

Quick start guide

CredoID is an innovative access control software and has been designed with the goal of providing a simple and at the same time highly effective interface to enable users of all levels to have a complete control over the system. This quick start guide will provide steps for quick access control system setup, including user management, access rights, schedules and reports.

- [1. Installation](#)
 - [Troubleshooting](#)
- [2. Device Preparation](#)
 - [Aperio](#)
 - [HID configuration](#)
 - [Mercury configuration](#)
- [3. How to add device](#)
 - [Aperio Device](#)
 - [ASB Security device](#)
 - [Digifort server](#)
 - [HID device](#)
 - [Mercury Device](#)
- [4. How to create schedules](#)
- [5. How to create doors](#)
- [6. How to create access levels](#)
- [7. How to create user](#)
- [8. How to create report](#)

1. Installation

CredoID installation and application requires latest Windows updates.

1. Run the installer.
2. Select components to be installed.

If you are planning to install Microsoft SQL server manually, uncheck "Preconfigured SQL express server"

3. To change installation folder press  button.
4. Press Install.



- CredoID service
- CredoID core service
- Preconfigured SQL express server

I accept [Midpoint-Security license terms](#)



Install

Exit

Troubleshooting

Problem	Solution
Installer is not starting.	Install pending Windows updates. Restart machine and run installer again.

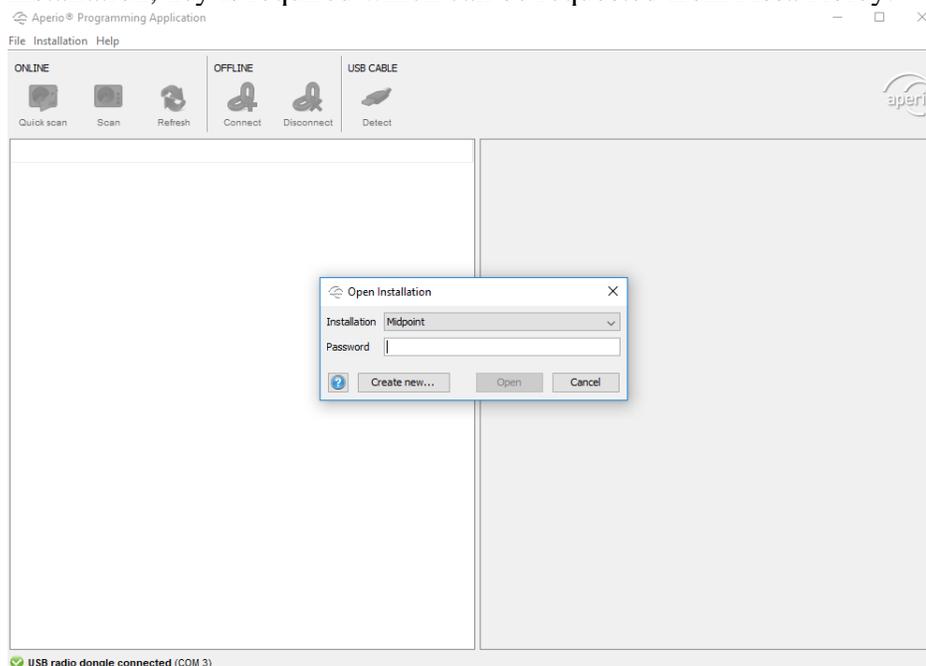
2. Device Preparation

Controller network setup depends on the configuration of your network. You may use either DHCP server or assign static IP addresses to controllers. If the controller is on a different segment of the network, you must enter gateway addresses as well.

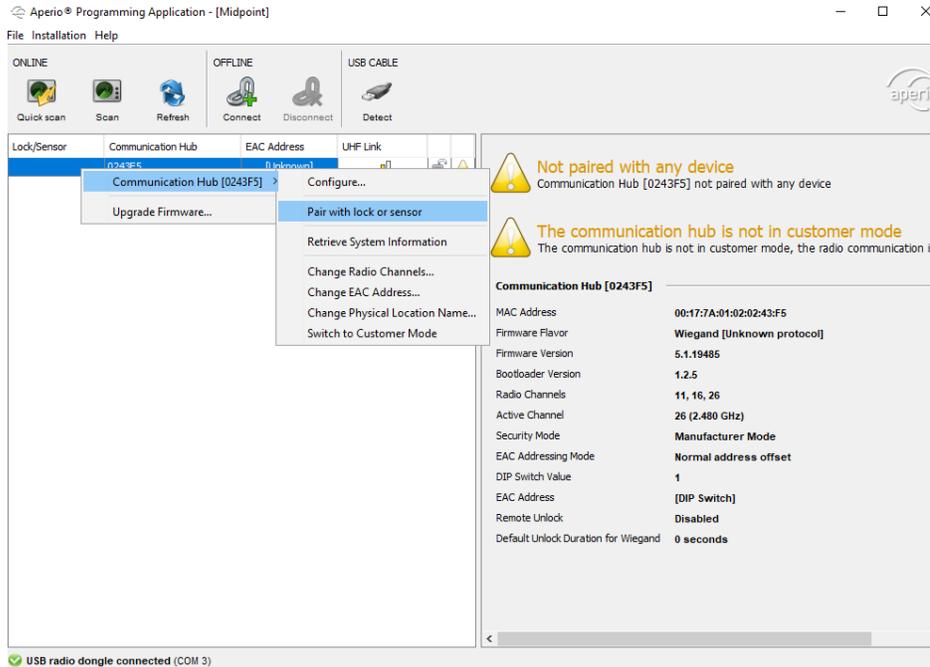
- [Aperio](#)
- [HID configuration](#)
- [Mercury configuration](#)

Aperio

1. For Aperio Hub configuration, Aperio configuration dongle may be required for correct system setup, if the Hub was not configured by installer.
2. Launch Aperio Programming Application and open installation or create new. For new installation, key is required which can be requested from Assa Abloy.



3. **USB radio dongle connected (COM 3)**
4. Press "Scan" Button.
5. Hubs with dongle range should appear on the list. Double clicked of target hub.
6. In the List, second click on hub and press "Pair with lock or sensor" and follow further instructions.



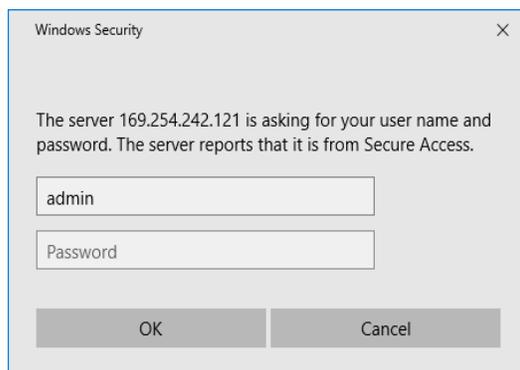
7.

HID configuration

Supported devices: EDGE Plus E400 (E400, ER40, ERP40), EDGE Plus EVO EH400 (EH400, EHR40, EHRP40), VertX EVO V1000, VertX EVO V2000.

Steps to configure HID device:

1. Open a web browser and enter the HID devices IP. By default, every HID controller is configured to respond to a fixed IP address, that is 169.254.242.121. Be sure that your network settings are configured correctly to be able to connect to the controller.
2. You should be greeted with a login screen. If connecting to the controller for the first time, in the User name field, enter "admin" and leave the password field empty. If not, enter a configured password.



3. After authentication is done, you should be presented with basic setup information window, where network and other settings can be configured. It is highly recommended to configure a static IP address, for more stable connection. After configuring network settings, set up a password (optional). Set CS/HOST Addressing to the service machine address, where CredoID service is installed and running. Press "Submit" to update configuration.

Basic Network Setup

Controller Addressing DHCP Static

Allows for DHCP (Dynamic Host Configuration Protocol) or maintains a Static IP address (which is a permanently assigned address) for the controller's network parameters. For Static, the Controller Addressing information should be provided by the local network administrator.

IP Address: . . .

A number that identifies the controller on a network. This address will be used to access the controller. Example: 192.168.1.129

Subnet Mask: . . .

A number used to determine which IP addresses are contained within the local network.

Default Gateway: . . .

The Default Gateway forwards traffic to a destination outside of the subnet of the controller. This address provides a communication link between the controller and external networks.

Primary DNS Server: . . .

Primary Server that translates domain names into IP addresses.

Secondary DNS Server: . . .

Alternate Server that translates domain names into IP addresses.

Basic Central Station/Host Communications Setup

CS/Host Addressing

IP Address: . . .

A number that identifies the Central Station/Host on a network. This address will be used by the controller to access the Central Station/Host. Example: 192.168.1.130

-- OR --

Host Name:

An identifier used by the controller to access a Central Station/Host on a network. Example: CSHost.CompanyX.com

Here I Am Interval (sec):

The time interval in which a controller sends a Here I Am message to a Central Station/Host. Valid entry is 20 to 86400 seconds.

Login Password

The login password for the *admin* user has been set.

[Change Login Password](#)

Submit

Copyright (c) 2010-2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved. This software is protected by copyright law and international treaties. Any unauthorized reproduction, distribution or use of the software is prohibited.

Mercury configuration

1. Connect an Ethernet cable to the controller and enable controllers default settings, by turning ON switch '2' in DIP switches.
2. Open web browser and connect to controller over IP address: 192.168.0.251

LP1501 Configuration Manager

Login

Enter your user name and password.

Username:
Password:

Login

3. Turn on switch "1" to enable default login details:
Username: admin
Password: password
4. At "Network" tab configure IP address of the device.
5. At "Host Comm" set "Host IP" to machine address, where CredoID service is running.
Set "Connection Mode" to "Continuous".

Home	Host Communication	
Network	Communication Address: <input type="text" value="0"/> <input type="checkbox"/> Use IPv6 Only	
Host Comm	Primary Host Port	
Device Info	Connection Type: <input type="text" value="IP Client"/>	Data Security: <input type="text" value="TLS if Available"/>
Advanced Networking	Interface: <input type="text" value="NIC1"/>	Port Number: <input type="text" value="3001"/>
Users	Host IP: <input type="text" value="192.168.11.20"/>	Retry Interval: <input type="text" value="5sec"/>
Auto-Save	Connection Mode: <input type="text" value="Continuous"/>	<input type="checkbox"/> Enable Peer Certificate
Load Certificate	Alternate Host Port	
OSDP File Transfer	Connection Type: <input type="text" value="Disabled"/>	Data Security: <input type="text" value="None"/>
Status	<input type="button" value="Accept"/>	
Security Options	* Select APPLY SETTINGS to save changes.	
Diagnostic		
Restore/Default		
Apply Settings		
Log Out		

6. Press "Accept" and then "Apply Settings". Set all switches to OFF.

3. How to add device

If devices were configured correctly, it should appear at discovered devices

1. Press on Hardware → Devices → Discover
2. Select device from list, which needs to be added to the system, press "Select" button.

Each device has slight different setting options, select the link accordingly to your device:

- [Aperio Device](#)
- [ASB Security device](#)
- [Digifort server](#)
- [HID device](#)
- [Mercury Device](#)

Windows Firewall may be blocking the connection and device will not appear on "Discovered" list so additional ports opening may be required in Windows Firewall:

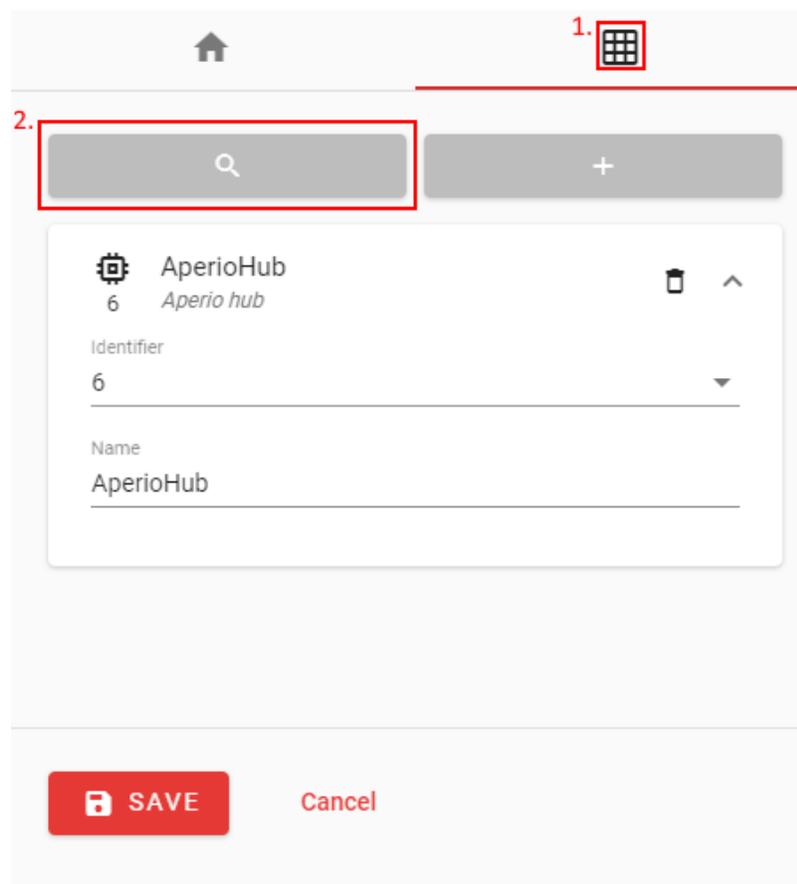
- Mercury – 3001;
- HID – 4050, 4070;
- ASB Security – 20002, 2005;

Aperio Device

Select Mercury device, at which Aperio Hub is connected over RS484.

1. Press "Device modules"
2. Press "Search Modules" button.

During door configuration, select "Module name" as configured at the device modules (in example AperioHub).



ASB Security device

ASB Security panels cannot be detected automatically and needs to be added manually. Make sure no other software is connected to the device, otherwise connection may not be established.

1. Enter device name.
2. Enter device MAC address.
3. Enter device IP address.
4. Enter Installer code.
5. Enter flash password.

Warning! To apply changes device must be disabled/enabled

Main ^

1.

Identifier

2.
Field is required

Network ^

3.

Encrypted configuration port *
20002

Diagnostics port *
20005

4.

5.

6.

6. Confirm flash password.

After these steps press "Save" to save device.

Digifort server

In order to use cameras on Digifort server, Digifort service must be installed and running.

1. Press "Add" button.
2. Create a name.
3. Create "Identifier". It must be unique on the system.
4. Enter machine IP address, where Digifort service is running.
5. Press "Save".
6. Open "Device modules".
7. Press "Detect devices" button. All configured cameras on Digifort service should appear on the list.

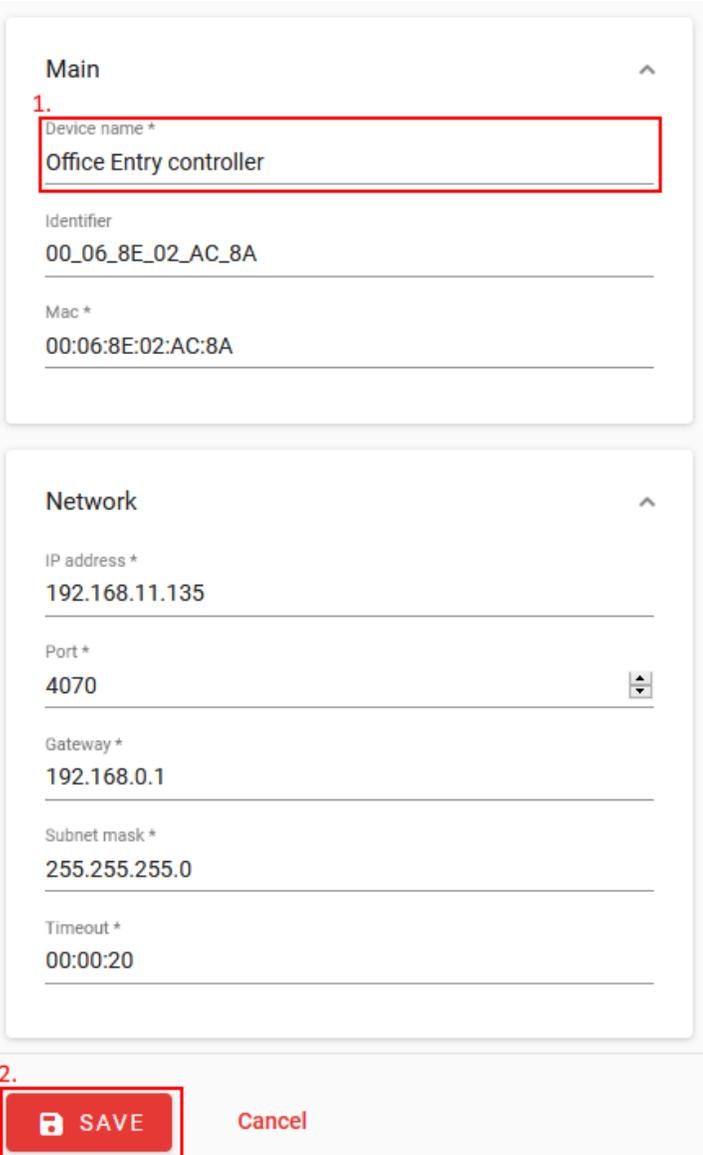
The screenshot shows the 'Devices' management interface. The left pane has a table with columns 'Identifier', 'Port', and 'Name'. The right pane has a form with sections 'Main' and 'Network'. The 'Main' section has fields for 'Device name *', 'Identifier *', 'Username *' (with value '20005'), and 'Password *'. The 'Network' section has fields for 'IP address *', 'Port *' (with value '8601'), and 'Timeout *' (with value '00:00:00:20'). A red box labeled '1' highlights the 'ADD' button. Red boxes labeled '2', '3', and '4' highlight the 'Device name *', 'Identifier *', and 'IP address *' fields respectively. A red box labeled '5' highlights the 'SAVE' button.

The screenshot shows the 'Device modules' interface. The top bar has a grid icon highlighted with a red box and number '6'. Below is a search bar highlighted with a red box and number '7'. The main area shows a list of devices, with one device named 'Camera 1' listed as a 'Video camera'. At the bottom, there are 'SAVE' and 'Cancel' buttons.

HID device

VertX EVO V2000

1. Enter device name. Use meaningful name like "Front door controller" or similar, because later device name will be used when creating doors, access levels and etc.
2. Press "Save".
3. Device should appear on the list with "Out of Sync" state.
4. Press "Sync"  to upload all the configuration the device.



Main ^

1. Device name *
Office Entry controller

Identifier
00_06_8E_02_AC_8A

Mac *
00:06:8E:02:AC:8A

Network ^

IP address *
192.168.11.135

Port *
4070

Gateway *
192.168.0.1

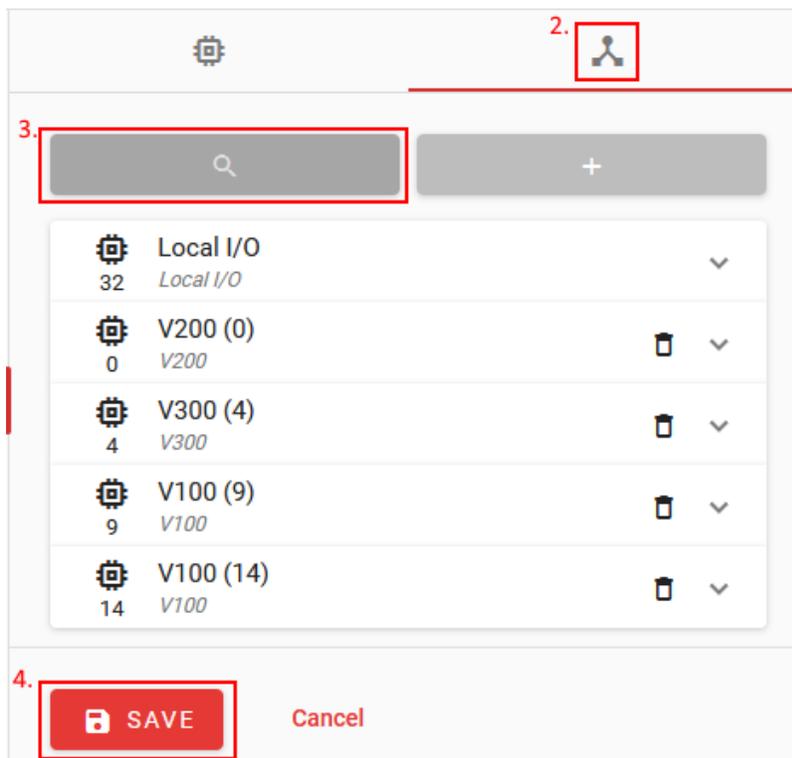
Subnet mask *
255.255.255.0

Timeout *
00:00:20

2.  Cancel

VertX EVO V1000

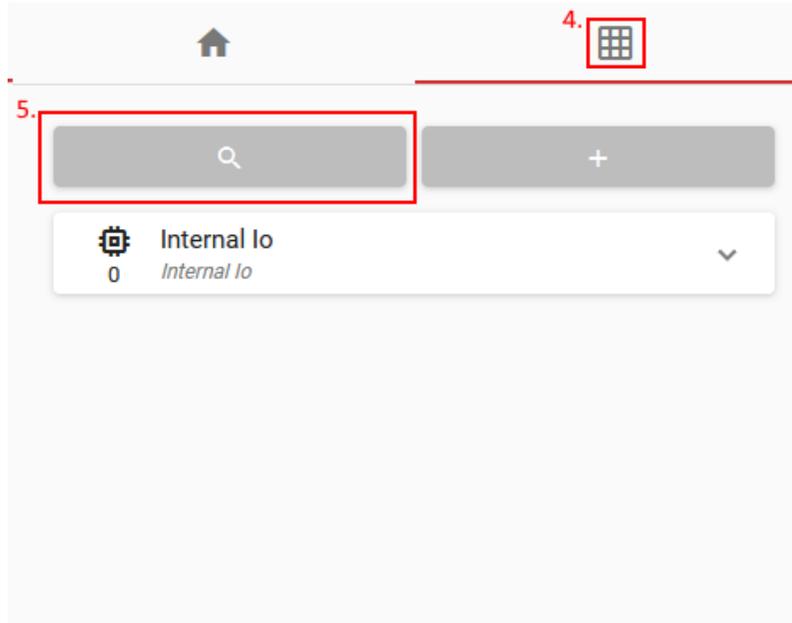
1. First steps are the same as adding EVO V2000 controller.
2. Switch to "Device modules" .
3. Press Detect Modules Button.
4. Press Save.
5. Press "Sync"  to upload all the configuration the device.



Mercury Device

LP1501, EP1501

1. Enter device name.
2. Mark checkbox "Use First Port For RS485" if Mercury modules will be connected instead of reader. If readers will be used, skip to step 6.
3. Set baud rate of RS485. This field only appears if port 1 will be used for RS485 communication.
4. Press "Device modules".
5. Press "Detect modules" button. All connected modules should appear on the list.



6. Press "Save"

Main ^

1. Device name *
LP1501

Identifier
00_OF_E5_07_B0_2E

Mac *
00:0F:E5:07:B0:2E

Network ^

IP address *
192.168.11.205

Port *
3001

Gateway *
192.168.0.1

Subnet Mask *
255.255.255.0

2. Use First Port For RS485

3. Baud Rate
38400

6. Cancel

LP1502, EP1502, LP2500, EP2500, LP4502, EP4502

1. Enter device name.
2. Set RS-485 baud rate (if external modules are used).
3. Press "Save"

Main

1. Device name *
LP1502

Identifier
00_05_B1_00_DD_AE

Mac *
00:05:B1:00:DD:AE

Network

IP address *
78.78.7.87

Port *
3001

Gateway *
192.168.0.1

Subnet Mask *
255.255.255.0

2. Baud Rate
38400

Baud Rate 2
38400

3. **SAVE** Cancel

4. How to create schedules

Schedules will be used for access levels.

1. Open "Time Settings → Schedules".
2. Press "Add" button.
3. Enter "Schedule" name.
4. Select "Day" of the new schedule.
5. Select "Start" time interval and "End" time interval.

To change time, select format, change your browser language accordingly

6. Press "Add Interval" button.
7. After adding all intervals in schedule, press "Save".

The screenshot shows a web interface for creating a schedule. It is divided into two main sections: 'Schedule' and 'Days'.

Schedule Section: A text input field labeled 'Name *' contains the text 'Custom schedule'. A red box labeled '3.' highlights this field.

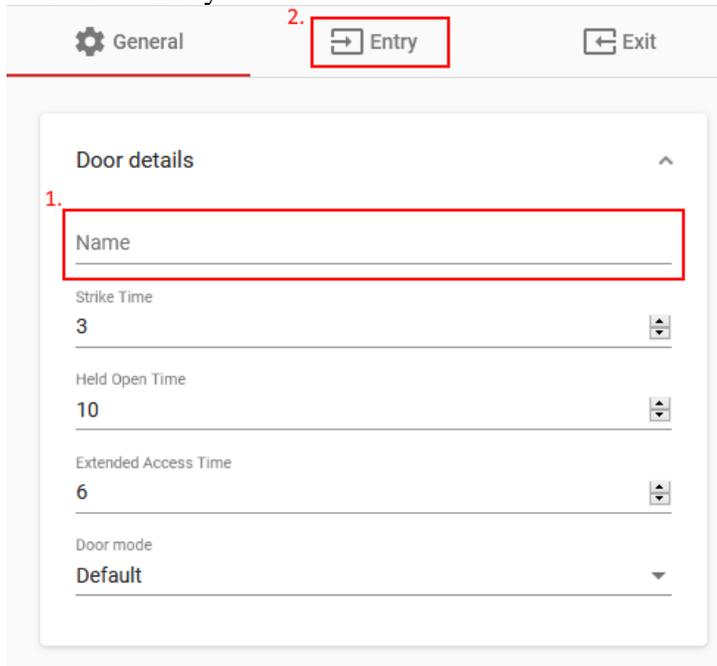
Days Section: This section contains a 'Days *' dropdown menu with 'Mo' selected, a 'Start *' time field with '08:00', and an 'End *' time field with '17:00'. A red box labeled '4.' highlights the 'Days *' dropdown, and another red box labeled '5.' highlights the 'Start *' and 'End *' time fields. To the right of these fields are two buttons: a red 'ADD INTERVAL' button (labeled '6.') and a grey 'CLEAR ALL' button.

Calendar Grid: Below the input fields is a calendar grid with columns numbered 00 to 23 and rows labeled Su, Mo, Tu, We, Th, Fr, Sa, NH, and OH. The grid is currently empty.

Bottom Section: At the bottom left, there is a red 'SAVE' button (labeled '7.') and a 'Cancel' button.

5. How to create doors

1. Enter door name.
2. Switch to "Entry" tab.



The screenshot shows a configuration interface with three tabs: "General", "Entry", and "Exit". The "Entry" tab is selected and highlighted with a red box, labeled with a red "2.". Below the tabs is a "Door details" section, which is expanded to show several fields. The "Name" field is highlighted with a red box and labeled with a red "1.". The other fields are "Strike Time" (set to 3), "Held Open Time" (set to 10), "Extended Access Time" (set to 6), and "Door mode" (set to Default).

3. Select "Door device type".
4. Select "Device name" from the list.
5. Select "Module name" of the device.
6. Select "Reader address" from the list.
7. Set "Authentication mode". If set to "None", doors cannot be accessed.

General Entry **8. Exit**

3. Door device type
Reader

Reader

4. Device name **5.** Module name

6. Reader address **7.** Authentication mode
None

Time and attendance
None

8. Switch to Exit tab.
9. Select "Door device type" to exit button. (If reader type is selected, repeat steps from nr. 4)
10. Select "Device Name" from the list.
11. Select "Module name" from the list.
12. Press "Save". After saving doors, device Synchronization is required at the "Hardware → Devices tab".

General Entry Exit

9. Door device type
Exit button

Exit button

10. Device name **11.** Module name

6. How to create access levels

Access level is the selection of doors that can be assigned to the user.

1. Open "Users → Access Levels".
2. Press "Add" button.
3. Enter door name.
4. Select doors, which will be assigned to access level.

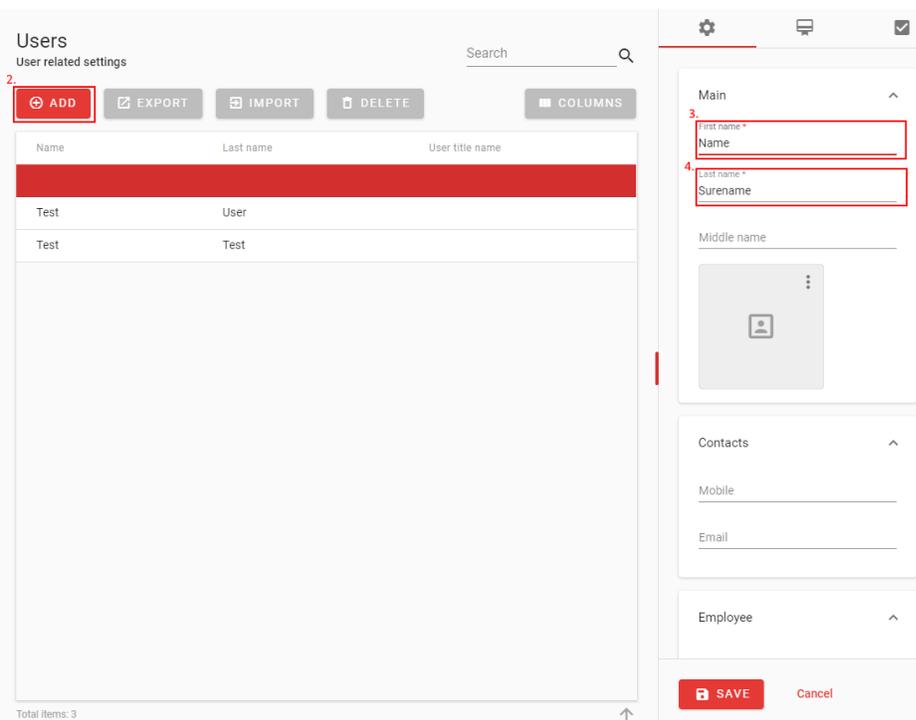
The screenshot shows two panels. The top panel, titled 'Access level', contains a text input field labeled 'Name *' which is highlighted with a red box and the number '3.'. The bottom panel, titled 'Doors', contains two columns. The left column has two checkboxes: 'Front Door' and 'Back door', both highlighted with a red box and the number '4.'. The right column has two 'Entry' dropdown menus, both set to 'Always', also highlighted with a red box and the number '5.'.

5. Assign schedule to access level for each door.
6. Press Save.

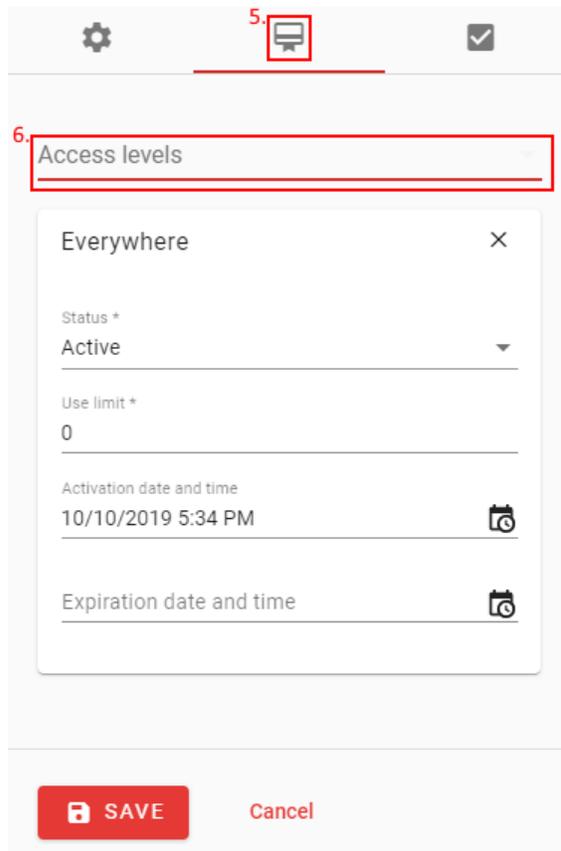
7. How to create user

1. Open Users → Users tab.
2. Press Add Button.
3. Enter "First Name" and "Last Name" (required fields).
4. Enter other fields if required.

When adding new Company/Department/Title, if it doesn't exist, press ADD button at the end of the input field.



5. Switch to  (Access Levels) tab.



6. Assign Access level to user (can be selected more than one).
7. Switch to (identifications) tab.
8. Press  button to add new identification set.
9. Assign card by entering card details manually or by Scan card tool .

Scan card

Select device

Evo2k

SCAN

Cancel

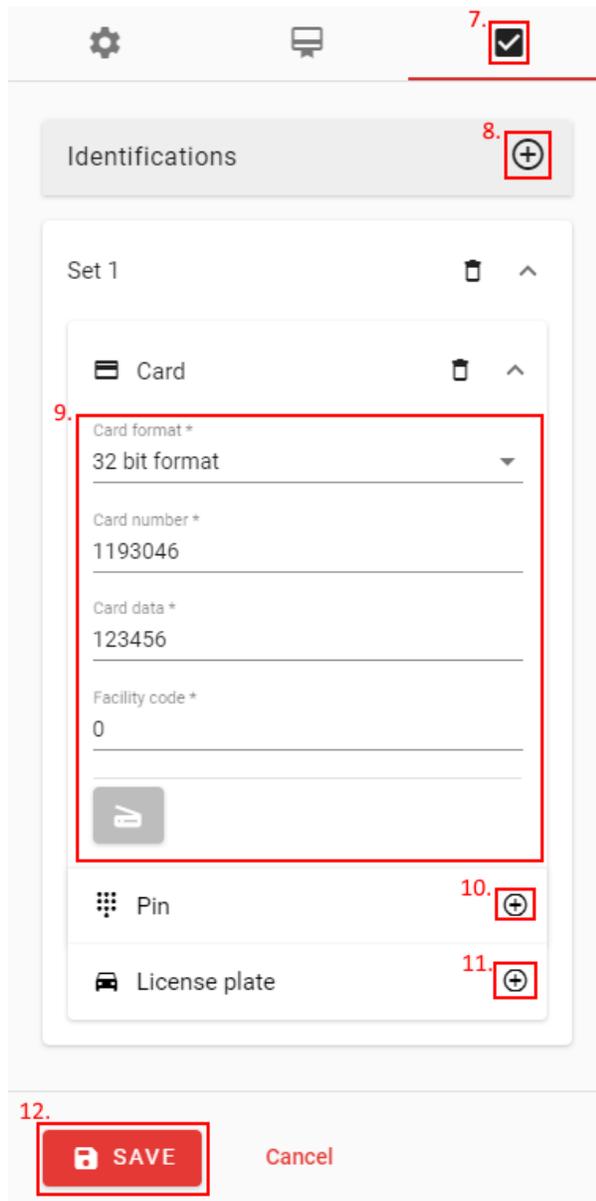
Scan Card

1. Select Device from the list, at which card will be scanned.
2. Press Scan and present Card to the reader connected to the selected device.

10. Assign PIN code by pressing  (optional).

11. Assign License plate  (optional).

12. Press "Save" button.



7. 

8. 

9. 

10. 

11. 

12. 

Cancel

8. How to create report

Open "Monitoring" → "Events" tab.

1. Press "Export" button.
Additional "Report" window will open.
2. Select "Start" date and time, from which events will be added.
3. Select "End" date and time, which events will be added.
4. Enter "Search" keyword, by which events in the report will be filtered.
5. Press "Generate Report" button.

Generated report should appear in the browser window as downloadable file.

The screenshot shows the 'Events' interface with the following elements:

- Header: 'Events' and 'Events related settings'.
- Filters: 'From' and 'To' date pickers, 'Filters' dropdown, and 'Search' input.
- Buttons: 'EXPORT' (highlighted with a red box and '1'), 'IMPORT', and 'COLUMNS'.
- Table:

Type name	Time	First name	Door name
Device offline	2019-10-11 09:45:38		
Tamper off	2019-10-11 09:17:32		
AC normal	2019-10-11 09:17:32		
Battery normal	2019-10-11 09:17:32		
Door closed	2019-10-11 09:17:32		
Door forced open cleared	2019-10-11 09:17:32		
Exit button released	2019-10-11 09:17:32		

The screenshot shows the 'Report' dialog box with the following elements:

- Header: 'Report'.
- Fields:

2. Start *: 10/02/2019 10:50 AM
3. End *: 10/11/2019 10:06 AM
4. Search: Search
5. GENERATE REPORT button (highlighted with a red box and '5').

Close