

# Adding and operating Satel devices in Partizan mobile application

## Manual



BE DIFFERENT  
            
LEAD WITH IT

[WWW.PARTIZAN.GLOBAL](http://WWW.PARTIZAN.GLOBAL)

2021

1. Getting started .....	3
2. Presetting .....	5
2.1. Satel Devices working in Partizan mobile application conditions .....	5
2.2. Adding Partizan device to a cloud account .....	6
2.3. Checking of Partizan device settings .....	7
2.4. Ethernet-module of Satel device .....	11
3. Adding Satel device to Partizan mobile application .....	13
3.1. Connection Settings .....	13
3.1.1. IP-address .....	15
3.1.2. Port .....	15
3.1.3. Device name .....	16
3.1.4. Code page .....	17
3.1.5. User code .....	18
3.1.6. Connection completion .....	19
4. Satel device and its Groups control in Partizan mobile application .....	22
4.1. Arming and disarming the device .....	22
4.2. Security groups and modes .....	26
4.3. Partial arming .....	30
4.4. The event log .....	33
4.5. Zones and their exclusion .....	34
4.6. Outputs .....	37

## 1. Getting started

Satel integrated devices are supported by **Partizan Cloud Storage** service and **Partizan** mobile application for Android.

### Partizan Cloud Storage advantages:



Your data cannot be stolen or damaged.



No one can access your devices, as well as live and archived video without your permission.



Access to your account and devices is possible from anywhere in the world. You only need Mobile Internet access.



Partizan app won the international award as "**Best Mobile Video Surveillance App 2019**".

To take full advantage of joint use of Partizan and Satel devices, install **Partizan mobile application** for Android:

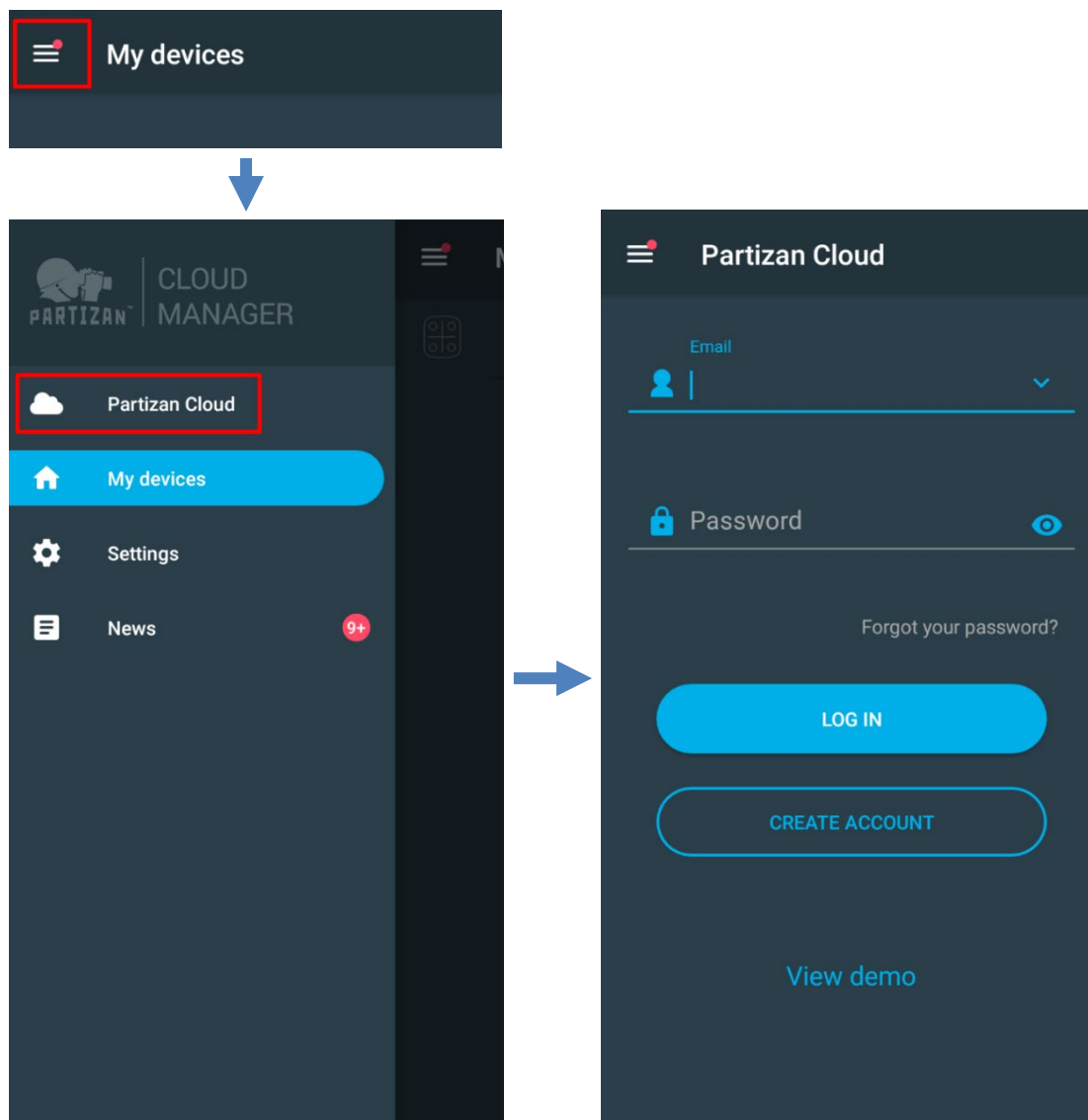


Partizan mobile application for Android:

<https://play.google.com/store/apps/details?id=com.partizan.pro>

To work with Satel Devices in Partizan mobile application, you need to **log into your cloud account**.

Open the app, use an **existing account** or **create a new one**:



After logging into the cloud account, you can proceed directly to setting up devices for joint work.

**If you have any questions, please contact our technical support:**

E-mail: [support@partizan.global](mailto:support@partizan.global)  
Skype: partizan-support  
Messengers: +420 777 054 888  
(Viber, Telegram, WhatsApp)



Technical support working time:  
<https://partizan.global/support/technical-support>



Partizan software:  
<https://apps.partizan.global/>

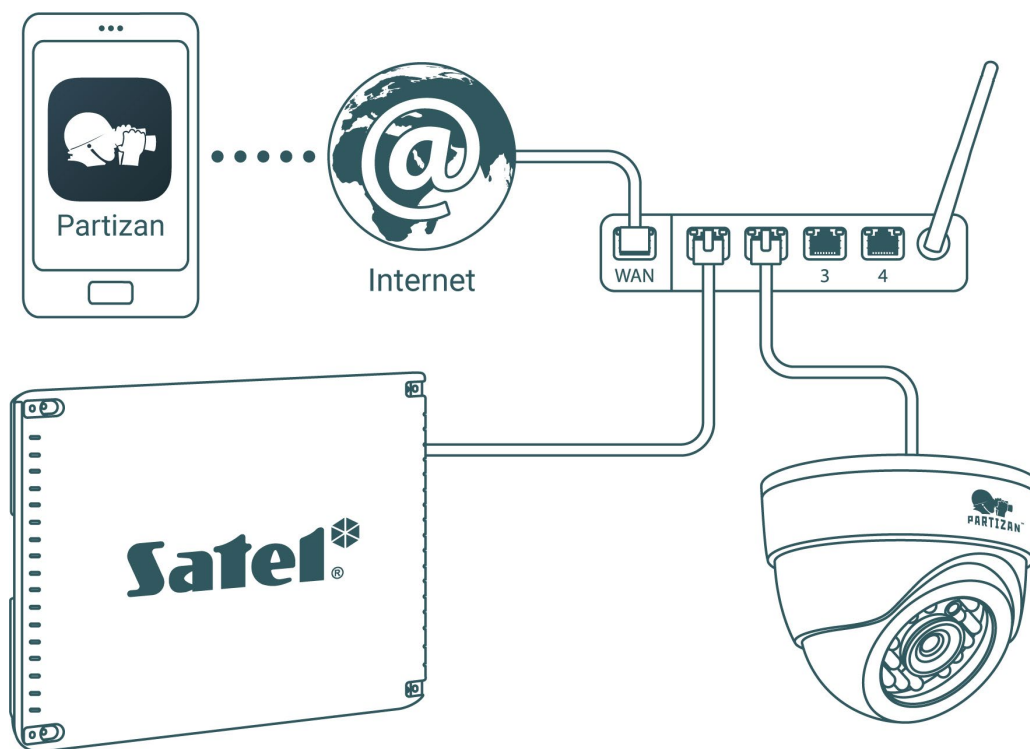
## 2. Presetting

### 2.1. Satel Devices working in Partizan mobile application conditions

To work with Satel Device you need:

- Installed mobile application **Partizan for Android** and registered cloud account (see paragraph “1. Getting Started” to read more about application and registration of a cloud account,).
- Partizan device (CCTV camera or video recorder) with cloud protocol version 3 or higher, which must be added to the cloud account in the Partizan Cloud service.
- Satel device with network (Ethernet) module ETHM.
- Partizan and Satel devices must be in the same local network.

Connection diagram:



## 2.2. Adding Partizan device to a cloud account

Instructions for adding Partizan devices to your cloud account are available on the official YouTube channel:

- Adding by scanning QR code: <https://youtu.be/uPpmANCncjY>



- Adding using search in the network: <https://youtu.be/empFWDv0Smw>

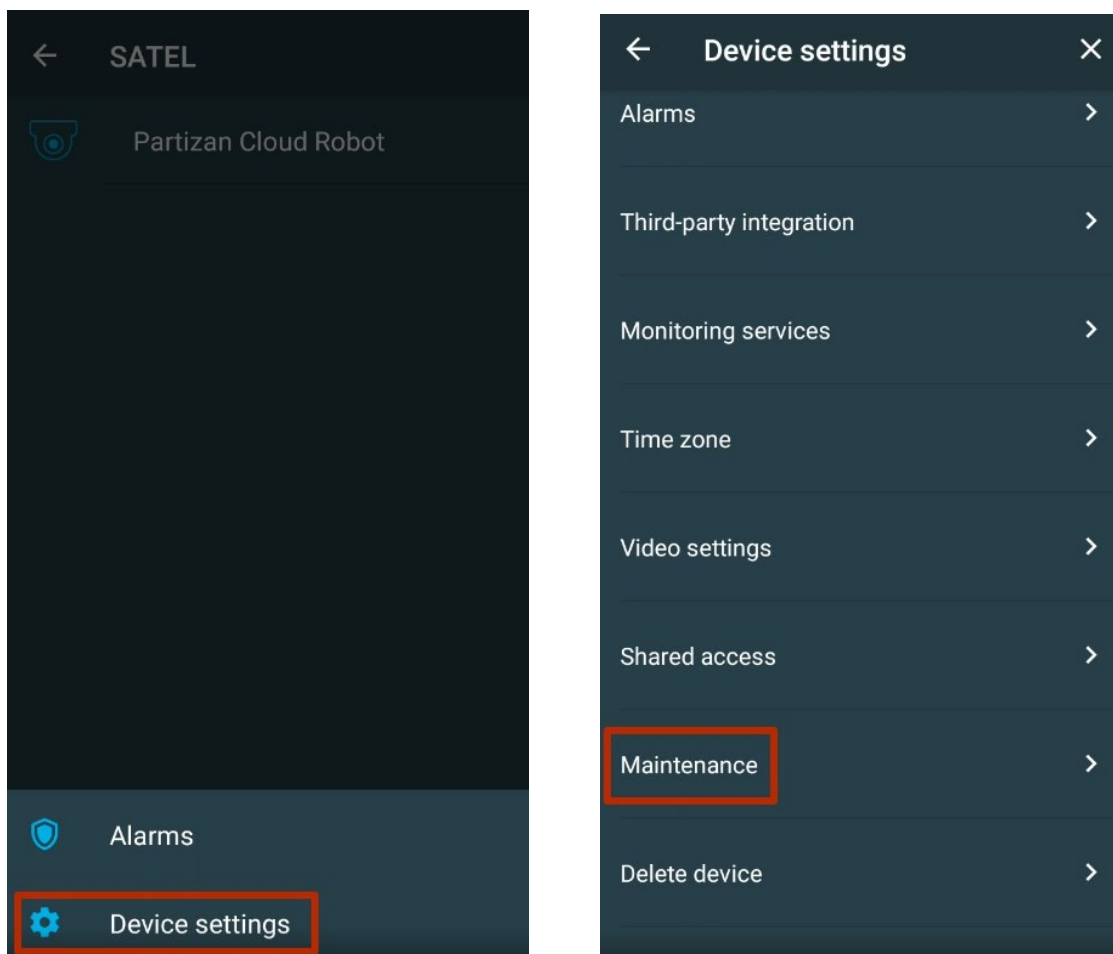


- Adding devices that support WIRELESS CONNECT technology:  
<https://youtu.be/mBXa5OJARfw>



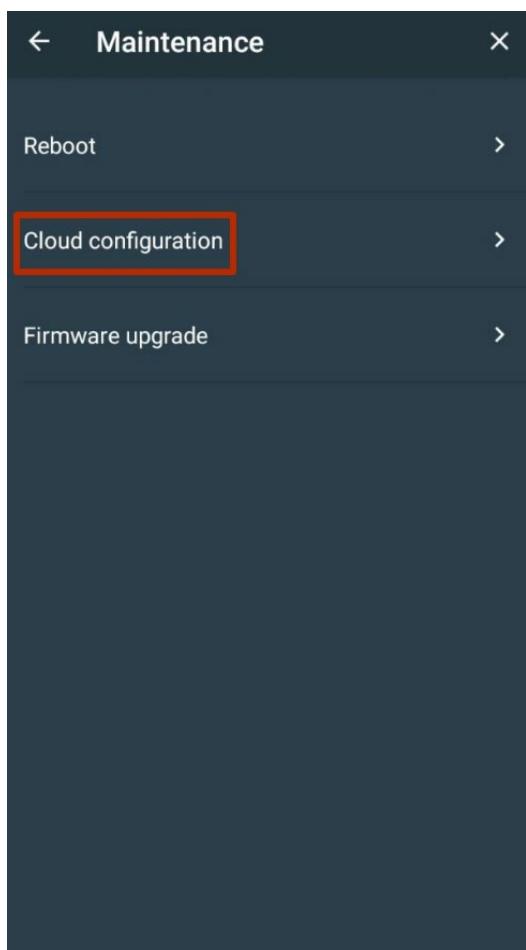
### 2.3. Checking of Partizan device settings

To check the settings of Partizan device in the mobile application, you need to make a long press on the name of the added device and press **Device Settings** in the menu that opens, then press the **Maintenance** tab:



Click **Cloud Configuration**. The screen that opens will show all the necessary information:

- MAC address of the device
- Device firmware version
- Cloud protocol version
- Cloud driver version



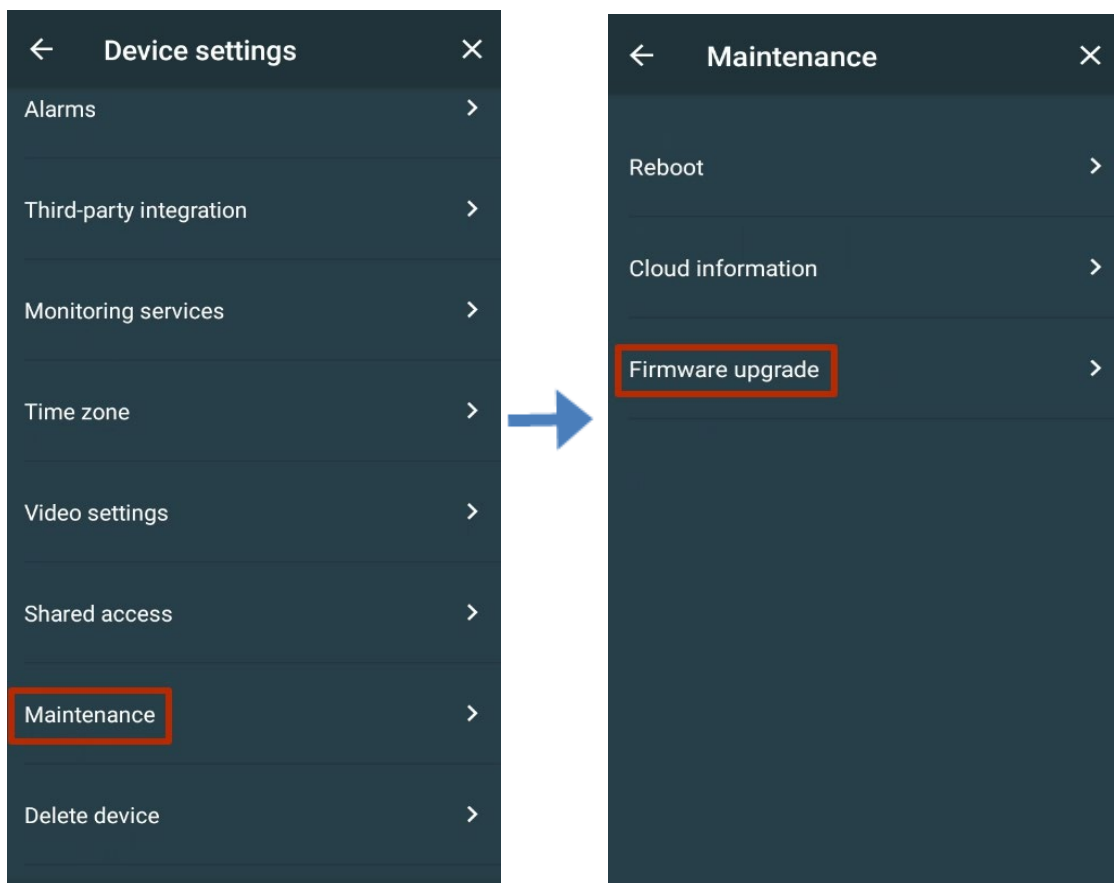
**ATTENTION!**

**Cloud protocol version must be 3 or higher.**

**If the cloud protocol version of the added device is lower, you need to update the device firmware.**

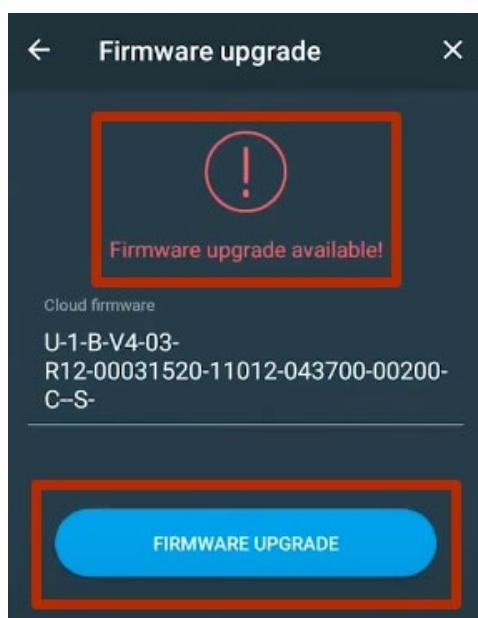


To update the device firmware, return to the **Maintenance** menu and click **Firmware upgrade**:



A notification about outdated firmware is shown on the screen.

To update the firmware, press the **FIRMWARE UPGRADE** button and follow the instructions on the screen:



**ATTENTION!**

**We strongly recommend that you always use the latest firmware version of your device.**

Instructions for updating the device firmware are available on the official YouTube channel: <https://youtu.be/nTztXd45bb8>



## 2.4. Ethernet-module of Satel device

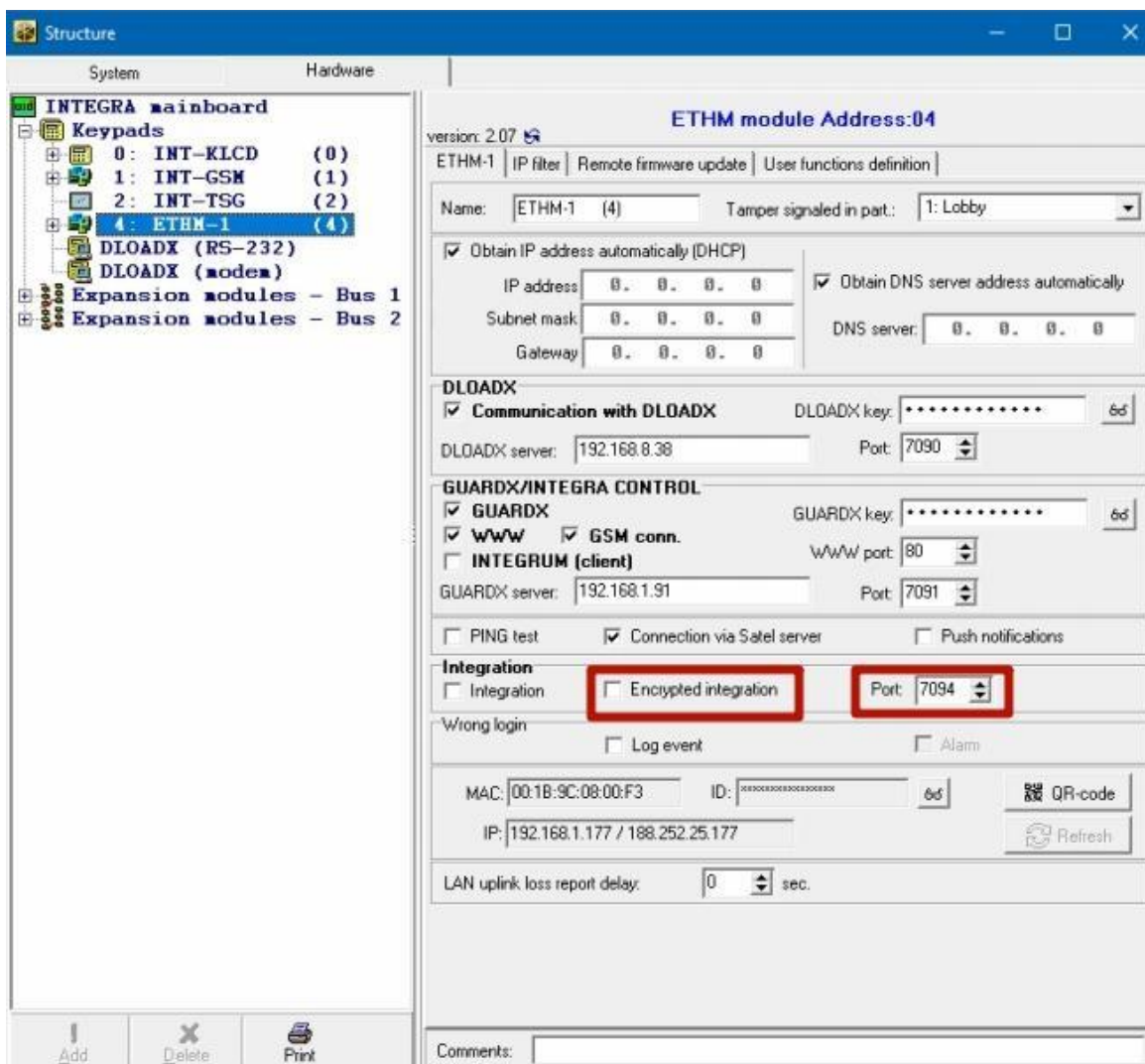
Satel device **must be equipped with ETHM network (Ethernet) module** and work in the same local network as Partizan CCTV camera.



**ATTENTION!**

**"Encrypted integration" in this case should be DISABLED!**

**ETHM module settings must be ON and the integration port must be configured. By default, this is port 7094, but it can be different. It will not affect performance.**



**Structure**

System Hardware

INTEGRA mainboard

- Keypads
  - 0: INT-KLCD (0)
  - 1: INT-GSM (1)
  - 2: INT-TSG (2)
  - 4: ETHM-1 (4)
- DLOADX (RS-232)
- DLOADX (modem)
- Expansion modules - Bus 1
- Expansion modules - Bus 2

**ETHM module Address:04**

version: 2.07

ETHM-1 | IP filter | Remote firmware update | User functions definition

Name: ETHM-1 (4) Tamper signaled in part.: 1: Lobby

☒ Obtain IP address automatically (DHCP)

IP address: 0. 0. 0. 0

Subnet mask: 0. 0. 0. 0

Gateway: 0. 0. 0. 0

☒ Obtain DNS server address automatically

DNS server: 0. 0. 0. 0

**DLOADX**

☒ Communication with DLOADX DLOADX key: .....

DLOADX server: 192.168.8.38 Port: 7090

**GUARDX/INTEGRA CONTROL**

☒ GUARDX GUARDX key: .....

☒ WWW ☒ GSM conn. WWW port: 80

☐ INTEGRUM (client) GUARDX server: 192.168.1.91 Port: 7091

☐ PING test ☒ Connection via Satel server ☐ Push notifications

**Integration**

☐ Integration ☐ Encrypted integration Port: 7094

Wrong login ☐ Log event ☐ Alarm

MAC: 00:1B:9C:08:00:F3 ID: .....

IP: 192.168.1.177 / 188.252.25.177

LAN uplink loss report delay: 0 sec.

QR-code Refresh

Comments:



You can find out more about Ethernet module for SATEL devices in the special user manual:

[https://smartel.ua/upload/medialibrary/76c/smartel.ua\\_rukovodstvo\\_ethernet\\_modul\\_satel\\_ethm\\_1\\_plus.pdf](https://smartel.ua/upload/medialibrary/76c/smartel.ua_rukovodstvo_ethernet_modul_satel_ethm_1_plus.pdf)



#### ATTENTION!

**It is important to remember that ETHM module in integration mode can only work with one system at a time!**

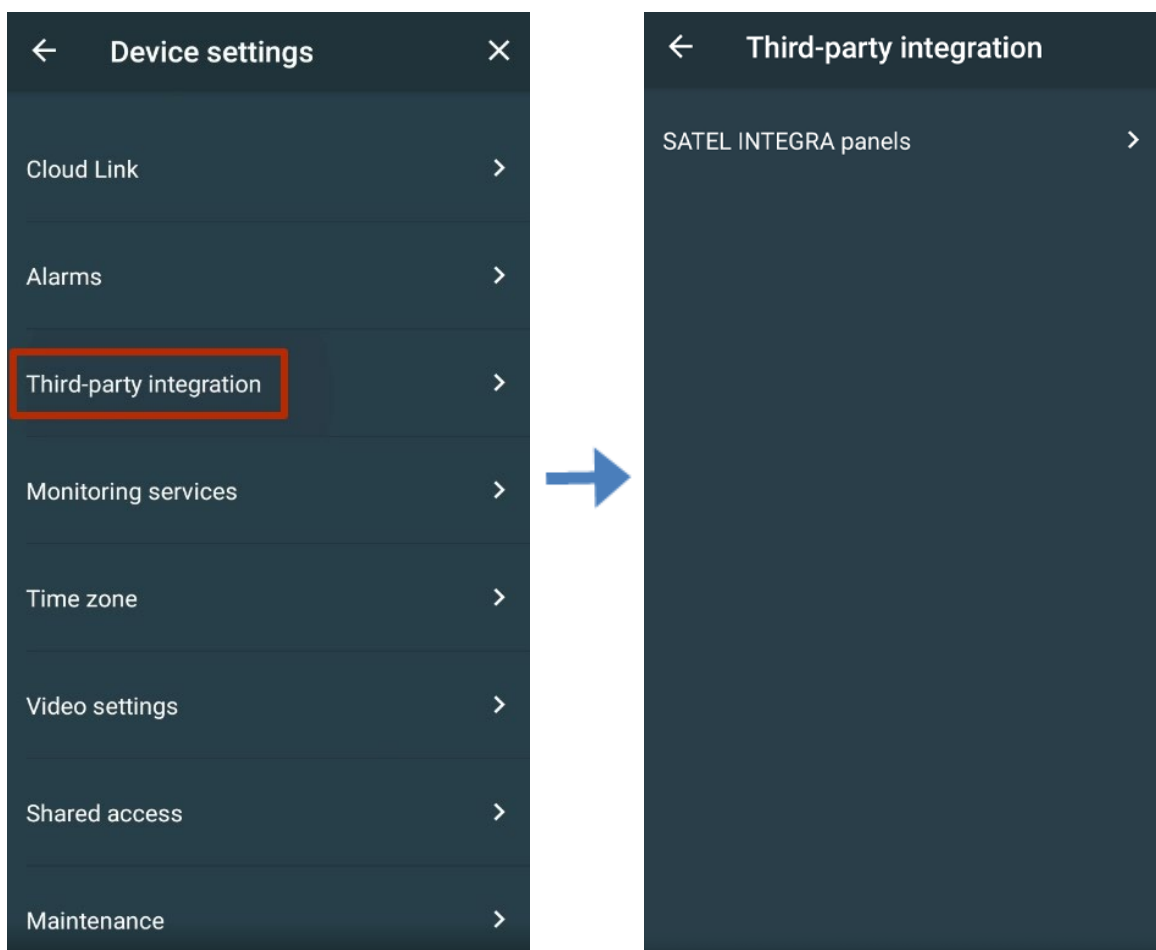
**For example, if a Satel Device is connected to a “smart home”, it will no longer be able to interact with Partizan equipment. And vice versa, if the Device is integrated with Partizan, it will be impossible to connect devices for “smart home”.**

### 3. Adding Satel device to Partizan mobile application

#### 3.1. Connection Settings


To enter Partizan device settings you need to make a long press on the name of added device and in the menu that opens, click **Device Settings**.

Then click **Third-party integration** and in the screen that opens, select **SATEL INTEGRA** panels:



The screen that opens contains text fields for adding information about the integration:

- IP-address of the device
- Port
- Device name
- Code page
- User code

 **Third-party integration**

IP address


Port

7094

Device name

Integra 64

Code page

Win-1251

User code

Remember User code

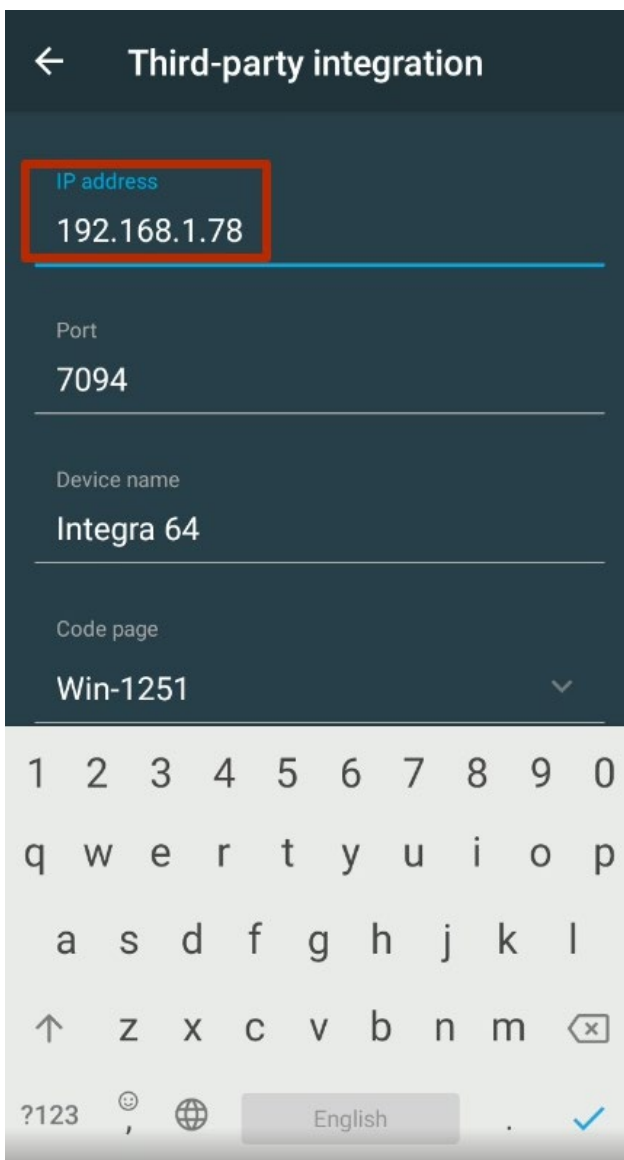
☒

[Show less](#)

### 3.1.1. IP-address

In this field you need to enter **IP-address of Satel device**.

Partizan and Satel devices must be in the same local network, that is, they must be connected to the **same router or switch**.



### 3.1.2. Port

In addition to **local connection**, remote connection via **Internet** is available for Satel devices.

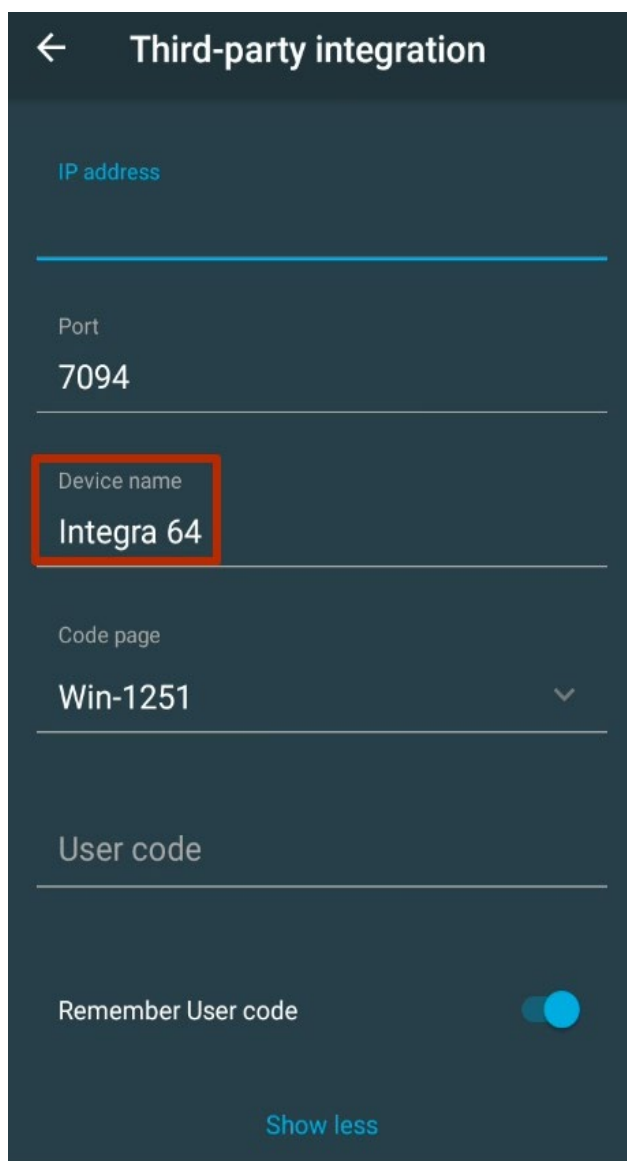
If Partizan and Satel devices are located in different local networks, you must:

- The router to which Satel device is connected must have a static IP address.
- In the IP-address field, specify the static address of the router.
- Redirect port 7094 from router to Satel device.

### 3.1.3. Device name

You must enter the **name of the device**, which will be displayed in the list of equipment added to the cloud account.

For example: “**INTEGRA 64**”.



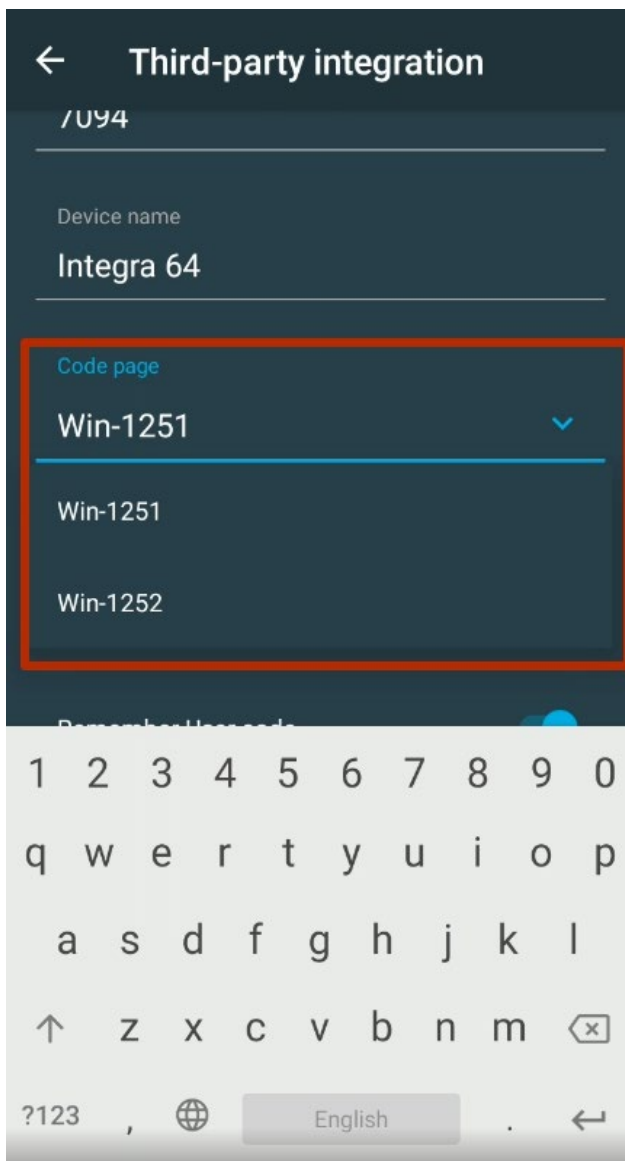
The screenshot shows a mobile application interface for 'Third-party integration'. The form includes the following fields and controls:

- IP address**: A text input field.
- Port**: A text input field containing the value '7094'.
- Device name**: A text input field containing the value 'Integra 64', which is highlighted with a red rectangular box.
- Code page**: A dropdown menu showing 'Win-1251'.
- User code**: A text input field.
- Remember User code**: A toggle switch that is currently turned on (blue).
- Show less**: A link at the bottom right of the form.



### 3.1.4. Code page

Partizan mobile application **supports Satel devices with English and Russian firmware.** For correct operation, you must select the encoding Win-1252 for the English language and Win-1251 for the Russian language.

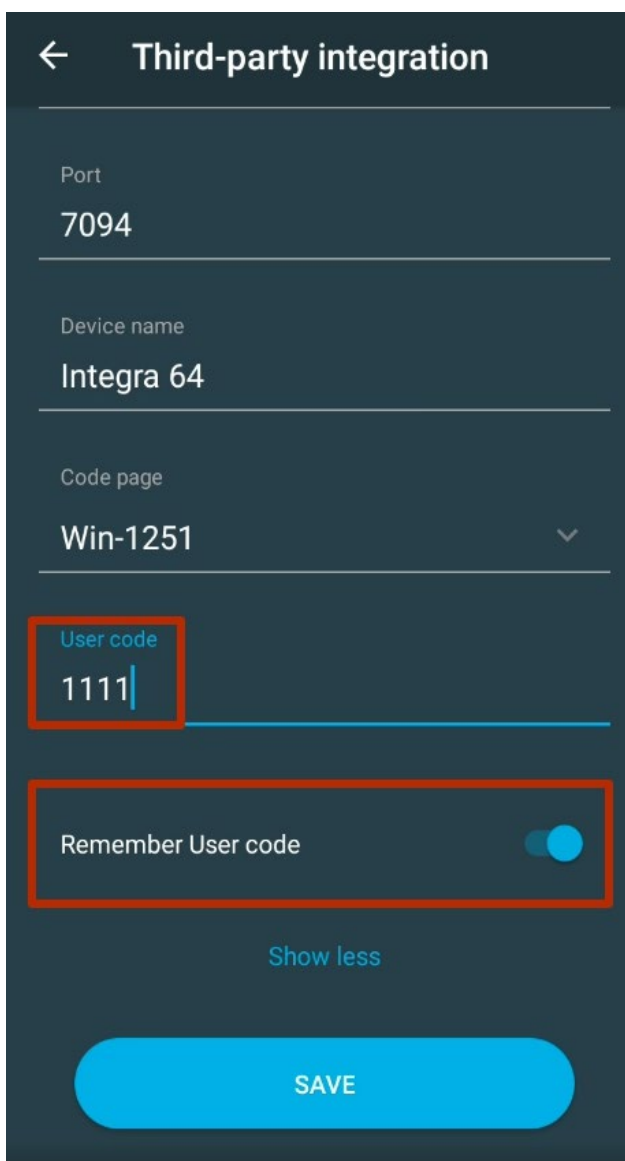


### 3.1.5. User code

You need to set user code.

By default, the application asks for a password when arming and disarming the device.

In order not to enter the password every time, you must enable the **Remember user code** switch.



← Third-party integration

Port  
7094

Device name  
Integra 64

Code page  
Win-1251

User code  
1111

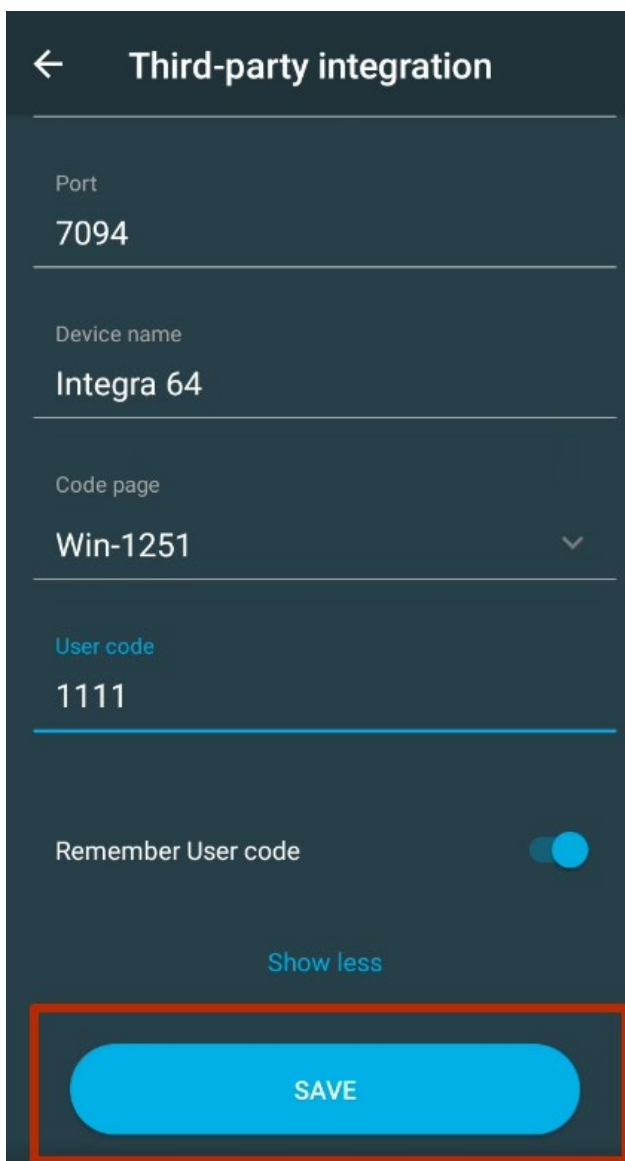
Remember User code ☒

Show less

SAVE

### 3.1.6. Connection completion

After completing all the settings on the Third-party integration screen, click Save button.



← Third-party integration

Port  
7094

Device name  
Integra 64

Code page  
Win-1251

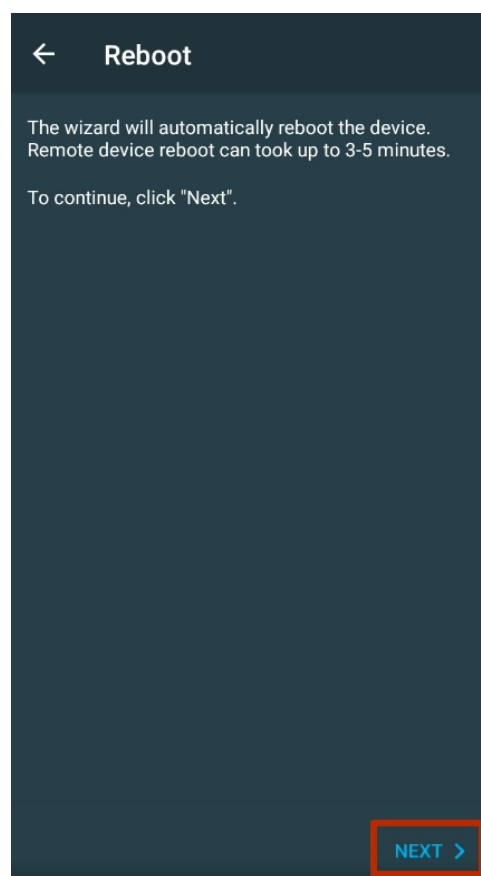
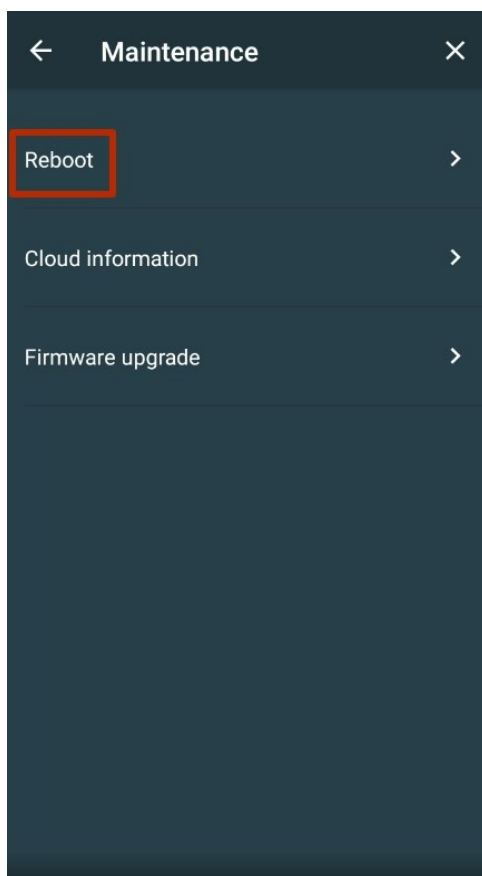
User code  
1111

Remember User code ☒

Show less

SAVE

Now you need to reboot the device, to do it click **Reboot** in the **Device Settings/Maintenance** menu and in the screen that opens, click **Next**:

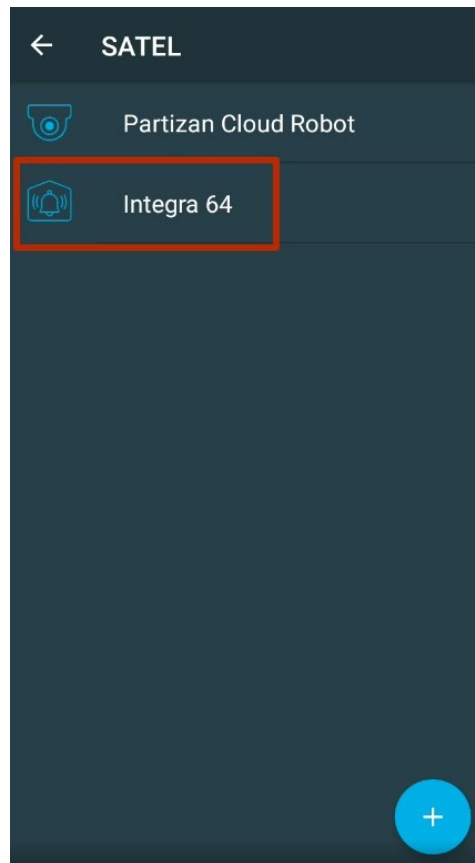
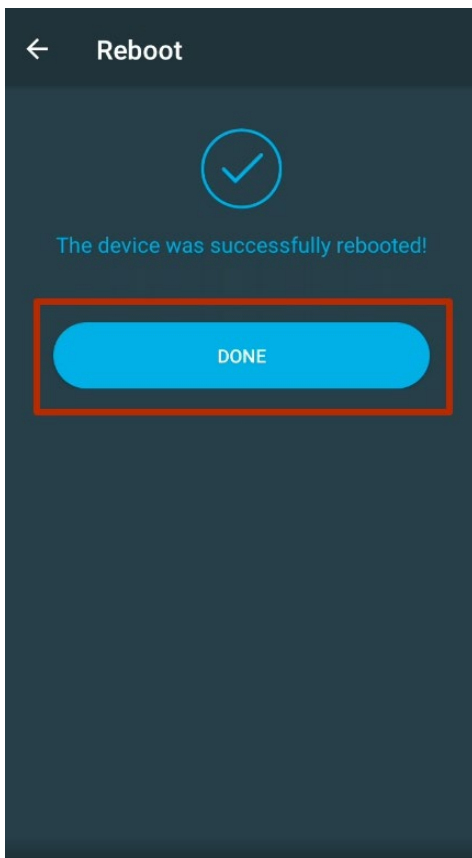


**ATTENTION!**

**The reboot can take several minutes!**

After the reboot is complete, click **Done**.

The main screen of the application will open:



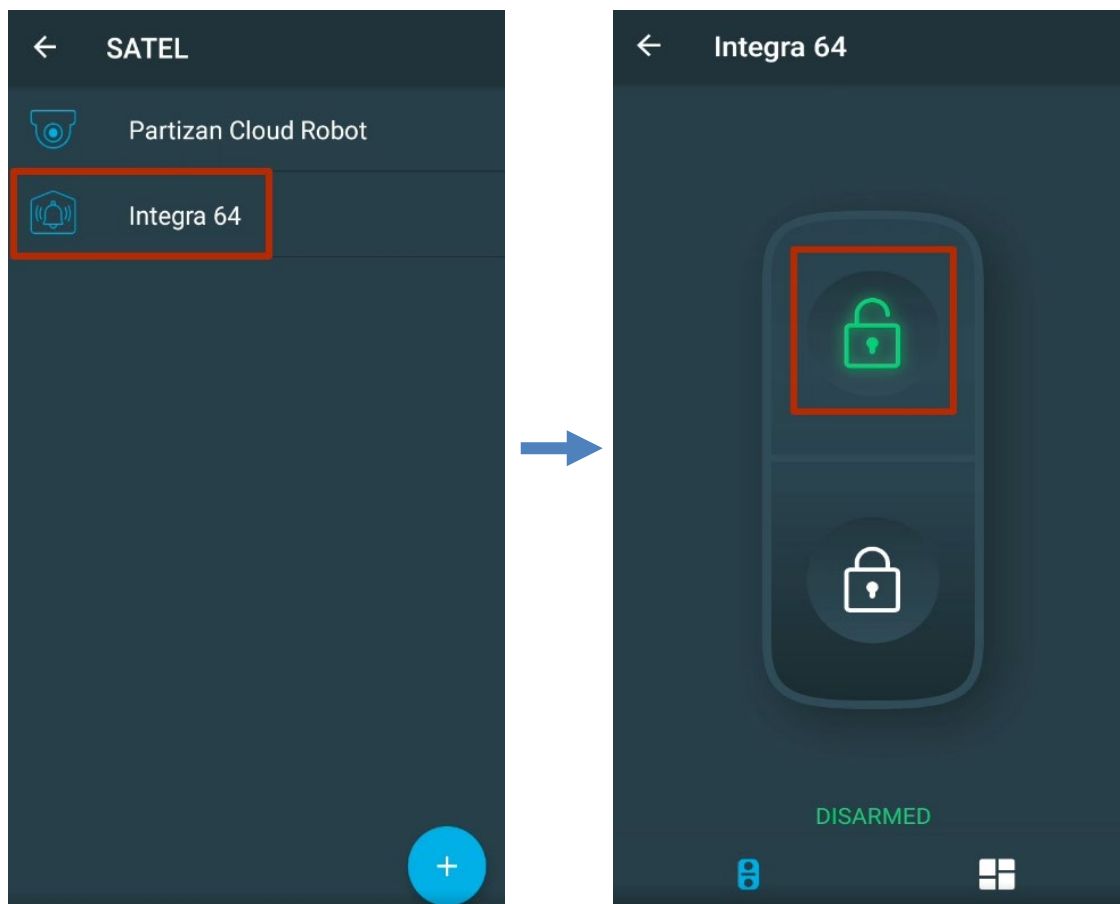
**Satel device is ready for work!**

## 4. Satel device and its Groups control in Partizan mobile application

Partizan mobile application for Android allows arming and disarming both the **entire device** and its **individual Groups**.

### 4.1. Arming and disarming the device

When you click on the device name, you will go to controls interface.



A green image of an open lock means that the Device is disarmed.



When you press the button with the image of a **closed lock**, a pop-up menu with **security modes** will appear at the bottom of the screen.



**Full Arm:** applies if everyone has left the protected area.



**Full arm + bypasses:** bypassing zones (allows you to stay within the protected zone) - bypassing all zones for which the installer has enabled the BYPASSING IF NO EXIT option is enabled.

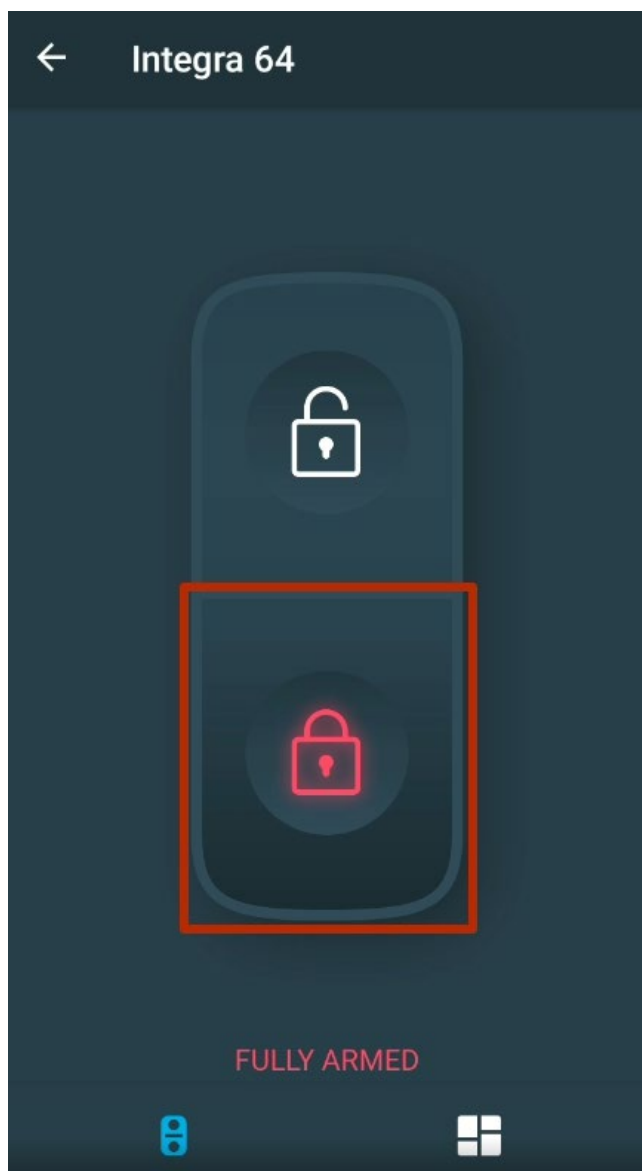


**Arm (Stay)** - (permission to stay indoors, i.e. windows and doors are armed, but all motion detectors in the house are disabled): no internal zones (allows you to stay within the protected area): internal zones will not be armed; violation of external zones will trigger a silent alarm; violation of another security zone will trigger a loud alarm.



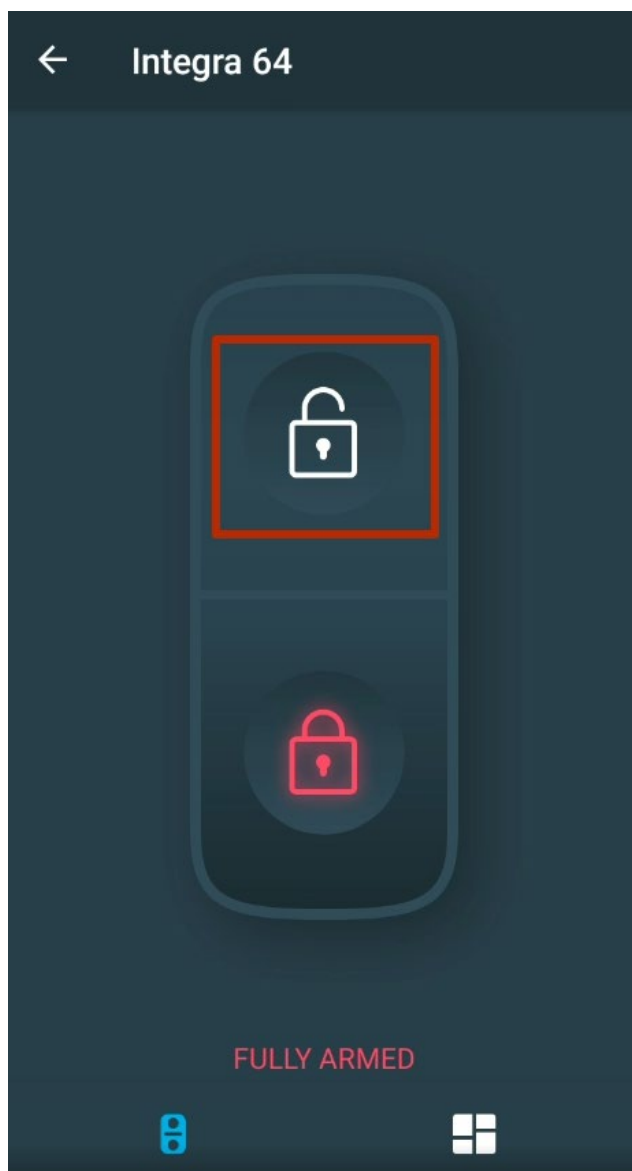
**Arm (stay, no delay):** no interior zones and entry delay = (allows you to stay within the protected area - used if no one else enters the protected area) - the type of arming mode is the same as the previous one, but delayed zones work as instant (no entry delay).

When one of the indicated modes is selected, the device will be **fully armed (all groups will be armed in the selected armed mode)**.





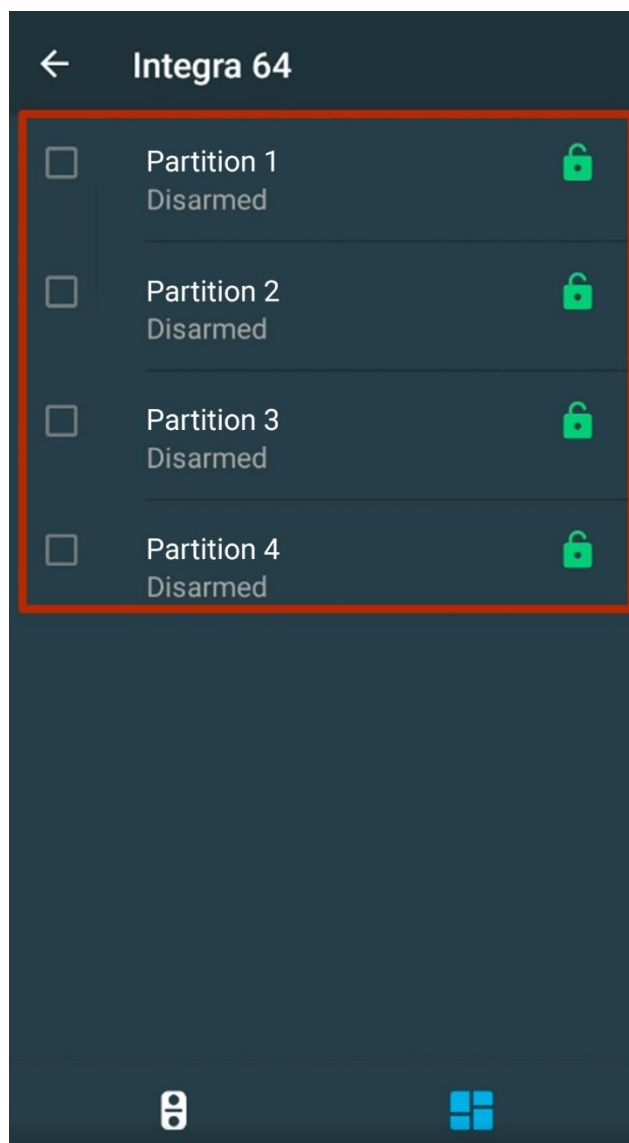
To **disarm the Device**, click on the image of an open lock.



## 4.2. Security groups and modes



Clicking on the icon will open a screen with **Groups**.

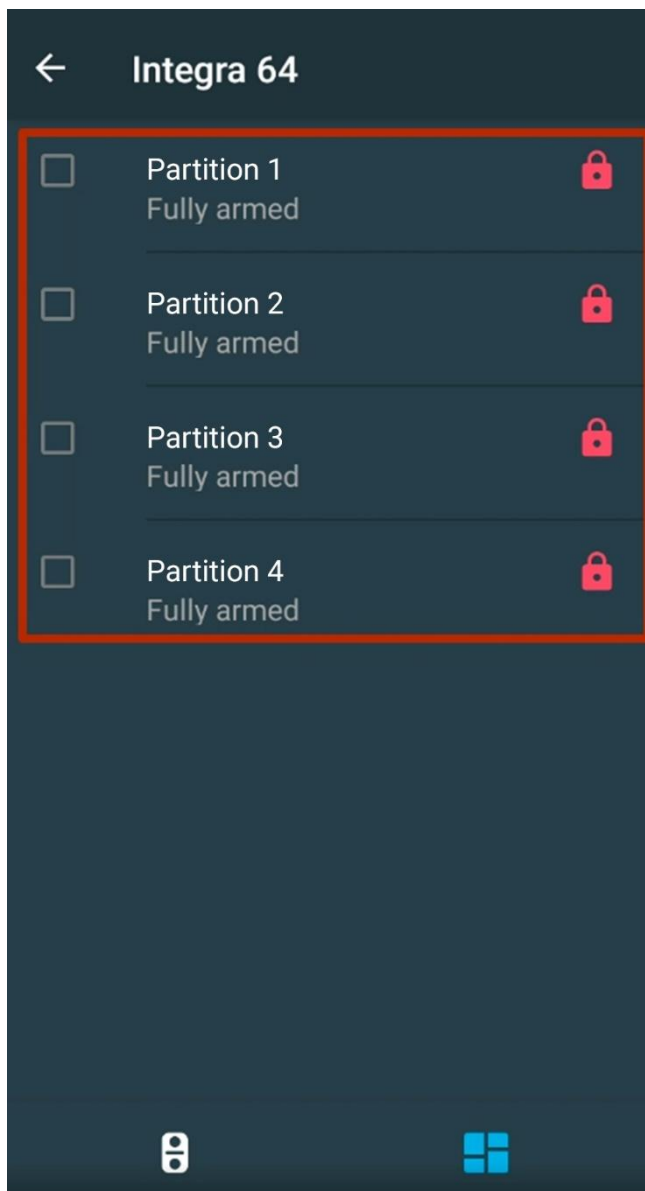


Groups (Partitions) are created in Satel software for easy control and arming/disarming.

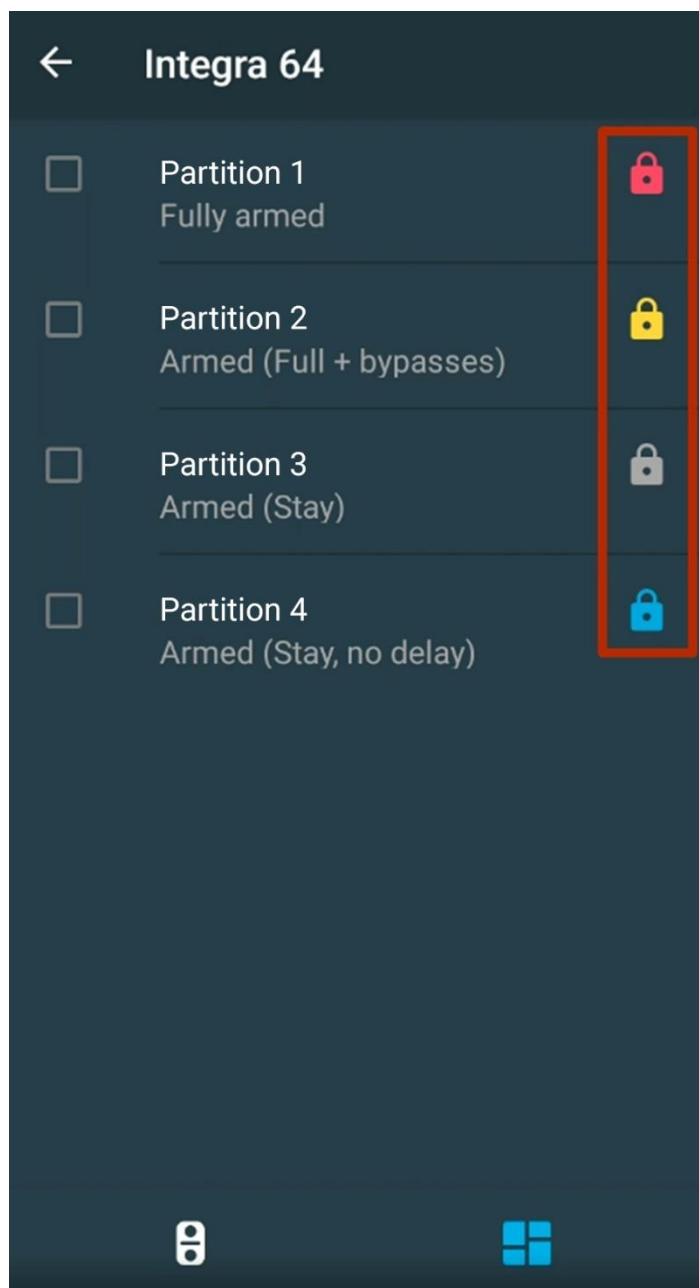
A group is considered to be **the software integration of various devices** connected to the central Satel panel.

If the Device is **disarmed**, this will apply to all Groups as well.

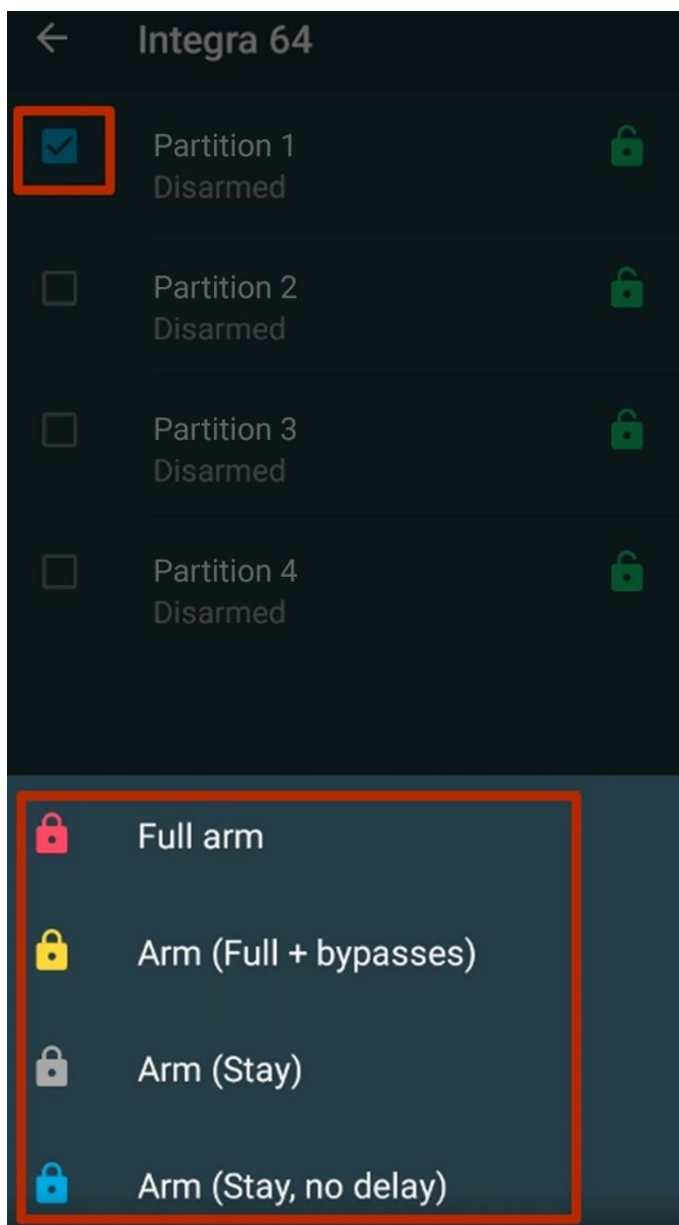
The same applies to the mode when the Device is **armed**.



Any of the Groups or several Groups can be assigned their **own armed mode**.



To do this, mark the Group with a tick in the appropriate box and select the required **arming mode**.



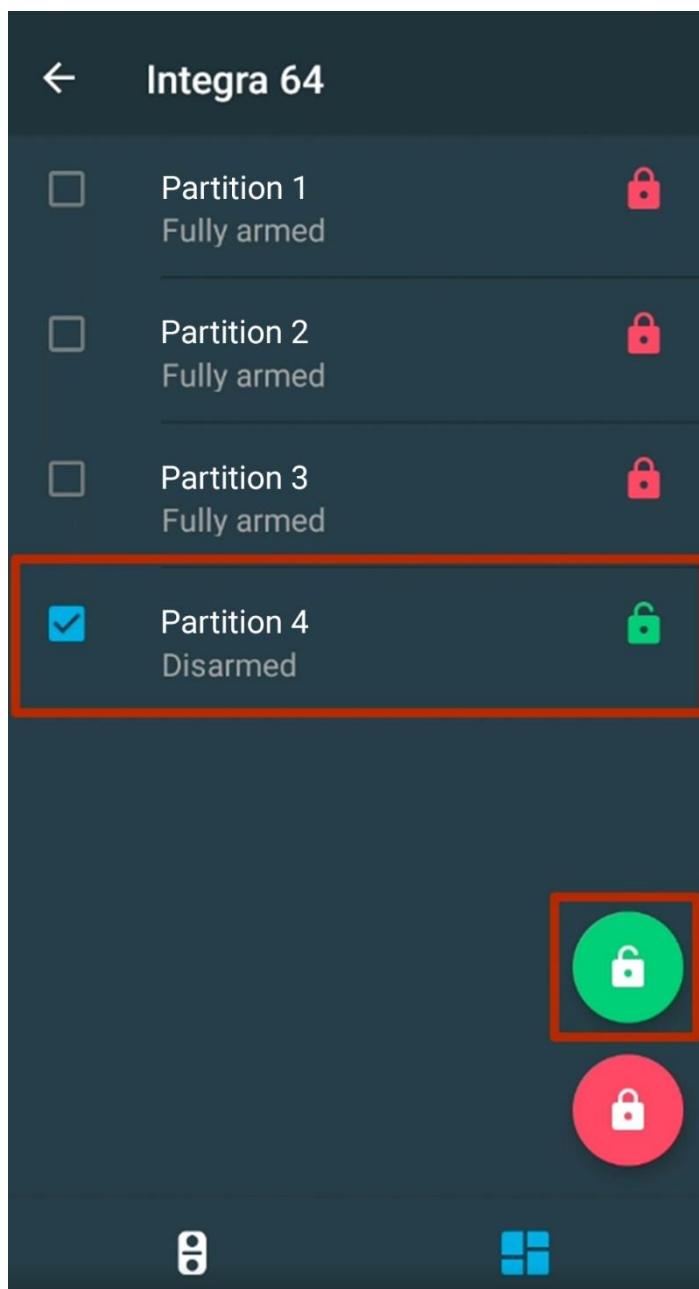
The screenshot displays the 'Integra 64' interface. At the top, there is a back arrow and the title 'Integra 64'. Below this, a list of four partitions is shown, each with a checkbox, the partition name, its status, and a lock icon. The first partition, 'Partition 1', is checked and its status is 'Disarmed'. The other three partitions are unchecked and also show 'Disarmed' status. At the bottom of the screen, a menu is open, listing four arming modes, each preceded by a lock icon: 'Full arm' (red lock), 'Arm (Full + bypasses)' (yellow lock), 'Arm (Stay)' (grey lock), and 'Arm (Stay, no delay)' (blue lock). The entire interface has a dark theme.

Partition	Status	Arming Mode
Partition 1	Disarmed	Full arm
Partition 2	Disarmed	Arm (Full + bypasses)
Partition 3	Disarmed	Arm (Stay)
Partition 4	Disarmed	Arm (Stay, no delay)

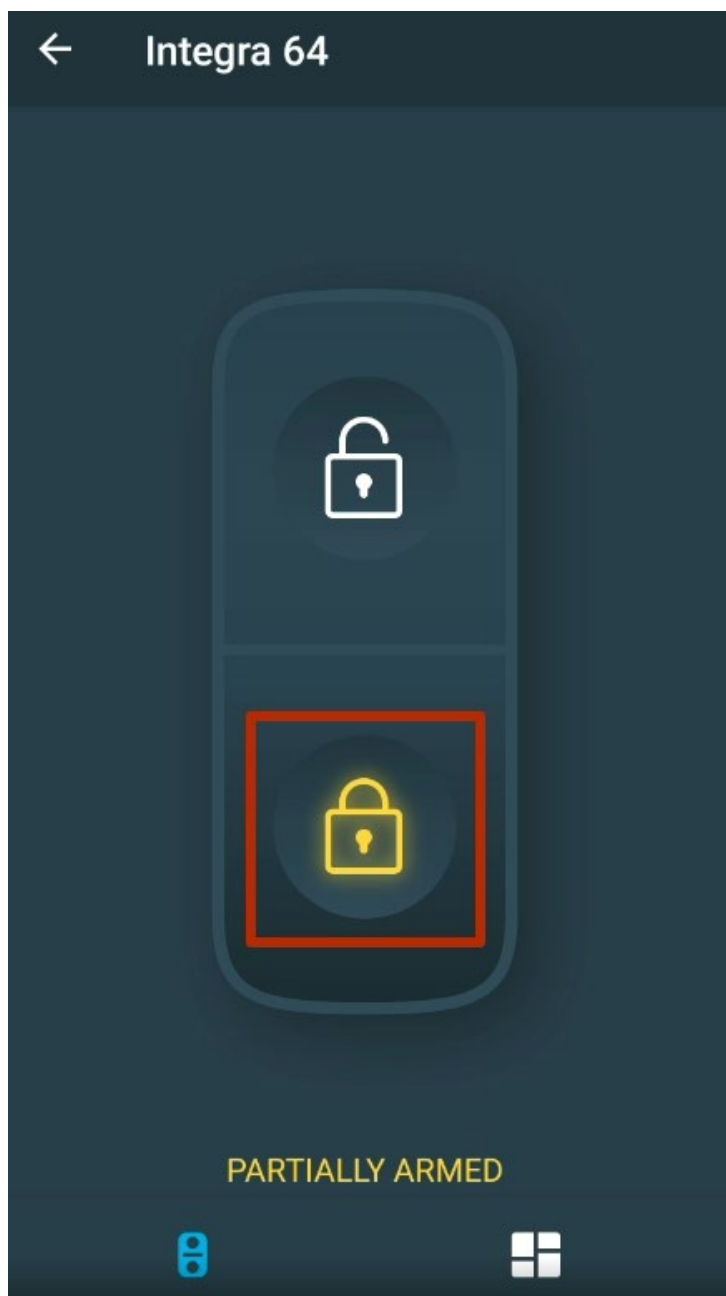
### 4.3. Partial arming

**Partial arming** is active if only some **part of the existing group** is armed.

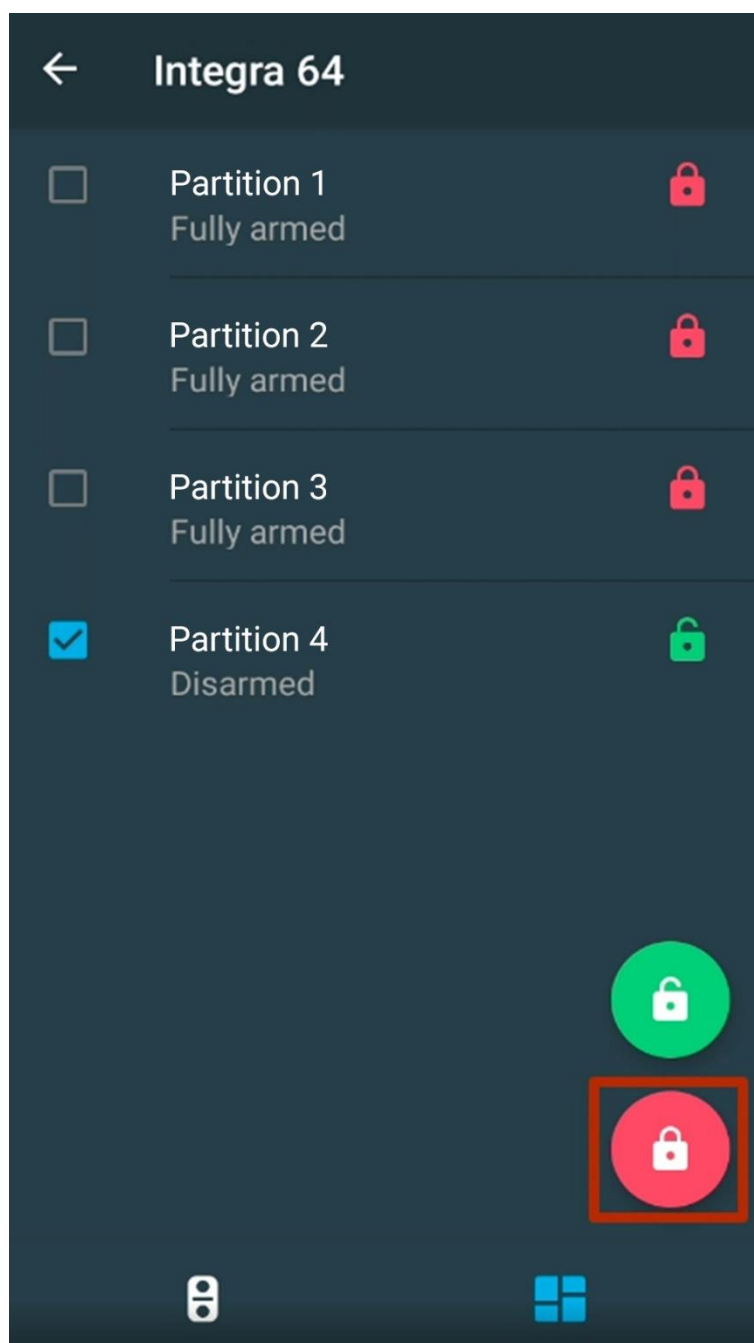
To arm the device in partial armed mode, mark the required Group/Groups and press the **green button with the lock open**.



After that, the Device will switch to **partial arming mode**, which will be displayed on the Main screen - the image of the closed lock will turn **yellow**.




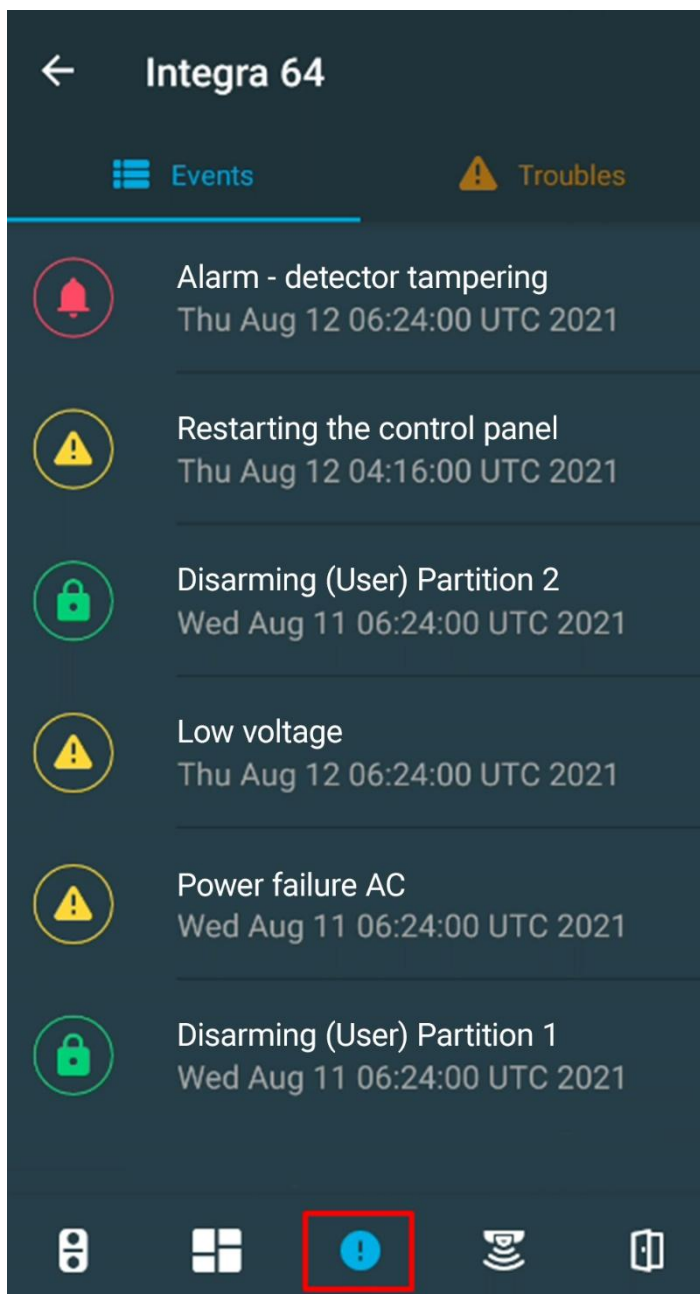
To **fully arm** a Group/Groups, select one or several groups and press the red button with a closed padlock.





#### 4.4. The event log

Open the event log by pressing  button.




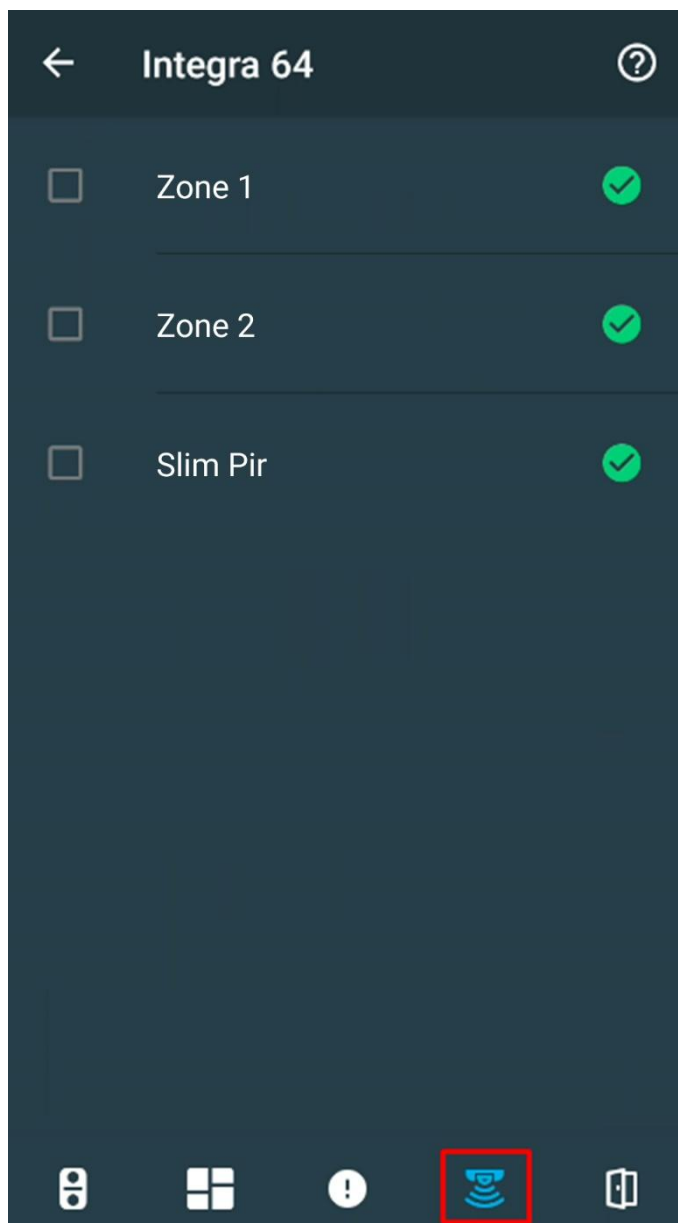
The alerts screen contains two tabs: **Events** and **Troubles**.


The **Events** tab provides information on alarms, tamper, disarming and arming, power status, bypassing Zones, etc.

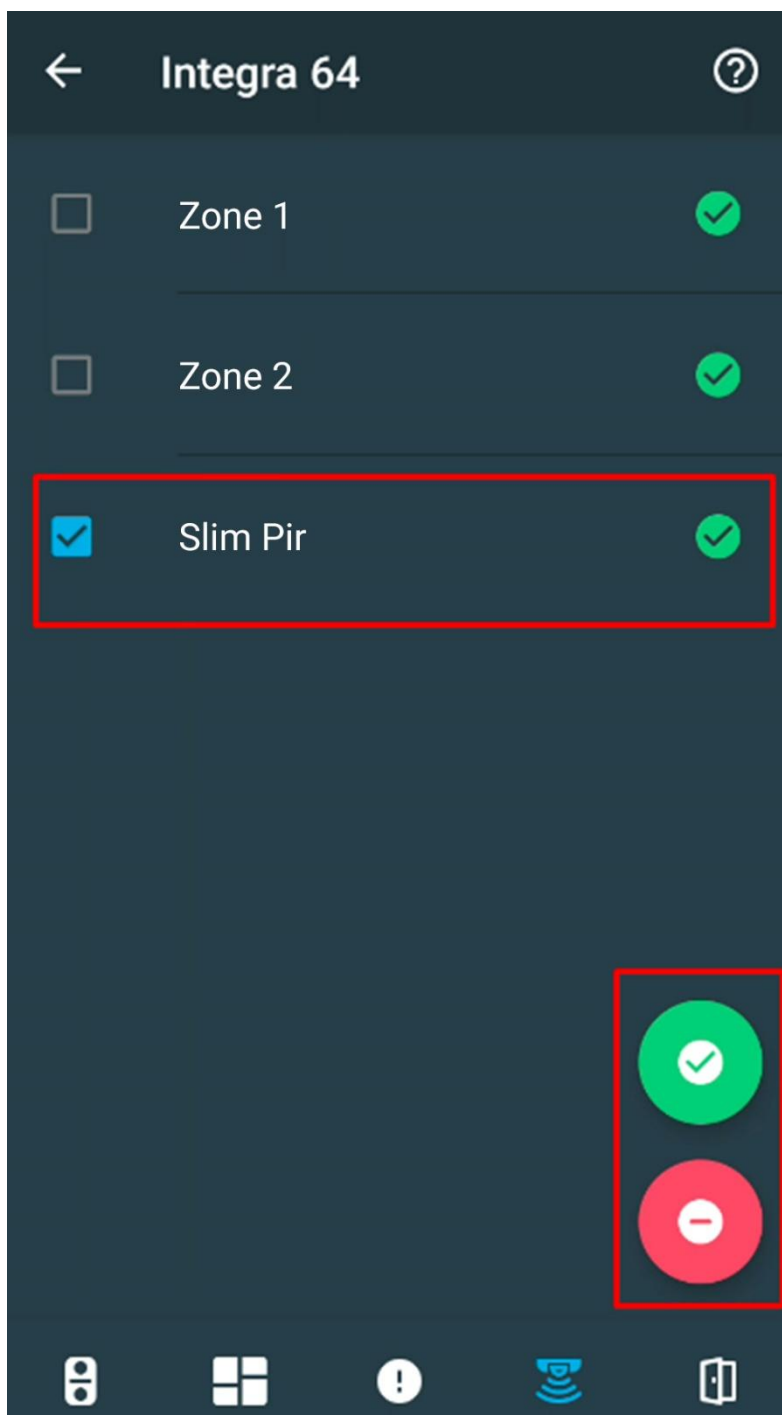
**Troubles** tab informs about technical problems of the device.

#### 4.5. Zones and their exclusion

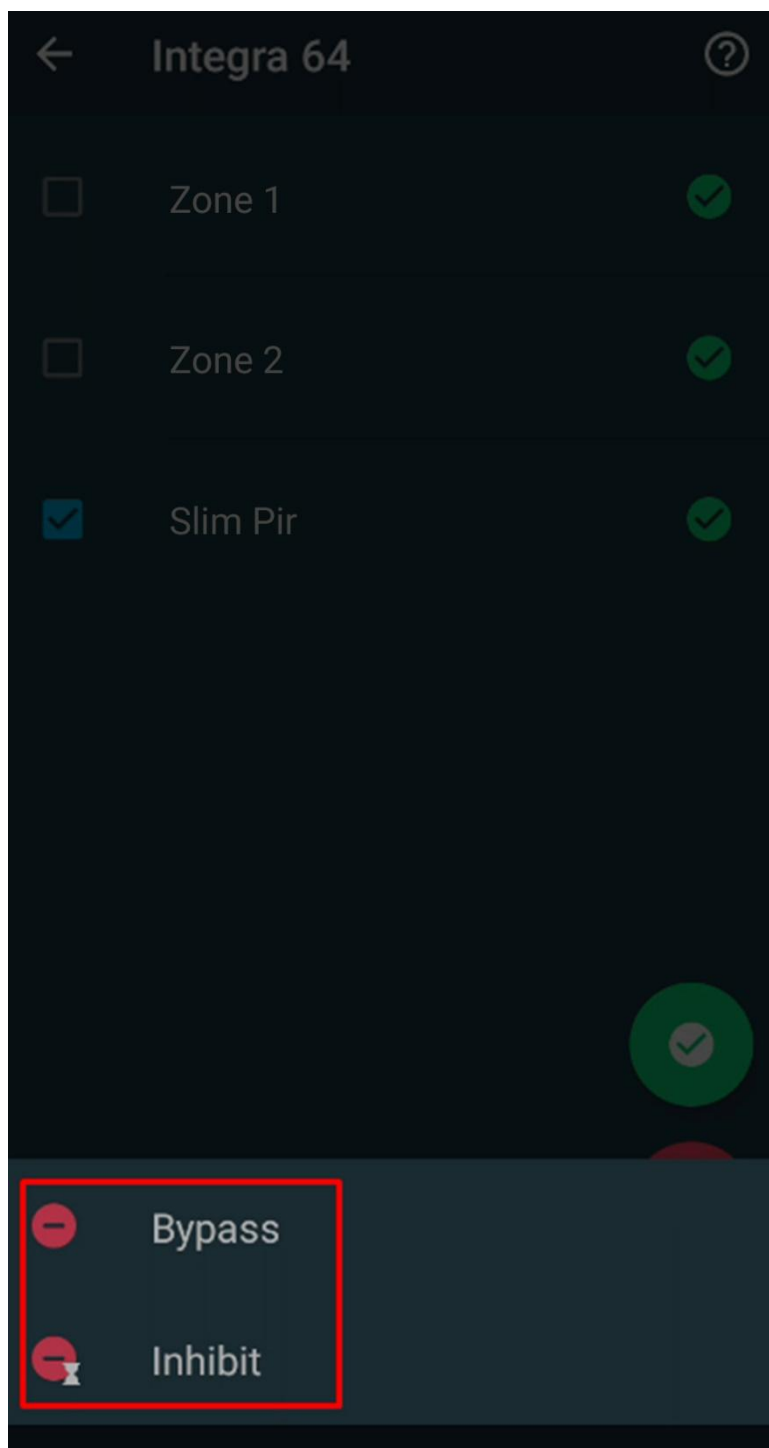
Open the **Zones** screen by pressing  button. The term "**Zone**" means the area covered by Satel sensor.




Having selected one or several Zones, it (they) can be excluded by pressing  button.



This will provide two exclusion modes: **Bypass (constant exclusion)** or **Inhibit (temporary exclusion)**.



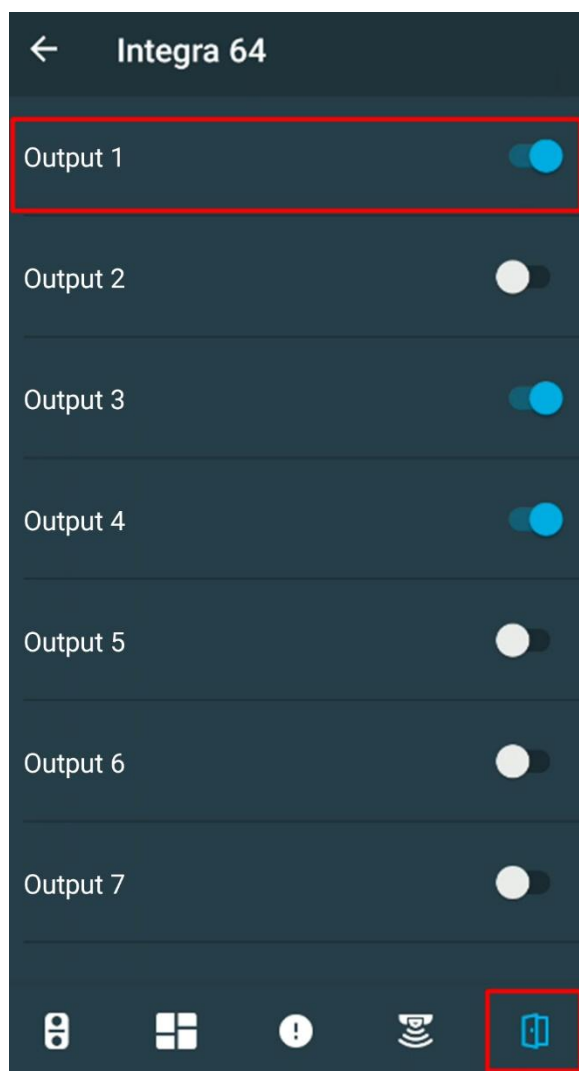
To cancel excluding of the Zone, press  button.

#### 4.6. Outputs

Open **Outputs** screen by pressing  button.

This screen controls gates, doors, roller shutters, etc.

Having selected one or several **Outputs** using the slider, you can open or close it (them).



*The integration of Satel equipment with Partizan mobile application opens up new opportunities for both security system installers and end-users!*

***Use and enjoy!***

### Technical support:

E-mail: [support@partizan.global](mailto:support@partizan.global)

Skype: partizan-support

Messengers: +420 777 054 888 (Viber, Telegram, WhatsApp)



Technical support working time:

<https://partizan.global/support/technical-support>



Partizan software:

<https://apps.partizan.global/>