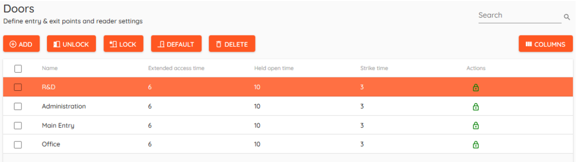
Access points

Doors

At this tab, all door configurations are made. Each Location door list is shown separately.

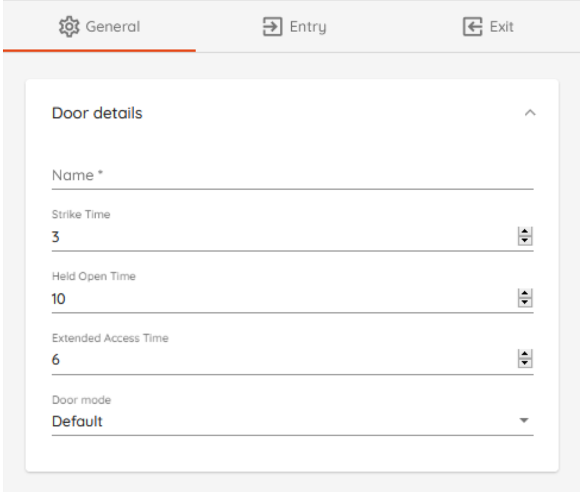


Doors

Define entry & exit points and reader settings

□	Name	Extended access time	Held open time	Strike time	Actions
□	R&D	6	10	3	🔒
□	Administration	6	10	3	🔒
□	Main Entry	6	10	3	🔒
□	Office	6	10	3	🔒

Control button	Function
UNLOCK	Unlocks the door for unlimited time.
LOCK	Locks the door for unlimited time. During the lock, nobody can access.
DEFAULT	Disables "Unlock" or "Lock "mode and sets door for the default operation.
🔒	Unlocks the door for strike time only.
🔓	Indicates state that door is unlocked.



Door details

Name *

Strike Time: 3

Held Open Time: 10

Extended Access Time: 6

Door mode: Default

Create new door

HID EDGE EVO EH400 - 400, HID EDGE EVO EHR40-K, HID EDGE EVO EHRP40-K doesn't support 2 separate doors configuration.

To create new access level, press press ADD

Name - name of the doors (required field).

Strike Time - time in seconds for the lock remaining unlocked after granting access.

Help Open Time - the time given for closing the door. If the door is not closed within this time period, “Held open” alarm event is generated.

Extended Access Time - time in seconds for the lock remaining unlocked after granting access, when user has extended access.

Door mode "Unlock" - in this mode doors will be unlocked using schedule.

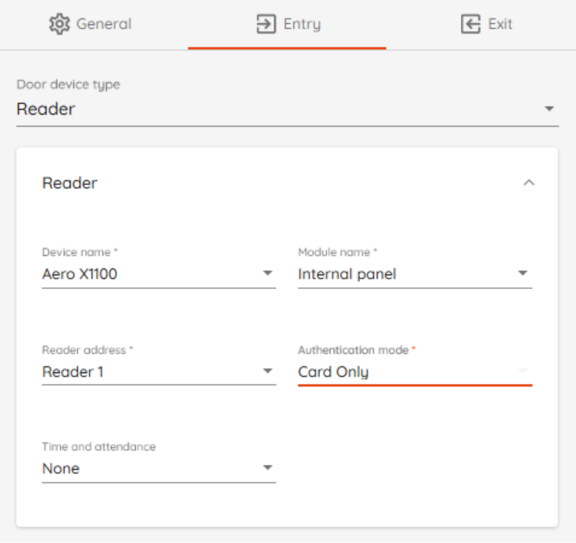
Entry

Device Name -select device from the list, to which doors will be assigned.

Module name - depending on the system setup, select module at which reader is located.

Reader address - Reader physical location on the controller.

Authentication mode - select authentication methods allowed for the door.



Door device type: Reader

Reader

Device name *: Aero X1100

Module name *: Internal panel

Reader address *: Reader 1

Authentication mode *: Card Only

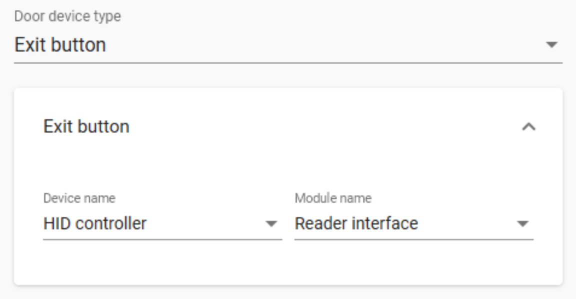
Time and attendance: None

Exit

Device name - select device, at which exit button is installed

Module name - depending on the system setup, select module at which exit button is located.

If reader is used, configuration steps are the same as entry.



Door device type: Exit button

Exit button

Device name: HID controller

Module name: Reader interface

Advanced settings

- Suppress "Door forced open " alarm - when door is opened without access grant, forced opened event will not be generated.
- "Classroom" mode - when enabled, double swipe valid credential over short period will change door state to "Unlocked" state. Door will remain in this state, until next double swipe . This functionality is not supported by HID VertX EVO series devices.
- LED & Beeper template - will activate reader color template configured at "Settings Devices" tab. Wiegand reader color scheme is limited only to green and red colors.
- Use "Quiet REX" - Generate event that exit button is pressed, but do not trigger strike relay.

Contact type settings

Assign input default state. For "REX" input, door must have have exit button configured.

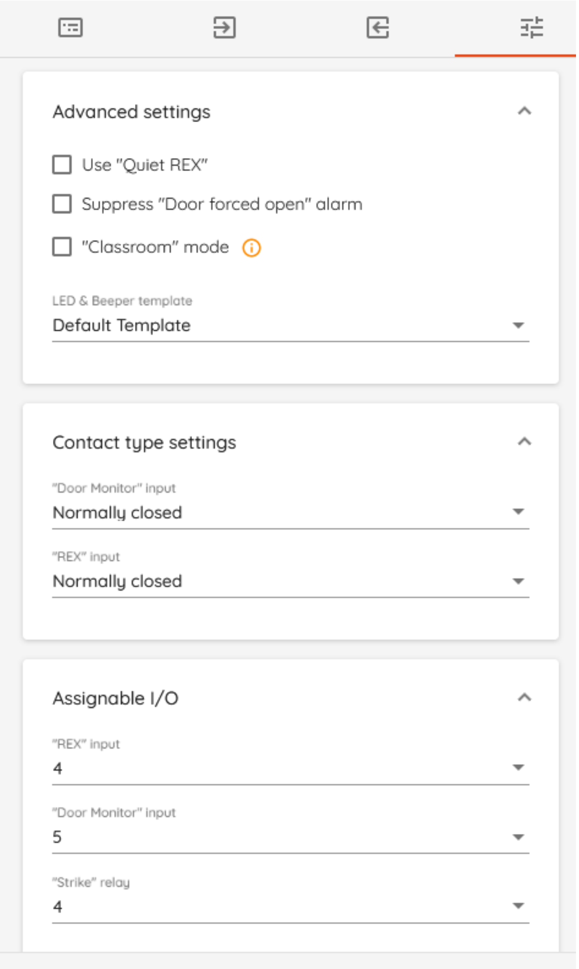
Possible contact types:

- Normally open
- Normally closed
- Supervised 2K1K normally closed
- Supervised 2K1K normally open

Assignable I/O

Select inputs for door configuration. Same input should not be assigned for different purposes.

HID VertX EVO series devices dedicated inputs cannot be modified.



Advanced settings

□ Use "Quiet REX"

□ Suppress "Door forced open" alarm

□ "Classroom" mode

LED & Beeper template: Default Template

Contact type settings

"Door Monitor" input: Normally closed

"REX" input: Normally closed

Assignable I/O

"REX" input: 4

"Door Monitor" input: 5

"Strike" relay: 4

OSDP configuration

Hardware support:

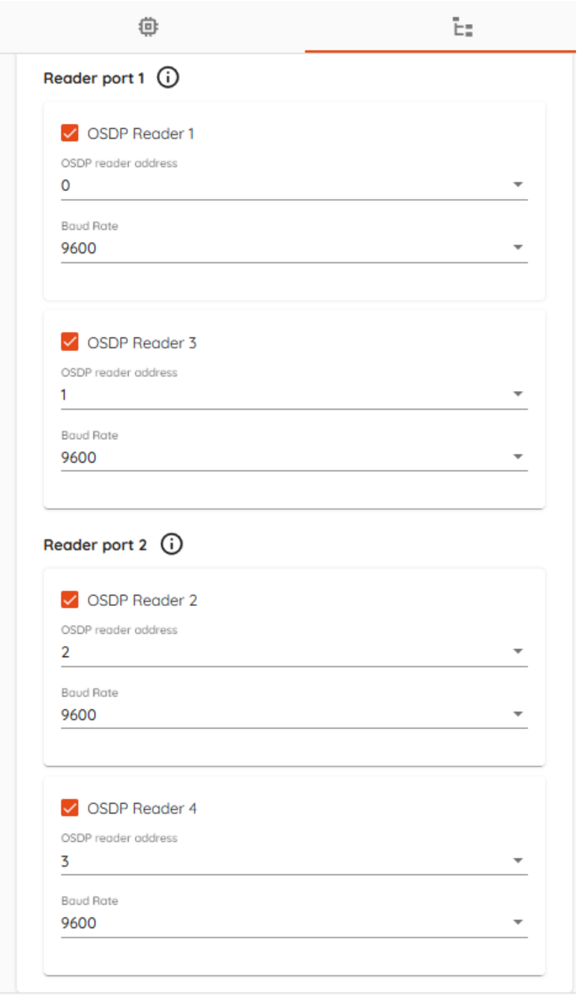
HID Aero - max 2 readers per 1 reader port configured for OSDP.

Mercury - max 1 reader per 1 reader port configured for OSDP.

For each reader, you can assign internal address (0 - 3). Don't use same reader address on the same port and only single reader is used per port, configure those readers for OSDP Reader 1 and OSDP Reader 2

On reader port 1, "OSDP Reader 1" and "OSDP Reader 3" can be assigned with internal address.

On reader port 2, "OSDP Reader 2" and "OSDP Reader 4" can be assigned with internal address.



Reader port 1

☑ OSDP Reader 1

OSDP reader address: 0

Baud Rate: 9600

☑ OSDP Reader 3

OSDP reader address: 1

Baud Rate: 9600

Reader port 2

☑ OSDP Reader 2

OSDP reader address: 2

Baud Rate: 9600

☑ OSDP Reader 4

OSDP reader address: 3

Baud Rate: 9600

Keep in mind, that later at door configuration, "OSDP Reader 1", "OSDP Reader 2".. etc. will be used as reference and not the reader address.

Available dedicated door inputs configuration table for Aero X1100, X100 controllers:

Door configuration	Input	Function
Up to 2 doors	IN1, IN3	Door monitor
	IN2, IN4	Rex button if configured
More than 2 doors	IN1, IN2, IN3, IN4	Door monitor

Anti - Passback

Anti Pass-back (APB) feature prevents an access card or PIN from being used to enter an area a second time without first leaving it (so that the card cannot be passed back to a second person who wants to enter). APB only applies within single controller scope (controller + modules).

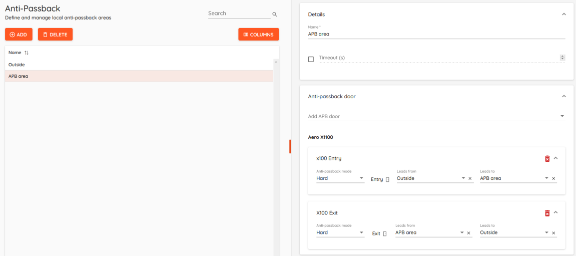
It is recommended to create areas before selecting readers.

Name - name of determined APB area.

Timeout - timed value in seconds, after which APB status is reset for the user.

Add APB door - select available door from the list and assign to APB Area. Door must have Entry/Exit readers in order to selected for APB.

APB reset can be executed at "Users" tab.



Anti-Passback

Define and manage local anti-passback areas

Name
Outside
APB area

Details

Name *: APB area

☐ Timeout (s)

Anti-passback door

Add APB door

Aero X1100

x100 Entry

Anti-passback mode		Leads from	Leads to
Hard	Entry	Outside	APB area

X100 Exit

Anti-passback mode		Leads from	Leads to
Hard	Exit	APB area	Outside

Door monitor must be activated, otherwise APB will not be applied to the user.

Creating, updating, deleting access level will reset HID APB status for all users!

How to create APB Area

1. Click "Add" button.
2. Enter APB Area name.
3. Click "Add APB door" and select reader.
4. Select "APB mode".
   Hard - access is denied and "Access denied" event with "Anti-passback violation" reason is generated.
   Soft - access is granted and "Access granted" event with "Anti-passback violation" reason is generated.

5. Select "Leads from" and "Leads to" areas.
6. Depending on configuration, these doors can be used for area entry or exit. If the first door is configured to enter APB area, configure door to exit APB area by adding additional reader to area using 3-5 steps.

⚠ **Supported devices and configurations**

Anti-Passback feature is supported on HID Aero and Mercury Security devices only.

The feature is implemented in hardware mode to ensure standalone operation in case of connection loss to the server. Therefore, APB zone(s) should be designed within the scope and capacity of a single master controller, and will be limited to the maximum supported door module count on the said device(s).