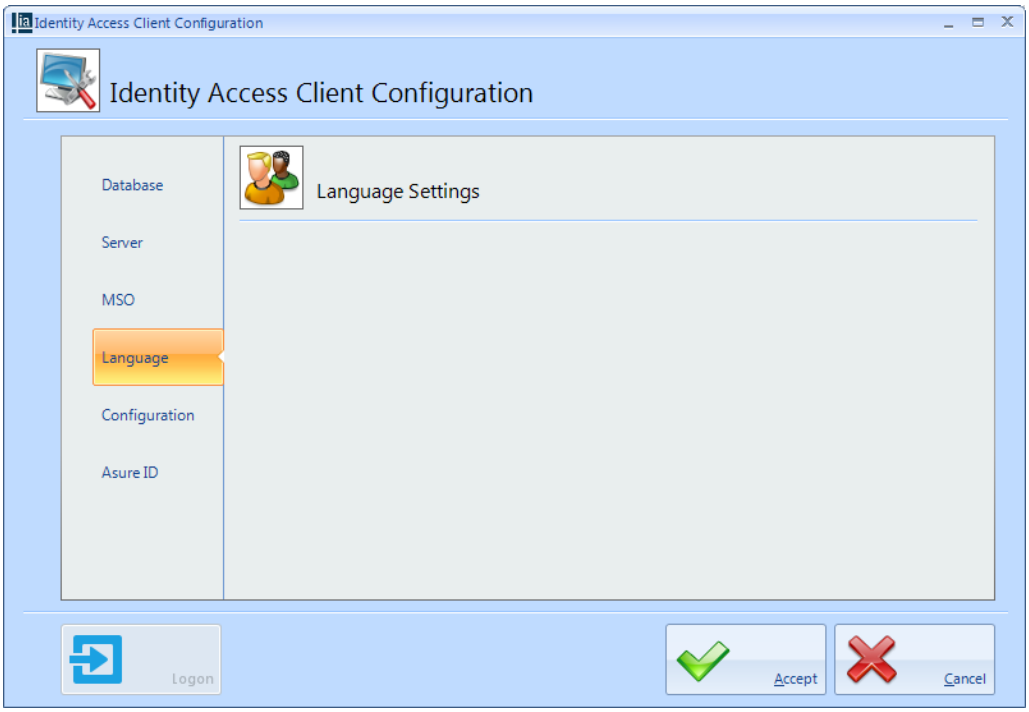
Timeout indicates the duration (in seconds) that the Fingerprint Acquisition box will be displayed without a finger present. Simply move the slider to adjust this setting.



Use this screen to test the operation of enrolling a fingerprint. Click the **[Enroll]** button to read the fingerprint, and the **[Verify]** button to check it.

2.8.4 Client Configuration - Language

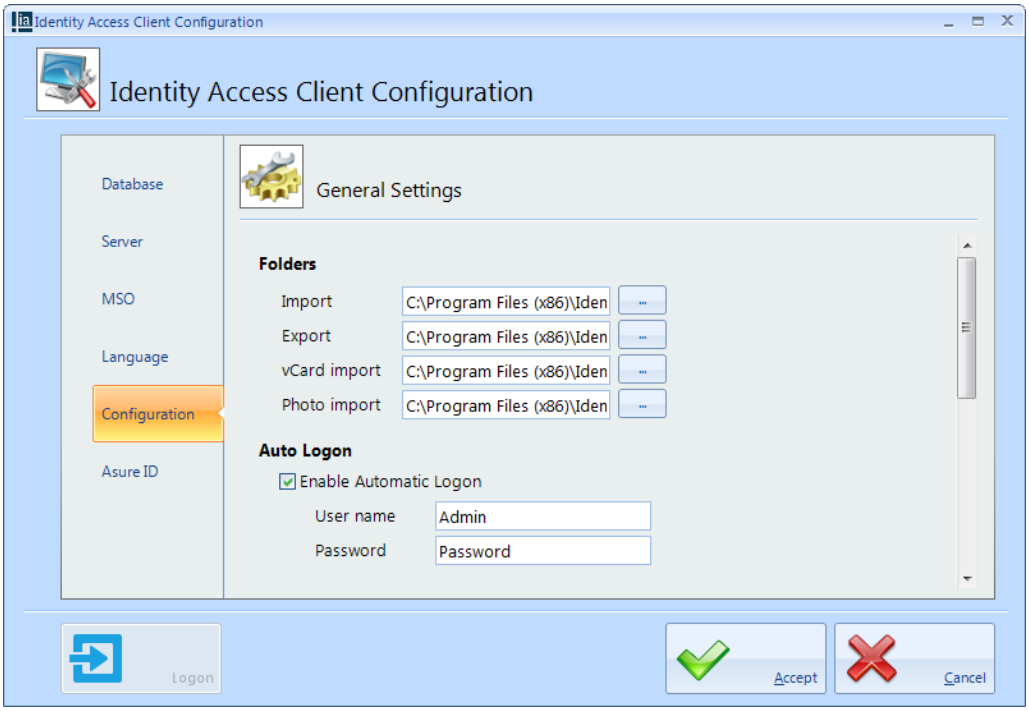
The **Language** tab is used to configure the language options open to the operator:



NOTE: Language options are not currently available in Identity Access.

2.8.5 Client Configuration - Configuration

The **Configuration** tab defines the location of various folders, whether the client automatically logs on when run and the location of the Log Buffers:

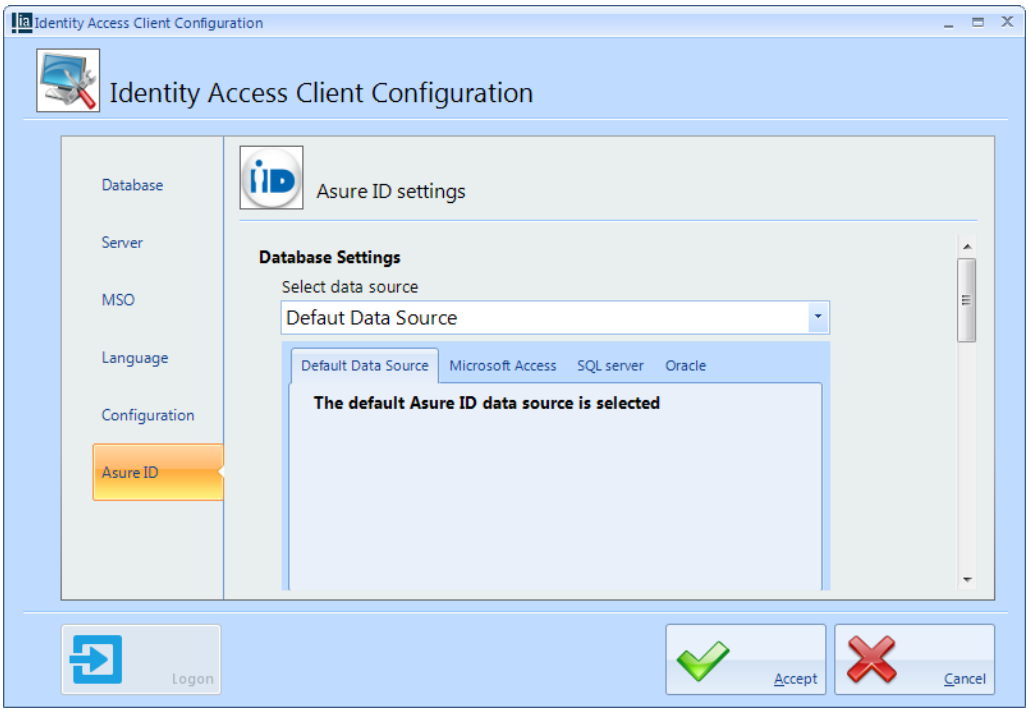


NOTE: Automatic Logon should be used with care as it reduces the security of the system as login credentials will not be required.

The **Log Buffer** strings should not be adjusted unless instructed to do so by Controlsoft Technical Support.

2.8.6 Client Configuration - Asure ID

Identity Access works in conjunction with HID's Asure ID software to print cards.



Database Settings are preconfigured to work with the Identity Access database.

Card Designer Login is preconfigured with the default login credentials for Asure ID. If these credentials are changed in Asure ID, they will need to be changed here as well

Card Designer Field Mapping maps the required fields in Asure ID to the relevant fields in the Identity Access database. We recommend that you do not change the default mapping.

Register Copy of Asure ID needs to be completed to register the Asure ID software. Once registered, the status will be shown at the botton of the screen

Preparing for IP Connection

3 Preparing for IP Connection

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

NOTE: A default i-Net Controller is configured with the IP Address 10.0.1.230

The procedure is to configure the PC to an IP Address on the same network segment as the i-Net (e.g. 10.0.1.200), then use Controlsoft's i-Net Configurator software to reconfigure each i-Net to an individual IP Address on the target network (see Assigning a Fixed IP Address to the i-Net Controller 83). If you are unsure which IP Address the i-Nets should use, please speak to someone from the site's IT department.

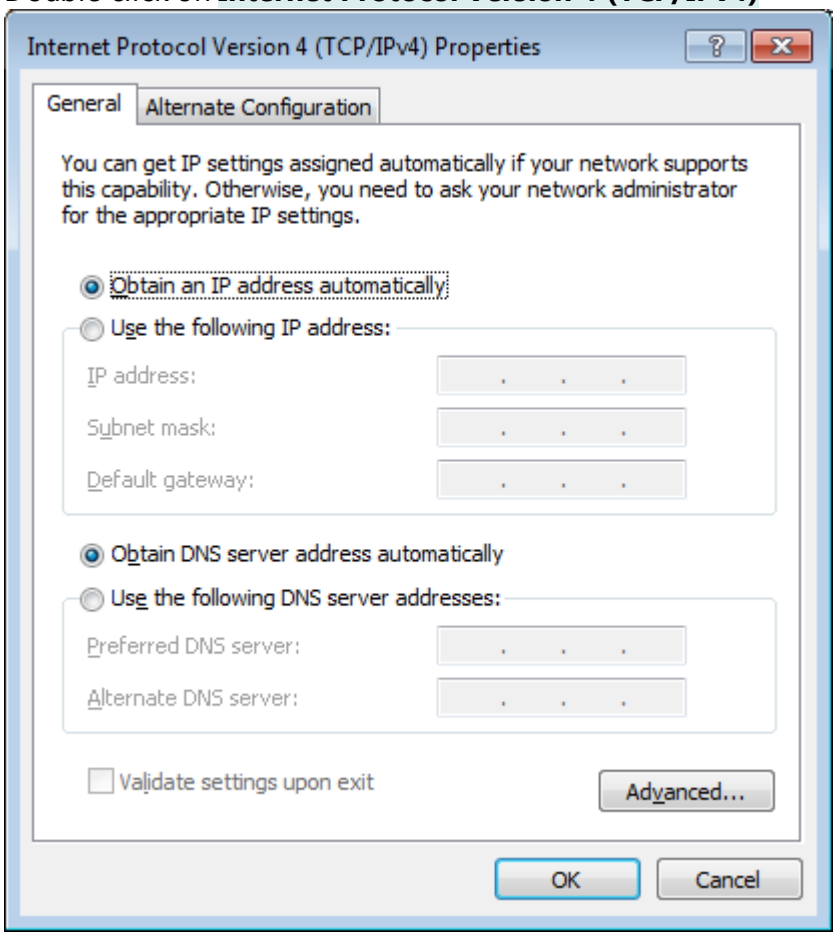
When all the i-Net Controllers have been configured, change the PC's IP Address back to the its original settings.

3.1 Configure the PC

To communicate with the i-Net over a TCP/IP network, the PC and i-Nets must be configured on the same IP range.

1. Click on the Start button and select **Control Panel** (see Appendix C - Windows Commands 222 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]**

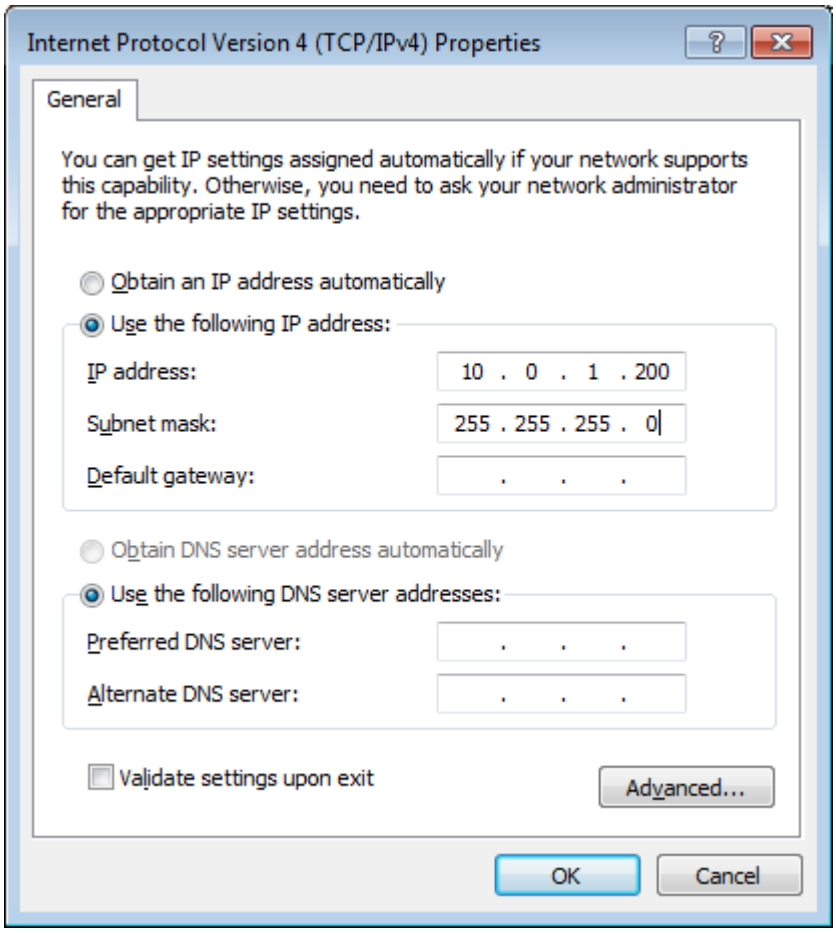
4. Double click on **Internet Protocol Version 4 (TCP/IPv4)**



5. The IP Address needs to be set to an address in the same range as the default IP Address of the i-Net 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



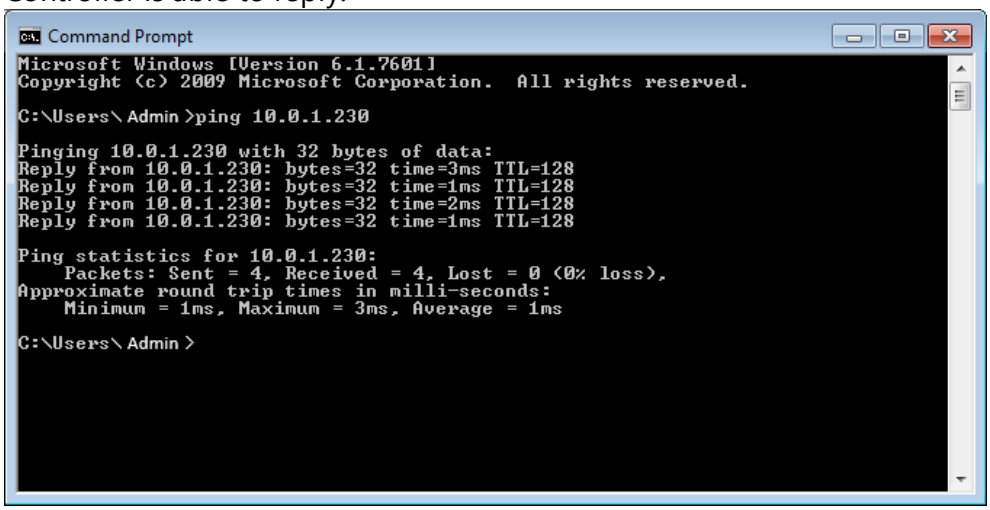
8. Click on **[OK]**, **[OK]**, **[Close]**, then close the Network Connections window.

3.2 Ping the i-Net Controller

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

1. Run the **Command Prompt** (see Appendix C - Windows Commands) 222, then enter the command **`ping 10.0.1.230`** and confirm that the i-Net

Controller is able to reply:



2. If the i-Net controller does not respond, check the network wiring between the PC and the controller.

3. If the i-Net 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 on the right hand edge of the board and hold it in for 30 seconds. Wait for the i-Net 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

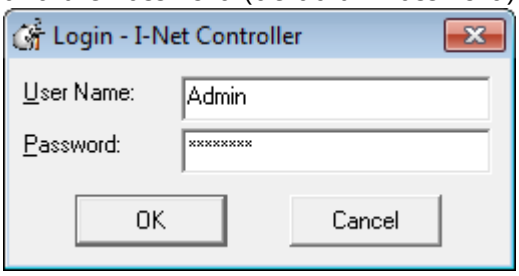
Before assigning IP Addresses to the i-Net Controllers, first contact the IT department for the site and obtain IP addresses for each of the controllers installed.

NOTE: i-Net controllers MUST be configured with FIXED IP Addresses.

Launch i-Net Configurator software previously installed:

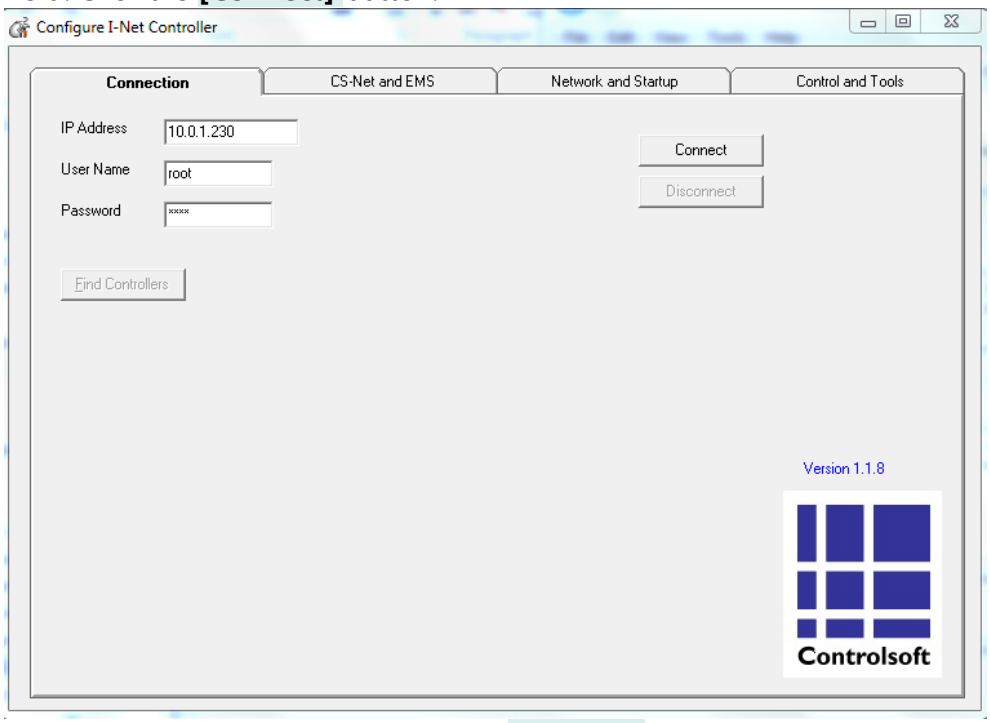
Select **Start** > **All Programs** > **Controlsoft** > **Identity Access** > **Tools** > **i-Net Configurator** > **i-Net Configurator**

When the Login screen is displayed, enter the Username (default = Admin) and the Password (default = Password) as shown below:



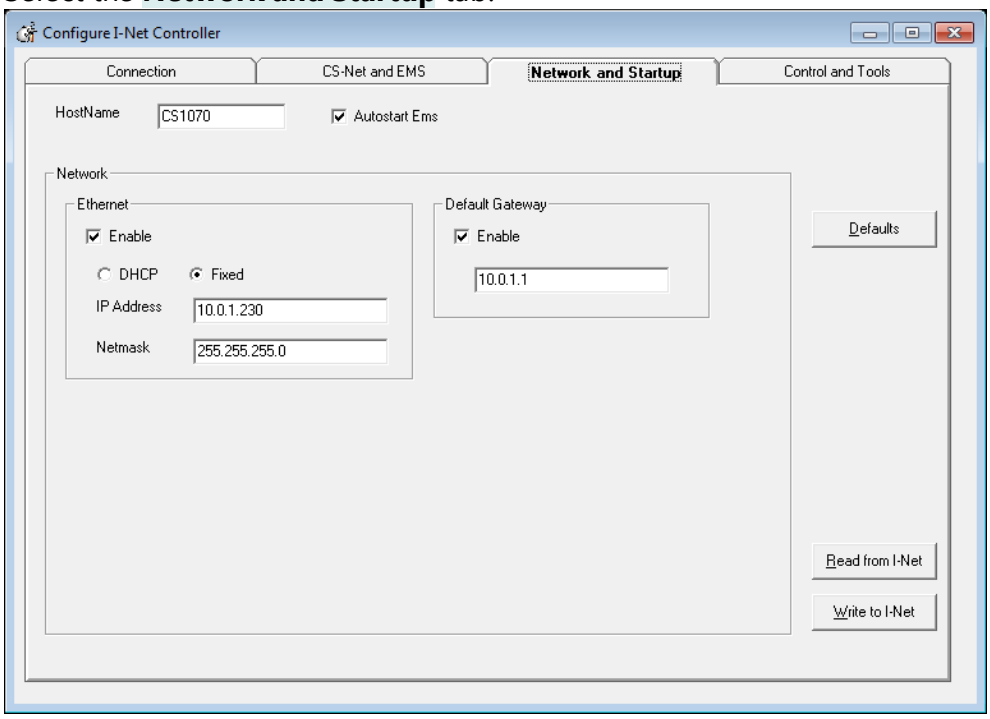
1. Connect one i-Net to the network and ping it to confirm that a connection is possible

2. On the **Connection** tab, enter the IP address of the i-Net in the **IP Address** field. Click the **[Connect]** button.



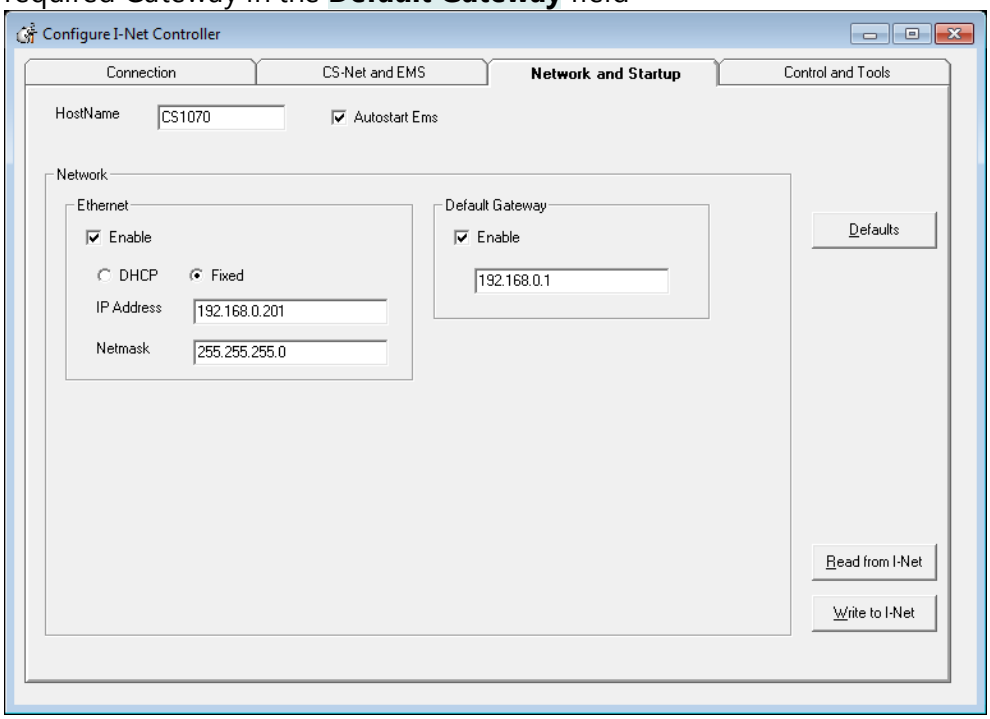
When a connection is established, the **[Connect]** button will grey out and the **[Disconnect]** button will become live.

3. Select the **Network and Startup** tab.



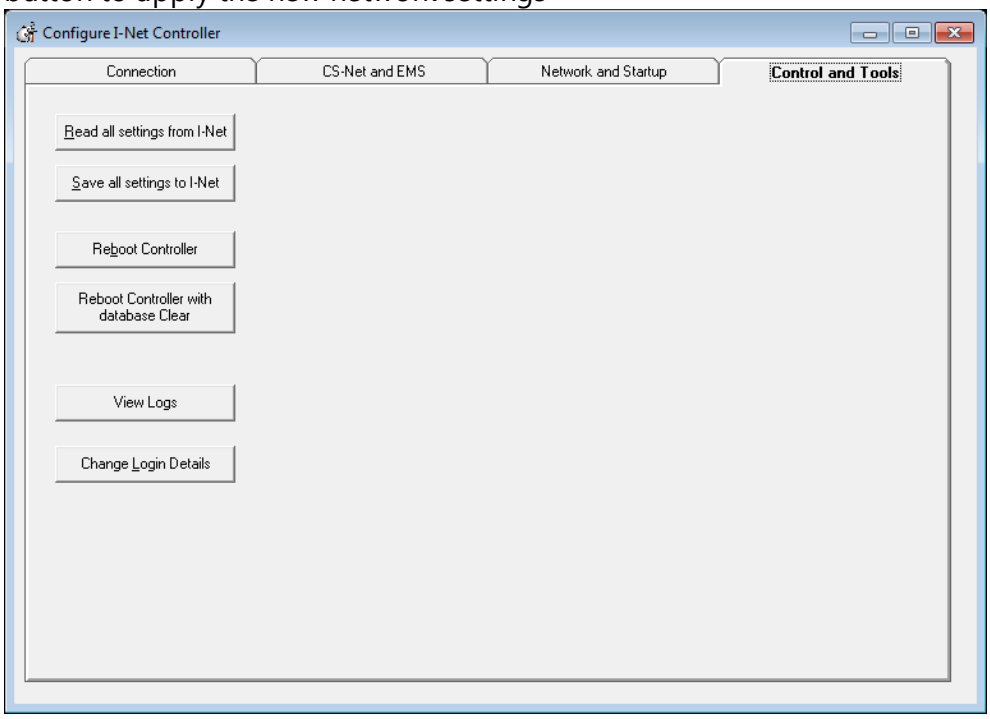
4. Ensure that **Autostart EMS** is checked. Ensure that **Ethernet** is enabled and **Fixed** is selected. Enter the required IP Address in the Ethernet **IP Address** field and the required subnet mask in the Ethernet **Netmask** field

5. Ensure that the **Default Gateway** option is enabled, and enter the required Gateway in the **Default Gateway** field



6. Click the **[Write to i-Net]** button to send the new network settings to the i-Net Controller.

7. Select the **Control and Tools** tab and click the **[Reboot Controller]** button to apply the new network settings



8. When the i-Net has rebooted, ping the controller (see Ping the i-Net Controller) 82 on its new IP address and ensure that it responds

Repeat from step 1 for each i-Net Controller.

When all the i-Nets have been configured, return the IP Address of the PC to its original settings.

Starting the Identity Access Software

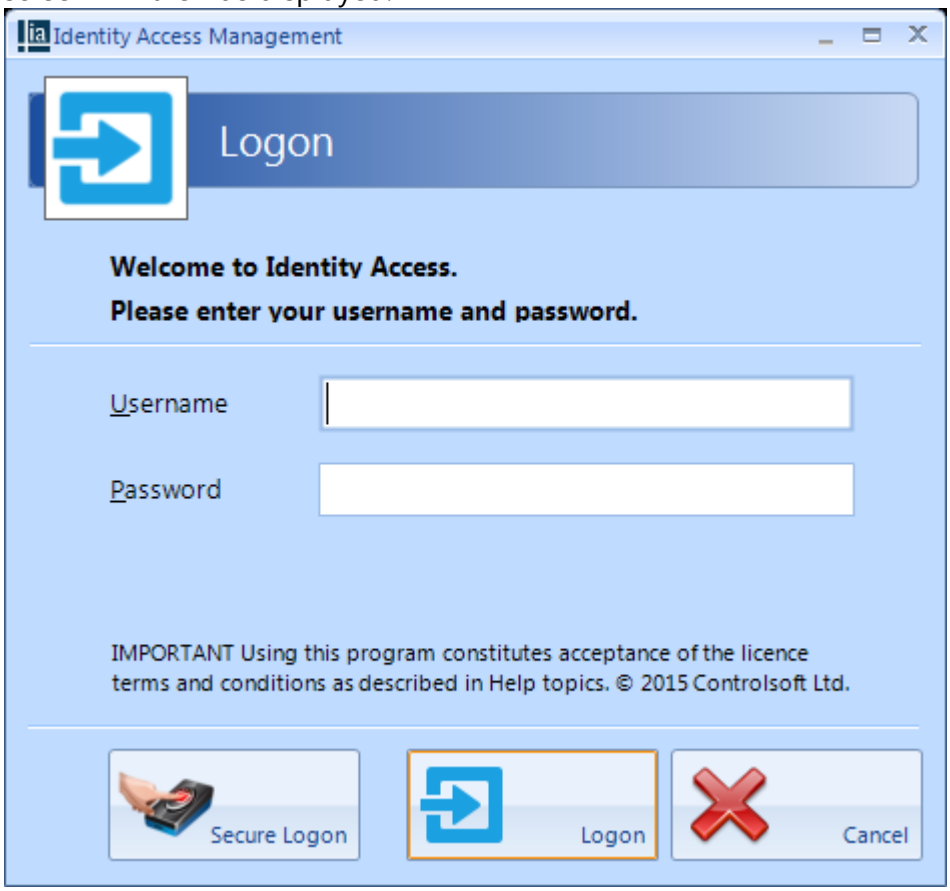
4 Starting the Identity Access Software

To launch the Identity Access software:

1. Start Identity Access as follows.
   Select **Start** > **All Programs** > **Controlsoft** > **Identity Access** > **IA User Interface** (for Windows 7)
   or **Start** > **All Apps** > **Controlsoft** > **IA User Interface** (for Windows 8.1 / 10)
   NOTE: Starting the IA User Interface will automatically start Log Server and Download Server

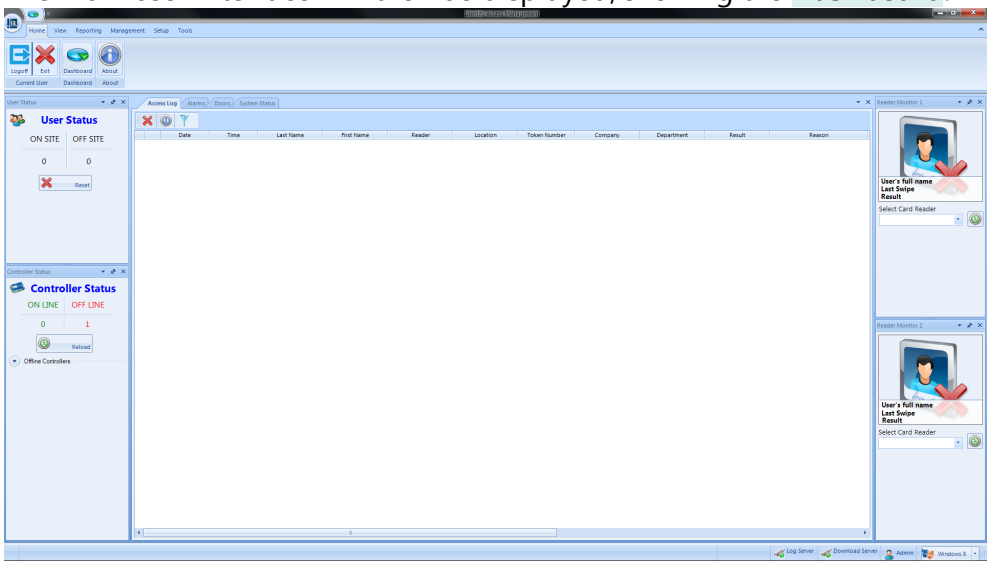
   The following splash screen will be displayed:

2. If Autologon is not enabled in the Client Configuration utility, the Logon screen will then be displayed:



3. 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.***

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

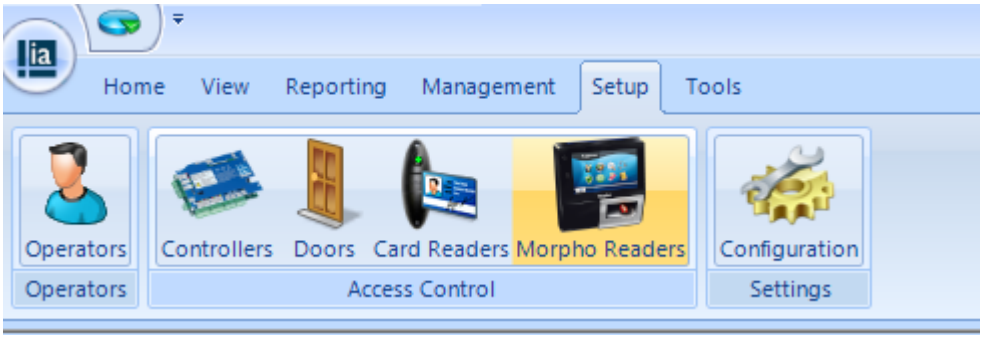


Note: The most common technique to log on to the software is to enter a Username and Password as described above If the operator is also a user, it is possible to log on to the software using a fingerprint.

- 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 the Menu bar and the Ribbon bar, for example:

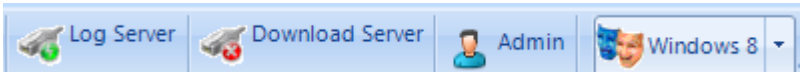


 Use this icon to quickly return to the Dashboard from anywhere in the software.

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

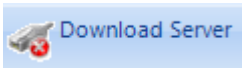
Below the Menu bar is the Ribbon bar, which provides access to individual functions depending on which Menu bar option is selected.

At the bottom of the screen is the footer bar:

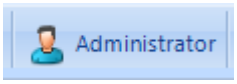


The various icons represent the following conditions:

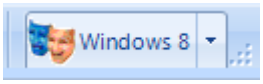
indicates the status of the connection between the Identity Access software and the Log Server (in this example, the green icon indicates that the Log Server is connected)



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



indicates which Operator is currently logged into the software



indicates which colour theme is selected.

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

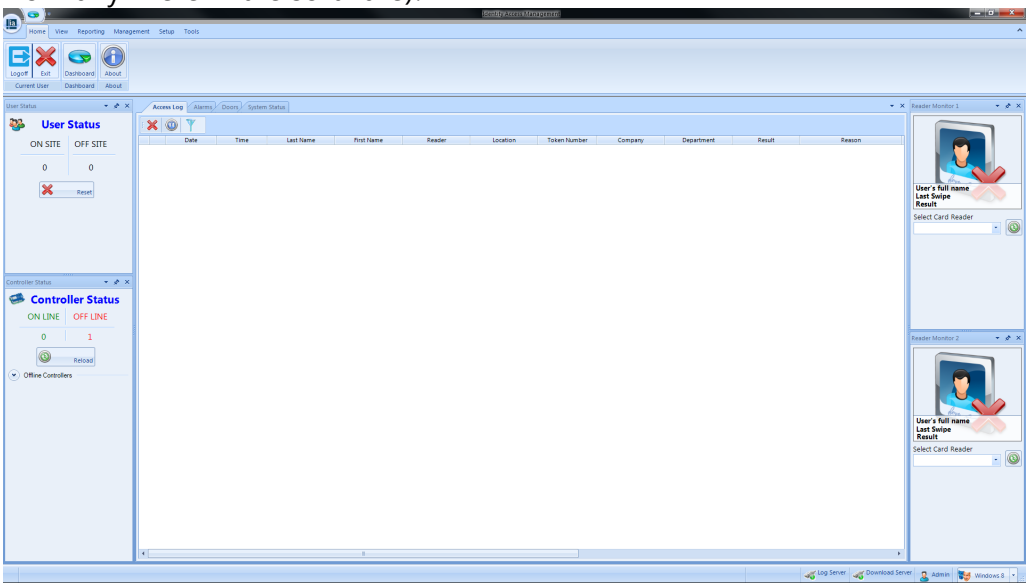
Position the mouse for the required option and click to select.

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) 138

Controller Status: Indicates the number of controllers on line and off line. This is updated depending on whether the Download Server can communicate with each controller

Offline Controllers: Click this option to see which controllers 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 or Fire Alarms). When an alarm condition has been investigated, it 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.

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 door open period (usually 5 seconds), then relock automatically. To unlock the door for a longer period, click the **[Force Open]** button. To subsequently relock the door, simply click the **[Force Closed]** button.

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 latched open through the software by the operator.

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

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

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

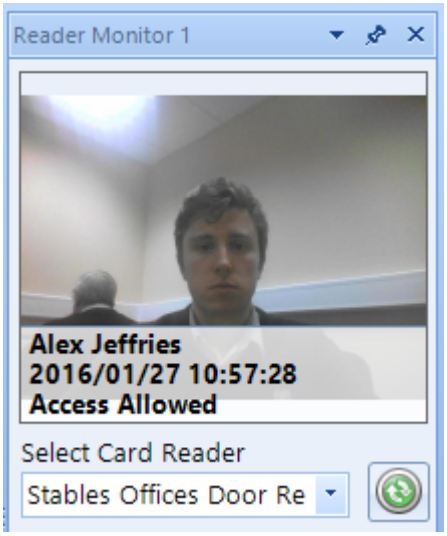
 Access Denied. This symbol indicates that access was denied via the reader and the door was not unlocked.

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

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

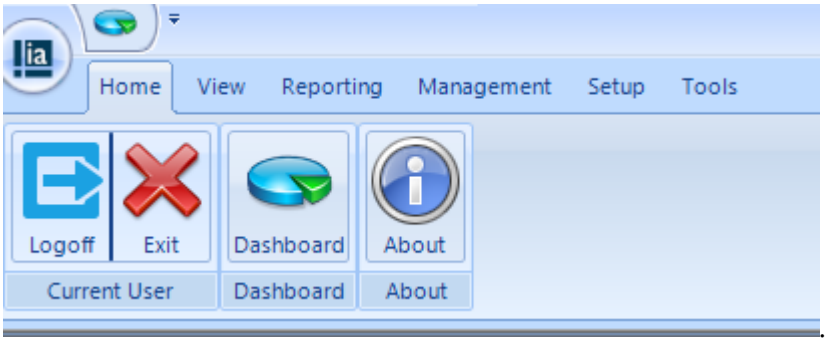
To the right of the Dashboard are two **Reader Monitors**.

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:



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)

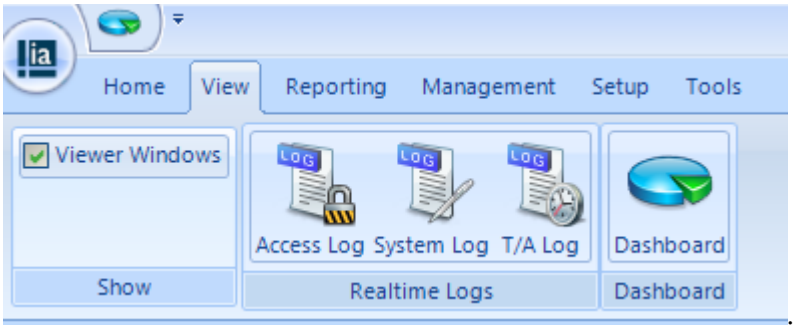
Dashboard: displays the system Dashboard (See The Dashboard) 92

About: This screen shows information about the software, such as version number.

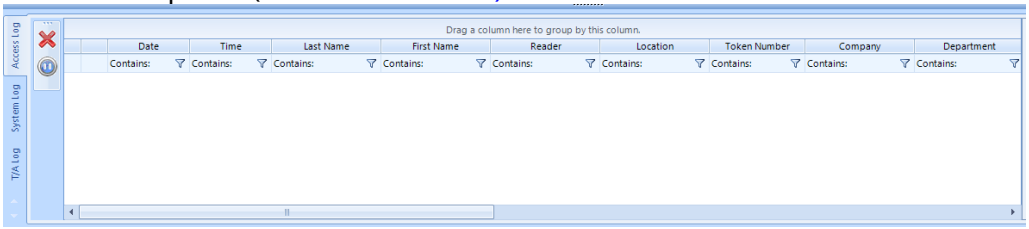
Select the **[System]** tab and click the **[System Information]** button to generate a System Information report on about the system environment. This may be requested by Controlsoft Technical Support if you are experiencing issues.

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 or Time & Attendance events as required (see Event Viewers) 191:



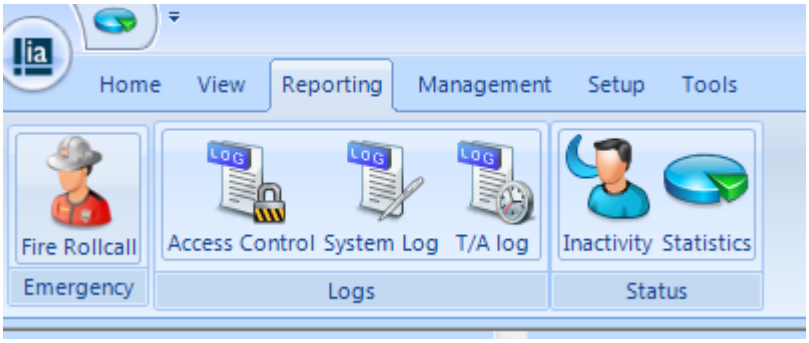
Realtime Logs: Allows the Operator to view live **Access** events, **System** events or **T/A** events in the Viewer window. ***NOTE: These buttons do the same as the side tabs in the viewer window.***

Dashboard: Allows the Operator to view a summary status of the system (see The Dashboard) 92

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:



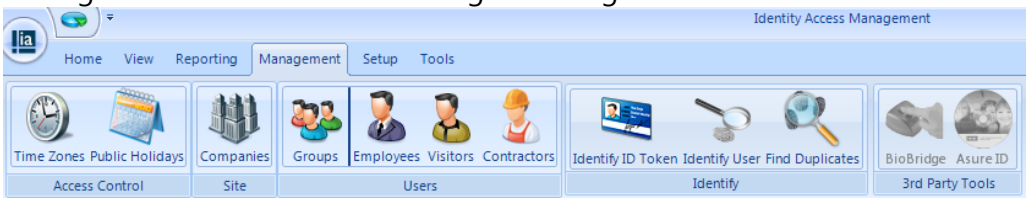
Emergency: In the event of a Fire Alarm, this icon will generate a fire roll call report, showing which users are on site. This report can be triggered from the Server or a Client machine. In addition, the server can be configured to automatically generate a Fire Roll call report when a fire alarm has been activated (see Server Configuration - Download Server 60). ***NOTE: This facility is not available in Identity Access unless a Professional Features License is applied (part number IA-PRO).***

Logs: 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 reports looking for **Inactivity** (users who have not used their tokens for a defined period) and **Statistics** (system configuration report)

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.

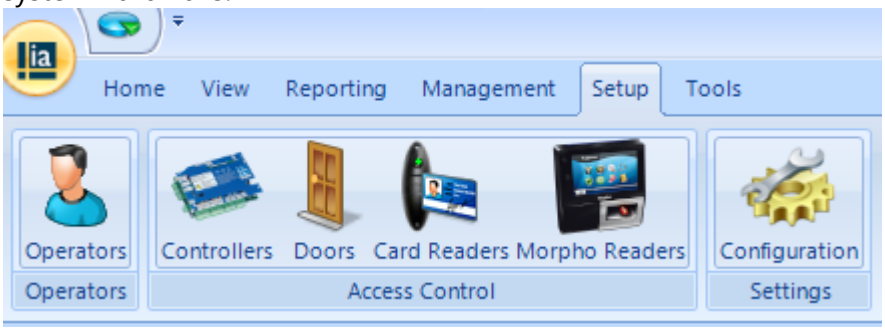
Users: Allows **Groups**, **Employees**, **Visitors** and **Contractors** to be created & edited.

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 **Biobridge** (interface to Morpho Manager software) and **Asure ID** (HID card printing software)

4.8 Identity Access Setup Tab

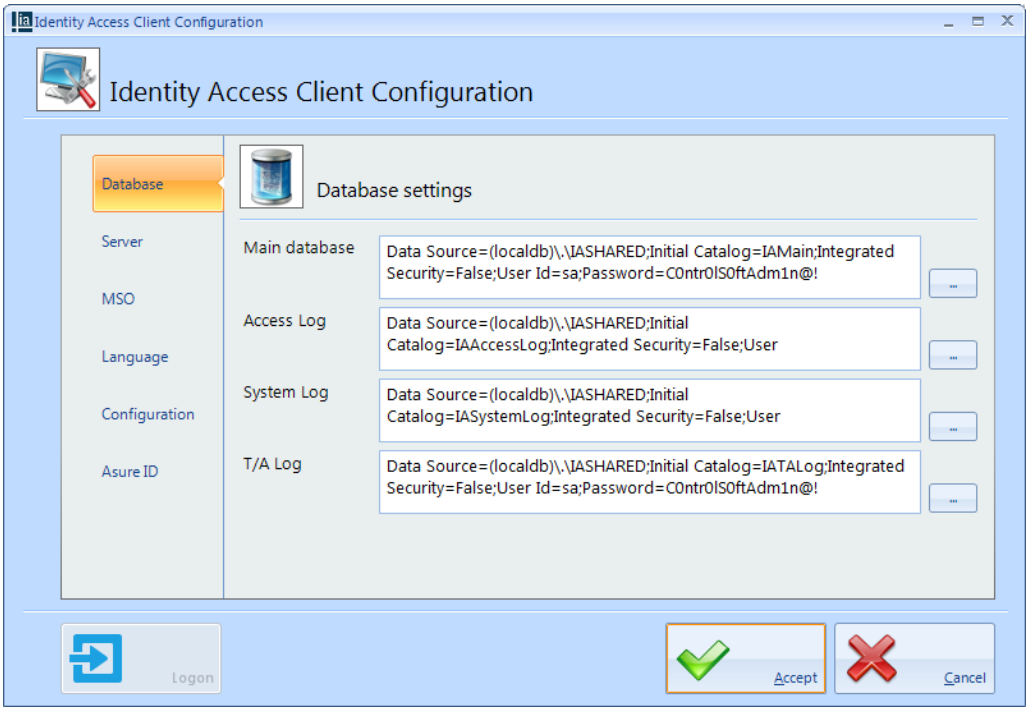
The **Setup** tab contains buttons required to commission the Access Control system hardware:



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

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

Settings: The **Configuration** option is used to launch the Identity Access Client Configuration utility:

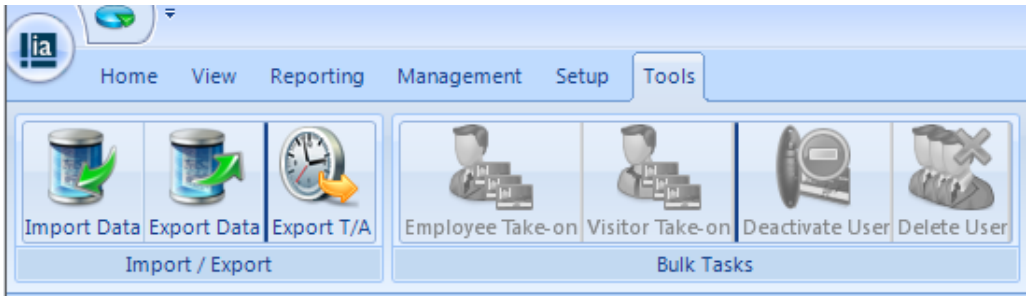


For further information on the Client Configuration utility, please refer to Identity Access Client Configuration 71

NOTE: The Setup tab is only accessible to Operators with Administrator rights. It is not accessible to Operators with Manager rights.

4.9 Identity Access Tools Tab

The **Tools** tab is used for a variety of background tasks



Import / Export: Used to **Import Data** and **Export Data** relating to the user database, and to **Export T/A** data

Configuring Operators

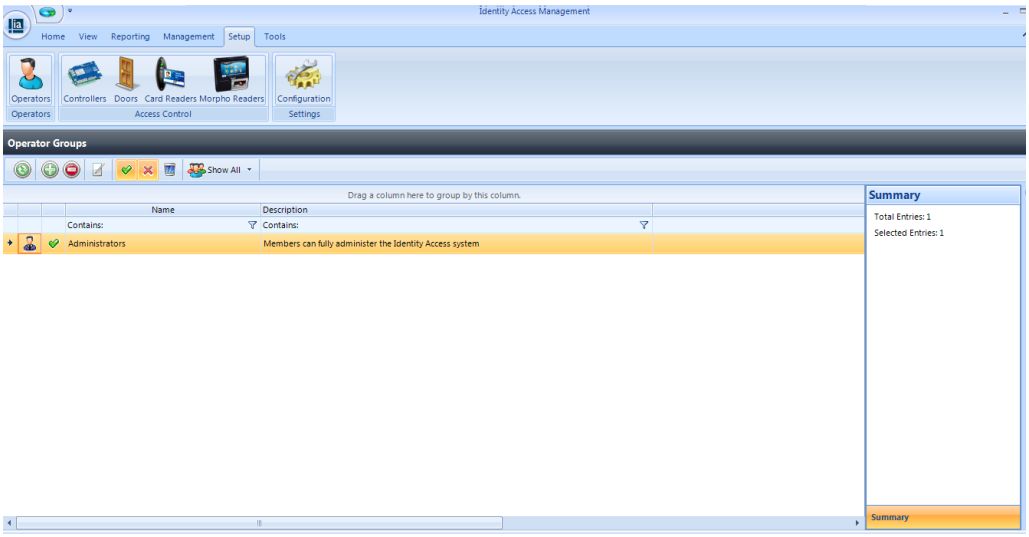
5 Configuring Operators

Operators are people who are 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.

There are 2 types of Operator, namely **Administrator** and **Manager**. Administrators have full access to the software, whereas Managers may be restricted from certain functions. Multiple operator groups can be created, each with different levels of access to the software functions.

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 forget 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. 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

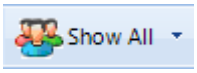
 Add: Creates a new operator group in the list

 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.

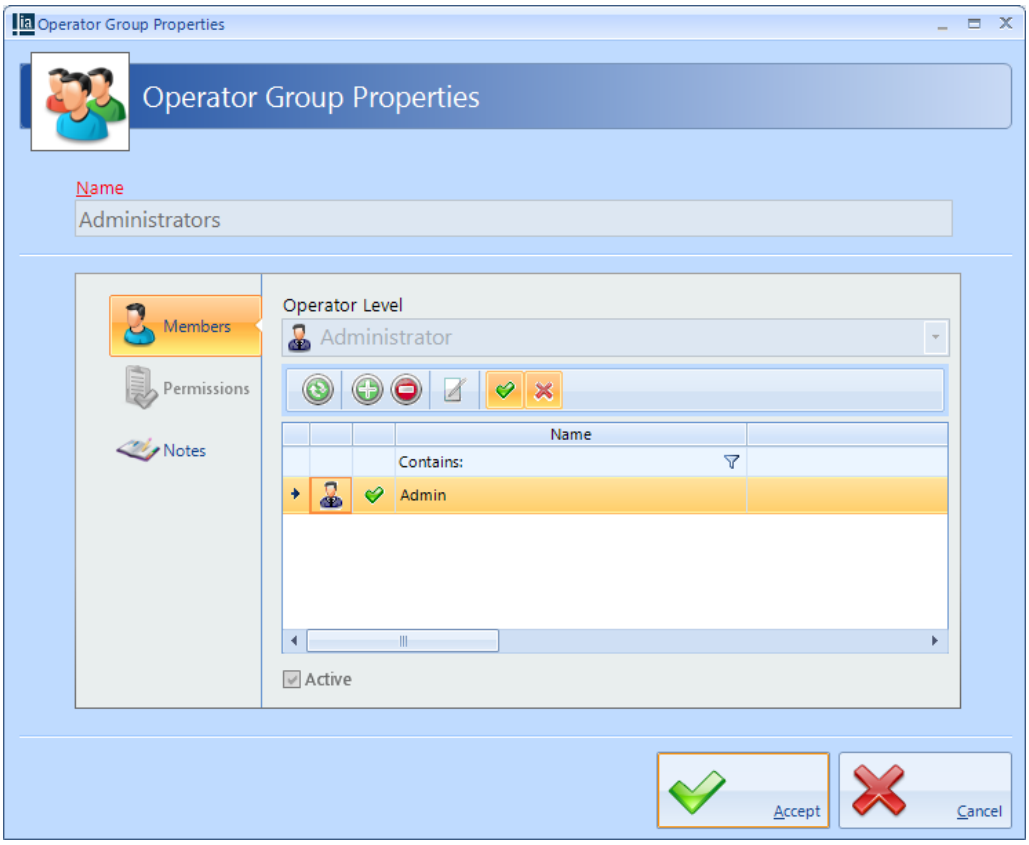


If there are many operator groups in the list, this option will either show all groups, or only Administrator groups, or only Manager Groups.

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

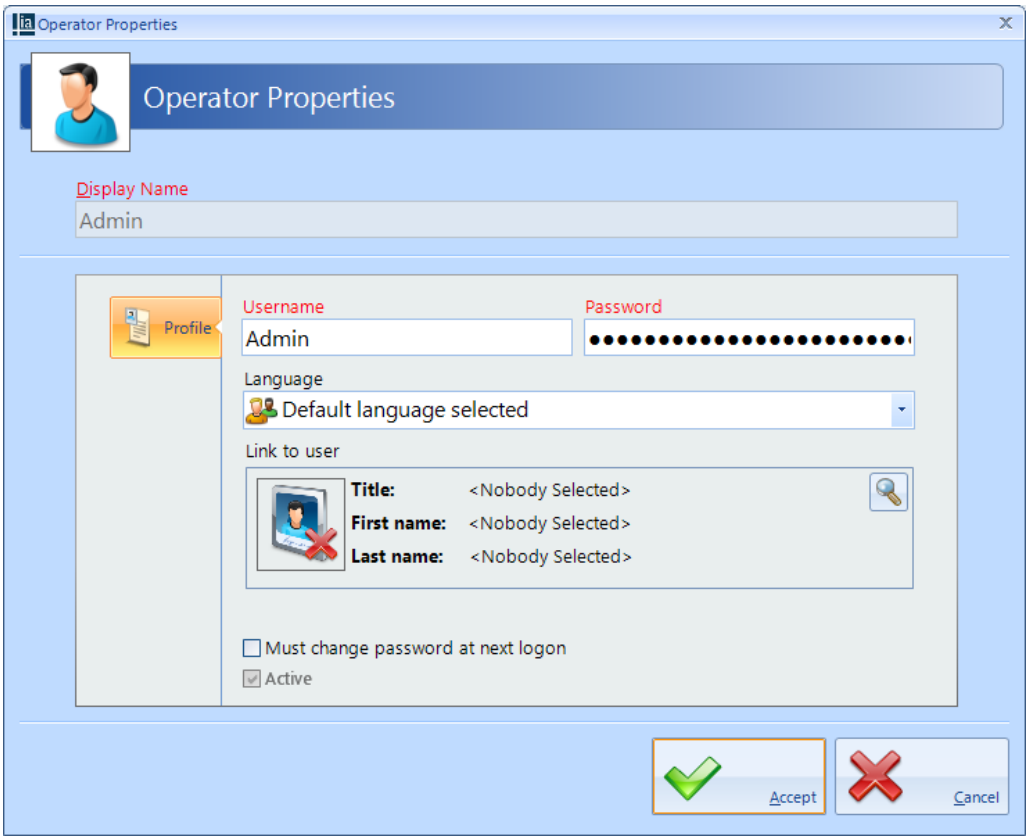
Delete: Removes the selected member/s from the list

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, click the Edit button:



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

Enter a **Username** and **Password** as required. ***NOTE: The default is Admin and Password***.

Change the **Language** if the Operator want the software in a different language ***NOTE: Each Operator can work in a different language if required***.

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.

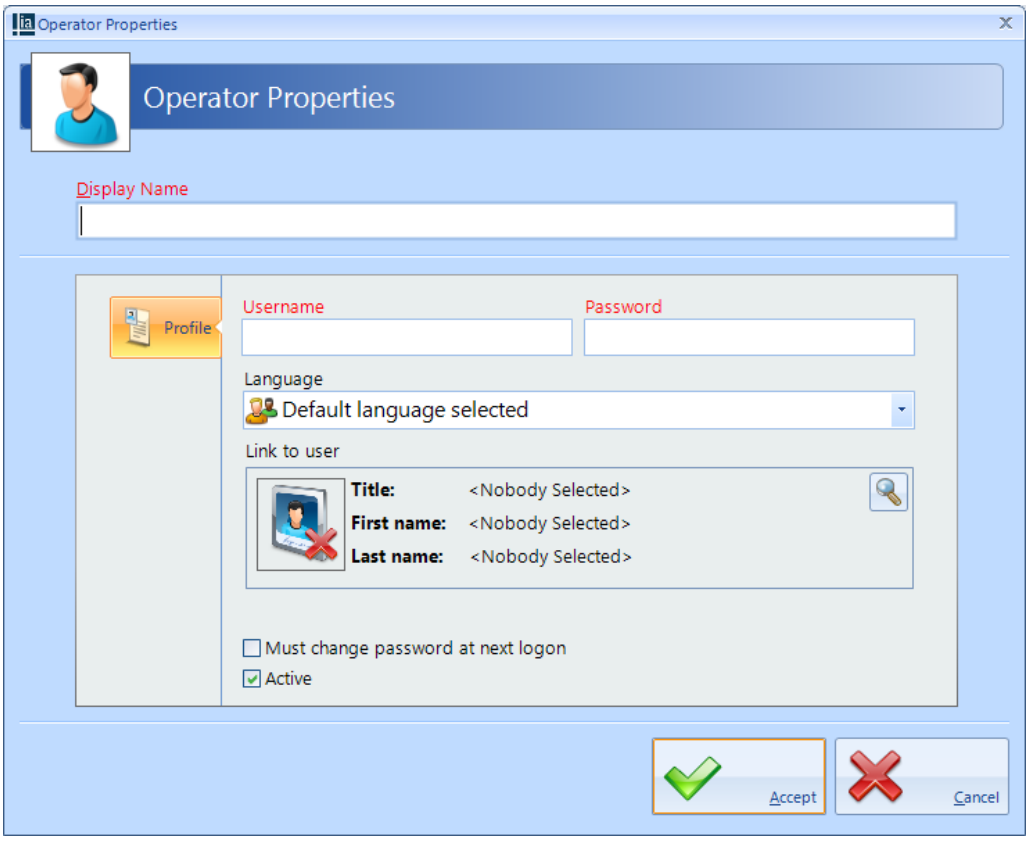
If you tick the option **Must change password at next logon** the operator will be forced to enter a new password when they next log on.

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

Click **[Accept]** when done.

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.

Change the **Language** if the Operator want the software in a different language ***NOTE: Each Operator can work in a different language if required***.

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.

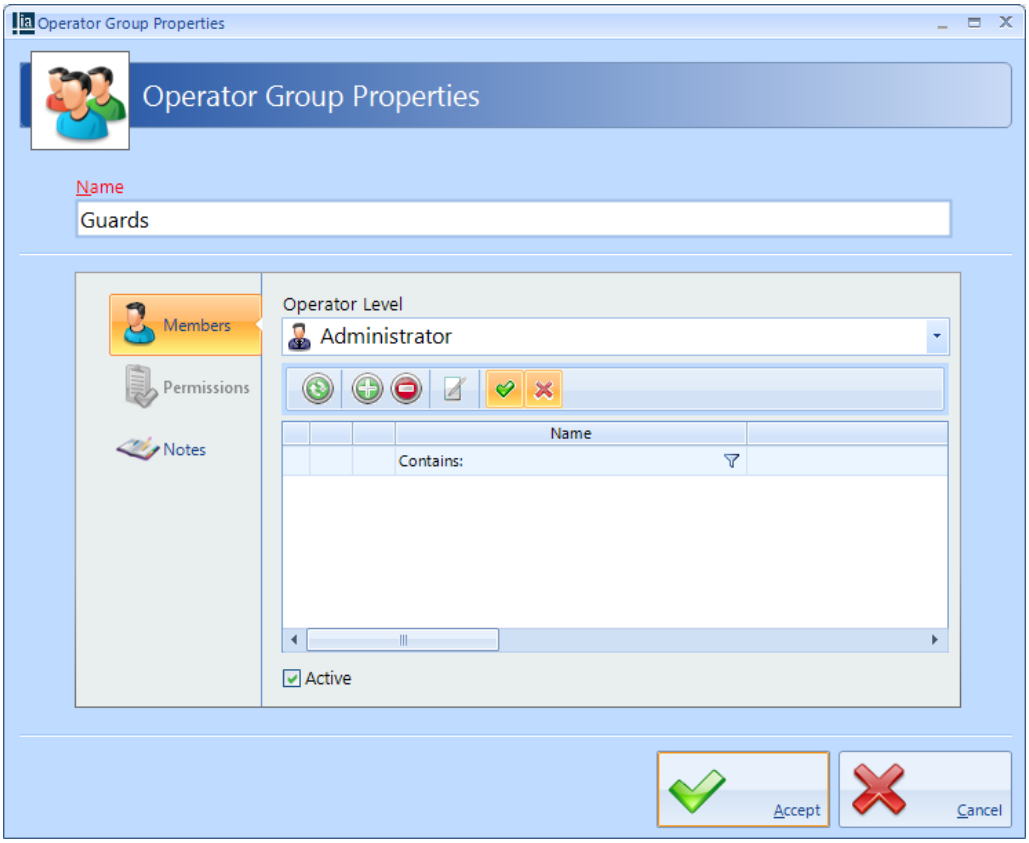
Tick the option **Must change password at next logon** to force the operator to enter a new password when they next log on.

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

Click **[Accept]** when done.

5.3 Adding an Operator

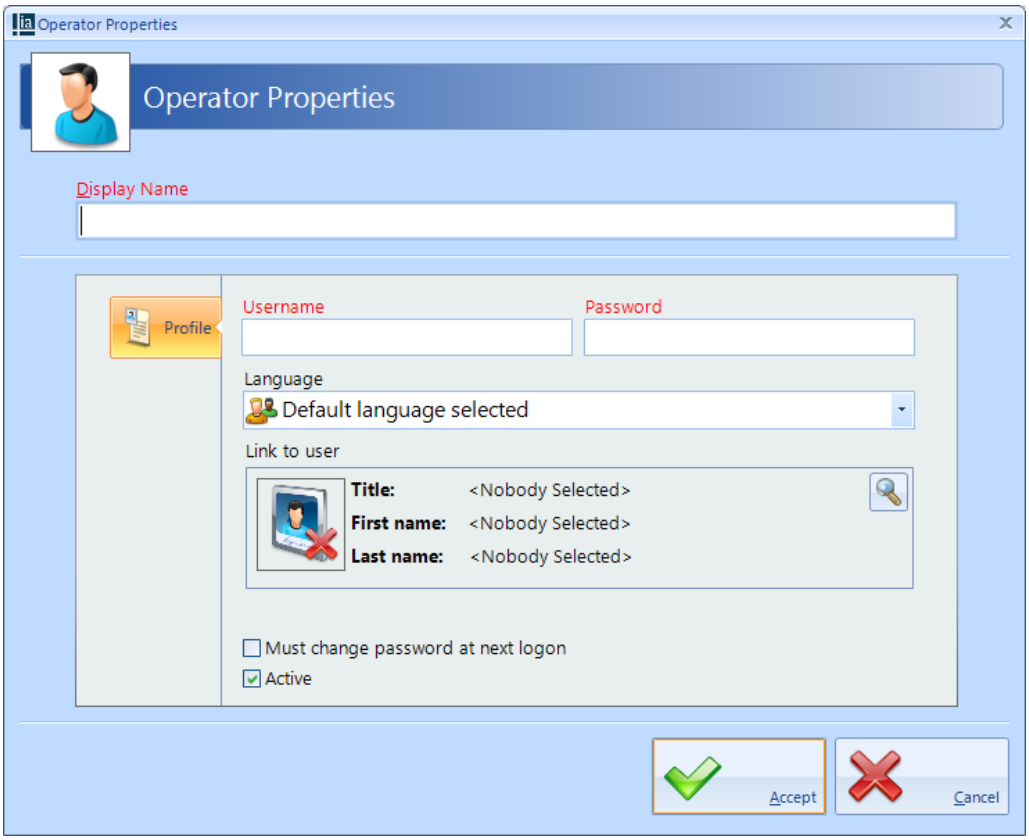
To Add a new Operator's Group to the software, click the **Add** icon in the **Operator Groups** window to display the **Operator Group Properties**:



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

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

Click the Add icon  to add a new member within the group:



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

Enter a **Username** and **Password** as required.

Change the **Language** if the Operator want the software in a different language ***NOTE: Each Operator can work in a different language if required***.

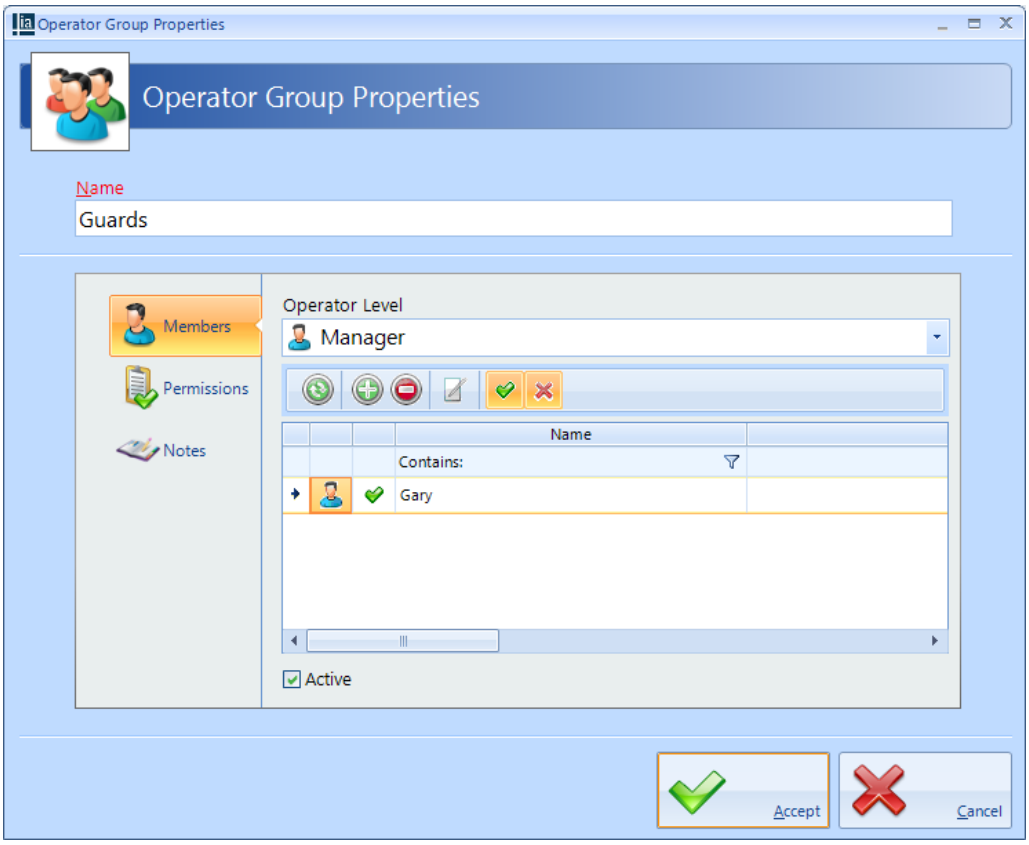
If the Operator is also a User, it is possible to use their fingerprint to log onto the Identity Access software. To link the Operator to a User, click on the magnifying glass under **Link to user** and select the User from the list which appears.

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

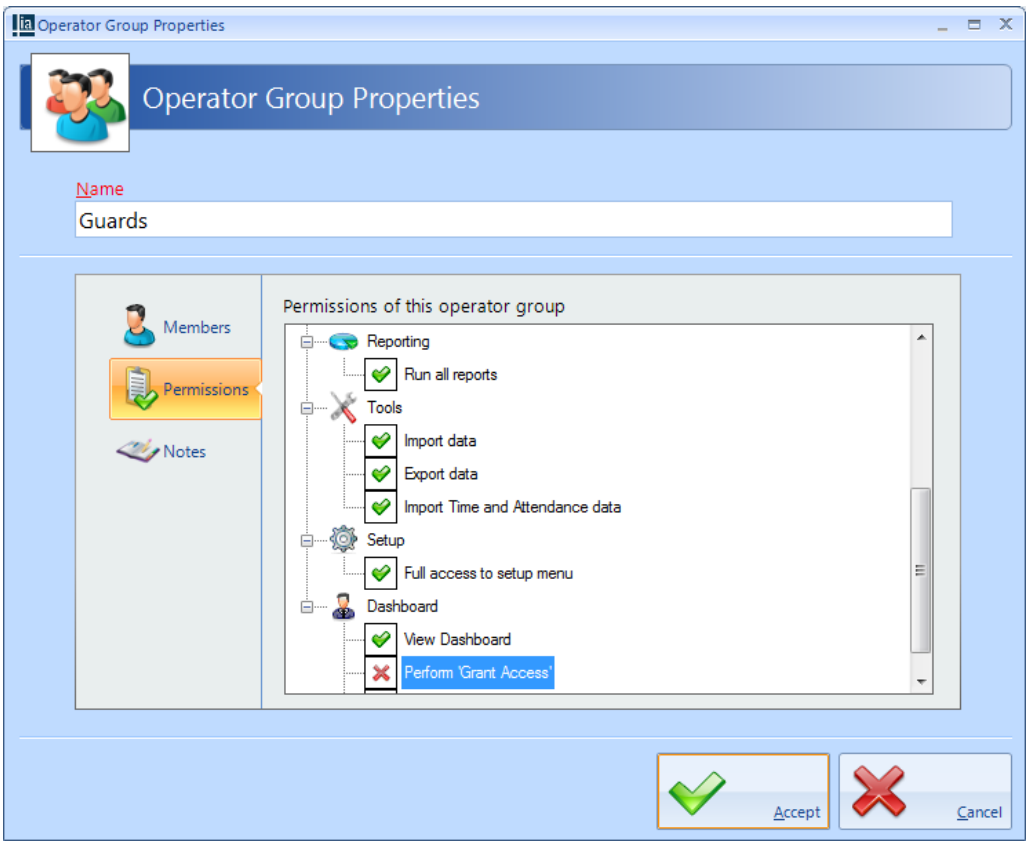
Tick the option **Active** to make the operator active.

Click **[Accept]** when done.

if the Group's Operator Level has been selected as Manager, set the functions permissible for members of that group:



Selecting the Permissions tab:



Changing a green tick for any function shown to a red cross will disable that function.

For example, to prevent members of this Operator Group from Granting Access through doors via the dashboard, scroll to the relevant option and double click the green tick (function enabled) to change it to a red cross (function disabled) as shown above.

NOTE: Operators configured as Manager do not have access to the Setup tab.

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:

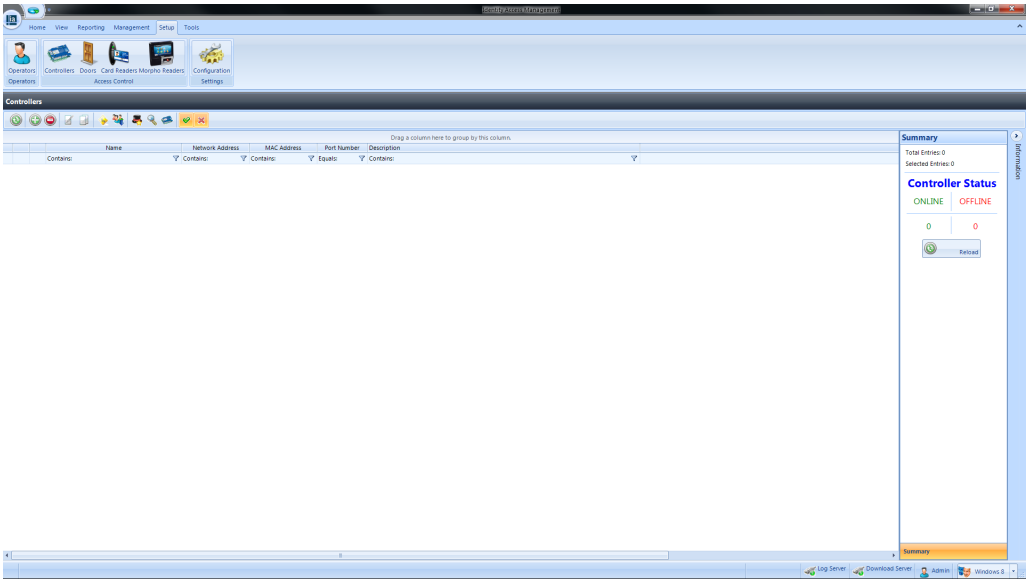
1. Configure the Master Controllers (Installer function)
2. Configure the Doors and link them to the relevant Master Controllers (Installer function)
3. Configure the Readers and link them to the relevant Doors (Installer function)
4. Configure Time Zones and link them to the relevant Master Controllers (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.



The 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 118).

 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 i-Nets in that IP range (see Find IP Controller Wizard 115).

 Configure: This feature allows the controller's internal webpage to be configured, as per i-Net Configurator. (see IP Controller Configurator 116)

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

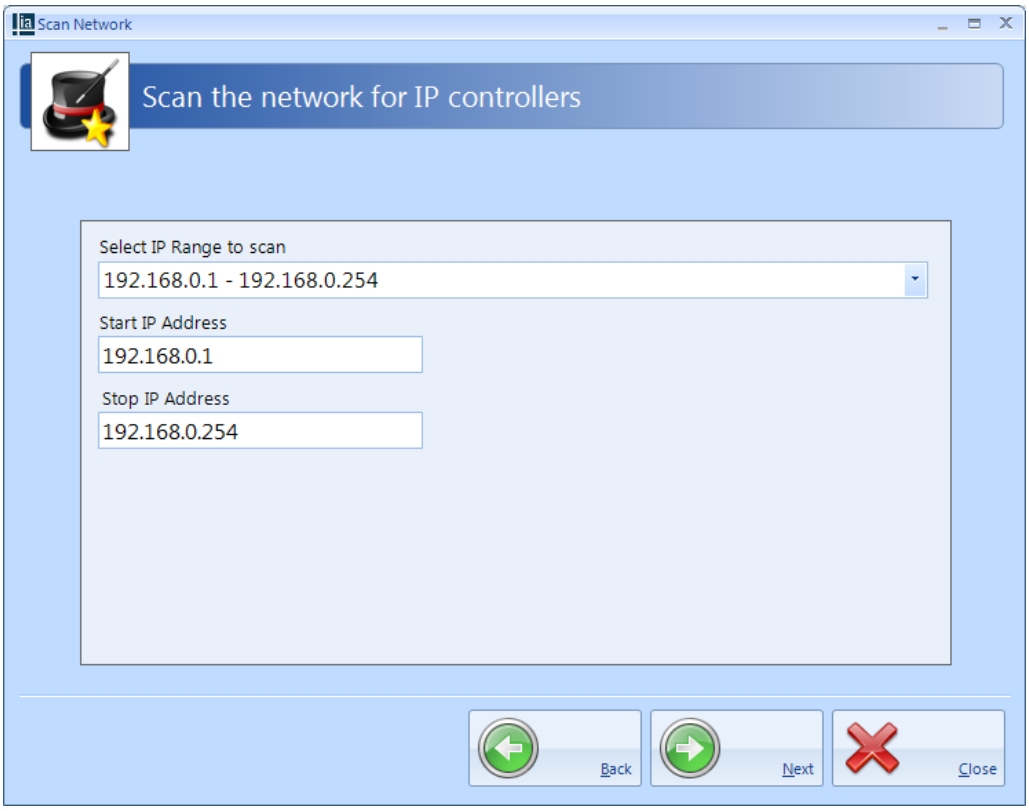
 Show/Hide Inactive: This button will show or hide Controllers not selected as Active.

Click on the **Add** button  to create a new Master Controller and display the **Controller Properties** window

NOTE: When the controller is fully configured, confirm that it is communicating with the Log Server and Download Server

7.1 Find IP Controller Wizard

Firstly, select the Start IP Address and Stop IP Address to define the range to be scanned:



The software will then find all controllers in that range. When the scan is complete, devices that are not i-Nets will be hidden from view:

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. The right hand side will show the **Controller Status** for the new controller/s as **OFFLINE**. Click the **[Reload]** button and their status will change to **ONLINE**.

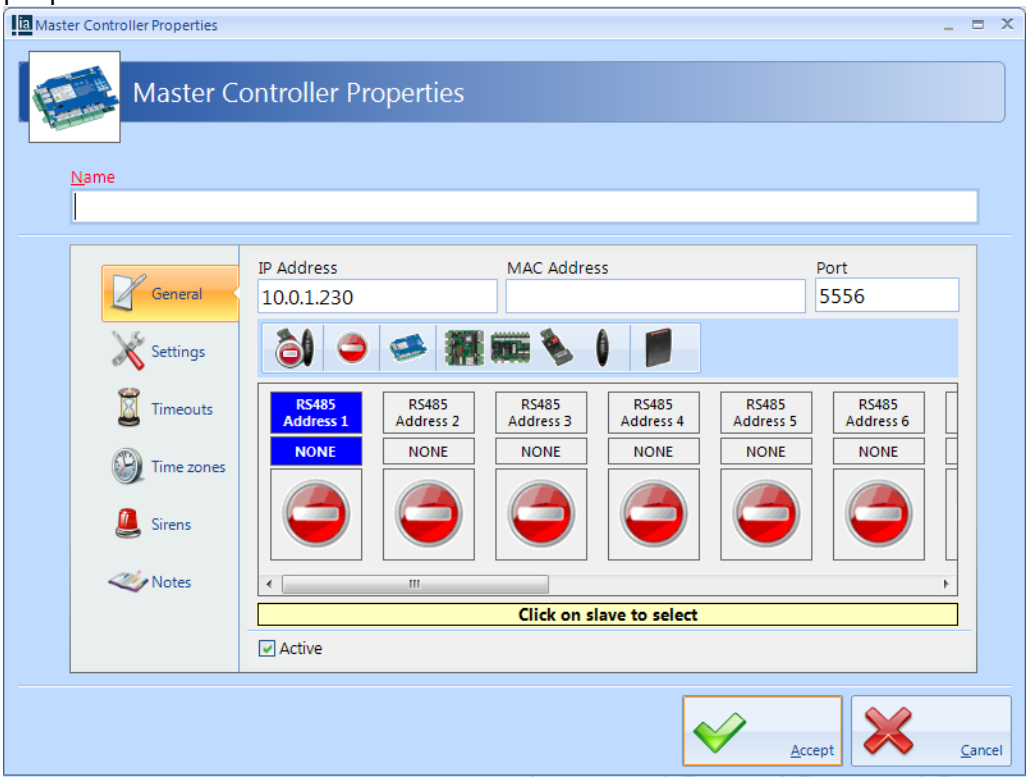
7.2 IP Controller Configurator

The IP Controller Configurator feature allows the the internal configuration options of an i-Net Master Controller to be configured. The operation of this feature is similar to the i-Net Configurator program available from the Controlsoft website.

7.3 Controller General

The **General** tab in the **Controller Properties** window displays the basic

properties of the Master Controller



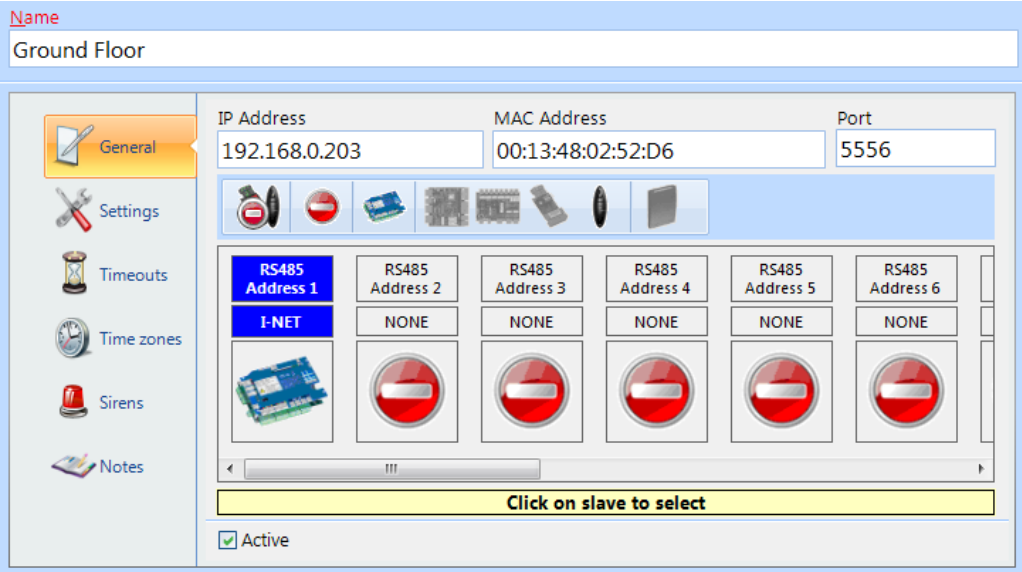
Enter a **Name** to identify the controller (e.g. Ground Floor)

Enter the **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 all i-Nets start with 00:13:48***

The **Port** is preset to 5556. ***NOTE: THIS VALUE MUST NOT BE CHANGED***.

It is then possible to define the type of expansion used on that Master Controller. For example, to add a slave i-Net which has Address 1 on the RS485 bus, highlight **RS485 Address 1** then click on the image of the i-Net.



This information will then be used during the programming to define which inputs, outputs etc. are available for use. ***NOTE: Slave i-Nets and expanders cannot be combined on a single RS485 bus. Selecting a Slave i-Net greys out other expanders (and visa versa) reducing the possibility of configuration errors.***

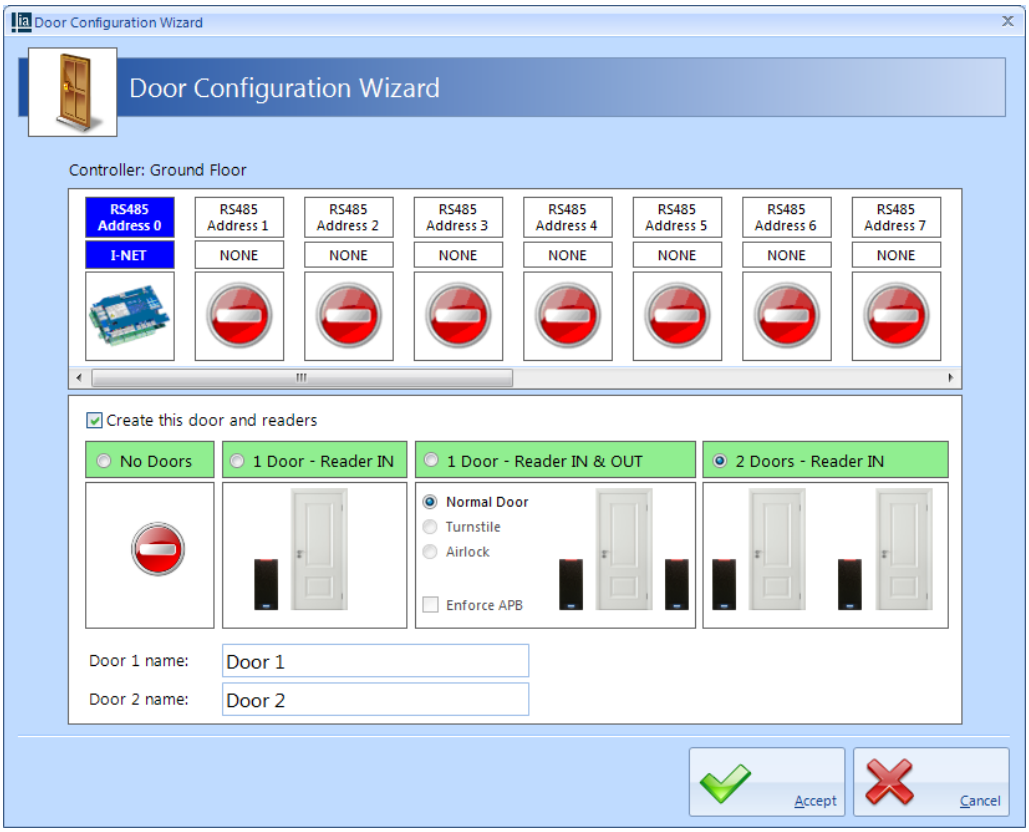
When the **Active** box is ticked, data for that channel will be sent to the hardware during a Full Download.

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

Having configured the Master Controller, activate the Door Configuration Wizard by selecting the Door Configuration Wizard icon  .



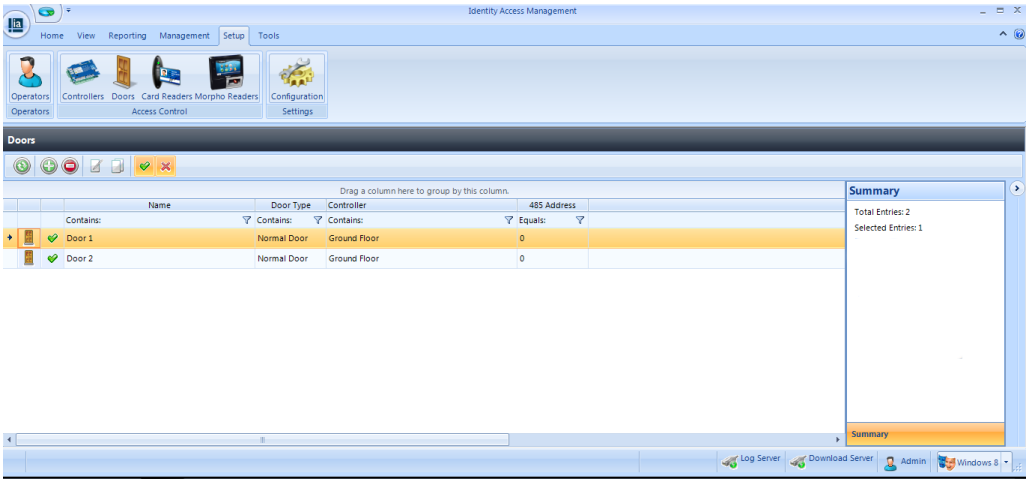
Ensure that the option **Create this door and readers** is ticked.

Select the 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).

NOTE: **Turnstile**, **Airlock** and **Enforce APB** are greyed out in this example as these options are only available in Identity Access Professional Edition. For further information on AntiPassBack (APB), please refer to Appendix E - AntiPassBack 228

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:



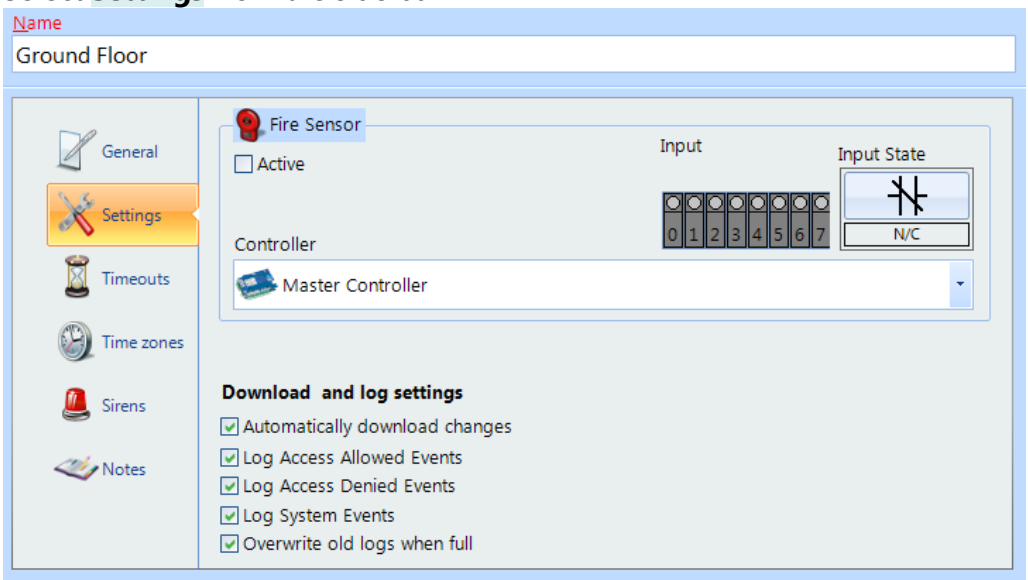
As can be seen, the Master Controller called "Ground Floor" now has 2 doors called "Door 1" and "Door 2". These names can be changed if required by editing the door properties (see Door Properties General 128)

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

NOTE: Identity Access supports a maximum of 24 doors and 24 readers unless a Professional Features License is installed (Part Number IA-PRO), when the system then supports an unlimited number.

7.5 Controller Settings

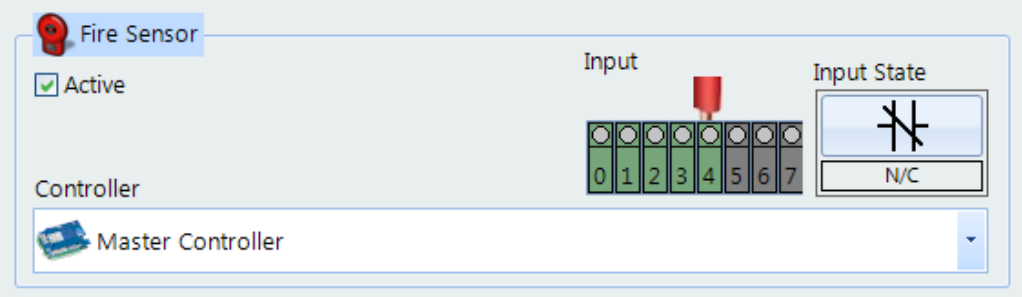
Select **Settings** from the side bar



If doors on this channel are to be released during a fire alarm, tick the **Active** box under **Fire Sensor**, 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)

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



If **Automatically download changes** is ticked, any changes made to this channel will be sent to the hardware, without requiring a Rebuild command

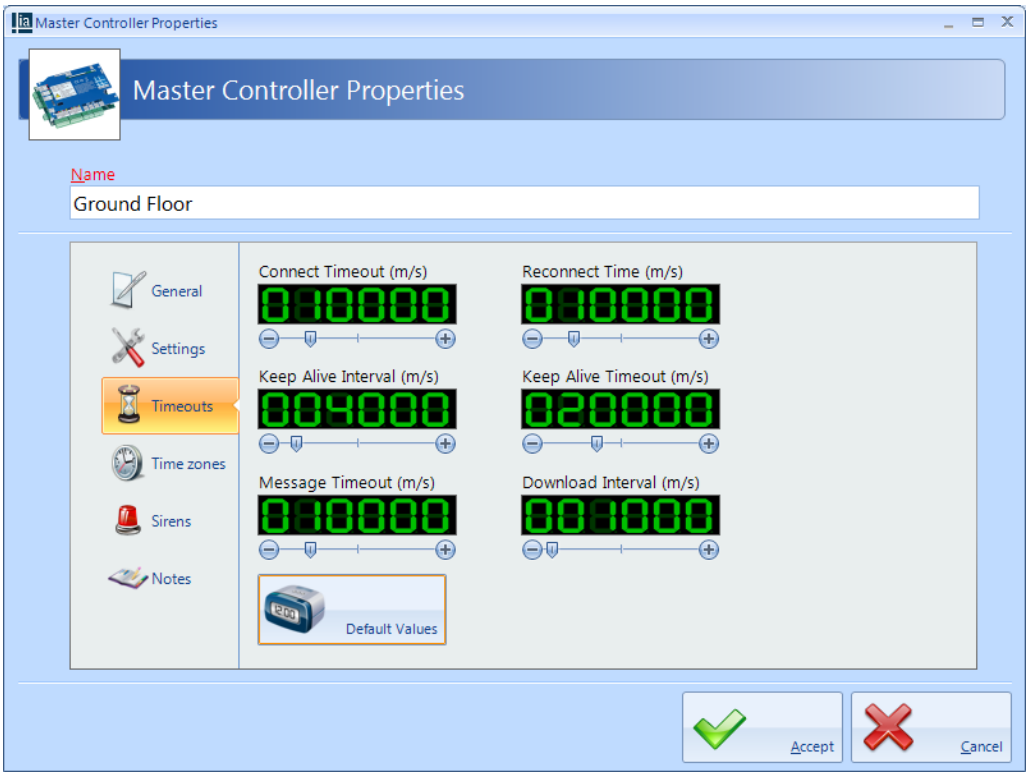
Log Access Allowed Events, **Log Access Denied Events** and **Log System Events** define which events are logged in the Master Controller's Offline Event Log (i.e. when it is unable to communicate with the Download Server software).

When the **Overwrite old logs when full** option is ticked, the controller will lose the oldest events when its Offline Event Log is full. When un-ticked, the controller will stop recording new events when the Offline Event Log is full.

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.

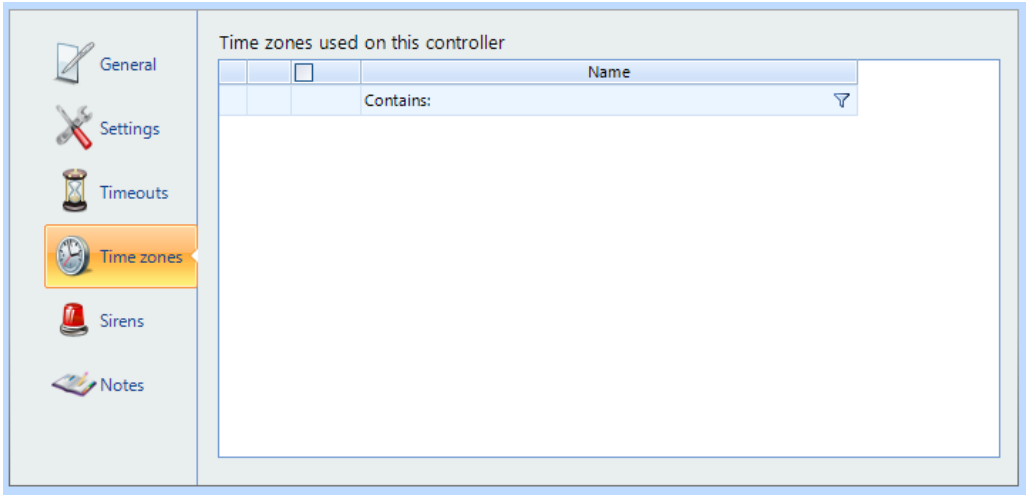


NOTE: All the timers in this window are in milliseconds.

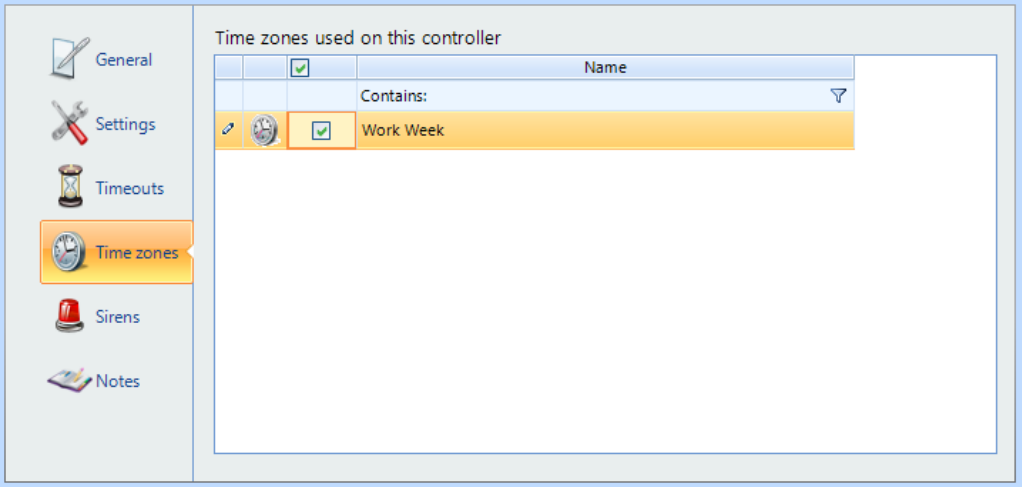
If changes are inadvertently made, use the **[Default Values]** button to restore all timers to their correct values.

7.7 Controller Time Zones

Selecting one or more Time Zones in the the **Time Zones** tab in the side bar defines which Time Zones are applicable to the controller.

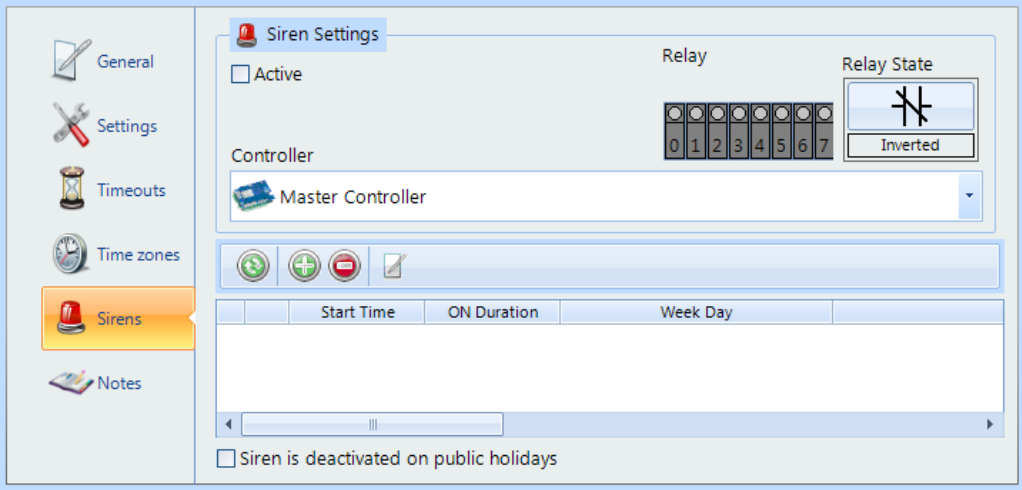


In this instance, Time Zones have not yet been created. When one or more Time Zones exist, these can be selected as required for each controller:



7.8 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:



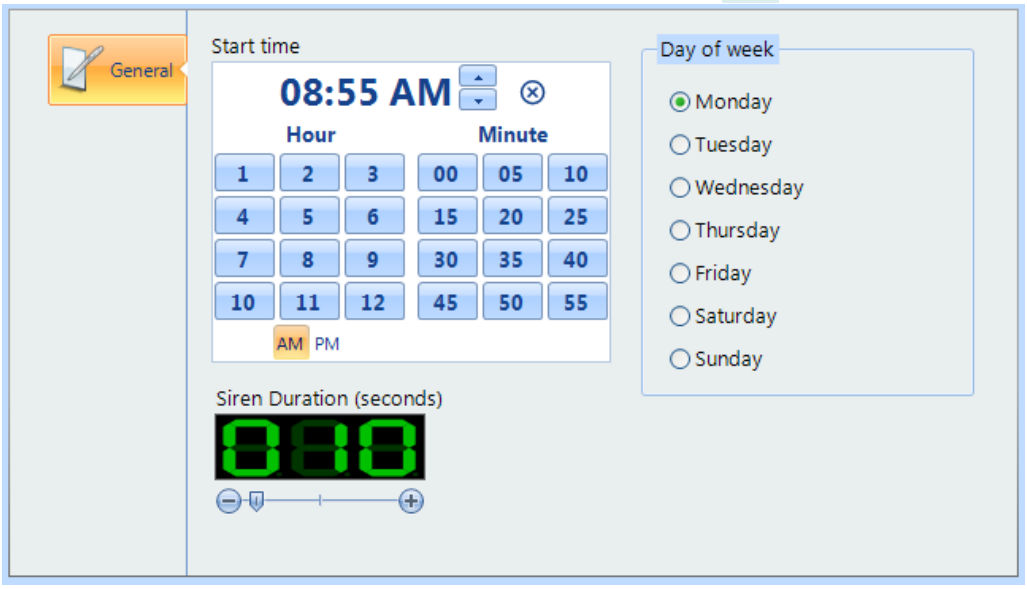
Tick the **Active** box under **Siren Settings** to enable the function.

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).

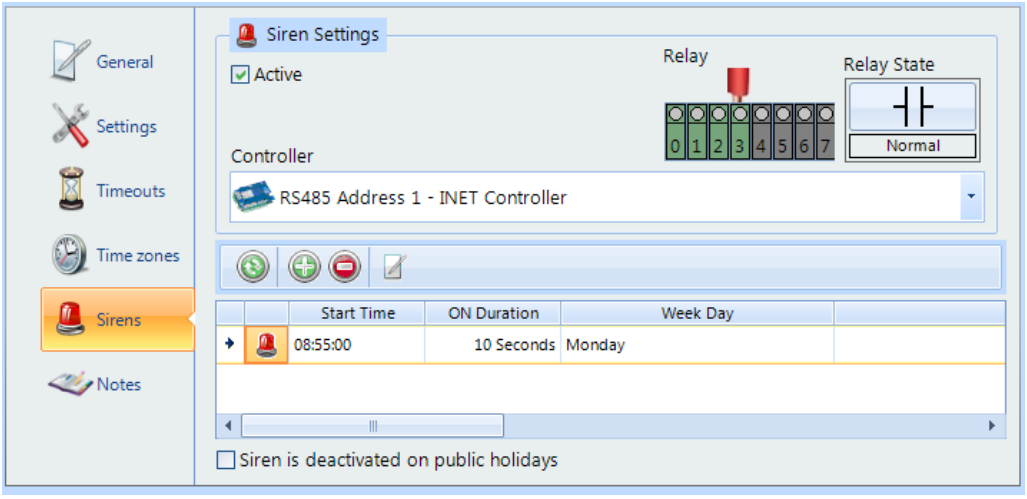
Relay State defines whether the selected relay will be Normal (energises to sound the siren) or Inverted (de-energises to sound the siren)

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



Select the **Start time** using the 12 **Hour** and 12 **Minute** buttons, or the up and down arrows. Set the **Siren Duration** and **Day of the week** as required (e.g. 8:55am for 10 seconds on Mondays).

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

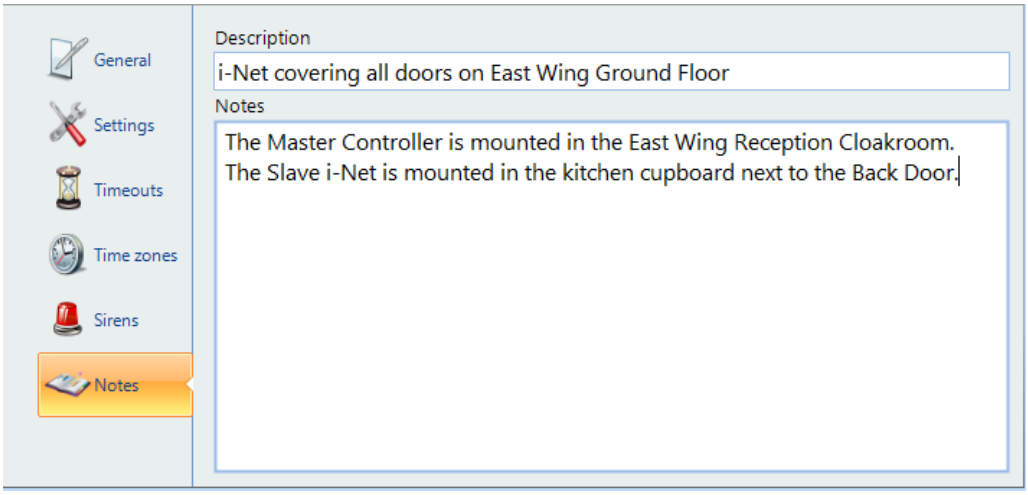


Finally, tick the box **Siren is deactivated on public holidays** if the siren is not to sound on certain days.

7.9 Controller Notes

The Notes section, accessed from the side bar, provides 2 text fields called

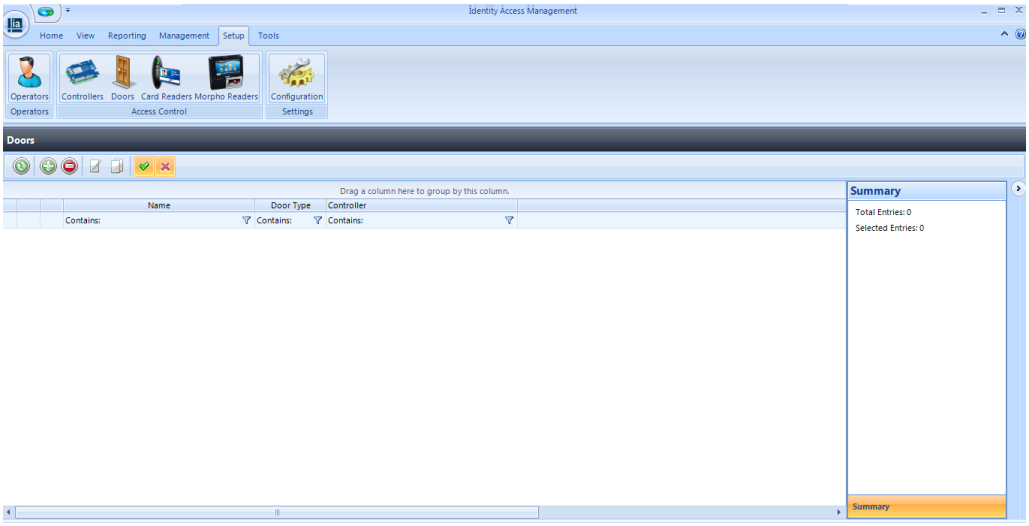
Description and **Notes** to help a Service Engineer during their first visit.



Configuring Doors

8 Configuring Doors

Doors can be configured using the **Door Configuration Wizard** (see Door Configuration Wizard 118), 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.

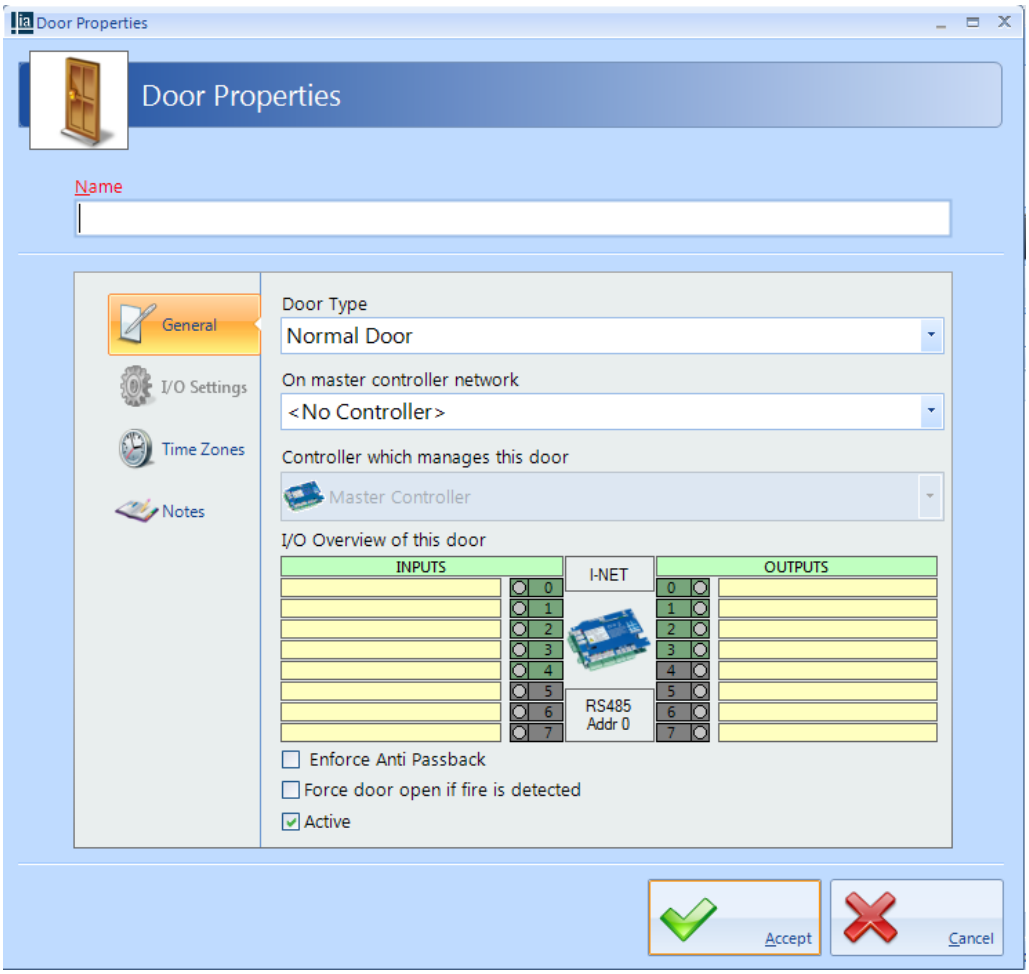
 Show/Hide Inactive: This button will show or hide Doors not selected as Active.

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

NOTE: Identity Access supports a maximum of 24 doors unless a Professional Features License is installed (Part Number IA-PRO), when the system then supports an unlimited number.

8.1 Door Properties General

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



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

Enter the **Door Type** selectable between Normal, Turnstile and Airlock. For more information on Door Types, please refer to Appendix A - Types of Door 209 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. RS485 Address 1).

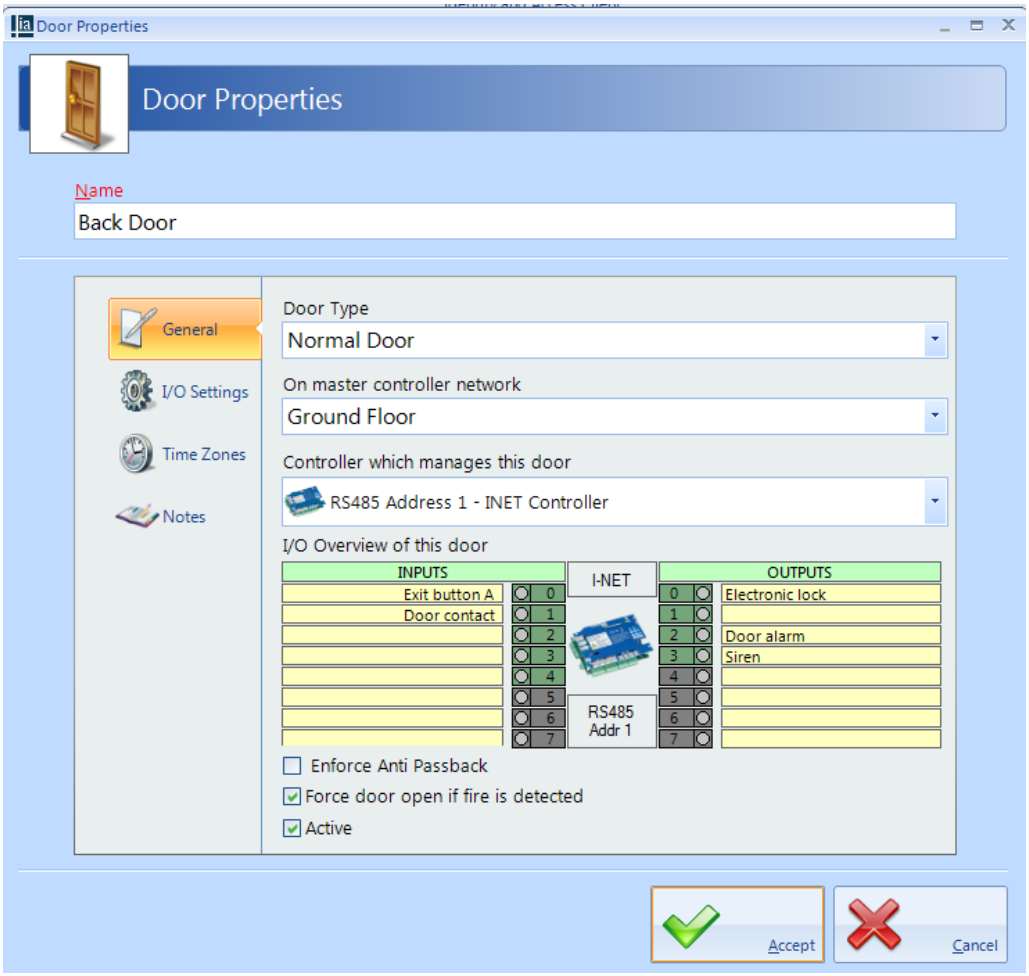
The **I/O Overview** of this door gives a quick overview of the inputs and outputs used for the door (not yet configured in this screenshot)

Select the **Enforce Anti Passback** 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**

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.

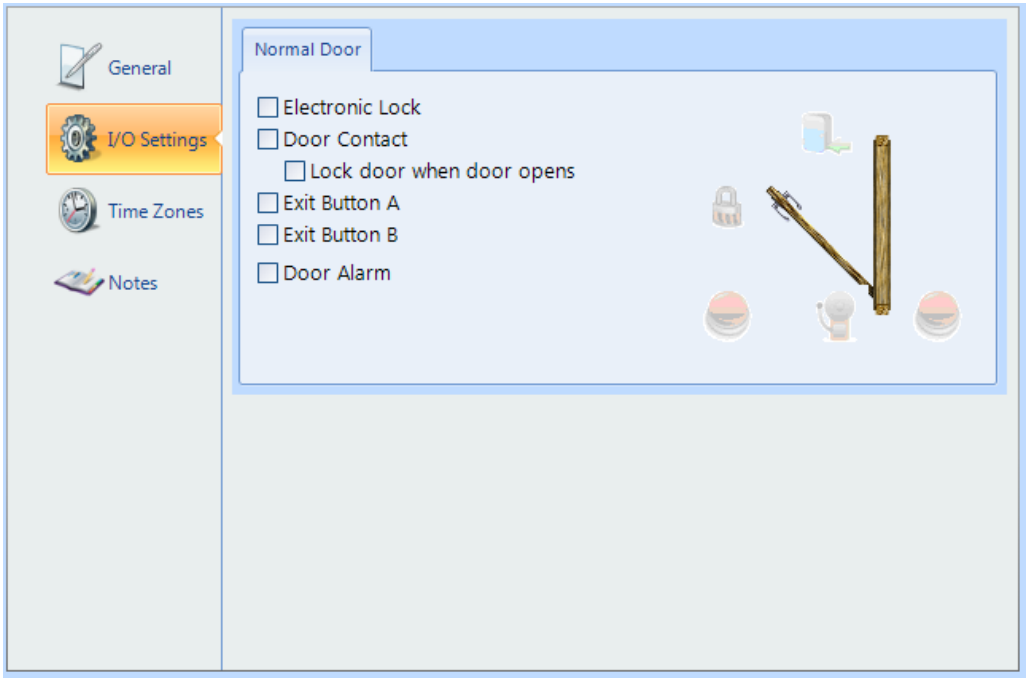
When the door is fully configured, the **General** tab should look something like this:



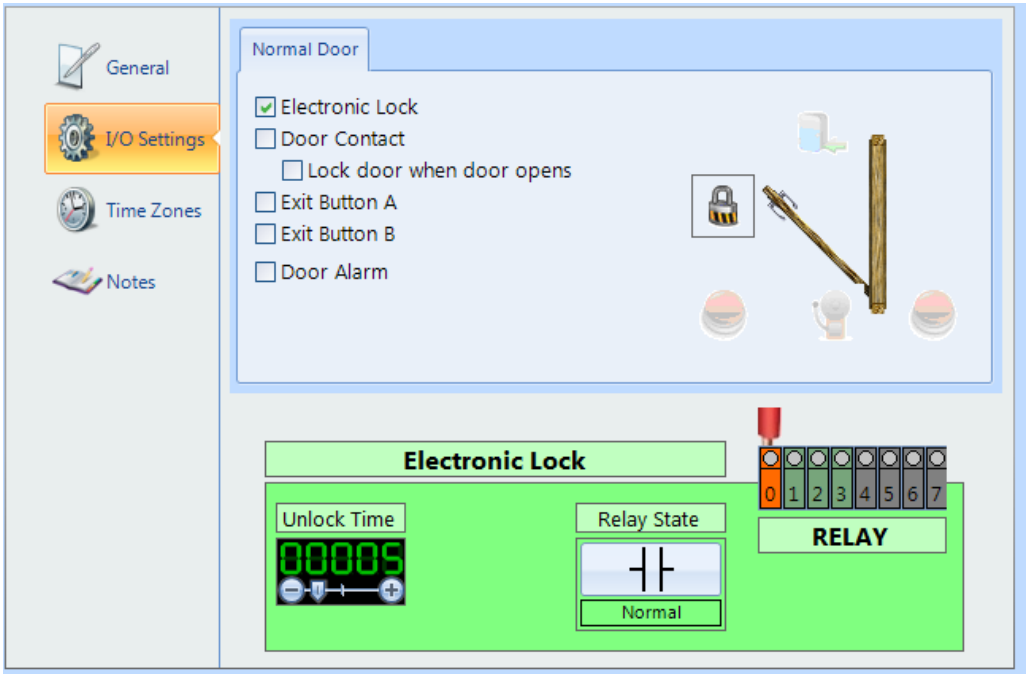
Press the **[Accept]** button when done.

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:



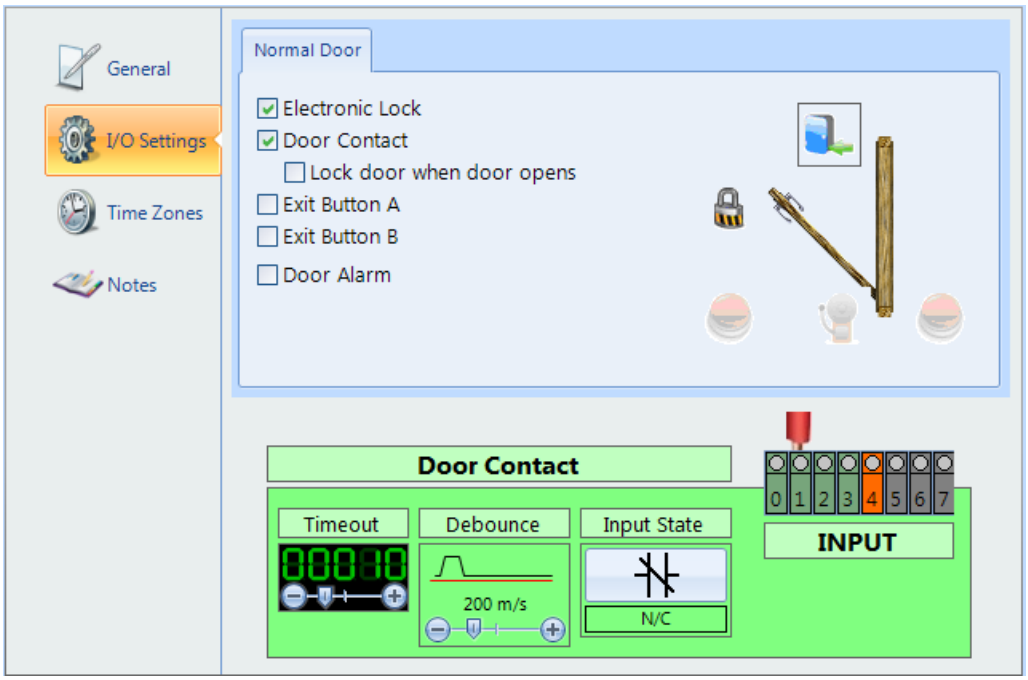
The **Unlock Time** is the duration that the door will remain unlocked, in this instance 5 seconds.

If **Relay State** is **Normal**, the relay will energise to release the door. Conversely, **Inverted** 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 as shown above.

NOTE: When used with i-Net 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:



Timeout is the duration that the door is left open before generating a Door Held alarm (10 seconds in this instance).

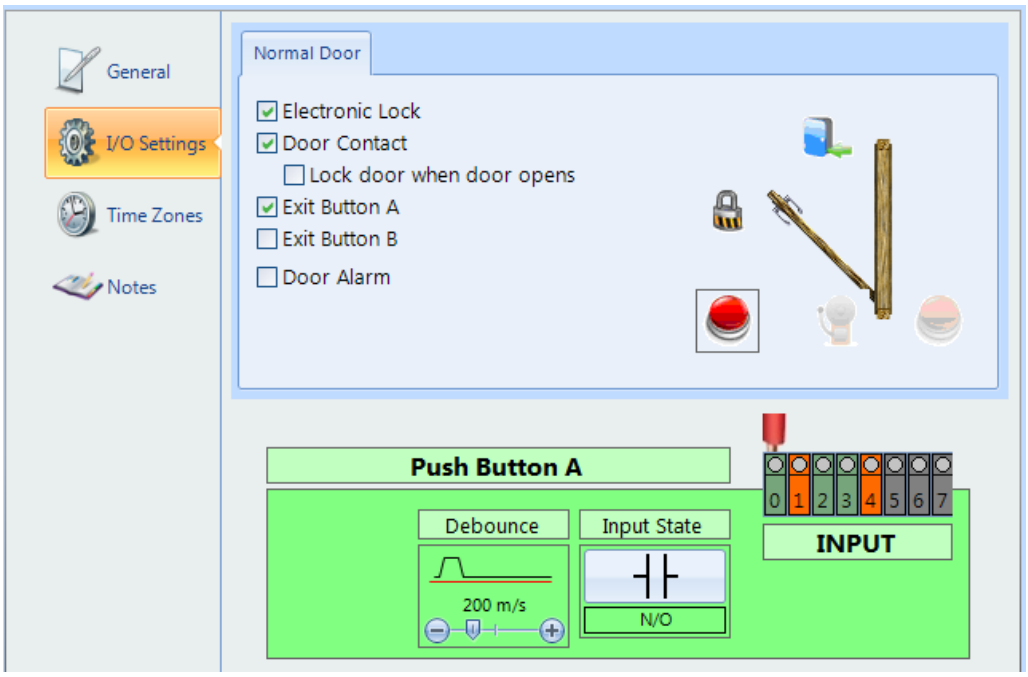
NOTE: If the* Lock door when door opens *option is selected, the door is re-locked as soon as the door opens, overriding any remaining Unlock Time

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 device, the graphic will show orange as shown above

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



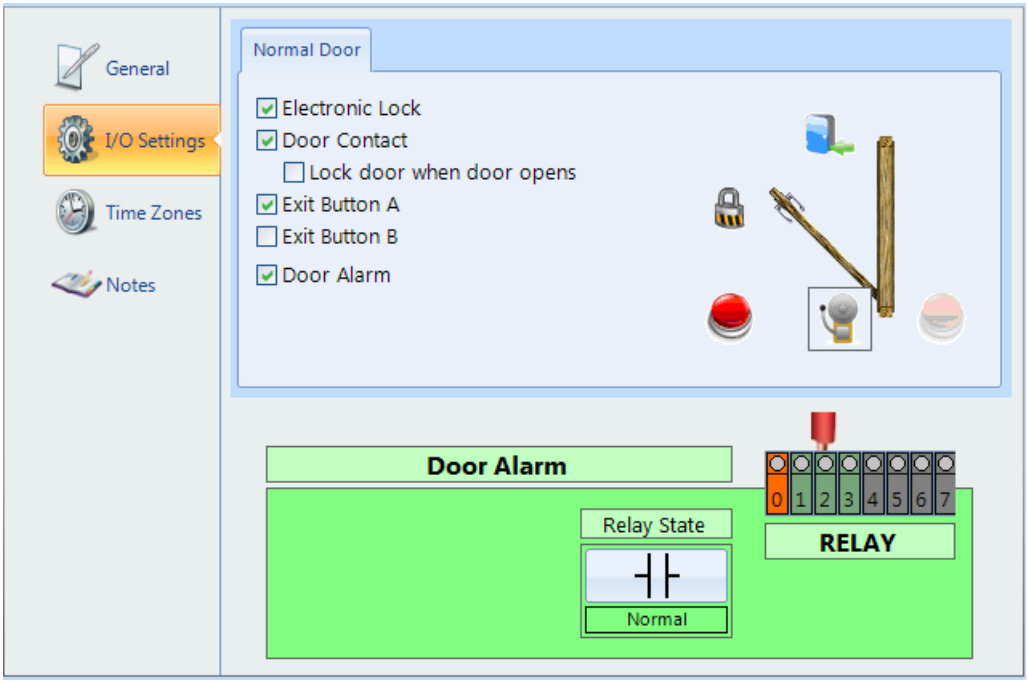
Debounce is a short delay between the door contact opening and the system processing the information. The default for this delay is 200 milliseconds, which should be suitable for all but the noisiest of environments.

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 device, the graphic will show as orange as shown above

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:

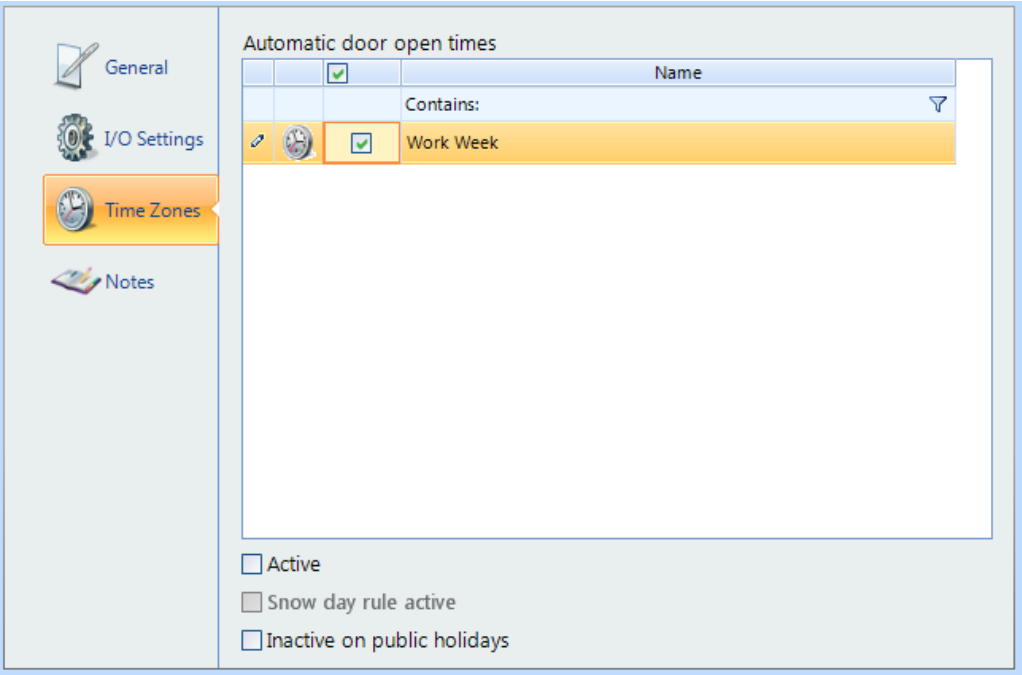


If **Relay State** is **Normal**, the relay will energise to activate the sounder. Conversely, **Inverted** will de-energise the relay to activate the sounder.

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

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.

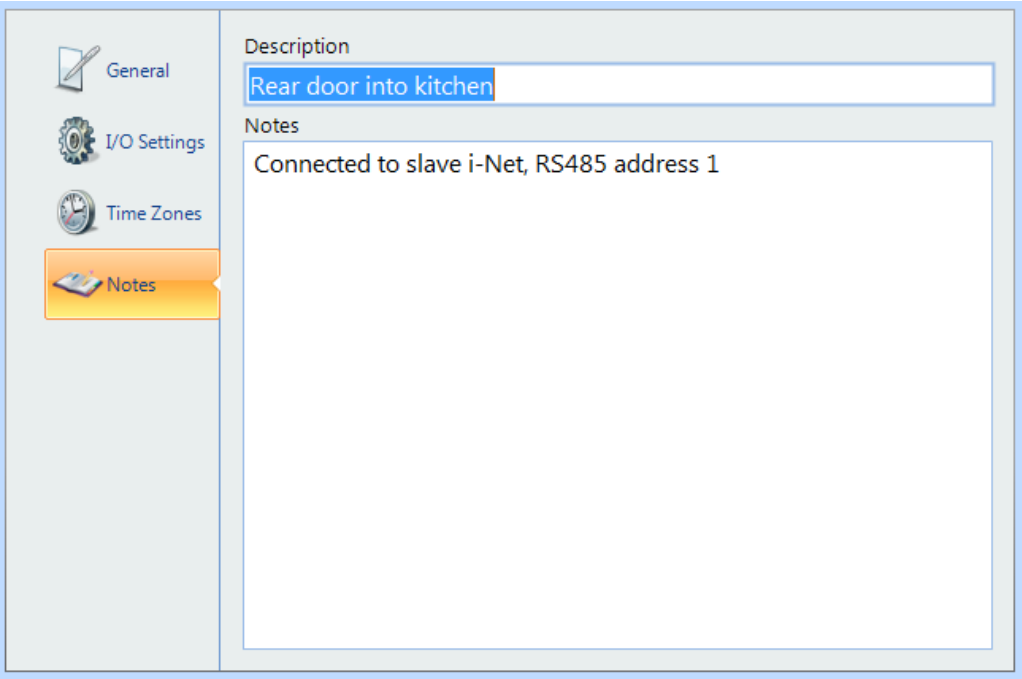


When a Time Zone is allocated to a door, the door will remain unlocked for the duration of that Time Zone.

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

8.4 Door Properties Notes

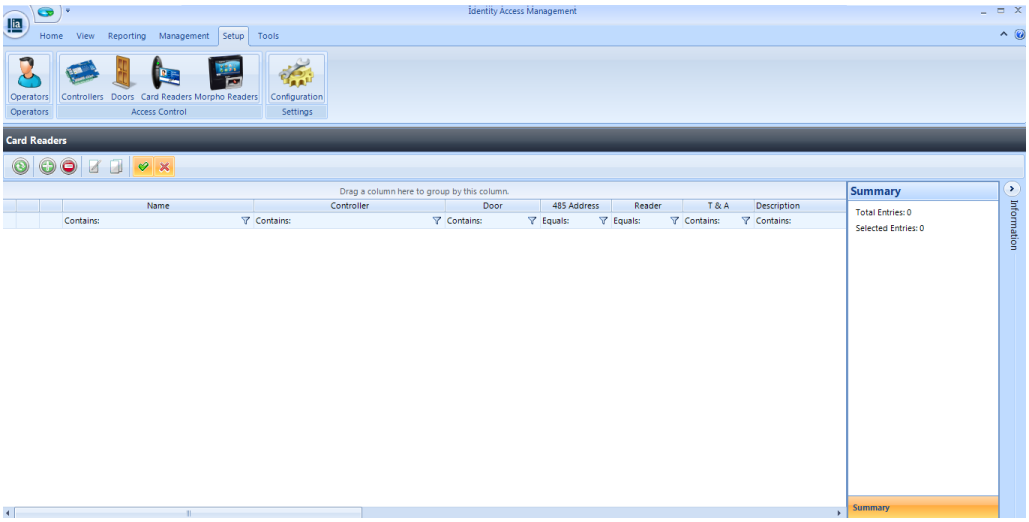
The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.



Configuring Card Readers

9 Configuring Card Readers

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



The 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.

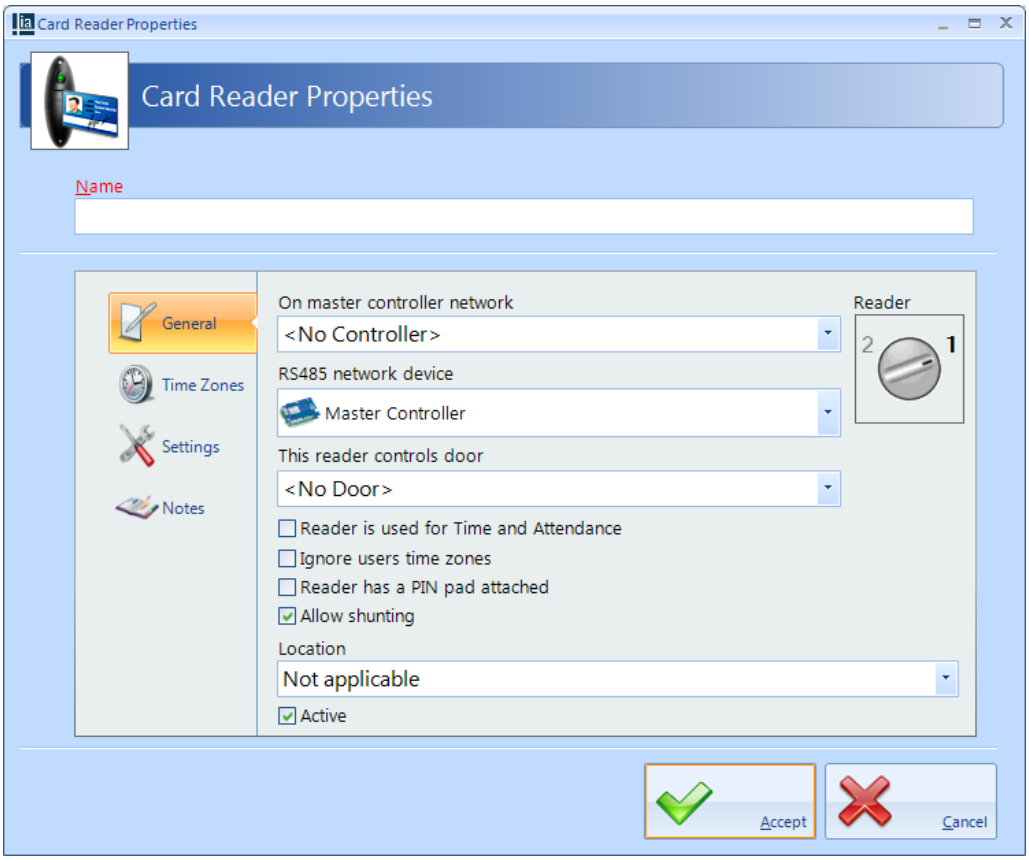
To create a new reader, click on the Add button 

When the reader is fully configured, click the **[Accept]** button.

NOTE: Identity Access supports a maximum of 24 readers unless a Professional Features License is installed (Part Number IA-PRO), when the system then supports an unlimited number.

9.1 Card Reader General

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



Enter a **Name** for the reader

On master controller network defines which channel the reader is connected to

RS485 network device is the device that the reader is connected to

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

This reader controls door defines the door which will release when the reader is used

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.

Ignore users time zones should be ticked for OUT readers to ensure that employees can exit 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.

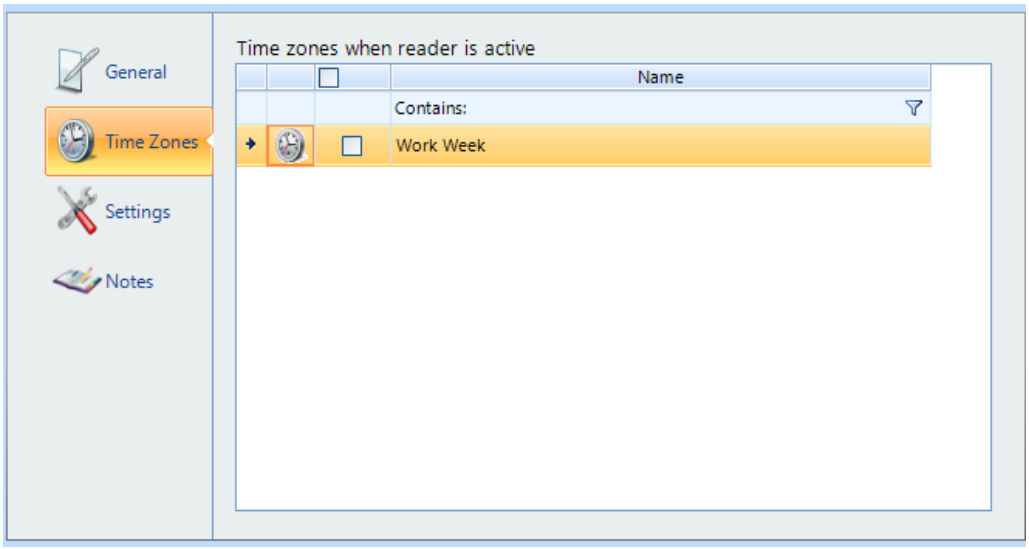
Allow shunting speeds up the operation of the reader by not having to wait for the door to close before the reader can be used a second time.

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.

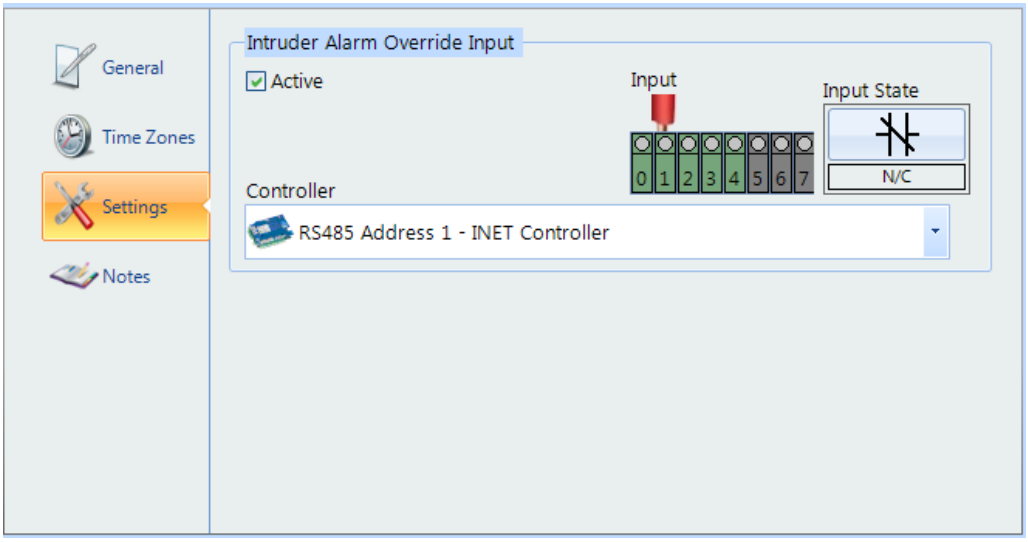


NOTE: Controlsoft do not recommend allocating a Time Zone to a card reader except in exceptional circumstances, as during the Time Zone, NOBODY would be able to access the door. It is preferable to allocate Time Zones to Users, whereby some users

(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 into a computer server room if the halon fire extinguishing system has been activated).



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

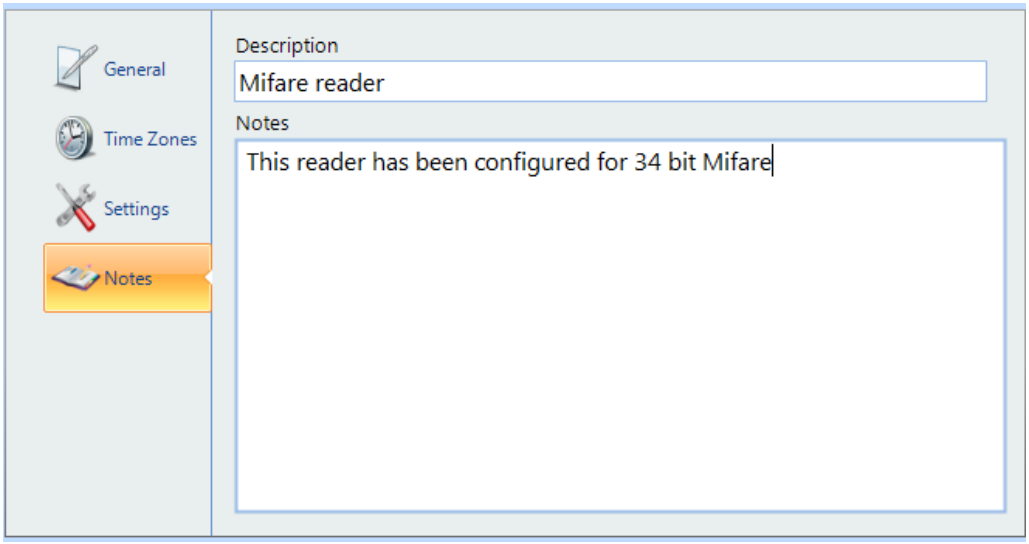
Select the appropriate **Input** connected to the external contact.

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 Notes

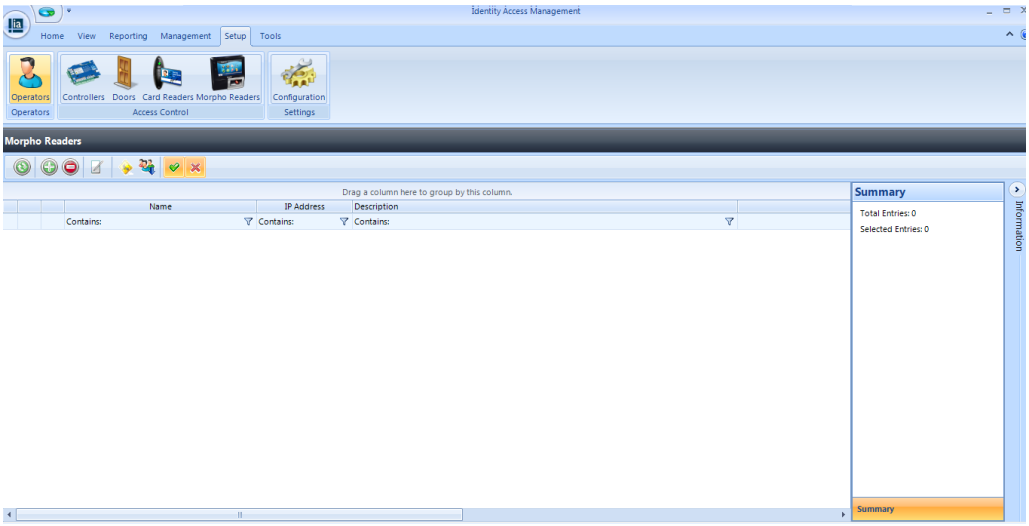
The **Notes** section, accessed from the side bar, provides 2 text fields called **Description** and **Notes** to help a Service Engineer during their first visit.



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

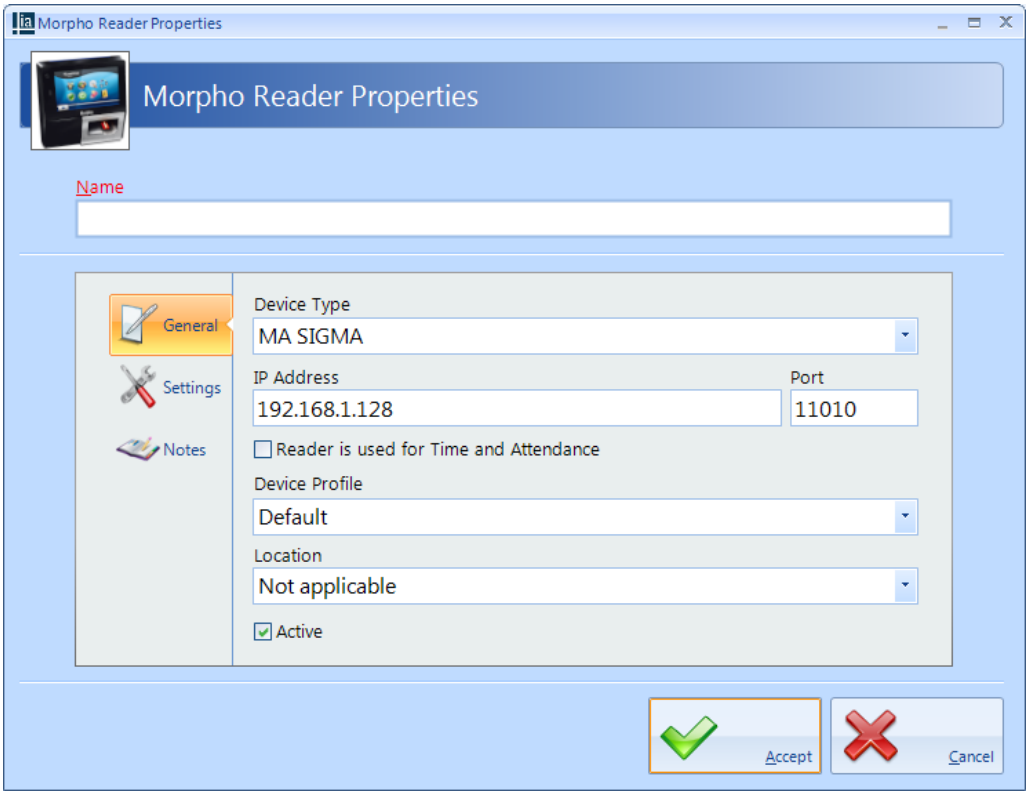
 Show/Hide Active: This button will show or hide Morpho Readers selected as Active.

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

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

NOTE: If using a Morpho reader which has previously been used on another system (e.g. Morpho Manager), it is important to first reset the Morpho reader. Format a flash drive (FAT16 or FAT32) and copy the files "Address.csv" and "Default.reg" to the root. With the reader powered up, place the flash drive into the reader's USB port and wait until the flashing LEDs change from purple to pale blue. Remove the flash drive, the reader will restart and will then be ready for download. For further information, please contact Controlsoft Technical Support.

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**

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.

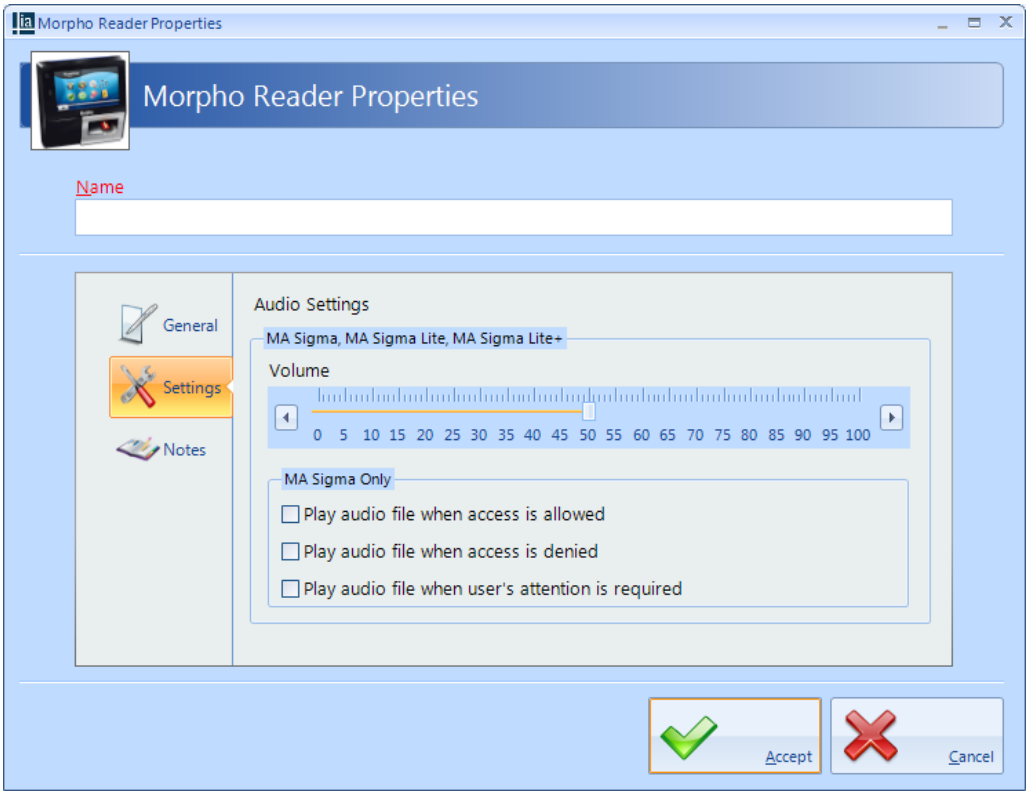
Select the relevant **Device Profile** from the dropdown list

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.

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.

10.2 Morpho Reader Settings

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



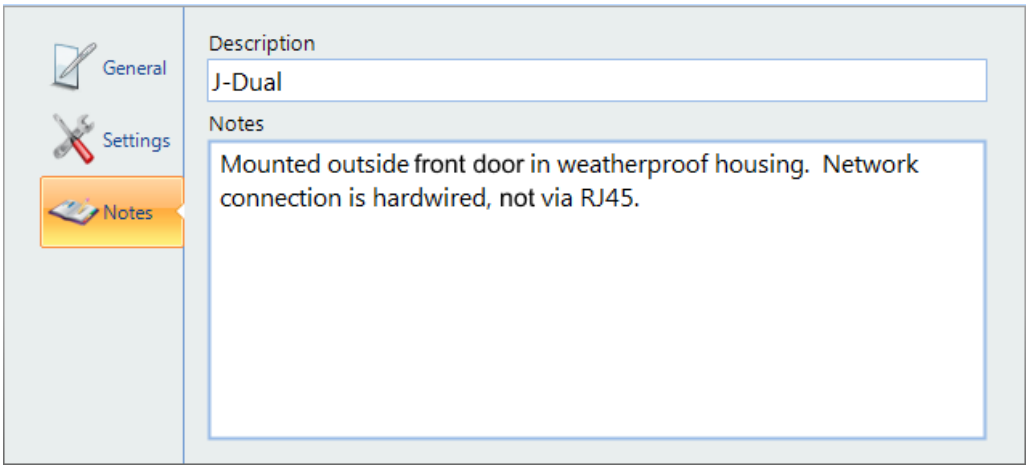
The **Volume** setting adjusts the volume of the selected reader

The MA Sigma allows audio files to be played under various conditions. These can be enabled or disabled by slecting **Play audio file when access is**

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

10.3 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.



Configure Time Zones

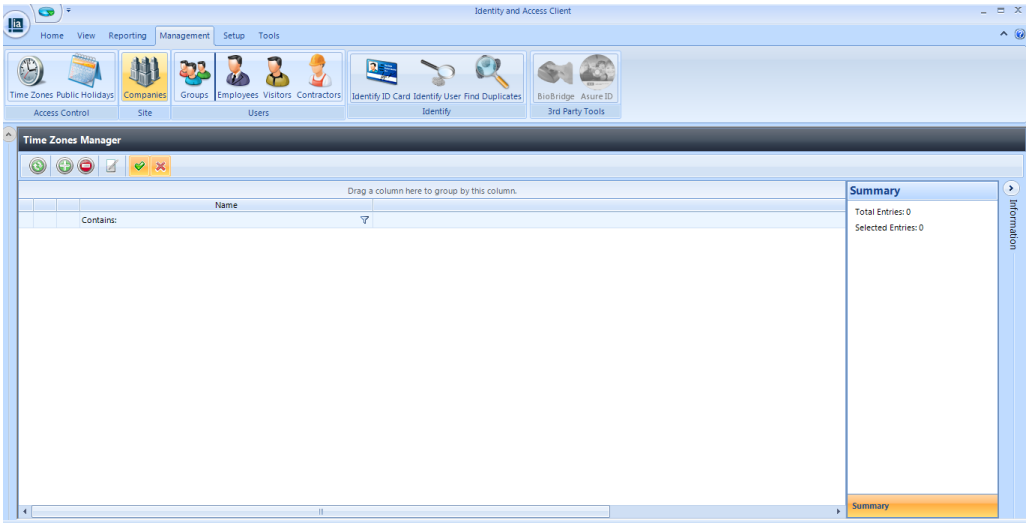
11 Configure Time Zones

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

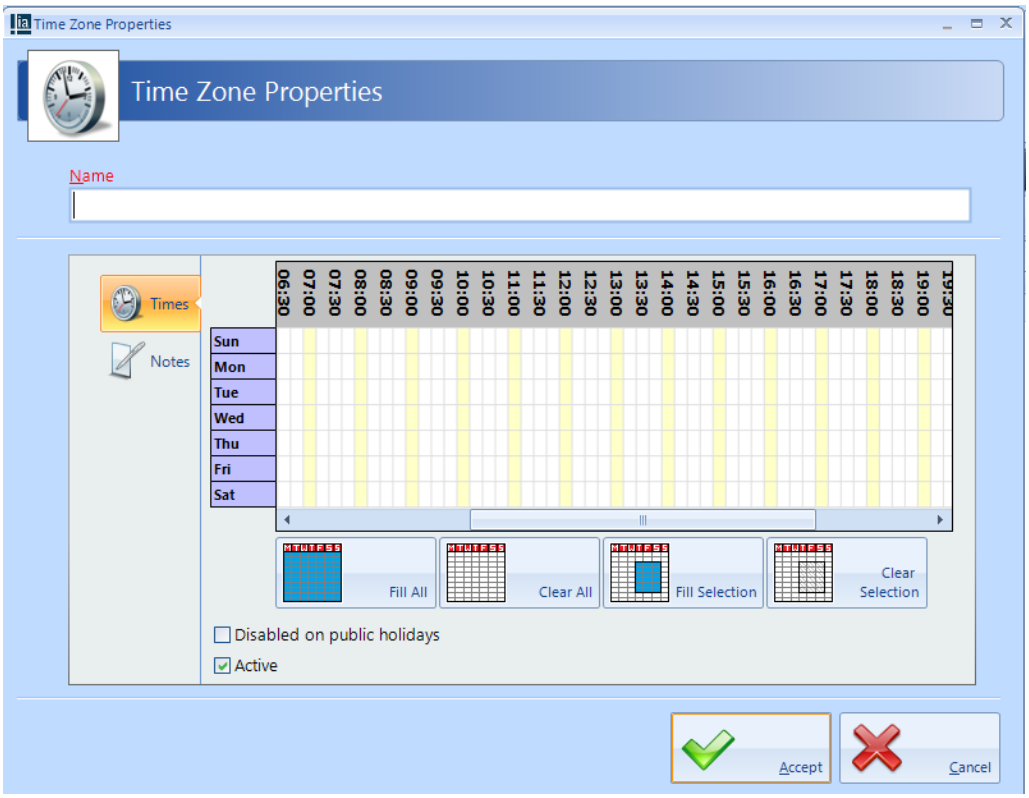
 Show/Hide Active: This button will show or hide Time Zones selected as Active.

 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 

11.1 Creating Time Zones

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



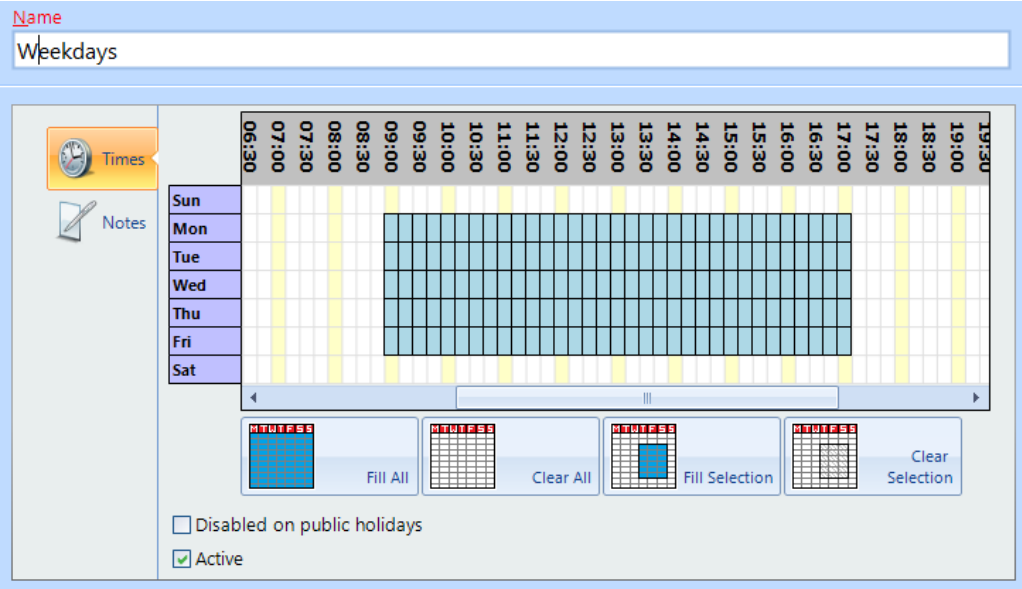
Enter a **Name** for the Time Zone

Use the mouse to select a range of times and days, then click **[Fill Selection]**

If **Disabled on public holidays** is selected, the Time Zone will not be active during defined public holidays.

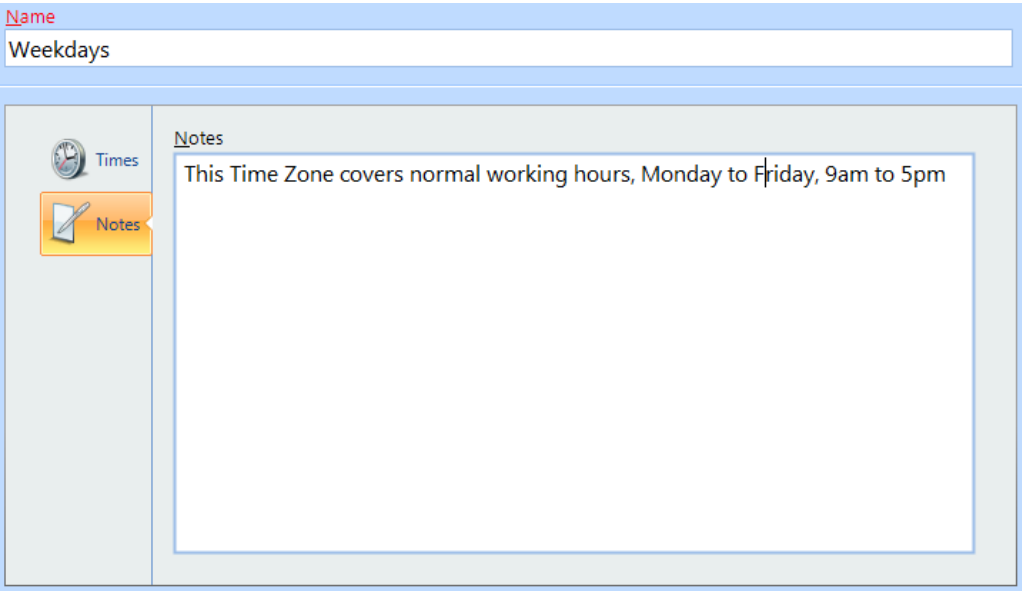
Ensure that **Active** is ticked otherwise it will not be possible to use the Time Zone.

A configured Time Zone will look something like this:



This Time Zone will operate from 9am to 5pm, Monday to Friday and will continue to operate on public holidays.

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.



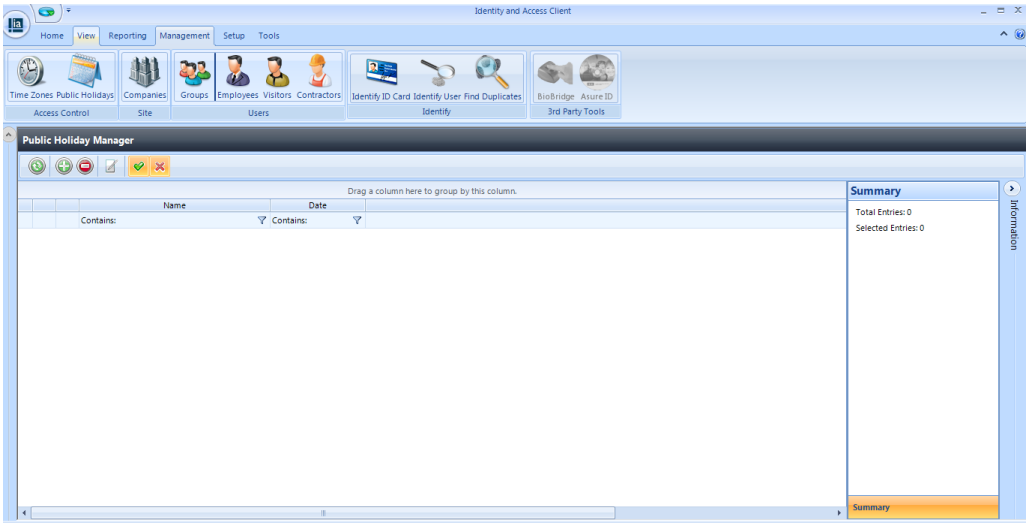
NOTE: Remember to associate Time Zones with the relevant Users / Doors, otherwise they will not be operational.

The i-Net controller can support up to 16 Time Zones when fitted with firmware version 98.33.21.9 or older, although it can support up to 62 Time Zones with firmware version 98.34.21.9 or later.

Public Holidays

12 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

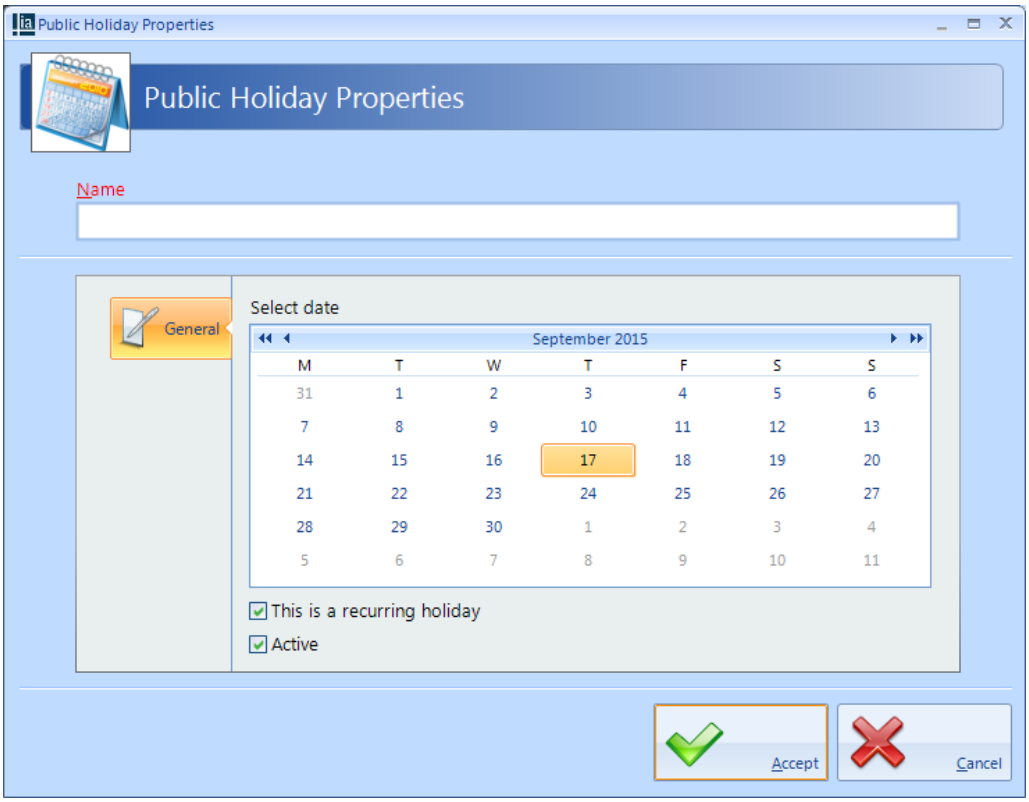
 Show/Hide Active: This button will show or hide Public Holidays selected as Active.

 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 

12.1 Creating Public Holidays

To configure a Public Holiday:

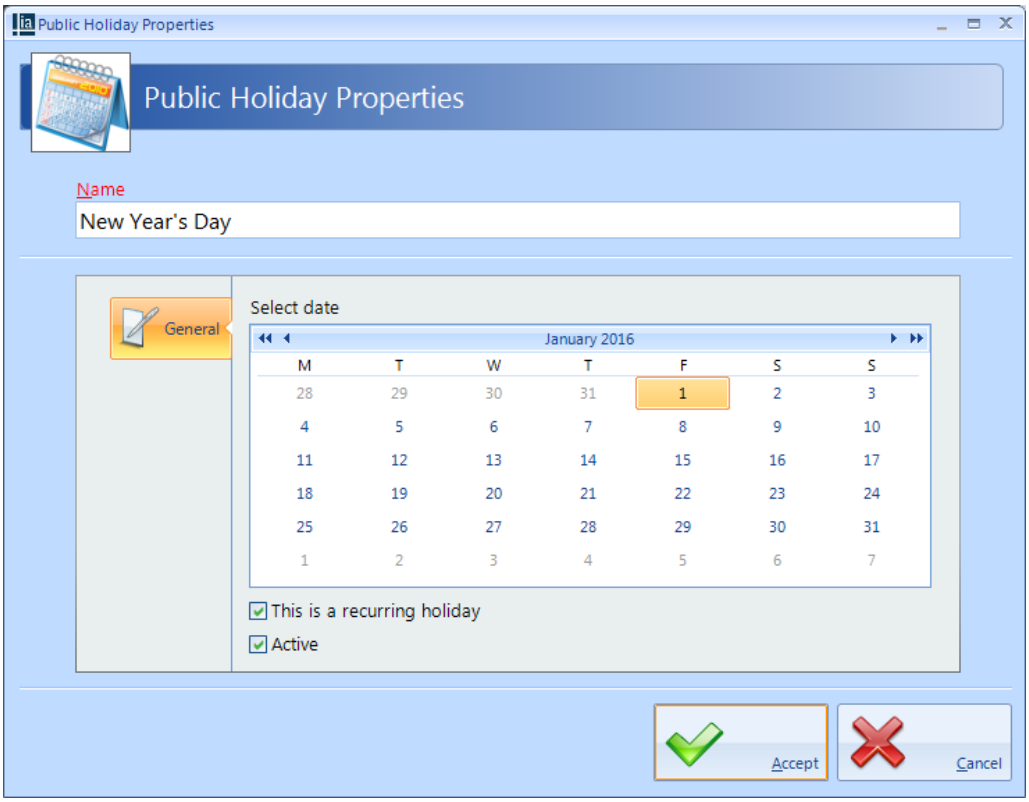


Enter a **Name** for the Public Holiday

Select date of the Public Holiday from the calendar

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

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



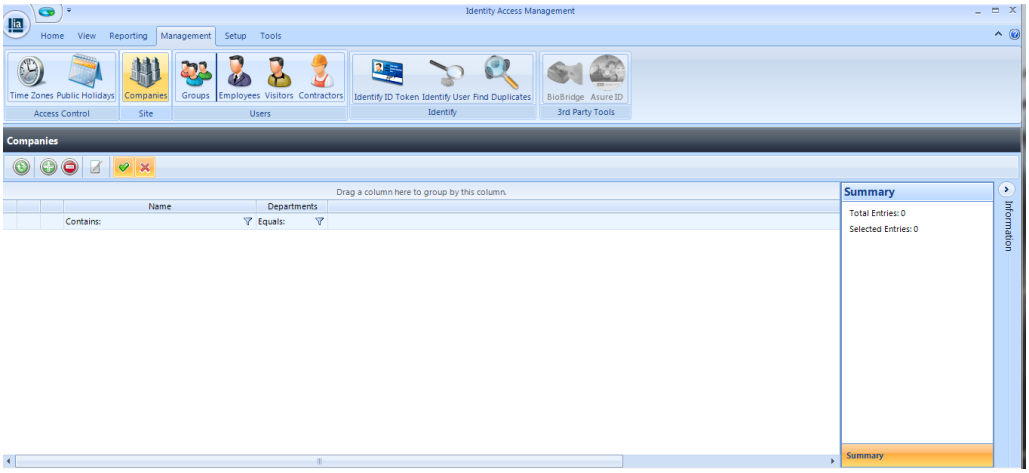
Click **[Accept]** when done.

Companies and Departments

13 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

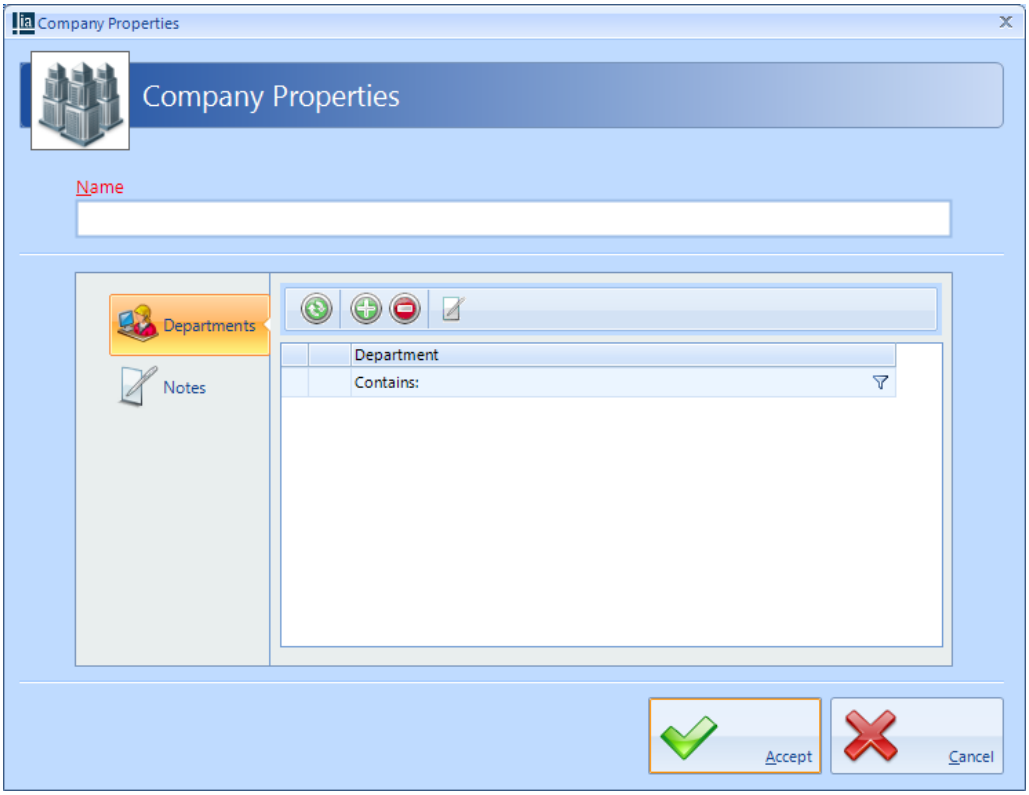
 Show/Hide Active: This button will show or hide Companies / Departments selected as Active.

 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) 175

13.1 Creating Companies and Departments

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



.

 Refresh: Updates the list of Departments

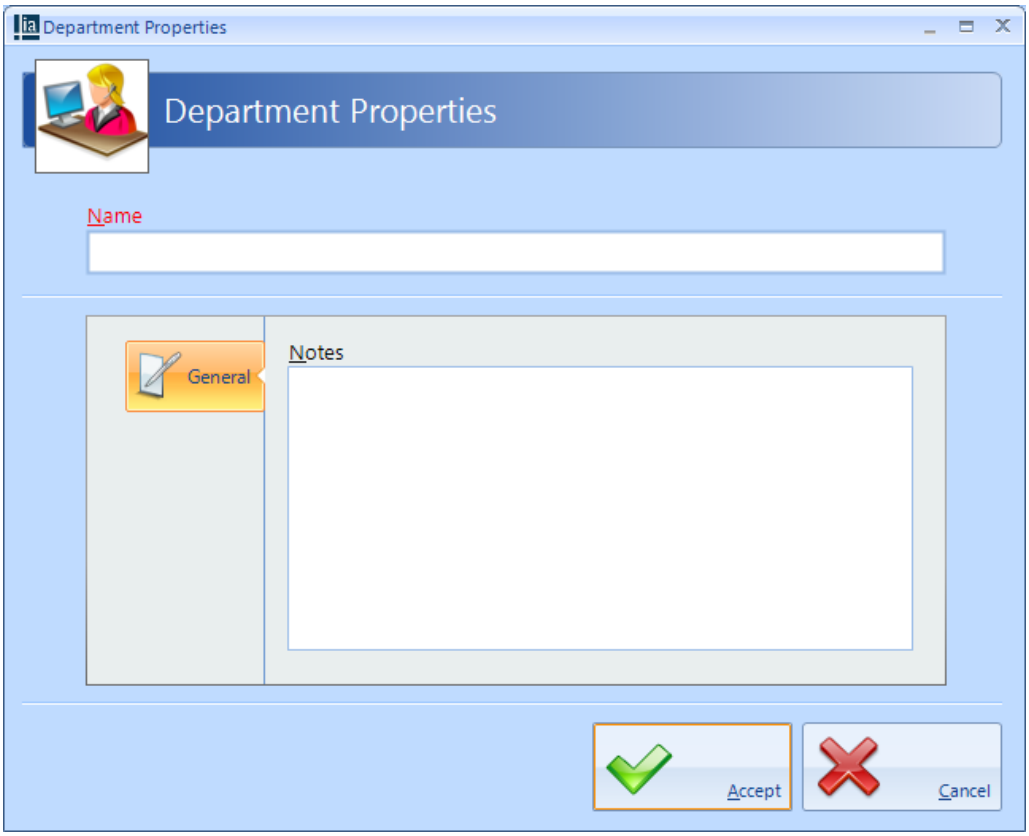
 Add: Creates a new Department in the list

 Delete: Removes the selected Department/s from the list

 Edit: Edits the selected Department

Name: Add a name for the new Company

Click the Add button  to create a Department for the Company



Name: Add a name for the new Department

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

NOTE: A Company can support multiple Departments.

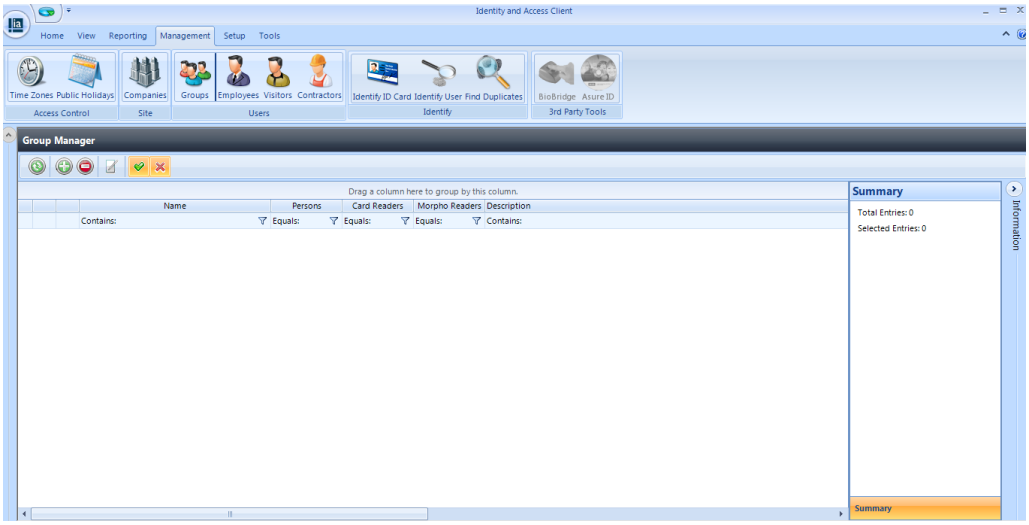
Configuring Groups

14 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.

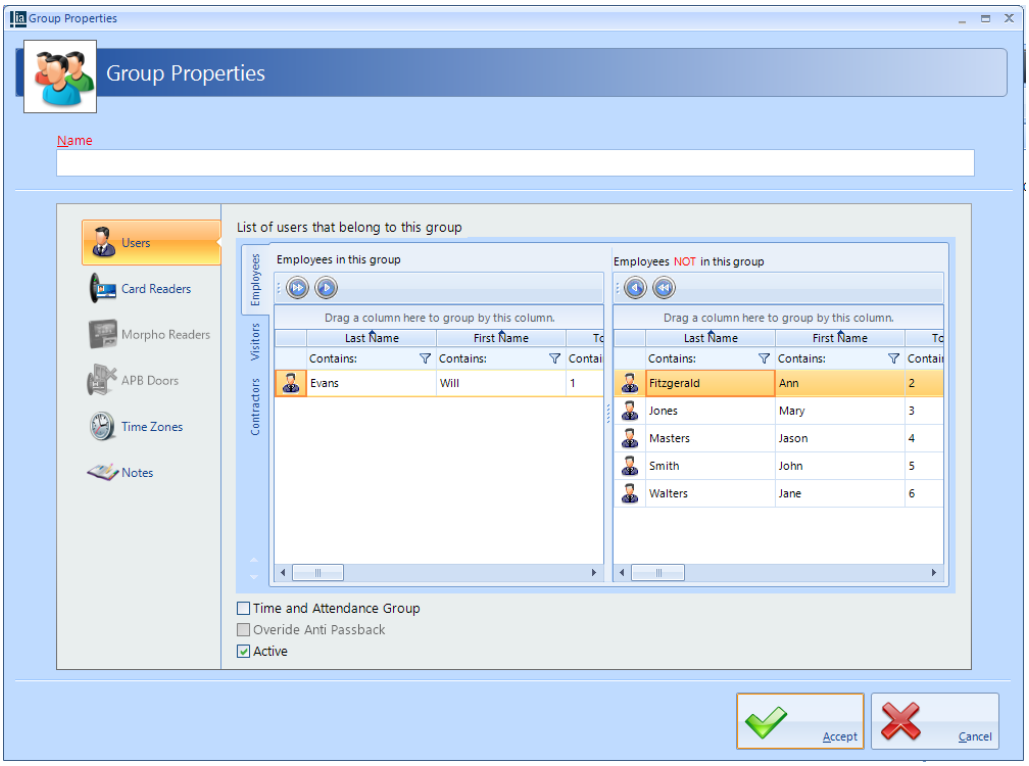
Select the **Add** New button 

14.1 Creating Groups

To configure the Group, use the Group Properties Window:

14.1.1 Groups Properties Users

The Group Properties window is used to configure the group.



Enter a **Name** for the Group

The **List of users that belong to this group** displays all users on the system. To allocate users to the Group, simply select one or more users and click  Alternately, click  to move all users to the group.

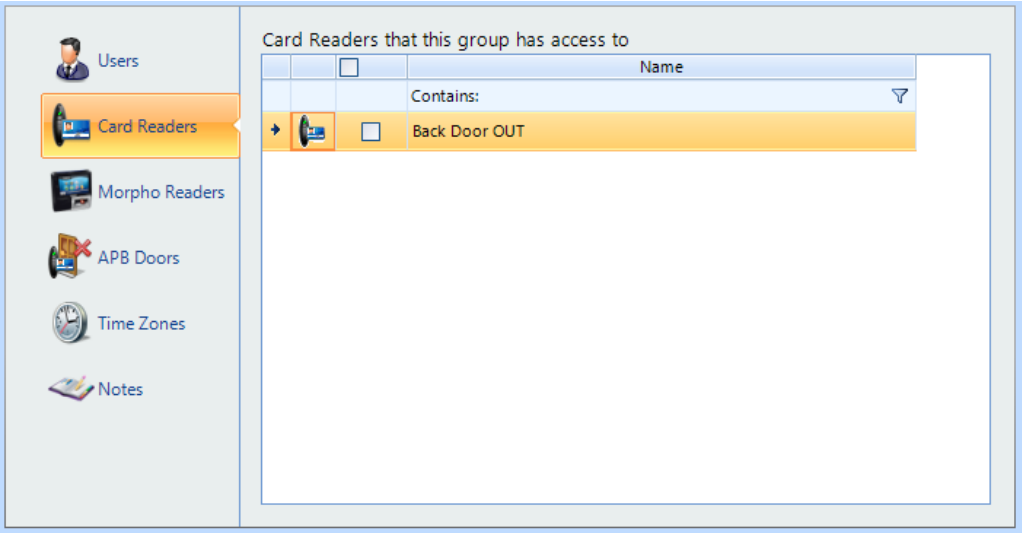
Tick the **Time and Attendance Group** box if members of this Group are to be monitored for Time & Attendance.

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

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

14.1.2 Groups Properties Card Readers

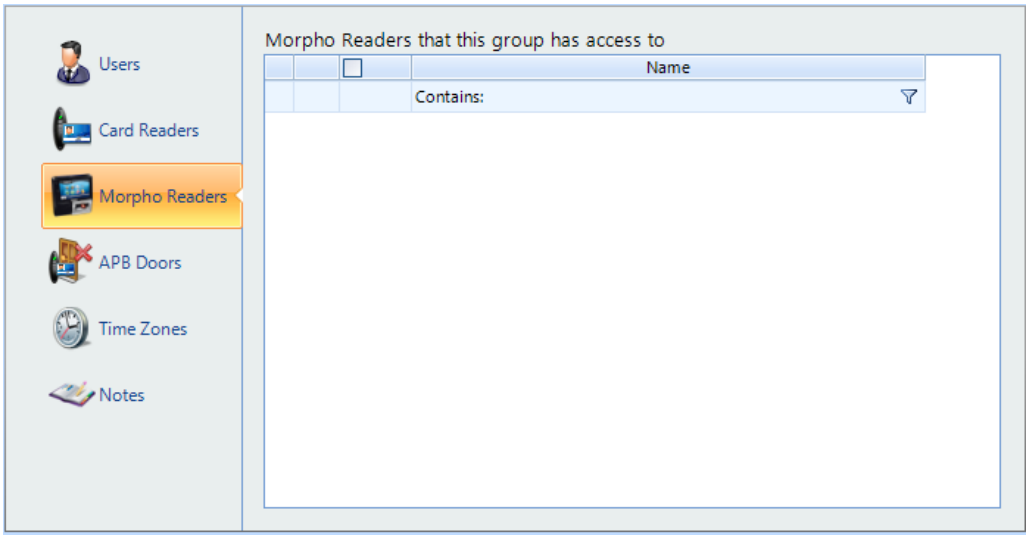
Select **Card Readers** in the side bar:



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

14.1.3 Groups Properties Morpho Readers

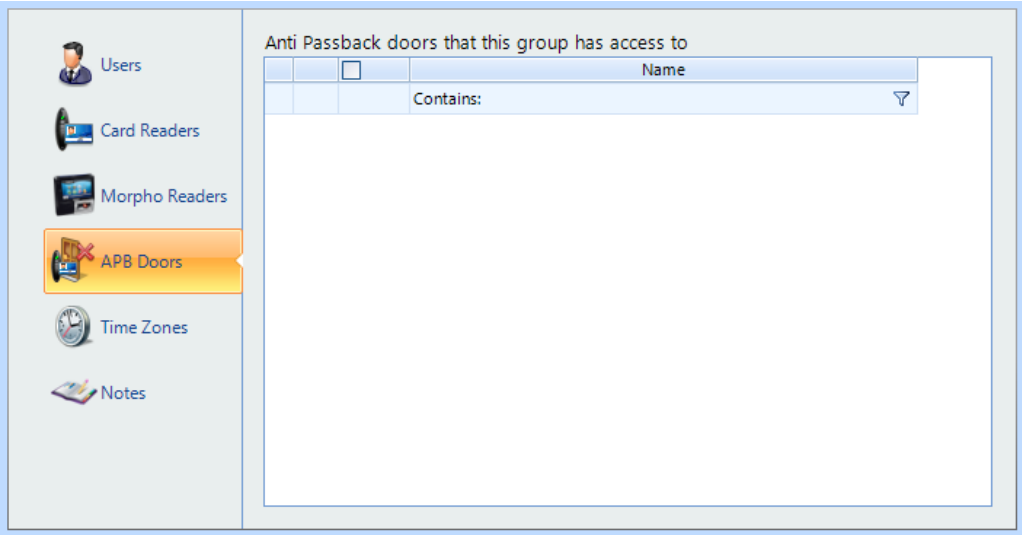
Select **Morpho Readers** in the side bar:



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

14.1.4 Groups Properties APB Doors

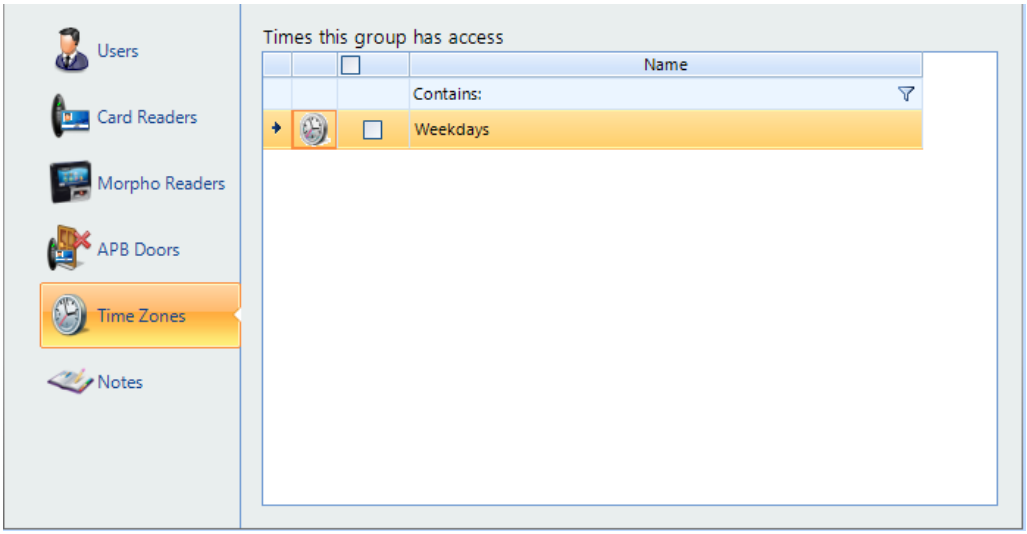
Select **APB Doors** in the side bar:



Select one or more Doors where members of this Group will be subject to Anti Passback

14.1.5 Groups Properties Time Zones

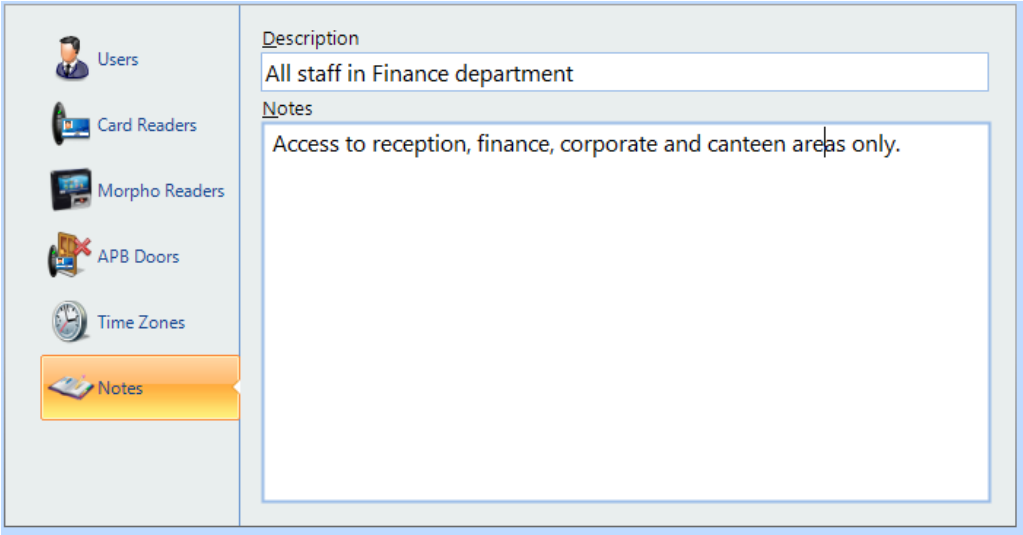
Select **Time Zones** in the side bar:



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

14.1.6 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:



14.2 Allocating Users to Groups

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

1. From within the User Properties 175 Window.

2. From within the Group Properties 161 Window.

NOTE: Users can be allocated to more than one Group, but please be aware that 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

Enrolment Readers

15 Enrolment Readers

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

AC-1051 for Controlsoft Proximity cards (see AC-1051 Controlsoft Proximity Reader) 167

AC-1052 for MIFARE CSN cards (see AC-1052 MIFARE CSN Reader) 170

Omnikey 5427CK for iCLASS or HID Proximity cards (see Omnikey 5427CK iClass and HID Prox Reader) 171

15.1 AC-1051 Controlsoft Proximity Reader

The CS-AC-1051 USB Enrolment Reader is compatible with Controlsoft 125KHz proximity cards or tags.

Used in conjunction with Controlsoft's 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.

Installing the IT LOCKS Software:

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

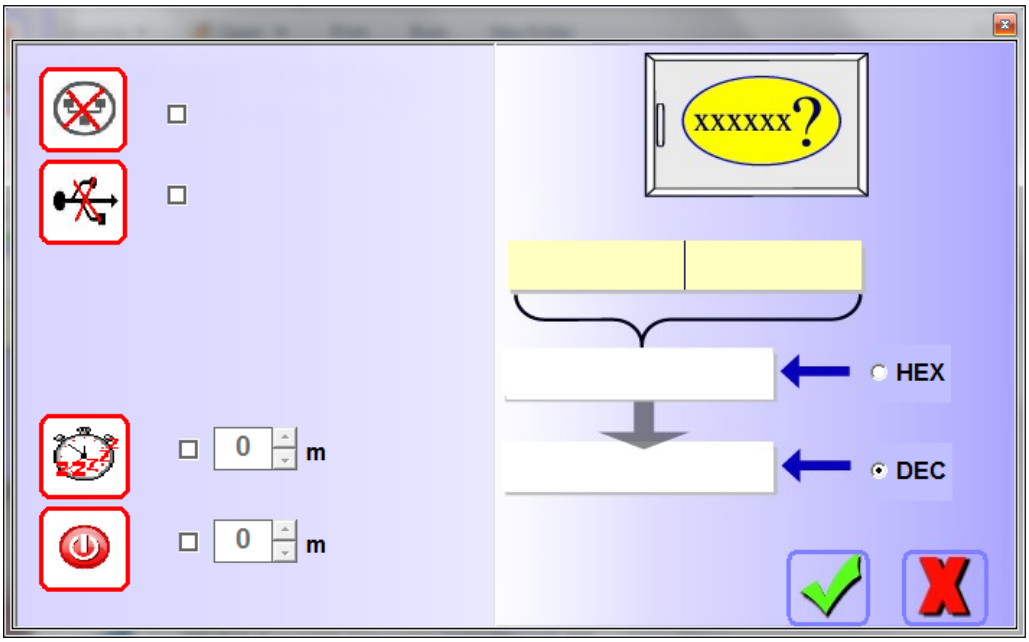
- Insert the Installation CD into the CD drive and close the tray.
- The installation wizard will start automatically
- Follow the on-screen instructions to install both the "IT Locks" and "Device Drivers".
- If using Windows 8.1, the application "SendInput.exe" is not always installed in the startup folder. To achieve this manually:
  - Open File Manager and browse to C:\Program Files (x86)\it locks\
  - Right click on the application "SendInput.exe" and select "Create shortcut"
  - Place the shortcut on the desktop and close File Manager
  - Right click the start button, select "Run", type shell:common startup in the box and click [OK]
  - Move "SendInput – Shortcut" from the desktop into the startup folder and close File Manager
- Reboot the PC.
- Plug the Enrolment Reader into the PC's USB socket.
- Windows will now search for the drivers (searching Windows Updates can take some time) and prompt when it has finished.
- Installation of the software and drivers is now complete.
- Reboot the PC if instructed to do so.

Setting the USB Reader to Enrolment Mode

After installation an "IT-Locks" icon will appear on the desktop.

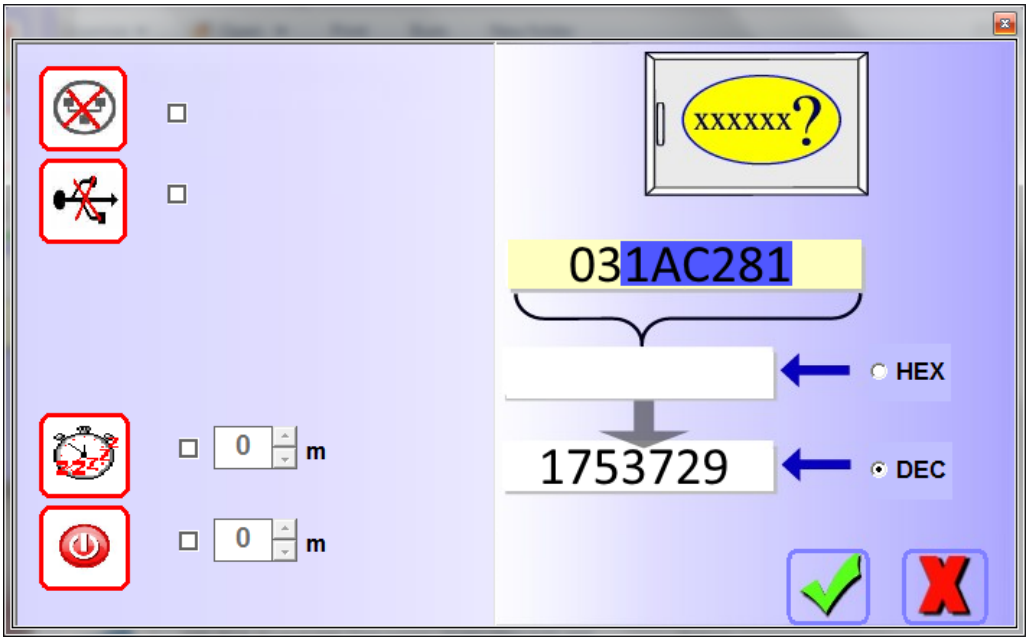
- Double click the "IT-Locks" icon and the Front Screen appears as shown below

- Click on the "Screwdriver and Hammer" icon and a password box appears.
- Enter the password "axxess78" and click on the green tick to progress to the next screen.



- The Enrolment Reader is supplied with a Configuration Card. Place this card onto the reader and check that a hex number appears in the orange box.

- Check that the Radio Button marked “DEC” is selected.
- Using the mouse, highlight the last 6 digits (for 26 bit card format) or the last 8 digits (for 34 bit card format) of the Hex number in the orange box. The “DEC” box will now display the number printed on the card.



- Click on the green tick to return to the IT-Locks Front Screen.
- Click on the “Keyboard” icon in the IT-Locks Front Screen and the window will disappear. A “Keyboard” icon will now appear in the Notification Area at the bottom right hand corner of the monitor.

- Reboot the computer and make sure the keyboard icon appears automatically when the PC has restarted.

When installed, please refer to User General 175 for information on using the Enrolment Reader when creating or editing users.

15.2 AC-1052 MIFARE CSN Reader

The CS-AC-1052 USB Enrolment Reader is compatible with MIFARE Smartcards.

Used in conjunction with Controlsoft's 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.

The AC-1052 uses the same IT LOCKS software as the AC-1051. Please refer to AC-1051 Controlsoft Proximity Reader 167 for further information.

15.3 Omnikey 5427CK iClass and HID Prox Reader

The Omnikey 5427CK 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.

- Insert the Installation CD into the CD drive and close the door.
- 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://192.168.63.99 171 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 **Store Changes**, followed by **Apply Changes**.

When installed, please refer to User General 175 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) 88.

Users

16 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.

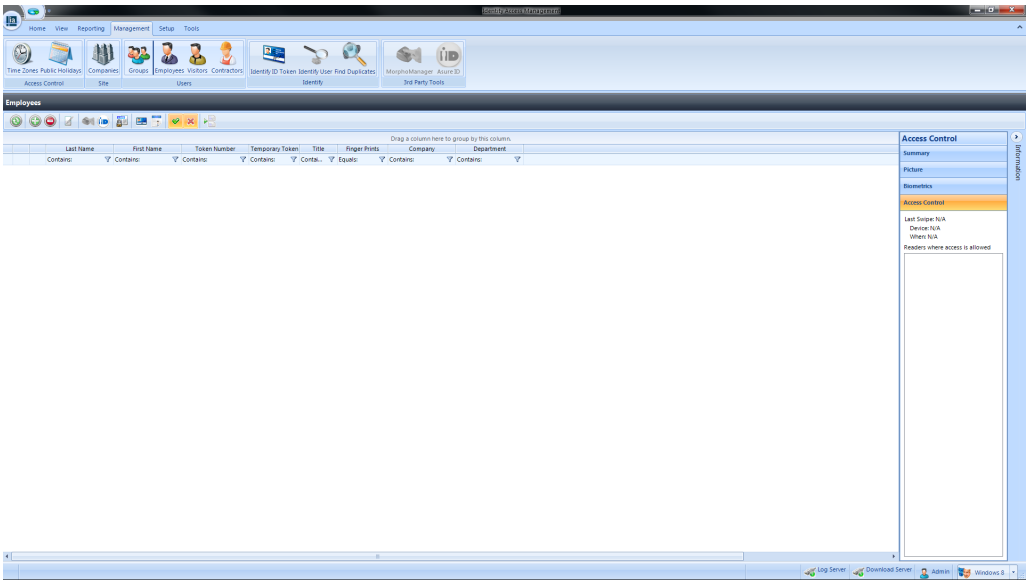
Visitors may have limited access to the premises and may be heavily managed on a day to day basis.

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. Only programming screens for Employees has been 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 (as shown) if MorphoManager is not enabled.

Print: Prints a card for the selected user

 Report: Run an access log report for the selected user

 Temporary Token: Assign or remove Temporary Token for a User

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

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

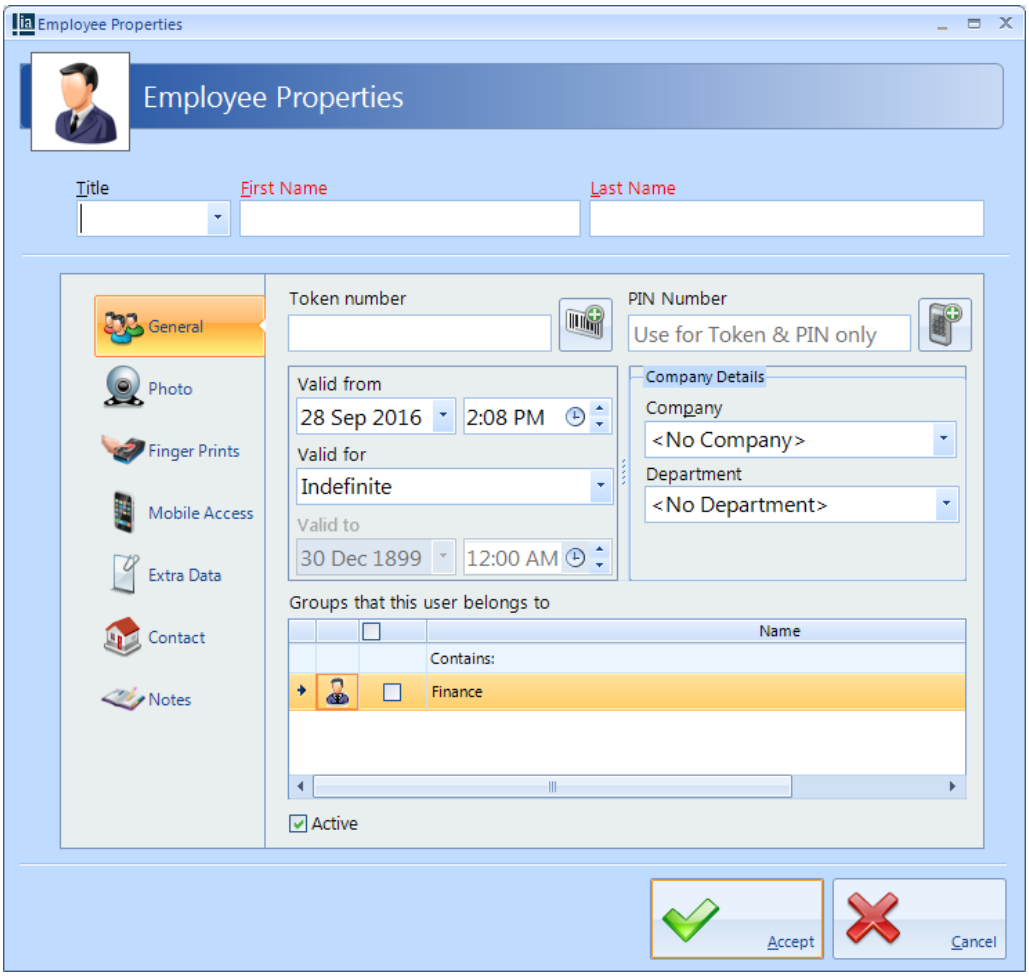
 Show/Hide Inactive: This button will show or hide Users not selected as Active.

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

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"

16.1 User General

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



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

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

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

The user will have no access to the system until the **Token is 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 **Token is valid for** expires (default is Indefinite).

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 a group, simple tick the box for that group.

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

NOTE: Users can be allocated to more than one Group, but please be aware that constraints exist when multiple Groups are combined:

EXAMPLE:

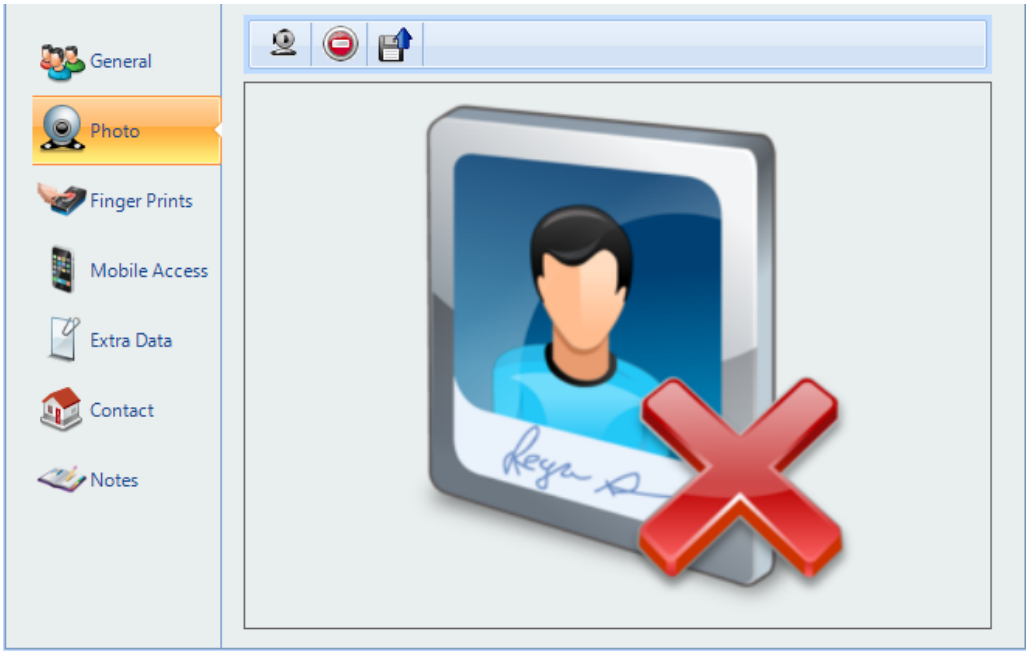
Group 1 has access to Reader A from 10:00 to 11:00

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

16.2 User Photo

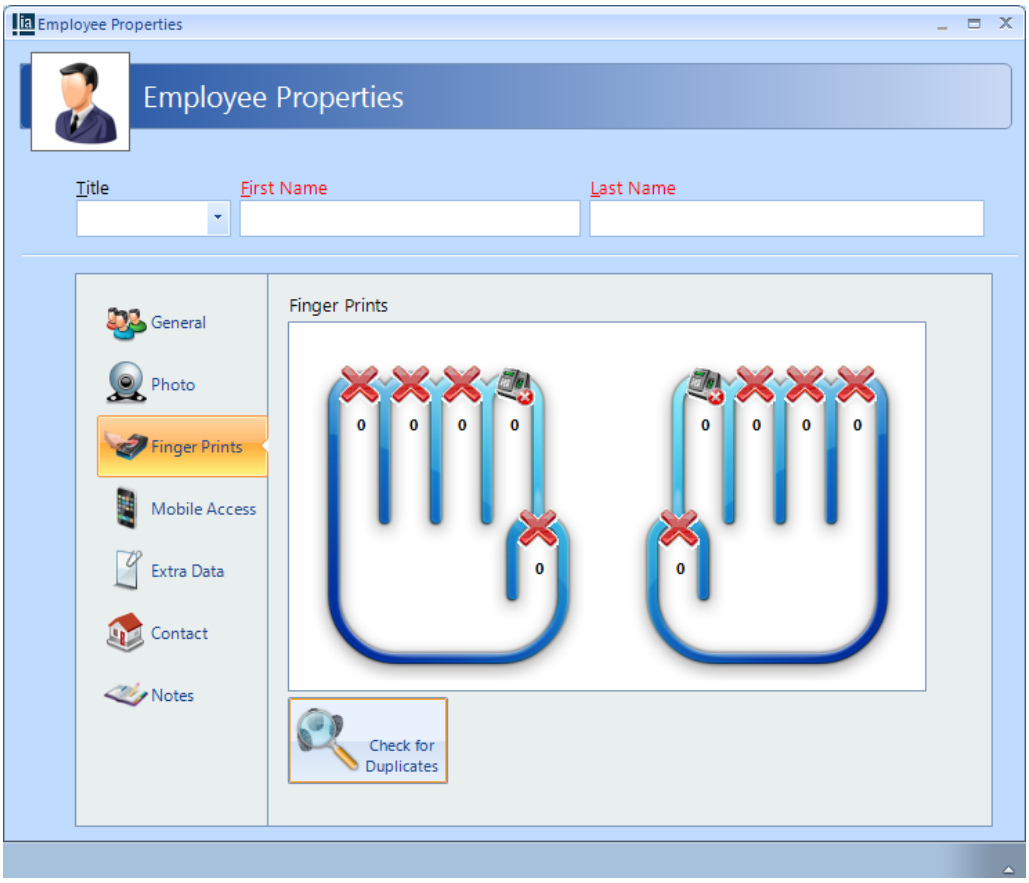
Allocating a photo to a user can be useful when identifying a lost card as it is possible to read the card and display the photo and other details of the relevant user. As standard there are two Reader Monitors located in the Dashboard to view the photos of people entering and exiting the premises.



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

16.3 User Fingerprints

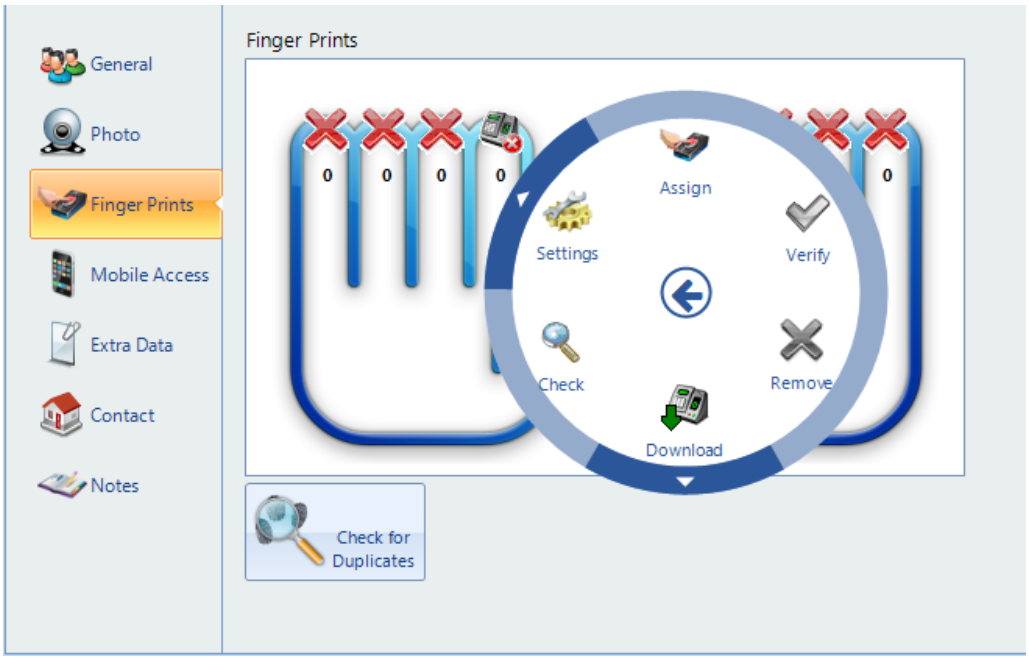
To read a fingerprint for a user, first select the finger to be read:



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

Read a fingerprint as follows:

Left click on the fingerprint you wish to add, then select **Assign** from the Option Wheel:

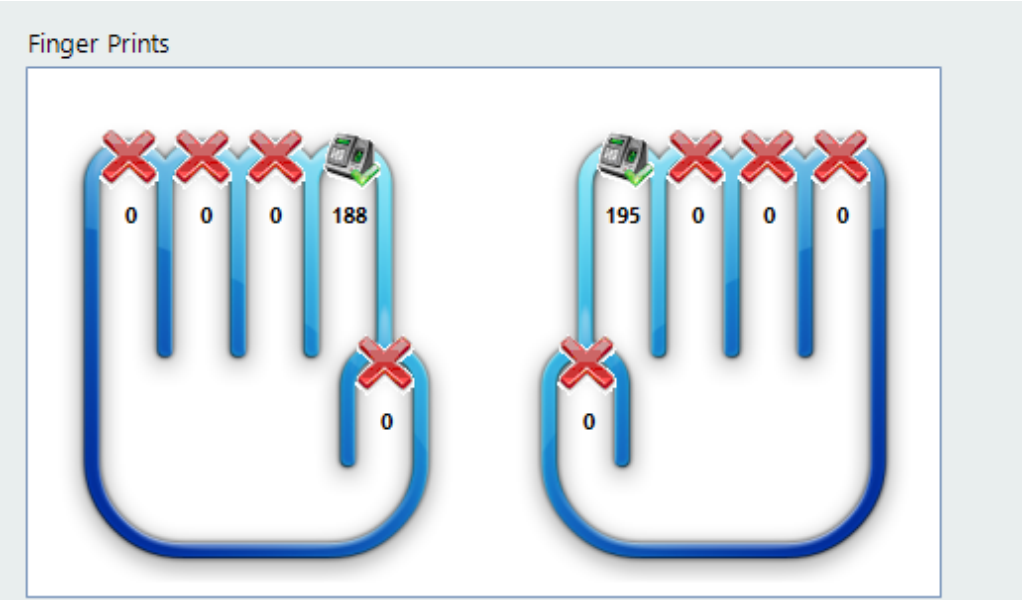


.

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

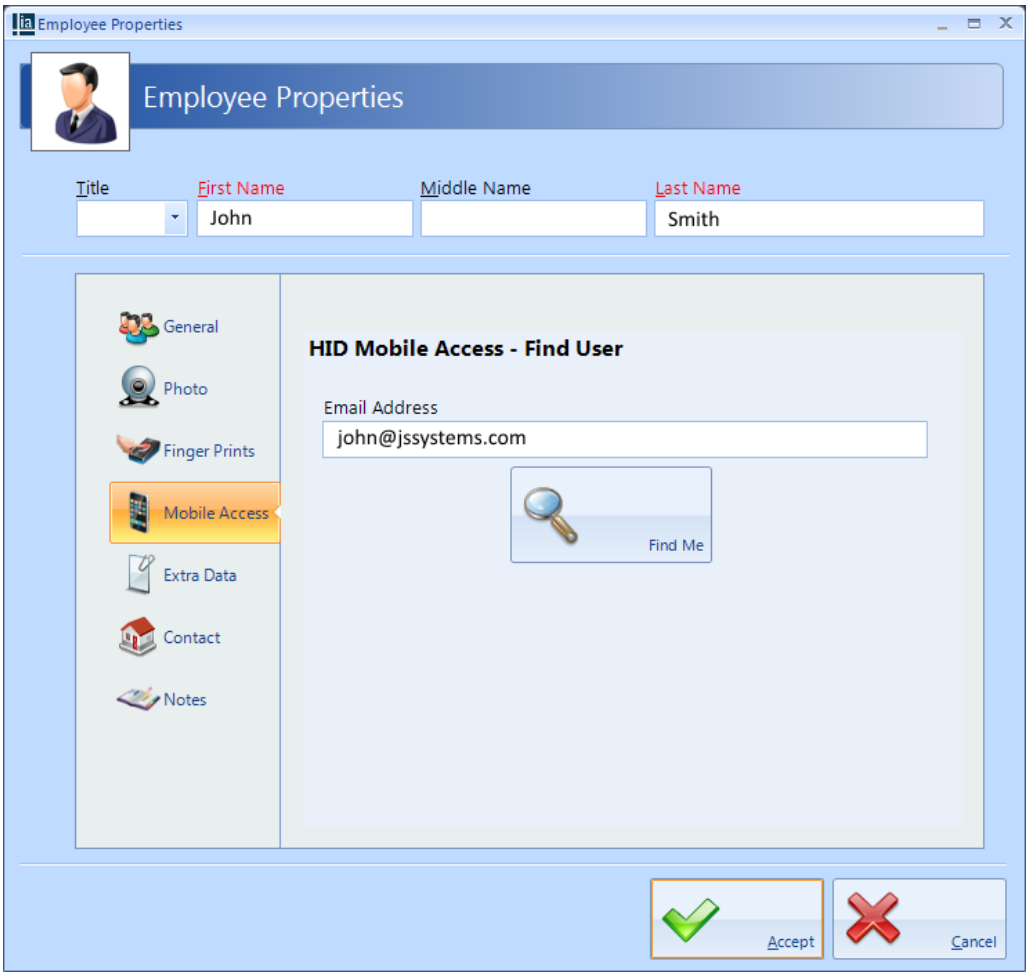
Assign a second finger. Qualify that both fingers have been enrolled and the score is satisfactory.

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.

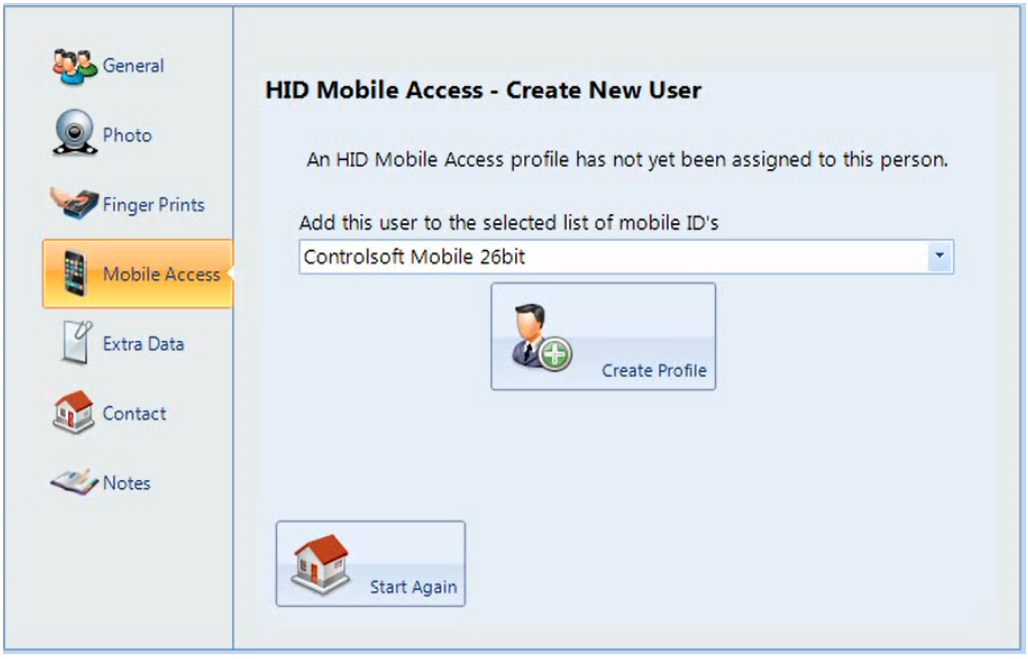


16.4 User Mobile Access

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

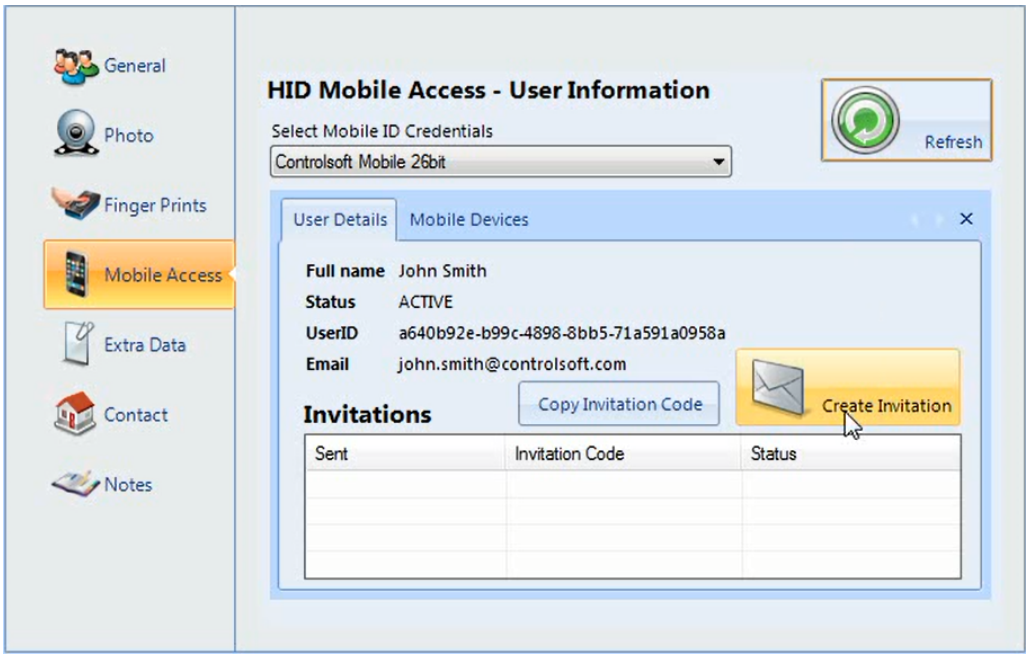


Having first entered the required information in the **General** screen and the user's email address in the **Contact** screen, select the **Mobile Access** tab and click **[Find Me]**



Assign the user to the relevant list of available Mobile IDs (example Controlsoft Mobile 26 bit), and click **[Create Profile]**

Click **[Refresh]** to update the user details:



When the user has installed the HID Mobile Access App on their phone, they select 'Enter Invitation Code' and enter the code which the system automatically emailed to them. ***NOTE: This invitation code is time limited and must be activated promptly.***

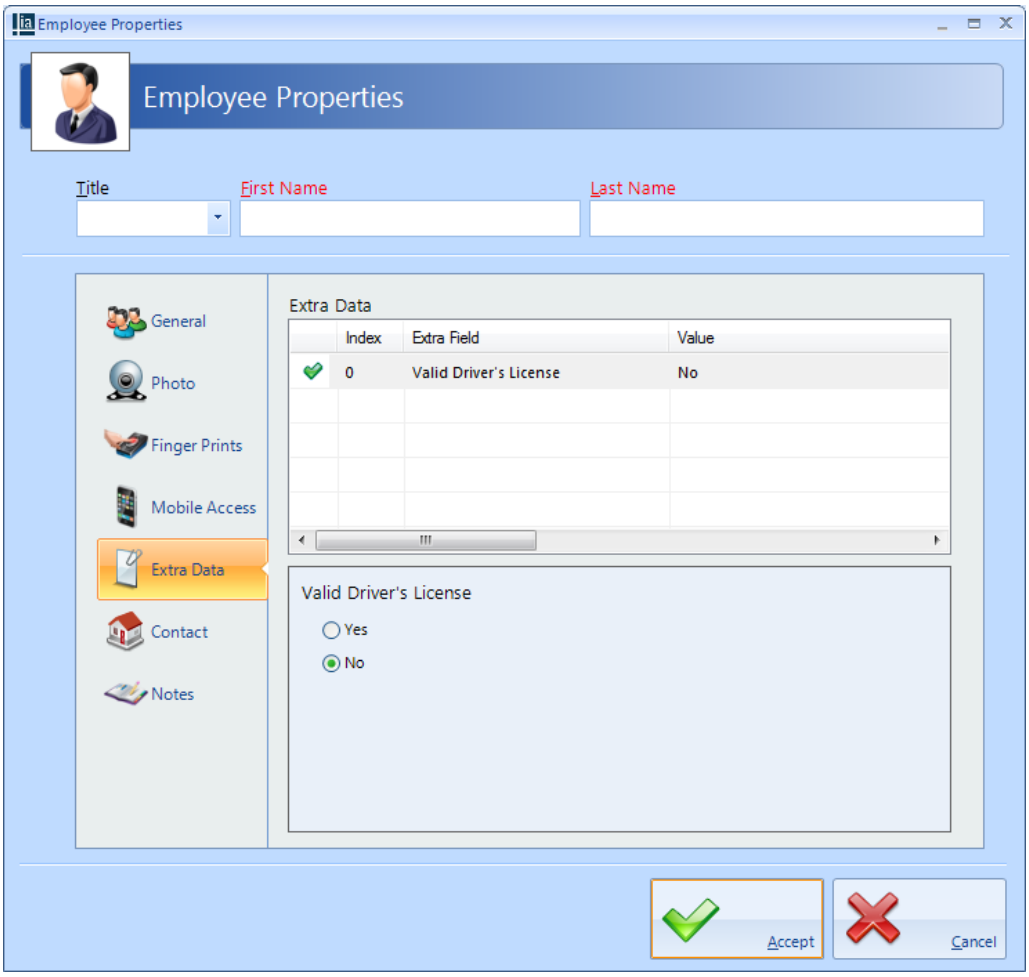
Once the user has confirmed that this has been completed, simply select **[Issue Mobile ID]** to complete the process.

16.5 User Extra Data

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

The Extra Fields are configured within the Identity Access Server Configuration software (see Identity Access Server Configuration 58).

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

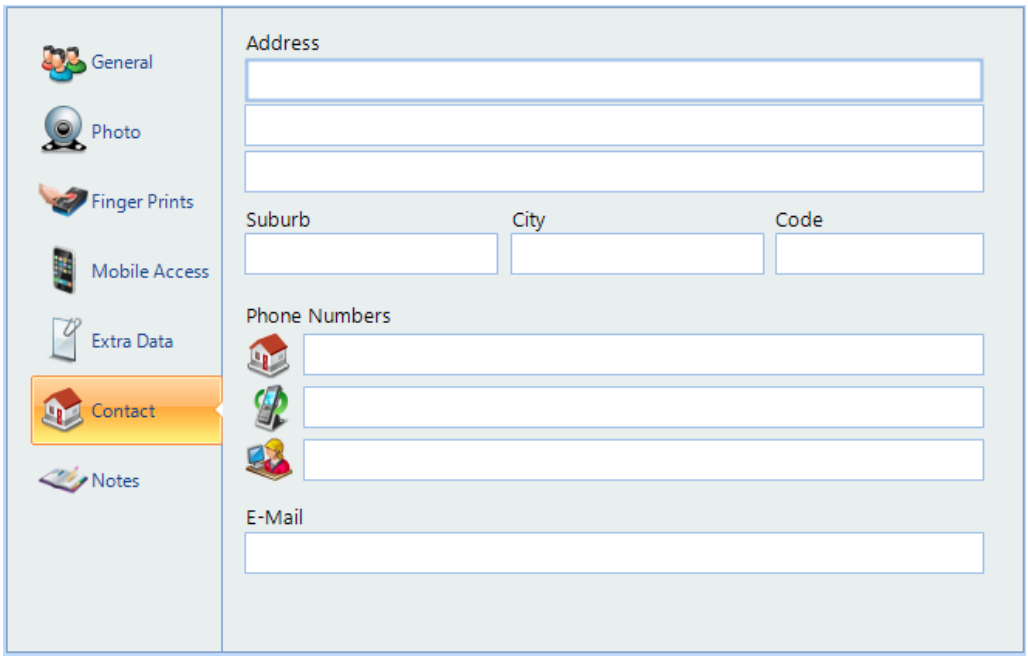


To record whether the user has a valid driver's license, simply select **Yes** followed by **[Accept]**.

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

16.6 User Contact

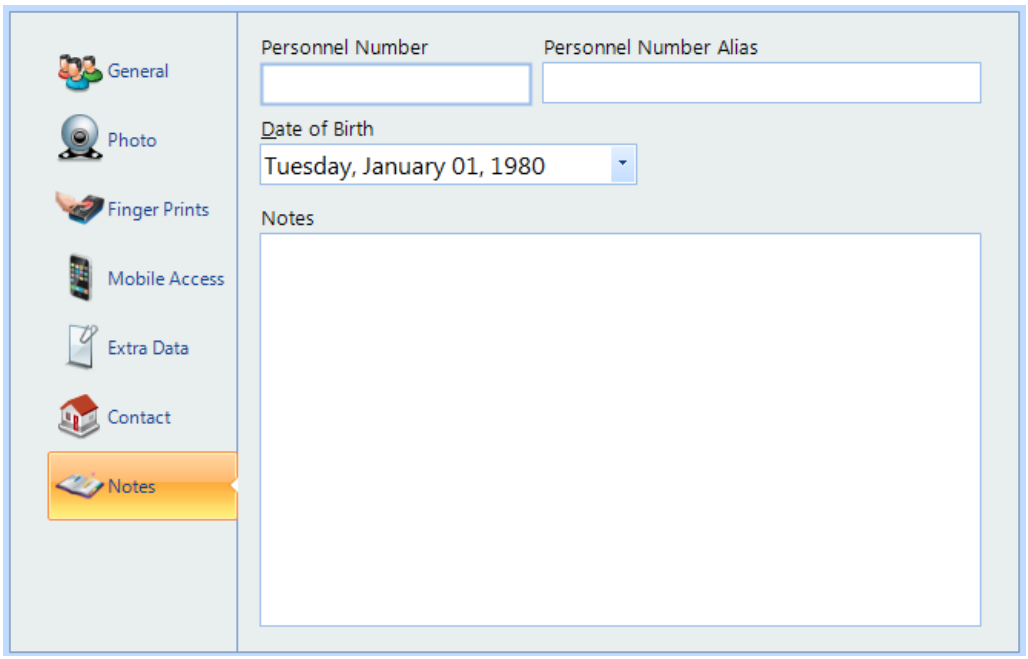
The Contact Details in this tab are not mandatory, but can be recorded if required:



.

16.7 User Notes

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



16.8 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 and follow the Import Wizard:

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

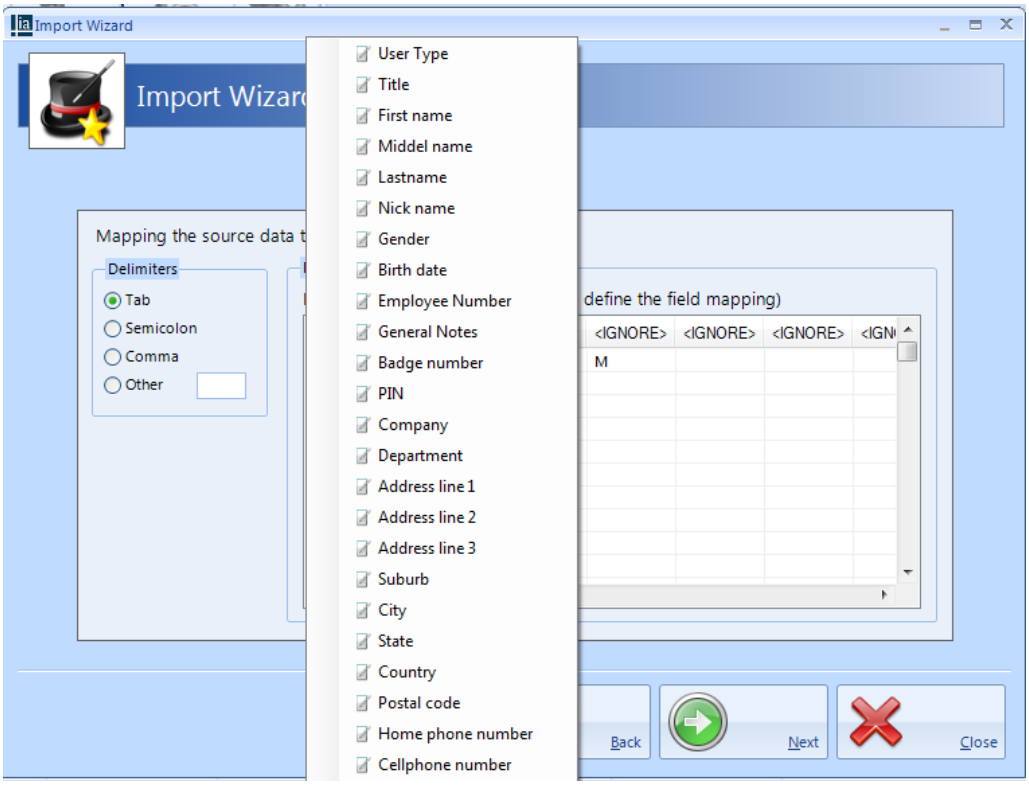
Under **Source File**, click the **[...]** button to browse to the .csv file. Select **Remove old data before importing new data** if required. Click **[Next]**.

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

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

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

Under **Delimiters**, choose which character has been used in the .csv to separate data (usually commas or tabs). Click **[Next]**. Under **Mapping the source data to the database fields**, link each column in the .csv file to the corresponding database field.

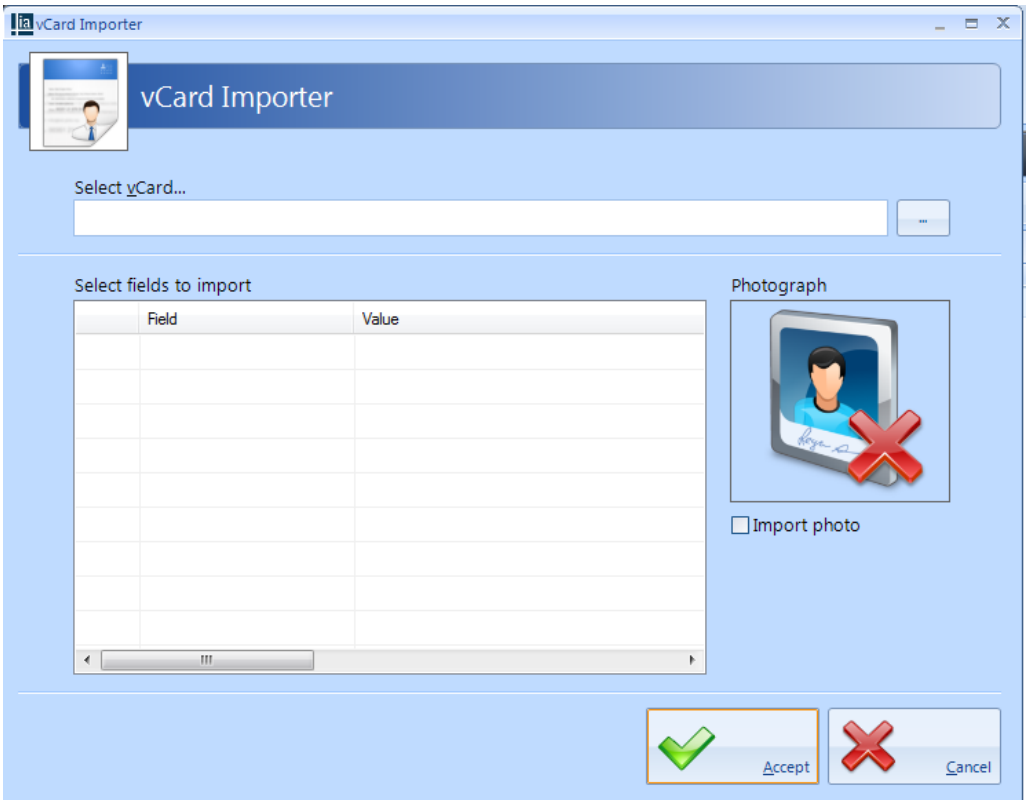


Click on each header **<IGNORE>** and select the appropriate field name for that field.

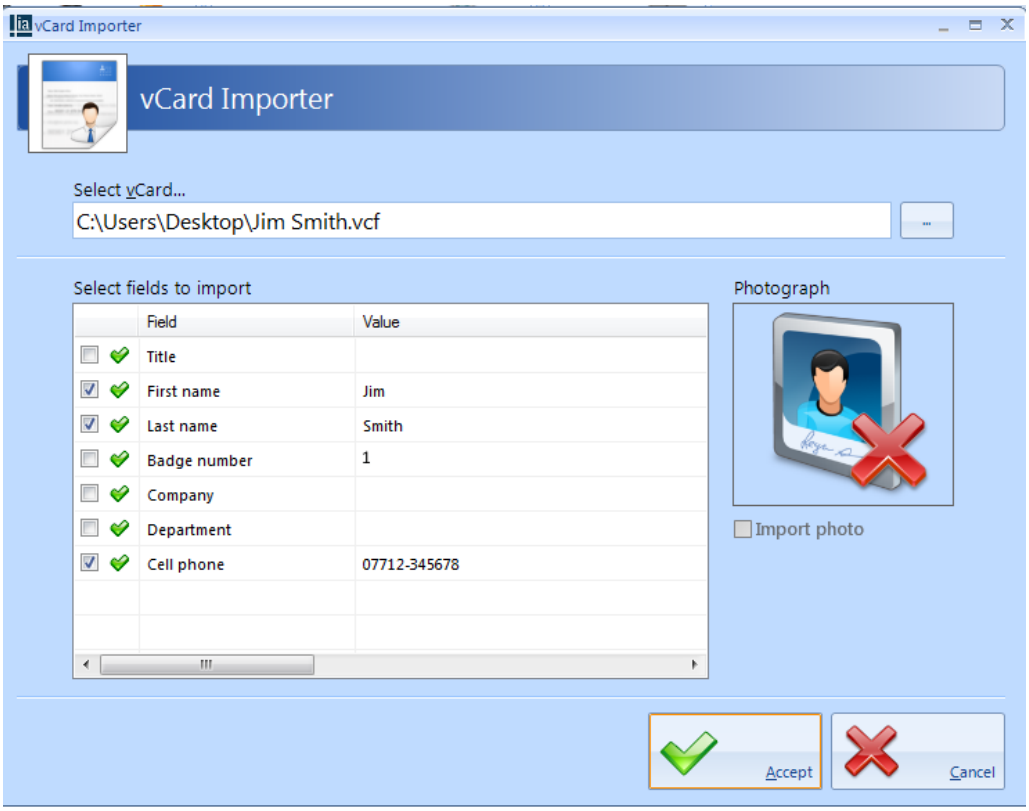
When complete, click **[Next]**, followed by **[Import]** to start the import process and **[Close]** when the import is complete.

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.



Use the **Select fields to be imported** to select the required information (in this example First name, Last name and Cell phone)

Select **Import photo** to add a photograph for the user.

Click the **[Accept]** button when complete.

NOTE: If the vCard is imported with no Token Number, Identity Access will allocate the first available number to it, in this instance '1'

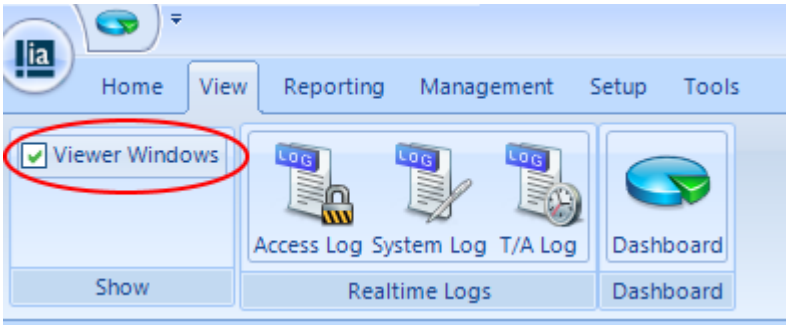
Event Viewers and Reports

17 Event Viewers and Reports

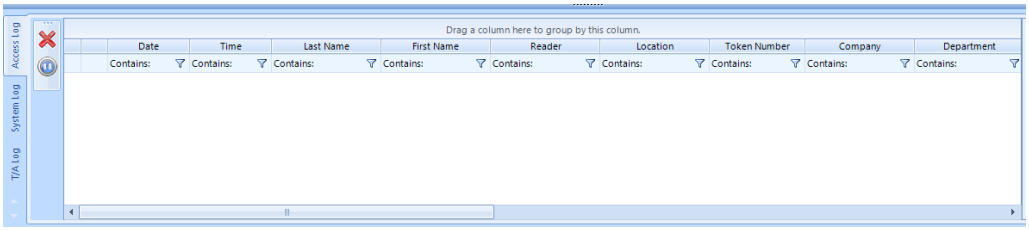
The Event Viewer in Identity Access software is a powerful tool for analysing system activity.

17.1 Event Viewers

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



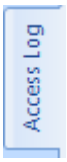
When selected, the viewer window will be visible in the lower half of the screen:



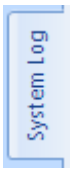
 Clear Window: Clears all events in the Viewer Window

 Pause/Run:

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



Displays events from the Access Log.



Displays events from the System Log.

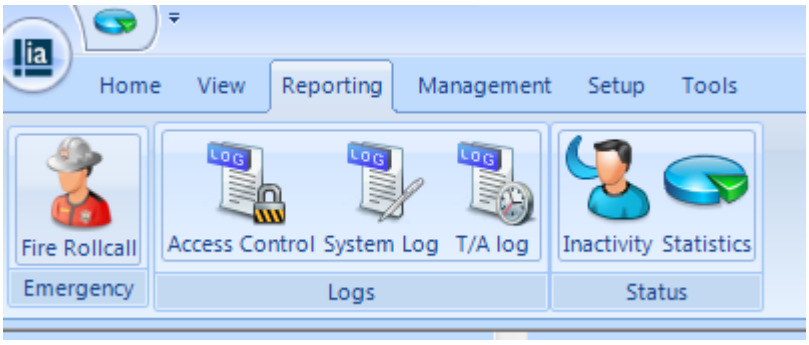
Displays events from the Time & Attendance Log

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

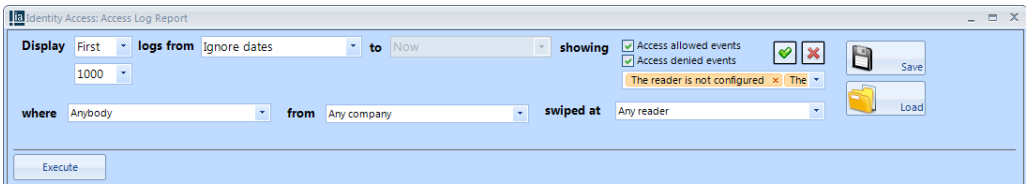
17.2 Access Control Reports

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 Control**.

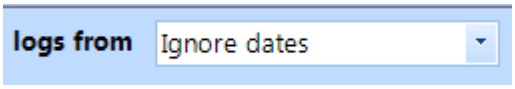


This then runs the Identity Access: Access Log Report form as shown below:

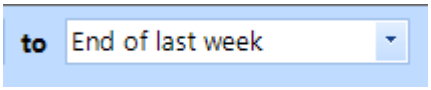


The options on generating the report are as follows:

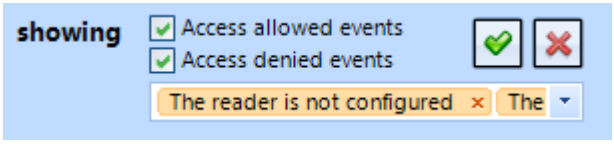
defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.



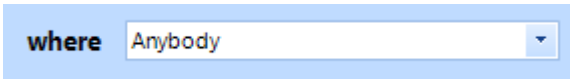
defines the date that the report starts (Example ignore dates, start of last month or 1st January 2016)



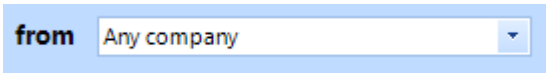
defines the date that the report ends (Example today or end of last month)



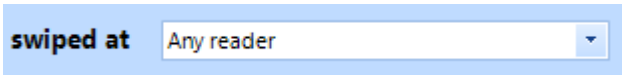
defines which events are to be reported on, Access Allowed and/or Access Denied and any combination of events from the drop down list . The Tick selects all events in the dropdown list and the Cross deselects all events in the dropdown list.



defines which user/s to report on

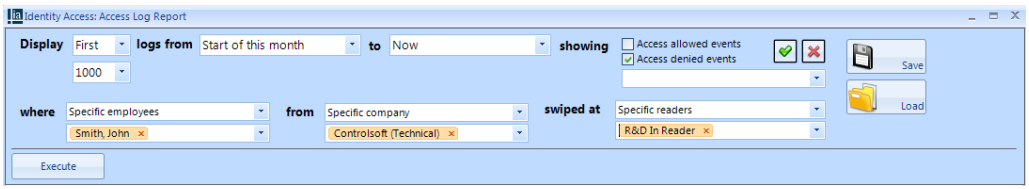


defines which Companies and Departments to report on



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:



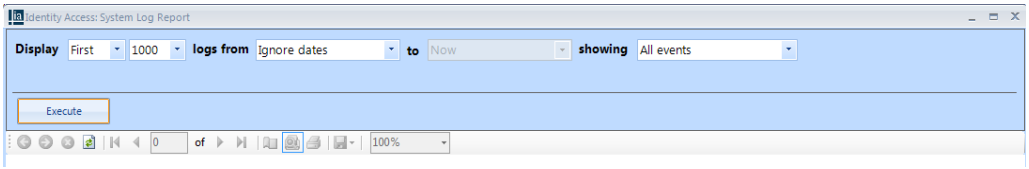
Once configured, click the **[Execute]** button to generate the report.

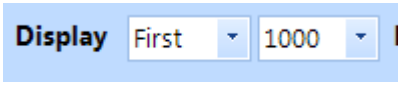
To run a report on a specific person it is also possible to go to **Management** and **Employee** / **Visitor** / **Contractor** (depending on who you wish to run your report on). Highlight the user by left clicking their entry and click the  icon. This will automatically generate a report for this specific 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.

17.3 System Log Reports

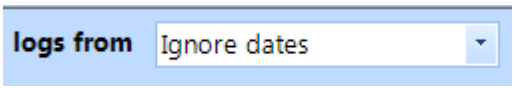
The System Log report is a record of all Identity Access system events, such as when people have logged on / off the software, when doors have been forced open or when database entries have been modified. The System Log Report menu can be accessed by selecting **Reporting** and **System Log.**

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

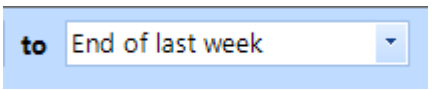




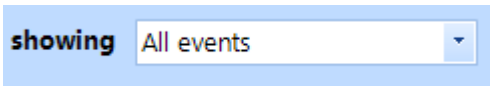
defines whether the report contains All events or the First or Last 100/500/1000/5000 events in the log.



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



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



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

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

17.4 Fire Rollcall Report

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

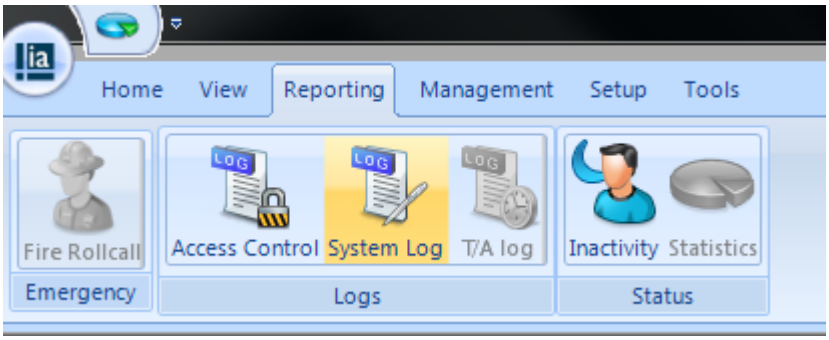
When generating a Fire Rollcall report, no configuration is required, simply click the Fire Rollcall button 

NOTE: The Fire Rollcall report is Not available in Identity Access unless an Identity Access Professional license is applied (part number IA-PRO).

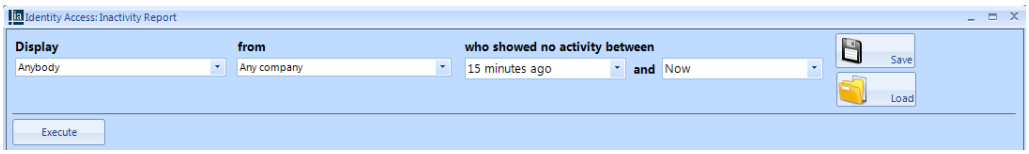
17.5 Inactivity Report

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

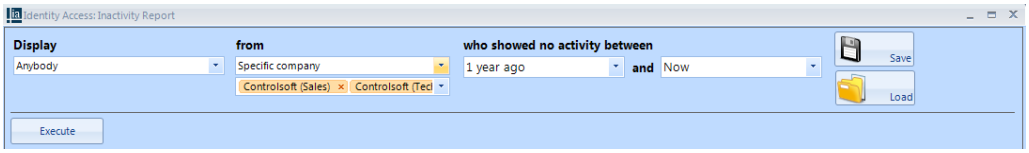


Display - selects specific users to report on

from - selects specific Companies and Departments to report on

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

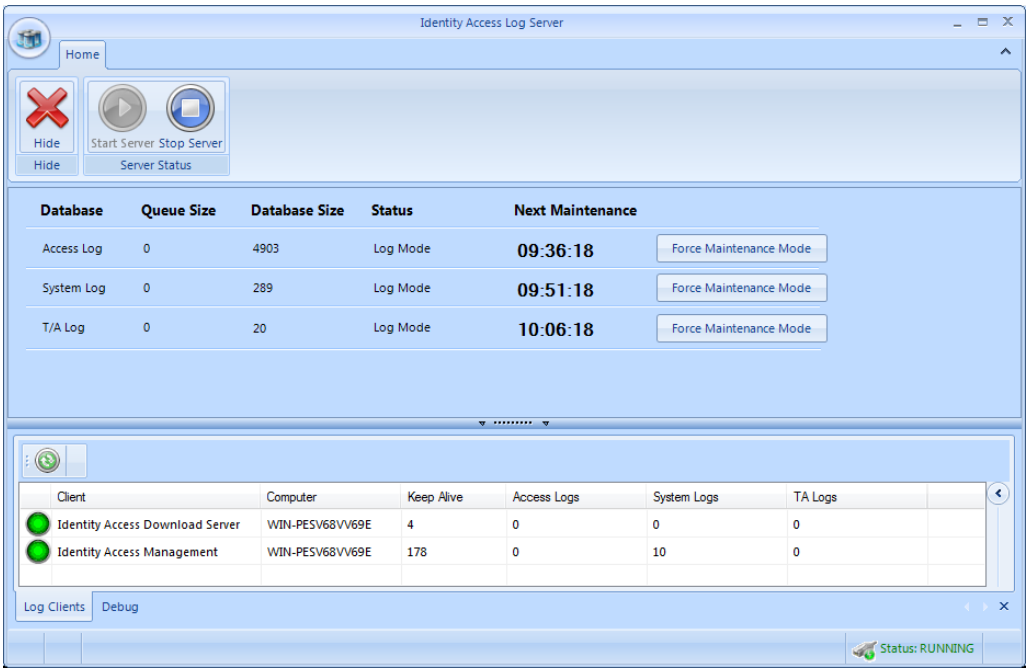
EXAMPLE: to report inactivity on anyone in Controlsoft Sales or Technical within the past year, the report configuration would look as follows:



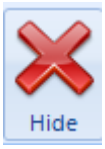
Log Server

18 Log Server

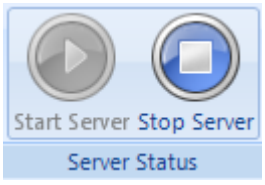
The **Log Server** accepts events from the Download Server and stores them in the SQL database. To access the Log Server, right click on the Log Server icon in the notification area and select **Show** then enter your username and password to access the software (Administrator users only):



The option buttons are:



Closes the Log Server.

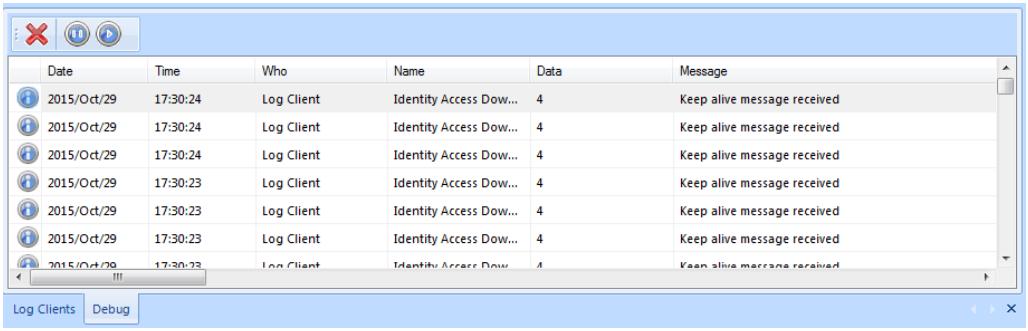


Starts and Stops the Log Server

The upper window shows the size of the Access, System and T&A database and queues and when the next system maintenance is due.

The **Log Clients** window shows devices connected to the Log Server, in this instance the Download Server and the Identity Access User Interface (both installed on the PC named WIN-PESV68VV69E)

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



Download Server

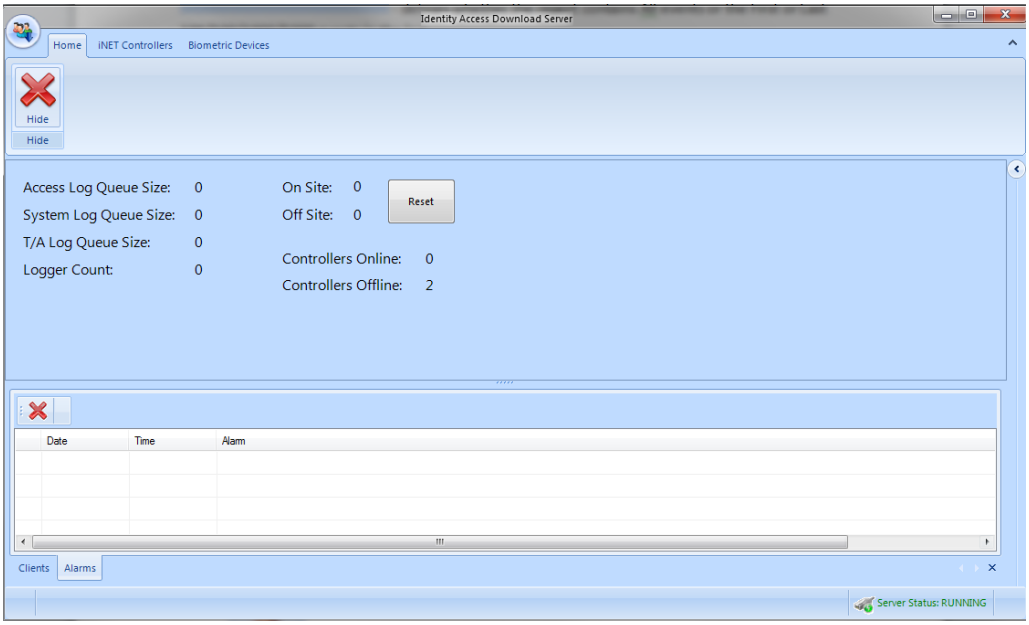
19 Download Server

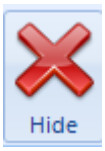
The **Download Server** handles all the communications between the Identity Access software and the Master i-Nets. To access the Download Server right click on the Download Server icon in the notification area and select Show, then enter your username and password (Administrator users only):

The Download Server has 3 tabs, **Home**, **i-Net Controllers** and **Biometric Devices**.

19.1 Home

Select the **Home** tab:





Closes the Download Server.

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 Server.

To the right of the log summary 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

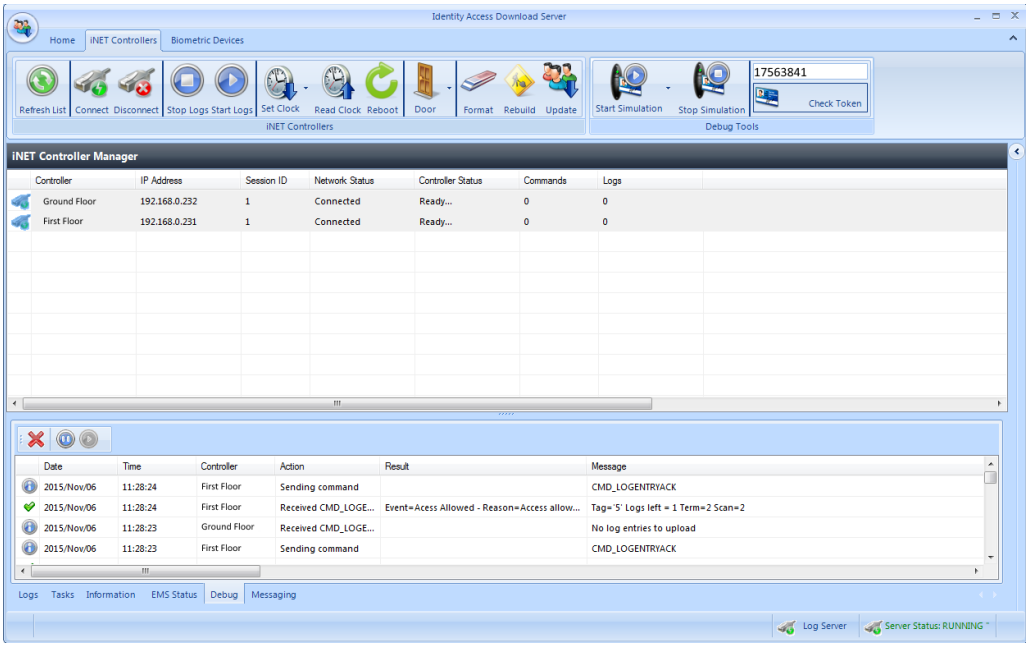
building. These counters can be reset to zero at any time by clicking the [Reset] button.

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

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

19.2 i-Net Controllers

Select the **i-Net Controllers** Tab**:**



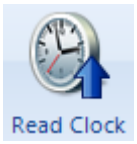
The icons available are as follows:

 Refresh the list of i-Net controllers

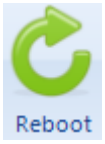
Connect or disconnect the selected controller/s in the list

Stop and start logging events for the selected controller/s

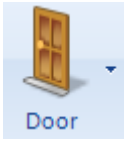
Set the clock in the selected i-Net controller/s. The dropdrown list allows the i-Net clock to be set to **Current Time** or **Custom Time**



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

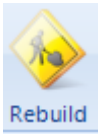


Reboots the selected controller/s



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

Clears the database in the selected controller/s

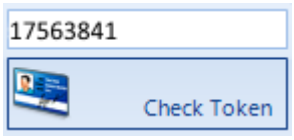


Downloads configuration data and user database to the selected controller/s

Downloads the most recent changes to the selected controller/s

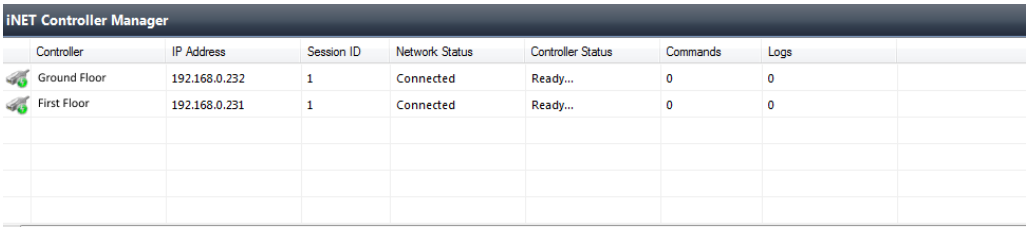
If **Show Debug Tools** is enabled in the Server Configuration utility, the following options will also be visible:

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



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

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



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

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

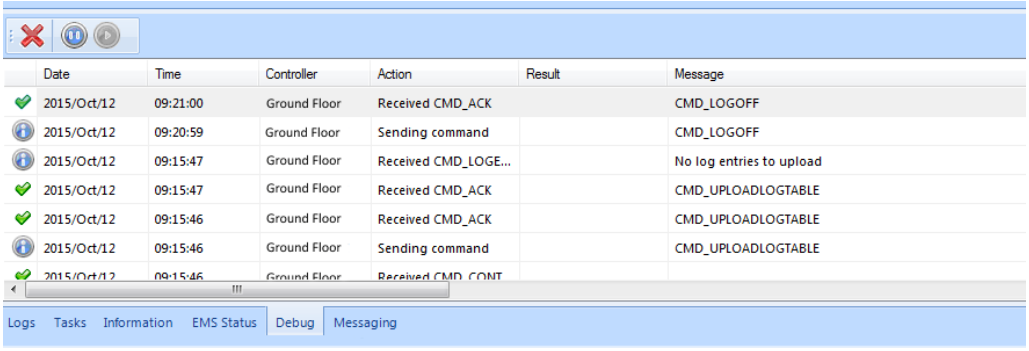
Session ID indicates if software is connected and communicating with the controller

Controller Status indicates whether the controller is "**Ready...**" to accept commands, or **Idle** (can be pinged but unable to accept commands)

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

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

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



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

Tasks: Displays commands issued to the controller awaiting completion

Information:

EMS Status: Displays the web page of the selected i-Net controller (see Appendix D - i-Net webpage) 224

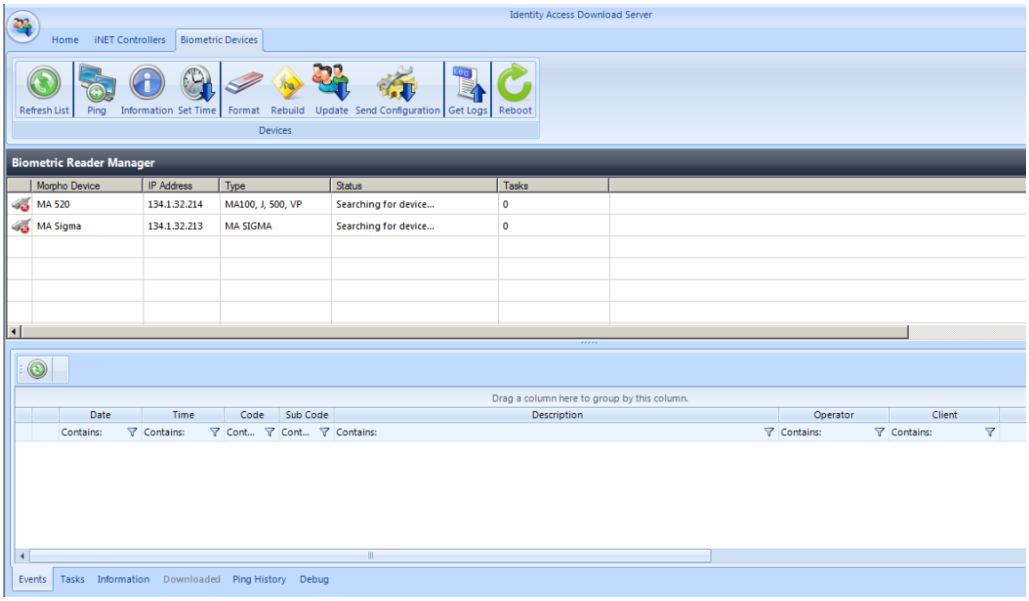
Debug: Displays commands and data being transmitted between the software and the controllers.

Messaging: This tab is for Controlsoft use only

19.3 Biometric Devices

NOTE: The Biometric Devices tab is only displayed if an Identity Access Professional license (Part Number: IA-PRO) is installed.

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



The icons available are as follows:

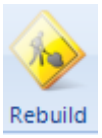
 Refreshes the screen to display the latest data

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

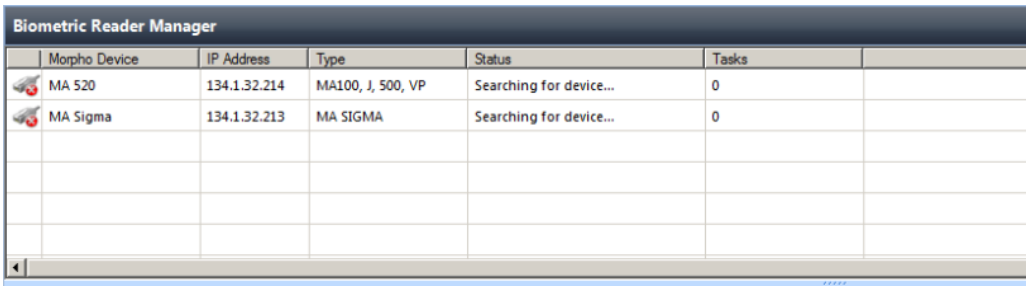
Sends most recent changes to the selected Morpho Reader/s

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:

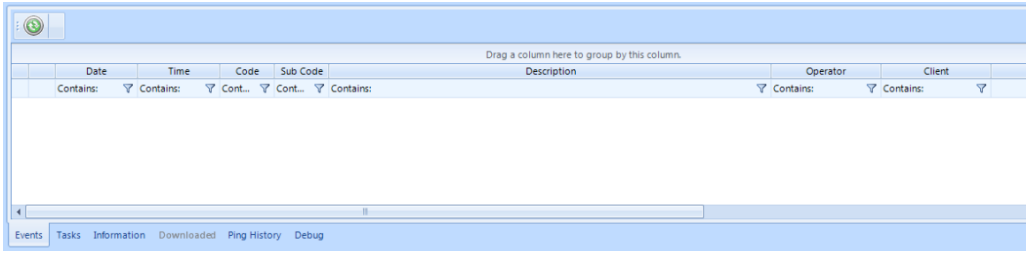


Morpho Device and **IP Address** shows the name and address of the reader as configured in Identity Access

Type shows the type of reader (e.g. J-Bio)

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

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



Events: Event logs as they are received by Download Server

Tasks: Tasks waiting to be sent to the reader

Information:

Downloaded: Data downloaded from the reader

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

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

Appendix A - Types of Door

20 Appendix A - Types of Door

Within the Identity Access software, it is possible to select 3 types of door, namely Normal Door, Airlock and Turnstile.

NOTE: To use Turnstiles or Airlocks, Identity Access Professional is required.

20.1 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 after contact release: 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.

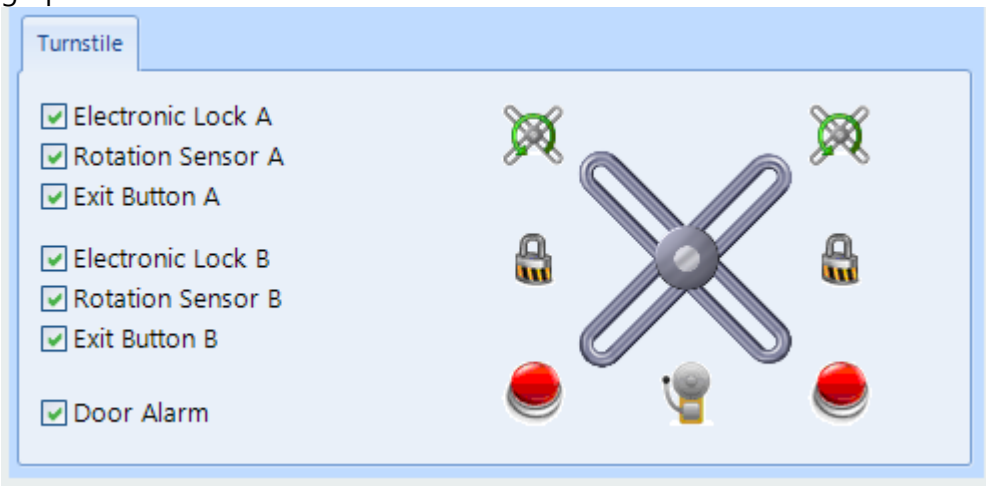
Exit Button: A Request to Exit (REX) button can be used to release the door from within the protected area. A REX is not required if the door uses an IN and an OUT reader. The Identity Access system

supports 2 REX buttons, 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. The relay output can be programmed for Normal or Inverted operation for maximum flexibility in the choice of sounder.

20.2 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

20.3 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:

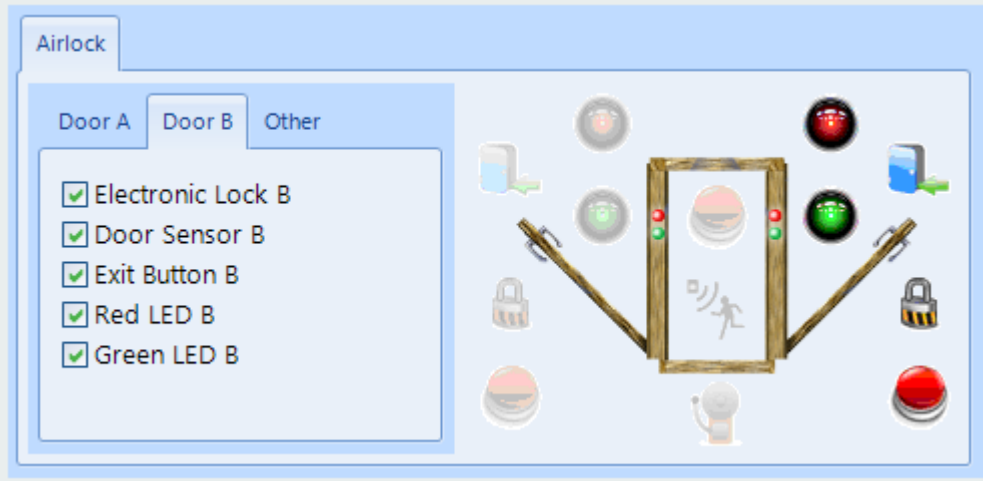
 **Electronic Lock A** defines the output that controls the lock

 **Door Sensor A** defines the input that monitors the door contact which detects when the door has been opened

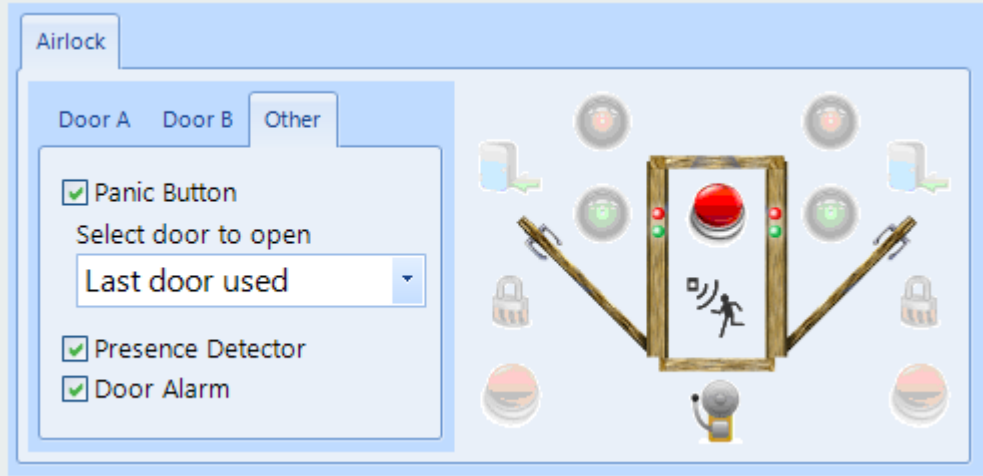
 **Exit Button A** defines the input that monitors the Request to Exit button to release the door

 **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)

Appendix B - HID Asure ID Software

21 Appendix B - HID Asure ID Software

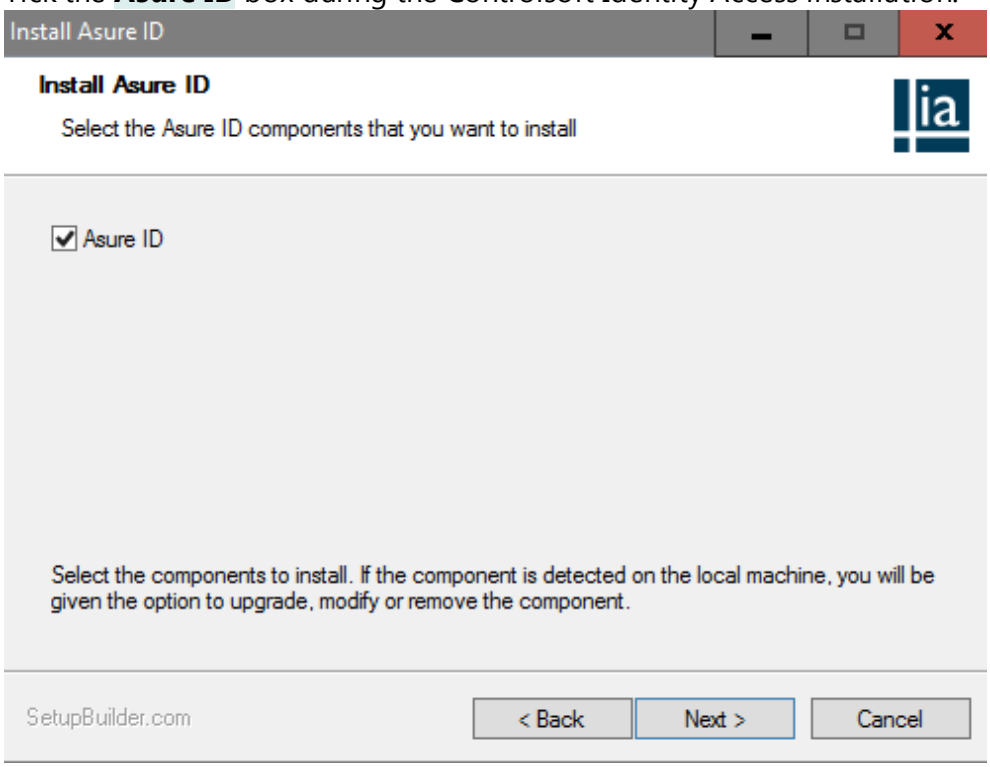
The Controlsoft Identity Access install flash drive includes a copy of HID Asure ID® 7. This is an ideal choice for organizations looking for an affordable and easy-to-use photo ID card software with direct integration with the Controlsoft Identity Access database.

Asure ID Enterprise has additional features like compound data fields, batch printing, conditional design and print rules, and password protection.

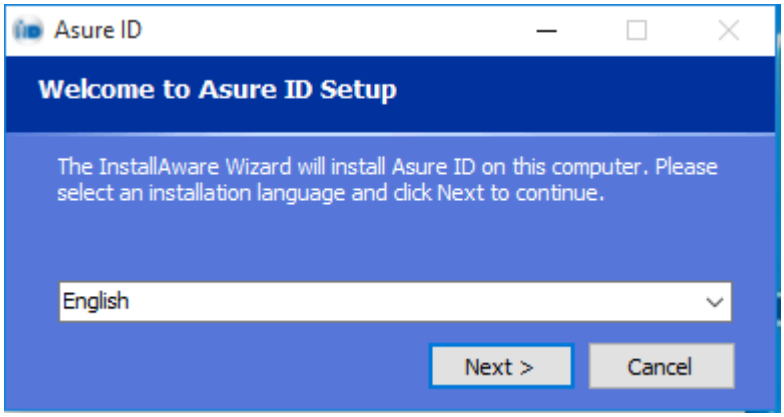
NOTE: The copy of Asure ID supplied with Identity Access is a 30 days trial copy. To use Asure ID beyond the 30 day trial period, you will require a license. Please contact your vendor for further details.

To install Asure ID:

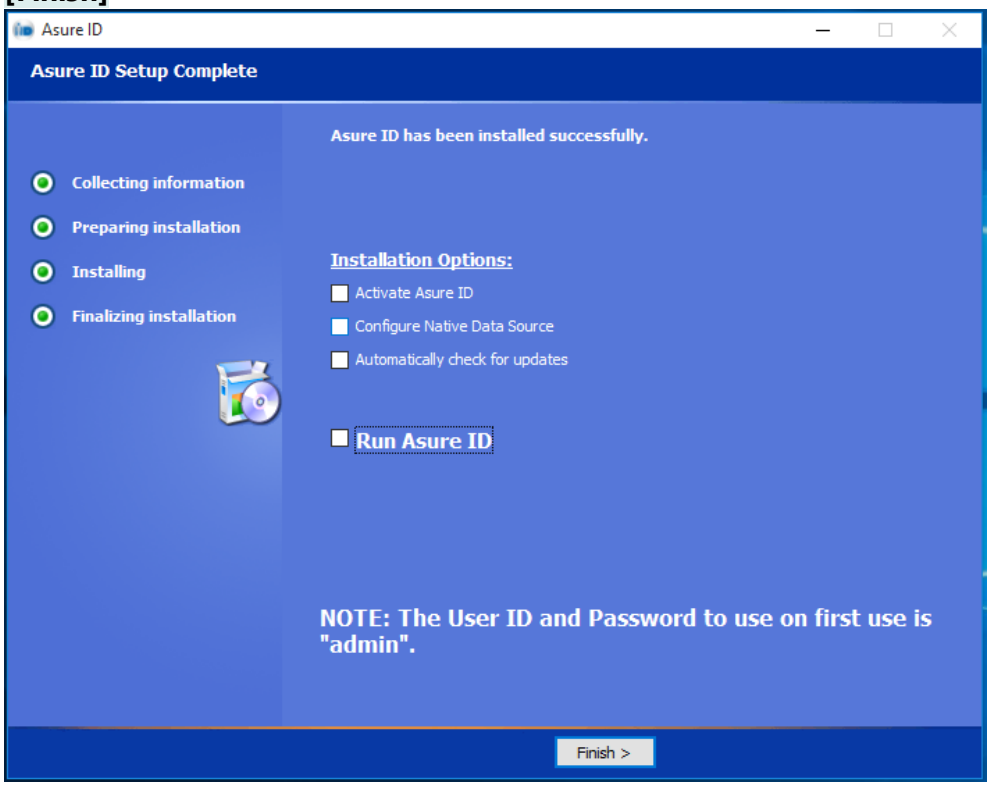
1. Tick the **Asure ID** box during the Controlsoft Identity Access installation:



2. The AsureID setup will start. First, select the Language you require:



3. Click **[Next]**, then read and **[Accept]** the License Agreement
4. Select where the Files are to be installed, then click **[Next]**
5. Following the installation, untick all **Installation Options** and click **[Finish]**



6. The Controlsoft Identity Access Installation will then continue

To configure Asure ID

Run the IA Client 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.

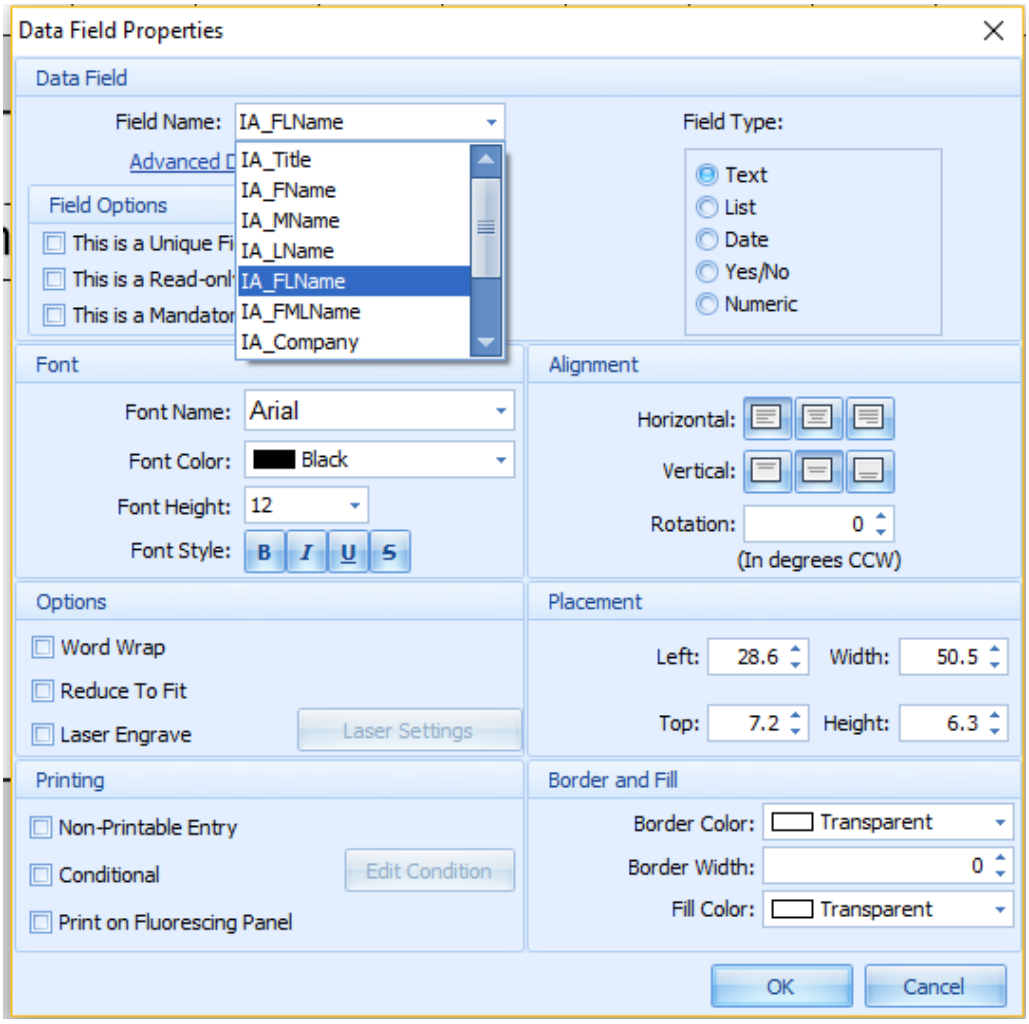
Card Designer Field Mapping is a list of fields that are configured to work between Controlsoft Identity Access and AsureID. The Names in this list should not be changed.

Register copy of Asure ID is used to license the copy of Asure ID. Add the License Key and Details into the relevant boxes and click **[Register]** (this option is only available when the PC is connected to the internet)

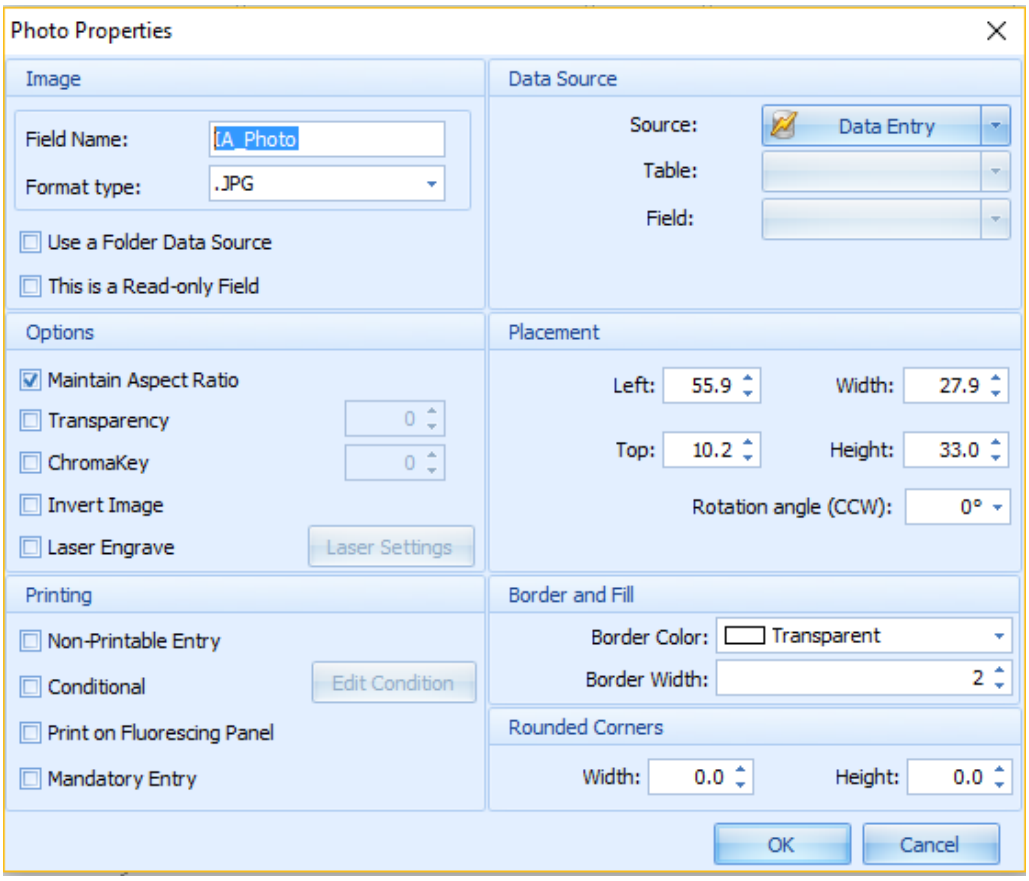
Asure ID Card Designer

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.



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** .



For further detailed information on how to use Asure ID, please refer to the HID documentation installed with the software.

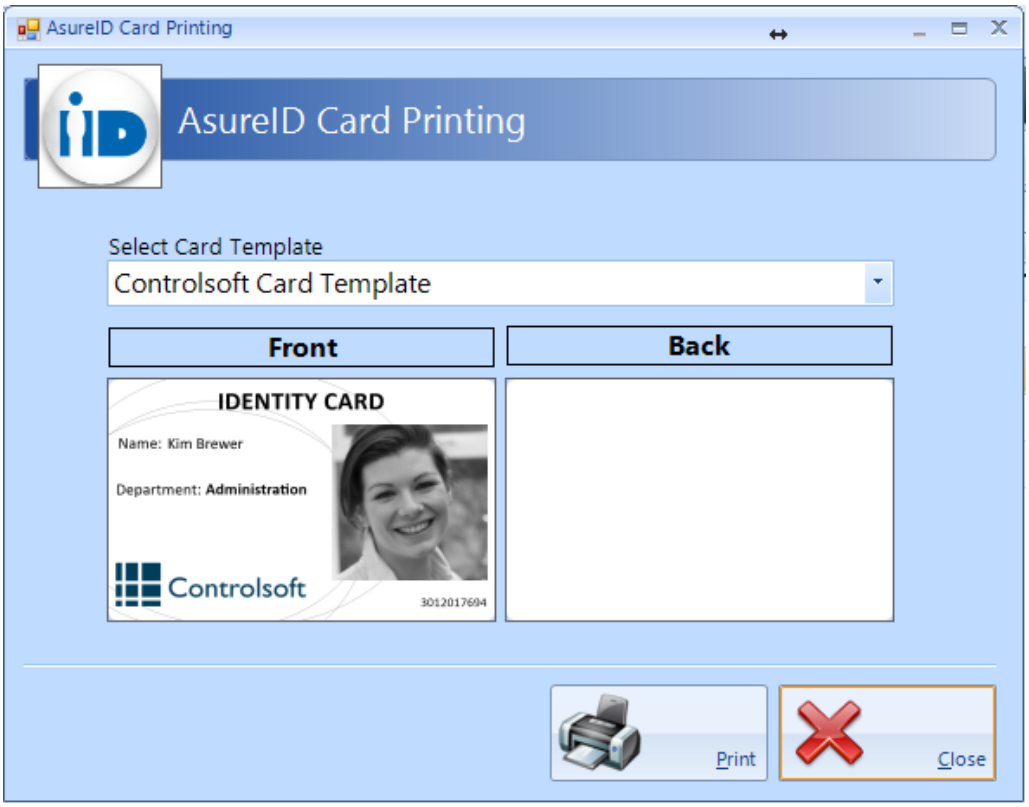
Once you have completed your card design click on **File** and **Save Template**. Exit the AsureID Card Designer, then restart the Identity Access User Interface.

Select Users and Print

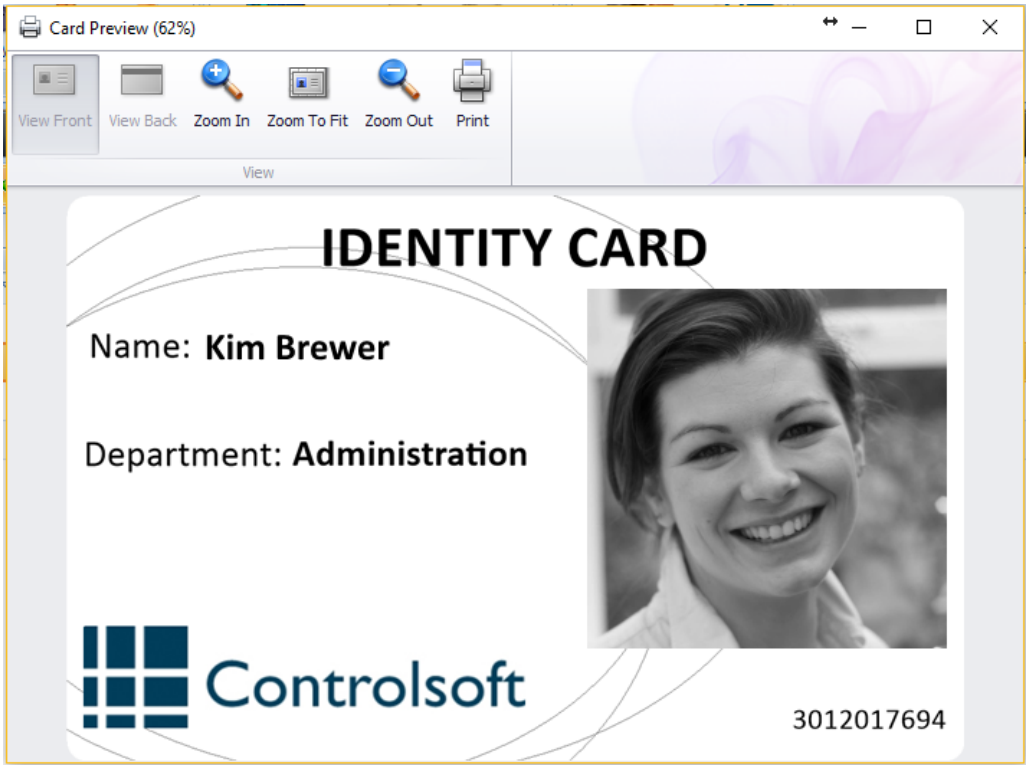
To Print a card from within Identity Access, select **Management** then Select **Employee** / **Visitor** / **Contractor** as appropriate.

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 and select **Print**



Click **[Print]** and select the required Printer.



Appendix C - Windows Commands

22 Appendix C - Windows Commands

To access Windows **Control Panel**

Windows 7 – Click the **Start** button, and select **Control Panel**

Windows 8.1 – Right click the **Start** button and select **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 7 – Click the **Start** button, click in the **Search programs and files** field, type `cmd` and select **cmd.exe**

Windows 8.1 – Place the cursor in the bottom right hand corner of the screen, select **Search**. Type `cmd` in the field and select **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**

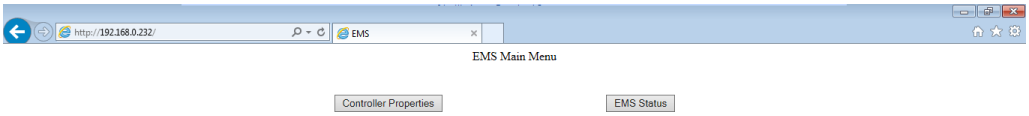
Windows Server 2012 – Place the cursor in the bottom right hand corner of the screen, select **Search**, type `cmd` in the text field and select **Command Prompt**

Appendix D - i-Net webpage

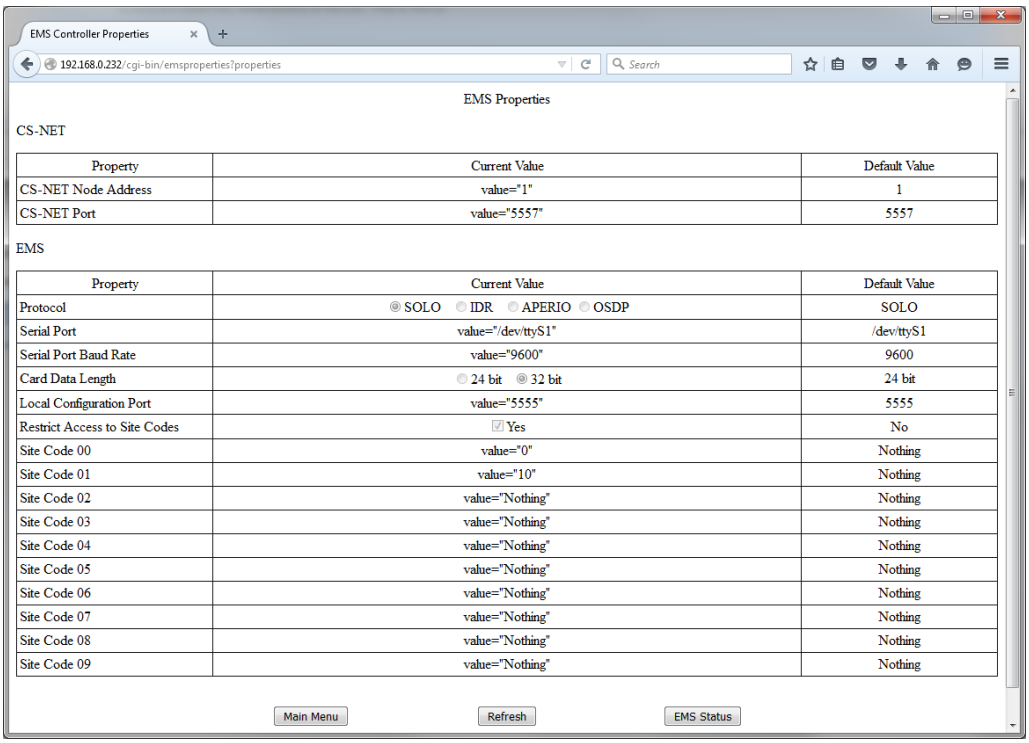
23 Appendix D - i-Net webpage

The i-Net 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 screen from firmware version 98.33.21.9 (the oldest version fully compatible with Identity Access software).

To access the webpage, use any browser (e.g. Internet Explorer, Firefox, Chrome) and enter the i-Net's IP Address. The landing page displays the options available:



Click the **[Controller Properties]** button:



This screen displays the configuration details of the i-Net ***NOTE - These parameters cannot be changed in the webpage, but can be changed from within the i-Net Configurator software***: (see IP Controller Configurator) 116

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 i-Nets connected as Master / Slave and for Master i-Nets connected to Expanders. **IDR** is only used with

legacy equipment. The **APERIO** option should not be used. Use **OSDP** when using a Master i-Net with HID OSPD readers

Serial Port: This must be at its default setting unless instructed otherwise by Controlsoft Technical Support

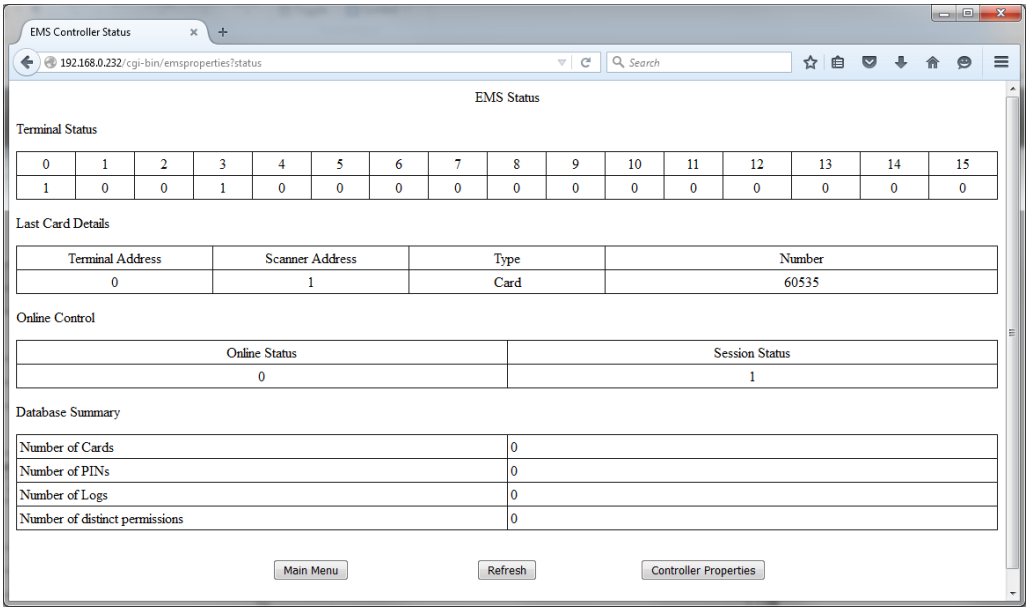
Serial Port Baud Rate: This must be at its default value, unless using the **IDR** or **OSDP** protocols. For **IDR**, the baud rate should be set to 19200. For **OSDP**, the baud rate should be set to 115200.

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.

Click on **[EMS Status]** to view the status of the controller:



Terminal Status displays the devices connected to the i-Net's RS485 bus. In this example, we have device address 0 (the Master i-Net itself), and a device with address 3.

Last Card Details shows information on the last number read by the system. **Terminal Address** is the address of the device that read the number (0 being the Master i-Net), **Scanner Address** is the Reader Port that the data came

through, **Type** indicates whether the data is from a card or a PIN, and **Number** indicates the card number / PIN read.

Online Control indicates whether the Master i-Net is in "online mode". **Online Status** will show a '1' if Controlsoft Pro is connected in online mode, or a '0' if used with Identity Access or Controlsoft Lite. **Session Status** will show a '1' if Identity Access, Controlsoft Pro, or Lite is connected.

Database Summary displays an overview of the configuration of the i-Net, the **Number of Cards** and **Number of PINs**, the **Number of Logs** waiting to be uploaded and the **Number of Distinct Permissions** (if everyone has access to all readers all the time, this is 1 distinct permission. If someone is then given access through 1 door in the mornings only, this will be a second distinct permission)

NOTE: These displays are not live. To update the screen, simply press the* [Refresh] *button

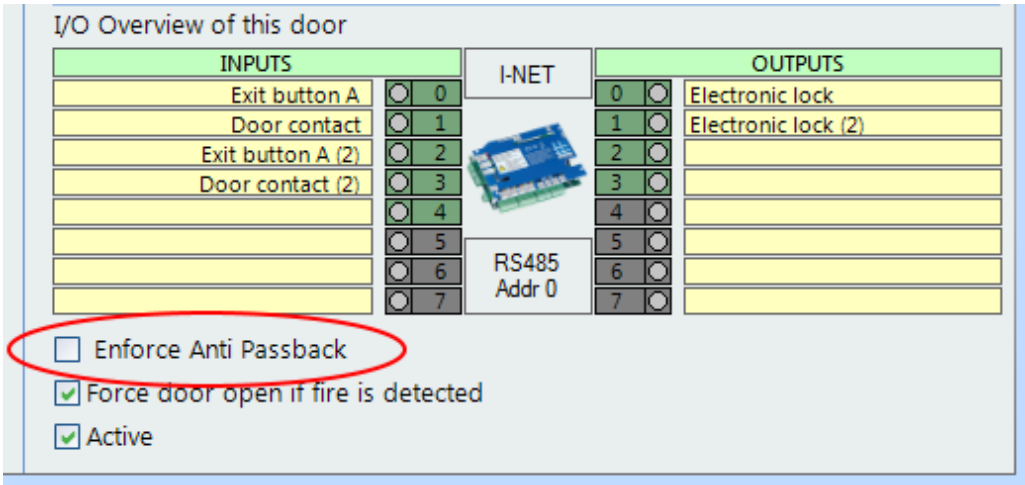
Appendix E - AntiPassBack

24 Appendix E - AntiPassBack

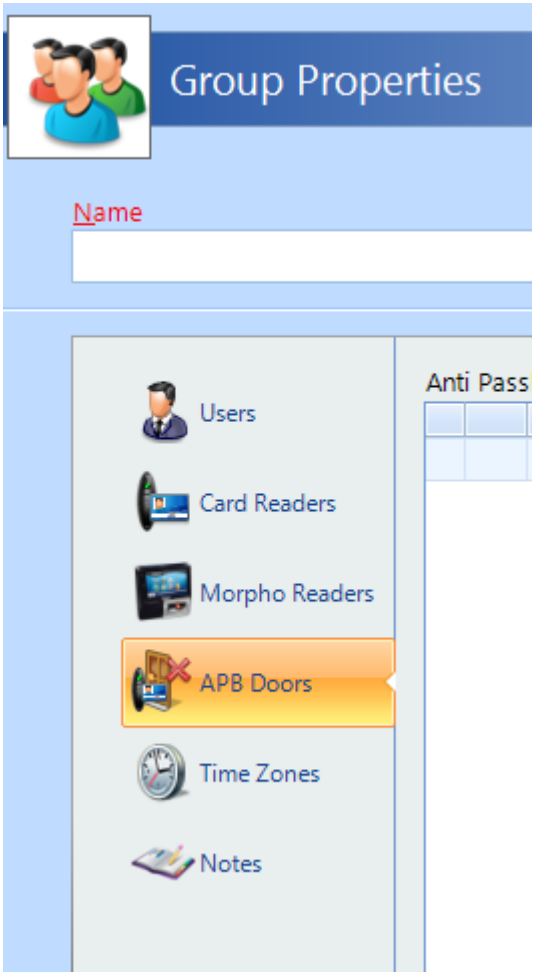
AntiPassBack is a feature available in Identity Access when the Professional Features License is installed which prevents illegal card movement when entering the building.

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, the system will deny access.

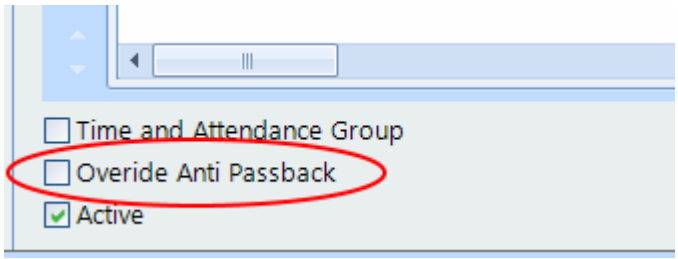
To use this feature, enable AntiPassback for each external door,



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 **Overide Anti Passback** for that Group.



NOTE: While the system supports AntiPassBack across doors on the same Master Controller, Identity Access does not support AntiPassBack across doors controlled by different master Controllers.

Appendix F - i-Net Configurator

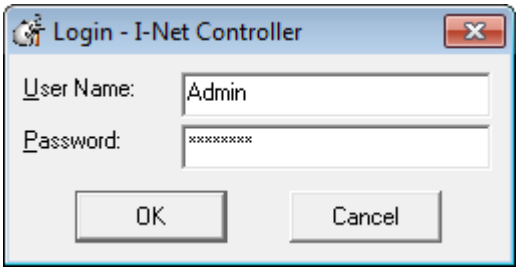
25 Appendix F - i-Net Configurator

i-Net Configurator is a small utility required to configure the internal settings of the i-Net controller. i-Net Configurator is installed automatically with Identity Access software.

Running i-Net Configurator

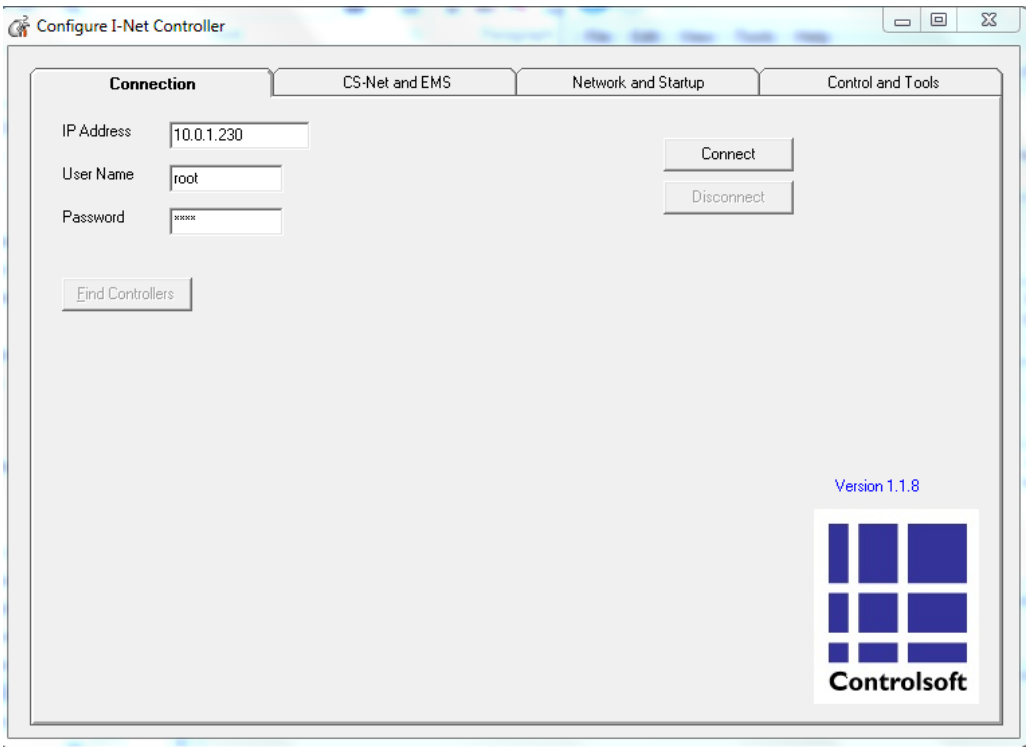
To run the i-Net Configurator software, select
Start > **All Programs/Apps** > **Controlsoft** > **Identity Access** > **Tools** >**i-Net Configurator** > **i-Net Configurator**

The login screen will then be displayed:



NOTE: The default login credentials are Username = Admin, Password = Password
These login credentials are case sensitive.

CONNECTION TAB



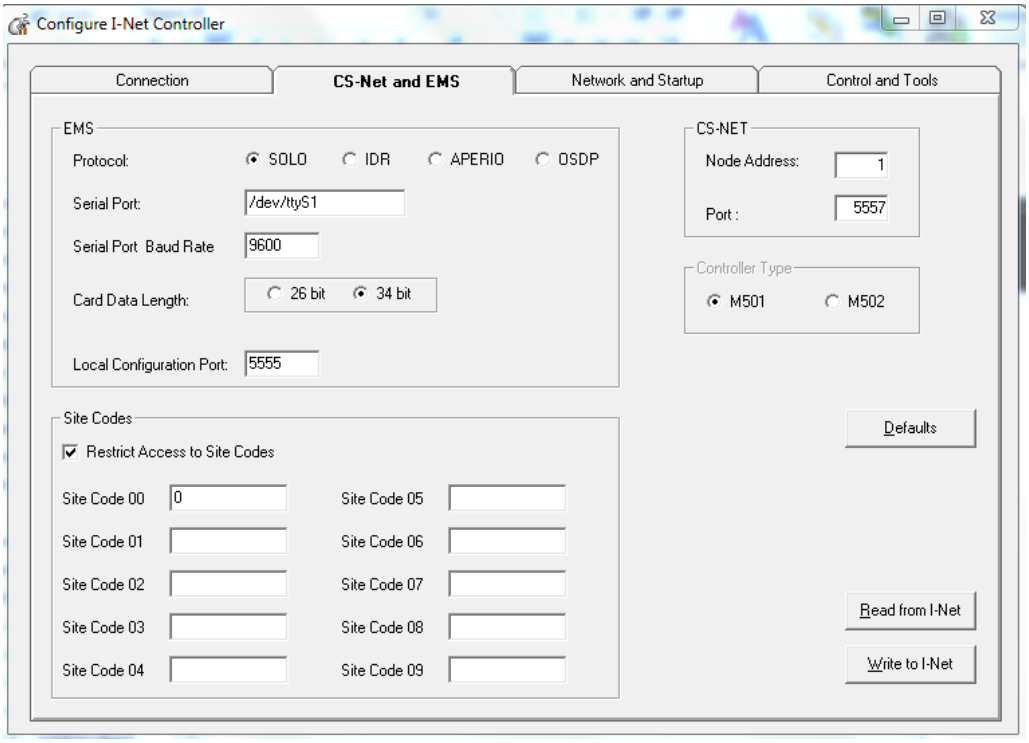
Enter the **IP Address** of the i-Net controller to be configured ***(NOTE: the default IP Address for an i-Net controller is 10.0.1.230)***

The **User Name** of the i-Net controller is 'root', this must not be changed

The **Password** for the i-Net controller must not be changed, unless you have previously altered this within the i-Net. If you clear this field, simply close i-Net Configurator and run it again.

Once the IP Address has been entered, click on **[Connect]** and wait for the [Connect] button to grey out and the **[Disconnect]** button to show as live.

CS-NET AND EMS TAB



This tab is used to select a variety of options within the i-Net controller.

EMS:

- **Protocol** – this defines the type of expansion hardware connected to the i-Net RS485 bus.
    - **SOLO** is the standard protocol used for slave i-Nets and slave AC-3151 or AC-4311 expanders
    - **IDR** is a legacy protocol used for AC-430x slave controllers.
    - **Aperio** – this option is not currently available.

- **OSDP** is the protocol required to communicate with HID OSDP readers connected to the i-Net RS485 bus

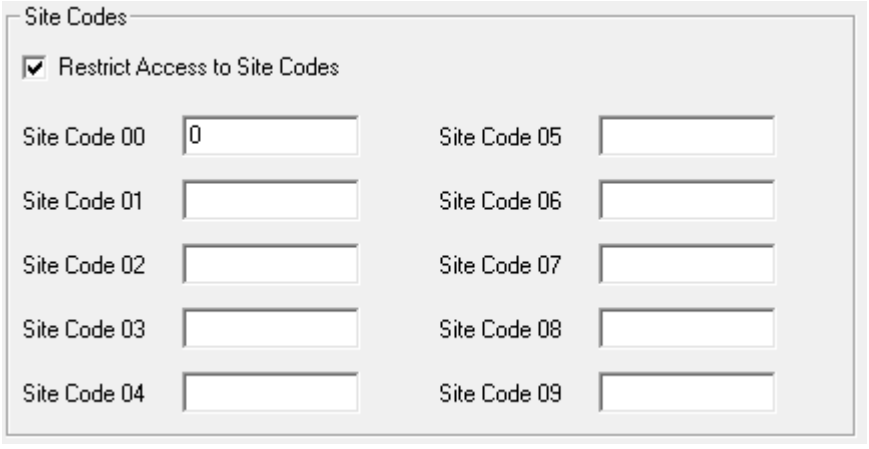
- **Serial port** – the default for this is /dev/ttyS1 and should not be changed unless instructed to do so by Controlsoft Technical Support.
- **Serial port baud rate** is the connection speed used on the RS485 bus. This should be set to 9600 for the SOLO protocol, 19200 for IDR or 115200 for OSDP
- **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 34 bit, the full card number (e.g. 34-bit, 47-bit, 56-bit) will be used.
- **Local configuration port** is set to 5555 by default and must not be changed unless instructed to do so by Controlsoft Technical Support.

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 i-Net 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 i-Net 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 i-Net controller can support up to 10 different site codes simultaneously. For example, to use cards with site code 10 and cards with site code 23, the i-Net should be configured as follows:



(NOTE: Most sites will only use one site code)

CS-NET

- **Node address** and **Port** are only applicable when using Controlsoft Professional software, and should not be changed when using Controlsoft Identity Access or Lite software. For further information on these settings, refer to the Controlsoft Professional documentation

CONTROLLER TYPE

This is an indication of the type of i-Net used and cannot be changed.

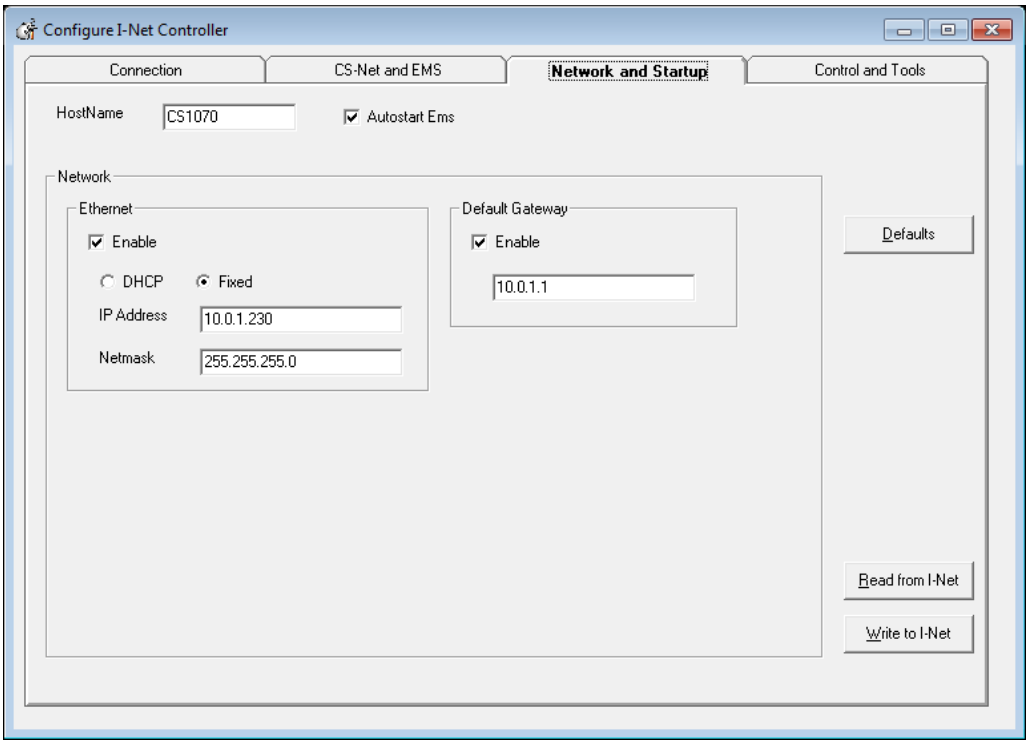
- **M501** refers to the processor board used in version 1 i-Net controllers (production units up to Q2 2016)
- **M502** refers to the processor board used in version 2 i-Net controllers (production units after Q2 2016)

[Defaults] – click this button to set all parameters to default values.

[Read from i-Net] – click this button to read all values from the i-Net controller

[Write to i-Net] – click this button to write all values to the i-Net controller

NETWORK & STARTUP TAB



Hostname will be filled in automatically when the software connects to the i-Net controller

Autostart EMS – ensure that this option is ticked when the software is connected to the i-Net controller

ETHERNET:

- **Enable** – ensure that this option is ticked
- **Fixed** – ensure that this radio option is selected. Controlsoft strongly recommend that you do NOT use DHCP
- **IP Address** – Enter the fixed IP Address for the i-Net controller. The customer's IT Department should advise on the IP Address to use.
- **Netmask** – Enter the netmask for the i-Net controller. The customer's IT Department should advise on the netmask to use.

DEFAULT GATEWAY:

- **Enable** – ensure that this option is ticked
- **Gateway** – Enter the gateway for the i-Net controller. The customer's IT Department should advise on the gateway to use

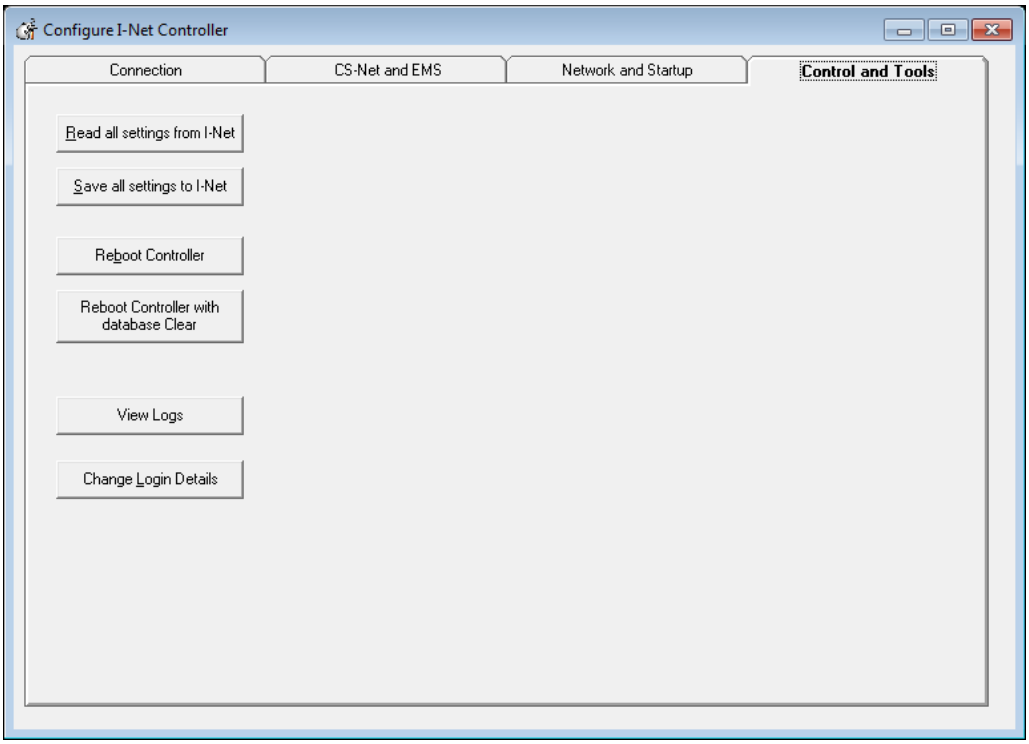
[Defaults] – click this button to set all parameters to default values.

[Read from i-Net] – click this button to read all values from the i-Net

[Write to i-Net] – click this button to write all values to the i-Net controller

NOTE: when changing the IP Address, the i-Net controller must be rebooted AFTER writing the settings to the i-Net. This can be done by selecting the Control and Tools tab and clicking on Reboot Controller.

CONTROL & TOOLS



[Read all settings from i-Net] – click this button to read all settings from the i-Net controller

[Save] – click this button write to all settings to the i-Net controller

[Reboot controller] – click this button to reboot the i-Net controller

[Reboot controller with database clear] – click this button to reboot the i-Net controller and clear its internal database

[View logs] – click this button to view data transmitted from the i-Net controller

[Change login details] – click this button to change the login credentials for i-Net Configurator software ***(NOTE: the default credentials are username = Admin and password = Password)***

Appendix G - Product History

26 Appendix G - Product History

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 62 (requires i-Net firmware v98.34.21.9 or later)
- "Tag Valid From" can now be set to the nearest minute
- Supports "Latched" door operation (requires i-Net firmware v98.34.21.9 or later)
- Data transfer speed increased during Uploads and Downloads (requires i-Net 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:

- License 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:

- License Manager added
- Airlocks
- AntiPassBack
- Fingerprint Enrolment (a Morpho MACI license will also be required)
- Fire Alarm Rollcall report
- Time Sheet Reports
- Turnstiles
- Integration with Asure ID (an HID license will also be required)
- Integrated issuance of HID Mobile Access credentials
- Identity Access Express withdrawn

NOTE: To upgrade a copy of Identity Access Express to v2016.2:

1. Install Microsoft SQL Management Studio 2014 (available from www.controlsoft.com) and backup the LocalDB database
2. Uninstall Identity Access v2016.1, then install Identity Access v2016.2 (available from xxx.controlsoft.com)
3. Use Microsoft SQL Management Studio 2014 to restore the original database

v2016.1 - Initial Release

Appendix H - Downloading Software

27 Appendix H - Downloading Software

Identity Access software can be downloaded for free from the Controlsoft website 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 - everything required required for a basic Identity Access installation, including the server software, SQL Express and manuals,

Identity Access Client - files required to install a Client and manual

Identity Access Extras - additional files for enrolment reader, videos, i-Net Configurator (standalone version), Morpho Toolbox and database backup software,

Identity Access SQL Management Studio - Microsoft software for advanced users to restore database backups.

Identity Access Update - files to update an exiting installation to the latest version

Download the required zip file and save it on the root of your hard drive (C:\ ). Extract the files to the root of your hard drive (C:\ ) and run the required software.

NOTE: Do not extract the software from the Downloads folder of your PC as this can cause problems with the subsequent installation. Always save the downloaded file on the root of the hard drive (C:\ )

It is possible to download all the zip files and recreate an IA-STD flash drive as follows:

1. Download Identity Access Server, Client, Extras and Management Studio and save them all on the root of your hard drive (C:\ ).
2. Extract each zip file to the root of your hard drive (C:\ ), which will build up the file structure in a new folder called IA_STD followed by the version number.

3. Save all the files in this new folder to the root of a flash drive or USB hard drive.
4. You can now use this drive for further installations.

NOTE: Always check the website periodically for new releases of Identity Access software.

Appendix - Glossary

28 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 i-Net via the RS485 245 bus.

AC-4311 - An I/O Expander Board providing 8 inputs and 8 output relays. The AC-4311 connects to the Master i-Net via the RS485 245 bus.

Administrator - An Operator who is authorised to use all functions within the Identity Access software.

Contractor - A temporary User with a token 245 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 i-Nets 244.

Download Server - Software which manages the communications between the Identity Access software and the controllers.

Employee - A User with a token 245 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.

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 i-Net's default IP Address is 10.0.1.230.

i-Net - 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.

Log Server - 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 00:13:48:02:52:D6).
NOTE: MAC addresses for all i-Nets start with 00:13:48:

Manager - An Operator who is authorised to use a subset of the functions within the Identity Access software.

Master i-Net: An i-Net controller connected to the software via an IP connection. ***NOTE: Master i-Nets 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 configured as Administrator 244 or Manager 245.

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 i-Net to Slave i-Nets or Expanders. Each device on the RS485 bus must be configured with a unique address to identify itself.

Slave Expander - A reader expander, I/O expander or reader connected to a Master i-Net 245 via an RS485 245 connection (AC-3151 244 or AC-4311 244).

Slave i-Net - An i-Net 244 controller connected to a Master i-Net 245 via an RS485 245 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 i-Nets 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.