

Application for control of the INTEGRA / INTEGRA Plus
alarm system for iOS

INTEGRA CONTROL

Application version 6.1

EN

CE

integra_control_ios_en 02/24

Satel® 

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. 58 320 94 00
www.satel.pl

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.

Please visit us at:
<http://www.satel.pl>

The following symbols may be used in this manual:



- note;



- caution.

CONTENTS

1	Introduction.....	3
2	Features	3
3	Required settings of the ETHM-1 Plus / INT-GSM / INT-GSM LTE module	3
3.1	QR code.....	5
4	Installation and first start of the application.....	6
5	Application settings.....	6
6	Objects	7
6.1	Adding a control panel.....	8
6.1.1	Adding communication settings manually.....	9
6.1.2	Importing communication settings by using a QR code	10
6.2	Deleting a control panel.....	10
6.3	Adding macro commands.....	10
6.4	List of cameras.....	10
6.4.1	Adding a camera	11
6.5	Control panel searching	14
6.6	Establishing communication with the control panel.....	14
7	Information about the control panel	14
8	Operating the alarm system	14
8.1	Status bar.....	14
8.2	Shortcut bar.....	15
8.2.1	Customizing the shortcut bar	15
8.3	Macros	16
8.3.1	Customizing the macros layout.....	16
8.3.2	Running macros from the “Shortcuts” app.....	16
8.4	System.....	17
8.4.1	Partitions	17
8.4.2	Controlling partitions	18
8.4.3	Zones	19
8.4.4	Temperatures.....	20
8.4.5	Bypasses / violations / tampers / alarms	20
8.4.6	Bypassing zones	20
8.4.7	Zone searching	20
8.5	Control	20
8.5.1	Outputs.....	20
8.5.2	Thermostatic outputs	22
8.5.3	Output searching.....	24
8.6	Timers.....	24
8.6.1	Editing system timers	24
8.6.2	Editing partition timers	24
8.7	Users.....	25
8.7.1	User searching	26
8.7.2	Adding a user	26
8.7.3	Editing a user	26
8.7.4	Deleting a user	29
8.8	Cameras	29
8.8.1	Video footage from camera.....	30

8.9	Troubles	31
8.10	Events	32
8.10.1	Filtering events.....	33
8.10.2	Event searching	33
8.11	Keypad	34
8.12	Notifications	34
8.13	Help	35
9	Disconnecting from the control panel and logging out.....	35
10	Manual update history	35

1 Introduction

INTEGRA CONTROL is a mobile application for remote control of the INTEGRA / INTEGRA Plus alarm system. The ETHM-1 Plus and/or INT-GSM / INT-GSM LTE module must be connected to the control panel. The mobile device on which the application will be used must have access to the Internet.




Only one user of the application at a time may connect to the control panel via one communication module. The communication module does not allow multiple users to operate the control panel simultaneously. If you want multiple users to be able to connect to the control panel simultaneously, connect more communication modules to the control panel.

2 Features

- Status check of partitions, zones and outputs.
- Ability to arm / disarm the system or clear alarm.
- Ability to bypass / unbypass the zones.
- Control of the outputs.
- Overview of the troubles.
- Access to the event log.
- Full functionality of the alarm system keypad.
- Ability to implement automation functions by means of macro commands.
- Secure, encrypted connection to the control panel.
- Push notifications with option of personalized configuration.
- Option to use the SATEL connection setup service.
- Video footage from IP cameras.
- Editing settings of the partition timers and system timers.
- Editing thermostatic outputs settings.
- Managing users.

3 Required settings of the ETHM-1 Plus / INT-GSM / INT-GSM LTE module

You can configure the module settings using the DLOADX program: “Structure” window → “Hardware” tab → “Keypads” branch → *[module name]*.

- Enable the “GUARDX” option.
- Enter the “GUARDX key”. It is a string of up to 12 alphanumeric characters (digits, letters and special characters). Click on the icon  to view the key entered.
- Enable the “Connection via Satel server” option if connection is to be established via the SATEL server.
- Enable the „Push notifications” option if the application is to notify the user about the control panel status by means of push messages (see: “Notifications”).

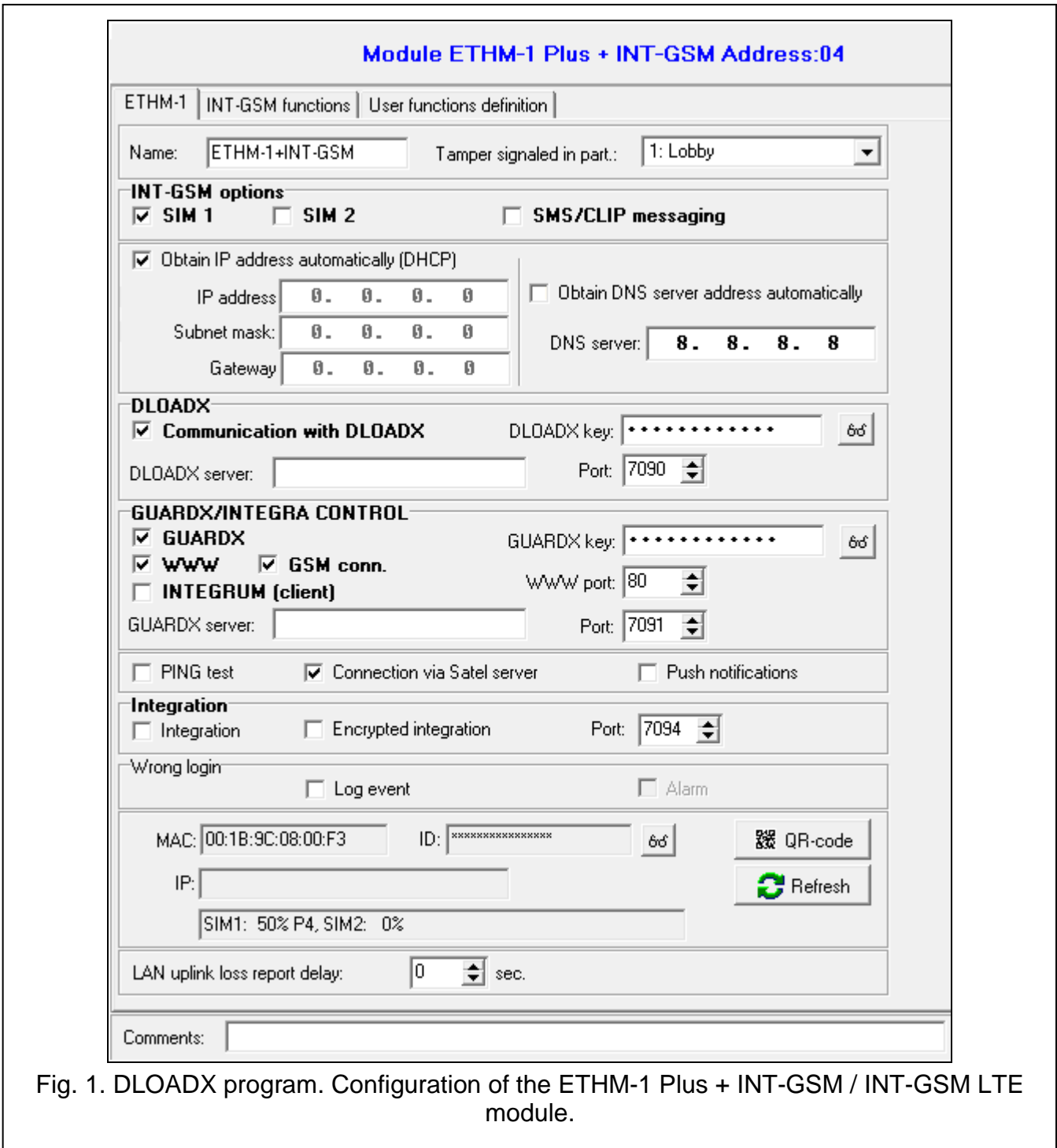


Fig. 1. DLOADX program. Configuration of the ETHM-1 Plus + INT-GSM / INT-GSM LTE module.

ETHM-1 Plus module / ETHM-1 Plus + INT-GSM / INT-GSM LTE module

- Configure the network settings of the ETHM-1 Plus module.

i *If the application is to connect to the ETHM-1 Plus module via the SATEL server, the DNS server address must be programmed in the module (the “Obtain DNS server address automatically” option must be disabled).*

- If the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module, configure the settings related to the transfer of data via cellular network.

i *The DNS server address must be programmed in the INT-GSM / INT-GSM LTE module.*

- Enable the “GSM” option.

- Set the number of the TCP port used for communication if connection is to be established directly with the module.



If the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module, data transfer via cellular network is used only when connection over Ethernet cannot be established.

INT-GSM / INT-GSM LTE module

- Configure the settings related to the transfer of data via cellular network.



The DNS server address must be programmed in the module.

- Enable the “INTEGRA CONTROL” option.

version: 2.00

INT-GSM | INT-GSM functions | User functions definition

Name: INT-GSM (3) Tamper signaled in part.: 1: Zone 1

INT-GSM options

SIM 1 SIM 2 SMS/CLIP messaging

DLOADX

Communication with DLOADX DLOADX key: [masked] [copy]

DLOADX server: 188.252.98.163 Port: 7090

GUARDX/INTEGRA CONTROL

GUARDX GUARDX key: [masked] [copy]

INTEGRA CONTROL

INTEGRUM (client)

GUARDX server: 188.252.98.163 Port: 7091

Connection via Satel server Push notifications

IMEI: 86-899603-978841-9 ID: [masked] [copy] QR-code

SIM1: 100% P4, SIM2: 0% Refresh

Fig. 2. DLOADX program. Configuration of the INT-GSM / INT-GSM LTE module.

3.1 QR code

The communication settings can be easily imported to the INTEGRA CONTROL application by using a QR code. You can generate the QR code in the DLOADX program: “Structure” window → “Hardware” tab → “Keypads” branch → [module name] (Fig. 1).



You will be able to generate the QR code only after you have enabled the “Connection via Satel server” option and the ID number has been generated by the server.

Click on . A window with the QR code will open. Underneath the QR code you will find a password required when scanning the code (press and hold to view the password).

You can save the code to a JPG file after clicking on .

Give the QR code and the password to the INTEGRA CONTROL application user.

4 Installation and first start of the application

You can download the INTEGRA CONTROL application from the “App Store”.

On first start of the application:

1. The application will request your permission to send notifications. You can either allow notifications or not (you can change the settings later).
2. A tutorial will be displayed. Tap “Skip” to proceed.
3. The “Objects” screen will open (see “Objects”).

5 Application settings

Tap  to open the application settings screen (Fig. 3):

Password protected – when this option is enabled, access to the application is password protected. You will be asked to set a password after you have enabled this option.



Instead of giving the password, you can scan your fingerprint on startup of the application, if such user authorization method is supported on your mobile device.

New password – tap to change the access password to the application. This function is available if the “Password protected” option is enabled.

Application data

Backup to file – tap to save the control panel data to file.

Restore from file – tap to download the control panel data saved to file.

Sounds – tap to configure the settings for sounds to indicate different events.

Version – information about the application version.

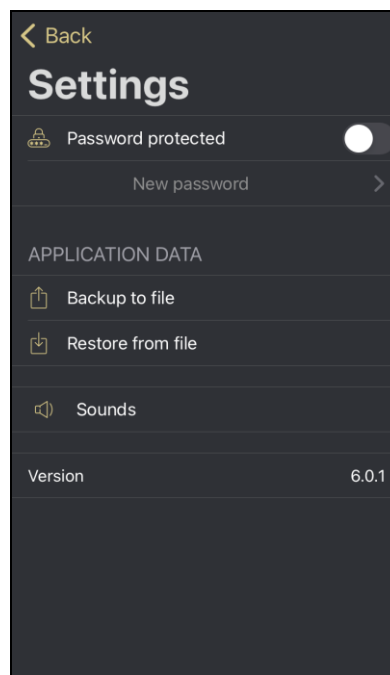


Fig. 3. INTEGRA CONTROL application. Application settings.

6 Objects

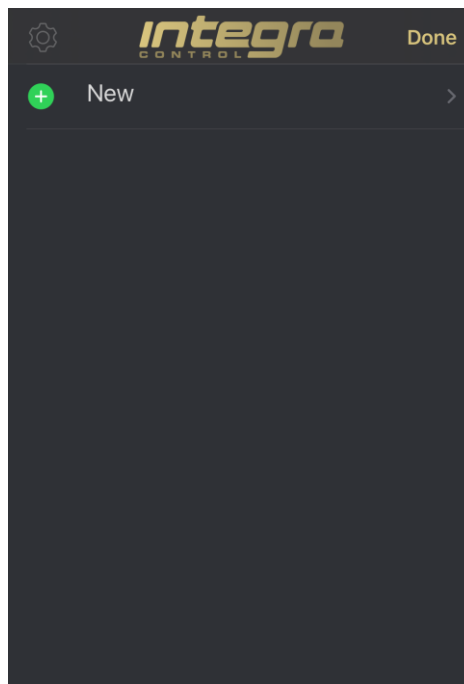







Fig. 4. INTEGRA CONTROL application. “Objects” screen before adding control panel.

After first start of the application, the screen will show the button “ New”. Tap the button to add a control panel (see: “Adding a control panel”).

The added control panels are displayed on the „Objects” screen. After swiping left the control panel’s name, the button  will appear. Tap it to display the QR code containing the settings related to communication with the control panel. Before the code is displayed, you will be asked to set a password required to scan the QR code on another mobile device. This allows you to easily import configured communications settings from one mobile device to another.

If you tap the “Edit” button:

- the following buttons will be displayed:
 - “ New” – tap to add a new control panel,
 -  – tap to delete a control panel (see: „Deleting a control panel”),
 -  – hold and drag the button up or down to change the order of the control panels on the screen,
 - “Done” – tap to exit the edit mode.
- you can tap the control panel’s name to edit its settings in the application.

6.1 Adding a control panel

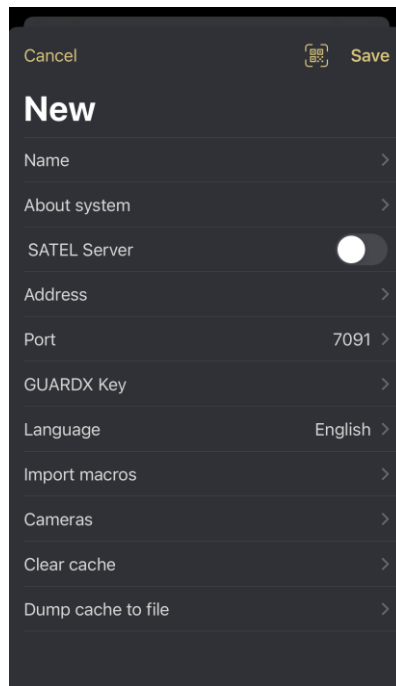


Fig. 5. INTEGRA CONTROL application. Control panel settings.

1. Configure the settings for communication with the ETHM-1 Plus / INT-GSM / INT-GSM LTE module. You can enter the settings manually (see: “Adding communication settings manually”) or import them by using a QR code (see: “Importing communication settings by using a QR code”).



The QR code contains the settings required for establishing connection with the control panel via the Satel server.

You can obtain the QR code from the installer or a user who has already entered the control panel data to the mobile application.

2. Enter the alarm system’s name. It will help you to identify the alarm system while using the application (you can define settings for multiple alarm systems).
3. Define the language of the control panel.
4. Define how the macro commands should be handled. By default, macro commands will be imported from the module (they will be downloaded during the first connection). If the macro commands are not to be, tap the screen in the “Import macros” area and change the settings (see: “Adding macro commands”). Macros settings can be changed at any time while using the application.
5. If you want to watch video footage from IP cameras in the application, enter the addresses of cameras (see: “Adding a camera”). If you do not want to use the application to watch video footage from IP cameras, skip this step. You can add new IP cameras or change the settings for cameras already added at any time while using the application.
6. Tap “Save” to save the settings.
7. A newly added control panel will appear on the list on the “Objects” screen (Fig. 6).

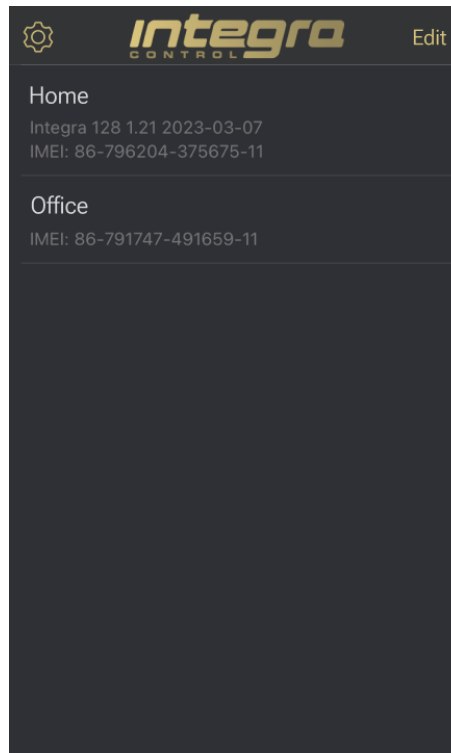


Fig. 6. INTEGRA CONTROL application. List of added control panels.

6.1.1 Adding communication settings manually

Connection to ETHM-1 Plus module

Direct communication with the module

1. Enter the network address of the module.
2. Enter the number of TCP port.
3. Enter the data encryption key – the same as in the module (“GUARDX Key”).

Communication via the SATEL server

1. Enable the “Server Satel” option.
2. Enter the module’s MAC address.
3. Enter the module’s ID number (identifier assigned to the module by the SATEL server).
4. Enter the data encryption key – the same as in the module (“GUARDX Key”).



You can check the network address, MAC address and ID number in the LCD keypad (by using the “IP/MAC/IMEI/ID” user function available in the “Tests” submenu – for a description of the function please refer to the user manual for the control panel).

Connection to INT-GSM / INT-GSM LTE module


1. Enable the “Server Satel” option.
2. Enter the IMEI number of the module cellular telephone.
3. Enter the module’s ID number (identifier assigned to the module by the SATEL server).




You can check the IMEI and ID numbers in the LCD keypad (“IP/MAC/IMEI/ID” user function available in “Tests” submenu – see user manual for control panel).

4. Enter the data encryption key – the same as in the module (“GUARDX Key”).

6.1.2 Importing communication settings by using a QR code

1. Tap .
2. Allow the application to access the camera.
3. Scan the QR code.
4. Enter the password protecting the QR code and tap “Done”.

6.2 Deleting a control panel

1. Tap “Edit”.
2. Tap  in front of the control panel name.
3. Tap “Delete”.


6.3 Adding macro commands

Macro commands enable automated operation of the alarm system and the connected devices. By default, macro commands will be imported from the module when the application is first connected to the control panel.

If you do not want the application to import macro commands, tap “Import macros” and then “No macros”.

If you want to import macro commands from the module, tap “Import macros” and then “Import from system”. The macros should be imported after each change of macro command settings in the module.

6.4 List of cameras

The  button will be available in the top right corner of the screen after the “Cameras” screen is displayed. Tap the button to add a new camera (see: “Adding a camera”).

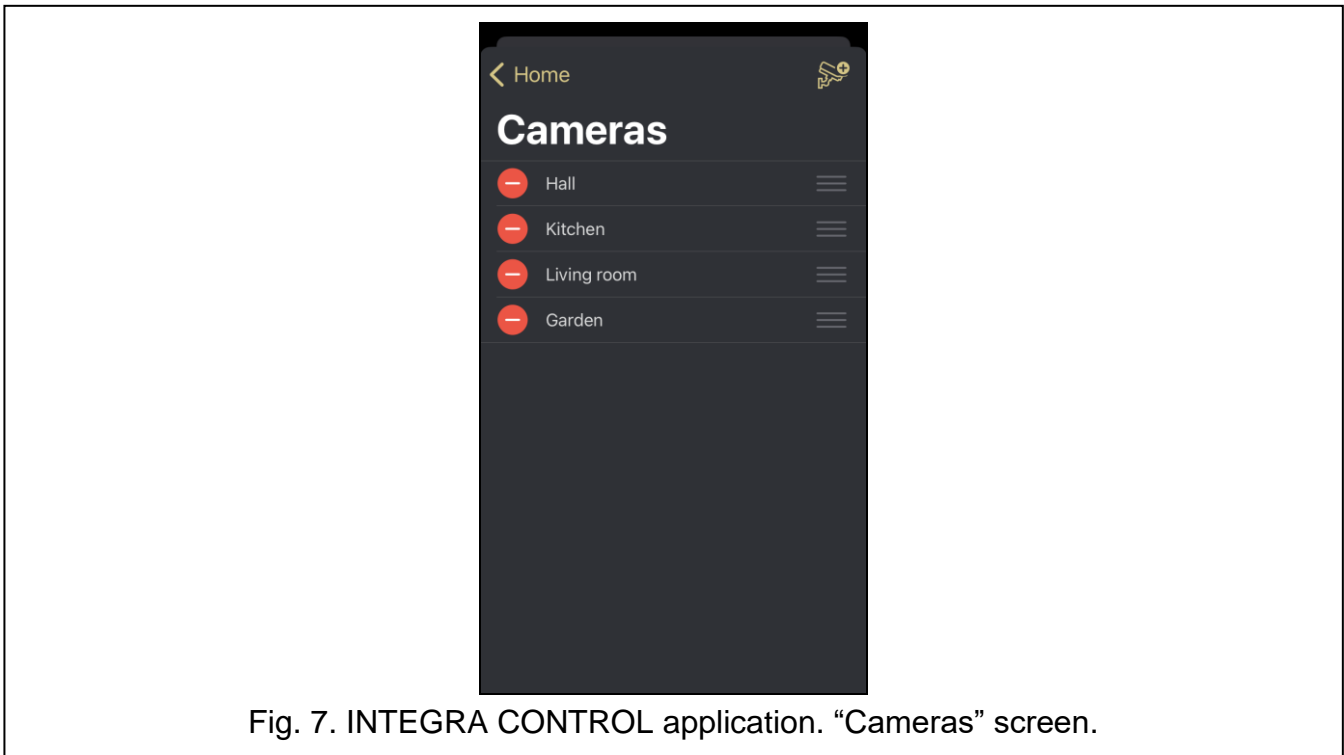



Fig. 7. INTEGRA CONTROL application. “Cameras” screen.

Cameras already added are displayed on the “Cameras” screen (Fig. 7). Tap the button  in front of the camera name to delete the camera. Tap the camera name to edit its settings. Tap “Back” to return to the settings screen for the selected control panel.

6.4.1 Adding a camera

Cameras added to the INTEGRA CONTROL application must have the following address: `rtsp://xxx.xxx.xxx.xxx:yyyy/zzzz`.

where “xxx.xxx.xxx.xxx” – IP address or domain name, “yyyy” – camera port, and “zzzz” – access path.


The following parameters are required for adding an IP camera:

- camera address (IP address or domain name),
- camera port,
- access path to image.



The INTEGRA CONTROL application supports only cameras with RTSP protocol.

Add manually

1. On the “Objects” screen, tap “Edit”.
2. Tap the control panel.
3. Tap “Cameras”. The cameras screen will be displayed.
4. Tap  and select “Add manually”. The screen for adding a camera will open (Fig. 8).
5. In the “Name” field, enter the camera name.
6. The camera protocol – rtsp – is displayed in the “Protocol” field.

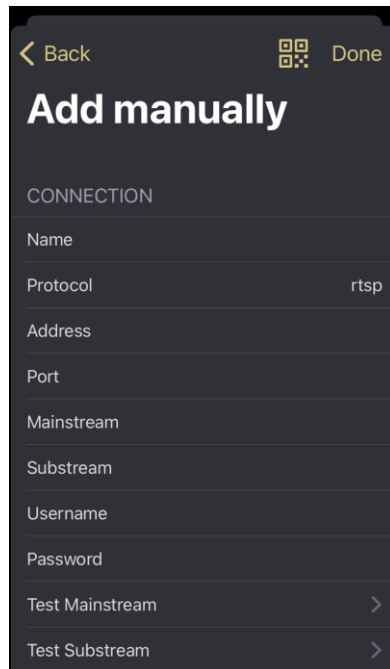


Fig. 8. INTEGRA CONTROL application. Screen for adding a camera with no settings defined.

7. In the “Host” field, enter the camera address (IP address or domain name) (xxx.xxx.xxx.xxx).

8. In the “Port” field, enter the port number used by the camera (yyyy).

i | Leave this field blank if the camera does not use a port number.

9. In the “Mainstream” field, enter the access path to high resolution video (zzzz).

10. In the “Substream” field, enter the access path used for quick preview of lower resolution video.

11. If the camera requires logging in, enter the login in the “User” field and user password in the “Password” field.

! | **It is advised to protect cameras with login and password in order to prevent unauthorized access.**

12. Tap “Test Mainstream” to check the connection to camera by using the path provided in the “Mainstream” field.

13. Tap “Test Substream” to check the connection to camera by using the path provided in the “Substream” field.

14. In the “Relations” section you can assign to the camera partitions / zones / outputs of the control panel, which you will be able to control while watching video footage from that camera.

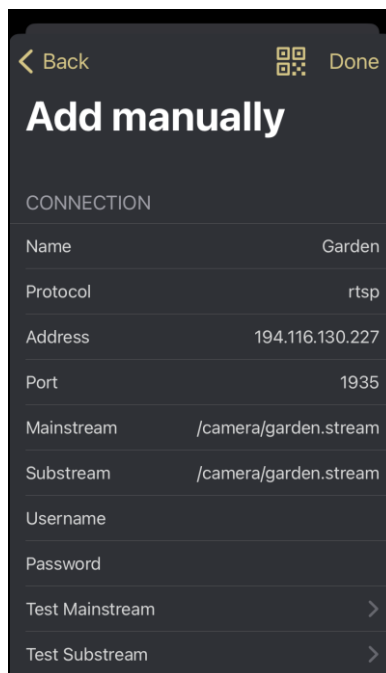


Fig. 9. Camera address entered as an IP address. The presented settings are just an example.

15. Tap “Back” to return to the list of cameras.

16. Tap “Control Panel” to return to the control panel settings screen.

17. Click “Save” to save the changes made.

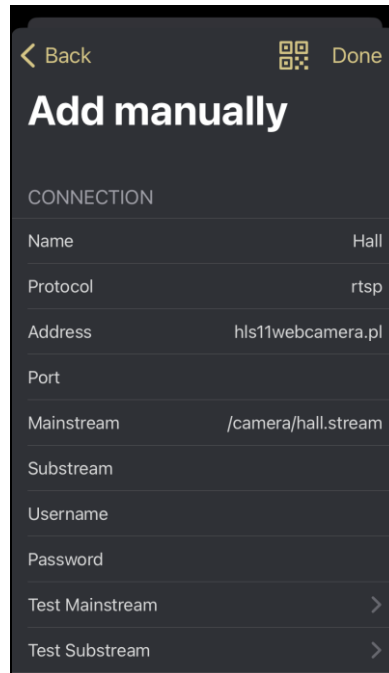




Fig. 10. Camera address entered as a domain name. The presented settings are just an example.


Search on the network

1. On the “Objects” screen, tap “Edit”.
2. Tap the control panel.
3. Tap “Cameras”. The cameras screen will be displayed.
4. Tap  and select “Search on the network”. The app will search for cameras connected to the same network as the mobile device.
5. Select a camera from the list of found cameras.
6. Enter login and password if access to the camera is protected.
7. The video streams will be displayed. The video quality of each stream may differ. Tap “OK” to add the camera.

Import

1. On the “Objects” screen, tap “Edit”.
2. Tap the control panel.
3. Tap “Cameras”. The cameras screen will be displayed.
4. Tap  and select “Import”.
5. Scan the QR code of the camera.
6. Enter password if access to the camera is protected.
7. The camera will be added.

Link

1. On the “Objects” screen, tap “Edit”.
2. Tap the control panel.
3. Tap “Cameras”. The cameras screen will be displayed.
4. Tap  and select “Link”.
5. Enter the link to the camera and tap “OK”. The camera will be added.

6.5 Control panel searching

Swipe down to display the search field. Tap the search field and enter the name or the IMEI number of the control panel you are searching for.

6.6 Establishing communication with the control panel

If the application is not connected to the control panel, tap the control system's name in order to establish connection with the control panel.

If only one alarm system is added to the application, it will connect to the control panel automatically after startup.

If the user is not remembered by the application or has been logged out, the application will ask you to enter the user code after it has established connection to the control panel. Check "Remember me" if you want the user to be automatically logged in after the application has connected to the control panel.

When communication with the control panel has been established for the first time, downloading of macros and names (of partitions, zones, outputs, expander modules, timers, phones and users) will start.



Macros and names may also be downloaded when communication with the control panel has been established after a longer break.

After communication has been established with the control panel, the screen set in the first position on the shortcut bar will be displayed (see: "Shortcut bar"). By default, it is the "Macros" screen.

7 Information about the control panel

Tap the top of the screen and swipe down to display information about the currently connected control panel:

- name,
- user logged in,
- control panel model, firmware version, release date (if new firmware version is available, a prompt to update firmware),
- model of communication module, firmware version, release date (if new firmware version is available, a prompt to update firmware).

8 Operating the alarm system

8.1 Status bar

The status bar is displayed on the top of the screen. The following icons are available:



– tap to disconnect from the control panel.



– trouble indicator. It is flashing when there is trouble condition in the alarm system (or the alarm memory condition if option "Grade 2" or "Grade 3" was enabled by the installer). Tap to go to the "Troubles" screen.



– arming indicator:

- ON – all partitions controlled from the app are armed;

- flashing – some partitions controlled from the app are armed or exit delay countdown is running.

Tap to go to the “System” screen, “Partitions” tab.



– service mode indicator. It is flashing when service mode is entered. Tap to go to the “Keypad” screen.



– alarm indicator:

- ON – alarm;
- flashing – alarm memory.

Tap to go to the “System” screen, “Alarms” tab.

8.2 Shortcut bar

On the bottom of the screen there is a shortcut bar where selected icons are displayed. The shortcut bar allows you to quickly access the selected screens in the application. You can customize the bar to your needs (see: “Customizing the shortcut bar”).

Click “More” to view the widgets (Fig. 11):

Macros – tap to go to the “Macros” screen.

System – tap to go to the “System” screen.

Control – tap to go to the “Control” screen.

Cameras – tap to go to the “Cameras” screen.

Troubles – tap to go to the “Troubles” screen.

Events – tap to go to the “Events” screen.

Timers – tap to go to the “Timers” screen.

Users – tap to go to the “Users” screen.

Keypad – tap to go to the “Keypad” screen.

Notifications – tap to go to the “Notifications” screen.

Help – tap to go to information about the application.

8.2.1 Customizing the shortcut bar

1. Tap and hold one of the widgets. The list of widgets will change its appearance (Fig. 11).
2. Hold and drag the widget to move it.




The icons of the first four widgets are displayed on the shortcut bar on the bottom of the screen.

The first widget shows which screen is displayed when the app connects with the control panel.

3. Tap “Save” to confirm the changes.



Tap  to undo all the changes made.

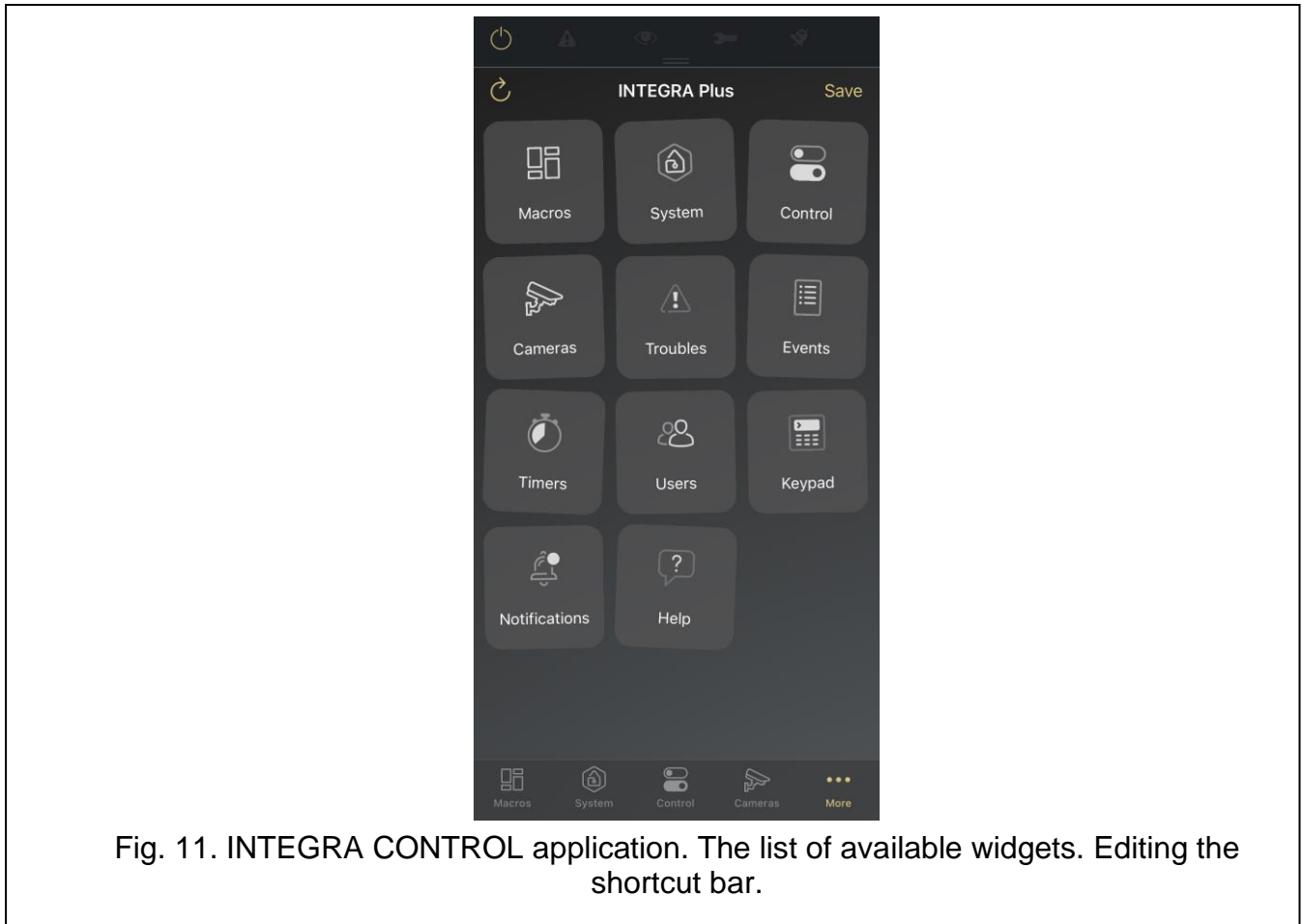


Fig. 11. INTEGRA CONTROL application. The list of available widgets. Editing the shortcut bar.

8.3 Macros

This screen allows you to operate the control panel by using macro commands. On the screen you will find macro commands imported by the application (Fig. 12).

Swipe the screen left or right to display a different group of macros.

Tap the macro to run it. The Face ID / Touch ID / password authentication may be required (depending on the iOS system version).

8.3.1 Customizing the macros layout

1. Tap and hold one of the widgets. The list of widgets will change its appearance.
2. Hold and drag the widget to move it.



The widgets cannot be moved from one group to another.

To assign a macro to a different group, use the DLOADX program.

3. Tap “Save” to confirm the changes.

8.3.2 Running macros from the “Shortcuts” app

You can use the “Shortcuts” app available in the iOS system to run macros. You can add macros to the app and group them. You can run them manually or with a voice command (using Siri).



If you want to run macros with a voice command, make sure that their names are in a language supported by Siri.

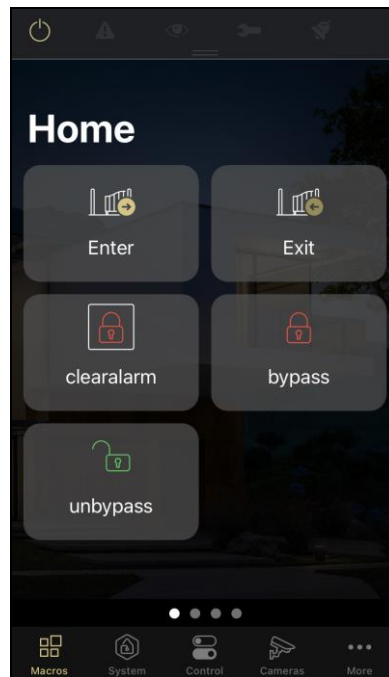


Fig. 12. INTEGRA CONTROL application. “Macros” screen.

8.4 System

Use the buttons on the top of the screen:



– tap to display the list of partitions.



– tap to display the list of zones.



– tap to display the list of zones to which ABAX 2 / ABAX devices with temperature sensors are assigned.



– tap to display the list of zones that are bypassed / violated / tampered / generated an alarm.

8.4.1 Partitions

This screen shows the list of partitions (Fig. 13). You can control them (see: “Controlling partitions”).

The icon displayed next to the partition name provides information on its current status:



– disarmed,



– exit delay countdown is running,



– armed – mode: “full”,







– armed – mode: “full + bypasses”,




– armed – mode: “without interior”,



– armed – mode: “without interior and without entry delay”,

-  – temporarily blocked,
-  – entry delay countdown is running,
-  – fire alarm,
-  – alarm. The number of alarms is displayed next to the icon.

The  icon is displayed next to the partition name. Tap it to view the list of events from the selected partition (see: “Events”).

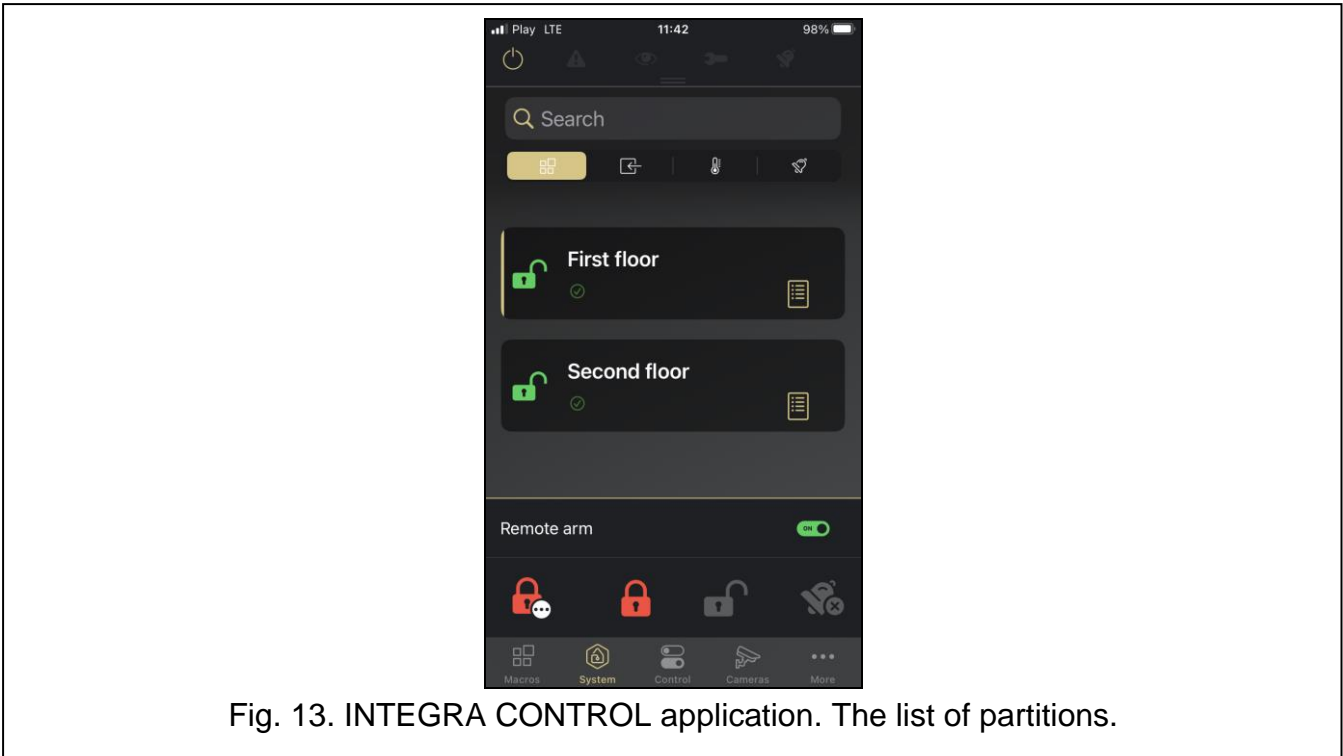




Fig. 13. INTEGRA CONTROL application. The list of partitions.

8.4.2 Controlling partitions


If you tap the partition name (you can tap several partitions to select them), the icons to control the partition and the option to remotely arm the partition will be displayed on the bottom of the screen.

Remote arming

The option allows you to arm the partition without entry delay and without bypassing the zones.

-  – remote arming is enabled. Tap to disable this option.
-  – remote arming is disabled. Tap to enable this option.

Controlling the partition

-  - tap to arm the partition / partitions. You can select one of the arming modes:
 - Full;
 - Full + bypasses;

- Stay;
- Stay, delay=0.



- tap to arm the partition / partitions.



- tap to disarm the partition / partitions.



- tap to clear alarm in the partition / partitions.

8.4.3 Zones

This screen shows the list of zones (Fig. 14). You can bypass them (see: „Bypassing zones”). The icon displayed next to the zone name provides information on its current status:



- zone inactive (not violated),



- zone violated,



- trouble: long violation,



- trouble: no violation,



- isolated,



- inhibited,



- tamper alarm,



- alarm,



- masking,



- masking memory.

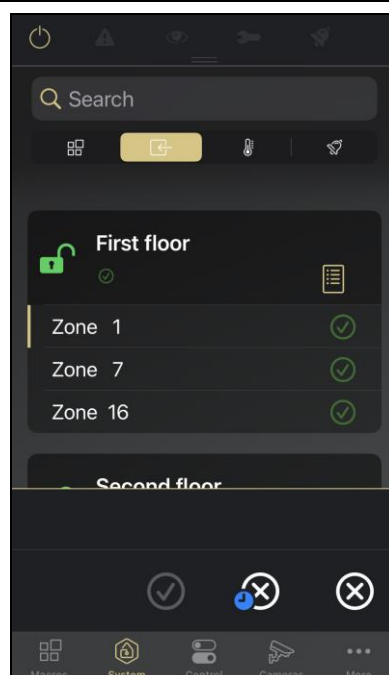


Fig. 14. INTEGRA CONTROL application. “Zones” screen.

8.4.4 Temperatures

This screen shows the list of zones to which ABAX 2 / ABAX devices with temperature sensors are assigned. Temperature information provided by the sensors is also displayed.

You can bypass the zones (see: “Bypassing zones”).

8.4.5 Bypasses / violations / tampers / alarms

This screen shows the list of zones that are bypassed / violated / tampered / generated an alarm.

You can bypass the zones (see: “Bypassing zones”).

8.4.6 Bypassing zones

Tap the zone name. The following icons will be displayed on the bottom of the screen:



- tap to unbypass zone,



- tap to inhibit zone,



- tap to isolate zone.

8.4.7 Zone searching

Swipe down to display the search field.

In the search field enter the name or number of the zone you are searching for.

8.5 Control

Use the buttons on the top of the screen:



– tap to display the list of controllable outputs.



– tap to display the list of roller shutter outputs.



– tap to display the list of thermostatic outputs.



– tap to display the list of non-controllable outputs.



– tap to display the list of all outputs.

8.5.1 Outputs

This screen shows the list of controllable outputs (Fig. 15). You can control them.

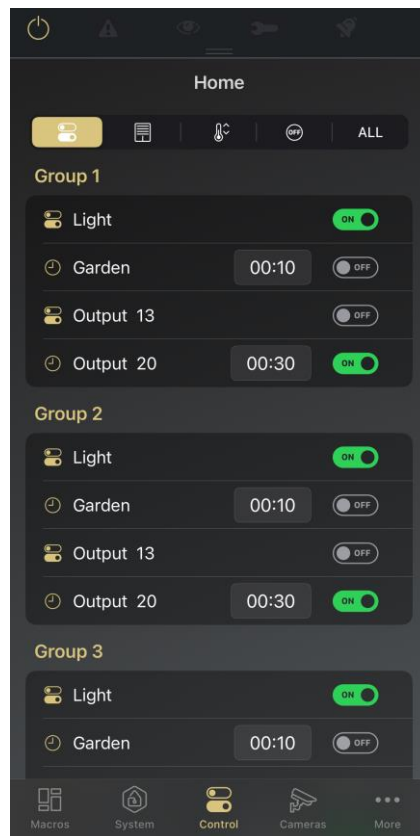


Fig. 15. INTEGRA CONTROL application. “Control” screen.

Tap the time field to set the time of output activation.

One of the following icons will be displayed next to the output name:



– controllable output turned off. Tap to turn it on.



– controllable output turned on. Tap to turn it off.



– non-controllable output turned off.



– non-controllable output turned on.



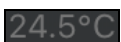
– roller shutter not moving. Tap to control it.



– roller shutter up. Tap to control it.



– roller shutter down. Tap to control it.



– thermostatic output turned off. Tap to edit its settings.



– thermostatic output turned on. Tap to edit its settings.



Temperature information is provided by wireless devices with temperature sensors.

Controlling the roller shutter

Tap the roller blind name. The following icons will be displayed on the bottom of the screen:



- tap to move the roller shutter up.



- tap to move the roller shutter down.

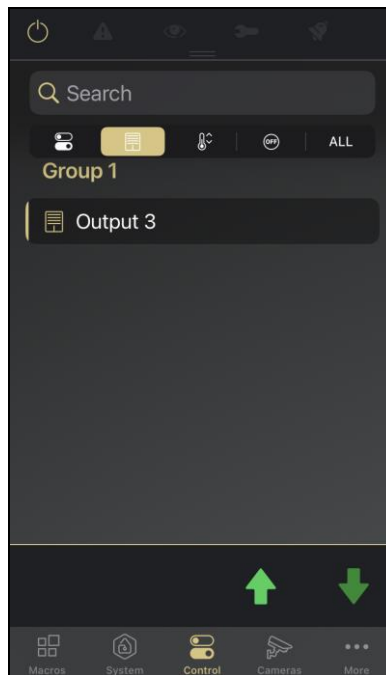


Fig. 16. INTEGRA CONTROL application. "Roller Shutters" screen.



8.5.2 Thermostatic outputs

This screen shows the list of thermostatic outputs (Fig. 17). You can edit their settings.



Fig. 17. INTEGRA CONTROL application. The list of thermostatic outputs.

Editing the thermostatic output settings

1. Tap the name of the thermostatic output whose settings you want to edit.
2. If you want to edit the first temperature threshold (economic temperature), tap the widget with the  icon. Slide your finger up or down the screen to set the temperature.
3. If you want to edit the second temperature threshold (comfortable temperature), tap the widget with the  icon. Slide your finger up or down the screen to set the temperature.

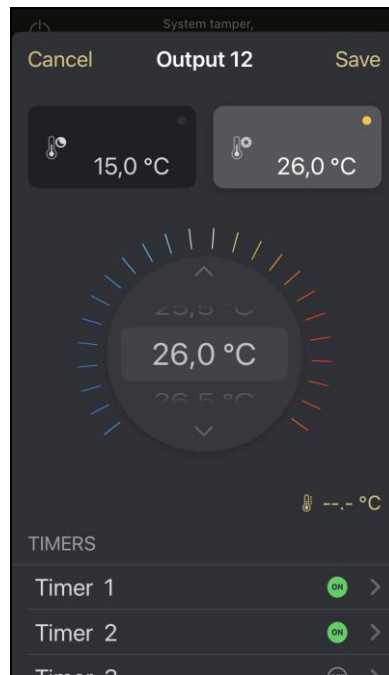


Fig. 18. INTEGRA CONTROL application. Editing the thermostatic output settings.

4. If the forcing output is available and it is controllable, you can turn it on to force the first temperature threshold (economic temperature).
5. If you want to change the settings of the timer controlling the temperature thresholds, tap the timer name – see: “Timers” (when the timer is turned on, the second temperature threshold is active).
6. Tap “Save” to save changes.



The yellow dot on the widget means that the temperature threshold is active.

The first temperature threshold (economic temperature) is active when all control timers are turned off or the forcing output is turned on. If the first temperature threshold is active, the output will be turned on when the temperature drops below the economic temperature.

The second temperature threshold (comfortable temperature) is active when the control timer is on and the forcing output is turned off. If the second temperature threshold is active, the output will be turned on when the temperature drops below the comfortable temperature.

If the output forcing the T1 temperature is turned on, the first temperature threshold is active (economic temperature) regardless of the timers.

The temperature displayed in the bottom right corner of the screen is the temperature currently registered by the sensor.

The thermostatic output settings are used to adjust the operating parameters of the ART-200 wireless radiator thermostats.

8.5.3 Output searching



Swipe down to display the search field.

In the search field enter the name or number of the output you are searching for.

8.6 Timers

The timers enable some functions to be automatically executed by the control panel (arming/disarming, turning on/off devices connected to outputs, etc.). The timer compares the time to that of the control panel clock and executes the selected function at the programmed time.

8.6.1 Editing system timers

1. Tap the timer name in the “Timers” section.
2. Select a day of the week / every day / exception. The screen with timer settings will open.
3. Set the timer start/end time. To set the time, slide the  and/or  button around the clock or tap the time field. You can set:
 - **ON/OFF** – start/end time;
 - **ON** – only start time;
 - **OFF** – only end time.
4. Tap “Save” to save changes.





Tap  to delete the settings of the edited timer.

Tap “Cancel” to finish editing. You can save the changes made or reject them.

5. Tap “Timers” to finish editing.

8.6.2 Editing partition timers

1. Tap the timer name in the “Partition timers” section.
2. Select a day of the week / every day. The screen with timer settings will open.
3. Set the timer start/end time. To set the time, slide the  and/or  button around the clock or tap the time field. You can set:
 - **ON/OFF** – start/end time;
 - **ON** – only start time;
 - **OFF** – only end time.
4. Select the partition arming type:



– Full;



– Full + bypasses;



– Stay;



– Stay, delay=0

5. Tap “Save” to save changes.



Tap  to delete the settings of the edited timer.

Tap “Cancel” to finish editing. You can save the changes made or reject them.

6. Tap the “Active” option to enable the timer.

7. Tap “Timers” to finish editing.

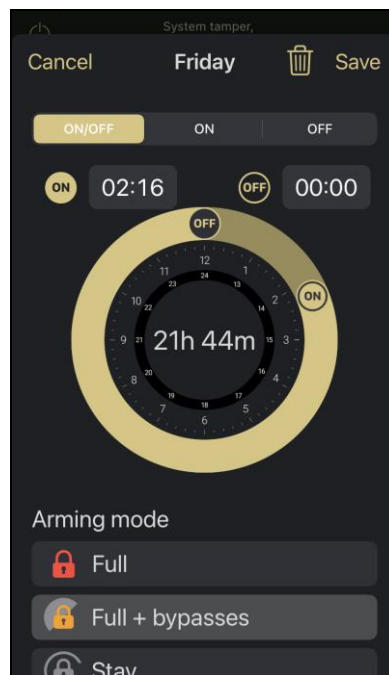


Fig. 19. INTEGRA CONTROL application. Editing the timer settings.

8.7 Users

This screen allows you to add, edit and delete the control panel users.



If you used the service code to log in, you can manage the administrators and users of all partitions.

Me

The name and type of the user currently logged in.

Tap the user name, then “Change code”, to change your code.

[Partition name]

The list of control panel users. The user type is displayed below the user name. Tap the user name to display and edit the user settings (see: “Editing a user” p. 26).

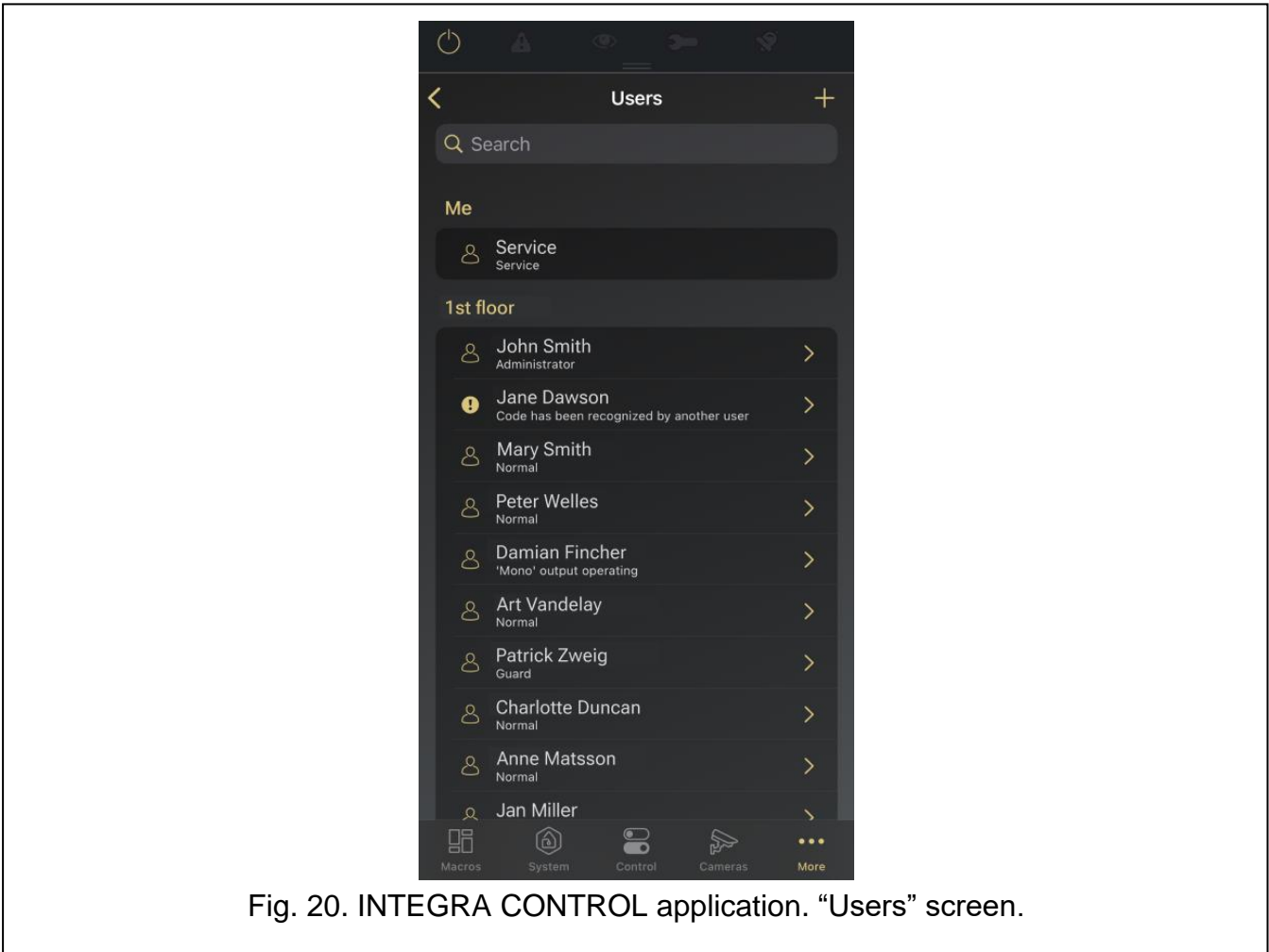



Fig. 20. INTEGRA CONTROL application. “Users” screen.

8.7.1 User searching

Swipe down to display the search field.

Tap the search field and enter the name or type of the user you are searching for.

8.7.2 Adding a user

1. Tap  in the top right corner of the screen.
2. Set the following: user name, user type, user code, access to partitions, authority level (see: “Editing a user”).
3. Tap “Save” to add a new user.

8.7.3 Editing a user

Tap the user name to edit the user settings.

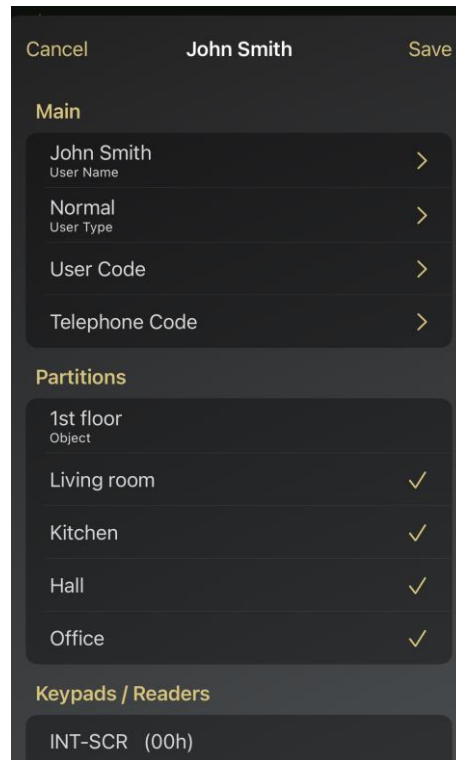


Fig. 21. INTEGRA CONTROL application. Editing a user screen.

Main

User Name – individual name of the user. Tap the field to change the name.

User Type – currently selected user type. Tap the field to change the type. The description below mentions only the codes but it applies to all identifiers assigned to the user.

- **Normal** – basic type of user.
- **One-time** – the user will get one-time access.
- **Renewable** – the user has access to the system for a defined period of time. The user validity time should be defined. Before the validity time expires, the control panel will prompt the user to change the code. After the code has been changed, the validity time will run from the beginning.
- **Temporary** – the user has access to the system for a defined period of time. The user validity time should be defined. After the validity time expires, the user will have no access to the system.
- **Duress** – code to be used in hold-up and duress situations. Use it to trigger a silent alarm and send the event code to the monitoring station.
- **'Mono' output operating** – code for control of the “MONO switch” type outputs.
- **'Bi' output operating** – code for control of the “BI switch” type outputs.
- **Blocking partition** – the code enables access to the armed partitions. Using the code will block the armed partition(s) (the partition zones will not trigger the burglary alarm). The blocking time is defined individually for each user within the range from 1 to 109 minutes. If, however, the time of blocking for guard round is defined for the partition and its duration is longer, the blocking will last longer.
- **Cash machine zone bypassing** – the code to be used to unblock access to the cash dispenser (the “24H Cash machine” type zones will be temporarily bypassed in the partition).

- **Guard** – using this code means having made the round (additionally, it can result in the partition being temporarily bypassed for the duration of guard round). The installer defines the modules which are used to confirm making the round and determines the time interval between successive rounds. If such a user is granted access to the partition, he/she will have the same capabilities as the “Normal” type user.
- **Scheduled** – the user has access to the system as per the time schedule for a specified period of time. It is necessary to select the schedule (the schedule is programmed by the installer) and define the user validity period.

Schedule number – number of the user schedule for the “Scheduled” user type. Tap to change it.

Time – depending on the type of user:

- “Renewable” / “Temporary” / “Scheduled” – validity time (number of days),
- “Blocking partition” – blocking time (number of minutes).

Tap to edit.

User Code – a string of 4 to 8 digits used for user authentication. Tap to edit.

Telephone Code – 4 digits used for user authentication when using the functions of telephone call answering and telephone control. Tap to edit.

Partitions

Object – name of the object to which the user belongs.

[Partition name] – partition that belongs to the object. Tap to grant the user access to the partition or revoke it:

empty field – the user has no access to the partition,



– the user has access to the partition.

Keypads / Readers

[Keypad/reader name] – partition keypads, code locks, proximity card reader expansion modules and DALLAS expansion modules in the system. Tap to grant the user access to the device or revoke it:

empty field – the user has no access to the device,



– the user has access to the device.

Authority Level



You cannot grant a user rights that you do not have.

[right name] – right that the user can be granted. Tap to grant the user the right or revoke it:



– the right granted to the user.



– the right not granted to the user.

Description of rights

Arming – the user can arm the system.

Disarming – the user can disarm the system.

Disarm, when other user arm – the user can disarm the system, if other user has armed it (without this right, users can only disarm the system when they have armed it themselves).

Partition alarm clearing – the user can clear alarms in partitions to which the user has access.

Object alarm clearing – the user can clear alarms in the object to which the user belongs.

Other objects alarm clearing – the user can clear alarms in other objects.

Tel. messaging canceling – the user can cancel telephone messaging.

Auto-arming deferment – the user can defer arming by the timer.

First code for two codes part. – the user can enter the first code, if 2 codes are needed to arm / disarm.

Second code for two codes part. – the user can enter the second code, if 2 codes are needed to arm / disarm.

Access temporary blocked part. – the user can disarm temporary blocked partitions (WITH TEMPORARY BLOCKING type partition).

Change access code – the user can change own access code.

Users editing – the user can add, edit and delete users.

Zones bypassing – the user can inhibit the zones.

Zone isolation – the user can isolate the zones.

Clock setting – the user can program the control panel clock.

Trouble state checking – the user can view the current troubles.

Event log reviewing – the user can view the event log.

Detectors resetting – the user can reset the 43. RESETABLE POWER SUPPLY type outputs (the user has access to RESET ZONES user function).

Options programming – the user has access to the user functions in the CHANGE OPTIONS submenu.

Access to menu TEST – the user has access to the user functions in the TESTS submenu.

Downloading starting – the user can initiate remote programming of the control panel from the keypad.

Access to BI & MONO outputs – the user can control the outputs.

System state review in GUARDX – the user can use the GUARDX program to operate the system.

Resetting outputs – the user can clear latched outputs (the user has access to CLR.LATCH.OUTS user function).

Simple user – after entering the code and pressing the # key, the user does not select the partitions to be armed / disarmed. All partitions the user has access to will be armed / disarmed.

Administrator – the user has access to the menu functions reserved for the administrator.

8.7.4 Deleting a user

1. Tap the name of the selected user.
2. Swipe the screen down.
3. Tap the “Delete User” button.
4. In the popup window tap “Delete User” to confirm.

8.8 Cameras

This screen shows video footage from cameras (Fig. 22).

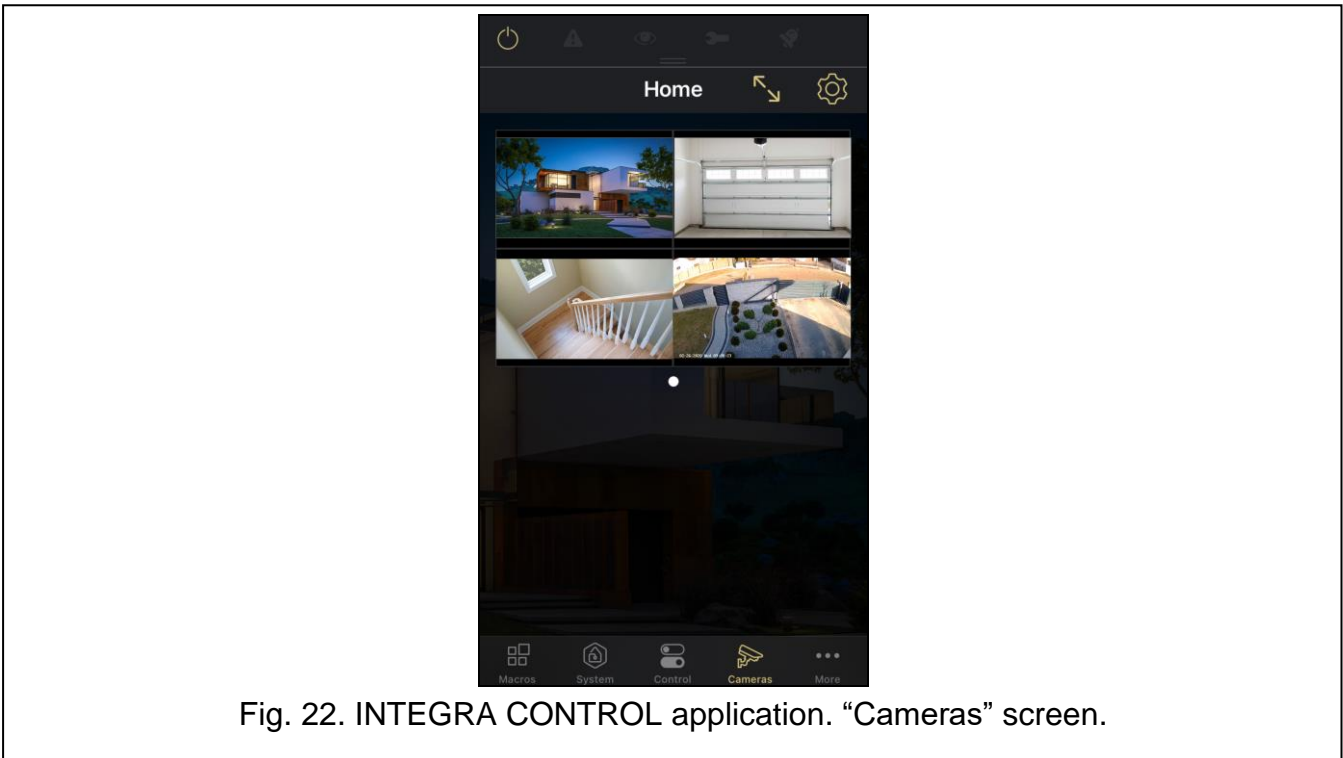




Fig. 22. INTEGRA CONTROL application. “Cameras” screen.



Tap  to display the video footage from camera(s) in full screen mode.

Tap  to change the number of videos displayed simultaneously on the screen.

Tap one of the videos. A new screen will open with video footage from the selected camera. You can activate macro commands assigned to that camera.


8.8.1 Video footage from camera


On the video screen you can control the macro commands assigned to the camera during its configuration (see: “Adding a camera”) (Fig. 23).

Tap  to change the video orientation to landscape. Tap  to return to portrait orientation.

Tap one of the videos. A new screen will open with video footage from the selected camera. You can activate macro commands assigned to that camera.


By default, the cameras display footage from the path provided in the “Substream” field.


 – the camera displays footage from the path provided in the “Substream” field – tap to display footage from the “Mainstream” path.

 – the camera displays footage from the path provided in the “Mainstream” field – tap to display footage from the “Substream” path.

Tap the video to exit and return to the “Cameras” screen.

If the camera can play audio, the icon to control the audio will be displayed on the video.

 – the camera displays video with no audio – tap to display video with audio.

 – the camera displays video with audio – tap to display video with no audio.

Swipe the screen left or right to switch between the videos from cameras.

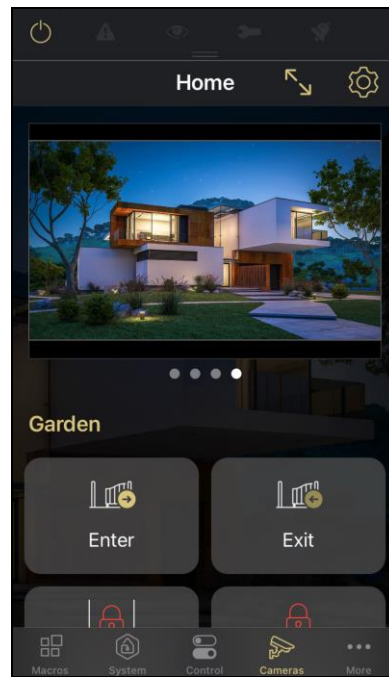



Fig. 23. INTEGRA CONTROL application. Video footage from camera.

8.9 Troubles

This screen contains a list of troubles and/or trouble memory.

When trouble memory is displayed, the  icon will be available on the bottom of the screen. Tap it to clear trouble memory (Fig. 24).

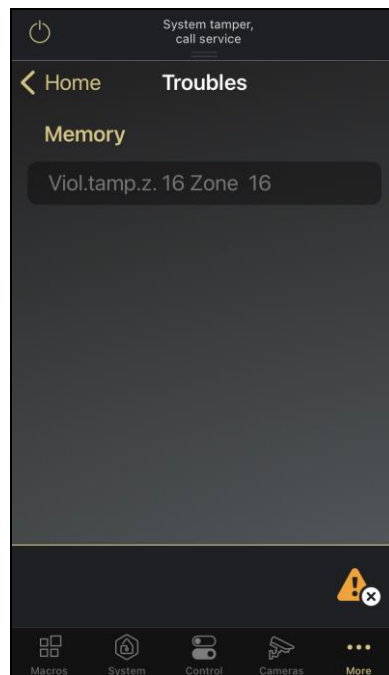













Fig. 24. INTEGRA CONTROL application. "Troubles" screen.


8.10 Events

This screen contains the control panel event log (Fig. 25). Swipe down to refresh the events.

 *The events are displayed only after the INTEGRA CONTROL application has been connected to the control panel.*

The icons displayed next to each description inform about event types:

-  – alarm from zones,
-  – other alarm,
-  – violation,
-  – restoration,
-  – arming/disarming,
-  – bypass,
-  – access control,
-  – trouble/restart,
-  – user function,
-  – system event.

You can save the event log to file. In order to do so, tap  and then choose how you want the file to be saved.

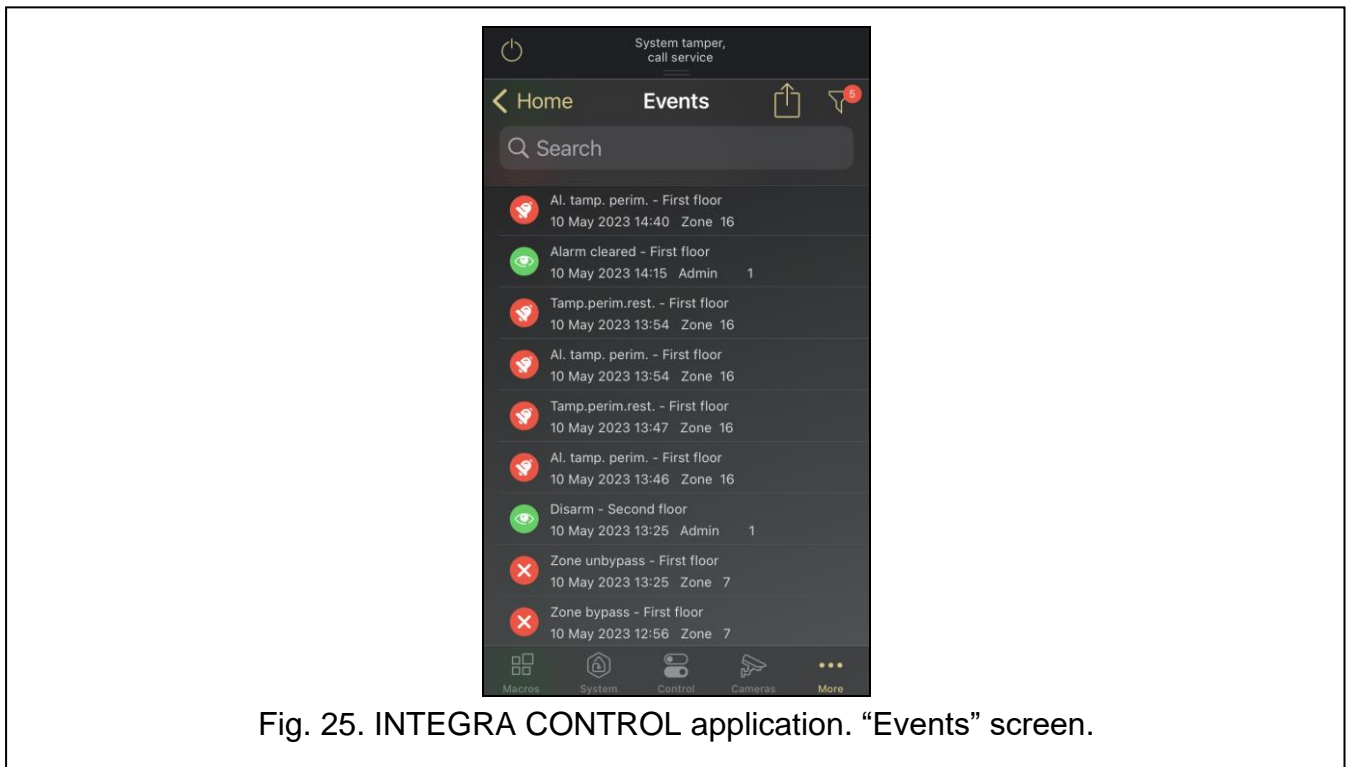



Fig. 25. INTEGRA CONTROL application. “Events” screen.

8.10.1 Filtering events

Use filtering to display on the “Events” screen only those events that meet specific criteria.

Tap  to open the events filtering screen (Fig. 26).

It allows you to filter events by:

- event types,
- partitions.

Filtering by event type

1. Tap the “Types” icon on the bottom of the screen.
2. A list of event types will be displayed.
3. Tap the event types you want to view.
4. Tap “Done” to complete the filtering. Those events that meet the selected criteria will be displayed.

Filtering by partitions

1. Tap the “Partitions” icon on the bottom of the screen.
2. A list of partitions will be displayed.
3. Tap the partitions from which you want to view events.
4. Tap “Done” to complete the filtering.

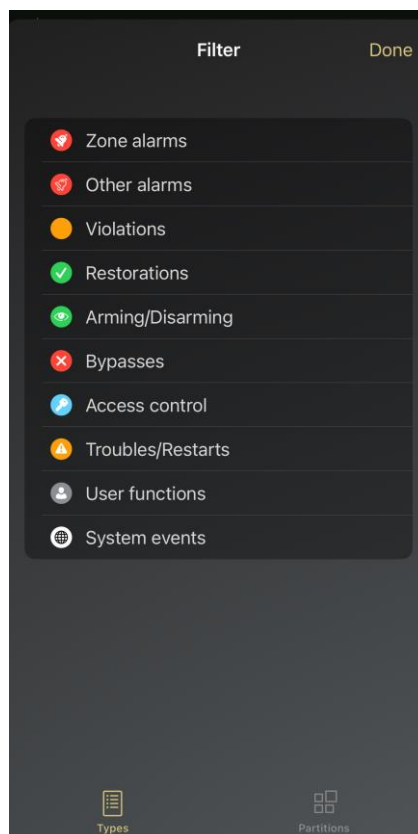


Fig. 26. INTEGRA CONTROL application. “Events” screen. Event filtering by event type.

8.10.2 Event searching

Swipe down to display the search field.

In the search field enter the name of the event you are searching for.

8.11 Keypad

The virtual keypad enables you to operate and program the alarm system in the same way as with a physical keypad.

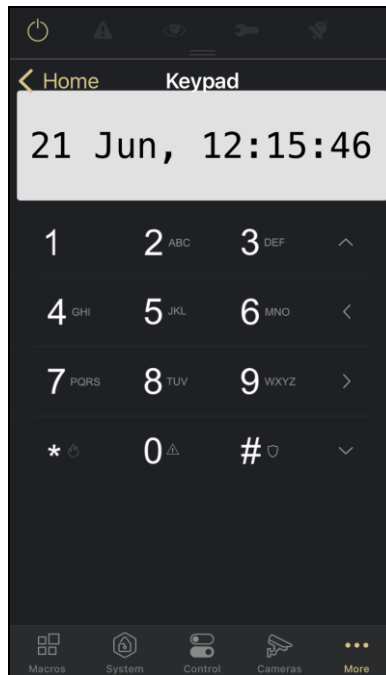


Fig. 27. INTEGRA CONTROL application. Virtual keypad.

8.12 Notifications

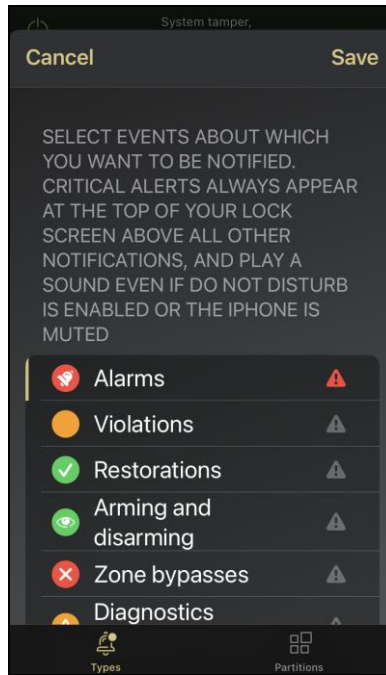


Fig. 28. INTEGRA CONTROL application. "Notifications" screen. Configuration of push notifications settings.

This screen allows you to configure the push notifications settings.

1. Tap “Add notifications”. The list of event types will be displayed.
2. Tap the event types that you want to be notified about (they will be highlighted in yellow on the left) (Fig. 28).
3. The icon on the right indicates:



– event does not generate a critical alert – tap if you want to change it.



– event generates a critical alert – tap if you want to change it.



Critical alerts always appear on your lock screen above all other notifications. The critical alert tone still plays when “Do Not Disturb” or silent mode is turned on in the device.

4. Go to the “Partitions” screen.
5. Select the partitions from which you wish to receive event notifications.
6. Tap “Save” to confirm the settings.

Push notifications will be displayed even when the application is turned off.

8.13 Help

The „Help” screen shows the icons used for notifications with explanation.

Tap „What’s new in the app” to see what has changed in the app.

9 Disconnecting from the control panel and logging out

In order to log out the current user of the control panel, tap and drag down the bar located on the top of the screen, and then tap “Logout”. You will be required to enter the control panel user password in order to connect to the control panel again.

10 Manual update history

Manual version	Introduced changes
05/23	<ul style="list-style-type: none"> • Some icons and screens from the app have been changed. • Section “Features” has been updated (p. 3). • Section “Application settings” has been updated (p. 6). • Section “Objects” has been updated (p. 7). • Section “Adding a control panel” has been updated (s. 8). • Section “Adding macro commands” has been updated (p. 10). • Section “List of cameras” has been updated (p. 10). • Description of the “Add manually” camera adding option has been updated (p. 11). • Description of the “Search on the network” camera adding option has been added (p. 13). • Description of the “Import” camera adding option has been added (p. 13). • Description of the “Link” camera adding option has been added (p. 13). • Section “Establishing communication with the control panel” has been updated (p. 14). • Section “Information about the control panel” has been updated (p. 14). • Section “Status bar” has been updated (p. 14). • Section “Shortcut bar” has been updated (p. 15). • Section “Customizing the shortcut bar” has been updated (p. 15).

	<ul style="list-style-type: none">• Section “Macros” has been updated (p. 16).• Section “Running macros from the “Shortcuts” app” has been added (p. 16).• Section “Partitions” has been updated (p. 17).• Section “Zones” has been updated (p. 19).• Section “Zone searching” has been updated (p. 20).• Section “Outputs” has been updated (p. 20).• Section “Thermostatic outputs” has been updated (p. 22).• Section “Editing the thermostatic output settings” has been added (p. 23).• Section “Output searching” has been added (p. 24).• Section “Timers” has been added (p. 24).• Section “Editing system timers” has been added (p. 24).• Section “Editing partition timers” has been added (p. 24).• Section “Cameras” has been updated (p. 29).• Section “Video footage from camera” has been updated (p. 30).• Section “Troubles” has been updated (p. 31).• Section “Notifications” has been updated (p. 34).• Section “Help” has been added (p. 35).
02/24	<ul style="list-style-type: none">• Section “Features” has been updated (p. 3).• Section “Control panel searching” has been added (p. 14).• Section “Shortcut bar” has been updated (p. 15).• Section “Customizing the shortcut bar” has been updated (p. 15).• Section “Customizing the macros layout” has been added (p. 16).• Section “Outputs” has been updated (p. 20).• Section “Users” has been added (p. 25).• Section “Video footage from camera” has been updated (p. 30).• Section “Events” has been updated (p. 32).• Section “Event searching” has been added (p. 33).