

GARDiS Access Management Software

User Manual
UM0105 – Issue 9



Foreword

Copyright © 2003 TDSi. All rights reserved.

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

Guarantee

For terms of guarantee, please contact your supplier.

Trademarks

Copyright © 2003 Time and Data Systems International Ltd (TDSi). This document or any software supplied with it may not be used for any purpose other than that for which it is supplied nor shall any part of it be reproduced without the prior written consent of TDSi. Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Cautions and Notes

The following symbols are used in this guide:



CAUTION! This indicates an important operating instruction that should be followed to avoid any potential damage to hardware or property, loss of data, or personal injury.



NOTE. This indicates important information to help you make the best use of this product.

Document Control

Issue	Date Issued	Change Summary	Issued by
1	13 th September 2017	Initial release	RT
2	29 th September 2017	Additional section after review	RT
3	10 th November 2017	Revision of sections, changes made	RT
4	5 th April 2018	Updated with new features and screens	RT
5	26 th July 2018	Updated with latest screens and features	RT
6	9 th October 2018	Updated from latest feedback and added user and ACU progress sections	RT
7	31 st October 2018	Added in feedback suggestions from FM	RT
8	1 st April 2019	New Sections and updates for Version 1.1	TBA
9	3 rd May 2019	Frankie Brand Update	FM

Contents

1	Relationship Diagram.....	4
2	Quick Start Steps	5
3	Log In.....	6
4	Screen Layout.....	7
4.1	General Display Area	7
4.2	System Toolbar.....	7
4.3	Navigation Menu	8
5	Dashboard.....	9
5.1	Archived Events.....	9
5.2	Live Events.....	10
5.3	ACU Progress Table	11
6	Organisation	12
6.1	Departments	12
7	Sites	13
7.1	Areas.....	13
8	Equipment.....	14
8.1	ACU Configuration	14
8.2	Door Configuration	15
8.3	Communication Details.....	16
8.4	Submit.....	16
8.5	Additional Configuration.....	17
8.5.1	Editing Computers and IP Channels	17
8.5.2	Editing an ACU.....	18
8.5.3	Editing a Door.....	19
9	Schedules	22
10	Access Levels	24
10.1	Add Access Level.....	24
10.2	Edit an Access Level.....	26
10.3	Delete an Access Level	27
10.4	Assign a Door to Multiple Access Levels.....	27
11	Credentials	28
12	People	30
12.1	Add Person	30
12.2	Edit/Delete Person	33
12.3	Import People	33

12.3.1	File Configuration	33
12.3.2	Import Wizard	35
12.3.3	Import Results.....	38
12.4	Assign Multiple People to an Access Level.....	40
13	System Test	41
14	Settings.....	42
14.1	Users	42
14.2	User Permissions	45
14.2.1	Organisations.....	45
14.2.2	Equipment	46
14.2.3	Access Level	48
14.2.4	Reports.....	48
14.2.5	Schedules	49
14.2.6	Roles	50
15	Event Management	51
16	Alarms	52
17	Reports	53
18	ACU	57
19	Cards.....	58
20	Icons.....	59

Glossary of Terms

Access Point – A point within the building that controls access using ID points

ACU – The Access Control Unit is used to control access within controlled areas

Area – A place within your building with an entry and exit

Channel – The communication link between the computer and the ACU

Credential – A Credential is the piece of technology assigned to a person so they can gain access to different areas of the building

Department – The area of the business a person works in, or is associated with

Door – A door is travelled through by a person from one area to another

Event – Something that happens in the building that triggers a response from the system

Filter – Apply filters to show only the information you require in an area of the system

ID – An ID is given to a person to make them unique in the system

ID Point – A reader or RTE used to gain access through a door

IP Address – The identifier for a computer or device on a TCP/IP network

IP Port – Identifies a specific process of an internet or network message from the server

Organisation – The main hub of your company, the starting point in your GARDiS system

Period – A period of time which identifies functionality of a schedule

Reader – A piece of equipment which is presented with a credential and passes the information to the ACU. The ACU then decides whether to grant or deny access to the area

Reader No – Identifies which reader is associated with which door

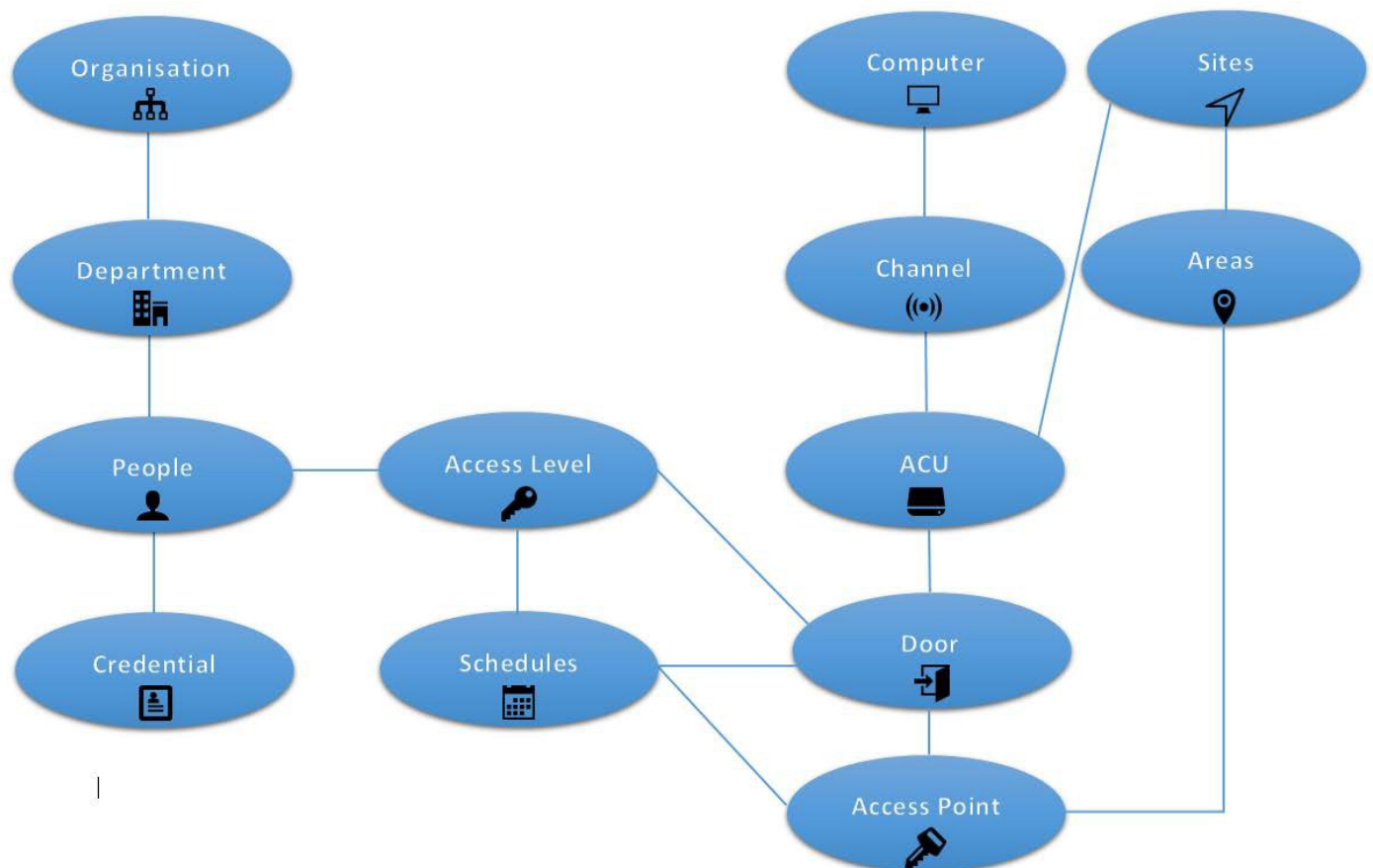
RTE (Request to Exit) – Also known as an Egress button, it's a button which is pressed to release a door, commonly found in an inside area to allow exit

Site – Organisations can have multiple buildings they operate from, therefore they can be named site 1, 2, 3 etc.

Third Party – Someone not directly involved in your company but has the same objective

User – A person with rights to the system who can log in, view and in some cases make changes to the system.

1 Relationship Diagram



2 Quick Start Steps

- Rename the pre-installed Organisation named Global to suit your business – **See section 5**
- Add the departments to the Organisation – **See section 5.1**
- Rename the existing site in GARDiS called Site 1 to suit your company – **See section 6**
- Click the Site and begin adding Areas to it – **See section 6.1**
- Configure your Equipment using the Wizard Tool – **See section 7**
- Set up the Access Level by choosing its schedule and assigning the Doors to it – **See section 9**
- Add the required Credentials to match your reader technology – **See section 10**
- Add the required People and assign their credentials and access level – **See section 11**
- Card presentation and configuration checking in the Dashboard tab – **See section 12**

3 Log In

GARDiS requires a user login (which will apply their user rights based on their assigned role) to operate GARDiS.

You will need to know the Username & Password.

The default login (which will open up a blank database from a new installation) is as follows:

Username: GARDiS

Password: TDSi\$1234

NOTE: You will be required to change this when you first log in.

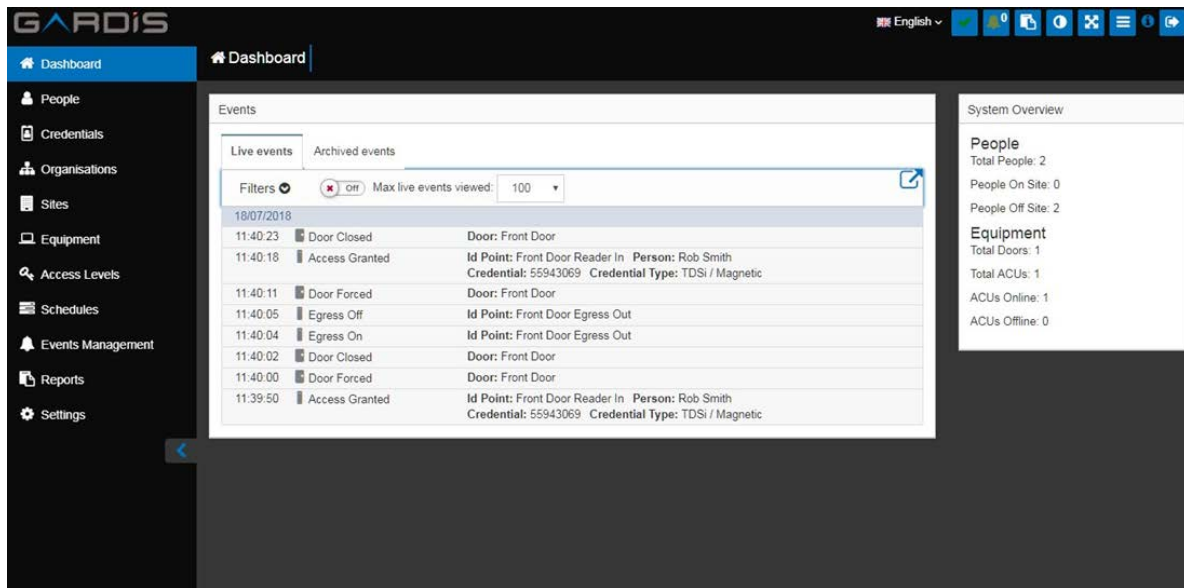


The image shows the GARDiS login interface. At the top is the GARDiS logo. Below it is the word 'Login' in blue. There are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'Username'. The 'Password' field contains a series of dots followed by a vertical cursor. Below the input fields is a blue 'Login' button.

4 Screen Layout

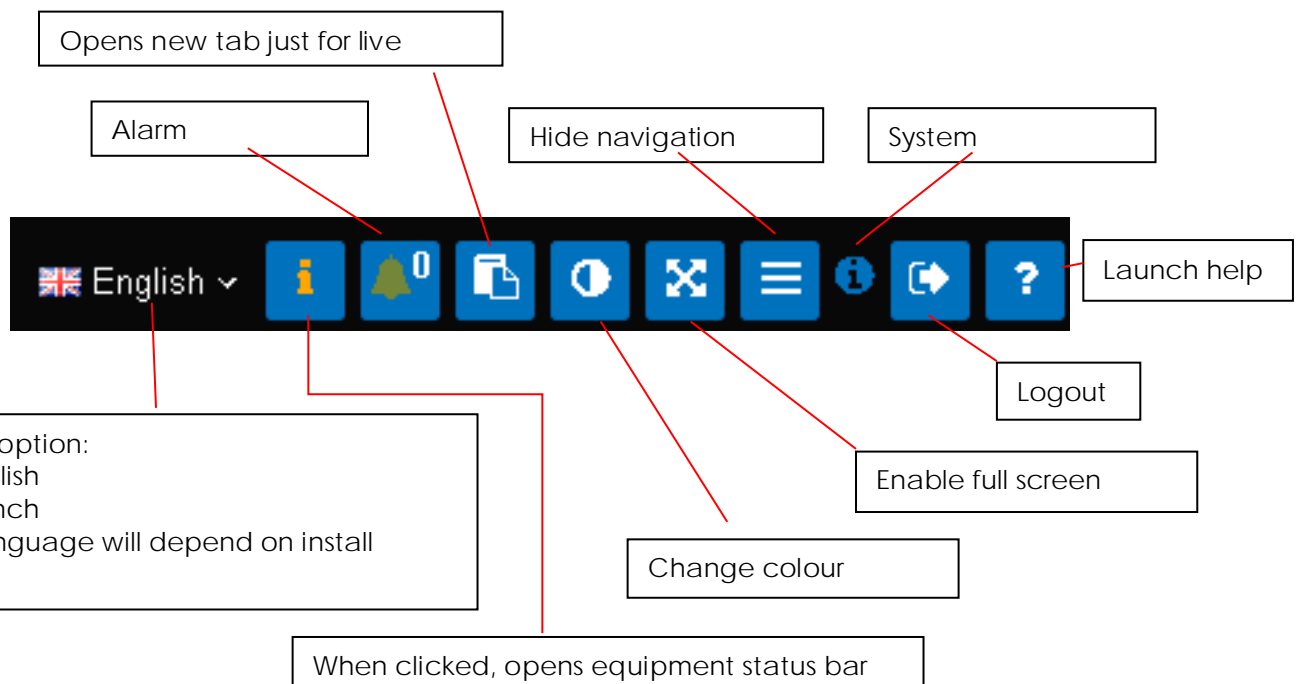
4.1 General Display Area

The Dashboard is your general display area and the default landing page when you log into GARDiS. From here you can see events and general system information.

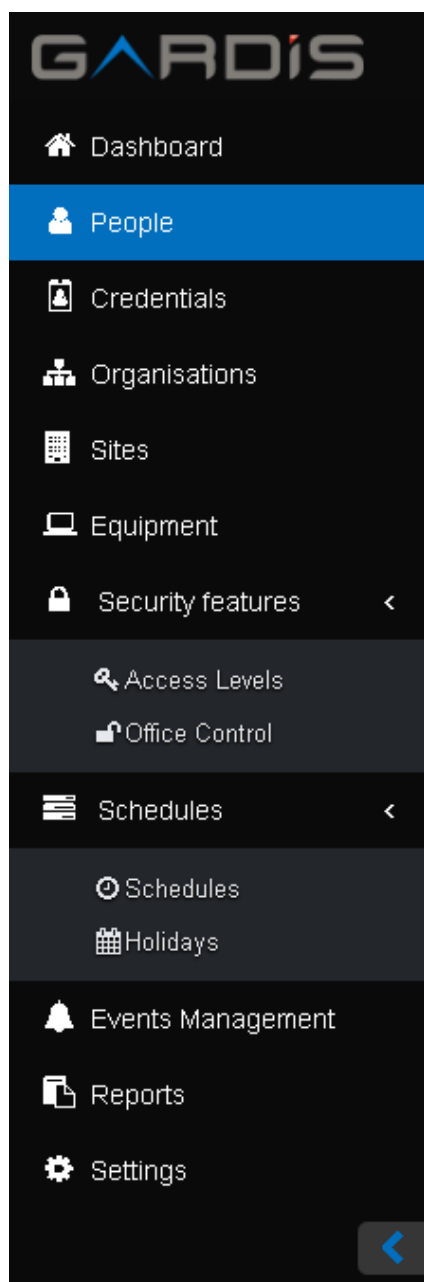


4.2 System Toolbar

Found in the top right corner of GARDiS you'll find the system toolbar, find an explanation of each icon below.





4.3 Navigation Menu



This is your main tool for navigating your GARDiS system. An easy to use simple menu which separates each area of the system.

You can also collapse this menu so it only shows the icons without the names next to them.

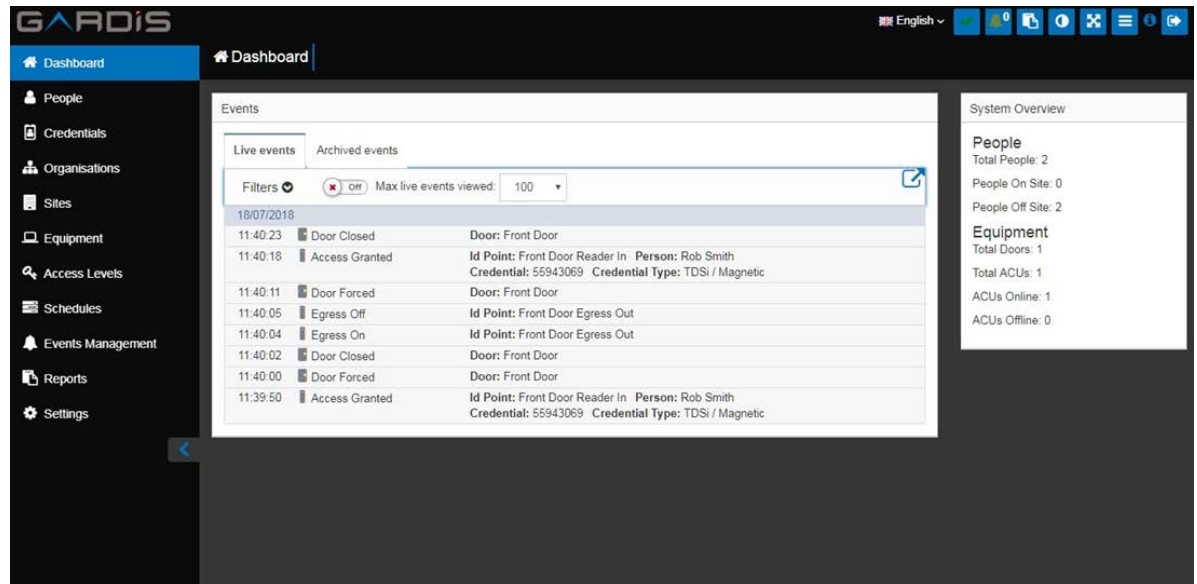
To collapse the menu click the  icon.

To expand the Navigation Menu click the  icon.

5 Dashboard

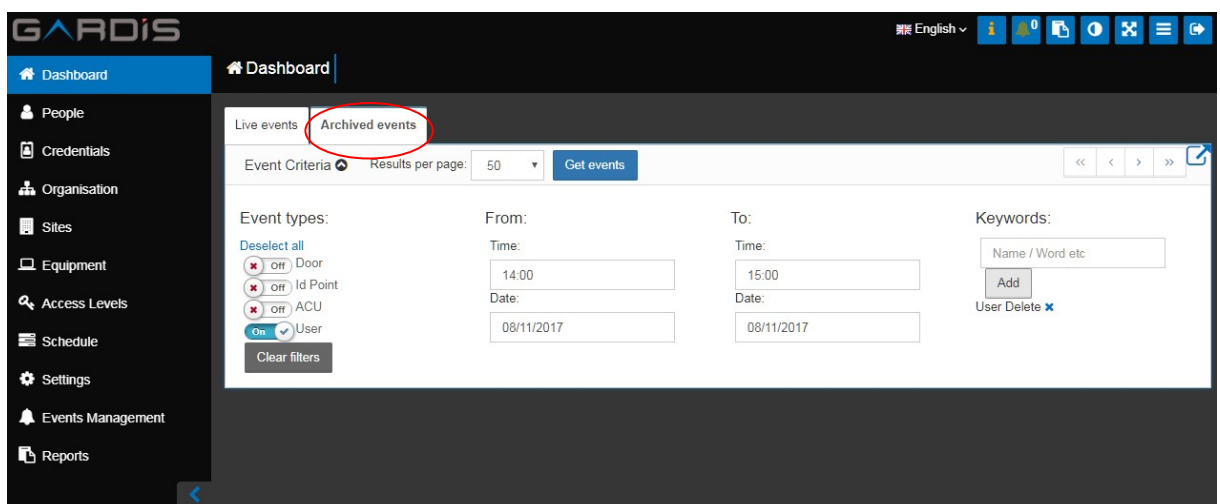
GARDiS' Dashboard is designed to take Access Control back to basics. With the Dashboard being used, site management has never been easier.

Here you will see everything happening in real time in your system, note that when you navigate away from this screen all the on screen events will still be sent to the Archive.

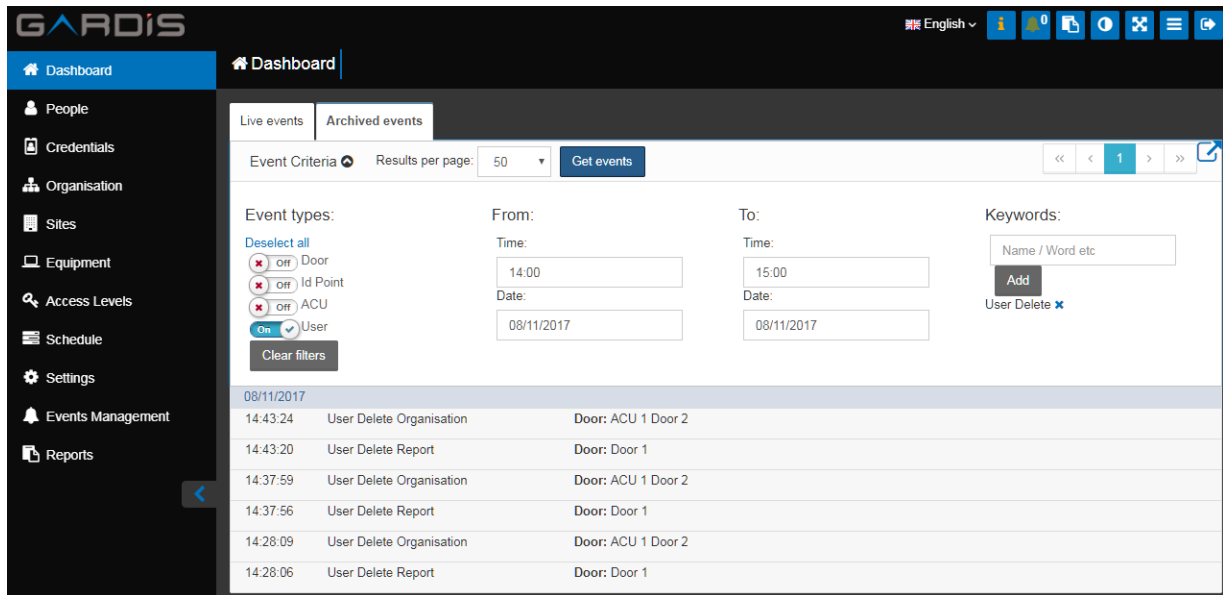


5.1 Archived Events


To access previous events that have been sent to the Archive, click the **Archived Events** tab. From here you can use the displayed options to configure which type of events you want to find, then click **Get Events**.



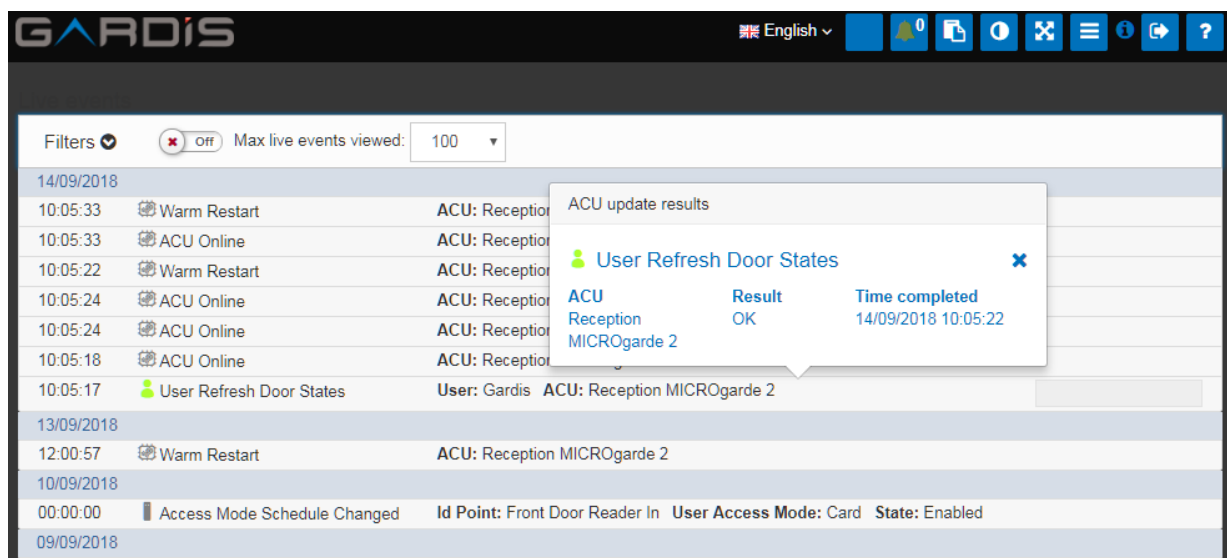
The required archived events will now be displayed.



5.2 Live Events

Click the **Live Events** icon in  the System Toolbar to open a new tab in your browser which will display real time events of everything happening in your system.

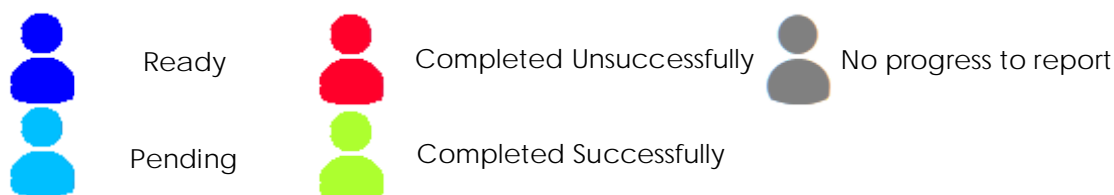
ACU Events can be viewed in more detail by clicking on them as shown in the below example. Go to the next page in the manual to find out more information on this.



5.3 ACU Progress Table

The following is a list of user events in GARDiS that would report progress from the ACU. This will change the colour of the icon to indicate the status. These events will appear in the Live Events window.

For example when a user makes changes to a credential and a user event "User edit Credential" is generated. A User icon is displayed blue to indicate the possible changes are ready. The ACU communications manager receives the command and reports the command is pending (Light blue). Finally the command is processed and the result is returned, indicating success (Green) or Failure (Red).



Object	Progress will be reported on
Access Levels	User Assign Person to Access Level
	User Remove Person from Access Level
	User Delete Access Level
	User Edit Access Level
	User Add Access Level
ACU	User Add ACU
	User Edit ACU
	User Initiate ACU Refresh
Credential	User Assign Credential
	User Changed Status of Credential
	User Edit Credential
	User Delete Credential
	User Unassigned Credential
Door	User Add Door
	User Release Door
	User Edit Door Details
	User Remove Door
ID	User Edit ID Point
Reader	User Assign Reader Mode
Schedule	User Update Schedule

6 Organisation

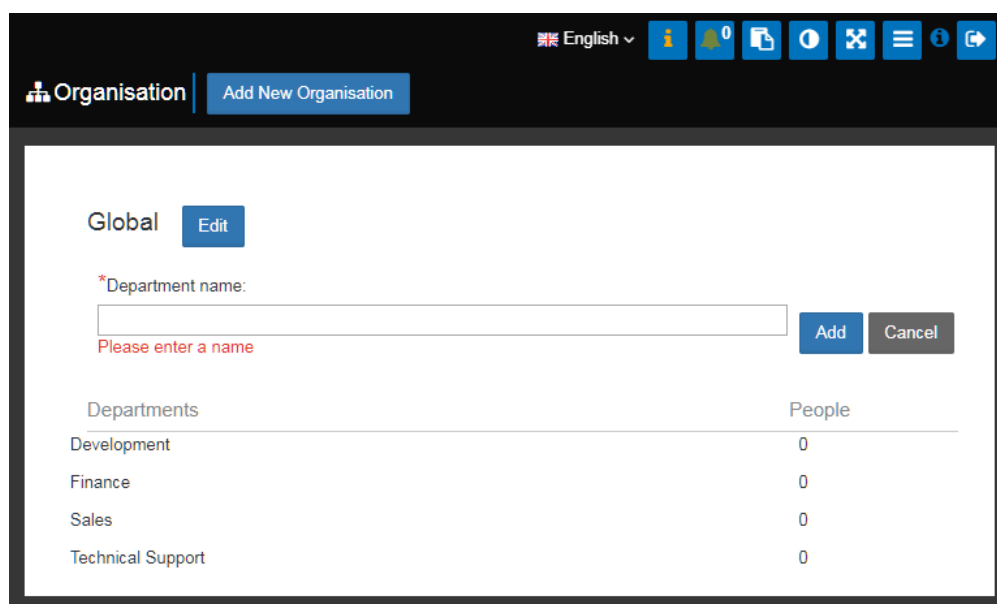
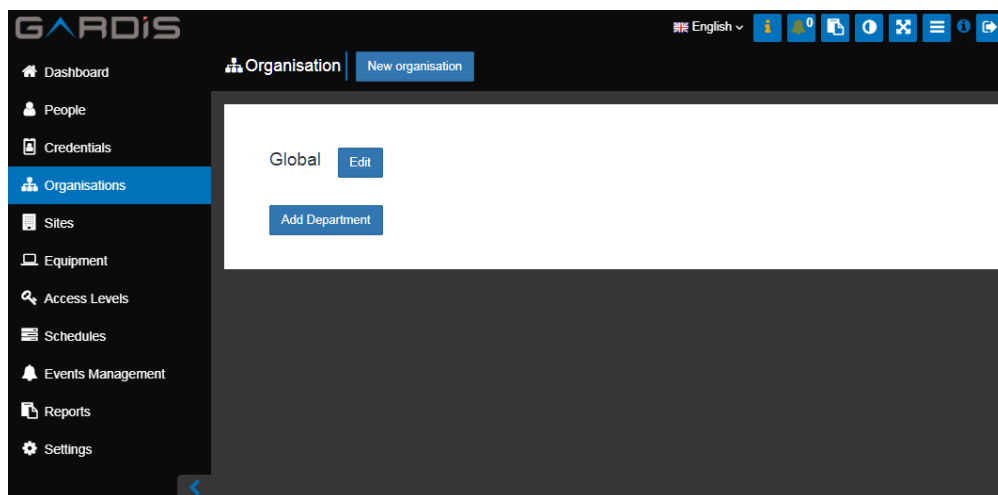
Your Organisation is the main base of your system and your company. By default, GARDiS comes with a pre-installed Organisation named Global. This is editable to suit your company name.

6.1 Departments

Once an Organisation has been selected you will be given the option to begin adding Departments.

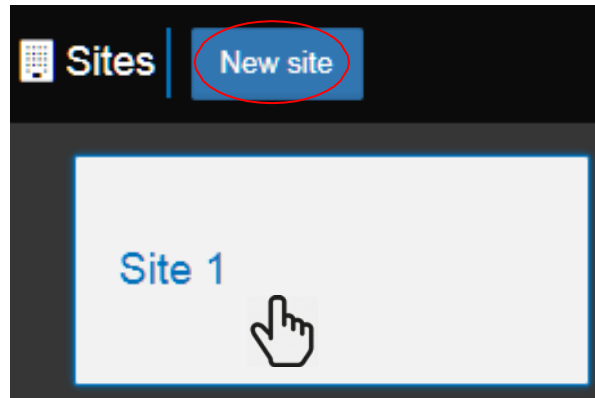
Departments can be useful when it comes to searching or filtering people once your system is populated.

Organisation and department properties can be edited from this screen.



7 Sites

Every system will have one or more Sites (Licensed option). By default, GARDiS has a Site already set up, called Site 1 which is editable to suit your environment. Sites are where you add the Areas of your building(s). Either click on the **Site** to edit it to your needs or click **New Site** to begin creating a new one.



7.1 Areas

Areas are used to specify access points when you're setting up your Equipment. You can add multiple areas to a site. To begin adding areas to the Site, just click on it and the menu below will appear. Once you're done adding your areas click **Close** to save the changes.

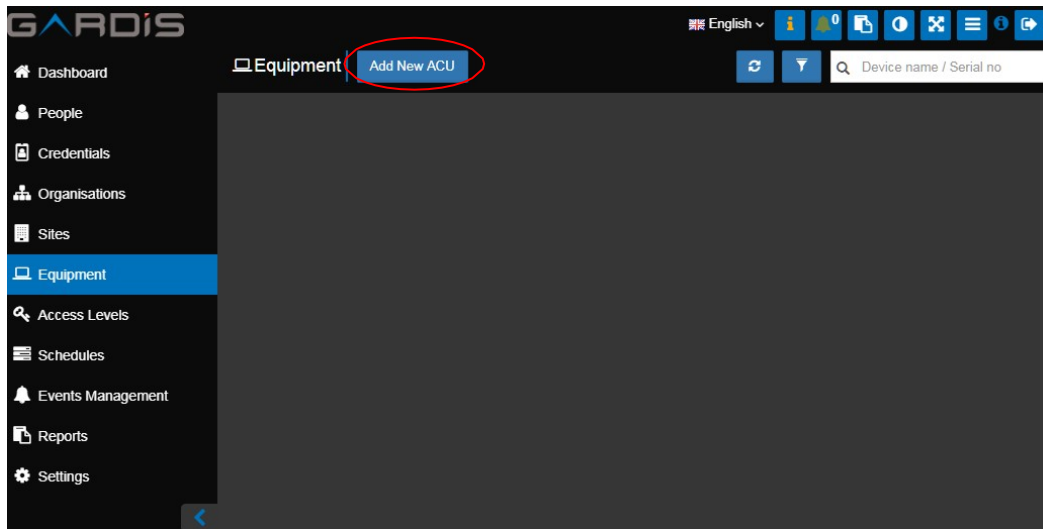
You can edit areas by clicking on the required one, then click **Edit**.

An area can be set as "On site" or "Off-site". This will affect reporting of people locations.

An area can be shared between sites. This will affect reporting of people in locations, allowing multi-organisation reporting.

8 Equipment

The ACU Wizard tool will guide you through setting up all your equipment step by step. To begin, click **Add New ACU**.



8.1 ACU Configuration

To configure the ACU:

- The **Serial Number (UID)** printed on the board of the ACU
- The **Name** you want to give the ACU (maximum 50 characters)
- The **Location** of where the ACU installed (maximum 50 characters)
- The **Site** where the ACU is located (a drop down to select existing or enter to create a new one). This is used for permissions and event reporting.
- Once complete, click **Next**.

The screenshot shows the 'Add acu' wizard with four steps: 1. Acu configuration, 2. Door configuration, 3. Communication details, and 4. Submit details. Step 1 is active. The form contains the following fields:

- Serial number (UID)**: Text input field containing '4-004-002-825'.
- Name**: Text input field containing 'ACU 1'.
- Location**: Text input field containing 'Reception'.
- Site name**: Dropdown menu showing 'Site 1'.

At the bottom of the form are three buttons: 'Previous' (disabled), 'Cancel' (disabled), and 'Next' (active).

8.2 Door Configuration

To configure the Door:

- Click the Disabled/Enabled switch so it shows **Enabled**
- Enter the **Door name** (maximum 50 characters). This automatically populates the Access area entering field
- Select the ID point options from the drop down. E.g. **Read in, Read out option**
- Select the Reader **Type**
- Select the **From** area from the drop down. This also is a free text entry box, if you enter a 'From Area' manually, the system will add it as an area in GARDiS on the site set in step 1.
- Select the **Access area entering** from the list, or leave it already populated
- Select whether the Door sensor is normally open or if it's normally closed
- Once complete, click **Next**

To set up multiple doors, click Door 2, 3 and 4 as required then repeat the above process.

Add acu

1 — 2 — 3 — 4
 Acu configuration Door configuration Communication details Submit details

Door 1 Door 2 Door 3 Door 4

Door number 1

Enabled ☒

Door name: Door 1

Id point options: Read in, request to exit

Type: TDSi / Magnetic

From area: Car Park

Access area entering: Door 1

Door sensor: Normally closed

Previous Cancel **Next**

8.3 Communication Details

To set up communications:

- Enter the computer **Name** or select an existing name from the drop down
- Enter the **IP Address** for a new channel or select an existing channel from the drop down list. GARDiS will automatically assign IP Port 10001 to a new channel. This can be changed in the channel settings if required (Section 8.5.1). In the drop down list of channels the IP address and port are shown as IPADDRESS:PORT e.g. 192.168.0.11:10001
- Enter the **Unit Number** of the ACU. If it's the first unit on the IP Address, set to 1 and increment for others on the same address. Unit numbers have an upper limit of 32. So the first device will be unit 1, the 2nd Unit 2, 3rd unit 3 etc. If you don't number the units sequentially from 1 it could impair performance
- Once complete, click **Next**

NOTE: If using a MICROgarde unit with the dial set from 1 to 8 then it must be added to GARDiS using this unit number as this may cause issues with communications.

8.4 Submit

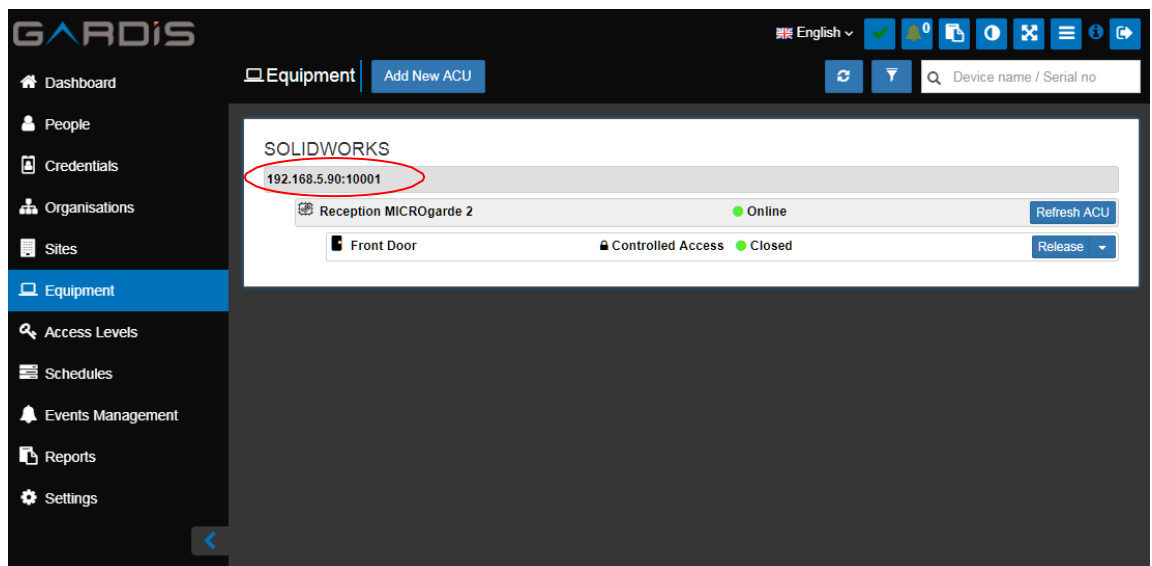
Your equipment is now ready to be submitted. Review the information in the New ACU Summary window. If you're happy to complete the setup, click **Finish**.

8.5 Additional Configuration

8.5.1 Editing Computers and IP Channels

Now the equipment is set up, by clicking on any of the three options available you can open the settings for that option.

If you click the IP address or channel name you've set up you will see this box appear.



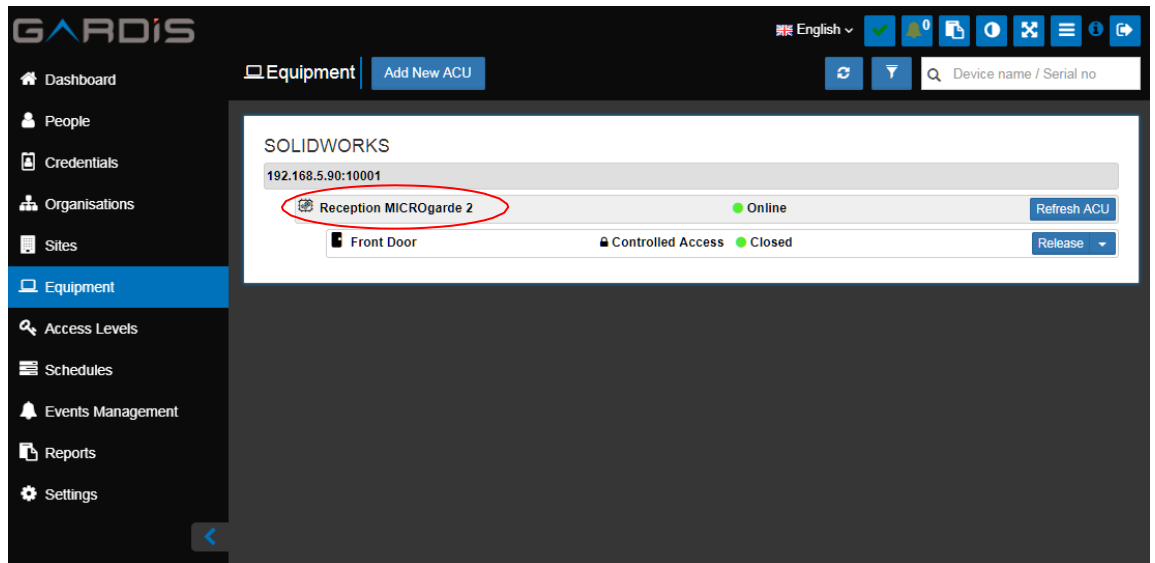
From here you can edit:

- The **IP Channel Name** (max 50 characters)
- The **IP Address**
- The **IP Port**

Once you're happy with the changes you've made, click **Submit**.

8.5.2 Editing an ACU

To edit the details of the ACU, click the required **ACU**.



From here you can edit:

- The ACU's **Name**
- The ACU **Serial Number/UID**
- Which **Site** the ACU is assigned to
- The **IP Channel**
- The **Unit number**

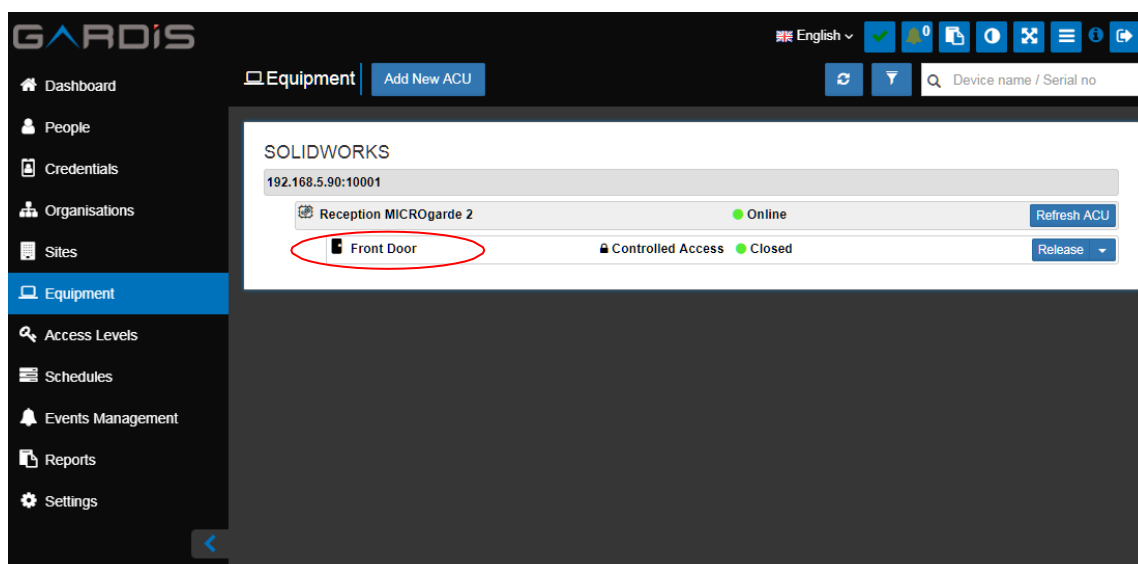
Once you're happy with the changes you've made to the ACU, click **Submit**.

Click here to edit the **Door Properties**

Click here to add a **second Door**

8.5.3 Editing a Door

To edit door details, click the required **Door**.



This will expand and open the ACU Properties Menu shown on the next page.

Click here to add a new door

Excel4 - Reception
✕

ACU

Door 1
Door 2
Add Door

Door Settings

Name

Door Release Time
 secs

Extended Door Release Time
 secs

Lockstrike Off Mode

Door Left Open
 secs

Extended Door Left Open
 mins

Door Sensor

Free Access Schedule

Holiday Free Access Schedule

Office Control
☒ Off

Id Point Settings

Id Point 1
Id Point 2

☒ Enable Reader
☐ RTE (egress)

Name

To Area

Reader Type

Reader No.

Access Mode Schedules

Card Only

Holiday Card Only

PIN Only

Holiday PIN Only

Card + PIN

Holiday Card + PIN

Submit
Delete Door
Cancel

Door settings:

- **Name** – Edit the door's name
- **Door Left Open** – Select the amount of time the door can be left open until a 'Door Left Open' event is generated by the ACU
- **Free Access Schedule** – Select the schedule that enables 'free access', which means the door will be unlocked during this schedule
- **Holiday Free Access Schedule** - Select the schedule that enables 'free access' on a holiday day, which means the door will be unlocked during this schedule.
- **Door Release Time** – How long the door will be unlocked once a card has been presented to the reader and access has been granted
- **Extended Door Left Open** – Select the amount of time the door can be left until an 'Extended Door Left Open' event is generated by the ACU
- **Lockstrike Off Mode** – Control the behaviour of the lock re-locking either when the door is opened, closed (both require door monitoring contact fitted), or when the Door Release Timer expires
- **Extended door release time** – This feature will extend the Door Release timer duration to this value for any Credential holder that is set as requiring DDA support
- **Door Sensor** – Selects whether the door input will show secure when the device connected is Normally Open circuit or Normally Closed circuit

ID Point Settings:

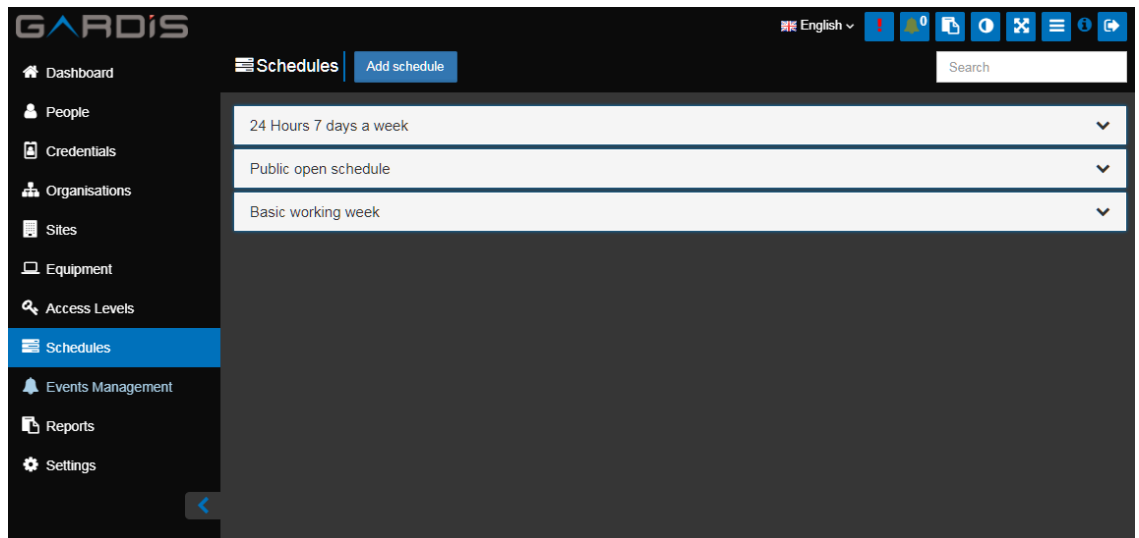
- **Name** – Edit the name of the reader/ID point
- **To Area** – Edit the name of the area that is being entered
- **Type** – Change the type of technology
- **Reader No.** – Change the number of the reader
- **Card Only** – Select the schedule when **Card Only** mode is to be used
- **PIN Only** – Select the schedule when **PIN Only** mode is to be used
- **Card + PIN** – Select the schedule when **Card + PIN mode** is to be used
- **Holiday Card Only** – Select the schedule when **Card Only** mode is to be used on holiday days
- **Holiday PIN Only** – Select the schedule when **PIN Only** mode is to be used on holiday days
- **Holiday Card + PIN** – Select the schedule when **Card + PIN mode** is to be used on holiday days
- **Enable Reader/RTE (egress)** – Use these buttons to change between reader and RTE

For example: This door operates in **Card Only** mode 24 hours a day

9 Schedules

Schedules are universal and are used wherever a schedule is needed, for example Schedules are used to determine the door free access. GARDiS already has three pre-configured Schedules that you can edit as required by clicking on them and making the required changes.

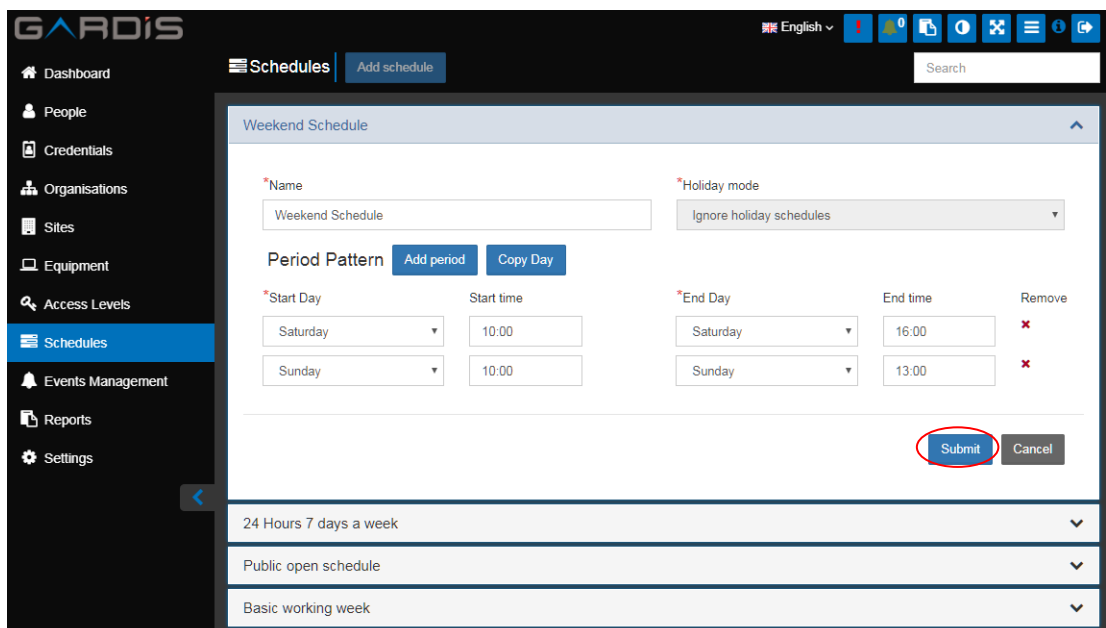
To add a new schedule to GARDiS, click the **Add schedule** button.



Give the new Schedule a name, then click the **Add period** button. You will see the **Start Day** and **End Day** options appear.

Configure the day and time you want the Schedule to begin, then the day and time you want the Schedule to end using the drop down boxes and entry fields.

Once complete, click **Submit** to save the new Schedule.



The new Schedule is now set up and ready to use.

24 Hours 7 days a week	▼
Public open schedule	▼
Basic working week	▼
Weekend Schedule	▼

For example, now when you enter the Doors with schedule screen, within Access Levels, you will notice the new 'Weekend Schedule' is available.

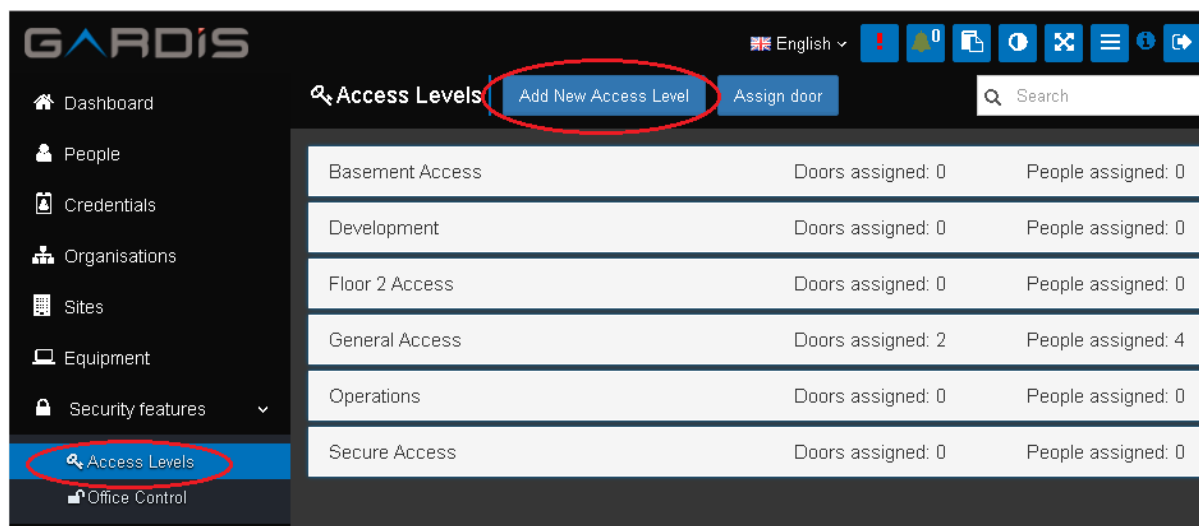
The screenshot shows a software interface for managing access levels. On the left, a modal dialog titled "Select a schedule" is open. It contains a search bar with the placeholder "Name" and a "Cancel" button. Below the search bar, a list of available schedules is displayed: "24 Hours 7 days a week", "Public open schedule", "Basic working week", and "Weekend Schedule". To the right of the dialog, the main screen is partially visible. It has a dark header with a "Delete access level" button. Below the header, there are search and filter controls: a "Search" input field containing "Door" and a "Site" dropdown menu set to "All". A section titled "*Selected" contains a message: "Please select doors from the available list opposite". At the bottom right of the main screen, there are two buttons: "Add selection to access level" and "Cancel".

10 Access Levels

Access Levels are assigned to people in GARDiS and they allow you to configure where people are allowed to go in the building(s) and when.

10.1 Add Access Level

Click "Access Levels" in the Navigation menu under "Security features", then click "Add New Access Level" button.



A window is displayed containing a list of the doors in the system. Select the doors to be added to the access level and click the top arrow to move the doors to the "Assigned doors" list.

Add new access level

* Access Level Name

Select doors to assign

Search

Assigned doors

Search

Name [Unselect all](#)

- ☒ Demo Room
- ☐ Development Door
- ☒ Front Door
- ☐ Operations
- ☐ Sales
- ☐ Server Room

Name **Standard Schedule** **Holiday Schedule** [Select all](#)

Submit

Cancel

The schedules that a people assigned to this access level can be configured per door. Each door has a "Standard Schedule" and a "Holiday Schedule". The schedules can be applied to multiple doors by selecting the doors, then clicking the schedule link. Select the available schedules from the list and it will then apply to those doors.

Add new access level

×

*Access Level Name

Select doors to assign

Search

Name	Select all
<input type="checkbox"/> Development Door	
<input type="checkbox"/> Operations	
<input type="checkbox"/> Sales	
<input type="checkbox"/> Server Room	

Assigned doors

Search

Name	Standard Schedule	Holiday Schedule	Unselect all
<input checked="" type="checkbox"/> Demo Room	24 Hours 7 days a week	24 Hours 7 days a week	
<input checked="" type="checkbox"/> Front Door	24 Hours 7 days a week	24 Hours 7 days a week	

Select a schedule

Search

Schedule

- 24 Hours 7 days a week
- [Basic working week](#)
- None
- Public open schedule

Click "Submit" when complete. In the screenshot below, the new access level "Visitors" will allow people through the "Front Door" and "Demo Room" doors using the "Basic working week" schedule. On days that are set as "Holidays", they will have no access.

Add new access level

×

*Access Level Name

Select doors to assign

Search

Name	Select all
<input type="checkbox"/> Development Door	
<input type="checkbox"/> Operations	
<input type="checkbox"/> Sales	
<input type="checkbox"/> Server Room	

Assigned doors

Search

Name	Standard Schedule	Holiday Schedule	Unselect all
<input checked="" type="checkbox"/> Demo Room	Basic working week	None	
<input checked="" type="checkbox"/> Front Door	Basic working week	None	

Once submitted, the new Access Level will display in the list of Access Levels along the total number of doors configured in the Access Level.

GARDIS

English

0

Dashboard

People

Credentials

Organisations

Sites

Equipment

Security features

Access Levels

Office Control

Schedules

Access Levels

Add New Access Level

Assign door

Search

Basement Access	Doors assigned: 0	People assigned: 0
Development	Doors assigned: 0	People assigned: 0
Floor 2 Access	Doors assigned: 0	People assigned: 0
General Access	Doors assigned: 2	People assigned: 4
Operations	Doors assigned: 0	People assigned: 0
Secure Access	Doors assigned: 0	People assigned: 0
Visitors	Doors assigned: 2	People assigned: 0

10.2 Edit an Access Level

Click "Access Levels" in the Navigation menu under "Security features". The list of access levels will display in the main window. Select the Access Level required for editing. This will open the properties of the Access Level in an edit mode.

Edit access level

*Access Level Name

Visitor Access

Select doors to assign

Search

Name

Name

Select all

☐ Demo Room
 ☐ Development
 ☐ Operations
 ☐ Reception
 ☐ Server Room 1
 ☐ Server Room 2

Assigned doors

Search

Name

Name

Standard Schedule

Holiday Schedule

Select all

Submit

Delete

Cancel

10.3 Delete an Access Level

Edit access level

* Access Level Name

Select doors to assign

Search

Name	Select all
<input type="checkbox"/> Demo Room	
<input type="checkbox"/> Development	
<input type="checkbox"/> Operations	
<input type="checkbox"/> Reception	
<input type="checkbox"/> Server Room 1	
<input type="checkbox"/> Server Room 2	

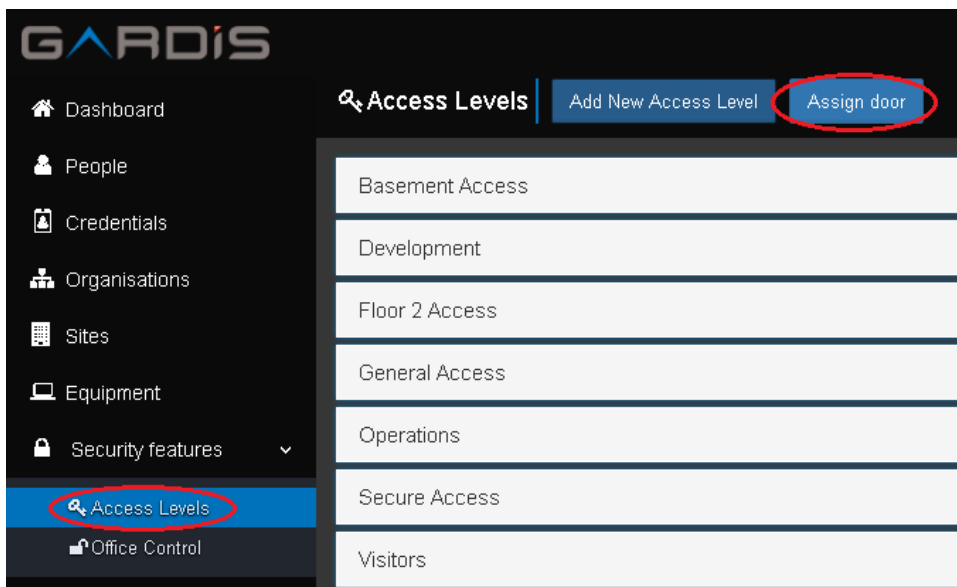
Assigned doors

Search

Name	Standard Schedule	Holiday Schedule	Select all
------	-------------------	------------------	------------

10.4 Assign a Door to Multiple Access Levels

When adding new doors to the GARDiS system you will may want to assign those doors to multiple Access Levels. From this view it is also possible to see the Access Levels a Door is already assigned to. Navigate to the Access Levels page and click "Assign Door" button.



A new window will appear. Click within the "Select door" text box. A list of doors will be displayed. Select the required door from the list.

Assign door to access levels

Select door

Please select a door to be assigned

Select door

Search

Name

Door name

ACU

[Demo Room](#)

Operations

Sales

Server Room

Development Door

Front Door

excelTest

excelTest

excelTest

excelTest

excel4

excel4

Standard Schedule

Holiday Schedule

[Unselect all](#)

Submit Cancel

Select the Access Levels you wish the Door to be added to and click the arrow button to move the Access Level across to the "Access Levels assigned" list box. For each Access Level it is added to, it is possible to define the Schedule you wish to set for both Normal days and Holidays. Click "Submit" when finished. The Door would then appear in those access levels. Any people assigned to those access levels will also be able to gain access through that door.

Assign door to access levels

Select door

Demo Room

Available access levels

Search

Name

[Unselect all](#)

☐ Basement Access

☒ Development

☐ Floor 2 Access

☐ General Access

☒ Operations

☐ Secure Access

Access levels assigned

Search

Name

[Select all](#)

☐ Visitors

Basic working week

None

>

<

Submit Cancel

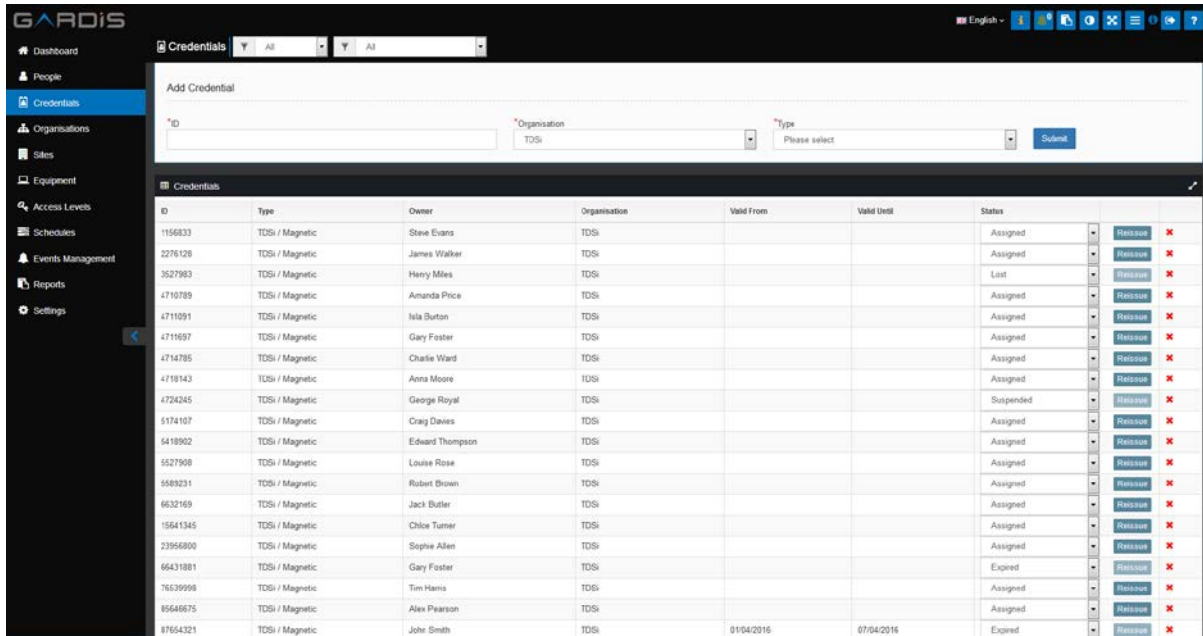
11 Credentials

Credentials must be assigned to a person before they can access an area through the door and reader. Navigate to the **Credentials** tab in the Navigation menu.

Enter the ID number of the Credential, then select the technology from the **Type** drop down menu, once complete, click **Add**.

Note that PIN Only cards have a default length of 8.

As you will see under the **Status** field, the status says **Available**. This means the Credential has been added and is ready to assign to a Person.



ID	Type	Owner	Organisation	Valid From	Valid Until	Status
1156033	TDSi / Magnetic	Steve Evans	TDSi			Assigned
2276126	TDSi / Magnetic	James Walker	TDSi			Assigned
3527963	TDSi / Magnetic	Henry Miles	TDSi			Lost
4710789	TDSi / Magnetic	Amanda Price	TDSi			Assigned
4711091	TDSi / Magnetic	Nila Burton	TDSi			Assigned
4711697	TDSi / Magnetic	Gary Foster	TDSi			Assigned
4714785	TDSi / Magnetic	Charlie Ward	TDSi			Assigned
4718143	TDSi / Magnetic	Anna Moore	TDSi			Assigned
4724245	TDSi / Magnetic	George Royal	TDSi			Suspended
5174107	TDSi / Magnetic	Craig Davies	TDSi			Assigned
5418902	TDSi / Magnetic	Edward Thompson	TDSi			Assigned
5527908	TDSi / Magnetic	Louise Rose	TDSi			Assigned
5589231	TDSi / Magnetic	Robert Brown	TDSi			Assigned
6632169	TDSi / Magnetic	Jack Butler	TDSi			Assigned
15641345	TDSi / Magnetic	Oliver Turner	TDSi			Assigned
23956890	TDSi / Magnetic	Sophie Allen	TDSi			Assigned
66431881	TDSi / Magnetic	Gary Foster	TDSi			Expired
76539998	TDSi / Magnetic	Tim Harris	TDSi			Assigned
85648675	TDSi / Magnetic	Alex Pearson	TDSi			Assigned
87654321	TDSi / Magnetic	John Smith	TDSi	01/04/2016	07/04/2016	Expired

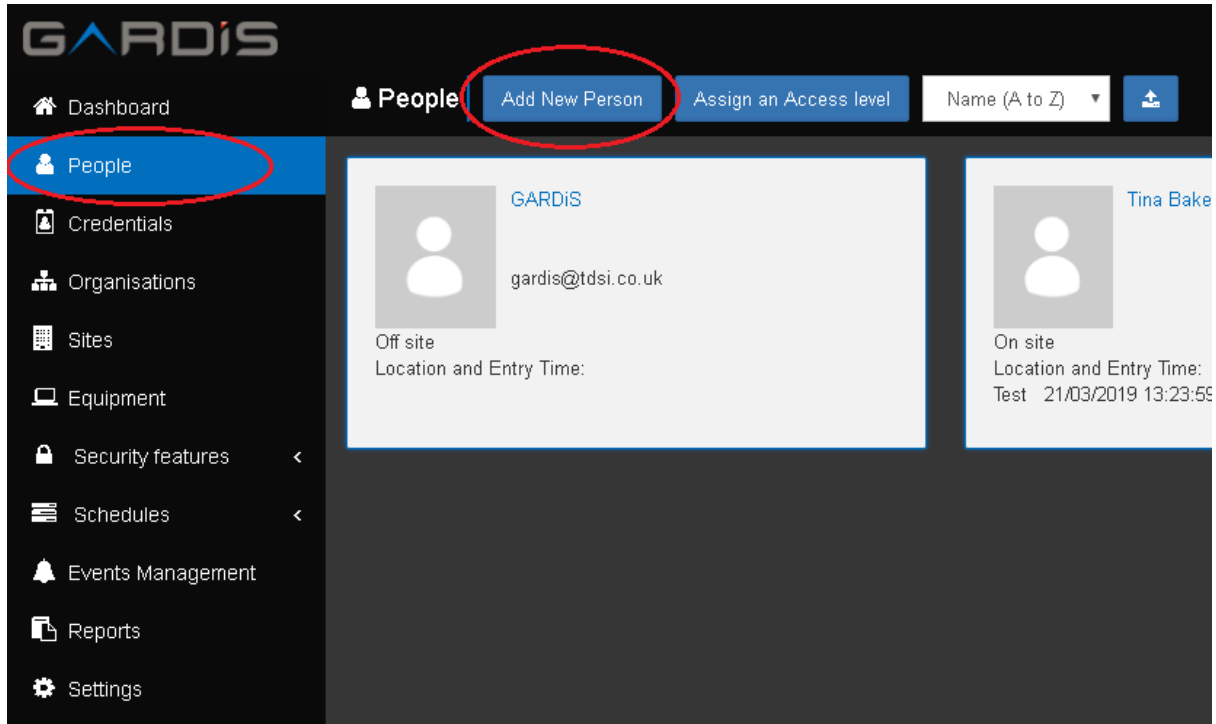
- **Assigned** – Assigned to a person and in use
- **Expired** – Previously assigned to a person who no longer requires it **or** the set timescale for it to be used in has passed
- **Damaged** – No longer usable due to damage
- **Suspended** – Temporarily out of use for any reason
- **Lost** – Was assigned to someone but the credential has been misplaced so is not active at the moment

NOTE: Changing the status of any credential will invalidate it in all ACUs.

12 People

12.1 Add Person

Navigate to the **People** tab in the Navigation menu to start, then click the **Add Person** button.



- **ID** – Set the unique identification number for the person or allow GARDiS to automatically set one. E.g. payroll or employee number, and it must be unique to that person in the GARDiS system
- **Department** - Every Department you've added in the Organisation tab will appear in this drop down list, select the relevant department from
- **Organisation** – Select organisation or it will default if only one is available
- **Job Title** – Enter the given name of the job the person does (optional)
- **Start date** – Enter the date the person began working at the company. This can be set in the future for new employees. If the start date is not known for existing employees then use today's date
- **End date** – If the person only requires access to the building during a certain timeframe e.g. a contractor for 1 month only, enter the end date. If no date is entered the person will remain valid on the system until they have their status changed by a User
- **Car Registration** – Enter the person's car registration
- **Person icon** – Click this icon to upload a picture of the person you're adding

Add New Person

×

1

Person details

2

Credential details

3

Security details

4

Summary

Person



Person Id

Leave blank to auto generate this

First Name

John

Last Name

Smith

*Organisation

Global

Department

None

Job Title

Developer

Start Date

dd/mm/yyyy

End Date

dd/mm/yyyy

Email

Car Registration

Previous

Cancel

Next

Finish

To assign a **Credential**, click "Next" to go to step 2. Click the **ID** box

Add New Person

×

1

Person details

2

Credential details

3

Security details

4

Summary

Credentials

ID

Type

Start Date

End Date

PIN

Status

Assigned

Clear

Previous

Cancel

Next

Finish

The assign credential pop up box will appear. From here you can either assign an existing credential or enter a number to add a new Credential. Click **Submit** to add the new Credential and assign it to the new person.

Add New Person

1 Person details
2 Credential details
3 Security details
4 Summary

Credentials

*ID	Type	Start Date	End Date	PIN	Status	
24534634	TDSi / Magnetic				Assigned	Clear
					Assigned	Clear

Previous
Cancel
Next
Finish

Add New Person

1 Person details
2 Assign Credential
3 Security details
4 Summary

Credentials

*ID

Previous
Next
Finish

Assign Credential

Credential number

Type

TDSi / Magnetic

Click submit to add new credential

Submit
Cancel

Now you've assigned a Credential you need to assign an Access Level, click "Next". The list of Access Levels will be displayed. Click on the sliders to assign person to Access Level. On this same screen, it is also possible to set the person to require Extended Access or they have Office Mode abilities.

Add New Person

1 Person details
2 Credential details
3 Security details
4 Summary

Access Levels

Access level

General Access

Member

Yes

Security Options

No Office Control

No Extended Access

Previous
Cancel
Next
Finish

Click "Next" to review the person configuration in the summary. Then click "Finish" to submit the New Person.

Add New Person ×



ID:

Display Name: John Smith

Credentials: 24534634

Access Levels: General Access

Previous

Cancel

Finish

12.2 Edit/Delete Person

To edit a person, click on the person card in the list of people. This will open the properties in editing mode. The delete button is also available in this view.


Fred Smith ×

Person details

Credential details

Security details

Person

	*Person Id	First Name	Last Name
	<input type="text" value="ID00000002"/>	<input type="text" value="Fred"/>	<input type="text" value="Smith"/>
	*Organisation	Department	Job Title
	<input type="text" value="Global"/>	<input type="text" value="None"/>	<input type="text"/>
Start Date	End Date	Email	Car Registration
<input type="text" value="dd/mm/yyyy"/>	<input type="text" value="dd/mm/yyyy"/>	<input type="text"/>	<input type="text"/>

Submit

Delete

Cancel

12.3 Import People

This section details how to import people and credentials into the GARDiS system.

12.3.1 File Configuration

A user can import people and their credentials from a file into the GARDiS system. When importing a file, the user can select the file's character encoding as Windows ANSI or Unicode UTF-8.

Windows ANSI uses the encoding loaded from the web.config. The default is ISO-8859-1 (Western European). Below is a table containing the fields that can be mapped within GARDiS along with the data type it supports.

GARDiS Field	Format Type	Example
Person Id*	String (Can be left empty with auto id)	ID000123
First Name	String	Taylor
Last Name	String	Smith
Organisation	String (Must match an organisation defined in system)	Global
Department	String (Must match department defined in system)	Development
Job Title	String	Manager
Email	String	Taylor.Smith@tdsi.co.uk
Car Registration	String	HJ60 7TB
Access Level	String (Must match access level defined in system)	General Access
Extended Access	String mapped to boolean. Accepted values for no extended access: "0", "false", "no". Accepted values for extended access: "1", "true", "yes".	true
Person Start Date	String (file format settings, date format to match. Default is dd/MM/yyyy)	21/03/2019
Person End Date	String (file format settings, date format to match. Default is dd/MM/yyyy)	21/06/2020
Credential Id	Integer	45346421
Type	String mapped to type, see table below.	Magnetic
PIN	Integer - (Limited to 4 digits)	2312
Credential Start Date	String (File format settings, date format to match. Default is dd/MM/yyyy)	21/03/2019
Credential End Date	String (File format settings, date format to match. Default is dd/MM/yyyy)	21/06/2020

* Mandatory Field

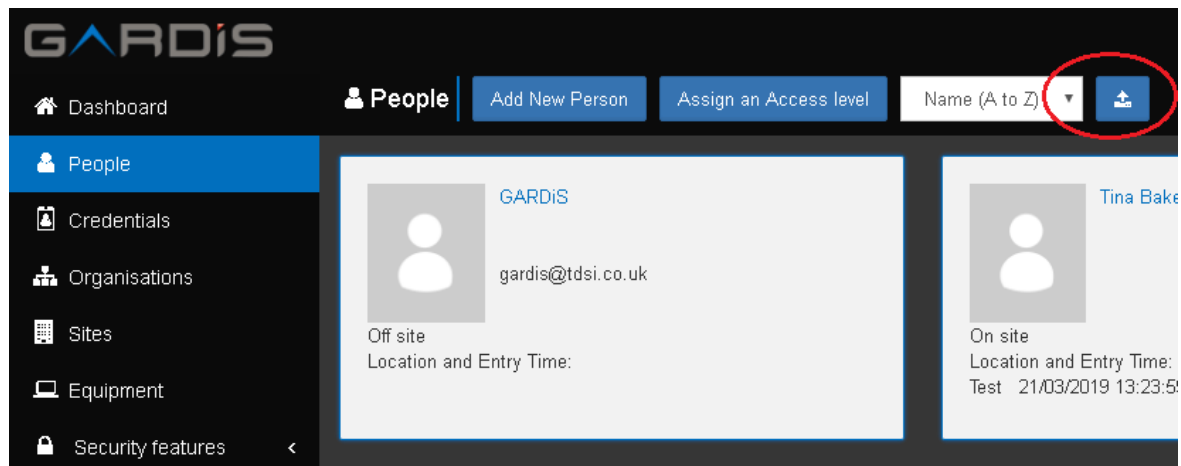
Credential Type
Microcard
TDSiWiegand
ASRProx
Magnetic
WiegandUnknown
Wiegand26Bit
Wiegand37Bit
Wiegand34Bit
Octopus44BitWiegand

MeLucky34BitWiegand
Octopus86BitWiegand
PinOnly

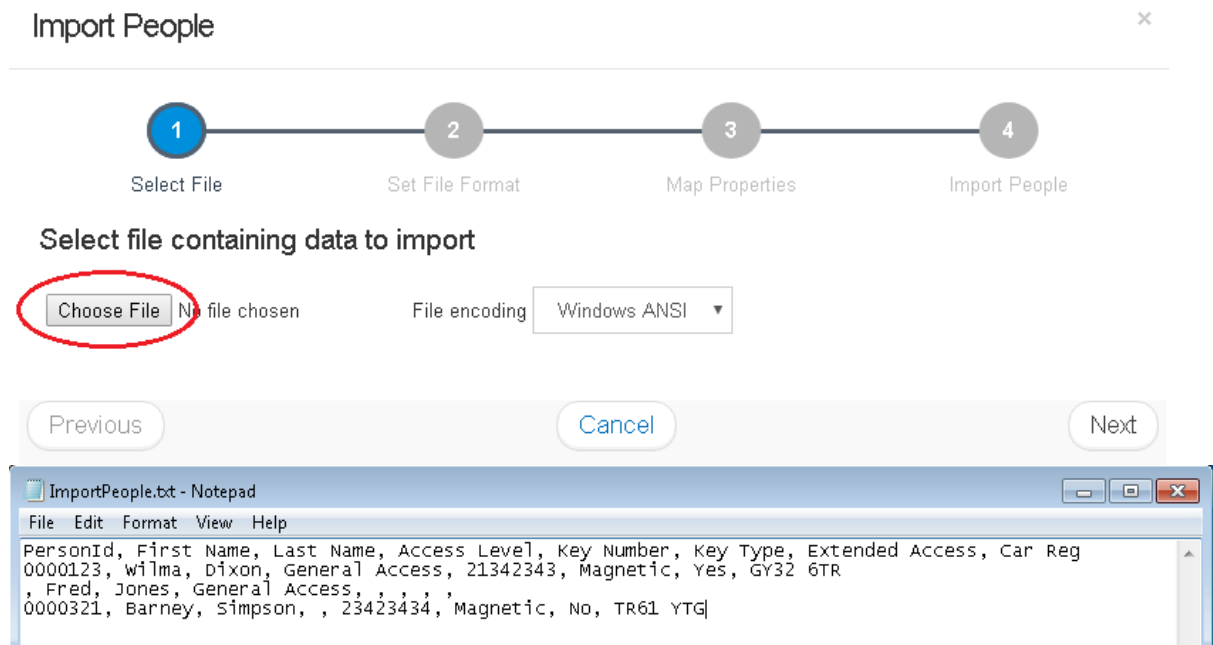
Note: String matching is not case-sensitive

12.3.2 Import Wizard

Click on the Import button within the People page. The Import Wizard will be displayed.



Step 1: Select the file to import. Below is an example of a text file using comma delimiter between columns.



Step 2: Define the settings within the import file. These include whether the file contains column headers, date formatting, the delimiter between columns and the string qualifiers if used. This step will also display a preview of the import data from the text file selected in Step 1.

Import People



1

Select File

2

Set File Format

3

Map Properties

4

Import People

Select file format settings

Delimiter Text qualifier No. of fields Date format

☒ Contains header

PersonId	First Name	Last Name	Access Level	Key Number	Key Type	Extended Access	Car Reg
0000123	Wilma	Dixon	General Access	21342343	Magnetic	Yes	GY32 6TR
	Fred	Jones	General Access				
0000321	Barney	Simpson		23423434	Magnetic	No	TR61 YTG

Previous

Cancel

Next

Step 3: Map the columns in the file to fields within the GARDiS System. If no Organisation is defined in the import file, the default will be applied. If the import has a credential number defined but no technology, it will use the default set. The drop down list contains the column headings from within the import file.



Select fields in imported file to map to properties in GARDiS

Defaults

If default values are selected these will be used when the mapped field is not defined or a mapping is not specified.

Organisation

Credential Type

Person Fields

Person Id

First Name

- Select field name
- PersonId
- First Name
- Last Name
- Access Level
- Key Number
- Key Type
- Extended Access
- Car Reg

Last Name

Organisation

Job Title

Email

Access level

Extended Access

Start Date

End Date

Credential Fields

ID

Type

PIN

Start Date

End Date

Previous

Cancel

Next

Step 4: Review the summary of the import.

Import People ×



Review file, format and mapped properties before import

File name

ImportPeople.txt

File format

Delimiter	Text qualifier	No. of fields
,		8
Date format	Contains header	
dd/MM/yyyy	Yes	

Mapped properties

Defaults

Organisation	Credential Type
Global	TDSi / Magnetic

Person Fields

ID	First Name	Last Name
PersonId	First Name	Last Name
Car Registration	Access level	Extended Access
Car Reg	Access Level	Extended Access
6 fields not mapped		

Credential Fields

ID	Type
Key Number	Key Type
3 fields not mapped	

Previous

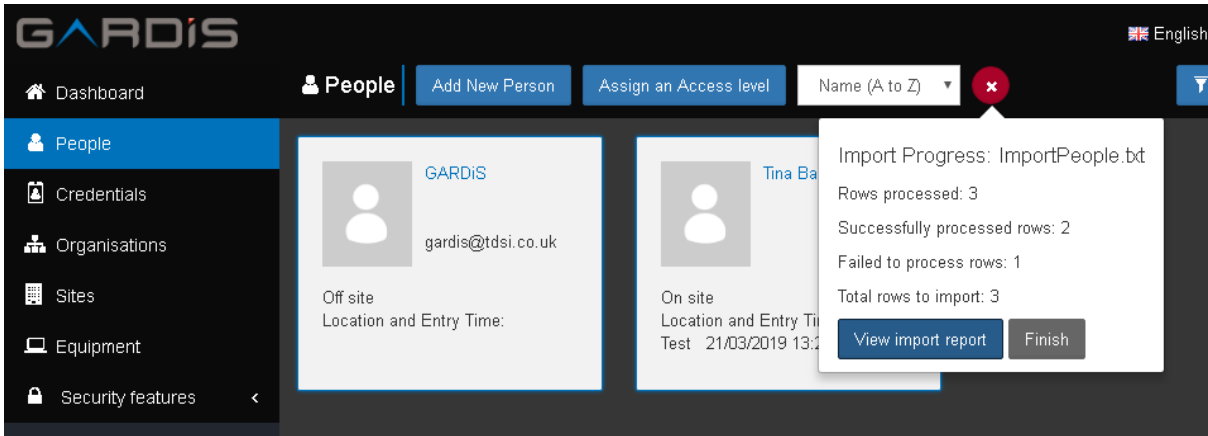
Cancel

Finish

12.3.3 Import Results

The import results can be reviewed in a number of places.

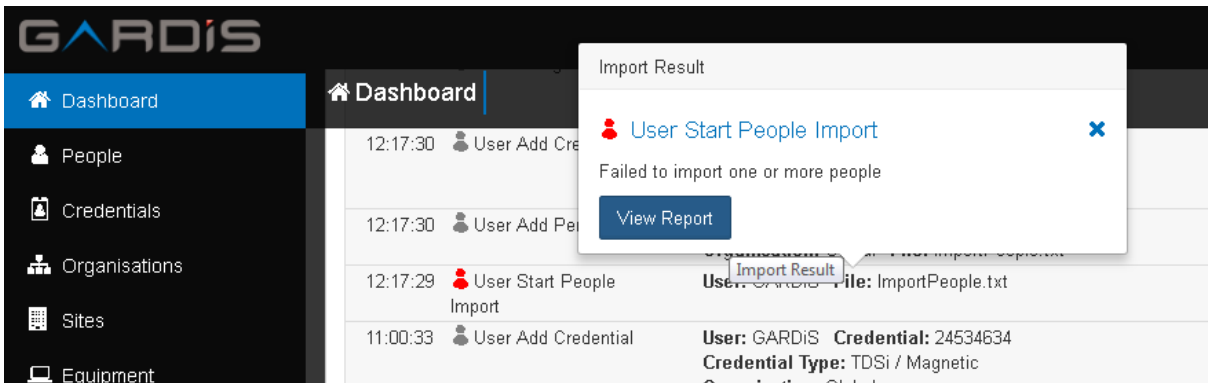
Initially, this can be viewed within the people section. The Import Button will indicate a result either by displaying a green tick or a red cross. Click the icon to view a summary and options to view the full report or Finish to reload the page with the items that successfully imported.



Click "View import report" will open the report within a new tab in the internet browser. The status against each row will indicate reasons of failure. Below is an example of a report.

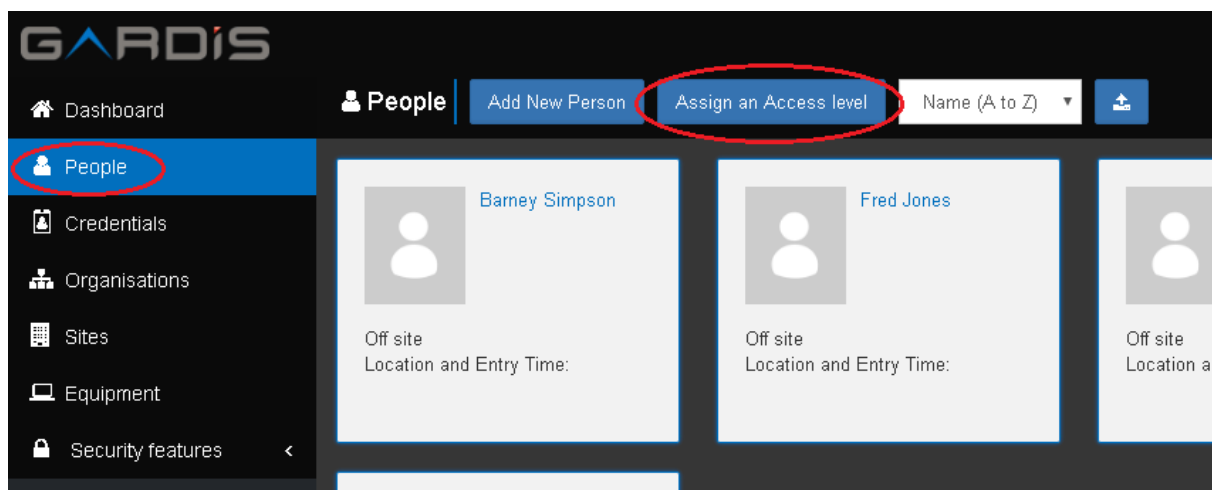
ImportPeople.txt								
Unique Ref	First Name	Last Name	Access level	Credential Number	Credential Type	Extended Access	Car Registration	Status
0000123	Wilma	Dixon	General Access	21342343	Magnetic	Yes	GY32 6TR	Success
	Fred	Jones	General Access					Failed to add credential
0000321	Barney	Simpson		23423434	Magnetic	No	TR61 YTG	Success

The report can also be retrieved from the event list. The event list will have an event "User Start People Import". The colour of the icon will indicate success or any failures. Clicking on the icon will display more information and the button "View Report". This will open the report in a new browser tab.

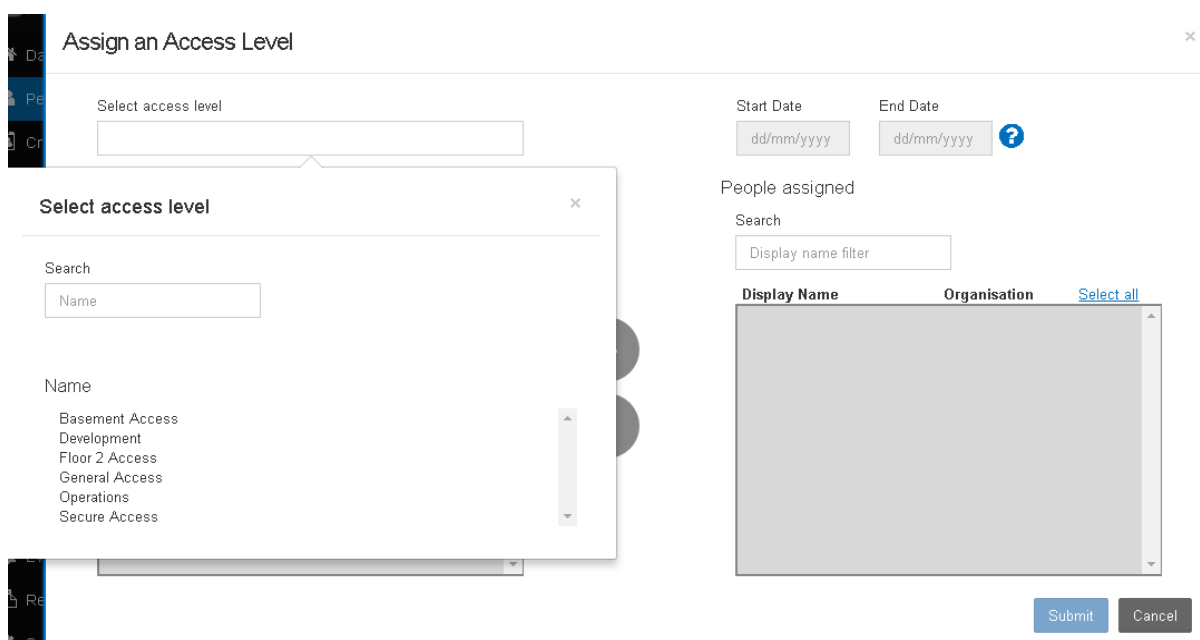


12.4 Assign Multiple People to an Access Level

Select "People" from the navigation pane and click the "Assign an Access Level" button.



A window will appear. Select the Access Level you wish to assign the people to by clicking in the text box.



If the Access Level already contains people, this will be displayed on the right hand side. The left hand side will contain people that are currently not within the Access Level. Select the people you wish to move into the access level. It is also possible to define a start and end date for temporary assignment to that Access Level. Click "Submit" to finish.

Assign an Access Level

×

Select access level

General Access

Start Date

dd/mm/yyyy

End Date

dd/mm/yyyy



People available

Search

Display name filter

Display Name Organisation [Unselect all](#)

<input checked="" type="checkbox"/>	Barney Simpson	Global
<input checked="" type="checkbox"/>	GARDIS	Global



People assigned

Search

Display name filter

Display Name Organisation [Select all](#)

<input type="checkbox"/>	Fred Jones	Global
<input type="checkbox"/>	Tina Baker	Global
<input type="checkbox"/>	Wilma Dixon	Global

Submit

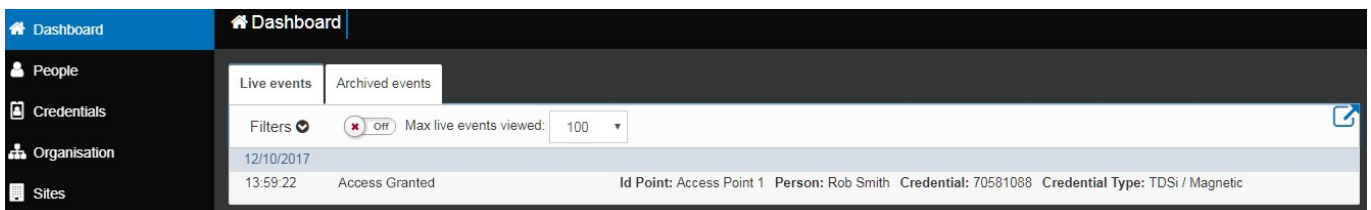
Cancel

13 System Test

Once the steps previous to this section have been completed, you are ready to now test the system to check it's been configured correctly.

To conduct this test, first navigate to the **Dashboard** tab in the Navigation menu.

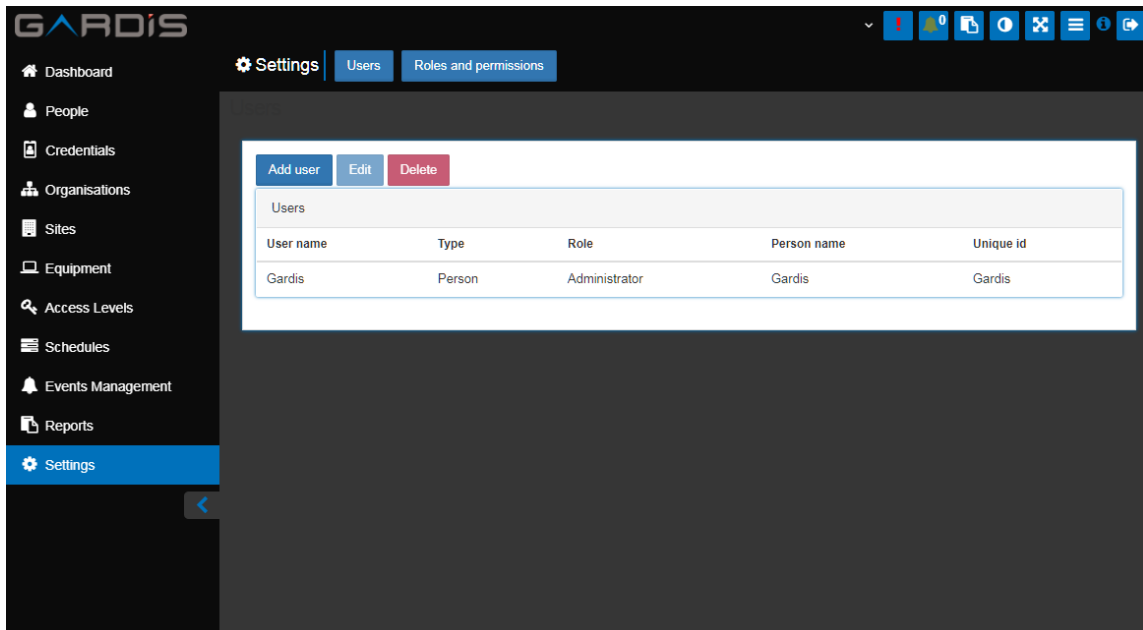
Once you're on the Dashboard, present the card to the reader and you will see the live event of Access Granted come through as a new event. This means the system has been configured correctly.



The screenshot shows the TDSi Dashboard interface. On the left is a navigation menu with options: Dashboard, People, Credentials, Organisation, and Sites. The main area is titled 'Dashboard' and contains a 'Live events' tab. Below the tab, there are filters and a 'Max live events viewed' dropdown set to 100. A table of live events is displayed, showing a date of 12/10/2017 and a time of 13:59:22. The event is 'Access Granted' and includes details: Id Point: Access Point 1, Person: Rob Smith, Credential: 70581088, and Credential Type: TDSi / Magnetic.

14 Settings

The Settings tab is where you'll be able to add users. Users will be given their own log in credentials to log into GARDiS. Depending on their Role and associated permissions that are given, they will be able to add and edit sections in GARDiS. Click **Add user** to begin.



14.1 Users

Now the User setup menu options are displayed, click the **Person** box.

The screenshot shows a 'User setup' modal window. At the top, it says 'Person' with a text input field. Below that, the 'User setup' section contains several fields: 'User name:' (required, with a person icon), 'Email:' (with an envelope icon), 'Password:' (required, with a lock icon), 'Confirm password:' (required, with a lock icon), 'Role:' (a dropdown menu showing 'select'), and 'Default language:' (a dropdown menu showing 'English'). A note at the bottom states: 'Minimum length 8 and include 1 uppercase, 1 lowercase, 1 numeric and 1 special character'. There is a checkbox labeled 'User must change their password when they next log in' which is checked. At the bottom right are two buttons: 'Add new user' and 'Cancel'.

A box will appear containing all the people currently added to GARDiS. Click the required Person.

Select person

Search

Name	Unique Reference
Sophie Brown	6265112
Toby Davis	564687
John Green	5725787
Rob Smith	41848

Once you've selected the required person, you can now set their **User name** and **Password**. When setting a password it must comply with the following criteria:

- Must be a minimum of 8 characters in length
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 special character e.g. ! ? #

Once the Username and Password have been set, you must select the **Role** of the person. This will set what level of access they have in the system, such as what they can see and what they can change.

Note: These can be customised by clicking **Roles and permissions** in the Settings tab

There are four roles configured in GARDiS by default and are editable:

- **Administrator** – Access to all areas of the system and can make changes, add or remove anything or anyone from all areas of GARDiS
- **Hardware systems manager** – Access to adding and removing equipment, sites, access levels and schedules
- **Operations manager** – Access to adding and removing people, assigning credentials. Access to editing Organisations and accessing reports
- **User operator** – Access to adding, removing people and assign credentials

Once complete, click **Add new user**.

User setup

Person

John Green

User setup

* User name:

John Green

* Password:

* Confirm password:

Email:

john.green@email.com

Role:

Administrator

Default language:

English

Minimum length 8 and include 1 uppercase, 1 lowercase, 1 numeric and 1 special character

☒ User must change their password when they next log in

Add new user

Cancel

By ticking this box the user will be required to change their password when they log in for the first time.

Choose the default language that will be displayed when the user logs in.

The user has been added successfully.

Settings

Users

Roles and permissions

Add user

Edit

Delete

Users				
User name	Type	Role	Person name	Unique id
Gardis	Person	Administrator	Gardis	Gardis
John Green	Person	Administrator	John Green	5725787

14.2 User Permissions

Once you've clicked the **Settings** tab in the Navigation bar, click **Roles and permissions**.

Role: Administrator

Add Edit Delete

Organisations Equipment Access Level Reports Schedules Roles

Organisations

Global

Permissions for Global

- ☒ Organisation Management
 - ☒ Can create organisations
 - ☒ Can edit this organisation
 - ☒ Can delete this organisation
 - ☒ Can view this organisation
 - ☒ Can use this organisation
- ☒ People and credential Management
 - ☒ Can add people and credentials
 - ☒ Can edit people and credentials
 - ☒ Can delete people and credentials
 - ☒ Can view people and credentials

- **Role** – Use the Role drop down menu to select the Role you want to set permissions for
- **Add** – Use the Add button to add a new Role
- **Edit** – Use the Edit button to edit the name of a Role
- **Delete** – Use the Delete button to delete a Role

14.2.1 Organisations

- **Organisation Management** – Use this tick box to enable or disable all organisation options at once
- **Can create organisations** – the user can create new organisations in GARDiS
- **Can edit this organisation** – the user can edit the name of this organisation and add departments
- **Can delete this organisation** – the user can remove the organisation from GARDiS
- **Can view this organisation** – the user can open the organisation and see further details
- **Can use this organisation** – the user can assign the organisation to other items
- **People and credential Management** - use this tick box to enable or disable all people and credential options at once
- **Can add people and credentials** – the user can add people and credentials to GARDiS
- **Can edit people and credentials** – the user can edit the details of a person or credentials

- **Can delete people and credentials** - the user can remove people and credentials from GARDiS
- **Can view people and credentials** – can open and view people and credentials in further detail

14.2.2 Equipment

Role: Administrator

Add Edit Delete

Organisations Equipment Access Level Reports Schedules Roles

Site

Site 1

Permissions for Site 1

- ☒ Site Management
- ☒ Can create sites
- ☒ Can edit this site
- ☒ Can delete this site
- ☒ Can view this site
- ☒ Can use this site
- ☒ Equipment Management
- ☒ Can add equipment to this site
- ☒ Can edit equipment for this site
- ☒ Can delete equipment on this site
- ☒ Can view equipment on this site
- ☒ Can control equipment in this site
- ☒ Equipment Event Management
- ☒ Can edit equipment events details for this site
- ☒ Can view equipment event details for this site
- ☒ Can view events for this site
- ☒ Can acknowledge alarms for this site

- **Site Management** – use this tick box to enable or disable all site options at once
- **Can create sites** – the user can add new sites to GARDiS
- **Can edit this site** – the user can edit the name of sites and add areas to the site
- **Can delete this site** – the user can delete this Site from GARDiS
- **Can view this site** – the user can view the site and open further details
- **Can use this site** – the user can assign site to other items
- **Equipment Management** – use this tick box to enable or disable all Equipment options at once
- **Can add equipment to this site** – the user can use the ACU wizard to set up new equipment or can add doors to existing ACU's
- **Can edit equipment** – the user can edit current equipment set up in GARDiS
- **Can delete equipment** – the user can remove equipment in GARDiS
- **Can control equipment in this site** – the user can control the ACU's and doors such as releasing the door
- **Equipment Event Management** – use this tick box to enable or disable all equipment event options at once
- **Can edit equipment event details for this site** – the user can edit the event details generated by equipment in this site

- **Can view equipment event details for this site** – the user will be able to see events generated by the equipment in further detail in the live events window
- **Can view events for this site** – the user can see events for this site
- **Can acknowledge alarms for this site** – the user will be able to acknowledge alarms raised by events

14.2.3 Access Level

Role: Administrator

Add Edit Delete

Organisations Equipment Access Level Reports Schedules Roles

Access Level

General Access

Permissions for General Access

- ☒ Access Level Management
- ☒ Can add access levels
- ☒ Can edit this access level
- ☒ Can delete this access level
- ☒ Can view this access level
- ☒ Can assign people to this access level

- **Access Level Management** – use this tick box to enable or disable all access level options at once
- **Can add access levels** – the user will be able to add new Access Levels to GARDiS
- **Can delete the access level** – the user can delete Access Levels
- **Can view the access level** – the user can open the Access Level and view it in further details
- **Can assign people to this access level** – the user can change or assign access levels to people

14.2.4 Reports

Role: Administrator

Add Edit Delete

Organisations Equipment Access Level Reports Schedules Roles

Permissions for All Reports

- ☒ Report Management
- ☒ Can create a report template
- ☒ Can edit a report template
- ☒ Can delete a report template
- ☒ Can view report templates
- ☒ Can run a report

- **Report Management** – use this tick box to enable or disable all report management options at once
- **Can create a report template** – the user can configure and run a report which will be saved for future use
- **Can edit a report template** – the user can edit the configuration of a previously ran report
- **Can delete a report template** – the user can delete a report that's stored in GARDiS

- **Can view report templates** – the user will be able to view the results of a stored report template
- **Can run a report** – the user will be able to run a report that's stored in GARDiS

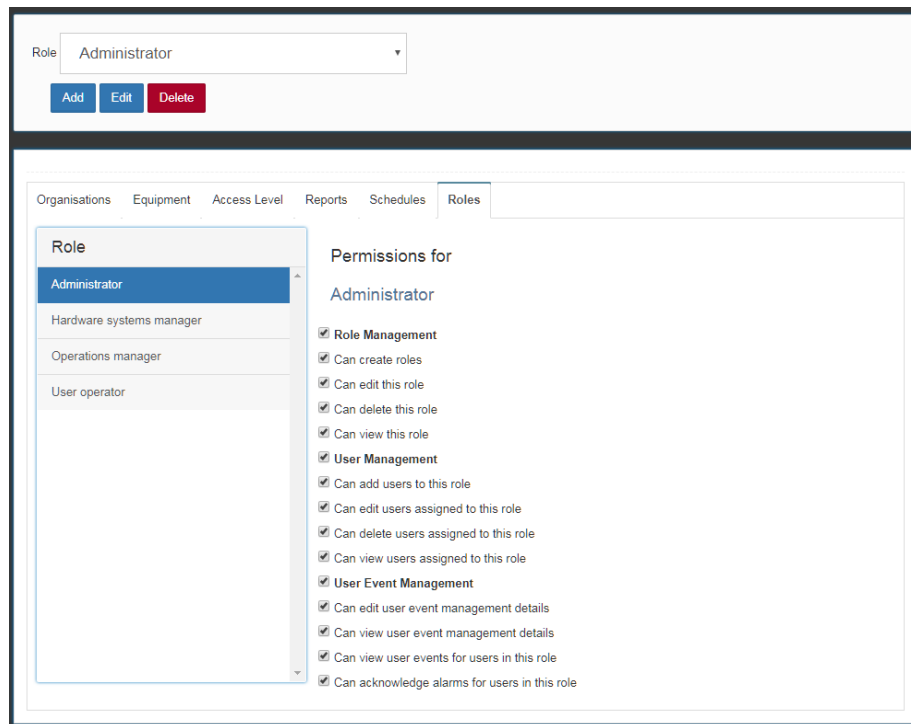
14.2.5 Schedules

The screenshot shows the 'Schedules' tab in the permissions configuration interface. At the top, a dropdown menu shows the role 'Administrator'. Below it are three buttons: 'Add' (blue), 'Edit' (blue), and 'Delete' (red). The main content area has a tabbed interface with 'Organisations', 'Equipment', 'Access Level', 'Reports', 'Schedules' (selected), and 'Roles'. Under the 'Schedules' tab, the section 'Permissions for All Schedules' lists several permissions, all of which are checked:

- ☒ **Schedule Management**
- ☒ Can create new schedules
- ☒ Can edit schedules
- ☒ Can delete schedules
- ☒ Can view schedules
- ☒ Can assign schedules to other resources

- **Schedule Management** – use this tick box to enable or disable all Schedule Management options at once
- **Can create new schedules** – the user can create new schedules
- **Can edit schedules** – the user can edit pre-existing schedules
- **Can delete schedules** – the user can remove schedules completely from GARDiS
- **Can view schedules** – the user can open schedules and view them in further detail
- **Can assign schedules to other resources** – the user can assign schedules, for instance assign a schedule to a door to determine its behaviour

14.2.6 Roles



- **Role Management** – use this tick box to enable or disable all Role Management options at once
- **Can create roles** – the user will be able to add new roles to assign to users
- **Can edit this role** – the user can edit the permissions and name of a role
- **Can delete this role** – the user can delete roles
- **Can view this role** – the user will be able to view what permissions are set for a role
- **User Management** – use this tick box to enable or disable all user management options at once
- **Can add users to this role** – the user will be able to add users to a role
- **Can edit users assigned to this role** – the user can edit the users that are assigned to a role
- **Can delete users assign to this role** – the user can delete users that are assigned to a role
- **Can view users assigned to this role** – the user can view which users are assigned to a role
- **User Event Management** – use this tick box to enable or disable all user event management options at once
- **Can edit user event managements details** – the user will be able to manage user events in the event management tab
- **Can view user event management details** – the user can view the configuration of the user events
- **Can view user events for users in this role** – the user can view user events in event list and reports
- **Can acknowledge alarms for users in this role** – the user will be able to acknowledge alarms raised by user assigned to this role

15 Event Management

Event Management is used to enable or disable events generated by different aspects of the system and also used to configure these events as alarms if required.

Once you have selected the required object type(s) by clicking on the **Select object type** box click **Go**. By clicking on the X by an object type you can remove it.

NOTE: User events cannot be disabled in GARDiS.

Events Management

Select object type: Door X Go

- IdPoint
- ACU
- User

Events

Show 10 entries Search:

Object type	Name	Message	Alarms	Enabled
No data available in table				

Showing 0 to 0 of 0 entries First Previous Next Last

In the example below we have selected Door from the drop down list and clicked **Go**.

You can now go through the list and enable or disable the events to be displayed in the system by clicking the on/off switches.

You can also select which events you want to trigger alarms in GARDiS. Once the alarm enabled event occurs in the system, it will trigger a pop up notification to appear in the top right of the screen.

Events Management

Select object type: Door X Go

Events

Show 10 entries Search:

Object type	Name	Message	Alarms	Enabled
Door	Door 1	Door Opened	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Door Closed	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Door Forced	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Door Open Too Long	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Extended Door Open Too Long	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Door Egress On	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Door Egress Off	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Reader Gone	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Reader Back	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On
Door	Door 1	Panel Disarm Timeout	<input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On

Showing 1 to 10 of 14 entries First Previous 1 2 Next Last

16 Alarms

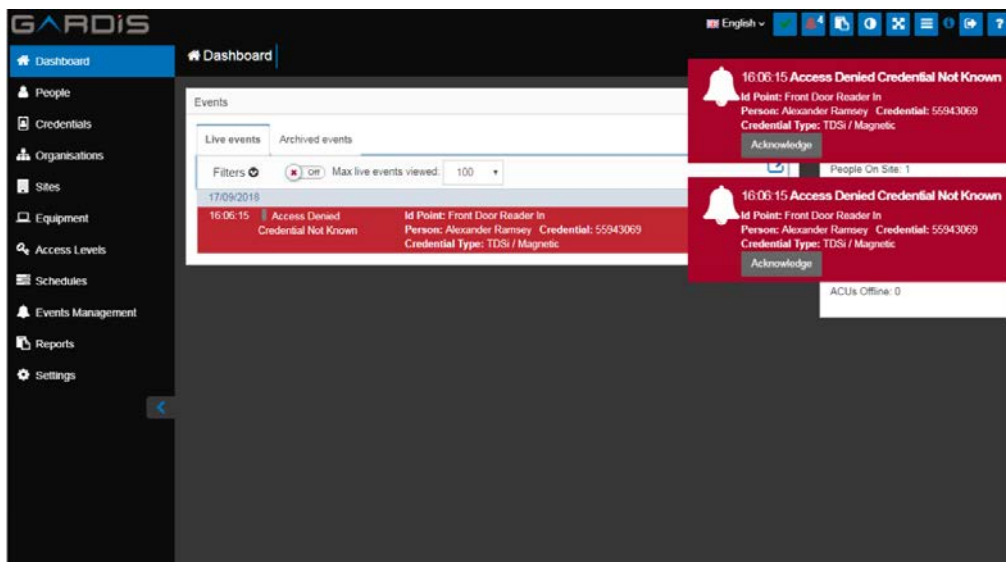
Alarms allow you to enable pop up notifications when certain events happen within the system. You can configure these notifications in the Events Management tab in the Navigation Menu. When one of your chosen Alarm events happen, you'll see a box appear in the top right hand corner of the screen.



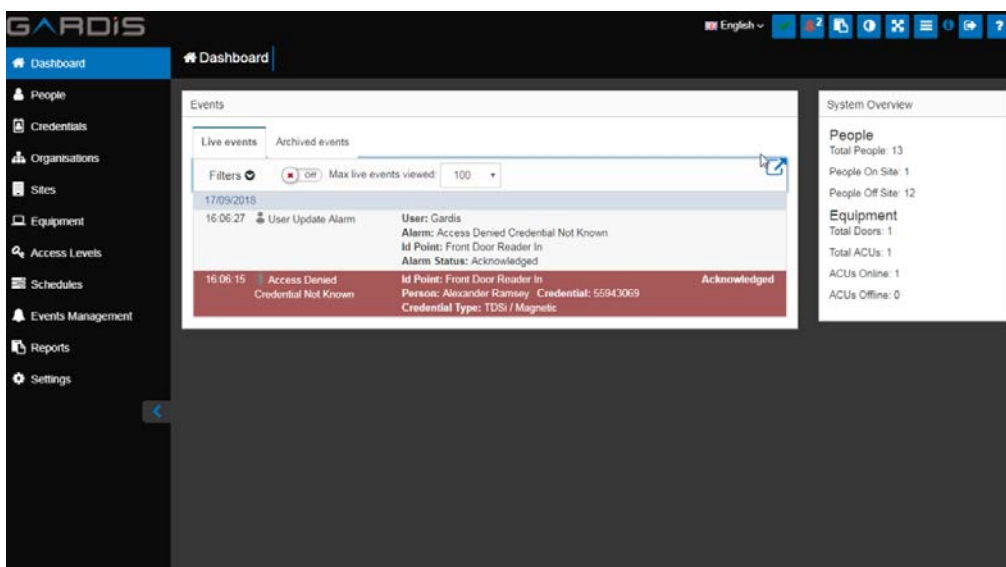
This displays the number of unacknowledged alarms in the system

When an alarm is triggered, you will see red pop up boxes such as the ones in the image below.

Click **Acknowledge** if the alarm does not require investigation.



Once the alarm has been acknowledged it will appear like so.

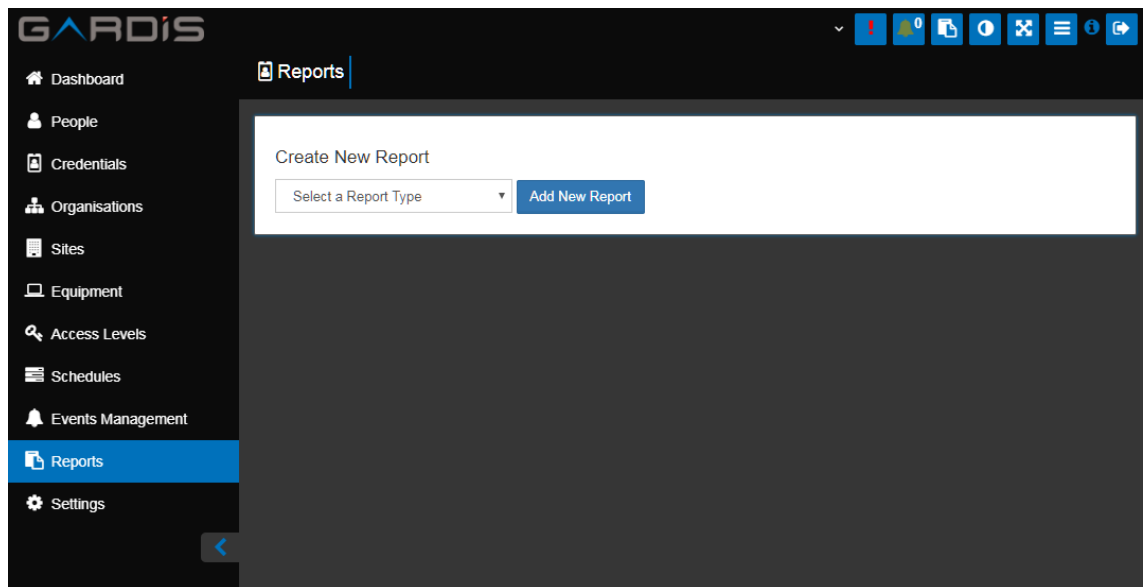


17 Reports

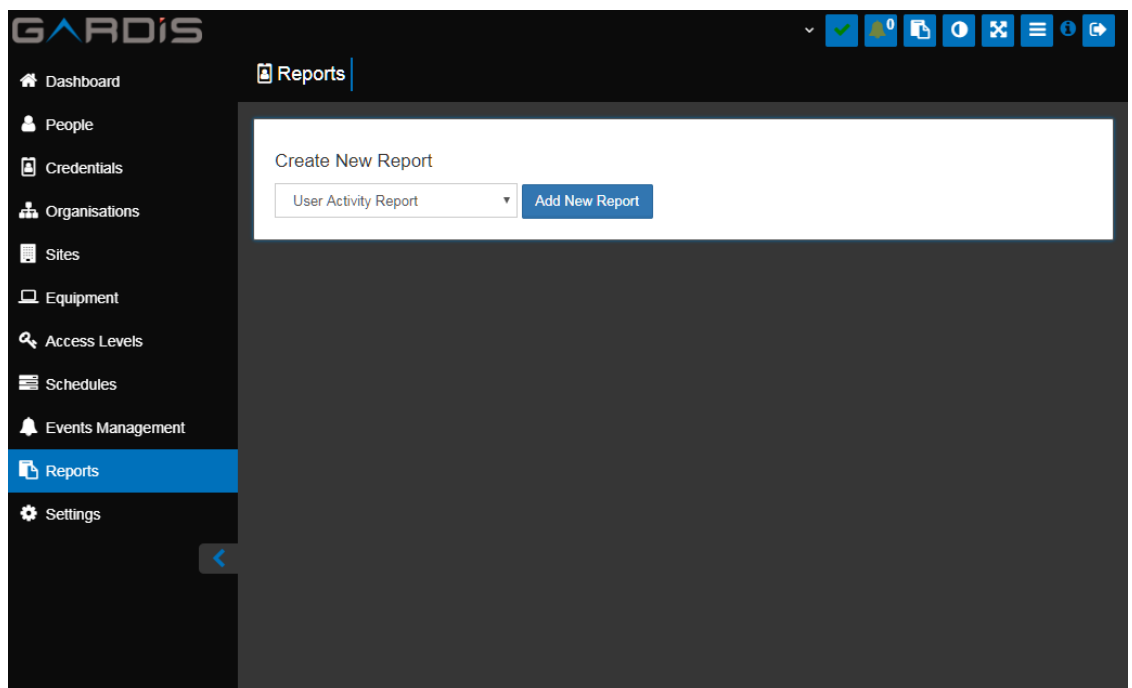
GARDiS has the functionality to run many different kinds of reports. Once you've created a report template, it can be re-run any time. So if it's a weekly report you have to run, there's no need to reconfigure it every week, it'll be waiting for you when you need it.

To begin, navigate to the **Reports** tab in the Navigation menu.

Under **Create New Report**, click the drop down menu to select the type of report you want to create.



Click **New Report** once you've selected the report type



For example, select User Activity Report:

- **All Users** - to run an activity report on all users active in GARDiS
- **Selected Users** - to select specific users to see their activity

User Activity Report

Cancel

1

2

3

4

Users

Events

Date and Time Range

Confirm Filters

Filter by User

☒ All Users
 ☐ Selected Users

Previous

Next

Next select:

- **All Events** - to see all events from users
- **Selected Events** - to select to see specific events only

User Activity Report

Cancel

✓

2

3

4

Users

Events

Date and Time Range

Confirm Filters

Filter by Event

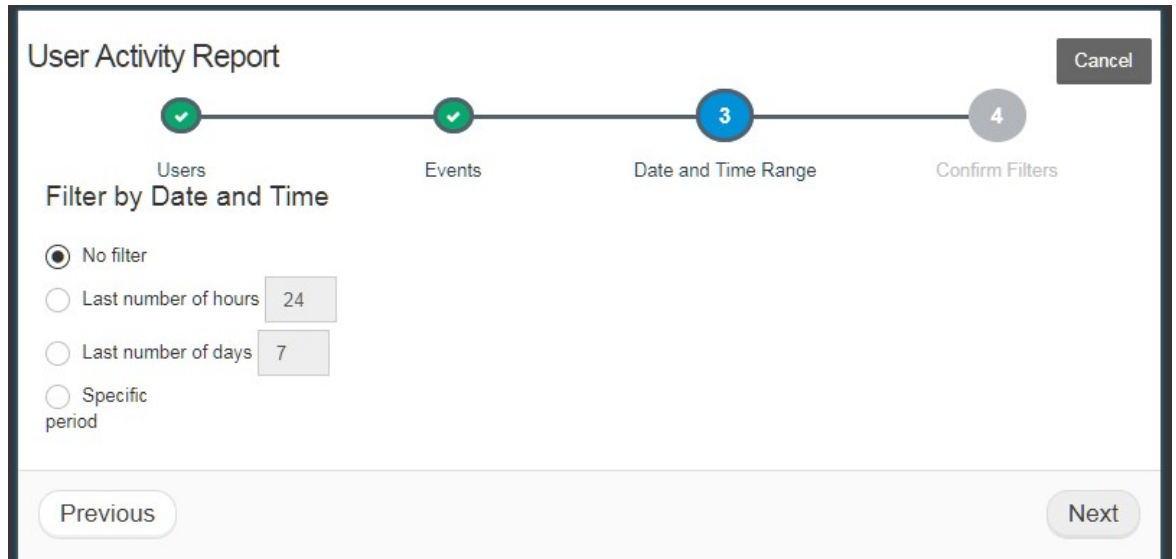
☒ All Events
 ☐ Selected Events

Previous

Next

Next select:

- **No filter** – to run the report and search the entire event list from the oldest event held to the newest
- **Last number of hours** - to define the number of hours prior to now that you want the report to go back by
- **Last number of days** - to define the number of days you want to run the report over
- **Specific period** - to define a certain time period to filter by



User Activity Report

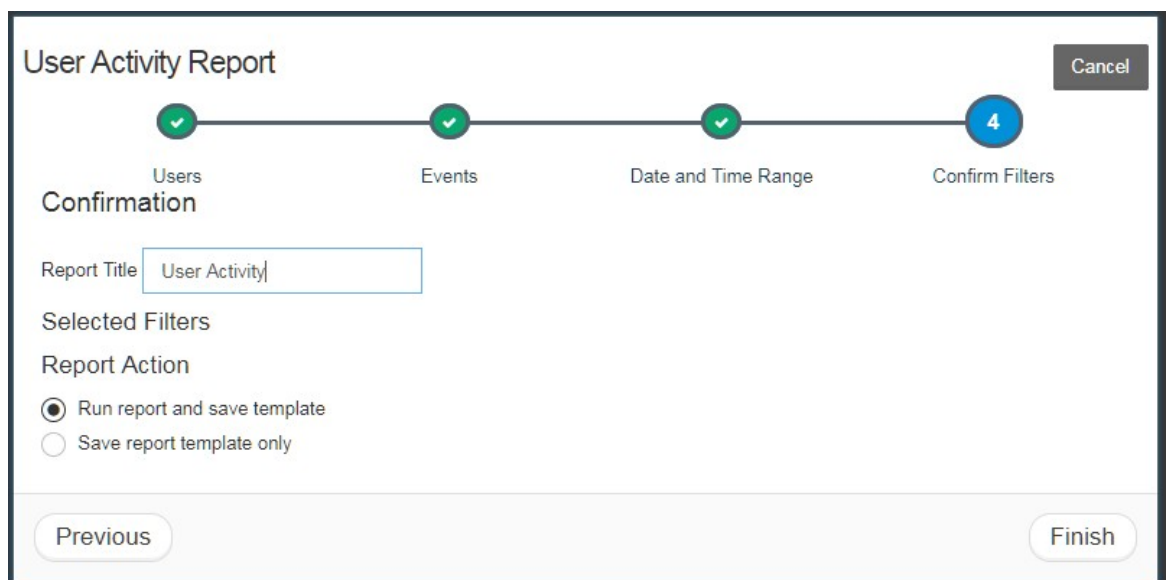
Progress: 1. Users (✓) 2. Events (✓) 3. **Date and Time Range** 4. Confirm Filters

Filter by Date and Time

☒ No filter
☐ Last number of hours
☐ Last number of days
☐ Specific period

Previous Next Cancel

Give the report a title, then click **Finish**.



User Activity Report

Progress: 1. Users (✓) 2. Events (✓) 3. Date and Time Range (✓) 4. **Confirm Filters**

Confirmation

Report Title

Selected Filters

Report Action

☒ Run report and save template
☐ Save report template only

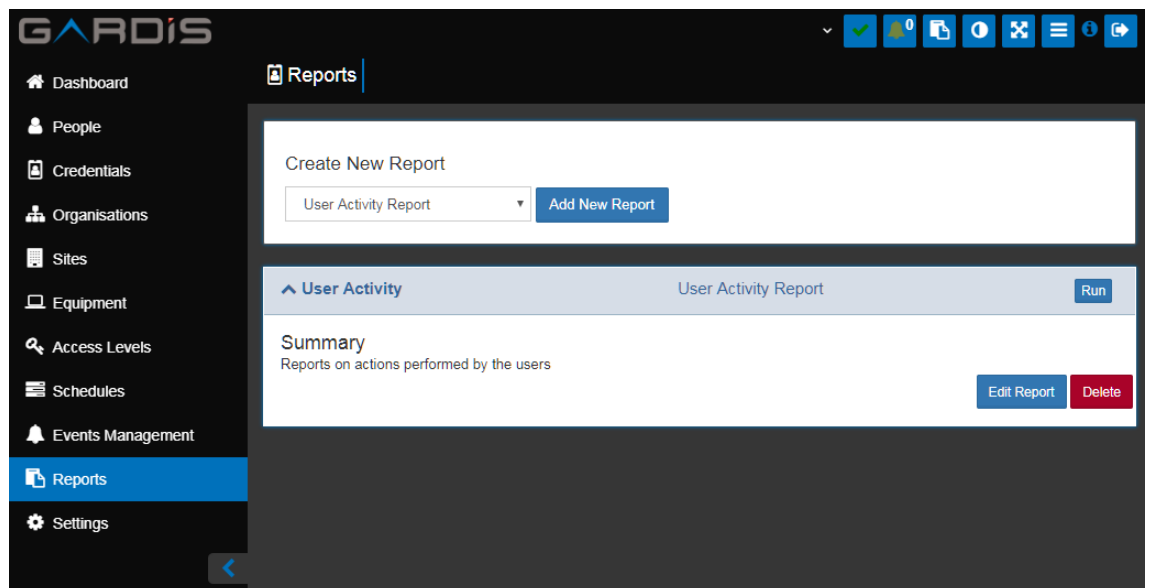
Previous Finish Cancel

As you can see, the report has generated, no user alarms were raised in the last 7 days.

Now you can save the file in the required format.

User Activity			
Show 100 entries		<div> <div>Re-run Report</div> <div>Print Report</div> <div>Save Report as CSV</div> <div>Save Report as PDF</div> </div>	
		Search: <input type="text"/>	
Event Time	User	Event Message	Event Sources
26/07/2018 12:34:29	Gardis	User Login	Role: Administrator;
26/07/2018 12:34:50	Gardis	User Changed Password	Role: Administrator;
26/07/2018 12:34:52	Gardis	User Logout	Role: Administrator;
26/07/2018 12:35:02	Gardis	User Login	Role: Administrator;
26/07/2018 12:35:23	Gardis	User Add Credential	Credential: 3646366; Organisation: Global; CredentialType: TDSi / Magnetic; Role: Administrator;
26/07/2018 12:35:24	Gardis	User Add Person	Person: Test; Organisation: Global; Role: Administrator;
26/07/2018 12:35:26	Gardis	User Assign Credential	Organisation: Global; Credential: 3646366; Person: Test; Role: Administrator;
26/07/2018 12:37:33	Gardis	User Add Area	Area: Front Door; Site: Site 1; Role: Administrator;
26/07/2018 12:37:33	Gardis	User Add Area	Area: Car Park; Site: Site 1; Role: Administrator;
26/07/2018 12:37:34	Gardis	User Assign Area to Site	Area: Car Park; Site: Site 1; Role: Administrator;
26/07/2018 12:37:34	Gardis	User Assign Area to Site	Area: Front Door; Site: Site 1; Role: Administrator;

The report will be saved in GARDiS for you to run again as required.



The screenshot shows the GARDiS Reports interface. On the left is a sidebar with navigation links: Dashboard, People, Credentials, Organisations, Sites, Equipment, Access Levels, Schedules, Events Management, Reports (highlighted), and Settings. The main content area is titled 'Reports' and contains a 'Create New Report' section with a dropdown menu showing 'User Activity Report' and an 'Add New Report' button. Below this is a 'User Activity' report card titled 'User Activity Report' with a 'Run' button. The card also includes a 'Summary' section stating 'Reports on actions performed by the users' and buttons for 'Edit Report' and 'Delete'.

18 ACU

An ACU (Access Control Unit) is what allows access to each person access through the doors connected to it.

The ACU (Access Control Unit) will be loaded with Credentials (card or fob numbers) and will only grant access to any of the Credential it knows. Any Credential which is not allowed access through its doors (controlled by GARDiS), will not be loaded into the ACU.

If access is granted, an on board relay will change state and complete or break (dependent on if the door is Fail-Safe or Fail-Secure) the circuit for the lock. This will release the lock and the door can be opened.

As part of creating a new ACU in GARDiS, you will be configuring how many & how to use the doors the ACU will be controlling. This will also lead to the reader configuration (how many readers per door).

Each ACU will have a UID (Unique Identifier) which is not duplicated on any other controller. Each ACU model will start with certain values which can help determine what ACU model it is:

ACU Model	UID Starting Ref
Expert	1-xxx-xxx-xxx
Expert Slave / Expander2	2-xxx-xxx-xxx
Excel2	3-xxx-xxx-xxx
Excle4	4-xxx-xxx-xxx
MICROgarde II	5-xxx-xxx-xxx
MICROgarde I	6-xxx-xxx-xxx

19 Cards

Once the TDSi Access Control System has been installed, commissioned and handed over to the end user, it's their responsibility to look after their cards.



Once a credential has been reported as lost/stolen the credential status should be changed from "Assigned" to "Lost".

If a credential is damaged in a way that means it cannot be used anymore its status should be changed to "Damaged".

If a credential needs to be stopped from working for some other reason change the status of it to "Suspended"

Any credential with a status of Lost/Damaged/Suspended will be removed from the ACUs and therefore will no longer allow access to be granted.

20 Icons



Access Levels



Change Contrast



Credentials



Dashboard



Edit



English Language



Equipment



Event Management



Expand Nav Menu



French Language



Full Screen



Grid View Enabled



Grid View Disabled



List View Enabled



List View Disabled



Hide ~~Nav~~ Menu



Logout



Alarm Notifications



Open in new tab



Organisations



People



Live Event Tab



Schedules



Settings



Sites



System Error



System Warning