

PASSCONTROLLER

Controller and door management module for access control systems



Addressee for this information: User | Installer

1 COMPATIBILITY I

Update PASSMANAGER to version v1.5.0 or higher.

2 TECHNICAL DATA I

Model		PASSCT01	PASSCT02	
General features				
Power supply		PoE / DC 12 V	12 Vcc	
Operating voltage	Maximum operating voltage	15.0		V
	Minimum power supply	5.0		V
Consumption at power voltage	Idle mode	110		mA
	Max. power consumption	150		mA
O.C. output maximum current		20		mA
LED indicators		1 RGB LED, 2 TX LEDs, 2 RX LEDs		
Housing		DIN rail housing, 12 DIN modules		
Working temperature		-10 - 55		°C
Dimensions		W 213 × H 91 × D 62		mm
Weight		~335		g

Parts supplied: technical manual; 2× 680 Ω termination resistors.

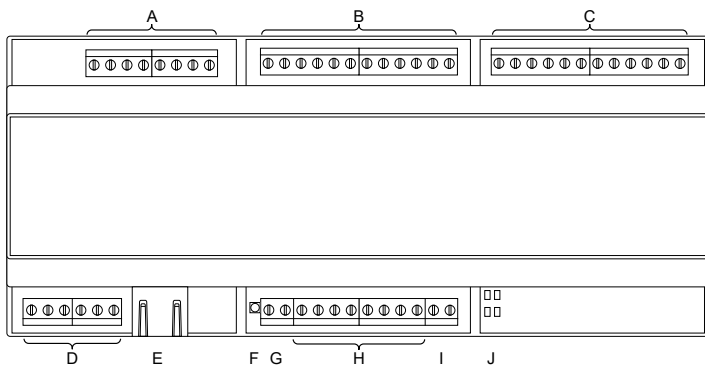
You need to respect the following PTC-imposed maximum current consumptions:

- readers power output - max 1 A total;
- Open Collector output power output - up to 250 mA total;
- TERABUS MASTER power output - max 1 A.

In case of PoE power supply (PASSCT01 only) the power consumption of all connected loads must also be below the following limits:

- PoE 30 W - max 1 A;
- PoE 10 W - max 450 mA.

3 DESCRIPTION



- A** Reader wiring
- B** Zones
- C** Open collector outputs
- D** Relay outputs
- E** 10/100 Mbps LAN port
- F** RGB LED
- G** DC 12 V power input
- H** TERABUS serial lines
- I** Tamper input
- J** Serial line transmission/reception LEDs

PASSCONTROLLER is a single gate controller, expandable to 32 by adding up to 31 PASSGATE modules over a dedicated TERABUS line.

PASSCONTROLLER allows the authorized users only to activate an electric door lock (or an electric strike, or an electric handle).

The opening can happen:

- reading a credential code both to enter and exit;
- reading a credential code to enter and pushing a button to exit.

The credential code comes from a reader appropriate to the specific technology (a key card reader, a QR code reader, an electronic tags reader) that has a Wiegand output.

If the reader has a keypad:

- instead of reading the credential code you can type it on the keypad, followed by "#".
- after the credential code has been acquired by the reader, the user might also be required to key in a numeric PIN.

Note: Keypads that use the single-digit mode can only be used to key in Wiegand 34 card codes.

The code is compared with a user database created with the PASSMANAGER software.

If the user with that credential code is authorised to opening the specific gateway, PASSCONTROLLER activates the electric door opener.

PASSCONTROLLER is an active controller that hosts a copy of the part of PASSMANAGER's database relating to the gates controlled by PASSCONTROLLER itself and by all passive controllers connected to the dedicated TERABUS serial line (TERABUS MASTER terminals); it is therefore able to authorise the opening of those gates even if it disconnects from the PASSMANAGER server.

4 INSTALLATION

! General warnings are at the end of this manual.

PASSCONTROLLER è pensato per essere installato su barra DIN in un armadio dotato di protezione contro l'apertura realizzata a cura dell'installatore.

4.1 Pre-installation programming

Part of the programming can be done before connecting PASSCONTROLLER to the system.

Follow ch. 4.3 p. 5.

4.2 Wirings

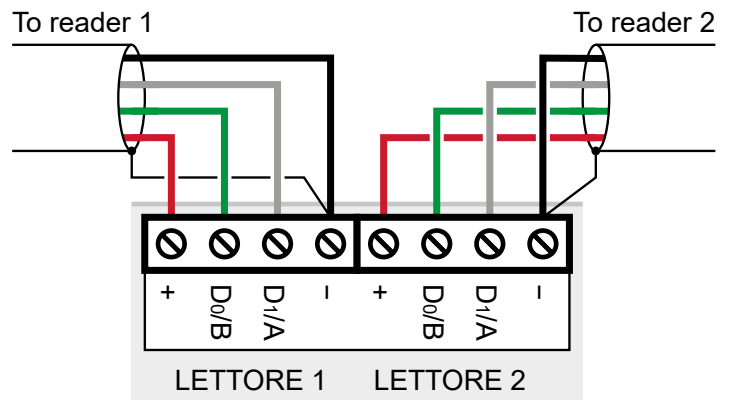
! Wire devices while they are disconnected from power/mains.

! The electronic board may be damaged by electrostatic discharges; the installer must avoid any presence of electrostatic discharges both during installation and maintenance.

4.2.1 Reader wiring

Use 26 or 34 bit Wiegand readers.

- wire the outdoor reader, which is necessary, to the READER 1 terminals
- wire the indoor reader, which is optional, to the READER 2 terminals



Max total current consumption: 1 A @ DC 12 V, PTC limited.

4.2.2 Input wiring

Each input is made of a numbered positive terminal and of a negative terminal (each serving the two positives immediately to its left).

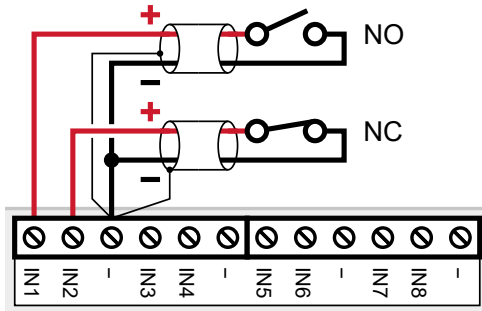
Inputs are assigned to the following functions:

IN1	Door opening button	Usually NO
IN2	Door status monitoring through magnetic contact	Usually NC
IN3	General input	-
IN4	Not used	Do not use

IN5	Tamper input	Usually NC
IN6	Not used	Do not use
IN7	Not used	Do not use
IN8	Not used	Do not use

The NO/NC behaviour of inputs (default NO) can be changed using PASSMANAGER (ch. 4.3.3 p. 6).

Note: the NO/NC behaviour set for input 5 is also applied to the TAMPER input (ch. 4.2.5 p. 4).

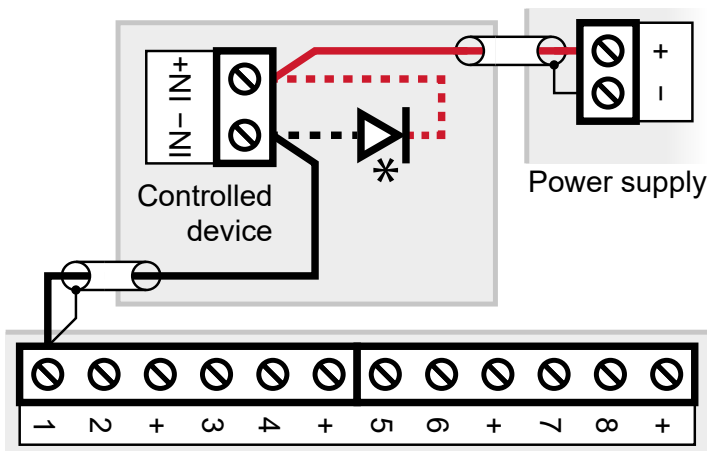


4.2.3 Open collector output wiring

Outputs are assigned to the following functions:

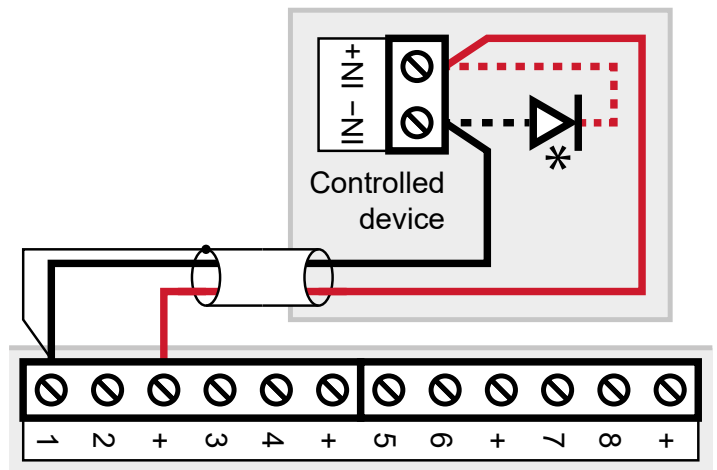
1	Follows the activation of relay 1
2	Follows the activation of relay 2
3	TTL1
4	TTL2
5	Follows the activation of the buzzer
6	Not used
7	Not used
8	Not used

All outputs connected like shown for output 1 in the diagram. These being Open Collector outputs, the numbered terminals can be connected to any DC 12 V positive.



*Only wire the diode and the dotted wires if the load of the controlled device is inductive.

The terminal strip also has some DC 12 V terminals marked "+" which can be used for this purpose.



*Only wire the diode and the dotted wires if the load of the controlled device is inductive.

Max total current consumption: 250 mA @ DC 12 V, PTC limited.

4.2.4 Relay output wiring

The REL1 output controls the electric door lock that opens the gateway.

The REL2 output controls an acoustic signalling device.

Maximum supported voltage: DC 24 V, AC 120 V.

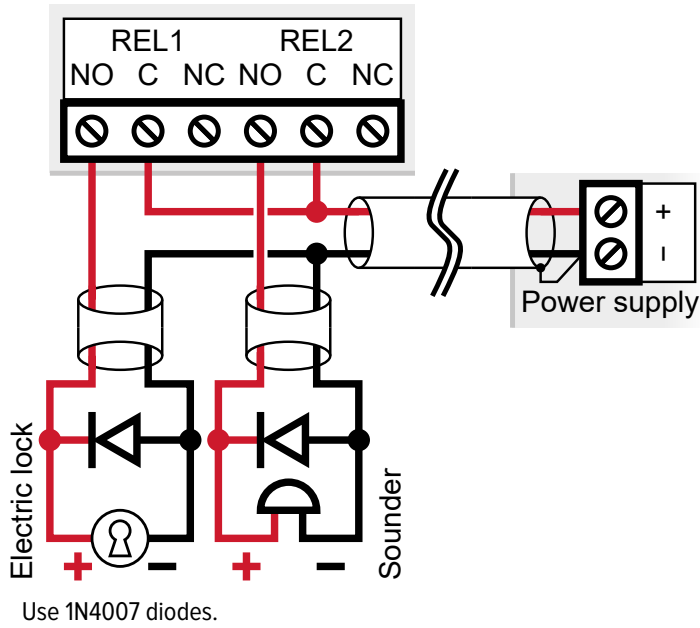
Maximum current on each relay: 3 A.

By default, the REL2 output activates in the following events:

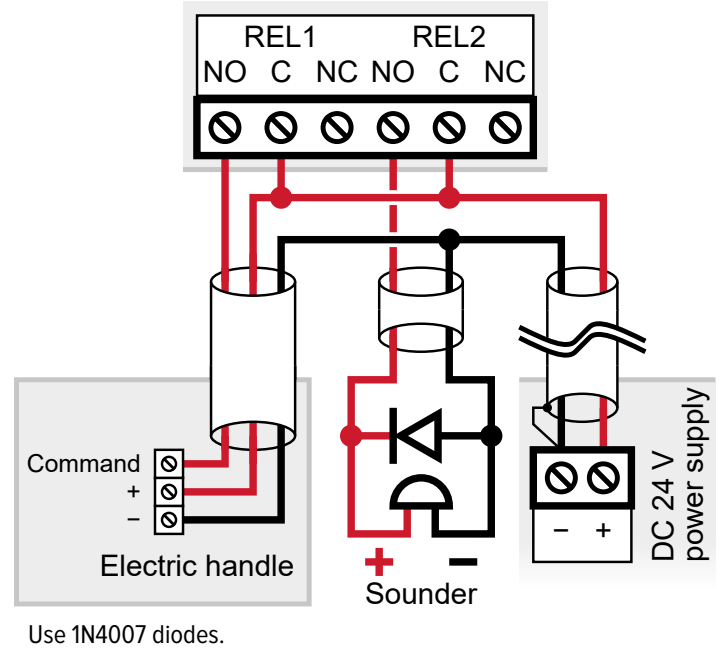
- access attempt with invalid credential;
- access attempt outside the established time slots
- if the antipassback function is active (default: no), two consecutive entries (or exits) by the same user;
- gate opening without credentials (forcing it open, using a panic bar, ...)*;
- gate opening lasting longer than the max door opening value (default: unlimited)*.

* **only if the gate's opening status is monitored by a magnetic contact connected to the IN2 input (ch. 4.2.2 p. 2).**

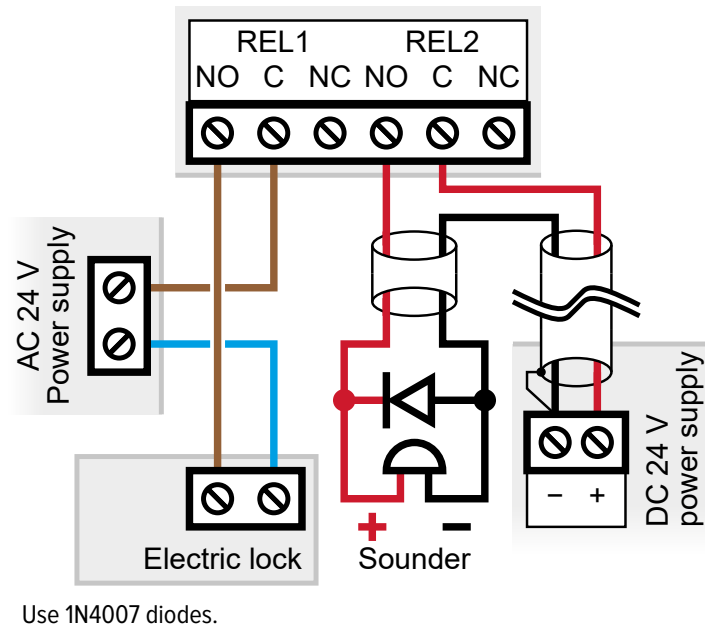
With DC electric lock



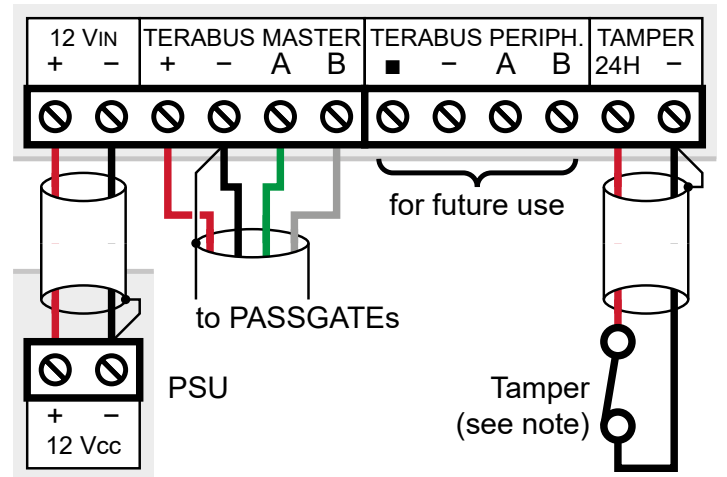
With electric handle



With AC electric lock



4.2.5 Tamper input, serial line and power terminals wiring



Tamper against opening

- to monitor the opening of the cabinet, connect the tamper against opening to the 24H terminals

Note: the NO/NC behaviour of the TAMPER input is the same that has been set for input 5 (ch. 4.2.2 p. 2).

Serial line

The TERABUS MASTER terminals are the starting point of a dedicated TERABUS serial line to which up to 31 PASSGATE controllers can be connected.

- wire detector power and serial line terminals

Use shielded cables with the following section: $2 \times 0.75 \text{ mm}^2$ (power) + $2 \times 0.22 \text{ mm}^2$ (signal).

The serial line may be extended with branches, provided that the following rules are followed:

- the sum of the lengths of the branches must not exceed 1 km;

- 680 Ω termination resistors must be connected to the ends of the two longest branches.

Max total current consumption: 1 A @ DC 12 V, PTC limited.

Power supply

PASSCONTROLLER can be powered:

- via PoE (PASSCT01 only, maximum output current limited to 1 A);
- using an external DC 12 V power supply (maximum output current limited to 3 A).

The single loads are PTC-protected and have the maximum current draw stated in ch. 2 p. 1.

The diagram at the beginning of this chapter shows how to connect the external power supply.

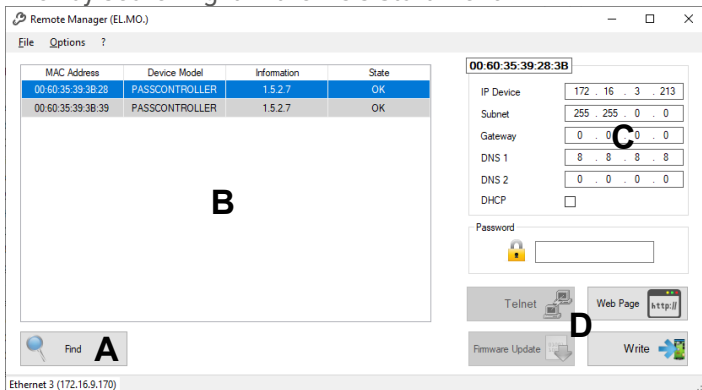
4.3 Programming

Programming PASSCONTROLLER requires using three software: Remote Manager, an Internet browser and PASSMANAGER.

- connect the PC and PASSCONTROLLER to the same Ethernet network, or connect them directly by using an Ethernet cable

4.3.1 Remote Manager

- go to PASSCONTROLLER's page on www.elmospa.com
- download, unzip and install the Remote Manager 1.5.0 software
- run Remote Manager by double clicking its desktop icon or by searching it in the PC's Start menu



- click on **Find (A)**

Remote Manager scans the network and lists all found devices (**B**), including PASSCONTROLLER.

- find PASSCONTROLLER and select it by clicking on it
- If there is more than one PASSCONTROLLER listed, choose the one with the same MAC Address shown on the label on the Ethernet port.

The network settings of PASSCONTROLLER are shown in the area in the top right (**C**).

The default IP address is 192.168.1.100.

- press the **Web Page (D)** button
- if the configuration web interface opens, proceed to ch. 4.3.2 p. 5

Otherwise, change the network settings of PASSCONTROLLER so that the controller belongs to the same subnet as the PC

used for configuration.

- ask the system administrator to provide network parameters for PASSCONTROLLER and type them in Remote Manager's interface (**C**)
- enter the default password, "Admin"
- press the **Write** button (**D**) to save
- press the **Web Page** button **Web Page (D)**

The web interface login screen opens.

Now that we are sure that the computer and PASSCONTROLLER belong to the same subnet, we can also reach the login screen of the web interface by typing PASSCONTROLLER's IP address in the address bar of an Internet browser.

4.3.2 Web interface

To access PASSCONTROLLER's web interface you need to use a computer that is connected to the same Ethernet network as PASSCONTROLLER.

In addition, the IP addresses of the computer and of PASSCONTROLLER have to belong to the same subnet.

To make sure of this, log in for the first time using Remote Manager (ch. 4.3.1 p. 5).

Afterwards it will be sufficient to open an Internet browser, to type PASSCONTROLLER's IP address in the address bar and to press enter.

The web interface login screen opens.

- enter the access credentials in the proper fields (default: Admin, Admin), then click **Sign In**

Use the menu on the left to browse the interface.

Dashboard

This page shows some information about PASSCONTROLLER:

- the current time;
- PASSCONTROLLER's IP address;
- PASSCONTROLLER's firmware version;
- PASSCONTROLLER's microprocessor version;

Network

This page shows lets you see and change the remaining connection parameters.

- input the network parameters chosen by the network admin and press **Apply**

Once the IP address has changed the browser will disconnect from PASSCONTROLLER.

You can access the web interface again by typing the new IP address in the address bar and pressing enter as long as the PC is in the same network subnet of PASSCONTROLLER.

Devices

This page can be used to enable PASSCONTROLLER and all PASSGATEs connected to the TERABUS MASTER serial line. The State column shows if each controller is properly functioning:

- green = connected and working;
- grey = disconnected;

- red = not working.

The Version column shows the firmware version of each connected PASSGATE.

States

This page shows the activity of all inputs and outputs of PASSCONTROLLER and of all connected PASSGATES.

PASSCONTROLLER is shown as Device 0.

All connected PASSGATES that have been set as active in the **Devices** page are listed along with their address.

Each input and output follows an icon detailing its state:

- green = active input or output;
- grey = inactive input or output.

This page is useful while testing the system: activate inputs and outputs and verify that the icons change colour as expected.

Backup

You can create backup files that include one or both of these topics: configuration and events.

When restoring a backup, you can decide which topics to restore; the backup will overwrite current data only for that topic, if the backup file includes it.

The backup files have the .xml format.

Change password

- to change the password, type the required data and click **Apply**

Utilities

This page allows you to perform some ancillary operations.

▼ Date and Time

Synchronize PASSCONTROLLER's internal clock to the PASSMANAGER server (default), to an NTP server or set the date and time manually.

If you choose manual settings, input the current date and time in the dedicated field.

If you choose to use the NTP server you can type in the address of the preferred server.

PASSCONTROLLER uses the server entered in the **Server NTP** field if available, if not it goes over a list of pre-defined servers and synchronizes with the first available one.

If you choose to use the NTP server you need to specify the **TimeZone** of the installation place.


Press **Apply and restart** to save the settings.

▼ Firmware upgrade

Firmware update files are available on PASSCONTROLLER's product page su www.elmospa.com.

Click Browse and locate the downloaded update file.

Click Run.

 *Do not power down PASSCONTROLLER during the update.*

▼ Miscellaneous

Press **Restart** to restart PASSCONTROLLER.

Press **Factory default** to restore all settings, IP address included, to default values.

4.3.3 PASSMANAGER

PASSMANAGER is the management software of the access control system.

It is used for:

- link card codes to the users of the access control system;
- choose which users can open a specific gate and in which time slots;
- set the NO/NC behaviour of PASSCONTROLLER's inputs;
- set the activation conditions of PASSCONTROLLER's outputs.

Note: the NO/NC behaviour set for input 5 (ch. 4.2.2 p. 2) is also applied to the TAMPER input (ch. 4.2.5 p. 4).

For its use, see its technical manual.

5 DIAGNOSTICS

The status LED in the lower part of PASSCONTROLLER provides a quick panoramic of the device's status

More information is available in the web interface (ch. 4.3.2 p. 5).

Status LED indicators

Colour	Status	Indication
Green	ON steady	Firmware operative
Blue	Blinking	Operating System startup
Violet	Blinking	Factory default restored

Serial line activity LEDs

TB1 LEDs show the activity of the TERABUS MASTER serial line.

TB2 LEDs show the activity of the TERABUS PERIPH. serial line (for future use).

Yellow (TX) LEDs indicate data transmission.

Blue (RX) LEDs indicate data reception.

6 RESET AND FACTORY DEFAULT

It is advantageous to run the reset and factory default operations from within the web interface (ch. 4.3.2 p. 5).

If it is not possible to access the web interface, follow the instructions in this chapter instead.

Reset

- disconnect and re-connect one of PASSCONTROLLER's power supply wires (ch. 4.2.5 p. 4)

If the reset operation is successful, the status LED (ch. 5 p. 6) blinks blue, then goes back to steady green.

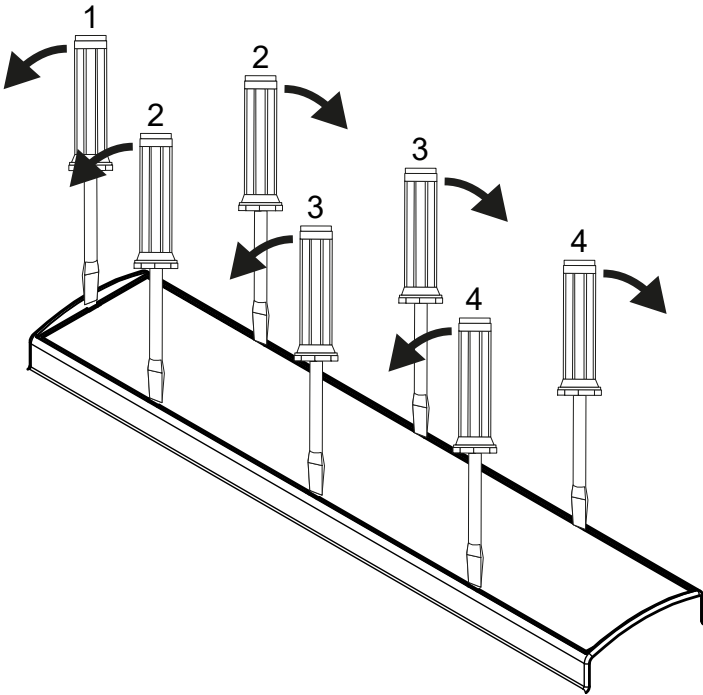
If this does not happen, perform a factory default.

Factory default

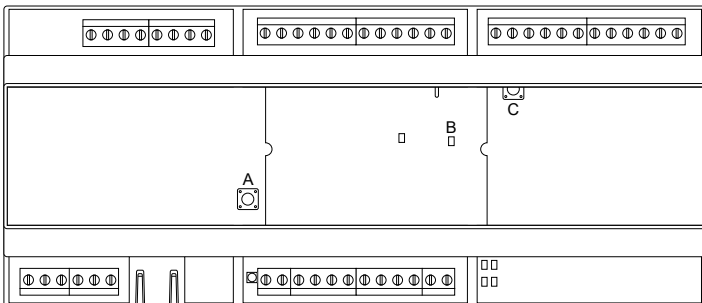
! A factory default sets all of PASSCONTROLLER's settings (including the IP address) to their initial values, requiring you to run the entire configuration process again.

Use a flat, small screwdriver to pry the front cover from its compartment:

- insert the screwdriver's tip in one of the side slots of the cover, slightly lifting it up
- insert the screwdriver's tip in each slot, proceeding towards the other short side, opening all clips as shown in the diagram



Inside, the central part of the board that supports the terminal strips can be seen.



- A** DEFAULT button **C** RESET button
B Power ON LED (green)

- keep the DEFAULT button pressed for about 10 seconds, until the status LED (ch. 5 p. 6) blinks violet.

Upon release, the status LED blinks blue, then goes back to steady green.

7 USE



To open the door from the outside, an authorized user must

authenticate to the outdoor reader as required by the reader, for instance:

- by placing a key card near to the reader;
- by typing the credential code on the keypad, followed by "#";

Note: Keypads that use the single-digit mode can only be used to key in Wiegand 34 card codes.

- by placing a proximity key near to the reader;
- by placing a token or a tag near to the reader;
- by placing a smartphone near to the reader to transfer the credentials over wireless transmission technologies;
- by showing to the reader's camera a specifically generated QR code;
- in any of the previous ways followed by typing a PIN on the reader's keypad.

To open the door from the inside, you might have to:

- authenticate yourself at a second reader;
- press a door opening button;
- press an authorization button before using a handle or a panic bar.

EU DECLARATION OF CONFORMITY

The product complies with current European EMC and LVD directives.

The full text of the EU declaration of conformity is available at the following internet address: www.elmospa.com – registration is quick and easy.



GENERAL WARNINGS



This device has been designed, built and tested with the utmost care and attention, adopting test and inspection procedures in compliance with current legislation. Full compliance of the working specifications is only achieved in the event the device is used solely for its intended purpose, namely:

Controller and door management module for access control systems

The device is not intended for any use other than the above and hence its correct functioning in such cases cannot be assured. Consequently, any use of the manual in your possession for any purpose other than those for which it was compiled - namely for the purpose of explaining the product's technical features and operating procedures - is strictly prohibited.

Production processes are closely monitored in order to prevent faults and malfunctions. However, the components adopted are subject to an extremely modest percentage of faults, which is nonetheless the case with any electronic or mechanical product.

Given the intended use of this item (protection of property and people), we invite you to adapt the level of protection offered by the system to suit the actual situation of risk (allowing for the possibility of impaired system operation due to faults or other problems), while reminding you that there are specific standards for the design and production of systems intended for this kind of application.

We hereby advise you (the system's operator) to see that the system receives regular routine maintenance, at least in accordance with the provisions of current legislation, and also check on as regular a basis as the risk involved requires that the system in question is operating properly, with particular reference to the control unit, sensors, sounders, dialler(s) and any other device connected. You must let the installer know how well the system seems to be operating, based on the results of periodic checks, without delay.

Work involved in the design, installation and maintenance of systems incorporating this product should be performed only by personnel with suitable skills and knowledge required to work safely so as to prevent any accidents. It is vital that systems be installed in accordance with current legislation. The internal parts of certain equipment are connected to the mains and therefore there is a risk of electrocution when maintenance work is performed inside without first disconnecting the primary and emergency power supplies. Certain products include batteries, rechargeable or otherwise, as an emergency backup power supply.

If connected incorrectly, they may cause damage to the product or property, and may endanger the operator (explosion and fire).

INSTALLER WARNINGS



Comply strictly with current standards governing the installation of electrical systems and security systems, and with the manufacturer's directions given in the manuals supplied with the products.

Provide the user with full information on using the system installed and on its limitations, pointing out that there are different levels of security

performance that will need to suit the user's requirements within the constraints of the specific applicable standards. See that the user looks through the warnings given herein.

Work involved in the design, installation and maintenance of systems incorporating this product should be performed only by personnel with suitable skills and knowledge required to work safely so as to prevent any accidents. It is vital that systems be installed in accordance with current legislation. The internal parts of certain equipment are connected to the mains and therefore there is a risk of electrocution when maintenance work is performed inside without first disconnecting the primary and emergency power supplies. Certain products include batteries, rechargeable or otherwise, as an emergency backup power supply. If connected incorrectly, they may cause damage to the product or property, and may endanger the operator (explosion and fire).

USER WARNINGS



Check the system's operation thoroughly at regular intervals, making sure the equipment can be armed and disarmed properly.

Make sure the system receives proper routine maintenance, employing the services of specialist personnel who meet the requirements prescribed by current regulations.

Ask your installer to check that the system suits changing operating conditions (e.g. changes in the extent of the areas to be protected, change in access methods, etc...)

MAIN SAFETY RULES

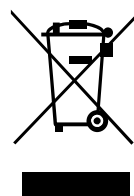


The use of the device is forbidden for children and unassisted disabled individuals.

Do not touch the device when bare footed, or with wet body parts. Do not directly spray or throw water on the device.

Do not pull, remove or twist the electric cables protruding from the device even if the same is disconnected from the power source.

DISPOSAL WARNINGS



IT08020000001624

In accordance with Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), please be advised that the EEE was placed on the market after 13 August 2005 and must be disposed of separately from normal household waste.