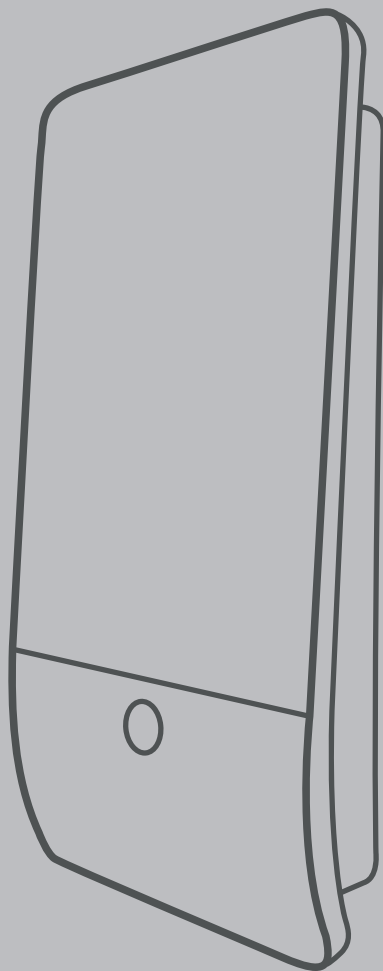


JABLOTRON 100⁺

EN User manual



JABLOTRON

TABLE OF CONTENTS

1. INTRODUCTION	23	5.7. BY DIALLING IN	35
2. CONTROLLING THE JABLOTRON SYSTEM	23	5.8. BY SMS	36
3. WAYS OF CONTROLLING THE JABLOTRON SYSTEM	24	6. BLOCKING IN THE SYSTEM	36
3.1. ON-SITE OPERATING	24	6.1. PROTECTION AGAINST THE CODE BREAKING ATTEMPT (ONLY FOR SECURITY GRADE 3)	36
3.1.1. CONTROL BY READER OR KEYPAD	24	6.2. ANTIMASKING (ONLY FOR SECURITY GRADE 3)	36
3.1.2. KEYPAD OPTICAL INDICATION	25	6.3. SYSTEM WATCHDOG (ONLY FOR SECURITY GRADE 3)	36
3.1.3. SYSTEM CONTROL USING KEYPADS AND READERS WITH SEGMENTS	25	6.4. BLOCKING USERS	36
3.1.3.1. AUTHORISATION USING TAGS AND CARDS	25	6.5. BLOCKING DETECTORS	36
3.1.3.2. AUTHORISATION BY ENTERING A CODE ON THE KEYPAD	25	6.6. DISABLING TIMERS	37
3.1.3.3. ALARM SETTING	26	7. USER SYSTEM SETTINGS	37
3.1.3.4. ALARM UNSETTING	27	7.1. CHANGING THE USER ACCESS CODE	37
3.1.3.5. PARTIAL ALARM SETTING	27	7.2. CHANGING THE TELEPHONE NUMBER OR USER NAME	37
3.1.3.6. DURESS ACCESS CONTROL	28	7.3. ADDING A NEW USER / DELETING A USER	38
3.1.3.7. CANCELLING THE TRIGGERED ALARM	28	8. CALENDAR SETTINGS	38
3.1.3.8. SECTION CONTROL FROM THE LCD KEYPAD MENU AND BY SEGMENTS	29	9. EVENT HISTORY	38
3.1.3.9. CONTROL VIA THE JA-116E / JA-156E KEYPAD	30	9.1. BY BROWSING EVENTS ON THE KEYPAD WITH LCD DISPLAY / TOUCH SCREEN	38
3.1.3.10. SYSTEM CONTROL WITH A REMOTE CONTROLLER	33	9.2. READING EVENTS WITH THE JA-100-LINK SOFTWARE ON A COMPUTER	38
4. REMOTE CONTROLLING	33	9.3. BY LOGGING INTO MyJABLOTRON (ON THE WEBSITE OR IN THE SMARTPHONE APP)	38
4.1. CONTROLLING THE SYSTEM USING THE MyJABLOTRON APP (ON YOUR MOBILE PHONE OR ON THE WEB)	33	10. TECHNICAL SPECIFICATIONS	39
4.2. CONTROLLING THE SYSTEM USING THE VOICE MENU	34		
4.3. CONTROLLING THE SYSTEM USING SMS	34		
4.4. CONTROLLING THE SYSTEM REMOTELY USING COMPUTER (JA-100-LINK)	34		
5. CONTROL OF THE PROGRAMMABLE OUTPUTS PG	35		
5.1. USING THE KEYPAD SEGMENT (SLIDER ON THE DISPLAY IN THE CASE OF TOUCH KEYBOARDS)	35		
5.2. USER AUTHORISATION ON THE KEYPAD	35		
5.3. FROM THE KEYPAD MENU WITH LCD DISPLAY	35		
5.4. BY KEYFOB	35		
5.5. MyJABLOTRON APPLICATION ON YOUR PHONE	35		
5.6. MyJABLOTRON WEB INTERFACE	35		



PERIODICAL MAINTENANCE

- To ensure reliable operation of the entire system, regular maintenance intervals must be observed.
- Most maintenance requirements should be carried out by a service company as part of regular service inspections at least once a year.
- User maintenance consists mainly of keeping the individual devices clean.
- To open the detectors (to replace batteries) or remove them from the installation, if necessary, the ADMINISTRATOR can switch the system to MAINTENANCE mode. Consult the installation company regarding the request for MAINTENANCE mode. When setting up a system that complies with EN 50131-1, Security Grade 2 or 3, MAINTENANCE mode is not available.
- The switch can be made using the JA-100-Link programme or from the menu of the keypad with LCD display or touch screen. After authorisation, select „Maintenance mode“ from the menu and then select the sections in which it is required. In this mode, no alarms will be triggered from the selected sections, even if the detectors are opened or removed from their mounting.
- Maintenance mode is indicated by the activation button flashing green (2 flashes every 2 seconds) and both buttons on the segment of the given section going out.
- When handling devices, take extra care not to damage the plastic and mechanisms that ensure the detectors function properly.
- The cover is usually secured with a flexible latch, which must be gently pressed into the detector body with a small tool (screwdriver) and then the cover can be lifted off. In some cases, this latch is secured with a small screw, which must first be unscrewed or turned with a locking mechanism marked with a lock symbol.
- Always replace all batteries in the detector at the same time (use batteries of the same type and from the same manufacturer).
- Some devices may require testing (e.g. fire detectors). For more information, contact a service technician.

1. INTRODUCTION

The JABLOTRON system is designed for up to 600 users and can be divided into up to 15 separate sections. It allows the use of up to 230 devices and offers up to 128 programmable outputs for multifunctional use, e.g. for home automation.

2. CONTROLLING THE JABLOTRON SYSTEM

The security system can be controlled in various ways. Authorisation, i.e. user identification, is always required for setting. The system recognises which user is currently using it and allows them to control the parts to which they have access according to their preset authorisation.

For setting, you can choose between setting with or without authorisation. If setting without authorisation is set, authorisation is not required and setting can be performed simply by pressing the right button on the access module segment. Every action, including the date, time and user name, is recorded in the system memory. This information is available for an unlimited period of time. Simply authorising the user can also cancel an alarm (turn off the sirens) in those parts of the system that the user has access rights to, but this does not automatically unset the system (unless the default setting has been changed).

Note: Depending on the installed configuration and system settings, not all of the methods and options described below may be available. Consult your service technician about the system settings.

3. WAYS OF CONTROLLING THE JABLOTRON SYSTEM

3.1. ON-SITE OPERATING

- System access module (reader or keypad)
- Remote controller
- Computer via USB cable using the JA-100-Link software

3.1.1. CONTROL BY READER OR KEYPAD

Various keypad models can be used to control the JABLOTRON system, which not only enable control, but also clearly indicate the status of individual components.

TYPES OF KEYPADS AND READERS

JA-116E / JA-156E

Touch keypad with reader
(bus and wireless versions)



JA-115E / JA-155E

Four-segment keypad with
LCD display and reader
(bus and wireless versions)



JA-114E / JA-154E

Access module with LCD
display and keypad
(bus and wireless versions)



JA-113E / JA-153E

Access module with keypad
and reader
(bus and wireless versions)



JA-112E / JA-152E

Access module with reader
(bus and wireless versions)



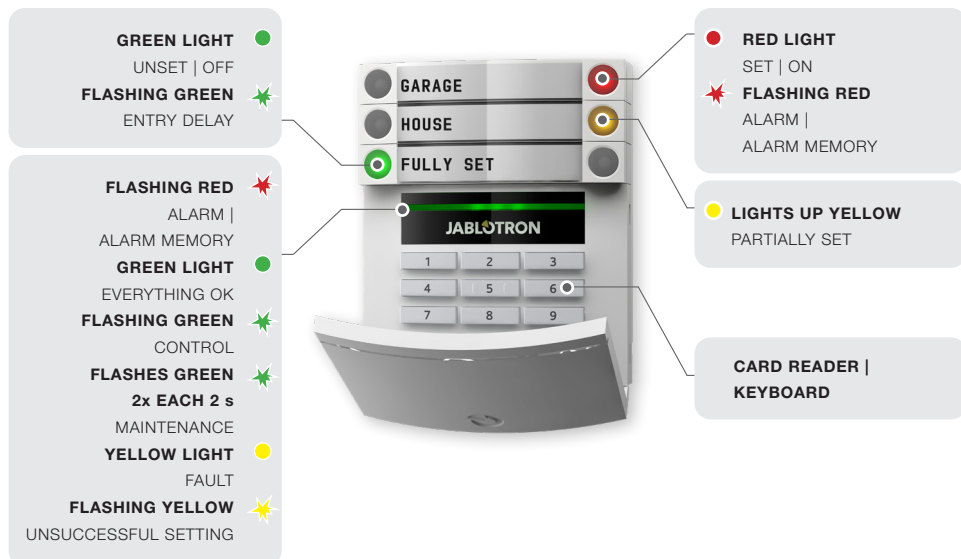
Authorisation is possible by card, tag, or by entering a code on the keypad, or by combining two types of authorisation for higher Security grade.

The system control (setting or unsetting the system and other automation functions) is performed using a touch screen or two-button segments. The segment buttons can be clearly labelled and their status is clearly indicated by LEDs with traffic light logic.

The segment can also be used to status indication (e.g. open garage door) or to control various automation devices (e.g. heating or blinds).

The segments are removable, a maximum of 20 segments can be connected to one keypad. Only 4 segments are available for the JA-115E / JA-155E keypad. The segment can also be used to call for help in an emergency (medical or panic alarm).

3.1.2. KEYPAD OPTICAL INDICATION



3.1.3. SYSTEM CONTROL USING KEYPADS AND READERS WITH SEGMENTS

3.1.3.1. AUTHORISATION USING TAGS AND CARDS

The basic authorisation element is an RFID / NFC tag or a card, which are assigned to a specific user in the system. At the same time, the user may be assigned an authorisation code. Each user can have a maximum of one authorisation code and up to two RFID / NFC tags or cards. If a higher Security grade is required from the alarm during system control, it is possible to set up confirmed authorisation using both tag / card and code (optional function). If the user wants to control multiple segments (sections) at once, they press the segments of the desired sections one after the other after authorisation. This makes it possible, for example, to set the house and unset the garage at the same time.



*NFC tags / cards can only be assigned to the system via the keypad / reader.

CAUTION: If the selected system profile is EN 50131-1 Security Grade 3, authorization is only possible by entering the code on the keypad!

3.1.3.2. AUTHORISATION BY ENTERING A CODE ON THE KEYPAD

The system supports 4-, 6- or 8-digit codes. The system can be set up to use codes with a prefix (suitable for systems with a large number of users) or without a prefix (default setting).

CAUTION: If the selected system profile is EN 50131-1 Security Grade 3, only 6-digit and longer codes are permitted!

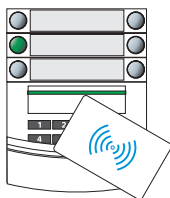
Without prefix: **KKKK** (4, 6 or 8-digit code within the permitted range of 0000 – 99999999)
 With prefix: **PPP*KKKK** (where PPP = user's numeric position in the permitted range of 0 to 600, * - separator, KKKK – code as above)

Whether the system will use codes with a prefix is programmed by the installation technician based on the consultation with the system administrator mind configuration requirements according to the Security grade. The prefix consists of the user's numeric position, which makes the digit code unique and prevents two codes collision. If users are to set their own codes in larger systems, it is necessary to have active codes with a prefix.

Default administrator codes

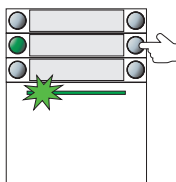
Without prefix: **1234; 123456; 12345678**
 With prefix: **1*1234; 1*123456; 1*1234578**

3.1.3.3. ALARM SETTING



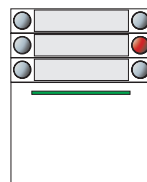
Authorisation by card / tag or by entering codes on the keypad

Authorisation by card / tag or by entering codes on the keypad.



Press the right button

To secure the desired section. It is possible to secure multiple sections in succession. However, the delay between section selections must not exceed 2 seconds.



The command is executed

The keypad acoustically indicates the entry delay time. The section is now set, and only detectors with a „Delayed“ response during the entry delay period allow the guarded area to be exited.

The segment of the secured section lights up red.

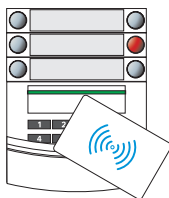
How will the system react if any of the detectors are active when setting? (e.g. an open window). It depends on the settings during installation; the following scenarios are available:

- A) When setting, the system does not indicate active detectors in any way. The detectors will automatically return to operation after they have been deactivated (e.g. window closed).
- B) The system indicates by flashing the red segment button (for 8 seconds) that there are active detectors in the system. If the user does not cancel the action (by unsetting), the system will automatically set itself (**default setting**).
- C) The system will indicate by flashing the red segment button. If the user does not confirm his intention to set the section by pressing the button again despite the active detector, the system will not be set.
- D) An active detector prevents the section from being set. This status is indicated by the red segment button flashing.

The devices preventing system setting can be seen in the LCD keypad menu.

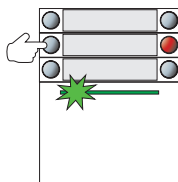
Unsuccessful setting is indicated by the yellow indication button flashing (the „Unsuccessful setting“ function must be enabled). [A required system behaviour must be consulted with an installer.](#)

3.1.3.4. ALARM UNSETTING

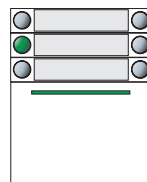


Entry into the building and authorisation

As soon as the system detects entry into the building, it will signal the entry delay with a continuous beeping sound and flashing of the green button of the section in which the entry delay is occurring. It is necessary to authorise yourself in the usual manner.



Press the left segment button for the sections you want to unlock



The command is executed

The segments indicate the unsetting of the given sections with a continuous green light.

Note: If the „Authorisation unsets the section during entry delay“ option is enabled, mere authorisation will unset the section in which the entry delay is running. A required system behaviour must be consulted with an installer.

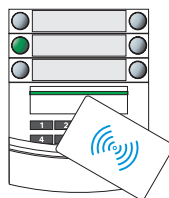
3.1.3.5. PARTIAL ALARM SETTING

The system can also be set partially, which allows monitoring using only selected detectors in the section.

Example: It allows you to leave the windows and doors set during the night and motion detectors inside the protected premises won't respond.

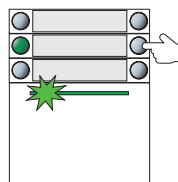
If you want to set the entire building where partial setting is enabled, you must press the full setting button twice. After the first press, the button lights up yellow, after the second press, it lights up red.

If the system is partially set (yellow light), press the yellow button after authorisation to switch to full setting. After pressing, the system will be fully set and the button will turn red.

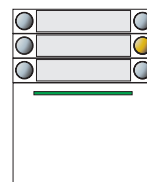


Authorisation on the keypad

By entering a code, reading a tag or card on the reader. The indicator button will flash green.



Pressing the right button of the relevant section



The command is executed

The segment will flash yellow continuously to indicate that the section is partially set.

3.1.3.6. DURESS ACCESS CONTROL

This function provides unsetting of the system in a special mode. The system seemingly unsets, however it triggers a silent panic alarm, which is then reported to selected users (including ARC). Duress access control is executed by adding 1 to the last number in a valid code.

Enabling this function reduces the number of combinations by half.

The function can be disabled (by a service technician).

Example for codes with a prefix: Valid code: **2*9999** Code entered under duress: **2*9990**

Example for codes without a prefix: Valid code: **9999** Code entered under duress: **9990**

3.1.3.7. CANCELLING THE TRIGGERED ALARM

An ongoing alarm is indicated on the keypad by rapid flashing of the red segment button and the illuminated indicator button. To cancel the alarm, you must authorise yourself on the keypad.

The section remains set, and rapid red flashing on the segment indicates that an alarm has been triggered. The signal remains even after unsetting.

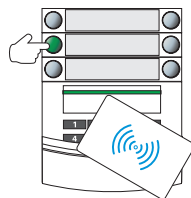
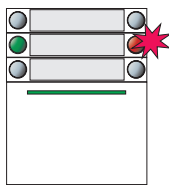
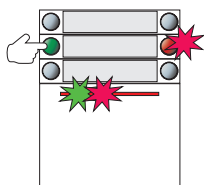
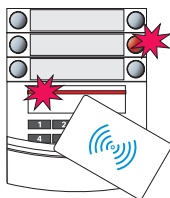
If an alarm is indicated in your absence, look for the source of the alarm in the event history and be vigilant when checking the property or wait for the security agency to arrive (if your system is connected to a monitoring centre).

Alarm memory indication remains indicated on the segment until the next system setting, or it can be cancelled by repeated setting and unsetting. On keypads with an LCD display, the alarm memory indication can be cancelled in the [Main Menu](#) – „Cancel Warning Indication“.

The indication of a tamper alarm can only be cancelled by a service technician or administrator.

Note: In settings that comply with the EN 50131-1 standard, Security Grade 2 / 3, it is always necessary to authorise first and then perform the required action.

When cancelling an alarm with the remote control, the relevant section is also unset.



Authorisation on the keypad

By entering a code on the keypad or by placing a tag or card on the reader.

Pressing the left button of the section in which the alarm is occurring

Unsetting and mute the sirens

A green button indicates that the relevant section has been unset. A red button flashes to indicate an alarm memory.

Cancelling the alarm memory

After re-authorisation, press the left button again to cancel the alarm memory indication. The indicator button lights up continuously to indicate that the system is unset.

3.1.3.8. SECTION CONTROL FROM THE LCD KEYPAD MENU AND BY SEGMENTS

Structure and description of the internal menu valid for the JA-114E, JA-154E, JA-115E, JA-155E keypads.

**Administrator
or User
authorization
by the code or
RFID tag / card**

CANCEL WARNING INDICATION

Allows you to cancel alarm / unsuccessful setting indication in all sections to which the user has access rights

SECTION CONTROL

Allows you to control the system's sections to which the user has access rights and are enabled in the internal settings.

PG CONTROL

Allows the user to control PG programmable outputs depending on the user's permissions and according to the internal settings.

EVENT MEMORY

Displays a detailed list of the event memory.

SETTING PREVENTED

Shows a list of triggered detectors preventing setting the system, provided this option is activated in the control panel configuration.

FAULTS IN SYSTEM

Displays a list of all detectors indicating system faults from sections to which the user has access rights.

BYPASSED DETECTORS

Displays a list of all blocked detectors in sections to which a user has access rights.

SYSTEM STATUS

Shows system status (list of triggered detectors, triggered tamper contacts, low batteries, bypassing, etc.).

SETTINGS

Allows editing of users and devices (only when USB is disconnected).

DISPLAY SETTING

Allows adjustment of keypad backlight intensity and display contrast.

MAINTENANCE MODE

Allows the Administrator to switch assigned sections to the Maintenance mode.

3.1.3.9. CONTROL VIA THE JA-116E / JA-156E KEYPAD

AUTHORISATION AND UNSETTING

CAUTION: When the system profile in a configuration with EN 50131-1 Security Grade 3 is selected, authorization is only possible with a user code; RFID / NFC tags and card are not supported.

Authorisation is the same as for previous keypads. You can authorise yourself by placing your card or tag on the reader, or by pressing the button and entering the code on the keypad. After a valid authorisation, the display shows the individual sections and their status, who has authorised themselves, and the menu in the top bar of the screen.



Entry into the building and authorisation on the keypad.

After entering the building, an entry delay is triggered. On the display, press the **Unset** button, authorise yourself and unset the necessary sections using the sliders.

KEYPAD MENU AFTER AUTHORISATION



Logout



Displays the status of individual sections



Displays the status of PG outputs

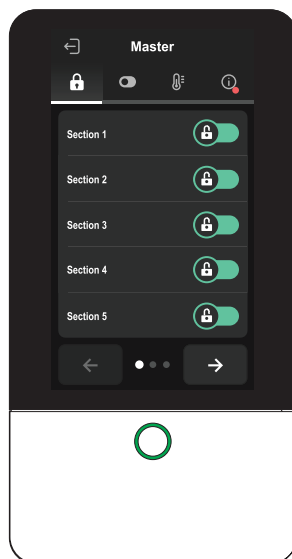


Displays temperatures from thermometers and thermostats



Displays information about the last action / status in the system.

Option to further configure the display, display service contact details, switch to Maintenance mode and display the event history

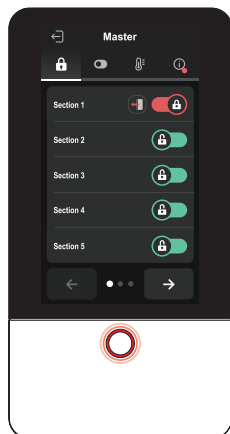


ALARM SETTING

1. Authorisation
2. Set sections using sliders on the home screen.
3. If successfully set, the slider turns red.
4. The exit delay (if set) is running and the keypad indicates this by beeping and flashing the red LED on the button.
5. Once a double beep is heard, the section is set.

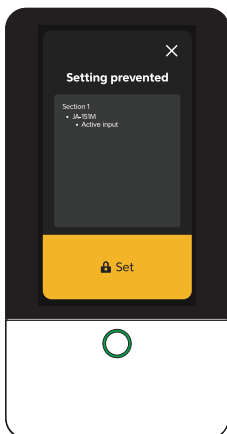
Setting the system may be prevented by status detectors that are active in the system, e.g. an open window with magnetic detector. In this case, the way of setting depends on the system settings:

- A) The keypad will set the system even if a status detector is active.
- B) The keypad will warn of active detectors; if the user does not respond or confirm, setting will be performed (**default setting**).
- C) The keypad will warn the user to active detectors, and the user must confirm setting despite the active detectors. If the user does not confirm, setting will be interrupted.
- D) The keypad warns the user to an active status detector via a screen showing which detector is preventing setting. It is not possible to leave the premises and set the system while the status detector is active. Only after the detector has been deactivated (e.g. by closing a window with an active magnet) is it possible to set the system.



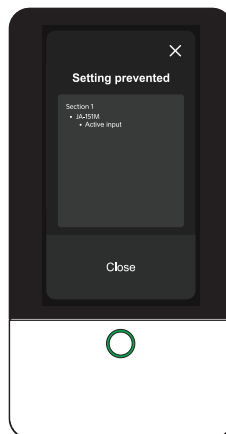
Exit delay

after successful setting.



Set with warning

Warn you to an active detector that is preventing setting. Press to Set and authorise.



Block the setting

If the detector is active, it prevent setting – the section cannot be set until the detector is deactivated.

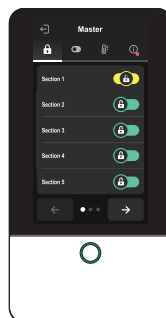
PARTIAL ALARM SETTING

CAUTION: This option is an additional feature of the alarm system.

The system can also be set partially, it allows monitoring using only selected detectors in the section.

If the partial setting function is enabled and you want to set partially, press the slider once – the slider will turn yellow. If you want to set the entire section, press a second time and the slider twice and it will turn red.

Example: It allows you to leave the windows and doors set during the night and motion detectors inside the protected premises won't respond.



DURESS ACCESS CONTROL

This function provides unsetting of the system in a special mode. The system seemingly unsets, however it triggers a silent panic alarm, which is then reported to selected users (including ARC).

This is done by adding the number 1 to the last digit of the valid code. The function can be disabled (by a service technician).

Enabling this function reduces the number of combinations by half.

Examples: Valid code: **9999** Code entered under duress: **9990**
Valid code: **1234** Code entered under duress: **1235**

CANCELLING THE TRIGGERED ALARM

An ongoing alarm is indicated on the display by a red window with a bell symbol and a red flashing LED on the control button. The alarm is cancelled terminated by pressing the Unset and cancel alarm memory option on the keypad display and subsequent authorisation.



Ongoing alarm and unsetting

Alarm indication when absent

If the acoustic alarm signal ends (always time-limited - set by a technician) and no authorisation and unsetting takes place, the display locks and the alarm memory flashes red on the LED on the button to indicate that an alarm has occurred until it is unset.

TEMPERATURE DISPLAY

If thermostats or thermometers are connected to the system, it is also possible to monitor the temperature in the building from the touch keypad under the thermometer icon in the main menu.

3.1.3.10. SYSTEM CONTROL WITH A REMOTE CONTROLLER

Remote controllers (keyfobs) must be assigned to the system by an installation technician. They can be assigned to specific users, which prevents notification SMS messages from being sent to the user who is currently controlling the system (if notifications are enabled). Remote controllers check and indicate their battery status and are equipped with visual and audible indications.

Bi-directional remote controller (keyfob)

The button functions are differentiated by lock icons. The closed lock icon sets programmed sections; the opened lock icon unsets them. Correct command execution is confirmed by an LED light; unsetting – green, setting – red. A communication fault (out of the control panels range) is indicated by a yellow LED light flashing. The buttons with symbols of full and empty circles can control another section. Buttons of the keyfob can also be configured to control PG outputs in different modes: the first button switches on / the second switches off, each button can have programmed an individual function: impulse mode or change status.

For more functions, it is possible to press two buttons at the same time. This way a 4-button keyfob can have up to 6 individual functions or one PG status output (e.g. turn the lights on and off), alternatively two PG outputs (e.g. a garage door and door lock).

If the system is configured to Set after confirmation the detector will indicate unsuccessful setting with a green LED if a device is triggered. It is necessary to confirm setting by pressing the lock button again. A set section will be confirmed by a red LED.

The keyfob buttons can be blocked to prevent accidental pressing. A command will be sent out when a button is pressed repeatedly. A low battery is indicated acoustically (with 3 beeps) and optically with a yellow flashing LED after pressing a button. For more information, consult configuration of the keyfob with your service technician.

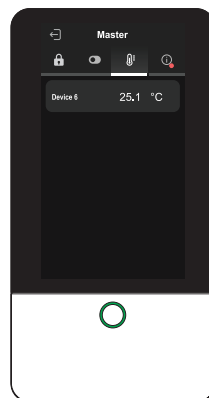
Unidirectional remote controller (keyfob)

One-way keyfobs send a signal every time a button is pressed without receiving feedback from the control panel. Sending a signal is confirmed only by a short flash of the red LED and alternatively with a beep.

4. REMOTE CONTROLLING

4.1. CONTROLLING THE SYSTEM USING THE MyJABLOTRON APP (ON YOUR MOBILE PHONE OR ON THE WEB)

The MyJABLOTRON service provides the highest level of comfort for remote control and system management. It is an application that allows online access to devices manufactured by JABLOTRON. It is intended for end users to monitor and control devices. It can be used either as a mobile or web application.



The service allows users of the JABLOTRON security system to:

- check the current status of the system
- set / unset the system or part of it
- control programmable outputs

- browse the event history
- send notifications to selected contacts via SMS, e-mail or PUSH notifications
- take pictures from photo verification devices and browse their history in the photo gallery tab or directly in the event history
- check the current values of temperature or energy consumption detectors, including displaying the measurement history in graphs and other useful functions

Depending on your country or region, a web account in MyJABLOTRON can be set up by an authorized JABLOTRON partner. The login name is the user e-mail address. The password for the first log in will be sent to this address. The password can be changed anytime in the user settings.

4.2. CONTROLLING THE SYSTEM USING THE VOICE MENU

Depending on the type of communicator used, the system can be controlled from a telephone using a voice menu, which guides the user through the range of functions in a preset language. To access the voice menu, you need to call the security system's telephone number (the telephone number of the SIM card used).

Access to the voice menu can be granted either to all phone numbers without restriction or only to contacts stored in the system. Depending on the settings, authorisation may be required by entering a valid user code on the phone keypad. After entering the menu, the system will announce the current status of all sections assigned to the given user. These sections can then be controlled using the telephone keys according to the menu, either collectively or individually.

The system default is set up to answer incoming calls after three rings (approx. 15 seconds of ringing).

4.3. CONTROLLING THE SYSTEM USING SMS

Individual sections and programmable outputs can be controlled by SMS command, similar to the button segments on the keypad. The format of the control SMS message is CODE COMMAND. The text of the command for controlling sections is preset (SET / UNSET), with the option to add a specific section number. There is a standard space between the code and the command, as well as between words in the SMS message.

Multiple sections can be controlled at once within a single SMS. In this case, section numbers are assigned to the command.

Example: SMS command to set sections 2 and 4.: **CODE_SET_2_4**

The texts of commands for controlling PG outputs can be programmed by an installation technician, e.g. BLINDS DOWN. It is possible to program that the code before the command is not required. In such case the command is simply automatically identified when the system recognizes the user's phone number from which the SMS was sent. The setting is performed by a service technician.

4.4. CONTROLLING THE SYSTEM REMOTELY USING COMPUTER (JA-100-LINK)

The JABLOTRON system can be controlled remotely using a computer with the JA-100-Link software installed. Only users with the Administrator role have authorisation to control the JA-100-Link system.

You can download it from the website <https://www.jablotron.com/en/software>.

5. CONTROL OF THE PROGRAMMABLE OUTPUTS PG

5.1. USING THE KEYPAD SEGMENT (SLIDER ON THE DISPLAY IN THE CASE OF TOUCH KEYBOARDS)

Press the right button to turn on the PG output, press the left button to turn it off. If the output is programmed to pulse, it is switched off automatically according to the pre-set time. In the case of keypads with a touch screen, PG is controlled in the main menu using the slider in the same way as for segments. Moving to the right switches PG on and the button turns green; moving to the left switches it off and the button turns red.

PG control may or may not be stored in the control panel's event memory. The setting is performed by a service technician.

Depending on the system settings, authorisation may or may not be required to control the PG output.

5.2. USER AUTHORISATION ON THE KEYPAD

It is possible to activate a PG output just by user authorization on this keypad (by entering a code or attaching RFID / NFC tag). This function is suitable, for example, for electrically controlled door locks.

5.3. FROM THE KEYPAD MENU WITH LCD DISPLAY

After authorisation in the menu, the keypad with LCD display can be used to control the PG outputs for which the authorised user has permission.

Control procedure from the menu:

- Authorisation with a valid code or keyfob.
- Enter the menu by pressing the ENTER key.
- PG control → ENTER.
- Use the arrow keys to select the desired PG group (1-32) (33-64) (65-96) (97-128) → ENTER.
- Use the arrow keys to select the desired PG → ENTER.
- Pressing the ENTER key repeatedly changes the PG status (the active PG output is indicated on the display by the PG number in a solid rectangle).
- After completing the control, exit the menu by pressing the ESC key.

5.4. BY KEYFOB

By pressing the assigned button on the keyfob. On two-way keyfobs, PG activation is confirmed by the LED.

5.5. MyJABLOTRON APPLICATION ON YOUR PHONE

Press the segment of the given PG in the PG outputs tab.

5.6. MyJABLOTRON WEB INTERFACE

By clicking on Off / On in the Automation (PG) tab.

5.7. BY DIALLING IN

For each telephone number used in the system (one user can have one telephone number set), control of one PG output can be set up by dialling in without establishing a connection. Dialling in means dialling the telephone number of the SIM card used in the security system and then hanging up before the call is picked up by the system. By default the system will answer the call after the third ring (approx. 15 seconds of ringing). This function is particularly suitable for controlling entrance gates, doors or barriers to buildings with a large number of users. The SIM card must have an active caller identification service (CLIP).

5.8. BY SMS

By sending an SMS message with the pre-set text to turn the given PG output on / off. Authorisation is / is not required depending on the settings.

Format: **CODE_CONFIGURED TEXT**

Example: „1234 gate“

6. BLOCKING IN THE SYSTEM

6.1. PROTECTION AGAINST THE CODE BREAKING ATTEMPT (only for Security grade 3)

In the event of 10 invalid authorisations, the number of authorisation attempts will be exceeded and the system will be blocked. From the moment of announcement, a 90-second timer is started, during which access to the entire system is disabled. This status cannot be cancelled in any way. After 90 seconds, it is necessary to enter the correct code on the first attempt; if this is not successful, the system is locked immediately after the first invalid attempt.

If 21 consecutive invalid codes are entered, the control panel will declare sabotage.

6.2. ANTIMASKING (only for Security grade 3)

This is a situation where any device in the system is covered by some object and then the detector cannot be detect any movement. In this case, the entire section enters the Antimasking state and sets an insurmountable obstacle to securing the system.

6.3. SYSTEM WATCHDOG (only for Security grade 3)

The control panel monitors its own correct and safe operation. In the event of an error or malfunction, it automatically resets itself. The fact that the system is in Watchdog mode can be recognised by a yellow optical signal and the display of the malfunction in the event history on the keypad.

This is an insurmountable obstacle for security. Only a service technician can cancel the Watchdog memory signal.

6.4. BLOCKING USERS

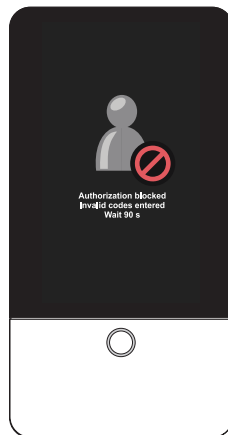
To temporarily disable a user's access (e.g. due to disclosure of the code or loss of the tag), any user can be blocked. This block will prevent the user from accessing the system, and their code and tags will not be accepted by the system. No SMS messages with reports or call notifications will be sent to the blocked user's phone number.

User blocking may be performed by the system administrator or service technician. It can be configured in the LCD keypad menu using the following procedure: Settings / Users / User / Blocking by selecting „Yes“ for „ „. It is also possible to block users via local or remote access from the JA-100-Link software by clicking on the user in the Settings / Users / Deactivation column.

A red dot symbol will appear next to blocked (disabled) users in the programme until the block is removed.

6.5. BLOCKING DETECTORS

To temporarily disable any detector, use the same procedure as for blocking a user. Detectors are blocked when their activation is not desired (e.g. motion detection in a room where an animal is present). Only the alarm function is blocked; tamper and service events are still processed.



Blocking may be performed by the system administrator or service technician. Detector blocking can be configured in the LCD keypad menu using the following procedure: Settings / Devices / Blocking by selecting „Yes“. It is also possible to block detectors from the JA-100-Link software by clicking on the detector in the Settings / Diagnostics / Disable column. A yellow dot symbol will appear in the software for a blocked detector until the blocking is cancelled, which is done using the same procedure. It is also possible to block devices using the MyJABLOTRON application for smartphones.

6.6. DISABLING TIMERS

To temporarily disable automated scheduled events in the system, a timer can be disabled. Disabling a scheduled event (e.g. unsetting the system from partially setting at a pre-set time) will prevent execution of that event (e.g. while on vacation).

A timer can be disabled locally or remotely through the JA-100-Link software by clicking on the section in the Settings / Calendar / Blocked column. A disabled timer is marked with a red dot until it is turned back on using the same procedure.

7. USER SYSTEM SETTINGS

7.1. CHANGING THE USER ACCESS CODE

If the system is configured to be controlled using codes without a prefix, only the system administrator and service technician are authorised to change the codes. The system administrator can make changes not only from the LCD keypad menu, but also via the JA-100-Link software or the MyJABLOTRON application for smart mobile phones. The code can be changed using the LCD keypad after authorisation by selecting Settings / Users / User / Code. To enter a new code, edit the item (make it flash) by pressing the Enter key, enter the new code and confirm with the Enter key. After making the changes, select the „Save“ option when prompted with the question „Save Settings?“.

If the system is configured to control using codes with a prefix, it is also possible to allow users to change their code from the keypad menu with a touch or LCD display.

These changes are made after authorisation by selecting Settings / Users / User / Access Card 1 (or 2). To insert a new RFID tag or card, edit the item („flash“) by pressing the Enter key and place the RFID tag or card on the reader part of the keypad (i.e. in front of the keys) or enter the serial number listed under the barcode and confirm again with the Enter key. To delete an access card, enter a single zero „0“ instead of the serial number when editing the field. After making changes, select „Save“ when prompted „Save Settings?“.

The system administrator can make changes not only from the keypad menu with an LCD display, but also via the JA-100-Link software.

7.2. CHANGING THE TELEPHONE NUMBER OR USER NAME

If the system is configured to be controlled using codes with a prefix, each user can add, change or delete their telephone number from the menu on the LCD keypad. Changes are made after authorisation by selecting Settings / Users / User / Tel. number. To make changes, edit the items (make them flash) by pressing the Enter key, enter the new data and confirm again with the Enter key.

To delete a telephone number, enter a zero „0“ in the field instead of the telephone number when editing. After making changes, select „Save“ when prompted „Save Settings?“.

The system administrator and service technician also have the authority to add, change and delete telephone numbers or change user names. The system administrator can make changes not only from the LCD keypad menu, but also via the JA-100-Link software.

7.3. ADDING A NEW USER / DELETING A USER

Only the system administrator or service technician has the authorisation to add a new user (delete an existing user). A new user can only be added to the system (an existing user deleted) using the JA-100-Link software, or in the case of a service technician, using the F-Link software.

When creating a new user, they must have access rights to individual sections and control of programmable outputs with the required authorisation.

8. CALENDAR SETTINGS

Calendar events (unsetting / setting / partial setting, and controlling or PG blocking) can be configured in the system. Calendar events are programmed in the JA-100-Link software in the Calendar tab.

For each event, you can configure the action, sections or PG outputs and the time of the event. The day can be defined by the day of the week, month or year. On the pre-set day, you can configure up to 4 times to perform the action or program it to repeat at regular intervals.

Calendar events can thus be variably adapted not only for section control, but also for controlling various technologies in the building using PG outputs.

9. EVENT HISTORY

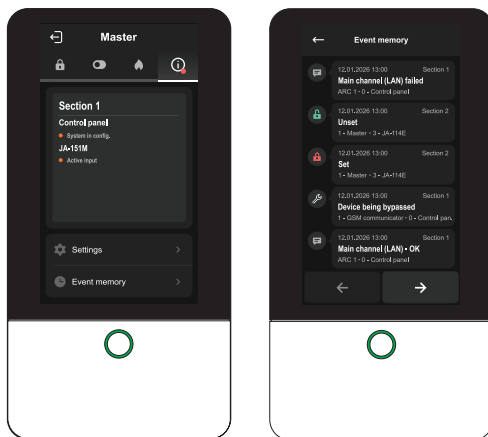
The security system stores all performed operations behaviour and events (setting, unsetting, alarms, faults, reporting to users and the ARC reports) in the control panel memory on a micro SD card. All events are always accompanied by the date and time of occurrence or termination and the source of the event (cause or origin).

Events can be viewed in several ways:

9.1. BY BROWSING EVENTS ON THE KEYPAD WITH LCD DISPLAY / TOUCH SCREEN

For keypads with an LCD display, user authorisation is required to access events on the keypad. After authorisation, the items available according to the relevant authorisation are displayed in the Event Memory item. Records can be browsed using the arrows.

On keypads with a touch screen, the event memory can be found under the (i) icon in the main menu and then under the History item.



9.2. READING EVENTS WITH THE JA-100-LINK SOFTWARE ON A COMPUTER

Event history can be loaded in parts using the JA-100-Link software via a remote connection, depending on the volume of data being downloaded. Loaded events can be filtered in detail, colour-coded for clarity and, if necessary, saved to a file on your computer's hard drive.

9.3. BY LOGGING INTO MyJABLOTRON (ON THE WEBSITE OR IN THE SMARTPHONE APP)

All events in the system are available in the MyJABLOTRON web interface. This data can be read after logging into your MyJABLOTRON user account. The account respects the display of the history range according to the account owner's settings.

10. TECHNICAL SPECIFICATIONS

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
FUNCTIONAL CHARACTERISTICS					
Max. number of devices	50	50	230 Max. 120 wireless devices at positions 1–120		Max. 60 devices per 1 Bus terminal
(I-)bus outputs	1x bus terminal 1x I-bus onboard (JA-11xR only)	1x bus terminal 1x I-bus onboard (JA-11xR only)	2x bus terminal 1x I-bus onboard		
Max. number of JA-11xR radio modules	3	3	3	0 for Security grade 3 3 for Security grade 2	Max. number of JA-11xR radio modules
Max. number of users	50	50		600	
Maximum number of independent sections	8	8		15	
Maximum number of programmable outputs	32	32		128	Only PG 1 - 32 can be used for wireless transmission.
Blocking of user inputs in case of incorrectly entered codes		No blocking		after 10 incorrectly entered codes, then every other attempt	User input is, for example, a keypad or F-Link
Alarm Sabotage due to incorrect code entry / blocking time		after 10 incorrect entries		Optional: from 10 to 21 incorrect code entries	
Event memory		approx. 7 million recent events including date and time			

ALARM SYSTEM FEATURES

Compliant with standards	EN 50131-3, EN 50131-5-3, EN 50131-6, EN 50131-10 (EN 50136-2, EN 50136-1) INCERT T 031	---
Classification	Security Grade 2	Security Grade 3 or 2
Environment class	II Indoor general	
Power supply type	Type A according to EN 50131-6	
		According to profile

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
ATS classification	SP2-SP5 (LAN) SP2-SP5 (GSM) DP3 (LAN+GSM)	SP2-SP5 (LAN) SP2-SP5 (GSM) DP3 (LAN+GSM)	SP2-SP5 (LAN) SP2-SP5 (GSM) DP3 (LAN+GSM)	SP5 (LAN) SP5 (GSM) DP3 (LAN+GSM)	When using a GSM communicator, see the separate communicator manuals for more information.
Certification body	Trezor Test s.r.o. (No. 3025), Kiwa Nederland b. v.				Trezor Test s.r.o. (No. 3025)

EXTERNAL COMMUNICATION

LAN communicator	on board Ethernet 10/100 BASE			
GSM communicator	Yes, using accessories			
- SMS reports	Up to 8 users		Up to 50 users	Not included in the control panel
- voice reports	Up to 8 users		Up to 15 users	5 reports per event
- Caller identification (CLIP)	ETSI EN 300 089			

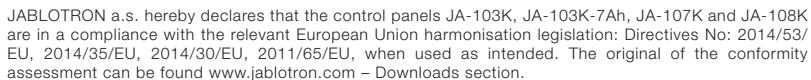
CONTROL PANEL POWER SUPPLY

Power supply voltage	110 ÷ 230 V _{AC} , 50 ÷ 60 Hz			
Maximum current consumption	Max. 0.28 A		Max. 0.85 A	
AC power consumption	Max 30 VA		Max 55 VA	At maximum bus load and with GSM module
Current protection	Fuse 5x20 F1.6 A/250 V			
Electrical protection class	II.			

ELECTRICAL PARAMETERS FOR CALCULATING BATTERY BACKUP

Nominal DC current consumption of the control panel board with LAN	90 mA	105 mA	Current consumption measured from the battery
Nominal DC current consumption of the control panel board without LAN	60 mA	70 mA	Current consumption measured from the battery
Low battery fault voltage	11 V		
Voltage at the end of low battery voltage detection	12.2 V		

Feature / Type	JA-103K	JA-103K-7Ah	JA-107K	JA-108K	Note
ELECTRICAL PARAMETERS FOR CALCULATING BATTERY BACKUP					
Deep discharge protection – Battery disconnect voltage	9.6 V				
POWER OUTPUTS					
Bus voltage	12.0 to 13.8 V				
Max. continuous consumption from the control unit	1000 mA		2000 mA		Terminals (red – black) JA-107K / JA-108K provides 2x bus terminal blocks and an I-bus connector for expansion. The maximum consumption from the control panel must be divided between both outputs.
Max. continuous load of one Bus terminal	1000 mA		2000 mA (max 3000 mA / 60 min)		
Bus terminal	bus 1 + 4-pin connector (I-bus) for radio module		bus 1, bus 2 + 4-pin connector (bus 3) for connecting a radio module or hub JA-110Z-D		For JA-107K, the individual buses are isolated from each other, i.e. short-circuiting one branch will not affect another
Maximum bus cable length	500 m		3 x 500 m		Can be extended using JA-120Z modules
OPERATING CHARACTERISTICS					
Dimensions	357 x 297 x 105 mm				
Weight with battery / without battery	1844 g / 970 g	3755 g / 1665 g	7027 g / 1809 g		
Operating temperature range	-10 °C to +40 °C				
Average operating humidity	75 % RH, non-condensation				
Recommended backup 12V battery	12 V / 2.6 Ah (lead-acid gel)	12 V / ≤ 7 Ah (lead-acid gel)	12 V / 18 Ah (lead-acid gel)		
Maximum time to recharge the battery to 80% capacity	48 hours				



Note: Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling. Please return the product to the dealer or contact your local authority for further details of your nearest designated collection point.



NOTES:

[illegible]

www.jablotron.com



M-MULTI100+
(MMD28005)