AV-08FB

AV-08FB

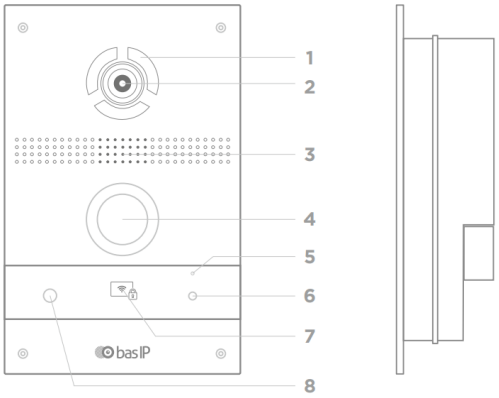
Exported on 06/28/2023

Table of Contents

1 Device description

AV-08FB is a stylish and unique individual entrance panel with face recognition. The panel is equipped with a 2-megapixel camera, a piezoelectric call button, and a UKEY reader. The model is presented in 3 color schemes, thanks to which it looks very stylish on different types of building facades and suits different interiors.

1.1 Appearance



1 - Backlight.
2 - Camera.
3 - Loudspeaker.
4 - Piezoelectric button.
5 - Microphone.
6 - Proximity sensor.
7 - Card reader.
8 - Proximity sensor.

2 Technical parameters

2.1 Main features

Panel type: Individual

Camera: 1/3,

Angle: 90° horizontal x 56° vertical

Camera resolution: 2 MP

Output Video: 1080p (1920x1080), H.264 Main Profile

Night backlight: 6 LEDs

Minimum illumination: 0,01 LuX

Protection class: IP65

Operating temperature: -40 - +65 ℃

Power consumption: 6,5 W, standby - 3,6 W

Power: PoE, +12V

Body: Aluminum

Colors: Silver, Black, Gold

Dimensions for installation: 108×181×58 mm

Size of the panel: 125×199×48 mm

Installation Type: Flush mounting, Wall mounting (with BR-AV8)

2.2 Functionality

Interface: Multilingual web interface

Opening the lock: By means of a monitor, a QR code, a guest link, an access card, the BAS-IP Intercom app, the BAS-IP UKEY app, Face Recognition

Access Control: Face Recognition, UKEY (EM-Marin/ MIFARE®/NFC/Bluetooth), Multi-factor authentication

Access control integration: Output WIEGAND-26, 32, 34, 37, 40, 42, 56, 58, 64

Number of call melodies: 4 polyphonic melodies, ability to customize melodies for different actions

Authentication: Separate password for web interface

Talk mode: Duplex

Additional: SIP P2P, Built-in Relay, PoE electromechanical lock Power supply, 2 Separate inputs for Door sensors, Proximity Sensor, Tamper sensor, Open API, Link Software support

3 Configuration through the web interface

3.1 Login

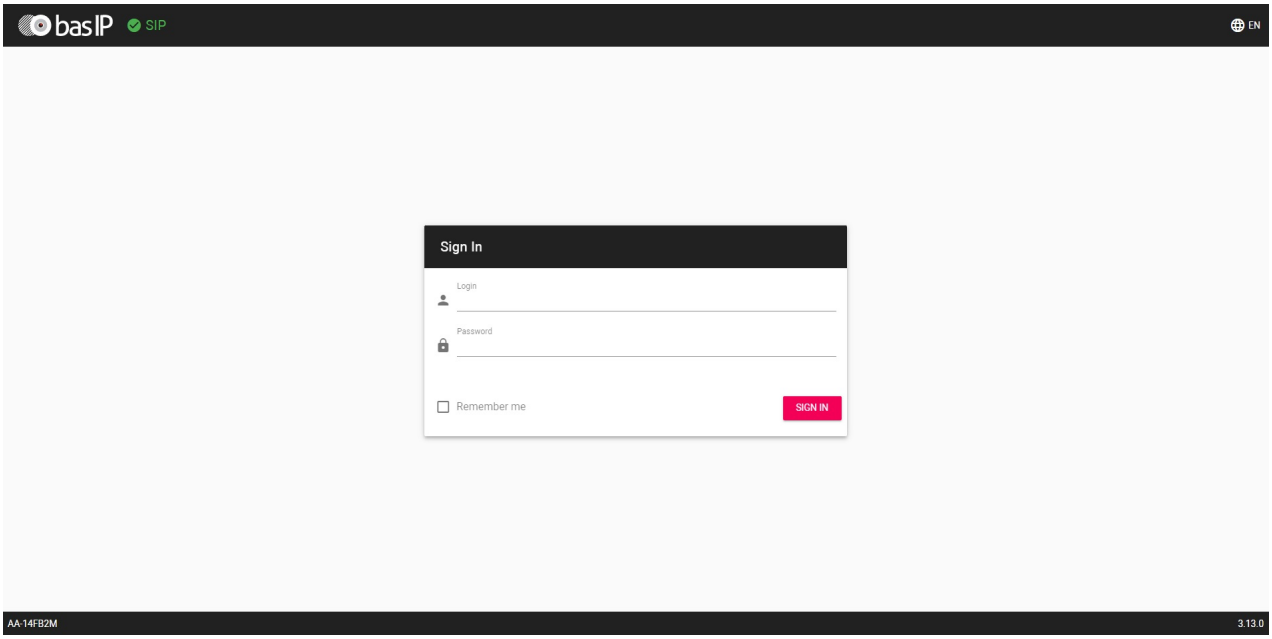
An outdoor panel is configured remotely through the web interface by connecting to the device via an internet browser on the PC. The panel and PC from which you plan to access the device must be connected to the same network segment.

In the Internet browser, you must enter the panel IP address into the address input line. To find the device and figure out its IP address you can use this search and upgrade tool[1] that shows all connected to the network devices.

After entering an IP address in the browser, a window to type a login and password will appear. At the top right corner, you can change the interface language. Russian, English, Ukrainian, Spanish, Polish, and Dutch languages are available.

Also, you can find a device model name at the left lower corner and the current firmware version at the right lower corner.

1 http://cdn.bas-ip.com/files/Software/Remote_Upgrade_Tool.zip



Info

Default values to enter the web interface:

Login: **admin**

Password: **123456**

The password for logging into the web interface is the administrator password. By default, it is 123456, but you can change it in the appropriate tab[2].

3.2 Dashboard

After successful authorization, the following **device information** will be displayed:

- **framework**;
- **launcher** (firmware) version;
- device **serial number**;
- current connection **mode of the hybrid adapter;**
- **hybrid** adapter **version;**
- **device name**;
- **temperature sensor** availability, its version, type, board type.

2 https://wiki.bas-ip.com/aa07/security-135955147.html

Device info

Framework 1.9.0 20210604	Launcher 3.13.0	Serial number 70520d2d-3856-4140-bde4-34871ac8d909
Hybrid mode Disabled	Hybrid version	Device name AA-14FB2M
Temperature sensor(Version, Sensor type, Board type) Not installed		

The page also contains **network information**:

- current state of the **DHCP** connection (automatic network settings acquisition mode);
- current **IP address** of the panel;
- **subnet Mask**;
- main **gateway** address;
- **DNS server** address;
- Panel **MAC address**.

Network info

DHCP Disabled	IP address 192.168.1.209	Subnet mask 255.255.255.0
Gateway 192.168.1.1	DNS server 8.8.8.8	MAC address 70:69:79:E0:F0:36

3.3 Network

In the tab, you have access to the network, custom NTP, and management system settings.

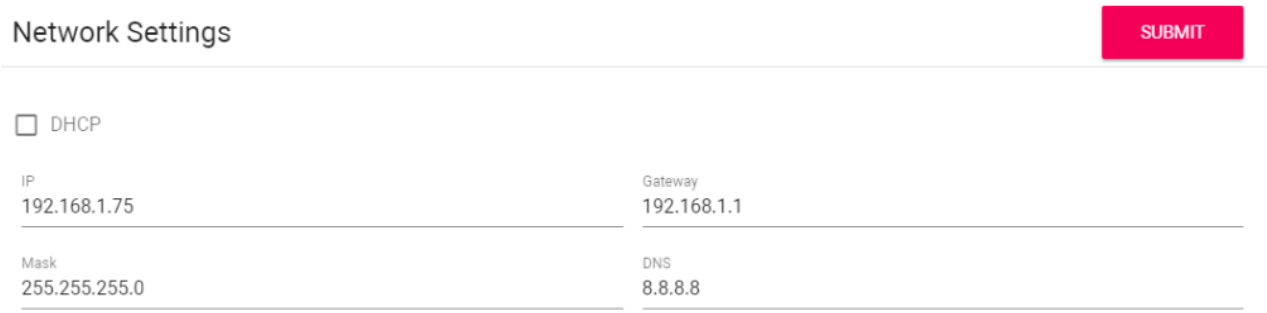
- Network settings(see page 10)
- Custom NTP(see page 11)
- Management system(see page 12)
- MQTT protocol configuration(see page 13)
- HTTP protocol configuration(see page 14)

3.3.1 Network settings

Here you can turn on/off **DHCP** connection and get network settings automatically or enter it manually.

For correct panel work you must enter:

- panel **IP** address;
- subnet **mask**;
- the main **gateway**;
- **DNS** server address;



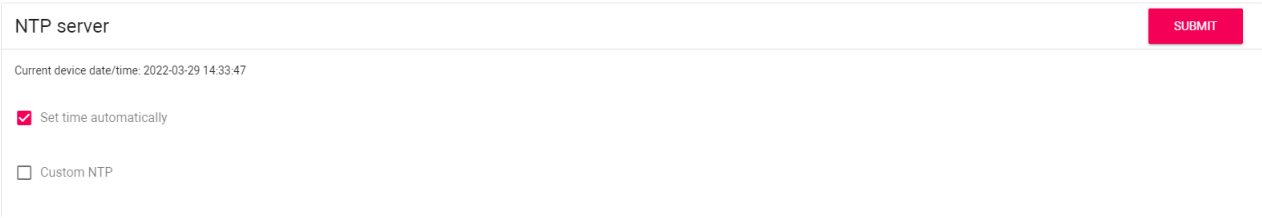
Tip

By default, a device can have a static IP address 192.168.1.90 or 192.168.1.91.

3.3.2 Custom NTP

NTP server data is used for time and date automatic synchronization between a panel and a server.

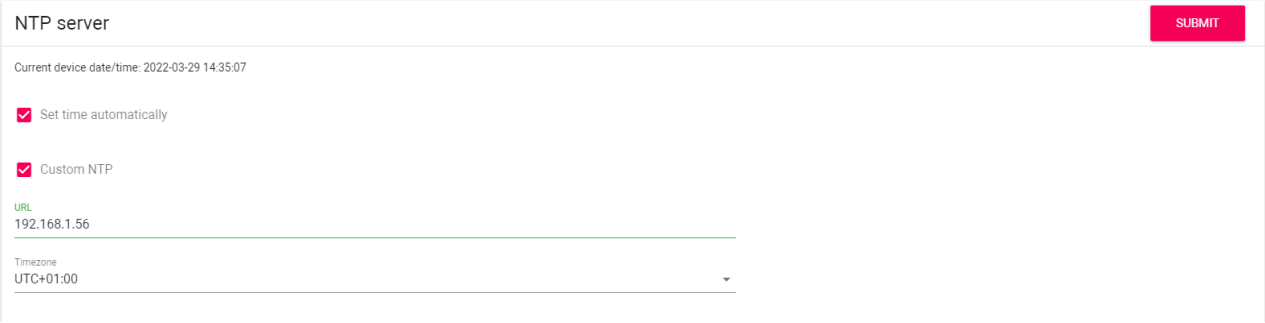
Using the automatic setting of time, data will be automatically synchronized with a server via the Internet. Therefore, this option requires an Internet connection.



Also, you can use custom NTP for automatic synchronization with the necessary server via a local network. To do this, you must:

1. Tick **Set time automatically** and **Custom NTP** boxes.

2. Enter server **URL** or **IP address**.
3. Choose the required **timezone**.
4. Submit changes.



You can also set the time and date manually. To do it, you need to deactivate **Set time automatically** and **Custom NTP** features then set the date and timezone and save these settings.

3.3.3 Management system

In this section, you can enable/disable and configure the server for access control, management, and monitoring of devices, e.g. BAS-IP Link server.

To do it, you must:

1. Log in to the device web interface. By default, the username is **admin**, and the password is **123456**.
2. Go to the **Network** tab > **Management system** section.
3. Select the necessary **protocol:** HTTP or MQTT (is recommended to use) in the **Mode** field.
4. Enter all requried data.
5. Submit settings.

MQTT allows organizing the interaction of BAS-IP Link with devices, which are located in different networks/subnets/behind NAT without additional settings from the network infrastructure (port forwarding, etc.) as **HTTP** requires. We recommend to use MQTT protocol as it is less compex, more effective, provides data security, fast and efficient message delivery.

3.3.4 MQTT protocol configuration

If you select MQTT, you must enter:

- management system broker **address** and **port**;
- **password** for interaction with management system;

Also, you can activate **sending real-time logs** to the server. If necessary, you can enable/disable integrated message **encryption** or add your certificate by clicking the **File** field and selecting the appropriate one. Sending of **heartbeat** (current status: online/offline) is done by defaul here without ability to enable/disable it.

If you need to get current state of MQTT client go to **System** > Debug[3].

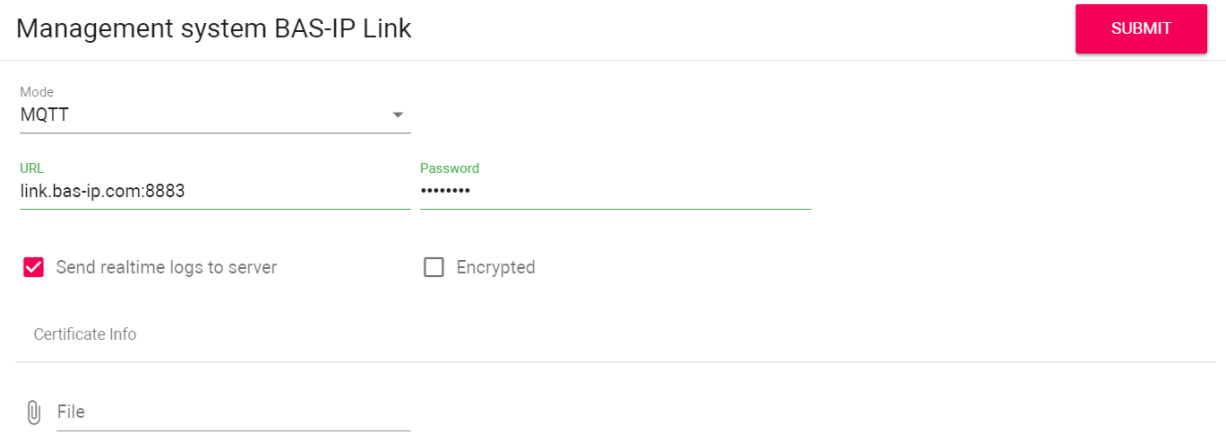
Info

If **sending logs** feature **is enabled** and the **server is available**, the data is sent in real time.

In case when **the feature is enabled**, but the **server is not available**, the panel accumulates all logs and tries to send them every minute until the server becomes available. After successful action, the device proceeds sending in real time. The delayed event log can include up to 1000 entries, and if this number is exceeded, the oldest ones will be cleared, and the server will take them on its own.

If **the feature is disabled**, the server periodically takes logs on its own.

3 https://wiki.bas-ip.com/aa07/debug-135955163.html



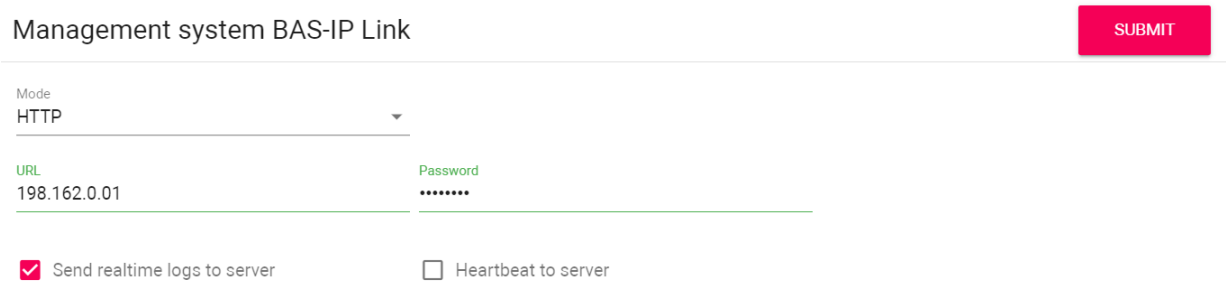
For correct functioning, MQTT protocol is required settings from the management system side. See for details[4].

3.3.5 HTTP protocol configuration

If you select HTTP, you must enter:

- an **IP address** or **domain name** of the server where the Link software is installed;
- device **password** to the server.

If necessary, you can activate **sending real-time logs** and **heartbeat** (current status: online/offline) from the panel to the server.



3.4 Panel

In the tab, you configure settings for apartment, device, calls, and SIP calls.

- Apartment Settings(see page 15)
- SIP settings(see page 16)
- Call settings(see page 17)

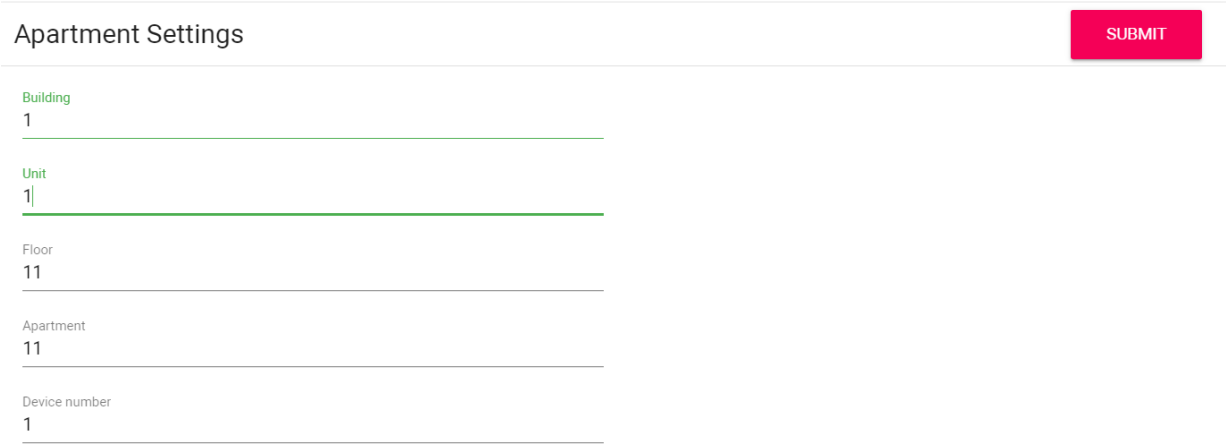
4 https://wiki.bas-ip.com/basiplinken

- Device settings(see page 19)

3.4.1 Apartment Settings

For correct panel functioning, you must enter information about its logical address (more information about logical address formation find here[5]):

- **building** number;
- **unit** number;
- **floor** number;
- apartment number;
- **device number**.



Info

If you have more than 1 entrance panel with the same logical address, you need to specify their **device numbers**, starting from 1 for the main device, and from 2 to 9 for others.

Note:

The individual entrance panel is directly connected to the monitor. For correct functioning, the panel and the monitor must have the same building, unit, floor, and apartment number in apartment settings. Also for monitors, you must indicate their device numbers.

5 https://wiki.bas-ip.com/en/logical-addresses-forming-40468875.html

According to the panel settings from the photo above, the monitor with logical address (number) 0001-01-11-11 will be called. In this logical address, 0001 is a Building No., 01 stands for Unit No., 11 is a Floor No., and 11 is a number of apartment. Thus, the same logical address must be set in the monitor settings: building - 1, unit - 1, floor - 11, apartment - 11.

If there are no such settings, you must make forwarding queues[6] for apartments with IP addresses or SIP numbers of monitors.

3.4.2 SIP settings

These settings are required for the correct work of calls via SIP protocol. Step-by-step guide how to get SIP nubmers and configure a panel for SIP calls if you use BAS-IP SIP server you can find here[7].

To configure SIP calls for the panel, you must **enable** device **SIP registration** and enter the following parameters:

- SIP server **proxy** that can be represented by both an IP address and a domain name.

Data format:

Before the proxy address, you must enter "**sip:**", e.g. sip:gb.sip.bas-ip.com[8]. A full list of BAS-IP servers for each country is available here[9].

If you use a third-party SIP server, you can also indicate a non-standard port in the format:

sip:gb.sip.bas-ip.com[10]**:1506** where gb.sip.bas-ip.com[11] is a SIP server proxy, 1506 is a non-standard port.

- **SIP server address** that can be represented by both an IP address and a domain name.

Data format:

If you use a third-party SIP server, you can also indicate a non-standard port in the format:

sip:gb.sip.bas-ip.com[12]**:1506** where gb.sip.bas-ip.com[13] is a SIP server, 15061 is a non-standard port.

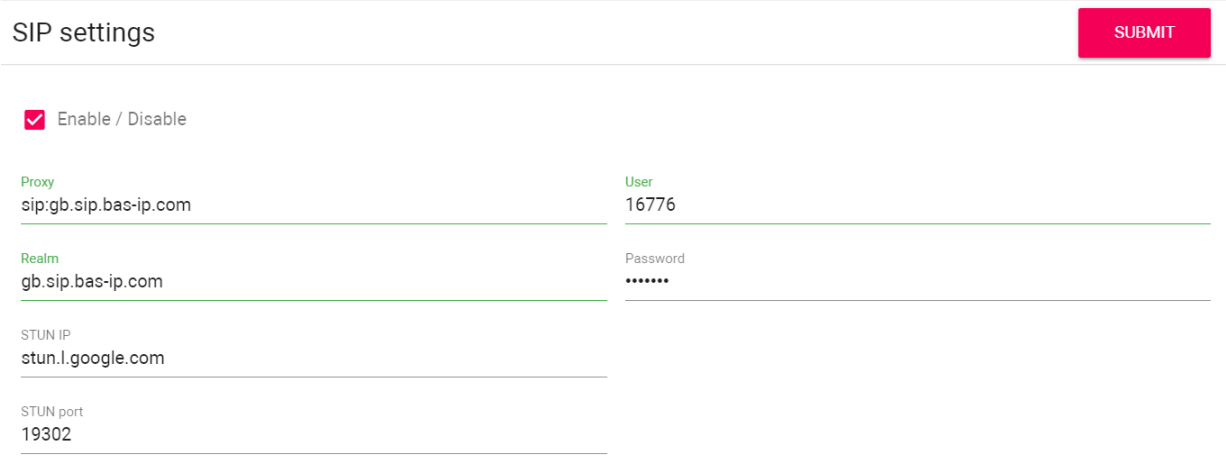
- server **STUN IP** address. For example, stun.l.google.com[14]

6 https://wiki.bas-ip.com/av08fb/forward-135956989.html
7 https://wiki.bas-ip.com/basipcloudservice/step-by-step-guide-how-to-configure-an-entrance-panel-for-calls-via-sip-135957663.html
8 http://gb.sip.bas-ip.com
9 https://wiki.bas-ip.com/basipcloud/en/list-of-countries-and-their-corresponding-servers-88244374.html
10 http://gb.sip.bas-ip.com
11 http://gb.sip.bas-ip.com
12 http://gb.sip.bas-ip.com
13 http://gb.sip.bas-ip.com
14 http://stun.l.google.com

- **port** of the **STUN** server.

> **Note:**
>
> 19302 port is used for Google STUN server.

- **user** SIP number (up to 20 characters).
- **password** for SIP number (up to 20 characters).



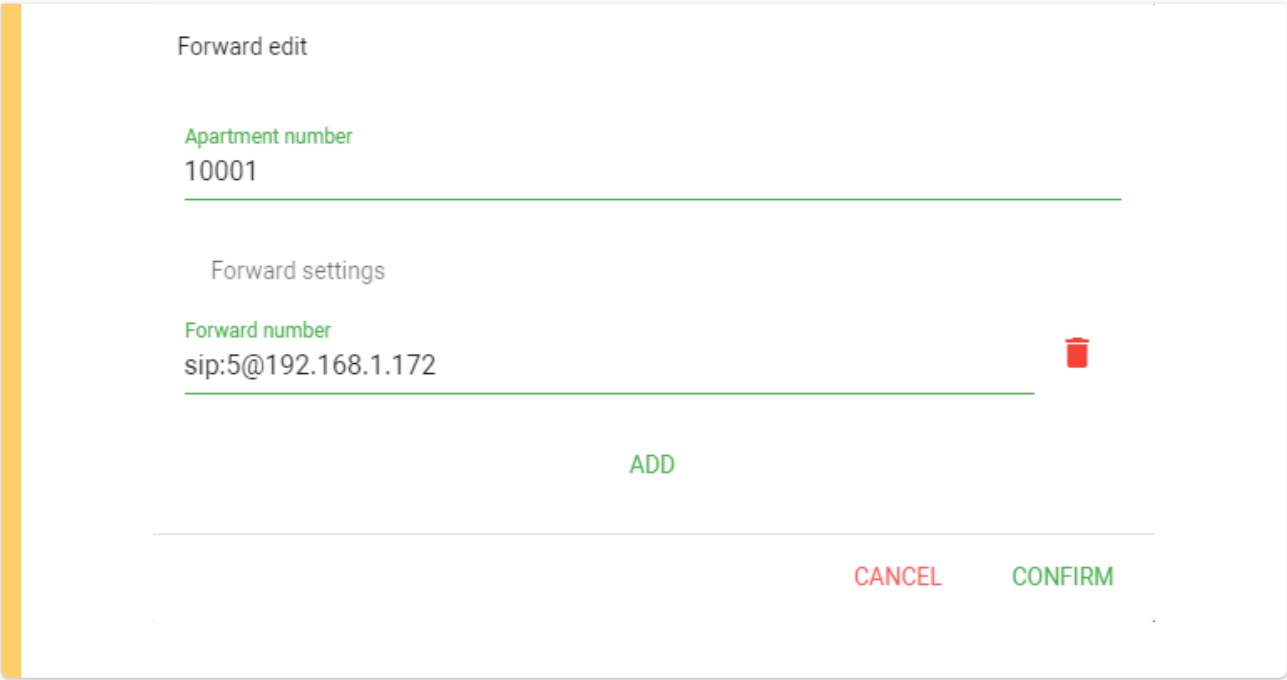
3.4.3 Call settings

At this part you can:

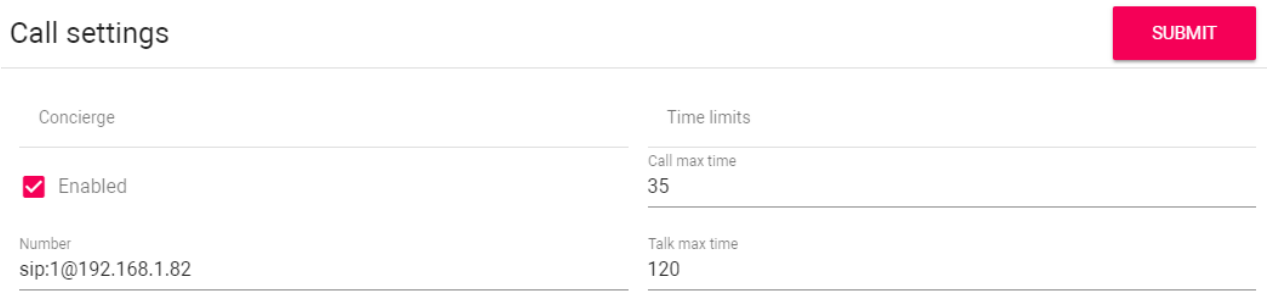
- enable/disable a call to the specified (concierge) number when pressing a button connected to the door sensor input (Concierge call[15] mode must be set);
- indicate the direction (concierge **number**) to which the call will be made when pressing the connected button;

> **Forwarding when pressing the concierge button:**
>
> You can also set up a call to a specified number/s (up to 8) when you press the concierge button using the Forwarding feature. In the Apartment number field, you must enter 1000X, where X is the concierge monitor device number. So, for the 1st concierge monitor apartment number will be 10001. Also, you must enter the forward number in one of the formats: **sip:SIP number@address of the SIP server** (if you need calls to be done via SIP protocol) or **sip:any number@device IP address** (if calls must be done via P2P protocol).

15 https://wiki.bas-ip.com/av08fb/ascess-management-135956970.html



- configure **call max time** (period (10-120 sec) after which the panel automatically ends an outgoing call if there is no answer).
- configure **talk max time** (period (10-300 sec) after which the panel automatically ends the outgoing conversation).



Info

If **the feature is disabled**, the concierge is called via an internal protocol. If the system has concierge monitors, the call will go to the main monitor. If it does not answer, the call will be transferred to the other monitors in the system (if they are).

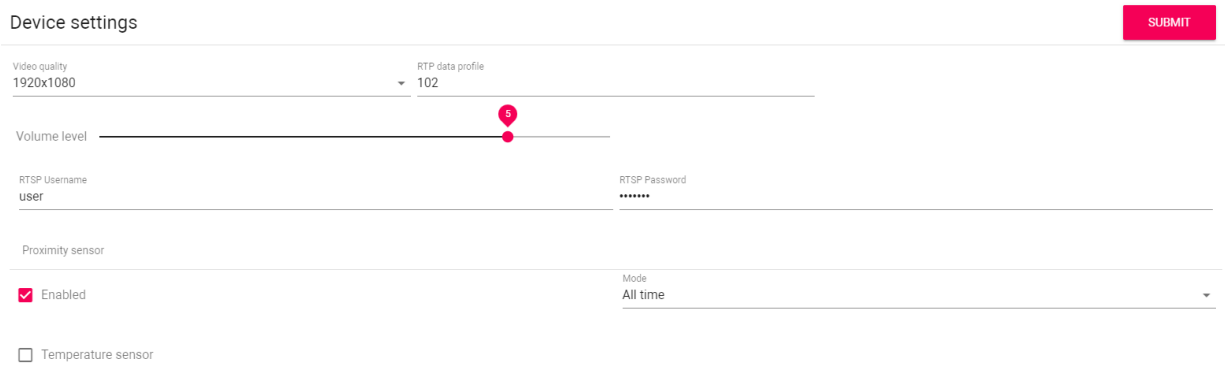
Info

Talk time for an incoming call is limited to 2 min.

3.4.4 Device settings

In this section you can:

- select preferred **video quality** (resolution) (640x480/1280x720/1920x1080 (optional));
- select preferred **RTP data profile**;
- adjusts a **volume level** of a panel speaker;
- enter **RTSP username** (login to get access to a panel RTSP stream);
- enter **RTSP password** (password to get access to a panel RTSP stream);
- enable/disable a **proximity sensor** for the panel automatic turning on the keyboard backlight and face recognition feature when motion is detected at a distance of 50 cm;
- select the appropriate proximity sensor **mode:**
    - **all time** mode: the sensor is active all time and triggered when motion is detected at a distance of 50 cm;
    - **adaptive** mode (appropriate when the panel is installed in front of a wall or an object): the sensor gets used to a constant object in front of it and does not react to it, but only triggers when there is movement;
- enable/disable connected to the panel **temperature sensor**. During an outgoing call, the panel will take the temperature of the person in front of the panel and display it on the called person internal monitor during the call/talk.



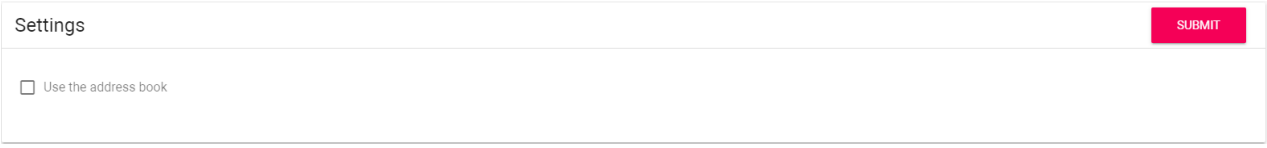
3.5 Apartments

- How to add a new apartment to the device memory(see page 20)

Here you can add, edit or look at a list of flats and get detailed information about each apartment.

An apartment is a logical entity to bind identifiers, access codes, redirection rules, and other information about residents.

Also, you can **use** apartments as **address book** entries to search and call the apartments. At this tab, you can enable/disable its display on the main screen of a multi-apartment entrance panel.

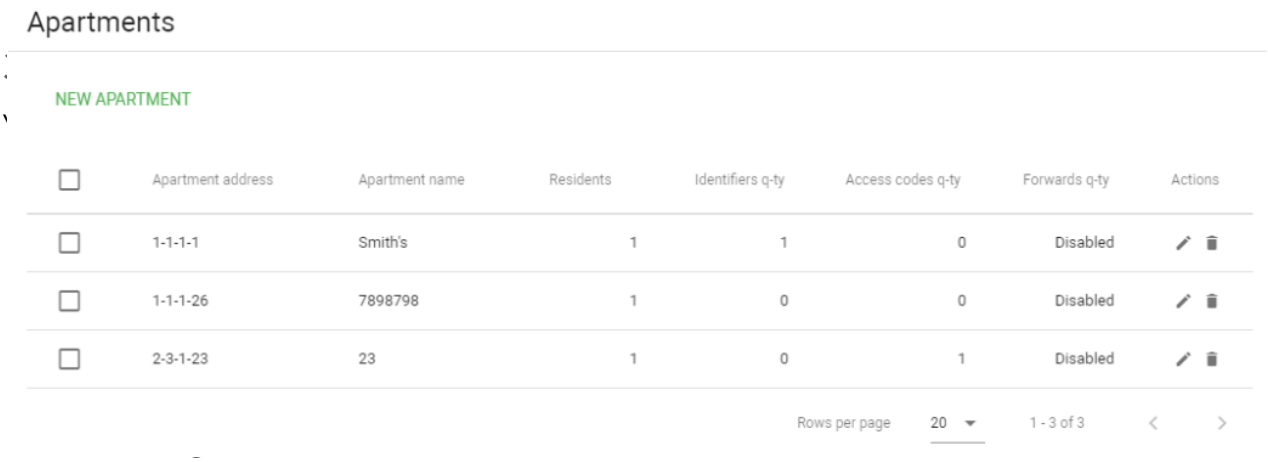


3.5.1 How to add a new apartment to the device memory

1. Log in to the device web interface. By default, the **username** is admin and the **password** is 123456.
2. Open the **Apartment** tab.
3. Click **New Apartment** and fill in the required information:
   - **building** No. (from 0001 to 9999);
   - **unit** No. (from 00 to 99);
   - **floor** No. (from 00 to 98);
   - **apartment** No. (from 01 to 99).
4. Enter an **Apartment name.** For example, Smith's.
5. Indicate the number of **residents** for this flat.
6. Confirm information to save it.

After saving the information, the apartment is added to the general table, which contains:

- apartment address;
- apartment Name;
- conditional number of inhabitants in an apartment;
- amount of identifiers that are issued to a particular apartment. Identifiers can be created in the Identifiers[16] section of the Access management tab;
- amount of access codes issued for the apartment. Access codes can be created in the Identifiers[17] section of the Access management tab (indicator is relevant for multi-apartment entrance panel);
- amount of created forward queues for the apartment. Forwardings are configured in the corresponding tab[18];
- ability to edit information or delete one or several selected apartments;



- QR recognition(see page 27)
- Exit button(see page 27)

16 https://wiki.bas-ip.com/aa07/identifiers-135955094.html
17 https://wiki.bas-ip.com/aa07/identifiers-135955094.html
18 https://wiki.bas-ip.com/aa07/forward-135955120.html

- Door sensor input(see page 28)

3.6.1 Access management

At this part, you can change information about:

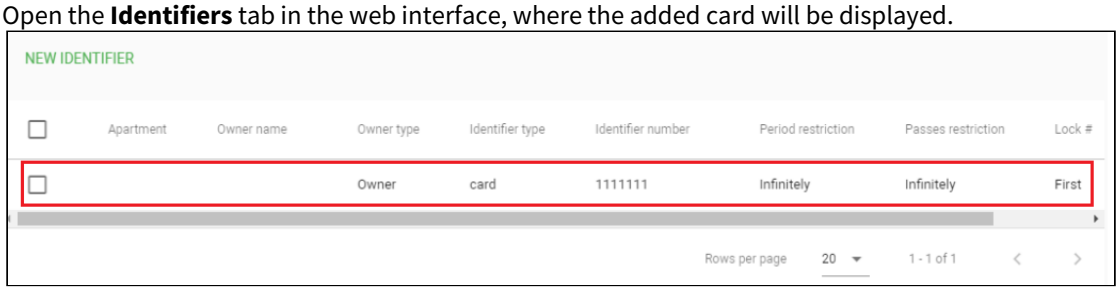
- **master card.** This card is used to add other cards to panel memory. Here you can specify the card number;

To add a master card if its number is unknown:

1. Open **Access management** tab of panel wen interface.
2. Enter **0** in the **Master card** field and submit changes.
3. Bring the card to a panel reader and wait for the BEEP signal, which means that the master card has been successfully registered.

To add a user card using the master card:

1. Bring the card to a panel reader to switch to the adding user cards mode.
2. Bring the user card to the reader. After reading the card, you will hear the BEEP signal, which means the successful registration of the card.
3. Open the **Identifiers** tab in the web interface, where the added card will be displayed.

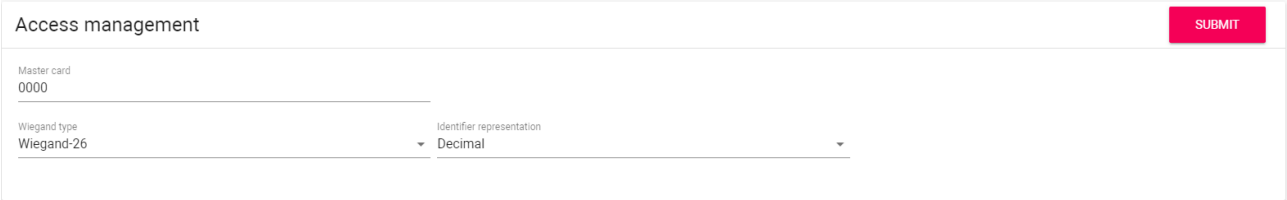


4. Add missing information about the card and save changes.

The time between adding cards must not exceed 10 seconds.

This method is convenient for mass and quick identifiers adding. But identifiers are not connected to the necessary apartment, so we recommend adding identifiers through the web interface[19].

- **wiegand type** for a card reader. Wiegand-26, Wiegand-34, and Wiegand-58 types are available for work.
- **identifier representation** systems. All identifiers can be displayed in Decimal and HEX numeral systems.



19 https://wiki.bas-ip.com/av08fb/identifiers-135956985.html

Info

Support and update of new Wiegand modes require updating the firmware of the Wiegand controller in the service center.

3.6.2 Access mode

There is a multifactor authorization feature in panel settings. In addition to the normal operation of identifiers, you can enable the mandatory use of several identifiers to open the lock/s. For example, the user must first bring the card to the reader and then show a QR code to get access.

In this section, you can enable the necessary access mode. Two options are available:

- **normal mode** is basic access by one identifier that is linked to an apartment or user;
- **global mode** activates the use of several identifiers for all added users.

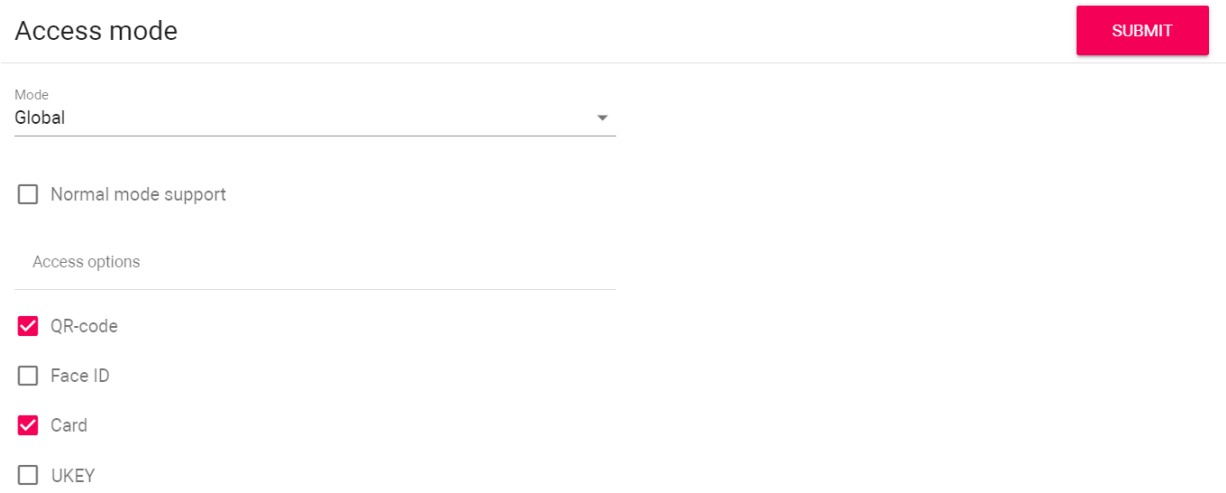
3.6.3 How to configure Global access mode

1. Log in to the device web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to **Access management** > **Access mode.**
3. Choose **Global** in Mode field.
4. Select necessary identifier types that users must use to get access: QR code, Face ID, Card, Ukey.
5. Submit settings.

Tip

It is possible to enable/disable and configure multifactor authorization parameters for concrete users in the corresponding tab.

For correct feature functioning all identifiers must be linked with users. Also you can enable **normal mode support** that allows to get access by one identifier, if it is not linked with user. So, multifactor authorization wil not work for identifiers that are not linkes with users.

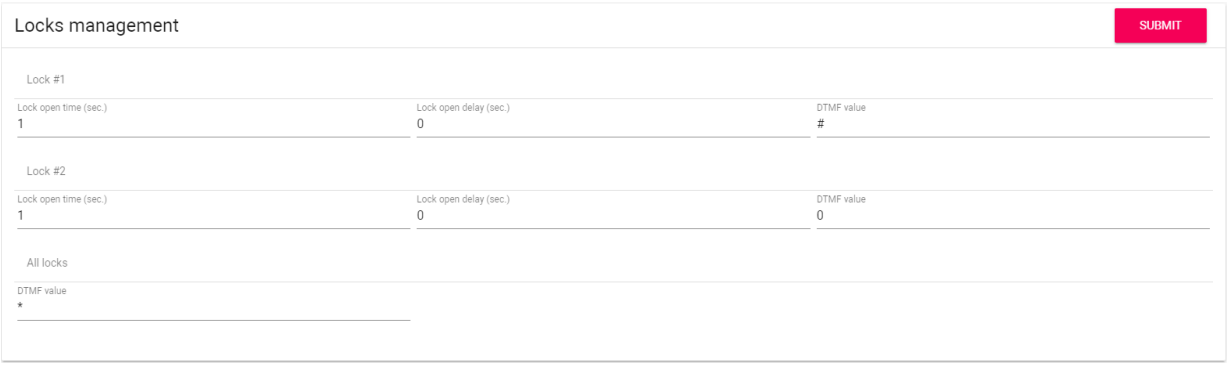


3.6.4 Locks management

At this part, you can configure the functioning of 1 or 2 (when using SH-42) locks. The following parameters can be configured:

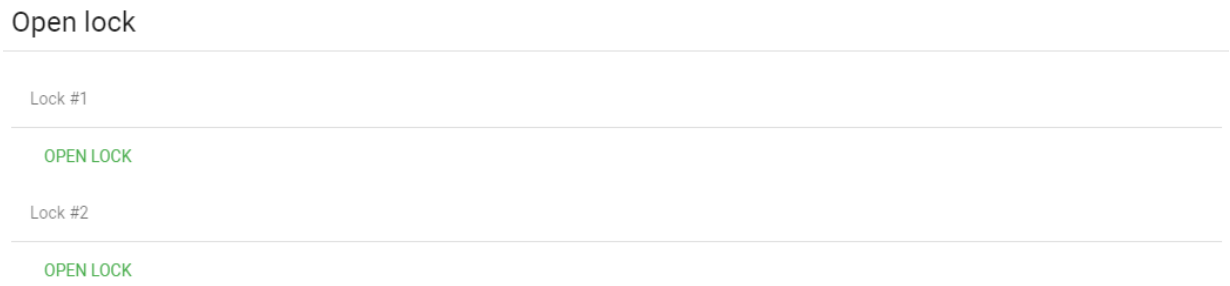
- **lock open time** is a period (1-300 sec) during which relay contacts will be closed or open (depending on the lock type), and a lock will stay open;
- **lock open delay** is a period (0-300 sec) after which relay contacts will close or open after sending a signal to open a lock;
- **DTMF value** is a code (max length - 4 characters) after entering which the lock will open. By default, all entrance panels are set to receive # to unlock the 1st lock and 0 to unlock the 2nd one;

> This feature allows you to use non-standard DTMF symbols (#, *, and 0) to open locks.
>
> This solves the problem with usage #, *, and 0 symbols for other functions by third-party devices (for example, SIP phones often use these characters to forward or put a call on hold).
>
> In case of using a private SIP server, be sure to enable the RFC2833 mode for DTMF.



3.6.5 Open lock

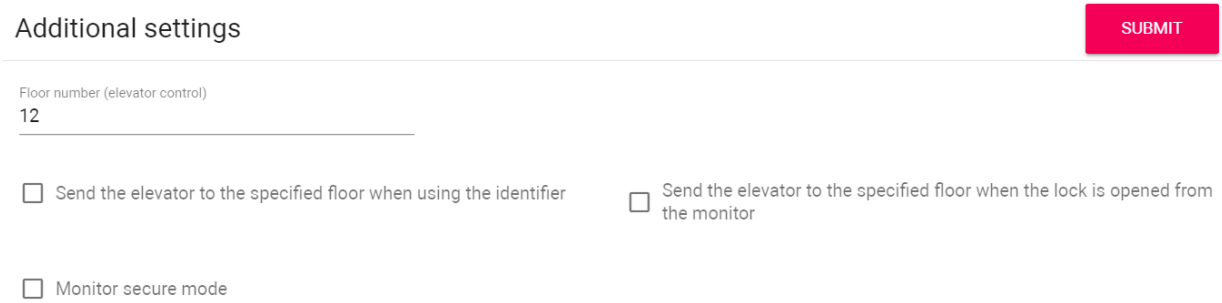
In this section, you can remotely open lock #1 or lock #2 (when using SH-42) by clicking the corresponding button.



3.6.6 Additional settings

Here you can:

- set the **Floor number** for further features that work only with the lift control module EVRC-IP[20];
- enable/disable features of **sending the elevator to the indicated floor** number **when** the lock is open **using identifier** or **from the monitor**;
- enable/disable **monitor secure mode** is a feature of alarm deactivation on an indoor monitor when bringing an identifier (that is linked with the monitor) to the panel reader.



3.6.7 External Wiegand controller

BAS-IP panel can be connected with an external controller via the Wiegand interface. In the section, you can enable/disable playing custom sound and displaying a custom text when the lock is open.

20 https://bas-ip.com/catalog/accessories/evrc-ip/

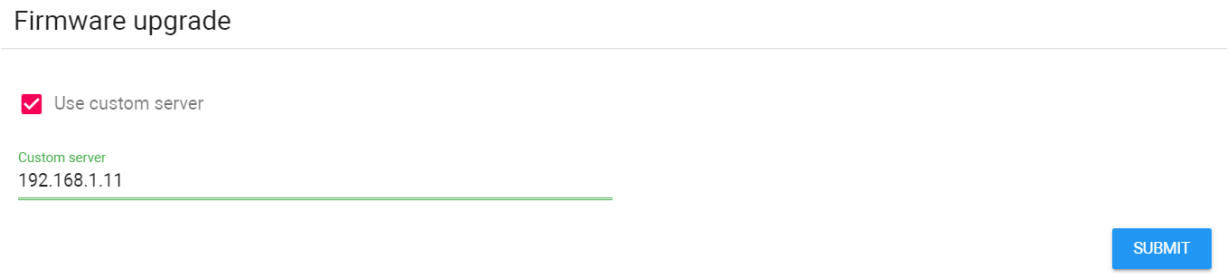
You also can customize sound notifications[21] for door opening by identifiers added to the controller.

3.6.8 Server manage access

In this section, you can enable and configure working mode when all identifiers are not stored in a panel memory but on a server. When the identifier is brought to the reader, the panel will send a request to the server and wait for a response - to give access or not.

To configure this feature you must:

1. Log in to the entrance panel web interface. By default, the **username** is admin, and the **password** is 123456.
2. Open the **Access management** tab and find the **Server manage access** section.
3. Enable the feature.
4. Click **Use custom server** and enter it. You can use Link server.
5. Submit settings.



Info

The timeout for receiving a response from the server is up to 15 seconds. After this time, the panel automatically goes to its database and gives access or not.

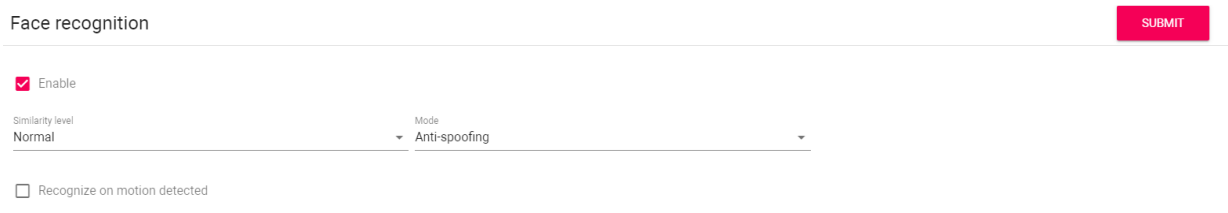
3.6.9 Face recognition

21 https://wiki.bas-ip.com/av08fb/advanced-135956991.html

Visitors faces can be used as an identifier to get access to a place. Here you can enable and configure this feature.

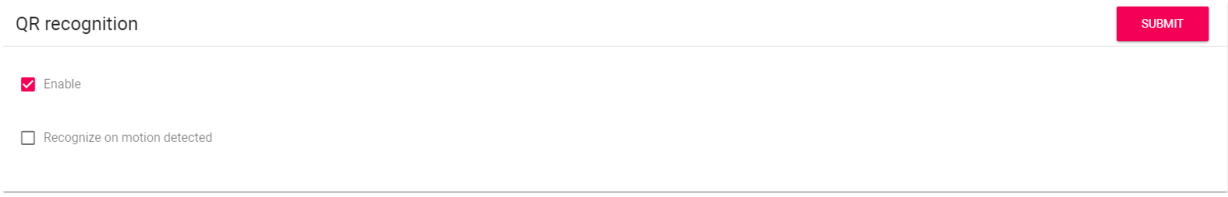
1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Open the **Access management** tab and find the **Face recognition** section.
3. Enable the feature by ticking the corresponding box.
4. Choose **similarity level** (the lower the similarity level, the greater the error can be in scanning a face and granting access):
   - **low**: the minimal similarity is necessary for access (changes in appearance (glasses, beard, presence of a hat) will not be taken into account);
   - **normal**: some changes in appearance are taken into account, but not detailed (recommended for homes and offices);
   - **high**: the maximum similarity is necessary for access (recommended for high-security places).
5. Choose the appropriate **mode**:
   - **software**: the software recognition algorithm is used, there is a possibility of giving access by photos;
   - **anti-spoofing**: more detailed software recognition algorithm is used to prevent access by photos;
   - **3D** (is available for panels with a built-in 3D sensor): detailed face recognition using IR sensors and building a face heat map to prevent spoofing.
6. Submit settings.

Also, you can turn on/off **automatic face recognition when motion is detected**. When a person approaches a panel (at a distance up to 50 cm) motion sensor becomes active, and a panel will exit standby mode and turn on the face recognition feature.



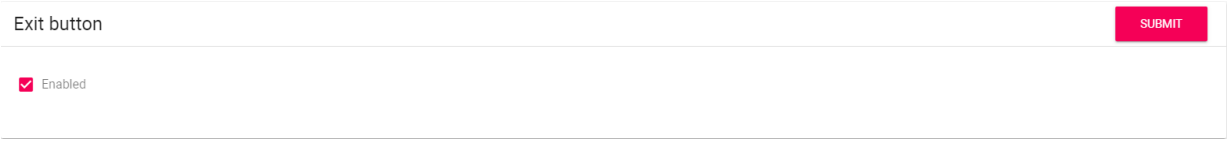
3.6.10 QR recognition

QR codes also can be used as identifiers. Here you can enable/disable **QR code recognition** in general and **when motion is detected** (at a distance up to 50 cm motion sensor becomes active, and a panel will turn on the QR recognition).



3.6.11 Exit button

You can connect a button to a panel for lock opening from the inside. At the section, it is possible to activate/deactivate an exit button.



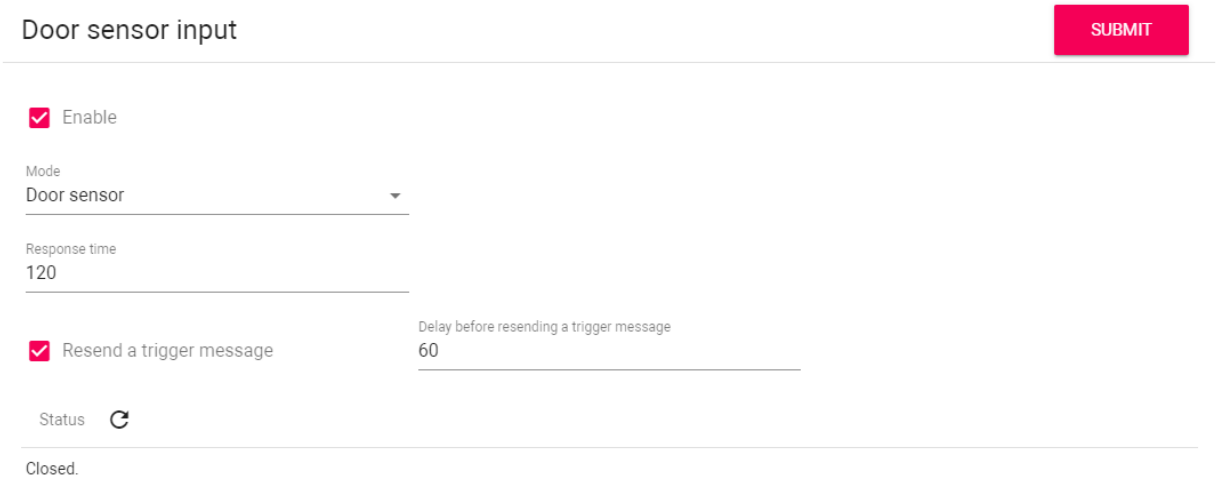
3.6.12 Door sensor input

It is possible to connect a door sensor or additional button to the door sensor input. In this section, you can enable/disable and configure their work.

After device installation and electric connection, you must do the following steps for correct work:

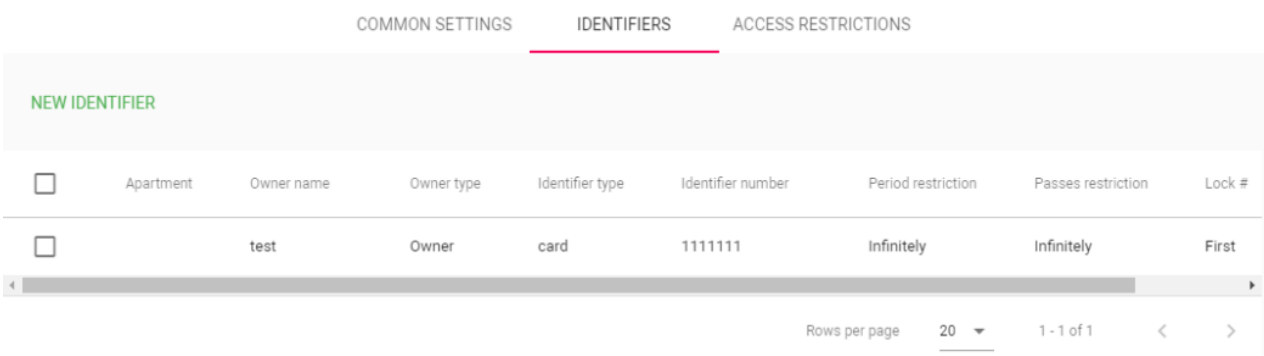
1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Open the **Access management** tab and find the **Door sensor input** section.
3. Enable sensor or button functioning by ticking the corresponding box.
4. Choose the appropriate **input mode**:
   - **door sensor** mode is used to monitor the door state. If the door is not closed, after the expiration of the response time in Logs/Syslog/Link logs/Email notifications will be shown that the door is open;
   - **door entry button** mode is recommended when the connected button is used as an additional, remote from the panel, entry button;
   - **concierge call** mode is appropriate when the connected button is used to call the concierge using the internal protocol.
5. Set the **Response time** after which the mode will be activated.
6. For Door sensor and Door entry button modes, you can enable the option to **resend a trigger message** to Logs/Syslog/Link logs/Email notifications and set the delay time before resending.
7. Submit settings.

Also, you can check and update the current door sensor input **status** (open/closed).



3.6.13 Identifiers

Here you can add or view a table with previously added identifiers. This table contains information about the identifier owner, its type, number, validity period, amount of available passes, and the number of the lock that identifiers are allowed to open.



There is an option of everyday automatic deletion of guest identifiers that expired a week ago.

3.6.13.1 How to add a new identifier to a panel memory

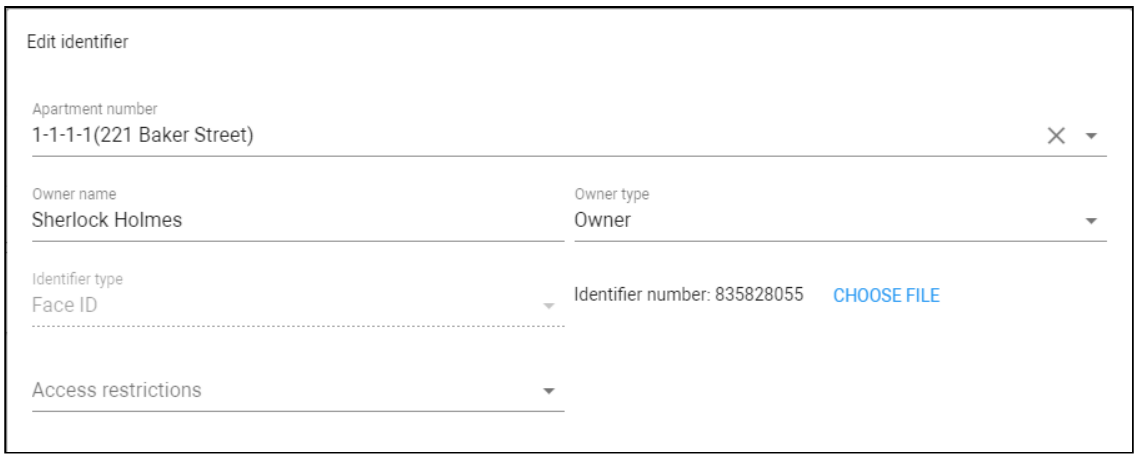
1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to **Access management** > **Identifiers**.
3. Click **New Identifier**.

4. Enter all required information in the opened window:

- choose an **Apartment number** from the previously created list in the corresponding tab[22];
- **Owner name**;
- **Owner type**: Guest or Owner;
- **Identifier type** and number;

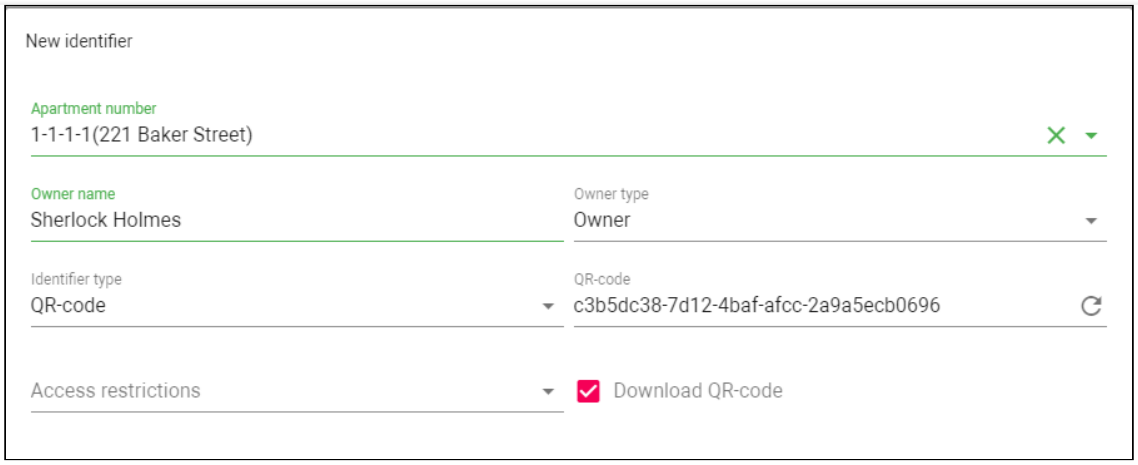
5 identifiers types are available:

- **card**: EM-Marin or Mifare card. In the **Identifier number** field, you must enter a card number in decimal format, without commas. Usually, the number is printed on the card in decimal or hexadecimal format. You can use this link[23]to convert a value from one to another system. Also, you can bring the card to a panel reader, and the number will be displayed in this tab or Logs, from where it can be copied;
- **UKEY** allows using smartphones as identifiers (BAS-IP UKEY[24] app is required). You must enter the identifier number in the **Identifier number** field. UKEY number can be found on the purchased QR code. If it is lost, bring the phone to a reader and the number will be displayed in the Logs, from where it can be copied into this field;
- **access code** that must be entered on the panel keypad to open lock/s. In the **Access Code** field, you must indicate a numeric code (no more than 30 characters) that will be used as a user identifier;
- **face ID** (available for devices with FB abbreviation) allows opening the lock by scanning visitors faces. When adding this identifier type, you must upload a vertical or horizontal user photo, that will be converted into a hash. Further, this hash will be used to verify visitors;

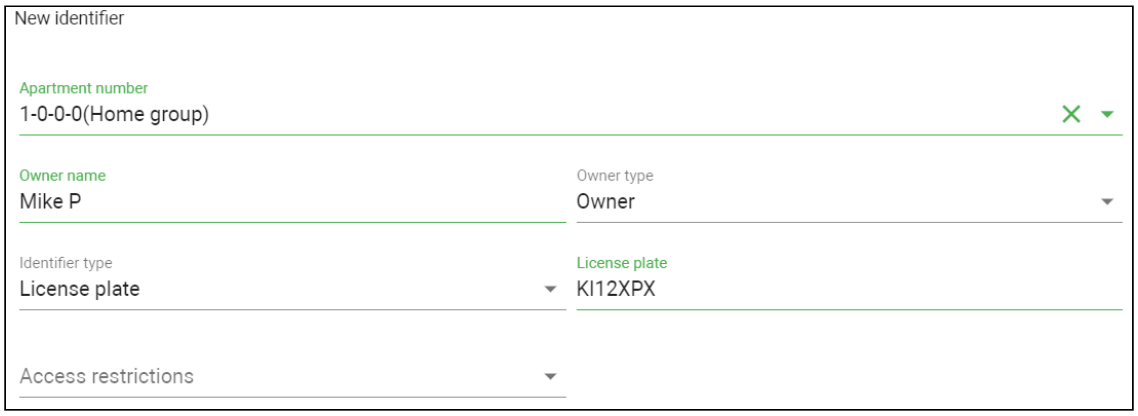


- **QR code:** The automatically generated QR must be downloaded from the web interface and uploaded to a mobile device for further use;

22 https://wiki.bas-ip.com/aa07fben/apartments-135955225.html
23 https://www.binaryhexconverter.com/hex-to-decimal-converter
24 https://bas-ip.com/catalog/soft/bas-ip-ukey/



- **license plates** can be added and used to open lock/s. In the **License plates** field, you must enter the plate number. For this identifier to work, you need an Axis camera[25] with ALPR option for plate scanning and installed AXIS License Plate Verifier software to send a number to the panel (detailed instructions about configuration are given below). In a case of a guest ID, you can create several identifiers with one license plate number.



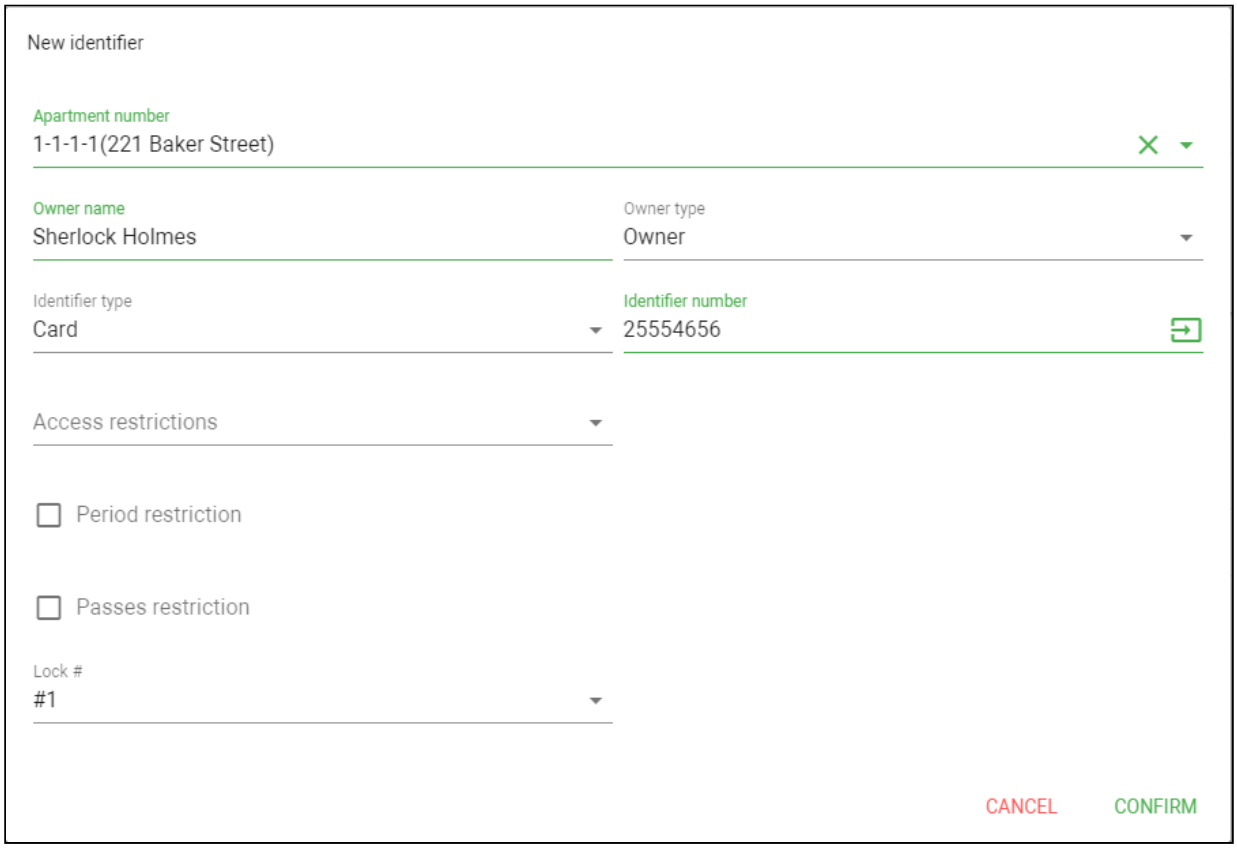
For accurate recognition, it is necessary to import a full-face photo, where the face occupies about 80% of the space. The image must be:

- in .jpeg format;
- with a resolution of at least 320x240px and no more than 5120×2700px;
- with a neutral background;
- with a well-lit face;
- with real face proportions.

- choose **Access restrictions** (when access is allowed for the identifier) from the previously created list in the corresponding tab[26] (optional);

25 https://www.axis.com/solutions/license-plate-recognition
26 https://wiki.bas-ip.com/aa07fben/access-restrictions-135955252.html

- set **Period restrictions** for identifier validity (optional);
- set Passes **restrictions** (optional);
- set **Lock #** that is allowed to open for the identifier (#1, #2 (if SH-42[27] is used) or both);



6. Confirm the information.

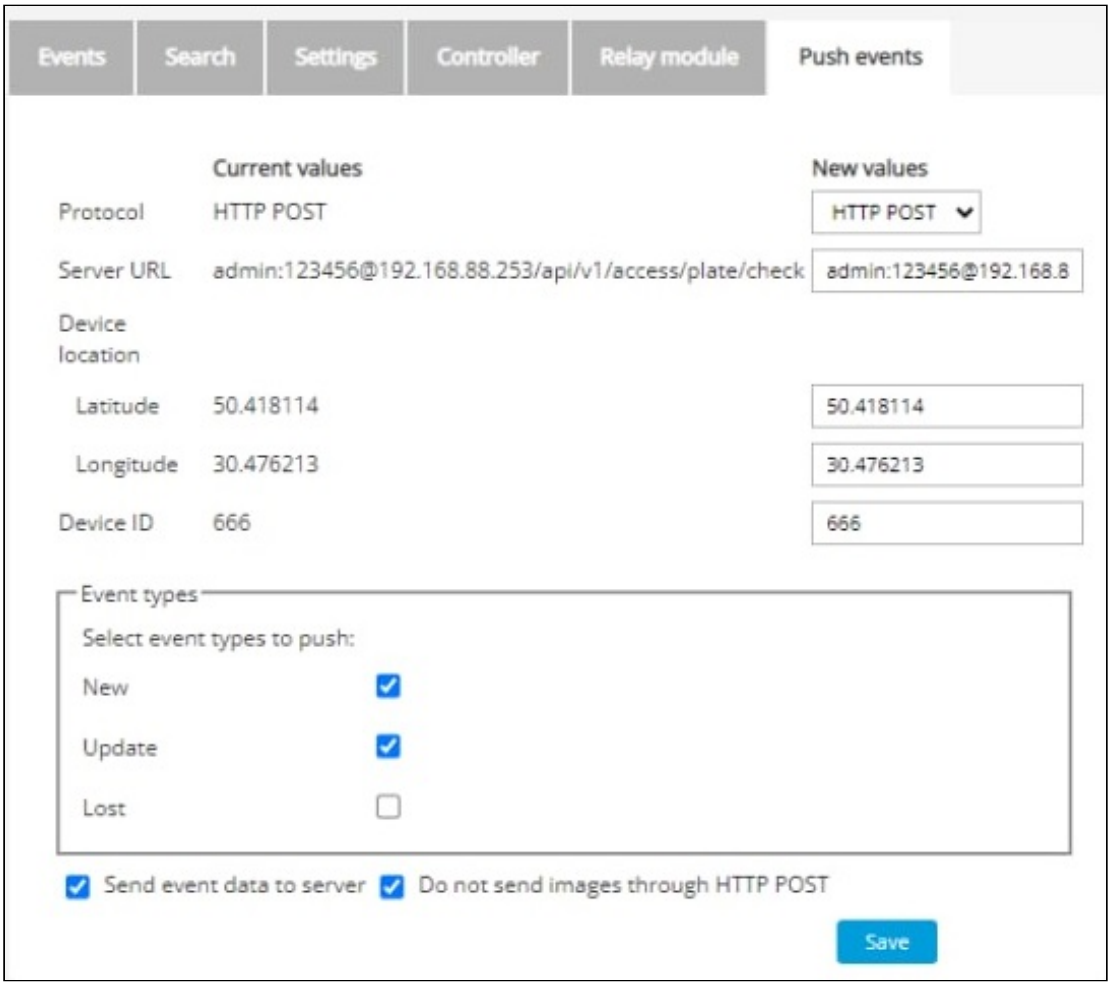
If necessary, you can edit/delete added identifiers.

3.6.13.2 How to configure License plates use as an identifier

1. For this identifier to work, you need an installed Axis camera[28] with ALPR option and **Axis License Plate Verifier** software. Detailed information about software and its installation you can find on the Axis website.
2. In AXIS License Plate Verifier, select HTTP Post protocol.
3. Enter **the server URL** that consists of the panel username and password, panel IP address, and API endpoint, where the camera will send the recognized number. For example, **admin:123456@192.168.1.178/api/v1/access/plate/check**, where the username is admin, the user password is 123456, and 192.168.1.178 is panel IP.
4. Save AXIS License Plate Verifier settings.
5. Open panel web interface. By default, the **username** is admin and the **password** is 123456.
6. Go to **Access management** > **Identifiers**.
7. Add license plate number as identifier.

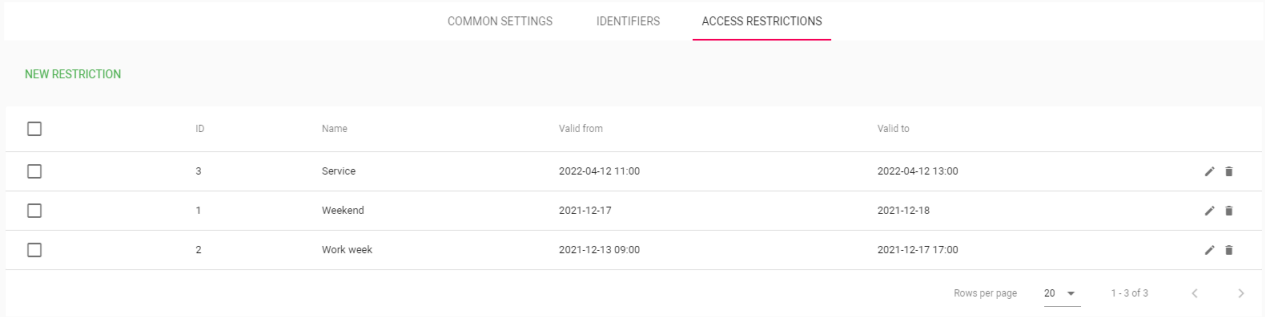
After these actions added license plate number will be recognized by the camera, and access will be provided for 10 sec.

27 https://bas-ip.com/catalog/accessories/bas-ip-sh-42/
28 https://www.axis.com/solutions/license-plate-recognition



3.6.14 Access restrictions

In this menu, you can set the access restrictions according to which the access peculiarities of various users and their identifiers are determined. For example, you can create a restriction that will provide access at a chosen time or day and apply it to necessary identifiers.

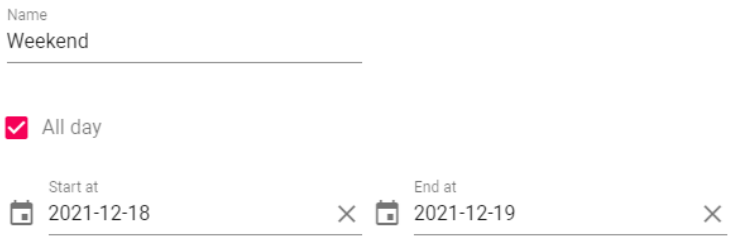


3.6.14.1 How to add a new restriction

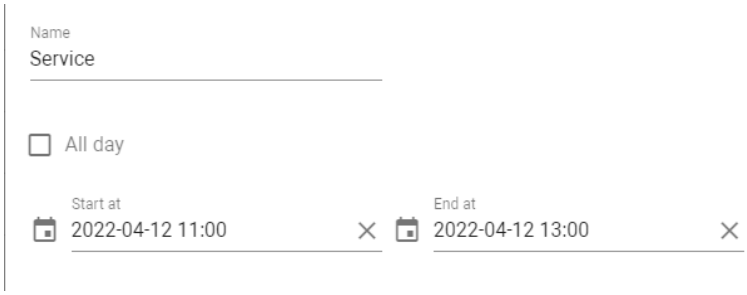
1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to **Access management** > **Access Restrictions.**
3. Click **New Restriction** and enter all required information:

- restriction **Name**;
- date of restriction **start** and **end;**

There are two options for a period indicating:
- **all day**: you are required to specify only the date (day/month/year) of the beginning and end of this rule;



- if the **All day** option is disabled, you must specify the date (day/month/year) and set the start and end time of this restriction.

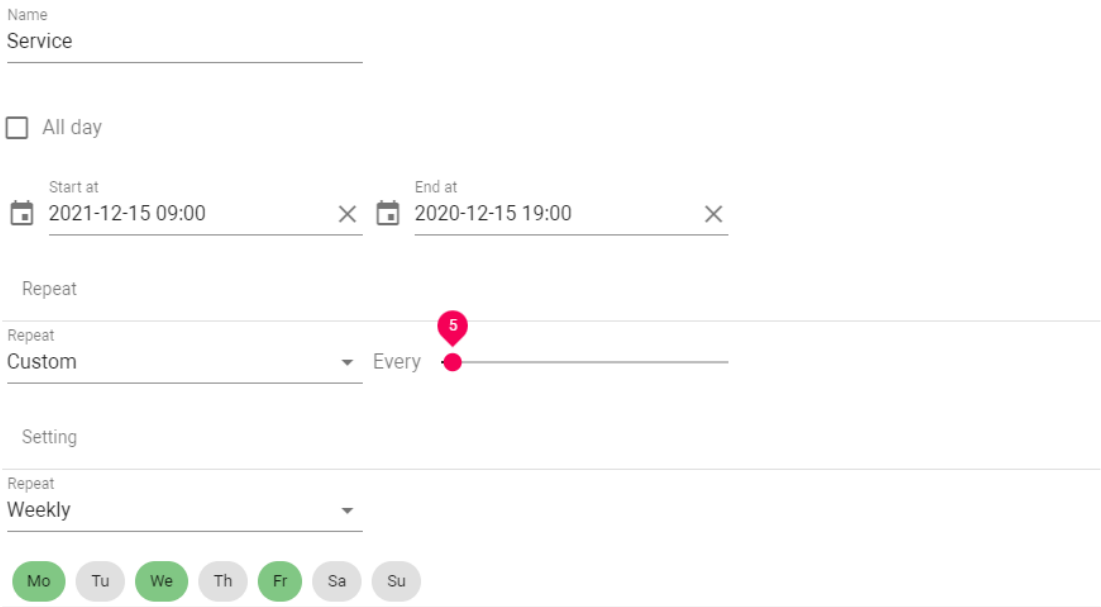


- frequency of **repetitions**;

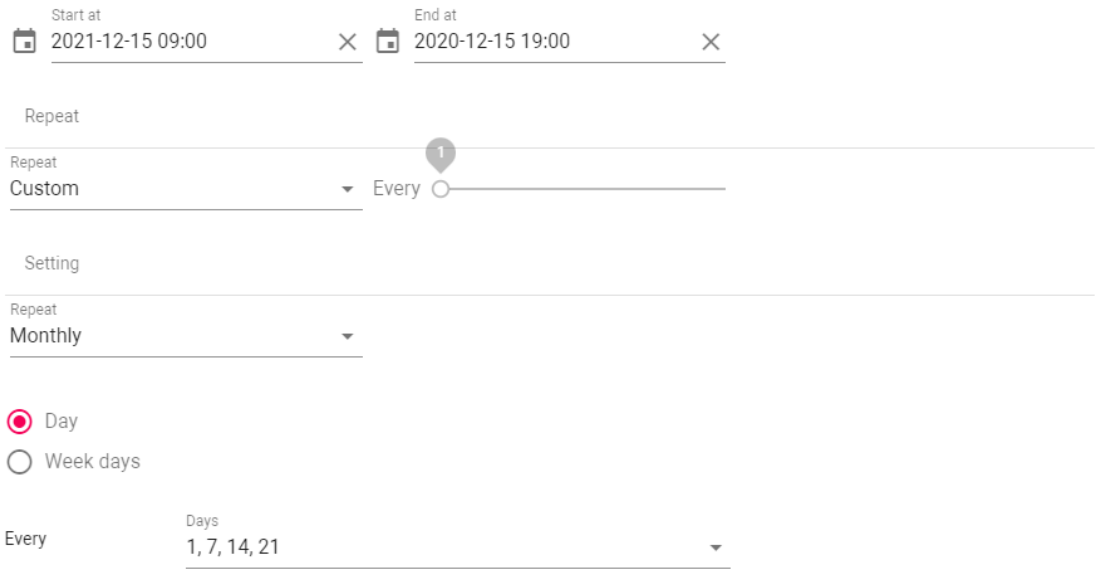
Available options are:

- **daily**: the restriction will be active every day for a specified time period. For example, the identifier will work every day from 9:00-18:00;
- **weekly**: the restriction will work on the specified days and hours, e.g., every Tuesday or every Monday and Friday (depending on settings);

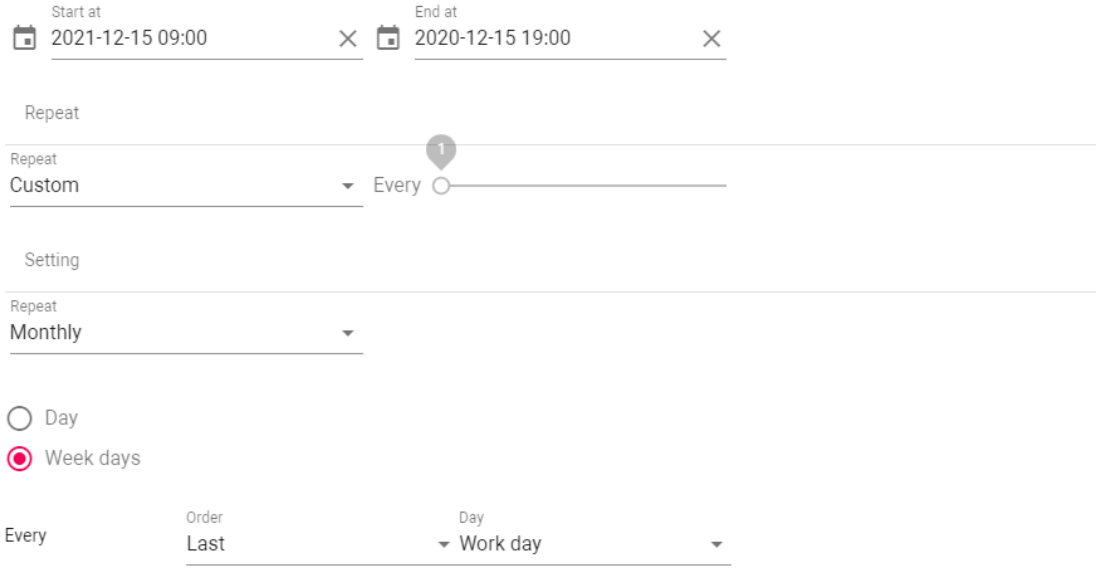
- **every 2 weeks**: the restriction will repeat every two weeks on the specified days. For example, if you create a restriction that works from Monday to Wednesday, then the identifier will be active from Monday to Wednesday with 2 weeks intervals;
- **monthly**: the restriction will be active every month, e.g., every 15th day of the month;
- **yearly**: the restriction will repeat every year, e.g., every 15th of December;
- **custom**: you can set the necessary dates, days, and months for restriction repetition:
    - **daily**: the restriction will be active every day for a specified time period. In **Every** column, you can indicate after how many days the restriction will be activated again, e.g., every 5th day.
    - **weekly**: you can configure restriction repetition on specific days of the week. In **Every** column, you can indicate after how many weeks the restriction will be activated again. According to the screen, the identifiers linked with the restriction will work from 9:00-19:00 on Mondays, Wednesdays, and Fridays every 5 weeks.



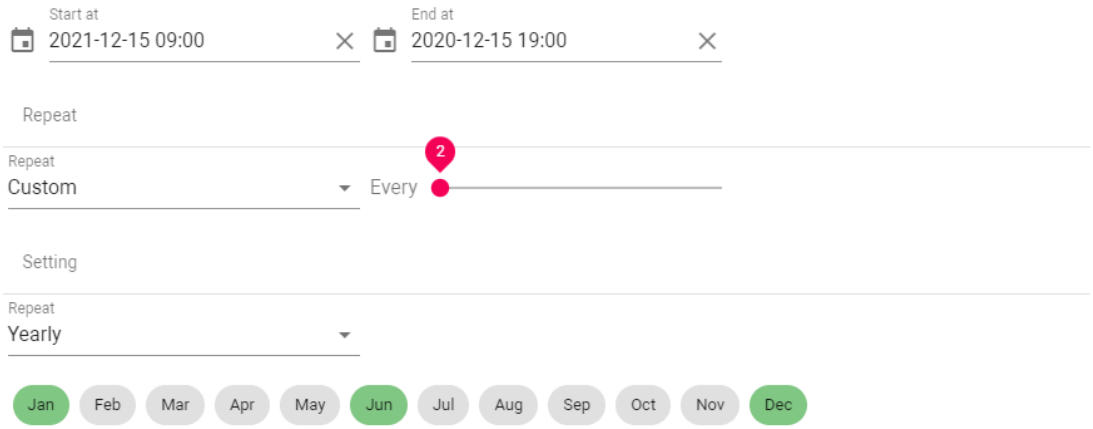
- **monthly**: you can configure restriction repetition on specific dates each month. According to the screen, the identifiers linked with the restriction will work from 9:00-19:00 every 1st, 7th, 14th, and 21st day of the month. In **Every** column, you can indicate after how many months the restriction will be activated again, e.g., every 7th month.



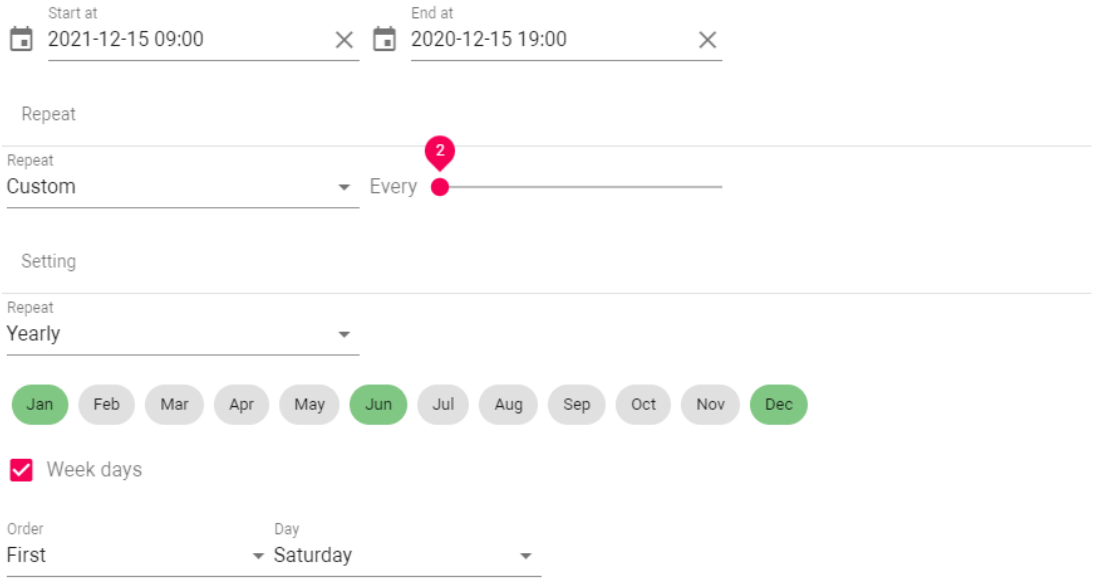
Also, it is available to configure restriction repetition every month on the first/second/third/fourth/fifth/last specific day of the week, e.g., on the first Tuesday of every month. According to the following image, the identifiers linked with the restriction will work from 9:00-19:00 every last working day of the month.



- **yearly**: you can configure restriction repetition in a specific month of a year. In **Every** column, you can indicate after how many years the restriction will be activated again, e.g., every 3 years. According to the screen, the identifiers linked with the restriction will work from 9:00-19:00 every 15th of January, June, and December with 2 years frequency.



Also, it is available to configure restriction repetition every year on the first/second/third/fourth/fifth/last specific weekday of chosen months, e.g., the first Tuesday of January. According to the following image, the identifiers linked with the restriction will work from 9:00-19:00 every first Saturday of January, June, and December with a 2 years frequency.

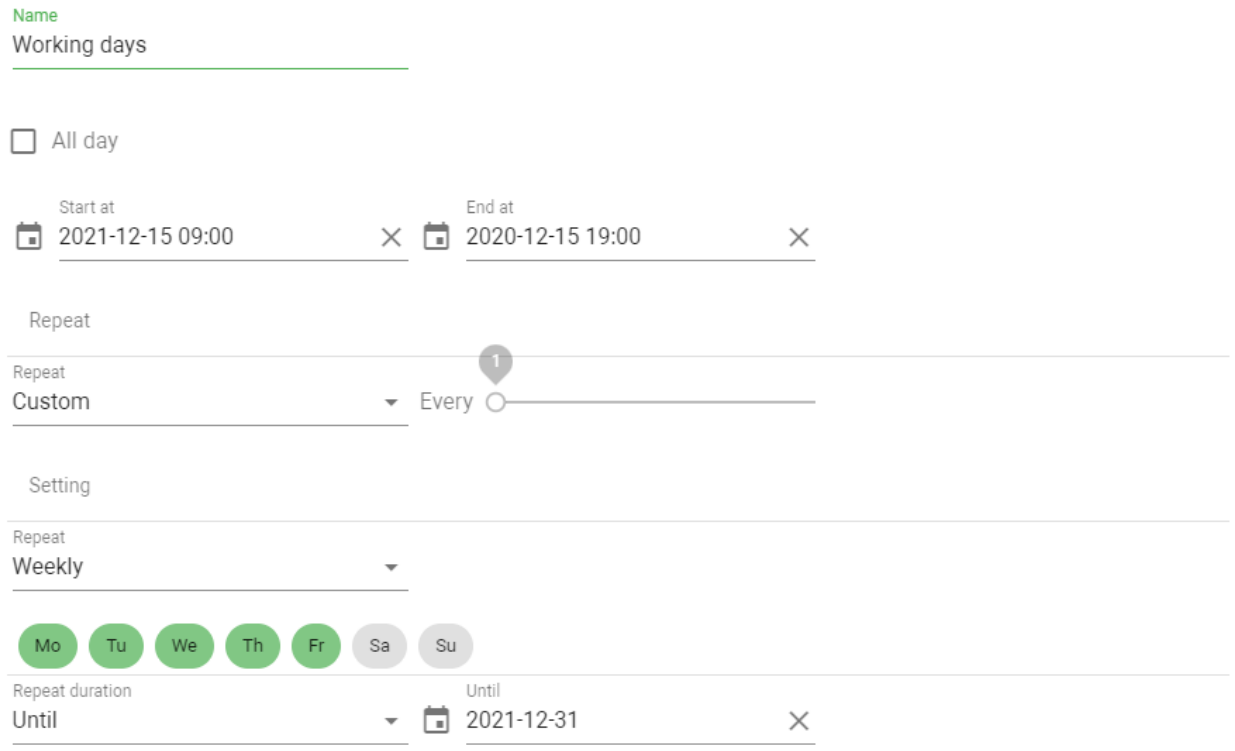


- **repeat duration** of restriction;

Two parameters are available:

- **infinitely**: a restriction will always work;
- **until**: a restriction will be active until the indicated date.

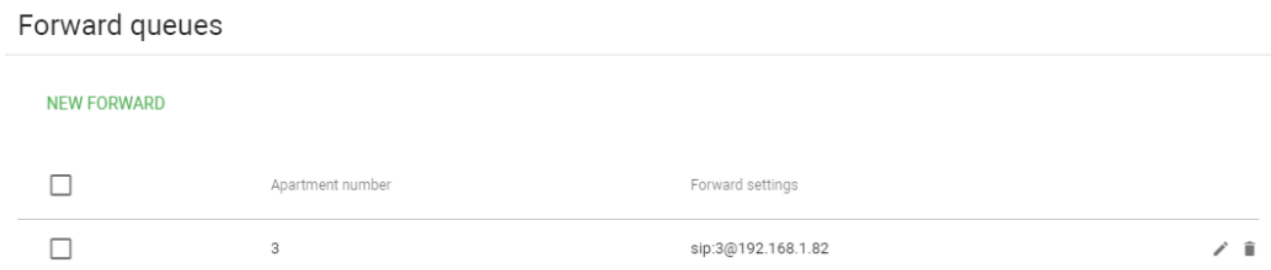
4. Confirm settings.



3.7 Forward

To make a call between a panel and an indoor video entry phone (monitor) by pressing the button of the required apartment or entering its number, the panel and the monitor must have the same building and unit number in apartment settings. Also for monitors, you must indicate corresponding information about the floor, apartment, and device number.

If there is no monitor, it is turned off or such settings are missing, you must make forward queues for apartments to redirect calls to IP addresses or SIP numbers.



3.7.1 Forward settings

Two forwarding modes are available:

- **all at once**: the call is made to all numbers simultaneously.
- **one by one**: the call is made to the numbers in turn with a 20 seconds delay.

3.7.2 How to make a new forward queue

1. Log in to the entrance panel web interface. By default, the **username** is admin, the **password** is 123456.
2. Open the **Forward** tab and click **New Forward**.
3. Enter your **Apartment Number** which consists of the floor and room number. For example, 223 indicates apartment 23 located on the 2nd floor. Entering this number on the panel the queue will work.
4. Enter **Forward Number** (directions for call forwarding). You can add up to 8 numbers for forwarding. Calls can be made both via P2P and via the SIP protocol.

Format for calls via P2P:

Two formats for numbers are available:

- **sip:1@192.168.1.65**, where 1 is the desired number to be displayed for the callee, 192.168.1.65 is the IP address of the callee SIP client (if you use a softphone, the IP address of a device where the softphone is installed);
- **sip:192.168.1.65,** where 192.168.1.65 is the IP address of the callee SIP client (if you use a softphone, the IP address of a device where the softphone is installed).

Format for calls to **SP-02** is:

- **sip:192.168.1.99**, where 192.168.1.99 is the IP address of the callee handset.

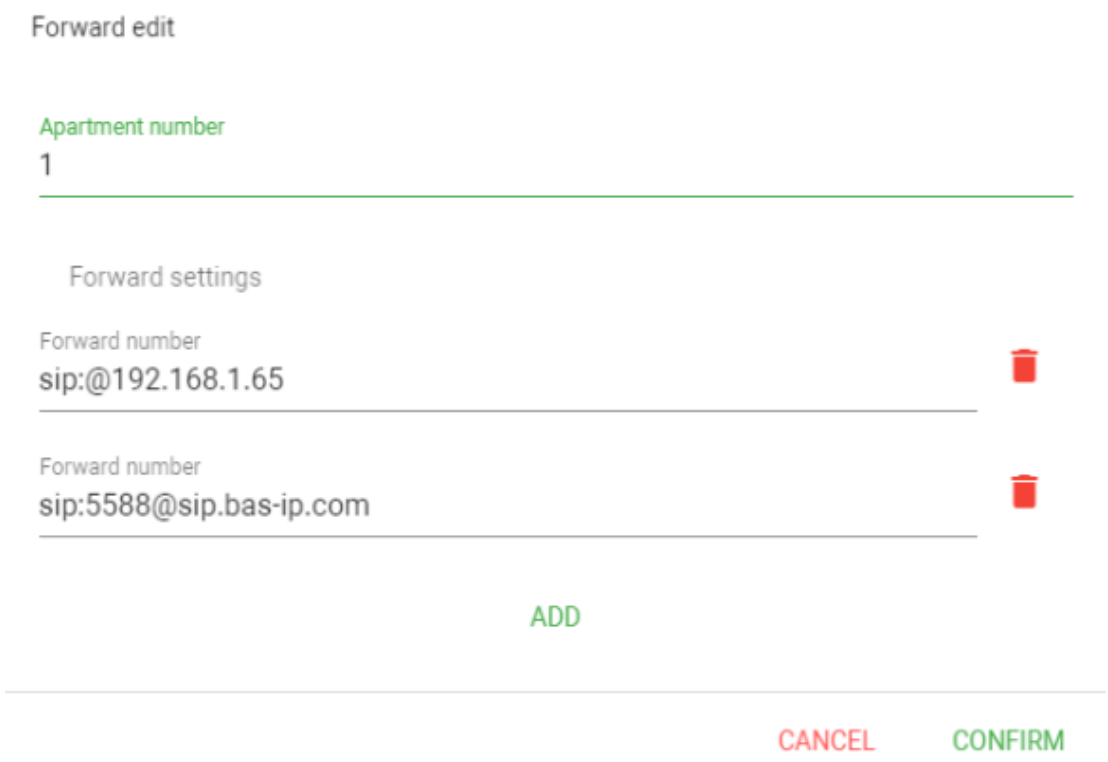
Format for calls via SIP:

- **sip:5588**@us.sip.bas-ip.com[29], where 5588 is the callee SIP number, us.sip.bas-ip.com[30] is the address of the SIP server, which can be either the IP address or domain name.

You can also use the short form and enter only the callee SIP number of the called device ("sip:" at the beginning and the SIP server address can be skipped). So, it is enough to enter 5588.

For the forwarding correct function, the SIP numbers in one queue must be registered on the same SIP server. For example, forwarding will work for your SIP numbers registered on the us.sip.bas-ip.com[31] server.

5. Save the forward queue by clicking **Confirm**.



Tip

Forwarding will work correctly even if numbers for both P2P and SIP calls are entered in the same queue.

29 mailto:2255@sip.bas-ip.com
30 http://us.sip.bas-ip.com
31 http://us.sip.bas-ip.com

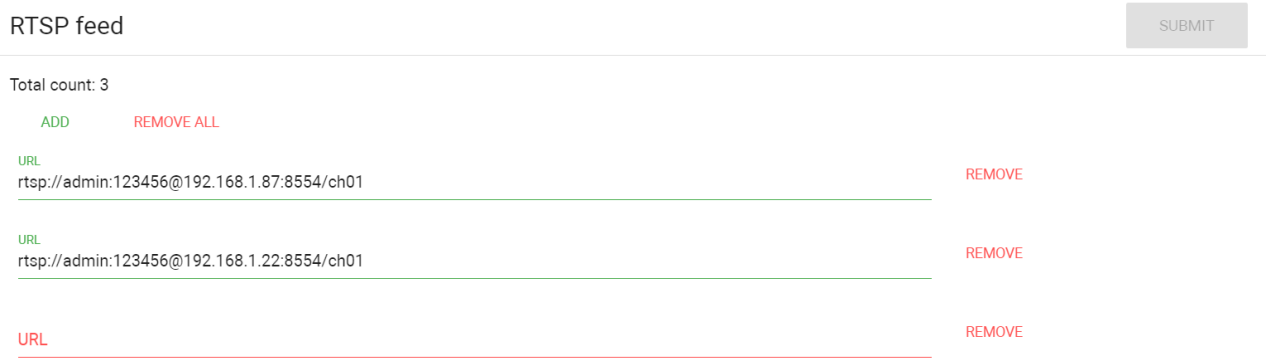
3.8 Advanced

In this section, you can add an RTSP stream to view additional cameras and set up custom notifications.

3.8.1 RTSP Feed

By entering RTSP streams (up to 4) in this section, you can view images from third-party IP cameras on a monitor during a call from an entrance panel. The feature is available for v4 monitors and other SIP devices with a keyboard.

1. Generate an RTSP stream of the camera according to its manual.
2. Log in to the device web interface. By default, the **username** is admin and the **password** is 123456.
3. Open the **Advanced** tab.
4. Enter generated at 1st step URL at **RTSP feed** field. You can add up to 4 RTSP streams.
5. Save settings by clicking **Submit.**



Tip

Example of the URL for RTSP stream:

rtsp://admin:123456@192.168.1.178:8554/ch01. It includes the username (admin), user password (123456), 192.168.1.178 - panel IP; 8554 - number of a camera access port; ch01 - channel number.

Info

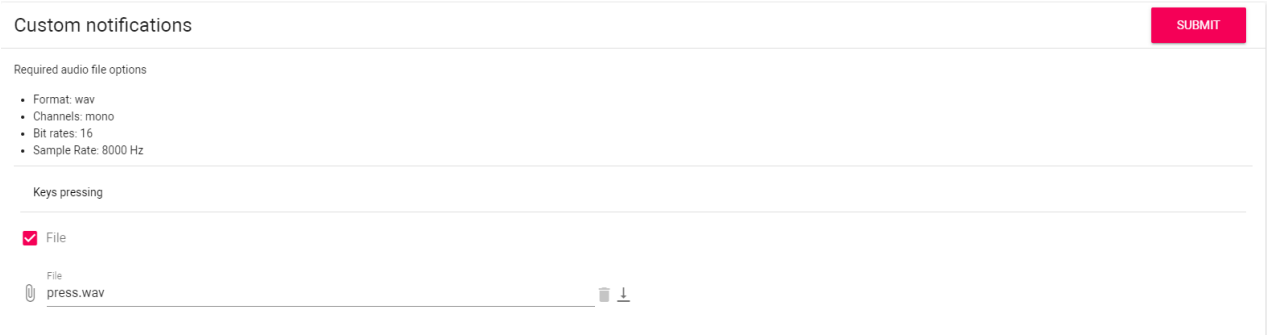
During a call from an entrance panel, open the keyboard and switch between cameras by pressing 1-5 buttons (1 is the entrance panel camera, 2-5 are additional cameras).

3.8.2 Custom notifications

You can use both standard sounds and upload your own sounds for keys pressing, ring back, door unlocking, errors or door unlocking if the external Wiegand controller is connected.

3.8.3 How to set custom sound notification

1. Log in to the device web interface. By default, the **username** is admin and the **password** is 123456.
2. Open the **Advanced** tab and scroll to the **Custom notifications** section.
3. Choose what event sound you want to change: **Keys pressing, Ring back, Door unlock, Errors, External Wiegand controller** (relevant parameter only if the panel is connected to the external controller via Wiegand. The sound is produced when the lock is opened by an identifier added to the external controller).
4. Tick **File** and upload audio with .wav extension. If the **File** box is disabled, a standard sound will be used.
5. Submit settings.



Info

Audio file requirements:

- Format: .wav
- Channels: mono
- Bit rates: 16
- Sample Rate: 8000 Hz

3.9 Logs

This tab contains a log that displays all the events that happened with the panel: login to the web interface, lock opening using an identifier, to or from which number a call was made, etc. Log is cleared every 182 days.

Log

FILTERS

Date/time	Category	Priority	Event	Info
1970-01-02 07:22:29	System	Medium	Login to the web interface	Successful (admin) login to the web interface
1970-01-02 07:05:36	System	Medium	Login to the web interface	Successful (admin) login to the web interface
1970-01-02 03:58:21	Access	Medium	Lock opened by response device	Lock 2 opened while talking to sip:1010113@192.168.0.51
1970-01-02 03:57:38	Info	Medium	Outgoing call	Outgoing call to number sip:1010113@192.168.0.51, call was accepted
1970-01-02 03:56:59	Info	Medium	Outgoing call	Outgoing call to number sip:1010113@192.168.0.51, call was accepted
1970-01-02 03:56:15	Info	Medium	Incoming call	The incoming call from the number 1010113@192.168.0.51 is completed, the call was accepted
1970-01-02 03:50:50	System	Medium	Login to the web interface	Successful (admin) login to the web interface
1970-01-02 03:45:17	Access	Medium	General access code entered	
1970-01-02 03:45:09	Access	High	Wrong input code	Invalid access code 0000 entered
1970-01-02 03:14:11	System	Medium	Login to the web interface	Successful (admin) login to the web interface

List of all events displayed in the log:

Priority	Category	Event
Low	Information	Device Booted
	System	SIP registration lost
Medium	Access	Door was opened
	Access	Door was closed
	Access	Lock opened by free access button
	Access	Lock opened by exit button
	Access	Lock opened by identifier
	Access	General access code entered
	Access	Lock opened by face identifier
	Access	The lock is open on alarm
	Access	Door sensor opened
	Access	Door sensor closed
	System	Login to the web interface

Priority	Category	Event
	System	Failed login attempt to the GUI settings
	System	Entered to GUI settings
	Information	Incoming call
	Information	Outgoing call
	Information	Outgoing call from web
	Information	Missed outgoing call
High	Access	Access denied by remote server
	Access	Access granted by remote server
	Access	Wrong input code
	Access	Unknown identifier
	Access	Not valid face identifier
	Access	Unknown QR code
	Access	Access granted by the web interface
	Access	Access denied by the web interface
	Access	Lock opened by response device
	Access	Not valid identifier
	Emergency	Tamper triggered
	System	Failed login attempt to the web interface
Critical	Access	Door is not closed too long

You can sort events by date from most recent to oldest and vice versa. To do this, click the **Date/Time** column.

Log

FILTERS

Date/time	Category	Priority	Event	Info
1970-01-02 07:22:29	System	Medium	Login to the web interface	Successful (admin) login to the web interface
1970-01-02 07:05:36	System	Medium	Login to the web interface	Successful (admin) login to the web interface
1970-01-02 03:58:21	Access	Medium	Lock opened by response device	Lock 2 opened while talking to sip:1010113@192.168.0.51
1970-01-02 03:57:38	Info	Medium	Outgoing call	Outgoing call to number sip:1010113@192.168.0.51, call was accepted
1970-01-02 03:56:59	Info	Medium	Outgoing call	Outgoing call to number sip:1010113@192.168.0.51, call was accepted
1970-01-02 03:56:15	Info	Medium	Incoming call	The incoming call from the number 1010113@192.168.0.51 is completed, the call was accepted
1970-01-02 03:50:50	System	Medium	Login to the web interface	Successful (admin) login to the web interface
1970-01-02 03:45:17	Access	Medium	General access code entered	
1970-01-02 03:45:09	Access	High	Wrong input code	Invalid access code 0000 entered
1970-01-02 03:14:11	System	Medium	Login to the web interface	Successful (admin) login to the web interface

Also, there is a filter by date and parameters, with the help of which you can configure a flexible data display and quick search. To do this, you need to click the **Filters** button and set the necessary parameters:

- in the **Column** line, select the search parameter:
  - **priority**: display of events with selected low/critical/medium/high priority;
  - **category**: display of events with the selected category (emergency, access, system, information);
  - **name**: display of events from previous tables by their names;

- choose search **condition**:
  - **more** (available for priority parameter): display of events that are higher in priority than selected. So, if you select **more** than low, then you will see events with critical/medium/high priority;
  - **less** (available for priority parameter): display of events that are lower in priority than selected. So, if you select **less** than medium, then you will see events with low priority;
  - **equal** (available for all parameters): display of events by a selected parameter. So, if you select events equal to low priority, you will see all Device Booted and SIP registration lost events;
- choose **Value** depending on the selected column.

3.9.1 E-mail notifications

There is a feature of sending notifications to the concrete email about activated events (from logs). Here you can enable/disable and set the feature.

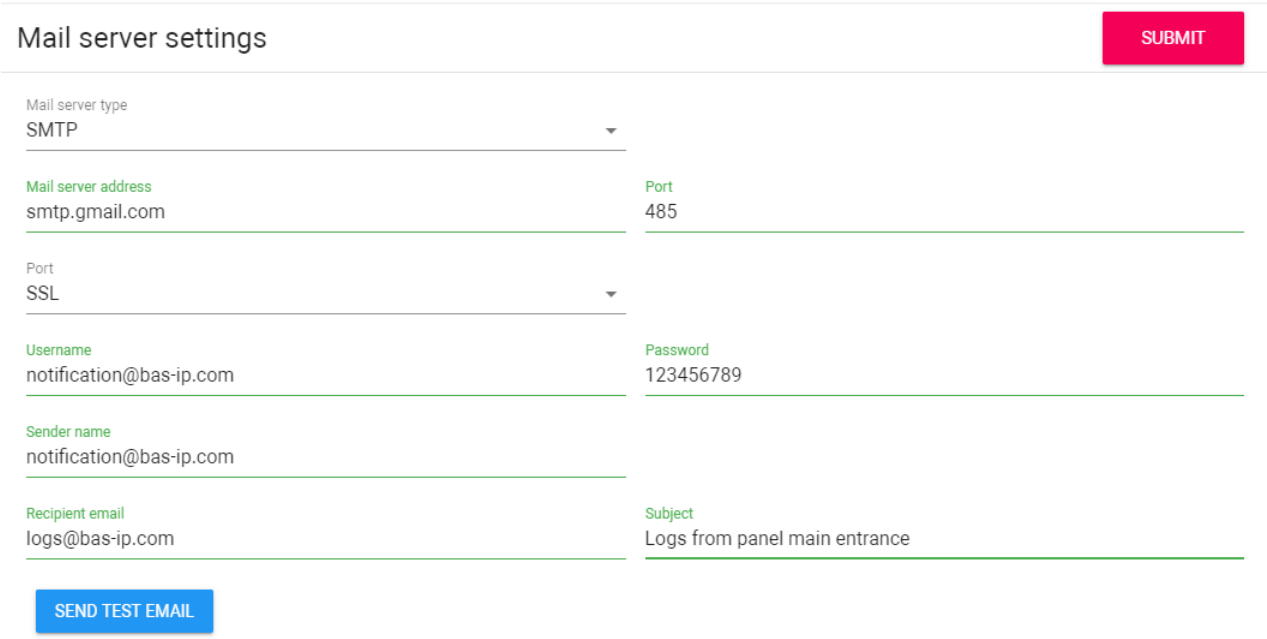
3.9.1.1 Mail server settings

For the email notifications to function, you need to enable the feature and enter the mail server settings:

1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to **Logs** > **Email notifications.**
3. For the **Mail server type** field choose **SMTP** (outgoing mail server).
4. Enter the required data:
   - **mail server address**;
   - **mail server port number;**
   - preferred **encryption type**: SSL or TLS;
   - SMTP server **username** (sender email address);
   - sender email address **password**;
   - **sender name** that will be indicated in letters;
   - recipient email;
   - letter **subject** that will be shown as email title.
5. Submit settings.

Info

You can find the **mail server (SMTP) address** and used **port number** in the official documentation of the mail service you use to send/receive emails (Gmail, Yahoo!, etc.)



3.9.1.2 How to configure email notifications feature

1. Log in to the entrance panel web interface. By default, the **username** is admin, and the **password** is 123456.
2. Open **Logs** > **Email notifications.**
3. Set up the mail server according to the instructions on the page above.
4. Select events from the list to send notifications when they happen:
    - access denied by not valid identifier;
    - access denied by not valid Face ID;
    - access denied by not valid input code;
    - access denied by remote server API call;
    - access denied by the web API call;
    - access denied by unknown card;
    - access granted by API call;
    - lock opened by response device;
    - access granted by master code;
    - access granted by remote server API call;
    - access granted by valid identifier;
    - access granted by valid Face ID;
    - lock is opened too long;
    - lock opened by exit button;
    - lock was opened by free access button;
    - incoming call;
    - outgoing call;
    - incorrect login API call;
    - successful login API call;
    - device rebooted;
    - SIP registration lost;
    - tamper triggered.

5. Submit settings.

Tip

Use **Send Test Email** button to check the correctness of the entered data and send letter for trial.

3.9.2 Sending photos to the server

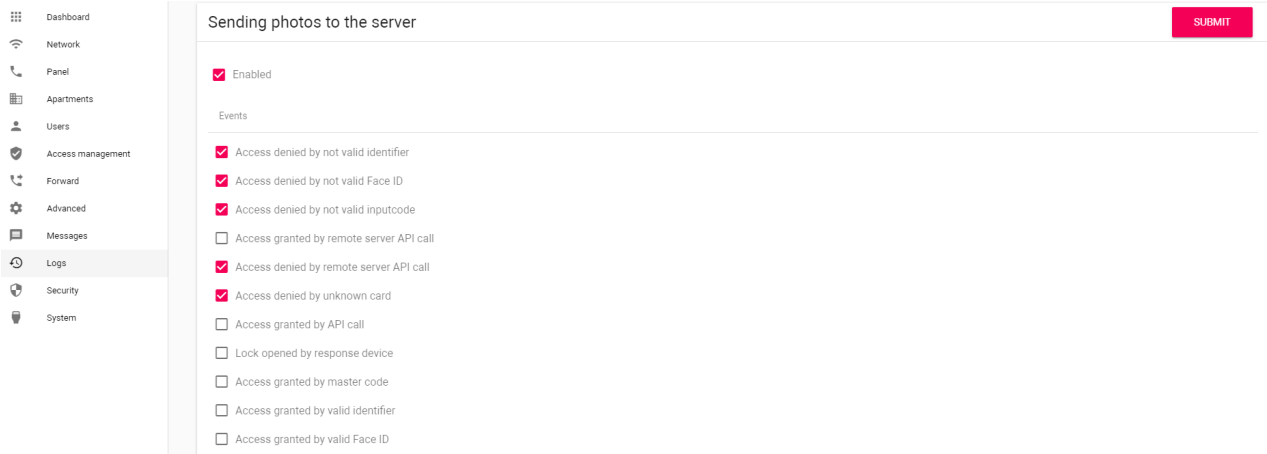
In panel settings, you can enable/disable and configure the feature of sending photos from the panel camera to the BAS-IP Link server.

3.9.2.1 How to configure Sending photos to the server feature

1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to **Logs** > **Sending photos to the server**.
3. **Enable** the feature by ticking corresponding field.
4. Select events from the list to send photos when they happen:
    - access denied by not valid identifier;
    - access denied by not valid Face ID;
    - access denied by not valid input code;
    - access denied by remote server API call;
    - access denied by the web API call;
    - access denied by unknown card;
    - access granted by API call;
    - lock opened by response device;
    - access granted by master code;
    - access granted by remote server API call;
    - access granted by valid identifier;
    - access granted by valid Face ID;
    - lock is opened too long;
    - lock opened by exit button;
    - lock was opened by free access button;
    - incoming call;
    - outgoing call;
    - incorrect login API call;
    - successful login API call;
    - device rebooted;
    - SIP registration lost;
    - tamper triggered.
5. Submit settings.

! Warning

The feature works only when synchronization with Link is enabled (use this[32] manual for Link configuration).



3.9.3 Syslog

The panel has the feature of sending logs to the Syslog server. In this tab, you can enter data for feature functioning.

3.9.3.1 SysLog Settings

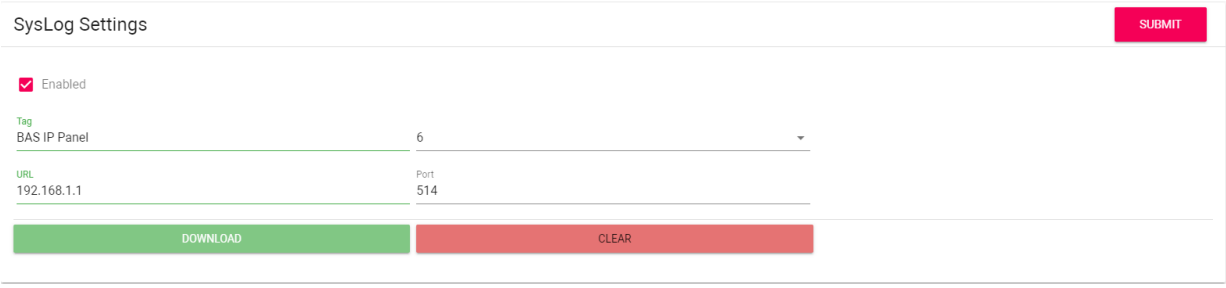
To configure sending data to the Syslog server, you need:

1. Log in to the entrance panel web interface. By default, the **username** is admin and the password is **123456**.
2. Go to **Logs** > **SysLog server**.
3. **Enable** the feature by ticking corresponding field.
4. Specify a **tag** that will distinguish this device data from other logs.
5. Select the required **Syslog level**. Messages in the log have levels, and the selected level will allow reading messages from the initial level to chosen one. For example, if you select level 5, the server will be able to read messages from 1st to 5th levels. You can check levels of messages coming from the panel in **Event types** table (**Severity** column).
6. Enter Syslog server address in **URL** field.
7. Indicate **port** required for the server work.
8. Submit settings.

32 https://wiki.bas-ip.com/basiplinken

Info

The log is cleared every 182 days.



By using the **Download** button, you can save the log to your device, and by clicking the **Clear** button, log entries will be deleted.

3.9.3.2 Message Format

The syslog message follows RFC 5424[33]standard.

The content of the event messages is:

```
EVENT:{event_type}:{arg1}:{arg2}:{argN}:{text}
```

Field description:

Field	Description
{event_type}	Event type identifier
{arg1} ... {argN}	Arguments characterizing the event (if any).
{text}	Readable description of the event in free form. Free to use: inside this field.

SysLog example

33 https://datatracker.ietf.org/doc/html/rfc5424

```
<70> 1970-01-02T02:00:23.575Z 192.168.68.90 AA-07_3.7.0_001FDEAABBCC EVENT:402:Device booted
<70> 1970-01-02T02:06:57.396Z 192.168.1.89 BI-12FB_3.7.0_706979E07098 EVENT:402:Device booted
<70> 1970-01-02T02:11:35.068Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010010@192.168.1.250:Door 1 opened by call host: sip:1010010@192.168.1.250
<70> 1970-01-02T02:11:36.238Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010010@192.168.1.250:Door 1 opened by call host: sip:1010010@192.168.1.250
<70> 1970-01-02T02:11:36.937Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:1010010@192.168.1.250:true:Outgoing call. call number: sip:1010010@192.168.1.250, call was accepted
<70> 1970-01-02T02:18:20.773Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:1010001@192.168.1.96:true:Outgoing call. call number: sip:1010001@192.168.1.96, call was accepted
<70> 1970-01-02T02:18:24.730Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010001@192.168.1.96:Door 1 opened by call host: sip:1010001@192.168.1.96
<70> 1970-01-02T02:18:41.090Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:10001@192.168.1.87:true:Outgoing call. call number: sip:10001@192.168.1.87, call was accepted
<70> 1970-01-02T02:18:47.995Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:1042343:Unknown card/UKEY:1042343 was used
<70> 1970-01-02T02:18:50.412Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:4072715:Unknown card/UKEY:4072715 was used
<70> 1970-01-02T02:18:51.811Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:4072715:Unknown card/UKEY:4072715 was used
<70> 1970-01-02T02:18:53.648Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:4072715:Unknown card/UKEY:4072715 was used
<70> 1970-01-02T02:18:55.506Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:105:Door opened by exit button
<70> 1970-01-02T02:20:12.704Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:1010010@192.168.1.250:true:Outgoing call. call number: sip:1010010@192.168.1.250, call was accepted
<70> 1970-01-02T02:00:04.629Z multiapartment-panel BI-12FB_3.7.0_ EVENT:402:Device booted
<70> 1970-01-02T02:01:59.599Z 192.168.1.89 BI-12FB_3.7.0_001FDEAABBCC EVENT:402:Device booted
<70> 1970-01-02T02:03:12.720Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:1010001@192.168.1.99:true:Outgoing call. call number: sip:1010001@192.168.1.99, call was accepted
<70> 1970-01-02T02:03:16.054Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010001@192.168.1.99:Door 1 opened by call host: sip:1010001@192.168.1.99
<70> 1970-01-02T02:04:11.787Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:4072715:Unknown card/UKEY:4072715 was used
<70> 1970-01-02T02:04:18.379Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:1042343:Unknown card/UKEY:1042343 was used
<70> 1970-01-02T02:00:04.668Z 192.168.1.89 BI-12FB_3.7.0_001FDEAABBCC EVENT:402:Device booted
<70> 1970-01-02T02:01:53.304Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:1010002@192.168.1.100:true:Outgoing call. call number: sip:1010002@192.168.1.100, call was accepted
<70> 1970-01-02T02:01:59.051Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010002@192.168.1.100:Door 1 opened by call host: sip:1010002@192.168.1.100
<70> 1970-01-02T02:02:02.563Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:501:sip:1010002@192.168.1.100:Incoming call. Call number: sip:1010002@192.168.1.100
<70> 1970-01-02T02:02:05.135Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010002@192.168.1.100:Door 1 opened by call host: sip:1010002@192.168.1.100
<70> 1970-01-02T02:02:05.278Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:1010002@192.168.1.100:Door 1 opened by call host: sip:1010002@192.168.1.100
<70> 1970-01-02T02:02:13.291Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:500:sip:10001@192.168.1.92:true:Outgoing call. call number: sip:10001@192.168.1.92, call was accepted
<70> 1970-01-02T02:02:18.580Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:106:1:sip:10001@192.168.1.92:Door 1 opened by call host: sip:10001@192.168.1.92
<70> 1970-01-02T02:02:21.353Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:5673191:Unknown card/UKEY:5673191 was used
<70> 1970-01-02T02:02:22.631Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:300:16093246:Unknown card/UKEY:16093246 was used
<70> 1970-01-02T02:02:25.295Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:105:Door opened by exit button
<70> 1970-01-02T02:00:04.572Z 192.168.1.89 BI-12FB_3.7.0_001FDEAABBCC EVENT:402:Device booted
<86> 2021-12-08T10:45:15.561Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:600:Login to the web interface
<86> 2021-12-08T10:45:29.412Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:600:Login to the web interface
<70> 2021-12-08T10:45:34.878Z 192.168.1.89 BI-12FB_3.7.0_706979E177C1 EVENT:107:1:Door opened from the web interface. Lock 1 was opened
<86> 2021-12-08T10:49:07.053Z 192.168.1.199 BI-12FB_3.7.0_706979E177C1 EVENT:600:Login to the web interface
<70> 2021-12-08T10:49:16.784Z 192.168.1.199 BI-12FB_3.7.0_706979E177C1 EVENT:107:1:Door opened from the web interface. Lock 1 was opened
<70> 2021-12-08T10:52:06.515Z 192.168.1.63 BI-12FB_3.12.2_001FDEAABBCC EVENT:402:Device booted
<86> 2021-12-08T10:53:14.905Z 192.168.1.199 BI-12FB_3.12.2_706979E177C1 EVENT:600:Login to the web interface
<86> 2021-12-08T14:56:02.554Z 192.168.1.199 BI-12FB_3.12.2_706979E177C1 EVENT:600:Login to the web interface
<70> 1970-01-02T02:00:04.885Z 192.168.1.199 BI-12FB_3.12.2_001FDEAABBCC EVENT:402:Device booted
<86> 2021-12-09T09:30:08.202Z 192.168.1.217 BI-12FB_3.12.2_706979E177C1 EVENT:600:Login to the web interface
```

Info

For example, the Door opened by general access code event might look like this:

```
EVENT:100:0000:
Door opened by general access
code:0000
```

where, **100** is an identifier of Door opened by general access code event, **0000** is an event argument (in this case, the key that opened the door) and, further, a free-form description of the event: **Door opened by general access code: 0000**.

3.9.3.3 Event types

Table with event types and their parameters:

ID	Description	Parameters	Facility	Severity	PRI
000	Any events not listed below		8	6	70
100	Door opened by general access code	Code number, door number	8	6	70
101	Door opened by access code	Code number, apartment number, door number	8	6	70
102	Door opened by card	Card number, apartment number, door number	8	6	70
103	Door opened by UKEY	Card number, apartment number, door number	8	6	70
104	Door opened by Face identifier	Face ID, apartment number, door number	8	6	70
105	Door opened by exit button		8	6	70
106	Door opened by call host	Subscriber number, apartment number, door number	8	6	70
107	Door opened from the web interface	Door number	8	6	70
108	Door opened by remote server	Door number	8	6	70
109	Door opened by free access button				
110	Door opened by QR code	QR number, apartment number, door number	8	6	70
111	Access denied via multi factor access	One identifier	8	6	70

ID	Description	Parameters	Facility	Severity	PRI
112	Access denied via multi factor access	Two identifiers	8	6	70
113	Access denied via multi factor access	Three identifiers	8	6	70
114	Access denied via multi factor access	Four identifiers	8	6	70
115	Access denied via multi factor access	Five identifiers	8	6	70
116	Access granted via multi factor access	One identifier	8	6	70
117	Access granted via multi factor access	Two identifiers	8	6	70
118	Access granted via multi factor access	Three identifiers	8	6	70
119	Access granted via multi factor access	Four identifiers	8	6	70
120	Access granted via multi factor access	Five identifiers	8	6	70
121	Access denied to identifiers without linkage to user	Identifier number, identifier type	8	6	70
122	Access granted by valid license plate	Plate, car owner, lock number	8	6	70
123	Access denied by invalid identifier plate	Plate, car owner	8	6	70
124	Access denied by unknown identifier plate	Plate	8	6	70

ID	Description	Parameters	Facility	Severity	PRI
200	The door is not closed for more than N seconds	Time in seconds, how long the door has been open	8	6	70
201	Door was closed		8	6	70
202	Door was opened with door sensor	Sensor type	8	6	70
203	Door was closed with door sensor		8	6	70
204	Door was opened with enter button		8	6	70
300	Unknown card/UKEY was used	Card number	8	6	70
301	Unknown access code was used	Code number	8	6	70
302	Invalid card was used	Card number, apartment number	8	6	70
303	Invalid access code was used	Code number, apartment number	8	6	70
304	Invalid UKEY was used	UKEY number, apartment number	8	6	70
305	Invalid Face ID was used	Face ID number, apartment number	8	6	70
306	Access denied by remote server		8	6	70
307	Invalid QR code was used	QR number, apartment number	8	6	70

ID	Description	Parameters	Facility	Severity	PRI
308	Unknown QR code was used	QR number	8	6	70
309	The lock is open on alarm	Lock number, unlock time in seconds	8	6	70
400	SIP registration OK		8	6	70
401	SIP registration lost		8	6	70
402	Device booted		8	6	70
403	Email sent successfully	Recipient email, event ID	2	6	22
404	Email not sent	Recipient email, event ID	2	6	22
500	Outgoing call	Subscriber number, apartment number	8	6	70
501	Incoming call	Subscriber number	8	6	70
502	Outgoing call failed	Subscriber number, apartment number	8	6	70
600	Login to the web interface		10	6	86
601	Failed login attempt to the web interface		10	6	86

3.9.3.4 App Name

In addition, the log entry contains information about the model, software version and MAC address of the device.

Field format:

```
TAG:{model}_{version}_{mac}
```

Field description:

Field	Description	Example
TAG	Device tag (optional)	Panel near the road
{model}	Model name	AA-07B
{version}	Firmware version	3.5.0
{mac}	MAC address without separators	706979EEEEEE

3.10 Security

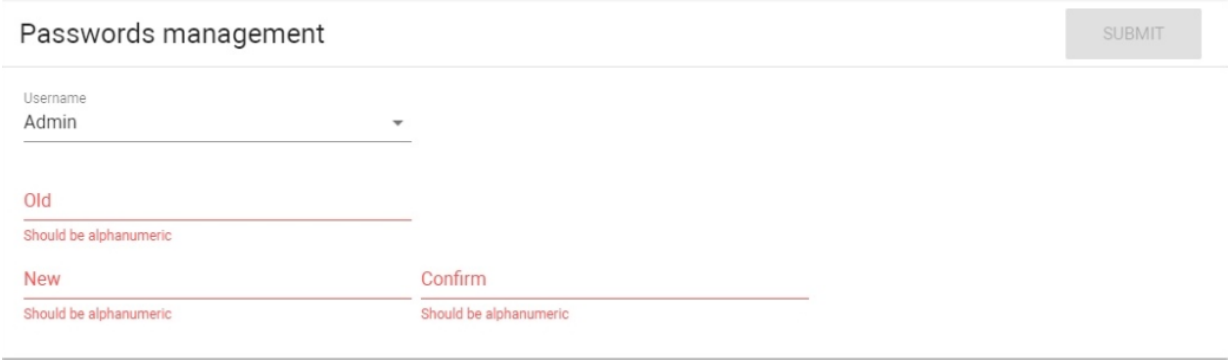
In this tab, you can change the administrator password that is used to enter the web interface and panel settings.

3.10.1 How to change the administrator password

1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to the **Security** tab.
3. Enter the current password in the **Old** field.
4. Create a **new** password and enter it in the appropriate field. The password can be up to 16 digits and contain all ASCII symbols (a-z, A-Z, 0-9 and a selection of punctuation marks).
5. **Confirm** the new password by re-entering.
6. Submit changes.

Info

The default administrator password is **123456**.

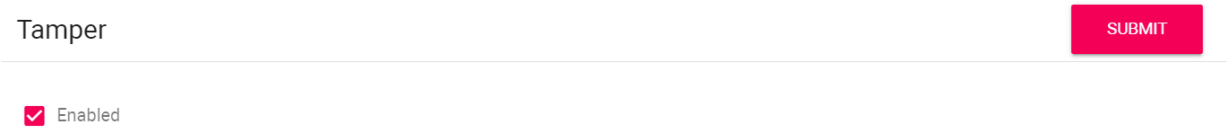


3.10.2 Tamper settings

A tamper is a button that is activated by an attempt to remove the device (it is installed on the panel back cover), for example, while stealing. When the tamper is triggered, the siren turns on and a notification is displayed in the log. Also, information about tamper activation can be sent by email[34] as well a photo[35] from the panel can be sent to the server (if these options are enabled and configured).

In this section, you can activate the tamper work. To do this complete steps:

1. Log in to the entrance panel web interface. By default, the **username** is admin and the **password** is 123456.
2. Open **Security** > **Settings** tab.
3. Enable the feature.
4. Submit settings.



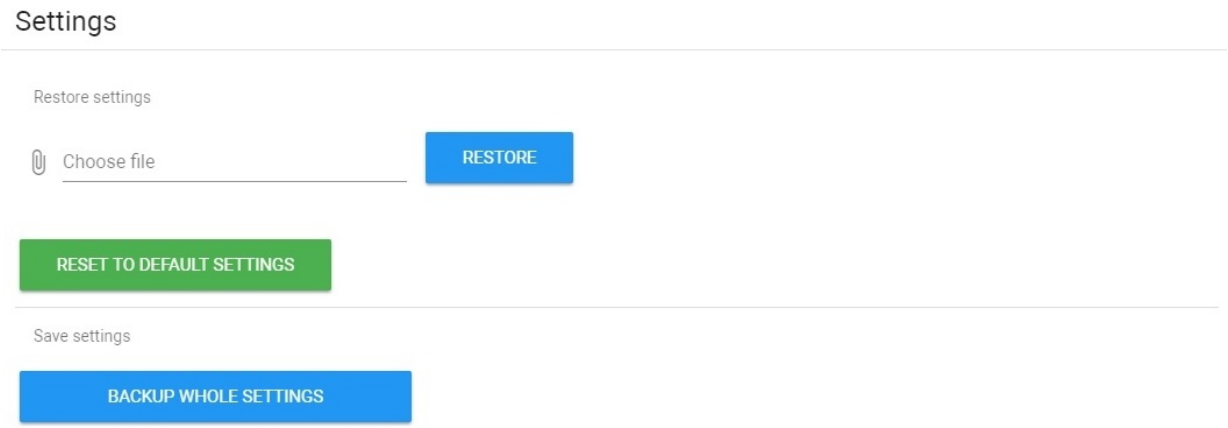
3.11 System

In this tab, you can back up or restore panel settings, export/import data, update software, change language, reboot the device, etc.

34 https://wiki.bas-ip.com/aa07/email-notifications-135955137.html
35 https://wiki.bas-ip.com/aa07/sending-photos-to-the-server-135955140.html

3.11.1 Settings

In this section, you can back up all web interface settings (except network settings) by clicking the **Backup whole settings** button. If necessary, you can select the downloaded file and restore the settings (the feature works only if the firmware version of uploaded settings is the same as the current panel version). You can also **reset** the device **to the default settings** by clicking the corresponding button.

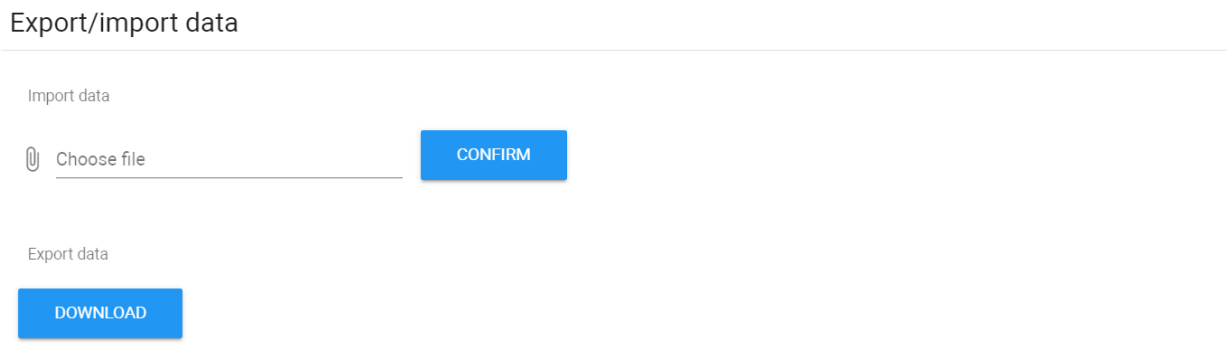


3.11.2 Export/Import data

If necessary, you can export or import data from the **Apartments**, **Forward**, **Identifiers**, and **Access Restrictions** tabs. To export, you must click **Download** and a ZIP archive with tables will be saved on your computer.

Data import is used to copy the exported information to other panels. To do this, **choose ZIP archive** and click **Confirm**.

When importing data into the panel, all current data in the **Apartments**, **Forward**, **Identifiers**, and **Access Restrictions** tabs will be deleted and replaced with new (importing) information without the possibility of restoring.

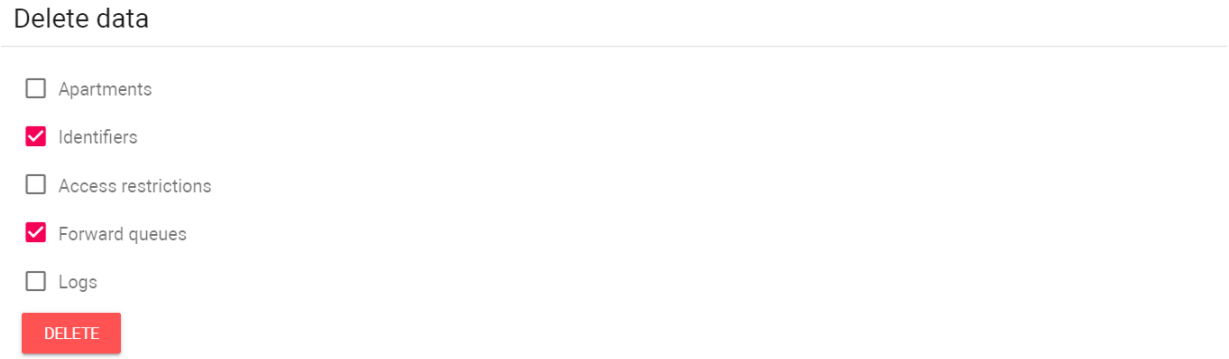


! Warning

Import of incorrect format data will cause the panel malfunctioning.

3.11.3 Delete data

In this section, you can delete data about one or more categories: **Apartments**, **Identifiers**, **Access restrictions**, **Forward queues**, and **Logs**. To clear data, select category/ies and click **Delete**. As a result, the data will be irrevocably deleted.



3.11.4 Device language

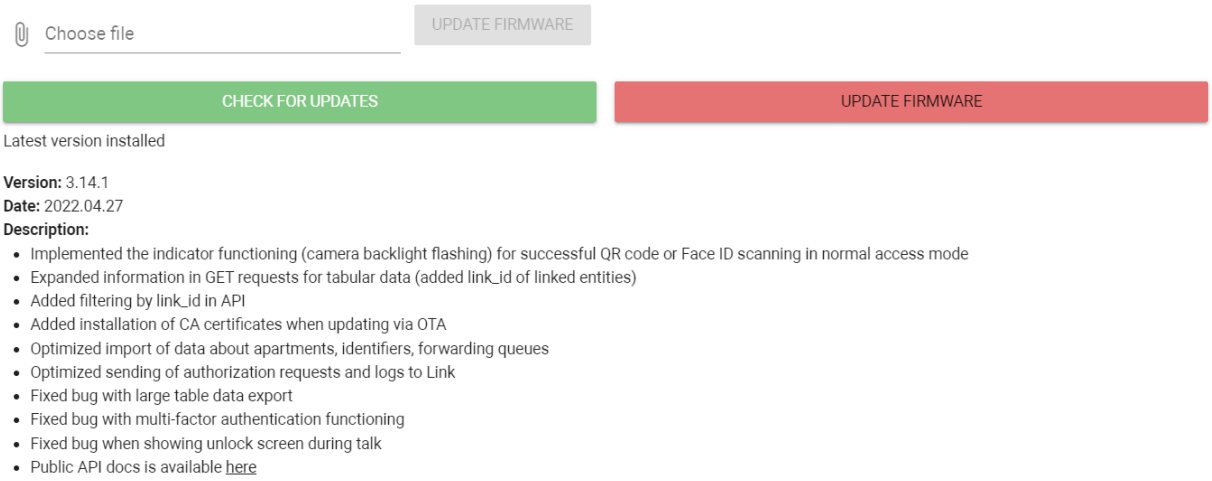
6 device languages are available for setting:

- English;
- Russian;
- Ukrainian;
- Spanish;
- Polish;
- Dutch;
- Turkish.

3.11.5 Firmware upgrade

By default, the BAS-IP server is used for updates. You have several ways to update panel firmware:

- **automatically**: **check for** software **updates** and if it is released, click **Update Firmware.** The update process will take some time and in the end, the panel will reboot. If there are no updates, information about the current firmware version will be provided;

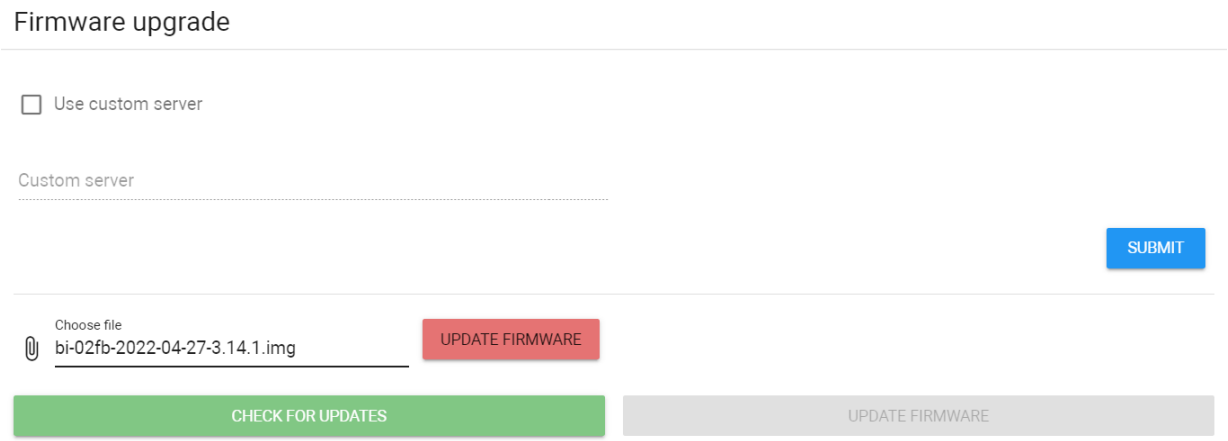


! Warning

Before each software update, make a panel settings backup copy, so that in case of an update error, you can always restore the previous settings.

- **manually**: download the necessary firmware from the webpage[36], click **Choose file** and upload the downloaded file. Click **Update Firmware** and wait for the process to complete (in the end the panel will reboot);

36 https://wiki.bas-ip.com/en/firmware-for-bas-ip-devices-27852807.html



You also can use a **custom server** (is used in closed intercom networks) for firmware updates.

The custom server must meet certain conditions for its correct work: the server must have the version.json file and the file with the necessary firmware.

The **version.json** file must contain information and structure as in the example:

- **firmware version**;
- **name** (doubles the firmware version);
- **firmware build date**;
- **device type** (panel version): panel_v4 is a standard value for all panels;
- **description of changes**;
- **link to the firmware file.**

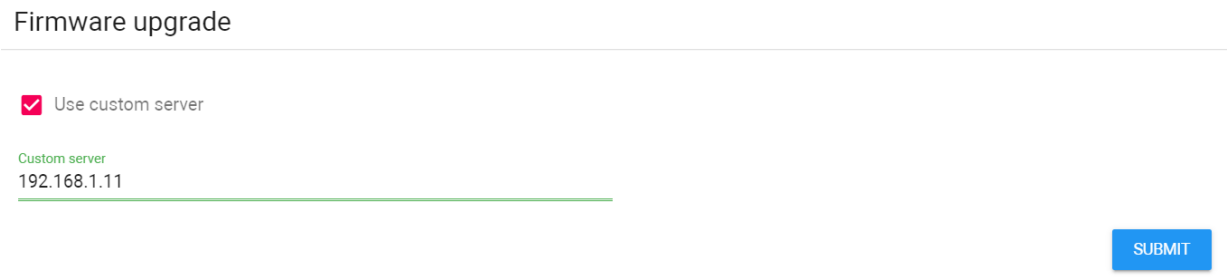
Custom server

```
{
"version": "3.13.0",
"name": "3.13.0",
"date": "2021.12.02",
"device_type": "panel_v4",
"description": "<ul>
<li>Added screen brightness setting</li>
<li>Added custom concierge name feature on the conversation screen</li>
<li>Fixed problem with updating firmware via web interface</li>
<li>Fixed problem with displaying messages in the web interface of AA-14FB</
li>
<li>Fixed problem with sorting in the contact book</li>
<li>The maximum number of digits in the access code has been increased from
eight to ten</li>
<li>Fixed search for apartments in the identifier menu</li>
<li>Fixed problem with internal calls when SIP settings are enabled, but there
is no access to the SIP server</li>
```

```
<li>Added port option to SIP proxy settings and forward numbers</li>
<li>Added horizontal scrolling in the contact book</li>
<li>Added support for AA-07FBV2M and AA-07FBC2M models</li>
<li>Added support for external temperature sensor</li>
<li>Minor fixes</li>
<li>The new version of the API is available via <a href=https://
developers.bas-ip.com//%3Ethe link</a></li>
</ul>",
"url_address": "https://192.168.1.11/url-to-firmware-image.img"
}
```


3.11.6 How to configure custom server use for firmware updates

1. Log in to the device web interface. By default, the **username** is admin and the **password** is 123456.
2. Go to **System** tab>**Software upgrade** section.
3. Enable **use** of a **custom server**.
4. Enter the link to the server (with version.json and firmware files) in the **Custom server** field.
5. Submit settings.



To update firmware from a custom server, you also must **check for updates** and click **Update Software**.

3.11.7 Reboot

The section contains a button for panel soft reset.

3.11.8 Debug

In this tab, you have access to the panel system logs and the ability to make remote outgoing calls to other devices.

- System logs(see page 65)
- Outgoing call(see page 65)

- MQTT client debug(see page 66)

3.11.8.1 System logs

This section is necessary in case of system errors or panel malfunctions. You can **download** system logs and send them to the BAS-IP support team to work on fixing them.

With the **Clear** button, you can delete all information from logs.

System logs

DOWNLOAD CLEAR

3.11.8.2 Outgoing call

With the help of this feature, you do not need to be near the panel to check the connection or correct operation of calls between the panel and a monitor, softphone, etc. To make a call, enter the number of the callee device (can be a logical address, SIP number, or number for P2P calls) and click the **Call** button. To end the call, click **Stop**.

The call will be displayed on the panel, and the event "Outgoing call made from the web to the number" will appear in the logs.

Number formats:

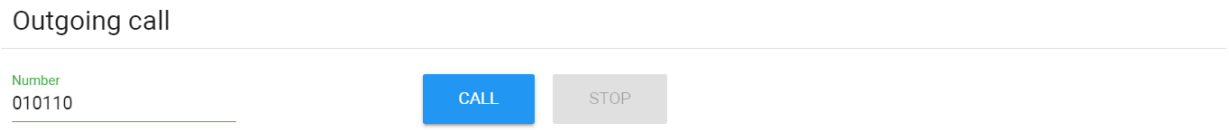
If the call is made via the internal protocol, enter the device logical address:

- for multi-apartment entrance panels, you must specify **Building No. - Unit No. - Device No.** For example, 0001-01-2.
- for individual entrance panels, you must enter **Building No. - Unit No. - Floor No.** - **Apartment No. - Device No.** For example, 001-01-02-04-1.
- for indoor video entry phone (monitor), you must specify **Building No. - Unit No. - Floor No.** - **Apartment No.** For example, 0001-02-03-15.

If the call is made via P2P, enter the number in the format: **sip:any number@IP address of the callee SIP client.** For example, sip:3@192.168.1.25.

If the call is made via SIP, enter the number in the format: **sip:callee SIP number@SIP server address.** For example, sip:2255@us.sip.bas-ip.com[37].

37 http://ru.sip.bas-ip.com/



3.11.8.3 MQTT client debug

In this section, you can get the current MQTT client state or its actions: the client is enabled, the client is successfully connected, etc. Click start to get information, and the corresponding button to stop the process.

> This feature works only if the MQTT protocol[38] is enabled.

38 https://wiki.bas-ip.com/aa07/network-135955054.html

4 Device usage

4.1 Recieving the RTSP stream from the panel camera

To get the RTSP stream from the camera of the call panel to the video surveillance system, you need to put in the add line of the camera rtsp://admin**:**123456@192.168.1.16[39]**:8554/ch01**, where **admin** is the login, **123456** is the password to access the WEB interface, **192.168.1.16** is the IP address of the panel, **8554** is the port of access to the camera, **ch01** is the channel number.

4.2 UKEY mobile access

4.2.1 Description

Ukey Mobile Access from BAS-IP is a universal technology for gaining access to the premises or to the territory of an object with the possibility to use in one reader simultaneously: EM-Marin cards and MIFARE/encrypted cards MIFARE Plus/MIFARE Classic, cell phone (Bluetooth and NFC).

Advantages of UKEY:

- Ability to use several standards of identification simultaneously: EM-Marin, MIFARE, Bluetooth and NFC
- Ability to use a cell phone as an identifier
- Adjustable range of mobile identifier (when using Bluetooth)
- Low power consumption
- Special encryption algorithm for mobile IDs and MIFARE Plus cards
- Ability to apply to any types of objects
- Ability to install UKEY Mobile access in previously aquired outdoor panels
- Convenience in use

4.2.2 Working principle

39 mailto:123456@192.168.1.16

Identification and unlocking is possible due to the presence of the built-in module BME-03 in the panels, supporting UKEY Mobile Access.

Multi-format Module BME-03 which can be equipped with all the outdoor panels BAS-IP with a built-in reader, allows you to identify the user by the UKEY technology using different identifiers (cards, pendants, cell phone), and performs the role of universal reader of access control system.

4.2.3 Mobile access with UKEY application[40]

For users' ease of operation with BAS-IP outdoor panels equipped with multi-format readers, the company BAS-IP has released a new mobile Ukey application which, after receiving the mobile ID, is used to open the doors/gates/parking gate arms.

For each outdoor panel equipped with a reader module with support for UKEY Mobile access, a different range of the mobile ID can be configured, in the range of 2 centimeters to 10 meters. The response distance depends not only on the selected mode, but also on the thickness of the walls in the room, weather conditions (when placing the panel outside) and other factors.

Operation modes (operational range of mobile ID):

- Touch (working distance up to 2 cantimeters)
- Door (working distance up to 1 meter)
- Gate/barrier (adjustable distance from 0,5 meter to 10 meters)

4.2.4 Triple-clicking setup with UKEY Cfg[41] application

Application abilities:

- Adjusting operating mode of EM-Marin cards, MIFARE and BLE (Bluetooth Low energy) - enable/disable standards of reading
- Setting ecryption for UKEY identifier. This will enable you to link the encrypted ID key to the selected reader
- Enable/disable encrypting mode for MIFARE Classic and MIFARE Plus cards
- Enable diversification for MIFARE Classic and MIFARE Plus cards
- Adjusting sound confirmation when waving mobile identifiers near the reader in standby and reader mode
- Setting operating mode: door, touch, gate/barrier
- Adjusting range operating mode when select gate/barrier mode

40 https://wiki.bas-ip.com/basipidapp
41 https://wiki.bas-ip.com/display/BASIPCONFIGID/UKEY+Cfg

- In connection with reader TR-03, configurator allows you to to record MIFARE Classic and MIFARE Plus encryption cards
- Storing a file with settings for defined reader
- Ability to download configuration file with settings for restoring reader parameters and copying settings to other readers

4.2.5 Ways to get mobile ID and access card

Scan QR-code with the UKEY Application

The user submits an application to purchase the required number of QR-codes to the administrator of his service company, wherein one QR-code = one mobile device. Afterwards, the user gets the QR-code in the printed form or in electronic form (by e-mail, Viber, Telegram, etc.). Then the user scans the code received or imports it from the file system and thus gets the mobile ID.

Before the identifier is issued to the user as a QR-code, it is recorded by the administrator of the management company in the Management Software. The QR code cannot be reused on multiple cell phones, as it is linked to only one mobile device, providing a high level of reliability and security of mobile identifiers. You cannot copy or duplicate an identifier.

Using BAS-IP TR-03B reader

In order for the administrator of the management company to be able to use TR-03B to issue mobile identifiers or to record access cards, it is necessary to specify the master-card, which will be needed for the reader to work in the future. The Master- card is specified when the reader is first started.

Create a master card:

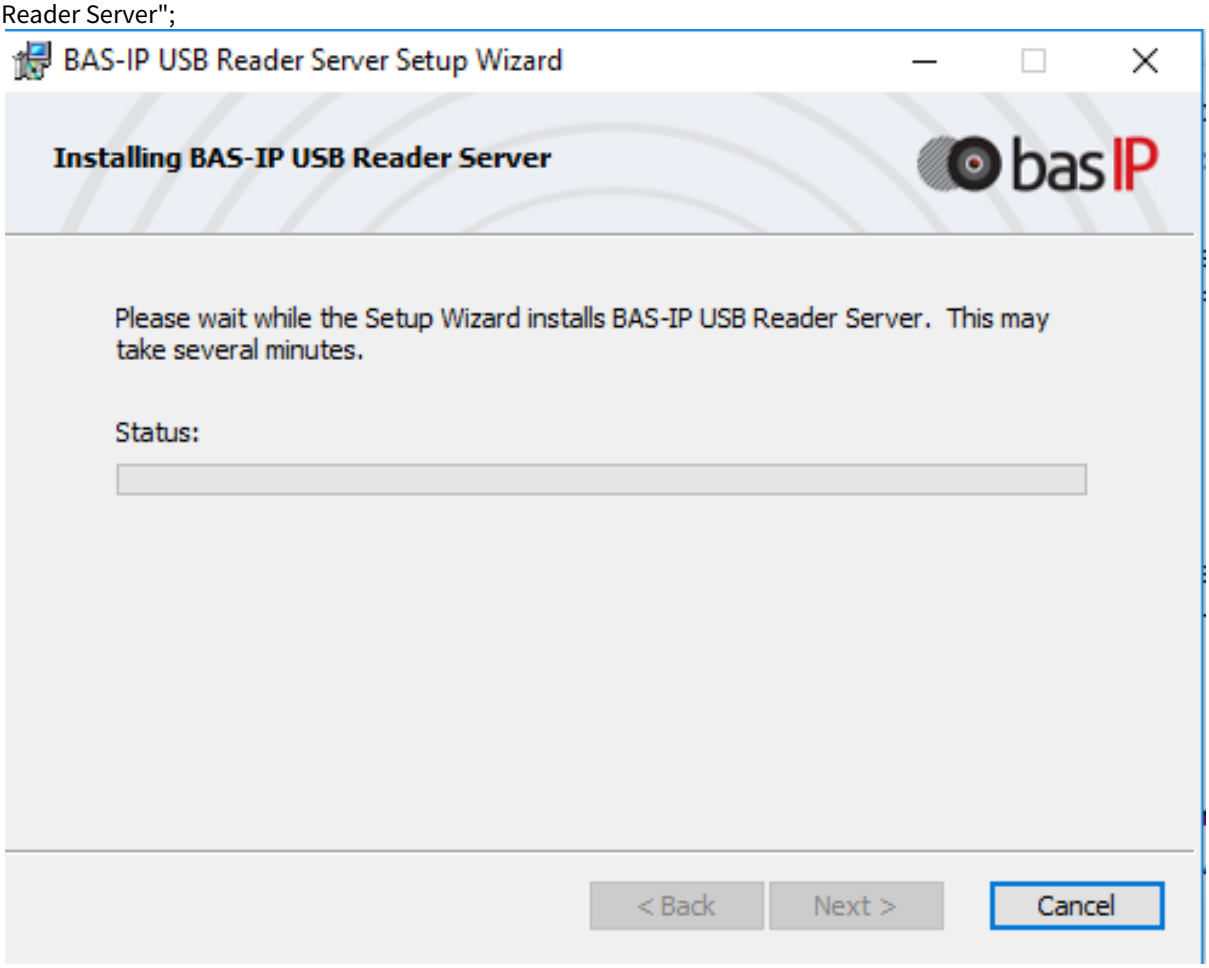
1. Download and install UKEY Cfg mobile application;
2. Connect TR-03B reader to the power source +5V (USB);
3. Launch UKEY Cfg app and press Search button;
4. The app will find the reader, it is necessary to enter the settings, More menu, then Change master-card tab;
5. Bring EM-Marin card or MIFARE to the reader;
6. Reader will make a record to the card with encryption, after that it becomes a master-card for this reader;
7. To keep on working with the reader, you should reconnect to it in the UKEY Cfg App.
8. For more details about features of the desktop reader, follow the link

Once the master-card has been created, the administrator can issue mobile ID's as well as add encrypted keys to MIFARE Plus cards.

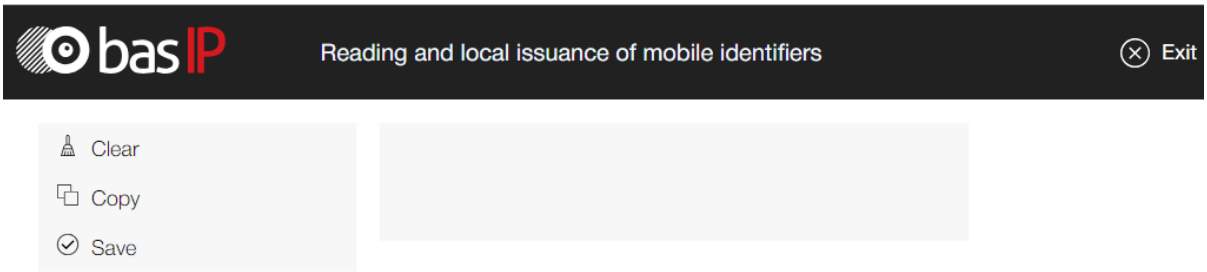
Obtain Mobile IDs using TR-03B

1. Download and install UKEY mobile application;

2. Install and launch the program on a PC with the Windows Family OS to write the identifiers "BAS-IP USB Reader Server";



3. Connect the reader to PC;
4. Bring a master-card to the reader;
5. Bring a cell phone to the reader (make sure Bluetooth is on) and enter UKEY App, then press Obtain button or select Obtain BAS-IP TR-03 key.
6. The reader will transmit a mobile ID to your cell phone, thus "Your key is ready" will appear in the app.



4.3 API integration

API interaction description and specifications are available here[42].

42 https://developers.bas-ip.com/category/android-panels/

5 Installation and connection

5.1 Completeness check

Before installation of the outdoor panel, it is necessary to check that it is complete and all components are available.

The outdoor panel kit includes:

Outdoor panel	1 pcs
Flush mount bracket	1 pcs
Installation instructions	1 pcs
Set of wires with connectors for connection of power supply, lock, and additional modules.	1 pcs
A set of plugs for connections	1 pcs
Wrench set screws	1 pcs

5.2 Electrical connection

After verifying whether a device is complete, you can switch to the connection step.

For connection you will need:

- an Ethernet UTP CAT5 or higher cable connected to a network switch/router;

> The maximum length of the UTP CAT5 cable segment should not exceed 100 meters, according to the IEEE 802.3 standard.

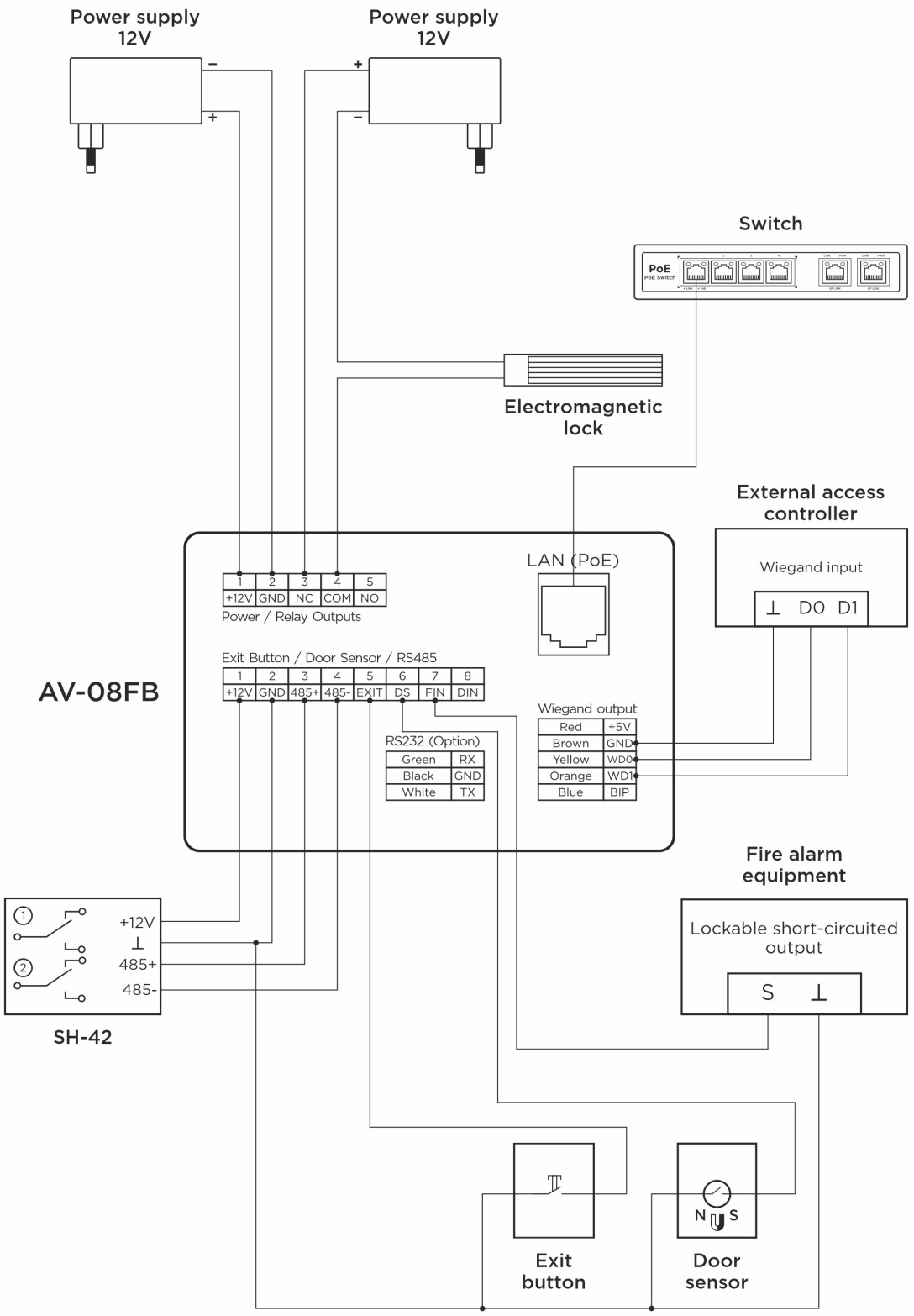
- power supply at + 12V, 2 Amps;
- wires must be brought for connecting the lock and additional modules (optional).

You can connect any type of electromechanical or electromagnetic lock for which the switched current does not exceed 5 Amps.

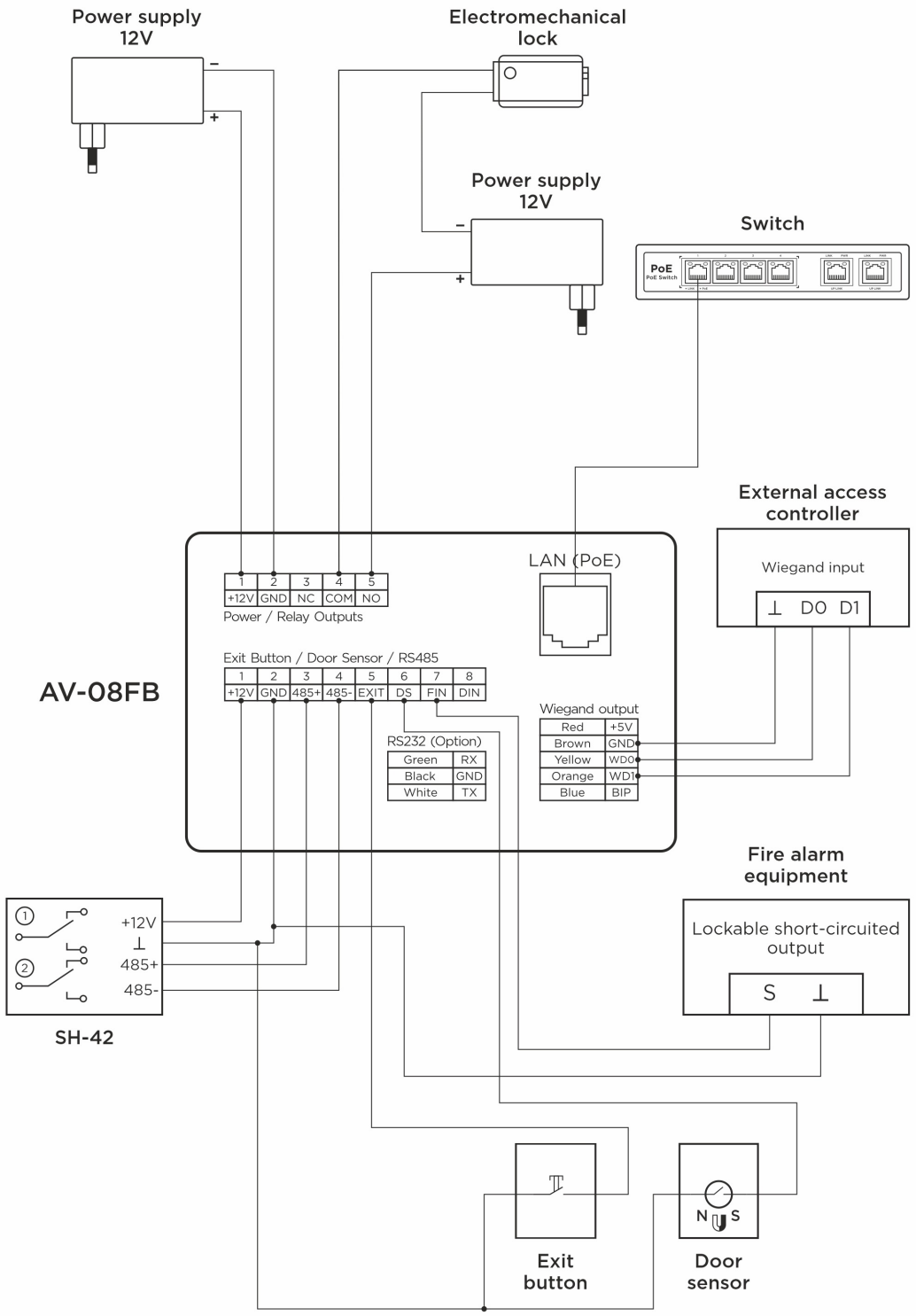
The following are typical connection schemes of all elements to the outdoor panel:

- Connection using an external power supply and an electromagnetic lock(see page 73)
- Connection using an external power supply and an electromechanical lock(see page 75)

5.2.1 Connection using an external power supply and an electromagnetic lock

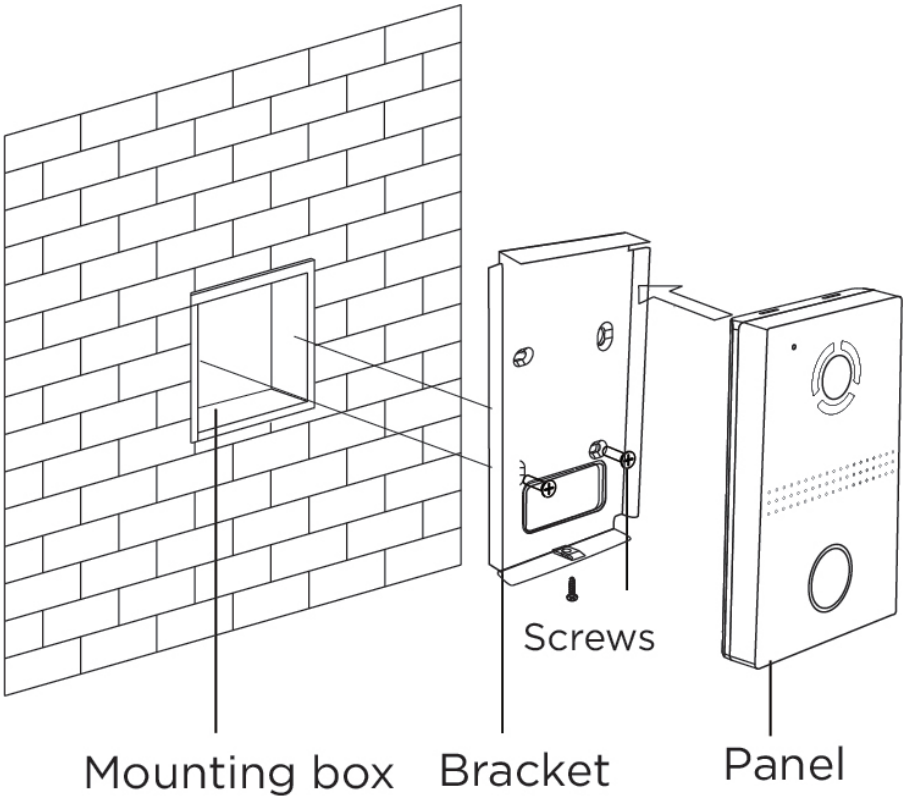

Power supply
12V
Power supply
12V
Switch
PoE
Electromagnetic
lock
External access
controller
Wiegand input
⊥ D0 D1
LAN (PoE)
1 2 3 4 5
+12V GND NC COM NO
Power / Relay Outputs
Exit Button / Door Sensor / RS485
1 2 3 4 5 6 7 8
+12V GND 485+ 485- EXIT DS FIN DIN
AV-08FB
RS232 (Option)
Green RX
Black GND
White TX
Wiegand output
Red +5V
Brown GND
Yellow WD0
Orange WD1
Blue BIP
Fire alarm
equipment
Lockable short-circuited
output
S ⊥
+12V
⊥
485+
485-
SH-42
N S
Exit
button
Door
sensor

5.2.2 Connection using an external power supply and an electromechanical lock


Power supply
12V
Electromechanical
lock
Power supply
12V
Switch
PoE
PoE Switch
External access
controller
Wiegand input
⊥ D0 D1
LAN (PoE)
1 2 3 4 5
+12V GND NC COM NO
Power / Relay Outputs
Exit Button / Door Sensor / RS485
1 2 3 4 5 6 7 8
+12V GND 485+ 485- EXIT DS FIN DIN
AV-08FB
Wiegand output
Red +5V
Brown GND
Yellow WD0
Orange WD1
Blue BIP
RS232 (Option)
Green RX
Black GND
White TX
Fire alarm
equipment
Lockable short-circuited
output
S ⊥
+12V
⊥
485+
485-
SH-42
N S
Exit
button
Door
sensor

5.3 Mechanical mounting

Before mounting the door panel, a hole or recess in the wall with dimensions of 110 x 183 x 60 mm (for flush mounting) must be provided. It is also necessary to provide for the supply of power cable, add. modules and local network.



5.4 Connection of additional modules

The following modules can be connected to all multi-apartment panels:

- Module to control two locks SH-42;
- Module to control elevator equipment EVRC-IP.