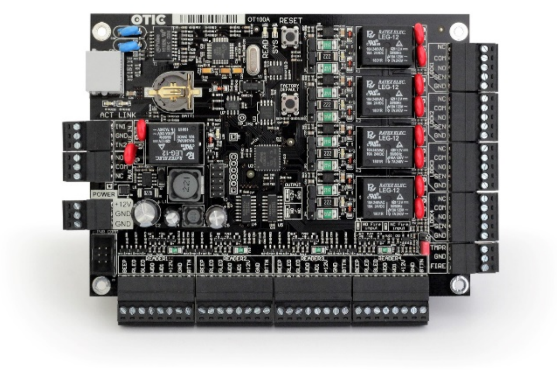
User manual

TABLE OF CONTENTS

INSTALL

SOFTWARE INSTALLATION

Before installation:



- Administrator access is required in the computer – run the Otic installer as Administrator.
- The computer should meet the minimum or recommended system requirements, which are shown in the following table.

Component	Minimal	Recommended
Processor (CPU)	2 GHz, 2 cores (ie. Intel Core i3 or equivalent)	2,4 GHz, 4 cores (ie. Intel Core i5 or equivalent)
Memory (RAM)	2 GB RAM	4 GB RAM
Storage	1 GB	2 GB
Display resolution	1366x768	1920x1080
Network	100 Mbit Ethernet	1000 Mbit Ethernet

By default, the system uses the following ports, which must be enabled on the firewall for proper communication.

Port	Direction	Function
UDP 60000	Software → Controller	The controllers' port. The software uploads the settings through this.
UDP 60001	Software → Controller	Service port for door controllers. It isn't reconfigurable and has only a secondary role.
UDP 60002	Software ← Controller	The software's port. Controllers report to the server through this port when they initiate.

LED FEEDBACK

CONTROLLER FEEDBACKS

- The controller is functional when the System LED flashes once per second.
- The controller is in bootloader mode when the System LED and the READ LED flashes once per second. Coin cell battery is low OR firmware is corrupted, firmware upgrade may be necessary.
- Invalid datetime when the System LED flashes rapidly (three per second).
- Relays' LEDs flash when the relay is pulled.
- Link LED is lit when Ethernet link is present.
- Act LED flashes when data exchange is in progress.
- Read LED flashes when a card was read.
- Read LED flashes quickly (4 times) when a card was read, but the Wiegand D0 and D1 lines are swapped.

READER FEEDBACKS

Access denied: red LED flashes quickly, 4 times.

Do not disturb: the green and red LED flash alternately.

Reader is waiting for further input (card, PIN, etc.): green LED flashes 1 per second.

Getcard mode (Read card by the software to assign user card): green LED flashes 400ms / 1000ms.

FIRST STEPS

CREATING A DATABASE

The system displays a database selection screen before login. Here can be created a new one or selected an existing database. Choose a directory where the program can write without administrator rights, for example, your own Documents (or Linux home) directory.

LOGIN

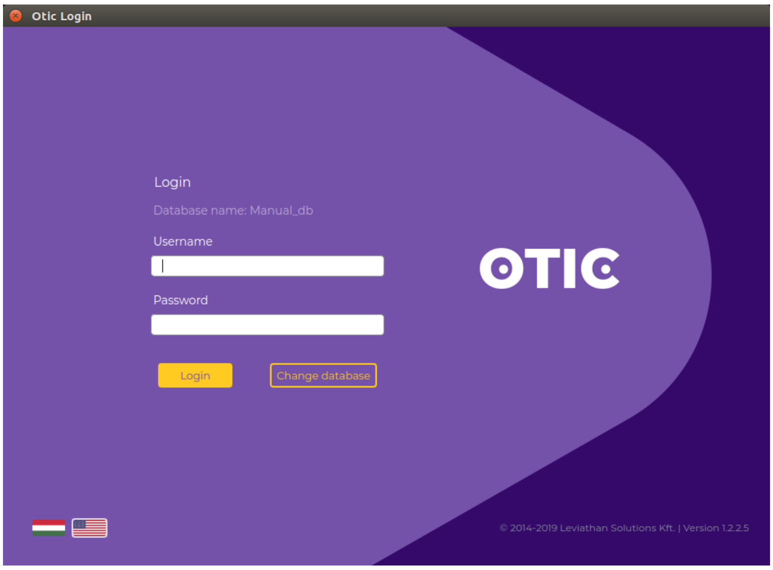
The language of the login popup window can be set by clicking on the flags below. After login the software's language can changed.

If you are to change the database, click on the „change database" button.

The database type is **SQLite**.

The last modified database will be opened if you don't choose.

The default username: admin, password: admin



Database name: Manual_db

© 2014-2019 Leviathan Solutions Kft. | Version 1.2.2.5

Software interface

Clicking on the Otic logo will navigate you to the Dashboard.

Use the arrows in the header (top left) to move forward and backward through the previously opened windows, just like internet browsers.

In case of an alert, the color of the Otic logo changes to red and the alert can be seen on the top right corner. By clicking the alert further operations can be performed.

The Upload button turns yellow when changes are pending.

By clicking on the column title in the purple header of the tables, the table can be sorted according to the content of the column (except the monitoring window). The width of the columns can be changed.

Filters: You can save your filtering criteria with the save icon and load it later with just one click 🗀.

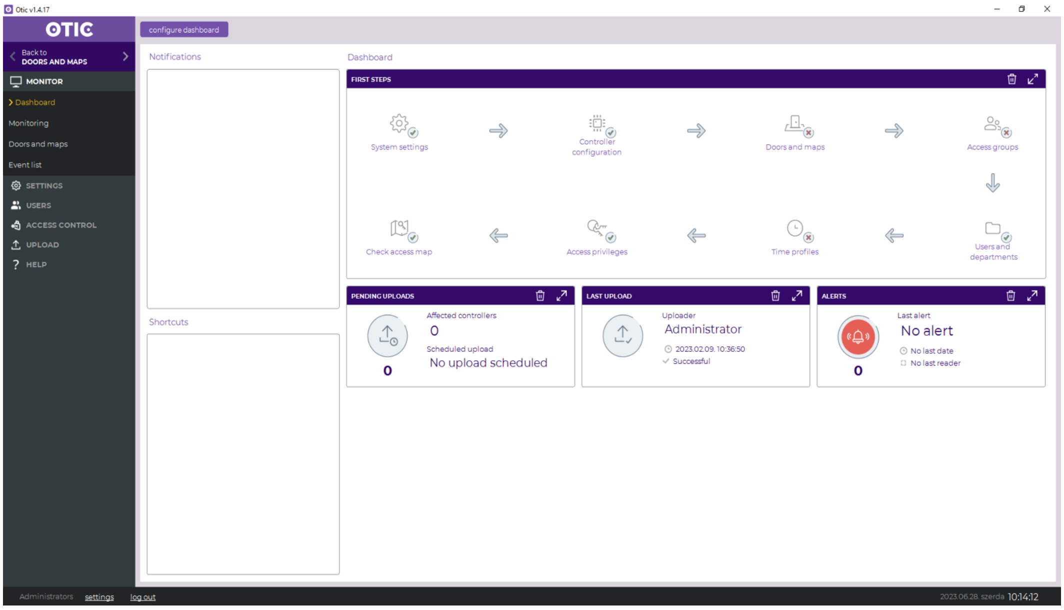
Edit button: to avoid accidental changes, you need to enable the changes with the "edit" button edit . In some menus, the drag and drop function is activated by the button either.

MONITOR MENU

Dashboard

The start screen of the software is the Dashboard menu, which provides a quick overview of important system events. Each tiles can be magnified for details or these can navigate you to the certain menu.

The first steps tile guides you through the system configuration steps, each icon function as a link. Green check mark can be seen on the icon if the configuration is done. Red x sign appeared if a configuration step is missed.



Affected controllers: 0
Scheduled upload: No upload scheduled
0

Uploader: Administrator
2023.02.09. 10:36:50
Successful

Last alert: No alert
No last date
No last reader
0

2023.06.28. szerda 10:14:12

Click the following links to jump to the appropriate point in the document:

1. step: *System defaults*
2. step: *Controllers*
3. step: *Doors and maps*
4. step: *Access groups*
5. step: *Users and departments*
6. step: *Time profiles*
7. step: *Access privileges*
8. step: *Access map*

MONITORING

The Monitoring window is used for real-time monitoring of the system, the events are listed in chronological order. Furthermore you can view here the current status of the gateways.

The events can be paused ⏸ and restart ▷ at any time.

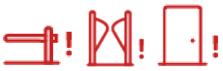
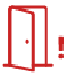
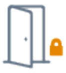
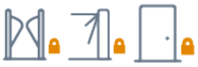
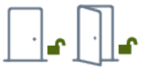
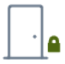
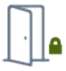
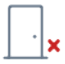
***TIP:** Select a door and with a right click you can choose options from a drop-down list. You can open the door, view the datasheet, etc.*

***TIP:** Open the monitoring in a new window* ↗ *to keep an eye on the events while you are checking other menu.*

Doors

Graphic feedback on the current status of the doors is also provided. Right-click to perform quick operations on each door. For instance, you can initiate a remote open.

The current status of doors is indicated by the following icons:

	alert, door is closed
	alert, door is open (opening sensor signal)
	door lock is locked, but door is open
	door is locked
	relay is released
	door closed, relay is closed
	door open, relay is closed
	no connection with the door

Display and management of alerts

Alerts are highlighted with red in the event list and the current alerts can be viewed in the drop-down menu on the right side of the header.

TIP: *The location of the alarm event is instantly displayed on the map view.*

Doors and maps

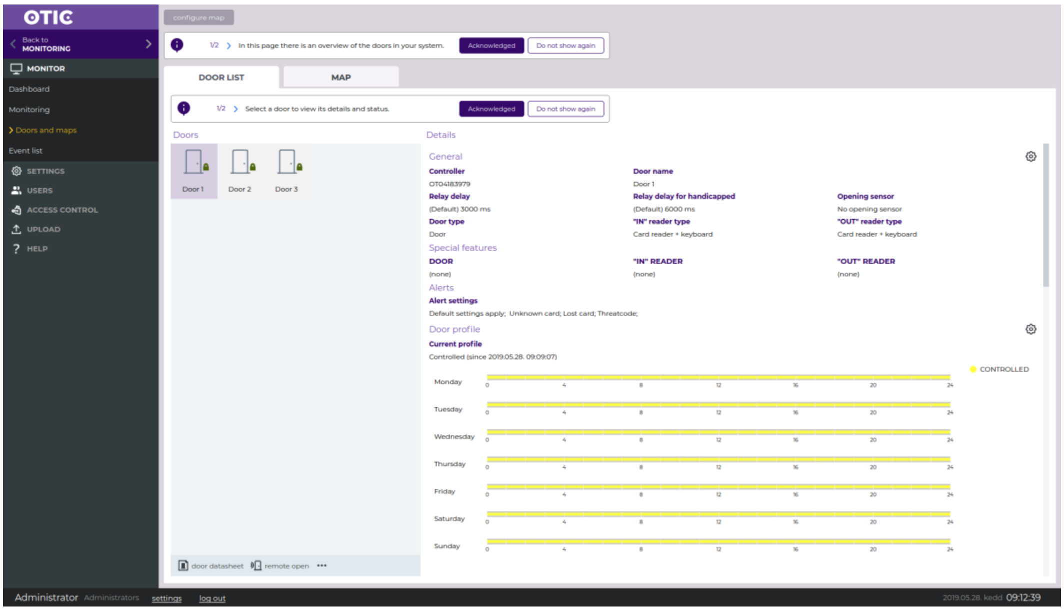
The icons of doors and controllers can be placed on the map (use „drag and drop”). The size and color of the icons can be customized. The current status of each door can be seen on the icons.

Door list

The first tab shows the system gateways with graphical real-time status feedback. Clicking on the icons of each gateway will display a preview of the most important parameters of the door. The operating mode and the time profile of the door can be seen on the preview right side.

In the "Assign Profile" ⋯ dialog you can assign the previously created door profiles to one or more doors. Here you can also specify the time interval for the door profiles.

Right-clicking on the icons allows you to perform additional operations.



1/2 In this page there is an overview of the doors in your system.

1/2 Select a door to view its details and status.

General

Controller OT04183979	**Door name** Door 1	
Relay delay (Default) 3000 ms	**Relay delay for handicapped** (Default) 6000 ms	**Opening sensor** No opening sensor
Door type Door	**"IN" reader type** Card reader + keyboard	**"OUT" reader type** Card reader + keyboard

Special features

DOOR (none)	**"IN" READER** (none)	**"OUT" READER** (none)

Alerts

Alert settings

Default settings apply; Unknown card; Lost card; Threatcode;

Door profile

Current profile

Controlled (since 2019.05.28. 09:09:07)

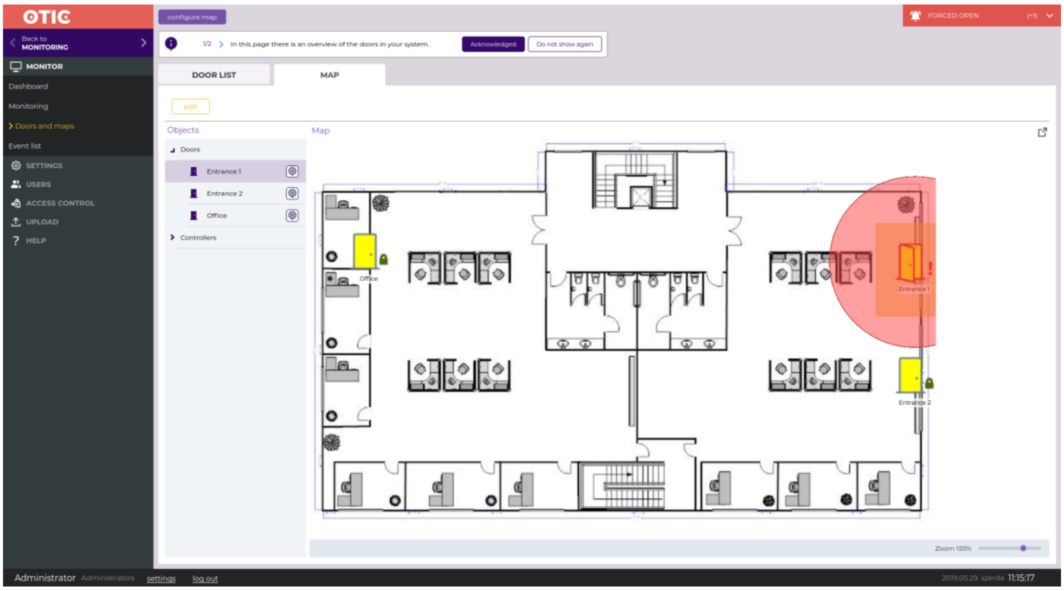
Map

The size of the uploaded map can be changed as desired by the control bar.

The icons of gateways and controllers can be placed on the map. The size and color of the icons can be customized.

The ◎ icon can be seen next to the items that are already drag and dropped on the map.

When an alarm event occurs, the map will show the affected door with a "show door on map" option and highlight the gateway icon with a red circle.



1/2 In this page there is an overview of the doors in your system.

Event list

The event list window can be filtered by time ranges, locations, users, departments, access groups, etc. The configured filtering conditions can be saved.

After setting the filtering criteria, you can hide the filters by „**hide filters**".

⚠ ***ATTENTION! With the "Delete old movement data" function you can permanently delete events which are older than 6 months.***

The quick filters on the top provides quick overview of important events. (For example, by clicking on the "Alerts", "Today" or "Last Hour" filtering criteria.)

Export daily activities

This module allows you to export your employees' daily first and last access events and the system automatically calculates the work time between the two time flags.

SETTINGS MENU

System settings

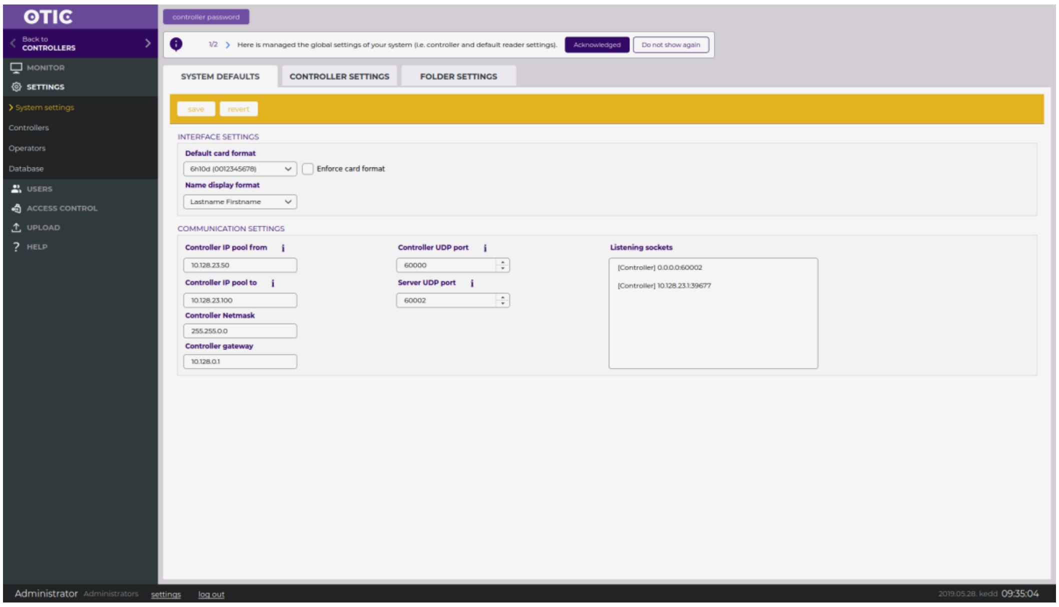
System defaults

Here can be found the basic communication and security settings of the system. Editing the data on each tab must be enabled with the "edit" button.

⚠ ***ATTENTION!*** *It is important to set up the communication parameters and the defaults of the controllers before discovery.*

Enter an IP address range. The system will automatically assign an IP address to the controllers from this address range.

The default IP address of the controllers is 192.168.0.200



1/2 > Here is managed the global settings of your system (i.e. controller and default reader settings).

INTERFACE SETTINGS

Default card format: 6h10d (0012345678) □ Enforce card format

Name display format: Lastname Firstname

COMMUNICATION SETTINGS

Controller IP pool from: 10.128.23.50

Controller IP pool to: 10.128.23.100

Controller Netmask: 255.255.0.0

Controller gateway: 10.128.0.1

Controller UDP port: 60000

Server UDP port: 60002

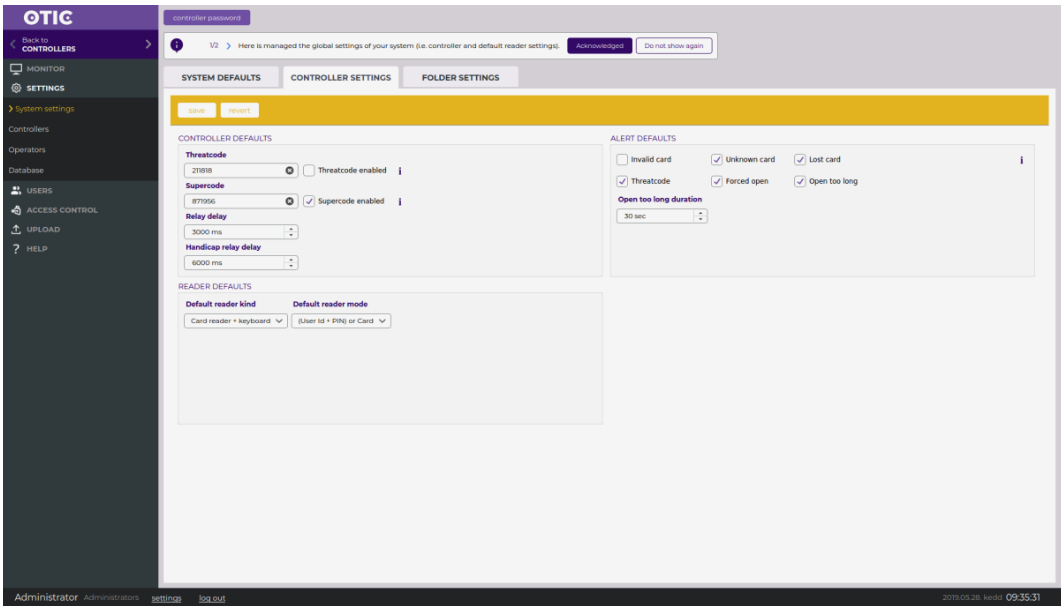
Listening sockets:
[Controller] 0.0.0.0:60002
[Controller] 10.128.23.1:39677

Administrator Administrators

2019.05.28. kedd 09:35:04

Controller settings

On this tab you can set the alert parameters, read mode, etc. These default settings can be individually overwritten in the controller configuration wizard window.



1/2 > Here is managed the global settings of your system (i.e. controller and default reader settings).

CONTROLLER DEFAULTS

Threatcode: 211818 □ Threatcode enabled

Supercode: 871956 ☑ Supercode enabled

Relay delay: 3000 ms

Handicap relay delay: 6000 ms

ALERT DEFAULTS

□ Invalid card ☑ Unknown card ☑ Lost card

☑ Threatcode ☑ Forced open ☑ Open too long

Open too long duration: 30 sec

READER DEFAULTS

Default reader kind: Card reader + keyboard

Default reader mode: (User Id + PIN) or Card

Administrator Administrators

2019.05.28. kedd 09:35:31

Controller defaults

Threat code: Even the locked doors can be opened by entering the threat code. The function can be enabled or disabled per door.

CAUTION! *The threat code overrides the interlock rules either! Use it carefully!*

Supercode: By entering the code, the doors in normal operating mode can be opened without a card. Locked doors cannot be opened. The function can be disabled per door.

Opening time: The default opening time of the door opener relay.

Opening time for disabled: The default hold time for the door opener, if disabled user is entering. The users can be set as disabled in the edit user window.

Alert defaults

The selected event types will generate software alerts. Opening sensor is required for the "Forced open" and "Open to long" alerts. The function can be changed per door.

Reader defaults

The commonly used reader type and the identification method should be specified here. The default parameters can be overwritten in the edit controller window per reader.

There are several options to choose from:

- **Card:** you only need to read a card to pass
- **Card + PIN:** after card reading, PIN code is also needed to pass
- **(User ID + PIN) or card:** you can pass through by reading your card. If the card is not available, enter the user ID then the PIN code. **After a user ID, you have to press # or Enter and then enter the PIN.**
- **(Card or User ID) + PIN:** after reading a card or typing a user ID, PIN code is mandatory. **Entering User ID + PIN: Press # or Enter after user ID, then enter PIN.**

Controller password: (button at the top) The communication with the controllers can be encrypted by entering a password so that our system controllers will only communicate with us. Other Otic systems in the network won't be able to communicate with our controllers.

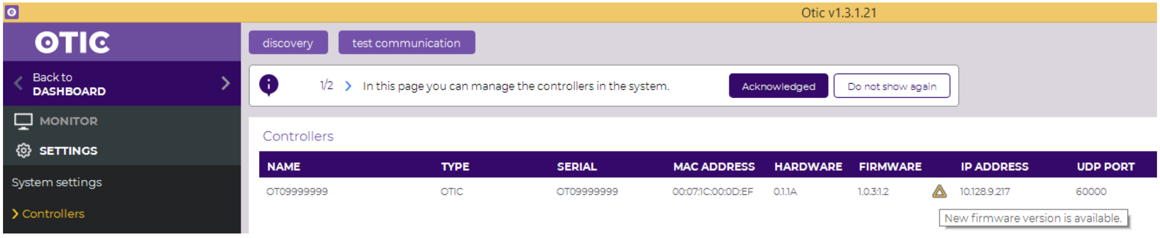
CONTROLLERS

In this menu you can add controllers and edit them.

Discovery: The controllers in the network can be detected and add to the system.

Test communication: Performs a real time test to determine the connection quality.

The most important parameters of the controllers can be viewed in the table view. If any controller needs firmware upgrade the dashboard displays a notification, and also a yellow triangle appears in the controller's row.

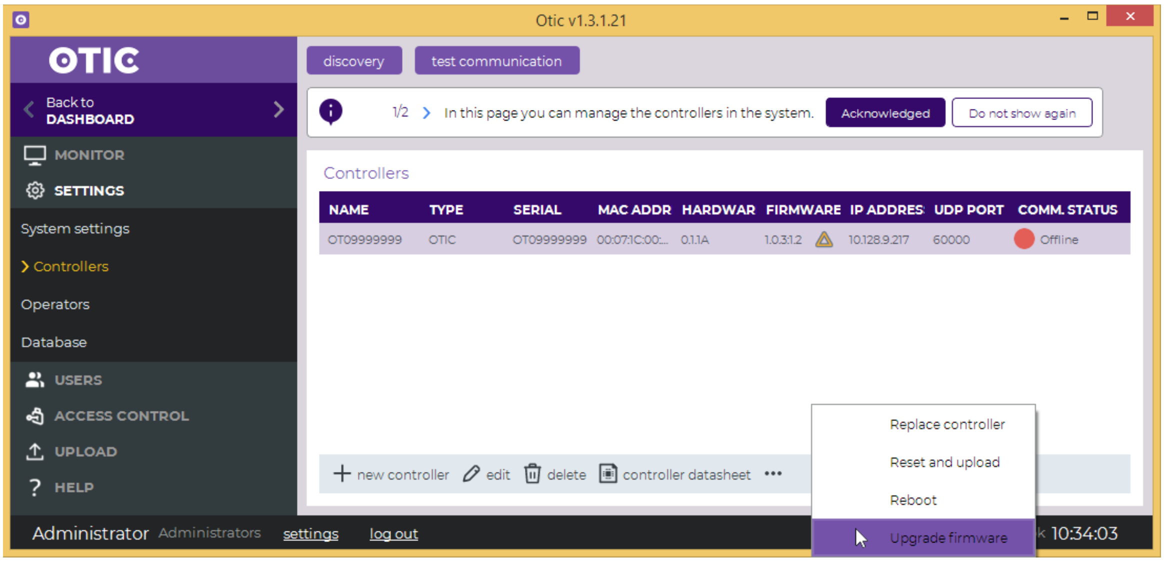


In this page you can manage the controllers in the system.

Controllers

NAME	TYPE	SERIAL	MAC ADDRESS	HARDWARE	FIRMWARE		IP ADDRESS	UDP PORT
OT09999999	OTIC	OT09999999	00:07:1C:00:0D:EF	0.1.1A	1.0.3.1.2	⚠	10.128.9.217	60000

The firmware can be upgraded by selecting the controller(s) and then clicking on the more options "…" button, then selecting the Upgrade firmware option.



In this page you can manage the controllers in the system.

Controllers

NAME	TYPE	SERIAL	MAC ADDR	HARDWAR	FIRMWARE		IP ADDRES	UDP PORT	COMM. STATUS
OT09999999	OTIC	OT09999999	00:07:1C:00:...	0.1.1A	1.0.3.1.2	⚠	10.128.9.217	60000	● Offline

The controllers can be configured by double-clicking on each controller or by clicking on the edit icon.

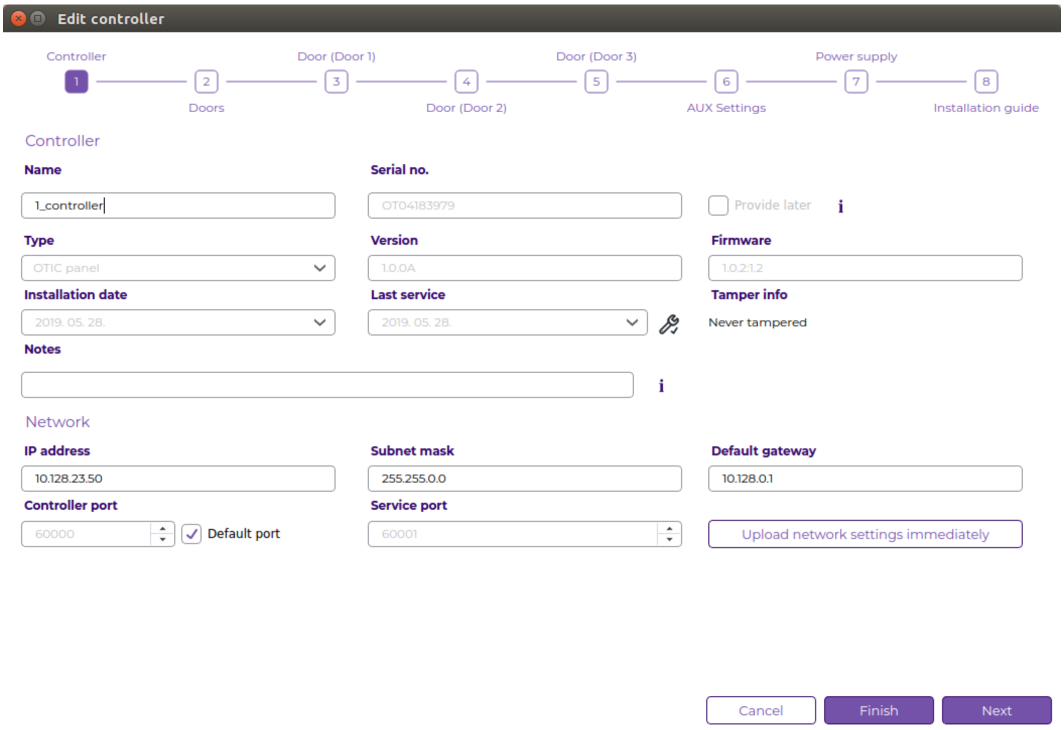
Controller configuration wizard

The first page is for basic configuration.

TIP: *Click the „new controller" + icon, then select the "'Provide later" option next to the serial number. This allows you to create virtual controllers. All the settings can be set at home, without knowing the actual serial number. On-site pre-configured "virtual" controllers must be replaced (by the "replace" function) with the real controllers. This way all the settings can be loaded on the real controllers by one click.*

Service mode: Disables the tamper input during the service and maintenance. Use the wrench icon 🔧 to activate this function.

Note: Notes can be written about the controller or about the installation. The note will turn up by pointing to the "Info" icon next to the controller.



Controller

Name: 1_controller

Serial no.: OT04183979

□ Provide later

Type: OTIC panel

Version: 1.0.0A

Firmware: 1.0.2.1.2

Installation date: 2019. 05. 28.

Last service: 2019. 05. 28.

Tamper info: Never tampered

Notes:

Network

IP address: 10.128.23.50

Subnet mask: 255.255.0.0

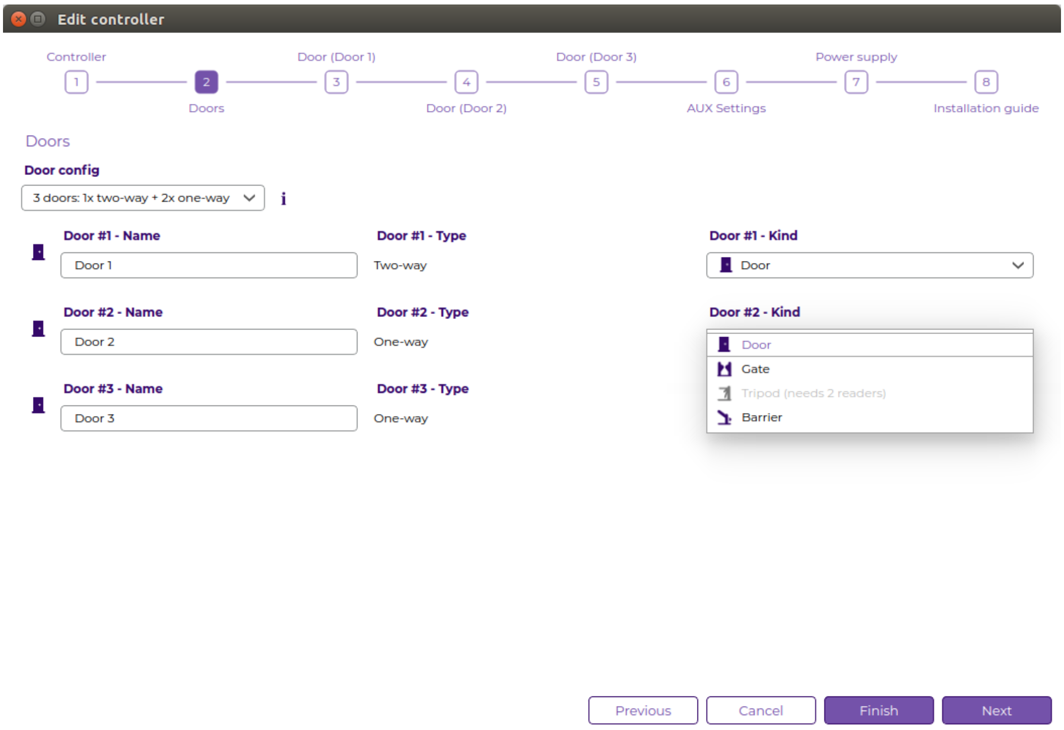
Default gateway: 10.128.0.1

Controller port: 60000 ☑ Default port

Service port: 60001

Upload network settings immediately

Number of Doors: The controller can be freely configured to control 1, 2, 3 or even 4 doors. As the device has 4 Wiegand reader inputs, it can manage up to 2 doors in 2-way or 4-door 1-way control.



Doors

Door config: 3 doors: 1x two-way + 2x one-way

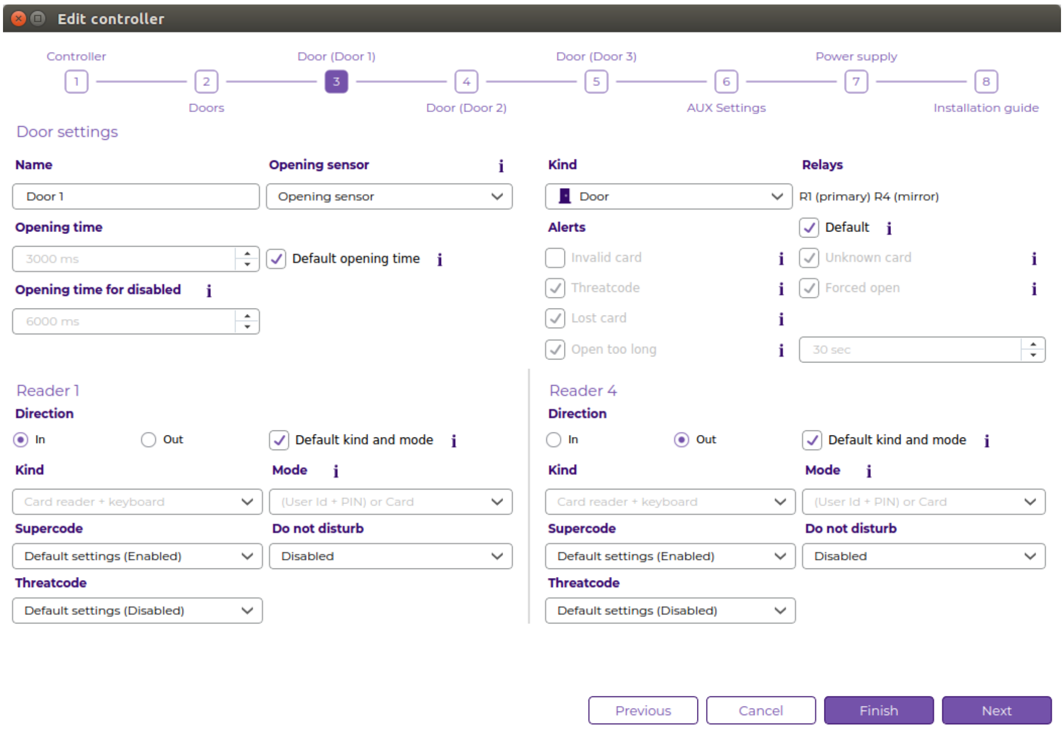
Door #1 - Name	Door #1 - Type	Door #1 - Kind
Door 1	Two-way	Door

Door #2 - Name	Door #2 - Type	Door #2 - Kind
Door 2	One-way	Door

Door #3 - Name	Door #3 - Type
Door 3	One-way

Doors and readers settings

Setting of doors: If you enable the default settings in each section, the settings set in the menu are used.



Door settings

Name: Door 1

Opening sensor: Opening sensor

Opening time: 3000 ms ☑ Default opening time

Opening time for disabled: 6000 ms

Kind: Door

Relays: R1 (primary) R4 (mirror)

Alerts ☑ Default

□ Invalid card ☑ Unknown card

☑ Threatcode ☑ Forced open

☑ Lost card

☑ Open too long 30 sec

Reader 1

Direction ● In ○ Out ☑ Default kind and mode

Kind: Card reader + keyboard

Mode: (User Id + PIN) or Card

Supercode: Default settings (Enabled)

Do not disturb: Disabled

Threatcode: Default settings (Disabled)

Reader 4

Direction ○ In ● Out ☑ Default kind and mode

Kind: Card reader + keyboard

Mode: (User Id + PIN) or Card

Supercode: Default settings (Enabled)

Do not disturb: Disabled

Threatcode: Default settings (Disabled)

Door type:

- **Normal door, gate and barrier:** The opening relay is pulled during the specified opening time.
- **Tripod/turnstile:** In this case the opening is initiated by contact. 2 relays are required for operation.

Opening sensor: Only the doors with opening sensor can generate *Open too long* and *Forced open* events/alerts. Use opening sensor to indicate the opening status of the door.

Built-in opening sensor: This option should be chosen when a door-lock magnet is installed with a built-in opening sensor. The magnet will be released till the end of the predefined opening time, regardless of the door is open or closed.

Do not disturb: Usually it can be activated with a switch or remote control. While the function is active, the reader will reject all cards. The reader also indicates the “Do not disturb” operating mode.

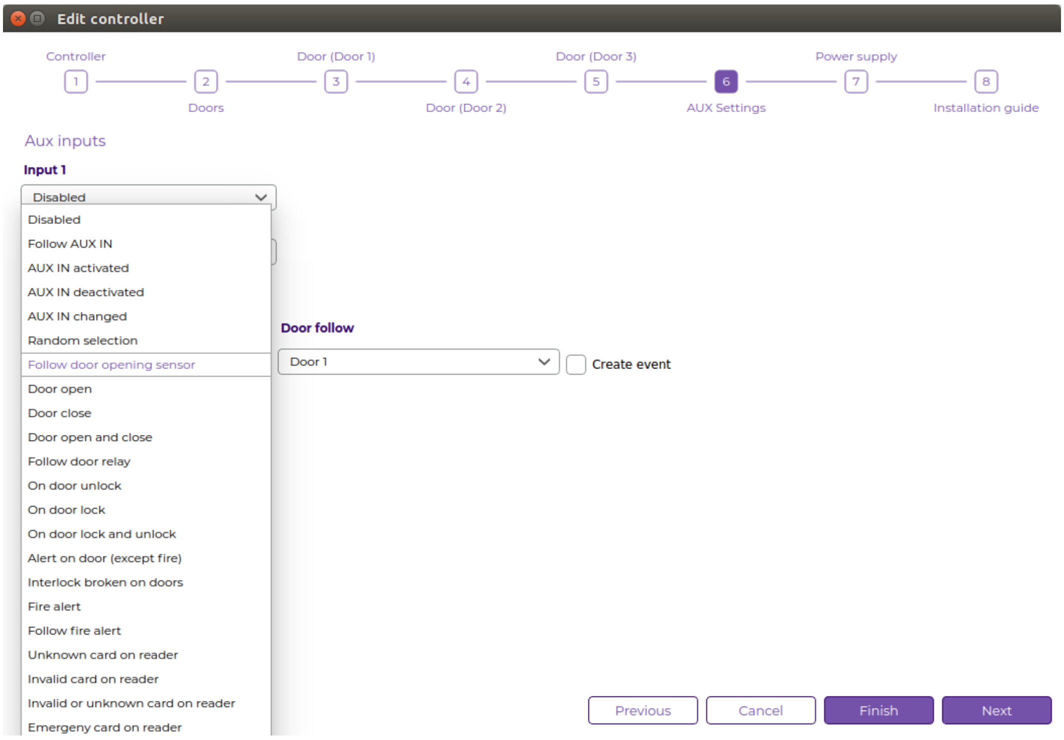
AUX settings

You can configure here the AUX OUT relay and the two AUX inputs. Use input for „do not disturb”, random selection with AUX out or input can be followed by AUX out.

AUX output:

- **Follow AUX input**: The relay will follow the status of the selected input.

- **AUX IN activated:** The AUX relay will be active for the predefined time period, if the input status changed to activated.
- **AUX IN deactivated**: The AUX relay will be active for the predefined time period, if the input status changed to deactivated.
- **AUX IN state changed**: The AUX relay will be active for the predefined time period, if the input status is changed.
- **Random selection**: The AUX relay follows the status of the selected input with the specified probability.
- **Follow opening sensor**: The AUX relay will be activated till the door is open.
- **Door open**: The door opening event will activate the AUX relay for the predefined time period.
- **Door close**: The door closing event will activate the AUX relay for the predefined time period.
- **Door open / close**: The AUX relay will be active for the predefined time period, if the door opening sensor state is changed.
- **Follow door relay**: The AUX relay will follow the state of the door opening relay
- **On door unlock:** The AUX relay will be active for the predefined time period, if the door opening relay’s state changed to released.
- **On door lock:** The AUX relay will be active for the predefined time period, if the door opening relay’s state changed to pulled.
- **On door lock and unlock:** The AUX relay will be active for the predefined time period, if the door opening relay’s state is changed.
- **Alert on door (except fire)**: The AUX relay will be active for the predefined time period in case of any alert event (except fire).
- **Interlock broken on doors**: The AUX relay will be active if interlock is broken on the specified door(s).
- **Fire alert**: The AUX relay will be active for the predefined time period, if fire alert is activated.
- **Follow fire alert:** The AUX relay will be activated till the fire alert is active.
- **… card on reader**: If the selected card type is presented on the reader, the AUX relay will be activated.
- **Emergency card on reader**: If emergency card is presented on the reader, the AUX relay will be activated.
- **Threatcode on reader:** The threatcode will activate the AUX relay.
- **Supercode on reader:** The supercode will activate the AUX relay.
- **Periodic**: The AUX relay can be activated at any time for an arbitrary time period.
- **Manager user**: If a manager card is presented, the AUX relay will be activated.


Edit controller

Controller 1 — 2 Doors — 3 Door (Door 1) — 4 Door (Door 2) — 5 Door (Door 3) — 6 AUX Settings — 7 Power supply — 8 Installation guide

Aux inputs

Input 1: Disabled

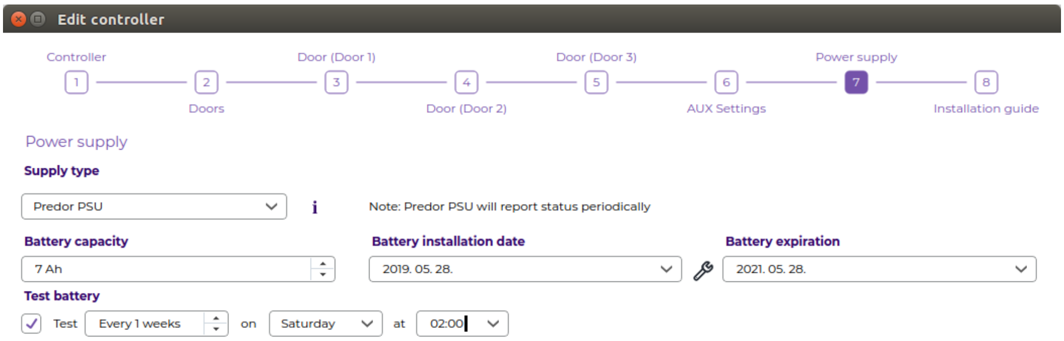
- Disabled
- Follow AUX IN
- AUX IN activated
- AUX IN deactivated
- AUX IN changed
- Random selection
- Follow door opening sensor
- Door open
- Door close
- Door open and close
- Follow door relay
- On door unlock
- On door lock
- On door lock and unlock
- Alert on door (except fire)
- Interlock broken on doors
- Fire alert
- Follow fire alert
- Unknown card on reader
- Invalid card on reader
- Invalid or unknown card on reader
- Emergeny card on reader

Door follow: Door 1 □ Create event

Power supply

If the controller is used with a Predor power supply, the controller will send state of battery and status information about the power supply.

In the ACU datasheet window, the measurement results can be seen with the estimated breakdown time.


Edit controller

Controller 1 — 2 Doors — 3 Door (Door 1) — 4 Door (Door 2) — 5 Door (Door 3) — 6 AUX Settings — 7 Power supply — 8 Installation guide

Power supply

Supply type: Predor PSU

Note: Predor PSU will report status periodically

Battery capacity: 7 Ah

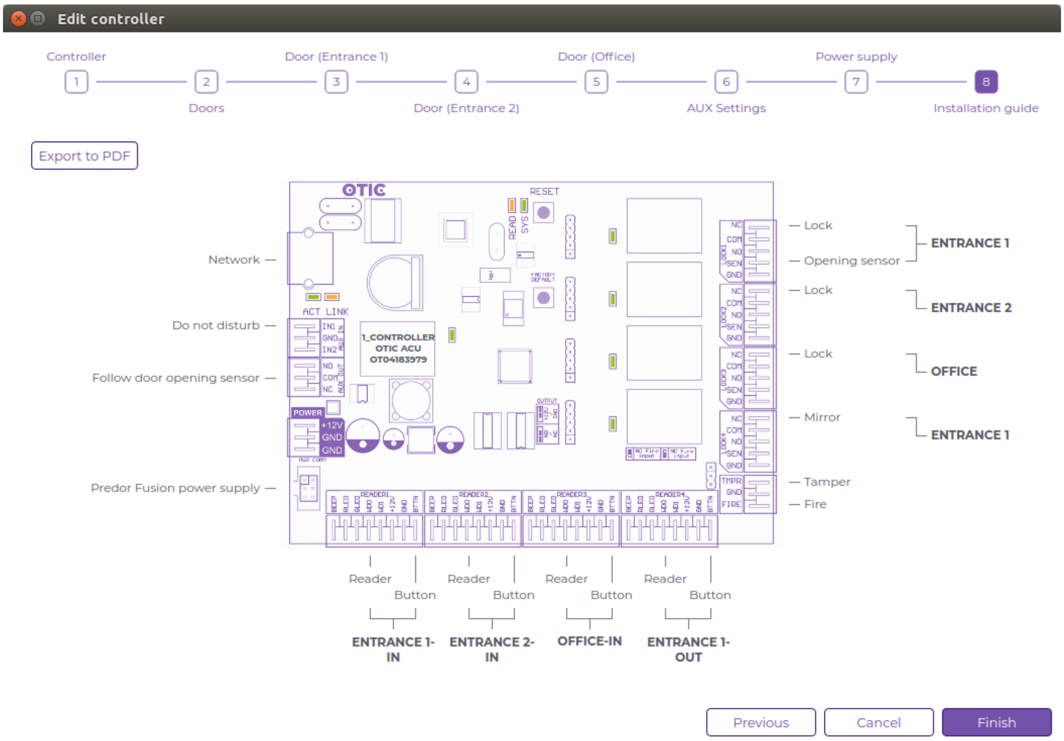
Battery installation date: 2019. 05. 28.

Battery expiration: 2021. 05. 28.

Test battery: ☑ Test Every 1 weeks on Saturday at 02:00

Installation guide

Don't worry about wiring anymore! The software creates unique wiring diagram (installation guide) for each controller based on your settings and labels. In this way, this part of the installation can be outsourced.

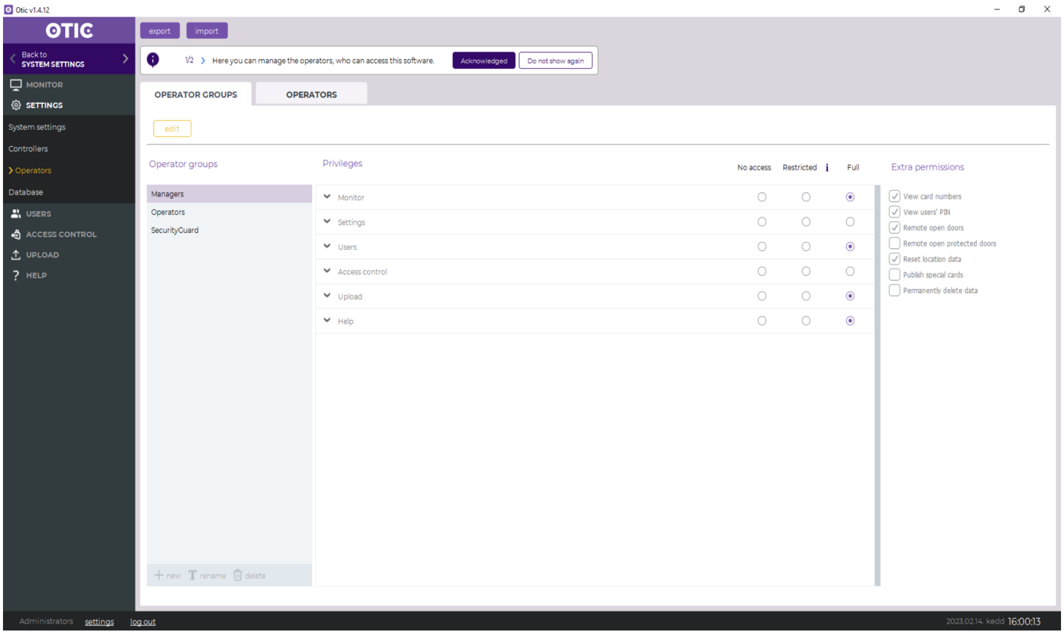


OPERATORS

Operators are the people who use the software. Do not confuse them with the card holder users.

Under the "Operator groups" tab the authorization levels can be adjusted (operator groups).

- **No access**: The operator cannot see this menu.
- **Restricted:** The operator can see this menu, but cannot modify.
- **Full:** The operator can modify and delete as well.



1/2 Here you can manage the operators, who can access this software. Acknowledged | Do not show again

Operator groups: Managers, Operators, SecurityGuard

Privileges	No access	Restricted	Full
Monitor	○	○	●
Settings	○	○	○
Users	○	○	●
Access control	○	○	○
Upload	○	○	●
Help	○	○	●

Extra permissions

- ☑ View card numbers
- ☑ View users' PIN
- ☑ Remote open doors
- □ Remote open protected doors
- ☑ Reset location data
- □ Publish special cards
- □ Permanently delete data

2023.02.14. kedd 16:00:13

Extra permissions can be added:

- **View card numbers**: If enabled, the operator can view the number of the cards.
- **View users' PIN:** If enabled, the operator can view the pin codes.
- **Remote open doors:** If enabled, the operator can open doors from the software.
- **Reset location data:** If enabled, the operator can reset the location data of the users.
- **Publish special cards:** If enabled, the operator is authorized to give out emergency cards.
- **Permanently delete data:** If enabled, the operator can delete data from the system permanently. : *delete old movement data* button.

In new operator window the access level (operator group) for the new operator should be specified.

DATABASE

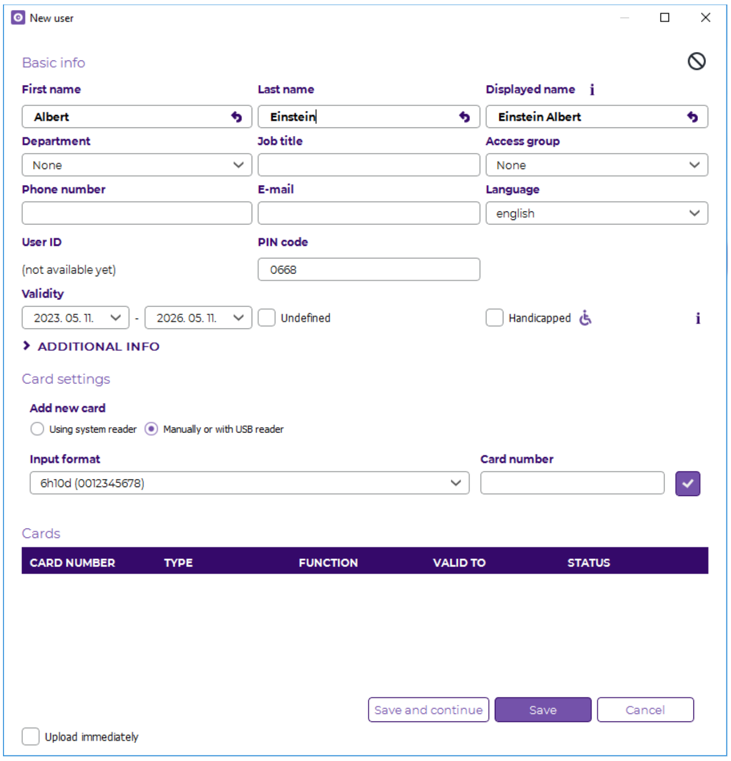
On this screen, the details can be viewed of the currently active database.

⚠ ***CAUTION!*** *Periodic database backup is essential to avoid data loss.*

USERS MENU

USERS AND DEPARTMENTS

This is an overview of system users and departments. Between the filters and the table, you can see how many users can be added to the system. You can add a new user by clicking on the **+new user** button in the bottom menu bar. The name (First Name, Last Name) and the displayed name are required, the other fields can be filled in optionally. The **displayed name** is the name used by the person in the software, so it is possible to distinguish between multiple users with the same name in the system.



New user

Basic info

First name	Last name	Displayed name
Albert	Einstein	Einstein Albert
Department	Job title	Access group
None		None
Phone number	E-mail	Language
		english
User ID	PIN code	
(not available yet)	0668	

Validity

2023. 05. 11. - 2026. 05. 11. □ Undefined □ Handicapped

› ADDITIONAL INFO

Card settings

Add new card

○ Using system reader ● Manually or with USB reader

Input format: 6h10d (0012345678)

Card number:

Cards

CARD NUMBER	TYPE	FUNCTION	VALID TO	STATUS

□ Upload immediately

The default start date for the **validity** is today, but it can be changed freely. The end date of the validity period can be a fixed date or undefined. All user identifiers will be invalidated outside the validity period, so the user will not be able to move within the system.

The system uses the **PIN code** for code access. When a user is created, a 4-digit code is automatically generated and can be changed. The PIN code can contain 4 to 8 digits.

The **handicapped** option can be used to indicate that the controllers should keep the door locks open for a longer period of time when entering.

By clicking on the **additional info** text, other extra information can be added for users.

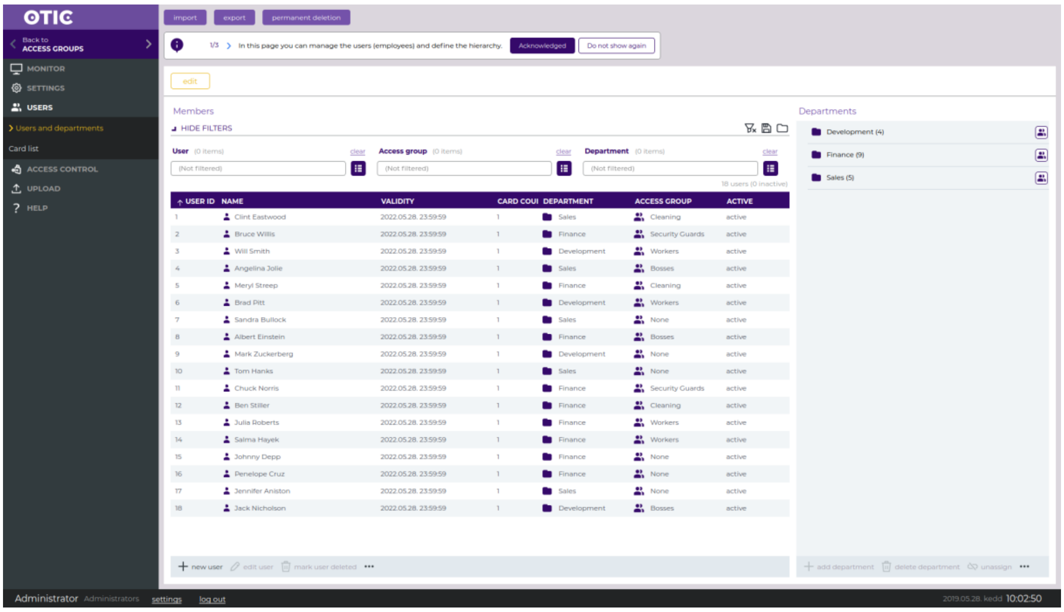
You can also manage the cards of users in this window. Cards can be assigned to users with the card readers used for identification in the system, with a USB card reader, or manually entered. The cards assigned to a user are displayed in a table called **Cards**. Clicking the delete button in the card's row will remove the card from the user.

By selecting the **upload immediately** option, the user's data will be uploaded to the controllers immediately by clicking on the save button, so manual upload isn't required.

By clicking on the disable icon in the top right corner of the window, the user will be temporarily disabled and all their identifiers will become invalid. To reactivate, click on the enable button that appears on the same place.

By clicking on the **Save and continue** button, the user is registered in the system and a new editing window opens immediately. Clicking on the Save button closes the editor window.

New departments and complete department tree can be created. The users can be categorized by "drag and drop" method. To make changes, edit button should be clicked first.



1/3 In this page you can manage the users (employees) and define the hierarchy.

Members

User (0 items) (Not filtered)

Access group (0 items) (Not filtered)

Department (0 items) (Not filtered)

18 users (0 inactive)

USER ID	NAME	VALIDITY	CARD COUI	DEPARTMENT	ACCESS GROUP	ACTIVE
1	Clint Eastwood	2022.05.28. 23:59:59	1	Sales	Cleaning	active
2	Bruce Willis	2022.05.28. 23:59:59	1	Finance	Security Guards	active
3	Will Smith	2022.05.28. 23:59:59	1	Development	Workers	active
4	Angelina Jolie	2022.05.28. 23:59:59	1	Sales	Bosses	active
5	Meryl Streep	2022.05.28. 23:59:59	1	Finance	Cleaning	active
6	Brad Pitt	2022.05.28. 23:59:59	1	Development	Workers	active
7	Sandra Bullock	2022.05.28. 23:59:59	1	Sales	None	active
8	Albert Einstein	2022.05.28. 23:59:59	1	Finance	Bosses	active
9	Mark Zuckerberg	2022.05.28. 23:59:59	1	Development	None	active
10	Tom Hanks	2022.05.28. 23:59:59	1	Sales	None	active
11	Chuck Norris	2022.05.28. 23:59:59	1	Finance	Security Guards	active
12	Ben Stiller	2022.05.28. 23:59:59	1	Finance	Cleaning	active
13	Julia Roberts	2022.05.28. 23:59:59	1	Finance	Workers	active
14	Salma Hayek	2022.05.28. 23:59:59	1	Finance	Workers	active
15	Johnny Depp	2022.05.28. 23:59:59	1	Finance	None	active
16	Penelope Cruz	2022.05.28. 23:59:59	1	Finance	None	active
17	Jennifer Aniston	2022.05.28. 23:59:59	1	Sales	None	active
18	Jack Nicholson	2022.05.28. 23:59:59	1	Development	Bosses	active

Departments

- Development (4)
- Finance (9)
- Sales (5)

Administrator Administrators 2019.05.28. kedd 10:02:50

TIP: *The users, the complete department tree, the access groups, user card numbers etc. can be imported from an Excel sheet with just one click.*

The data can be filtered by name, department, or even access group.

To create a subdepartment, select the appropriate parent department, then click the new icon.

Permanent (irrevocable) deletion: After marking selected users for deletion the users' events can be listed. The selected users are added to a final deletion list, they can be listed in a dialog window. If the deletion is confirmed here, **all movement events will be deleted with their personal data!**

CAUTION! *The user's personal data and movement events will be permanently deleted if you choose the permanent deletion!*

ATTENTION! *Departments only indicate the organizational structure of the company and do not affect the access privileges. The access groups and individual privileges determine the access permissions.*

TIP: *Save time, do not add the user’s cards one by one. Select multiple users and in the „additional menu” ∘∘∘choose „Assign cards”. In the opening window click Read and present as many cards in the appropriate reader as many users was selected. Each user will have one card.*

CARD LIST

The registered cards of the system can be viewed in this view, and the list can be shortlisted by detailed filters.

Card History: This view provides information about the history of the card. You can check the issuance date, the former owners or the operator who has issued the card.

Lost cards: If a user has lost their card, the badge must be marked as lost. If an unauthorized person tries to enter with a lost card, the system will generate an alert event.

Deactivation: The cards can be quickly and easily deactivated if it’s needed. These cards can be activated any time just by a click.

ACCESS CONTROL MENU

ACCESS GROUPS

Before setting the access rights, it is advisable to specify the members of the access groups. If you change the access group of a certain user, their access rights also will be changed immediately. It makes the permission handling prompt and easy.

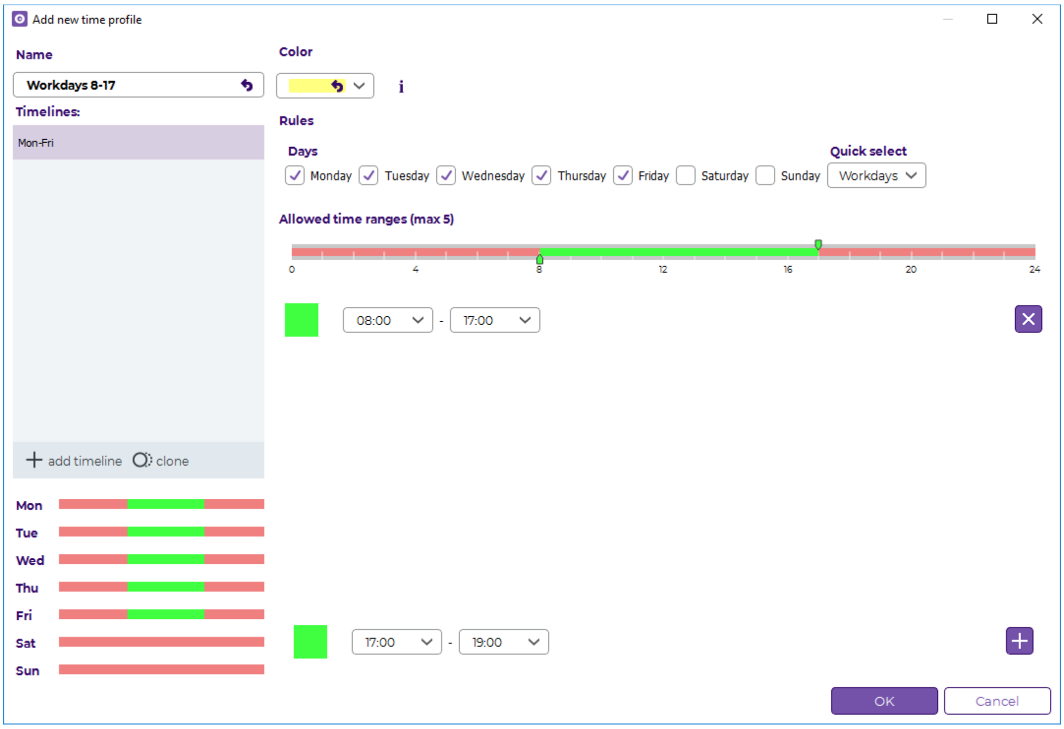
Click on each group to list all members of the group.

TIME PROFILES

By creating time profiles, you can configure the time periods, when the users are allowed to pass through certain doors. The time profiles created here can be assigned to users or access groups.

New Profile: In the new profile dialog you can create and configure time profiles. Enter the name of the profile, and choose the days of the week the profile will be applied. Then set the time periods on the timeline you in which the entry is allowed. Different timelines can be created for different days.

Copy settings: If you are to create a new profile which is similar to an existing time profile, select the existing profile and click "clone profile". This way you can copy the settings and only the differences must be set.



Add new time profile

Name: Workdays 8-17

Color

Timelines: Mon-Fri

Rules

Days: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

Quick select: Workdays

Allowed time ranges (max 5)

🟩 08:00 - 17:00

🟩 17:00 - 19:00

ACCESS PRIVILEGES

The access rights are assigned to users, not to cards. A user may have several access credentials.

In the “new privileges” dialog window you can set the access rights.

Who?: Select the appropriate users or access groups in the window and click on the Select button.

Where?: Use the same method to select the readers where you wish to grant access.

When?: Select the proper time profile from the drop-down list.

The "Add selected items" button turns yellow color to indicate that all required parameters are selected. You can apply the changes by clicking on this button, then click to save.

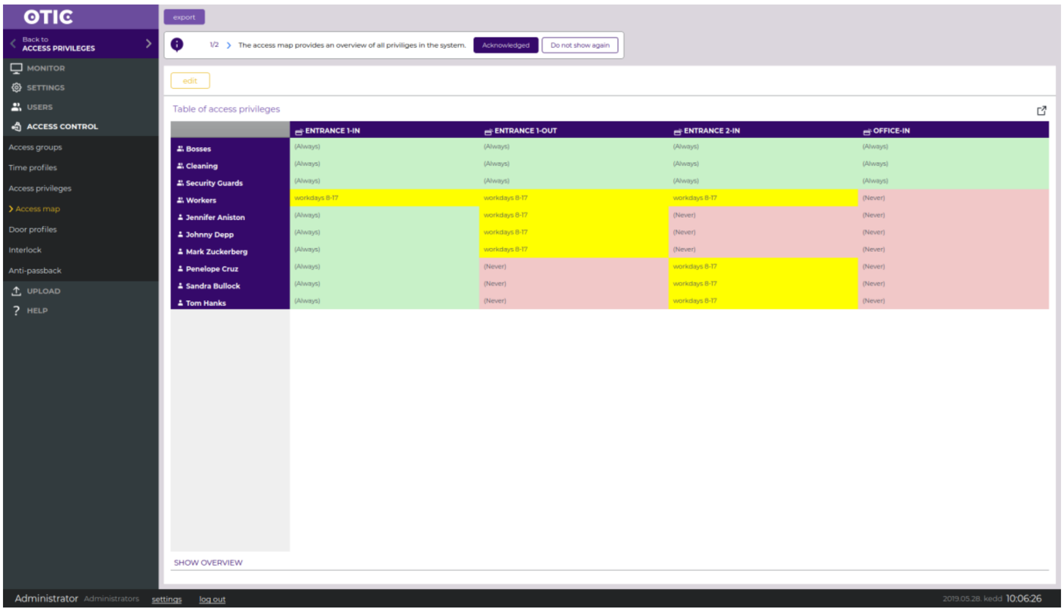
ACCESS MAP

The access map allows you to quickly overview the access rights.

The columns of the matrix show the readers of the system.

The rows of the matrix show the access groups and the individual users.

In each cell can be seen the assigned time profile. So you can check that in which time period is allowed to the user to enter the given zone.



1/2 The access map provides an overview of all priviliges in the system.

Table of access privileges

	ENTRANCE 1-IN	ENTRANCE 1-OUT	ENTRANCE 2-IN	OFFICE-IN
Bosses	(Always)	(Always)	(Always)	(Always)
Cleaning	(Always)	(Always)	(Always)	(Always)
Security Guards	(Always)	(Always)	(Always)	(Always)
Workers	workdays 8-17	workdays 8-17	workdays 8-17	(Never)
Jennifer Aniston	(Always)	workdays 8-17	(Never)	(Never)
Johnny Depp	(Always)	workdays 8-17	(Never)	(Never)
Mark Zuckerberg	(Always)	workdays 8-17	(Never)	(Never)
Penelope Cruz	(Always)	(Never)	workdays 8-17	(Never)
Sandra Bullock	(Always)	(Never)	workdays 8-17	(Never)
Tom Hanks	(Always)	(Never)	workdays 8-17	(Never)

TIP: *You can modify the time profiles just by a right click, if you change to edit mode first.*

The access map can be opened in new window and also can be exported to Excel.

Door profiles

Door operating modes can be configured. For instance, closed, open, only managers etc. You can create door profile if you determine time periods for the certain door operating modes. For instance, it can be useful if a door needs to opened or closed independently from access rights.

New profile: In the new profile dialog you can create door profiles. Enter the name of the profile, and choose the days of the week the profile will be applied. Then set the time periods and the operating modes on the timeline. Different timelines can be created for different days. If the operating mode requires, the managers also must be determined.

By default the whole timeline is in Controlled mode.

Operating modes:

- **Controlled:** The users can pass through whose have the privileges to open the door.
- **Open:** The door is open, anyone can enter to the area.
- **Closed:** The door is closed, therefore no one can enter, even if the user has privilege to enter. The closed doors will open in case of emergency, for instance when the fire alarm goes off.
- **Managers only:** Only users with managerial privileges can pass through the door. The manager users can be chosen in the assign profile window.

- **Exit only:** When the door is completely locked, there is a risk of someone being trapped in the room. In “only exit” mode the users cannot enter the area, but they are able to get out. Manager users can go inward.
- **Enter only:** Opposite of the Exit only mode.
- **Manager ->…**: The operation mode changes due to valid card reading of a manager. This way, a person with managerial rights can change the operating mode with his or her own badge without opening the software

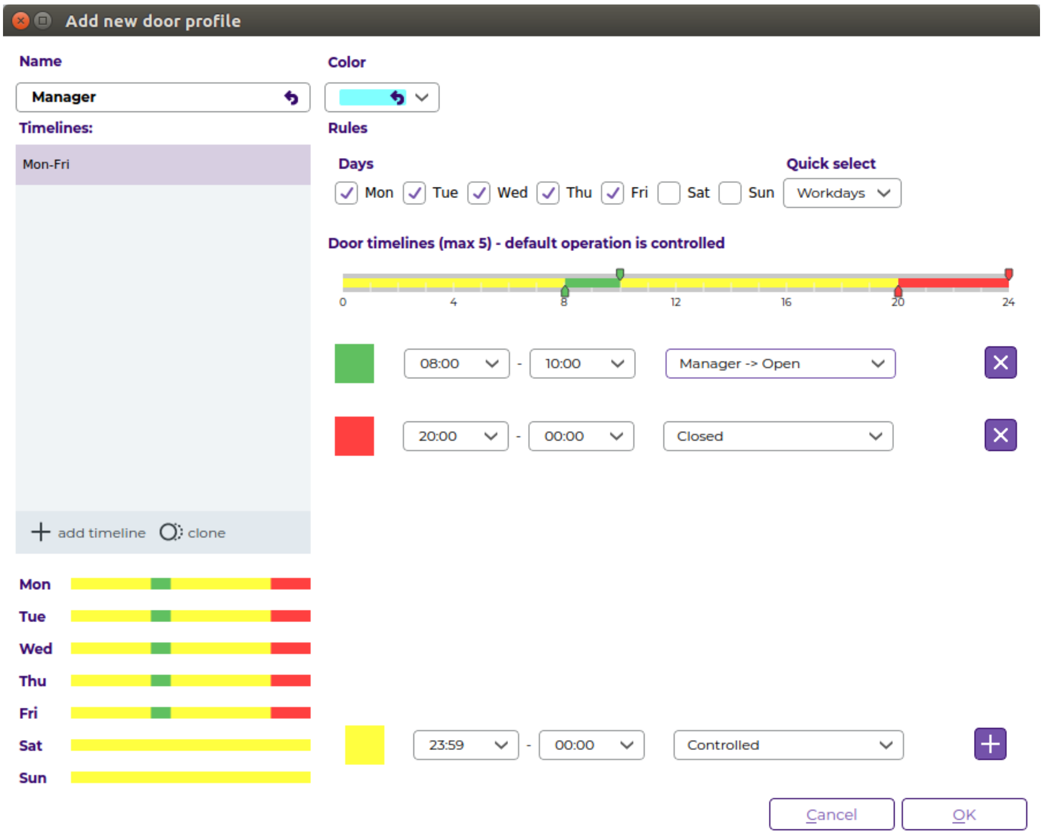
Assign profile: Each door profile can be assigned to any doors. In addition, in the dialog window the profile time range and the manager users must be determined.

Copy settings: If you already set a door profile, the existing door profile settings can be copied. This way you just need to modify the different data.

The Door Profiles tab lists the default and created door profiles. Clicking on them the preview can be seen. The color codes indicate which operating modes are active at which time range.

The doors tab shows the list of doors and the assigned profiles. You can see what profiles each door was operating on.

Profile History: You can check the history of previously assigned profiles.



Add new door profile

Name: Manager

Color

Timelines: Mon-Fri

Rules

Days: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

Quick select: Workdays

Door timelines (max 5) - default operation is controlled

🟩 08:00 - 10:00 Manager -> Open

🟥 20:00 - 00:00 Closed

🟨 23:59 - 00:00 Controlled

Interlock

With interlock you can create areas, in which only one door can be open at the same time. The doors in the same interlock area have to belong to the same controller.

***TIP:** This feature is useful where you have to keep air pressure difference between rooms. For example in laboratories or in operating rooms.*

Create new interlock area:

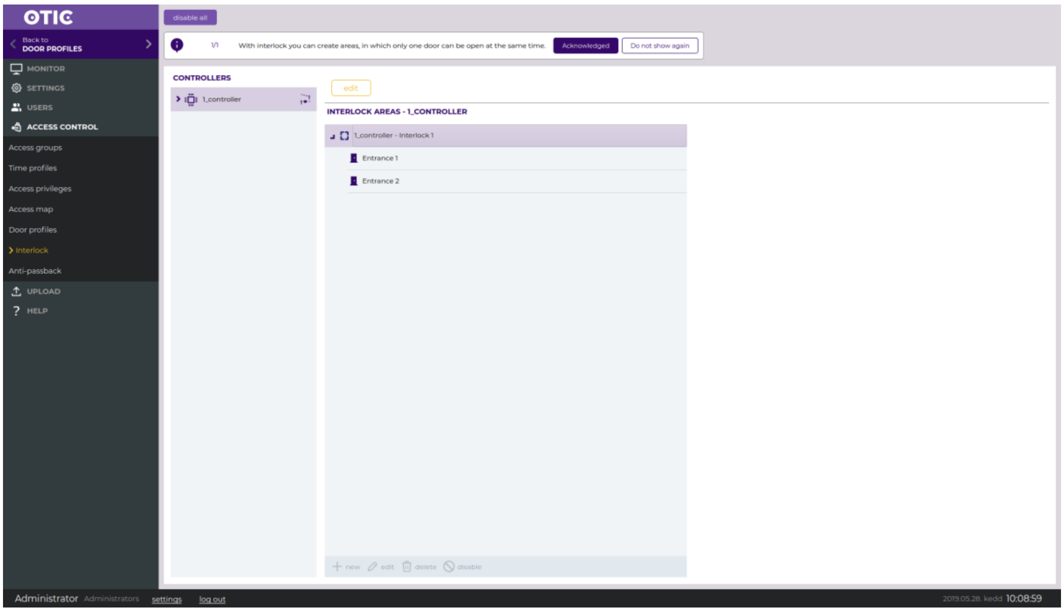
1. step: Select the controller.

2. step: Click the Edit button.

3. step: Click the new + button, type the name of the area and select the doors. Then press OK.

4. step: Save the settings.

You can disable temporarily the function with the disable ⃠ icon.



1/1 With interlock you can create areas, in which only one door can be open at the same time.

ANTI-PASSBACK

Anti-passback is used to prevent the users to pass back their cards, or neglect card reading. Anti-passback violations can generate alerts, or the user can be blocked optionally.

Users or groups can be marked as exceptions, thus no violation will be reported.

Settings

Areas are defined using the readers of the same controller.

Anti-passback method:

- **Log only**: The users may pass the gateway according to their privileges, even if they did not identify themselves on the previous reader. The system generates a warning event and an alert (if checked).

- **Block:** If the users did not read their card previously on the appropriate reader, the system will prevent to pass through. The user has to read his/her card on the appropriate reader to enter.

Alert on violation: When someone transgress the anti-passback rule (log only or block), the system generates an alert.

Create an anti-passback rule:

1. step: Select the controller

2. step: Press the Edit button and select the anti-passback method. Check the „Alert on violation” checkbox if required.

3. step: Press the new + button, type the name of the area and select the inward and the outward readers.

4. step: Each area must have at least one IN and one OUT reader.

5. step: You can add exception users or access groups. They can enter even if the rule would not permit them.

6. step: Save the settings.

You can disable temporarily the function with the disable ⊘ icon.

UPLOAD

The upload button turns yellow if there are pending changes. You have to navigate in the Upload menu and click the „upload now” button.

In the Upload history menu you can view the previous successful or failed uploads.

HELP

You can find the User manual here.

Please read carefully before the first use.

SOFTWARE UPGRADE

If there is an available upgrade, the software generates a notification on the Dashboard. The upgrade process has to start manually. Close the running Otic software. Start the „Maintenance tool” program (it is in the installation folder).

It is recommended to create a backup of the database and the installation folder. The Maintenance tool connect to the central server, download and install the update. After a successful upgrade, you can start the updated software.

ABOUT

Information about the software displayed here.