

Step 1. Pre Installation Checks

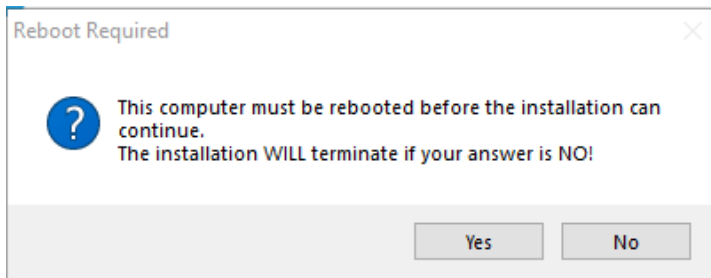
Before you start the installation, it is important to run through the following pre-installation checks.

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

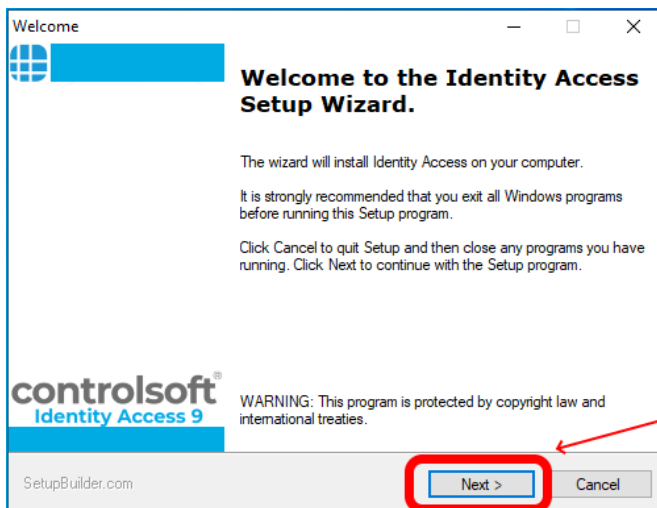
[Click here: for further information on how to perform these checks on the various Windows operating systems.](#)

Step 2. Installing Identity Access Software

- Download the Identity Access Software from our website at www.controlsoft.com/login
- Navigate to your Downloads folder, and double click **Install_IdentityAccess.exe**
- During installation, if prompted to restart the installation click **Yes**.



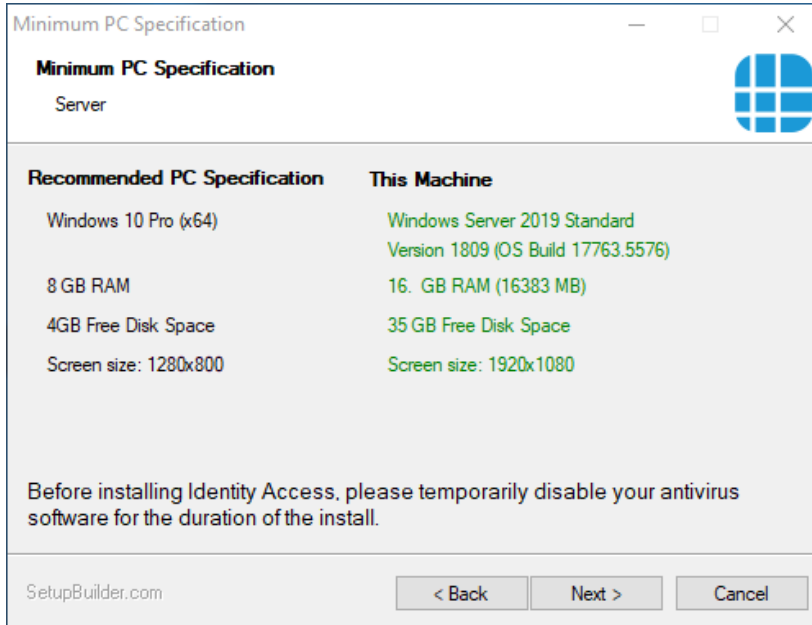
- Once restarted the installation will restart automatically if you are logged in as an administrator. If you are providing administrator details when prompted, you must restart the installation manually from the Downloads folder.



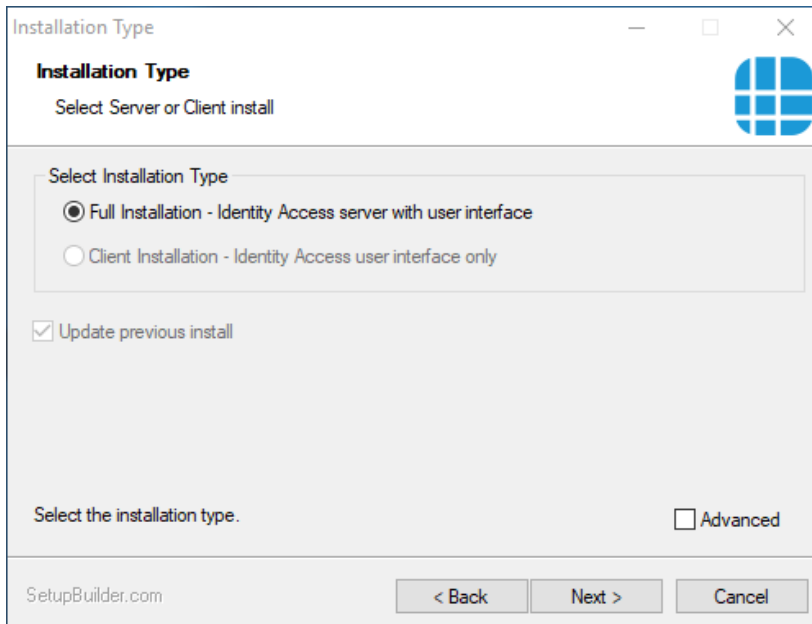
Press [Next] to continue

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

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



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



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

Set Passwords

Set Passwords

Please set the System Integrator and End User Administrator passwords

System Integrator

Username

Password

Confirm Password

Administrator

Username

Password

Confirm Password

Accept

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

Step 3. (Optional) Licensing Identity Access

If you requires a Professional or Enterprise license, [please click here](#). Otherwise go to Step 4.

Step 4. Launching the Identity Access Software

To launch the Identity Access software:

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

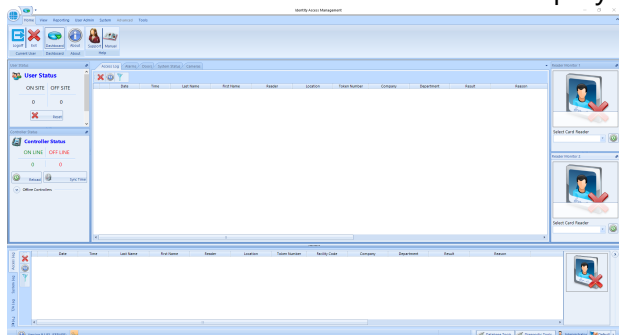
NOTE: The Splash screen may show "**Error: Checking connection to the main database... Retrying**". This is because the SQL 2022 database engine take longer to start. Wait 2 minutes and Identity Access will connect.



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



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



[Further details can be found in the "5.2 The Dashboard" section of the Identity Access Software Guide](#)

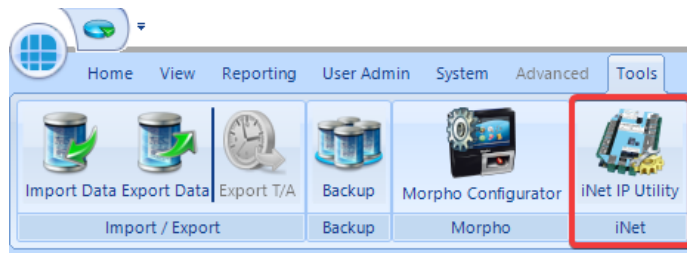
Step 5. Configure IP Controller(s)

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

[Click here if you are plugging an iNet controller directly to the PC.](#)

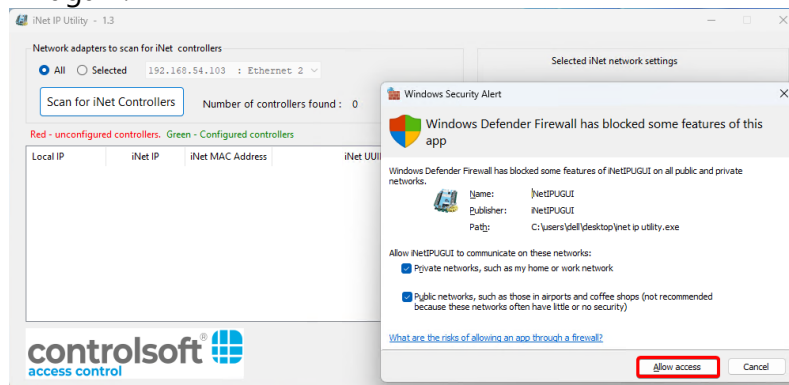
NOTE: If you are unsure what IP Address, Subnet Mask and Gateway the iNets should use, speak to IT.

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

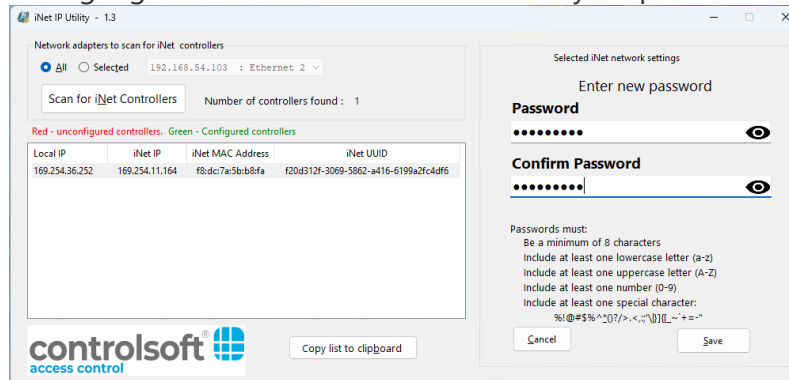


2. Press **Scan for iNet Controllers.**

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



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



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

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

Network adapters to scan for iNet controllers

All Selected 192.168.54.103 : Ethernet 2

Scan for iNet Controllers Number of controllers found : 1

Red - unconfigured controllers. Green - Configured controllers

Local IP	iNet IP	iNet MAC Address	iNet UUID
169.254.36.252	169.254.11.164	f8:dc:7a:5b:b8:fa	f20d312f-3069-5862-a416-6199a2fc4df6

controlsoft®
access control

Copy list to clipboard

Selected iNet network settings

UUID : f20d312f-3069-5862-a416-6199a2fc4df6

IP Address assignment

Dynamic (DHCP) Static

Current Address

IP Address 192.168.54.210

Netmask 255.255.255.0

Gateway 192.168.54.1

DNS Servers

Undo changes Save changes

Note : After saving the changes, the iNet Controller will restart and will take up to a minute before it will respond to Scan requests

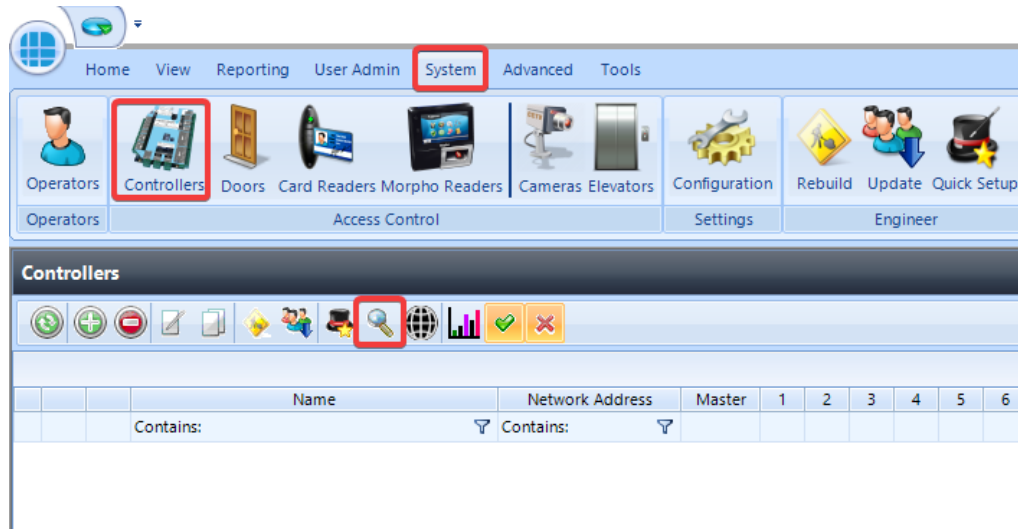
6. Press **Save Changes** and the iNet will set the IP address and automatically restart.

7. Close the iNet IP Utility.

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

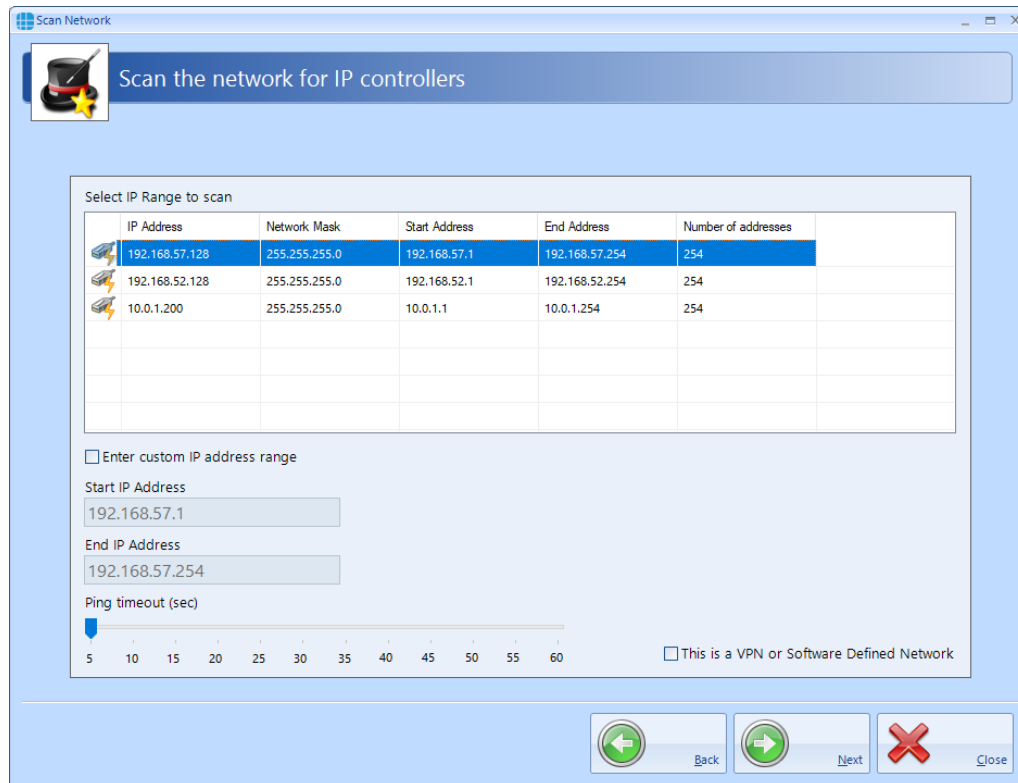
Step 6. Add IP Controller(s)

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

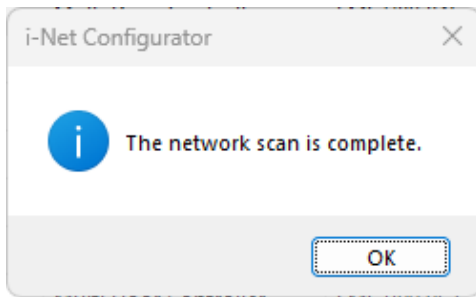


2. Click on the Scan button  then click **[Next]**.

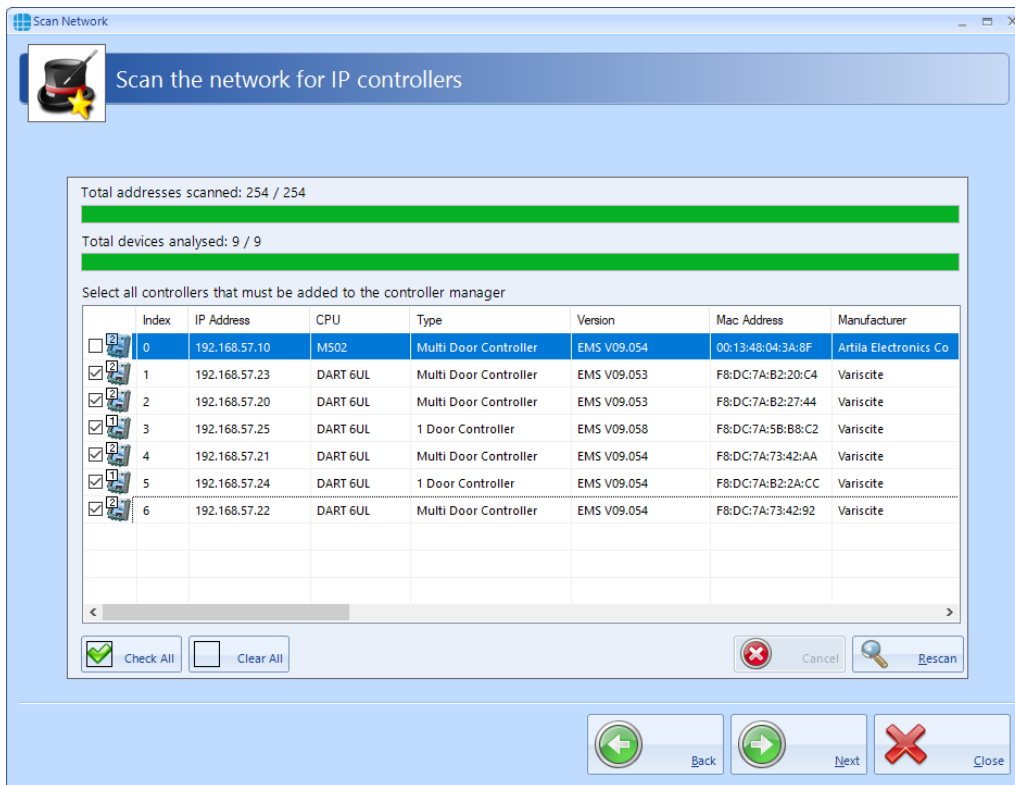
3. If there are multiple network ranges, highlight the network range which has been programmed into the iNet Controller(s) and click **[Next]**



4. Click **[OK]**



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



[For information on manually creating a controller see the "7. System > Controllers" section of the Identity Access Software Guide.](#)

Step 7. Add Downstream RS-485 Controllers

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

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

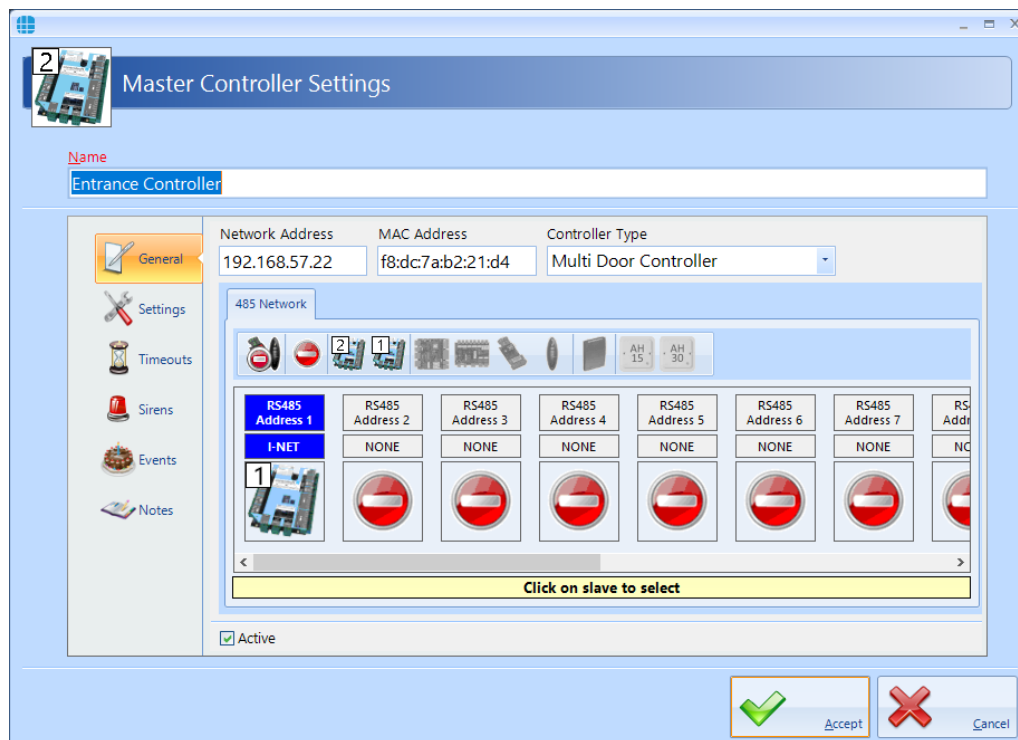


Add a 2 Door iNet to the RS-485 bus



Add a 1 Door iNet to the RS-485 bus

[For other device types see the "7. System > Controllers" section of the Identity Access Software Guide](#)



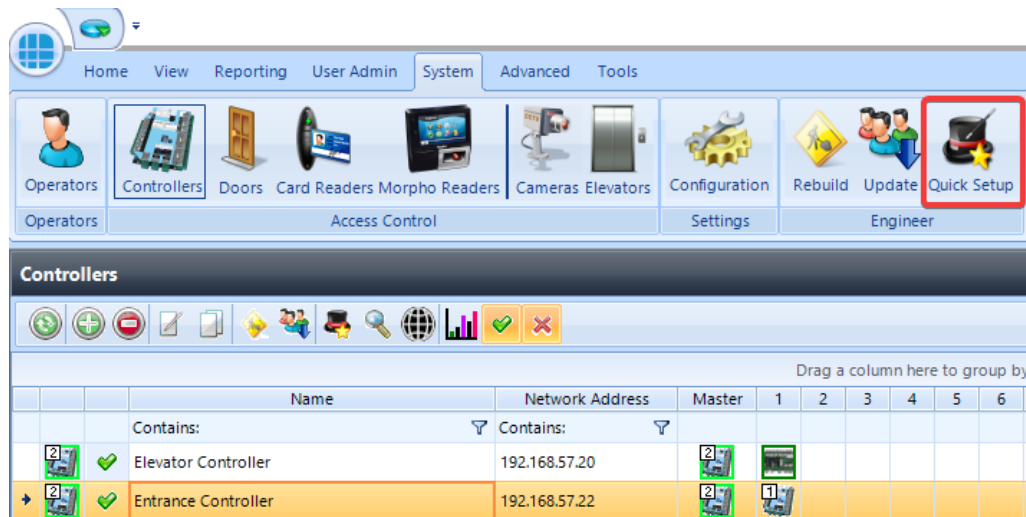
3. Click **[Accept]** to save the new Downstream Controllers.

[For more information on Controller Settings, see the "7.1 Controller General" section of the Identity Access Software Guide.](#)

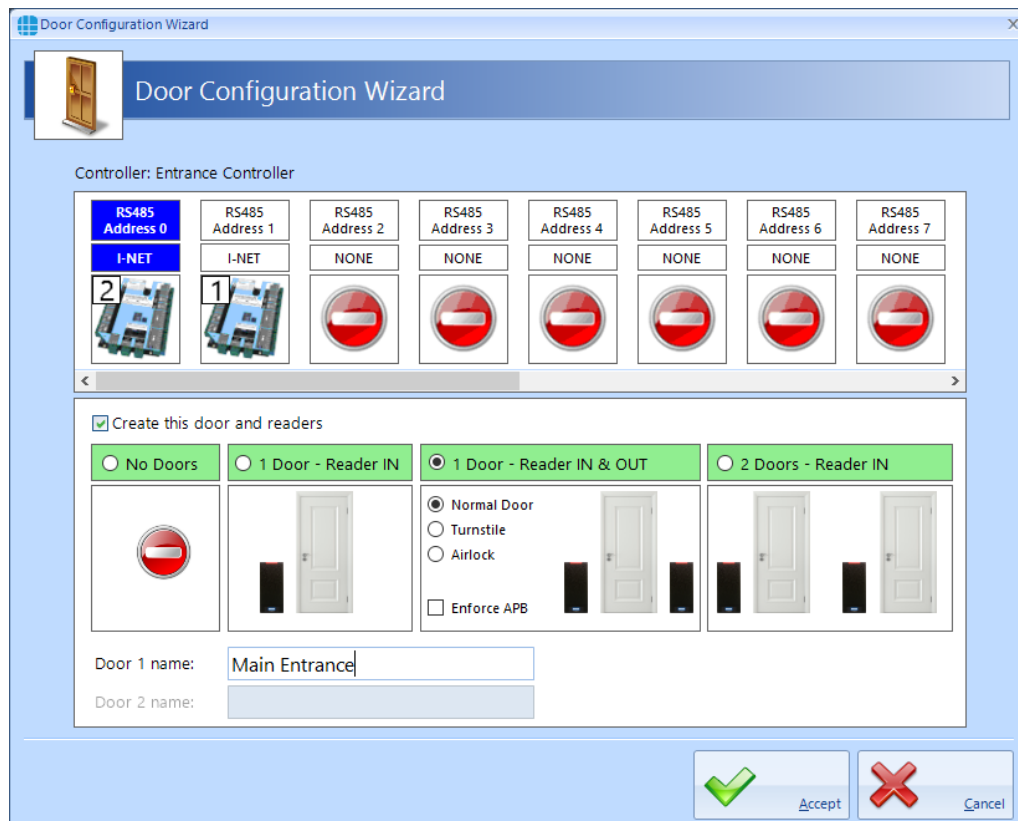
Step 8. Add Doors / Readers using Door Wizard

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

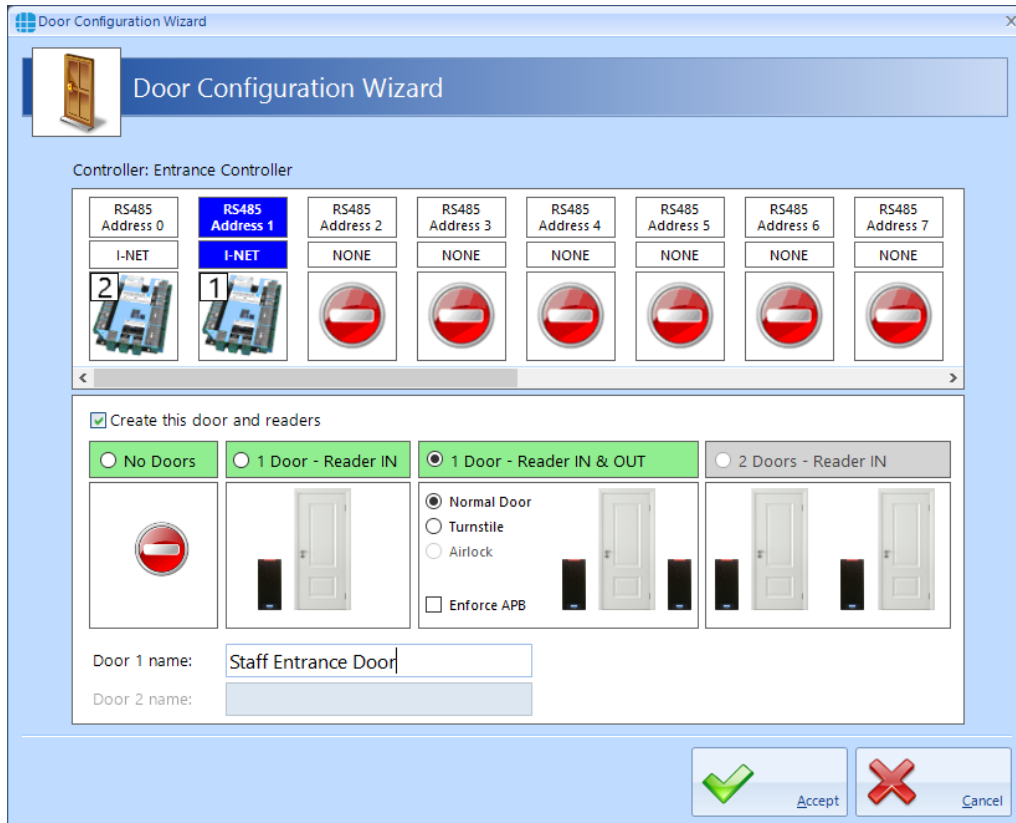
1. Highlight the IP controller and select the **Quick Setup** button.



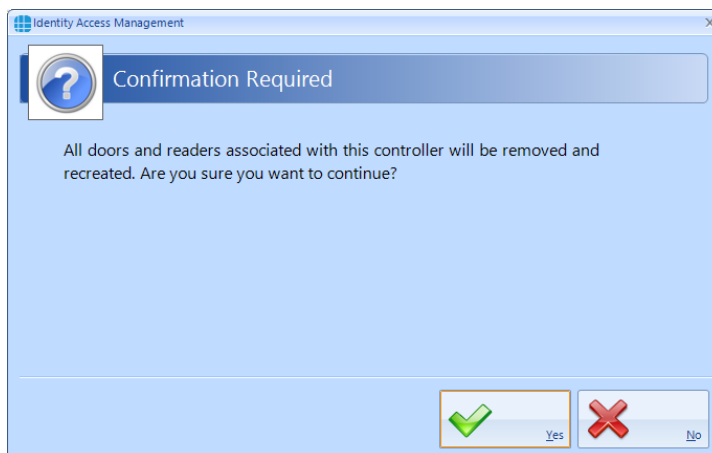
2. Select either **1 door with an IN reader**, **1 door with IN and OUT readers**, or **2 doors with IN readers** depending on your installation.
3. Enter the door name(s).



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



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



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

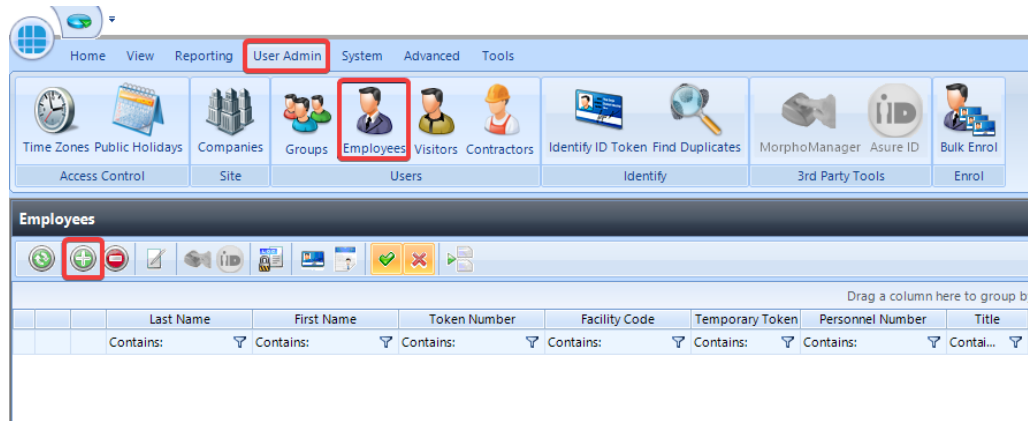
[For changing Reader Settings, see the "9. System > Card Readers" section of the Identity Access Software Guide.](#)

Step 9. Add Employee

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

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

2. Select 



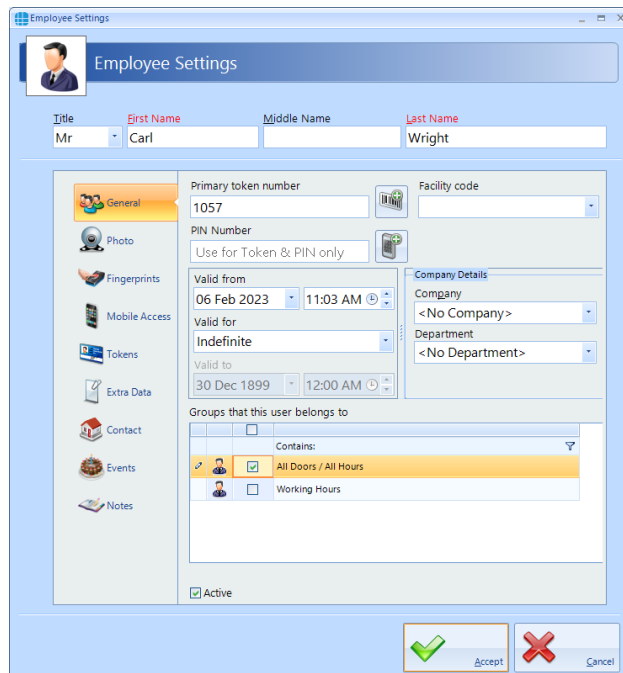
3. Enter the **First Name** and **Last Name** of the user.

4. Enter **Primary Token Number**. This may be written on the card/keyfob or read via an USB Desktop reader.

5. If using HID cards select the **Facility Code** from the dropdown list. Add New if necessary. For further information on facility codes, see the ["27. Appendix D - Facility Codes" section of the Identity Access Software Guide](#)

6. Select **All Doors/All Hours** under **Groups that this user belongs to**

7. Click **Accept**



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

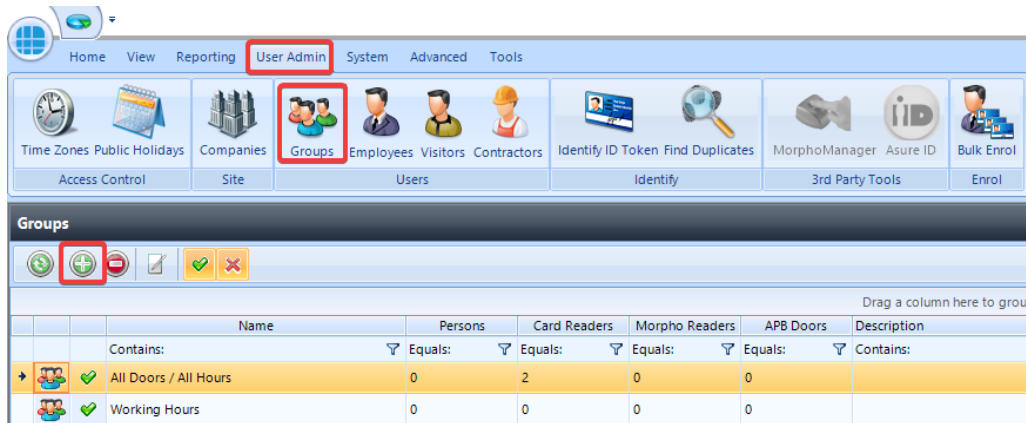
Below are the next steps to follow after a system test.

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


On installation, 2 default groups are configured:

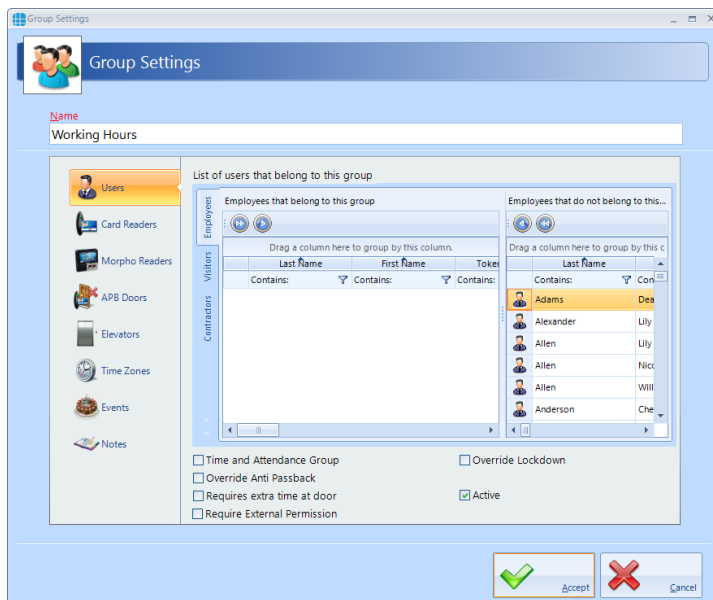
"All Doors / All Hours" is automatically assigned every door, elevator, anti-passback door and Morpho Reader to make it easier to test on initial setup. This group can be deleted but cannot be edited.

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

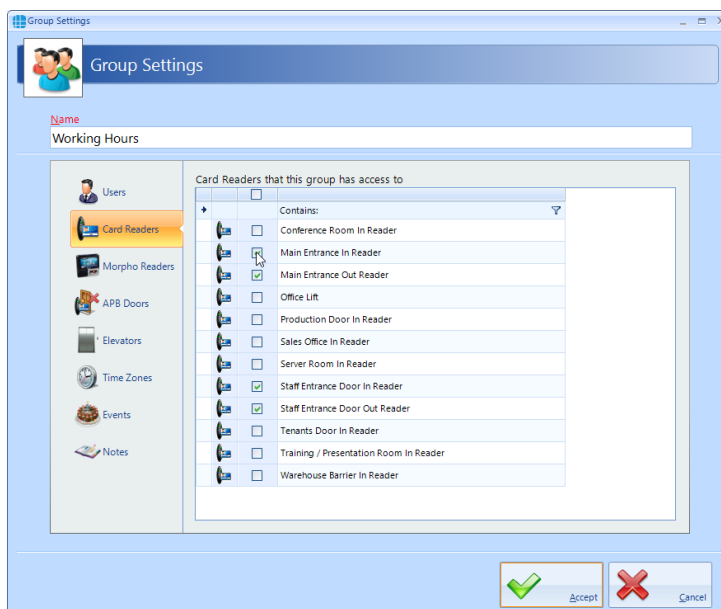


Continued on next page

1. To create a new Group, select the **User Admin** Tab, then select **Groups** from the ribbon bar. Select the **Add New** button .
2. Give the Group a name. The Users tab can be used to assign users into this Group if they are already added to the system.



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




[For more information on Groups, see the "16. User Admin > Groups" section of the Software Guide.](#)

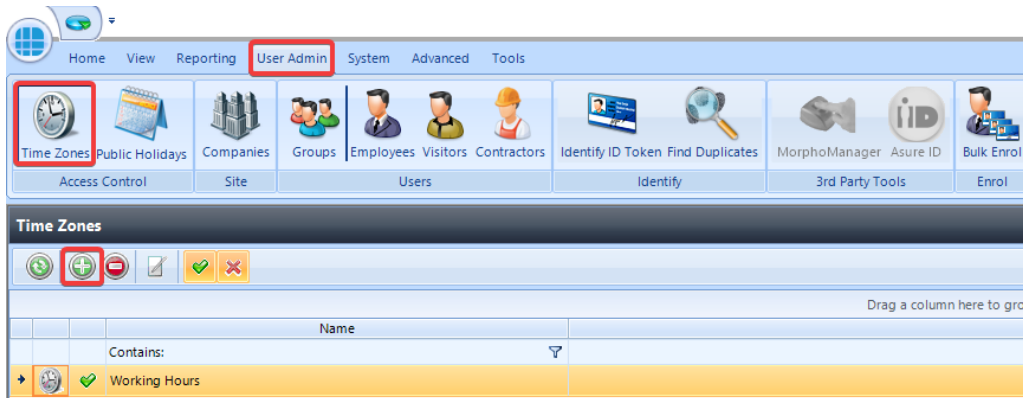
This step is optional, if Time Zones are not required, [click here to move onto Backups and Installing Identity Access Client.](#)

Time Zones can be used in 2 ways:

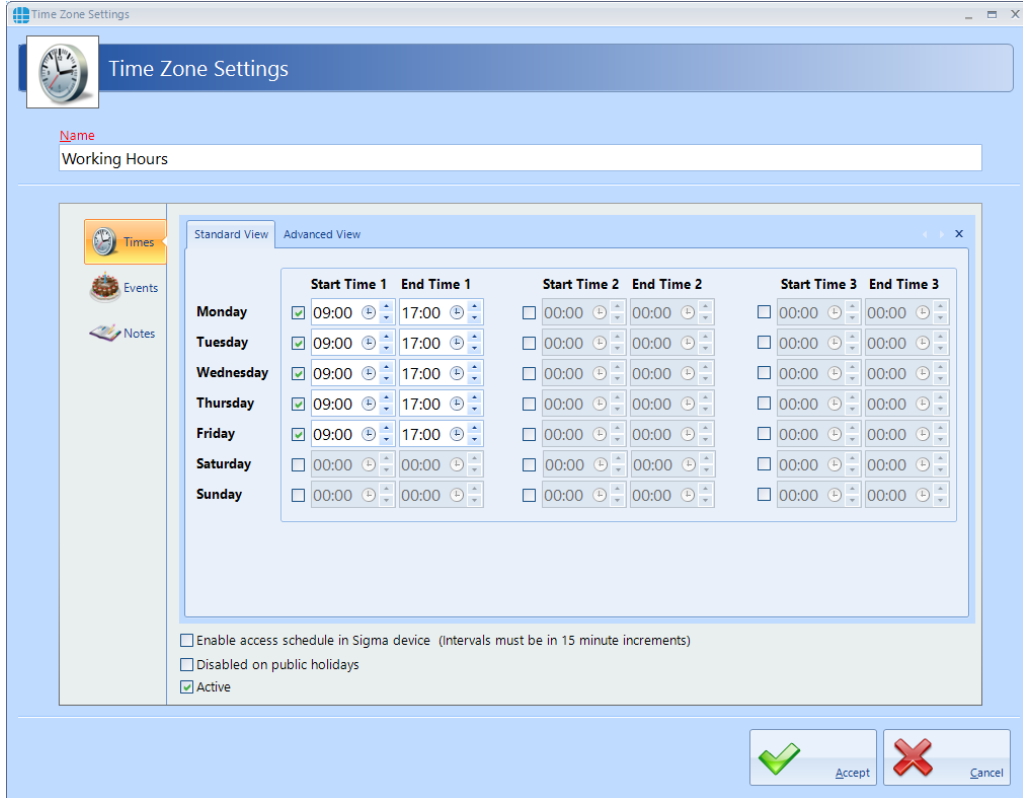
1. To use Time Zones, select the **User Admin** tab, then click **Time Zones** in the ribbon bar.

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

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

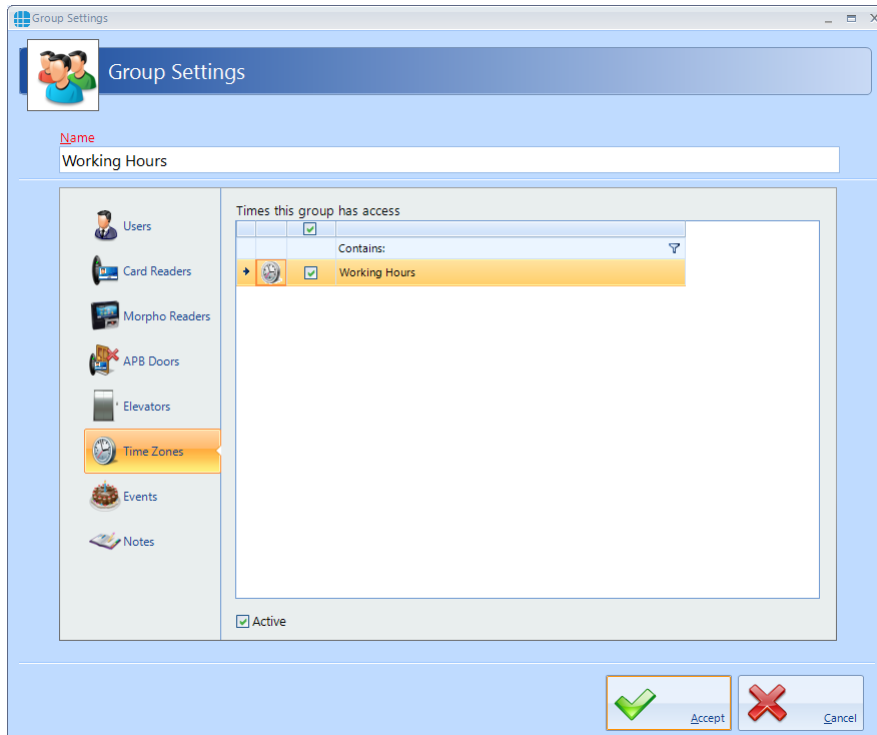


2. Select the Start and End Time for the Time Zone.



Adding a Time Zone to a Group

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

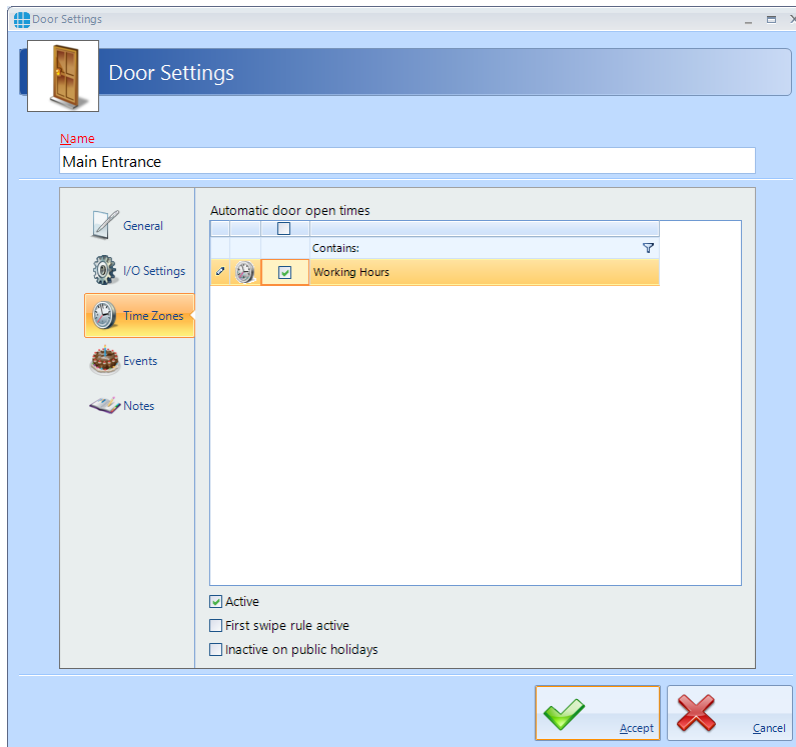


4. Press **Accept**.

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

Adding a Time Zone to a Door

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



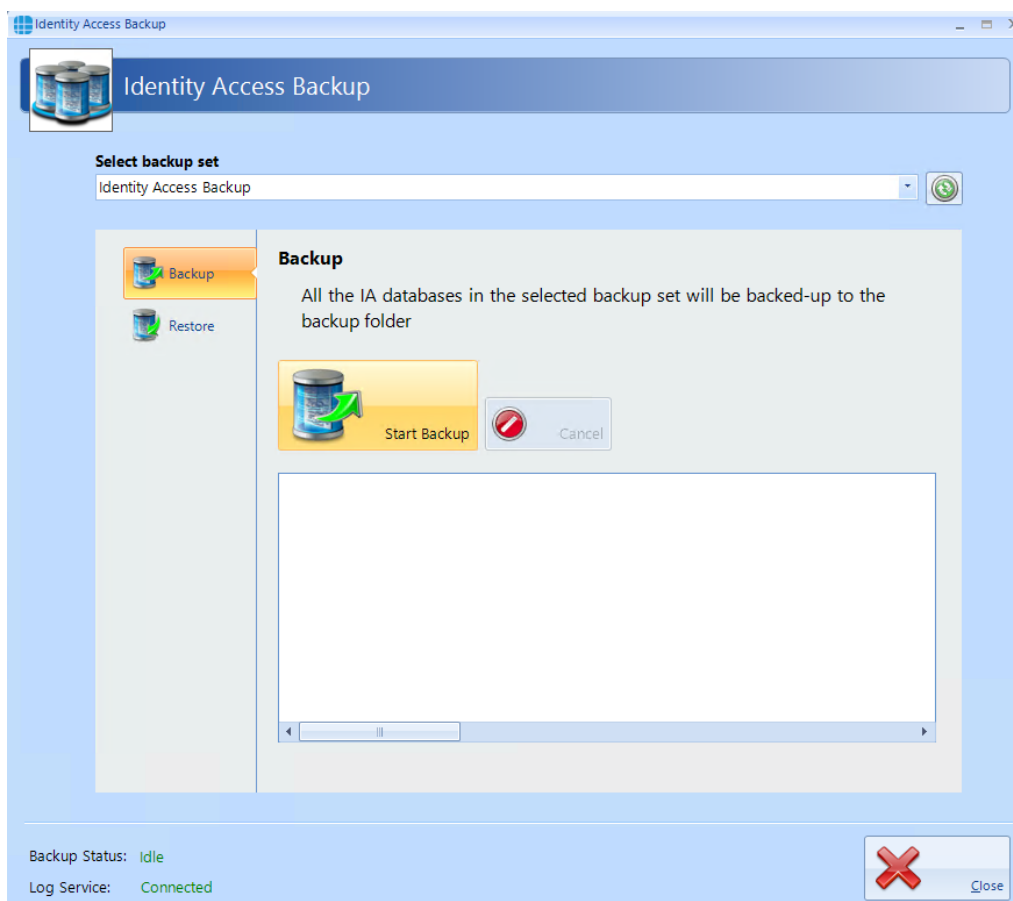
Identity Access is automatically set to backup to "C:\ProgramData\Controlsoft\IdentityAccess\Backup" daily at 13:00. By default it is setup to keep the last 7 days of backups. [To adjust these settings, see Chapter 23.14 of the Identity Access Software Guide.](#)

To manually backup the system:

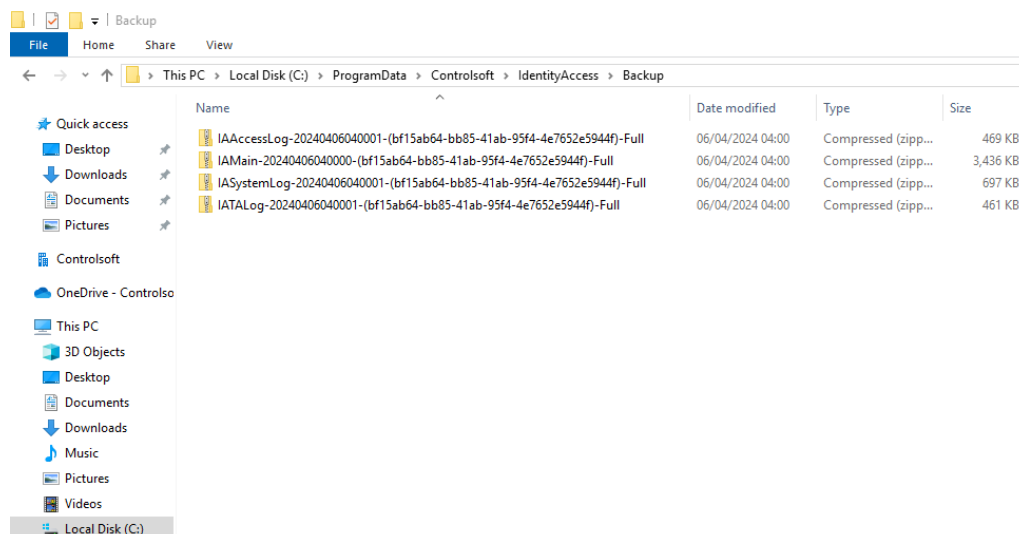
1. Click on the **Tools** tab and select **Backup**.



2. Select "Backup".



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



Installing Identity Access Client

For further information or the setup of other functions of Identity Access, please see the [Identity Access Software Guide](#)

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

[Click here, for information on how to configure the Identity Access Server for a Client connection and installing the Identity Access Client.](#)