

The BLOCKER program

User manual for the Blocker program
version 9.0.5.38



User manual for Blocker

2023 in Naklo

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

© Jantar d.o.o.

Table of Contents

Chapter 1 Blocker	5
1.1 License information.....	5
1.2 Disclaimer and Warranty.....	6
1.3 Contact information	6
Chapter 2 Description and installation instructions	7
2.1 Cable installation	7
2.2 System requirements.....	8
2.3 Software installation.....	8
2.4 Backing up and deleting the Blocker database	10
Chapter 3 The Blocker interface	11
Chapter 4 Launching Blocker for the first time	13
Chapter 5 Hardware setup	14
5.1 Adding communication lines	15
5.1.1 Manually adding communication lines	15
5.1.2 Automatically adding communication lines	17
5.1.3 Remove communication line	19
5.2 Adding controllers.....	20
5.2.1 Automatically adding controllers	20
5.2.2 Manually adding controllers	23
5.2.3 Remove controller	24
5.3 Adding readers.....	25
5.3.1 Automatically adding readers	25
5.3.2 Manually adding readers	26
5.3.3 Remove reader	28
5.4 Status of communication.....	29
Chapter 6 Users & Accesses	30
6.1 Adding users.....	31
6.1.1 Manually adding users	31
6.1.2 Import users	32
6.1.3 Read cards	33
6.1.4 Remove user	35
6.2 Adding groups and organizing users into groups.....	36
6.2.1 Add group	36
6.2.2 Organizing users into groups	37

6.2.3 Assigning access rights to groups	37
6.2.4 Remove group	38
6.3 Send tables	39
Chapter 7 View Events	40
7.1 Show live events.....	40
7.2 Event filtering.....	40
7.3 Print report.....	41

1 Blocker

Blocker is a free and simple software designed for smaller access control systems. It enables simple access control using standalone access controllers (e.g. with one of the Rex controllers). It is intended for users who do not require advanced settings, e.g. private users or multi-residential buildings, commercial buildings, etc.

1.1 License information



- Logo "Hand" is registered at EUIPO (The European Union Intellectual Property Office) and is exclusively owned by Jantar d.o.o. You may not copy, imitate, rent, lease, sell, modify or otherwise use the "hand" logo, except as provided in this or any other agreement with Jantar d.o.o. Any such unauthorized use will result in immediate and direct termination of this license and may result in criminal and/or civil prosecution.

The Blocker software is distributed together with the Jantar hardware or separately as a replacement system for an existing access control system, which means:

- All copyrights of Blocker are exclusively owned by the author, Jantar d.o.o.
- You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program, or any subset of the licensed program, except as stated in this agreement. Any such unauthorized use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.
- The Blocker binary code may NOT be used or reverse engineered to re-create the access control or communication algorithms which are proprietary and protected by copyright law.
- Blocker is distributed "as is". No warranty of any kind is expressed or implied. You use the Blocker software at your own risk. Neither the author nor his authorized distributors will be liable for any data loss, damages, loss of profits or any other kind of loss while using, misusing or being unable to use this software.
- All rights not expressly granted here are reserved by Jantar d.o.o.
- By installing and using the Blocker software you are accepting the terms and conditions of this license.
- If you do not agree with the terms of this license you must remove all Blocker files from your storage devices and cease using the product.

1.2 Disclaimer and Warranty

Disclaimer

The information in this document is subject to change without notice. While the information contained herein is assumed to be accurate, Jantar d.o.o., assumes no responsibility for any errors or omissions. We also reserve the right to discontinue or change the specifications of products without prior notice. No claim can be made in the case of profit or loss from use or sale of any products bought or delivered by us. Errors reported will be corrected in new software releases.

Warranty

This manual comes "as is" - no warranty of any kind, expressed or implied. Jantar d.o.o. does not give any assurances or guarantee in connection with information in this document.

Although we strive to include accurate and up to date information, Jantar d.o.o., without prejudice to the generality of this paragraph does not guarantee that the information in this manual is complete, true, accurate and not misleading.

The information in this manual is designed for user purposes and not as a substitute for information from customer regulations, technical manuals/documents or other official documents. Customers using this manual can report errors or omissions, recommendations for improvement or other comments to Jantar d.o.o.

1.3 Contact information

Jantar has more than 30 years of experience in the development and production of access control, time attendance, and visitor control systems. What sets us apart from our competitors is that we develop and manufacture all of our software and most of our hardware ourselves. Our systems are installed and utilized at airports, office buildings, financial institutions, factories, shopping centers, hospitals, etc. Our products are present virtually anywhere our clients need basic or advanced access control and time and attendance systems.

Jantar, elektronski sistemi, d.o.o.

Kranjska cesta 24, SI-4202 Naklo

SLOVENIA

VAT ID: SI34737332

E-mail: info@jantar.si

Web page: www.jantar.si

Support

E-mail: support@jantar.si

2 Description and installation instructions

Blocker is a free and simple software designed for smaller access control systems. It enables simple access control using standalone access controllers (e.g. with one of the Rex controllers). It is intended for users who do not require advanced settings, e.g. private users or multi-residential buildings, commercial buildings, etc.

The Blocker software package contains:

- the installation file for the Blocker program and
- instruction manual for the Blocker program.



2.1 Cable installation

Cable installations must be ready before installation of Jantar hardware devices (communication converters, readers and controllers). It is not recommended to use old or previously used cable installations. We strongly advise against the usage of existing abandoned telephone lines (telephone twisted pairs). Cable installation must be clearly labeled on both sides.

The cables used must meet the requirements specified in the technical specification for Jantar systems. The total length of cable must not exceed the maximal length of system specification. To make it easier to connect the cables to the hardware, depending on the type of hardware, the cables at the ends should be slightly longer than the required length (suggested cable spare lengths are approximately 30 cm for readers, 50 cm for controllers and 30cm for door strikes).

Controller's housing should be mounted on the wall and cables ran inside the housing. Door strikes should be mounted in doors. Their maximal power consumption should not exceed 250mA otherwise additional power supply is needed. Please read details in hardware specification manual.

For more information and wiring diagrams for specific Amber Devices please contact us.

2.2 System requirements


Minimal system requirements for the successful operation of Blocker:

- a server installed with the Windows 10 operating system or newer,
- available free USB ports or ethernet (LAN) ports for hardware connections,
- display resolution at least 1366 x 768 px (recommended resolution 1440 x 900 px),
- installed Microsoft .NET Framework 4.8,
- a minimum of 4 GB of RAM and a dual-core processor,
- at least 10 GB of space on the hard drive,
- PDF Reader software for viewing generated reports.


2.3 Software installation

NOTE

Before installing the Blocker software on your computer:

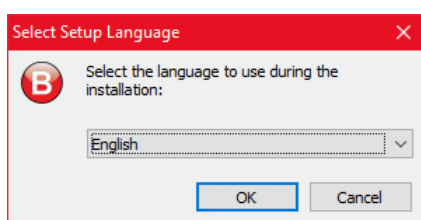
- Check the [system requirements](#) .
- Make sure the .NET Framework (at least) version 4.8 is already installed on your server, otherwise, install it on your server. (The Windows 8 operating system and newer already have the .NET Framework installed by default. Older versions of operating systems may require the framework to be installed manually.)

1. Start the program installation by double-clicking on the JantarBlockerSetup-v9.0.5.38.exe file:

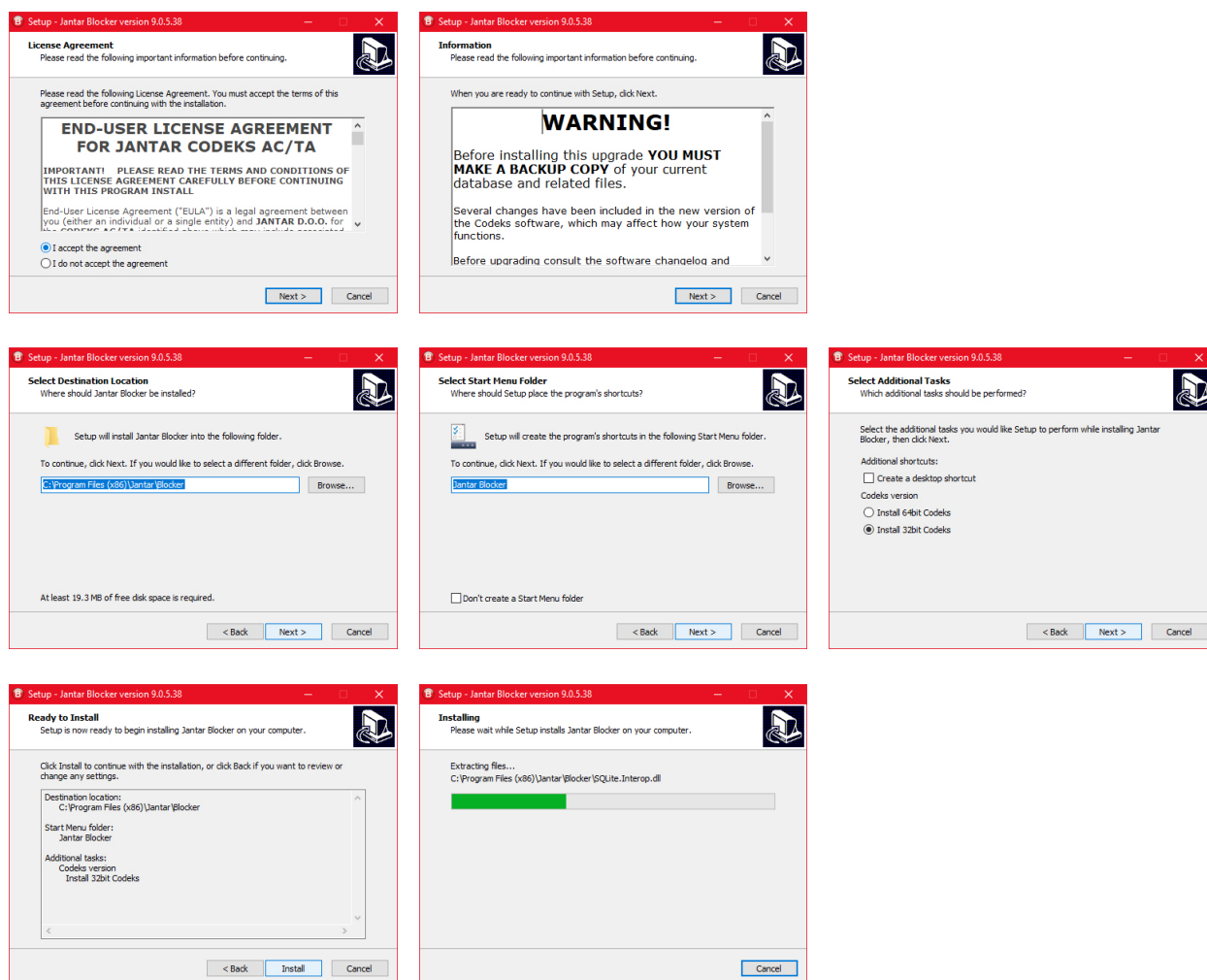
 **JantarBlockerSetup-v9.0.5.38.exe**

2. Select the language for the installation.

The selection of the installation language is important as it also determines which default settings and tools will be loaded during the Blocker software installation.



3. Read and accept the terms of the license agreement, then, click *Next* and follow the instructions of the installation process:



4. At the end of the installation process, you will be offered the option to start Blocker and display the PDF quick instructions when you first start the program.

2.4 Backing up and deleting the Blocker database

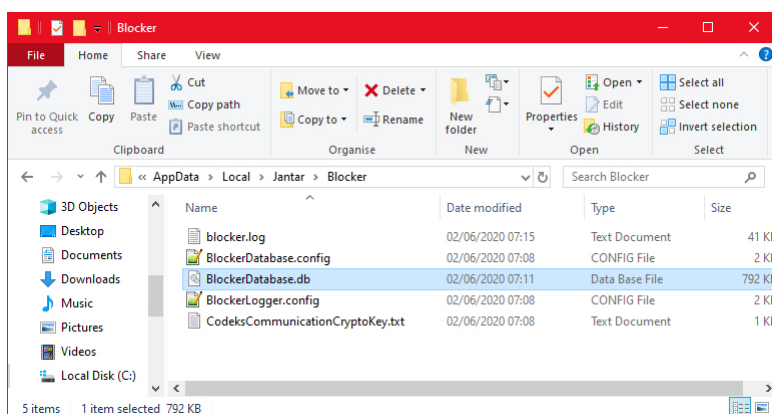
Backing up is mandatory!

Backing up the database and other user files is the responsibility of the owner and administrator of the blocker system! The Jantar company is in no way responsible for the loss of your data in any event!

Backing up your files protects them from permanent loss or irreversible alteration due to accidental deletion, virus or worm attacks as well as software or hardware failure. In the case of any of the mentioned scenarios, you can easily restore the original files, if you have their backup copies. A backup copy of the original files must be stored in a different location than the original. To track changes in your files, create multiple backup copies.

Making a backup copy of the database

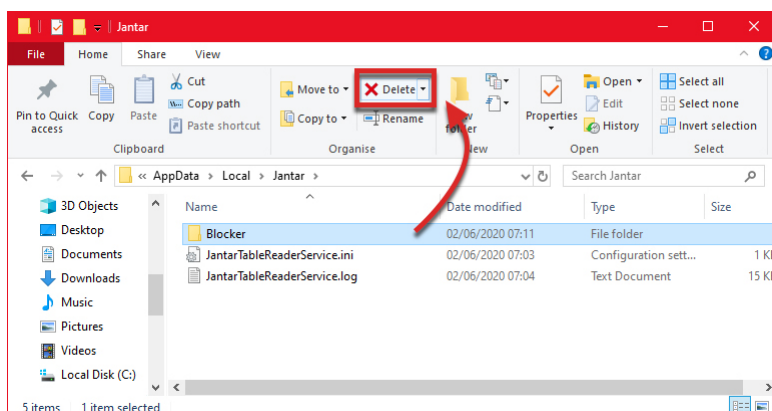
1. To back up the Blocker database on a computer (server), locate the program folder in the *AppData* folder of the current user (for example, C:\Users\User\AppData\Local\Jantar\Blocker).
2. Then copy the BlockerDatabase.db file.



3. Save the copied database in a secure location as it contains important and security-sensitive data.

Deleting the database

In case you need to delete the current Blocker database for any reason, find the program folder in the *AppData* folder of the current user (e.g. C:\Users\User\AppData\Local\Jantar\Blocker) and delete it completely.

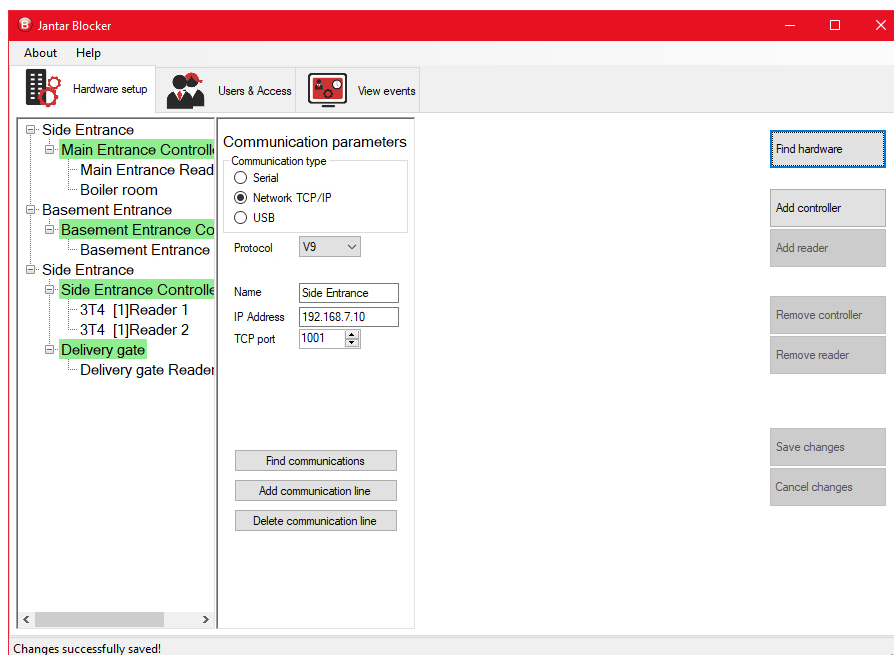


3 The Blocker interface

The *Blocker* program consists of three tabs:

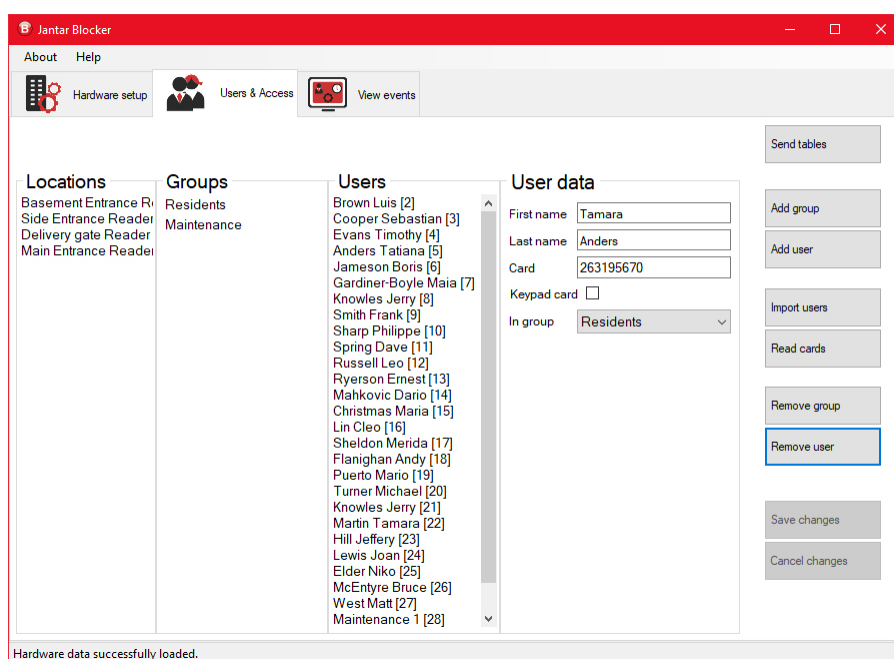
- Hardware setup

In this tab, you can edit the communication and add controllers and readers to the Blocker system. You can also adjust the hardware settings here.



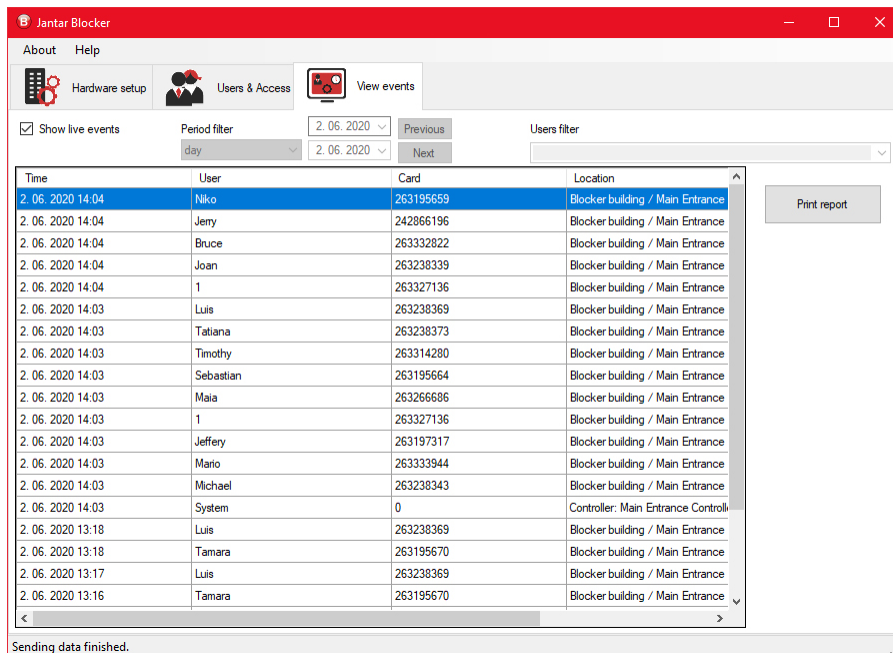
- Users & Accesses

In this tab, you can add and edit groups and users, assign user cards to users, and assign access rights to groups.



- View Events

In this tab, you can view current user movements through different passages in your system, and you can also generate event reports.



The screenshot shows the 'Jantar Blocker' application window with the 'View events' tab selected. The interface includes a sidebar with 'About', 'Help', 'Hardware setup', 'Users & Access', and 'View events'. The 'View events' tab displays a table of user movements with columns for Time, User, Card, and Location. The table is filtered for the date 2. 06. 2020 and the time range 14:03 to 14:04. A 'Print report' button is visible on the right side of the table.

Time	User	Card	Location
2. 06. 2020 14:04	Niko	263195659	Blocker building / Main Entrance
2. 06. 2020 14:04	Jemy	242866196	Blocker building / Main Entrance
2. 06. 2020 14:04	Bruce	263332822	Blocker building / Main Entrance
2. 06. 2020 14:04	Joan	263238339	Blocker building / Main Entrance
2. 06. 2020 14:04	1	263327136	Blocker building / Main Entrance
2. 06. 2020 14:03	Luis	263238369	Blocker building / Main Entrance
2. 06. 2020 14:03	Tatiana	263238373	Blocker building / Main Entrance
2. 06. 2020 14:03	Timothy	263314280	Blocker building / Main Entrance
2. 06. 2020 14:03	Sebastian	263195664	Blocker building / Main Entrance
2. 06. 2020 14:03	Maia	263266686	Blocker building / Main Entrance
2. 06. 2020 14:03	1	263327136	Blocker building / Main Entrance
2. 06. 2020 14:03	Jeffery	263197317	Blocker building / Main Entrance
2. 06. 2020 14:03	Mario	263333944	Blocker building / Main Entrance
2. 06. 2020 14:03	Michael	263238343	Blocker building / Main Entrance
2. 06. 2020 14:03	System	0	Controller: Main Entrance Controll
2. 06. 2020 13:18	Luis	263238369	Blocker building / Main Entrance
2. 06. 2020 13:18	Tamara	263195670	Blocker building / Main Entrance
2. 06. 2020 13:17	Luis	263238369	Blocker building / Main Entrance
2. 06. 2020 13:16	Tamara	263195670	Blocker building / Main Entrance

Sending data finished.

4 Launching Blocker for the first time

When launching the Blocker program for the first time, no hardware is connected to it and users and their access rights have not yet been entered.

To use Blocker you need to:

1. In the [Hardware setup](#)^[14] tab, first, connect the installed controllers and readers through the prepared communication lines.
2. Then, in the [Users & Accesses](#)^[30] tab, add the users and organize them into groups, and then add access rights to the groups.
3. Finally, you have to [Send tables](#)^[39] to all the controllers to activate the user access rights.

Once you have finished editing the initial settings in Blocker and have sent the tables to the connected controller, you can start using the access control system on a regular basis. Access controllers record the user passage events and forward them to the Blocker program, where you can view the in the [View events](#)^[40] tab.

Using the access control system without an active connection with the Blocker program

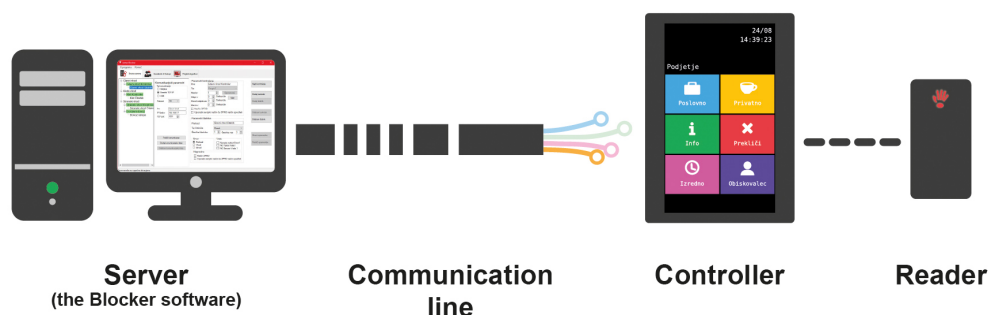
You can also use the access control system constructed with the Blocker program without an active connection to the program. Access controllers can operate completely independently, as they store the users' access rights in their local memory. This way, you don't need to keep your controllers connected to Blocker, and you don't need a computer (or server) that is always turned on. You only need to reconnect Blocker to devices when you want to add a new user or delete a specific user, and when you want to change user access rights.

The disadvantage of using an access control system this way is that you do not receive up-to-date data on user events. Events recorded by controllers can be retrieved the next time you connect the hardware to Blocker, as controllers store data in their local memory, but controllers can only store a limited amount of events (when they reach the maximum number of events, they delete the oldest events). Such use of an access control system does not guarantee the acquisition of all user events.

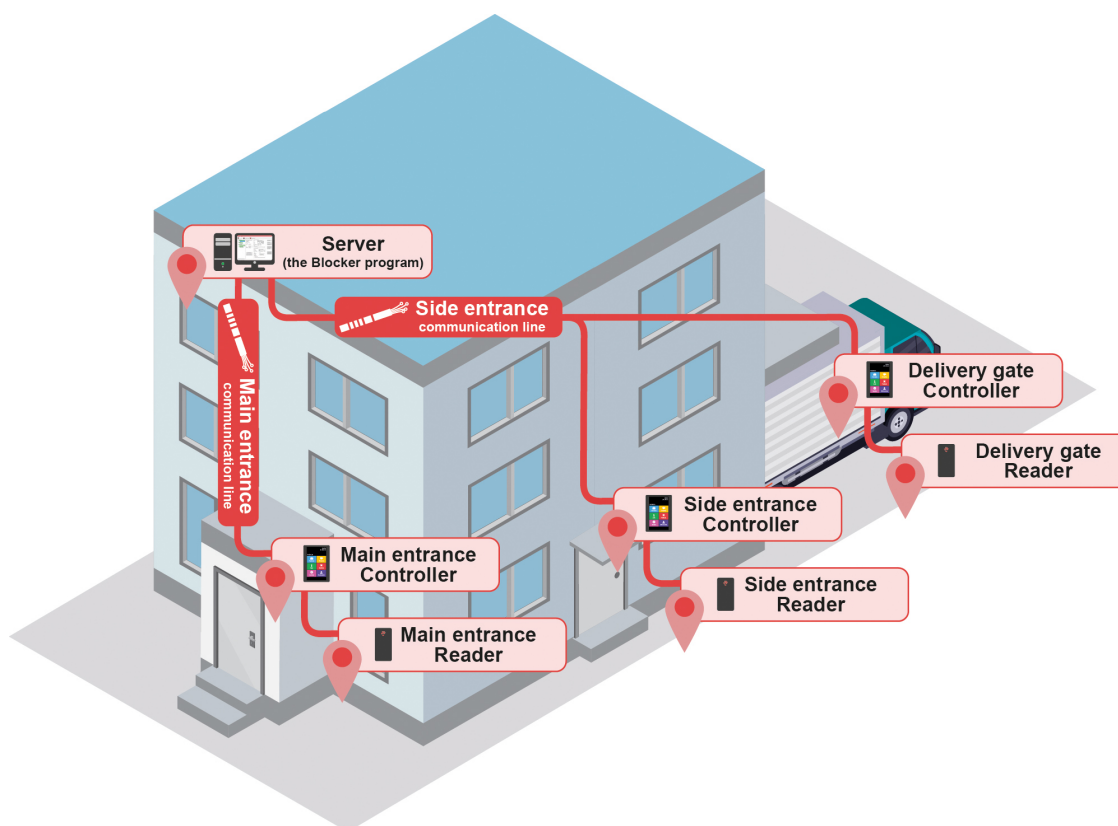
5 Hardware setup

In the *Hardware setup* tab, you can edit the communication and add controllers and readers to the Blocker system. You can also adjust the hardware settings here.

Each *Jantar* access control system consists of three hardware components: a communication line, a controller, and a reader. A communication line leads to each controller in the access control system. A controller can then either already contain a card reader in its own housing, or a separate card reader can be connected to the controller.

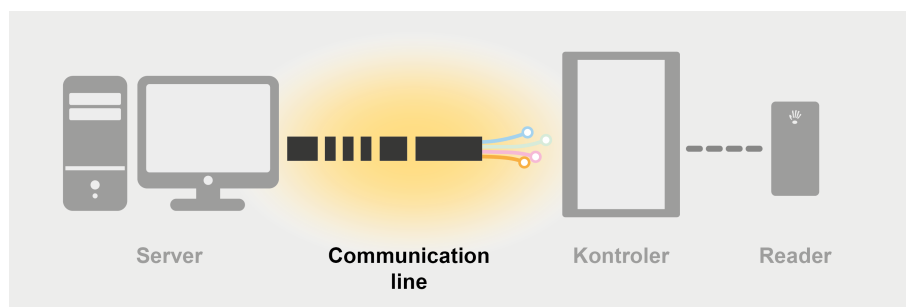


Each communication line can connect several different controllers and several card readers can be connected to each controller. (The latest version of the program, Blocker 9.0.5.38, now also allows multiple communication lines to be connected to the same system.)



5.1 Adding communication lines

The *communication line* (leading to controllers) is the first necessary component of a hardware (device) entry in Blocker.

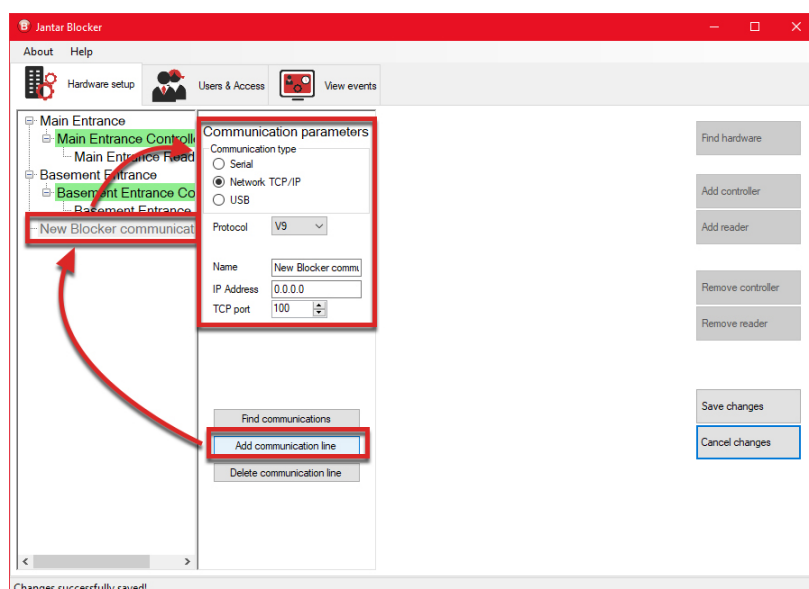


5.1.1 Manually adding communication lines

1. To manually add a communication line, first, click the *Add communication line* button.

The entry fields for setting the communication line will be enabled and a new entry will be added to the list of hardware on the left.

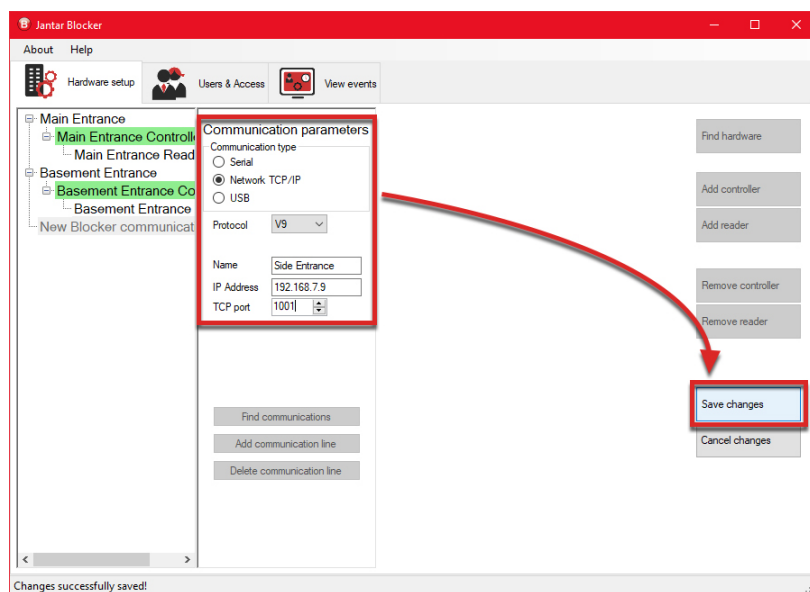
2. Set the appropriate settings for the communication line.



Communication type	The communication type setting. You can choose between: <ul style="list-style-type: none"> - Serial - a serial communication line connects the hardware devices with the server by using a COM port connection. This type of communication line is used also to connect devices via USB connector to the server. - Network TCP/IP - an IP communication line, using the TCP communication protocol. - USB - a communication line that connects devices to the server using a USB interface is only designed to connect older Jantar devices (which still use the FTDI chip).
Protocol	The communication protocol of Jantar devices used to communicate with software. Newer Jantar devices use the <i>V9 protocol</i> , while the <i>V7 protocol</i> is only used by older devices and thus only recommended for older existing access control systems.
Name	A custom name for the communication line.
IP Address ¹	The IP address of the communication line. ¹ This setting is only available, if the <i>Network TCP/IP communication type</i> is selected.
TCP port ¹	The TCP port through which devices connected to this communication line will communicate. ¹ This setting is only available if the <i>Network TCP/IP communication type</i> is selected.
Serial port ²	The name of the virtual COM port to which the communication line is connected. ² This setting is only available if the <i>Serial communication type</i> is selected.

USB id ³ The number of the USB serial port (only used for older Jantar devices).
³ This setting is only available if the *USB communication type* is selected.

3. When you are done, click *Save changes*.

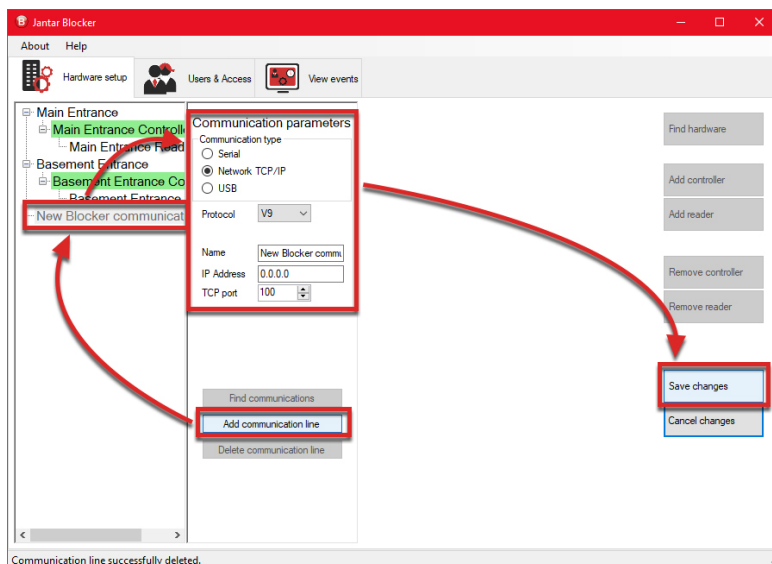


5.1.2 Automatically adding communication lines

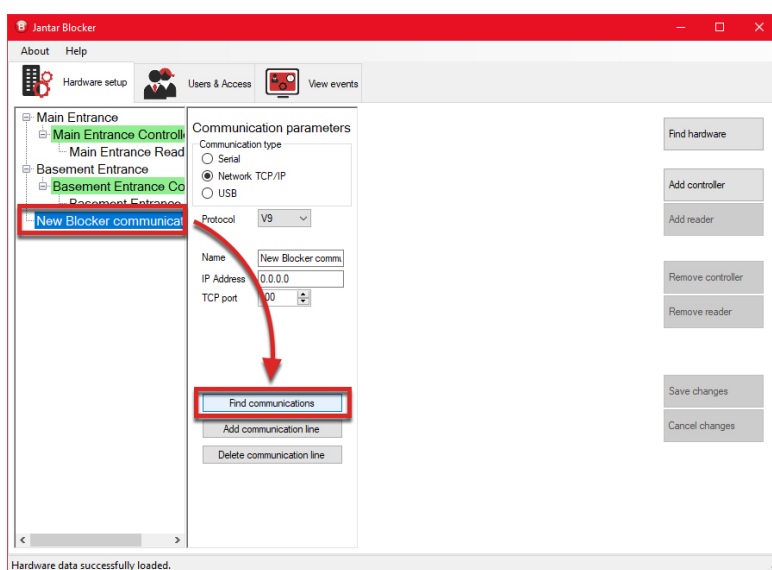
1. To add a communication line automatically, first, click the *Add communication line* button.

The entry form for the communication line settings will be enabled, and, a new record will be added to the hardware list on the left.

Click *Save changes*.

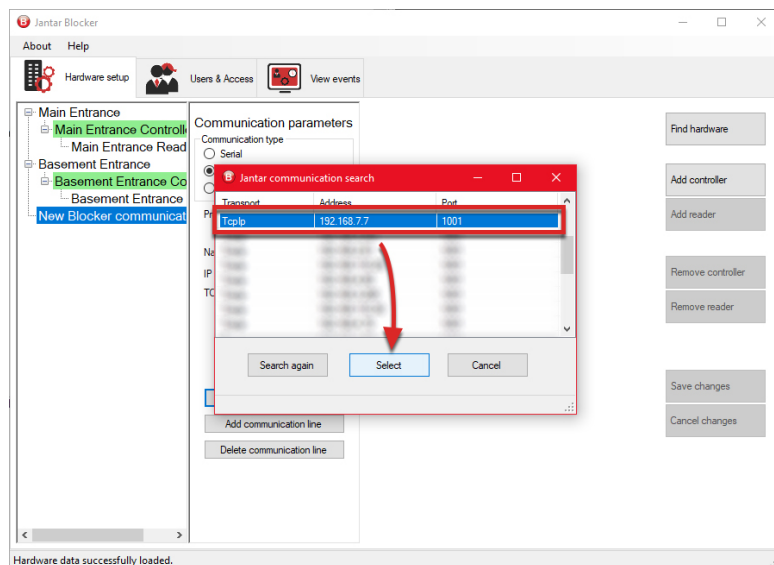


2. Then, mark the newly added communication line on the list on the left, and, click the *Find communication* button.



3. A new window will open showing all found communication lines leading to Jantar devices in the local network.

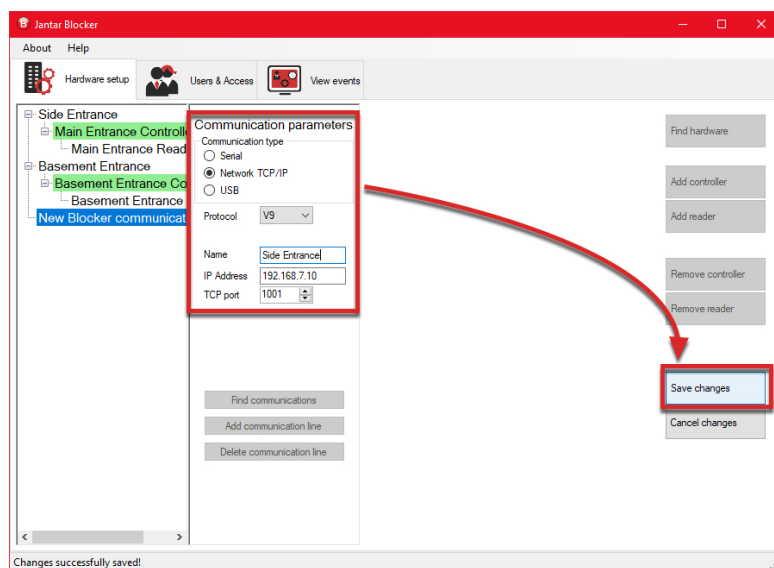
Highlight the appropriate communication line and click *Select*.



4. The new communication line will be added to the list on the left.

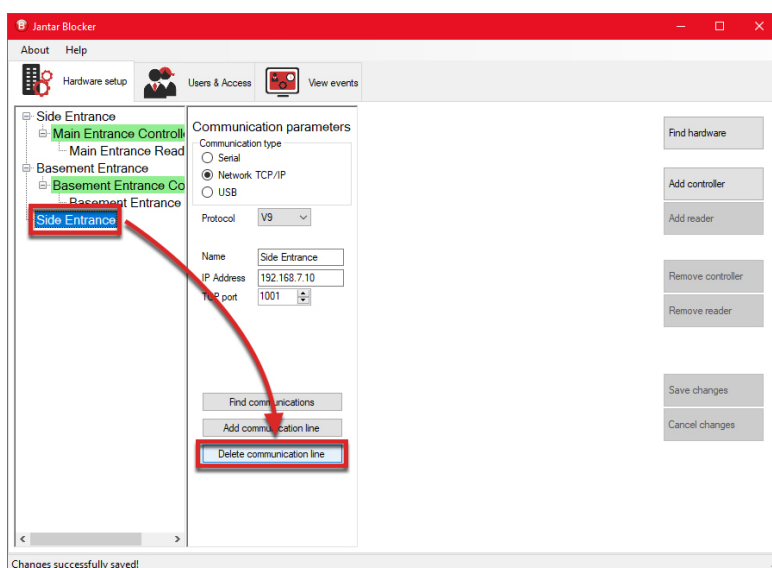
5. To edit the settings of the new communication line, mark the communication line on the list again, and, edit its settings.

6. Finally, click *Save changes*.

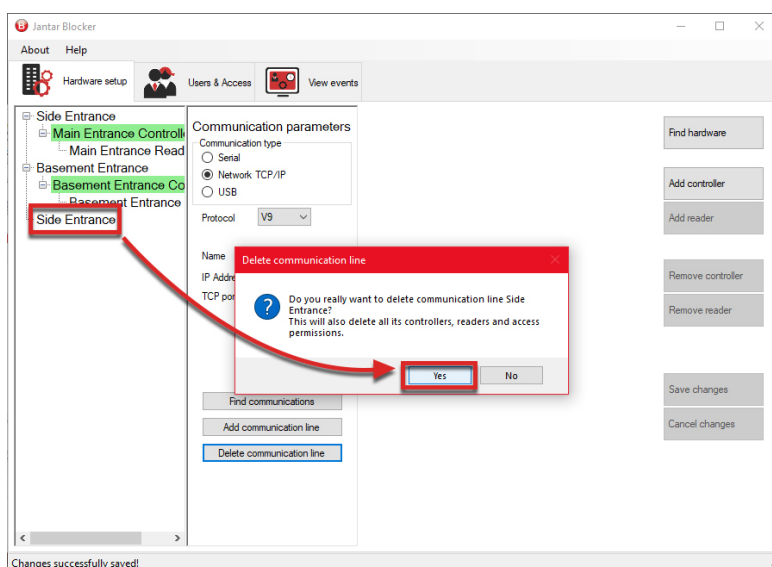


5.1.3 Remove communication line

1. To delete a communication line, first, mark the communication line on the list of hardware. Then click the *Delete communication line* button.



2. A pop-up window will appear warning you that you are about to delete a communication line and all controllers and readers connected to it. Click *Yes* to permanently delete the communication line.

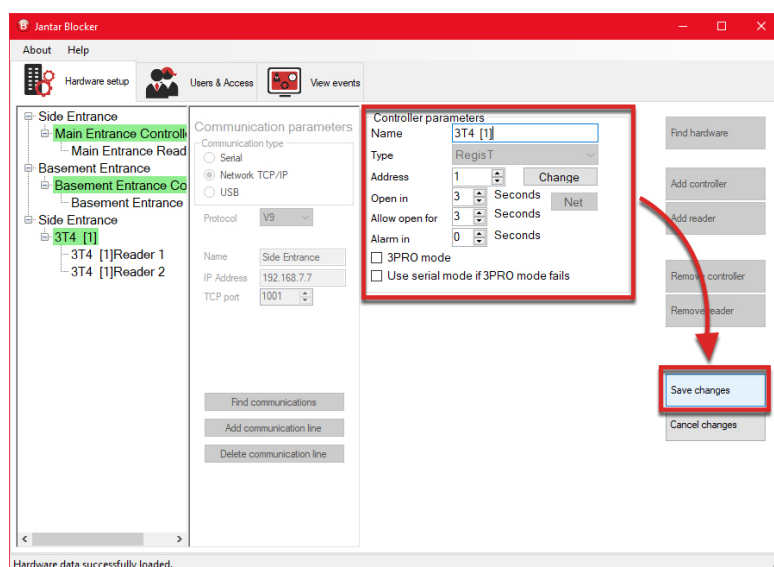


3. The communication line will be removed from the Blocker program.

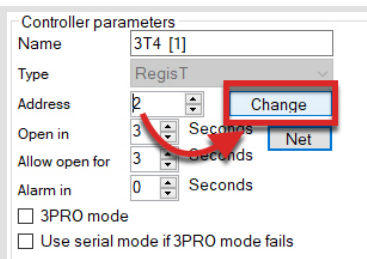
3. The controller will be added to the list of hardware along with the readers connected to it.

* You can read more about editing readers in chapter [Adding readers](#) ²⁵.

4. Click on the controller to show and enable the entry fields for the controller settings.



Name	A custom name for the controller.
Type	The type of controller.
Address	<p>The controller's address is one of the key settings of controllers, as it defines the address through which the controller communicates with the software. To change the controller address set a new value in the settings field and click <i>Change</i>.</p> <div data-bbox="300 1115 1031 1541" data-label="Complex-Block"> <p>NOTE All controllers which are connected through the same communication line must be assigned unique addresses (on the communication line). This is because the Blocker software cannot communicate with controllers using the same address on the same communication line.</p> <p>NOTE The address of the controller (i.e. the numerical value between 1 and 249 or 255) must already be assigned to the controllers during the installation process itself. If you choose to manually add the controller, you must carefully record this device information. If you add the controller using the <i>Find hardware</i> function the program will automatically find and insert the correct controller address.</p> </div>
Open in	The time duration (in seconds) of the energy pulse when the door lock is unlocked.
Allow open for	The time period (in seconds) when the doors are allowed to be open before the pre-alarm or alarm is triggered.
Alarm in	The time period (in seconds) after which the alarm is triggered if the doors are still open.



Net

A link to the controller's network settings. By clicking on the *Net* button a pop-up window will open where you can change the controller's network settings.

IP Address	Controller IP address that specifically defines it within the local area network.
Netmask	The network mask of the subnet that the controller can access.
Gateway	The IP address of the router that allows IP packets to be exchanged to and from the local network.
DNS 1	Primary DNS server address.
DNS 2	Secondary DNS server address.
TCP Port	TCP port through which the controller will communicate with the software.
Net timeout	The setting determines how long (in minutes) after a sudden or unwanted interruption of communication with the client, the device releases a communication port (port) so that another or the same client (e.g. server) can reconnect to it. (Example: A sudden disconnect of a cable somewhere on the network.)
Enable net	Setting for some older Jantar devices with firmware versions 9.5.1 and older.

3PRO mode

If this setting is enabled, the controller will not read the card's default serial number, but will instead search for an encrypted card number located within the card's internal memory. If this 3PRO setting is enabled on a controller, you must also enable it on all the readers connected to this controller.

Use serial mode if 3PRO mode fails

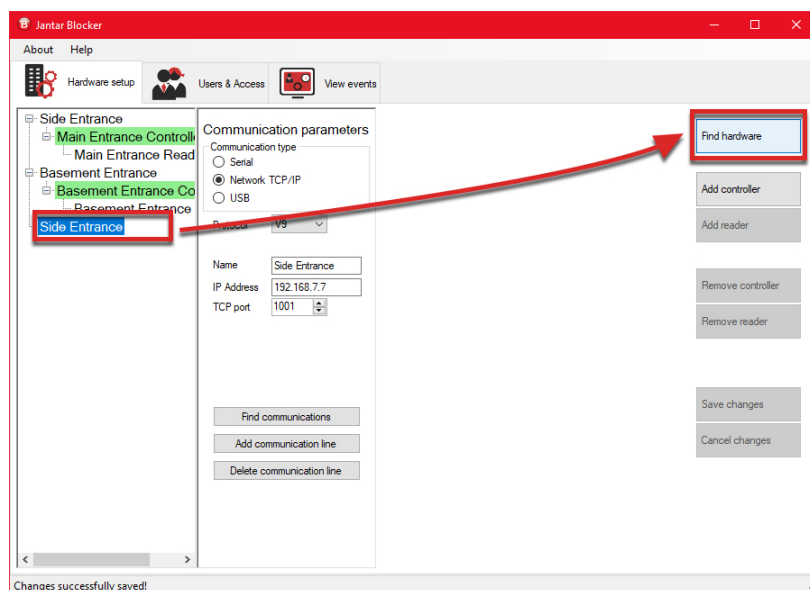
This setting can only be used if the previous setting *3PRO mode* is also enabled. If this setting is enabled, the controller will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.

5. When you are done with editing the controller settings, click *Save changes*.

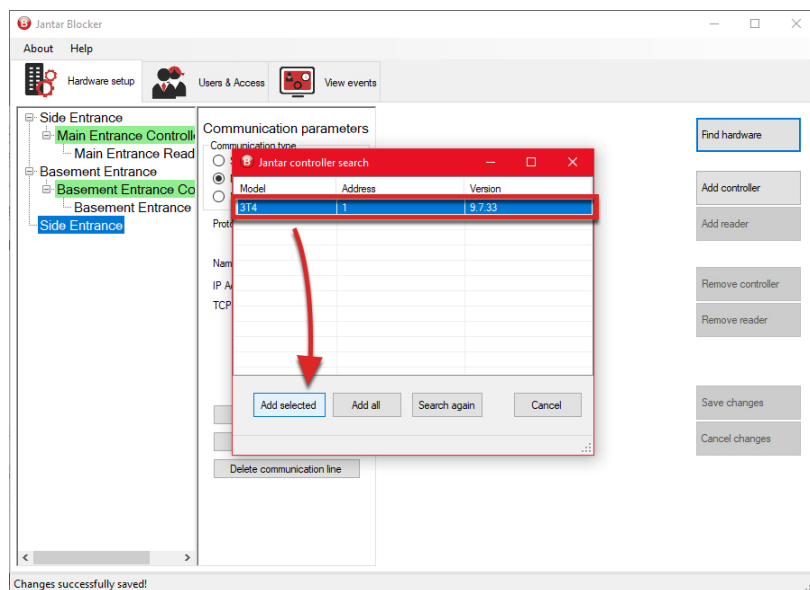
5.2.2 Manually adding controllers

1. To manually add a controller, first, select the communication line to which you want to add a new controller on the list of hardware.

Then, click *Add controller*.



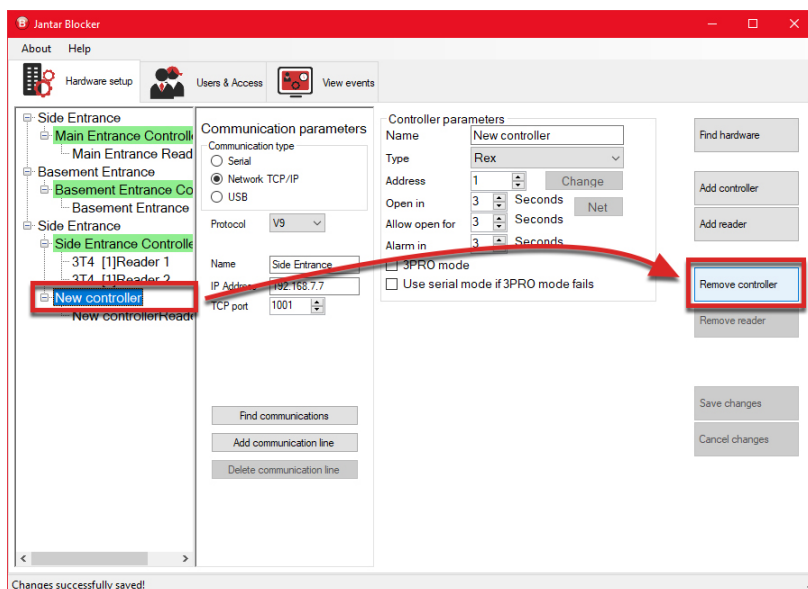
2. A new controller will be added to the hardware list under the selected communication line and the fields for editing the controller settings will be enabled.



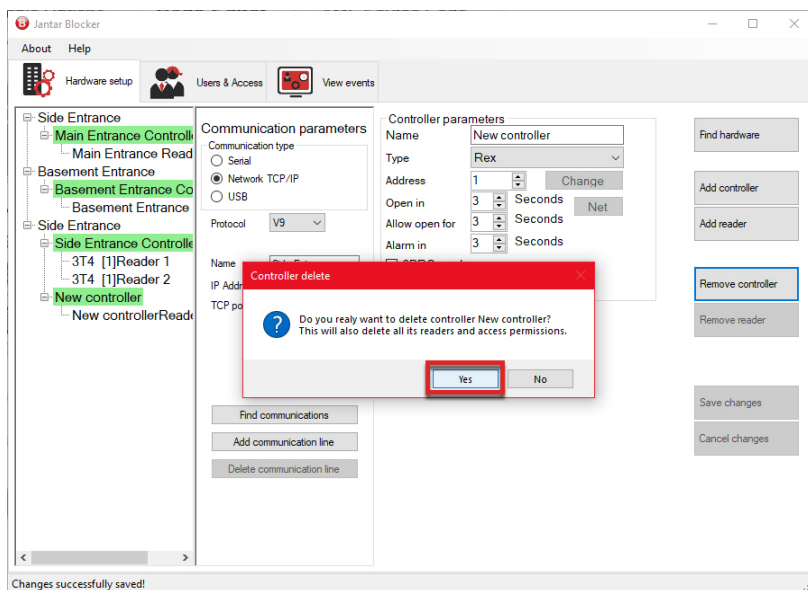
3. When you have finished editing the controller settings, click *Save changes*.

5.2.3 Remove controller

1. To delete a controller, first, mark the controller on the list of hardware. Then click the *Remove controller* button.



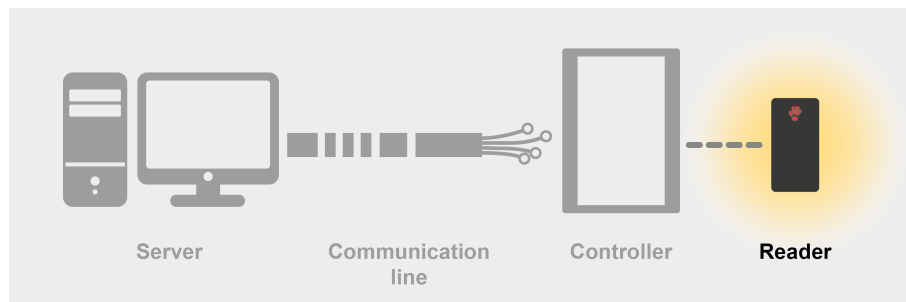
2. A pop-up window will appear warning you that you are about to delete a controller and all readers connected to it. Click *Yes* to permanently delete the controller.



3. The controller will be removed from the Blocker program.

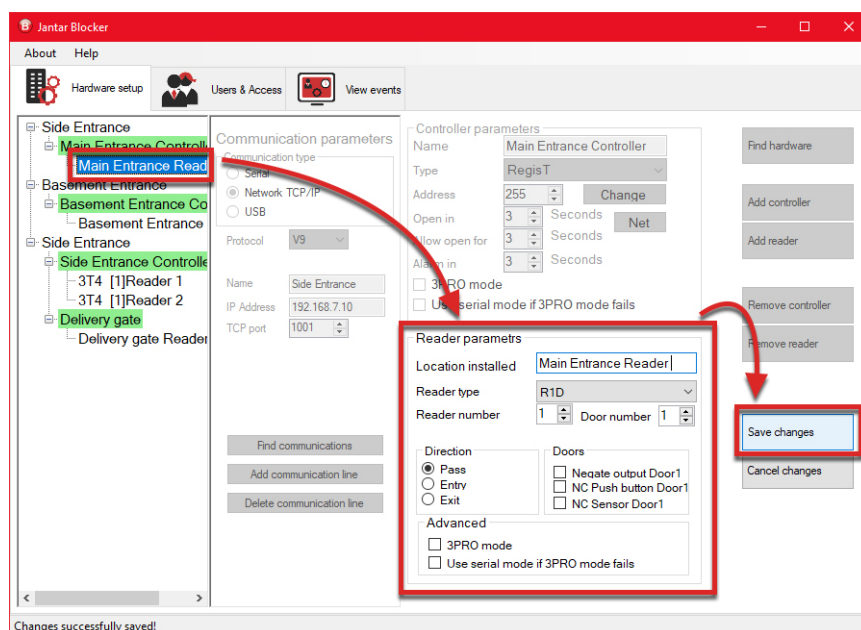
5.3 Adding readers

The *Reader* is the third component of a hardware (device) entry in Blocker.



5.3.1 Automatically adding readers

1. Readers are automatically added to the system along with the controller they are connected to. When [adding a controller](#) the readers linked to it will also appear on the list of hardware.
2. To edit a reader, first, select the appropriate reader from the hardware list. Clicking on the reader will display and enable the fields for editing reader settings.



Location installed	A custom name for the reader.
Reader type	The type of reader.
Reader number	The sequential number of the reader of the controller. The number of readers that can be connected to a controller differs depending on the <i>type of controller</i> . All readers connected to the same controller must have a different reader number assigned.
Door number	The number of the output on the controller that will be activated upon registration on the reader (i.e. which door will open).
Direction	<p>This setting defines the direction of the reader at the passage. You can choose between the following values:</p> <ul style="list-style-type: none"> - <i>Passage</i> - the users can freely move through the passage, regardless of the direction. - <i>Entry</i> - by registering at the reader the users record that they are entering the room (i.e. they register an <i>Entry</i> event). - <i>Exit</i> - by registering at the reader the users record that they are leaving the room (i.e. they register an <i>Exit</i> event). <p>The setting is used to monitor the presence in the room and when using the anti pass-back function.</p>

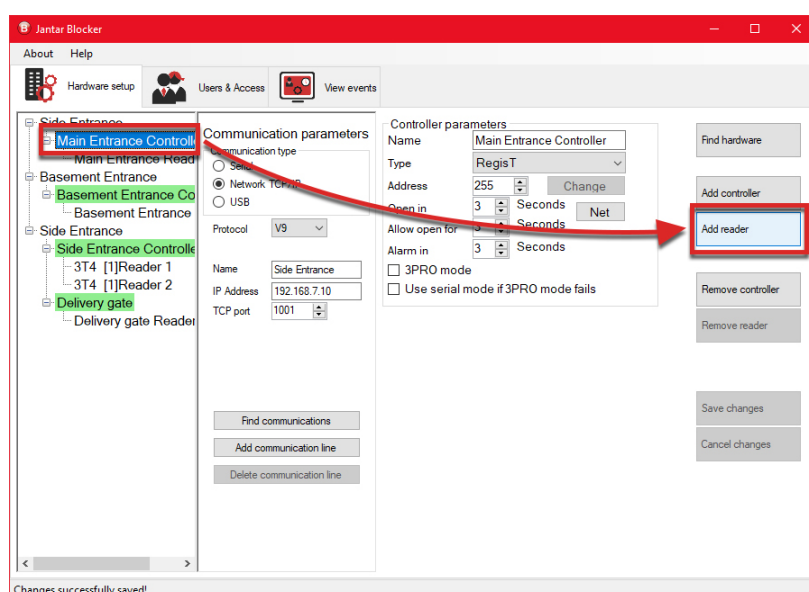
Doors	Additional reader settings for opening doors.	
	Negate output Door 1	Enable this setting, if you are using such a device (e.g. a magnet or door strike) on a particular controller output that needs energy (a pulse) in the closed (locked) state, and requires the energy to be cut to open the door.
	NC Push button 1	Enable this setting, if you are using a push button sensor that has a closed contact when in idle mode.
	NC Sensor Door 1	Enable this setting, if you are using a door sensor that has a closed contact when in idle mode (when the doors are closed).
Advanced	Advanced reader settings.	
	3PRO mode	If this setting is enabled, the reader will read the encrypted 3PRO card number located within the card's internal memory. This setting must be enabled for all readers connected to a controller using the 3PRO functionality.
	Use serial mode if 3PRO mode fails	This setting can only be used if the previous setting <i>3PRO mode</i> is also enabled. If this setting is enabled, the reader will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.

3. When you are done with editing the reader settings, click *Save changes*.

5.3.2 Manually adding readers

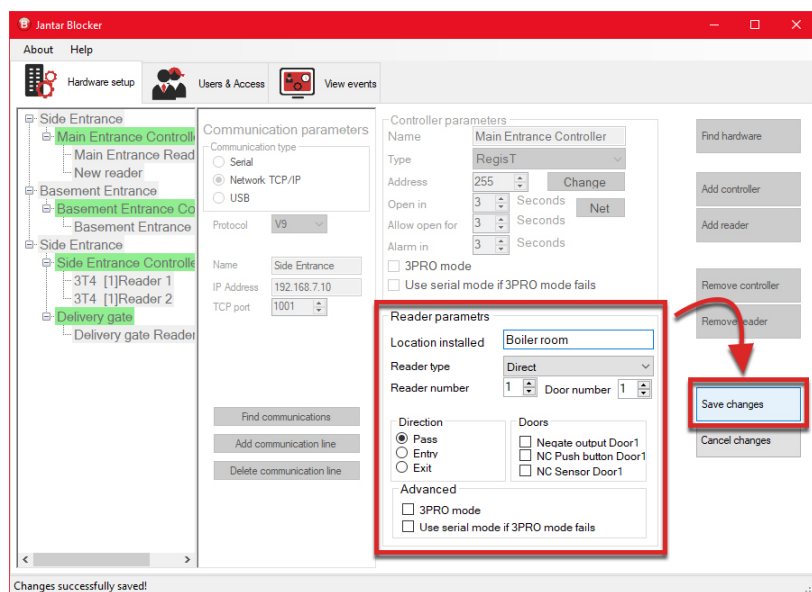
1. To manually add a reader, first, select the controller to which you want to add a new reader on the list of hardware.

Then, click *Add reader*.

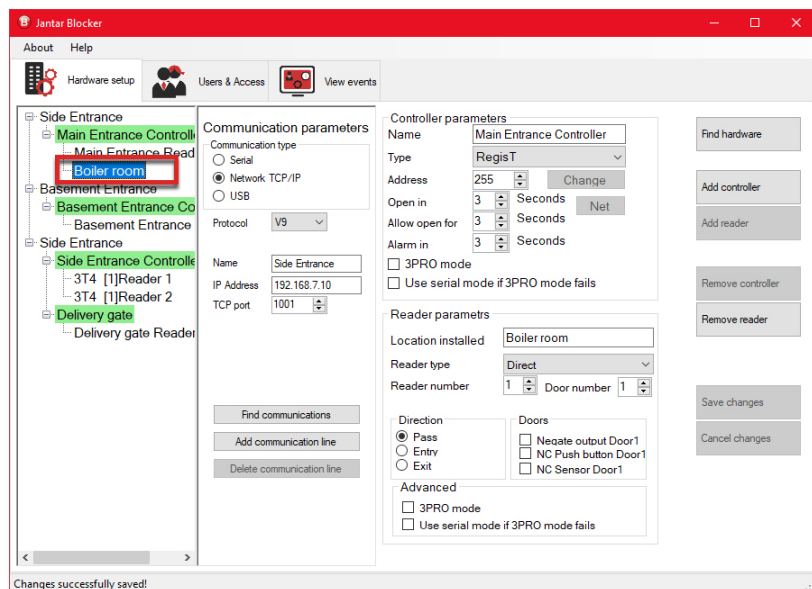


2. A new reader will be added to the hardware list under the selected controller and the fields for editing the reader settings will be enabled.

3. When you have finished editing the reader settings, click *Save changes*.

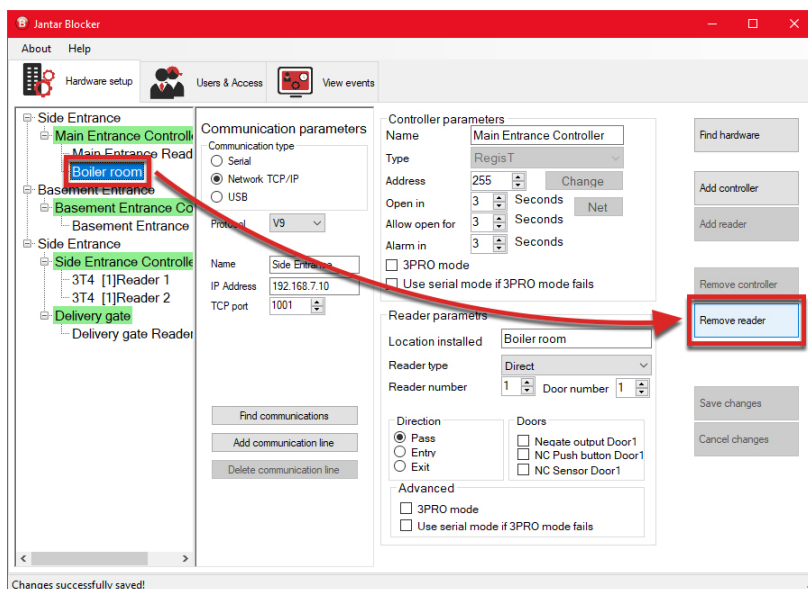


4. A new reader will be added to the list of hardware.

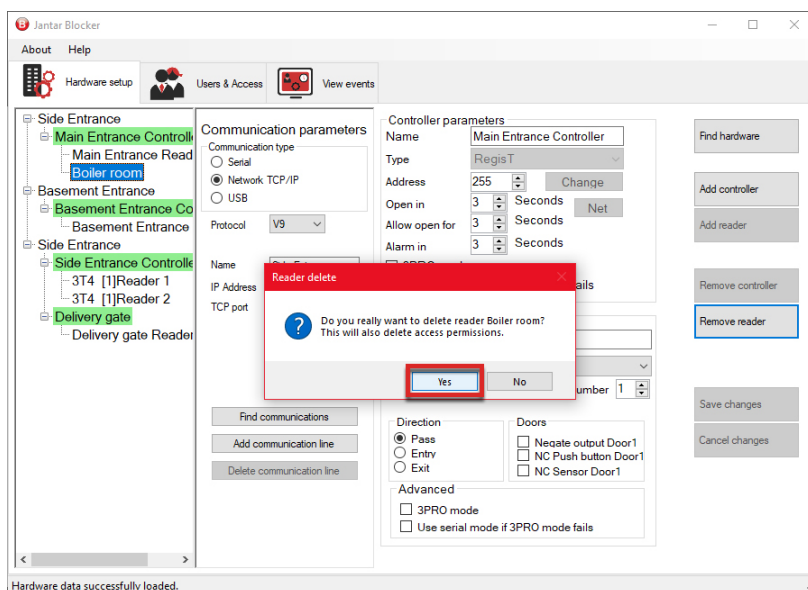


5.3.3 Remove reader

1. To delete a reader, first, mark the reader on the list of hardware. Then click the *Remove reader* button.



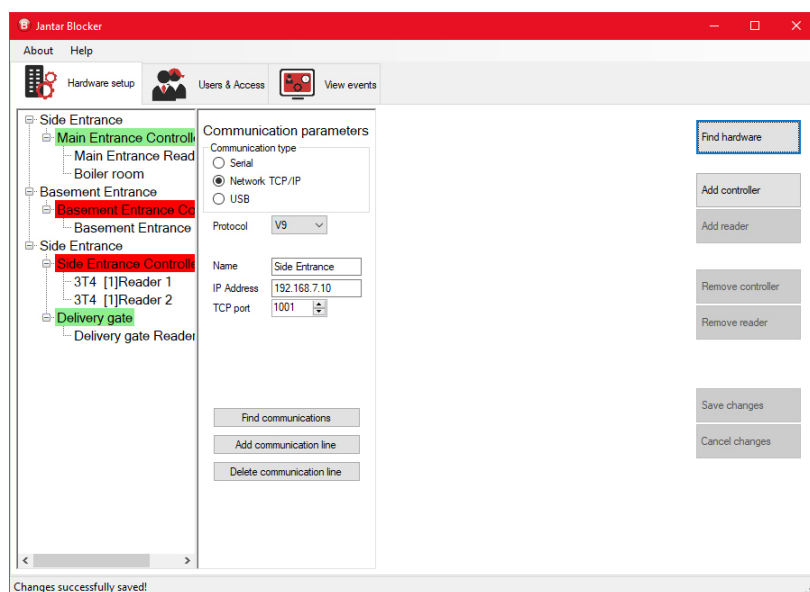
2. A pop-up window will appear warning you that you are about to delete a reader. Click *Yes* to permanently delete the reader.



3. The reader will be removed from the Blocker program.

5.4 Status of communication

In the list of hardware, the background color of the controller indicates the status of communication with the controller:

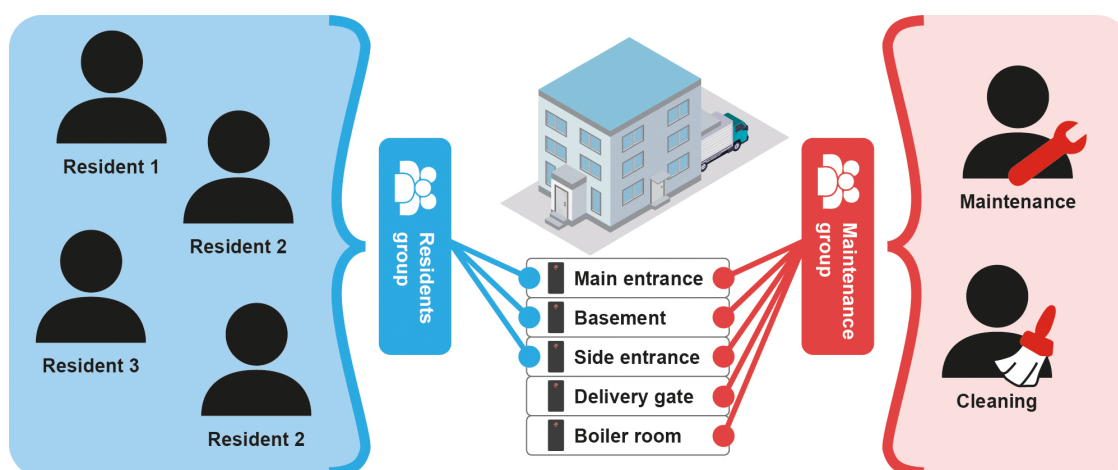


- if communication with the controller is operating normally, the background of the controller will be colored green;
- if communication with the controller is not established, the background of the controller will be colored red.

6 Users & Accesses

In the *Users & Access* tab, you can add and edit groups and users, assign user cards to users, and assign access rights to groups.

In Blocker, access rights at certain locations are assigned at the group level. Users can therefore only access locations that are allowed to them through the group to which they belong. Each user can only belong to one group, but each group can have an unlimited number of access rights. Only one identification means (a card, tag or PIN code, etc.) can be assigned to each user, which allows him to pass at locations.

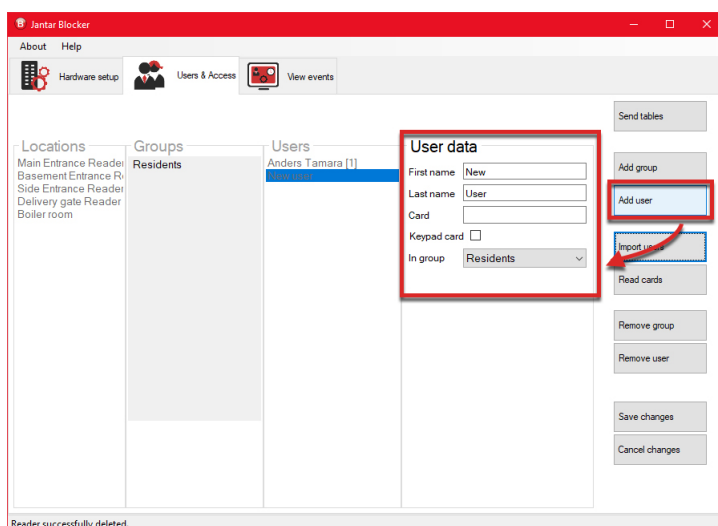


6.1 Adding users

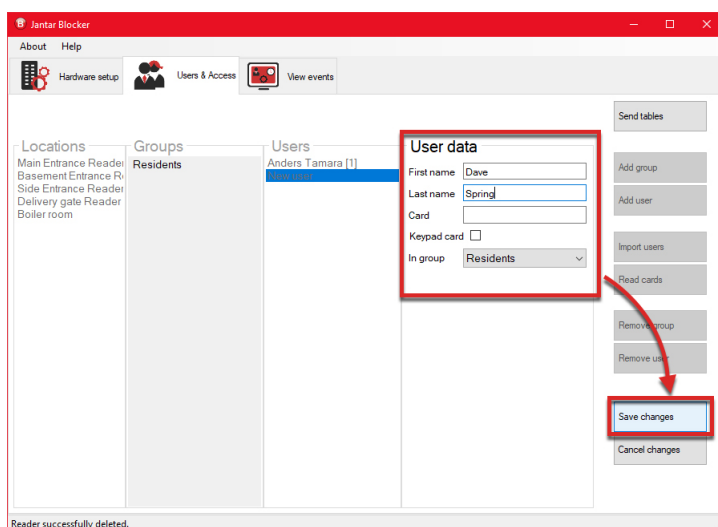
You can [add users to Blocker manually](#)^[31] or [import them into the program in bulk using a specially prepared file](#)^[32].

6.1.1 Manually adding users

1. To manually add a user click the *Add user* button.
2. The entry fields for adding a new user will be enabled.



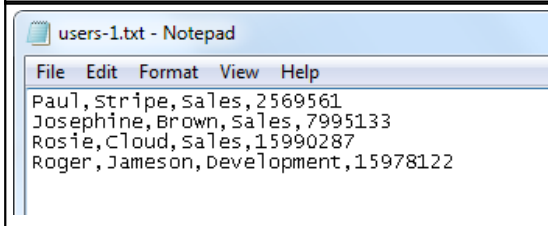
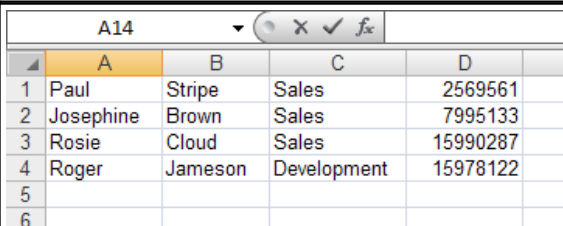
3. Enter the desired data about the user and click *Save changes* when you are done.



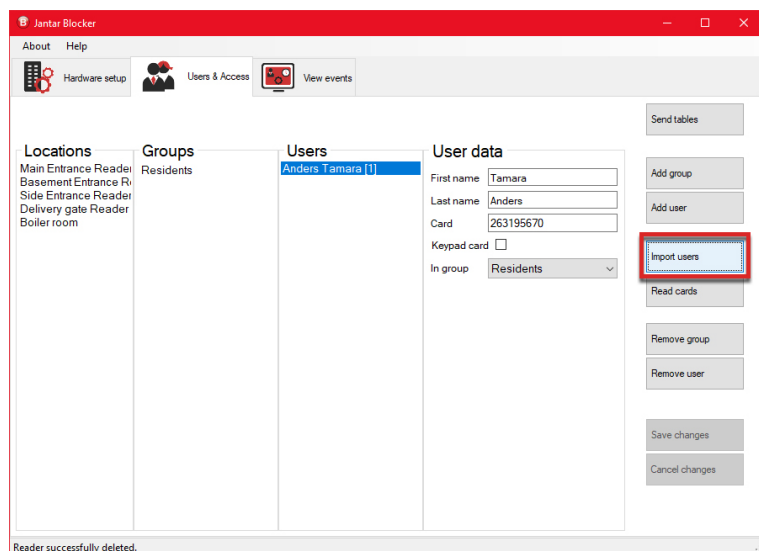
First name	The user's first name.
Last name	The user's last name.
Card	The number of the card (or another means of identification) issued to the user that enables them access at different locations. You can enter the card number manually or use the Read cards ^[33] function, which allows you to assign a card by reading the cards on a specified reader. When using the <i>Keypad card</i> *function, which allows access to locations by entering a numeric code on the reader's keyboard, enter the assigned number code in this field.
Keypad card*	If this setting is enabled, the user will have to type a numeric code on the reader's keyboard to pass through at locations. The numeric code is entered in the <i>Card</i> setting field.
In group	The group to which the user is assigned and through which they are granted access rights at specific locations.

6.1.2 Import users

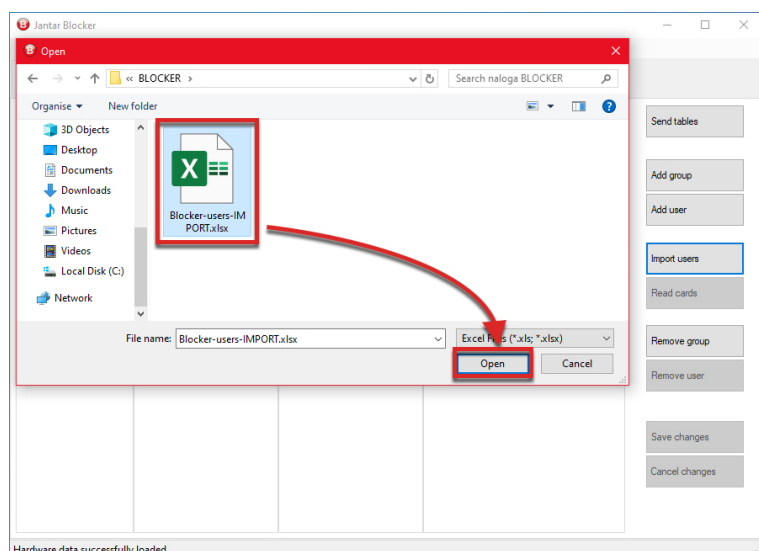
To import users into the Blocker program, you first need a specifically prepared file containing the necessary user information. You can prepare a *.csv text file* or an *.xlsx Excel spreadsheet*.

<p>CSV text file</p> <p>The file must contain four types of data about every user. The data must be separated by commas and must be listed in the following order:</p> <ul style="list-style-type: none">1 - Name2 - Last name3 - Group4 - Card number	<p>Excel spreadsheet</p> <p>The file must contain four types of data about every user. Each data type must be entered in a separate column of the spreadsheet and must be listed in the following order:</p> <ul style="list-style-type: none">1 - Name2 - Last name3 - Group4 - Card number																																			
 <pre>Paul,Stripe,Sales,2569561 Josephine,Brown,Sales,7995133 Rosie,Cloud,Sales,15990287 Roger,Jameson,Development,15978122</pre>	 <table><tr><th></th><th>A</th><th>B</th><th>C</th><th>D</th></tr><tr><td>1</td><td>Paul</td><td>Stripe</td><td>Sales</td><td>2569561</td></tr><tr><td>2</td><td>Josephine</td><td>Brown</td><td>Sales</td><td>7995133</td></tr><tr><td>3</td><td>Rosie</td><td>Cloud</td><td>Sales</td><td>15990287</td></tr><tr><td>4</td><td>Roger</td><td>Jameson</td><td>Development</td><td>15978122</td></tr><tr><td>5</td><td></td><td></td><td></td><td></td></tr><tr><td>6</td><td></td><td></td><td></td><td></td></tr></table>		A	B	C	D	1	Paul	Stripe	Sales	2569561	2	Josephine	Brown	Sales	7995133	3	Rosie	Cloud	Sales	15990287	4	Roger	Jameson	Development	15978122	5					6				
	A	B	C	D																																
1	Paul	Stripe	Sales	2569561																																
2	Josephine	Brown	Sales	7995133																																
3	Rosie	Cloud	Sales	15990287																																
4	Roger	Jameson	Development	15978122																																
5																																				
6																																				

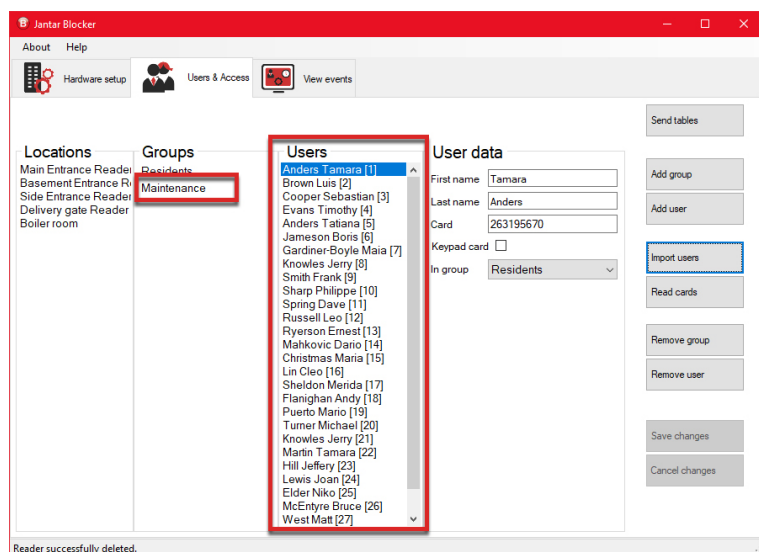
1. To import the prepared file, click the *Import users* button.



2. A new window for selecting a file to import will open. Select the file and click *Open*.



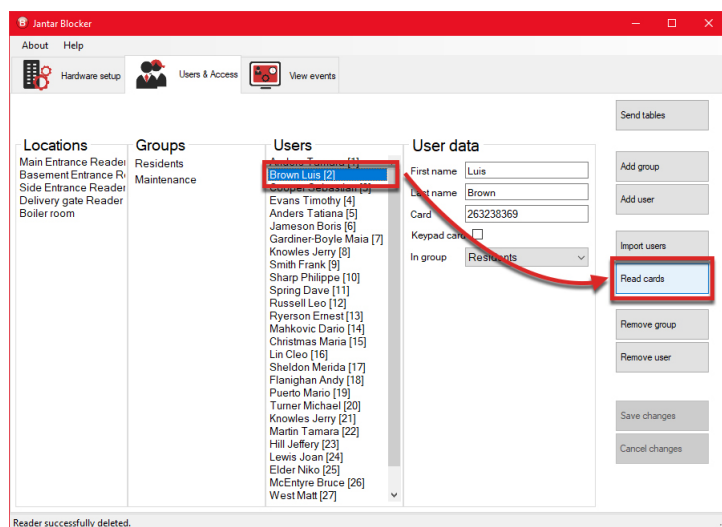
3. Users will be imported into Blocker. If a user is assigned a group that does not yet exist in Blocker, the program will automatically add it when importing the data.



6.1.3 Read cards

The *Read cards* function enables you to simply assign cards to users by reading the cards at a selected reader.

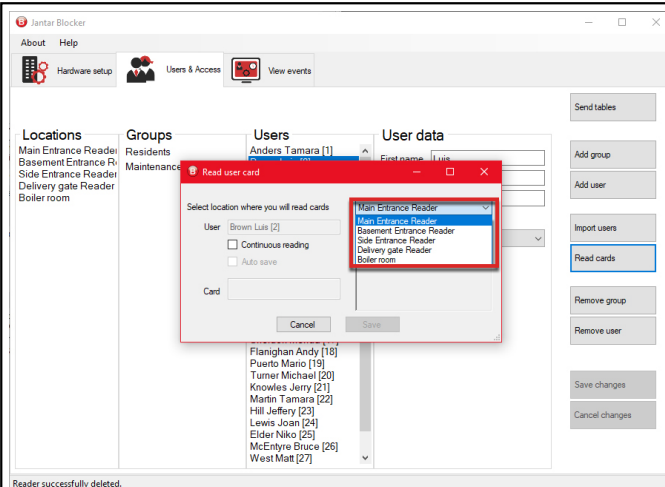
1. First, mark the user whom you wish to assign a card on the list of users.



2. Then, click the *Read cards* button.

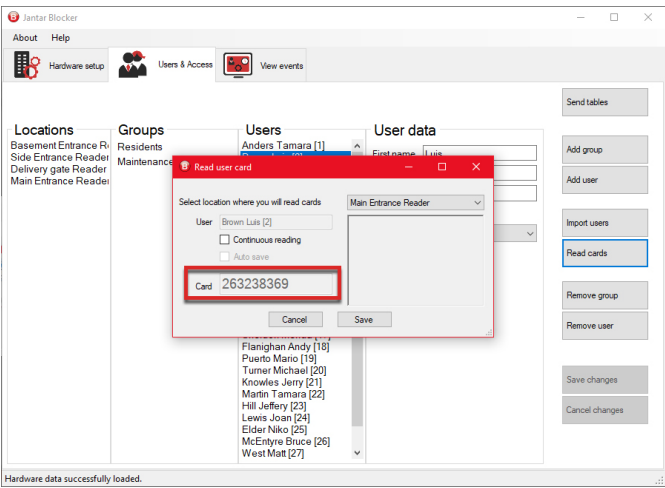
A new window will open.

3. In the new pop-up window, first, select the reader where you will read the card for the user.

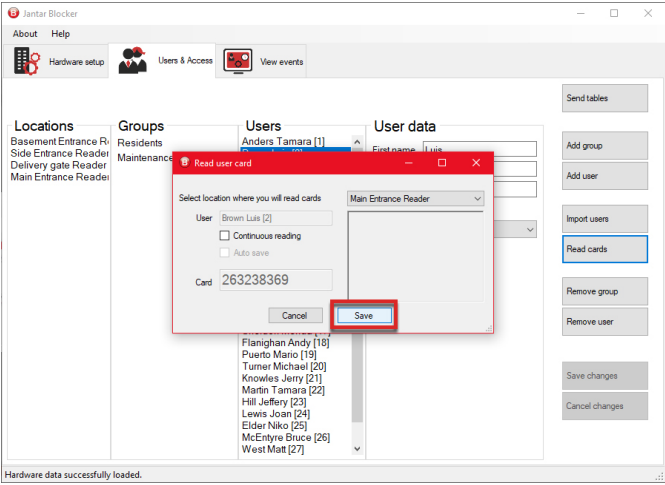


Select location where you will read cards	Select the location (reader) where you will read the card that you will assign to the user.
User	The name of the user to whom you will assign a card.
Continuous reading	If this setting is enabled, then the function of adding cards to multiple users in a row will be enabled.
Auto save	If the field is enabled, the program will save the entered cards automatically when using the function of adding cards to multiple users. If you are not using this function, you must click <i>Save</i> for each card entered.
Card	The number of the card that was read on the reader will be displayed in this field.
List of assigned cards and users	A list of all users who have already been assigned a card in this process.

4. Then put the card on the reader. When the reader reads the card the card's number will be displayed in the *Card* field.

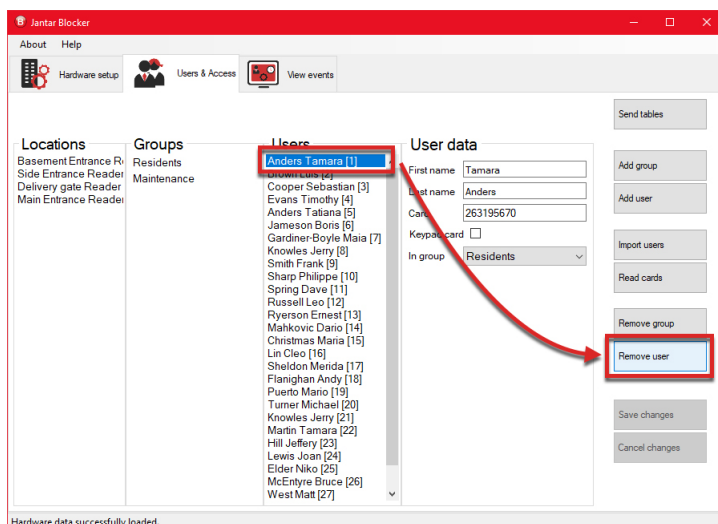


5. When you are done reading cards, click *Save*.

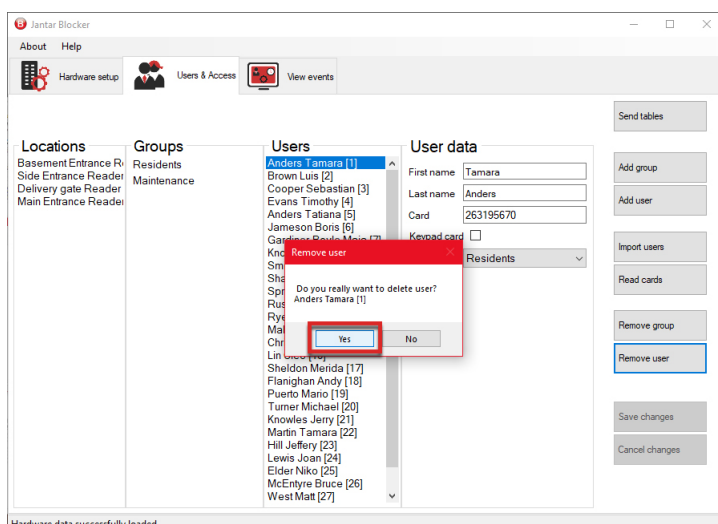


6.1.4 Remove user

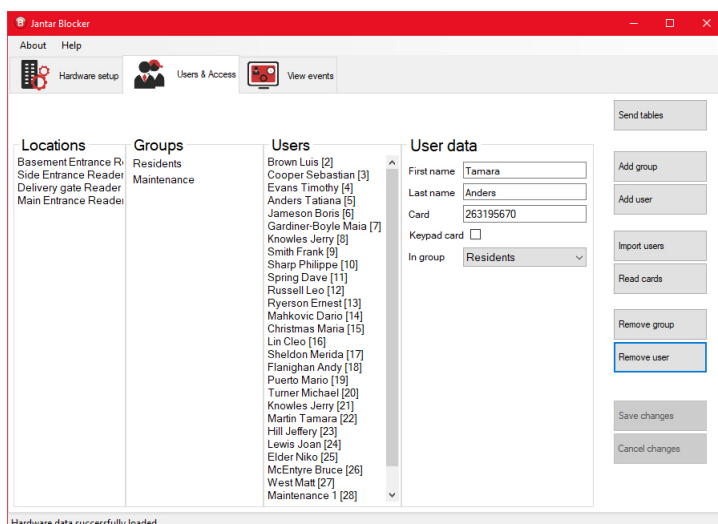
1. To delete a user, first, mark the user on the list of users.
Then click the *Remove user* button.



2. A pop-up window will appear warning you that you are about to delete a user.
Click *Yes* to permanently delete the user.



3. The user will be removed from the Blocker program.



6.2 Adding groups and organizing users into groups

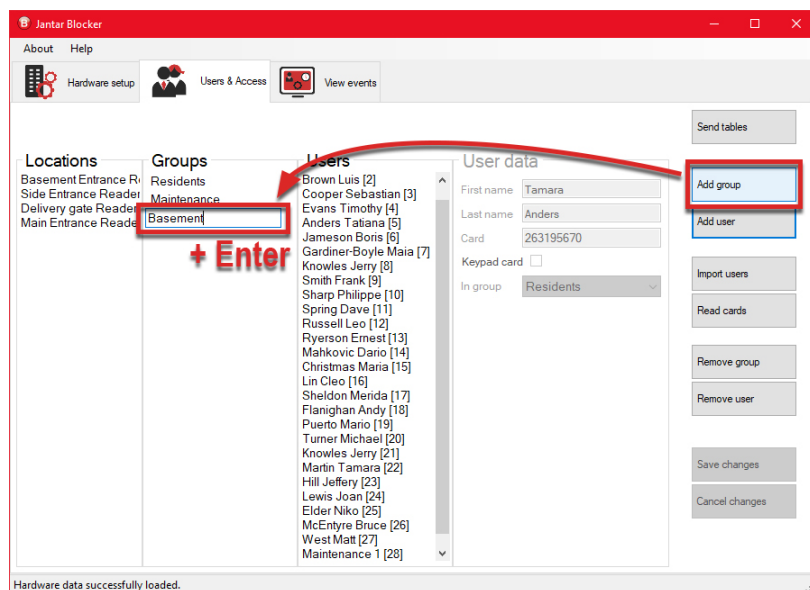
To define access rights in Blocker you must do so at the group level. A particular user can only be assigned to one group, but each group can have an unlimited number of access rights.

6.2.1 Add group

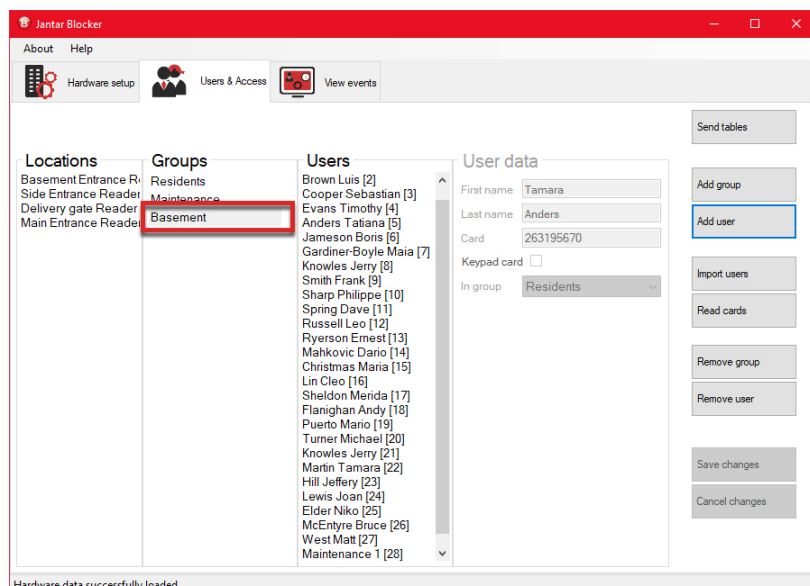
1. To add a new group to the system, click the *Add group* button.

2. A new field will be added to the list of groups.

Change the name of the new group, and, then click *Enter* on your keyboard.



3. A new group will be added to the Blocker program.

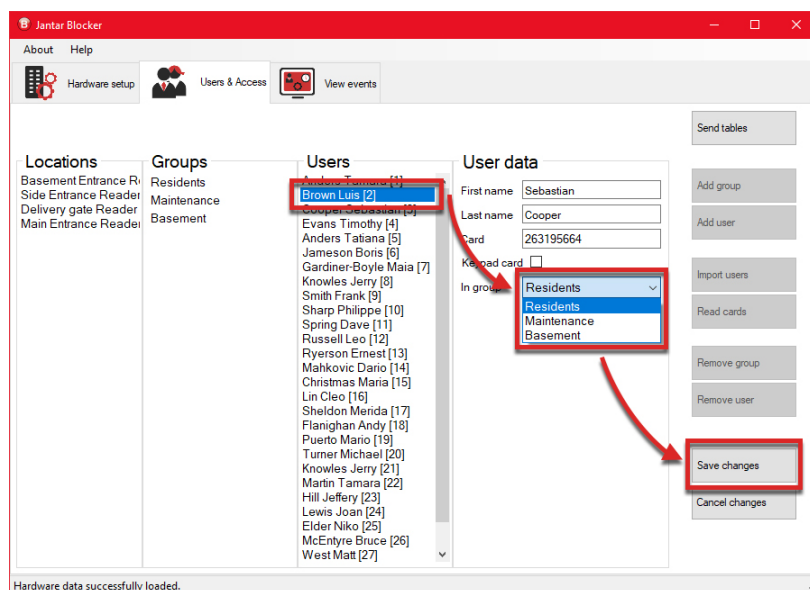


* A new group can also be created automatically when [importing users](#) ³² into the Blocker program.

6.2.2 Organizing users into groups

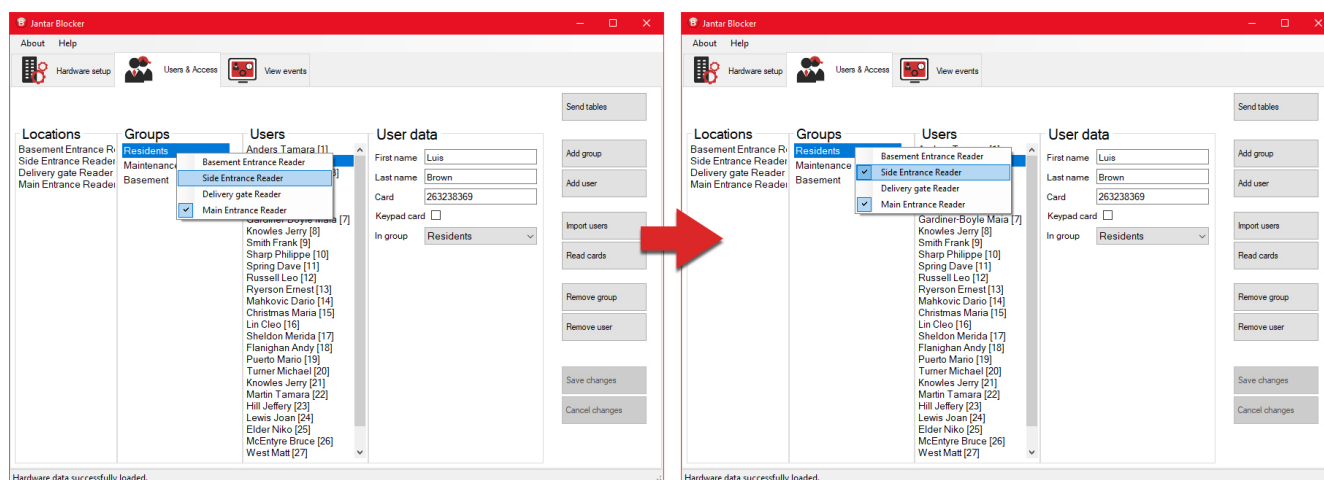
In Blocker, access rights at certain locations are assigned at the group level. Users can therefore only access locations that are allowed to them through the group to which they belong. Each user can only belong to one group, but each group can have an unlimited number of access rights.

1. To assign an individual user to an appropriate group, first, click on the user to enable the entry form fields for the user's information.
2. Then select the appropriate group under the *In group* setting in the entry form.
3. Finally, click *Save changes*.



6.2.3 Assigning access rights to groups

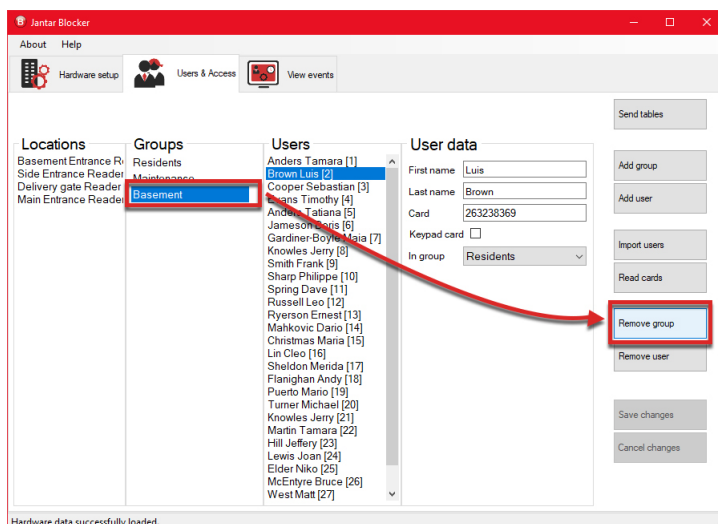
1. To add access rights to a group, first, mark the group in the list of groups and right-click it. A list of all locations (readers) will be displayed.
2. To grant access rights to a group at a specific location, click on the location. When the location is clicked, a checkmark will be added to it indicating that members of this group have the right to pass at this location.



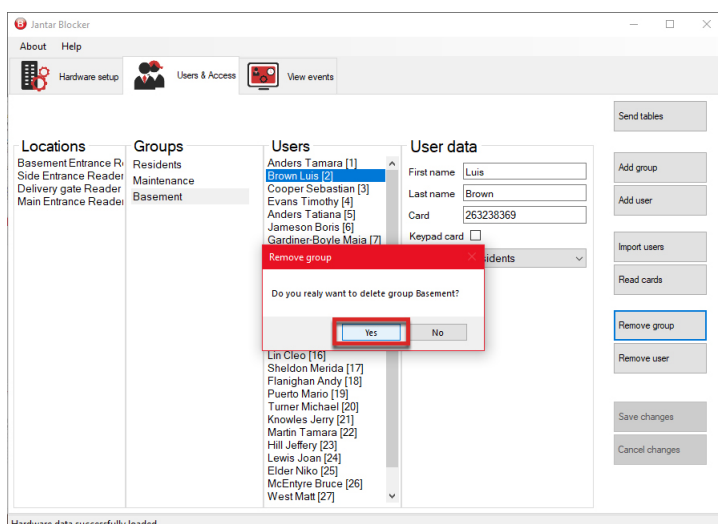
3. The changes you have made to access rights will be promptly automatically saved.

6.2.4 Remove group

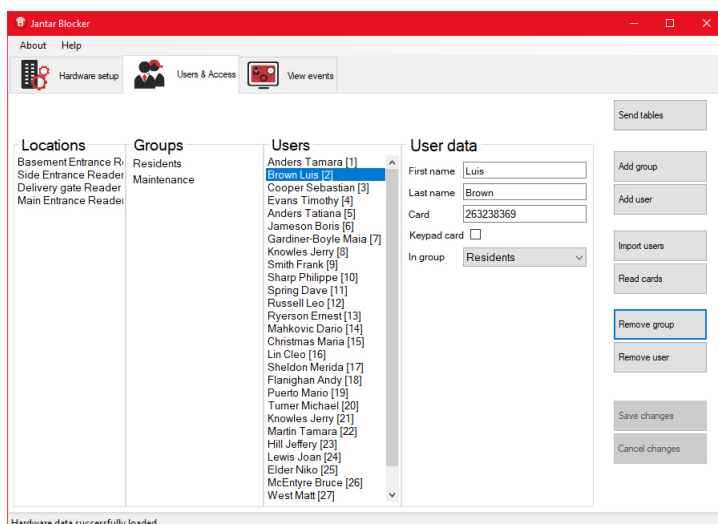
1. To delete a group, first, mark the group on the list of groups. Then click the *Remove group* button.



2. A pop-up window will appear warning you that you are about to delete a group. Click *Yes* to permanently delete the group.



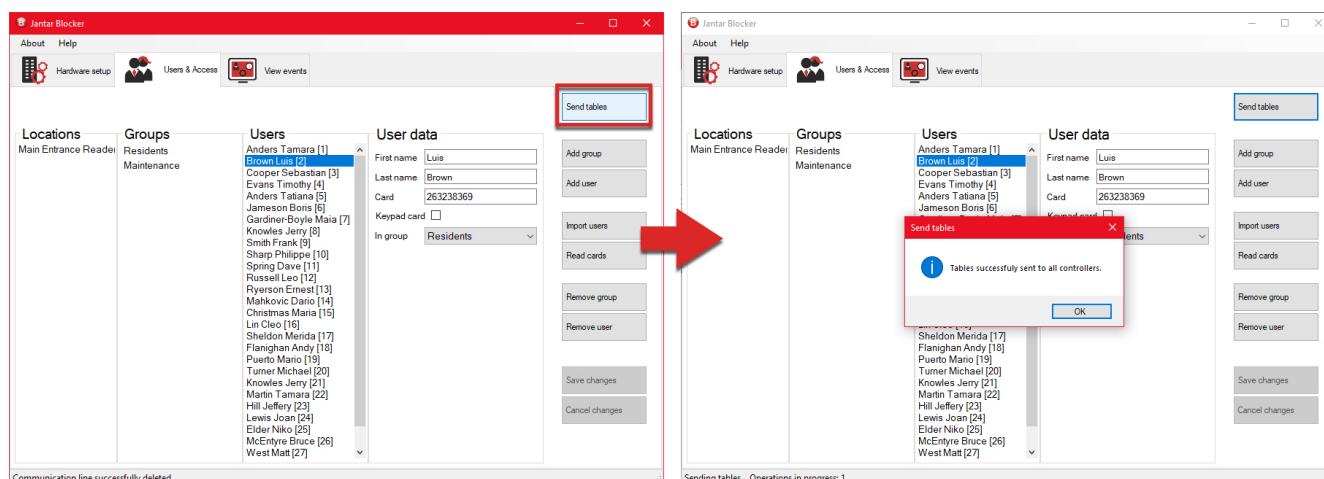
3. The group will be removed from the Blocker program.



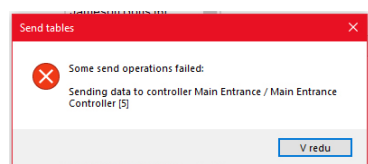
6.3 Send tables

Sending tables is the last step of the initial settings for the access control system. Using this action you will send the information about which users have access rights at individual locations to all controllers, which will then store this information in their local memories. You must send tables each time you change hardware settings, add or remove users and groups, and change group access rights.

Click the *Send tables* button to send tables to controllers. The system will start the process of sending tables, and, when it is complete, send display a message about the successful sending of tables.



If all controllers are not in use or do not have active communication, table sending will not be successful and the program will warn you with a notification.

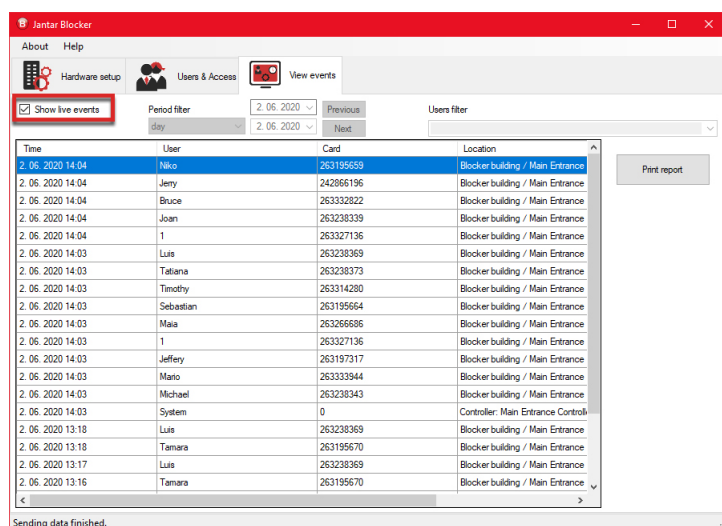


7 View Events

In the *View events* tab, you can view current user movements through different passages in your system, and you can also generate event reports.

7.1 Show live events

When the *Show live events* field is enabled, the *Event View* tab will display the current events that users are currently creating.

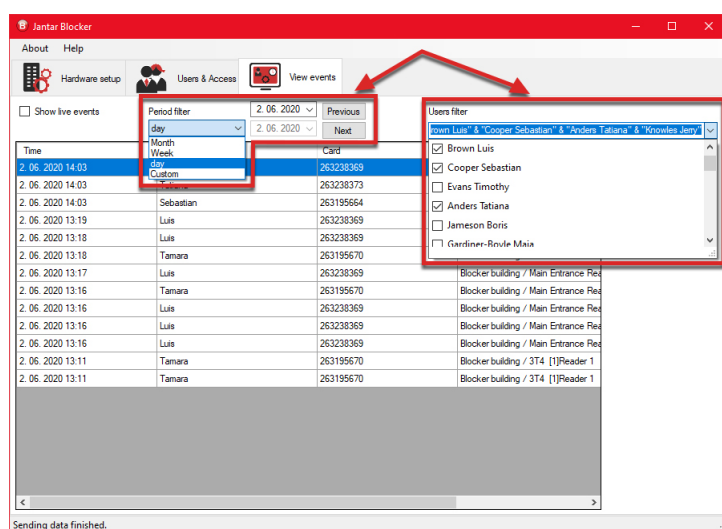


7.2 Event filtering

NOTE

Filtering options and the function of generating the report are only available when the *Show live events* option is turned off.

At the top of the tab, you can filter events by date or users.

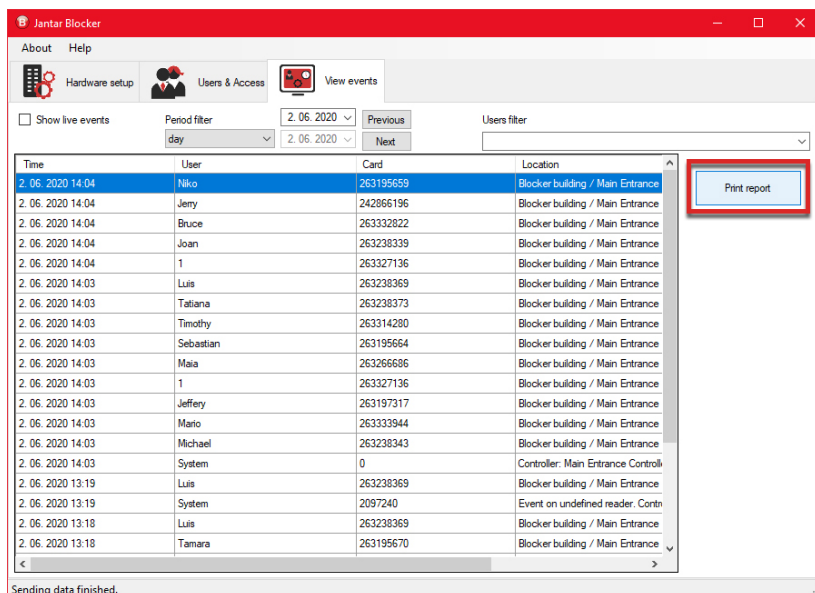


7.3 Print report


NOTE

Filtering options and the function of generating the report are only available when the *Show live events* option is turned off.

1. To create a report click the *Print report* button.



2. A PDF report will be generated containing all events, which are currently displayed in the *View events* tab.



Event report

User	Card	Passage	Date and time	Event	Button	Time&Attendance
Elder Niko	263195659	Blocker building / Main Entrance Reader	2. 06. 2020 14:04:14	Pass	0	
Knowles Jerry	242866196	Blocker building / Main Entrance Reader	2. 06. 2020 14:04:10	Pass	0	
McEntyre Bruce	263328222	Blocker building / Main Entrance Reader	2. 06. 2020 14:04:08	Pass	0	
Lewis Joan	263238339	Blocker building / Main Entrance Reader	2. 06. 2020 14:04:05	Pass	0	
Maintenance 1	26327136	Blocker building / Main Entrance Reader	2. 06. 2020 14:04:02	Wrong card	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:59	Pass	0	
Anders Tatiana	263238373	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:57	Pass	0	
Evans Timothy	263314280	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:55	Pass	0	
Cooper Sebastian	263195664	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:54	Pass	0	
Gardner-Boyle Maia	263266686	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:51	Pass	0	
Maintenance 1	26327136	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:45	Wrong card	0	
Hill Jeffery	263197317	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:42	Pass	0	
Puerto Mario	263333944	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:38	Pass	0	
Turner Michael	263238343	Blocker building / Main Entrance Reader	2. 06. 2020 14:03:36	Pass	0	
System	0	Controller: Main Entrance Controller, Reader: 0	2. 06. 2020 14:03:14	Reset	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 13:19:24	Wrong card	0	
System	2097240	Event on undefined reader. Controller: Main Entrance Controller, Reader number: 5	2. 06. 2020 13:19:05	Comm 9 wrong roll	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 13:18:22	Wrong card	0	
Anders Tamara	263195670	Blocker building / Main Entrance Reader	2. 06. 2020 13:18:00	Wrong card	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 13:17:46	Wrong card	0	
Anders Tamara	263195670	Blocker building / Main Entrance Reader	2. 06. 2020 13:16:28	Wrong card	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 13:16:24	Wrong card	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 13:16:15	Wrong card	0	
Brown Luis	263238369	Blocker building / Main Entrance Reader	2. 06. 2020 13:16:11	Wrong card	0	
Anders Tamara	263195670	Blocker building / 374 [1]Reader 1	2. 06. 2020 13:11:28	Pass	0	
Anders Tamara	263195670	Blocker building / 374 [1]Reader 1	2. 06. 2020 13:11:01	Pass	0	