

# 1Control Web Admin Area

The 1Control web admin area allows you to manage 1Control ACCESS and 1Control ENTRY devices.

It is accessible here: <https://web.1control.eu/web/en/>

## ‘Your Devices’ page

This page shows all the devices associated with your account. It is possible to view them in list mode and in map mode.

The screenshot displays the 1Control Web Admin Area interface. At the top, there is a navigation bar with the 1Control logo and several menu items: 'Your devices', 'Executions', 'Users', 'Groups', 'Alias', 'Assistance', 'Profile', and 'Log out'. A user profile icon is also present. Below the navigation bar is a 'Welcome' message: 'Welcome to the 1Control Web Administrative Area. From here you can manage your devices, create and edit shares, view the access history and manage all the services you have activated.'

The main section is titled 'Your devices'. It features a 'Filter:' input field and two tabs: 'List' and 'Map'. The 'List' tab is currently selected, showing a card for 'Access Demo' (1Control Access, Serial number: 800013) and a button to 'Add device' (Add another device).

Below the 'List' tab, the 'Map' tab is highlighted with a red box. The map view shows a Google Map with several location pins. The pins are color-coded: a green pin for 'Verniciature Bresciane Cataforesi VBC (SRL)', a blue pin for '1Control', a red pin for 'RISTO BAR OASI DEL GUSTO Temporarily closed', and a blue pin for 'REXENERGY'. A yellow pin for 'New GPR' is also visible. The map includes standard Google Map controls like zoom in/out buttons and a street view icon.


In map mode, the color of the device icon indicates its status:

- Green: 'Open' status (door open)
- Blue: 'Closed' status (door closed)
- Green with letter "F": 'Forced open' status (door always open)
- Red: 'Error' status
- Grey with question mark: 'Unknown' status (if the open/close sensor has been installed, it will be necessary to perform an opening cycle of the device to realign the actual state)
- Grey: 'Offline' status (device has no internet connectivity)

To add a device choose "List" mode and press add. Then select the type of device (an ACCESS device is shown in the figure) and enter the serial number and secret code found in the manual supplied with the device itself.


List

Map



**Access Demo**  
1Control Access  
Serial number: 800013  


DETAILS




**Add device**  
Add another device  

ADD


What type of device do you want to add?




Solo



Dory



Access



Entry

To add a new Access device to the administrative area, you must enter the serial number of the device and its secret code in the area below.

The serial number can be found on a label at the bottom, near the cable gland (it is a 6-digit number starting with an "8").

The secret code can be found in the manual supplied with the device.

Device serial:

Secret code:

CONFIRM

## 'Device details' page

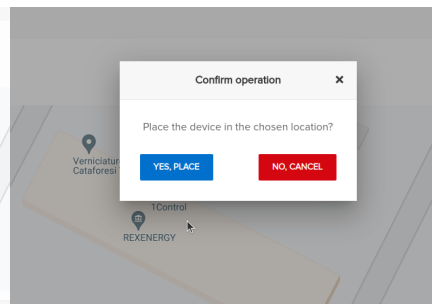
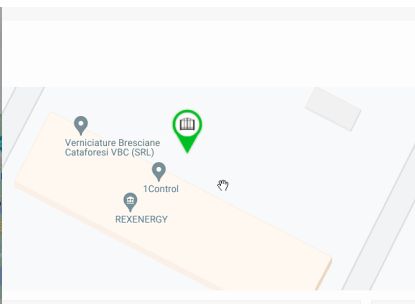
This page shows the details of the device and allows you to control it.

As the first step it is necessary to set the position of the device on the map. This also allows you to prevent unauthorized remote openings.

To place the device press on "Move device", then insert the address where it has been placed, press "Confirm". Once done, the area relative to the address entered is shown on the map. Click on the map on the exact position of the device; a confirmation window will appear, press "Yes, place".

The screenshot displays the 1Control web interface. At the top, there is a navigation bar with links: Your devices, Executions, Users, Groups, Alias, Assistance, Profile, Log out, and a globe icon. Below the navigation bar, the 'Access Demo' section shows a device type of 'Access' and a serial number of '800013'. To the right of this section are two buttons: 'DISCONNECT' (red) and 'MOVE DEVICE' (blue, highlighted with a green border). Below these buttons is a map of the area around Macina, Italy, with a green pin indicating the device location. Below the map, the 'Device details' section is visible, containing fields for 'Telephone number' (No associated number), 'Address' (Via del Mella 13), 'City' (Brescia), and 'State' (IT). To the right of the details is the 'Device status' section, showing 'State: Open', 'Last update: 17:40 - Thu 16 June 2022', and 'Operate the device:' with two buttons: 'OPERATE' (orange) and 'ENABLE FORCED OPEN' (yellow).

The 'Positioning of the device' dialog box is shown. It has a title bar with a close button. The main text says 'Enter the address where you would like to place the device'. Below this is a text input field containing 'Via Del Mella 13 Brescia'. Below the input field, there is a note: 'After confirming the address, the map will show the selected place and it will be possible to select the exact location by clicking with the mouse'. At the bottom, there are two buttons: 'CONFIRM' (blue) and 'CANCEL' (red).



To change the device name (which is shown to users in the app) and other data, press the edit

button



A modal window titled "Device details" with a close button (X) in the top right corner. It contains four input fields: "Device Name:" with the value "Access Demo", "Address:" with "Via del Mella 13", "City:" with "Brescia", and "State:" with "IT". At the bottom, there are two buttons: a blue "CONFIRM" button on the left and a red "CANCEL" button on the right. The modal is overlaid on a background showing an "Access log" table.

In the "Device status" section it is possible to check the device status in real time (open/closed), operate the device (button highlighted in orange) or set the 'forced open' status (button highlighted in yellow, function available only if supported by the automation connected to the device).


In the "Access log" section it is possible to view the accesses made by users with the possibility of indicating a range of dates and filtering by table fields. For example, to search for Mario Rossi's accesses in a selected period or by searching by access method, as in the following image (in red).


The "Access log" interface features a header with the title "Access log". Below the header, there are three filter sections: a green box containing radio buttons for "Today", "Yesterday", and "Personalized" (which is selected); a red box containing a "Filter:" label and a text input field with the value "0000214B"; and a yellow box containing "Start date:" and "End date:" labels, each followed by a date input field (showing "11/1/2022" and "4/28/2023" respectively) and a "CONFIRMATION" button. To the right of the date filters is a blue circular refresh icon. Below these filters, a table displays access logs. The table has five columns: "Date", "User", "Identifier", "State", and "Method". It shows three rows of data, all with the identifier "0000214B" and "Access granted" state. The "Method" column shows a remote control icon and the text "Remote control". At the bottom right of the table, there is pagination information: "Items per page: 200" and "1 - 63 of 63", along with navigation arrows.

Date	User	Identifier	State	Method
Thu 17 November 2022 09:20:12	Test	0000214B	Access granted	Remote control
Thu 17 November 2022 09:20:12	Test	0000214B	Access granted	Remote control
Thu 17 November 2022	Test	0000214B	Access granted	Remote control

## 'Users' page




This page shows the list of users and allows you to manage their access permissions.

Your devicesExecutions**Users**GroupsAliasAssistanceProfileLog out


Users

IMPORT USERSADD USER

Filter:

Name ↑	Description	Group	Phone number	
Test user 1	user 1	No one	+393917475300	
Test user 2	user 2	Test Group	+393917475310	
Test user 3	user 3	Admin Group	+393917475320	

To add a new user press on "Add user" (highlighted in green)

Add user

First name

Description

Telephone number

Group

CREATE USER

It is possible to indicate a name and a description, which are used to identify the user more easily and the telephone number which must necessarily be the same one used by the user during registration in the app. You can also add the user to a group.

To confirm the creation of the user press "Create user". Once done, a new section is shown with the possibility of assigning opening permissions and setting the access methods.

Activated devices

List

Map

Filter:

Serial ↑	Description	Permits	Remote control button	Remote opening
<input type="checkbox"/>	800013	Access Demo	-	

Access methods

Type	Code
App	App

SAVE

To enable the user to operate a device select it in the list by pressing the relative tick (highlighted in orange in the image) and then enter the desired permissions.

Device permissions 800013

Start date:

4/28/2023

End date:

5/28/2023

Remote control button

1

Days of validity:

☒ Mon
 ☒ Mar
 ☒ Wed
 ☒ Thu
 ☒ Fri
 ☒ Sat
 ☒ Sun

Remote opening

☐

Validity times:

Valid all day

ADD TIME SLOT

CONFIRM

DISCARD CHANGES

It is possible to set different permissions for each device. You can select a start date and an expiry date, the days of validity and the time slots in which you want to enable the user to open (for example it is possible to enable openings only from Monday to Friday, from 9am to 1pm and from 2pm to 6pm).

If remote controls are used, it is possible to choose which button of a remote control the device is operated with (this is useful for providing a single remote control to a user and in the case of automations close to each other, associating each automation with a different button).

It is possible to enable the ability to open remotely with the App.

If disabled, the user must be within a radius of approximately 100 meters from the automation to be able to open. The distance is calculated using the GPS position provided by the phone and compared with the position set on the map on the device detail page.

If enabled, the user can open with the App without distance limits from the automation.

Once all the necessary permissions have been set, to confirm them it is necessary to press "Confirm". By closing the permissions window or pressing on "Discard changes" all applied changes will be ignored.

In the "Access methods" section it is possible to manage access methods available for the user, such as for example the 1Control WHY remote control or opening via license plate (this only in the case of a device equipped with a 1Control camera for detecting license plates).

Type	Code	Guide ?
App	App	
1Control remote	00001234	-
License plate	AA0000AA	-

+

CONFIRMATION

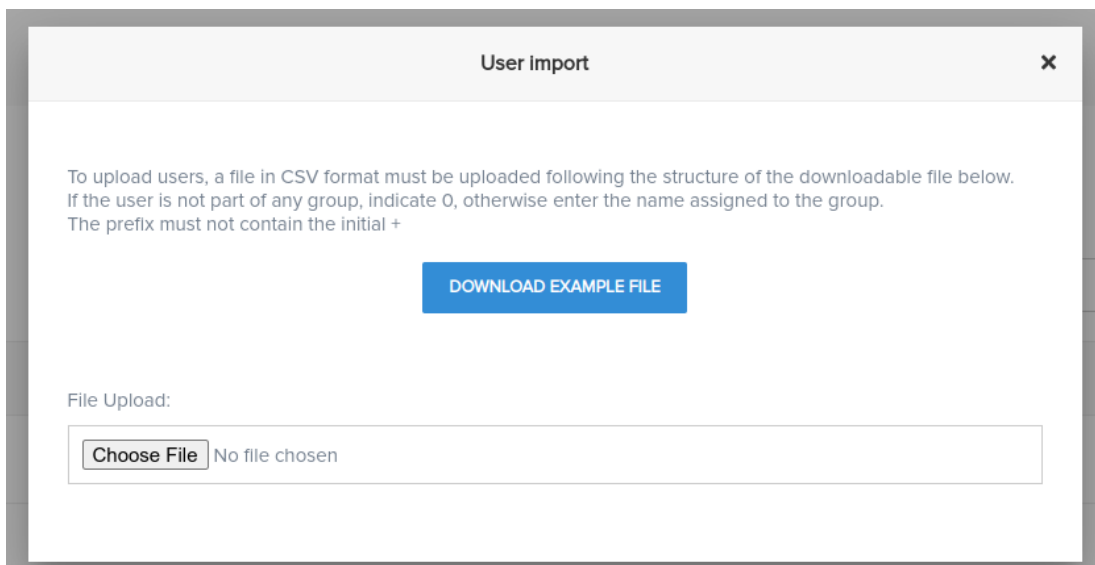
To add a new access method, press the "+" key (highlighted in green in the image), select the type of method required, for example remote control or plate, and enter the identification code. On remote controls, the code is on the back of the remote. For number plates, instead, the complete number plate must be entered.

All of these access methods are limited by the permissions set above. Therefore also remote controls and plates are authorized to open only in the selected time periods.

Once all the access methods have been set, press "Save" to confirm the changes applied.

The permissions can be changed whenever you want from the "Users" page and by pressing the edit button to the right of the user details (highlighted in orange in the image at the beginning).

In the "Users" page it is also possible to import a list of users via csv file. By pressing the "Import users" button (highlighted in red in the image at the beginning) it is possible to download a sample file which shows how to correctly format the csv file.



**User Import** ✕

To upload users, a file in CSV format must be uploaded following the structure of the downloadable file below.  
If the user is not part of any group, indicate 0, otherwise enter the name assigned to the group.  
The prefix must not contain the initial +

[DOWNLOAD EXAMPLE FILE](#)

File Upload:

[Choose File](#) No file chosen

You can directly set a group for users to import via csv file. So by importing for example the list of your employees, you can associate them directly to the "Employees" group.

All imported users are immediately enabled to open via App. To add further access methods it is necessary to do it individually for each user.

Example of correctly formatted csv file:


<u>UserName</u>	Description	Prefix	<u>PhoneNumber</u>	Group
User 1	Description for user 1	39	1919191919	0
User 2	Description for user 2	39	2919191919	group1
User 3	Description for user 3	39	3919191919	group2

For users you don't want to associate a group with, set "0" (zero) in the "Group" field.





## 'Groups' page

This page allows you to manage user groups.

 Groups

[ADD GROUP](#)

Filter:

Name	Description	
Test Group	Group	
Admin Group	System Administrators	

Groups are used to be able to modify and set the permissions of multiple users at the same time. Groups are especially useful when you have many users to manage. For example, it is possible to create an "employees" group authorized to open only during working hours and without remote opening permission and an "administration" group with no time or distance restrictions.

Creating a group is similar to creating a user. It is necessary to indicate a name to be attributed to the group and enter a description (optional). Once the group has been created, its permissions can be changed, in the same way they are managed for users.

Once the group has been created, it must be assigned to users on a user's detail page.

To edit the permissions of a group, just go to the "Groups" page and press the edit button on the right of the details.

All changes applied to the permissions of a group are automatically applied to all users belonging to the group itself.

For example, in the case of a company closure for public holidays, it is possible to disable the opening permission of the employee group.

## 'Executions' page

This page allows you to create and manage automatic executions of your devices.

The executions allow you to program the opening of the automation. It is possible to create periodic executions (based on the days of the week) or programmed (based on a selected period).

To use the executions, the automation must be compatible with the "forced open" function.

A single execution can manage several devices at the same time.

In the "Programmed executions" section it is possible to create executions with a start date and an end date, for example for particular events during which you want to keep the automations open.

## Executions

Programmed executions

Periodic executions

ADD PROGRAMMED EXECUTION

Filter:

Serial number	Description	Start date	End date	State	
800013	Test	Fri 28 April 2023 12:40:00	Sat 29 April 2023 12:40:00	Waiting	

In the example above, an automation has been created that activates device 800013 from 12:40 p.m. on April 28 to 12:40 p.m. on April 29, 2023.

In the "Periodic executions" section it is possible to create executions that repeat periodically by setting the days of the week and the time slots in which you want the device to operate automatically. For example, it is possible to set the gate to open during the times when employees enter and leave.

## Executions

Programmed executions

Periodic executions

ADD PERIODIC EXECUTION

Filter:

Serial number	Description	days of the week	Time slots	State	
800013	Test	Business Days (Mon-Fri)	From 08:00 to 08:30, from 18:00 to 18:30	Waiting	

In the example above, an automation has been created that activates device 800013 from 8:00 a.m. to 8:30 a.m. and from 6:00 p.m. to 6:30 p.m. every day from Monday to Friday.

Periodic executions have no time limit and are performed every day until they are manually deleted.

## Technical assistance

In the event of disruptions or doubts regarding the functioning of the service, please write to [support@1control.it](mailto:support@1control.it). Our technicians will provide you with all the help you need.