

Contents

a	(☑ 1.) Unsplit system	(☑ 2.) Partially split system	(☑ 3.) Split system
0	No event	No event	No event
1	Set all	Set all	Set all
2	Unset all	Unset all	Unset all
3	Set all	Set A	Set A
4	Set all	Set AB	Set B
5	Unset all	Unset all	Unset A
6	Unset all	Unset all	Unset B

Example:
 To program setting (arming) the AB section of a partially split system at 22:45 everyday, enter:

64 0 4 22 45

To cancel the schedule, enter: **64 0 0**

- Notes:**
- If the control panel is in the requested setting/unsetting state before the scheduled event time, the event will not change the setting/unsetting.
 - If any automatic event is selected, it will be performed everyday at the programmed time with all its consequences. It means that the system will be set even when people are still on the premises,
 - To cancel a scheduled event, enter 64 n 0
 - As a factory default, all automatic events are switched off.

19. Programming phone numbers for SMS messages

This setting is usually performed by an installer during the installation. The programming of the phone numbers can be also done by the administrator in Maintenance mode if enabled (☑ **B.**). Follow the manual supplied with the communicator.

Dear OASiS user2

What is a security system?2

System access codes (cards)3

1. System setting (arming)4
2. During the setting (arming) process5
3. After the system has just been set (armed)6
4. System unsetting (disarming)6
5. To stop the alarm7
6. Operating the system from an outdoor keypad8
7. Panic alarm8
8. Controlling connected devices from a keypad8
9. Remote control – by phone, Internet.....9

User configuration – access codes (cards).....9

10. Programming the master code (card)10
11. Programming user codes (cards).....10
12. Key-fob setting12

User configuration – Maintenance mode12

13. Entering Maintenance Mode12
14. System testing13
15. Displaying which user/card positions are occupied13
16. Bypassing.....14
17. Setting the internal clock15
18. Automatic setting/unsetting schedule15
19. Programming phone numbers for SMS messages16

Contacts for when you need help:

Your Installer:

Manufacturer:

JABLOTRON ALARMS Inc. <http://www.jablotron.com/>

Dear OASiS user

The development and production of your security system have been done by the **manufacturer** with maximum care so that your oasis of safety – your room, house or company premises – can be protected as well as possible.

The second party having an impact on the quality of a security system is the **installer**. The installer company should know the system well, therefore do not hesitate to contact them if you have any questions about system operation or when you need an in-depth explanation of how the system works.

However, the most important participant of a properly working security system is you, the daily **user**. Please, follow these guidelines as well as the installer's instructions when you take over the system. During the system's everyday use, you can read information from the keypad display. This way you can be informed that a balcony door is open or that maintenance of a particular device is needed.

What is a security system?

Any electronic security system (ESS) has a control panel as its essential part. The control panel comprises all the system's important functions. Among the control panel's constituent optional parts, there is a communicator for transmitting messages to an alarm receiving centre, and a back-up battery, which ensures that the system works properly (for a given period) after a power supply outage.

The control panel should be installed in a hidden place. In the case of an intrusion, a hidden-working control panel transmits messages even if all other parts of the ESS have been destroyed.

The connection between you and the control panel is established via a keypad. This way you can operate the system or, conversely, the system informs you via the keypad display or LED signalling.

House premises are protected by detectors. These react to various events: movement (PIR), door or window opening (magnetic detector), glass pane breaks (glass break detector). In addition, smoke detection or combustible gas leak detection can be included in a system's functionality. This way an ESS can detect threats to property or health.

When a security system detects movement in a protected area, information is sent, depending on the system configuration, to your mobile phone or to an alarm receiving (central monitoring) company, which performs on-site physical intervention. Outdoor sirens let the neighbourhood know that something is going on, whereas the main purpose of indoor sirens is to discourage the intruder.

- Any bypass programmed for a single setting/unsetting cycle will be automatically cancelled after unsetting (disarming) the system.
- The existing bypass configuration can be checked or modified in the bypass menu.
- If the installer enters service mode all bypasses will be cancelled.. Alternatively, you can cancel all bypasses using key **4** in the bypass menu.

17. Setting the internal clock

The control panel has a built in real-time clock which is used to time-stamp all recorded events in the control panel memory. The clock should be set during installation. However, the administrator can re-set the clock. This can be used for summer time offsets when automatic summer time is disabled (**A.**). To set the clock, enter:

4 hh mm DD MM YY

where: **hh** hours
mm minutes
DD day
MM month
YY year

Example:

at 21:30 on April 29, 2007 enter: **4 21 30 29 04 07**

If automatic summer time is enabled (**A.**), the control panel's internal clock is automatically offset by +1 hour on March 31st at midnight. The offset is then removed on October 31st at midnight to return to winter time.

18. Automatic setting/unsetting schedule

This can be used to program an automatic sequence of daily setting/unsetting events. Up to 10 daily events can be programmed. The events will occur every day of the week.

To program an automatic schedule enter: 64 n a hh mm

where: **n** is the event number from 0 to 9
a is the type of event from 0 to 6 (see the following table)
hh hours (time of event)
mm minutes (time of event)

To display the positions:

- Press key **5** (the display indicates “Codes 01: Code” – or the name of the code holder).
- Using the arrow keys ▲ and ▼ all user positions (01 to 50) can be scrolled through. The **A** indicator shows whether a **code** is programmed or not, and the **B** indicator shows whether a **card** is programmed or not. (This means if both indicators are lit, the position is occupied by a code and a card.)
- To exit this code/card display mode press the # key.

Notes:

- Code programming is only possible when the system is unset (disarmed) and in Operating mode. When the system is in Maintenance mode, code programming is disabled.
- The most convenient way to administer codes is by using a PC running Olink software – select the “Codes” menu option.

16. Bypassing

In practice, you may need to set (arm) the system while excluding particular zones (potential sources of alarms). This exclusion is referred to as a **bypass**.

To set up a bypass:

1. Press key **1** to open the bypass menu while in maintenance mode.
2. Using the ▲ and ▼ keys, you can scroll through all potential alarm sources. Select the source (detector, controller...) which you want to bypass and:
 - a. press key **2** to **bypass** the source for the next setting/unsetting cycle (the ⚠ indicator will start flashing),
 - b. press key **3** to **bypass the source permanently** (the ⚠ indicator will light continuously).
 - c. Multiple pressing and holding of the keys (**2** or **3**) will toggle the bypass on – off – on ...
 - d. Using key **4** will cancel all device bypasses in the system.
3. All the desired bypasses can be reprogrammed by repeating step 2.
4. Press the # key to exit the bypass menu. Pressing # again exits maintenance mode.

Notes:

- If a system with bypassed devices is being set, then bypass text will be displayed on the keypad unit.

The OASiS system is configurable and its exact behaviour is determined by system settings. The following text contains references to the system configuration table which is to be found at the end of this manual. The table should be filled in by an installer during the installation process. References are numbered, like for instance (☑ 4.). In this case you can find particular settings for the 4th parameter in the table.

System access codes (cards)

The system status can be controlled via a keypad (internal or external) using access codes or cards. To prevent misuse by a stolen card, you can set that card access must be confirmed by entering a proper code (☑5.). In addition, you can operate the system wirelessly by key-fob or remotely via phone or using internet access (see www.GSMLink.cz).

Access codes and cards

Access codes and cards allow system operation – i.e. setting (arming), unsetting (disarming), stopping triggered alarms, triggering silent alarms (PANIC), etc. Access code functionality can be configured during installation. The system allows for up to 50 different access codes (cards) to be assigned to different users. This way it is possible to distinguish (at the alarm receiving centre or in the control panel memory) who has operated the device and when. As a factory default, all access codes are blank. It is up to you – the system administrator (master) – to define access codes as desired, using a Master code or card.

Note: Entering an invalid access code ten times in a row will trigger a tamper alarm.


The Master code (card)

The master code (card) is an access code or card with a higher priority which, in addition to allowing system control, enables you to change or configure access codes for other users. Knowing the master code or possessing a master access card is necessary for any user configuration of the system.

Usually, the master code is used by the system owner or administrator, who performs a change of the factory default value 1234 to his or her required master code after taking the system over from the installer. An access card can be set up in place of a master access code. This should be kept in a safe place.

The service code



The service code is a special code designed for a service company. The code allows maintenance technicians system configuration and testing.

Note: it can be set by a service technician that by means of a service code it is possible to unset the system to provide full service and maintenance of the system under any circumstances (he will not be able to modify or add user codes). Unsetting the system by the service code can only be enabled with the **written agreement of the owner of the system** – see  15.






1. System setting (arming)

There are several ways to set (arm) the system.

An unsplit system (1.)

- **Enter a code** (present a card).
- **On the key-fob**, press the  button.
- If operation without an access code is enabled (4.), you can set (arm) the system by pressing the ABC key.

A system with partial setting (arming) (2.)

- If operation without an access code is enabled (4.), you only have to press the A button to set section A, the B button to set both sections A and B, or the ABC button to set the entire system.
- When the system is only partially set (e.g. only section A), it is possible to extend the proportion of the system armed by pressing the corresponding button (B or ABC). All detectors configured to delayed or next-delayed reactions will provide an exit delay. Thus, you will not need to turn off partial setting first to set the whole system each time you leave the house. Instead, you can perform total setting straight away and the system allows departure through all zones covered by delayed and next delayed detectors.
- If operation without an access code is disabled (4.), then pressing the A, B, or ABC key must always be followed by entering an access code (or by presenting an access card).
- **Key-fob:**
 - press  for total setting (A + B + C)
 - press  to set section A
 - press  to set sections A+B

14. System testing

The administrator should test the system monthly. For testing, the control panel should be in operating mode and unset (it can also be in maintenance mode). When in operating mode, the control panel indicates the triggering of a detector, but no alarm can be triggered if the system is unset.

We recommend triggering the detectors (zones) one by one and verifying that the triggering is indicated on the keypad display – by displaying the signal type and source. Remote controllers (key-fobs) or panic buttons can be tested in a similar way.

Note: some detectors (for example the JA-80P wireless motion detector) are equipped with battery-saving functionality which prevents repetitive triggering in short intervals. In this case a pre-programmed time has to elapse before subsequent triggering is possible (up to 5 minutes).

In maintenance mode, **close the wireless keypad's flip cover** if you are not working with it to save battery energy.

If anything does not work properly during testing, call the installer for help.

In maintenance mode it is possible to replace discharged batteries in the devices. But it is highly recommended to ask your installer to replace the battery.

Improper handling can result in damaging the device and loss of warranty.

Recommendations: the system should be annually inspected by a professional installer who should check the backup battery voltage and perform functionality testing.

15. Displaying which user/card positions are occupied

When in maintenance mode, the control panel can display which positions in the range 01 to 50 are occupied by codes or cards.

- The administrator can check which positions (01 to 50) are occupied by a code or card in maintenance mode – see 15.
- To erase a code without knowing its nn position use sequence *** 6 master code (card) 00 code**
- **To erase all codes and cards set * 6 master code (card) 00 0000.** The master code (card) will not be effected.

12. Key-fob setting

Setting or adding other key-fobs to the system can be done by the installer who is also able to block or replace a lost key-fob. An immediate bypass can be done by the administrator of the system - see 16).

User configuration – Maintenance mode

The following description is intended for a system administrator, who knows the control panel master code or possesses a master card which is authorized to modify the system configuration.

All the settings can be performed via keying-in on a system keypad. An unfinished sequence can be escaped from by pressing the # key. A sequence is stored into control panel memory only after the sequence has been completely entered.

13. Entering Maintenance Mode


You can enter maintenance mode when the control panel is unset by keying-in *** 0 master code (card)**. The mode will be indicated on the keypad display.

Maintenance mode enables the following:

- internal-clock configuration
- automatic setting/unsetting schedule
- programming telephone numbers for alarm reporting
- testing detectors or opening their covers without triggering an alarm
- zone bypassing configuration
- displaying which code/card positions are already occupied

Exit maintenance mode by pressing the # key.

A split system (☒3.)

- If operation without an access code is enabled (☒4.), you only have to press the A or B button to set (arm) the corresponding section. Pressing the ABC button results in total setting.
- If operation without an access code is disabled (☒4.) and you perform setting (arming) via an access code or card, then only the section assigned to the code (card) is set (A, B or ABC).
 - If the code (card) belongs to the whole system (ABC), then it is possible to set only section A or B by pressing button A or B before entering the code (card).
- Using an access code (card) assigned to section C will set the entire system (ABC). You can also set either section A or B alone – by pressing the A or B button respectively before you enter a code (or present a card).
- By pressing the  button on the key-fob the section to which the key-fob belongs will be set.
- When both sections A and B are set, the common section C is set automatically too

2. During the setting (arming) process ...

The system will warn you when anything is going wrong. Pay attention at the moment of setting to the information on the keypad.

If the (☒10.) parameter is enabled, then by displaying “Triggered det.” on the keypad, the system gives you notice that a detector is triggered (usually a window or a door is open). By pressing the ? key you will be shown which particular detector it is. If there are more detectors triggered, you can access them on the display by pressing (?) repetitively. Naturally, in such situation, it is appropriate to check through the building and close the doors and/or windows.

If the (☒10.) parameter is disabled, then **no “Triggered det.” text will be displayed.** Nonetheless, pressing the ? key lets you display the list of triggered detectors.

If the (☒11.) parameter is enabled and “Triggered det.“ is shown on the keypad display, then after entering an access code (card) or after pressing the A B or ABC button for quick setting (arming) **you will be offered the possibility of a bypass** – which means the temporary removal of triggered zones from the system. If you wish to accept/confirm the bypass suggestion, press *. **If no**

confirmation is made, the system will not be set! The system behaves the same way when bypassing has been pre-programmed **in maintenance mode**.

If the (▣11.) parameter is disabled, any triggered detector is bypassed automatically – no key-press confirmation is needed.

While setting (arming) the system via a key-fob controller, any triggered zone is bypassed automatically regardless of the (▣11.) parameter.

If a detector has been bypassed, it starts to protect as soon as it is de-triggered (for example, if a door is closed).

3. After the system has just been set (armed)

- The keypad **beeps** and an exit delay will begin. The keypad displays “**Exit delay**”.
- The keypad indicates which sections have been set (A; B; C).
- If exit delay acoustic signalling (▣6.) is enabled, the exit delay is indicated by regular beeps from the keypad (the beeps get faster in the last 5 seconds).
- For a partially set system, the exit delay may not be signalled acoustically (▣7.).
- You have to leave protected areas before the exit delay (▣20) elapses.
- If **final-door** detector mode (▣12.) is triggered during an exit delay, then the exit delay is extended to the moment when the final door is closed. So you can set and leave the house comfortably without any haste. If the final-door detector is not triggered, then the system provides a normal exit delay.

4. System unsetting (disarming)

After you step into a set (armed) section, an **entrance delay** will begin. This is indicated by displaying “Entrance delay” on the keypad. Also, the keypad starts to beep fast if entrance delay acoustic signalling is enabled (▣8.) (the wireless keypad only if it is powered from the AC adaptor or the door detector is connected to the keypad or when you open its cover). Additionally, the entrance delay time can be indicated by an indoor siren.

- During the entrance delay (▣21) you have to unset (disarm) the system by entering a valid access code (or, alternatively, presenting a valid access card, or using a valid key-fob).

Code programming is only possible when the system is unset (disarmed) and not in maintenance mode.

In practice, it is convenient that each user has his own user code pre-programmed. The system stores to its memory which code was used for what event and when. As a factory default, all access codes (cards) are blank. To define a user code, enter the following sequence:

*** 6 xxxx nn yyyy**

where

xxxx is the master code

nn is the user code index (from 01 to 50)

yyyy is the new user code. By inserting 0000 the code in the nn position will be erased

Example:

If the master code is 1234 and user 3's new code should be 5277, enter:

*** 6 1234 03 5277**

Alternatively, assign a card to user 3 by entering:

*** 6 1234 03 and present user 3's card**

Notes:

- Both a **code and a card** can be assigned to **every position**
- If you want to assign a code and a card to position nn set the code and then on the same position the card (or vice versa)
- **If the system is programmed to require card verification by code (▣5.), a user who has a code and card set always uses both (no matter which order). If the user has only a code or a card then verification does not concern him.**
- If the administrator records the codes on the table in the appendix of this manual it is necessary to keep it hidden in a safe place. Better would be to use and store them in the Olink software (access is encrypted)..
- The installer sets the reaction of the system to each code and the code assignments to each section (A,B,C).
- A code cannot be assigned to 2 different positions. Code relocation can be done by deleting the code (card) and, subsequently, programming it to a new position.
- For security reasons, do not use codes which are easily predictable such as four equal digits, birth dates, company personal numbers, etc.

10. Programming the master code (card)

The master code is used by the house owner or administrator (supervisor). The factory default setting is 1234. The administrator should program his/her own four-digit code while taking the system over from an installer. This prevents other parties from accessing the system configuration. **Master code programming is only possible when the system is unset (disarmed) and not in maintenance mode.**

To change an existing master code enter:

*** 5 xxxx yyyy yyyy**

where

xxxx is the existing master code

yyyy is the new master code (the new code must be entered twice to avoid errors). Combination 0000 cannot be used. The master code cannot be erased.

Example:

Existing code 1234 will change to 6723 by entering: * 5 1234 6723 6723

If you wish to use an access card instead of a code, you can enter * 5 xxxx and then present the card. This makes the card authorized for system configuration.

If you forget the master code (or if you lose the card), an installer can reset the code to the factory default setting 1234 (this requires the system to be unset (disarmed). All other pre-programmed codes (cards) in the system remain unaffected.

11. Programming user codes (cards)

The system allows for up to 50 different access codes (cards). Their modification or deletion is only available to the system administrator who knows the master code. The most comfortable way to edit the user code is via Olink software.

- If final-door detector mode (☒12.) is active and you came in through the corresponding door, then the entrance delay would be six times longer than if it had been triggered by an ordinary detector (i.e. if you had come in through a “main door”). This way you have enough time for unsetting the system (☒ 22). However if any other delayed detector is activated the entrance delay will be shortened to a normal entrance delay time.
- If the ⚠ is **flashing on the keypad** and the display is showing which device was triggered, it means that there was an **alarm**. Unset the system and carefully check the reason for the alarm. Keep in mind that there could be somebody hidden on the premises. **Alarm memory** – flashing - ⚠ can be erased from the display by pressing button #

An unsplit system (☒1.)

- Enter a code (present a card).
- Use a key-fob: by pressing the Ⓞ (or ○) button you will unset the whole system.

A system with partial setting (arming) (☒2.)

- Enter a code (present a card).
- Use a key-fob: By pressing the Ⓞ (or ○) button you will unset the whole system.

A split system (☒3.)

- Enter a code (present a card) or use a key-fob to unset the corresponding system section.

5. To stop the alarm

If there is an alarm in the system it can be stopped by **entering a code (presenting a card or using a Ⓞ on the key-fob).**

Alarm signalling – a flashing ⚠ and information about the reason for the alarm – this can be terminated (after stopping the alarm) by pressing the # button. The **memory entry for the last alarm** can be displayed by pressing *4, to scroll through the history keep pressing button 4.



Keep in mind that there could be somebody hidden on the premises. If you have any doubts, then it is recommended to have the premises checked by a security service from the alarm receiving station.

6. Operating the system from an outdoor keypad

If the system is equipped with a JA-80H outdoor keypad or a JA-80N external card reader, then the outdoor device can be set to work the same way as an indoor keypad. The system will be set/unset after entering a code (presenting a card).

A more common usage of the outdoor keypad is to open the entrance door:



- Performing setting or unsetting the system is only possible via an indoor keypad (or via a key-fob controller).
- Enter a valid access code or present a valid card to the outdoor keypad to open the electronic door lock.

If the system is set, and the door is opened via an outdoor keypad, an entrance delay will begin. During this delay period the system has to be unset using an indoor keypad unit (or a key-fob).

7. Panic alarm

If you are in danger you can trigger a silent panic alarm to inconspicuously call for help. After triggering a panic alarm the system will send voice messages, SMS messages, and pass data to an alarm receiving centre (central monitoring station), depending on installation settings. A set system will be unset.

A panic alarm can be triggered as follows:

- **On the keypad** – enter * 7 before entering an access code (before presenting a card). If the system has been in a set state, it will be unset = operation under duress.
- On the **key-fob** controller – press both  and  buttons simultaneously. If desired, the controller can be re-configured (by an installer) for Panic Mode, in which pressing any button will trigger the Panic alarm.
- By pressing a **large-sized panic button** (that can be installed on a wall, under a desk etc.).
- By a **panic code or card** on the keypad.

8. Controlling connected devices from a keypad

The control panel allows you to control various devices in the building, e.g. heating, air conditioners, ... (13.) and (14.). Control can be performed via a keypad by keying-in the following:

Device X (13.)	turn ON	* 81 (or by pressing ▲)
	turn OFF	* 80 (or by pressing ▼)
Device Y (14.)	turn ON	* 91
	turn OFF	* 90

The outputs may be used to unlock locks – opening a door via a short impulse). In this case, enter the following:

an impulse to operate (13.) is provided by pressing * 8 (or by pressing ▲)
an impulse to operate (14.) is provided by pressing * 9

Optionally, the system can be pre-programmed by a service company so that the above operations require an access code (card).

9. Remote control – by phone, Internet

If the control panel is equipped with a suitable communicator (C.) you can control it remotely by mobile phone (directly by using the phone's keypad or by SMS). It can be also controlled via the Internet – after registration on www.GSMLink.cz For further details see also the communicator's manual.

User configuration – access codes (cards)

The following description is intended for a system administrator, who knows the control panel master code or possesses a master card which is authorized to modify the system configuration.

All the settings can be performed via keying-in on a system keypad (or very comfortably via a PC running Olink software). An unfinished sequence can be cancelled by pressing the # key. A sequence is stored into control panel memory only after the sequence has been completely entered.

*Note: The Oasis JA-80 system has three modes: **operating mode, maintenance mode and service mode.** Operating mode is for the day-to-day use of the system by all authorized users, e.g. setting/unsetting (arming/disarming). Maintenance mode is for the holder of the master code (system administrator) to have limited programming of the system, e.g. changing codes/cards, bypassing and is inaccessible to all other users. Service mode is only for installers and is used to program and control all aspects of the system.*