GARDiS Controller Embedded Web Server

User Manual

UM0121 Issue 3

Foreword

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

Five years warranty included. For further terms of guarantee, please contact your supplier.

Trademarks

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.

Contents

1. Introduction

Thank you for purchasing your TDSi GARDiS Controller door access control system.
There are 3 main types of GARDiS master controller: -

- **GARDiS 1**
  - 1-door controller with connections for 1-2* readers.
- **GARDiS 2**
  - 2-door controller with connections for 2-4* readers.
- **GARDiS 4**.
  - 4-door controller with connections for 4-8* readers.

The GARDiS controller is operated independently and requires no separate software installation.

Configuration of the access control system is provided to the user via an embedded web server that can be accessed from any compatible web browser.

The GARDiS controller can operate as a master controller with up to 10** extension modules. Extension modules include slave GARDiS controllers that can allow capacity for up to 44 doors, I/O modules allowing the monitoring and control of equipment and wireless IP Locks***. More information on these extension modules will also be provided in this manual along with installation guides.

This manual will guide you through the configuration of GARDiS controllers via the embedded web server.

* The upper limit requires TDSi readers for the Reverse LRC protocol (In/Out Readers).
** Licensing dongle is required to allow more doors on the system.
*** Wireless IP Locks is limited to 10 doors.

2. Information and Recommendations

In accordance with the European directive UTE C00-200 incorporating directives 2004/108/CE, GARDIS complies with the following standards:

CE

- NF EN 50081-1 governing electromagnetic radiation
- NF EN 50082-1 governing electromagnetic susceptibility

3. Specification

TDSi Part No.	GARDiS 1 5002-6001 GARDiS 2 5002-6002 GARDiS 4 5002-6004
Features	
Max	5000 Credentials
Doors	1,2 or 4 doors
Readers	Up to 2 TDSi readers **per door** in a read-in read-out configuration. Alternatively, 1 reader per door equipped with industry standard clock & data, Wiegand multiformat or RS 485 output formats.
Inputs	1 per door Additional available with I/O Module
Outputs	Control Relay: 1 A / 12V - 1A / 24v 1 used per installed door GARDIS 1: 2 Outputs GARDIS 2: 3 Outputs GARDIS 4: 5 Outputs
Expansion Options	GARDiS 4+ (4 door); 8 Inputs/8 Outputs module; Wireless IP Locks
Time Groups	128
Anti-Passback	Timed and true
Mantrap Function	Yes
Communications	TCP/IP and RS 485 for extension modules

4. Setting the IP Address

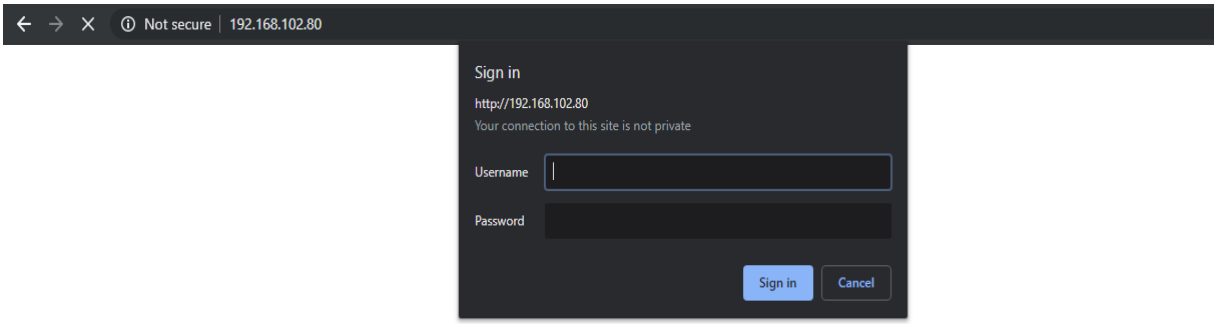
Static IP Mode: Default IP Address is 192.168.2.150 Subnet mask 255.255.255.0

The computer used to connect to the unit must have an IP Address within the 192.168.2.xxx range.

Step 1

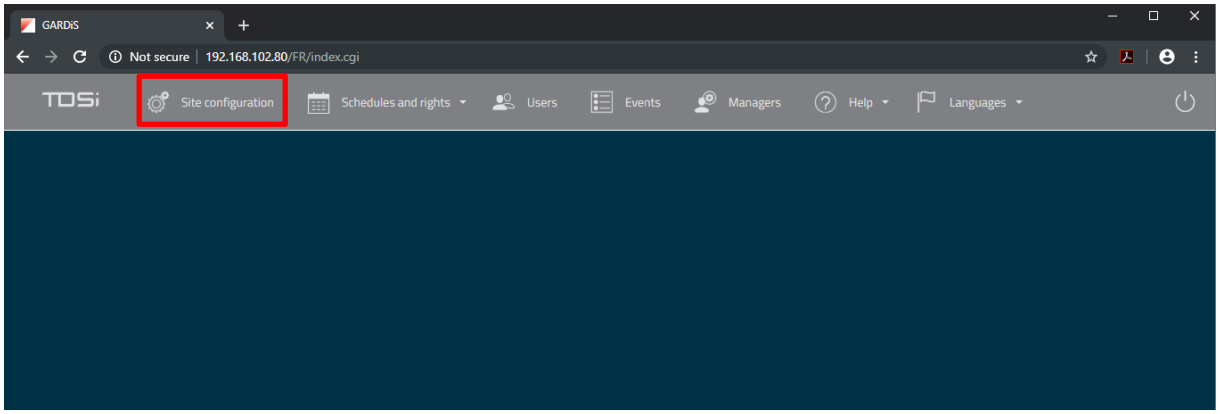
Open a web browser e.g. Chrome, Firefox, Microsoft Edge.
Enter the IP Address 192.168.2.150

A pop-up box will appear.
Enter the username: admin
Password: Printed on the sticker located on the plastic case of the GARDiS unit.



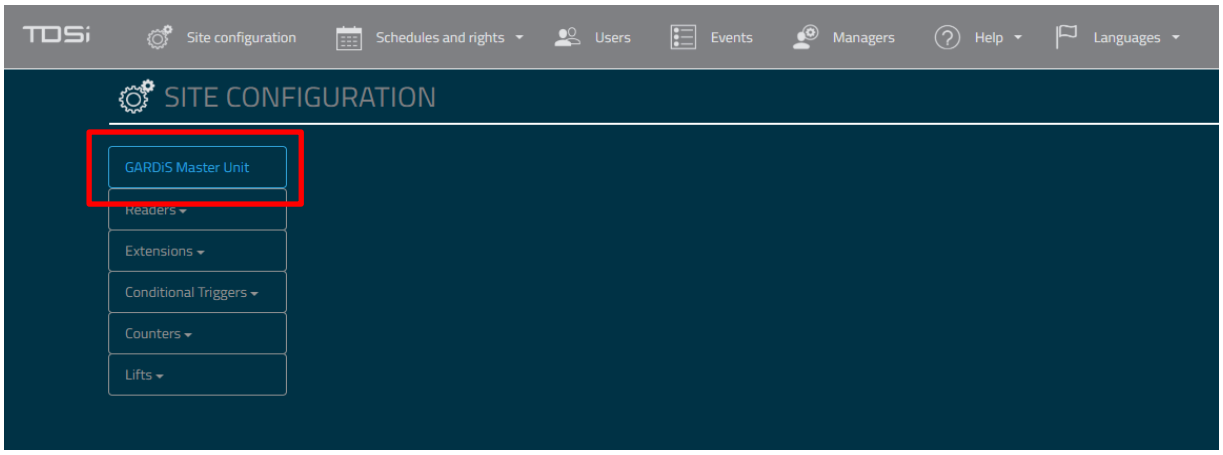
Step 2

After login, the following screen is displayed. **Click Site configuration.**



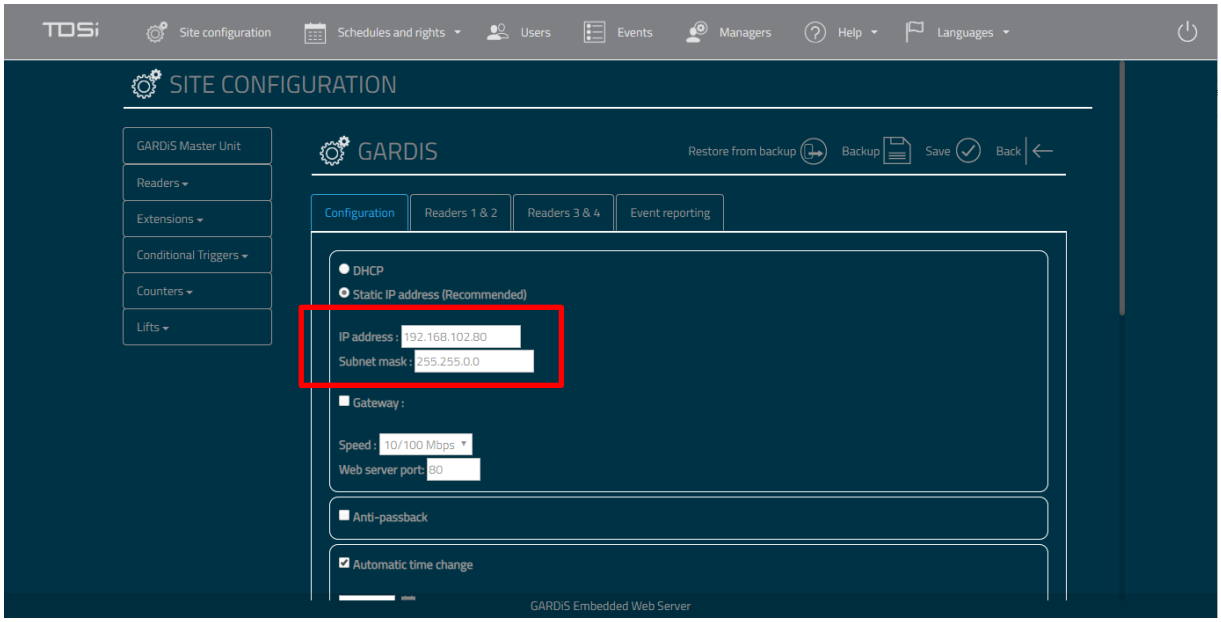
Step 3

Click GARDiS Master Unit from menu.



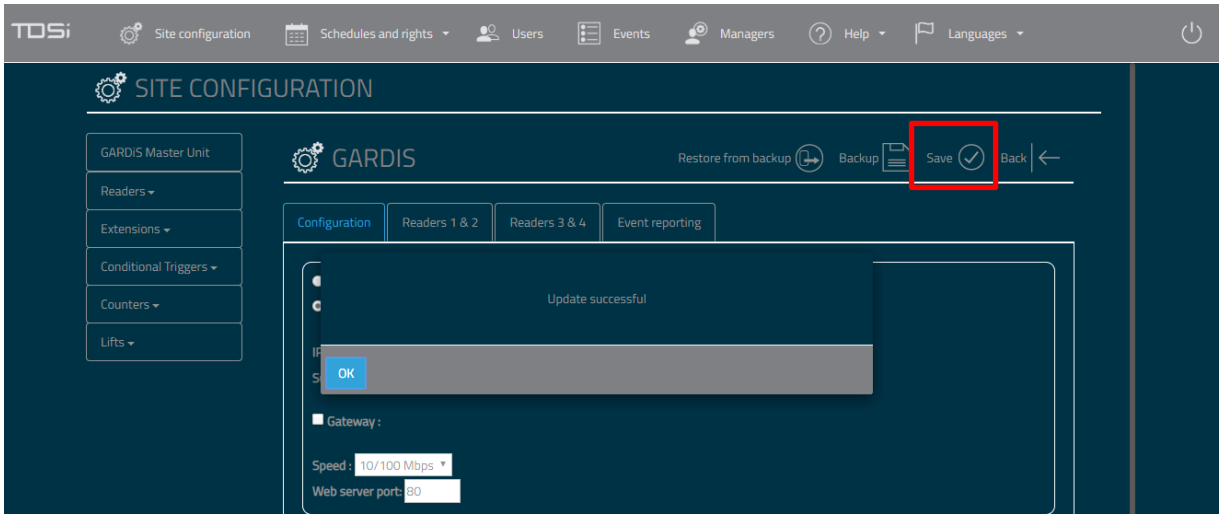
Step 4

Enter the required IP settings.



Step 5

Click Save



5. Validating a credential

This chapter steps you through setting up a door controller unit to give an "**access granted**" to a credential.

Step 1

Select the reader configuration

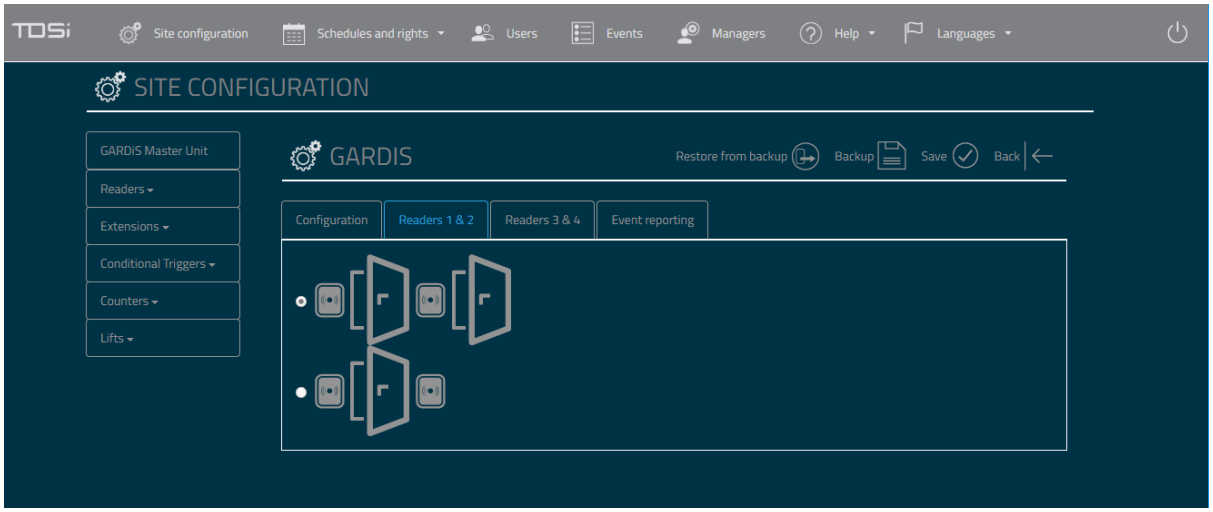
Option 1 - 1 reader per door

e.g. Reader channel 1 mapped to door 1, Reader channel 2 mapped to door 2

Option 2 – In/Out reader per door

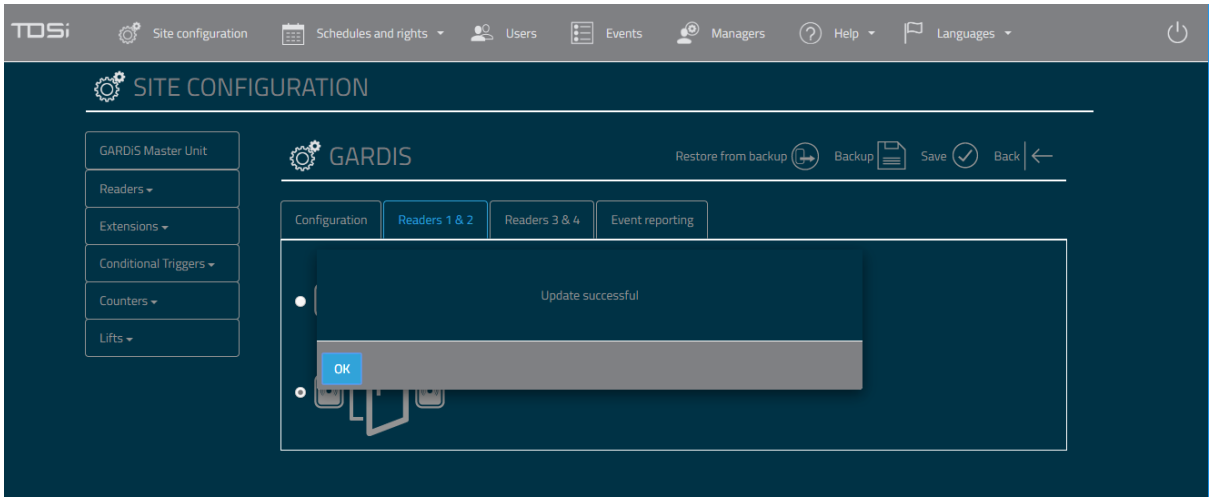
e.g. Reader channel 1 mapped to door 1 (In reader), reader channel 2 mapped to door 1 (Out reader)

Note: To configure the controller for reverse LRC, option 1 is the option to select. Limitations to reverse LRC include access group rights (inherit from main reader) and conditional triggers (only the main reader can be selected).



Step 2

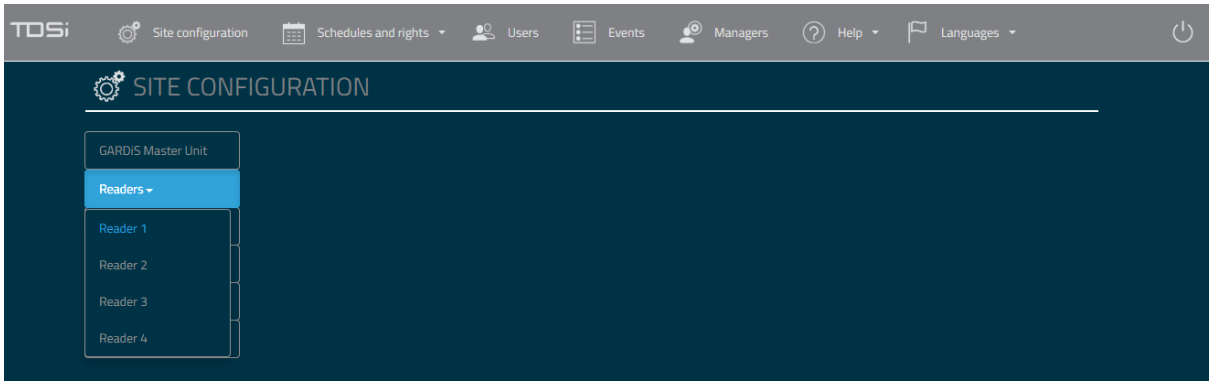
Click Save.



Step 3

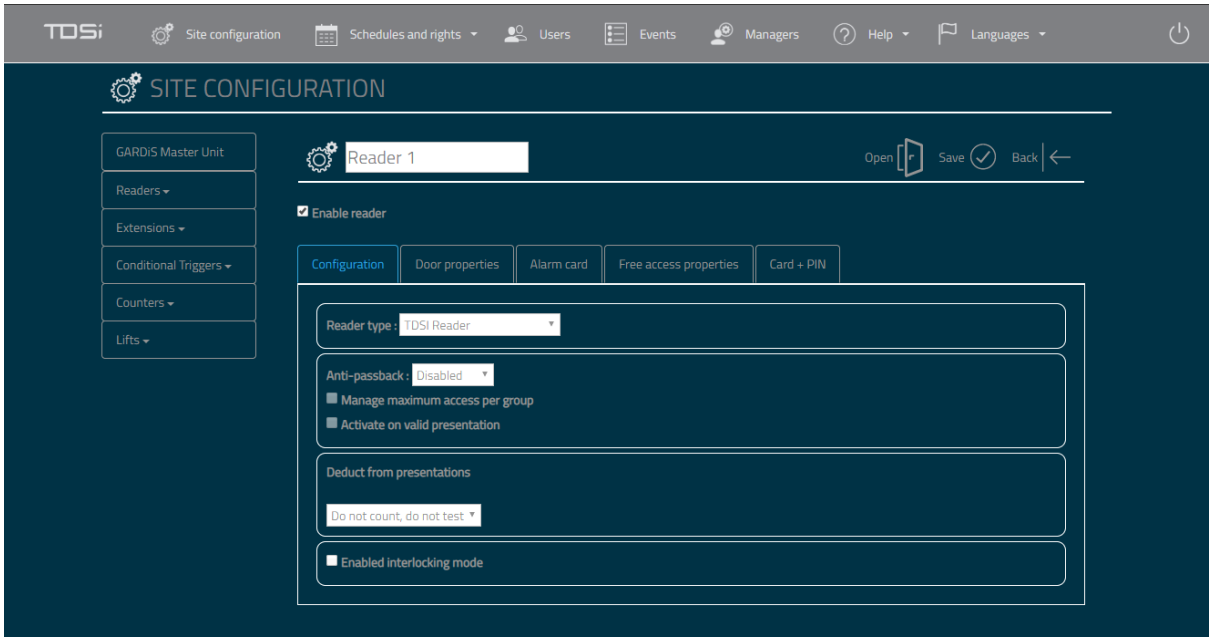
Configure Readers.

Select the reader to configure i.e. Reader 1.



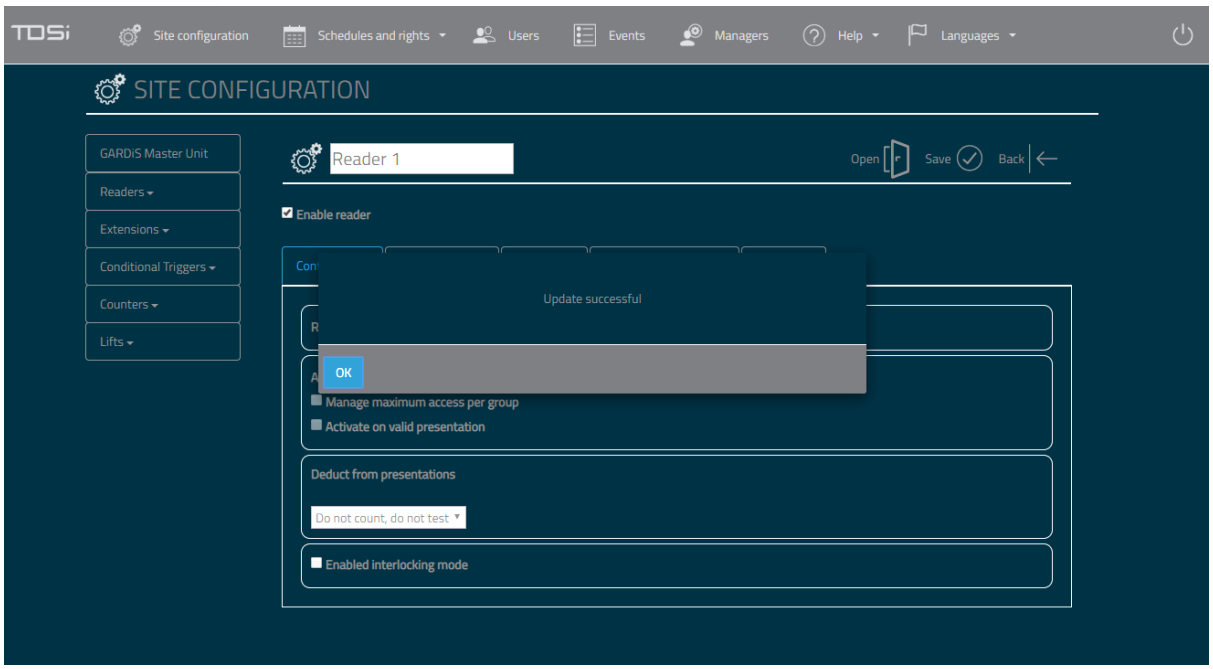
Step 4

Set reader type to TDSi Reader.



Step 5

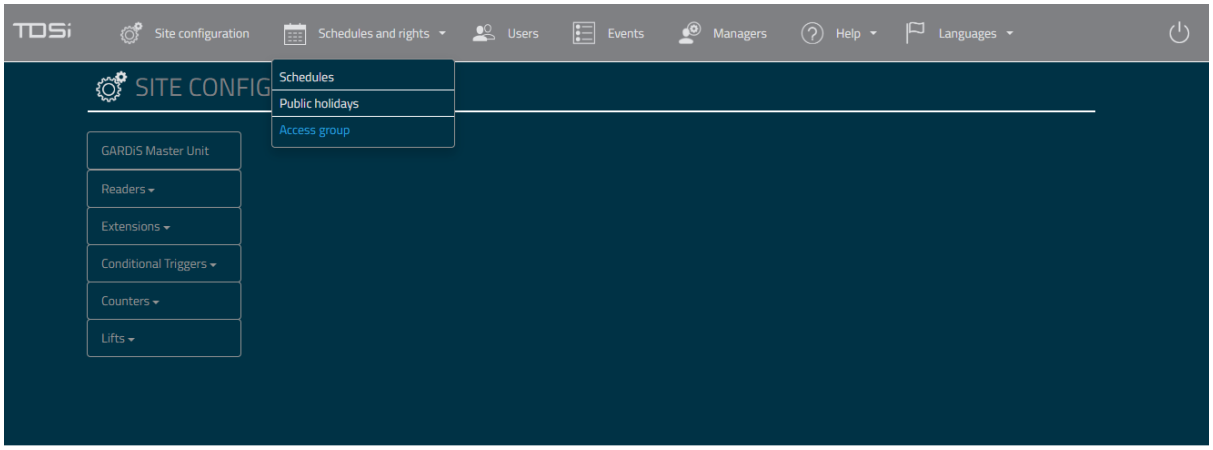
Click Save.



Step 6

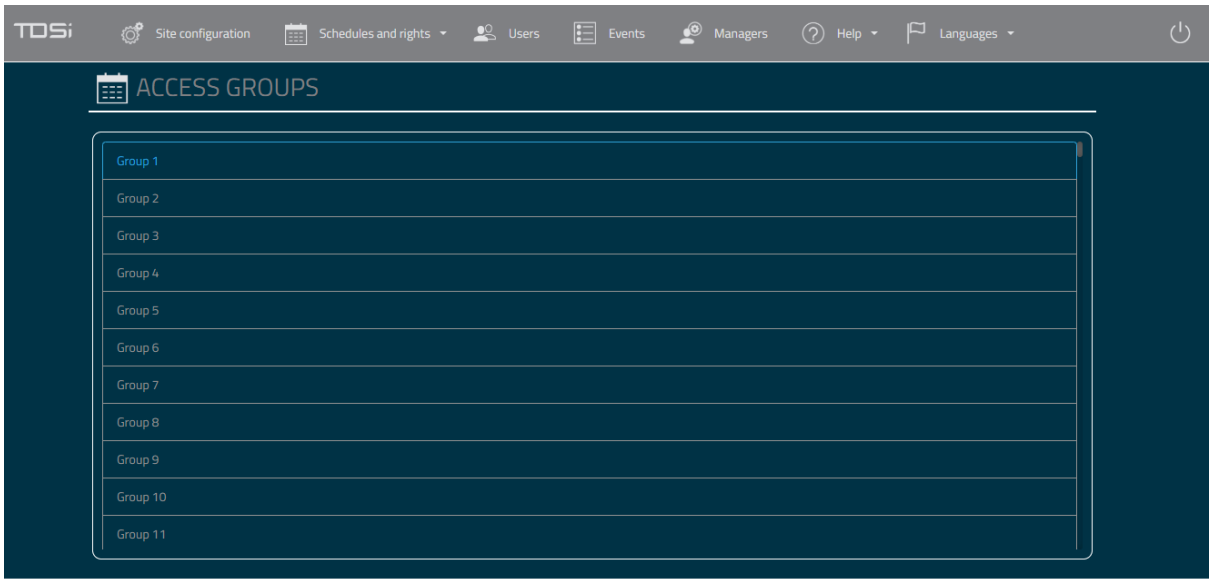
Set up the Access Groups

Add readers to the required access group. Note: A reader must belong to at least 1 access group in order to gain access (Access granted).



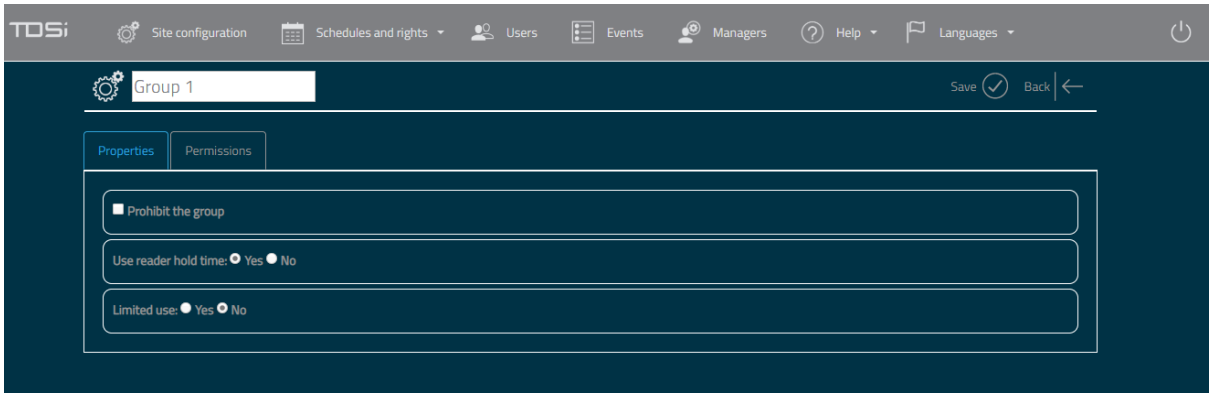
Step 7

Select Group 1.



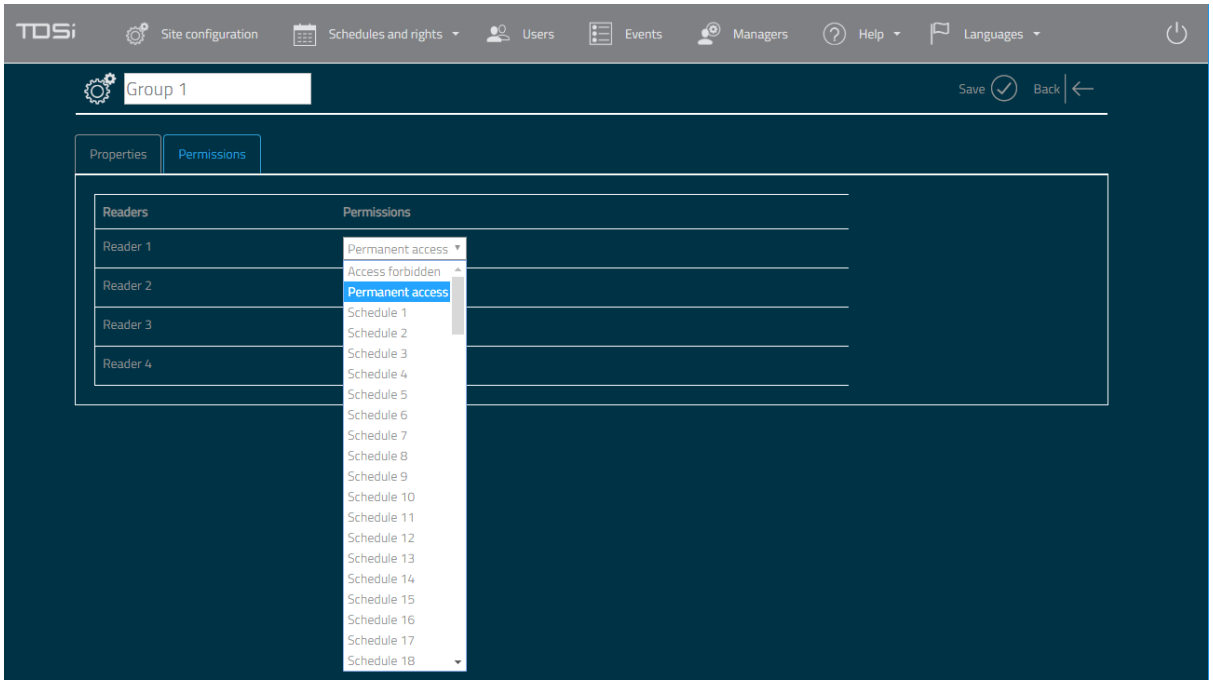
Step 8

Untick Prohibit the group checkbox.



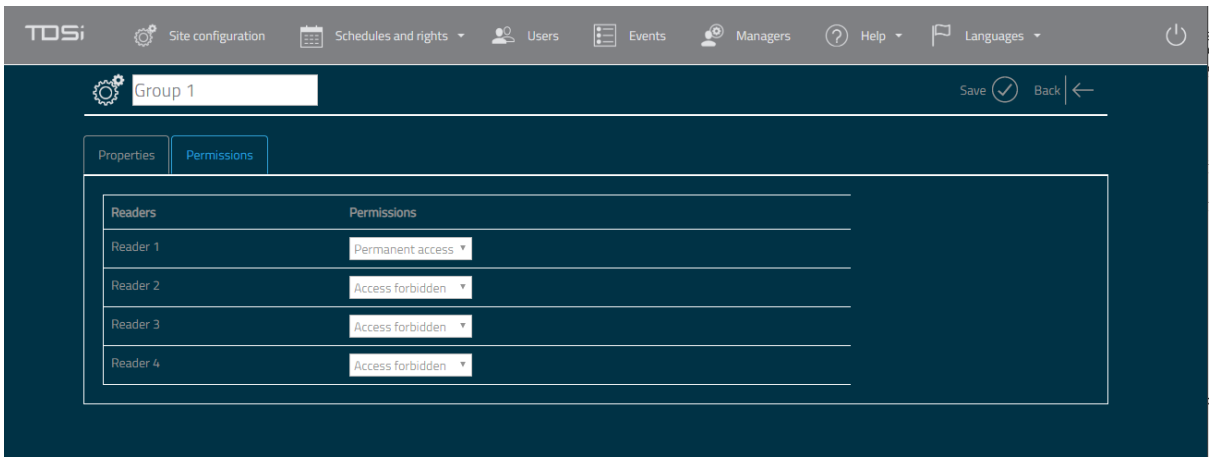
Step 9

Go to the Permissions tab. Select the schedule per reader within the access group



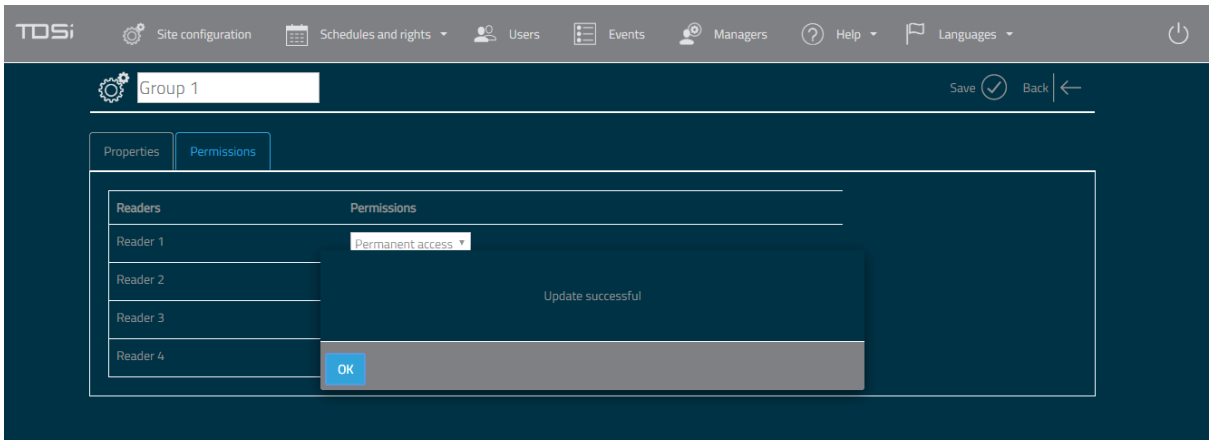
Step 10

Select permanent access for 24/7 access through the reader.



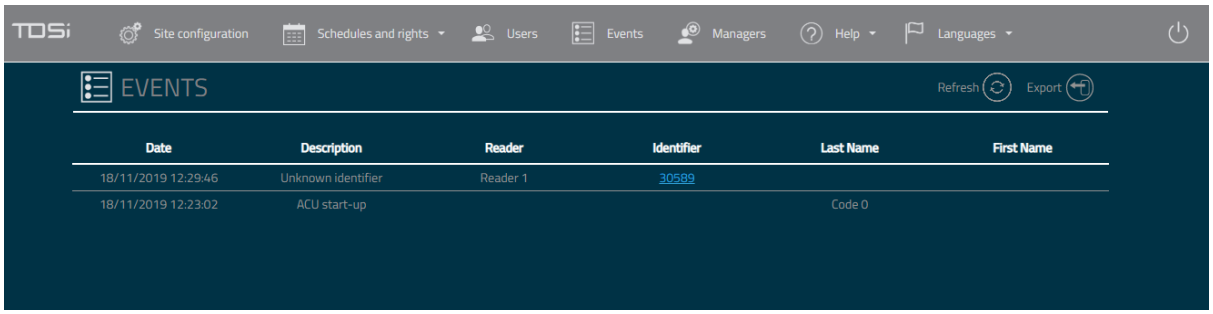
Step 11

Click save. Success will be indicated.



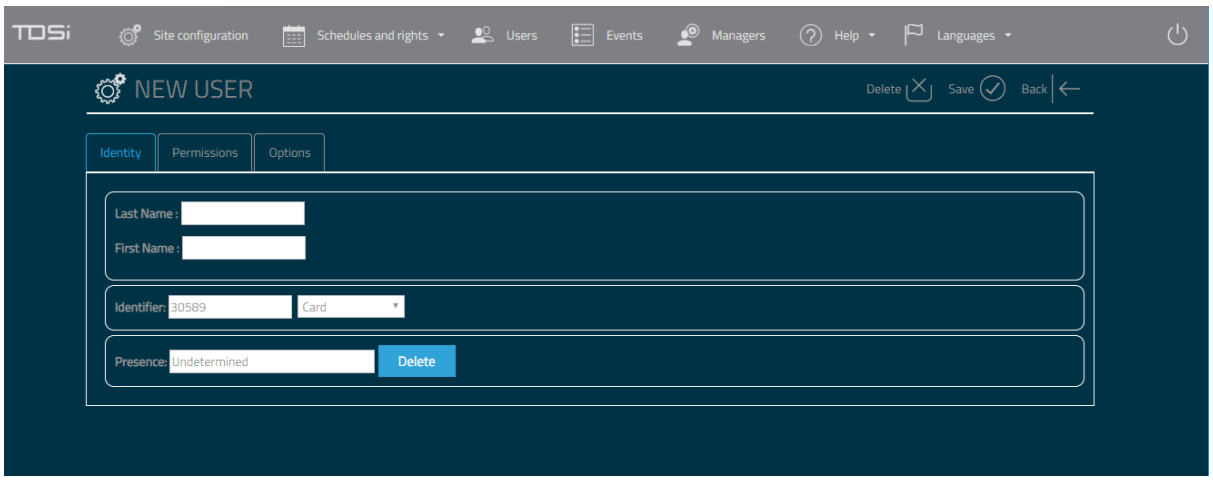
Step 12

Present the required card to the reader. Click Events menu option. Unknown identifier event should be displayed in list of events.



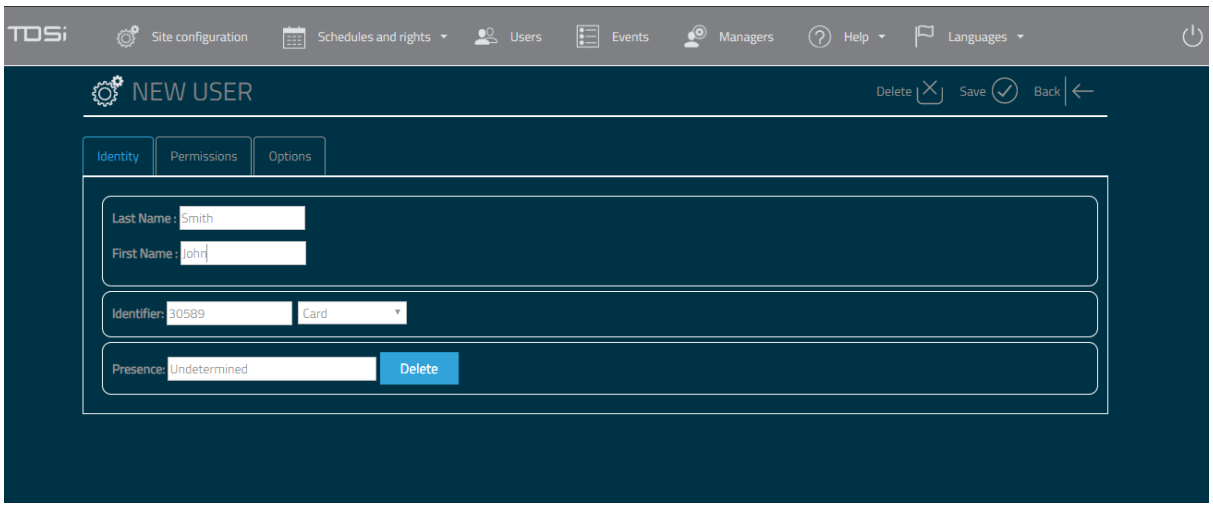
Step 13

Click the number in the Identifier column. This will open a New User form to create a new user. The card number is already defined.



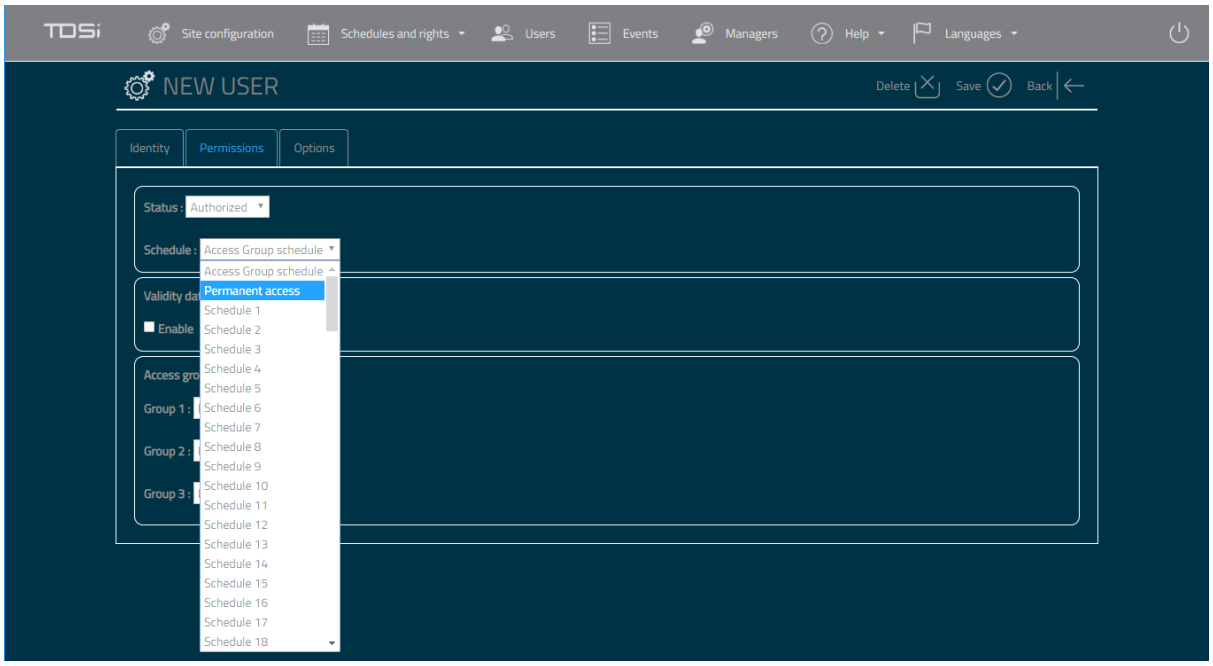
Step 14

Enter details for the new user i.e. last name



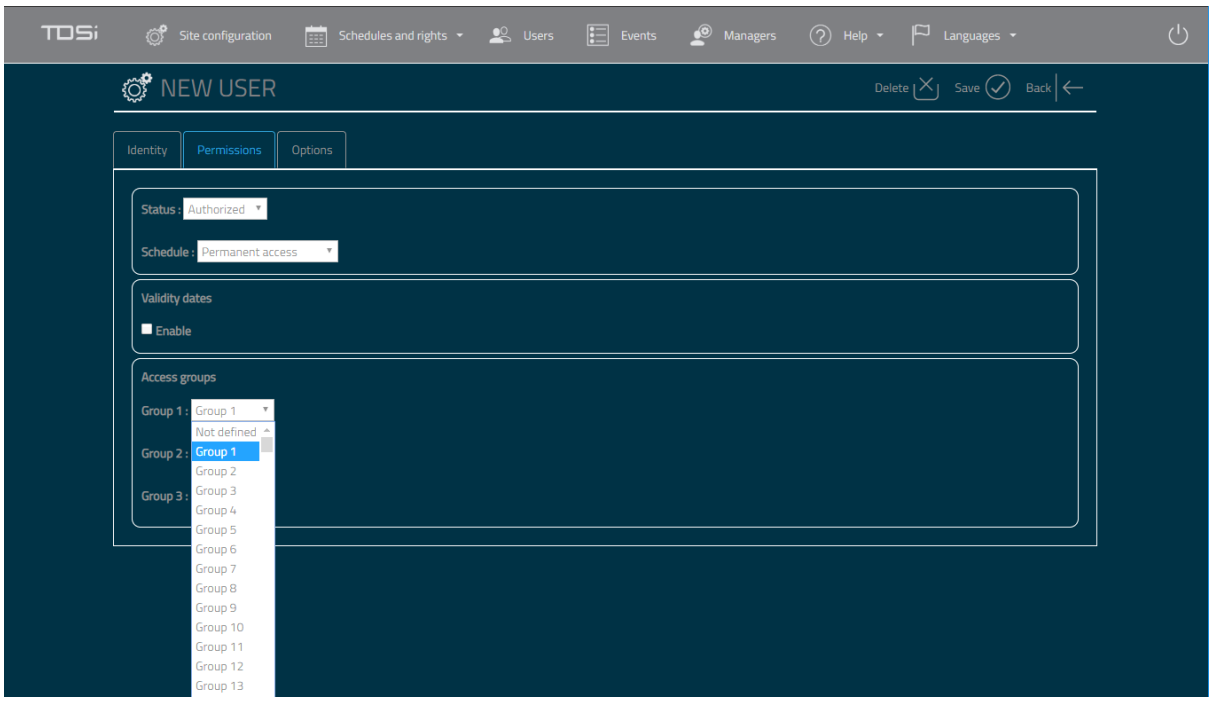
Step 15

Go to Permissions tab. Select Permanent access to say they are authorised 24/7.



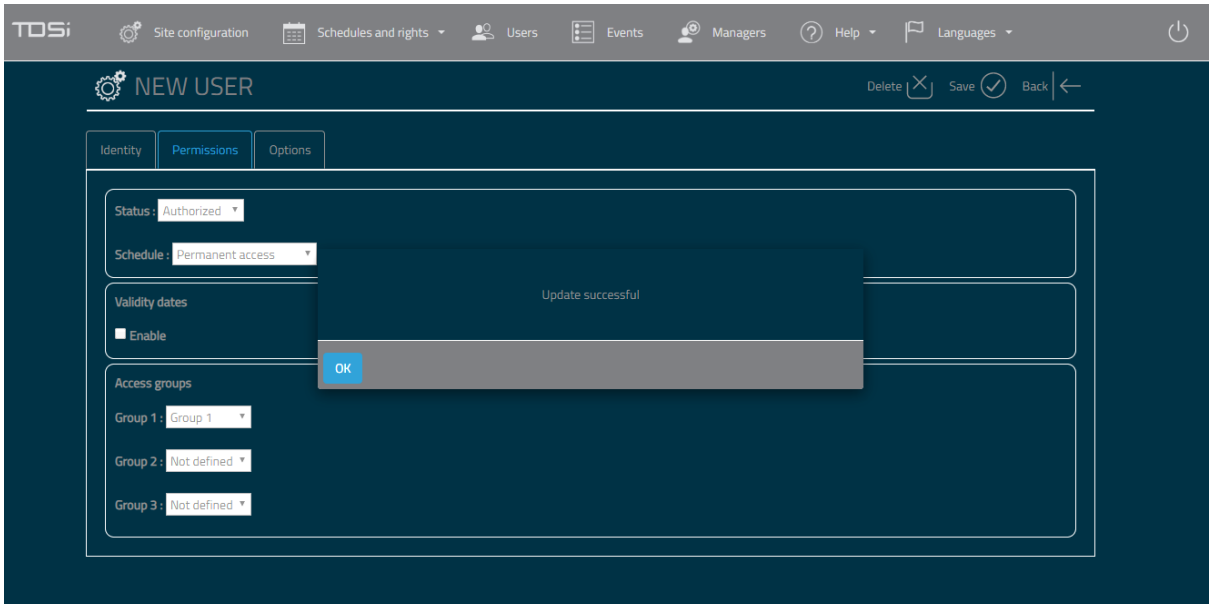
Step 16

Select Group 1 to assign user to Access Group. Note: Limit of up to 3 Access groups per user.



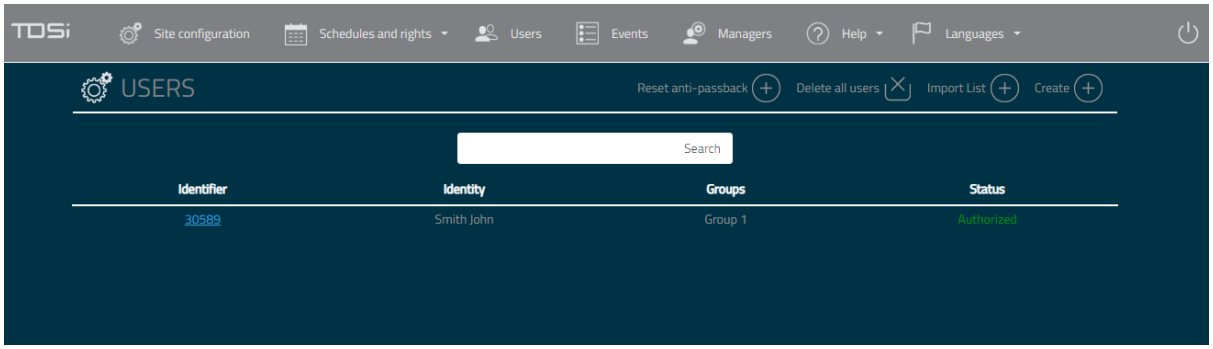
Step 17

Click save. Success is indicated.



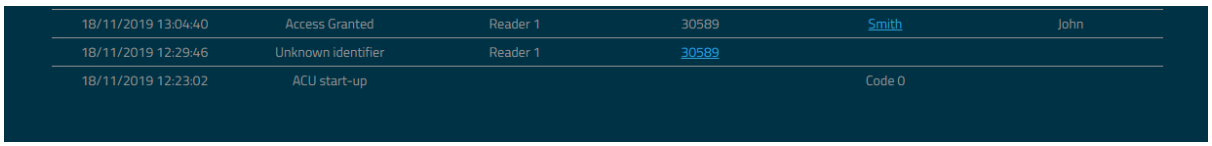
Step 18

Person is now in list of users.



Step 19

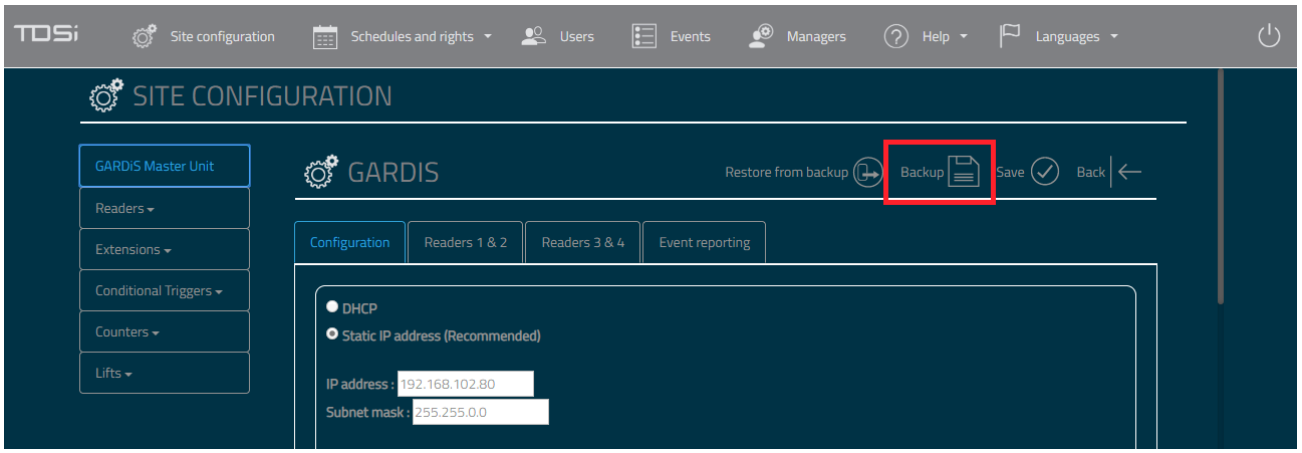
Place card on reader



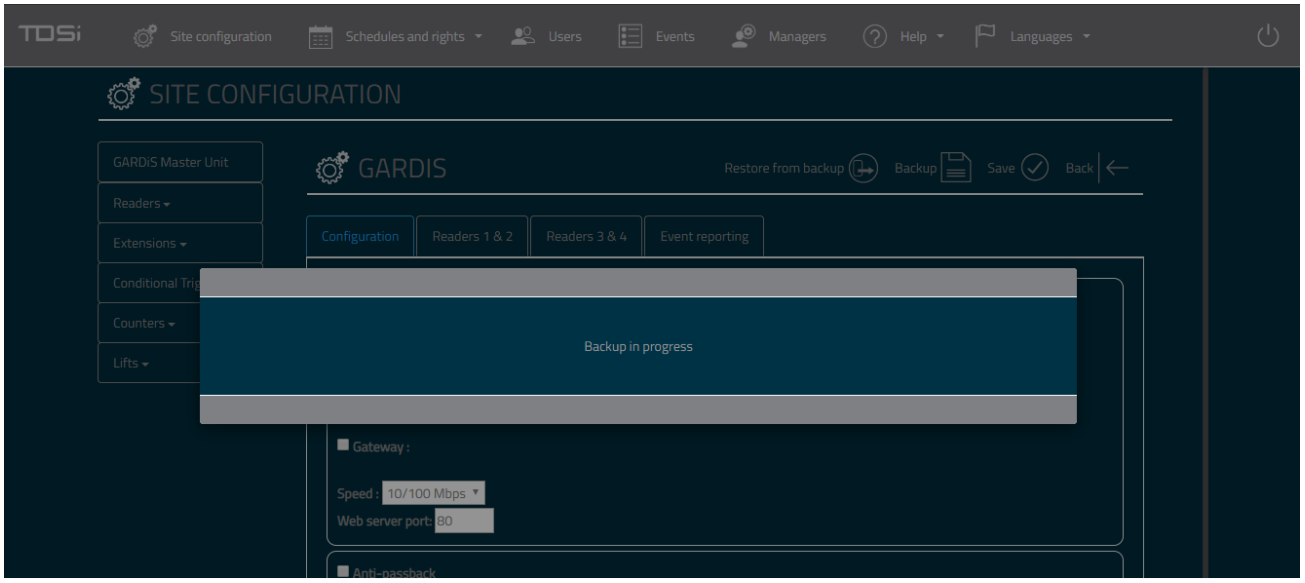
Access granted is now displayed containing details of card number and the person's name.

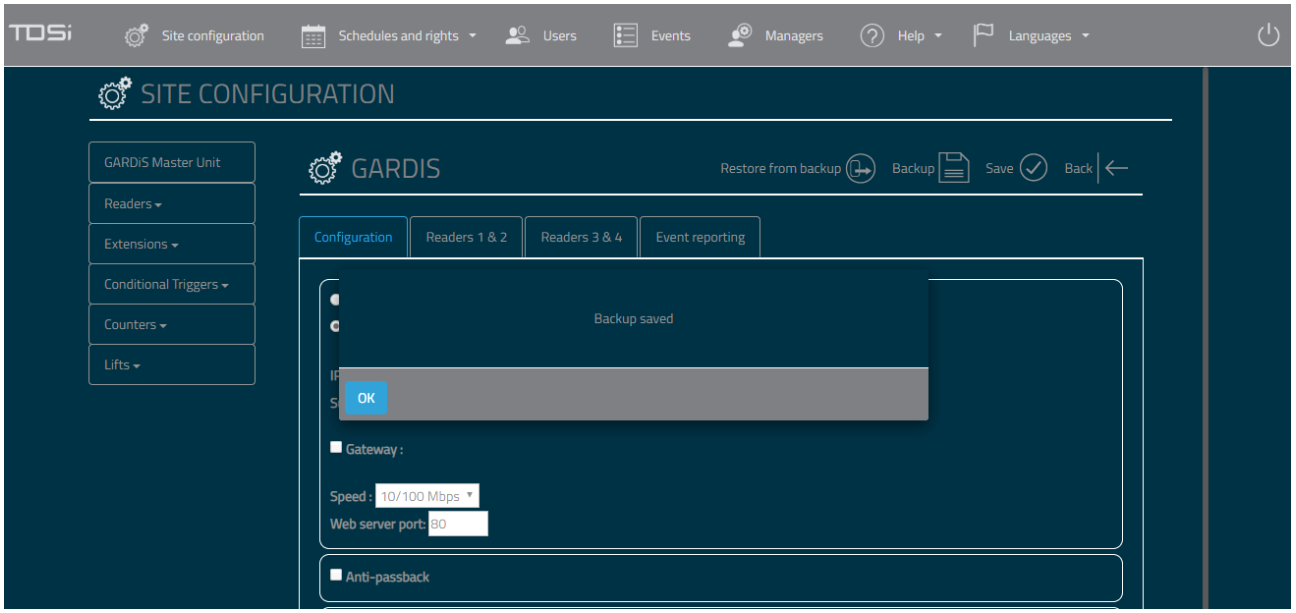
6. Backup

It is advisable to back up the database within your GARDiS Unit.
Click on Site Configuration from the top menu, then click GARDiS Master Unit from the left menu. Click Backup.

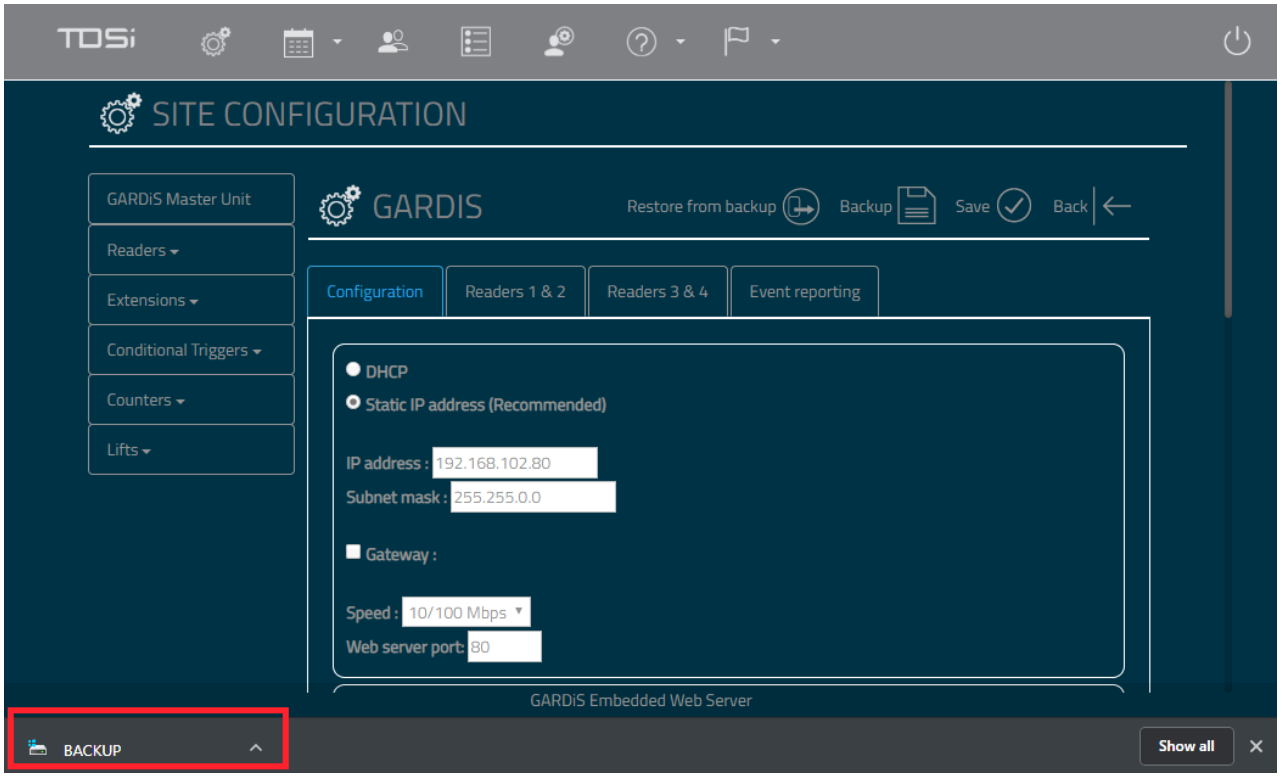


This will initiate the backup process and display a completed message box when finished.



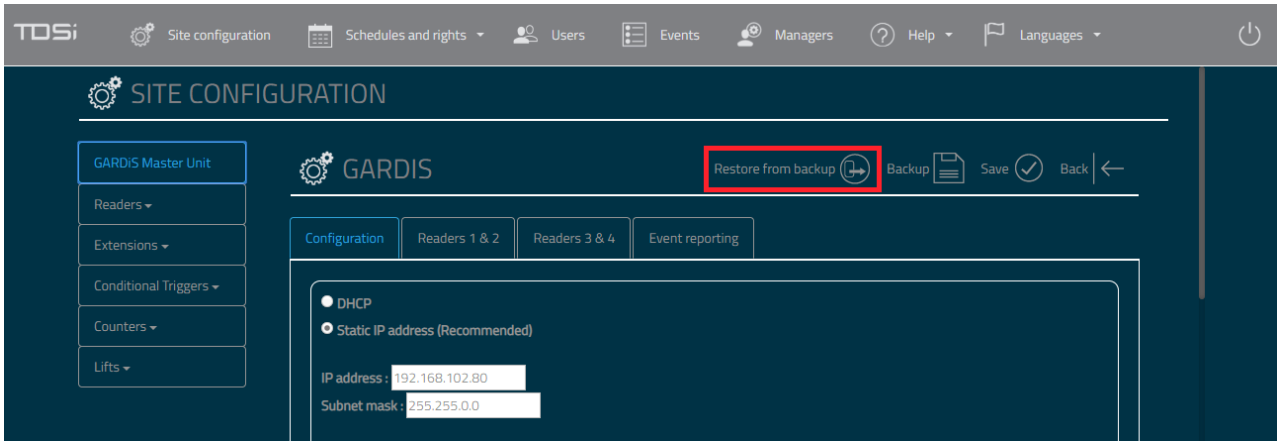


The backup file will be downloaded into the default downloads folder

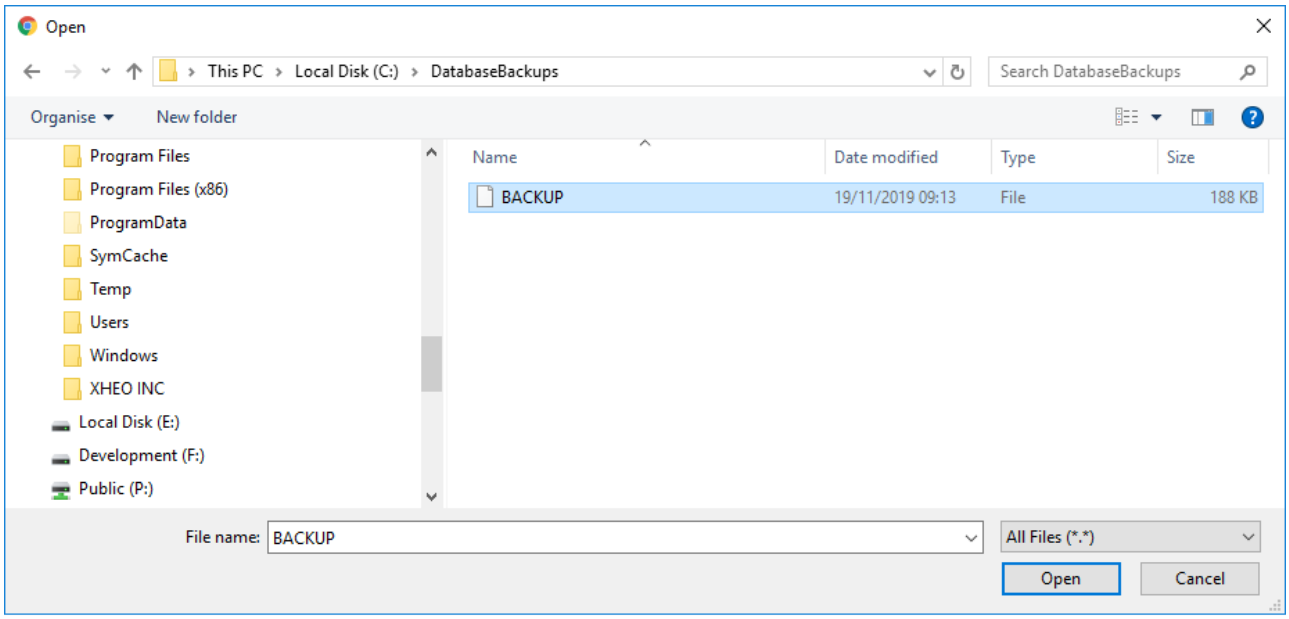


7. Restore from Backup

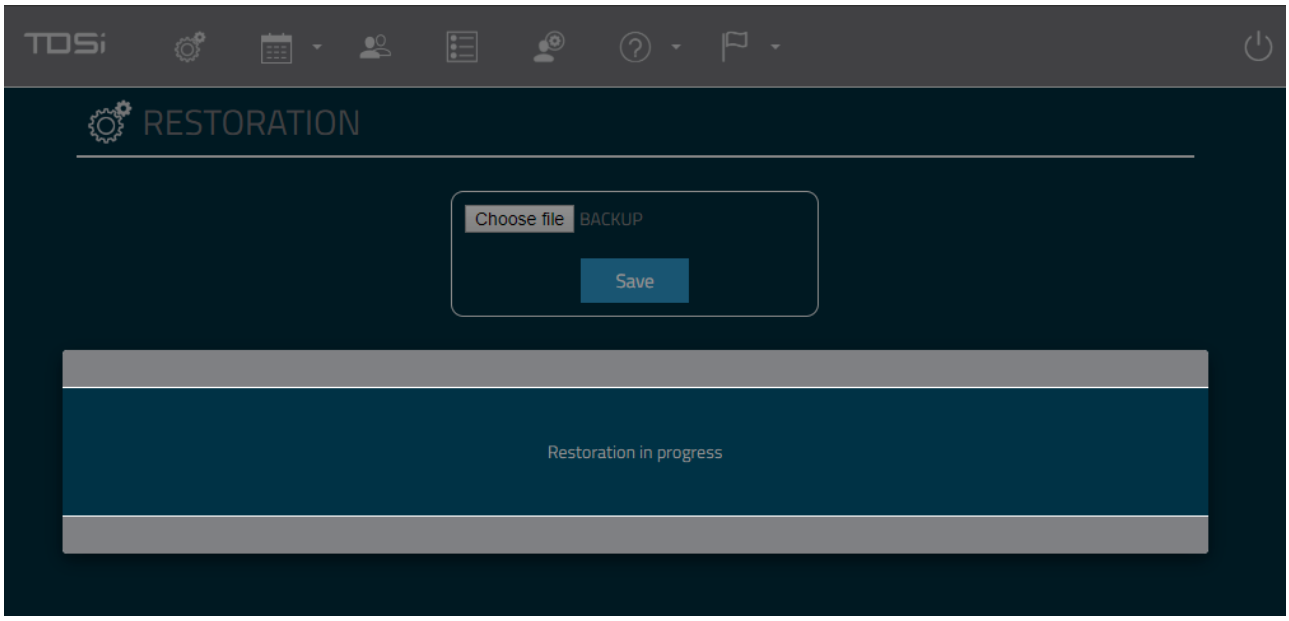
To restore from a backup, **click on Site Configuration from the top menu, then click GARDiS Master Unit from the left menu.**
Click Restore from backup.



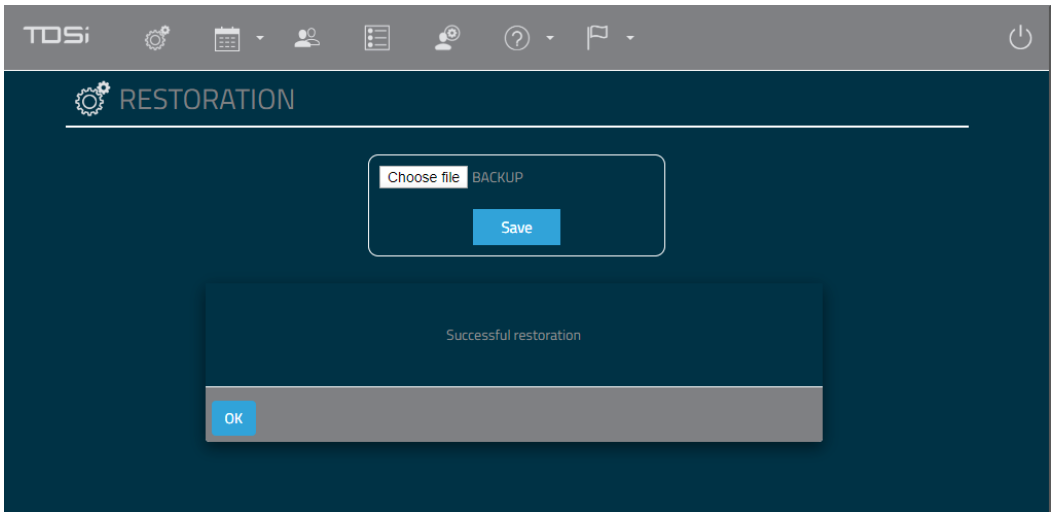
A file explorer window will open. Navigate to the required directory and select the backup file to restore.
Note: The backup file must be named BACKUP (cannot use a renamed file).



Once selected, **click open**. This will initiate the restore process.



A message box will display once completed.



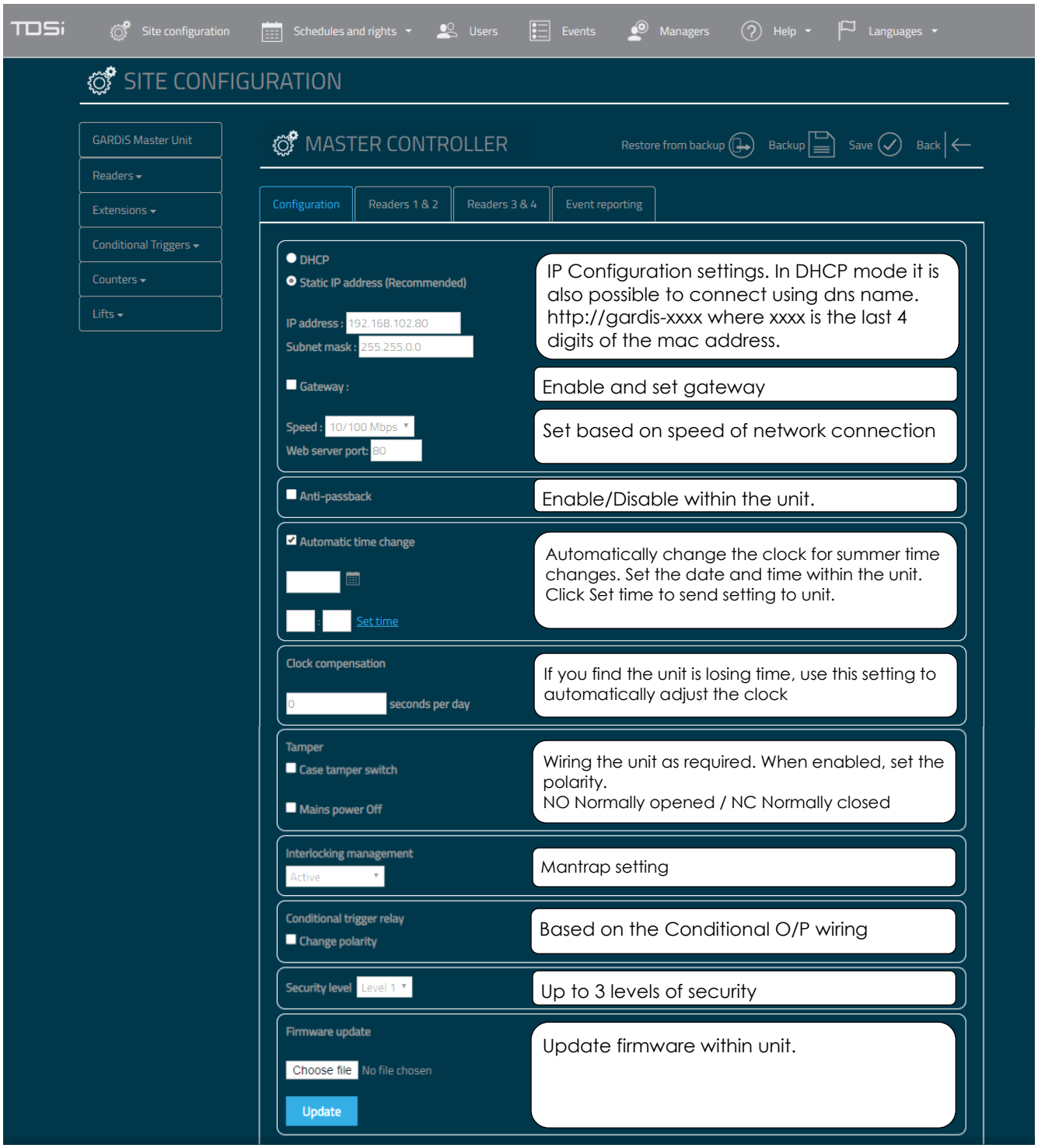
8. Site Configuration

This chapter will provide details of the individual properties of the controller settings.

8.1 GARDiS Master Unit

8.1.1 Configuration

General configuration of the door controller.

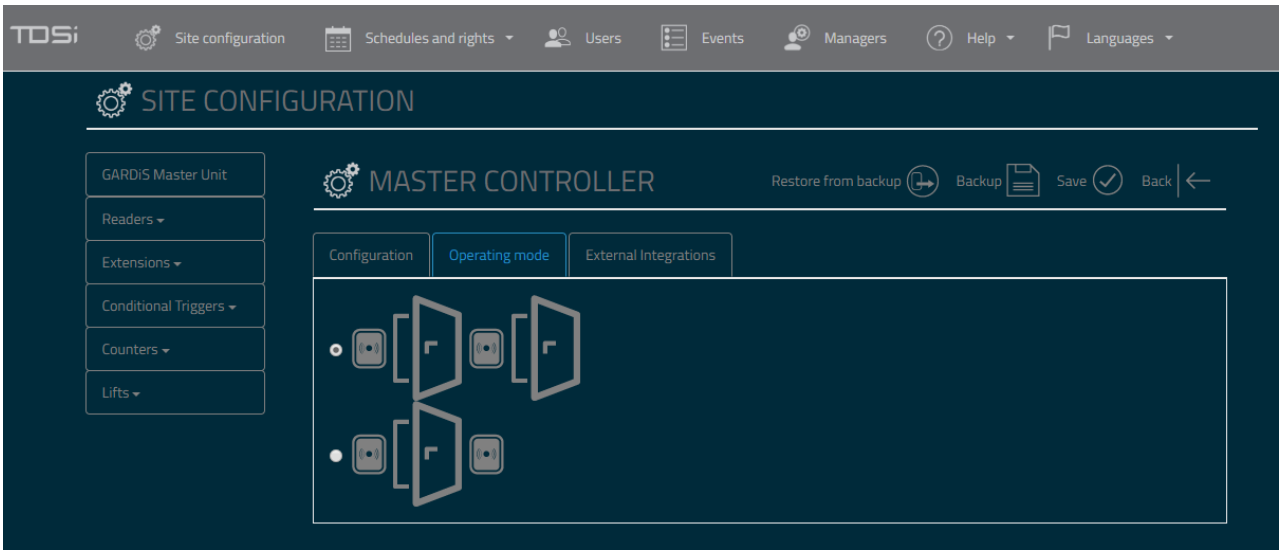


8.1.2 Operating Mode/Readers

On GARDiS 4, the "Operating mode" tab highlighted below is displayed across 2 tabs, grouped by readers.

Select the first option for a reader channel per door i.e. Reader 1 operating door 1, Reader 2 operating door 2.

Select the second option for read in (reader channel 1) and read out (reader channel 2)



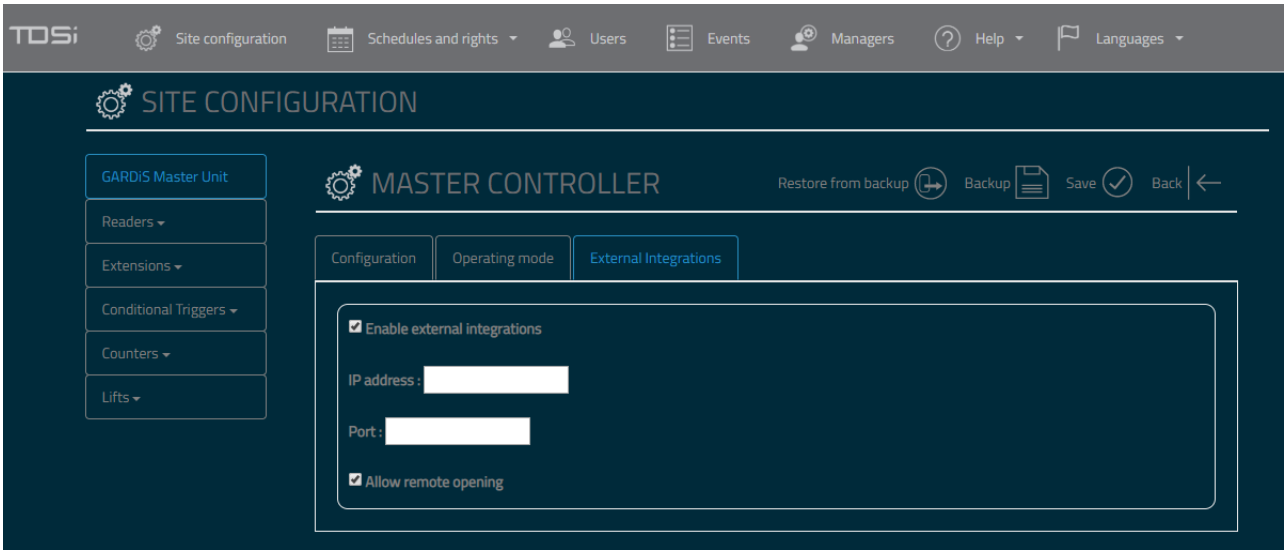
8.1.3 External Integrations

External Integrations allows for third parties to integrate with the GARDiS controller.

Enable external Integrations: Selecting this option displays an IP Address and Port text box. Enter the details of the endpoint you wish to send event information.

Allow remote opening: By ticking this option, the GARDiS controller will allow an http request to open a door. An example of the http request is displayed below, where the index indicates the door relay to open i.e. door 1 and the IP address is the unit's IP Address. The response will contain OK if actioned. The event "Opening by CTM" will be generated along with the reader number associated to the door.

http://192.168.102.54/open.iws?index=1



8.2 Readers

Select the reader technology required from the drop-down menu. The available configurations for that technology is automatically updated on the screen.

Reader Type: Select the required technology of the reader. Supported reader types: Wiegand, clock & data, OSDP, SSCP. Changing the reader type will alter the first section to contain configuration required for the selected type.

Anti-Passback: This allows the reader to be configured for anti-passback. By default, it is set to

Disabled. Other options include:

- **Entry**: Entry reader.
- **Exit**: Exit reader.
- **Entry / Exit**: Entry and exit reader.

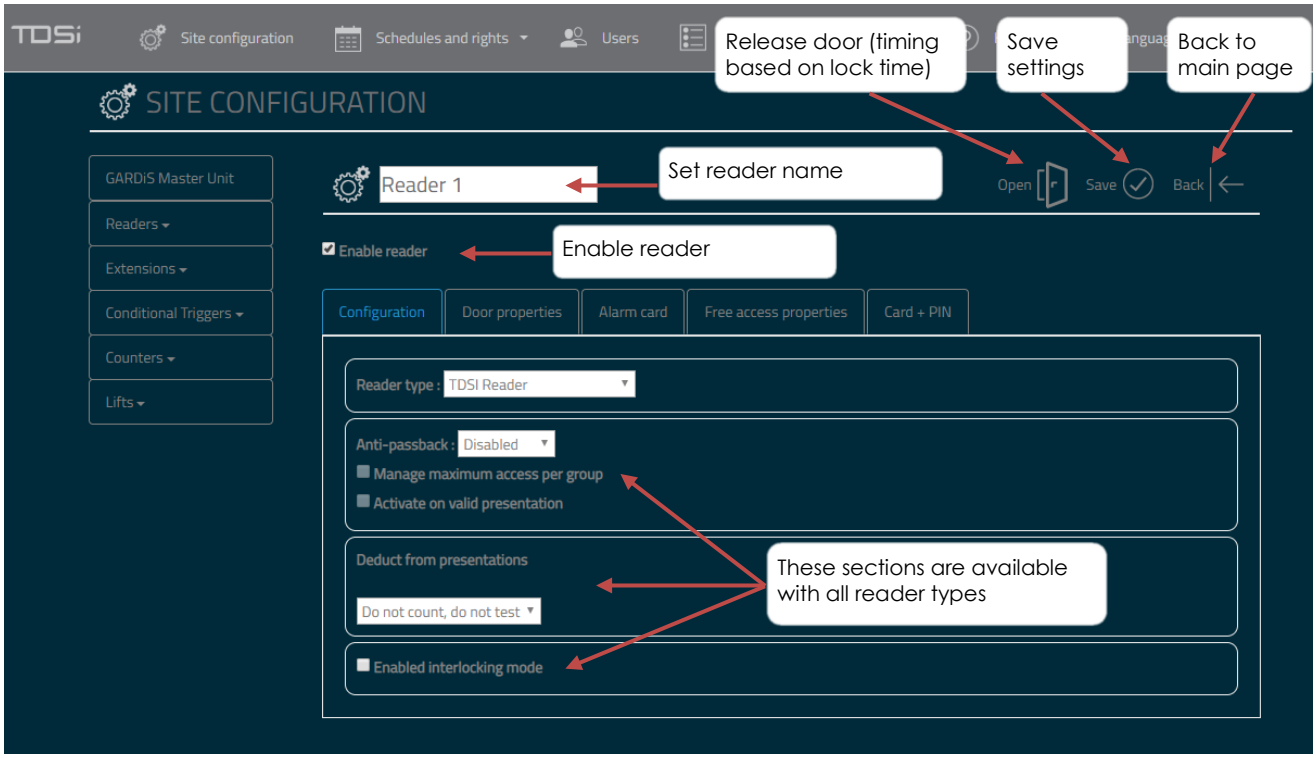
Manage maximum access per group: Enable limitations of the number of entries through a reader based on access group.

Activate on valid presentation: Activate the anti-passback in collaboration with the door sense i.e. when the user presents a valid credential and opens the door. In order for this functionality to work the *Door properties* must be configured to have the *Door sense* property set. By default, this is set to *Disabled*. Note: This changes the events generated by the unit. When a valid credential is presented to the unit, "User awaiting validation" event is generated first. When the user opens the door (within the lock delay), the Access Granted" event is then generated.

Deduct from presentations: This enables the amount of times a credential has operated a reader. The credential must also be configured with the *Number of presentations* option ticked and an initial value set. Options include:

- **Do not count, do not test:** Perform no validation checks
- **Test:** Test the number of times the credential has been used on the reader without counting. Block the user if the amount is 0. When the limit has been reached, the event "Access limit reached" is generated.
- **Test and count**: Test the number of times a credential has been used on the reader and deduct from the count, then block the credential if the access count amount is 0. New event is generated with this option "Access Count". The event includes the amount of counts left for that credential. When the limit has been reached, the event "Access limit reached" is generated.
- **Daily Count**: Deduct from the count a maximum of 1 per day. The credential can be presented to the reader numerous times in a single day and only 1 would be deducted from the count.

Enable interlocking mode: Enable man trap.



8.2.1 Keypad readers

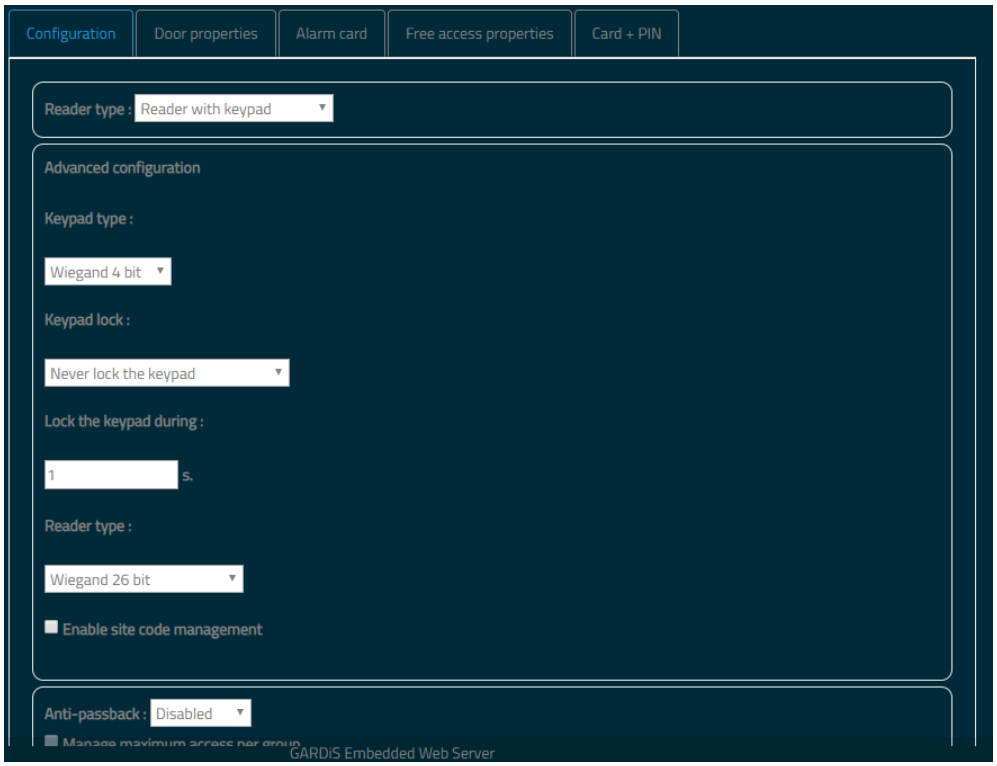
When using a reader with a keypad, select **Reader with keypad** from the **Reader type** drop down. A new section will be displayed to allow further configuration.

Keypad type: Select the required output type. Available options: - Wiegand 4 bit (send out each key press as a 4 bit data) or Wiegand 26 bit (send out a number of key presses as 1 26 bit data length). Set Wiegand 4 bit option for TDSi Keypad readers.

Keypad lock: Select whether you would like the keypad to be disabled after a number of incorrect PIN entries (Maximum of 10). This option is set to "Never lock the keypad" by default.

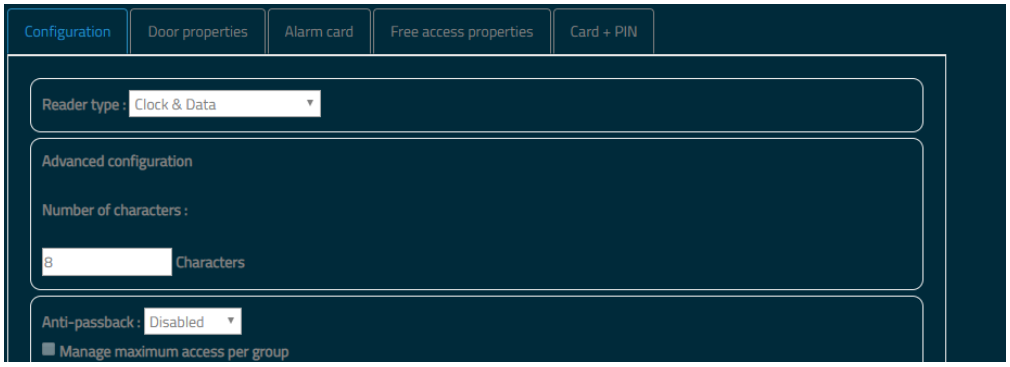
Lock the keypad during: Set the number of seconds to lock the keypad if Keypad lock option is set. Maximum value 255, Minimum value 1.
Reader type: Set the Wiegand output type. Additional options are available depending of the Wiegand option selected e.g. Site code management. Set Wiegand 26 bit for TDSi readers.

Below is a typical setup for TDSi readers with keypad.



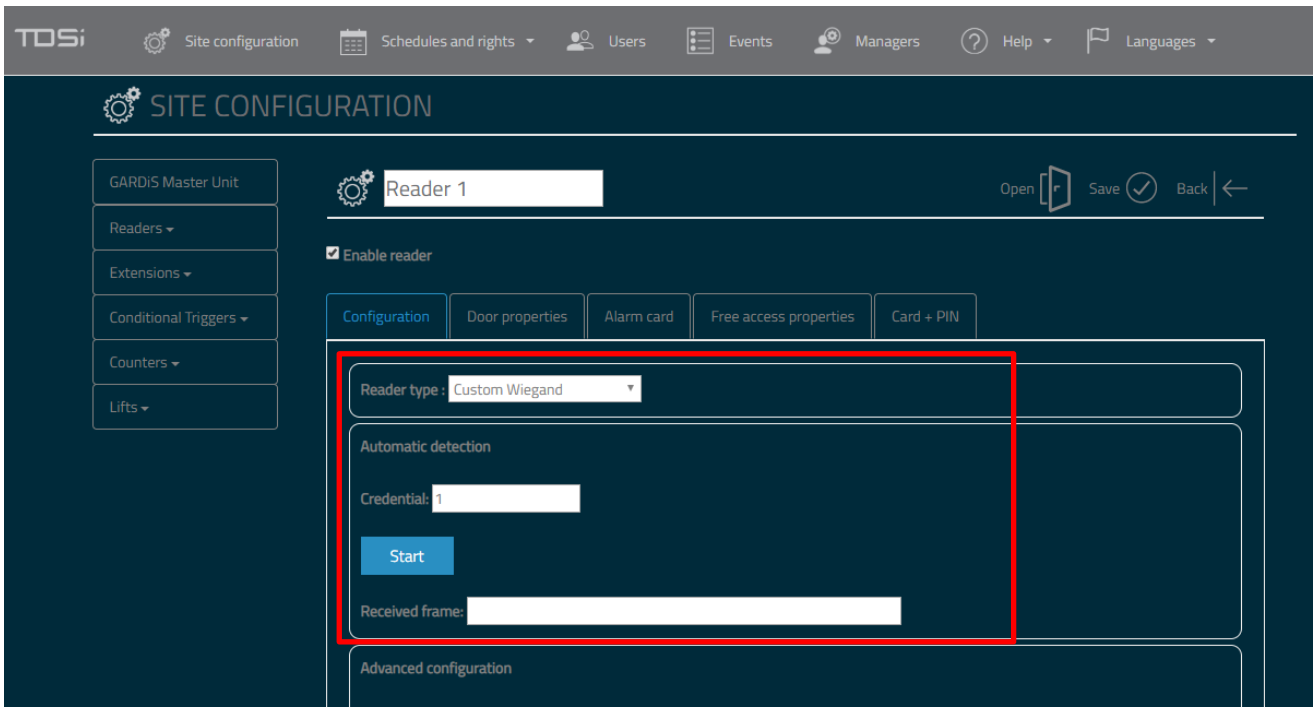
8.2.2 Clock & Data

It is possible to set the number of characters when setting the reader to Clock & Data. Maximum value 13. Minimum value 1. This will take the least significant digit (LSD). For example if an output was set to 8 digits and the following was reported: 85476456. If the output was then set to 4, the number taken by the unit would be 6456.



8.2.3 Custom Wiegand

Select Custom Wiegand from the dropdown menu.
Auto detection of the Wiegand format is provided. Ensure the required reader is attached to the reader channel. Enter the card number in the **Credential** data field. Click **Start** and present the card to the reader. The Received frame data field will display the Wiegand data received by the unit. Click **Save** to program the Wiegand format to the controller.



8.2.4 Door properties

This tab allows the configuration of properties relating to the door equipment.

Lockstrike off mode

End of open door command: This sets the lockstrike to off when the door is opened. To use this function, set the *Door sense* property.

Allow access group delay: This allows access groups to use their own defined lock time.

Lock time: Number of seconds to release the lock relay. Setting to 0 will toggle the relay. Maximum value 255.

LED output: Options to drive the behavior of the reader LED.

- **Trigger by door release**: When the door relay is activated display success.
- **Trigger by door sense**: When the door is opened display success.
- **Trigger by door sense and lock state**: This can be used in conjunction with End of open door command.

Conditional input: This is linked to the conditional I/P connection available on the unit. By default this is set to *Disabled*. Available options:

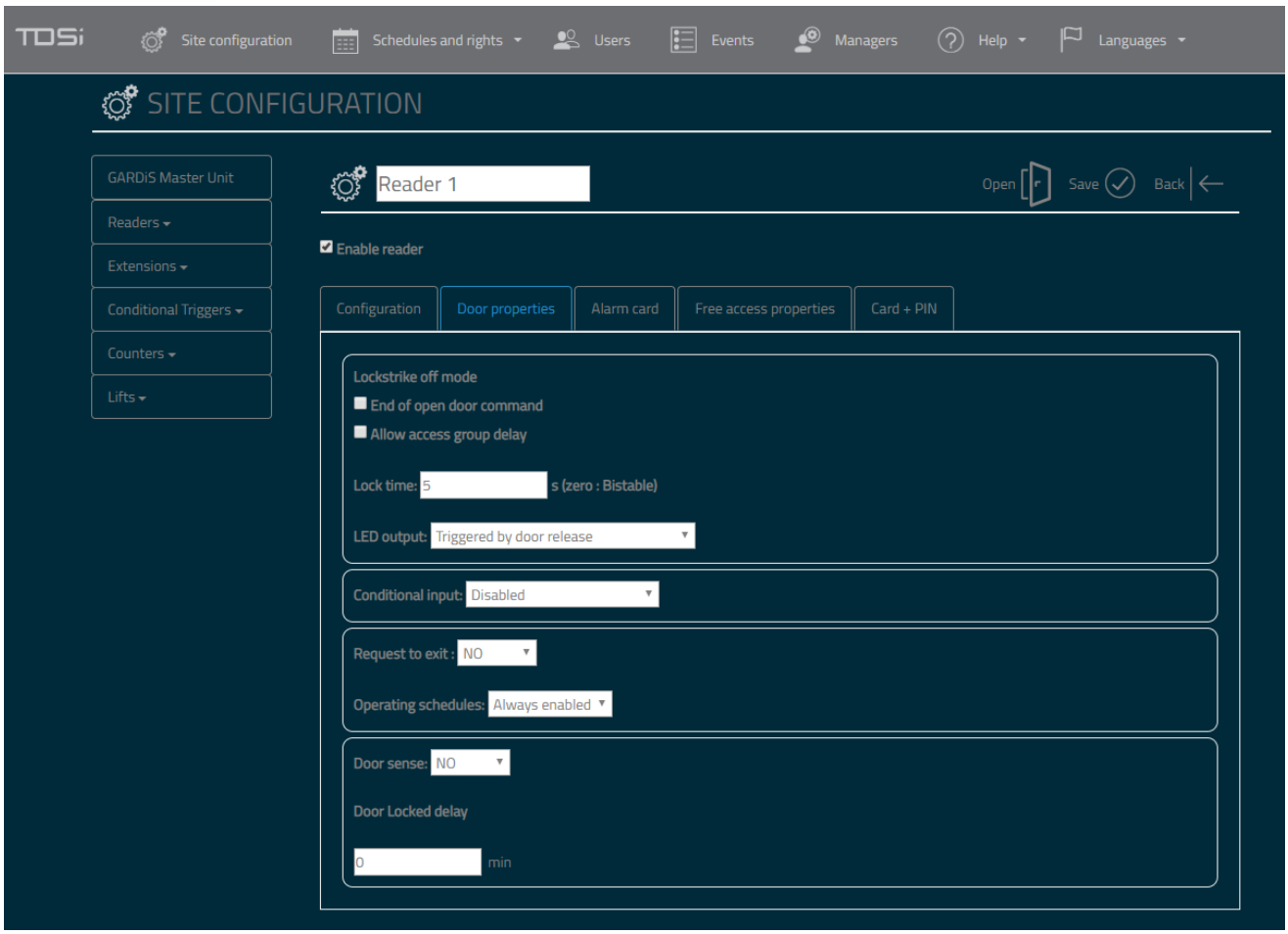
Vehicle Detection NO
Vehicle Detection NC
Intruder Armed NO
Intruder Armed NC
Break glass monitoring NO
Break glass monitoring NC

Request to exit: This is linked to the Exit button connection on the unit. By default this is set to Disabled. Set to the required polarity i.e. Normally opened (NO) or Normally Closed (NC).

Operating schedules: The request to exit button can be configured to be enabled only during a schedule. By default it is set to *Always enabled*.

Door Sense: This is linked to the Door sense connection on the unit. By default this is set to Disabled. Set to the required polarity i.e. Normally opened (NO) or Normally Closed (NC).

Door Locked Delay:

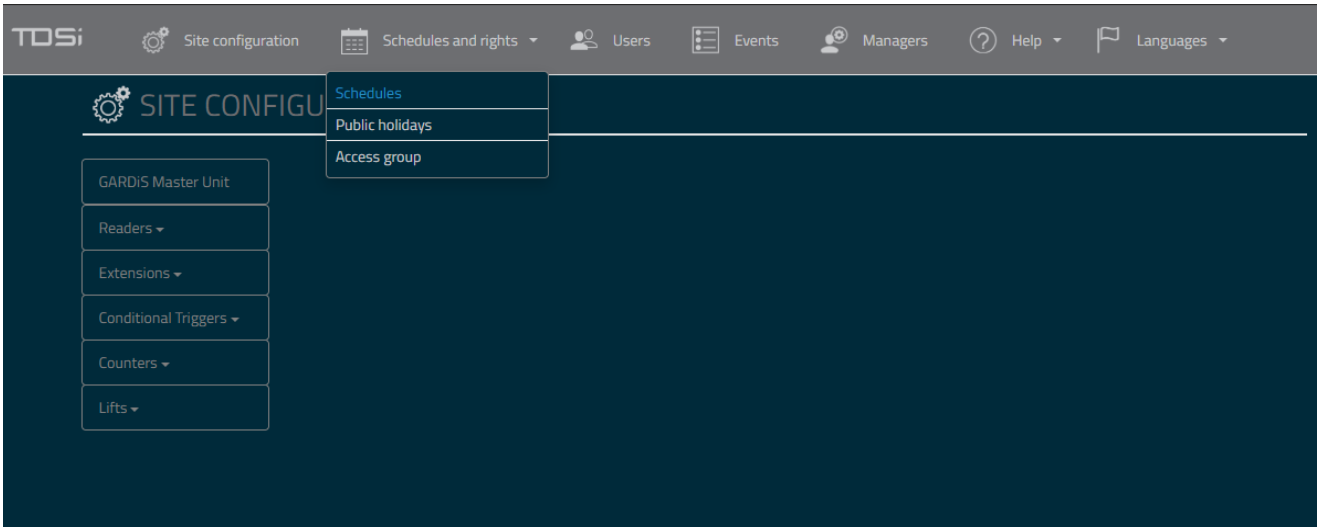

TDSi
Site configuration
Schedules and rights
Users
Events
Managers
Help
Languages
SITE CONFIGURATION
GARDiS Master Unit
Readers
Extensions
Conditional Triggers
Counters
Lifts
Reader 1
Open
Save
Back
Enable reader
Configuration
Door properties
Alarm card
Free access properties
Card + PIN
Lockstrike off mode
End of open door command
Allow access group delay
Lock time: 5 s (zero : Bistable)
LED output: Triggered by door release
Conditional input: Disabled
Request to exit : NO
Operating schedules: Always enabled
Door sense: NO
Door Locked delay
0 min

9. Schedules

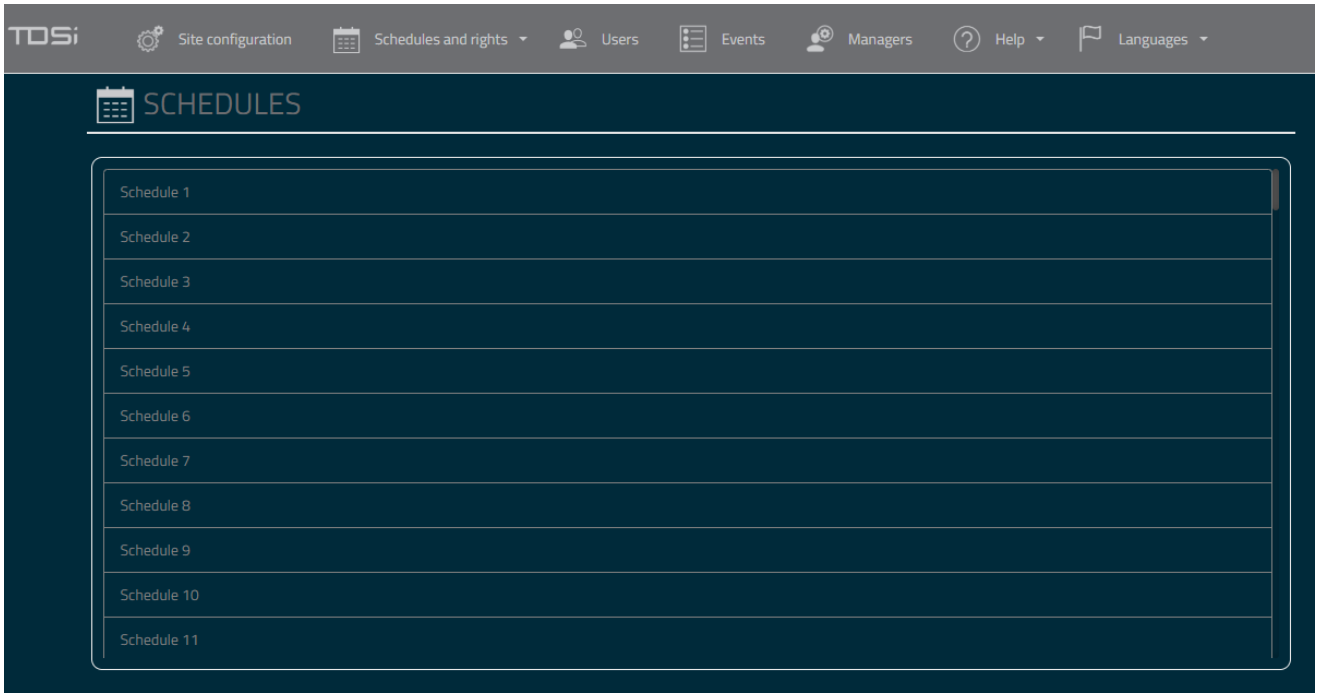
The GARDiS controller allows the end user to create up to 128 schedules.

9.1 Creating a Schedule

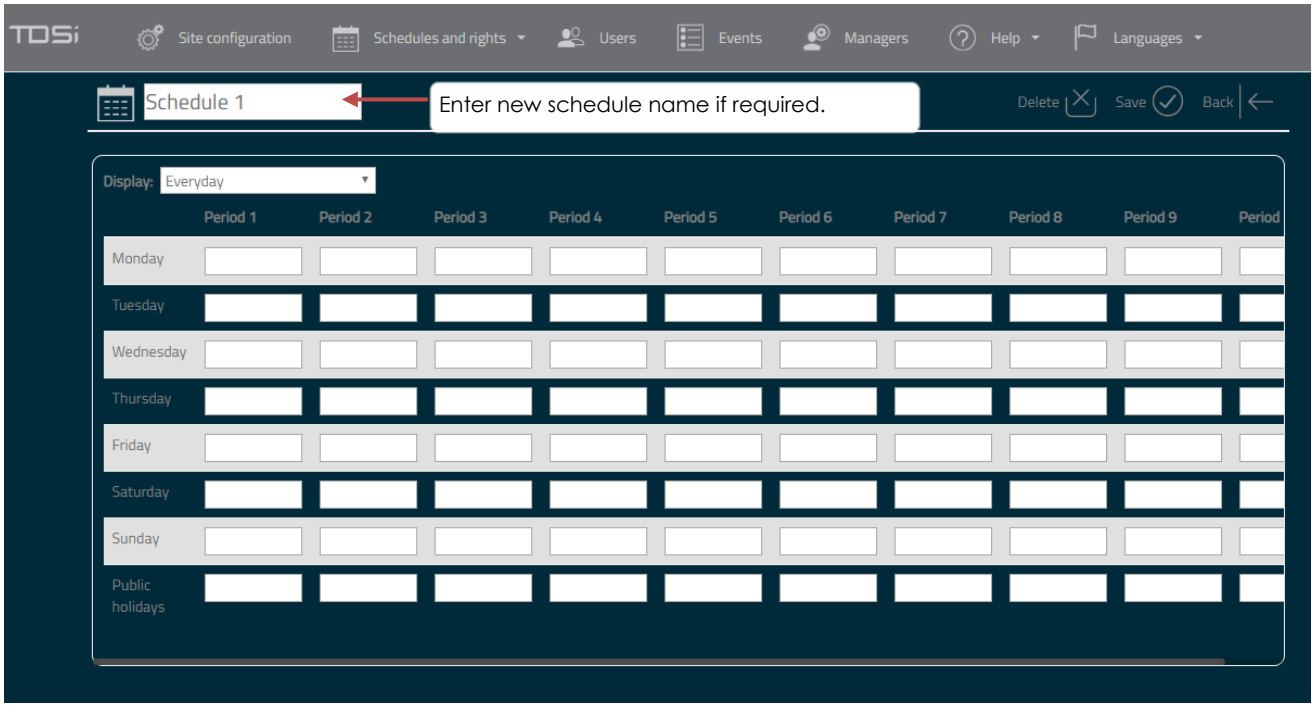
To setup a schedule, click **Schedules and rights** from the top menu bar and then click **Schedules**.



Select the first available schedule in the list. In this example, **Schedule 1** will be used.



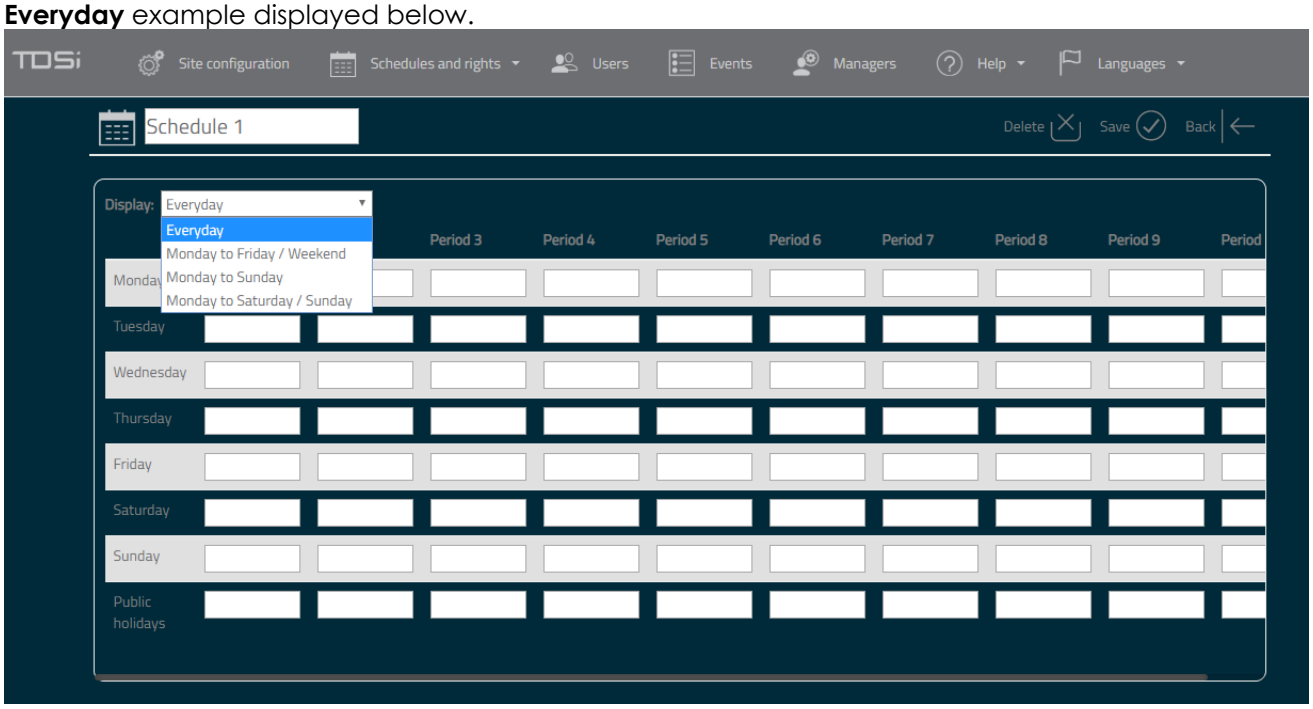
A new name can be defined for the schedule. Up to 10 Schedule periods within 1 day can be defined.



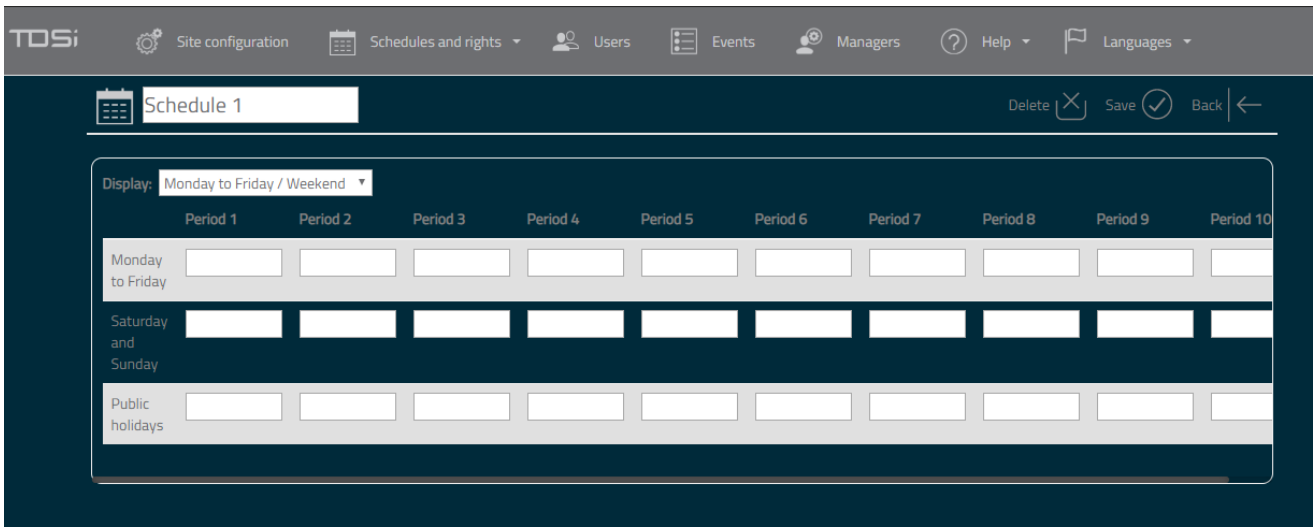
Select the frequency period. It allows easy configuration for repeated schedules. This also updates the table displayed.

- **Everyday** – Allow individual configuration per day.
- **Monday to Friday / Weekend** – Define periods to be repeated Monday to Friday, a separate period definition for the weekend and a separate period definition for Public holidays.
- **Monday to Sunday** – Define periods to be repeated Monday to Sunday and a separate period definition for Public Holidays.
- **Monday to Saturday / Sunday** – Define periods to be repeated Monday to Saturday and a separate period definition for Sundays and a separate period definition for Public Holidays.

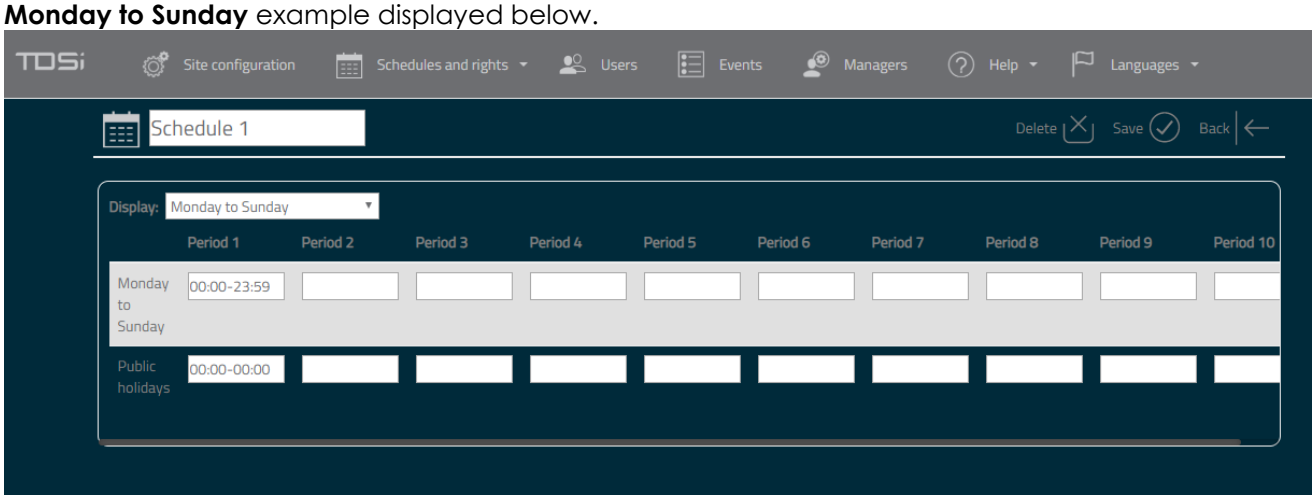
Everyday example displayed below.



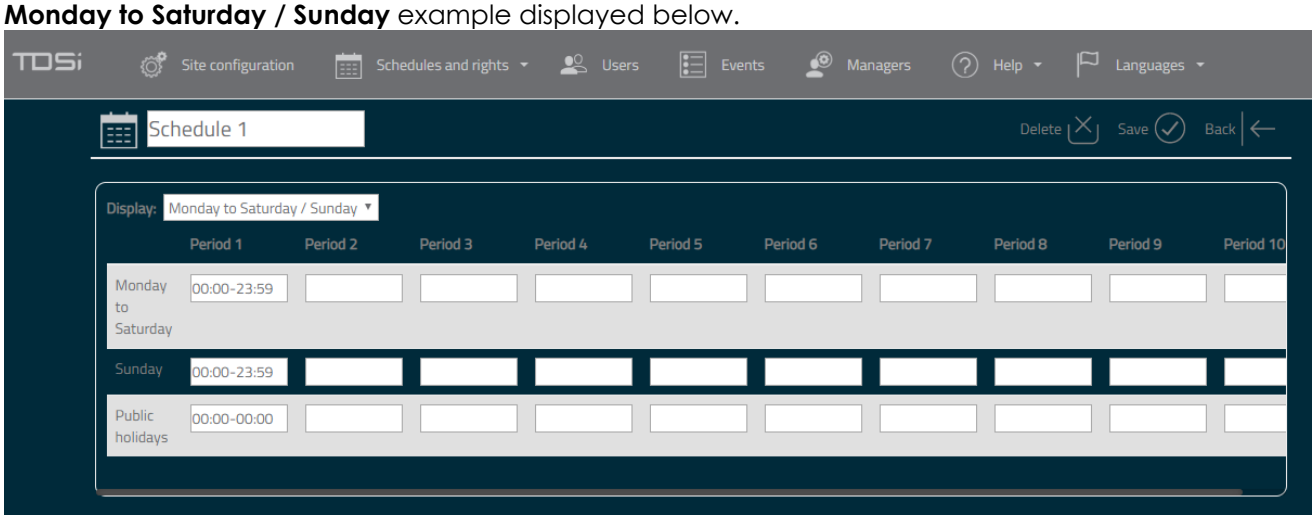
Monday to Friday / Weekend example displayed below.



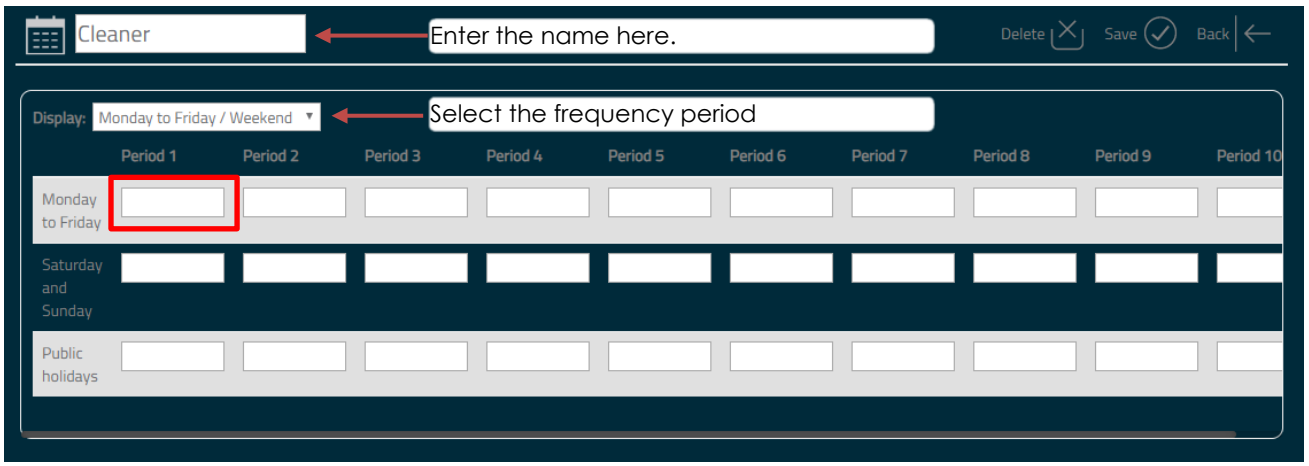
Monday to Sunday example displayed below.



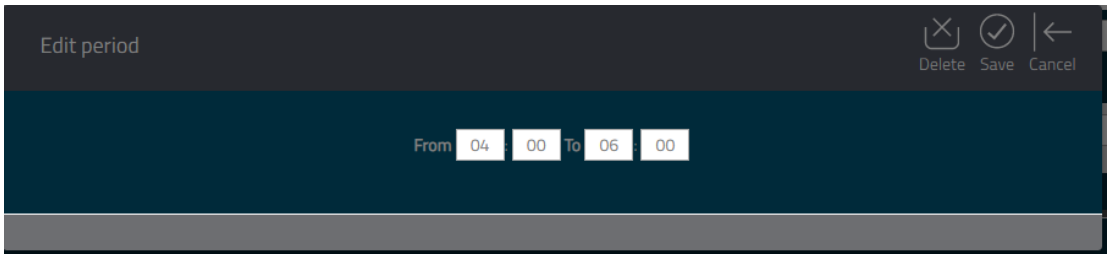
Monday to Saturday / Sunday example displayed below.



Enter a name for the schedule and select the required frequency period. Click in the first period text box.

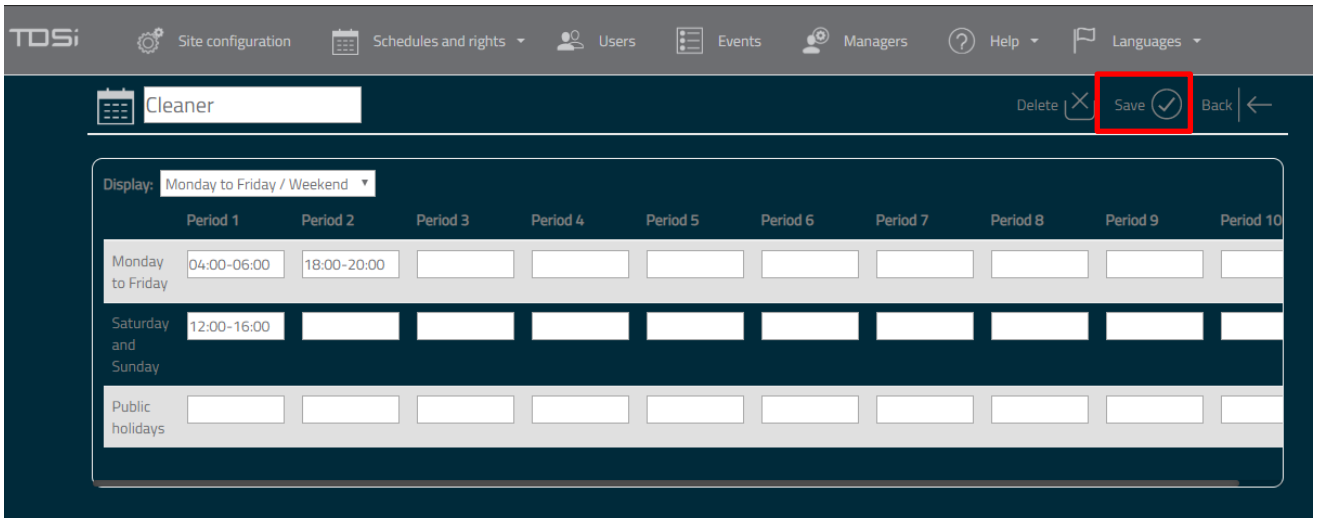


A new window is displayed. This allows the entry of a start and end time. The below example is setting a schedule period of 4am to 6am. Enter the required values into the boxes (hour and minutes in 24-hour format) Click **Save**.



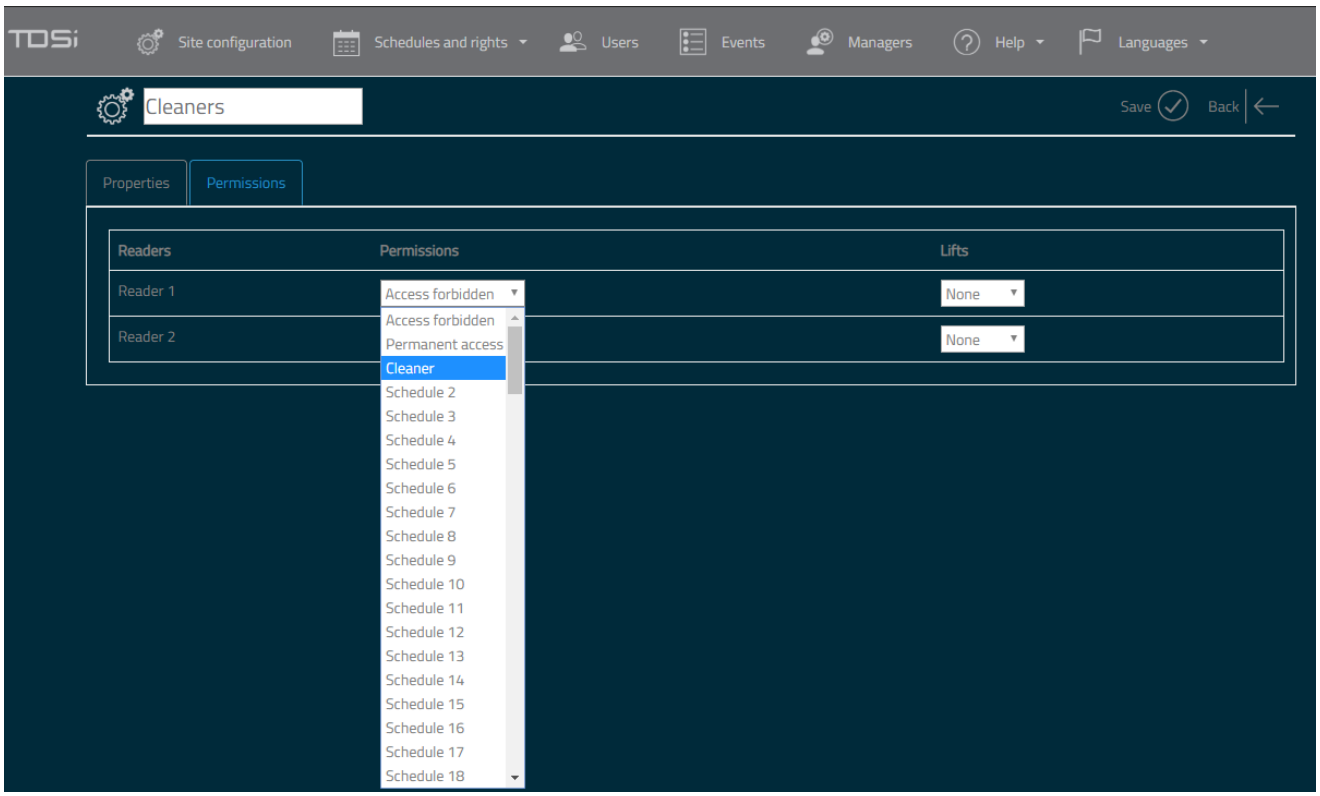
NOTE: To have an all day 24/7 schedule, enter 00:00 to 00:00.

This will enter the values into the Period 1 text box. Continue to enter required schedule periods. The below example is set to allow entry 4am-6am and 6pm to 8pm during the week. At weekends entry is set to 12pm to 4pm. On public holidays there is no allowed entry. Click **Save** when complete. This schedule is now available to use on objects such as Access Groups.



9.2 Assigning a schedule to an access group

To assign a schedule to an access group, click **Schedules** and rights and then click **Access Groups**. Configure the access group as required i.e. set the name etc. Click **Permissions** tab and select the required schedule per reader from the **Permissions** dropdown.

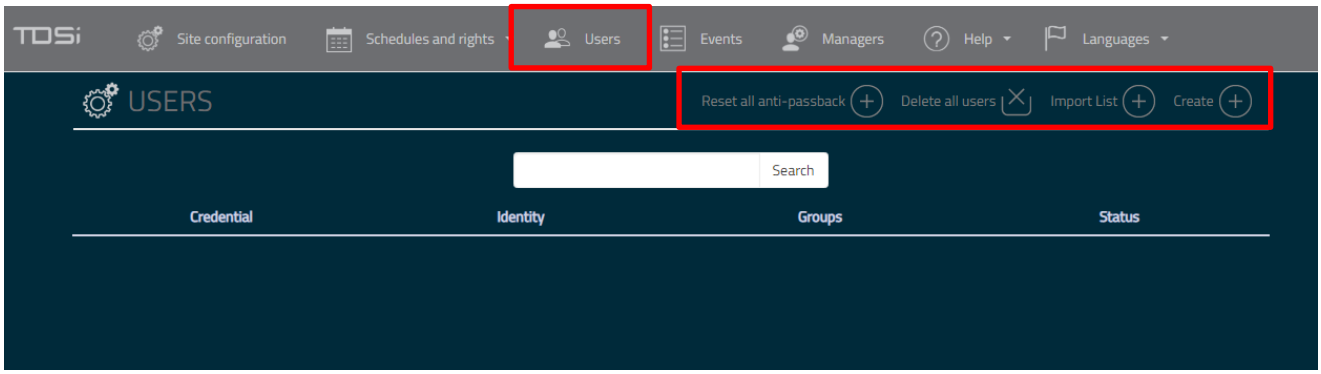


This will set the selected schedule within the dropdown.

10. Users

This section allows credentials to be added to the controller. Access this section by clicking Users along the top menu. A list of existing credentials are displayed.
Actions available in this section:

Reset all anti-passback: Reset all credentials anti-passback settings. This will allow all credentials access to the reader if anti-passback has been enforced.
Delete all users: Delete all credentials in the unit. This requires an addition confirmation action.
Import List: Import credentials from a file.
Create: Add a new credential into the unit.



10.1 Create new user

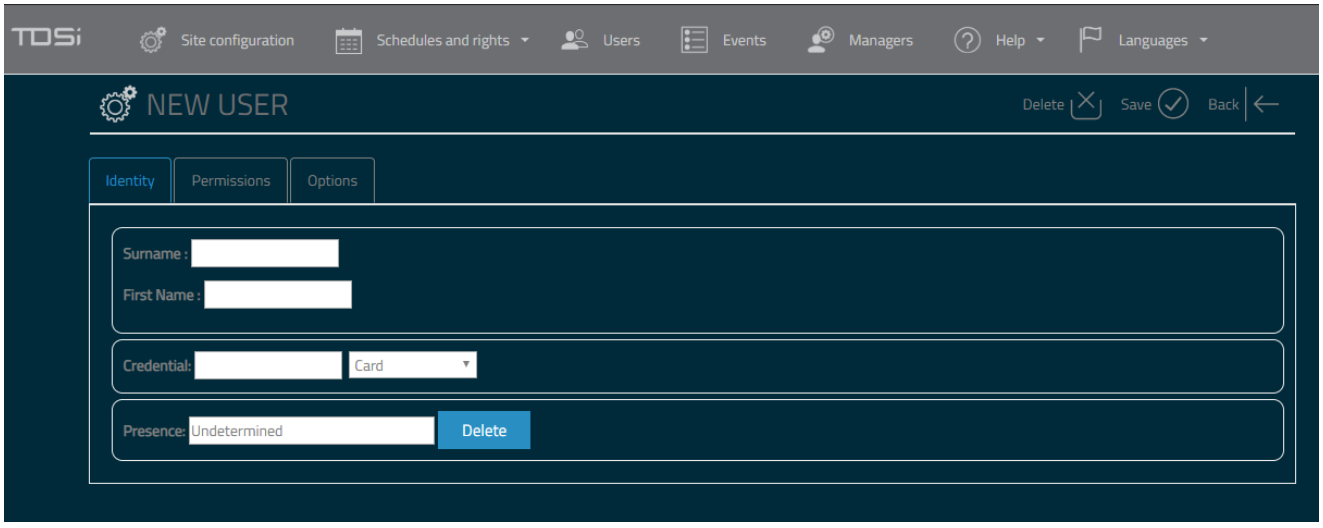
To create a new user/credential in the unit, click Create in the User section. User properties are divided into three sections, **Identity**, **Permissions** and **Options**.

10.1.1 Identity Tab

Surname: Last name of person
First name: First name of person
Credential: Credential number. Select the type from the dropdown. Available options:

- Card
- Card Application
- RF key fob
- Keypad

Presence: Date and time of entry. This data is automatically filled in by the system when anti-passback is enforced. Use the Delete button to reset an individual's anti-passback. Note: Click Save to update this option. Undetermined is the default display.



10.1.2 Permissions Tab

This tab allows the access permissions for a credential to be defined. Note: Up to **3 Access Groups** can be defined per credential.

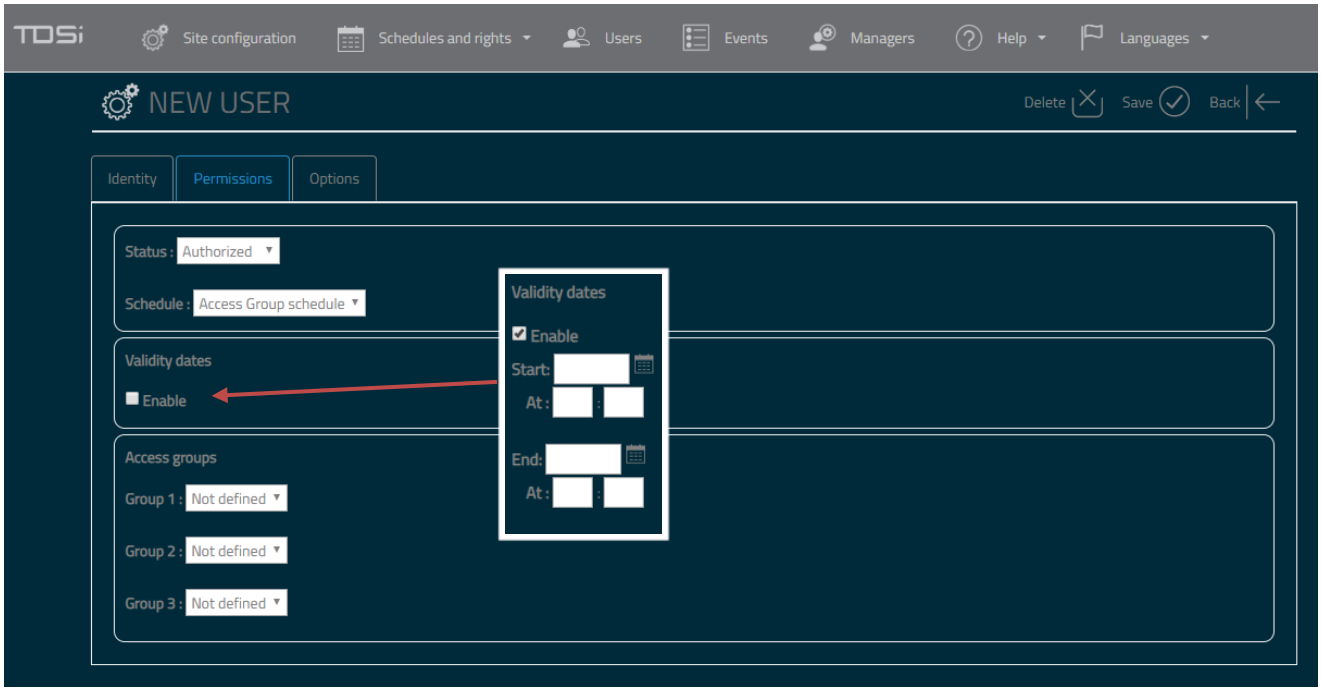
Status: Easily set a credential to be authorized or not allowed.

Schedule: Set the credential to follow a schedule. The options include:

- **Access Group schedule** (default option). Follow the schedule of the access groups.
- **Permanent access**. Allows allow through the readers without following any schedule.
- **Select a schedule** from the system that the credential uses.

Validity dates: Tick the enabled option to display start and end dates and times. This will validate the credential during the period set.

Access groups: Select up to 3 access groups per credential.



10.1.3 Options Tab

This tab allows additional properties to be set.

Intruder management: Set the credential to be an intruder user.

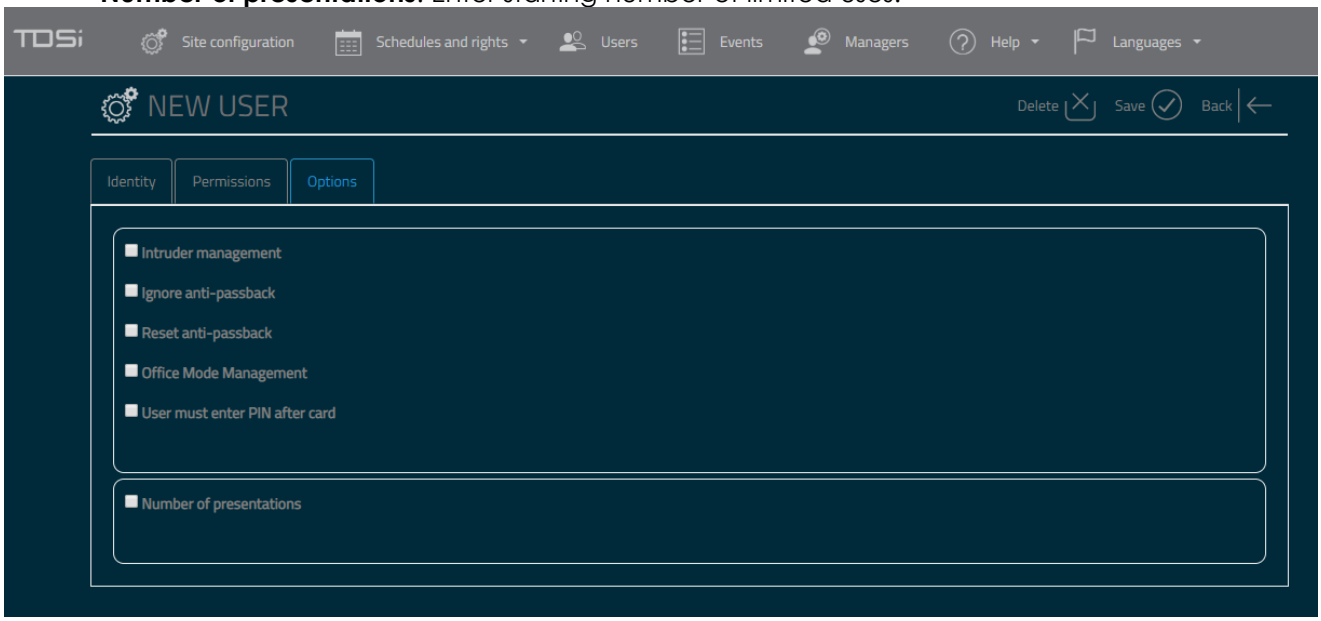
Ignore anti-passback: The credential is not checked for anti-passback.

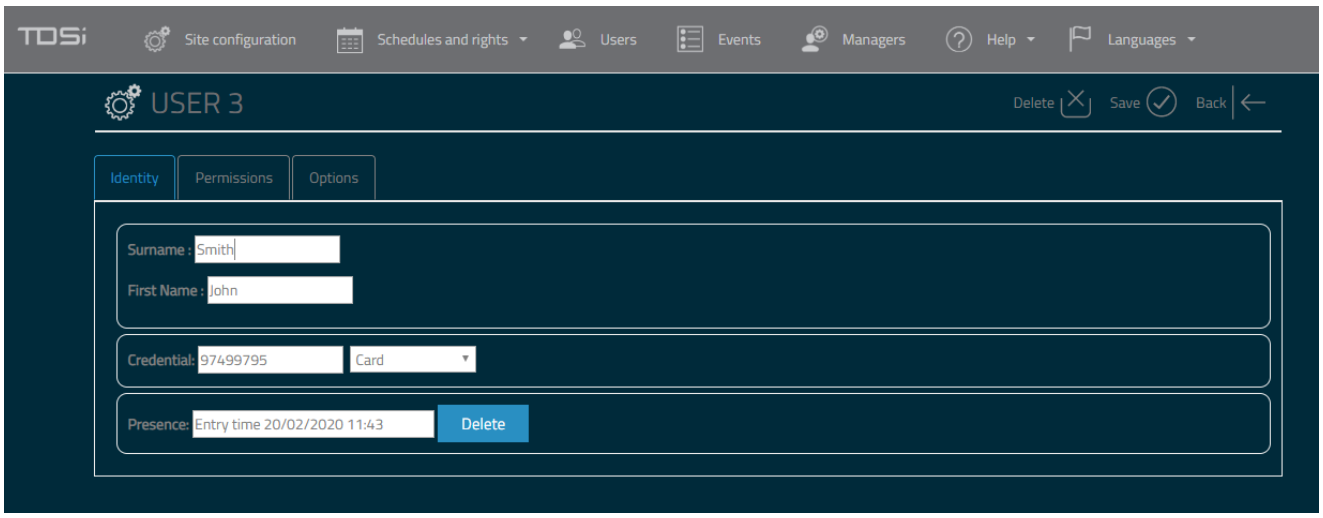
Reset anti-passback: Reset the anti-passback.

Office Mode Management: Allow the credential to use Office Mode.

User must enter PIN after card: If reader is configured to use Card or Card + PIN, this credential must use Card + PIN.

Number of presentations: Enter starting number of limited uses.

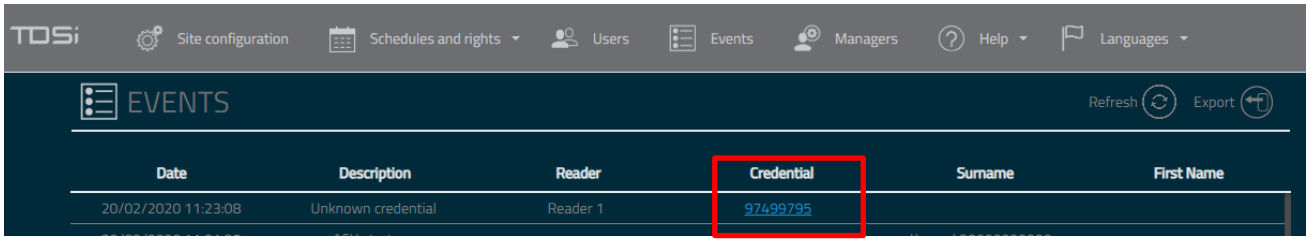




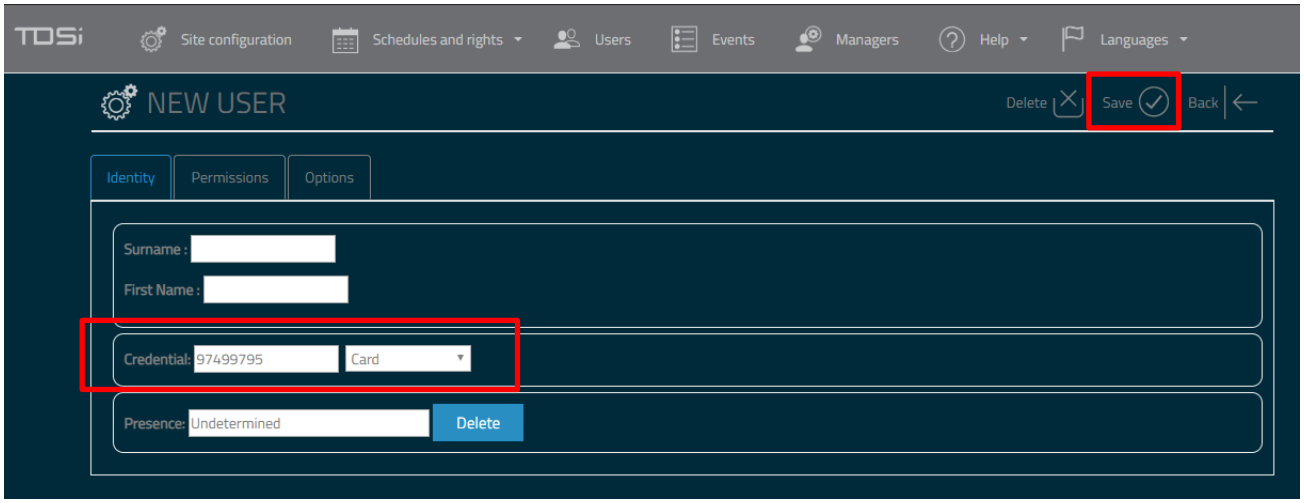
10.2 Create new user from event

The embedded web server allows the creation of a user from the event list.

Step 1 Click on the credential number that is highlighted as a link.

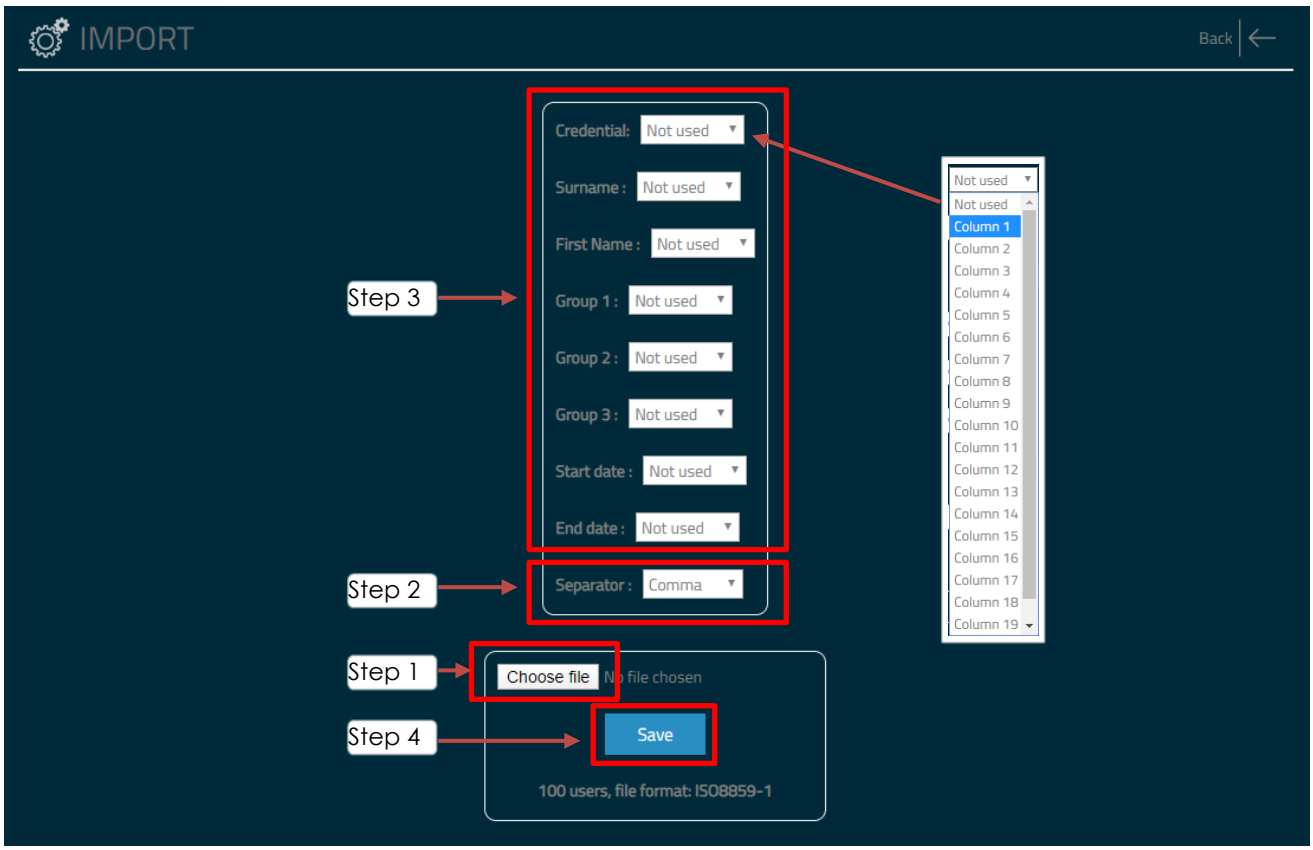


Step 2 The system will automatically load the New User screen with the credential number automatically filled in. Enter any further properties required and then click **Save**.



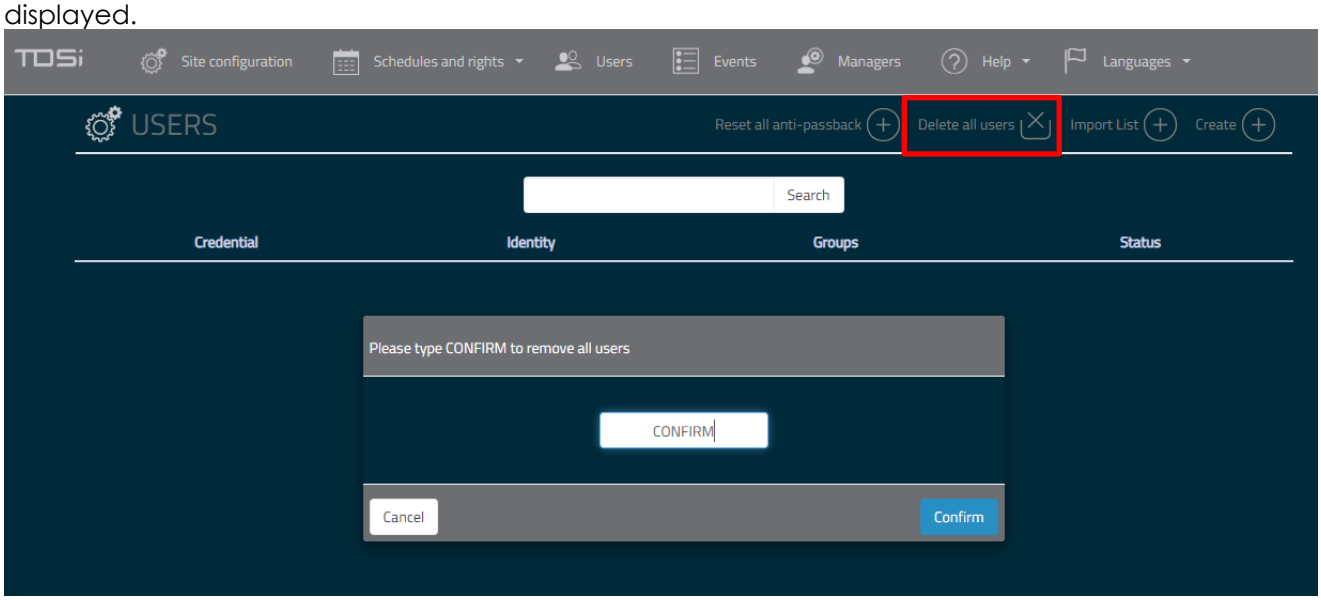
10.3 Importing Credentials

There is a limitation of 100 users using the ISO8859-1 file format. The available properties that can be mapped: **Credential, Surname, First Name, Group 1, Group 2, Group 3, Start Date, End Date**.
The **comma** character is set by default as the delimiter, other options include tab and semicolon.
Select the column to map to each property. The import process can read up to 20 columns.
Step 1 Select required file by clicking **Choose file** button.
Step 2 Select character separator from the dropdown menu.
Step 3 Map required properties by selecting the matching column.
Step 4 Click **Save** to start the import process.


IMPORT
Back
Credential: Not used
Surname : Not used
First Name : Not used
Group 1 : Not used
Group 2 : Not used
Group 3 : Not used
Start date : Not used
End date : Not used
Separator : Comma
Step 3
Step 2
Step 1
Step 4
Choose file
No file chosen
Save
100 users, file format: ISO8859-1
Not used
Not used
Column 1
Column 2
Column 3
Column 4
Column 5
Column 6
Column 7
Column 8
Column 9
Column 10
Column 11
Column 12
Column 13
Column 14
Column 15
Column 16
Column 17
Column 18
Column 19

10.4 Delete all Users

To delete all users, click **Delete all users** from the action bar.
A confirmation window appears. Type CONFIRM then click the **Confirm** button.
A new window is displayed to indicate deletion is in progress. When completed, Success window is displayed.

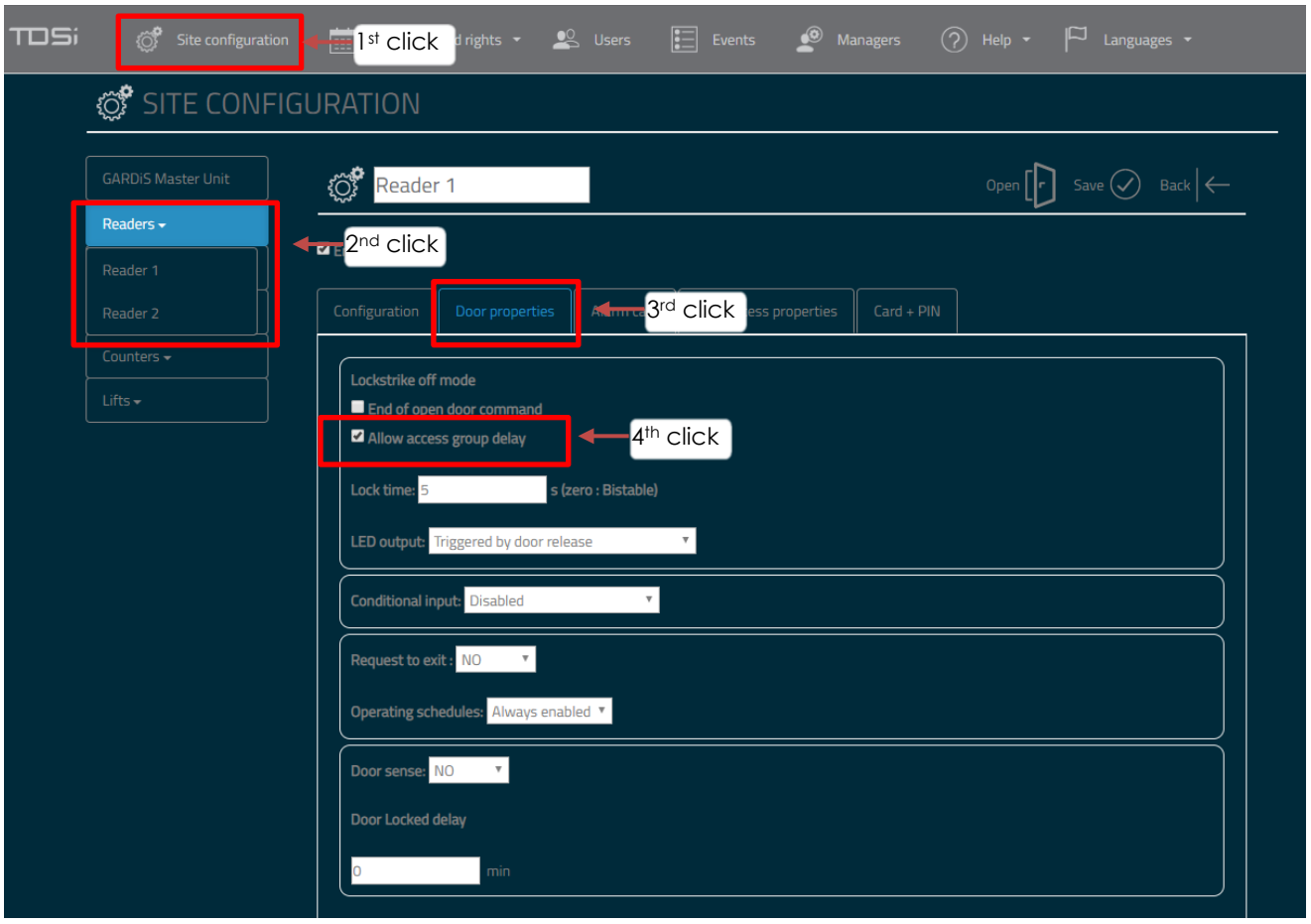


10.5 DDA Users

This section details how to allow required credentials extra time to gain entry through a door. This option is actioned using an access group rather than the individual credential.

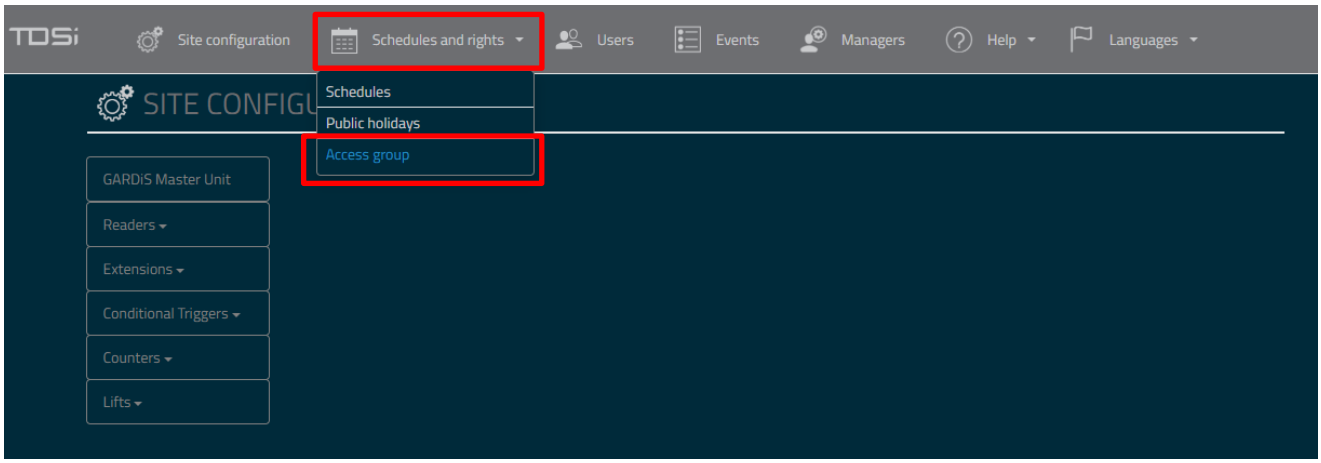
Step 1 Configure the door properties

Click **Site configuration**, select the required **reader** from the left menu and click the **Door properties** tab. Then check the box **Allow access group delay**.

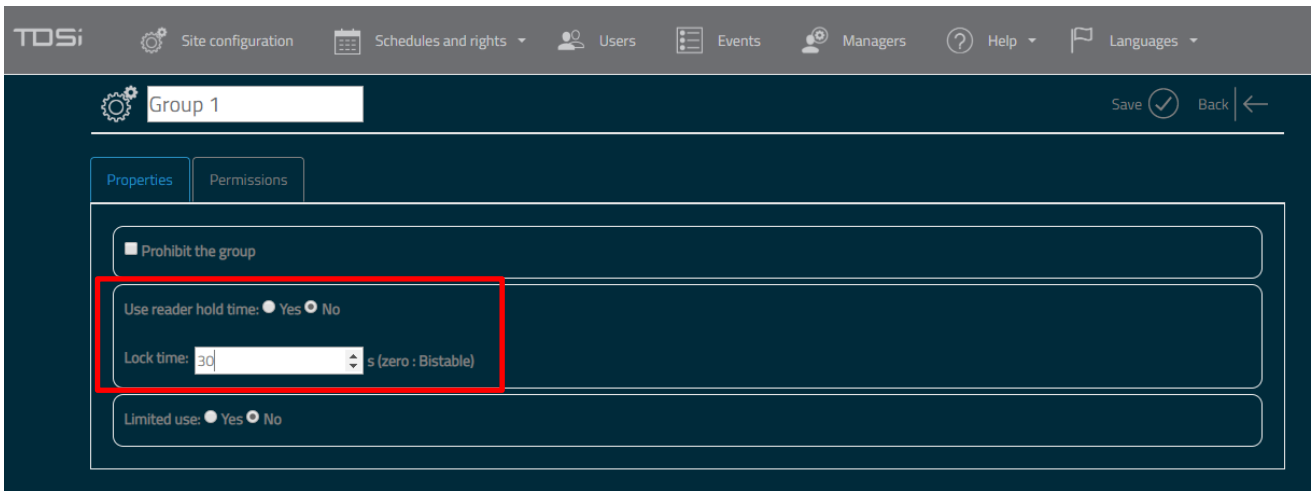


Step 2 Configure the Access group

Click **Schedules and rights** from the top menu, then click **Access group**.



Click the required Access group from the list e.g. Group 1. Then select **No** for **Use reader hold time** to override the reader hold time. This allows the configuration of the lock time for credentials within this access group. In the example below, credentials in this group will have 30 seconds to open the door. Maximum value 254. Click **Save.**



11. Adding Extensions

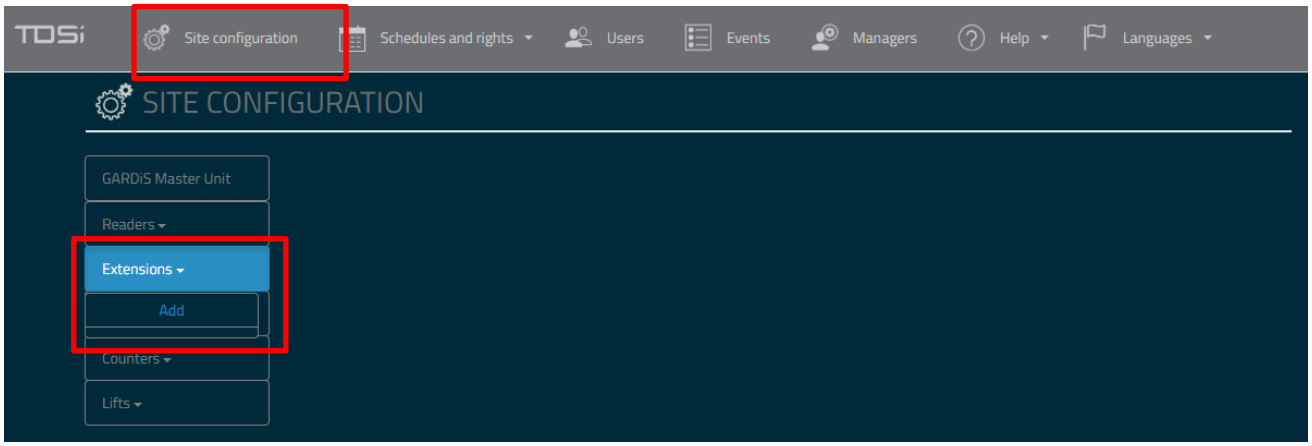
A GARDiS master can support

- Up to 10 x (GARDiS 4 EXT OR GARDiS IO EXT extension units)

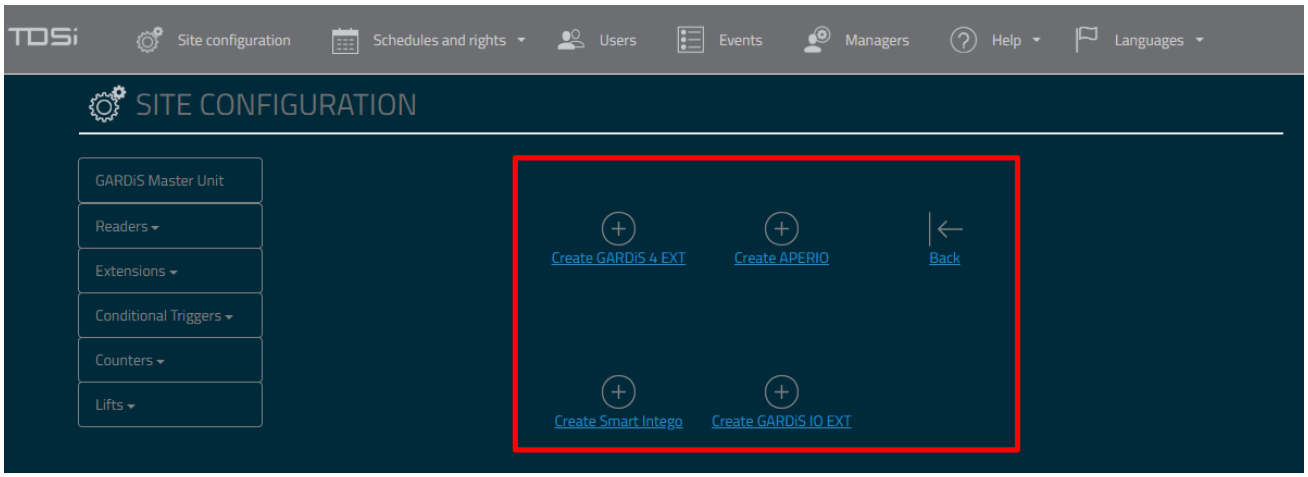
OR

- 1 IP Lock Hub with up to 10 IP Locks.

To add extension modules to the master controller, click **Site Configuration**, then click **Extensions** then **Add** from the left-hand menu.



The extensions available will display in the main window.



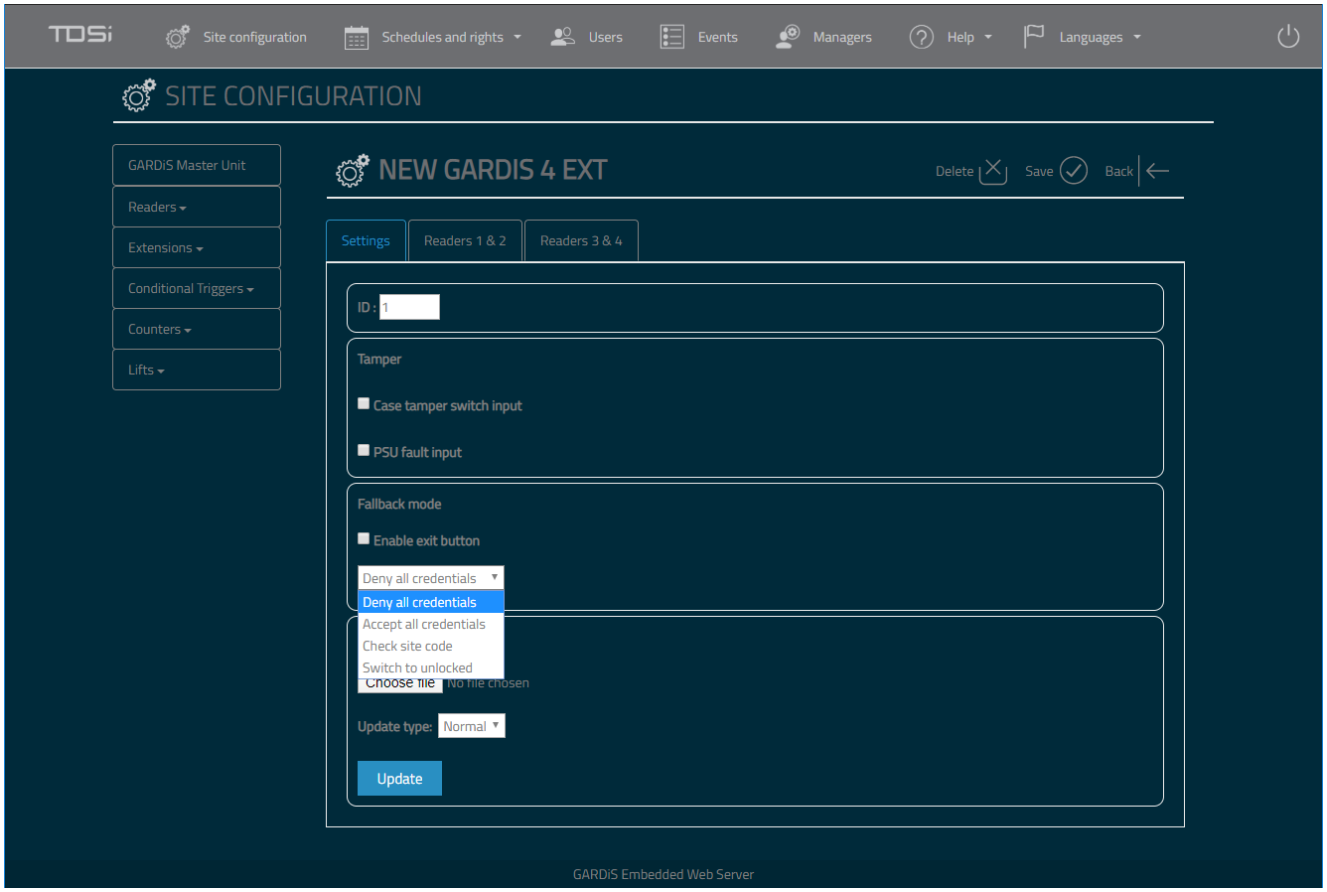
11.1 GARDiS 4 EXT

These slave controllers allow up to 4 doors per controller (up to a maximum of 10) to be added the master controller.

11.1.1 Fallback Mode

If a slave unit loses communication to a master controller there are a number of fallback modes available to end users.

Disable\Enable the exit button. This allows the end user to configure egress function when connection to master is lost.



Fallback Modes Available

- **Deny all credentials** – deny all credentials presented to the readers.
- **Accept all credentials** – accept all credentials presented to the readers.
- **Check site code** – Accept credentials that match the site code of the readers.
- **Switch to unlocked** – Unlock the doors on the slave unit to allow access.

11.2 Aperio

This allows an Aperio 485 hub to be added to the master controller. (These cannot be added along with slave controllers.)

11.3 Smart Intego

This allows a Simons Voss 485 hub to be added to the master controller. (These cannot be added along with slave controllers.)

11.4 GARDiS IO EXT

This allows a GARDiS IO extension board to be added to the controller. Limit of up to 10 slave units on a single master controller.

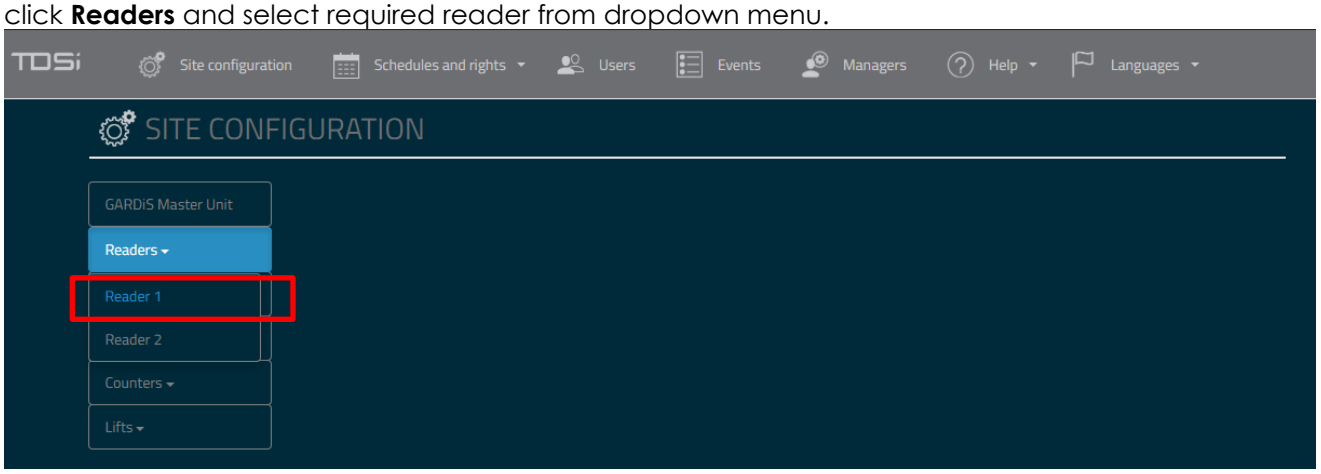
Fallback Modes
Keep the previous state
Enable all outputs
Disable all outputs

12. Lift Control

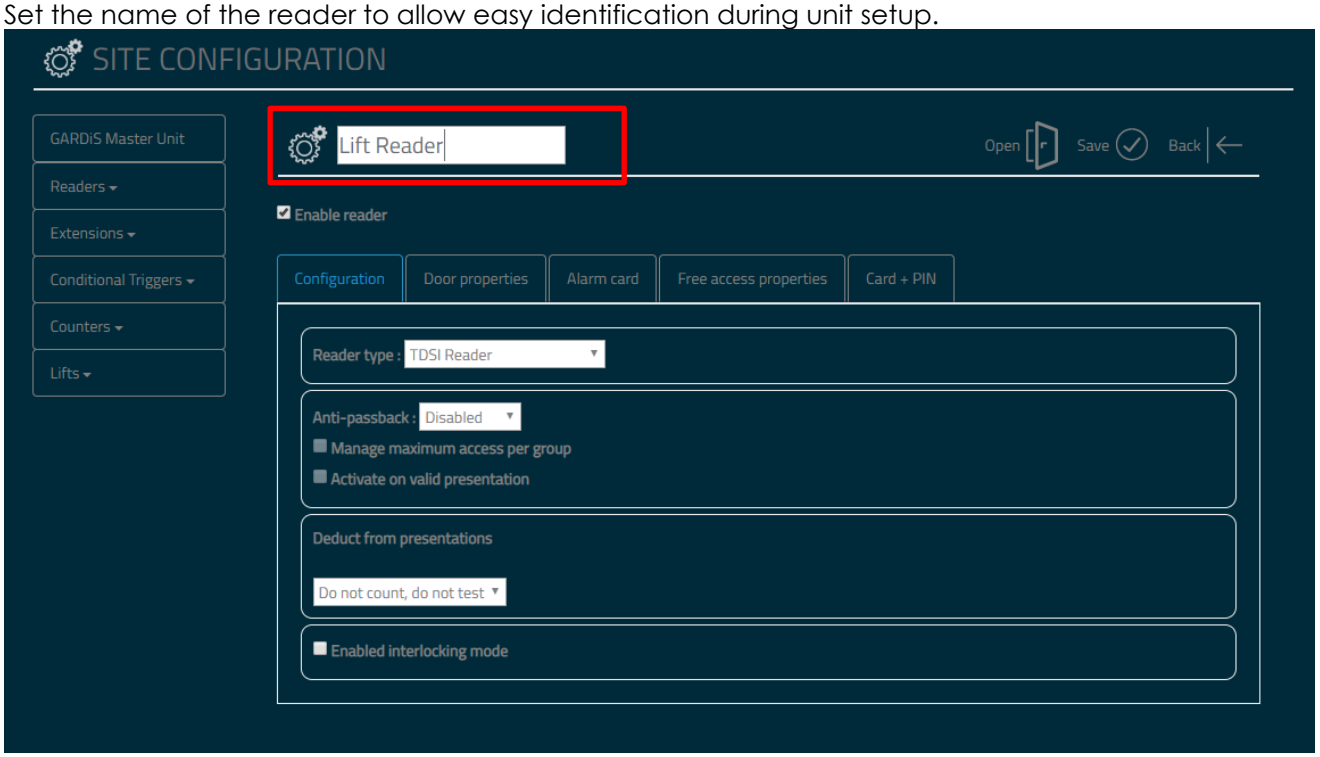
To configure lift control, a GARDiS IO Extension board must be used.

Step 1 Configure the reader

Select the reader that is controlling the lift outputs. Click **Site Configuration** from the top menu, then click **Readers** and select required reader from dropdown menu.

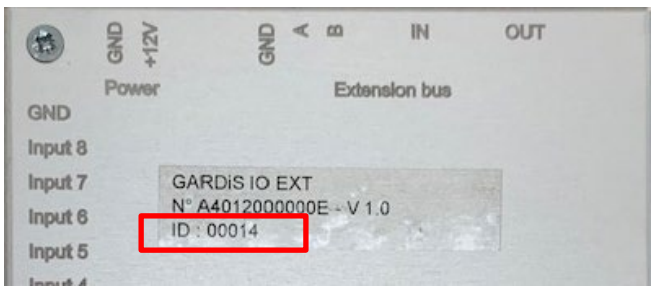


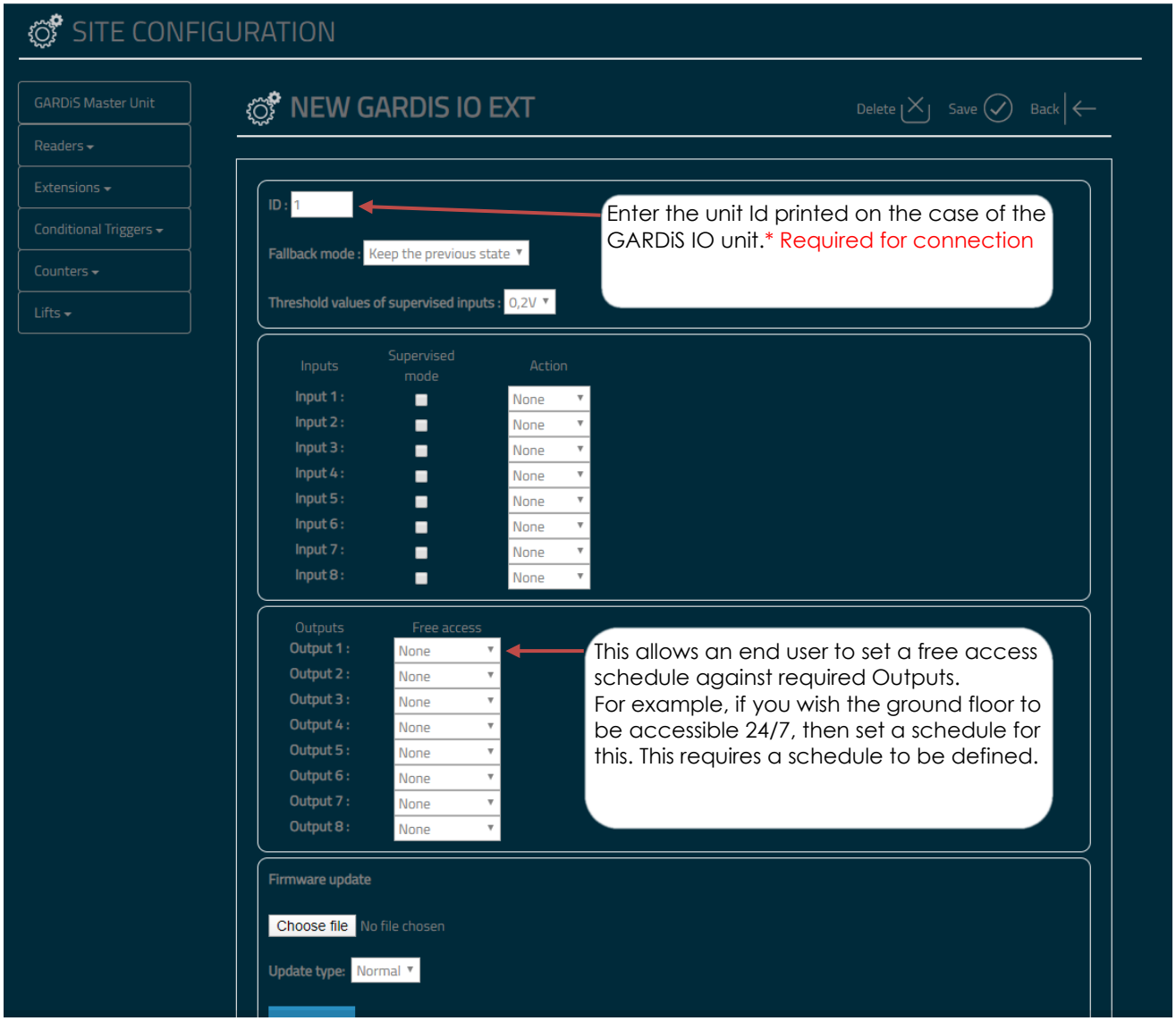
Set the name of the reader to allow easy identification during unit setup.



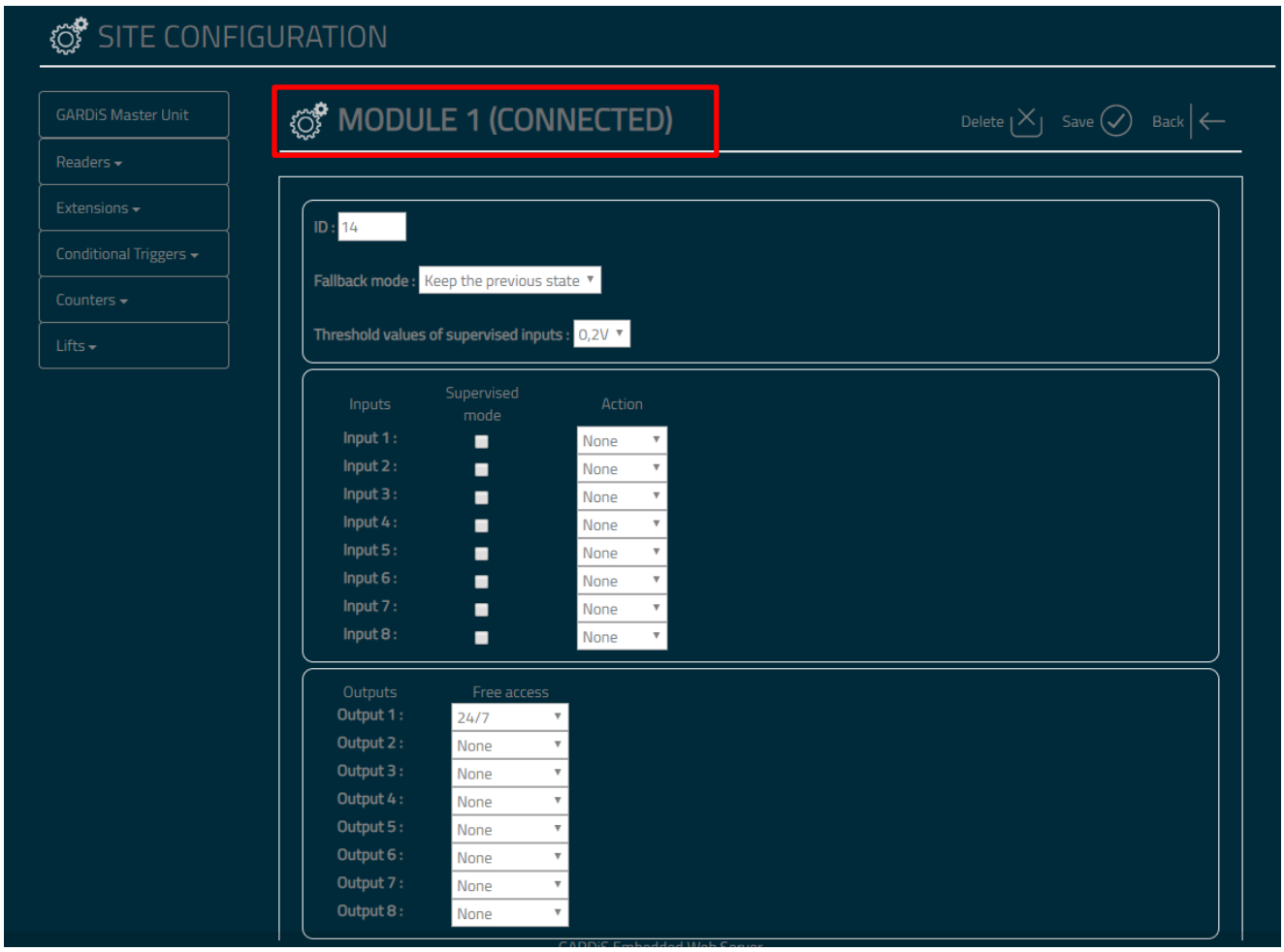
Step 2 Add the GARDiS IO Extension Module

Go to **Site Configuration** and click **Extensions** and then **Add**. Click **Create GARDiS IO EXT** from the main display. The following screen will be displayed. Have the ID of the GARDiS IO EXT ready. This is located on the unit, printed on the label.



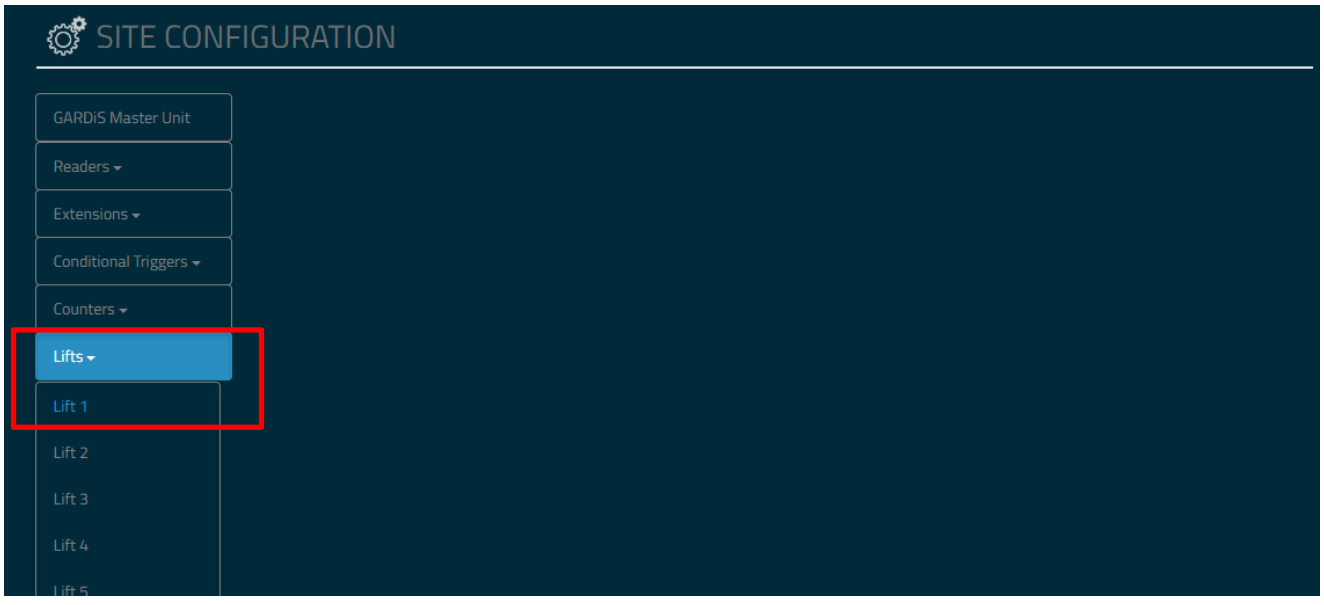


Once the required details are entered. The name of the module at the top will display **(CONNECTED)**. In the example below, the unit number is set to **14** and I have set Output 1 to have a free access schedule of 24/7. A schedule that has been configured in the unit.

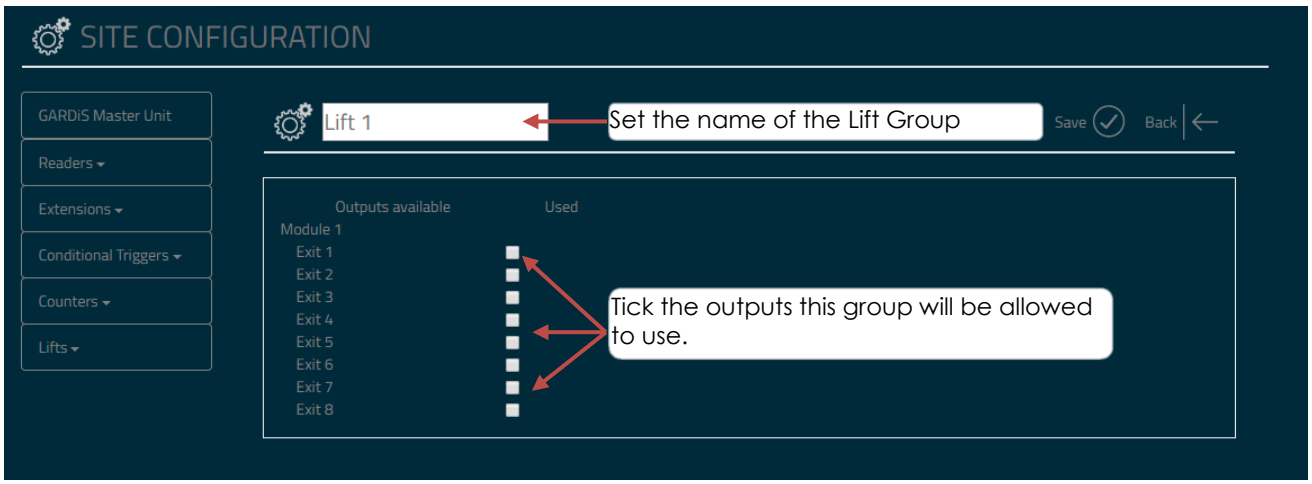


Step 3 Configure the Lift Groups

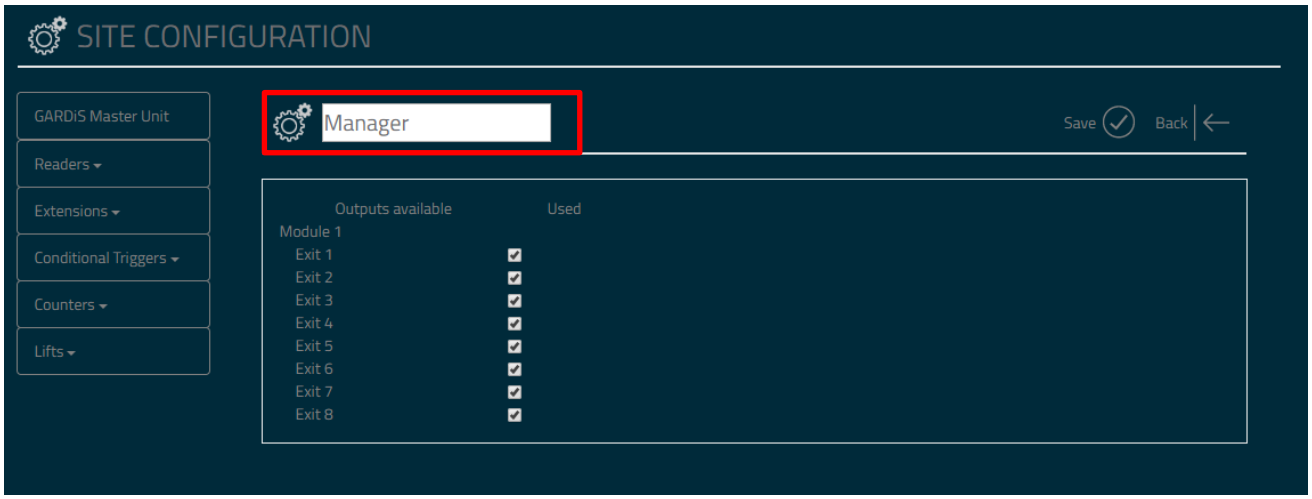
Up to 256 lift groups can be defined. Select the 1st available lift group.



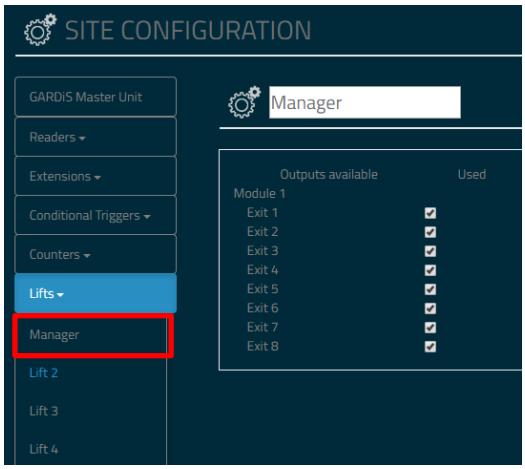
The configuration for that group is displayed in the main window.



Enter the required configuration and click **Save**. In the following example demonstrates a new lift group called **Manager**. This group will have access to all 10 outputs.



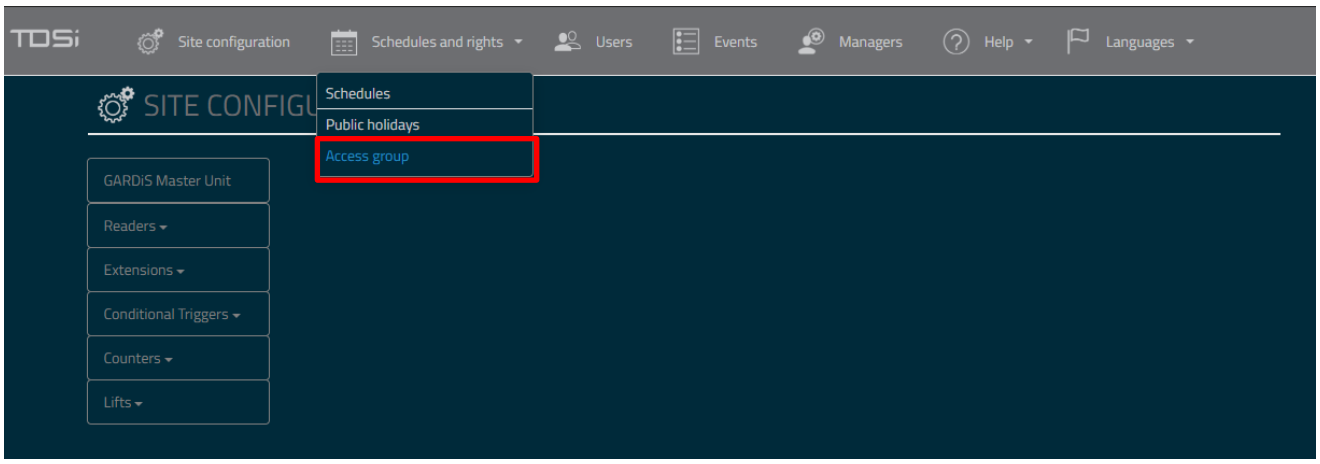
The list is now updated with the new name.



Continue to create lift groups as required.

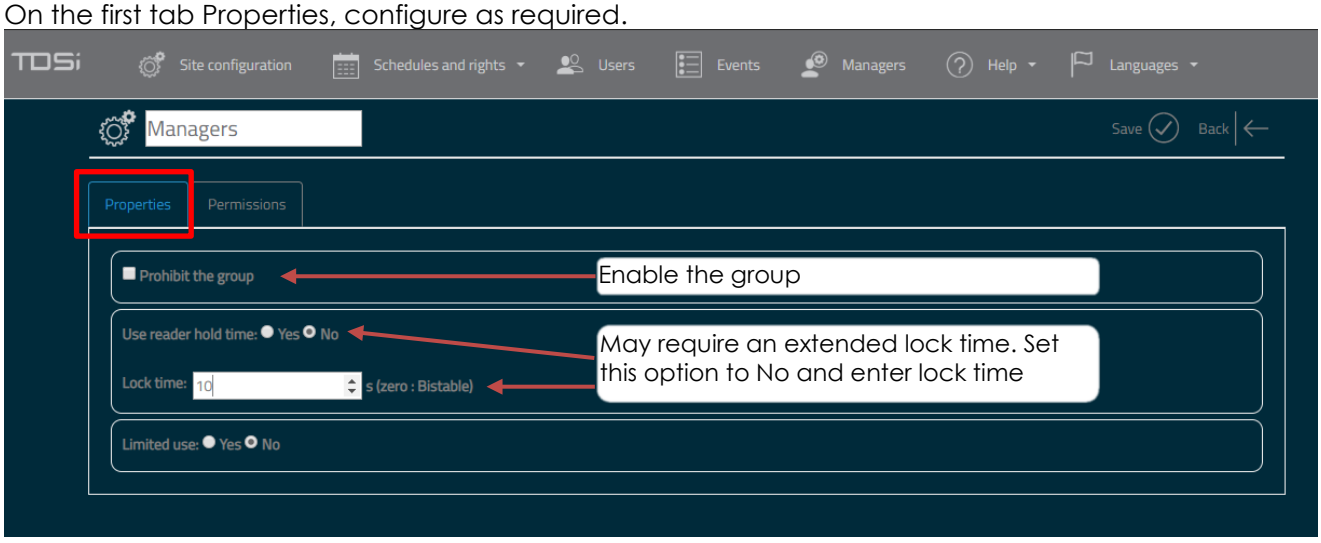
Step 4 Configure Access Groups

Click **Schedules and rights** from top menu and then click **Access Groups**.

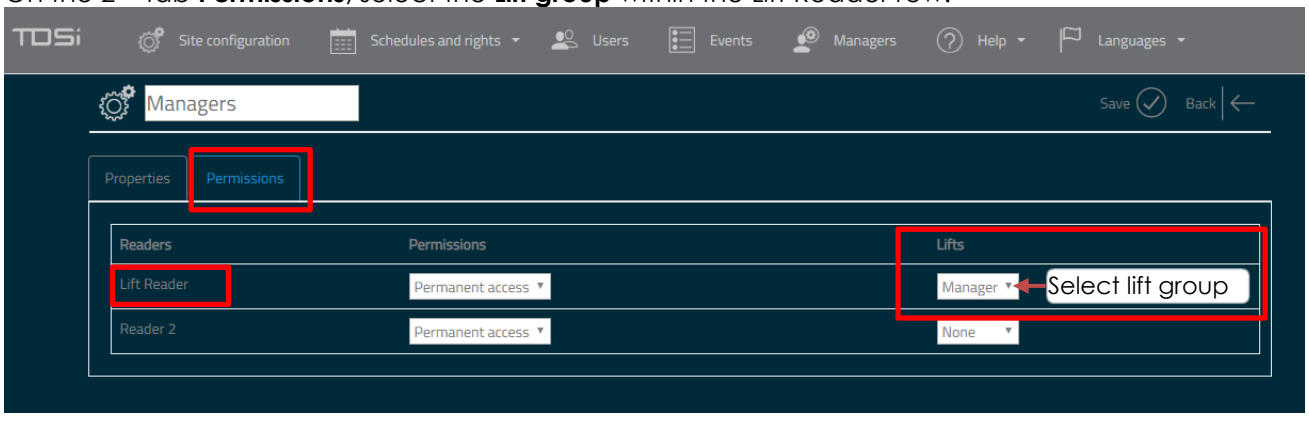


Select the access group to assign the lift group.

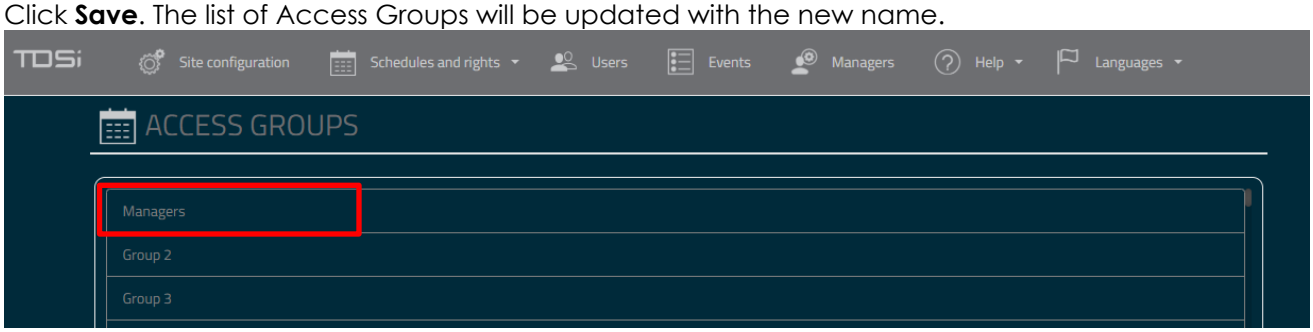
On the first tab Properties, configure as required.



On the 2nd tab **Permissions**, select the **Lift group** within the Lift Reader row.

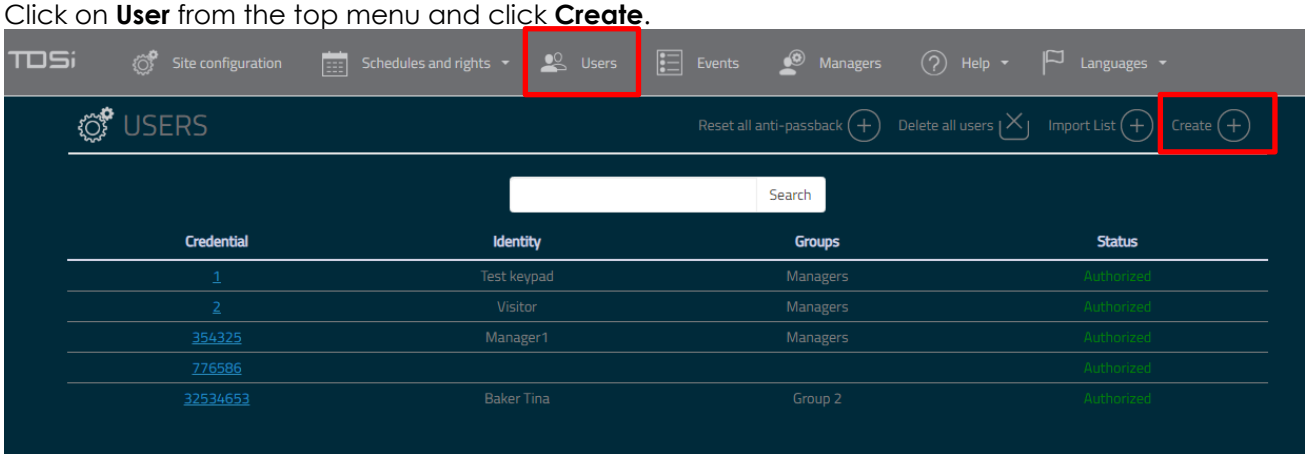


Click **Save**. The list of Access Groups will be updated with the new name.

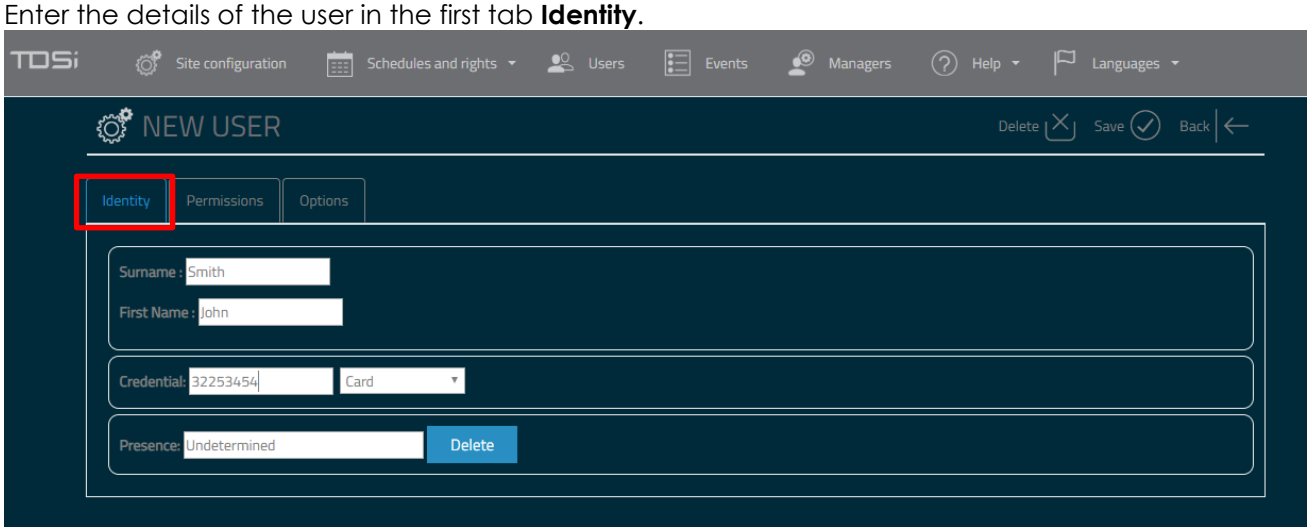


Step 5 Create a user with the new access group

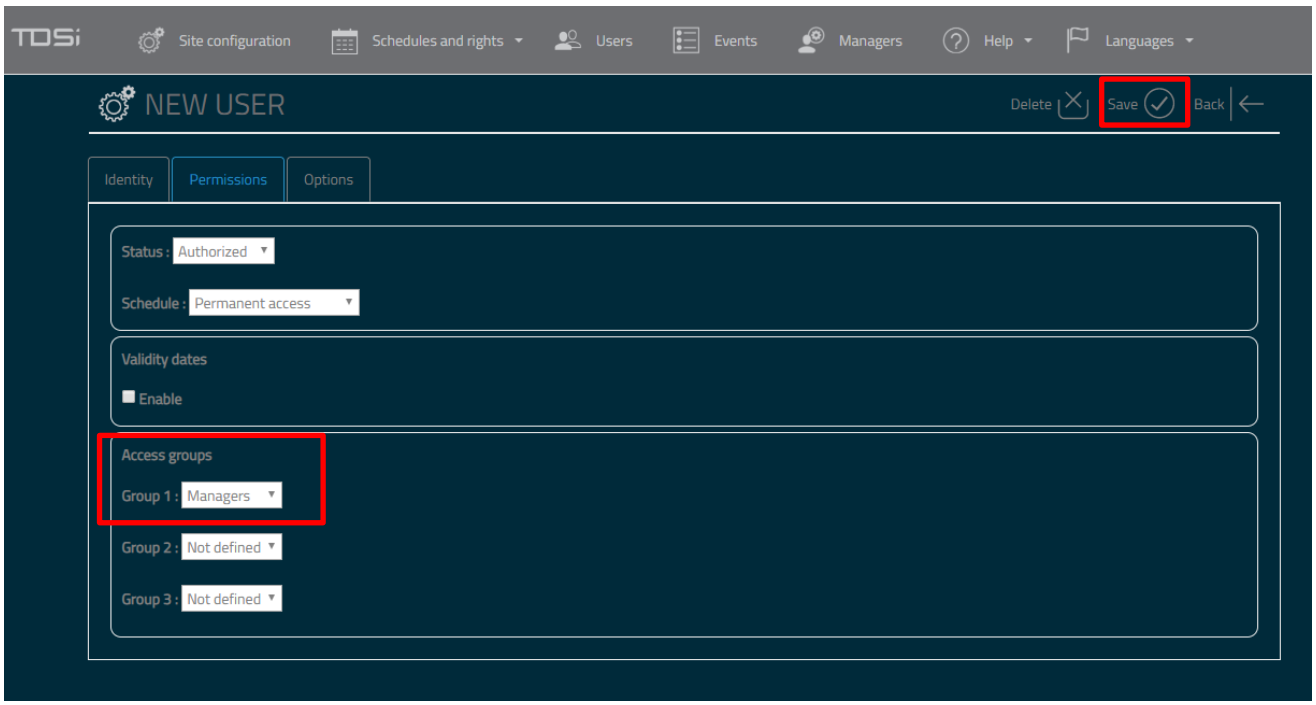
Click on **User** from the top menu and click **Create**.



Enter the details of the user in the first tab **Identity**.



Click the next tab **Permissions** and set the required configuration. Within the **Access Groups** section, select the group with the configured Lift group. Then click **Save**.



This user is now configured to use the lift reader.

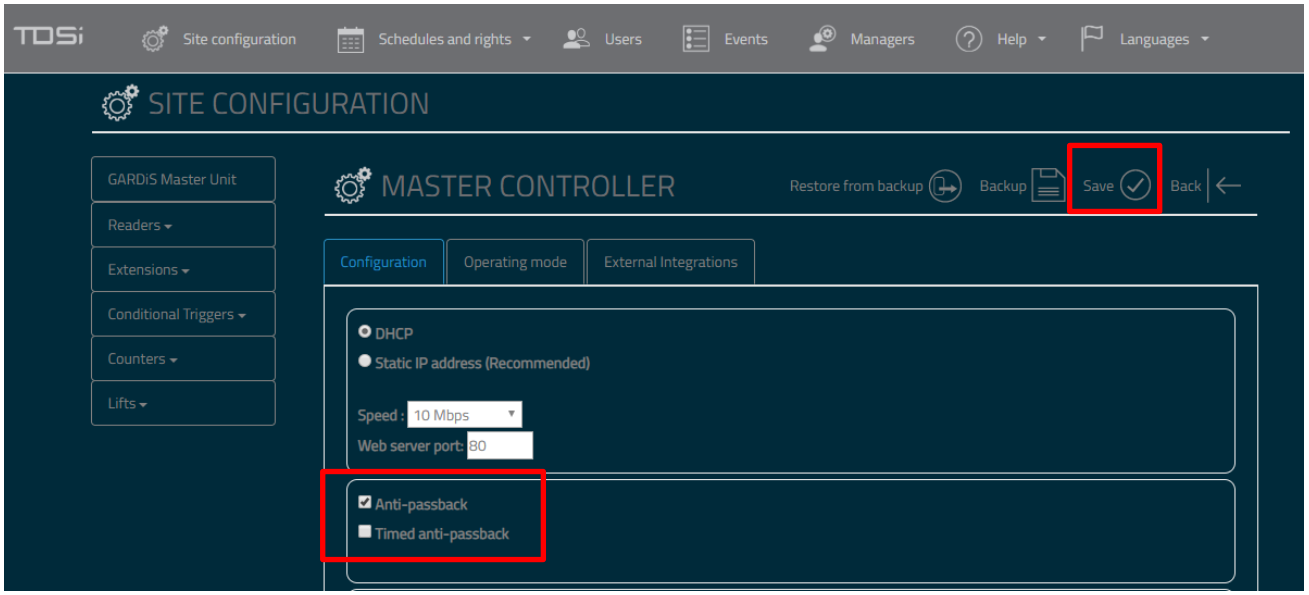
13. Anti-passback

There a number of anti-passback options available, true anti-passback and timed anti-passback. It is also possible to update the anti-passback value when the person opens the door, not when only present the card to the reader. This requires the setting of the door sense property within Door properties.

13.1 True Anti-passback

Step 1 Enable anti-passback on the unit.

Click Site configuration from the top menu, then **click GARDiS Master Unit** from the left hand menu. **Tick Anti-passback** checkbox. **Click Save**.

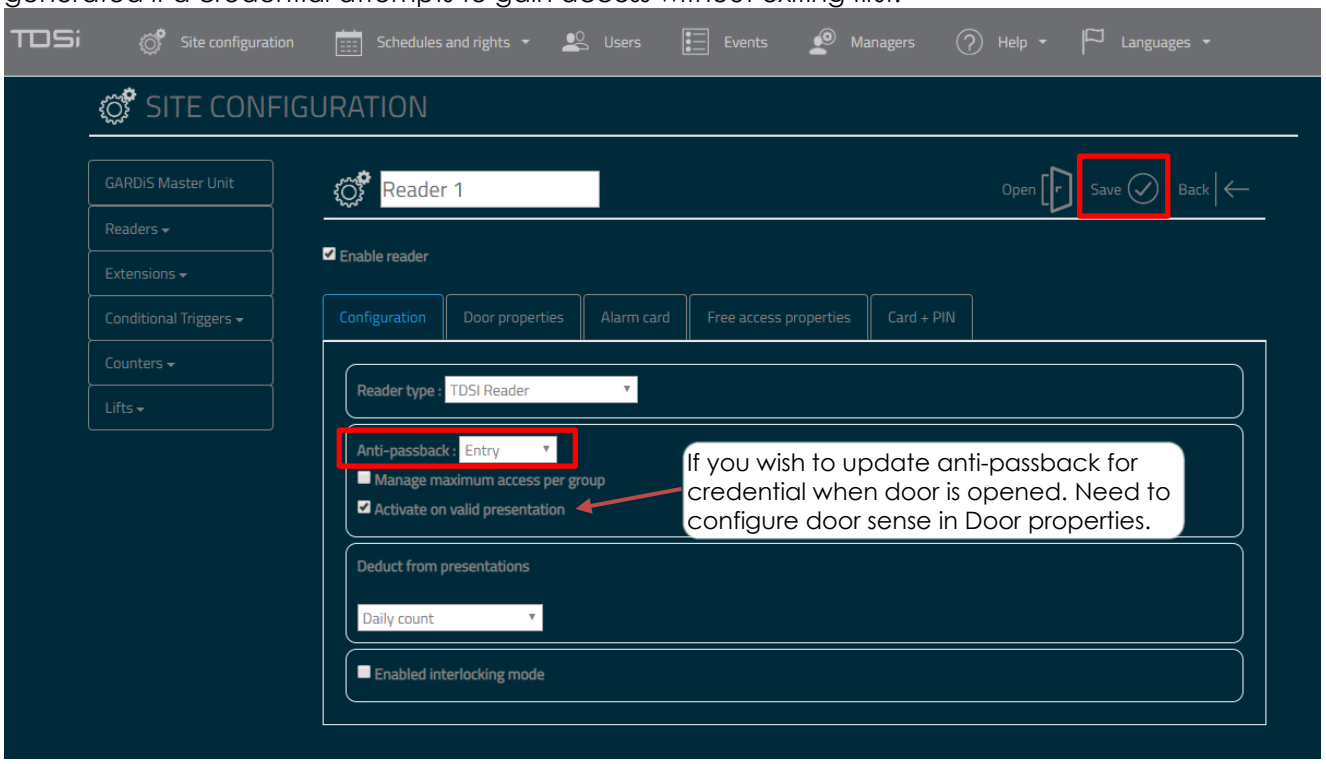


Step 2 Configure the readers for anti-passback

Click Readers and **select the required reader** from the menu. In the **Configuration tab** navigate to the Anti-passback section. Select the required option for the reader. The options available are:

Disabled (default): Not enforcing anti-passback
Entry: Set reader as entry reader

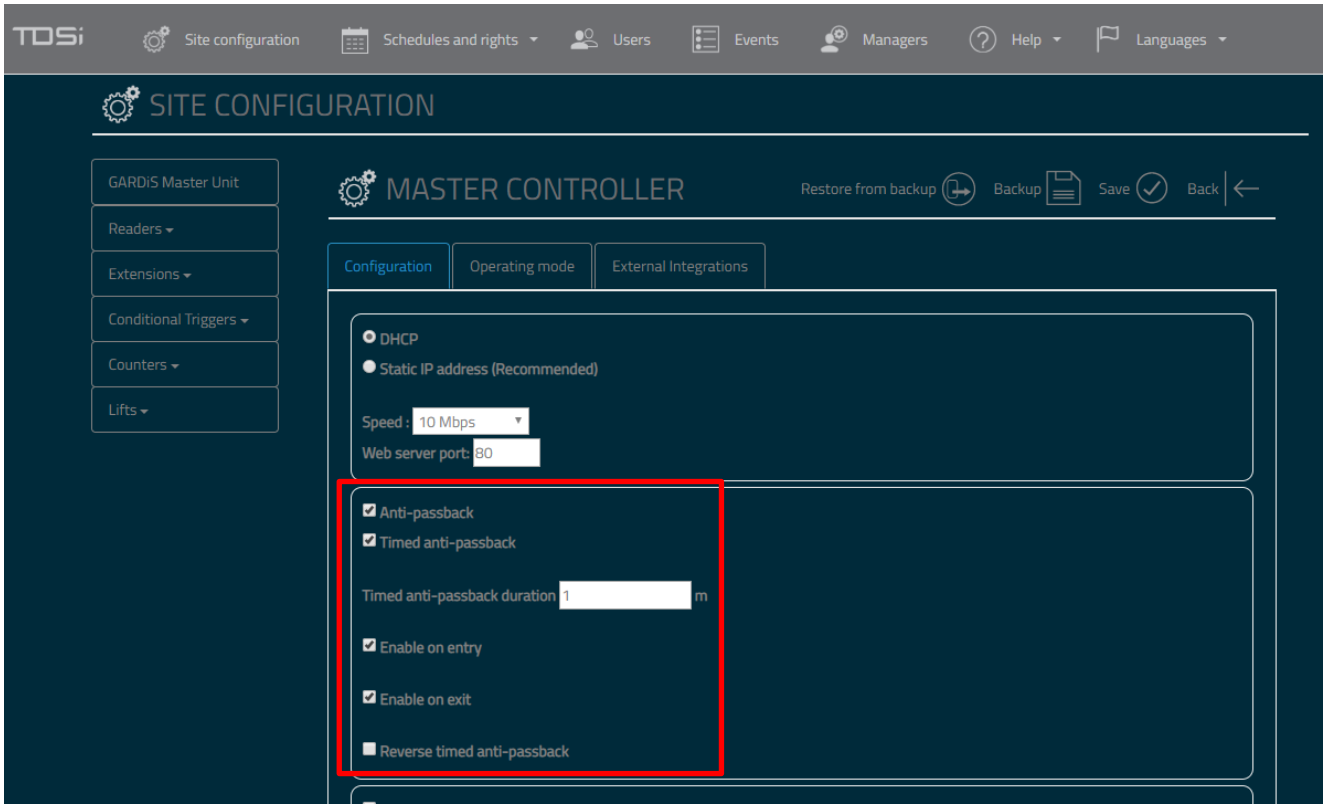
Exit: Set reader as exit reader
Entry \ Exit: Set reader to ignore anti-passback
Then click **Save**. Anti-passback is now setup on the controller. The event "User already entered" will be generated if a credential attempts to gain access without exiting first.



13.2 Timed Anti-passback

Step 1 Enable anti-passback settings

Click Site configuration from the top menu, then **click GARDiS Master Unit** from the left-hand menu. **Tick Anti-passback** and **Timed anti-passback** checkboxes. Set the length of time you wish to enforce anti-passback. This can be enabled on the Entry or Exit readers. **Click Save**. Follow **step 2** from 13.1True Anti-passback to configure the reader settings.

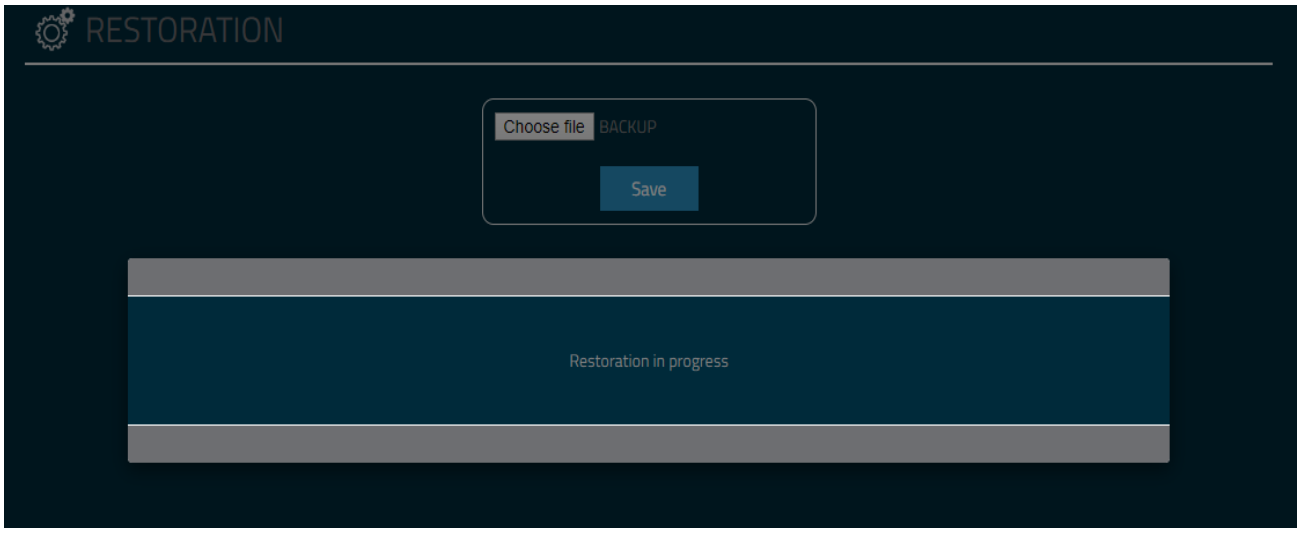


14. Troubleshooting

This chapter will provide typical issues that may arise.

14.1 Restoring from backup

Symptom: When restoring from backup, the following message is stuck on the screen and it does not finish the restoration.



Fix: A backup must occur in-between restorations. Create a new backup. Then follow the restore from backup process, selecting the required backup file.

Do you have any technical questions?

Contact our free technical support:

TDSi UK:
T: +44 (0) 1202 723 535
E: support@tdsi.co.uk

TDSi Export:
T: +33 (0) 1 58 84 20 90
E: info@tdsi-france.com

Because everyone deserves peace of mind

TDSi UK
Unit 10 Concept Park, Innovation Close, Poole, Dorset BH12 4QT United Kingdom
t 44 0 1202 723535 f 44 0 1202 724975 e sales@tdsi.co.uk

TDSi France
Immeuble ATRIA, 2 rue du Centre, 93160 NOISY LE GRAND France
t 33 0 1 58 84 20 90 f 33 0 1 58 84 20 91 e info@tdsi-france.com