

The background of the page features a modern, abstract design with large, overlapping geometric shapes in various shades of blue (dark blue, medium blue, and light blue) and white. The shapes create a dynamic, angular pattern that frames the central text.

GARDiS-Controller – Integrierter Webserver

Bedienungsanleitung

UM0121 Ausgabe 3

Vorwort

Copyright © 2002 TDSi. Alle Rechte vorbehalten.

Time and Data Systems International Ltd verfolgt eine Politik der kontinuierlichen Verbesserung und behält sich das Recht vor, Spezifikationen, Farben oder Preise seiner Produkte ohne vorherige Ankündigung zu ändern.

Garantie

Fünf Jahre Garantie inklusive. Für weitere Garantiebedingungen wenden Sie sich bitte an Ihren Lieferanten.

Marken

Copyright © 2002 Time and Data Systems International Ltd (TDSi). Dieses Dokument sowie die mitgelieferte Software dürfen ausschließlich für den vorgesehenen Zweck verwendet werden; eine Vervielfältigung von Teilen dieses Dokuments ist ohne vorherige schriftliche Zustimmung von TDSi untersagt.

Microsoft und Windows sind eingetragene Marken der Microsoft Corporation.

Alle anderen Marken und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer.

Hinweise und Anmerkungen

In dieser Anleitung werden die folgenden Symbole verwendet:



VORSICHT! Dies weist auf eine wichtige Betriebsanweisung hin, die befolgt werden sollte, um mögliche Schäden an Hardware oder Eigentum, Datenverlust oder Personenschäden zu vermeiden.



HINWEIS. Dies kennzeichnet wichtige Informationen, die Ihnen helfen, dieses Produkt optimal zu nutzen.

Inhaltsverzeichnis

	Einleitung.....	5
1.	Informationen und Empfehlungen	5
2.	Spezifikation.....	6
3.	Einstellung der IP-Adresse	7
4.	Überprüfung eines Nachweises	9
5.	Sicherung.....	17
6.	Wiederherstellung aus der Sicherung.....	18
7.	Standortkonfiguration	20
8.1	GARDiS-Master-Einheit	20
8.1.1	Konfiguration	20
8.1.2	Betriebsmodus/Lesegeräte.....	21
8.1.3	Externe Integrationen.....	21
	Lesegeräte.....	21
8.2.1	Tastaturleser	22
8.2.2	Takt & Daten	23
8.2.3	Benutzerdefiniertes Wiegand-Protokoll.....	23
8.2.4	Türeigenschaften.....	24
	Zeitpläne	26
9.1	Erstellen einer Aufstellung.....	26
9.2	Einem Zugriffsbereich einen Zeitplan zuweisen.....	29
9.	Benutzer	31
10.1	Neuen Benutzer anlegen	31
10.1.1	Registerkarte „Identität“	31
10.1.2	Registerkarte „Berechtigungen“	31
10.1.3	Registerkarte „Optionen“	32
10.2	Neuen Benutzer aus einem Ereignis anlegen	33
10.3	Anmeldedaten importieren.....	33
10.4	Alle Benutzer löschen.....	35
10.5	DDA-Benutzer	35
	Erweiterungen hinzufügen	36
11.1	GARDiS 4 EXT	37
11.1.1	Fallback-Modus	37
11.2	Aperio.....	38
11.3	Smart Intego.....	38
11.4	GARDiS IO EXT.....	38
	Liftsteuerung.....	39
	Anti-Passback	45
13.1	Echte Anti-Passback-Funktion	45
12.		
13.		

13.2	Zeitgesteuertes Anti-Passback	46
14.	Fehlerbehebung	47
14.1	Wiederherstellung aus dem Backup	47

1. Einleitung

Vielen Dank, dass Sie sich für das TDSi GARDiS Controller-Zutrittskontrollsystem entschieden haben. Es gibt drei Haupttypen von GARDiS-Master-Controllern: -

- **GARDiS 1**
 - 1-Tür-Controller mit Anschlüssen für 1–2* Lesegeräte.
- **GARDiS 2**
 - 2-Tür-Controller mit Anschlüssen für 2–4* Lesegeräte.
- **GARDiS 4.**
 - 4-Tür-Steuergerät mit Anschlüssen für 4–8* Lesegeräte.

Der GARDiS-Controller wird eigenständig betrieben und erfordert keine separate Softwareinstallation.

Die Konfiguration des Zutrittskontrollsystems erfolgt über einen integrierten Webserver, auf den der Benutzer von jedem kompatiblen Webbrowser aus zugreifen kann.

Der GARDiS-Controller kann als Master-Controller mit bis zu 10** Erweiterungsmodulen betrieben werden. Zu den Erweiterungsmodulen gehören GARDiS-Slave-Controller, die eine Kapazität von bis zu 44 Türen ermöglichen, sowie E/A-Module zur Überwachung und Steuerung von Geräten und drahtlosen IP-Schlössern***. Weitere Informationen zu diesen Erweiterungsmodulen sowie Installationsanleitungen finden Sie ebenfalls in diesem Handbuch.

Dieses Handbuch führt Sie durch die Konfiguration der GARDiS-Controller über den integrierten Webserver.

* Die Obergrenze setzt TDSi-Lesegeräte für das Reverse-LRC-Protokoll (Ein-/Ausgangsleser) voraus.

** Ein Lizenz-Dongle ist erforderlich, um weitere Türen im System zuzulassen.

*** Drahtlose IP-Schlösser sind auf 10 Türen begrenzt.

2. Informationen und Empfehlungen

Gemäß der europäischen Richtlinie UTE C00-200, die die Richtlinien 2004/108/EG einbezieht, erfüllt GARDiS die folgenden Normen:



- NF EN 50081-1 zur elektromagnetischen Strahlung
- NF EN 50082-1 zur elektromagnetischen Störfestigkeit

3. Spezifikation

TDSi-Teilenummer	GARDiS 1 5002-6001 GARDiS 2 5002-6002 GARDiS 4 5002-6004
Funktionen	
Max	5.000 Zugangsdaten
Türen	1, 2 oder 4 Türen
Lesegeräte	Bis zu 2 TDSi-Lesegeräte pro Tür in einer Ein- und Auslesekonfiguration. Alternativ 1 Lesegerät pro Tür, ausgestattet mit den branchenüblichen Ausgangsformaten „Clock & Data“, „Wiegand Multiformat“ oder „RS 485“.
Eingänge	1 pro Tür Zusätzlich verfügbar mit I/O-Modul
Ausgänge	Steuerrelais: 1 A / 12 V – 1 A / 24 V, 1 pro installierter Tür GARDIS 1: 2 Ausgänge GARDIS 2: 3 Ausgänge GARDIS 4: 5 Ausgänge
Erweiterungsoptionen	GARDiS 4+ (4 Türen); Modul mit 8 Eingängen/8 Ausgängen; drahtlose IP-Schlösser
Zeitgruppen	128
Anti-Passback	Zeitgesteuert und absolut
Mantrap-Funktion	Ja
Kommunikation	TCP/IP und RS 485 für Erweiterungsmodule

4. Einstellung der IP-Adresse

Statischer IP-Modus: Die Standard-IP-Adresse lautet 192.168.2.150, die Subnetzmaske 255.255.255.0

Der Computer, der für die Verbindung mit dem Gerät verwendet wird, muss eine IP-Adresse im Bereich 192.168.2.xxx haben.

Schritt 1

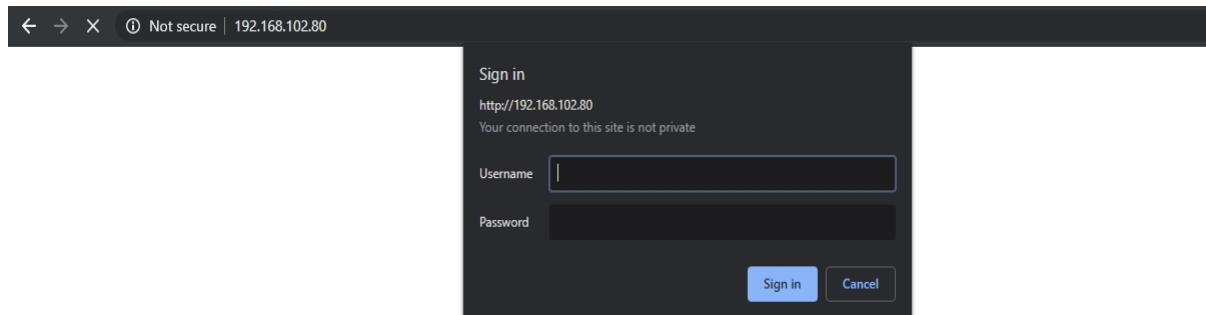
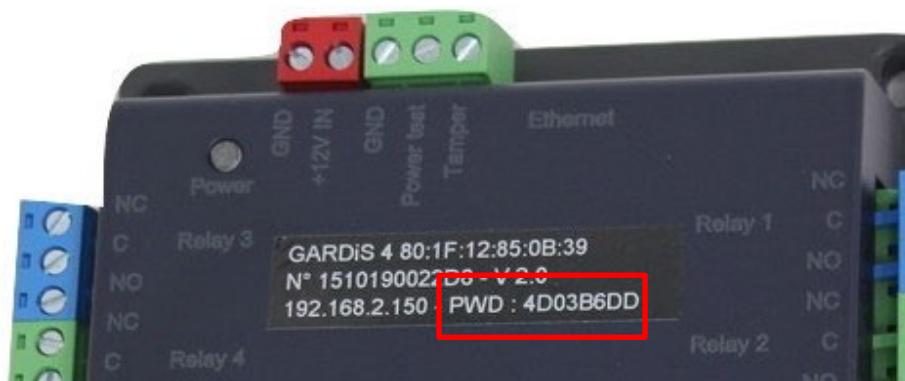
Öffnen Sie einen Webbrowser, z. B. Chrome, Firefox oder Microsoft Edge.

Geben Sie die IP-Adresse 192.168.2.150 ein

Es erscheint ein Popup-Fenster.

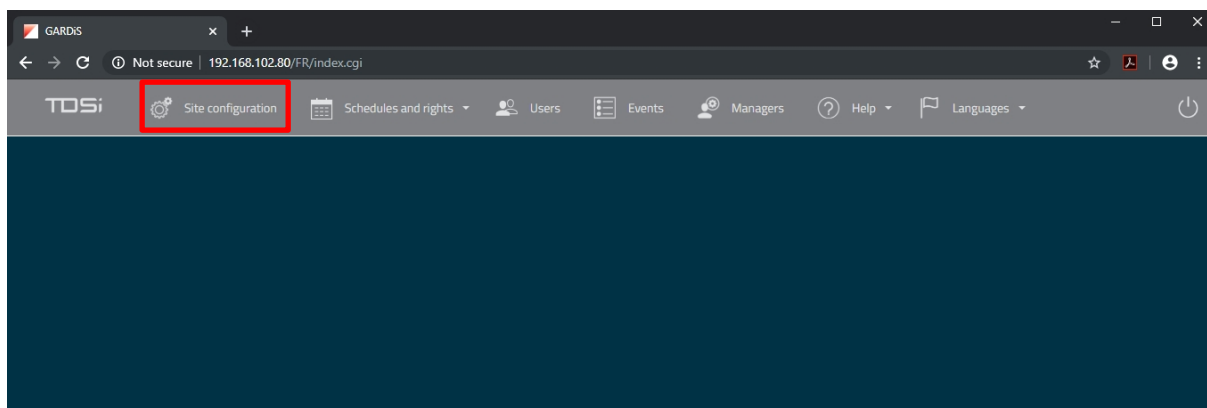
Geben Sie den Benutzernamen ein: admin

Passwort: Auf dem Aufkleber auf dem Kunststoffgehäuse des GARDiS-Geräts aufgedruckt.



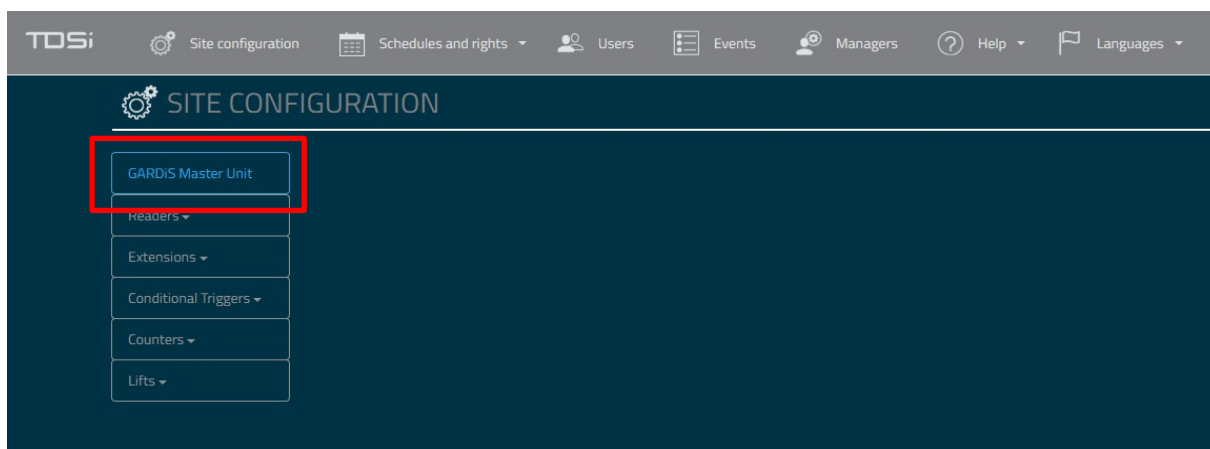
Schritt 2

Nach der Anmeldung wird der folgende Bildschirm angezeigt. **Klicken Sie auf „Site-Konfiguration“.**



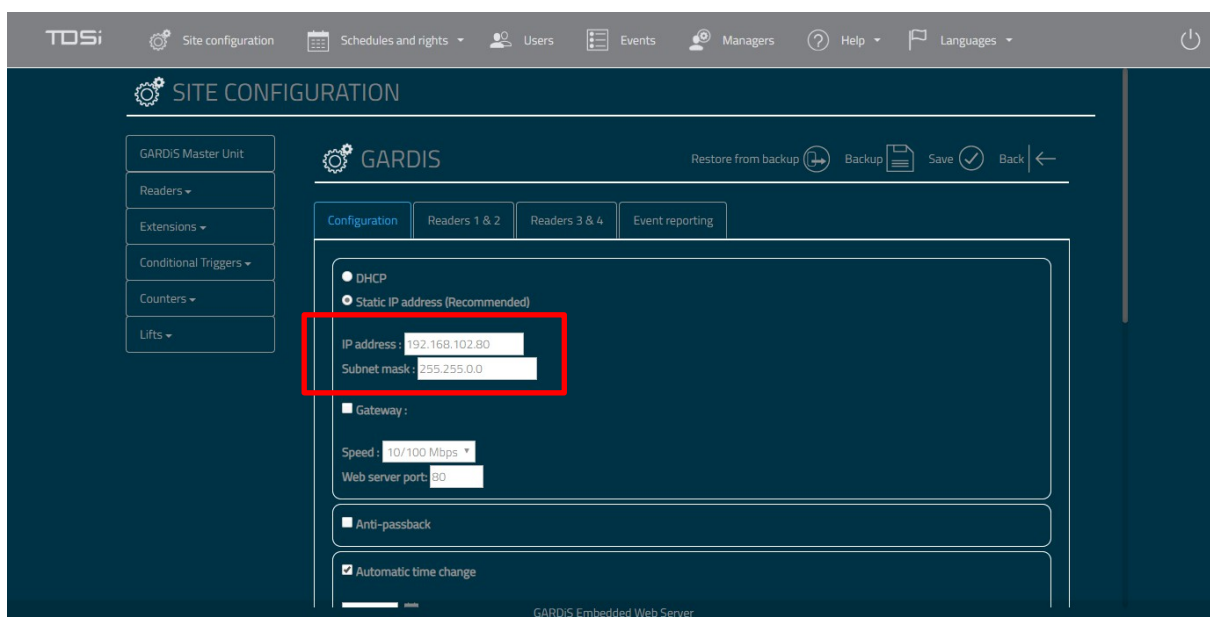
Schritt 3

Klicken Sie im Menü auf „GARDiS-Master-Einheit“.



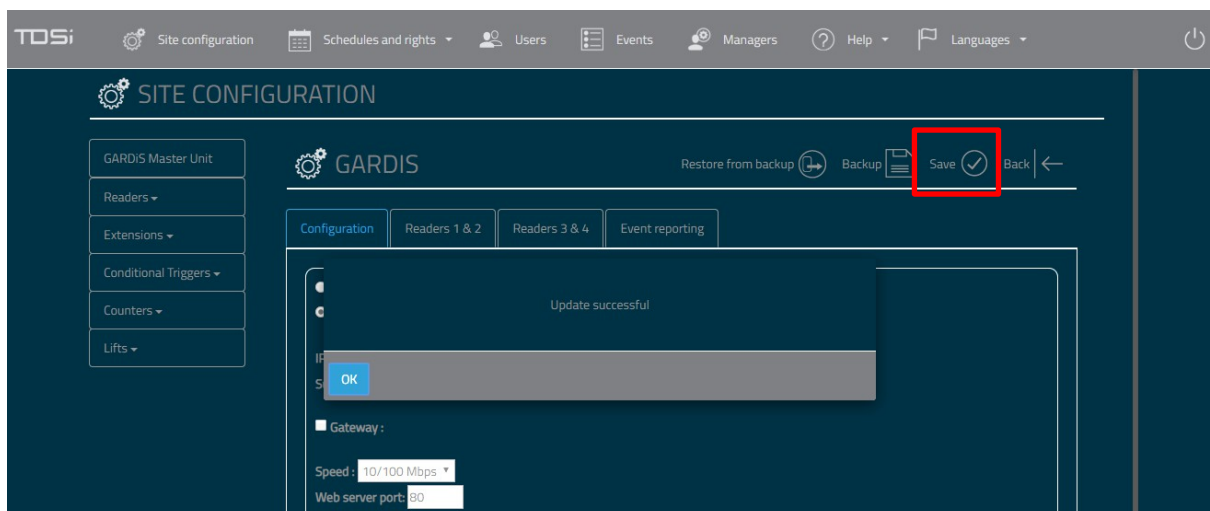
Schritt 4

Geben Sie die erforderlichen IP-Einstellungen ein.



Schritt 5

Klicken Sie auf „Speichern“.



5. Validierung eines Zugangsmediums

Dieses Kapitel führt Sie Schritt für Schritt durch die Einrichtung eines Türsteuerungsgeräts, um einem Zugangsnachweis die Berechtigung „**Zugang** gewährt“ zu erteilen.

Schritt 1

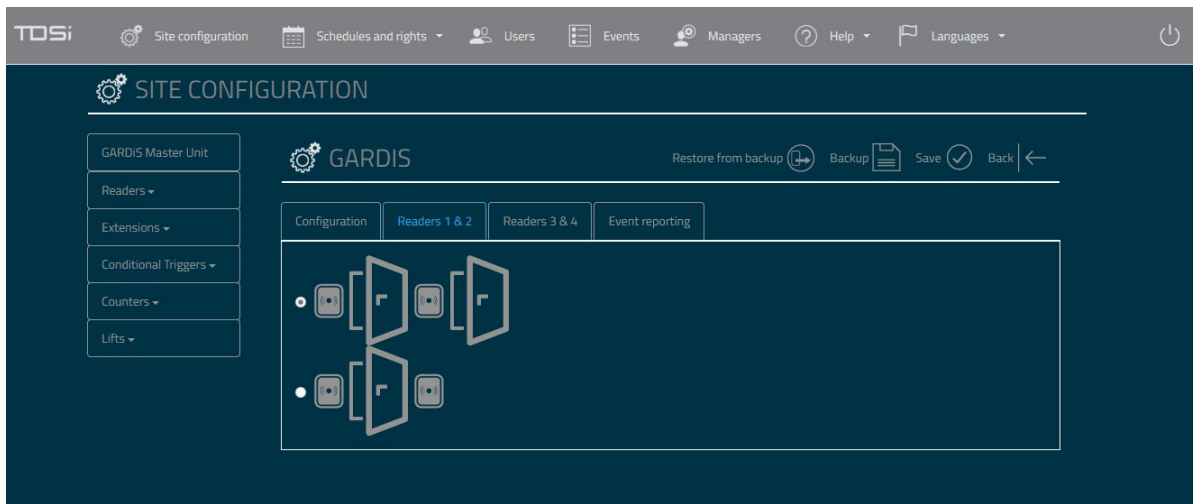
Wählen Sie die Leserkonfiguration aus

Option 1 – 1 Lesegerät pro Tür

z. B. Lesegerät-Kanal 1 ist Tür 1 zugeordnet, Lesegerät-Kanal 2 ist Tür 2 zugeordnet Option 2 – Ein-/Ausgangsleser pro Tür

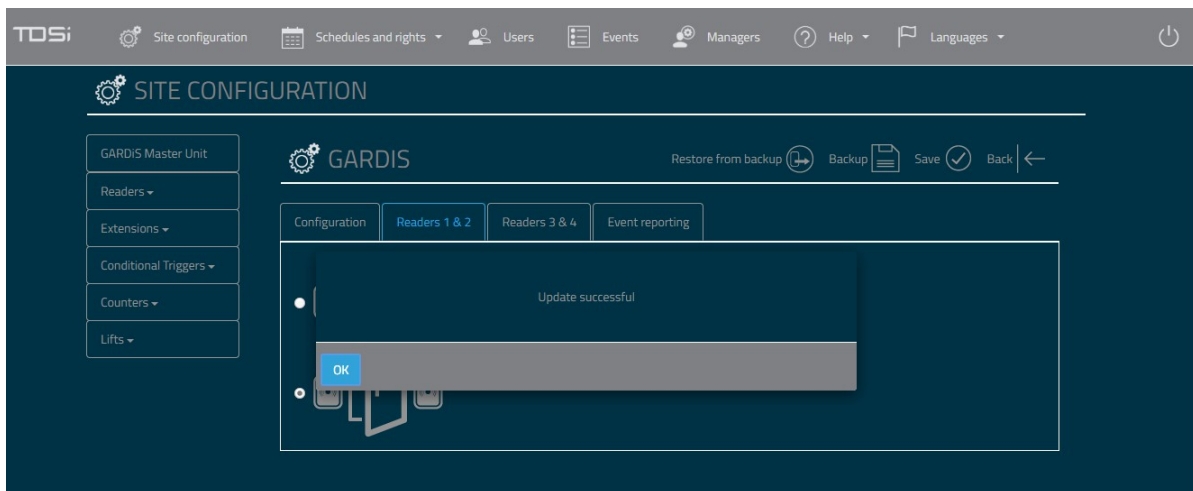
z. B. Lesegerät-Kanal 1 ist Tür 1 zugeordnet (Eingangsleser), Lesegerät-Kanal 2 ist Tür 1 zugeordnet (Ausgangsleser)

Hinweis: Um den Controller für „Reverse LRC“ zu konfigurieren, muss Option 1 ausgewählt werden. Zu den Einschränkungen bei „Reverse LRC“ gehören die Zugriffsgruppenrechte (werden vom Hauptleser geerbt) und bedingte Auslöser (es kann nur der Hauptleser ausgewählt werden).



Schritt 2

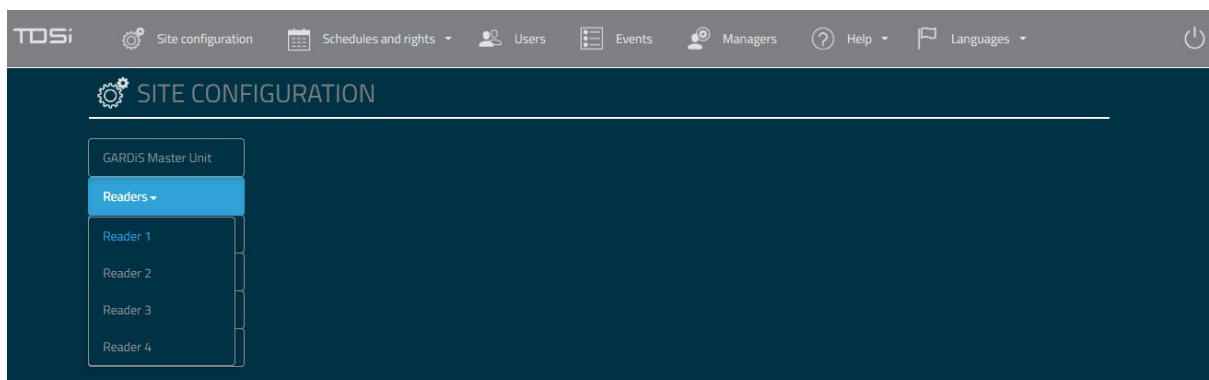
Klicken Sie auf „Speichern“.



Schritt 3

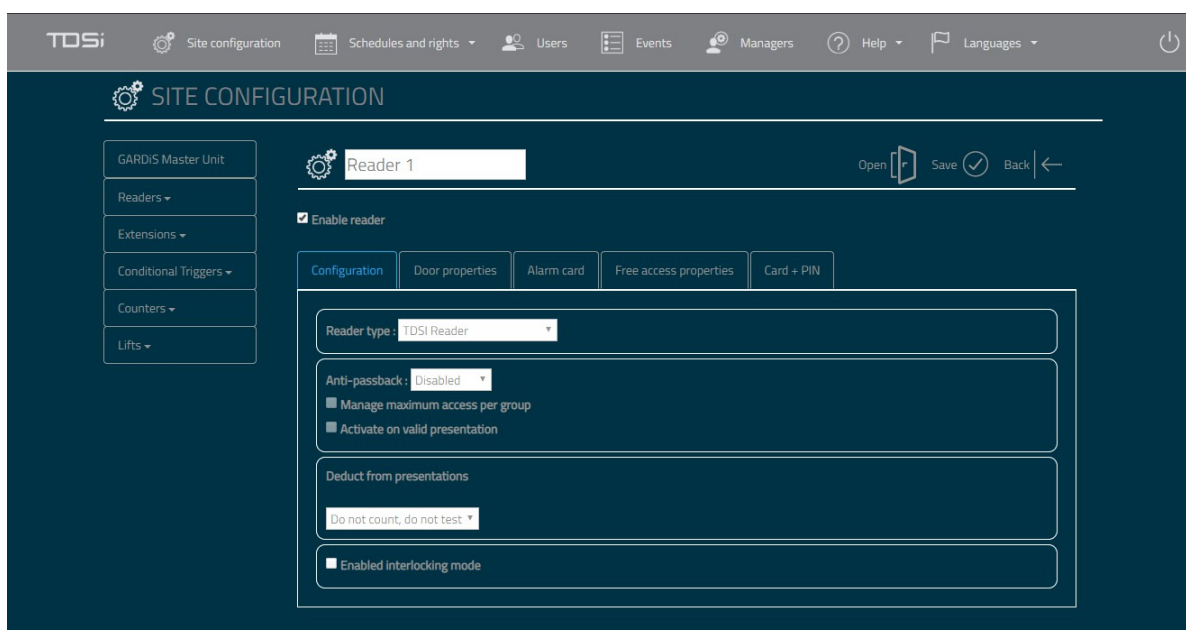
Lesegeräte konfigurieren.

Wählen Sie den zu konfigurierenden Lesegerät aus, z. B. Lesegerät 1.



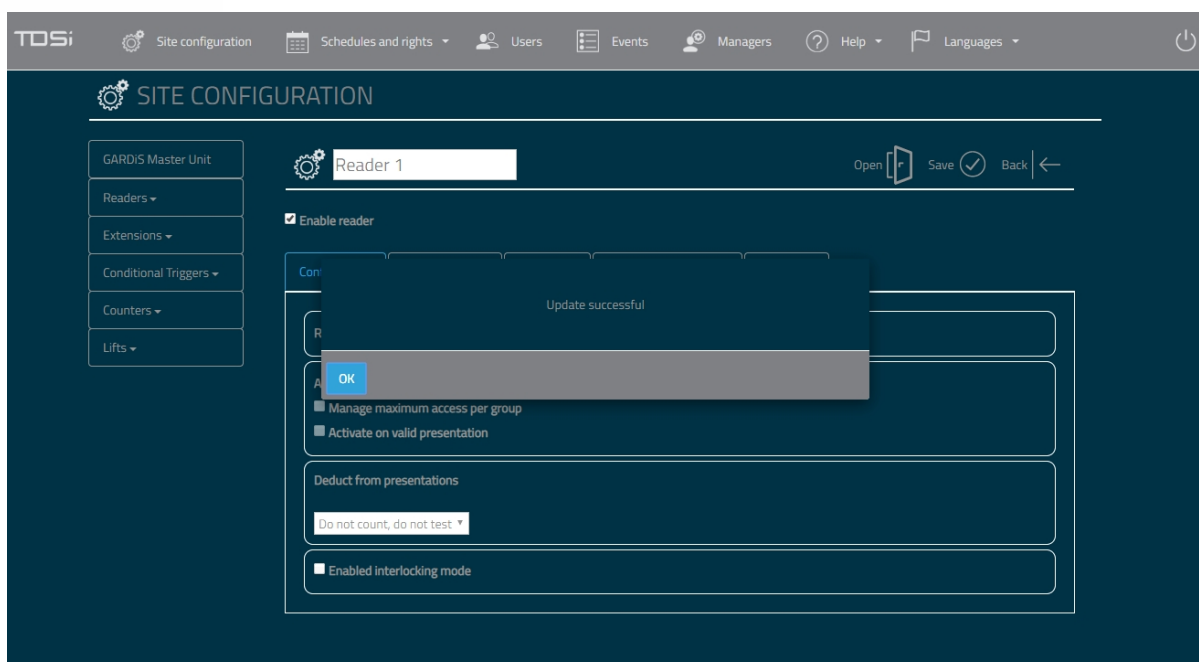
Schritt 4

Stellen Sie den Lesertyp auf „TDSi-Leser“ ein.



Schritt 5

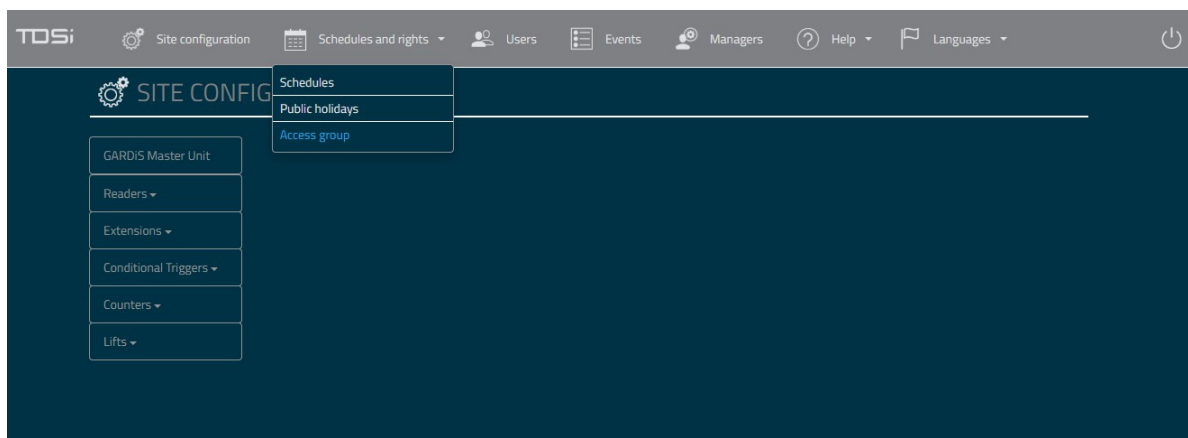
Klicken Sie auf „Speichern“.



Schritt 6

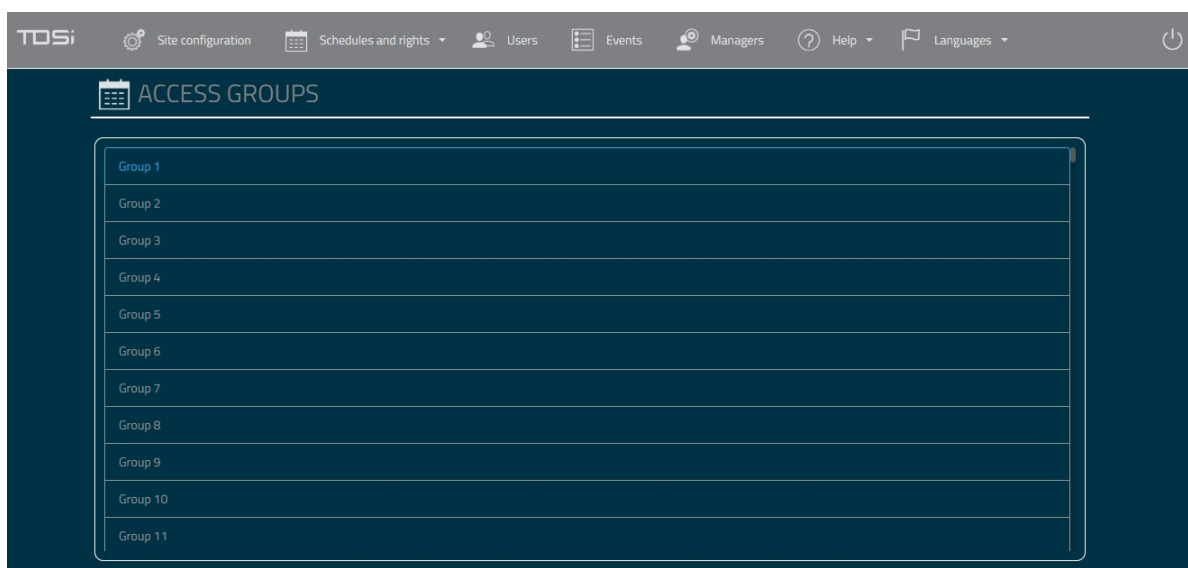
Richten Sie die Zugangsgruppen ein

Fügen Sie Lesegeräte zur gewünschten Zugangsgruppe hinzu. Hinweis: Ein Lesegerät muss mindestens einer Zugangsgruppe angehören, um Zugang zu erhalten (Zugang gewährt).



Schritt 7

Wählen Sie „Gruppe 1“ aus.



Schritt 8

Deaktivieren Sie das Kontrollkästchen „Gruppe sperren“.

The screenshot shows the 'Group 1' configuration page in the TDSi interface. The 'Properties' tab is selected. The 'Prohibit the group' checkbox is checked. The 'Use reader hold time' and 'Limited use' options are set to 'No'.

Schritt 9

Wechseln Sie zur Registerkarte „Berechtigungen“. Wählen Sie den Zeitplan pro Leser innerhalb der Zugriffsgruppe aus.

The screenshot shows the 'Group 1' configuration page in the TDSi interface. The 'Permissions' tab is selected. A dropdown menu is open for 'Reader 1', showing 'Permanent access' selected. The dropdown menu also lists 'Access forbidden' and 'Schedule 1' through 'Schedule 18'.

Schritt 10

Wählen Sie „Permanenter Zugang“, um rund um die Uhr über das Lesegerät Zugang zu erhalten.

The screenshot shows the 'Group 1' configuration page in the TDSi system. The 'Permissions' tab is active, displaying a table with four readers and their access permissions.

Readers	Permissions
Reader 1	Permanent access
Reader 2	Access forbidden
Reader 3	Access forbidden
Reader 4	Access forbidden

Schritt 11

Klicken Sie auf „Speichern“. Der erfolgreiche Abschluss wird angezeigt.

The screenshot shows the same 'Group 1' configuration page, but now with a modal dialog box overlaying the table. The dialog contains the text 'Update successful' and an 'OK' button.

Schritt 12

Halten Sie die erforderliche Karte an das Lesegerät. Klicken Sie auf den Menüpunkt „Ereignisse“. Das Ereignis „Unbekannte Kennung“ sollte in der Liste der Ereignisse angezeigt werden.

The screenshot shows the 'EVENTS' page in the TDSi system. It features a table with event data and 'Refresh' and 'Export' buttons.

Date	Description	Reader	Identifier	Last Name	First Name
18/11/2019 12:29:46	Unknown identifier	Reader 1	30589		
18/11/2019 12:23:02	ACU start-up			Code 0	

Schritt 13

Klicken Sie auf die Nummer in der Spalte „Identifikator“. Dadurch wird das Formular „Neuer Benutzer“ geöffnet, in dem Sie einen neuen Benutzer anlegen können. Die Kartennummer ist bereits vorgegeben.

TOSi
Site configuration
Schedules and rights
Users
Events
Managers
Help
Languages

NEW USER

Delete
Save
Back

Identity
Permissions
Options

Last Name:
First Name:

Identifier: 30589
Card

Presence: Undetermined
Delete

Schritt 14

Geben Sie die Daten für den neuen Benutzer ein, z. B. den Nachnamen.

TOSi
Site configuration
Schedules and rights
Users
Events
Managers
Help
Languages

NEW USER

Delete
Save
Back

Identity
Permissions
Options

Last Name: Smith
First Name: John

Identifier: 30589
Card

Presence: Undetermined
Delete

Schritt 15

Wechseln Sie zur Registerkarte „Berechtigungen“. Wählen Sie „Permanenter Zugriff“, um festzulegen, dass der Benutzer rund um die Uhr berechtigt ist.

The screenshot shows the 'NEW USER' form in the TDSi application. The 'Permissions' tab is selected. The 'Status' dropdown is set to 'Authorized'. The 'Schedule' dropdown is open, showing 'Access Group schedule' and 'Permanent access' (highlighted). The 'Validity dates' section has an 'Enable' checkbox. The 'Access groups' section shows three groups: Group 1, Group 2, and Group 3, each with a dropdown menu.

Schritt 16

Wählen Sie „Gruppe 1“ aus, um den Benutzer einer Zugriffsgruppe zuzuweisen. Hinweis: Pro Benutzer sind maximal 3 Zugriffsgruppen zulässig.

The screenshot shows the 'NEW USER' form in the TDSi application. The 'Permissions' tab is selected. The 'Status' dropdown is set to 'Authorized'. The 'Schedule' dropdown is set to 'Permanent access'. The 'Validity dates' section has an 'Enable' checkbox. The 'Access groups' section shows three groups: Group 1, Group 2, and Group 3, each with a dropdown menu. Group 1 is selected for Group 1, Group 2, and Group 3.

Schritt 17

Klicken Sie auf „Speichern“. Der Erfolg wird angezeigt.

The screenshot shows the 'NEW USER' configuration page in the TDSi interface. The 'Permissions' tab is active. A modal dialog titled 'Update successful' is centered on the screen, with an 'OK' button. The background form contains the following fields:

- Status: Authorized (dropdown)
- Schedule: Permanent access (dropdown)
- Validity dates: ☒ Enable
- Access groups:
 - Group 1: Group 1 (dropdown)
 - Group 2: Not defined (dropdown)
 - Group 3: Not defined (dropdown)

Schritt 18

Die Person befindet sich nun in der Benutzerliste.

The screenshot shows the 'USERS' management page. A search bar is at the top. Below it is a table with the following data:

Identifier	Identity	Groups	Status
30589	Smith John	Group 1	Authorized

Schritt 19

Legen Sie die Karte auf den Lesegerät.

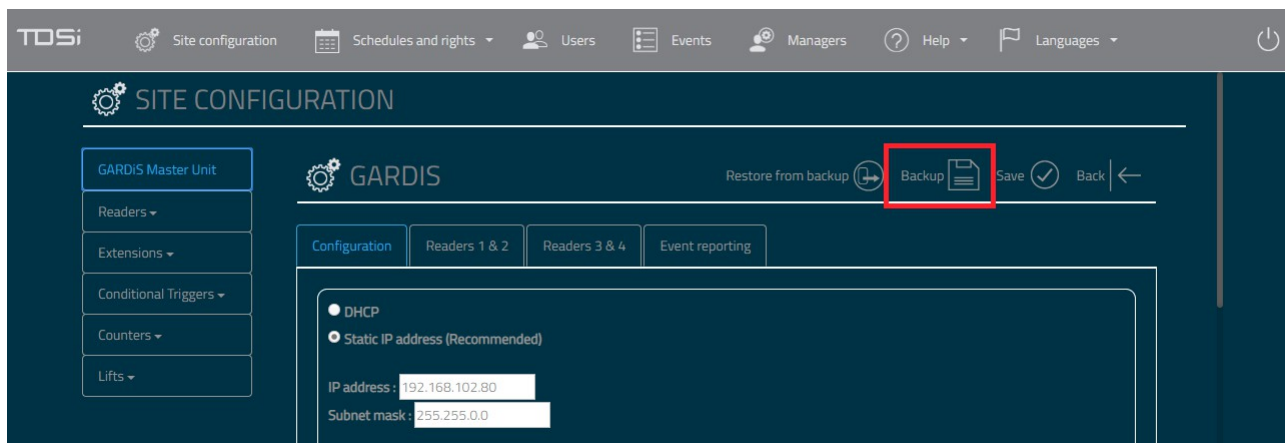
18/11/2019 13:04:40	Access Granted	Reader 1	30589	Smith	John
18/11/2019 12:29:46	Unknown identifier	Reader 1	30589		
18/11/2019 12:23:02	ACU start-up			Code 0	

Die erteilte Zugriffsberechtigung wird nun mit Angaben zur Kartennummer und zum Namen der Person angezeigt.

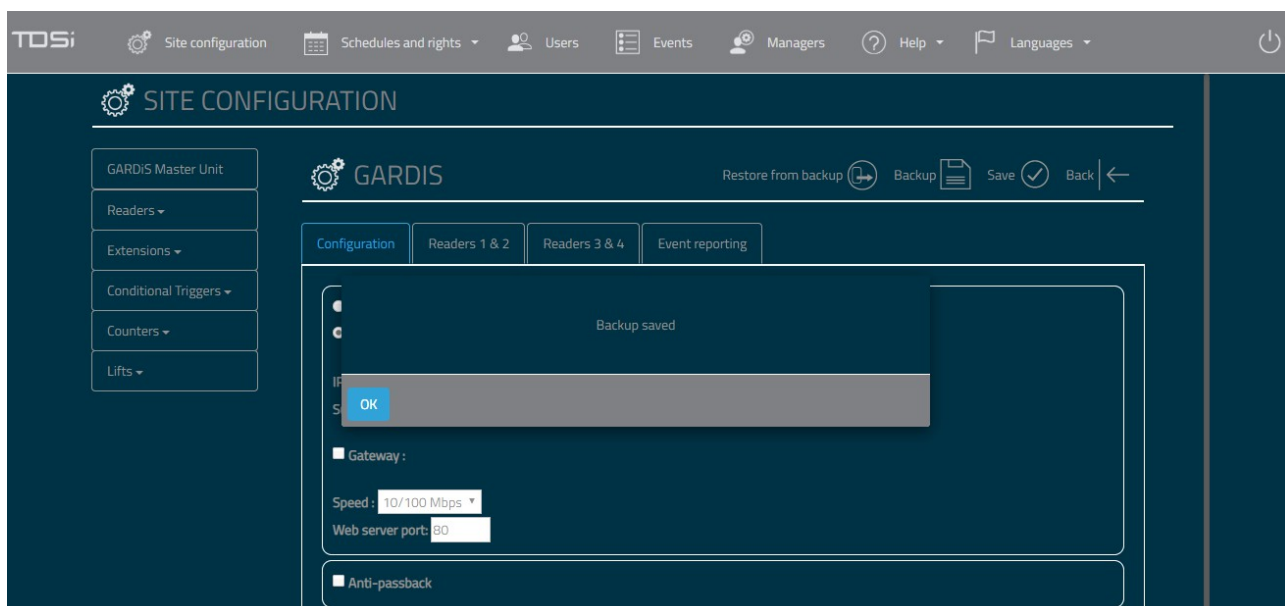
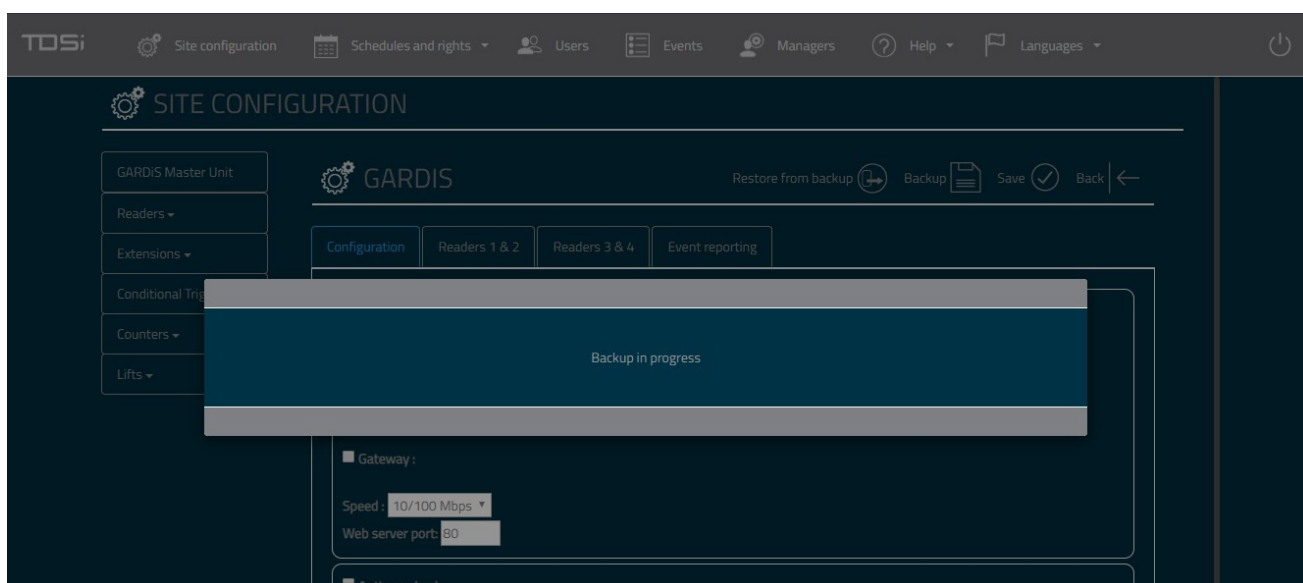
6. Sicherung

Es wird empfohlen, eine Sicherung der Datenbank in Ihrer GARDiS-Einheit durchzuführen.

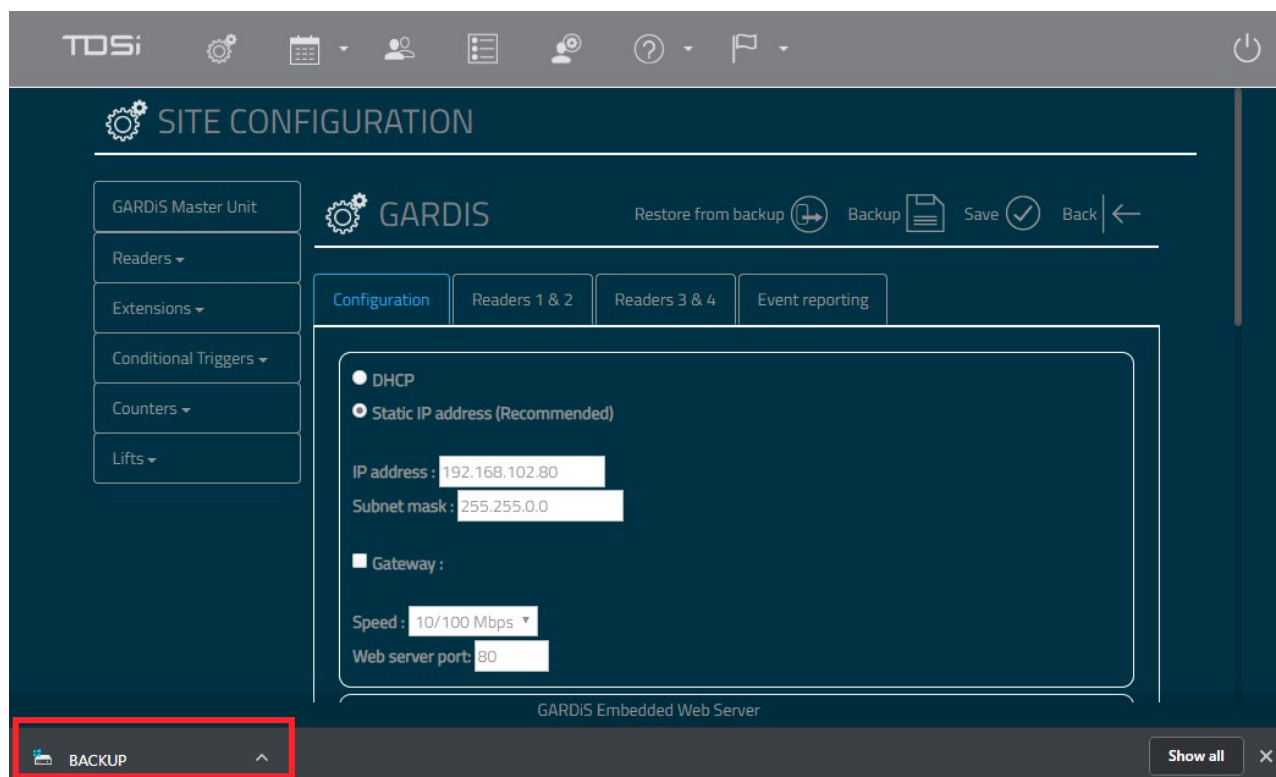
Klicken Sie im oberen Menü auf „Standortkonfiguration“ und anschließend im linken Menü auf „GARDiS-Master-Einheit“.
Klicken Sie auf „Sicherung“.



Dadurch wird der Sicherungsvorgang gestartet und nach Abschluss des Vorgangs wird eine Meldung angezeigt, dass der Vorgang abgeschlossen ist.

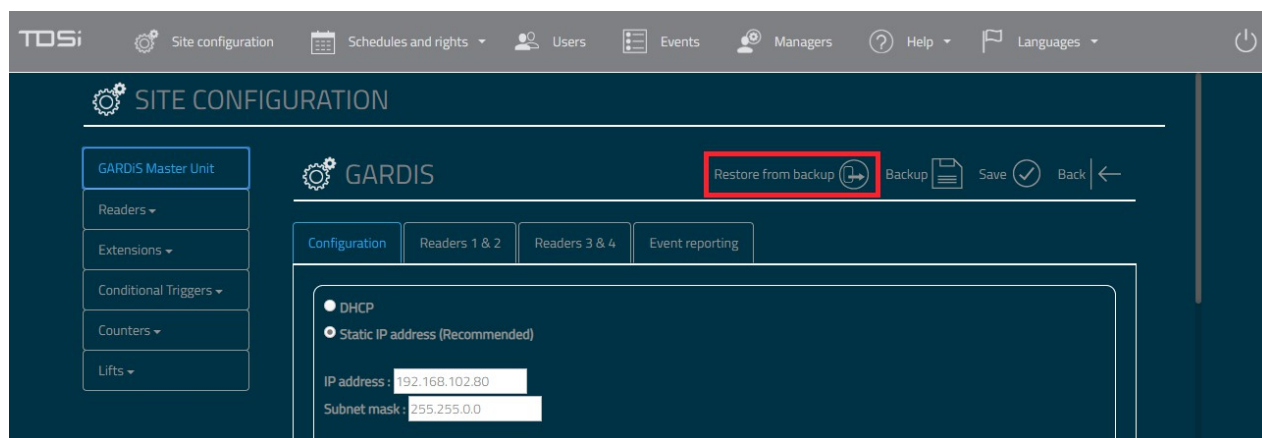


Die Sicherungsdatei wird in den Standard-Download-Ordner heruntergeladen.



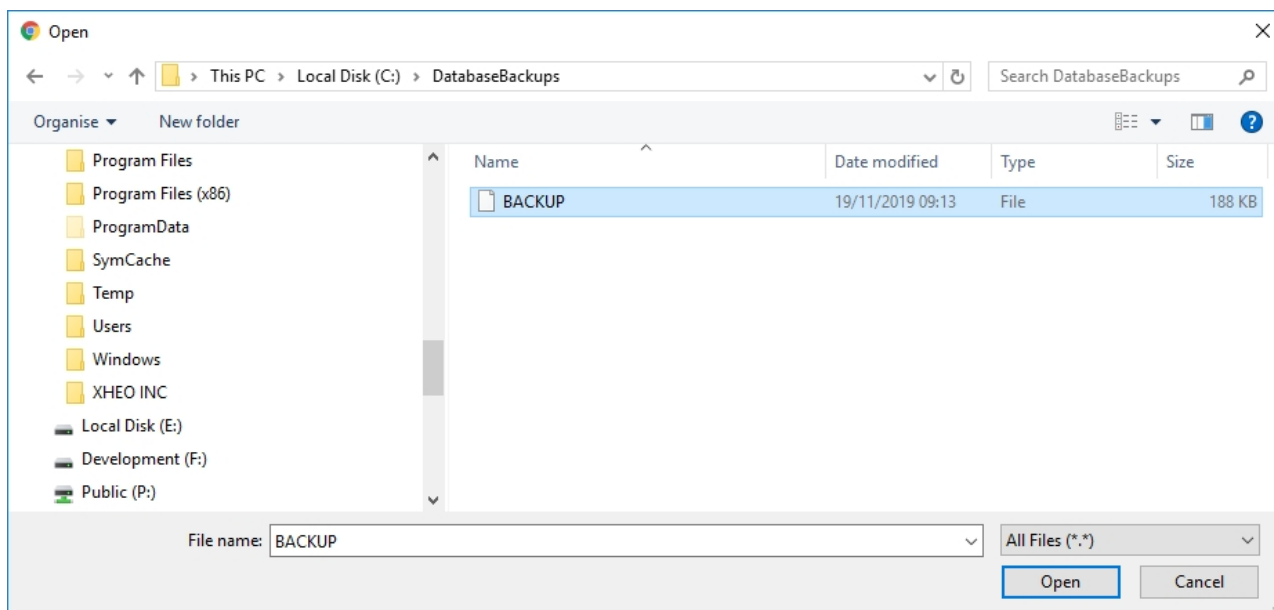
7. Aus Sicherung wiederherstellen

Um aus einer Sicherung wiederherzustellen, **klicken Sie im oberen Menü auf „Standortkonfiguration“ und anschließend im linken Menü auf „GARDIS-Master-Einheit“.**
Klicken Sie auf „Aus Sicherung wiederherstellen“.

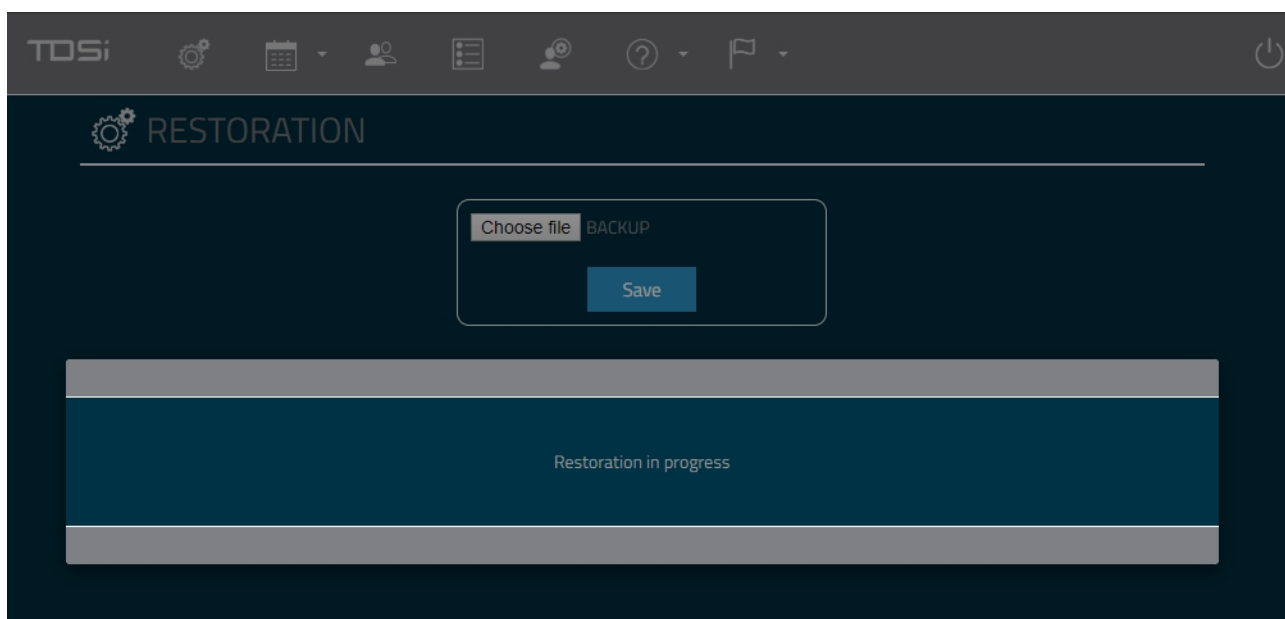


Es öffnet sich ein Datei-Explorer-Fenster. Navigieren Sie zum gewünschten Verzeichnis und wählen Sie die wiederherzustellende Sicherungsdatei aus.

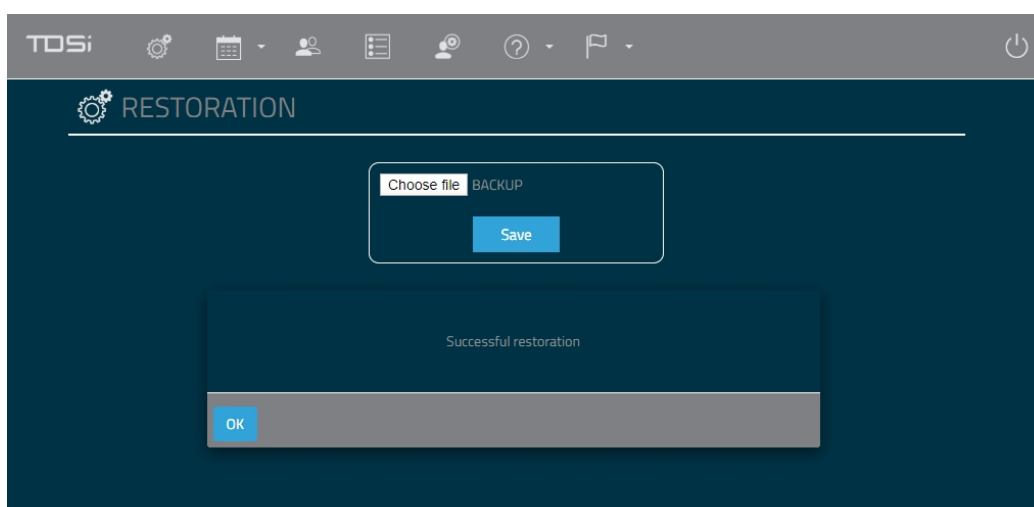
Hinweis: Die Sicherungsdatei muss den Namen „BACKUP“ tragen (umbenannte Dateien können nicht verwendet werden).



Klicken Sie nach der Auswahl auf „Öffnen“. Dadurch wird der Wiederherstellungsprozess gestartet.



Nach Abschluss des Vorgangs wird ein Meldungsfeld angezeigt.



8. Site-Konfiguration

In diesem Kapitel werden die einzelnen Eigenschaften der Controller-Einstellungen näher erläutert.

8.1 Konfiguration der

8.1.1 GARDiS-Master-Einheit „“

Allgemeine Konfiguration des Türcontrollers.

TDSi

Site configuration

Schedules and rights

Users

Events

Managers

Help

Languages

GARDiS Master Unit

Readers

Extensions

Conditional Triggers

Counters

Lifts

MASTER CONTROLLER

Restore from backup Backup Save Back

Configuration Readers 1 & 2 Readers 3 & 4 Event reporting

DHCP

Static IP address (Recommended)

IP address : 192.168.102.80

Subnet mask : 255.255.0.0

Gateway :

Speed : 10/100 Mbps

Web server port: 80

Anti-passback

Automatic time change

Clock compensation

Tamper

Interlocking management

Conditional trigger relay

Security level

Firmware update

Einstellungen für die IP-Konfiguration. Im DHCP-Modus ist es auch möglich, eine Verbindung über einen DNS-Namen herzustellen: http://gardis-xxxx, wobei xxxx für die letzten 4 Ziffern der MAC-Adresse steht.

Gateway aktivieren und einstellen

Einstellung basierend auf der Geschwindigkeit der Netzwerkverbindung

In der Einheit aktivieren/deaktivieren

Die Uhr wird bei der Umstellung auf Sommerzeit automatisch angepasst. Stellen Sie Datum und Uhrzeit im Gerät ein. Klicken Sie auf „Zeit einstellen“, um die Einstellung an das Gerät zu senden.

Wenn Sie feststellen, dass das Gerät die Zeit verliert, verwenden Sie diese Einstellung, um die Uhr automatisch anzupassen

Verkabeln Sie das Gerät wie erforderlich. Wenn diese Option aktiviert ist, stellen Sie die Polarität ein. NO (Normalerweise offen) / NC (Normalerweise geschlossen)

Mantrap-Einstellung

Basierend auf der Verdrahtung des bedingten Ausgangs

Bis zu 3 Sicherheitsstufen

Firmware-Update im Gerät.

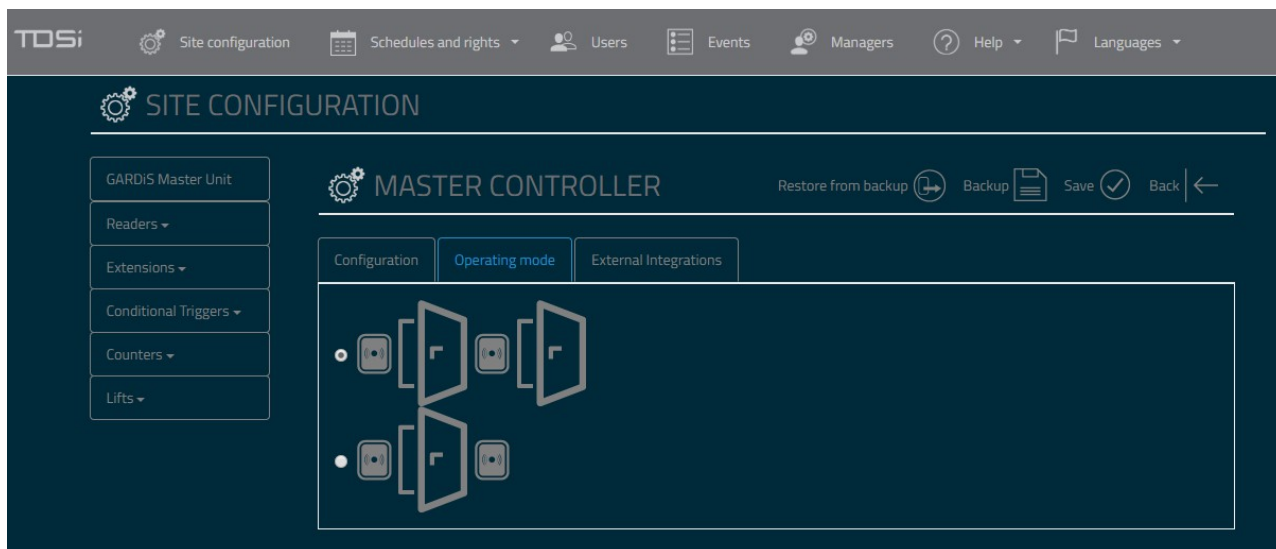
20

8.1.2 Betriebsmodus/Lesegeräte

Bei GARDiS 4 wird die unten hervorgehobene Registerkarte „Betriebsmodus“ auf zwei Registerkarten angezeigt, gruppiert nach Lesegeräten.

Wählen Sie die erste Option für einen Lesekanal pro Tür, d. h. Lesegerät 1 für Tür 1, Lesegerät 2 für Tür 2.

Wählen Sie die zweite Option für das Einlesen (Lesegerät-Kanal 1) und das Auslesen (Lesegerät-Kanal 2).



8.1.3 Externe Integrationen

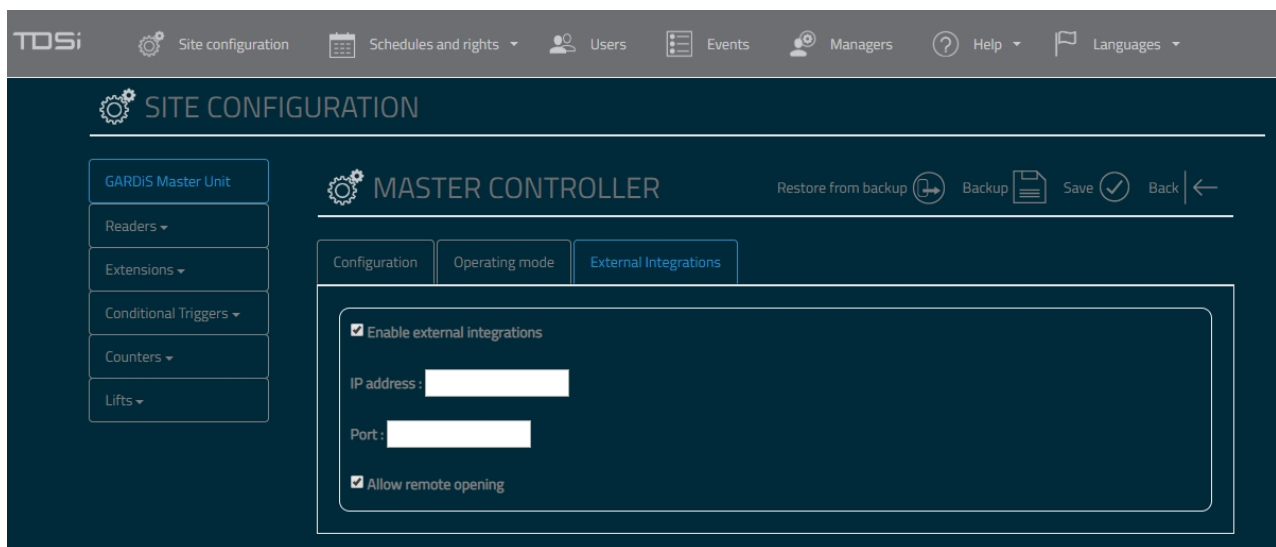
„Externe Integrationen“ ermöglicht die Anbindung von Drittanbietern an den GARDiS-Controller.

Externe Integrationen aktivieren: Wenn Sie diese Option auswählen, werden die Textfelder „IP-Adresse“ und „Port“ angezeigt. Geben Sie die Details des Endpunkts ein, an den Sie Ereignisinformationen senden möchten.

Fernöffnung zulassen: Wenn Sie diese Option aktivieren, lässt der GARDiS-Controller zu, dass eine Tür per HTTP-Anfrage geöffnet wird. Ein Beispiel für eine solche HTTP-Anfrage ist unten dargestellt, wobei der Index das zu öffnende Türrelais angibt (z. B. Tür 1) und die IP-Adresse die IP-Adresse des Geräts ist. Die Antwort enthält „OK“, wenn die Aktion ausgeführt wurde.

Das Ereignis „Öffnen durch CTM“ wird zusammen mit der der Tür zugeordneten Leser Nummer generiert.

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



8.2 Lesegeräte

Wählen Sie die gewünschte Lesegerätetechnologie aus dem Dropdown-Menü aus. Die für diese Technologie verfügbaren Konfigurationen werden automatisch auf dem Bildschirm aktualisiert.

Lesertyp: Wählen Sie die gewünschte Technologie des Lesegeräts aus. Unterstützte Lesertypen: Wiegand, Clock & Data, OSDP, SSCP. Durch Ändern des Lesertyps wird der erste Abschnitt so angepasst, dass er die für den ausgewählten Typ erforderlichen Konfigurationen enthält.

Anti-Passback: Hiermit kann der Lesegerätetyp für Anti-Passback konfiguriert werden. Standardmäßig ist diese Option auf

„Deaktiviert“. Weitere Optionen sind:

- **Eingang:** Lesegerät für den Eingang.
- **Ausgang:** Ausgangsleser.
- **Eintritt/Ausgang:** Ein- und Ausgangsleser.

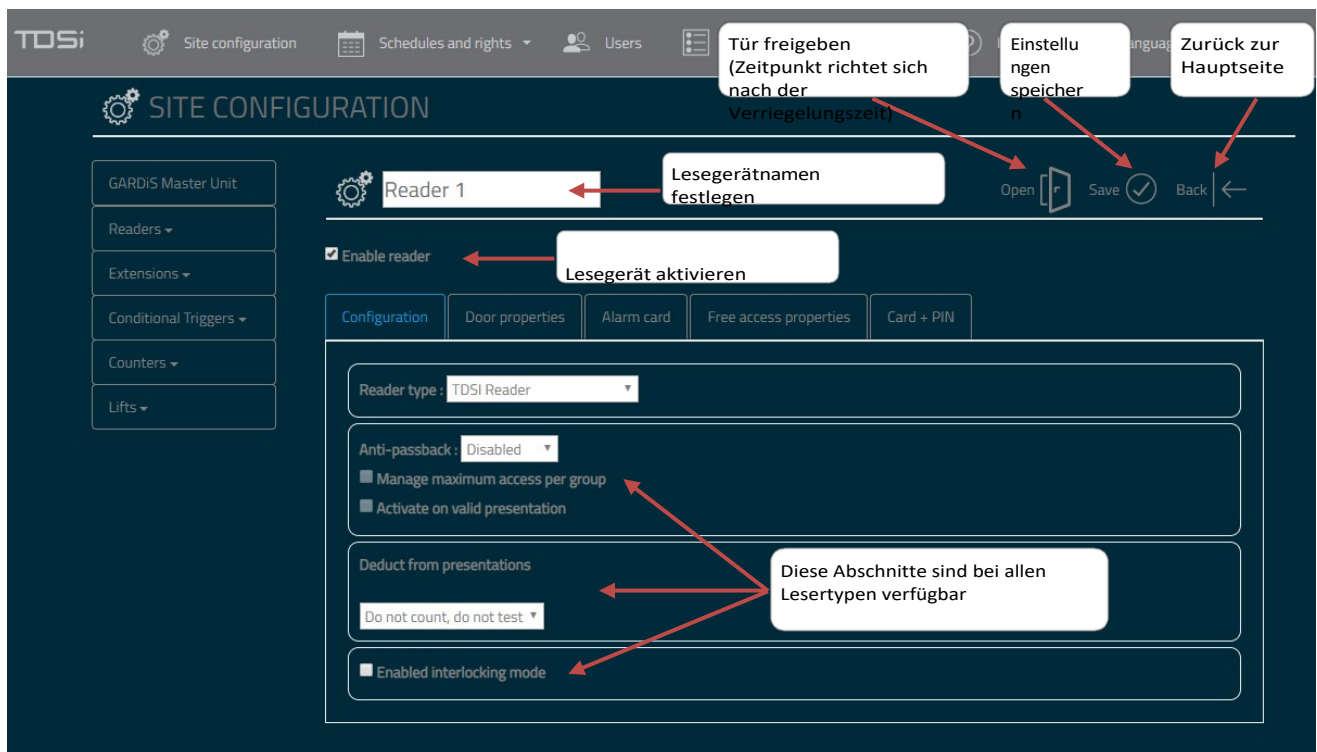
Maximale Zugriffe pro Gruppe verwalten: Ermöglicht die Begrenzung der Anzahl der Zugänge über einen Lesegerät basierend auf der Zugangsgruppe.

Bei gültiger Vorlage aktivieren: Aktivieren Sie die Anti-Passback-Funktion in Verbindung mit der Türerkennung, d. h., wenn der Benutzer einen gültigen Ausweis vorlegt und die Tür öffnet. Damit diese Funktion funktioniert, muss in den *Türeigenschaften* die Eigenschaft „Türerkennung“ konfiguriert sein. Standardmäßig ist diese auf „Deaktiviert“ gesetzt. Hinweis: Dies ändert die vom Gerät generierten Ereignisse. Wenn ein gültiges Zugangsmedium am Gerät vorgelegt wird, wird zunächst das Ereignis „Benutzer wartet auf Validierung“ generiert. Wenn der Benutzer die Tür öffnet (innerhalb der Verriegelungsverzögerung), wird anschließend das Ereignis „Zugang gewährt“ generiert.

Von den Vorhaltungen abziehen: Hiermit wird die Anzahl der Vorhaltungen erfasst, bei denen ein Zugangsmedium den Lesekopf betätigt hat. Das Zugangsmedium muss ebenfalls so konfiguriert sein, dass die Option „Anzahl der Vorhaltungen“ aktiviert und ein Anfangswert festgelegt ist. Zu den Optionen gehören:

- **Nicht zählen, nicht prüfen:** Keine Validierungsprüfungen durchführen
- **Testen:** Testen Sie, wie oft der Ausweis am Lesegerät verwendet wurde, ohne zu zählen. Sperren Sie den Benutzer, wenn die Anzahl 0 beträgt. Wenn das Limit erreicht ist, wird das Ereignis „Zugriffslimit erreicht“ generiert.
- **Testen und zählen:** Testen Sie, wie oft ein Zugangsmedium am Lesegerät verwendet wurde, und ziehen Sie die Anzahl von der Gesamtzahl ab. Sperren Sie das Zugangsmedium, wenn die Anzahl der Zugriffe 0 beträgt. Bei dieser Option wird ein neues Ereignis namens „Zugriffszahl“ generiert. Das Ereignis enthält die Anzahl der verbleibenden Zugriffe für dieses Zugangsmedium. Wenn das Limit erreicht ist, wird das Ereignis „Zugriffslimit erreicht“ generiert.
- **Täglicher Zählstand:** Pro Tag wird maximal 1 vom Zählstand abgezogen. Der Ausweis kann an einem Tag beliebig oft am Lesegerät vorgelegt werden, wobei jeweils nur 1 vom Zählstand abgezogen wird.

Verriegelungsmodus aktivieren: Man-Trap aktivieren.



8.2.1 Lesegeräte mit Tastatur

Wenn Sie ein Lesegerät mit Tastatur verwenden, wählen Sie im Dropdown-Menü „**Lesegerätetyp**“ die Option „**Lesegerät mit Tastatur**“ aus. Es wird ein neuer Abschnitt angezeigt, in dem Sie weitere Einstellungen vornehmen können.

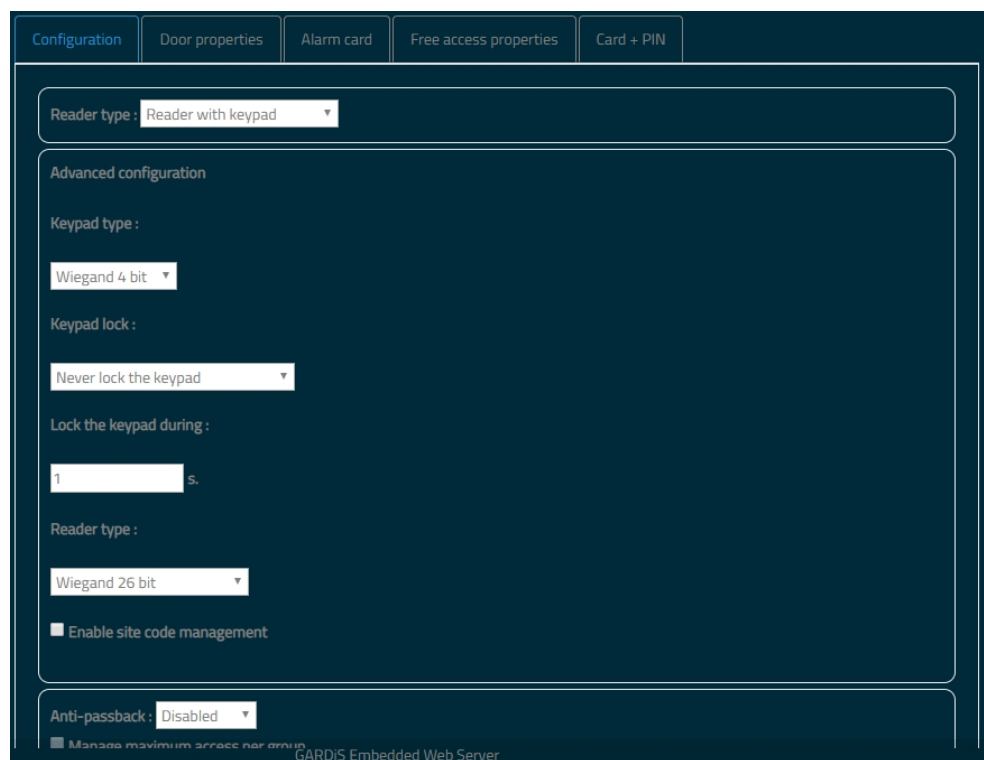
Tastaturtyp: Wählen Sie den gewünschten Ausgabebetyp aus. Verfügbare Optionen: – Wiegand 4 Bit (jeder Tastendruck wird als 4-Bit-Datenwert ausgegeben) oder Wiegand 26 Bit (mehrere Tastendrucke werden als ein 26-Bit-Datenwert ausgegeben). Stellen Sie für TDSi-Tastaturler die Option „Wiegand 4 Bit“ ein.

Tastatursperre: Legen Sie fest, ob die Tastatur nach einer bestimmten Anzahl falscher PIN-Eingaben (maximal 10) gesperrt werden soll. Diese Option ist standardmäßig auf „Tastatur niemals sperren“ eingestellt.

Tastatur sperren für: Legen Sie die Anzahl der Sekunden fest, für die die Tastatur gesperrt werden soll, wenn die Option „Tastatur sperren“ aktiviert ist. Maximaler Wert: 255, minimaler Wert: 1.

Lesertyp: Legen Sie den Wiegand-Ausgangstyp fest. Je nach ausgewählter Wiegand-Option stehen zusätzliche Optionen zur Verfügung, z. B. die Standortcode-Verwaltung. Stellen Sie für TDSi-Lesegeräte „Wiegand 26 Bit“ ein.

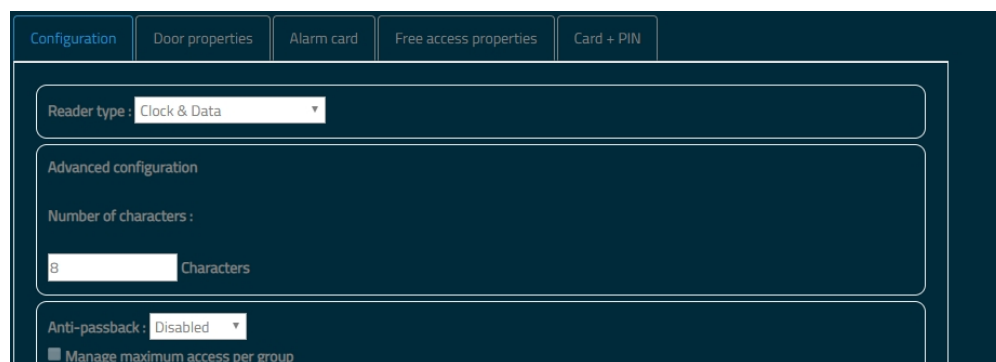
Nachfolgend finden Sie eine typische Konfiguration für TDSi-Lesegeräte mit Tastatur.



The screenshot shows the 'Configuration' tab of the TDSi web interface. The 'Reader type' is set to 'Reader with keypad'. Under 'Advanced configuration', the 'Keypad type' is 'Wiegand 4 bit', 'Keypad lock' is 'Never lock the keypad', and 'Lock the keypad during' is set to '1 s.'. The 'Reader type' is set to 'Wiegand 26 bit', and 'Enable site code management' is checked. At the bottom, 'Anti-passback' is 'Disabled' and 'Manage maximum access per group' is checked. The footer indicates 'GARDiS Embedded Web Server'.

8.2.2 Takt & Daten

Bei der Einstellung des Lesers auf „Takt & Daten“ kann die Anzahl der Zeichen festgelegt werden. Maximalwert 13. Minimalwert 1. Dabei wird die niedrigstwertige Ziffer (LSD) übernommen. Wenn beispielsweise ein Ausgang auf 8 Ziffern eingestellt war und Folgendes gemeldet wurde: 85476456. Würde der Ausgang dann auf 4 eingestellt, würde das Gerät die Zahl 6456 übernehmen.



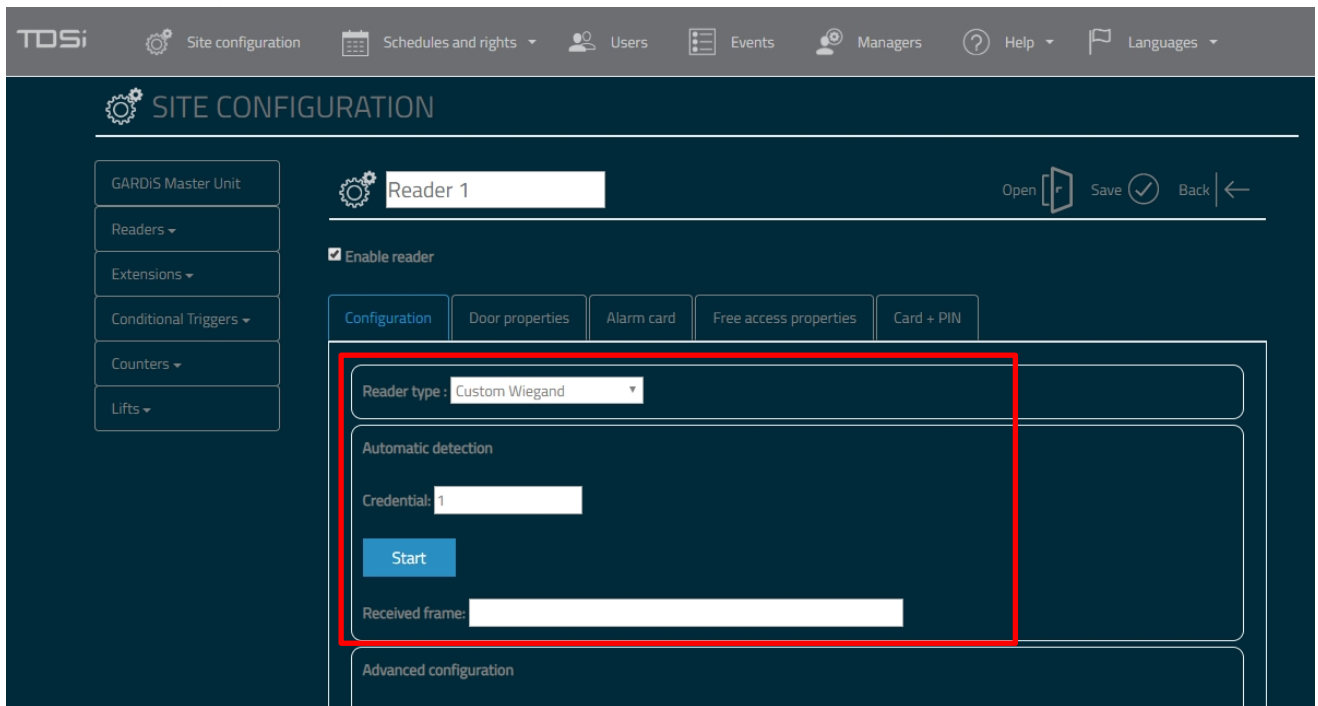
The screenshot shows the 'Configuration' tab of the TDSi web interface. The 'Reader type' is set to 'Clock & Data'. Under 'Advanced configuration', the 'Number of characters' is set to '8 Characters'. At the bottom, 'Anti-passback' is 'Disabled' and 'Manage maximum access per group' is checked.

8.2.3 Benutzerdefiniertes Wiegand

Wählen Sie „Benutzerdefiniertes Wiegand“ aus dem Dropdown-Menü aus.

Das Wiegand-Format wird automatisch erkannt. Stellen Sie sicher, dass das erforderliche Lesegerät an den Lesekanal angeschlossen ist. Geben Sie die Kartennummer in das Feld „Ausweisdaten“ ein. Klicken Sie auf „**Start**“ und halten Sie die Karte an das Lesegerät. Im Feld „Empfangene Frame-Daten“ werden die vom Gerät empfangenen Wiegand-Daten angezeigt.

Klicken Sie auf „**Speichern**“, um das Wiegand-Format auf den Controller zu programmieren.



8.2.4 Türeigenschaften

Auf dieser Registerkarte können Sie die Eigenschaften der Türausstattung konfigurieren.

Modus „Schließbolzen aus“

Befehl „Tür offen“ beenden: Hiermit wird der Türöffner ausgeschaltet, wenn die Tür geöffnet wird. Um diese Funktion zu nutzen, müssen Sie die Eigenschaft „Türerkennung“ einstellen.

Verzögerung für Zugangsgruppen zulassen: Damit können Zugangsgruppen ihre eigene definierte Verriegelungszeit verwenden. **Verriegelungszeit:** Anzahl der Sekunden, nach denen das Verriegelungsrelais freigegeben wird. Bei der Einstellung 0 wird das Relais umgeschaltet. Maximalwert 255.

LED-Ausgabe: Optionen zur Steuerung des Verhaltens der Lesegerät-LED.

- **Auslösung durch Türfreigabe:** Wenn das Türrelais aktiviert wird, Erfolg anzeigen.
- **Auslösung durch Türsensor:** Wenn die Tür geöffnet wird, Erfolg anzeigen.
- **Auslösung durch Türerkennung und Verriegelungsstatus:** Diese Option kann in Verbindung mit dem Befehl „Tür offen – Ende“ verwendet werden.

Bedingter Eingang: Dieser ist mit dem am Gerät verfügbaren bedingten I/P-Anschluss verknüpft. Standardmäßig ist dieser auf „Deaktiviert“ eingestellt. Verfügbare Optionen:

Fahrzeugerkennung NO

Fahrzeugerkennung NC

Einbruchalarm NO

Einbruchalarm NC

Glasbruchüberwachung NO

Glasbruchüberwachung NC

Ausstiegsanforderung: Dies ist mit dem Anschluss für die Ausstiegstaste am Gerät verknüpft. Standardmäßig ist diese Funktion auf „Deaktiviert“ eingestellt. Stellen Sie die gewünschte Polarität ein, d. h. „Normalerweise offen“ (NO) oder „Normalerweise geschlossen“ (NC).

Betriebszeitpläne: Die Taste „Ausgang anfordern“ kann so konfiguriert werden, dass sie nur während eines Zeitplans aktiviert ist. Standardmäßig ist sie auf „Immer aktiviert“ eingestellt.

Türsensor: Diese Einstellung ist mit dem Türsensoranschluss am Gerät verknüpft. Standardmäßig ist diese Option auf „Deaktiviert“ eingestellt. Stellen Sie die gewünschte Polarität ein, d. h. „Normalerweise offen“ (NO) oder „Normalerweise geschlossen“ (NC).

Verzögerung bei verriegelter Tür:

 SITE CONFIGURATION Reader 1

Open  Save  Back 

☒ Enable reader

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

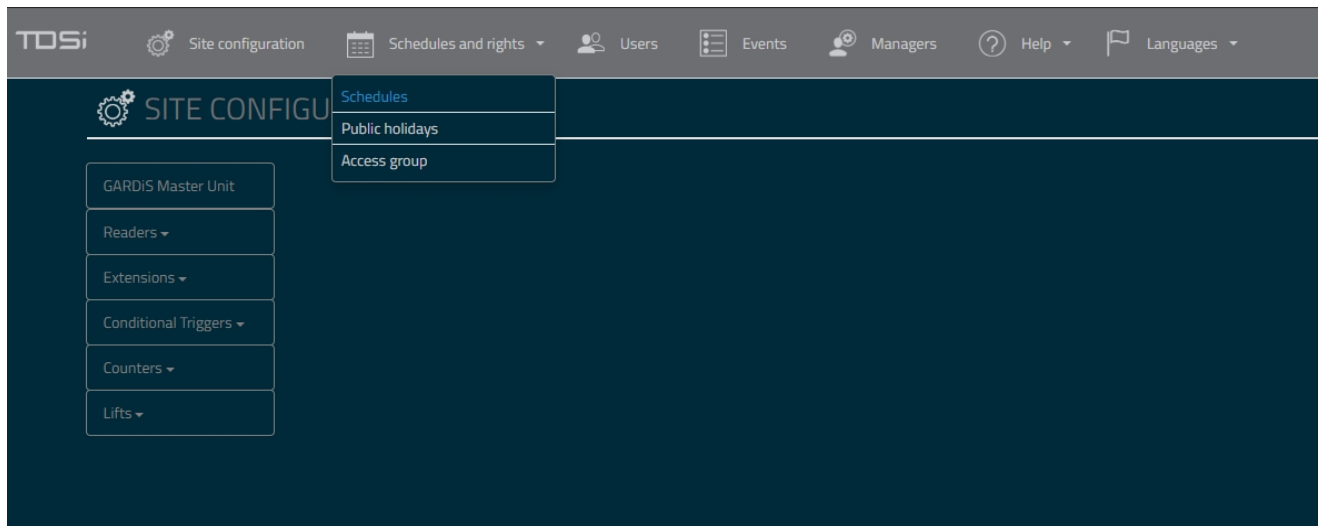
0 min

9. Zeitpläne

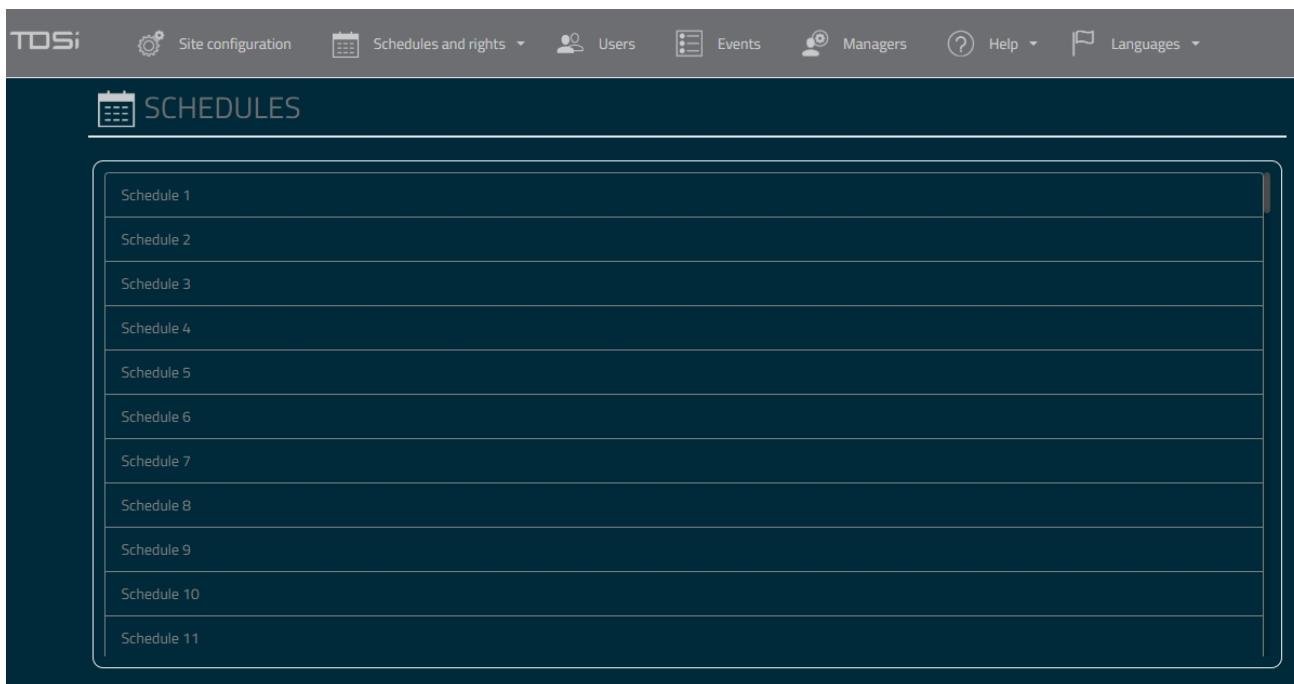
Mit dem GARDiS-Controller kann der Endbenutzer bis zu 128 Zeitpläne erstellen.

9.1 Zeitplan erstellen

Um einen Zeitplan einzurichten, klicken Sie in der oberen Menüleiste auf „**Zeitpläne und Rechte**“ und anschließend auf „**Zeitpläne**“.



Wählen Sie den ersten verfügbaren Zeitplan in der Liste aus. In diesem Beispiel wird **Zeitplan 1** verwendet.



Für den Zeitplan kann ein neuer Name festgelegt werden. Pro Tag können bis zu 10 Zeitplanperioden definiert werden.

Wählen Sie den Wiederholungszeitraum aus. Dies ermöglicht eine einfache Konfiguration für wiederkehrende Zeitpläne. Dadurch wird auch die angezeigte Tabelle aktualisiert.

- **Täglich** – Ermöglicht eine individuelle Konfiguration pro Tag.
- **Montag bis Freitag / Wochenende** – Legen Sie Zeiträume fest, die von Montag bis Freitag wiederholt werden sollen, sowie eine separate Zeitraumbestimmung für das Wochenende und eine separate Zeitraumbestimmung für Feiertage.
- **Montag bis Sonntag** – Definieren Sie Zeiträume, die von Montag bis Sonntag wiederholt werden sollen, sowie eine separate Zeitraumbestimmung für Feiertage.
- **Montag bis Samstag / Sonntag** – Legen Sie Zeiträume fest, die von Montag bis Samstag wiederholt werden sollen, sowie eine separate Zeitraumbestimmung für Sonntage und eine separate Zeitraumbestimmung für Feiertage.

Ein Beispiel für **den täglichen Ablauf** ist unten dargestellt.

Ein Beispiel für **Montag bis Freitag / Wochenende** ist unten dargestellt.

The screenshot shows the 'Schedules and rights' section of the TDSi UK application. The main heading is 'Schedule 1'. Below it, there's a 'Display:' dropdown menu set to 'Monday to Friday / Weekend'. The interface is organized into a grid with 10 columns labeled 'Period 1' through 'Period 10'. There are three rows: 'Monday to Friday', 'Saturday and Sunday', and 'Public holidays'. Each cell in the grid contains a text input field. The 'Monday to Friday' row has 10 empty input fields. The 'Saturday and Sunday' row has 10 empty input fields. The 'Public holidays' row has 10 empty input fields. At the top right, there are buttons for 'Delete', 'Save', and 'Back'.

Ein Beispiel für **Montag bis Sonntag** ist unten dargestellt.

This screenshot shows the same 'Schedules and rights' interface, but the 'Display:' dropdown is now set to 'Monday to Sunday'. The grid structure remains the same with 10 periods and 3 rows. In the 'Monday to Sunday' row, the first input field (Period 1) contains the text '00:00-23:59'. The 'Public holidays' row also has its first input field filled with '00:00-00:00'. The other input fields are empty.

Ein Beispiel für **Montag bis Samstag / Sonntag** ist unten dargestellt.

This screenshot shows the 'Schedules and rights' interface with the 'Display:' dropdown set to 'Monday to Saturday / Sunday'. The grid has 10 periods and 3 rows. The 'Monday to Saturday' row has its first input field filled with '00:00-23:59'. The 'Sunday' row also has its first input field filled with '00:00-23:59'. The 'Public holidays' row has its first input field filled with '00:00-00:00'. All other input fields are empty.

Geben Sie einen Namen für den Zeitplan ein und wählen Sie den gewünschten Wiederholungszeitraum aus. Klicken Sie in das Textfeld für den ersten Zeitraum.

Cleaner

Geben Sie hier den Namen ein.

Delete Save Back

Display: Monday to Friday / Weekend

Wählen Sie den Zeitabschnitt aus

Period 1 Period 2 Period 3 Period 4 Period 5 Period 6 Period 7 Period 8 Period 9 Period 10

Monday to Friday

Saturday and Sunday

Public holidays

Es wird ein neues Fenster angezeigt. Hier können Sie eine Start- und Endzeit eingeben. Im folgenden Beispiel wird ein Zeitfenster von 4:00 Uhr bis 6:00 Uhr festgelegt. Geben Sie die gewünschten Werte in die Felder ein (Stunden und Minuten im 24-Stunden-Format) und klicken Sie auf „**Speichern**“.

Edit period

Delete Save Cancel

From 04:00 To 06:00

HINWEIS: Um einen Zeitplan für den gesamten Tag (rund um die Uhr) festzulegen, geben Sie 00:00 bis 00:00 ein.

Dadurch werden die Werte in das Textfeld „Zeitraum 1“ übernommen. Fahren Sie fort, um weitere Zeiträume einzugeben. Im folgenden Beispiel ist der Zugang unter der Woche von 4:00 bis 6:00 Uhr und von 18:00 bis 20:00 Uhr erlaubt. An Wochenenden ist der Zugang von 12:00 bis 16:00 Uhr erlaubt. An Feiertagen ist kein Zugang erlaubt. Klicken Sie nach Abschluss auf „**Speichern**“. Dieser Zeitplan steht nun für Objekte wie Zugangsgruppen zur Verfügung.

TDSi Site configuration Schedules and rights Users Events Managers Help Languages

Cleaner

Delete Save Back

Display: Monday to Friday / Weekend

Period 1 Period 2 Period 3 Period 4 Period 5 Period 6 Period 7 Period 8 Period 9 Period 10

Monday to Friday 04:00-06:00 18:00-20:00

Saturday and Sunday 12:00-16:00

Public holidays

9.2 Zuweisen eines Zeitplans zu einer Zugangsgruppe

Um einer Zugangsgruppe einen Zeitplan zuzuweisen, klicken Sie auf „**Zeitpläne und Rechte**“ und anschließend auf „**Zugangsgruppen**“. Konfigurieren Sie die Zugangsgruppe nach Bedarf, d. h. legen Sie den Namen fest usw. Klicken Sie auf die Registerkarte „**Berechtigungen**“ und wählen Sie für jeden Leser den gewünschten Zeitplan aus dem Dropdown-Menü „**Berechtigungen**“ aus.

TDSi

Site configuration

Schedules and rights

Users

Events

Managers

Help

Languages

Cleaners

Save Back

Properties

Permissions

Readers	Permissions	Lifts
Reader 1	Access forbidden	None
Reader 2	Access forbidden	None
	Permanent access	
	Cleaner	
	Schedule 2	
	Schedule 3	
	Schedule 4	
	Schedule 5	
	Schedule 6	
	Schedule 7	
	Schedule 8	
	Schedule 9	
	Schedule 10	
	Schedule 11	
	Schedule 12	
	Schedule 13	
	Schedule 14	
	Schedule 15	
	Schedule 16	
	Schedule 17	
	Schedule 18	

Dadurch wird der ausgewählte Zeitplan in der Dropdown-Liste festgelegt.

10. Benutzer

In diesem Abschnitt können Zugangsdaten zum Controller hinzugefügt werden. Rufen Sie diesen Abschnitt auf, indem Sie im oberen Menü auf „Benutzer“ klicken. Es wird eine Liste der vorhandenen Zugangsdaten angezeigt.

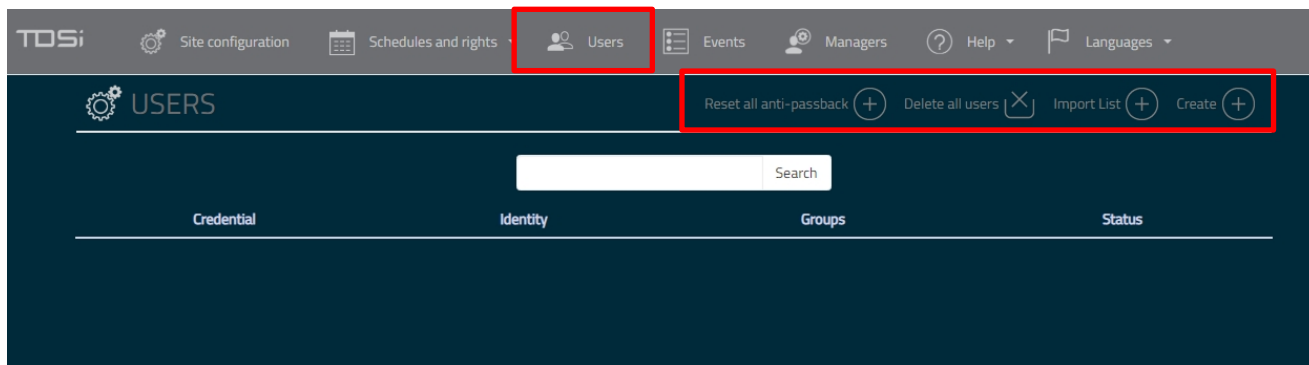
In diesem Abschnitt verfügbare Aktionen:

Alle Anti-Passback-Einstellungen zurücksetzen: Setzt alle Anti-Passback-Einstellungen für Zugangsdaten zurück. Dadurch erhalten alle Zugangsdaten Zugriff auf das Lesegerät, sofern Anti-Passback zuvor aktiviert war.

Alle Benutzer löschen: Löscht alle Zugangsdaten im Gerät. Hierfür ist eine zusätzliche Bestätigung erforderlich.

Liste importieren: Importieren Sie Zugangsdaten aus einer Datei.

Erstellen: Fügen Sie dem Gerät eine neue Zugangsberechtigung hinzu.



10.1 Neuen Benutzer anlegen

Um einen neuen Benutzer/eine neue Zugangsberechtigung im Gerät anzulegen, klicken Sie im Abschnitt „Benutzer“ auf „Anlegen“. Die Benutzereigenschaften sind in drei Abschnitte unterteilt: „Identität“, „Berechtigungen“ und „Optionen“.

10.1.1 Registerkarte „Identität“

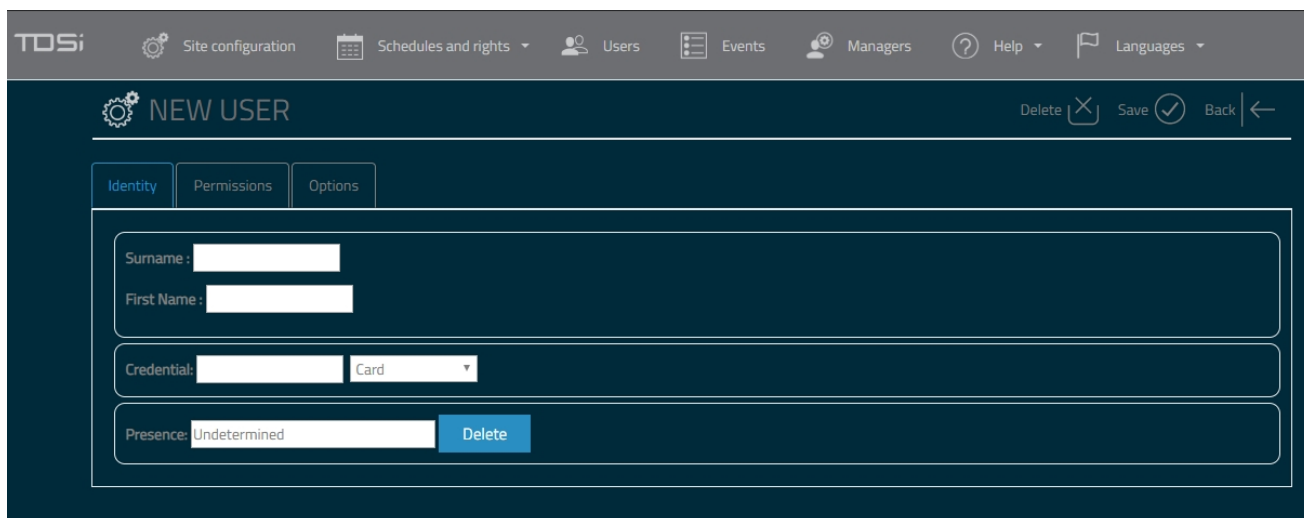
Nachname: Nachname der Person

Vorname: Vorname der Person

Zugangsdaten: Nummer der Zugangsdaten. Wählen Sie den Typ aus der Dropdown-Liste aus. Verfügbare Optionen:

- Karte
- Kartenantrag
- RF-Schlüsselanhänger
- Tastatur

Anwesenheit: Datum und Uhrzeit des Zutritts. Diese Daten werden vom System automatisch ausgefüllt, wenn die Anti-Passback-Funktion aktiviert ist. Verwenden Sie die Schaltfläche „Löschen“, um die Anti-Passback-Einstellung einer Person zurückzusetzen. Hinweis: Klicken Sie auf „Speichern“, um diese Option zu aktualisieren. „Unbestimmt“ ist die Standardanzeige.



10.1.2 Registerkarte „Berechtigungen“

Auf dieser Registerkarte können die Zugriffsberechtigungen für einen Ausweis definiert werden. Hinweis: Pro Ausweis können bis zu **3 Zugangsgruppen** definiert werden.

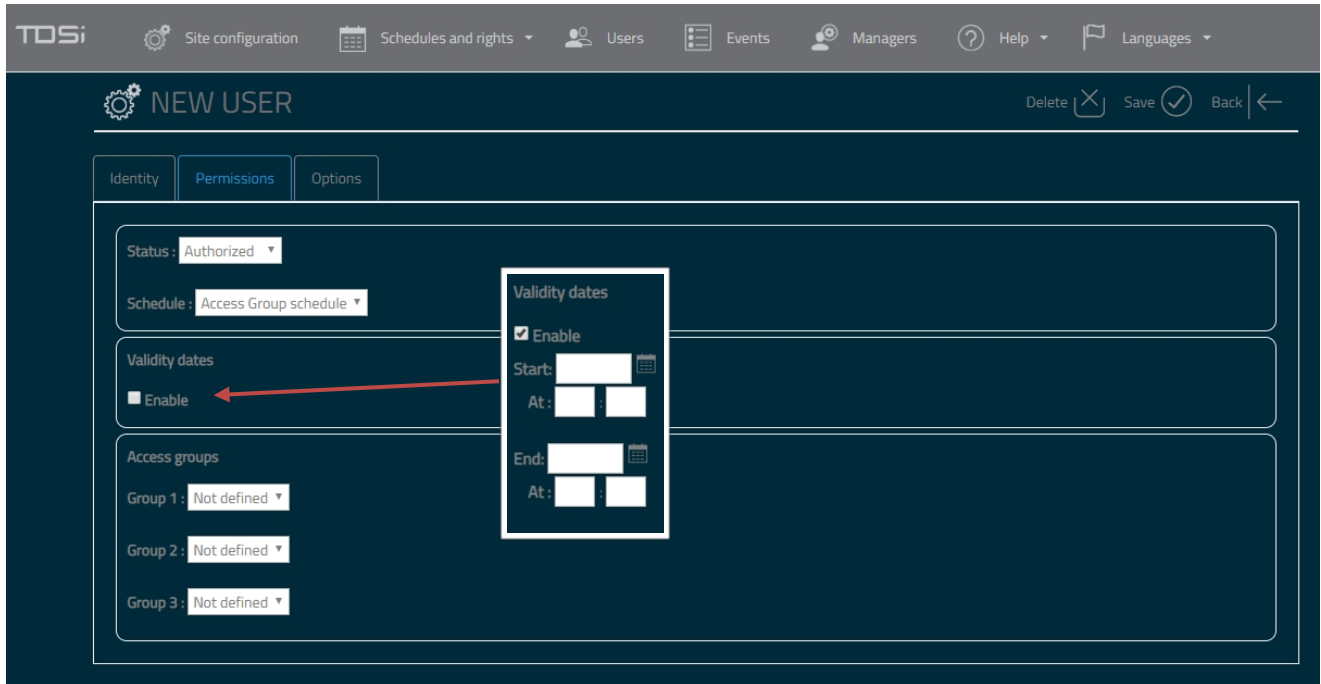
Status: Legen Sie ganz einfach fest, ob ein Zugangsmedium autorisiert oder nicht zugelassen ist.

Zeitplan: Legen Sie fest, dass die Anmeldedaten einem Zeitplan folgen sollen. Zu den Optionen gehören:

- **Zeitplan der Zugangsgruppe** (Standardoption). Der Zeitplan der Zugangsgruppen wird befolgt.
- **Permanenter Zugang.** Ermöglicht den Zugang über die Lesegeräte, ohne einem Zeitplan zu folgen.
- **Wählen Sie einen Zeitplan** aus dem System aus, den das Zugangsmedium verwendet.

Gültigkeitsdaten: Aktivieren Sie die Option, um Start- und Enddatum sowie -uhrzeit anzuzeigen. Dadurch wird der Ausweis während des festgelegten Zeitraums als gültig anerkannt.

Zugriffsgruppen: Wählen Sie bis zu 3 Zugriffsgruppen pro Zugangsberechtigung aus.



The screenshot shows the 'NEW USER' configuration page in the TDSi system. The 'Permissions' tab is selected. In the 'Validity dates' section, the 'Enable' checkbox is checked, and a red box highlights this section with a red arrow pointing to it. The 'Access groups' section below shows three groups, all set to 'Not defined'.

10.1.3 Registerkarte „Optionen“

Auf dieser Registerkarte können zusätzliche Eigenschaften festgelegt werden.

Eindringlingsverwaltung: Legen Sie fest, dass der Zugangsnachweis als Eindringlingsbenutzer gilt.

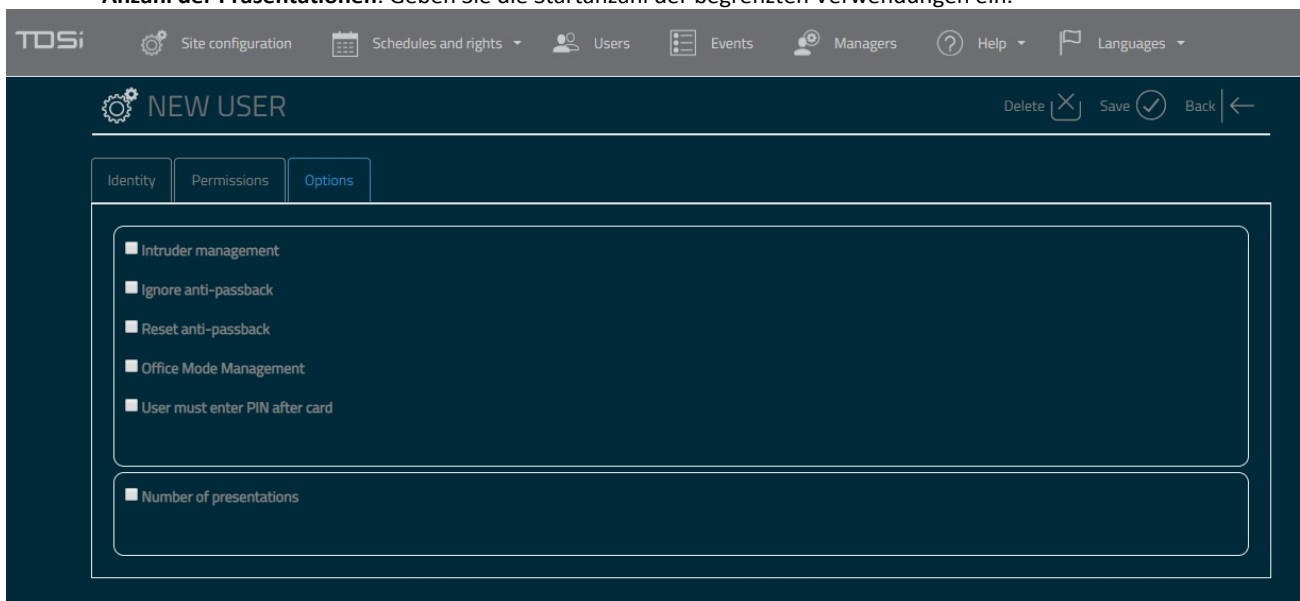
Anti-Passback ignorieren: Die Anmeldedaten werden nicht auf Anti-Passback geprüft.

Anti-Passback zurücksetzen: Setzen Sie den Anti-Passback-Schutz zurück.

Verwaltung des Office-Modus: Erlauben Sie der Berechtigung die Nutzung des Office-Modus.

Benutzer muss nach der Karte die PIN eingeben: Wenn der Lesegerät für die Verwendung von „Karte“ oder „Karte + PIN“ konfiguriert ist, muss dieses Zugangsmedium „Karte + PIN“ verwenden.

Anzahl der Präsentationen: Geben Sie die Startanzahl der begrenzten Verwendungen ein.



The screenshot shows the 'NEW USER' configuration page in the TDSi system, with the 'Options' tab selected. The 'Intruder management' section includes checkboxes for 'Intruder management', 'Ignore anti-passback', 'Reset anti-passback', 'Office Mode Management', and 'User must enter PIN after card'. The 'Number of presentations' section is also visible at the bottom.

10.2 Neuen Benutzer aus einem Ereignis erstellen

Der integrierte Webserver ermöglicht die Erstellung eines Benutzers aus der Ereignisliste.

Schritt 1 Klicken Sie auf die Ausweisnummer, die als Link hervorgehoben ist.

Date	Description	Reader	Credential	Surname	First Name
20/02/2020 11:23:08	Unknown credential	Reader 1	97499795		

Schritt 2: Das System lädt automatisch den Bildschirm „Neuer Benutzer“ und füllt die Ausweisnummer automatisch ein. Geben Sie alle weiteren erforderlichen Eigenschaften ein und klicken Sie anschließend auf „Speichern“.

10.3 Zugangsdaten importieren

Es gilt eine Beschränkung auf 100 Benutzer beim Verwendung des ISO8859-1-Dateiformats. Folgende Eigenschaften können zugeordnet werden: **Zugangsdaten, Nachname, Vorname, Gruppe 1, Gruppe 2, Gruppe 3, Startdatum, Enddatum.**

Als Trennzeichen ist standardmäßig das Komma eingestellt; weitere Optionen sind Tabulator und Semikolon. Wählen Sie die Spalte aus, die jeder Eigenschaft zugeordnet werden soll. Der Importvorgang kann bis zu 20 Spalten lesen.

Schritt 1: Wählen Sie die gewünschte Datei aus, indem Sie auf die Schaltfläche „Datei auswählen“ klicken. **Schritt 2:** Wählen Sie das Trennzeichen aus dem Dropdown-Menü aus.

Schritt 3 Ordnen Sie die gewünschten Eigenschaften zu, indem Sie die entsprechende Spalte auswählen. **Schritt 4** Klicken Sie auf „Speichern“, um den Importvorgang zu starten.

IMPORT

Back

Schritt 3

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

Schritt 2

Separator: Comma

Schritt 1

Choose file No file chosen

Save

Schritt 4

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

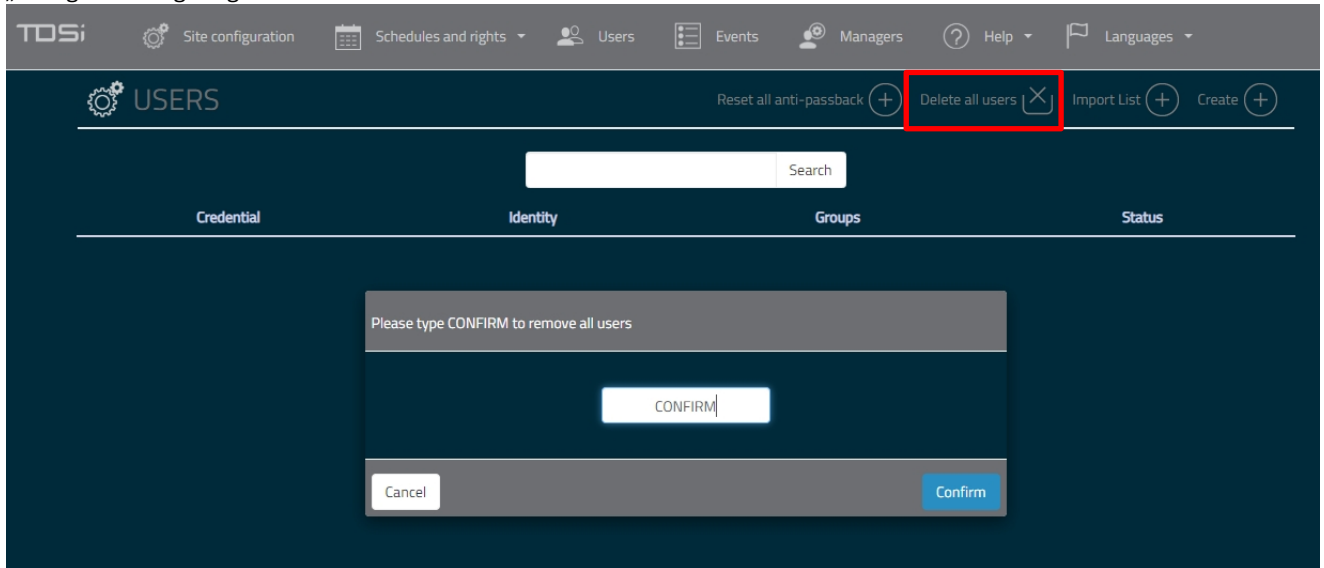
Column 19

10.4 Alle Benutzer löschen

Um alle Benutzer zu löschen, klicken Sie in der Aktionsleiste auf „**Alle Benutzer löschen**“.

Es erscheint ein Bestätigungsfenster. Geben Sie „CONFIRM“ ein und klicken Sie dann auf die Schaltfläche „**Bestätigen**“.

Es wird ein neues Fenster angezeigt, das angibt, dass der Löschvorgang läuft. Nach Abschluss des Vorgangs wird das Fenster „Erfolgreich“ angezeigt.

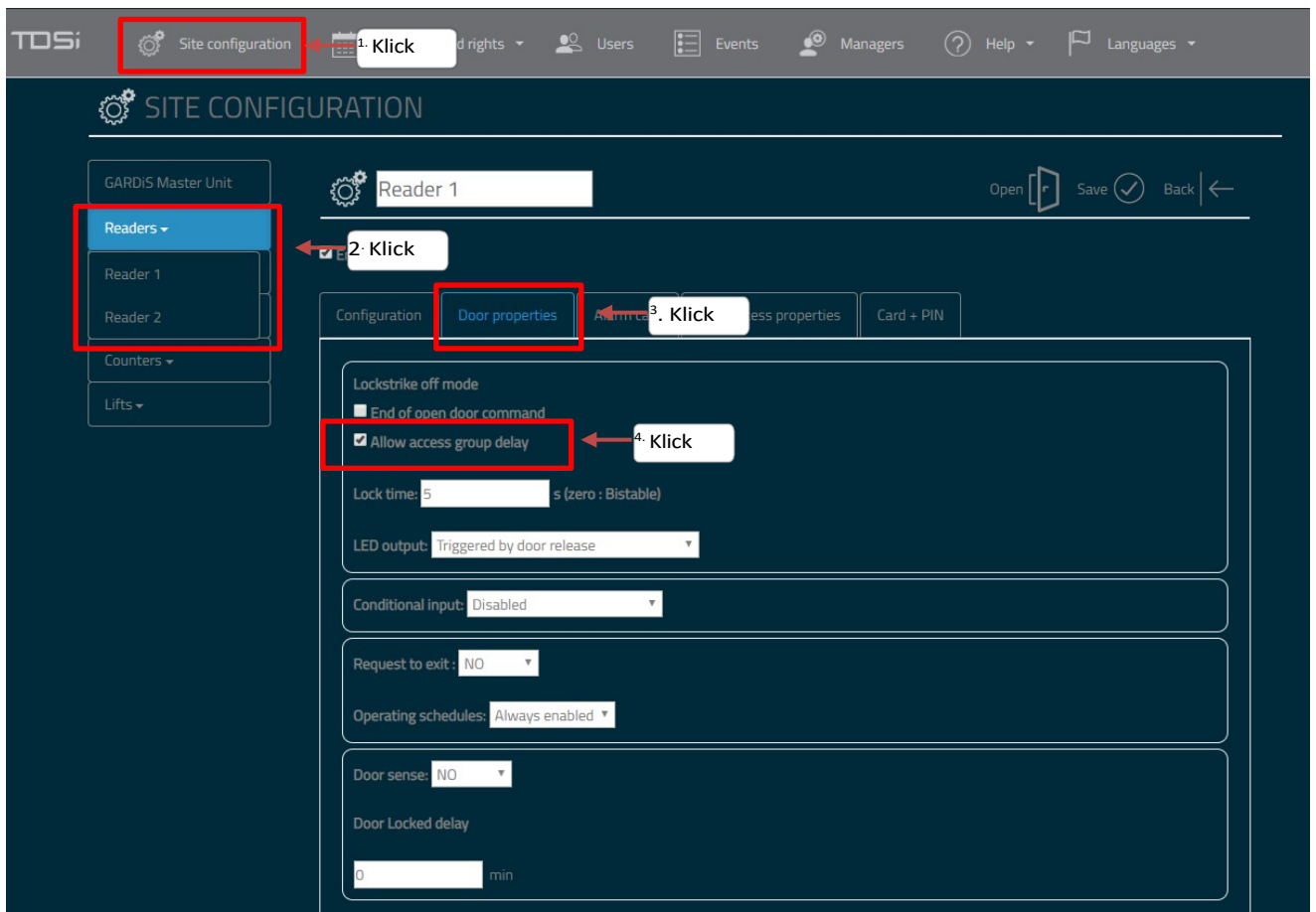


10.5 DDA-Benutzer

In diesem Abschnitt wird erläutert, wie man den erforderlichen Zugangsdaten zusätzliche Zeit für den Zutritt durch eine Tür einräumt. Diese Option wird über eine Zugangsgruppe und nicht über die einzelne Zugangsdatenkonfiguration aktiviert.

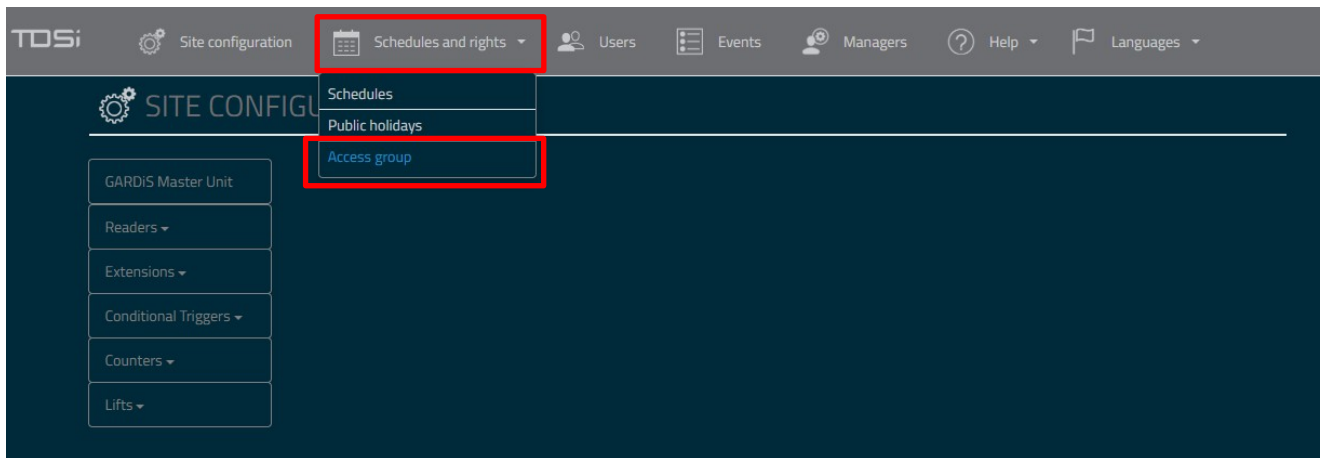
Schritt 1: Konfigurieren der Türeigenschaften

Klicken Sie auf „**Standortkonfiguration**“, wählen Sie im linken Menü den gewünschten **Lesegerät** aus und klicken Sie auf die Registerkarte „**Türeigenschaften**“. Aktivieren Sie anschließend das Kontrollkästchen „**Verzögerung für Zugangsgruppe zulassen**“.

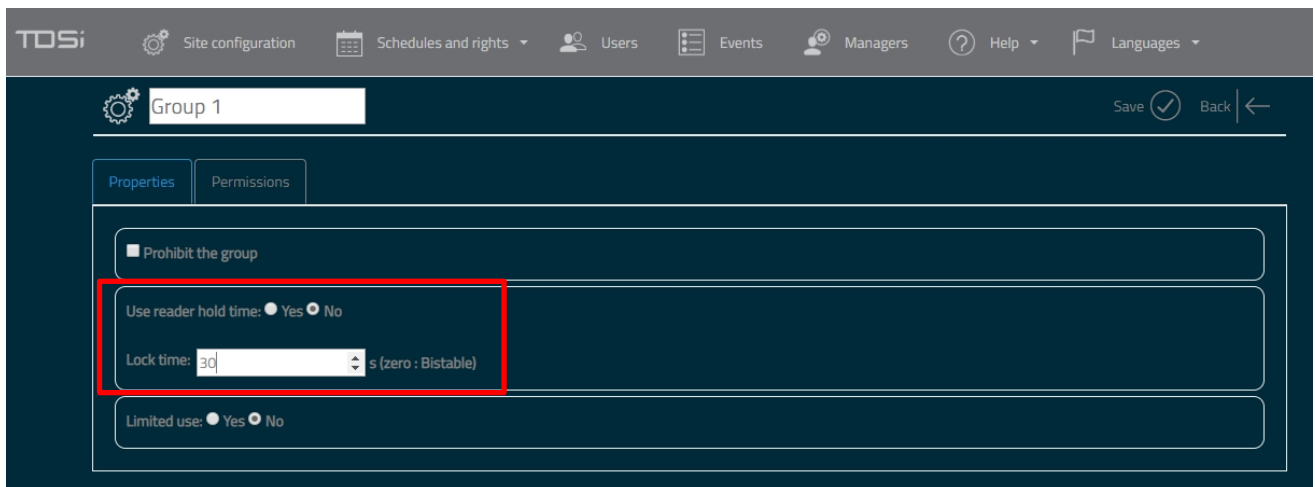


Schritt 2: Konfigurieren der Zugriffsgruppe

Klicken Sie im oberen Menü auf „**Zeitpläne und Rechte**“ und anschließend auf „**Zugriffsgruppe**“.



Klicken Sie in der Liste auf die gewünschte Zugangsgruppe, z. B. „Gruppe 1“. Wählen Sie anschließend bei „**Leser-Haltezeit verwenden**“ die Option „**Nein**“ aus, um die Leser-Haltezeit zu überschreiben. Dadurch können Sie die Sperrzeit für Zugangsdaten innerhalb dieser Zugangsgruppe konfigurieren. Im folgenden Beispiel haben Zugangsdaten dieser Gruppe 30 Sekunden Zeit, um die Tür zu öffnen. Der maximale Wert beträgt 254. Klicken Sie auf „**Speichern**“.

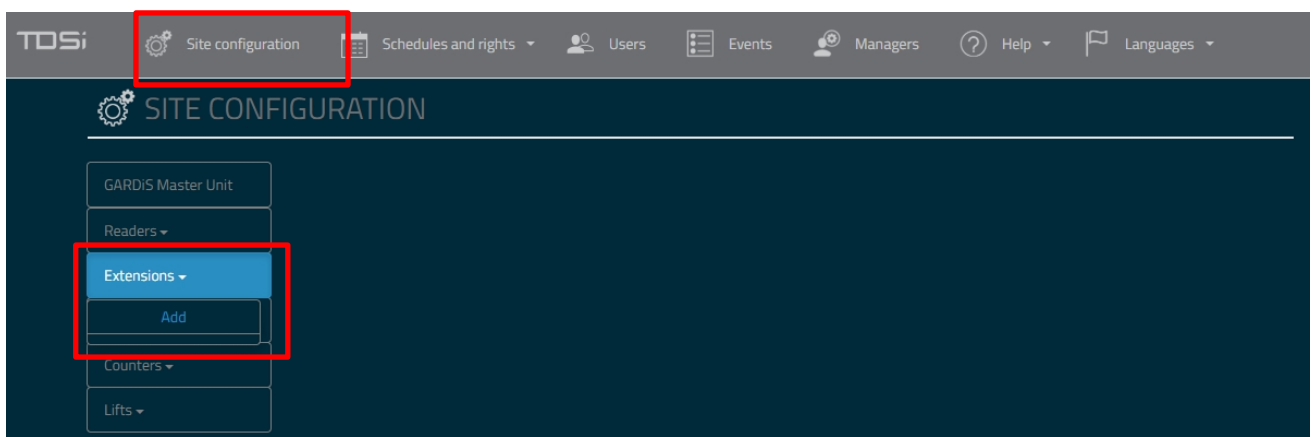


11. Erweiterungen hinzufügen

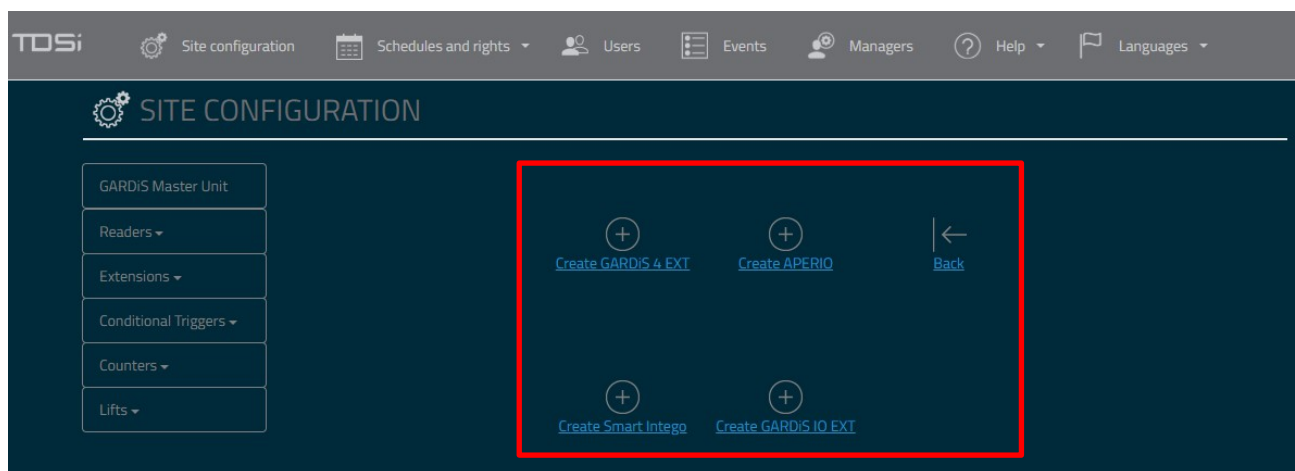
Ein GARDiS-Master unterstützt

- bis zu 10 x (GARDiS 4 EXT- oder GARDiS IO EXT-Erweiterungseinheiten)
- ODER
- 1 IP-Lock-Hub mit bis zu 10 IP-Locks.

Um Erweiterungsmodule zum Master-Controller hinzuzufügen, klicken Sie im linken Menü auf „**Standortkonfiguration**“, dann auf „**Erweiterungen**“ und anschließend auf „**Hinzufügen**“.



Die verfügbaren Erweiterungen werden im Hauptfenster angezeigt.



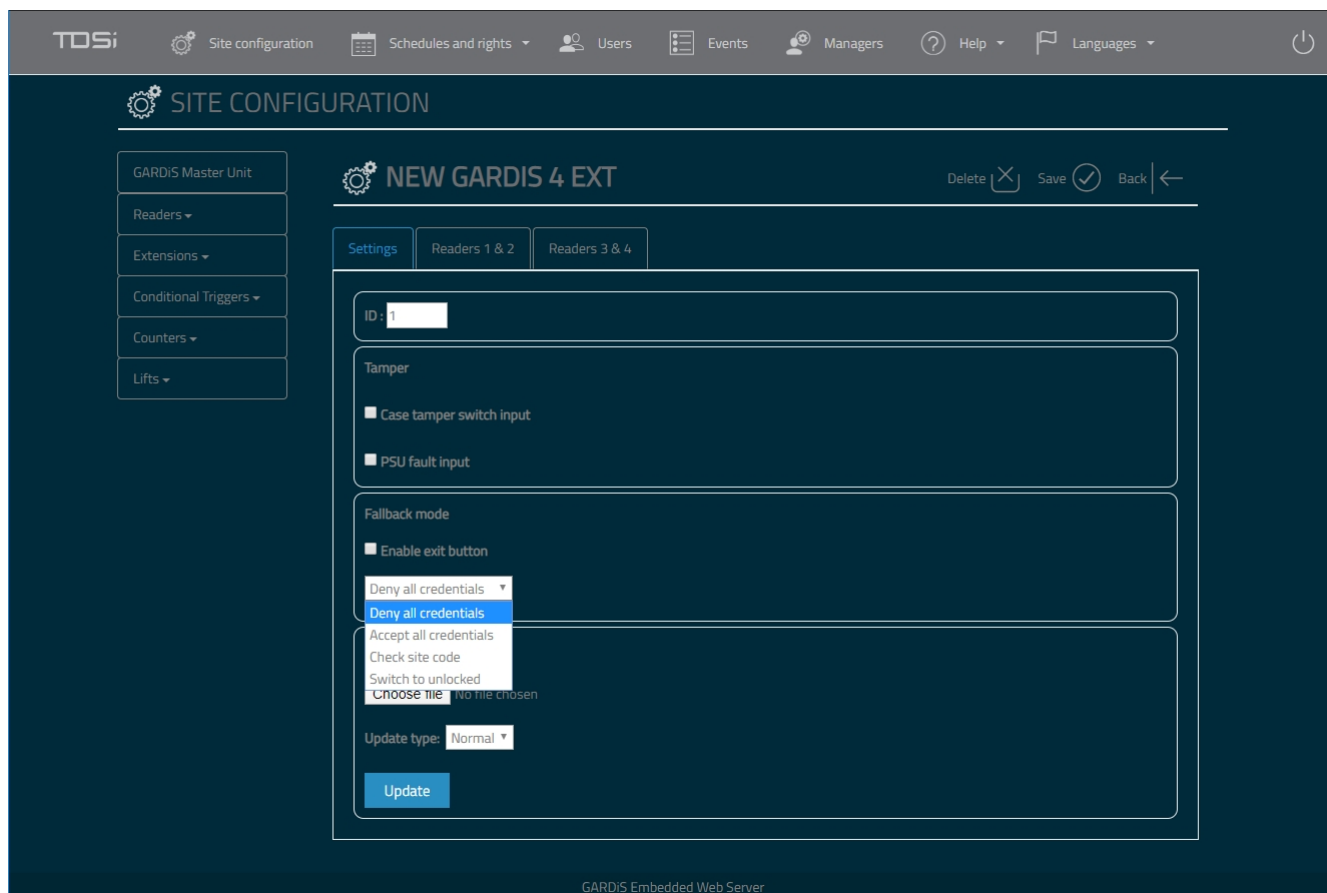
11.1 GARDiS 4 EXT

Mit diesen Slave-Steuerungen können bis zu 4 Türen pro Steuerung (insgesamt maximal 10) an die Master-Steuerung angeschlossen werden.

11.1.1 Fallback-Modus

Wenn eine Slave-Einheit die Kommunikation mit einem Master-Controller verliert, stehen Endbenutzern verschiedene Fallback-Modi zur Verfügung.

Ausgangstaste deaktivieren/aktivieren. Damit kann der Endnutzer die Ausgangsfunktion konfigurieren, wenn die Verbindung zum Master unterbrochen ist.



Verfügbare Ausweichmodi

- **Alle Zugangsdaten ablehnen** – alle an den Lesern vorgelegten Zugangsdaten werden abgelehnt.
- **Alle Zugangsdaten akzeptieren** – alle den Lesegeräten vorgelegten Zugangsdaten akzeptieren.
- **Standortcode prüfen** – Akzeptieren Sie Zugangsdaten, die mit dem Standortcode der Lesegeräte übereinstimmen.
- **Auf „Entriegelt“ umschalten** – Die Türen an der Slave-Einheit entriegeln, um den Zugang zu ermöglichen.

11.2 Aperio

Dadurch kann ein Aperio 485-Hub zum Master-Controller hinzugefügt werden. (Diese können nicht zusammen mit Slave-Controllern hinzugefügt werden.)

11.3 Smart Intego

Dadurch kann ein Simons Voss 485-Hub zur Master-Steuerung hinzugefügt werden. (Diese können nicht zusammen mit Slave-Steuerungen hinzugefügt werden.)

11.4 GARDiS IO EXT

Damit kann eine GARDiS-IO-Erweiterungskarte an den Controller angeschlossen werden. Maximal 10 Slave-Einheiten an einem einzelnen Master-Controller.

Fallback-Modi

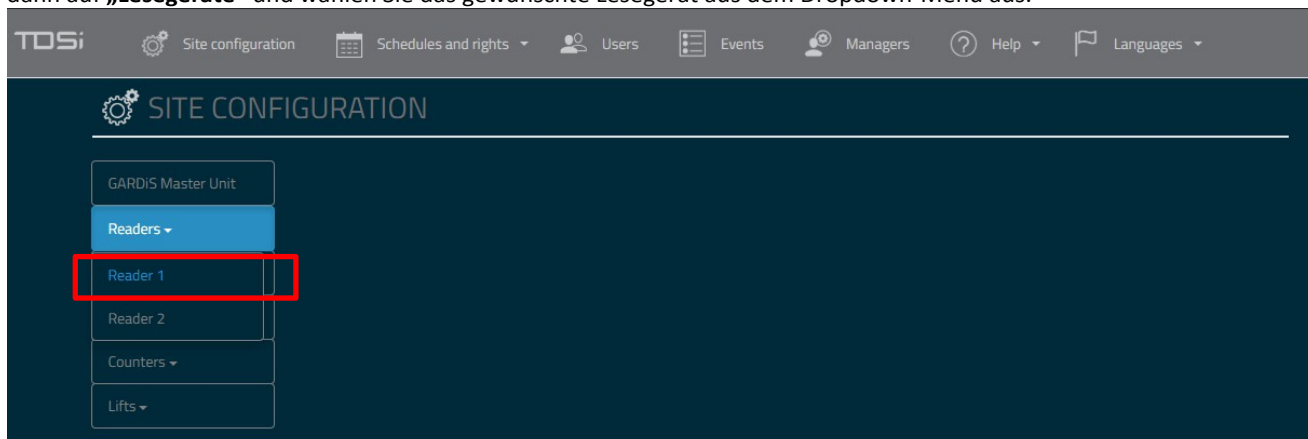
Vorherigen Zustand
beibehalten Alle Ausgänge
aktivieren Alle Ausgänge
deaktivieren

12. Aufzugssteuerung

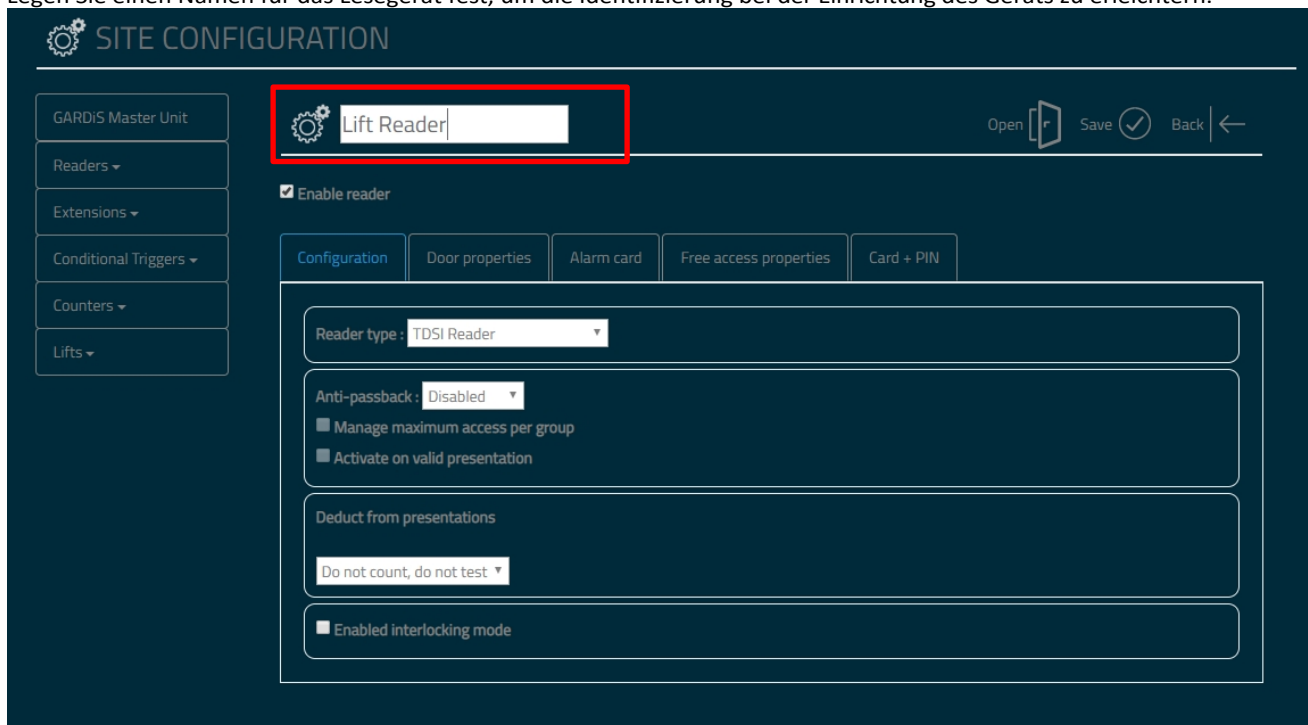
Zur Konfiguration der Aufzugssteuerung muss eine GARDiS IO-Erweiterungskarte verwendet werden.

Schritt 1: Konfigurieren Sie das Lesegerät

Wählen Sie den Lesegerät aus, der die Aufzugsausgänge steuert. Klicken Sie im oberen Menü auf „Standortkonfiguration“, dann auf „Lesegeräte“ und wählen Sie das gewünschte Lesegerät aus dem Dropdown-Menü aus.

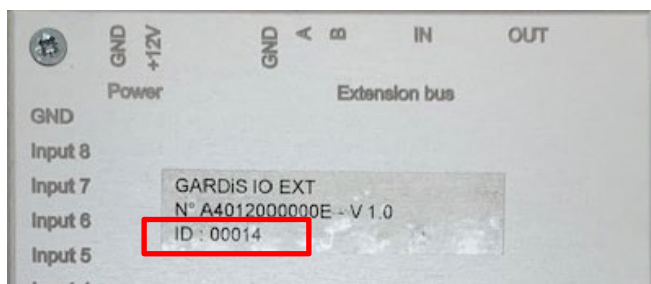


Legen Sie einen Namen für das Lesegerät fest, um die Identifizierung bei der Einrichtung des Geräts zu erleichtern.



Schritt 2: Hinzufügen des GARDiS IO-Erweiterungsmoduls

Gehen Sie zu „Standortkonfiguration“, klicken Sie auf „Erweiterungen“ und dann auf „Hinzufügen“. Klicken Sie im Hauptbildschirm auf „GARDiS IO EXT erstellen“. Der folgende Bildschirm wird angezeigt. Halten Sie die ID des GARDiS IO EXT bereit. Diese befindet sich auf dem Gerät und ist auf dem Etikett aufgedruckt.



CADDiS Embedded Web Server

Es können bis zu 256 Aufzugsgruppen definiert werden. Wählen Sie die ^{erste} verfügbare Aufzugsgruppe aus.

Die Konfiguration für diese Gruppe wird im Hauptfenster angezeigt.

SITE CONFIGURATION

GARDIS Master Unit

Readers ▾

Extensions ▾

Conditional Triggers ▾

Counters ▾

Lifts ▾

Lift 1 Save Back

Legen Sie den Namen der Aufzugsgruppe fest

Outputs available	Used
Module 1	
Exit 1	☐
Exit 2	☐
Exit 3	☐
Exit 4	☐
Exit 5	☐
Exit 6	☐
Exit 7	☐
Exit 8	☐

Markieren Sie die Ausgänge, die diese Gruppe nutzen darf.

Geben Sie die gewünschte Konfiguration ein und klicken Sie auf „**Speichern**“. Das folgende Beispiel zeigt eine neue Aufzugsgruppe namens „**Manager**“. Diese Gruppe hat Zugriff auf alle 10 Ausgänge.

SITE CONFIGURATION

GARDIS Master Unit

Readers ▾

Extensions ▾

Conditional Triggers ▾

Counters ▾

Lifts ▾

Manager Save Back

Outputs available	Used
Module 1	
Exit 1	☒
Exit 2	☒
Exit 3	☒
Exit 4	☒
Exit 5	☒
Exit 6	☒
Exit 7	☒
Exit 8	☒

Die Liste wird nun mit dem neuen Namen aktualisiert.

SITE CONFIGURATION

GARDIS Master Unit

Readers ▾

Extensions ▾

Conditional Triggers ▾

Counters ▾

Lifts ▾

Manager Save Back

Outputs available	Used
Module 1	
Exit 1	☒
Exit 2	☒
Exit 3	☒
Exit 4	☒
Exit 5	☒
Exit 6	☒
Exit 7	☒
Exit 8	☒

Manager

Lift 2

Lift 3

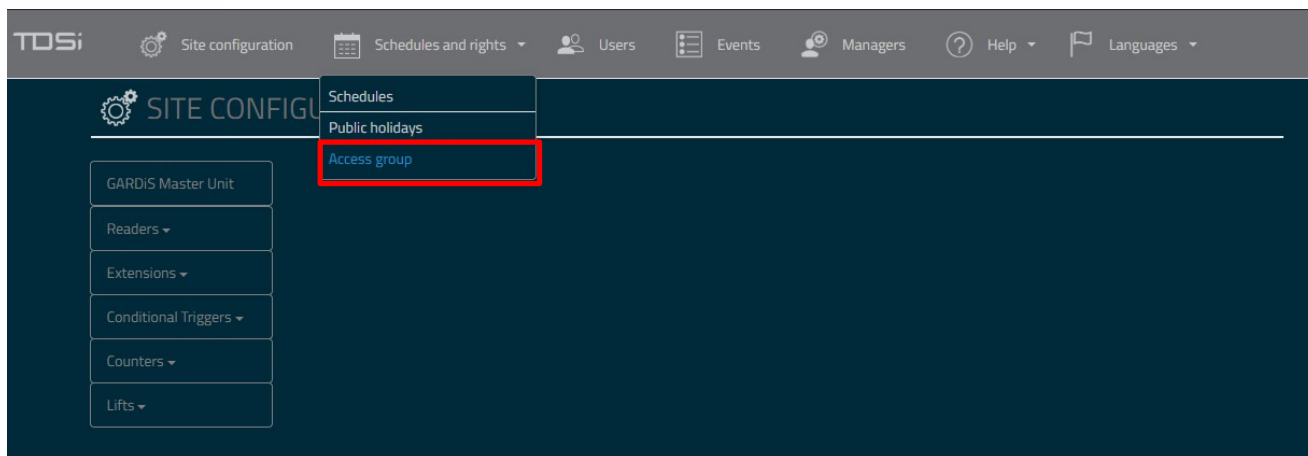
Lift 4

Fahren Sie fort, um nach Bedarf weitere

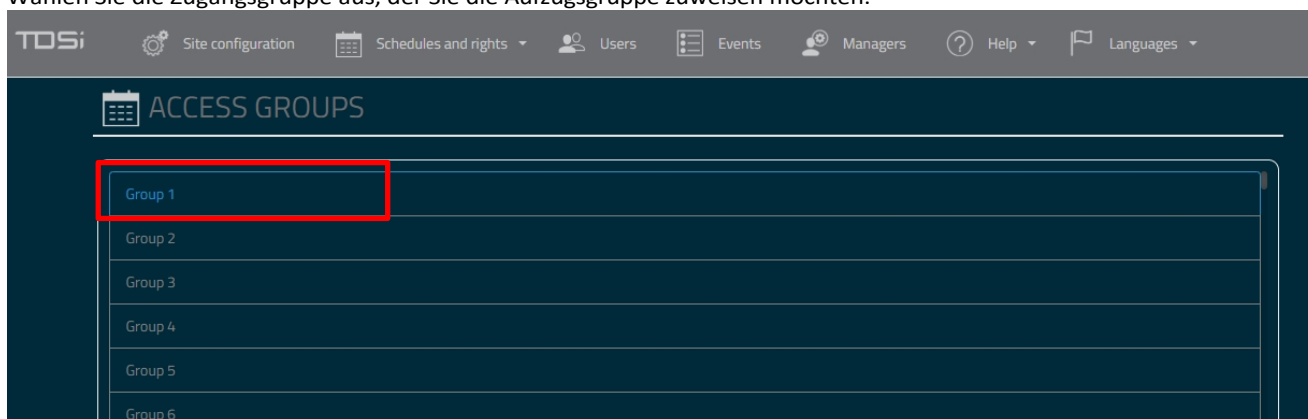
Aufzugsgruppen anzulegen. [Schritt 4: Zugriffsgruppen](#)

[konfigurieren](#)

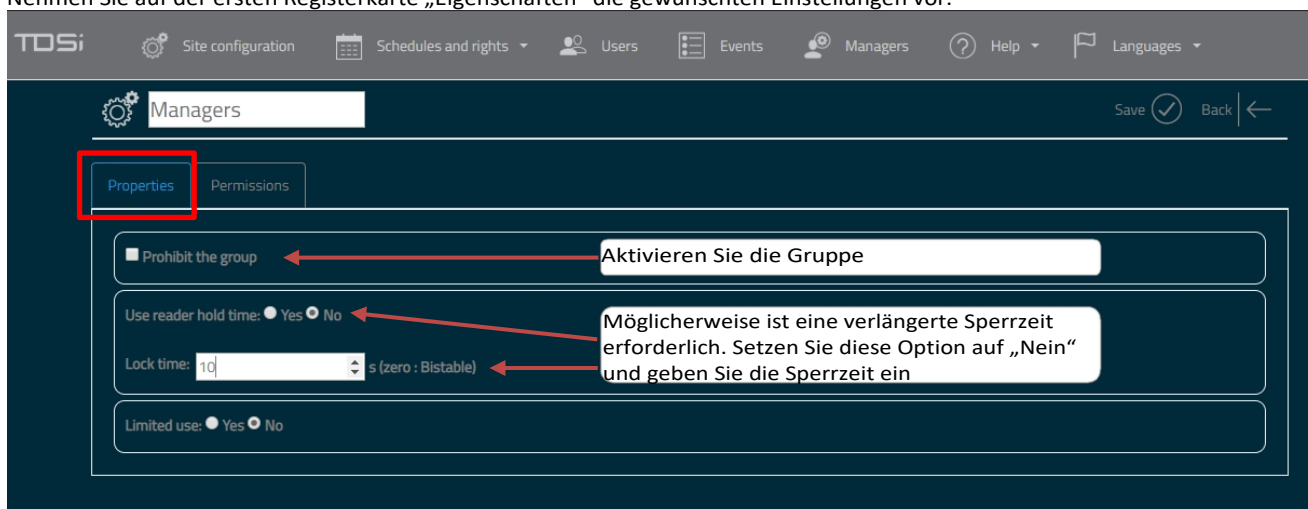
Klicken Sie im oberen Menü auf „**Zeitpläne und Rechte**“ und anschließend auf „**Zugriffsgruppen**“.



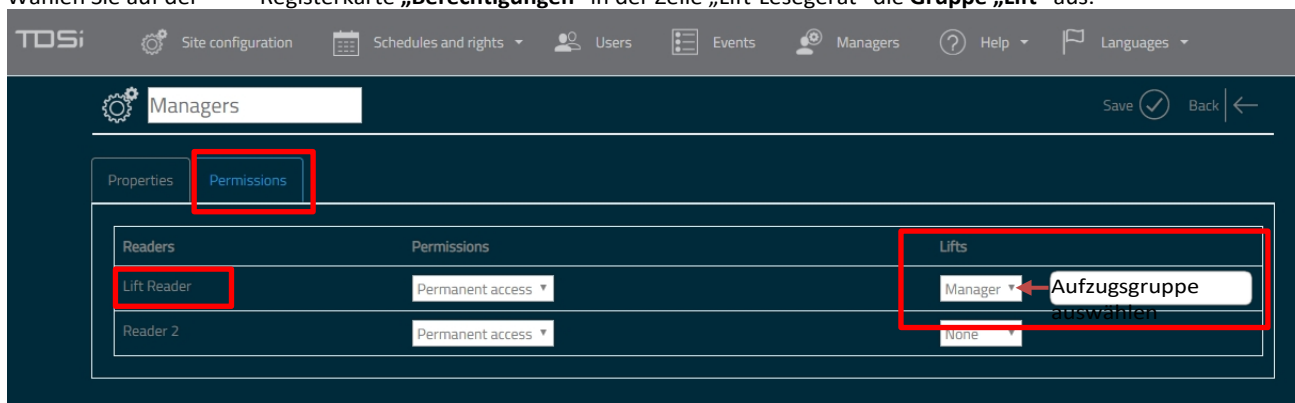
Wählen Sie die Zugangsgruppe aus, der Sie die Aufzugsgruppe zuweisen möchten.



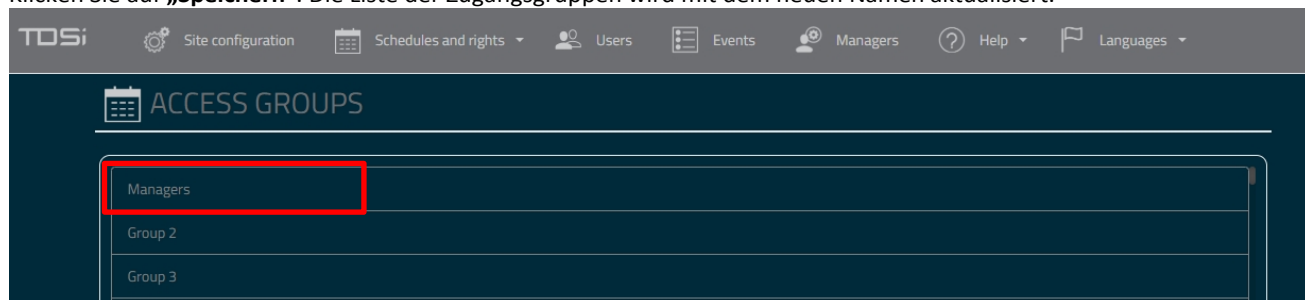
Nehmen Sie auf der ersten Registerkarte „Eigenschaften“ die gewünschten Einstellungen vor.



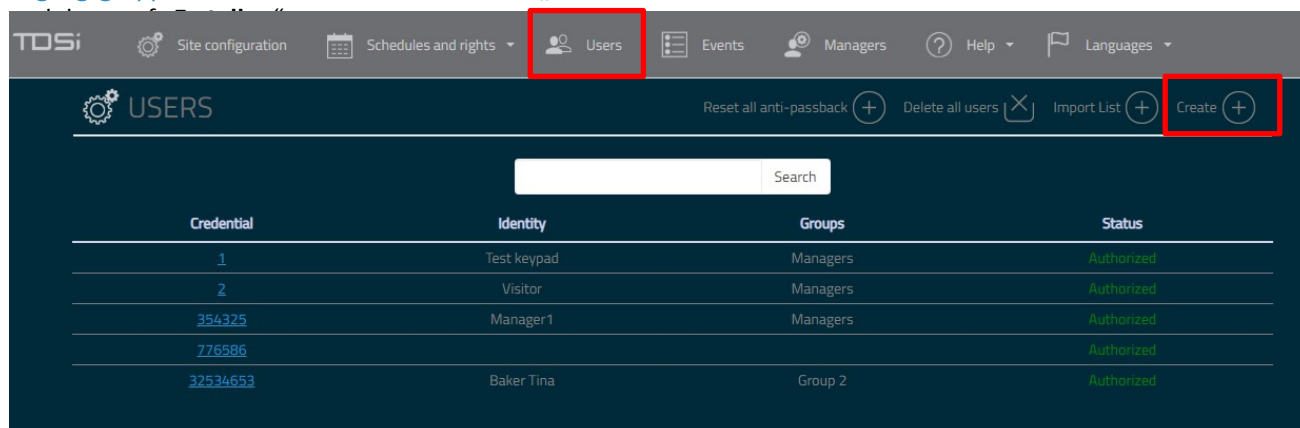
Wählen Sie auf der zweiten Registerkarte „Berechtigungen“ in der Zeile „Lift-Lesegerät“ die Gruppe „Lift“ aus.



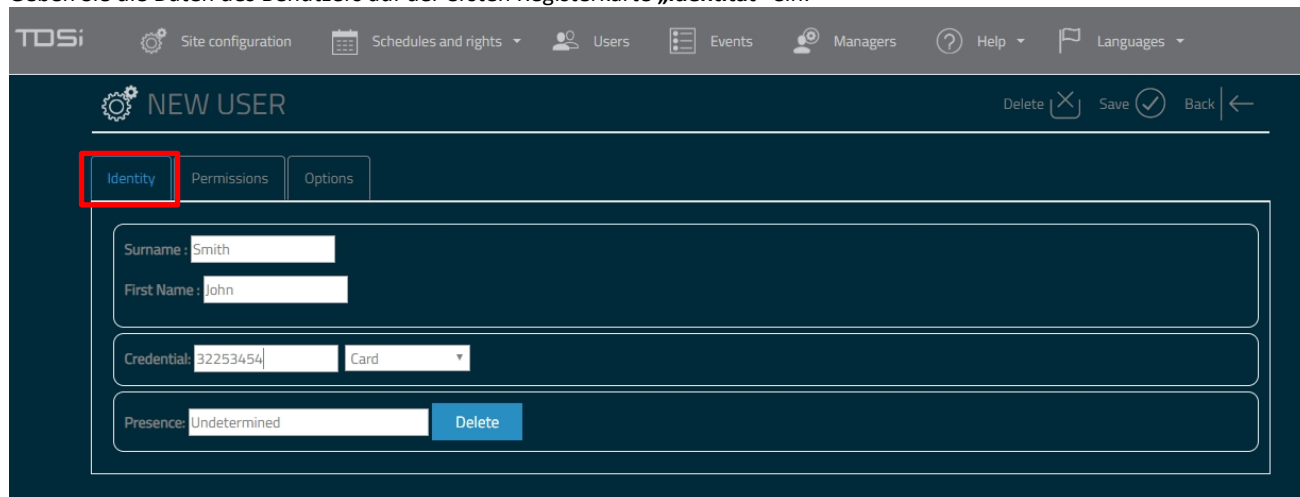
Klicken Sie auf „**Speichern**“. Die Liste der Zugangsgruppen wird mit dem neuen Namen aktualisiert.



Schritt 5: Erstellen Sie einen Benutzer mit der neuen Zugangsgruppe Klicken Sie im oberen Menü auf „**Benutzer**“



Geben Sie die Daten des Benutzers auf der ersten Registerkarte „**Identität**“ ein.



Klicken Sie auf die nächste Registerkarte „**Berechtigungen**“ und nehmen Sie die erforderlichen Einstellungen vor. Wählen Sie im Abschnitt „**Zugangsgruppen**“ die Gruppe mit der konfigurierten Aufzugsgruppe aus. Klicken Sie anschließend auf „**Speichern**“.

Dieser Benutzer ist nun für die Nutzung des Aufzugslesers konfiguriert.

13. Anti-Passback

Es stehen verschiedene Anti-Passback-Optionen zur Verfügung: „True Anti-Passback“ und „Timed Anti-Passback“. Es ist außerdem möglich, den Anti-Passback-Wert zu aktualisieren, wenn die Person die Tür öffnet, und nicht erst, wenn sie die Karte an den Lesegerät hält. Dazu muss die Eigenschaft „Door Sense“ in den Türeigenschaften entsprechend eingestellt werden.

13.1 Echtes Anti-Passback

Schritt 1: Aktivieren Sie den Anti-Passback auf dem Gerät.

Klicken Sie im oberen Menü auf „Standortkonfiguration“ und anschließend im linken Menü auf „GARDIS-Master-Einheit“. Aktivieren Sie das Kontrollkästchen „Anti-Passback“. Klicken Sie auf „Speichern“.

Schritt 2: Konfigurieren Sie die Lesegeräte für die Anti-Passback-Funktion

Klicken Sie auf „Lesegeräte“ und wählen Sie das gewünschte Lesegerät aus dem Menü aus. Navigieren Sie auf der Registerkarte „Konfiguration“ zum Abschnitt „Anti-Passback“. Wählen Sie die gewünschte Option für das Lesegerät aus. Folgende Optionen stehen zur Verfügung:

- Deaktiviert** (Standard): Anti-Passback wird nicht erzwungen
- Einlass:** Lesegerät als Einlassleser festlegen

Ausgang: Lesegerät als Ausgangslesegerät festlegen

Eintritt \ Austritt: Lesegerät so einstellen, dass „Anti-Passback“ ignoriert wird

Klicken Sie anschließend auf „**Speichern**“. Die Anti-Passback-Funktion ist nun auf dem Controller eingerichtet. Das Ereignis „Benutzer bereits eingetreten“ wird generiert, wenn ein Benutzer versucht, Zutritt zu erhalten, ohne zuvor den Ausgang passiert zu haben.

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

Reader type: TDSi Reader

Anti-passback: **Entry**

☐ Manage maximum access per group

☒ Activate on valid presentation

Deduct from presentations

Daily count

☐ Enabled interlocking mode

Wenn Sie die Anti-Passback-Funktion für ein Zugangsmedium aktualisieren möchten, wenn die Tür geöffnet wird, müssen Sie die Türerkennung in den Türeigenschaften konfigurieren.

13.2 Zeitgesteuertes Anti-Passback

Schritt 1: Anti-Passback-Einstellungen aktivieren

Klicken Sie im oberen Menü auf „**Site-Konfiguration**“ und anschließend im linken Menü auf „**GARDiS-Master-Einheit**“. **Aktivieren Sie** die Kontrollkästchen „**Anti-Passback**“ und „**Zeitgesteuertes Anti-Passback**“. Legen Sie die Zeitspanne fest, für die das Anti-Passback-Verfahren gelten soll. Diese Funktion kann an den Lesegeräten am Ein- oder Ausgang aktiviert werden. **Klicken Sie auf „Speichern“**. Befolgen Sie **Schritt 2** aus Abschnitt 13.1 „Echtes Anti-Passback“, um die Lesegeräteeinstellungen zu konfigurieren.

SITE CONFIGURATION

GARDiS Master Unit

Readers ▾

Extensions ▾

Conditional Triggers ▾

Counters ▾

Lifts ▾

MASTER CONTROLLER

Restore from backup Backup **Save** Back

Configuration Operating mode External Integrations

☒ DHCP

☐ Static IP address (Recommended)

Speed: 10 Mbps

Web server port: 80

☒ Anti-passback

☒ Timed anti-passback

Timed anti-passback duration: 1 m

☒ Enable on entry

☒ Enable on exit

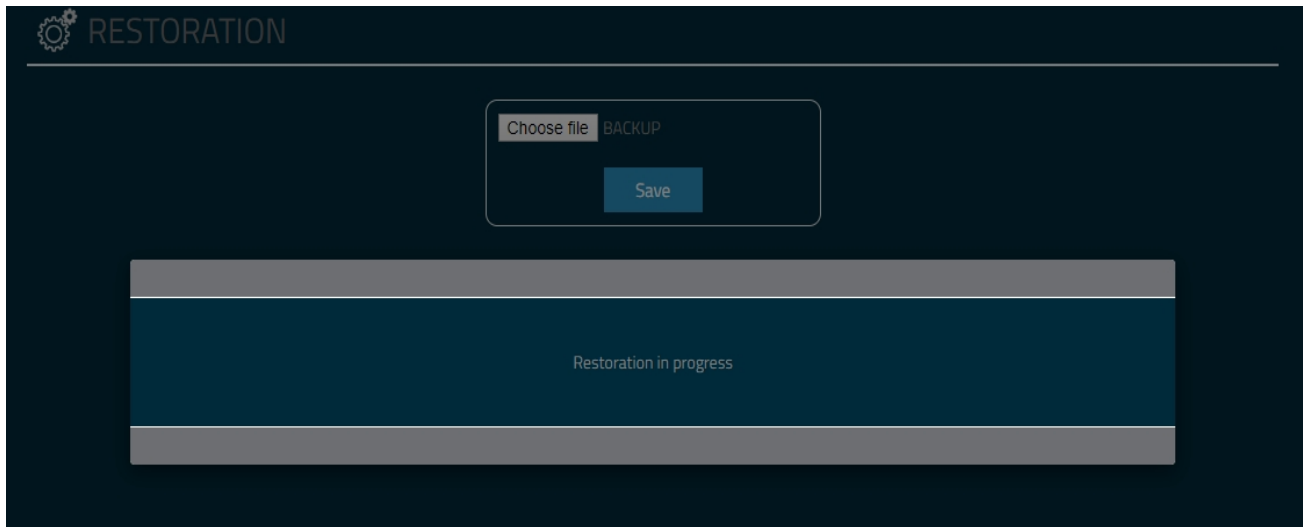
☐ Reverse timed anti-passback

14. Fehlerbehebung

In diesem Kapitel werden typische Probleme beschrieben, die auftreten können.

14.1 Wiederherstellung aus einer Sicherung

Symptom: Bei der Wiederherstellung aus einem Backup bleibt die folgende Meldung auf dem Bildschirm stehen und die Wiederherstellung wird nicht abgeschlossen.



Behebung: Zwischen den Wiederherstellungen muss eine Sicherung durchgeführt werden. Erstellen Sie eine neue Sicherung. Befolgen Sie anschließend den Vorgang zur Wiederherstellung aus einer Sicherung und wählen Sie die gewünschte Sicherungsdatei aus.

Haben Sie technische Fragen?

Wenden Sie sich an unseren kostenlosen technischen 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

Weil jeder ein Recht auf Sorgenfreiheit hat

TDSi UK
Unit 10 Concept Park, Innovation Close, Poole, Dorset BH12 4QT Vereinigtes Königreich t 44 0
1202 723535 f 44 0 1202 724975 E-Mail: sales@tdsi.co.uk

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

