

BAS-IP Link

BAS-IP Link

Exported on 06/29/2023

Table of Contents

1	Getting started	10
1.1	Software installation and launch	10
1.1.1	Hardware recommendations	10
1.1.2	General information.....	10
1.1.3	Installing Link under Linux using Docker	11
1.1.4	Used ports	14
1.2	Link version update	14
1.3	First authorization and the server initial setup	17
1.3.1	Server initial setup	17
1.4	Supported devices and firmware versions	21
1.5	Link Changelog.....	22
1.5.1	1.2.180.....	22
1.5.2	1.2.177.....	22
1.5.3	1.2.174.....	23
1.5.4	1.2.173.....	23
1.5.5	1.2.172.....	23
1.5.6	1.2.170.....	23
1.5.7	1.2.169.....	23
1.5.8	1.2.168.....	23
1.5.9	1.2.167.....	23
1.5.10	1.2.165.....	23
1.5.11	1.2.161.....	23
1.5.12	1.2.159.....	24
1.5.13	1.2.158.....	24
1.5.14	1.2.157.....	24
1.5.15	1.2.155.....	24
1.5.16	1.2.150.....	24
1.5.17	1.2.149.....	24
1.5.18	1.2.148.....	24
1.5.19	1.2.146.....	24
1.5.20	1.2.145.....	24
2	Dashboard	26

3	Profile	28
4	Notifications	29
4.1	How to configure important notifications	29
5	Users management	31
5.1	Users	31
5.1.1	How to register a new user	31
5.1.2	How to activate a user profile.....	33
5.1.3	Users filtering	34
5.2	Profiles	34
5.2.1	How to create a profile	36
5.2.2	Independent projects on the one server.....	37
5.2.3	How to create a root group administrator profile	37
5.2.4	Example of server configuration for hosting several projects	39
5.3	Groups	43
5.3.1	How to add root group	44
5.3.2	How to generate root groups	45
5.3.3	Group forward rules	48
6	Access management	50
6.1	Guest access	50
6.1.1	How to create a guest identifier	50
6.1.2	Guest passes filtering.....	56
6.2	Schedules	56
6.2.1	How to add a new schedule.....	57
6.2.2	Schedules filtering	61
6.3	Access restrictions	61
6.3.1	How to create access restriction	62
6.3.2	Access restrictions filtering.....	63
6.4	Identifiers	64
6.4.1	How to add an identifier	64
6.4.2	Identifiers filtering.....	66
6.5	Access matrix.....	67
6.6	ACS logs	68

7	Communications.....	70
7.1	Conversations	70
7.1.1	How to create a conversation.....	71
7.1.2	Conversations filtering.....	71
7.2	Announces	72
7.2.1	How to create an announce	73
7.2.2	Announces filtering.....	74
7.3	Info and polls.....	75
7.4	Emergency alerts	75
7.4.1	How to create an emergency alert	76
7.4.2	Alerts filtering.....	77
8	Telephony settings.....	78
8.1	Virtual numbers.....	78
8.1.1	How to create a virtual number	78
8.1.2	Virtual numbers filtering.....	80
8.2	Forward rules	81
8.2.1	How to create a forward rule.....	82
8.2.2	Forward rules filtering	83
8.3	Call history.....	84
8.4	Inbuild call service	86
9	Devices management	87
9.1	Devices.....	87
9.1.1	How to add a device to the Link server	88
9.1.2	Remote device configuration	89
9.1.3	Filter for devices display	93
9.2	Logs.....	94
9.3	Queue tasks	97
9.4	Status.....	99
9.5	Device initialization.....	100
10	Elevator management	102
10.1	Configuration from the EVRC-IP side.....	102
10.2	Elevators.....	103

10.2.1	How to configure an elevator controller.....	103
10.2.2	Elevators filtering.....	106
10.3	Elevator logs.....	106
10.4	Elevators access restrictions	110
10.4.1	How to create access restriction for an elevator	110
10.4.2	Access restrictions filtering.....	111
11	Settings.....	113
11.1	System audit.....	113
11.2	Backups	115
11.3	General	116
11.3.1	General	116
11.3.2	Mail Server settings.....	117
11.3.3	Notifications.....	118
11.3.4	Devices.....	118
11.3.5	SIP settings.....	119
11.3.5.1	SIP status	119
11.3.5.2	SIP settings.....	119
11.3.5.3	Network interfaces.....	120
11.3.5.4	Internal subnets	120
11.3.5.5	SIP nodes	121
11.3.5.6	Additional SIP functionality.....	121
11.3.5.7	Used ports	122
11.3.6	SIP trunks	122
11.3.6.1	How to configure SIP trunks functioning.....	122
11.3.7	Additional settings.....	125
11.3.7.1	Whitelabel.....	126
11.3.7.2	Markers	128
11.3.7.3	System settings.....	129
11.3.7.4	Data import	129
11.3.7.5	MQTT settings.....	129
11.3.8	Mail Templates.....	130
11.3.8.1	How to create a mail template.....	130
11.4	Licenses	131
11.5	System info.....	132

11.5.1	System logs	133
11.5.2	Info	133
11.5.3	Queues management.....	134
11.5.4	WEB metrics	134
12	FAQ.....	136
12.1	What settings must be done on the device for the Link server correct operation?	136
12.2	What server elements are required for a basic server functioning?	137
12.3	How to register a new user?	137
12.4	How limit users if they have not paid for some features?	139
12.5	How to activate a user profile?	139
12.6	How to add root group?	140
12.7	How to generate root groups?	143
12.8	How to create a guest identifier?	145
12.9	Why access restriction is required?	147
12.10	How to create access restriction?	147
12.11	How to add an identifier?	148
12.12	How to notify residents of important information or survey them?	149
12.13	How to create a virtual number?	150
12.14	How to add a device to the Link server?	152
12.15	How to configure an elevator controller?	153
12.16	How to create access restriction for an elevator?	156
12.17	How to configure hosting of several independent projects on the one server?	156
13	Example of the server configuration for a basic project	158
13.1	1. Configure basic server settings https://wiki.bas-ip.com/basiplinken/first-authorization-and-the-server-initial-setup-135955740.html for the correct functioning:	158
13.2	2. Add user profiles for various user and configure their permissions.	158
13.3	3. Add a group for the house/s.	159
13.4	4. Add users to the system.	161
13.5	5. Add devices to the system.	163
13.6	6. Add access restrictions for created groups/users.	165
13.7	7. Add identifiers for users.	168

13.8	8. Add and configure an elevator functioning.	169
13.9	9. Create virtual numbers for users.	173
13.10	10. Guest access providing.	174
13.11	11. Link app usage.....	186
14	Link mobile app.....	188

Bas-IP Link is software for all BAS-IP equipment and realizes centralized access control in residential complexes and office centers with varying complexity. It allows you to flexibly manage all the functionality of the intercom system from anywhere in the world.

You can work with Link on any device: a computer, a tablet, or a smartphone running any operating system. Link is available as a cloud service, while still providing additional privacy, though it can be installed locally for ease of use. Also, the mobile app is available, but with limited features.

All features and options are described further:

- [Getting started](#)(see page 10)
 - [Software installation and launch](#)(see page 10)
 - [Link version update](#)(see page 14)
 - [First authorization and the server initial setup](#)(see page 17)
 - [Supported devices and firmware versions](#)(see page 21)
 - [Link Changelog](#)(see page 22)
- [Dashboard](#)(see page 26)
- [Profile](#)(see page 28)
- [Notifications](#)(see page 29)
- [Users management](#)(see page 31)
 - [Users](#)(see page 31)
 - [Profiles](#)(see page 34)
 - [Groups](#)(see page 43)
- [Access management](#)(see page 50)
 - [Guest access](#)(see page 50)
 - [Schedules](#)(see page 56)
 - [Access restrictions](#)(see page 61)
 - [Identifiers](#)(see page 64)
 - [Access matrix](#)(see page 67)
 - [ACS logs](#)(see page 68)
- [Communications](#)(see page 70)
 - [Conversations](#)(see page 70)
 - [Announces](#)(see page 72)
 - [Info and polls](#)(see page 75)
 - [Emergency alerts](#)(see page 75)
- [Telephony settings](#)(see page 78)
 - [Virtual numbers](#)(see page 78)
 - [Forward rules](#)(see page 81)
 - [Call history](#)(see page 84)
 - [Inbuild call service](#)(see page 86)
- [Devices management](#)(see page 87)
 - [Devices](#)(see page 87)
 - [Logs](#)(see page 94)
 - [Queue tasks](#)(see page 97)
 - [Status](#)(see page 99)
 - [Device initialization](#)(see page 100)
- [Elevator management](#)(see page 102)
 - [Elevators](#)(see page 103)
 - [Elevator logs](#)(see page 106)
 - [Elevators access restrictions](#)(see page 110)
- [Settings](#)(see page 113)
 - [System audit](#)(see page 113)
 - [Backups](#)(see page 115)
 - [General](#)(see page 116)

- [SIP settings](#)(see page 119)
- [SIP trunks](#)(see page 122)
- [Additional settings](#)(see page 125)
- [Mail Templates](#)(see page 130)
- [Licenses](#)(see page 131)
- [System info](#)(see page 132)
- [FAQ](#)(see page 136)
- [Example of the server configuration for a basic project](#)(see page 158)
- [Link mobile app](#)(see page 188)

The software works with:

- multi-apartment entrance panels: AA-01, AA-03, AA-05, AA-07, AA-07B, AA-07B2M, AA-07BC, AA-07BV, AA-07BD, AA-07E, AA-07FB, AA-07FB2M, AA-07FBC2M, AA-07FBV, AA-07FBV2M, AA-07MF, AA-09, AA-09B, AA-09BV, AA-09E, AA-11, AA-11B, AA-11BV, AA-11E, AA-11FBV, AA-11M, AA-12, AA-12B, AA-12FB, AA-12FB2M, AA-14FB, AA-14FB2M, AA-14FBS;
- multi-button entrance panels: BI-02, BI-02B, BI-02FB, BI-02FB2M, BI-04, BI-04B, BI-04FB, BI-04FB2M, BI-06, BI-06B, BI-06FB, BI-06FB2M, BI-08, BI-08B, BI-08FB, BI-08FB2M, BI-12, BI-12B, BI-12FB, BI-12FB2M, BA-04, BA-04BD, BA-04MD, BA-08, BA-08BD, BA-08MD, BA-12, BA-12BD, BA-12MD;
- individual entrance panel: AV-01, AV-01T, AV-01TE, AV-01D, AV-01ED, AV-01MD, AV-01MFD, AV-01BD, AV-01KD, AV-02, AV-02D, AV-02IDE, AV-02IDE, AV-02IPD, AV-03D, AV-03BD, AV-04AFD, AV-04ASD, AV-04FD, AV-04SD, AV-05FD, AV-05SD, AV-07T, AV-07B, AV-08FB;
- access controllers: CR-02BD;
- indoor video entry phone (monitors): AQ-07, AQ-07L, AQ-07LA, AQ-07LL, AK-10, AK-10L, AK-10LP, AT-07L, AT-10, AT-10L, AM-02, AZ-07LL, AU-04LA, SP-03, SP-03F.

1 Getting started

Further, you can find the basic information and first configuration instructions:

- [Software installation and launch](#)(see page 10)
- [Link version update](#)(see page 14)
- [First authorization and the server initial setup](#)(see page 17)
- [Supported devices and firmware versions](#)(see page 21)
- [Link Changelog](#)(see page 22)

1.1 Software installation and launch

1.1.1 Hardware recommendations

-
- 64-bit processor with SLAT and Hyper-V support

Whether your processor supports Intel virtualization technology can be found at <https://www.intel.com/content/www/us/en/support/articles/000005486/processors.html>

- If Linux: Kernel is not older than 3.10
- If Windows: 10 Pro or higher
- 8 GB RAM
- 100 GB HDD

1.1.2 General information

First, the Link must be installed and configured on a computer to work correctly and provide access in a web browser. It can be done with the help of:

- multiple Docker containers and deployed with Docker Compose;
- Virtualbox virtual machine image;

Further, you will find detailed installation steps for both methods.

There are several Link server variations, so before the installation choose the one that is required:

- Link without SIP and without web proxy;
- Link without SIP but with web proxy;
- Link with SIP but without web proxy;
- Link without SIP but with web proxy;

Versions with SIP are recommended only for Linux OS installation.

Versions with web proxy are recommended to use if Link is going to be used as a public server and the connection will be via secure https protocol.

Versions without web proxy are recommended to use if Link is going to be used in a local network and the connection will be via http protocol.

In the beginning, you get Link basic version, and further you can buy access to the Link License server to expand software functionality. More details about functionality can be provided with licenses you can find in the corresponding [tab](#)¹.

1.1.3 Installing Link under Linux using Docker

1. Install Docker for your distro. The example below uses the installation for Ubuntu.

```
# Remove old versions

sudo apt-get remove docker docker-engine docker.io containerd runc

# Configure the repo
## Update apt index and install dependencies

sudo apt-get update

sudo apt-get install \
  apt-transport-https \
  ca-certificates \
  curl \
  gnupg \
  lsb-release

## Add Docker GPG key

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/docker-archive-keyring.gpg

## Add repo

echo \
  "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]
https://download.docker.com/linux/ubuntu \
```

¹ <https://wiki.bas-ip.com/basiplinken/licenses-135956024.html>

```
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

# Install Docker

sudo apt-get update

sudo apt-get install docker-ce docker-ce-cli containerd.io
```

2. Install `docker-compose`² for your distro.

```
# Download docker-compose

sudo curl -L "https://github.com/docker/compose/releases/download/1.29.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

# Grant execute permission for the file

sudo chmod +x /usr/local/bin/docker-compose

# Add symlink

sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
```

3. Clone the necessary project from our [GitHub](https://github.com/basip/link)³ with the help of command.

```
git clone https://github.com/basip/link.git
```

4. Create the necessary volumes in advance, with help of the command:

```
docker volume create name
```

Name changes depending on the volume name to be created. The list of required volumes (with external: true values) you can find at the end of the `docker-compose.yml` file.

² <https://docs.docker.com/compose/install/>

³ <https://github.com/basip/link>


```

198     - MYSQL_DATABASE=kamallio
199 volumes:
200   - sip-proxy-data:/var/lib/mysql
201 ports:
202   - "43306:3306/tcp"
203 logging:
204   driver: json-file
205   options:
206     max-size: "10m"
207     max-file: "5"
208   command: ["--innodb-buffer-pool-size=2G", "--innodb-log-file-size=256M"]
209 networks:
210   link-internal:
211     internal: true
212
213 volumes:
214   app-data: { external: true }
215   system-logs: { external: true }
216   app-storage: { external: true }
217   app-ssl-certs: { external: true }
218   device-broker-log: { }
219   device-broker-settings: { }
220   device-broker-app: { }
221   sip-proxy-data: { }
222   sip-proxy-app: { }
223   sip-node-app: { }
224   sip-proxy-log: { }

```

So, according to the example, the following commands must be done:

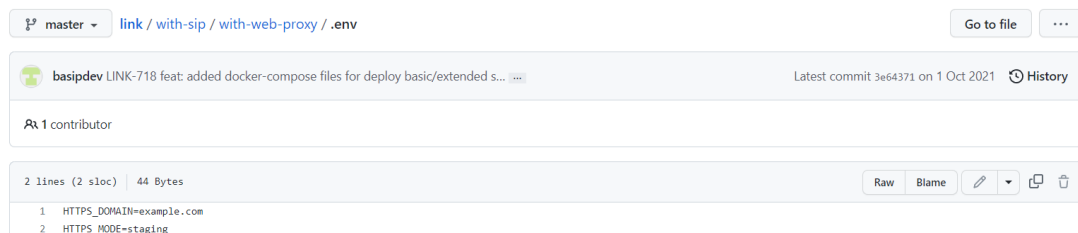
```

docker volume create app-data
docker volume create app-storage
docker volume create system-logs
docker volume create app-ssl-certs

```

If you are installing **a version with a web proxy**:

1. Copy the **env.example** file and name this copy as **.env**.
2. In the **.env** file you must enter the following data:
 - your Link server **address**, e.g. link.bas-ip.com⁴ for HTTPS_DOMAIN field;
 - **production** for HTTPS_MODE field;



The screenshot shows a GitHub commit for the file `.env` in the repository `basipdev/link / with-sip / with-web-proxy / .env`. The commit message is "basipdev LINK-718 feat: added docker-compose files for deploy basic/extended s...". The commit was made on 1 Oct 2021. The file content is as follows:

```

2 lines (2 sloc) | 44 Bytes
1 HTTPS_DOMAIN=example.com
2 HTTPS_MODE=staging

```

These parameters are required for correct encryption certificates to work.

5. Go to the folder of the version you want to install. For example, for the version without SIP, the command is:

⁴ <http://link.bas-ip.com>

```
cd link/without-sip
```

6. Run the project.

```
docker-compose up -d
```

You can **improve the productivity of extensive projects** by doing the following Docker configuration:

Change the **userland-proxy** attribute to **false** in the docker configuration **/etc/docker/daemon.json** file. If there is no such file, then create it with the content

```
{"userland-proxy": false}
```

1.1.4 Used ports

The application uses the following ports:

- 5060 TCP/UDP: unencrypted SIP traffic port;
- 5061 TCP: port for SIP using TLS;
- 80 TCP: HTTP port;
- 443 TCP: HTTPS port;
- 6001 TCP: WebSocket port;
- 10000-20000 UDP: RTP ports for audio/video;
- 1883 TCP: unencrypted MQTT;
- 8883 TCP: encrypted MQTT;

If SIP proxies and nodes are running on more than one server with the Link server application, then the following ports must be forwarded to them:

- 48080: SIP proxy management port;
- 48081: SIP node management port;

1.2 Link version update

To update the Link using Docker you must:

1. Check the current version of the server (in the left low corner of the Login page in the Link web interface).
2. In the [repository](#)⁵ check if there are no update peculiarities for the version you want to install. If there is, read the attached manual and complete the instructions.
3. Login to your server via SSH.

⁵ <https://github.com/basip/link>

4. Login as a superuser: **sudo su**, and enter the same password one more time.
5. Follow the directory where your Link is:

```
cd/home/link/
```

6. Choose the correct type of Link server. If you use the Link:
 - a. with SIP, but not using the domain name (e.g. <http://176.215.90.19>⁶, <http://3.111.25.45>⁷) perform:

```
cd with-sip
```

- b. with SIP, and with domain name (e.g. <https://preview.intercom.team>⁸) perform:

```
cd with-sip/with-web-proxy
```

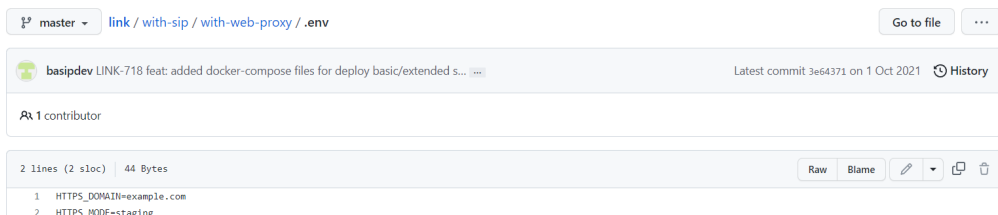
- c. without SIP, and without domain (simply management features) perform:

```
cd without-sip
```

- d. without SIP, but with domain (simply management features + SSL) perform:

```
cd without-sip/with-web-proxy
```

If you use the Link with-web-proxy, make sure, that the **.env** file in the current directory still contains your changes: vi **.env**
HTTPS_DOMAIN='your domain'
HTTPS_MODE=production
IMAGE=latest



```
master - link / with-sip / with-web-proxy / .env
basipdev LINK-718 feat: added docker-compose files for deploy basic/extended s...
Latest commit 3e64371 on 1 Oct 2021
1 contributor
2 lines (2 sloc) | 44 Bytes
1 HTTPS_DOMAIN=example.com
2 HTTPS_MODE=staging
```

If there are no changes, please, write down your data.

2. In case of updating from the **Link version lower than 1.2.126**, please, copy the **.env** file (as described in [Step 4](#)(see page 10)) and make changes after that: cp **.env.example .env**

7. Stop the current Link server with the command:

⁶ <http://176.215.90.19/>

⁷ <http://3.111.25.45/>

⁸ <https://preview.intercom.team/>

```
docker-compose down
```

It should be run in the directory with the corresponding type that you are use.

- Update installation images from which the new Link version will be deployed:

```
docker-compose pull
```

- Start your updated Link server in some seconds: `docker-compose up -d`

```
docker-compose up -d
```

- As a result new version will start functioning. Make sure that all of your containers are started and running properly:

```
docker ps
```

- Login to the Link using the previous IP/domain.

Info

If you have **trouble** running the Pull command because of the file on the machine with modifications that are not in Git, it is necessary to remove these changes and only then pull the update.

```
root@preview-intercom-team:/home/link/with-sip/with-web-proxy# git pull https://github.com/basip/link.git
From https://github.com/basip/link
 * branch          HEAD          -> FETCH_HEAD
Updating 5050463..14806c4
error: Your local changes to the following files would be overwritten by merge:
  with-sip/docker-compose.yml
  with-sip/with-web-proxy/docker-compose.yml
  without-sip/docker-compose.yml
  without-sip/with-web-proxy/docker-compose.yml
Please commit your changes or stash them before you merge.
Aborting
```

Try the following options:

- in this directory, run the following command with a dot at the end followed by a space. This will clean up any changes

```
git checkout.
```

- for force reset perform:

```
git reset --hard
```

1.3 First authorization and the server initial setup

After successful software installation, open the browser and go to the server address where the Link is installed. At the top right corner, you can change the interface language to English or Russian.

Also, you can find the current software version in the lower right corner.

Enter default values to get access to the Link for the first time.

Info

Default values to enter the web interface:

Login: admin@bas-ip.com⁹

Password: **qwerty11!@**

After logging in to the server you must complete the server initial setup for its further functioning.

1.3.1 Server initial setup

1. In the sidebar scroll to the **Settings** section.
2. Open the **General** tab and enter the following general settings:
 - your project name;

⁹ <mailto:admin@bas-ip.com>

- project description (if necessary);
- server URL, e.g., <https://link.example.com>;

If you don't have a server domain name (link.example.com¹⁰), enter the IP address of a device where the Link software is installed. Or if you use a Virtual box, enter the IP address given to the system inside the virtual box image. In this case, the server URL is <http://192.168.1.1>, for example.

- enable **Registration is allowed by reference** field to be able to invite new users;
- **allow** users to self-**recover** their **password** by ticking the corresponding box. Otherwise, only an administrator will be able to do it;
- select system language: English, Russian.

The screenshot shows the 'General' settings page in the BAS-IP Link application. The left sidebar contains a menu with 'General' highlighted. The main content area is titled 'General' and includes the following fields and options:

- Project name:** BAS-IP link
- Description:** project link
- Server url:** <https://link.bas-ip.com>
- Registration is allowed by reference.
- Password recovery allowed
- System language:** English

3. Enter **mail server settings** to be able to send registration link and emails to users:

- for the **mail server type** field select smtp (outgoing mail server);
- **mail server address**, e.g. smtp.gmail.com¹¹;
- mail server **port** number;
- SMTP server **username** (email address from which letters will be sent);
- email (from which letters will be sent) **password**;
- **sender email** (coincides with SMTP server username);
- **sender name** that will be indicated in letters;
- preferred **encryption type**: ssl or tls;

¹⁰ <http://link.example.com>

¹¹ <http://smtp.gmail.com>

Mail Server settings

Mail server type	smtp	
Mail server	smtp.gmail.com	Port 587
User name	linkbasip@gmail.com	Password
Sender's email	linkbasip@gmail.com	Sender's name linkbasip@gmail.com
Encryption	tls	
Send test e-mail	➤	

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.).

Tip

After entering the **mail server settings** check the correctness by **sending test email**.

4. Enter the **system administrator email** to get further information about system functioning. More about notifications for administrator read [here](#)¹².
5. Confirm changes and the end of the page.
6. Go to the **SIP settings** tab and enter the following data:
 - only **server external IP address** if a server with public IP only is used;
 - both **server external** and **internal IP addresses** if the server is behind NAT. In this case, server external address is router IP address, and the internal value is the server (computer) IP address where the Link is installed;

¹² <https://wiki.bas-ip.com/basiplinken/general-135955998.html>

If your Link system is more complex: SIP nodes are deployed on another server or a separate server with a node is behind NAT you must enter additional settings. Detailed information about them can be found [here](#)¹³.

In other cases, the value of the server external IP address will be used for blank fields.

Also, you can enable the feature of **automatic creation of forward rules for apartment group user/s**, sending them to device/s, and data correction for device/s (if there are some changes in virtual numbers or logical address). More details about the feature you can find [here](#)¹⁴.

SIP settings

Server external IP address

95.216.16.16

Server internal IP address

Port

5060

Video bitrate

512kb

RTP ports from

10001

RTP ports to

20001

7. Confirm changes and the end of the page.

! Warning

After entering all the data, you need to create and register a new account instead of the default user. Detailed information on how to register a new user you can find [here](#)¹⁵.

After logging in to your account, go to the **Users** section and **delete** admin@bas-ip.com¹⁶ user. This must be done to avoid unauthorized access to your server by third parties. Otherwise, any user who reads the information above will be able to access the server and make any changes to its configuration.

¹³ <https://wiki.bas-ip.com/basiplink/en/sip-settings-83460880.html>

¹⁴ <https://wiki.bas-ip.com/basiplinken/sip-settings-135956014.html>

¹⁵ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

¹⁶ <mailto:admin@bas-ip.com>

1.4 Supported devices and firmware versions

Link version	Type of device	Models	Device minimum firmware version
1.1.x	Multi- part ment panels	AA-01, AA-03, AA-05	2.0.0
		AA-07, AA-07B, AA-07B2M, AA-07BC, AA-07BV, AA-07BD, AA-07E, AA-07FB, AA-07FB2M, AA-07FBC2M, AA-07FBV, AA-07FBV2M, AA-07MF, AA-09, AA-09B, AA-09BV, AA-09E, AA-11, AA-11B, AA-11BV, AA-11E, AA-11FBV, AA-11M, AA-12, AA-12B, AA-12FB, AA-12FB2M, AA-14FB, AA-14FB2M, AA-14FBS	3.7.0
	Multi- button panels	BI-02, BI-02B, BI-02FB, BI-02FB2M, BI-04, BI-04B, BI-04FB, BI-04FB2M, BI-06, BI-06B, BI-06FB, BI-06FB2M, BI-08, BI-08B, BI-08FB, BI-08FB2M, BI-12, BI-12B, BI-12FB, BI-12FB2M	3.7.0
		BA-04, BA-08, BA-12	2.0.0
		BA-04BD, BA-08BD, BA-12BD	2.3.0
		BA-04MD, BA-08MD, BA-12MD	3.3.0
	Individual panels	AV-01, AV-01T, AV-01TE, AV-02	2.0.0
		AV-01D, AV-01ED, AV-01MD, AV-01MFD, AV-01BD, AV-01KD, AV-02D, AV-02IDE, AV-02IDE, AV-03D, AV-03BD, AV-04AFD, AV-04ASD, AV-04FD, AV-04SD, AV-05FD, AV-05SD, AV-07T, AV-07B, AV-08FB;	2.3.0
		AV-02IPD	3.3.0
	Access controllers	CR-02BD	2.3.0
	Indoor monitors	AQ-07, AQ-07L, AQ-07LA, AQ-07LL, AK-10, AK-10L, AT-07L, AT-10, AT-10L, AM-02, AZ-07LL, AU-04LA	4.2.1
		AT-10	5.1.0

Link version	Type of device	Models	Device minimum firmware version
		AK-10LP	5.4.0
	Hands-free	SP-03	1.1.0
		SP-03F	1.12.0

1.5 Link Changelog

Here you can find the list of all changes made to a project.

- [1.2.180](#)(see page 22)
- [1.2.177](#)(see page 22)
- [1.2.174](#)(see page 23)
- [1.2.173](#)(see page 23)
- [1.2.172](#)(see page 23)
- [1.2.170](#)(see page 23)
- [1.2.169](#)(see page 23)
- [1.2.168](#)(see page 23)
- [1.2.167](#)(see page 23)
- [1.2.165](#)(see page 23)
- [1.2.161](#)(see page 23)
- [1.2.159](#)(see page 24)
- [1.2.158](#)(see page 24)
- [1.2.157](#)(see page 24)
- [1.2.155](#)(see page 24)
- [1.2.150](#)(see page 24)
- [1.2.149](#)(see page 24)
- [1.2.148](#)(see page 24)
- [1.2.146](#)(see page 24)
- [1.2.145](#)(see page 24)

1.5.1 1.2.180

- Implemented SOS functionality

1.5.2 1.2.177

- Added ability to enable/disable call forwarding for an apartment
- Added link to the user agreement
- Removed unused buttons during registration
- Improved process of uploading SIP registration settings to devices

1.5.3 1.2.174

- Improved server and mobile app interaction when calling

1.5.4 1.2.173

- Fixed sending announces or polls functioning

1.5.5 1.2.172

- Updated the process of uploading SIP registration settings to devices
- Improved video delivery quality to mobile clients
- Fixed bug with displaying the Delete button in conversations for users who do not have this permission
- Fixed EVRC-IP interaction with identifiers added to the Link
- Fixed error display when confirming e-mail by a user who was deleted from Link

1.5.6 1.2.170

- Refactored mobile API for managing forwards

1.5.7 1.2.169

- Fixed bug with setting restriction period for guest identifiers on iOS

1.5.8 1.2.168

- Fixed automatic sending of apartment entities added in the Link to CR-02BD

1.5.9 1.2.167

- Fixed bug (Device problem) when using guest URL in Link
- Fixed e-mail uniqueness bug when adding/editing a user

1.5.10 1.2.165

- Corrected description of the panel features for the endpoint
- Fixed sending of announcements, after dividing permissions and profiles for multiple projects on the same server
- Decreased expiration time of registration for SIP number to 30 sec
- Optimized API

1.5.11 1.2.161

- Added support for 6th Model of face recognition

1.5.12 1.2.159

- Implemented the ability to connect the SIP server to trunks via Twilio

1.5.13 1.2.158

- Added ability to host several small projects on 1 server

1.5.14 1.2.157

- Implemented a set of default values for Whitelabel
- Added profile permission to get Whitelabel settings

1.5.15 1.2.155

- Added option to subscribe to family members actions in the mobile app
- Added ability to revoke identifiers
- Added validation of SIP login/password settings before sending to the device
- Learned the possibility of customizing server emails

1.5.16 1.2.150

- Fixed and tested API

1.5.17 1.2.149

- Added automatic data update for the user about number forwarding for the group the user is assigned to

1.5.18 1.2.148

- Added incoming call ringtones
- Fixed the display of the number name for incoming calls
- Fixed the display of contacts avatars
- Fixed bug with accepting incoming calls if notifications are disabled in the browser

1.5.19 1.2.146

- Refactored the functionality of the interaction with devices

1.5.20 1.2.145

- Fixed bug when deleting virtual numbers
- Corrected translations of device and elevator logs
- Fixed the display of assigned to groups virtual numbers
- Fixed custom groups generation
- Fixed virtual number display of deleted user

- Fixed avatar change for user profile
- Fixed bug with adding numbers to the call queues for forwards
- Fixed display of the entries number in the table on the Info and polls page

2 Dashboard

After successful authorization, you will access the control panel with the main system widgets and counters of added users added, identifiers, etc. In the section you can get information about:

- number of registered **users**;
- number of **identifiers** (an access code, a card, a UKEY, a QR code, etc.) added to the system;
- number of created **guest** (temporary) **passes**. By clicking Grant Access you can quickly create and share guest identifier. Detailed instructions are [here](#)¹⁷;
- **devices** connected to the system, their statuses and IP addresses. In this section you can [initialize device](#)¹⁸ (only for SP-03), [restart device queue](#)¹⁹ and [synchronize device data](#)²⁰;
- all events (**logs**) that happened with added devices. In the section you can also refresh, filter and export data (detailed information about these options you can find [here](#)²¹).

The screenshot shows the dashboard interface with the following data:

Name	Status	IP address	Actions
Unit 1 Entrance		192.168.1.2	🔍 📄 🔄
Monitor AQ-07	offline(2021-10-12 15:45)	91.225.165.47	🔍 📄 🔄
Entrance panel 1.46	offline(2021-12-28 16:53)	91.225.165.47	🔍 📄 🔄
Uncle Bob panel	offline(2021-09-20 22:39)	192.168.1.1	🔍 📄 🔄
AQ07L 4 flat	offline(2021-09-30 17:17)	91.225.165.47	🔍 📄 🔄

✓ Tip

You can access Users, Identifiers, and Guest access tabs by clicking corresponding widgets.

You can **edit** the widgets **display** by clicking the **Widgets** button in the upper right corner and selecting the menus you want to see.

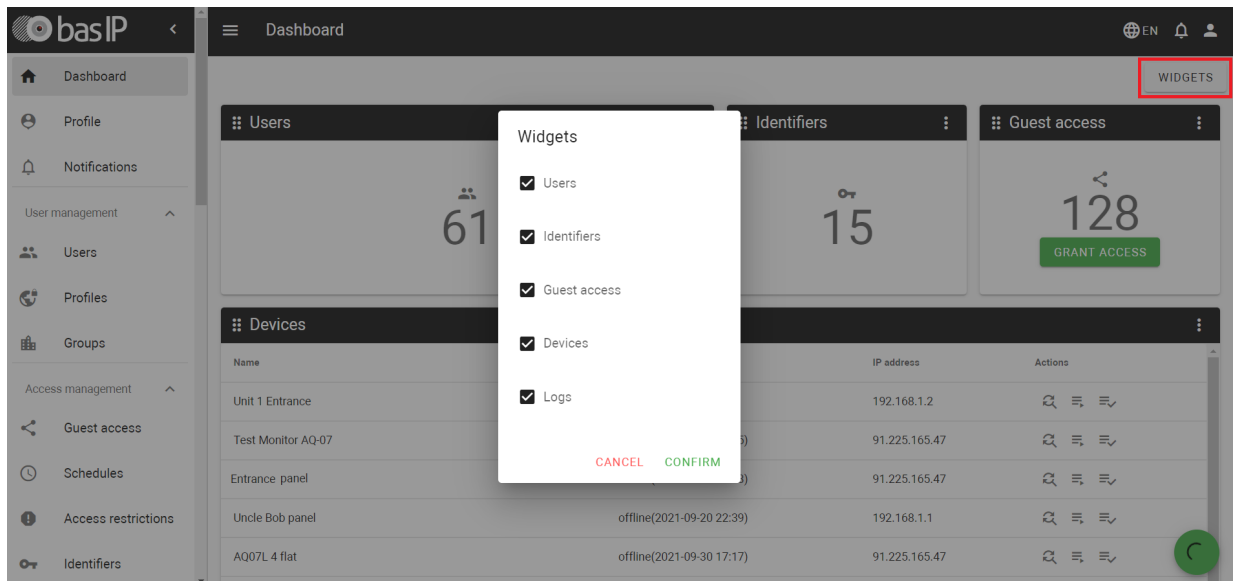
¹⁷ <https://wiki.bas-ip.com/basiplinken/guest-access-135955799.html>

¹⁸ <https://wiki.bas-ip.com/basiplinken/device-initialization-135955953.html>

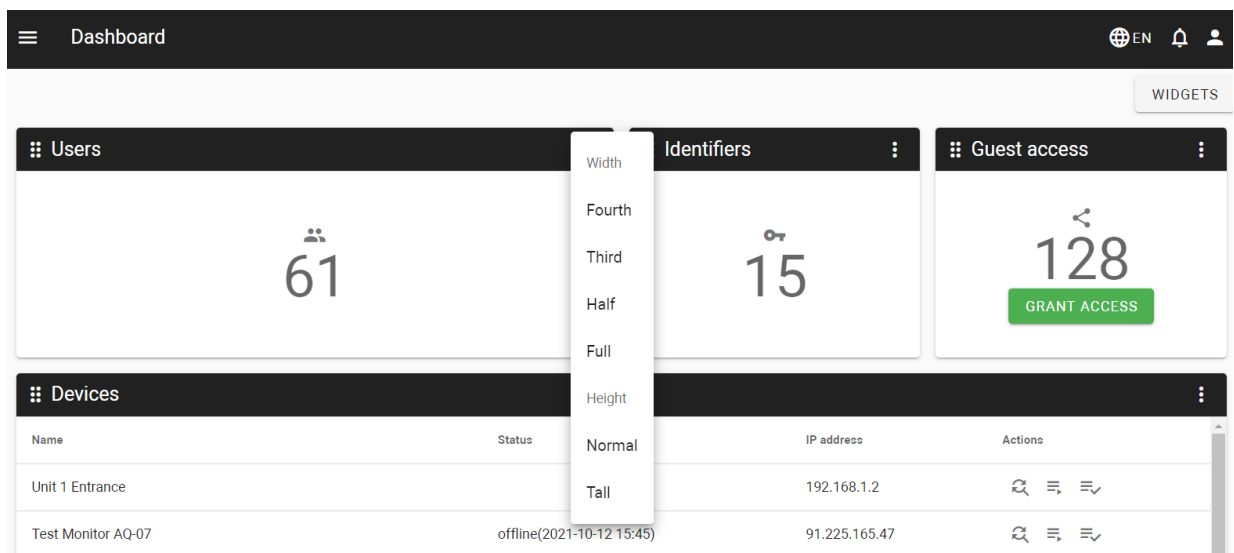
¹⁹ <https://wiki.bas-ip.com/basiplinken/queue-tasks-135955941.html>


²⁰ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

²¹ <https://wiki.bas-ip.com/basiplinken/logs-135955936.html>



Also, you can **resize sections** by clicking 3 dots in the widget upper right corner and selecting preferred height and width.



It is possible to **change widgets layout** by clicking and holding  button of a section and dragging it on the desired place.

3 Profile

Each confirmed user has a personal profile. This section displays the user basic data (with the possibility of editing):

- user name;
- their phone number (if required);
- their address (if required);
- preferred time display format;
- timezone;
- a user virtual number (can be assigned from the created in the [corresponding tab](#)²²) for SIP calls;
- preferred identifier representation format: Decimal or HEX numeral system;
- profile photo (if required);

When all data is entered, click **Confirm** to save changes.

The screenshot shows the 'Profile' page in the basIP interface. The page title is 'Profile' and the user is identified as 'admin@bas-ip.com - Administrator'. The profile information is displayed in a grid format:

User name Administrator	Time format YYYY-MM-DD	Identifier representation Decimal
Phone	Timezone UTC+03:00	
Address	Dialer virtual number	

At the bottom right of the form, there is a green 'CONFIRM' button. The left sidebar contains navigation options: Dashboard, Profile (selected), Notifications, User management (Users, Profiles, Groups), and Access management (Guest access, Schedules, Access restrictions, Identifiers).

²² <https://wiki.bas-ip.com/basiplinken/virtual-numbers-135955892.html>

4 Notifications


In this tab, you get notifications about the success/failure of some processes or connected with your profile, e.g sending new settings to devices, statuses of created announcements, or received announcements/polls, etc. This will help you not to control some processes in real-time but check only the result.

ALL	NORMAL	IMPORTANT	ACS	
				⚙️
				2022-09-29 13:33
				2022-08-16 21:33
				2022-08-16 21:33
				2022-07-19 12:44
				2022-06-23 17:27
				2022-06-13 13:39
				2022-06-06 19:27
				2022-06-02 20:57
				2022-05-11 17:25
				2022-02-01 14:21
				2022-02-01 14:17



You can monitor **all** notifications in the corresponding section or mark some messages (about user or device activity) as **important** and receive prioritized notifications. All other notifications not marked as important are displayed in the **Normal** tab.

ALL	NORMAL	IMPORTANT	ACS	
				⚙️
				2022-10-25 10:32
				2022-10-25 10:30

4.1 How to configure important notifications

1. Go to the **Notifications** tab.
2. Click  in the upper right corner.
3. Select important notifications **type**.
4. Select desired **color** and **icon** for notification.
5. Select **user/s** whose actions you want to be notified about.
6. Select **device/s** with those you want to receive notifications about interactions.

7. Confirm settings.

ACS	
Type Important	Example
Color red	
Icon 	
Users Administrator	
Devices AQ07L 4 flat	
CONFIRM	

5 Users management

In this section, you can add, delete and modify profiles with various permissions, manage users, and add/edit groups for buildings, or residential complexes.

- [Users](#)(see page 31)
- [Profiles](#)(see page 34)
- [Groups](#)(see page 43)

5.1 Users

- [How to register a new user](#)(see page 31)
- [How to activate a user profile](#)(see page 33)
- [Users filtering](#)(see page 34)

In this tab, you can add new users, manage already added ones, and check important information about them.




MATCH ALL		+ ADD FILTER								DELETE SELECTED
<input type="checkbox"/>	ID	Name	E-mail	Phone	Activation status	Profile	Groups			
<input type="checkbox"/>	1	Administrator	admin@bas-ip.com		No	Administrator	Home group			
<input type="checkbox"/>	2	Bob	bob.stilinski11@gmail.com		Yes	Administrator	Home group, Test residential complex, Building #1, Building #2, Apartment #1			
<input type="checkbox"/>	4	John	test@bas-ip.com	1811	Yes	User	Home group			
<input type="checkbox"/>	9	Green	greenfantom77+@gmail.com		Yes	User	Green			
<input type="checkbox"/>	10	Alex James	alex@gmail.com		No	User	Building #2, Apartment #1			
<input type="checkbox"/>	11	Andy Heart	adny.h@gmail.com		No	User	Home group			
<input type="checkbox"/>	86	Test User	link-test@bas-ip.com		No	User	Home group			

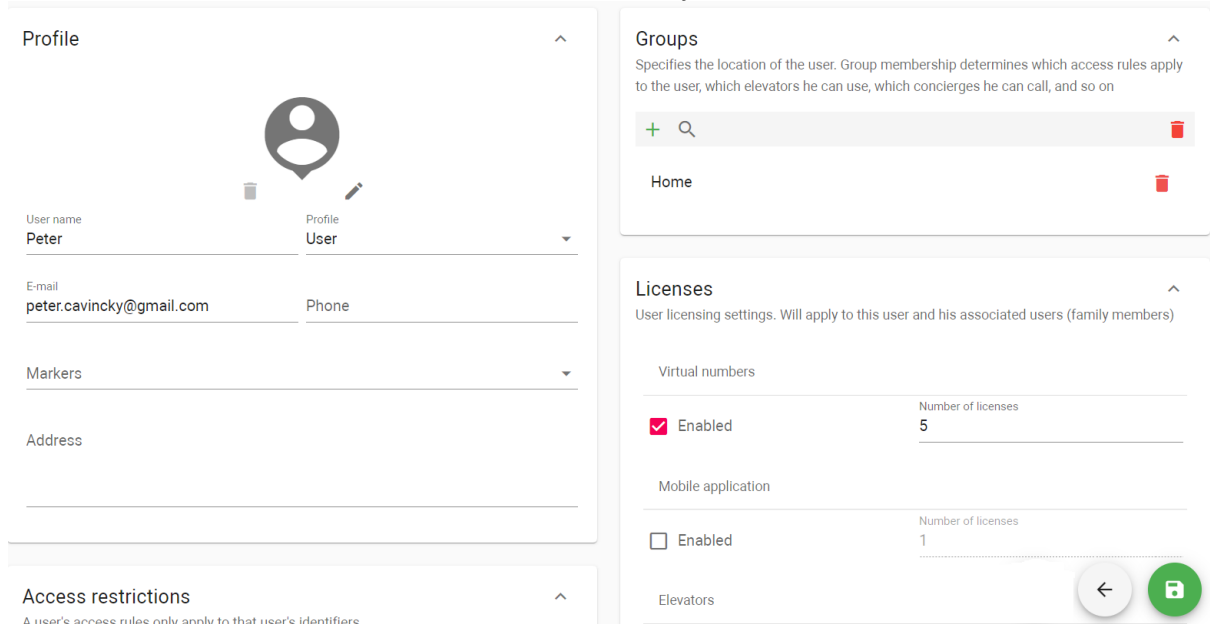
5.1.1 How to register a new user

1. Open the **User** tab of the User management section.
2. Click **plus** icon in the left low corner.
3. Enter a user **name**.
4. Add user photo if necessary.
5. Select the **profile**²³ from created to give the user the required permissions.
6. Enter the user **email** to send the registration link.
7. Enter user **phone** number if necessary.
8. If required, select a **marker** for the user.
9. If necessary, enter user **address**.
10. Add a user to a corresponding **group**²⁴ or create a new one for this user.

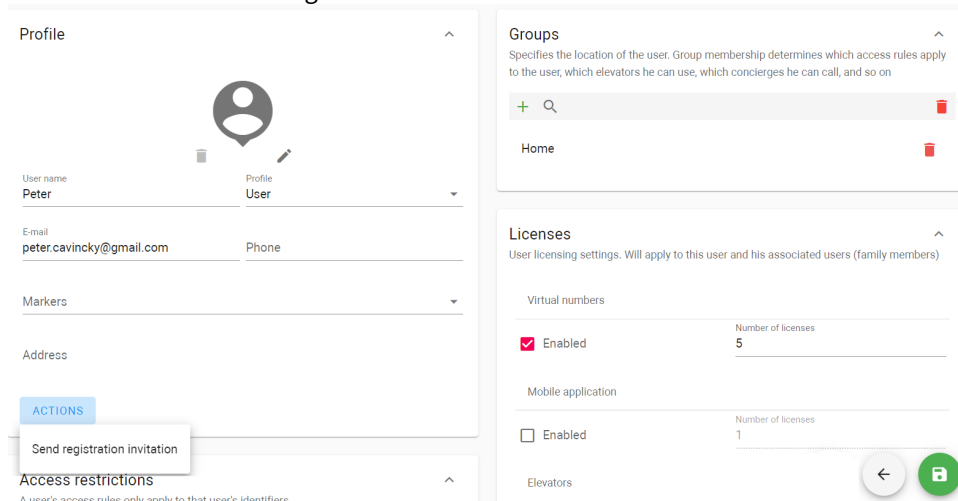
²³ <https://wiki.bas-ip.com/basiplinken/profiles-135955778.html>

²⁴ <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>

11. Select  from already added or create [access restrictions](#)²⁵. After clicking  you will be redirected to the [corresponding tab](#)²⁶ where it is possible to create restrictions.
12. Select  [identifier/s](#)²⁷ available for the user.
13. Set available for user **licenses** that they purchased.
14. Click the **Save** button in the left low corner when all necessary data is entered.



15. Open created user profile again.
16. Click **Actions** and send a registration invitation to the user.



17. Close the profile.

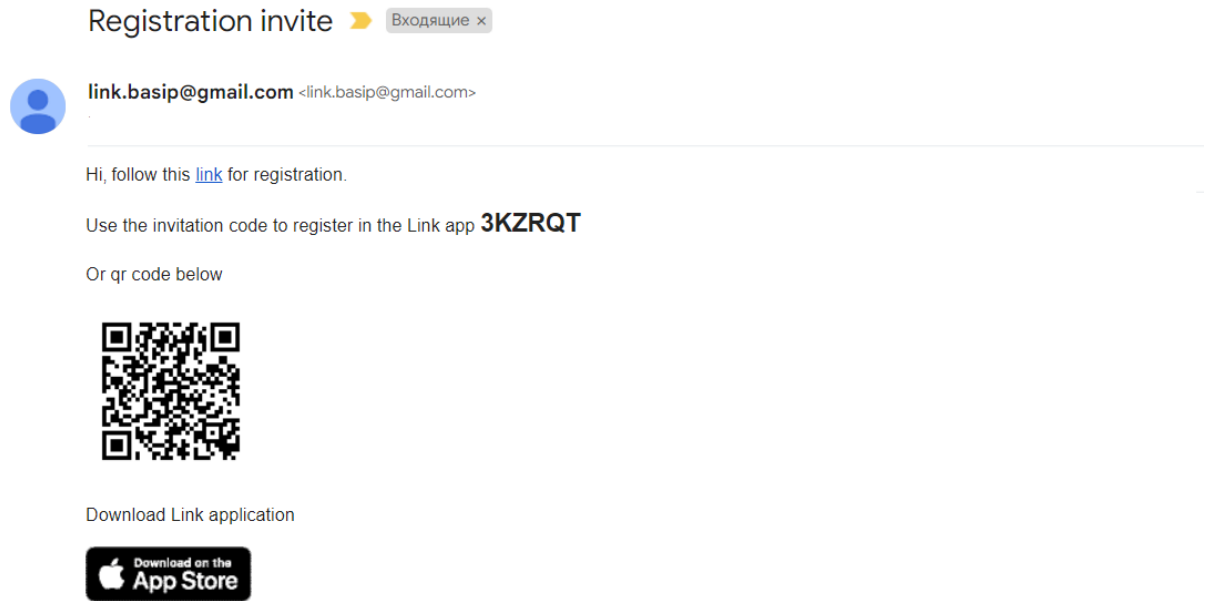
After receiving the invitation user must activate the profile. Detailed steps are further.

25 <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>
 26 <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>
 27 <https://wiki.bas-ip.com/basiplinken/identifiers-135955834.html>

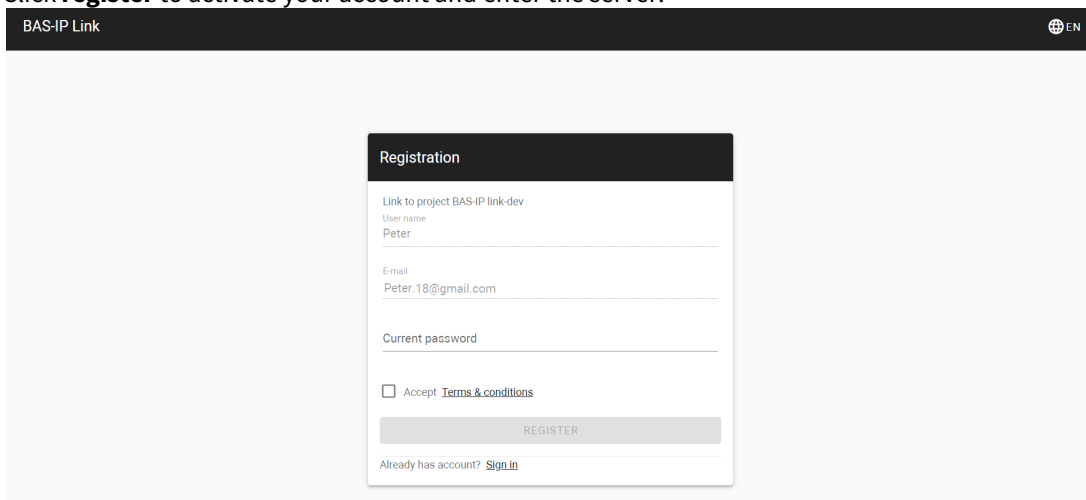
Also, when you open user entry after creating, you can check not only the information that you entered, and but Elevator access rules, Virtual numbers, [Mobile app clients](#)²⁸ available for the user, and also users (family members) invited by this user (can be done via the mobile app).

5.1.2 How to activate a user profile

1. Open your email and find the invitation letter from the Link server.
2. Follow the **link** indicated in the letter.



3. Create a **password** for your account.
4. Accept **Terms & Conditions**.
5. Click **register** to activate your account and enter the server.















²⁸ <https://wiki.bas-ip.com/basiplinkapp/bas-ip-link-110561562.html>

6. If you are going to register via the Mobile app, complete [these](#)²⁹ steps.











To enter your account next time, you are required to enter your email and password.

5.1.3 Users filtering

With the help of  and  buttons, you can edit or delete restrictions. Also, there is a filter by name, profile, groups, phone, e-mail, and marker. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or contain (**has**) it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

MATCH ALL								PROFILE IS USER	+ ADD FILTER	SAVE AS	DELETE SELECTED	
<input type="checkbox"/>	ID	Name	E-mail	Phone	Activation status	Profile	Groups					
<input type="checkbox"/>	4	John	test@bas-ip.com	1811	Yes	User	Home group					
<input type="checkbox"/>	9	Green	greenfantom777+@gmail.com		Yes	User	Green					
<input type="checkbox"/>	10	Alex James	alex@bas-ip.com		No	User	Building #2, Apartment #1					
<input type="checkbox"/>	11	Andy Heart	adny.h@gmail.com		No	User	Home group					
<input type="checkbox"/>	86	Test User	link-test@bas-ip.com		No	User	Home group					

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL								PROFILE IS USER	+ ADD FILTER	SAVE AS	SEGMENTS	DELETE SELECTED	
<input type="checkbox"/>	ID	Name	E-mail	Phone	Activation status	Profile	Groups						
<input type="checkbox"/>	4	John	test@bas-ip.com	1811	Yes	User	Home group						
<input type="checkbox"/>	9	Green	greenfantom777+@gmail.com		Yes	User	Green						
<input type="checkbox"/>	10	Alex James	alex@bas-ip.com		No	User	Building #2, Apartment #1						
<input type="checkbox"/>	11	Andy Heart	adny.h@gmail.com		No	User	Home group						
<input type="checkbox"/>	86	Test User	link-test@bas-ip.com		No	User	Home group						

5.2 Profiles

Not every user requires access to all menus and settings of the Link server. In the section, you can create general profiles (roles) for different user types and provide more or fewer permissions for them. These profiles will be applied to all users.

²⁹ <https://wiki.bas-ip.com/basiplinkapp/registration-110561569.html>

- [How to create a profile](#)(see page 36)
- [Independent projects on the one server](#)(see page 37)
- [How to create a root group administrator profile](#)(see page 37)
- [Example of server configuration for hosting several projects](#)(see page 39)

Below there are examples of the most common profiles that can be useful for your projects:

- **administrator:** users that control the whole system and have all possible permissions to perform system installation, configuration, and support;
- **concierge:** users that interact with residents and visitors, manage residents group(s), devices, and access conditions, send announcements and messages;
- **user:** an ordinary profile that has access to a personal account where it's possible to change personal settings, interact with messages, check the status of personal/shared devices, and their logs, change device settings, generate guest passes and check available identifiers and access restrictions.

MATCH ALL		+ ADD FILTER		DELETE SELECTED	
<input type="checkbox"/>	ID	Name	Description		
<input type="checkbox"/>	1	Administrator	admin		
<input type="checkbox"/>	2	User			
<input type="checkbox"/>	3	Concierge			

Total records: 5

Rows per page: 25 Records 1 - 5 of 5

Here is the list of all possible permissions that can be provided for profiles:

- **access restrictions:** can view/create/edit/delete access rules, can view all access rules;
- **announces:** can create/edit/delete/send announces, can view all/particular announces;
- **backups:** can create/delete/view/apply backup, apply/download backup file;
- **call history:** can view all call history;
- **calls:** can receive call like concierge, can call to all, can call to intercom;
- **conversations:** can view all conversations, can send messages to all, can create conversation/conversation message, can delete conversation, can accept messages from descendant users;
- **devices:** can view device tasks/status, can create/edit/delete/view devices, can view all devices, can view device events;
- **elevators:** can create/edit/delete elevator, can view elevators/all elevators, can view all elevator access rules;
- **emergency alerts:** can view particular/all emergency alerts, can create/edit/delete/playback emergency alerts;
- **forward rules:** can view/create/edit/delete forward rules, can view all forward rules;
- **groups:** can view all groups, can create root group, can delete/edit group, can create group-descendant;
- **identifiers:** can view all/particular identifiers; can create/edit/delete identifier; can create guest identifier, can import/export identifiers, can view ACS logs;
- **licenses:** can manage licenses;
- **markers:** can view/create/edit/delete/apply marker, can view all markers;

- **profiles:** can view roles, can create/edit/delete role, can grant permissions more than his own, can view all roles, not available roles only;
- **project settings:** can change/view project settings, can import device backup data, can view management company info;
- **schedule:** can view/create/edit/delete schedule, can view all schedules;
- **system:** can view audit/system info;
- **users:** can edit/view all users, create/edit/delete user;
- **virtual numbers:** can create/edit/delete/activate virtual number, can mark system virtual numbers, can view all virtual numbers;

5.2.1 How to create a profile









1. Go to the **Profiles** tab of the User management section.
2. Click the plus icon (in the low left corner).
3. Enter a profile **name** and add a description (if required).
4. Select the **permissions** (and, corresponding, the functionality) you want this user type to have.
5. Add other available profile types that this type can edit (if necessary). For example, for the administrator type, all profiles can be added in this section.
6. Save data by clicking the corresponding button in the left low corner.

The screenshot displays the 'Profiles' management interface. It is divided into three main sections:

- General:** Contains fields for 'Name' (filled with 'Pro User') and 'Description' (filled with 'User uses a paid subscription and has an extended list of permissions.').
- Available profiles:** A section for selecting additional profile types. It includes a search bar and a list with one item, 'User', which has a red trash icon next to it.
- Permissions:** A grid of permission categories. The 'Can view all call history' option is checked with a red square. Other categories include Access restrictions, Backups, Calls, Devices, Emergency alerts, Group types, Identifiers, Markers, Project settings, System, Virtual numbers, Announces, Call history, Conversations, Elevators, Forward rules, Groups, Licenses, Profiles, Schedule, and Users.

At the bottom right, there are navigation buttons: a back arrow, a save button (a green circle with a white document icon), and a refresh button.

As a result, the profile will be added to a list where you can edit or delete it. Also, you can filter profiles by name.

MATCH ALL		+ ADD FILTER		DELETE SELECTED	
<input type="checkbox"/>	ID	Name	Description		
<input type="checkbox"/>	1	Administrator	admin		
<input type="checkbox"/>	2	User			
<input type="checkbox"/>	3	Concierge			
<input type="checkbox"/>	4	Pro User	User uses a paid subscription and has an extended list of permissions.		

Total records: 6

Rows per page: 25 Records 1 - 6 of 6

To apply the profile to a user you can in the [Users](#)³⁰ tab.

5.2.2 Independent projects on the one server

It is possible to use a server for several small projects, e.g., for some separate areas with few devices. In this case, each root group stands for a single project. The administrators see only their root group info about subgroups, device(s), user(s), role(s), access rule(s), logs, etc. In other words, the administrator must be added to the root group to manage and monitor all linked with this group. So, they can not influence and access other projects they are not linked with.

If you are going to use this mechanism, it is required to limit the administrator default profile as it has permissions for access to all data available on the server. This default role can be renamed as the master administrator and used for those who monitor and configure all projects available on the server. So, for the root group administrator, a new profile must be created. You can use one profile for all projects or create it for each project. Also, user and concierge profiles can be created for all or each project.

5.2.3 How to create a root group administrator profile

1. Go to the **Profiles** tab of the User management section.
2. Click plus icon (in the low left corner).
3. Enter a profile **name** (e.g. root group administrator) and add a description (if required).
4. Select the following **permissions**:

³⁰ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

Info

Be aware, if you use one root group administrator profile for several projects, and if later you will expand the administrator permissions (e.g., for some projects), this will affect all projects.

- **access restrictions:** can view/create/edit/delete access rules;
- **announces:** can create/edit/delete/send announces, can view announces;
- **conversations:** can create conversation/conversation message, can delete conversation, can accept messages from descendant users;
- **devices:** can view device tasks, can create/edit/delete/view devices, can view device events;
- **elevators:** can create/edit/delete elevator, can view elevators;
- **emergency alerts:** can view emergency alerts, can create/edit/delete/playback emergency alerts;
- **forward rules:** can view/create/edit/delete forward rules;
- **groups:** can delete/edit group, can create group-descendant;
- **identifiers:** can view identifiers; can create/edit/delete identifier; can create guest identifier, can import/export identifiers, can view ACS logs;
- **markers:** can view/create/edit/delete/apply marker;
- **profiles:** can view roles, can edit role (these rules are applied to the list of available profile types set in the corresponding section);
- **schedule:** can view/create/edit/delete schedule;
- **users:** create/edit/delete user;
- **virtual numbers:** can create/edit/delete/activate virtual number, can mark system virtual numbers;

Info

We do not provide any permissions for call history and calls, as the user can see all calls of all users with subordinate profiles and can call them (by default).

5. Add other available profile types that this type can edit (if necessary), e.g. user, concierge.
6. Save data by clicking the corresponding button in the left low corner.

It is very important to set permissions for user and concierge profiles correctly because this will determine their functionality and scope. You can edit the default profiles or create new ones and the set of permissions can differ depending on the project. But the obligatory permissions for **concierge** are the following:

- **announces:** can create/edit/delete/send announces, can view announces;
- **calls:** can receive call like concierge, can call to intercom;
- **conversations:** can view all conversations, can send messages to all, can create conversation/conversation message, can accept messages from descendant users;

- **emergency alerts:** can view particular emergency alerts, can playback emergency alerts;
- **markers:** can view marker;

User must have such permissions as:

- **calls:** can call to intercom;
- **conversations:** can create conversation message;
- **identifiers:** can view identifiers; can create guest identifier;

After the profiles are created, they must be applied to the pre-created [users](#)³¹. Then users must be added to the [groups](#)³²: root group administrator must be added to the root group (the main project group), all other users must be added to the corresponding groups.

5.2.4 Example of server configuration for hosting several projects

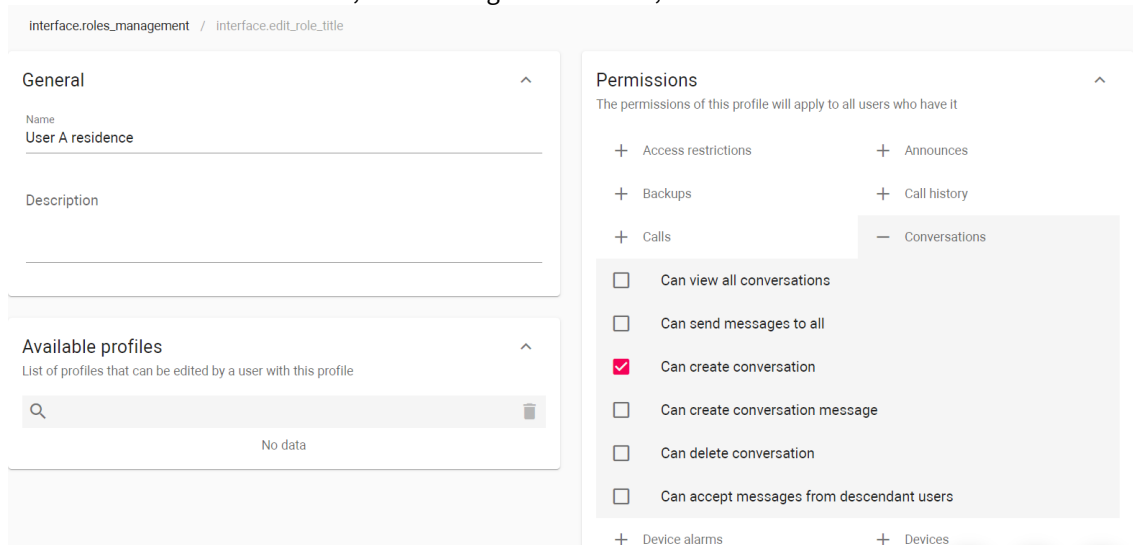
For example, we are managing 2 separate houses and must create conditions for users to interact only with houses groups they live in. Each house group must have its own administrator with the permissions to edit the list of users, devices, groups, apartments, etc. only within the house they are added to. In addition, each group must have its own resident users and concierges, who must be able to normally interact with each other, but not overlap with neighboring house group.

1. As the local (root group) administrators of each house have advanced rights only in their groups, the server must have a master administrator who can configure the whole server. So, you must **create the profile for this master administrator**. The default Administrator profile has all necessary permissions, so leave it, but rename to the master administrator. Apply this profile to the user who will manage the whole server.
2. Edit the default profile or create a new one for **users** and set the permissions (they can differ depending on the project). It is very important to set permissions because this will determine their functionality and scope. You can use one profile for all projects or create profiles for each project. In this example, we create separate profiles for each project. **User** must have such permissions as:
 - **calls:** can call to intercom;
 - **conversations:** can create conversation message;

³¹ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

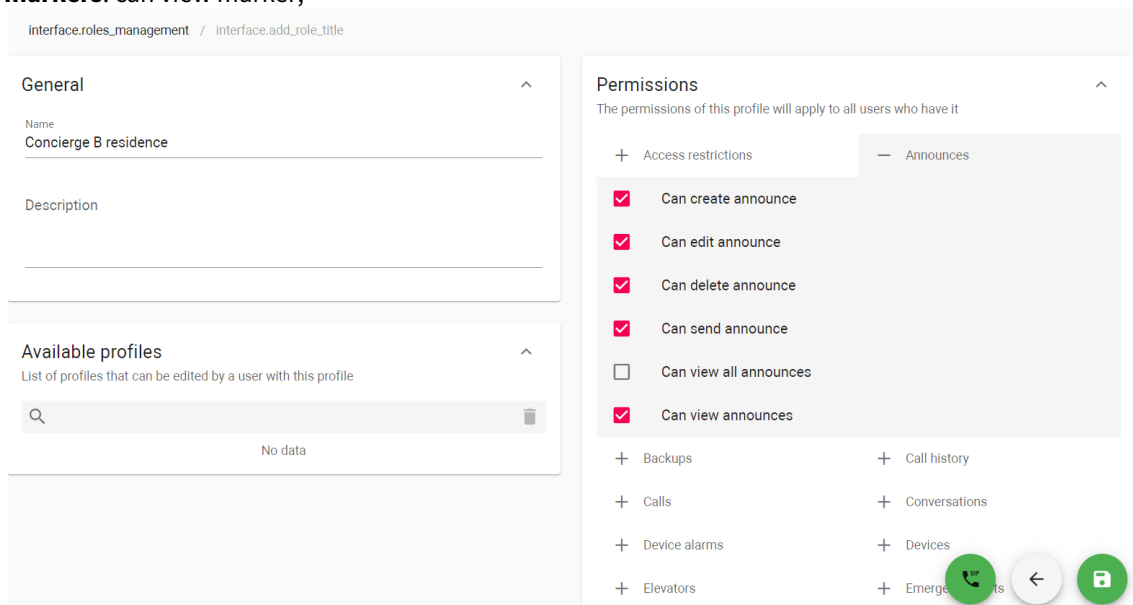
³² <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>

- **identifiers:** can view identifiers; can create guest identifier;



3. Edit the default profile or create a new one for **conciierge** and set the permissions (they can differ depending on the project). It is very important to set permissions because this will determine their functionality and scope. You can use one profile for all projects or create profiles for each project. In this example, we create separate profiles for each project. The obligatory permissions for **conciierge** are:

- **announces:** can create/edit/delete/send announces, can view announces;
- **calls:** can receive call like concierge, can call to intercom;
- **conversations:** can view all conversations, can send messages to all, can create conversation/conversation message, can accept messages from descendant users;
- **emergency alerts:** can view particular emergency alerts, can playback emergency alerts;
- **markers:** can view marker;



4. Create a profile for **root group administrator** as they must see only their root group, subgroups, device(s), user(s), role(s), access rule(s), logs, etc. You can use one profile for all projects or create profiles for each project. In this example, we create separate profiles. This profile must have the following permissions:

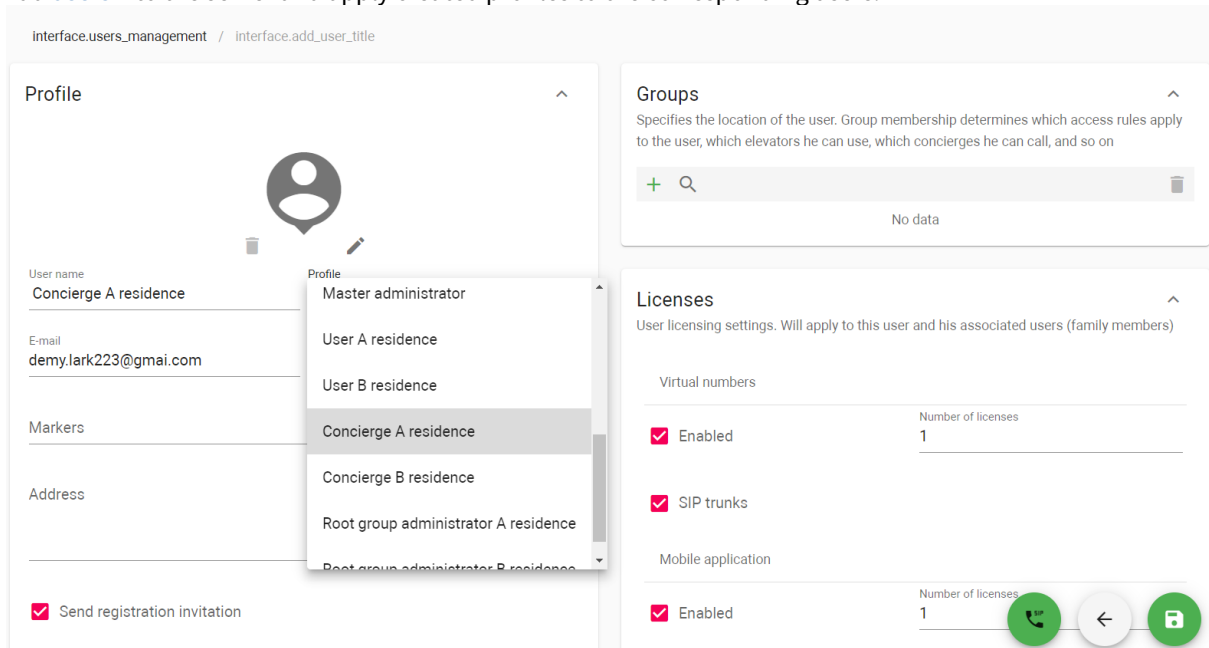
- **access restrictions:** can view/create/edit/delete access rules;
- **announces:** can create/edit/delete/send announces, can view announces;

- **conversations:** can create conversation/conversation message, can delete conversation, can accept messages from descendant users;
- **devices:** can view device tasks, can create/edit/delete/view devices, can view device events;
- **elevators:** can create/edit/delete elevator, can view elevators;
- **emergency alerts:** can view emergency alerts, can create/edit/delete/playback emergency alerts;
- **forward rules:** can view/create/edit/delete forward rules;
- **groups:** can delete/edit group, can create group-descendant;
- **identifiers:** can view identifiers; can create/edit/delete identifier; can create guest identifier, can import/export identifiers, can view ACS logs;
- **markers:** can view/create/edit/delete/apply marker;
- **profiles:** can view roles, can edit role (these rules are applied to the list of available profile types set in the corresponding section);
- **schedule:** can view/create/edit/delete schedule;
- **users:** create/edit/delete user;
- **virtual numbers:** can create/edit/delete/activate virtual number, can mark system virtual numbers;

Also, the root group administrator must be allowed to edit all subordinate profiles, so select the corresponding profiles of user and concierge as **Available profiles**.

5. Create a **root groups**(see page 44) that stand for the houses projects, e.g., the 1st group is A residence, and the 2nd is B residence.
6. Add the required number of **subgroups** (depending on the project structure).

7. Add users³³ to the server and apply created profiles to the corresponding users.



8. Add users to the created groups: root group administrator must be added to the root group (the main project group), and all other users must be added to the corresponding groups.



As a result, the administrator added to the root group can manage and monitor all linked with this group users, access restrictions, devices, schedules, etc. So, they can not influence and access other projects (root groups) they are not linked with. But both root groups are available for the master administrator.

³³ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

5.3 Groups

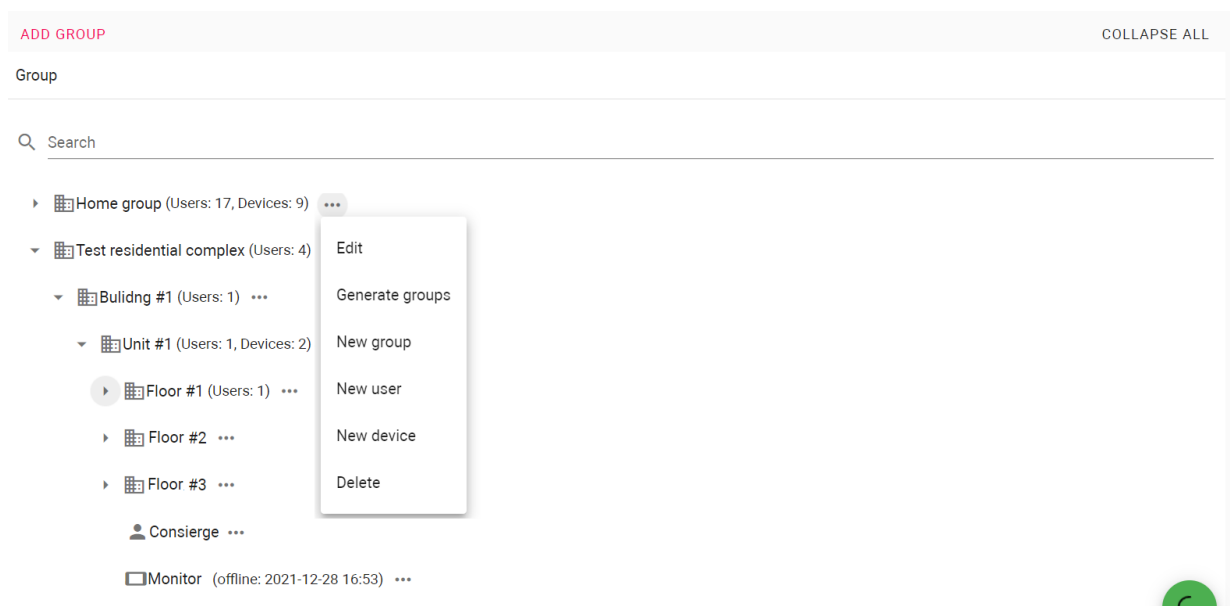
- [How to add root group](#)(see page 44)
- [How to generate root groups](#)(see page 45)
- [Group forward rules](#)(see page 48)

Group is a structure of your project for its easy management and one of the basic data that must be entered. A group can stand for a whole residential complex consisting of many houses, units, and apartments with thousands of users, or it can be a separate house or apartment, including one user.

For example, you can create a root group for a residential complex, and assign an administrator to this group who will install, configure, and monitor the whole system of this complex. Then, you can create subgroups for each house, and assign a manager for each of them (security guard or concierge) to register new users (tenants), be responsible for issuing access identifiers, and monitor the system.

By creating groups and adding users you give them access to devices, restrictions, and all other possibilities of the group, e.g. in one house (group) there is an elevator controller and users can use its features, but in another, there is no such option as an elevator controller is not installed.

In the tab, you can create groups and manage them: add new subgroups, devices (previously added in the corresponding [tab](#)³⁴), and users (previously added in the corresponding [tab](#)³⁵) to the group/subgroup, etc.



There are 2 options for creating a group: **Add root group** and **Generate root groups**. If the building is not very big and has few units, it is better to add a root group. Generating root groups is better for quickly creating a large number of groups and subgroups for complex projects (a lot of buildings, units, etc.).

34 <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>




35 <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

If you are going to host several independent projects on the one server, you must create root group for each project (as the main group) and then subgroups for houses, units, etc. It is important to provide correct permissions for user roles. More about this mechanism is [here](#)³⁶.

5.3.1 How to add root group

1. Go to the **Groups** tab in the User management section.
2. Click **Add group** and select **Add root group**.
3. Enter a group **name**.
4. Select its **type**: if the group is for building, unit, floor, apartment, or custom (for parking or service rooms). We recommend use custom group type for root groups.
5. Enter a **logical address**: depending on the group type it can be Building No., Unit No., Floor No., or Apartment No.
6. Select **SIP trunk** (from the previously [created](#)³⁷) will work for the group for calls to mobile numbers (if the Link version with SIP and the corresponding [license](#)³⁸ is used). Users of this group will use the assigned trunk when calling mobile numbers.

Only one trunk can be assigned to one group. Different trunks can be used for root group and its subgroups.

7. Add a description, if necessary.
8. Select **users** (must be previously added in the [Users](#)³⁹ tab).
9. Select **devices** (must be previously added in the [Devices](#)⁴⁰ tab) installed in the place for what you are creating the group.
10. Create **access restrictions**  or select  from already created. After clicking  you will be redirected to the [corresponding tab](#)⁴¹ where it is possible to create restrictions.

Applying access restriction is obligatory. This parameter helps to connect groups, devices, and users.

11. Enable and configure **forward settings** if necessary to redirect calls from devices/users added to the group to other devices.

³⁶ <https://wiki.bas-ip.com/basiplinken/profiles-135955778.html>

³⁷ <https://wiki.bas-ip.com/basiplinken/sip-trunks-135958438.html>

³⁸ <https://wiki.bas-ip.com/basiplinken/licenses-135956024.html>

³⁹ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

⁴⁰ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

⁴¹ <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>

More details about the configuration you can find [here](#)⁴². Forward rules will be applied to all group users.

- Click the **Save** button in the low left corner when all required data is entered.

The screenshot shows the 'Group management' interface for editing the group 'Heathfield House'. The interface is divided into several sections:

- General:** Contains fields for Name (Heathfield House), Type (Building), Logical address (1), SIP trunk (link twilio trunk), and Description.
- Users:** Lists users who have access to passageways, elevators, and concierge calls. One user, 'Mark (Security Guard)', is listed.
- Access restrictions:** Shows access rules assigned to the group and its descendants. Currently, there is 'No data'.
- Devices:** Lists devices belonging to the group. One device, 'monior D', is listed.

At the bottom right, there are three circular icons: a green phone icon, a grey back arrow icon, and a green save icon.

5.3.2 How to generate root groups

- Go to the **Groups** tab in the User management section.
- Click **Add group** and select **Generate root groups**.
- Click **Add group** in the opened window.
- Select groups **type**: if the group is for building, unit, floor, apartment, or custom.
- Enter groups **name**.
- Indicate the **number of buildings** for which you need to create groups.
- Set the number from which the numbering of buildings starts.
- Click plus icon to add subgroups (e.g. Unit) and enter the same information for this section: type names, amount of units in one building, and the number from which the numbering starts.
- Add and set the same settings for floors and apartment subgroups.


When entering the apartment amount, enter a general value of apartments on the one floor, not their No.


- If there are any specific subgroups (parking or service rooms), you need to create and select a custom group type.


⁴² <https://wiki.bas-ip.com/basiplink/en/forward-rules-110562890.html>


Generate groups


SETTINGS RESULT

☰ ▾ Add group Building with the name Building # in the amount of 2, number from 1 

☰ ▾ Add group Unit with the name Unit # in the amount of 3, number from 1 


☰ ▾ Add group Floor with the name Floor # in the amount of 5, number from 1 

☰ ▾ Add group Apartment with the name Apartment # in the amount of 4, number from 1 



CLOSE


GENERATE

For each group, by clicking  you will expand additional parameters to set:

- the number from which the numbering of logical addresses will start. To do this tick the **Start number** field and enter the required value in the **Logical address** field;
- number/s which will be excluded from the numbering (**exceptions**);

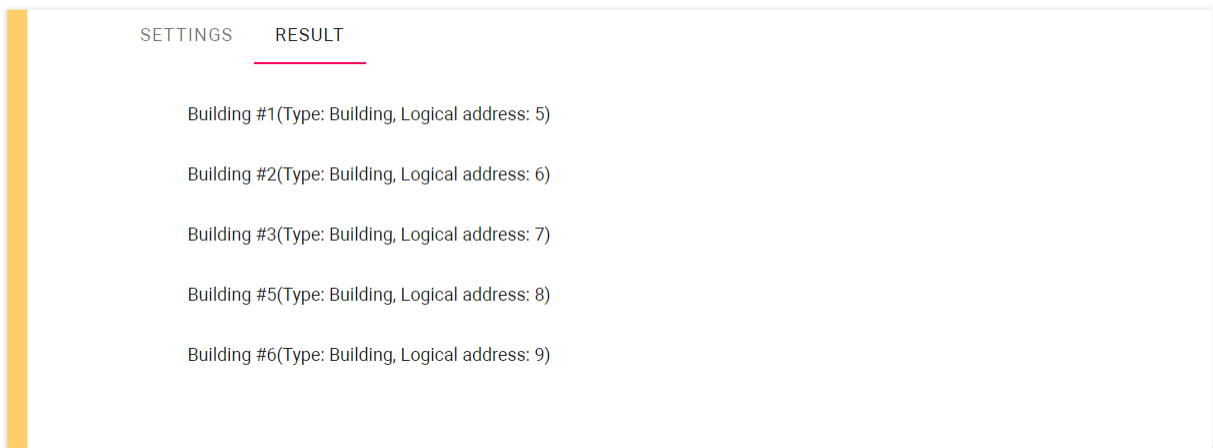
SETTINGS RESULT

☰ ▲ Add group Building with the name Building # in the amount of 5, number from 1

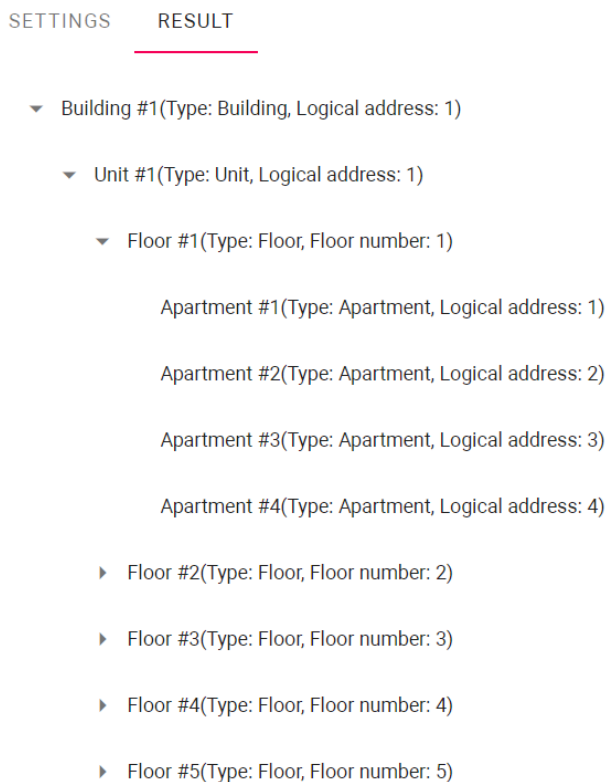
Start numbering Exceptions 4 

Logical address 5

As a result, groups will be created according to your settings:



11. When all data is entered click **Generate** and all groups will be created according to the entered data.
12. Check the correctness. Open the **Settings** tab to edit entered data.



13. Save generated groups and then add previously registered [users](#)⁴³, [devices](#)⁴⁴, or [access restrictions](#)⁴⁵.

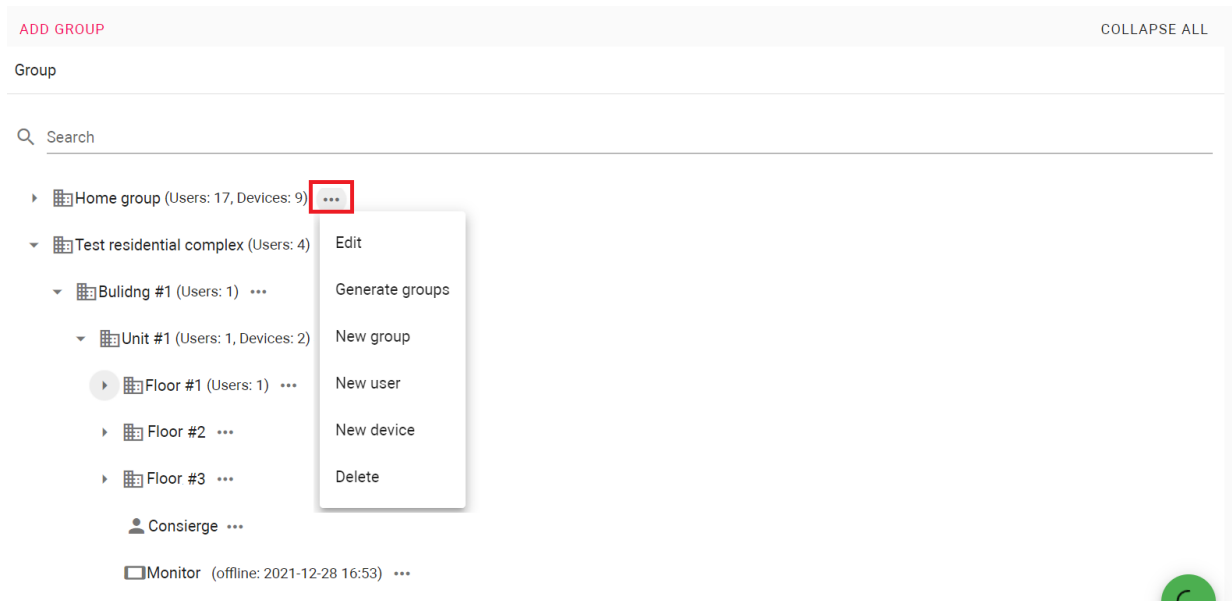
When adding a device to a group be careful with the place of its installation, whether it's a unit, floor, or user apartment. So, you need to add the device to the corresponding group.

⁴³ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

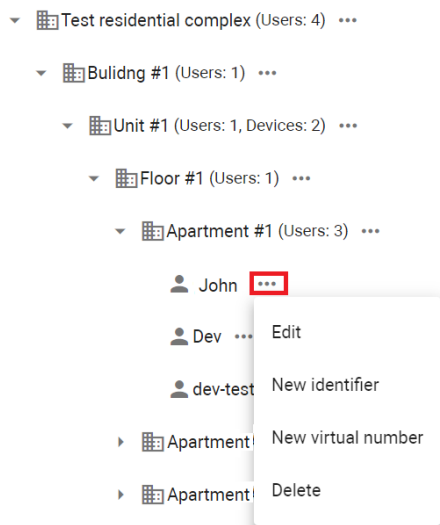
⁴⁴ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

⁴⁵ <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>

You can edit a root group and add a new subgroup/user/device by clicking **3 dots** near the necessary group name. After selecting the option, the corresponding menu will open.



If you click **3 dots** near the user name, you can edit/delete their profile or add a new identifier or virtual number.



5.3.3 Group forward rules

In the [SIP settings](#)⁴⁶, you can enable the feature of automatic creation of forward rules for apartment group user/s. When adding a user that has virtual number/s to a group, forwarding that includes all user numbers is automatically created. These rules will be sent to panel/s available for the group.

⁴⁶ <https://wiki.bas-ip.com/basiplinken/sip-settings-135956014.html>

The group will have its virtual number and logical address. And when calling from the added to the group panel to a device (entering group logical address), the call will be redirected to all user virtual numbers.

The screenshot displays the configuration interface for a group. On the left, the 'General' tab is active, showing the following fields:

- Group virtual number for forward rules - 1049**
- Name:** Apartment 1
- Type:** Apartment (dropdown menu)
- Logical address:** 1
- SIP trunk:** link twilio trunk (with edit and delete icons)
- Description:** (empty text field)

On the right, the 'Forward settings' tab is active, showing the following options:

- Forward settings:** General forwarding rules. Affect calls of users of this group and its descendants
- Forwarding options:**
 - Immediately
 - If no answer, then after 10 seconds forward to
- Call queue #1:** (with settings and delete icons)
- Queue members:** link(1058), 1010(1010), 1023(1023), and a plus sign for adding more.

! Warning

For correct feature functioning, logical addresses must be entered for all groups and subgroups.

If some data (logical address, virtual numbers, devices) is added/changed/deleted, then the old forward rule will be deleted and the new one (with updated data) will be created and sent to device/s.

You or a user can configure **forward settings** when editing the group with the device, or in the Link app. By default, forward rule includes immediate call redirection to all user numbers (by default they are indicated in the 1st queue), but you can add/delete numbers to/from the queue or create new queue/s.

Also, when the user will get new virtual number, it will be added to the call queue #1, if there is only 1 queue. If there are 2 or more call queues, new virtual number will be added to a new call queue.

In addition, you can edit forward settings for the group virtual number in the [Virtual number](#)⁴⁷ settings.

⁴⁷ <https://wiki.bas-ip.com/basiplinken/virtual-numbers-135955892.html>




6 Access management





































- [Guest access](#)(see page 50)
- [Schedules](#)(see page 56)
- [Access restrictions](#)(see page 61)
- [Identifiers](#)(see page 64)
- [Access matrix](#)(see page 67)
- [ACS logs](#)(see page 68)

6.1 Guest access

Here you can create and monitor temporary identifiers for guests, couriers, taxi drivers, etc. Such access provides additional security as it's possible to configure areas visitors will have access to, the time and date when the ID will work, and the number of available passes.

- [How to create a guest identifier](#)(see page 50)
- [Guest passes filtering](#)(see page 56)

In the tab, you see all created guest identifiers with detailed information about them. With the help of  and  buttons, you can edit or delete created identifiers. By clicking , the identifier will be shown and you can share it with a visitor.

MATCH ALL		+ ADD FILTER										DELETE SELECTED	
<input type="checkbox"/>	Type	Access restrictions	Owner	Value	Guest type	Valid from	Valid until	Maximum number of passes	Used	Created at			
<input type="checkbox"/>	Access code	Guest identifier #1461	Juli	528561	Courier	2022-07-27 14:26	2022-07-28 14:26	1	0	2022-07-27 14:26			
<input type="checkbox"/>	Url	Guest identifier #1462	Administrator		Courier	2022-07-27 14:26	2022-07-28 14:26	1	1	2022-07-27 14:26			
<input type="checkbox"/>	QR-code	Home group	Administrator		Guest	2022-07-28 15:32	2022-07-28 16:32	6	0	2022-07-28 15:32			
<input type="checkbox"/>	QR-code	Guest identifier #1482	John		Guest	2022-07-28 17:49	2022-07-28 18:49	5	0	2022-07-28 17:49			
<input type="checkbox"/>	QR-code	Guest identifier #1483	John		Guest	2022-07-29 12:24	2022-07-29 13:24	5	0	2022-07-29 12:25			
<input type="checkbox"/>	QR-code	Guest identifier #1484	Pete		Guest	2022-07-29 12:53	2022-07-29 13:53	infinitely	0	2022-07-29 12:53			
<input type="checkbox"/>	QR-code	Guest identifier #1485	Administrator		Guest	2022-07-29 13:04	2022-07-29 14:04	5	0	2022-07-29 13:04			
<input type="checkbox"/>	QR-code	Guest identifier #1486	Administrator		Guest	2022-07-29 13:17	2022-07-29 14:17	5	0	2022-07-29 13:17			
<input type="checkbox"/>	QR-code	Guest identifier #1488	Mari		Guest	2022-07-29 14:02	2022-07-29 15:02	6	1	2022-07-29 14:02			
<input type="checkbox"/>	QR-code	Guest identifier #1491	Juli		Guest	2022-07-29 14:20	2022-07-29 15:20	44	0	2022-07-29 14:20			
<input type="checkbox"/>	QR-code	Guest identifier #1492 ¹	Juli		Guest	2022-08-	2022-08-	1	0	2022-08-			

6.1.1 How to create a guest identifier

Only a user that has at least 1 access restriction and at least 1 device associated with this restriction can create a guest identifier.

1. Go to the **Guest access** tab in the Access management section.
2. Click **plus** icon in the left low corner.

3. Select ID **type**: **QR code** (available for panels with camera), **Access code** (available for panels with keypad), **URL** (available for all devices), or a **License plate** (available for panels and installed Axis camera with Axis License Plate Verifier software).
4. Select **guest type**: Courier or Guest.
5. Select the **access restrictions** you want to apply for the ID. Selected access restrictions must coincide with restrictions applied to the user is creates the ID.
6. Tick the **restriction period** field if it is necessary to limit the ID validity period.
7. Indicate the **beginning** and the **ending** of the ID active period. By default, the pass works for 1 day.
8. If necessary, tick the **limit the number of passes** field.
9. Enter the available **number of passes** for this ID. By default, 1 pass is available.

You may enable and set either a **restriction period** or a **number of passes** parameters.

10. Enter a **guest message** if required.
11. Click confirm when all data is entered.

Guest access

Type
QR-code

Guest type
Guest

Access restrictions
Test(SD)

Restriction period

Valid from

✕

Valid until

✕

Limit the number of passes

Maximum number of passes

Guest message

CANCEL CONFIRM

12. Copy the link/access code or download a QR code (or pkpass file for adding the QR code to Apple Wallet) and sent it to the guest for further use.

Name: Guest identifier



Valid time: 2022-09-06 00:01
2022-10-21 00:00

Number of passes: 3

DOWNLOAD QR-CODE

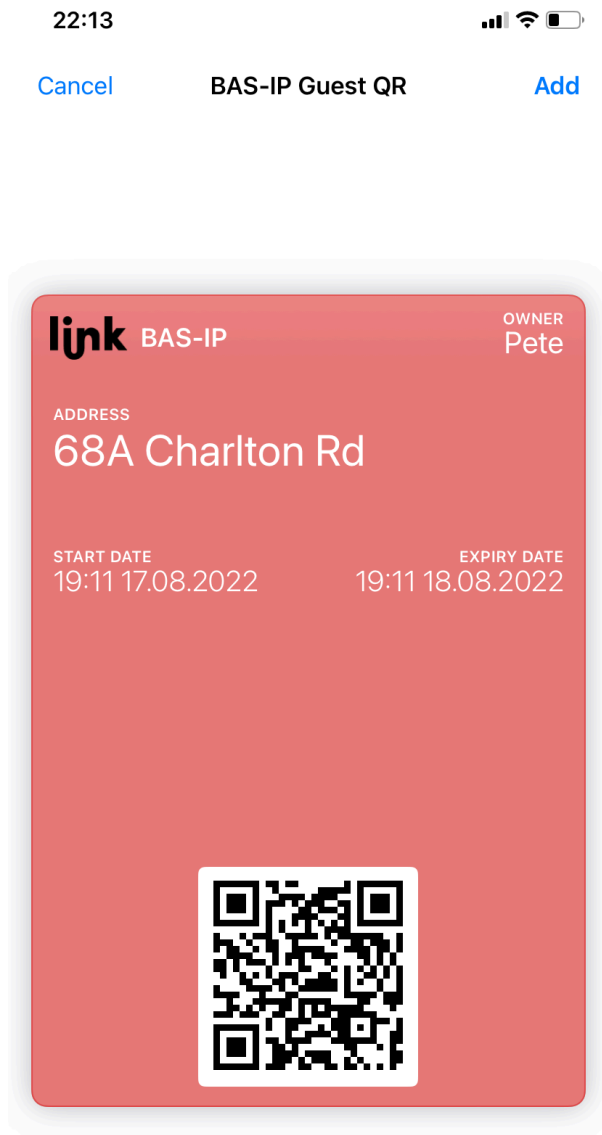
DOWNLOAD PKPASS-FILE

CLOSE

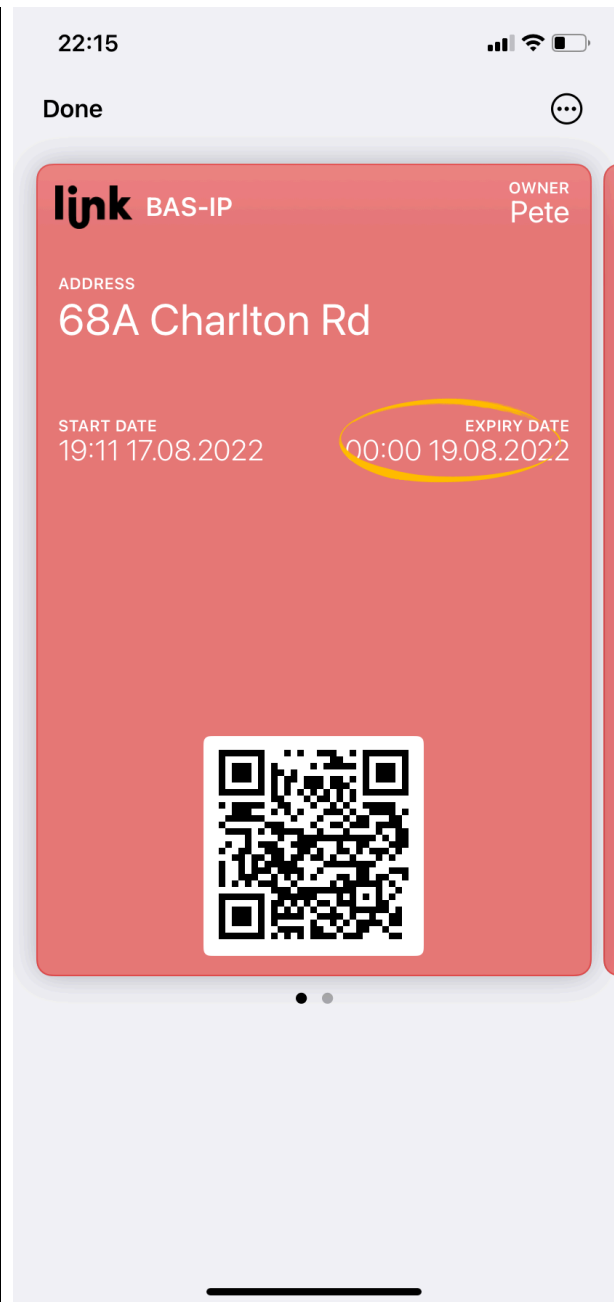
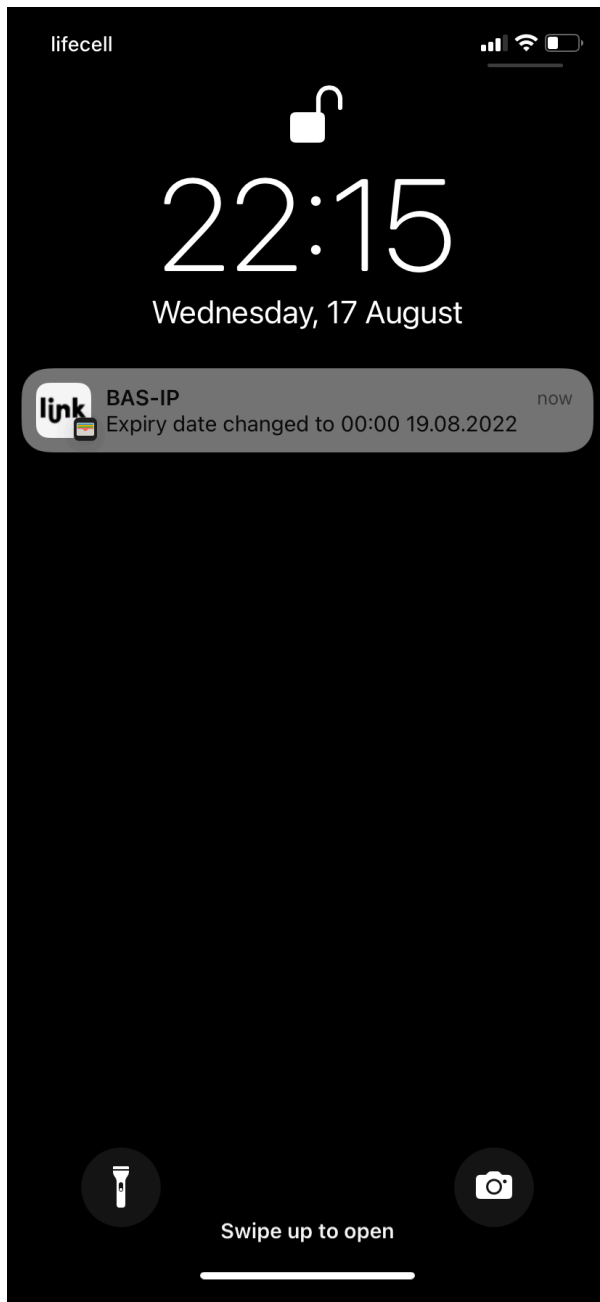
When you select a **QR-code** pass, you can share it as an image of the code and all the main information. Visitor can check all the necessary information (validity period, the number of available passes) and has to open it and show for entrance panel scanning.



In addition to the image, the QR code can be shared in a format for adding it to Apple Wallet if you/your visitor use **IOS**. When receiving a pass, a visitor must open it and press **Add** button. As a result, the visitor will get access to the pass by opening Apple Wallet.



Also, if some changes about the pass are done on the Link server, the visitor will be notified about it and they will be automatically applied. So, there is no need to send another pass.



You can configure how guests passes will look in the [Additional settings](#)⁴⁸ tab.

48 <https://wiki.bas-ip.com/basiplinken/additional-settings-135956004.html>

6.1.2 Guest passes filtering

There is a filter by the date the identifier was **created**, **owner**, and is the identifier **valid**. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all identifiers used before the date.



MATCH ANY											IS VALID EQUALS NO	+ ADD FILTER	SAVE AS	DELETE SELECTED
<input type="checkbox"/>	Type	Access restrictions	Owner	Value	Guest type	Valid from	Valid until	Maximum number of passes	Used	Created at				
<input type="checkbox"/>	QR-code	Home group	Administrator		Guest	2022-07-28 15:32	2022-07-28 16:32	6	0	2022-07-28 15:32				
<input type="checkbox"/>	QR-code	Guest identifier #1482	John		Guest	2022-07-28 17:49	2022-07-28 18:49	5	0	2022-07-28 17:49				
<input type="checkbox"/>	QR-code	Guest identifier #1483	John		Guest	2022-07-29 12:24	2022-07-29 13:24	5	0	2022-07-29 12:25				
<input type="checkbox"/>	QR-code	Guest identifier #1484	Pete		Guest	2022-07-29 12:53	2022-07-29 13:53	infinitely	0	2022-07-29 12:53				
<input type="checkbox"/>	QR-code	Guest identifier #1485	Administrator		Guest	2022-07-29 13:04	2022-07-29 14:04	5	0	2022-07-29 13:04				











You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ANY											IS VALID EQUALS NO	+ ADD FILTER	SAVE AS	SEGMENTS	DELETE SELECTED
<input type="checkbox"/>	Type	Access restrictions	Owner	Value	Guest type	Valid from	Valid until	Maximum number of passes	Used	Created at					
<input type="checkbox"/>	QR-code	Home group	Administrator		Guest	2022-07-28 15:32	2022-07-28 16:32	6	0	2022-07-28 15:32					
<input type="checkbox"/>	QR-code	Guest identifier #1482	John		Guest	2022-07-28 17:49	2022-07-28 18:49	5	0	2022-07-28 17:49					
<input type="checkbox"/>	QR-code	Guest identifier #1483	John		Guest	2022-07-29 12:24	2022-07-29 13:24	5	0	2022-07-29 12:25					
<input type="checkbox"/>	QR-code	Guest identifier #1484	Pete		Guest	2022-07-29 12:53	2022-07-29 13:53	infinitely	0	2022-07-29 12:53					
<input type="checkbox"/>	QR-code	Guest identifier #1485	Administrator		Guest	2022-07-29 13:04	2022-07-29 14:04	5	0	2022-07-29 13:04					

6.2 Schedules

- [How to add a new schedule](#)(see page 57)
- [Schedules filtering](#)(see page 61)

In the section, you can set active time schedules for devices and/or users. For schedule correct functioning, it must be applied to access restriction (to link devices and users). With the help of  and  buttons, you can edit or delete created schedules.

MATCH ALL		+ ADD FILTER					DELETE SELECTED	
<input type="checkbox"/>	ID	Name	Description	Valid from	Valid until			
<input type="checkbox"/>	1	Schedule from 18.04 to 2025		2022-04-18	2025-02-01			
<input type="checkbox"/>	3	Security		2021-10-22	2021-10-30			
<input type="checkbox"/>	4	For forwarding		2022-04-04	2023-04-04			
<input type="checkbox"/>	7	Endlessly		2022-05-01	2024-01-01			
<input type="checkbox"/>	8	Basic access		2022-08-04	2022-10-06			

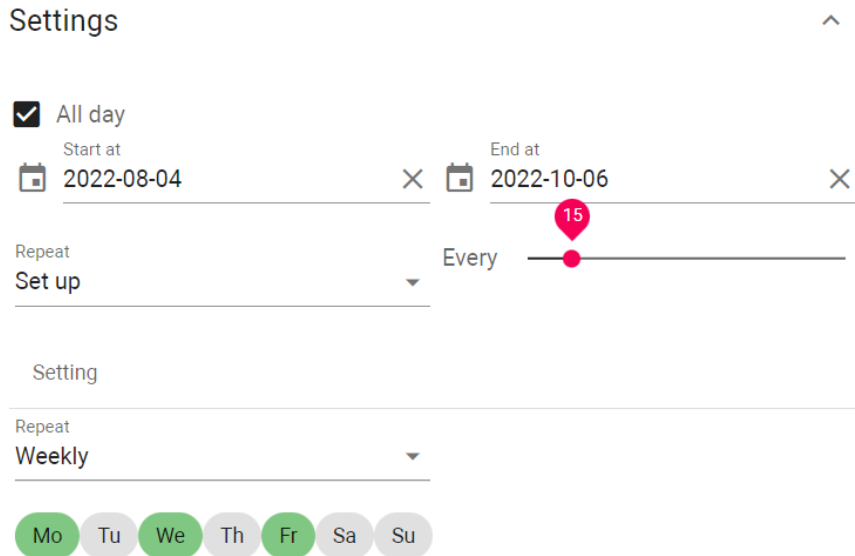
Total records: 5

Rows per page 25 Records 1 - 5 of 5

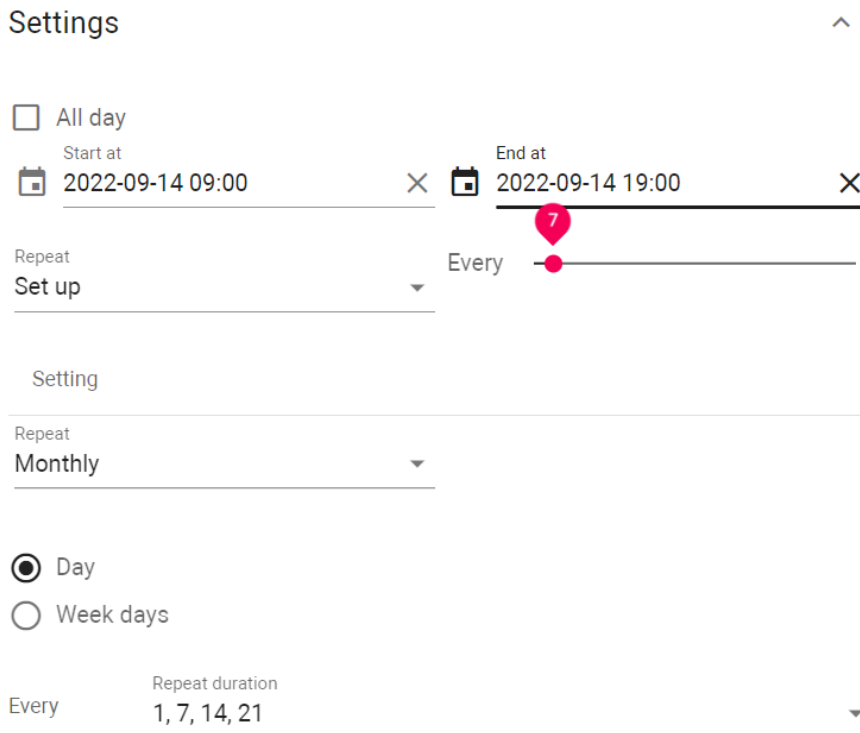
6.2.1 How to add a new schedule

1. Go to the **Schedules** tab of the Access management section.
2. Click **plus** icon in the left low corner.
3. Enter the schedule **name**.
4. Add a **description**, if required.
5. Set the time when the schedule must work:
 - enable **all day** and only the date (day/month/year) of the beginning and end of this schedule functioning;
 - if the **All day** option is disabled, specify the date (day/month/year) and set the start and end time of this schedule functioning.
6. If required, indicate the frequency of repetitions:
 - **never**: the schedule will function only on the indicated date;
 - **daily**: the schedule will be active every day for a specified time period. For example, the identifier will work every day from 9:00-18:00 (if you set a day and time);
 - **weekly**: the schedule will work on the specified days and hours, e.g., every Tuesday (if you select an all-day option and set a date);
 - **every 2 weeks**: the schedule will repeat every two weeks on the specified day/s. For example, if you create a schedule that works from Monday to Wednesday, then it will be active from Monday to Wednesday with 2 weeks intervals;
 - **monthly**: the schedule will be active every month, e.g., every 15th day of the month;
 - **yearly**: the schedule will repeat every year, e.g., every 15th of December;
 - **set up**: the schedule will be active on indicated dates, days, and months:
 - **daily**: the schedule will be active every day for a specified time period. In **Every** field, you can indicate after how many days the schedule will be activated again, e.g., every 5th day;
 - **weekly**: you can configure schedule repetition on specific days of the week. In **Every** field, you can indicate after how many weeks the schedule will be activated again. According to the

screen, it will work on Mondays, Wednesdays, and Fridays every 15 weeks;



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



Also, it is available to configure 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 schedule will work from 9:00-19:00 every last working day of every 7th

month.

Settings ^

All day

Start at 2022-09-14 09:00 X End at 2022-09-14 19:00 X

Repeat **Set up** Every 7

Setting

Repeat **Monthly**

Day Week days

Every Order **Last** Day **Monday**

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

Settings ^

All day

Start at 2022-09-14 09:00 X End at 2022-09-14 19:00 X

Repeat **Set up** Every 2

Setting

Repeat **Yearly**

Jan Feb Mar Apr May **Jun** Jul Aug Sep Oct Nov **Dec**

Also, it is available to configure repetition every year on weekdays (the option must be enabled): 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 schedule will work from

9:00-19:00 every first Saturday of January, June, and December with a 2 years frequency;

Settings

All day

Start at End at

Repeat **Set up** Every

Setting

Repeat **Yearly**

Jan
 Feb
 Mar
 Apr
 May
 Jun
 Jul
 Aug
 Sep
 Oct
 Nov
 Dec

Week days

Order **First** Day **Saturday**

7. Set the **repeat duration** of the schedule:

- **always:** the schedule will infinitely repeat;
- **until:** it will be active until the indicated date.

8. Select or add new **access restrictions** to link schedules, devices, and users.

9. Click the **Save** buttons in the left low corner.

The screenshot shows a configuration interface with three main panels on the left and a 'Settings' panel on the right. The 'Settings' panel is expanded and shows the same configuration as the previous image, including the 'Repeat' section with a slider set to 2 and the 'Repeat duration' section set to 'Until' with a date of 1970-01-01. The 'Access restrictions' panel shows a search bar and a list with one item 'Entrance panel'. The 'Synchronization' panel has a description: 'Displays the current schedule sync status to devices that are shared with the schedule and its owner via access rules'. At the bottom right, there are navigation buttons: a back arrow and a green 'Save' button.

6.2.2 Schedules filtering

Also, there is a filter by ID No., name, and valid time. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), they can be **less** or **great** than your parameter, or contain (**has**) it, e.g. search less than indicated ID will display numbers before it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

ID	Name	Description	Valid from	Valid until	
<input type="checkbox"/>	7	Endlessly	2022-05-01	2024-01-01	
<input type="checkbox"/>	8	Basic access	2022-08-04	2022-10-06	

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

ID	Name	Description	Valid from	Valid until	
<input type="checkbox"/>	7	Endlessly	2022-05-01	2024-01-01	
<input type="checkbox"/>	8	Basic access	2022-08-04	2022-10-06	

6.3 Access restrictions

- [How to create access restriction](#)(see page 62)
- [Access restrictions filtering](#)(see page 63)

Access restrictions are an integral part of the Link server that links devices, users, and schedules if required. You can quickly configure giving access or not to these or those devices for concrete users. Access restrictions must be applied to groups with added devices and users.

MATCH ALL + ADD FILTER

DELETE SELECTED

<input type="checkbox"/>	ID	Name	Description	Number of devices	Schedules	
<input type="checkbox"/>	1312	Access Restriction		1	Schedule from 18.04 to 2025	
<input type="checkbox"/>	1374	Entrance panel			Basic access	
<input type="checkbox"/>	1375	Test(SD)				
<input type="checkbox"/>	1426	Pass		1		
<input type="checkbox"/>	1429	Rule		2	Schedule from 18.04 to 2025	
<input type="checkbox"/>	1430	Pass Restriction		1	Schedule from 18.04 to 2025	

Total records: 6

Rows per page 25 Records 26 - 31 of 31

Info

The access restriction that is applied to a group will automatically be distributed and will be applied to all subgroups and their users.

6.3.1 How to create access restriction

1. Go to the **Access restriction** tab of the Access management section.
2. Click **plus** icon in the left low corner.
3. Enter the restriction **name**.
4. If necessary, enable the possibility to **use** this restriction **for guest identifiers**.
5. Add description, if required.
6. Select **devices** from the list or add new ones to allow their use. Further access restrictions will be applied to [users⁴⁹](https://wiki.bas-ip.com/basiplinken/users-135955765.html) or [groups⁵⁰](https://wiki.bas-ip.com/basiplinken/groups-135955783.html) to allow them to open indicated device/s.
7. If necessary, specify the access point the is allowed to use.
8. Select the number of locks (if 2 locks are connected) that are allowed to open by users: the first, the second or all
9. If necessary, select a **schedule** from the list or add a new one to indicate restriction functioning time.
10. Click the **Save** button in the low left corner after entering all required data.

⁴⁹ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

⁵⁰ <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>

General

Name
For cleaners

Use when issuing guest access

Description

Devices

The specified devices will be used to grant access to the owners of this access rule

Device Name	Access p...	Lock	
Unit 1 Entrance	Access p...	First	

Schedules

Schedules are used to clarify the conditions for granting access - by time, days of the week, etc.

No data

6.3.2 Access restrictions filtering

With the help of and buttons, you can edit or delete restrictions. Also, there is a filter by ID No., name, a number of devices, schedules, and devices. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), they can be **less** or **great** than your parameter, or contain (**has**) it, e.g. search less than indicated ID will display numbers before it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

MATCH ALL ID EQUALS 1374 + ADD FILTER SAVE AS DELETE SELECTED

<input type="checkbox"/>	ID	Name	Description	Number of devices	Schedules		
<input type="checkbox"/>	1374	Entrance panel Darina		1	Basic access		

Total records: 1

Rows per page: 25 Records 1 - 1 of 1

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL ID EQUALS 1374 + ADD FILTER SAVE AS SEGMENTS

DELETE SELECTED

<input type="checkbox"/>	ID	Name	Description	Number of devices	Schedules	
<input type="checkbox"/>	1374	Entrance panel		1	Basic access	

Total records: 1

Rows per page 25 Records 1 - 1 of 1

6.4 Identifiers

Here you can add or view a table with identifiers added to the system.

- [How to add an identifier](#)(see page 64)
- [Identifiers filtering](#)(see page 66)

You can check information about the identifier owner, its type, number, validity period, applied access restrictions, etc. With the help of and buttons, you can edit or delete created identifiers.

MATCH ALL + ADD FILTER

DELETE SELECTED

<input type="checkbox"/>	Identifier	Name	Type	Owner	Access restrictions	Valid from	Valid until	Used	Created at	
<input type="checkbox"/>	6481199	Pass	Card	Sam	Entrance panel	2022-06-01 12:30	2022-09-01 20:00	2022-07-01 23:32	2022-06-22 17:02	
<input type="checkbox"/>	8536513	ID	UKEY	Max	Entrance panel	2022-06-20 18:35	2022-10-22 05:25	2022-06-23 16:40	2022-06-23 15:17	
<input type="checkbox"/>	32423342	Card	Card	Pete	Entrance panel				2022-06-23 16:25	
<input type="checkbox"/>	4cd6759098b11bd0ce3f961eeb0b2029d2cfa666	Sam	Face ID	Sam	Entrance panel				2022-06-23 16:25	
<input type="checkbox"/>	1245545	Pass	Card	Juli	Entrance panel				2022-07-04 16:23	
<input type="checkbox"/>	12331	Code	Access code	Administrator	Entrance panel				2022-07-04 16:26	
<input type="checkbox"/>	676788890	Pass	Card	Consierge	Entrance panel				2022-07-04 16:34	
<input type="checkbox"/>	54646444	ID	UKEY	John	Entrance panel				2022-07-04 18:03	



6.4.1 How to add an identifier

1. Go to the **Identifiers** tab in the Access management section.
2. Click **plus** icon in the left low corner.
3. Enter the identifier name.
4. Select the user of this ID.
5. Select the identifier type (pay attention to a device characteristics) and enter its value:

- **card**: EM-Marin or Mifare card. In the **Identifier** 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](#)⁵¹ to convert a value from one to another system;
- **UKEY** allows using smartphones as identifiers (**BAS-IP UKEY**⁵² app is required). You must enter the identifier number in the **Identifier** field;
- **access code** that must be entered on the panel keypad to open lock/s. In the **Identifier** field, you must indicate a numeric code that will be used to open a lock;
- **face ID** allows opening the lock by scanning visitors faces. When adding this identifier type, you must upload a user photo with a well-lit face and real face proportions in .jpeg format. For AA-14FBS, face recognition works little differently and if you upload identifiers backup from AA-14FB, they will not work for AA-14FBS;

Requirements for a photo:

- strictly a full face photo: front view and open eyes;
- presents full head from top of hair to shoulders, face occupies about 80% of the space;
- with a neutral background;
- with a well-lit face, no shadows;
- face has natural expression and real proportions;
- in .jpeg format;
- with a resolution of at least 320x240px and no more than 5120x2700px;

- the automatically generated **QR code**. Enable the **Download QR code** option and after saving the identifier, it will be saved to the computer. Then it must be uploaded to a mobile device for further use;
 - **license plates** can be added and used to open lock/s. In the **Identifier** field, you enter the plate number. For this identifier to work, you need an Axis camera for plate scanning and installed AXIS License Plate Verifier software to send a number to the panel.
6. If necessary, enable and set restriction period restrictions for identifier validity.
 7. If necessary, enable and set the maximum number of passes in the passes **restrictions** field.
 8. Select  from already added or create **access restrictions**. After clicking  you will be redirected to the [corresponding tab](#)⁵³ where it is possible to create restrictions.

Applying access restriction is obligatory. This parameter helps to connect groups, devices, and users.

9. Click the **Save** button in the left low corner when all required data will be entered. The identifier will automatically be sent to the devices indicated in access restrictions. You can check where ID is added in the Synchronization section.

⁵¹ <https://www.binaryhexconverter.com/hex-to-decimal-converter>

⁵² <https://bas-ip.com/catalog/soft/bas-ip-ukey/>

⁵³ <https://wiki.bas-ip.com/basiplink/en/creating-access-restrictions-15794714.html>

General

The validity of an identifier is determined by the limitation of the duration of the identifier and the maximum number of passes

Name
Sam

User
Sam

Identifier type Identifier
Access code **23123**

Restriction period

Valid from Valid until
2022-09-07 00:00 × 2022-12-01 00:00 ×

Passes restrict

[ACTIONS](#)

Access restrictions

Access rules set on an identifier only apply to that user identifier without affecting others. In addition, the identifier is affected by the access rules assigned to the user.

+ Q 🗑️

Entrance panel 🗑️

Synchronization

Displays the current identifier sync status to devices shared with the identifier and its owner via access rules

- 🕒 **Unit 1 Entrance**
Synced at 2022-10-07 18:58 -
- ✅ **AV03BD**
Synced at 2022-10-07 18:58 -
- 🕒 **AA-14FB(AW)**
Synced at 2022-10-07 18:58 -
- ✅ **BI12FB**
Synced at 2022-10-07 18:58 -

⏪ 🔒

6.4.2 Identifiers filtering

There is a filter by value, name, ID type, owner, the date the identifier was used or created and is the identifier valid. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all identifiers used before the date. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

MATCH ALL CREATED AT GREAT OR EQUAL 2022-10-06 00:00 + ADD FILTER 📄 SAVE AS

🗑️ DELETE SELECTED

<input type="checkbox"/>	Identifier	Name	Type	Owner	Access restrictions	Valid from	Valid until	Used	Created at	⋮
<input type="checkbox"/>	23123	Sam	Access code	Sam	Entrance panel				2022-10-07 18:58	✎ 🗑️

Total records: 1

Rows per page: 25 Records 1 - 1 of 1 ⏪ ⏩

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL CREATED AT GREAT OR EQUAL 2022-10-06 00:00 + ADD FILTER SAVE AS SEGMENTS

DELETE SELECTED

<input type="checkbox"/>	Identifier	Name	Type	Owner	Access restrictions	Valid from	Valid until	Used	Created at	
<input type="checkbox"/>	23123	Sam	Access code	Sam	Entrance panel				2022-10-07 18:58	

Total records: 1

Rows per page 25 Records 1 - 1 of 1 < >

6.5 Access matrix

This tab contains information about all identifiers added to the system: their type, owner, group and device to which the ID can be applied, access restrictions and schedule that work for the ID. So, this tab is a perfect option for monitoring all identifiers and their connections. You can export all data by clicking the corresponding button.

MATCH ALL + ADD FILTER

EXPORT TO

Identifier	Type	Used	User	Owner type	Group	Access restriction	Schedule	Device	
302419	Card		Administrator	Owner	Home group	Restriction 1	Basic access	AA-14FB(AW)	
111111	Card		Juli	Owner	Home group	Restriction 1	Basic access	AA-14FB(AW)	
164785	Access code	2022-07-29 14:15	Maria	Guest	Home group	Restriction 1	For guests	AA-14FB(AW)	
8536513	UKEY		John	Owner	Home group	Access	Basic access	AA-14FB(AW)	
7d192999-bd04-412f-8178-b6dbf86301b8	QR-code		Alex	Guest	Home group	Access	For guests	Unit 1 Entrance	

If you click values in the User, Access restrictions, Schedule, or Device columns, you will be redirected to the corresponding tab for editing.

Also, there is a filter by **identifier**, **type**, **user** (owner), **device**, **access restrictions**, **schedule**, or the date the identifier was **used**. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all identifiers used before the date.

MATCH ALL USED LESS OR EQUAL 2022-09-12 00:00 DEVICE EQUALS UNIT 1 ENTRANCE + ADD FILTER SAVE AS EXPORT TO

Identifier	Type	Used	User	Owner type	Group	Access restriction	Schedule	Device
451688a9-db75-4b8d-8f8e-98d2e76c8595	QR-code	2022-07-29 14:15	Alex	Guest	Home group	Basic access		Unit 1 Entrance
451688a9-db75-4b8d-8f8e-98d2e76c8595	QR-code	2022-07-29 14:15	John	Guest	Home group			Unit 1 Entrance

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL USED LESS OR EQUAL 2022-09-12 00:00 + ADD FILTER SAVE AS SEGMENTS EXPORT TO

Identifier	Type	Used	User	Owner type	Group	Access restriction	Schedule	Device
451688a9-db75-4b8d-8f8e-98d2e76c8595	QR-code	2022-07-29 14:15	Alex	Guest	Home group	Basic access		Unit 1 Entrance
451688a9-db75-4b8d-8f8e-98d2e76c8595	QR-code	2022-07-29 14:15	John	Guest	Home group			Unit 1 Entrance

6.6 ACS logs

In the tab, you can monitor all events that are connected with access and identifiers. With the **online mode**, you can control all successful and unsuccessful passes in real time.

MATCH ALL + ADD FILTER ONLINE MODE EXPORT TO

Created at	Device	Identifier	Type	Owner	Owner type	ACS message
2022-10-05 15:59:32	AV03BD	6481199	Card	Pete	Guest	Access granted
2022-10-05 15:56:43	AV03BD	23123	Access code	Sam	Owner	Access granted
2022-10-05 15:24:13	AV03BD	54646444	UKEY	Consierge	Owner	Access granted
2022-10-05 15:21:43	AV03BD	12331	Access code	Juli	Guest	Access granted
2022-10-05 15:11:34	AV03BD	1111	Access code	Max	Owner	Access granted
2022-10-05 15:00:43	AV03BD	676788890	Card	Andy	Owner	Access granted
2022-10-04 12:32:24	AV03BD		API call			Access granted by remote host

Total records: 7

If necessary you can **export** all information to your computer.

Also, there is a filter by date, device, identifier, identifier type, owner, owner type, and ACS message. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display events that happened before the date.

Created at	Device	Identifier	Type	Owner	Owner type	ACS message
2022-10-04 12:32:24	AV03BD		API call			Access granted by remote host

Buttons: MATCH ALL, ACS MESSAGE EQUALS ACCESS GRANTED BY REMOTE HOST, + ADD FILTER, SAVE AS, ONLINE MODE, EXPORT TO

Footer: Rows per page 25, Records 1 - 1 of 1

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

Created at	Device	Identifier	Type	Owner	Owner type	ACS message
2022-10-04 12:32:24	AV03BD		API call			Access granted by remote host

Buttons: MATCH ALL, ACS MESSAGE EQUALS ACCESS GRANTED BY REMOTE HOST, + ADD FILTER, SAVE AS, SEGMENTS, ONLINE MODE, EXPORT TO

Footer: Rows per page 25, Records 1 - 1 of 1

7 Communications

- [Conversations](#)(see page 70)
- [Announces](#)(see page 72)
- [Info and polls](#)(see page 75)
- [Emergency alerts](#)(see page 75)

7.1 Conversations

- [How to create a conversation](#)(see page 71)
- [Conversations filtering](#)(see page 71)

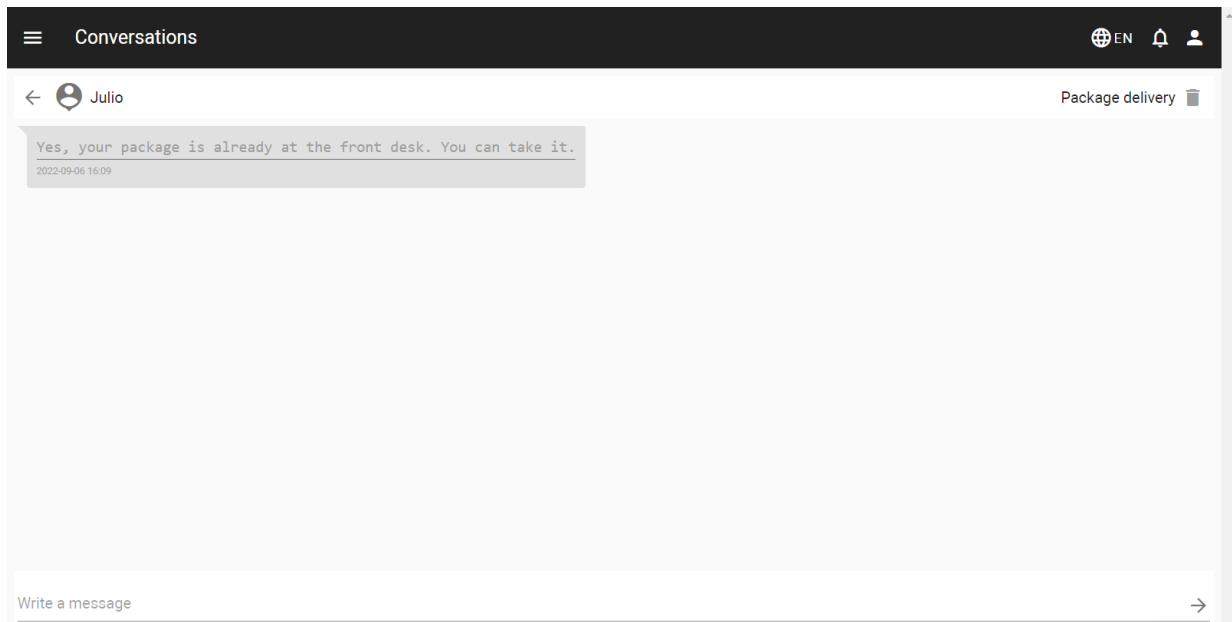
In this tab, users can communicate with other users. Depending on user rights, you see you see either all the conversations or only started by you, addressed to you messages.

MATCH ALL		+ ADD FILTER						DELETE SELECTED	
<input type="checkbox"/>	ID	Subject	Users	Last message	Creation date				
<input type="checkbox"/>	2	Package delivery	Julio	Yes, your package is already at the front desk. You can take it.	2022-09-06 16:09				
<input type="checkbox"/>	4	Question to neighbors	John	Do we need to clean the terrace more often?	2022-10-09 01:02				

Total records: 2

Rows per page 25 Records 1 - 2 of 2

You can click all available conversations to see correspondence or for a reply. If necessary, you can delete a conversation.



7.1.1 How to create a conversation

1. Go to the **Conversation** tab of the Communications section.
2. Click **plus** icon in the left low corner.
3. Enter the conversation **subject**.
4. Type a **message body**.
5. Select **recipient/s**.
6. Click Confirm to send the message.

Add conversation

GENERAL

Subject

Question to neighbors

Message body

Do we need to clean the terrace more often?

Recipient

John +

CANCEL CONFIRM

7.1.2 Conversations filtering

Also, there is a filter by subject, message body, users, and date of creation. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less, great** than your parameter, or contain (**has**) it, e.g. search less than indicated date will display all events before the date. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

MATCH ALL **USERS IS JOHN** + ADD FILTER SAVE AS DELETE SELECTED

<input type="checkbox"/>	ID	Subject	Users	Last message	Creation date	
<input type="checkbox"/>	4	Question to neighbors	John	Do we need to clean the terrace more often?	2022-10-09 01:02	

Total records: 1

Rows per page 25 Records 1 - 1 of 1

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL **USERS IS JOHN** + ADD FILTER SAVE AS **SEGMENTS** DELETE SELECTED

<input type="checkbox"/>	ID	Subject	Users	Last message	Creation date	
<input type="checkbox"/>	4	Question to neighbors	John	Do we need to clean the terrace more often?	2022-10-09 01:02	

Total records: 1

Rows per page 25 Records 1 - 1 of 1

7.2 Announces

- [How to create an announce](#)(see page 73)
- [Announces filtering](#)(see page 74)

On the Link server, it is possible to create announce or poll with important information and sent it to all necessary groups or users. This announcement will be displayed in [the Link web interface](#)⁵⁴ or on users monitors:

Messages

Show: All messages

All

Mailing

Polls

NEW Mailing 8:57 AM, Thu, 57-20-22 ✕

Power Outage


There will be no electricity tomorrow from 16 to 17 pm.

Poll 8:58 AM, Thu, 58-20-22 ✕


Cleaning

Do we need to clean the terrace more often?

⁵⁴ <https://wiki.bas-ip.com/basiplinken/info-and-polls-135955874.html>

In this section, you can create announcements or polls, set the time of their sending, check statuses (complete or not), and results of polls. If an entry is not necessary anymore delete it .

MATCH ALL		+ ADD FILTER									DELETE SELECTED
<input type="checkbox"/>	ID ↓	Name	Type	Scheduled date	Status	Sent	Received	Error			
<input type="checkbox"/>	47	Cleaning	Poll		New	0	0	0			
<input type="checkbox"/>	46	Poll	Poll	2022-10-09 11:00	Completed	0	0	0			
<input type="checkbox"/>	45	Power outage	Info		Completed	1	1	0			
<input type="checkbox"/>	44	Package delivery	Info		Completed	3	1	2			

With the help of the edit button,  you can check announces content or poll results in the corresponding section.

Announce type
Poll

Send via
e-mail

Send on

Result

Recipient: Administrator

Yes, let's do it every week

No, every 2 weeks is ok

Content

Subject
Cleaning

Do we need to clean the terrace more often?

Multi answers allowed Answer typed by user allowed

ADD POLL ANSWER

Answer
Yes, let's do it every week

7.2.1 How to create an announce

1. Go to the **Announces** tab of the Communications section.
2. Click **plus** icon in the low left corner.
3. Enter the entry **name** that will be displayed in the Announces tab.
4. Add a **description** if necessary.
5. Select the announce type: **info** (just message) or **poll** (message with a possibility to select variants or type answer).
6. Select in which way the announcement must be sent via **e-mail** or to **devices**.
7. Set the **date** of the announcement sending.
8. Add **recipients** in the corresponding section.
9. In the Content section enter data that will be displayed for recipients:
 - the **subject** of the announcement;
 - message **content**;
 - if you select a poll type, **add poll answers**;
 - for poll type, enable the options of selecting some variants of answer (**multi answers**) or typing free answer (**answer typed by user**).
10. Click the **Save** button in the low left corner when all required data will be entered.

General

Name
Cleaning

Description

Announce type
Poll

Send via
e-mail

Send on
2022-09-14 00:00

Result

Recipients

If a group is selected as the recipient, then all users in the specified group will receive the mailing list

- Administrator

Content

Subject
Cleaning

Do we need to clean the terrace more often?

Multi answers allowed Answer typed by user allowed

7.2.2 Announces filtering


Also, there is a filter by name, status, and type. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less, great** than your parameter, or contain (**has**) it. You can select a few parameters and choose whether the results will match all filters or any of them.



MATCH ALL NAME HAS POWER									
+ ADD FILTER SAVE AS									
DELETE SELECTED									
<input type="checkbox"/>	ID ↓	Name	Type	Scheduled date	Status	Sent	Received	Error	
<input type="checkbox"/>	48	Power outage	Info		Completed	1	0	0	✓ ✎ 🗑
									Total records: 1
						Rows per page	10	Records 1 - 1 of 1	< >

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL DEVICE TYPE EQUALS PANEL									
+ ADD FILTER SAVE AS SEGMENTS									
DELETE SELECTED									
<input type="checkbox"/>	Name	Duration	Status	File name	Device type	Created at			
<input type="checkbox"/>	Emergency	10	Done	video_2022-02-04_14-22-08 (online-audio-converter.com).wav	Panel	2022-02-07 10:58	▶ ✎ 🗑		
							Total records: 1		
						Rows per page	25	Records 1 - 1 of 1	< >

7.3 Info and polls


In this tab, you can check all addressed to you announcements and polls. To read it and answer, click  .

MATCH ALL + ADD FILTER				
ID	Name	Type	Status	
49	Power outage	Info	New	
47	Cleaning	Poll	Responded	

Total records: 2

Rows per page 25 Records 1 - 2 of 2


Also, there is a filter by name, status, and type. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or contain (**has**) it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

MATCH ALL STATUS EQUALS SENT + ADD FILTER SAVE AS				
ID	Name	Type	Status	
49	Power outage	Info	New	

Total records: 1

Rows per page 25 Records 1 - 1 of 1

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL STATUS EQUALS SENT + ADD FILTER SAVE AS SEGMENTS				
ID	Name	Type	Status	
49	Power outage	Info	New	

Total records: 1

Rows per page 25 Records 1 - 1 of 1

7.4 Emergency alerts

- [How to create an emergency alert\(see page 76\)](#)
- [Alerts filtering\(see page 77\)](#)

In the tab, you can create and manage emergency alerts that can be sent by the administrator or concierge in case of fire or other emergencies. An alert will be played on the device.

The feature is available for AQ-07LL, AZ-07LL, AU-04LA, AU-04LAF, SP-03, and SP-03F.

You can prepare alerts for different cases and manage them with the help of buttons: ▶ to start playing the alert, || to stop the sound. Also, you can edit ✎ or delete 🗑 alerts.

MATCH ALL		+ ADD FILTER							DELETE SELECTED	
<input type="checkbox"/>	Name	Duration	Status	File name	Device type	Created at				
<input type="checkbox"/>	Emergency	10	Done	video_2022-02-04_14-22-08 (online-audio-converter.com).wav	Panel	2022-02-07 10:58	▶		✎	🗑
<input type="checkbox"/>	Fire alarm	15	Done	video_2022-02-04_14-22-08 (online-audio-converter.com).wav	Monitor	2022-04-11 16:35	▶		✎	🗑

Total records: 2

7.4.1 How to create an emergency alert

1. Go to the **Emergency alert** tab of the Communications section.
2. Click **plus** icon in the left low corner.
3. Enter the event **name**.
4. Set the alert playback **duration**.
5. Upload a **sound file in .wav** format that will be played while alerting.
6. Select announce **type** depending on what device the alert will be sent to: panel, monitor, or all.
7. Enable the **open locks** option when an emergency alert is triggered.
8. Select or add a **group** or concrete **device**/s to which this alert will be applied.
9. Click the **Save** button in the left low corner when all required data will be entered.

General ^

When an emergency alert is triggered, an audio file will be played on the specified devices

Name
Emergency

Duration File name
10 video_2022-02-04_14-22-08 (on X)

Announce type
Panel ☑ Open locks

Groups ^

Devices from the specified groups will be selected to play the sound notification

+ 🗑

No data

Devices ^

You can specify a list of devices if they are not in the selected groups, but should play a sound notification

+ 🗑

Panel AA14 Office 🗑

←
🗑

7.4.2 Alerts filtering

Also, there is a filter by alert name, device type, and status. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or contain (**has**) it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

The screenshot shows a web interface for alert filtering. At the top, there are buttons for 'MATCH ALL', 'DEVICE TYPE EQUALS PANEL', '+ ADD FILTER', and 'SAVE AS'. Below these is a table with columns: Name, Duration, Status, File name, Device type, and Created at. A single record is displayed with the name 'Emergency', duration '10', status 'Done', and file name 'video_2022-02-04_14-22-08 (online-audio-converter.com).wav'. The device type is 'Panel' and the created at time is '2022-02-07 10:58'. At the bottom right, it shows 'Total records: 1' and 'Rows per page 25'.

Name	Duration	Status	File name	Device type	Created at
Emergency	10	Done	video_2022-02-04_14-22-08 (online-audio-converter.com).wav	Panel	2022-02-07 10:58

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

This screenshot is identical to the previous one, but with the 'SAVE AS' and 'SEGMENTS' buttons highlighted with red boxes. The 'SEGMENTS' button is located to the right of the 'SAVE AS' button in the top navigation bar.

8 Telephony settings



- [Virtual numbers](#)(see page 78)
- [Forward rules](#)(see page 81)
- [Call history](#)(see page 84)
- [Inbuild call service](#)(see page 86)











8.1 Virtual numbers

To make a call between a panel, an indoor video entry phone (monitor), or a user phone, the Link version with SIP must be deployed and the corresponding license must be applied for the server. Here you can create and manage virtual numbers.

For a user registered in the Link app, a virtual number is created and applied automatically. You can check the number in the user [profile](#)⁵⁵.

- [How to create a virtual number](#)(see page 78)
- [Virtual numbers filtering](#)(see page 80)

In the tab, you see all created virtual numbers with detailed information about them. With the help of  and  buttons, you can edit or delete numbers.

MATCH ALL		+ ADD FILTER										DELETE SELECTED
<input type="checkbox"/>	ID	Name	Number	User	Device	Group	Active	Status	Created at			
<input type="checkbox"/>	204	aq07	1131	Michael	AZ07	Apt 2	Yes	offline	2022-12-27 18:42			
<input type="checkbox"/>	206	1027	1027	Administrator	AA12FB-a	Apt 1	Yes	offline	2022-12-29 15:34			
<input type="checkbox"/>	207	AA14	1040	Administrator	AV08FB		Yes	offline	2022-12-29 18:26			
<input type="checkbox"/>	208	1049	1049	Administrator	AT-10	Apartment 1	Yes	offline	2022-12-30 16:52			
<input type="checkbox"/>	209	AA15	1052	Alex			Yes	offline	2022-12-30 19:22			

Total records: 5

Rows per page: 25 Records 126 - 130 of 130

8.1.1 How to create a virtual number

1. Go to the **Virtual numbers** tab of the Telephony settings section.
2. Click **plus** icon in the left low corner.
3. The system will automatically generate a SIP number. Enter a name for the number.
4. Create the password for the number.

⁵⁵ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

5. Tick the **Active** box to turn on the number operating.

To deactivate a number enable this box in the number settings.

6. Select the **user** (from previously added in the [User](#)⁵⁶ tab) of the number.
 7. Select the **device** on which the number must be used. If a user will use the number on a 3d-party device, leave the field blank.

The screenshot shows the configuration interface for a number. It is divided into two main sections: 'General' and 'Forward settings'.

General (Belongs to the mobile client, editing is limited):

- Name:** For entrance panel
- Number:** 1031
- Password:** qwed12
- Active**
- User:** Administrator
- Device:** Unit 1 Entrance



Forward settings (Allows you to more flexibly manage the call process, namely to set up forwarding queues for a given number):

- Forward mode:** Disabled

At the bottom right of the interface, there are two circular buttons: a back arrow and a lock icon.

8. If it is necessary, enable and **forward settings** for the number and set them manually or select a [forward rule](#)⁵⁷ from previously created.

The following options are available:

- to forward calls **immediately** to all indicated in the call queue field/s numbers;
- to forward calls to indicated in the call queue number/s **if there is no answer** from the main number;
- to set the **time** (5-30 sec) after which the call will be forwarded if there is no answer;
- **add** number/numbers (to which the call will be forwarded) to the **call queue** from the virtual number list;
- to set **call duration** by clicking  ;
- to set days and time when the forward is **valid** by clicking  ;
- forward calls to indicated in the call queue field/s numbers if the primary **number is busy or an error occurs**;

⁵⁶ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

⁵⁷ <https://wiki.bas-ip.com/basiplinken/forward-rules-135955902.html>

General

Belongs to the mobile client, editing is limited

Name: For entrance panel Number: 1031

Password: qwed12

Active

User: Administrator Device: Unit 1 Entrance

Forward settings

Allows you to more flexibly manage the call process, namely to set up forwarding queues for a given number

Forward mode: Manual settings

Immediately

If no answer, then after 10 seconds forward to

+ ADD CALL QUEUE

If busy or error, forward to

+ ADD CALL QUEUE

← 📄

9. Click the **Save** button in the left low corner when all required data will be entered.

8.1.2 Virtual numbers filtering

There is a filter by number, name, activeness, user, device, and group. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated number will display all numbers created before the indicated.

MATCH ALL										ACTIVE EQUALS YES	+ ADD FILTER	↓ SAVE AS
										DELETE SELECTED		
<input type="checkbox"/>	ID	Name	Number	User	Device	Group	Active	Status	Created at			
<input type="checkbox"/>	204	aq07	1131	Michael	AZ07	Apt 2	Yes	offline	2022-12-27 18:42			
<input type="checkbox"/>	206	1027	1027	Administrator	AA12FB-a	Apt 1	Yes	offline	2022-12-29 15:34			
<input type="checkbox"/>	207	AA14	1040	Administrator	AV08FB		Yes	offline	2022-12-29 18:26			
<input type="checkbox"/>	208	1049	1049	Administrator	AT-10	Apartment 1	Yes	offline	2022-12-30 16:52			
<input type="checkbox"/>	209	AA15	1052	Alex			Yes	offline	2022-12-30 19:22			

Total records: 5

Rows per page: 25 Records 126 - 130 of 130

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can **save** your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL ACTIVE EQUALS YES + ADD FILTER SAVE AS SEGMENTS

DELETE SELECTED

<input type="checkbox"/>	ID	Name	Number	User	Device	Group	Active	Status	Created at	:
<input type="checkbox"/>	204	aq07	1131	Michael	AZ07	Apt 2	Yes	offline	2022-12-27 18:42	
<input type="checkbox"/>	206	1027	1027	Administrator	AA12FB-a	Apt 1	Yes	offline	2022-12-29 15:34	
<input type="checkbox"/>	207	AA14	1040	Administrator	AV08FB		Yes	offline	2022-12-29 18:26	
<input type="checkbox"/>	208	1049	1049	Administrator	AT-10	Apartment 1	Yes	offline	2022-12-30 16:52	
<input type="checkbox"/>	209	AA15	1052	Alex			Yes	offline	2022-12-30 19:22	

Total records: 5

Rows per page 25 Records 126 - 130 of 130

8.2 Forward rules

- [How to create a forward rule](#)(see page 82)
- [Forward rules filtering](#)(see page 83)

In this tab, you can create forward rules for redirecting calls from one virtual number to other/s. These rules can be applied to required numbers in the [Virtual numbers](#)⁵⁸ tab. With the help of and buttons, you can edit or delete rules.

MATCH ALL + ADD FILTER

DELETE SELECTED




<input type="checkbox"/>	ID	Name	Queues	:
<input type="checkbox"/>	7	Forward from AT10 1629	3	
<input type="checkbox"/>	8	One by one call	2	

Total records: 2

Rows per page 25 Records 1 - 2 of 2

58 <https://wiki.bas-ip.com/basiplinken/virtual-numbers-135955892.html>

8.2.1 How to create a forward rule

1. Go to the **Forward rules** tab of the Telephony settings section.
2. Click **plus** icon in the left low corner.
3. Enter a rule name.
4. Select in what case the call will be forwarded. The following options are available:
 - to forward calls **immediately** to all indicated in the call queue field/s numbers;
 - to forward calls to indicated in the call queue number/s **if there is no answer** from the main number;
 - to set the **time** (5-30 sec) after which the call will be forwarded if there is no answer;
 - **add** number/numbers (to which the call will be forwarded) to the **call queue** from the virtual number list;
 - to set **call duration** by clicking  ;
 - to set days and time when the forward is **valid** by clicking  ;
 - forward calls to indicated in the call queue field/s numbers if the primary **number is busy or an error occurs**;
5. Click add **call queue** and select type number you want to add: **virtual** or **mobile phone number** (if [SIP trunks](#)⁵⁹ are enabled). You can add () several call queues with a few numbers in them.

If you want to receive calls to a mobile phone instead of the Link app, this number (in an international format) must be indicated in the call queue.

6. Click the **Save** button in the left low corner when all required data will be entered.

⁵⁹ <https://wiki.bas-ip.com/basiplinken/sip-trunks-135958438.html>

General ^

Name
Forward from outdoor panel

Forward settings ^

Allows you to more flexibly manage the call process, namely to set up forwarding queues for a given number

Immediately

If no answer, then after 10 seconds forward to

☰ Call queue #1 ⚙️ 🗑️

Call duration: ⌚ 60 seconds

Valid period: Mo Tu We Th Fr Sa Su 10:00 - 18:00

1299(1299) ✕ 1000(1000) ✕ +

☰ Call queue #2 ⚙️ 🗑️

Call duration: ⌚ 60 seconds

Valid period: Mo Tu We Th Fr Sa Su 00:00 - 00:00

1000(1000) ✕ +

+ ADD CALL QUEUE

If busy or error, forward to

+ ADD CALL QUEUE

📞
←
📄

8.2.2 Forward rules filtering

Also, there is a filter by rule name for quick search. To do this, you need to click the **Add filter** button, select the parameter and enter the rule name.

MATCH ALL NAME HAS FORWARD + ADD FILTER 📄 SAVE AS

DELETE SELECTED

<input type="checkbox"/>	ID	Name	Queues	
<input type="checkbox"/>	7	Forward from AT10 1629	3	✎️ 🗑️

Total records: 1

Rows per page 25 Records 1 - 1 of 1 < >

In addition, you can **save** your search for further use by clicking the corresponding button. All saved searches are displayed after clicking the **Segments** button.

MATCH ALL NAME HAS FORWARD + ADD FILTER SAVE AS SEGMENTS DELETE SELECTED

ID	Name	Queues
7	Forward from AT10 1629	3

Total records: 1

Rows per page 25 Records 1 - 1 of 1


8.3 Call history

This tab contains information about all virtual numbers calls, their duration, statuses, and dates they were made.

Call history

MATCH ALL + ADD FILTER

From	To	Duration(sec)	Talk duration(sec)	Status	Date	SIP trunk
1045(Conierge)	1644(John V)	13	0	Not answered	2023-04-04 18:40:39	basip
1045(Conierge)	1087(Juli)	8	6	Answered	2023-04-04 18:40:27	basip
1549 (Administrator)	1045(Conierge)	6	5	Answered	2023-04-04 18:13:09	basip
1644 (John V)	1549 (Administrator)	10	0	Not answered	2023-04-04 18:11:13	
1023(Pete)	1088(Max)	16	15	Answered	2023-04-04 18:09:21	link twilio trunk
1756(Anna)	1549 (Administrator)	7	0	Not answered	2023-04-04 18:07:31	
1023(Pete)	1045(Conierge)	12	11	Answered	2023-04-04 18:07:10	
1644(John V)	1087(Juli)	20	19	Answered	2023-04-04 18:06:03	
1088(Max)	1045(Conierge)	10	9	Answered	2023-04-04 18:05:42	link twilio trunk

By pressing , you can unfold the entity with detailed info about the call, its direction (virtual number, mobile number), and forwardings (if they are configured).

MATCH ALL		+ ADD FILTER														
From ↓	To	Duration(sec)	Talk duration(sec)	Status	Date	SIP trunk										
1045(Conierge)	1644(John V)	20	4	Answered	2023-04-11 01:19:34											
<table border="1"> <thead> <tr> <th>Dialed to</th> <th>Duration(sec)</th> <th>Talk duration(sec)</th> <th>Status</th> <th>Date</th> </tr> </thead> <tbody> <tr> <td>1644(John V)</td> <td>18</td> <td>4</td> <td>Answered</td> <td>2023-04-11 01:19:36</td> </tr> </tbody> </table>							Dialed to	Duration(sec)	Talk duration(sec)	Status	Date	1644(John V)	18	4	Answered	2023-04-11 01:19:36
Dialed to	Duration(sec)	Talk duration(sec)	Status	Date												
1644(John V)	18	4	Answered	2023-04-11 01:19:36												
1549 (Administrator)	1045(Conierge)	6	5	Answered	2023-04-04 18:13:09	basip										
1644 (John V)	1549 (Administrator)	10	0	Not answered	2023-04-04 18:11:13											
1023(Pete)	1088(Max)	16	15	Answered	2023-04-04 18:09:21	link twilio trunk										
1756(Anna)	1549 (Administrator)	7	0	Not answered	2023-04-04 18:07:31											
1023(Pete)	1045(Conierge)	12	11	Answered	2023-04-04 18:07:10											
1644(John V)	1087(Juii)	20	19	Answered	2023-04-04 18:06:03											
1088(Max)	1045(Conierge)	10	9	Answered	2023-04-04 18:05:42	link twilio trunk										

There is a filter by ID, a number from which the call was made, user, a number to which the call was made, date, call duration, and status. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate) or **has** the value, or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all calls made before that day.

MATCH ALL		DURATION EQUALS 13					+ ADD FILTER		SAVE AS	
From ↑	To	Duration(sec)	Talk duration(sec)	Status	Date	SIP trunk				
1045(Conierge)	1644(John V)	13	0	Not answered	2023-04-04 18:40:39	basip				

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can **save** your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

The screenshot shows a 'Call history' interface. At the top, there is a navigation bar with a hamburger menu icon, the text 'Call history', and icons for language (EN), notifications, and user profile. Below the navigation bar, there is a filter bar containing 'MATCH ALL', 'DURATION EQUALS 13', '+ ADD FILTER', 'SAVE AS' (highlighted with a red box), and 'SEGMENTS' (highlighted with a red box). The main content area is a table with the following columns: From, To, Duration(sec), Talk duration(sec), Status, Date, and SIP trunk. A single call record is displayed with a dropdown arrow on the left.

From ↑	To	Duration(sec)	Talk duration(sec)	Status	Date	SIP trunk	
1045(Conserge)	1644(John V)	13	0	Not answered	2023-04-04 18:40:39	basip	⋮

8.4 Inbuild call service







9 Devices management






























































- [Devices](#)(see page 87)
- [Logs](#)(see page 94)
- [Queue tasks](#)(see page 97)
- [Status](#)(see page 99)
- [Device initialization](#)(see page 100)

9.1 Devices

All devices (panels, controllers, monitors) must be added to the Link server to associate physical devices with data on the server. Adding a device to the Link server gives the ability for remote interaction and monitoring.

- [How to add a device to the Link server](#)(see page 88)
- [Remote device configuration](#)(see page 89)
- [Filter for devices display](#)(see page 93)

In the tab, you can add a new device, check already added device settings, edit  or delete  them. Also for each device, there is the ability to cope information , start [initialization](#)⁶⁰  (only for SP-03), restart the task [queue](#)⁶¹ , and synchronize device data (to send to a device all information about settings, identifiers, users, etc., that the server has) .

MATCH ALL		+ ADD FILTER						SEARCH DEVICES	DELETE SELECTED
<input type="checkbox"/>	ID	Name	Description	Group	Model	Communication protocol	Status		
<input type="checkbox"/>	2	Unit 1 Entrance		Home group	AA12(Panel)	HTTP(192.168.1.2:8)		     	
<input type="checkbox"/>	13	Test Monitor AQ-07	Test monitor	Unit #4	AQ07(Monitor)	HTTP(91.225.165.47:757)	offline(2021-10-12 15:45)	     	
<input type="checkbox"/>	17	Consierge		Unit #4	AM02(Monitor)	HTTP(91.225.165.47:798)	offline(2021-12-28 16:53)	     	
<input type="checkbox"/>	18	Bob panel		Apartment #5	AA12(Panel)	HTTP(192.168.1.1:8)	offline(2021-09-20 22:39)	     	
<input type="checkbox"/>	20	AQ07L 4 flat		Apartment #5	AQ07(Monitor)	HTTP(91.225.165.47:78)	offline(2021-09-30 17:17)	     	
<input type="checkbox"/>	23	General Device		Home group	AA12(Panel)	HTTP(127.0.0.1)		     	
<input type="checkbox"/>	28	Consierge	Unit 1	Unit #1	AM02(Monitor)	HTTP(192.168.1.46)	offline(2021-12-28 16:53)	     	
<input type="checkbox"/>	31	General monitor		Unit #1	AT07L(Monitor)	HTTP(192.168.1.198)	offline(2022-01-13 20:44)	     	
<input type="checkbox"/>	34	AA-07		Unit #4	AA07(Panel)	HTTP(91.225.165.47:91)	offline(2021-12-10 12:43)	     	
<input type="checkbox"/>	39	Monitor AT07L		Apartment #1	AT07L(Monitor)	HTTP(192.168.1.198)	offline(2022-01-13 20:44)	      	

60 <https://wiki.bas-ip.com/basiplinken/device-initialization-135955953.html>

61 <https://wiki.bas-ip.com/basiplinken/queue-tasks-135955941.html>

✓ Tip

Synchronize device data feature can be useful to automatically fill renewed device with existing data. For example, after replacing a broken device.

9.1.1 How to add a device to the Link server

1. Go to the **Devices** tab of the Device management section.
2. Click **plus** icon in the left low corner.
3. Enter the device **name**.
4. Select its **type**: panel, monitor, access controller.
5. Select the device **model**.
6. Indicate the device **Serial number** (check the [Dashboard](#)⁶² tab of the device web interface or device box).
7. Select a **group**/subgroup where the device is installed.
8. If necessary, set panels location **geodata**. This data is required for the Link app, when a visitor with a pass (added to Apple Wallet) approaches the available panel (with location), the pass will be automatically shown.
9. Add a **description**, if necessary.
10. Enable **using a camera to identify license plates**, if necessary.
11. Allow **remote lock opening** (from the device web interface, via API), if necessary.
12. Enter network settings for server and panel interaction:

! Warning

For correct server functioning, all devices must be added to the access rules that apply to the corresponding groups.

- select the appropriate **communication protocol**: HTTP or MQTT (is recommended to use);
- enter the device **IP address** and **port** (for HTTP only);
- enter **login** and **password** that are used to enter the device web interface;
- indicate server interaction password (is created in the Management system section ([Network](#)⁶³ tab) of the device web interface).

⁶² <https://wiki.bas-ip.com/aa07/dashboard-135955050.html>

⁶³ <https://wiki.bas-ip.com/aa07/network-135955054.html>

Also, the same network settings as for the server must be entered in the device web interface. The management system must be enabled for the device:

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 required data.
5. Submit settings.

Detailed instructions are [here](#)⁶⁴.

Management system BAS-IP Link
SUBMIT

Mode
MQTT ▼

URL
link.bas-ip.com:8883

Password

Send realtime logs to server

Encrypted

Certificate Info

File

13. Click the **Save** button in the left low corner when all required data will be entered.

9.1.2 Remote device configuration

Device basic configurations can be done in the device web interface. And if they are done, there is no need to set them from the Link side. But if some of the following parameters are missed or required corrections, so they, also, can be done in the corresponding sections. You must enable setting section you want to send.

⁶⁴ <https://wiki.bas-ip.com/aa07/network-135955054.html>

The following settings can be entered:

- **automatic forwarding**(see page 121) **settings** is a feature of automatic creation of forward rules for apartment group user/s and sending them to device/s. If this feature is enabled, for all groups will be automatically created and applied virtual numbers. And when adding a user that has virtual number/s to a group, forwarding that includes all user numbers is automatically created. In addition, SIP and address settings are also automatically created and sent to the device. But if there are troubles with them (e.g., logical addresses are already set for devices manually and do not match created on the server or the Link set and sent SIP settings for connecting to an external address, but internal is required, etc.), it is possible to set and sent the following settings to the device manually:
 - **SIP settings**⁶⁵ are required for calls via SIP protocol. For correct SIP functioning, you must:
 - **enable SIP**;
 - select SIP address type: server URL or server external IP address;
 - enter SIP **server address** (realm) that can be represented by both an IP address and a domain name, e.g. gb.sip.bas-ip.com⁶⁶;
 - enter **SIP server proxy** that can be represented by both an IP address and a domain name, e.g. sip:gb.sip.bas-ip.com⁶⁷. Before the proxy address, you must enter "sip:";
 - server **STUN IP address**, e.g., stun.l.google.com⁶⁸;
 - **port** of the STUN server, e.g., 19302;
 - SIP number (**login**);
 - **password** for the SIP number;

⁶⁵ <https://wiki.bas-ip.com/aa07/panel-135955062.html>

⁶⁶ <http://gb.sip.bas-ip.com>

⁶⁷ <http://gb.sip.bas-ip.com>

⁶⁸ <http://stun.l.google.com>

- **timeout** for re-registration to renew the lost connection with the SIP server.

Automatic forwarding settings ^

Model-specific settings. The settings will be automatically sent to the device.

SIP settings

SIP enabled

Select address

Server external IP address ▼

Realm address

135.181.101.136

Proxy address

sip:135.181.101.136

STUN address

stun.l.google.com

STUN port

19302

Login

1005

Password

ESV6u7WC

Timeout(sec)

120 ▼

- [address settings](#)⁶⁹ that are required for device correct display in the intercom system and connecting between devices. If you are adding a panel, you must select **panel operation mode** (more details are [here](#)⁷⁰). **Building No., Unit No., Floor No., Apartment No.** and **Device No.** must be indicated depending on the device type.

Address settings

Building

12

Unit

1

Floor

3

Room

1

Device number

0

Sync code

123456

⁶⁹ <https://wiki.bas-ip.com/aa07/panel-135955062.html>

⁷⁰ <https://wiki.bas-ip.com/aa07v4/en/konfigurirovanie-cherez-web-interfejs/vyzyvnaya-panel#id-Вызывнаяпанель-ApartmentSettings>

- for an [elevator controller](#)⁷¹ the following settings can be done:
 - enable/disable sending of settings on device;
 - select available **mode**: Up (an elevator moves only in the upward direction), Down (movement is only in the downward direction), Up and down (both directions are available), Access by identifier (movement only to those floors that are available for the used identifier);
 - select relay **type**: COM-NO/COM-NC;
 - set the **time** during which the relay will be switched;
 - set lift **release time** (during which relay will be closed/opened) for identifier and for API call;
 - enable/disable the **switching relay when turning on the device**;
 - create **+** a list of floors (depending on number of available relays) and corresponding relays for a unit;
 - enter **Floor No.** and **Relay No.** that connected to each floor at the controller;
 - indicate whether the floor is public or not. Users will always have access to the public floor despite their identifier settings;
 - select apartments located on each floor;

⁷¹ <https://wiki.bas-ip.com/evrc-ip-135957503.html>

Elevator controller settings ^

Send elevator controller settings on device

Mode

Mode	Controller relays
Access by identifier	COM-NO
Relay switch time (msec.)	
10	
Lift release time for identifier (sec.)	Lift release time for API call (sec.)
55	5

Switch when turning on the device

Controller relays: (used 4 from 16)

Floor name	Floor number	Relay numbers	
Floor #1	1	[1]	 
Floor #2	2	[2]	 
Floor #3	3	[3, 4]	 

9.1.3 Filter for devices display

There is a filter by name, device type, and IP domain. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less, great** than your parameter, or contain (**has**) it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

MATCH ALL		TYPE EQUALS PANEL		+ ADD FILTER		↓ SAVE AS							
								SEARCH DEVICES		DELETE SELECTED			
<input type="checkbox"/>	ID	Name	Description	Group	Model	Communication protocol	Status						
<input type="checkbox"/>	2	Unit 1 Entrance			AA12(Panel)	HTTP(192.168.1.2:80)							
<input type="checkbox"/>	18	Bob panel		Apartment #5	AA12(Panel)	HTTP(192.168.1.1:8)	offline(2021-09-20 22:39)						
<input type="checkbox"/>	23	Device		Home group	AA12(Panel)	HTTP(127.0.0.1:80)							
<input type="checkbox"/>	34	AA-07		Unit #4	AA07(Panel)	HTTP(91.225.165.47:91)	offline(2021-12-10 12:43)						
<input type="checkbox"/>	47	AA12FB		Home group	AA12(Panel)	HTTP(192.168.1.1:80)							

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL		TYPE EQUALS PANEL		+ ADD FILTER		↓ SAVE AS		SEGMENTS					
								SEARCH DEVICES		DELETE SELECTED			
<input type="checkbox"/>	ID	Name	Description	Group	Model	Communication protocol	Status						
<input type="checkbox"/>	2	Unit 1 Entrance			AA12(Panel)	HTTP(192.168.1.2:80)							
<input type="checkbox"/>	18	Bob panel		Apartment #5	AA12(Panel)	HTTP(192.168.1.1:8)	offline(2021-09-20 22:39)						
<input type="checkbox"/>	23	Device		Home group	AA12(Panel)	HTTP(127.0.0.1:80)							
<input type="checkbox"/>	34	AA-07		Unit #4	AA07(Panel)	HTTP(91.225.165.47:91)	offline(2021-12-10 12:43)						
<input type="checkbox"/>	47	AA12FB		Home group	AA12(Panel)	HTTP(192.168.1.1:80)							

9.2 Logs

This tab contains a log that displays all the events that happened with added to the Link devices (panels, monitors, elevator controllers): login to the web interface, lock opening using an identifier, to or from which number a call was made, elevator called, etc. You can export all logs by clicking the corresponding button.

With the online mode, you can monitor all events in real time.

MATCH ALL		+ ADD FILTER							
<input type="checkbox"/> ONLINE MODE		REFRESH DATA						EXPORT TO	
Created at	Category	Priority	Event	Markers	Info	Source			
2022-10-07 18:58:30	System	Low	Login to the web interface		Successful (admin) login to the web interface	AV03BD			
2022-10-07 13:52:57	Information	Low	Incoming call		Incoming call from number 1024@95.216.166.9, call was accepted	AV03BD			
2022-10-07 13:19:25	Access	Medium	Elevator called to the floor		Floor number - 1, name - Floor 1, source - interface.api	lift controller			
2022-10-07 13:19:25	Access	Medium	Access granted by the web interface		Lock All locks opened opened from the web interface	AV03BD			
2022-10-07 13:19:09	Information	Low	Sip registration lost			Unit 1 Entrance			
2022-10-07 13:19:09	Information	Medium	Outgoing call		Outgoing call to number sip:38307@sip.bas-ip.com, call was not accepted	Unit 1 Entrance			
2022-10-07 13:18:19	Access	Medium	Access granted by the web interface		Lock 1 opened from the web interface	Unit 1 Entrance			
2022-10-07 13:18:19	System	Low	Login to the web interface		Successful (admin) login to the web interface	Unit 1 Entrance			
2022-10-07 12:23:00	Access	Medium	Elevator called to the floor		Floor number - 1, name - Floor 1, source - interface.api	lift controller			

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 was opened by free access button
	Access	Lock opened by exit button
	Access	Lock opened by identifier
	Access	General access code entered
	Access	Access granted by valid face identifier
	Access	Lift called to floor
	System	Login to the web interface
	System	Unsuccessful attempt to enter GUI settings
	System	Successfully logging into GUI settings
	Information	Incoming call
	Information	Outgoing call
	Information	Incoming call without status
	Information	Outgoing call without status
	Information	Outgoing call from web-interface
	Information	Missed call

Priority	Category	Event
High	Access	Access denied by remote server
	Access	Access granted by remote server
	Access	Wrong input code
	Access	Unknown identifier
	Access	Access denied by invalid 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
	Access	Access granted by valid license plate
	Access	Access denied by not valid license plate
	Access	Access denied by unknown license plate
	Emergency	Tamper event
Critical	Access	Lock opened too long
	Access	Door is open too long
	Emergency	Abnormal event
	Emergency	Emergently event
	System	Firmware update

Also, there is a filter by **date** (created at), **category**, **priority**, **code**, **device**, **identifier**, **owner**, or created **marker**. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all events before the date.

The screenshot shows the search interface with the following filters and data:

- Filters: MATCH ANY, CREATED AT EQUALS 2022-09-22 00:00, CODE EQUALS INTERFACE.LIFT_CALLED_TO_FLOOR
- Buttons: + ADD FILTER, SAVE AS, ONLINE MODE, REFRESH DATA, EXPORT TO

Created at	Category	Priority	Event	Markers	Info	Source
2022-09-26 16:36:05	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2
2022-09-26 16:36:04	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

The screenshot shows the search interface with the following filters and data:

- Filters: MATCH ANY, CREATED AT LESS OR EQUAL 2022-10-19 18:30
- Buttons: + ADD FILTER, SAVE AS, SEGMENTS, ONLINE MODE, REFRESH DATA, EXPORT TO

Created at	Category	Priority	Event	Markers	Info	Source
2022-09-29 17:47:24	System	Low	Login to the web interface		Successful (admin) login to the web interface	Unit 1 Entrance
2022-09-26 16:36:05	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2

9.3 Queue tasks

Some data for [devices⁷²](https://wiki.bas-ip.com/basiplinken/devices-135955918.html) (SIP, Network, or Address settings), adding/deleting identifiers can be done in the Link and sent to the required device. In this section, you can monitor tasks status and results, restart queues or delete .

⁷² <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

MATCH ALL		+ ADD FILTER									DELETE SELECTED	
<input type="checkbox"/>	ID	Device	Type	Status	Result	Created at	Updated at					
<input type="checkbox"/>	14244	lift controller 2	Sending elevator controllers	Completed	controller settings updated, controller floor map updated	2022-10-04 16:59	2022-10-04 16:59					
<input type="checkbox"/>	14243	lift controller 2	Sending elevator controllers	Completed	controller settings updated, controller floor map updated	2022-10-04 16:58	2022-10-04 16:59					
<input type="checkbox"/>	14242	lift controller 2	Sending elevator controllers	Completed	controller settings updated, controller floor map updated	2022-10-04 16:57	2022-10-04 16:59					
<input type="checkbox"/>	14241	AV03BD	Sending identifiers	New		2022-10-04 12:29						
<input type="checkbox"/>	14240	Panel AA14 Office	Sending identifiers	New		2022-10-04 12:29						
<input type="checkbox"/>	14239	CR02BD	Sending identifiers	New		2022-10-04 12:29						
<input type="checkbox"/>	14238	AV03BD home	Sending identifiers	Completed	Success: 7, Errors: 0	2022-10-04 12:29	2022-10-04 12:29					

Here is the whole list of all tasks that can be displayed in the tab:

- sending settings;
- sending Link settings;
- sending SIP settings;
- sending virtual numbers;
- sending identifiers;
- deleting identifiers;
- sending identifiers to the elevator controller;
- deleting identifiers from the elevator controller;
- sending schedules;
- deleting schedules.

There is a filter by device and status (new, queued, started, completer, error). So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s.

MATCH ANY		STATUS EQUALS ERROR		+ ADD FILTER		↓ SAVE AS						DELETE SELECTED	
<input type="checkbox"/>	ID	Device	Type	Status	Result	Created at	Updated at						
<input type="checkbox"/>	14231	CR02BD	Sending identifiers	Error	Http client error: 0, cURL error 28: Connection timed out after 3000 milliseconds (see https://curl.haxx.se/libcurl/c/libcurl-errors.html) /share/app/Services/Transport/Http/HttpClient.php 141	2022-10-04 10:42	2022-10-04 10:42						
<input type="checkbox"/>	14227		Sending identifiers	Error	Http client error: 0, cURL error 28: Connection timed out after 3001 milliseconds (see https://curl.haxx.se/libcurl/c/libcurl-errors.html) /share/app/Services/Transport/Http/HttpClient.php 141	2022-10-04 10:42	2022-10-04 10:42						
<input type="checkbox"/>	14218	AA14 home	Deleting identifiers	Error	Http client error: 0, cURL error 28: Connection timed out after 3000 milliseconds (see https://curl.haxx.se/libcurl/c/libcurl-errors.html)	2022-10-04 10:41	2022-10-04 10:41						
<input type="checkbox"/>	14214	AV03BD	Deleting identifiers	Error	Http client error: 500, Server error: "POST http://localhost:48088/devices/request/8554d877-d9dc-48d7-9977-923a822b8bb3/46ca9bb5-21ca-477d-8567-98fd7c483b88? accessToken=1G10iarInogD88WJgrq3&connectionTimeout=3000&requestTimeout=600000" resulted in a "500 Internal Server Error" response: {"error": "device connection timeout reached"}	2022-10-04 10:41	2022-10-04 10:41						
<input type="checkbox"/>	14212	Panel camdroid AV01BD	Deleting identifiers	Error	Http client error: 0, cURL error 7: Failed to connect to 91.225.165.47 port 5313: No route to host (see https://curl.haxx.se/libcurl/c/libcurl-errors.html)	2022-10-04 10:41	2022-10-04 10:41						

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can **save** your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ANY		STATUS EQUALS ERROR		+ ADD FILTER		SAVE AS		SEGMENTS		DELETE SELECTED	
<input type="checkbox"/>	ID	Device	Type	Status	Result	Created at	Updated at				
<input type="checkbox"/>	14231	CR02BD	Sending identifiers	Error	Http client error: 0, cURL error 28: Connection timed out after 3000 milliseconds (see https://curl.haxx.se/libcurl/c/libcurl-errors.html) /share/app/Services/Transport/Http/HttpClient.php 141	2022-10-04 10:42	2022-10-04 10:42				
<input type="checkbox"/>	14227		Sending identifiers	Error	Http client error: 0, cURL error 28: Connection timed out after 3001 milliseconds (see https://curl.haxx.se/libcurl/c/libcurl-errors.html) /share/app/Services/Transport/Http/HttpClient.php 141	2022-10-04 10:42	2022-10-04 10:42				
<input type="checkbox"/>	14218	AA14 home	Deleting identifiers	Error	Http client error: 0, cURL error 28: Connection timed out after 3000 milliseconds (see https://curl.haxx.se/libcurl/c/libcurl-errors.html)	2022-10-04 10:41	2022-10-04 10:41				
<input type="checkbox"/>	14214	AV03BD	Deleting identifiers	Error	Http client error: 500, Server error: 'POST http://localhost:48088/devices/request/8554d877-d9dc-48d7-9977-923a822b8bb3/46ca9bb5-21ca-477d-8567-98fd7c483b88? accessToken=1G10iaRlnogD88WJgrq3&connectionTimeout=3000&requestTimeout=600000' resulted in a '500 Internal Server Error' response: {'error': 'device connection timeout reached'}	2022-10-04 10:41	2022-10-04 10:41				
<input type="checkbox"/>	14212	Panel camdroid AV01BD	Deleting identifiers	Error	Http client error: 0, cURL error 7: Failed to connect to 91.225.165.47 port 5313: No route to host (see https://curl.haxx.se/libcurl/c/libcurl-errors.html)	2022-10-04 10:41	2022-10-04 10:41				

9.4 Status

In the [Management system](#)⁷³ settings of each BAS-IP device, it is possible to select MQTT or HTTP protocol for connection with the Link server. If MQTT protocol is used, a device by default sends a heartbeat (current status: online/offline) to the server, for HTTP this option can be enabled/disabled.

Here you can monitor the statuses of devices that are online with enabled MQTT protocol or sending heartbeat feature for HTTP protocol.

MATCH ALL		+ ADD FILTER									
<input type="checkbox"/>	ID	Type	Model	IP address	Serial number	Communication protocol	Updated at				
<input type="checkbox"/>	48	panel	aa-12fb	181.199.86.7	eb42592-e63b-49fd-9d87-9ce9ae74944	http	2022-10-05 12:44				
<input type="checkbox"/>	76	lift-controller	evrc-ip	176.37.199.24	e9198a7-bd6b-48f2-9fb3-dc7451c8705	http	2022-10-05 12:44				
<input type="checkbox"/>	110	panel	av03bd	176.37.199.2	2d63240-259b-4e81-94e1-ec344347a3	http	2022-10-05 12:44				
<input type="checkbox"/>	109	panel	aa-14fb	46.149.80.23	c7565f4-a9c7-4274-81c9-5567a4371	http	2022-10-04 19:58				

Total records: 4

There is a filter by serial number, device IP address, model, type, and communication protocol. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

⁷³ <https://wiki.bas-ip.com/aa07/network-135955054.html>

MATCH ALL		TYPE EQUALS PANEL		COMMUNICATION PROTOCOL EQUALS HTTP		+ ADD FILTER		↓ SAVE AS	
<input type="checkbox"/>	ID	Type	Model	IP address	Serial number	Communication protocol	Updated at		
<input type="checkbox"/>	48	panel	aa-12fb	181.199.86.7	b42592-e63b-49fd-9d87-9ce9ae749449	http	2022-10-05 13:11		
<input type="checkbox"/>	110	panel	av03bd	176.37.199.2	d63240-259b-4e81-94e1-ec344347a3d1	http	2022-10-05 13:11		
<input type="checkbox"/>	109	panel	aa-14fb	46.149.80.23	7565f4-a9c7-4274-81c9-5567a4371325	http	2022-10-04 19:58		

Total records: 3

In addition, you can **save** your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL		TYPE EQUALS PANEL		COMMUNICATION PROTOCOL EQUALS HTTP		+ ADD FILTER		↓ SAVE AS		SEGMENTS	
<input type="checkbox"/>	ID	Type	Model	IP address	Serial number	Communication protocol	Updated at				
<input type="checkbox"/>	48	panel	aa-12fb	181.199.86.7	b42592-e63b-49fd-9d87-9ce9ae749449	http	2022-10-05 13:11				
<input type="checkbox"/>	110	panel	av03bd	176.37.199.2	d63240-259b-4e81-94e1-ec344347a3d1	http	2022-10-05 13:11				
<input type="checkbox"/>	109	panel	aa-14fb	46.149.80.23	7565f4-a9c7-4274-81c9-5567a4371325	http	2022-10-04 19:58				

Total records: 3

9.5 Device initialization

Only for SP-03 you can prepare some configurations on the Link server and apply them to the device. To send settings from the Link server to the device, you need:

1. Open the **Device**⁷⁴ tab to add the SP-03 device to the Link tab.
2. Add the device and enter all required settings (network, SIP, management system, address) you want to send to the device.

General ▼

Network ▲

Settings for connecting the device to the server. The IP address and port only need to be specified if the http protocol is used.

Communication protocol: HTTP | IP address: | Port: 8048

Login: admin | Password:

Server interaction password:

SETUP DEVICE

Synchronization ▼

Additional settings ▼

Device settings ▲

Model-specific settings. The settings will be automatically sent to the device.

Send on device

SIP settings

SIP enabled

Realm address: sip.bas-ip.com | Proxy address: sip.sip.bas-ip.com

STUN address: stun.l.google.com | STUN port: 19302

























Login: 1013 | Password: T8L6FK


Network

3. Save entered data.

⁷⁴ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

4. Find the added device in the list and click the **Initialize device** button.

MATCH ALL		+ ADD FILTER						SEARCH DEVICES	DELETE SELECTED
<input type="checkbox"/>	ID	Name	Description	Group	Model	Communication protocol	Status		
<input type="checkbox"/>	68	CR02BD		Home group	CR02BD(Access controller)	HTTP	offline(2022-08-12 16:24)	     	
<input type="checkbox"/>	69	AQ07LL		Unit 1	AQ07LL(Monitor)	HTTP	offline(2022-06-02 12:48)	     	
<input type="checkbox"/>	71	SP03	SP03 Home	Home group	SP03(Monitor)	HTTP	offline(2022-06-15 13:06)	     	
<input type="checkbox"/>	72	AV02	AV02	Unit 1	AV02(Panel)	HTTP	offline(2022-05-05 15:09)	     	

5. On the device, press  button for 5 sec to start sending settings. The changing backlight flashing indicates that the device has switched to the automatically receiving settings mode.
6. The process takes some time. In case of successful initialization, the device will play the corresponding sound and the backlight will flash in different colors 3 times. After this, the device will be ready to work.

10 Elevator management

This section is for EVRC-IP elevator controllers management and configuration. EVRC-IP allows users to call the elevator to the required floor from the monitor or Link app, to call the elevator to the ground floor for visitors, and to call it when bringing identifiers to the panel reader. Also, there is an opportunity to configure access to selected floors for each identifier.

An elevator controller must be [connected](#)⁷⁵ to the devices system and configured for operation with the Link server.

10.1 Configuration from the EVRC-IP side

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. Activate the **Use of the BAS-IP Link server**.
4. Enter an **IP address** or **domain name** of the server where the Link software is installed.
5. Provide device **password** to Link server.
6. If necessary, you can activate **sending of real-time logs** and **heartbeat** (current status: online/offline) from the elevator controller to the server.
7. Submit settings.

Management system SUBMIT

Use BAS-IP Link server

URL: link.bas-ip.com Password: *****

Send realtime logs to server Heartbeat to server

The following links contain information about the main steps of Link server configuration for operation with the EVRC-IP elevator controllers:

- [Elevators](#)(see page 103)
- [Elevator logs](#)(see page 106)
- [Elevators access restrictions](#)(see page 110)

⁷⁵ <https://wiki.bas-ip.com/evrcip/connection-scheme-135957519.html>

10.2 Elevators

In this section, you can manage EVRC-IP elevator controller settings for correct operation. For correct elevator controller work, [check](#)⁷⁶ what settings must be done from the EVRC-IP side.

- [How to configure an elevator controller](#)(see page 103)
- [Elevators filtering](#)(see page 106)

MATCH ALL		+ ADD FILTER				DELETE SELECTED	
<input type="checkbox"/>	ID	Name	Group	Number of controllers			
<input type="checkbox"/>	5	ANT	Unit #1	1			
<input type="checkbox"/>	8	lift	Unit 1	1			

Total records: 2

Rows per page 25 Records 1 - 2 of 2

✓ Tip

Full manual about an EVRC-IP elevator controller configuration and installation you can find [here](#)⁷⁷.

10.2.1 How to configure an elevator controller

Before controller configuration, it must be added in the [Device](#)⁷⁸ tab.

1. Open the **Elevators** tab of the Elevator management section.
2. Click **plus** icon in the left low corner.
3. Enter the elevator name.
4. Select a group where it is placed.
5. Tick **send elevator controller settings** on the device so that the settings data is transmitted to the controller.
6. Select available **mode**⁷⁹: Up (an elevator moves only in the upward direction), Down (movement is only in the downward direction), Up and down (both directions are available), Access by identifier (movement only to those floors that are available for the used identifier).
7. Select relay **type**: COM-NO/COM-NC.

⁷⁶ <https://wiki.bas-ip.com/basiplinken/elevator-management-135955958.html>

⁷⁷ <https://wiki.bas-ip.com/evrcip/evrcip-135957507.html>

⁷⁸ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

⁷⁹ <https://wiki.bas-ip.com/evrcip/device-135957549.html>

8. Set the **time** during which the relay will be switched.
9. Set lift **release time** (during which relay will be closed/opened) for identifier and for API call.
10. If necessary, enable the **switching relay when turning on the device**.
11. You can see the number of available and used relays. For Up and down mode only 8 relays are available, for other modes 16 can be used.
12. Create a list of floors and corresponding relays for a unit.

Edit controller relay

Mode

Mode Up and down ▼	Controller relays COM-NO ▼
Relay switch time (msec.) 100	
Lift release time for identifier (sec.) 2	Lift release time for API call (sec.) 3

Switch when turning on the device

Controller relays: (used 6 from 8)

+
-

Floor name	Floor number	Relay numbers	
Floor 1	1	[1]	✎ 🗑
Этаж #2	2	[2]	✎ 🗑
Этаж #3	3	[3]	✎ 🗑

CANCEL
CONFIRM

13. To add a floor click **plus** icon.
14. Enter **Floor No.** and **Relay No.** that connected to this floor at the controller.
15. Indicate whether the floor is public or not. Users will always have access to the public floor despite their identifier settings.
16. Select necessary apartments located on the floor (data is automatically taken from the Groups tab).

- Click Confirm to add the floor to the list.

Add controller relay

Floor name
Floor 1

Floor Floor 1(Floor number: 1) Relay numbers 1

Public floor

Apartments list

Add apartments on the floor
Apartment #1(1), Apartment #2(2), Apartment 3(3)

00-01 00-02 00-03

logical apartment address

CANCEL

CONFIRM

- Click **Confirm** to add the controller when you enter all necessary data.
- Click the **Save** button in the left low corner.

General ^

Name
lift

Group
Unit 1

Elevator access rules ^

No data

Controller settings ^

To operate the elevator, elevator controllers are used. Each controller corresponds to its range of floors, this is configured in the "Contacts of the controller" section

+

Elevator's controller	Controller mode	Controller direction	+
lift controller 2	COM-NO	Up and down	

←
+

- Open the **Device settings** tab of the Device management tab and find the controller.
- Check the correctness of settings (if they are the same as entered in the Elevators tab).
- Enable send on device feature to transmit entered settings to the controller.
- Save changes.

10.2.2 Elevators filtering

There is a filter by name and group. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate) or contain (has) it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.

ID	Name	Group	Number of controllers
8	lift	Unit 1	1

In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

ID	Name	Group	Number of controllers
8	lift	Unit 1	1

10.3 Elevator logs

This tab contains a log that displays all the events that happened with elevator controllers: login to the web interface, lock opening using an identifier, elevator called, etc. You can export all logs by clicking the corresponding button.

MATCH ALL		+ ADD FILTER					
<input type="checkbox"/> ONLINE MODE	<input type="checkbox"/> REFRESH DATA					EXPORT TO	
Created at	Category	Priority	Event	Markers	Info	Source	:
2022-09-29 17:47:24	System	Low	Login to the web interface		Successful (admin) login to the web interface	lift controller 2	
2022-09-26 16:36:05	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2	

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 was opened by free access button
	Access	Lock opened by exit button
	Access	Lock opened by identifier
	Access	General access code entered
	Access	Access granted by valid face identifier
	Access	Lift called to floor
	System	Login to the web interface
	System	Unsuccessful attempt to enter GUI settings

Priority	Category	Event
	System	Successfully logging into GUI settings
	Information	Incoming call
	Information	Outgoing call
	Information	Incoming call without status
	Information	Outgoing call without status
	Information	Outgoing call from web-interface
	Information	Missed call
High	Access	Access denied by remote server
	Access	Access granted by remote server
	Access	Wrong input code
	Access	Unknown identifier
	Access	Access denied by invalid 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
	Access	Access granted by valid license plate
	Access	Access denied by not valid license plate

Priority	Category	Event
	Access	Access denied by unknown license plate
	Emergency	Tamper event
Critical	Access	Lock opened too long
	Access	Door is open too long
	Emergency	Abnormal event
	Emergency	Emergently event
	System	Firmware update

Also, there is a filter by **date** (created at), **category**, **priority**, **code**, **device**, **identifier**, its **owner**, or created **marker**. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all events before the date.

MATCH ANY
CREATED AT EQUALS 2022-09-22 00:00
CODE EQUALS INTERFACE.LIFT_CALLED_TO_FLOOR
+ ADD FILTER
SAVE AS

ONLINE MODE
REFRESH DATA
EXPORT TO



Created at	Category	Priority	Event	Markers	Info	Source
2022-09-26 16:36:05	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2
2022-09-26 16:36:04	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

Created at	Category	Priority	Event	Markers	Info	Source
2022-09-29 17:47:24	System	Low	Login to the web interface		Successful (admin) login to the web interface	Unit 1 Entrance
2022-09-26 16:36:05	Access	Medium	Elevator called to the floor		Floor number - 1, name - #1, source - interface.api	lift controller 2

10.4 Elevators access restrictions

With the access restrictions help, you can configure giving access to these or those elevators for concrete users.

With the help of  and  buttons, you can edit or delete restrictions.

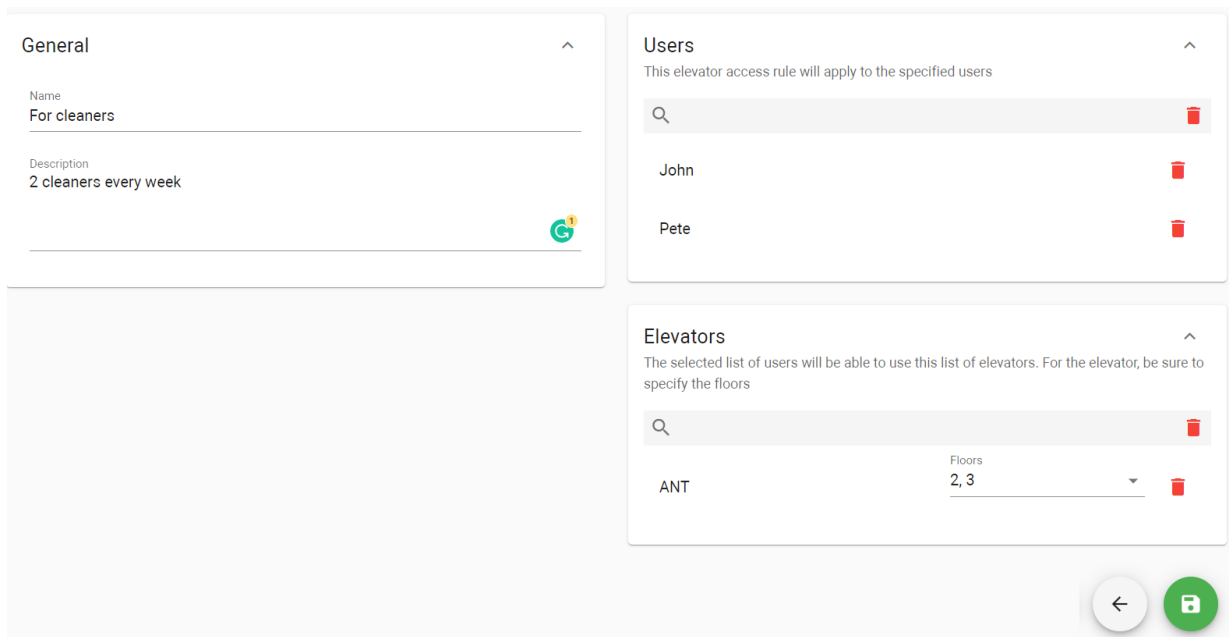
ID	Name	Description
21	Security	
22	For cleaners	2 cleaners every week
23	Lift Oleg	for oleg
24	Lift Julia + Admin	
25	lift for Consierge	

10.4.1 How to create access restriction for an elevator

1. Go to the **Access restriction** tab of the Elevator management section.
2. Click **plus** icon in the left low corner.
3. Enter the restriction **name**.
4. Add **description**, if required.
5. Select **user/s**⁸⁰ from the list to whom this restriction will be applied.
6. Select the **elevator**⁸¹ that the selected users can use.
7. Specify **floor/s** to which user/s will have access.
8. Click the **Save** button in the low left corner after entering all required data.

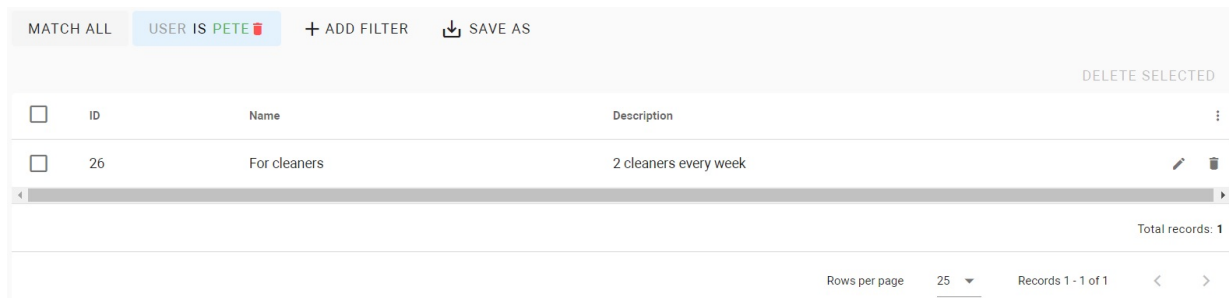
80 <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

81 <https://wiki.bas-ip.com/basiplinken/elevators-135955962.html>





10.4.2 Access restrictions filtering



Also, there is a filter by name, user, and elevator. So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameters. For some searches, results can **equal** your search (so to be exactly as you indicate), or **contain** (has) it. You can select a few parameters and choose whether the results will **match all** filters or **any** of them.



In addition, you can save your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

MATCH ALL USER IS PETE  + ADD FILTER  SAVE AS SEGMENTS

DELETE SELECTED

<input type="checkbox"/>	ID	Name	Description	
<input type="checkbox"/>	26	For cleaners	2 cleaners every week	 

Total records: 1

Rows per page 25 Records 1 - 1 of 1 < >

11 Settings

- [System audit](#)(see page 113)
- [Backups](#)(see page 115)
- [General](#)(see page 116)
- [Licenses](#)(see page 131)
- [System info](#)(see page 132)

11.1 System audit

This section displays a list of all events that happened in the system: adding/editing/deleting users, groups, areas, access restrictions, schedules, and identifiers. So, you can monitor all changes on the server, when they were, and who did them.

MATCH ALL		+ ADD FILTER					
From	User	To	User	Duration(sec)	Status	Date	:
1664	Consierge	1644	John	53	Answered	2022-09-13 17:28	
1664	Consierge	1644	Administrator	72	Canceled	2022-09-13 17:21	
1549	Juli	1644	Pete	69	Answered	2022-09-13 17:19	
1549	Administrator	1644	Anna	0	Failure	2022-09-13 17:01	
1549	Max	1644	Consierge	0	Canceled	2022-09-13 17:01	
1549	Anna	1663	Administrator	91	Canceled	2022-09-13 16:59	
1549	Pete	1756	Max	16	Not answered	2022-09-13 16:59	
1023	Administrator	1663	Juli	10	Answered	2022-09-13 16:57	
1023	John	1644	Consierge	0	Canceled	2022-09-13 16:56	
1023	Herman	1663	John	4	Answered	2022-09-13 16:55	

By clicking an event about adding or deleting data, this information will display to check what exactly was added/ deleted. By clicking an event about ending data, you can look at the original variant or edited.

Date	Event type	Action	User
2022-10-04 10:40	Schedule	Edited	Administrator
2022-10-04 10:40	Schedule	Edited	Administrator
2022-10-04 10:40	Schedule	Edited	Administrator
2022-10-04 01:40	Identifier	Added	Administrator
2022-10-04 01:35	Identifier	Added	Administrator
2022-10-03 14:35	Schedule	Edited	Administrator
2022-10-03 14:34	Schedule	Edited	Administrator
2022-10-03 14:31	Schedule	Edited	Administrator
2022-10-03 14:29	Schedule	Edited	Administrator
2022-10-01 02:40	Profile	Edited	Administrator
2022-10-01 02:39	Profile	Edited	Administrator

Original row
 Edited row

There is a filter by **date**, **user**, **audit type** (access restriction, authorization, announce, backup, device, group, identifier, mail server, marker, profile, schedule, user), and **audit event** (added, edited, deleted, setting changes, backup added, backup deleted). So, you can configure a flexible data display and quick search. To do this, you need to click the **Add filter** button and set the necessary parameter/s. For some searches, results can **equal** your search (so to be exactly as you indicate), or they can be **less** or **great** than your parameter, e.g. search less than indicated date will display all events happened before.

Created at	Audit type	Audit event	User
2022-07-05 19:27	Backup	Backup exported	Administrator
2022-07-05 19:26	Backup	Backup added	Administrator
2022-07-04 12:42	Backup	Backup added	Administrator
2022-06-13 12:28	Backup	Backup exported	Administrator
2022-06-13 12:28	Backup	Backup added	Administrator
2022-06-09 13:15	Backup	Backup exported	Administrator
2022-06-09 13:14	Backup	Backup added	Administrator
2022-06-09 13:00	Backup	Backup exported	Administrator
2022-06-09 13:00	Backup	Backup added	Administrator
2022-06-09 10:05	Backup	Backup added	Administrator

You can select a few parameters and choose whether the results will **match all** filters or **any** of them. In addition, you can **save** your search parameters for further use by clicking the corresponding button. All saved parameters are displayed after clicking the **Segments** button.

Created at	Audit type	Audit event	User
2022-07-05 19:27	Backup	Backup exported	Administrator
2022-07-05 19:26	Backup	Backup added	Administrator
2022-07-04 12:42	Backup	Backup added	Administrator
2022-06-13 12:28	Backup	Backup exported	Administrator
2022-06-13 12:28	Backup	Backup added	Administrator
2022-06-09 13:15	Backup	Backup exported	Administrator
2022-06-09 13:14	Backup	Backup added	Administrator
2022-06-09 13:00	Backup	Backup exported	Administrator
2022-06-09 13:00	Backup	Backup added	Administrator
2022-06-09 10:05	Backup	Backup added	Administrator

11.2 Backups

In this tab, you can save basic data (user, identifiers, groups, devices, access restrictions) from the server or restore settings from previous backups.

RESTORE FROM FILE			DELETE SELECTED	
<input type="checkbox"/>	Name	Backup data	Created at	:
<input type="checkbox"/>	1	Access configuration, Devices, Groups, Users/identifiers	2022-04-15 12:19	↓ ✓ 🗑
<input type="checkbox"/>	3	Groups, Devices, Access configuration	2022-05-09 10:26	↓ ✓ 🗑
<input type="checkbox"/>	20220513	Users/identifiers, Groups, Devices, Access configuration	2022-05-13 10:02	↓ ✓ 🗑
<input type="checkbox"/>	2022-05-20 2343	Users/identifiers, Groups, Devices, Access configuration	2022-05-20 23:44	↓ ✓ 🗑
<input type="checkbox"/>	20220602-203534	Users/identifiers, Groups, Devices, Access configuration	2022-06-02 20:35	↓ ✓ 🗑
<input type="checkbox"/>	20220603-162713	Users/identifiers, Groups, Devices, Access configuration	2022-06-03 16:27	↓ ✓ 🗑
<input type="checkbox"/>	test	Users/identifiers, Groups, Devices, Access configuration	2022-06-03 16:47	↓ ✓ 🗑
<input type="checkbox"/>	20220609-100458	Users/identifiers, Groups, Devices, Access configuration	2022-06-09 10:05	↓ ✓ 🗑
<input type="checkbox"/>	test	Users/identifiers, Groups, Devices, Access configuration	2022-06-09 13:00	↓ ✓ 🗑
<input type="checkbox"/>	20220609-131434	Users/identifiers, Groups, Devices, Access configuration	2022-06-09 13:14	↓ ✓ 🗑

To back up data, you must click **plus** icon in the left low corner, enter a **name** or confirm the suggested one. As a result, the copy will be displayed in the list where you can download ↓ it to your computer, restore ✓ or delete 🗑 this backup.

To restore data from the downloaded copy, click Restore from the file button and select the required file from the computer.

RESTORE FROM FILE				DELETE SELECTED
<input type="checkbox"/>	Name	Backup data	Created at	:
<input type="checkbox"/>	1	Access configuration, Devices, Groups, Users/identifiers	2022-04-15 12:19	↓ ✓ 🗑
<input type="checkbox"/>	3	Groups, Devices, Access configuration	2022-05-09 10:26	↓ ✓ 🗑
<input type="checkbox"/>	20220513	Users/identifiers, Groups, Devices, Access configuration	2022-05-13 10:02	↓ ✓ 🗑
<input type="checkbox"/>	2022-05-20 2343	Users/identifiers, Groups, Devices, Access configuration	2022-05-20 23:44	↓ ✓ 🗑
<input type="checkbox"/>	20220602-203534	Users/identifiers, Groups, Devices, Access configuration	2022-06-02 20:35	↓ ✓ 🗑
<input type="checkbox"/>	20220603-162713	Users/identifiers, Groups, Devices, Access configuration	2022-06-03 16:27	↓ ✓ 🗑
<input type="checkbox"/>	test	Users/identifiers, Groups, Devices, Access configuration	2022-06-03 16:47	↓ ✓ 🗑
<input type="checkbox"/>	20220609-100458	Users/identifiers, Groups, Devices, Access configuration	2022-06-09 10:05	↓ ✓ 🗑
<input type="checkbox"/>	test	Users/identifiers, Groups, Devices, Access configuration	2022-06-09 13:00	↓ ✓ 🗑
<input type="checkbox"/>	20220609-131434	Users/identifiers, Groups, Devices, Access configuration	2022-06-09 13:14	↓ ✓ 🗑

11.3 General

In this tab, you can configure general server settings. After changing any settings, click **Confirm** at the end of the page.

- [General](#)(see page 116)
- [Mail Server settings](#)(see page 117)
- [Notifications](#)(see page 118)
- [Devices](#)(see page 118)

11.3.1 General

In this section you can:

- enter your project **name**;
- add project **description** (if necessary);
- enter **server URL**, e.g., <https://linkbas-ip.com>⁸²;
- enable **Registration is allowed by reference** field to be able to invite new users;
- **allow** users to self-**recover** their **password** by ticking the corresponding box. Otherwise, only an administrator will be able to do it;
- select **system language**: English, Russian.

⁸² <https://dev.bas-ip.com>

General

Project name
BAS-IP link

Description
project link

Server url
<https://linkbas-ip.com>

Registration is allowed by reference.

Password recovery allowed

System language
English

11.3.2 Mail Server settings

These settings are required Enter mail server settings to be able to send registration link and emails to users. You must enter:

- for the **mail server type** field select smtp (outgoing mail server);
- **mail server** address, e.g. smtp.gmail.com⁸³;
- mail server **port** number;
- SMTP server **username** (email address from which letters will be sent);
- email (from which letters will be sent) **password**;
- **sender email** (coincides with SMTP server username);
- **sender name** that will be indicated in letters;
- preferred **encryption** type: ssl or tls;

After entering the **mail server settings** check the correctness by **sending a test email**.

⁸³ <http://smtp.gmail.com>

Mail Server settings

Mail server type
smtp

Mail server smtp.gmail.com Port 587

User name linkbasip@gmail.com Password

Sender's email linkbasip@gmail.com Sender's name linkbasip@gmail.com

Encryption tls

Send test e-mail >

11.3.3 Notifications

To get information about system functioning you must enter the **system administrator email**. And enable/disable what notifications you (as an administrator) want or don't want to receive:

- when devices become offline;
- when device tasks are filed.

Notifications

System administrator email

Notify about offline devices

Notify about failed device task

11.3.4 Devices

Here you can configure how long the device logs must be kept: a day, a week, 2 weeks, or a month.

Devices

Keep device logs for period
1 week(s)


CONFIRM

11.3.5 SIP settings



You can configure SIP settings in the section for correct SIP server functioning. After changing any settings, click **Confirm** at the end of the page.

- [SIP status](#)(see page 119)
- [SIP settings](#)(see page 119)
- [Network interfaces](#)(see page 120)
- [Internal subnets](#)(see page 120)
- [SIP nodes](#)(see page 121)
- [Additional SIP functionality](#)(see page 121)
- [Used ports](#)(see page 122)

11.3.5.1 SIP status

Here you can monitor SIP proxy and SIP node statuses. Click  to refresh the service.

SIP status

Type	IP address	Status	Actions
SIP proxy	95.216.166.9	online	
SIP node	95.216.166.9	online	

11.3.5.2 SIP settings

In this section, you can configure the SIP server. You must enter the following:

- only **server external IP address** if a public server is used;
- both **server external** and **internal IP addresses** if the server is behind NAT. In this case, server external address is router IP address, and the internal value is the server (computer) IP address where the Link is installed;
- UDP/TCP port for unencrypted SIP traffic. The default is 5060. For SIP over TLS, port 5061 is used;
- the maximum **bitrate** of the transmitted video stream. The default is 512kb/s.
- A pool from what **RTP ports** to what ports are used for audio/video transmission. The default values are from 10000 to 20000.

All ports require forwarding if the server is behind NAT.

SIP settings

Server external IP address 95.216.16.16	Server internal IP address
Port 5060	Video bitrate 512kb ▼
RTP ports from 10001	RTP ports to 20001

11.3.5.3 Network interfaces

The value of the server external IP address is not required if the Link system is not complex and the server is not behind NAT. If the fields are left blank, the value of the server IP address will be used for them.

You must enter an external IP address, if:

- the server is behind NAT and one NIC is used. In this case, the IP address of the network card must be entered in both fields;
- the server is behind NAT and 2 network cards are used:
 - for the internal network in which the door phones are located;
 - for the external network through which the server connects to the Internet.

Network interfaces

External ip address IP address	Internal ip address IP address
-----------------------------------	-----------------------------------

11.3.5.4 Internal subnets

You must enter the address of the subnets in which intercoms and SIP applications of users are connected. The record format is **subnet address/mask bit value**, for example, 192.168.1.0/24.

Internal subnetworks	
Internal subnetwork IP address	ADD
No data	

11.3.5.5 SIP nodes

These settings are required to fill if the container(s) of the SIP nodes are deployed on another server.

If a separate server with a node is behind NAT, then you must:

- enter the internal/external address of the node;
- forward a pool of RTP ports for a node.

If a separate server with a node is not behind NAT, then you must specify the external IP address of the node in both fields.

SIP nodes	
External ip address IP address	Internal ip address IP address
ADD	
No data	

11.3.5.6 Additional SIP functionality

Here you can enable the feature of automatic creation of forward rules for apartment group user/s, sending them to device/s (if some devices are added/deleted the corresponding data will be added/deleted to/from devices), and data correction for device/s (if there are some changes in virtual numbers or logical address).

This feature simplifies forward rules configuration (when it's required to redirect calls from a panel to all user numbers) and management (you don't need to have access to a device to change a rule - it can be done in the Link when [editing the group](#)⁸⁴ with the device or in the [Virtual numbers](#)⁸⁵ tab or by the user in the Link app).

Also, you can delete all created forwarding queues from the server and devices.

⁸⁴ <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>

⁸⁵ <https://wiki.bas-ip.com/basiplinken/virtual-numbers-135955892.html>

Additional SIP functionality

- Send group forward rules on devices

DELETE GROUP FORWARDING RULES FROM SERVER AND DEVICES

! Warning

If forwarding rules are already created, be careful when enabling the feature, because automatically created rules may break previously created ones.

11.3.5.7 Used ports

The application uses the following ports:

- 5060 TCP/UDP: unencrypted SIP traffic port;
- 5061 TCP: port for SIP using TLS;
- 80 TCP: HTTP port;
- 443 TCP: HTTPS port;
- 6001 TCP: WebSocket port;
- 10000-20000 UDP: RTP ports for audio/video;
- 1883 TCP: unencrypted MQTT;
- 8883 TCP: encrypted MQTT.

If SIP proxies and nodes are running on more than one server with the Link server application, then the following ports must be forwarded to them:

- 48080: SIP proxy management port;
- 48081: SIP node management port.

11.3.6 SIP trunks

SIP trunks enabling makes it possible to make and forward calls to mobile numbers. For now, the Link works only with the Twilio platform. You can add multiple trunks on a server and assign them to groups.

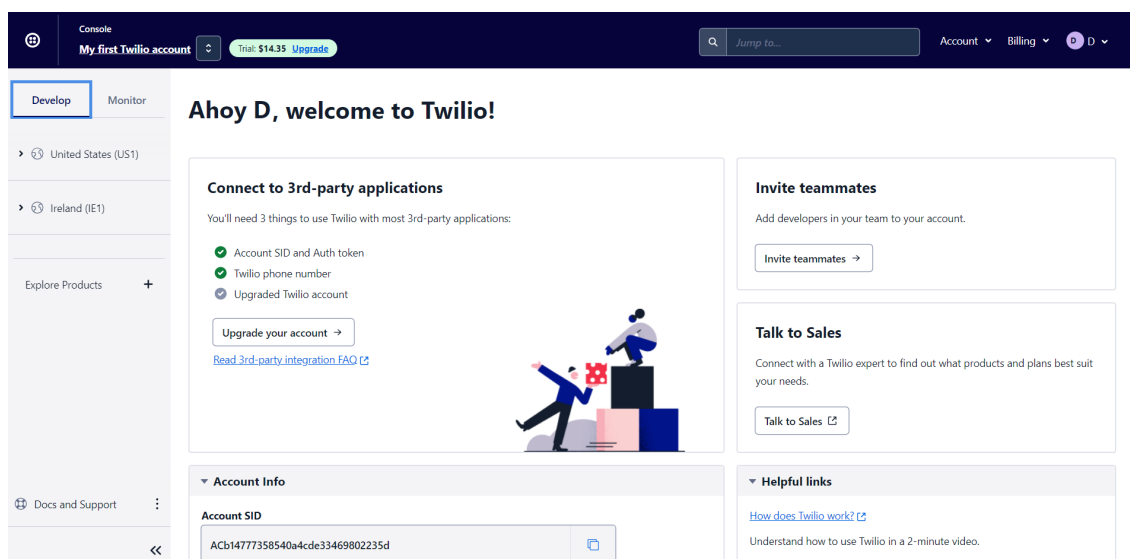
11.3.6.1 How to configure SIP trunks functioning

1. Register with Twilio.
2. Enter a reliable mobile number and verify it via SMS. It is used as CallerID.
3. Upgrade you account. It must not be Trial, as you will have to verify each called number manually. Also, you account must have positive balance.
4. Buy a number to make calls.

! Warning

For this feature, you must have the Link version with SIP and the purchased [license](#)⁸⁶ with enabled SIP trunks.

Usually, you are recommended to buy a number as a part of your registration process.



You can check whether you have purchased number or not in the Phone Numbers > **Active Numbers** section.

86 <https://wiki.bas-ip.com/basiplinken/licenses-135956024.html>

Active Numbers

Buy a number

A2P 10DLC registration required for US messaging. A registration process will be required for each US local number sending SMS/MMS messages to the US. [Initiate A2P 10DLC registration](#) or [check registration status](#)

Inventory Filters Configuration Filters

Number	Friendly Name	Capabilities				Active Configuration
		Voice	SMS	MMS	Fax	
+1 276 295 9324 ▲ Pennington Gap, VA, US	(276) 295-9324	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Voice Messaging Webhook to POST: https://demo.twilio.com/welcome/voice/ Webhook to POST: https://demo.twilio.com/welcome/sms/reply/

* Can send/receive calls to domestic numbers only
 † Can send/receive sms to domestic numbers only
 ‡ This number does NOT support SIP Trunking
 ▲ Can make emergency calls
 (national) A non-geographic number
 (beta) This number is new to the Twilio Platform

If there are no numbers, go to the **Buy a number** section. Select the country where the number is registered, its capabilities, and click Buy in the number line you are going to get.

5. Open Elastic SIP Trunks > Manage > **Trunks** and create SIP Trunk. The following settings are required for the trunk:

- disabled call recording;
- enabled SymmetricRTP;
- subdomain for SIP Trunks (in the Termination SIP URI section);
- IP access control list: media servers and SIP proxies IP addresses (in the Authentication section). Only these IP addresses will be able to communicate with the trunk;
- credentials with which entered media server will call (in the Credential lists section);
- CallPerSec values for regions;

6. In the **Numbers** section, add an existing (previously) created number for the trunk.

Numbers

Add a number

Choose one of your trunking-enabled numbers. After adding the number, inbound calls will be routed to the Trunk.

Filter Parameter	Number
Number	+1415GETTWLO

<input checked="" type="checkbox"/>	Number	Friendly Name	Country	Configuration
<input checked="" type="checkbox"/>	+12762959324	(276) 295-9324	United States	URL: https://demo.twili...

Cancel Add Selected

7. Select available for calls counties in the Voice > Settings > **Geo permissions** section.

8. Open General setting of the Link server and go to the **SIP trunks** tab.

9. Click plus icon (in the left low corner).

10. Enter all required data:

- trunk **name**;
- **termination SIP URI** (indicated in the step 5);
- **outgoing number** (number that the mobile user will see when he receives a call, CallerID);
- trunk **login** from twilio;
- trunk **password** from twilio.

11. Select **group(s)** for which this trunk will work. Users of these groups will use the trunks assigned to them when calling mobile numbers. It is possible to assign different trunks for root group(s) and subgroups.

Only one trunk can be assigned to one group. If you select a group with assigned another trunk, then it will be replaced with the current one. Different trunks can be used for root group and its subgroups.

In case when root group and subgroups have different trunks, the closest trunk to the user will be used for the call. For example, for Building #1 and Test residential complex different trunks are assigned. So, for a user from Building #1, trunks assigned to the Building #1 group will be used, as its the closest.

12. Save configurations.

General / Edit SIP trunk basip-qa

General

Name
basip

Termination URI
basip-test.pstn.twilio.com

Outgoing number
+15074193477

Login
supportbasip

Password

Groups
List of groups covered by sip trunk

- ▶ Home group
- ▼ Test residential complex
 - ▶ Bulidng #1
 - ▶ Building #2

11.3.7 Additional settings

Also in the General tab, you have access to some settings for the mobile app and system.

- [Whitelabel](#)(see page 126)
- [Markers](#)(see page 128)

- [System settings](#)(see page 129)
- [Data import](#)(see page 129)
- [MQTT settings](#)(see page 129)

11.3.7.1 Whitelabel

Here you set some settings for the mobile app.

In the Apple wallet section, you can configure how guests passes will look. You can set: the developer name, the text under the QR code, colors for all elements, and info to display on the back of the pass.



Apple Wallet

Name developer
BAS-IP

Text under the QR code

Developer name color #FFFFFF

Plate color #E97878

Font color #FFFFFF

Fields on the back of the pass

Field name	Field value	
Domain name	example.com	DELETE

CONFIRM

In the management company settings, you can add all the required for display information about the company.

Management company settings

Mobile app settings



Company name

Company address

Company email Company phone number

CONFIRM

11.3.7.2 Markers

In this section, you can create some markers and apply them to different users in the [corresponding tab](#)⁸⁷. All events connected to the mark user will also be marked. So, this can help to monitor required users actions.

To add a marker, click the **plus** icon in the left low corner, enter the marker name, and select color.

GENERAL SIP SETTINGS WHITELABEL **MARKERS** SYSTEM SETTINGS DATA IMPORT MQTT SETTINGS

DELETE SELECTED

<input type="checkbox"/>	Name	Color	
<input type="checkbox"/>	Basic users	■ #CA0606	

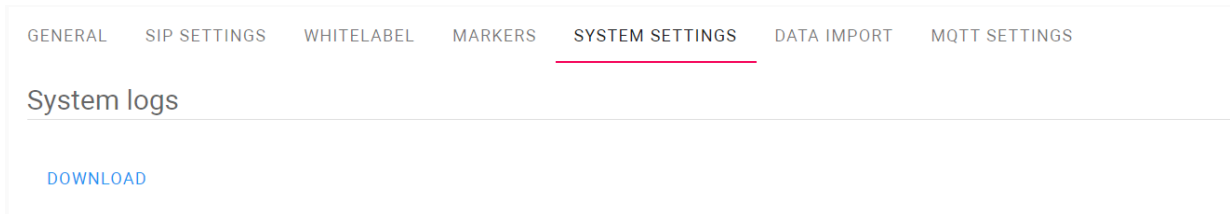
Total records: 1

Rows per page 25 Records 1 - 1 of 1 < >

⁸⁷ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

11.3.7.3 System settings

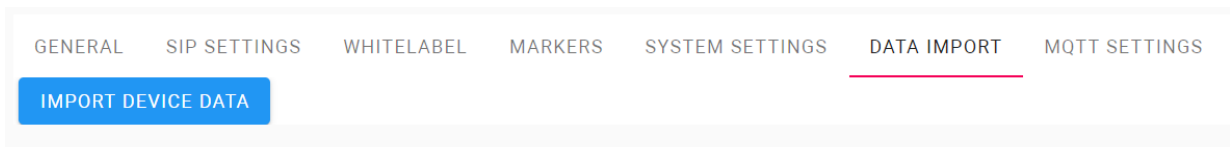
Here you can download system logs.



11.3.7.4 Data import

In the tab, you can import to the Link other device data such as identifiers from a panel. Data applies to the user that imports them and the devices available for the user.


This feature is necessary for not adding all the identifiers (available on the panel) to the Link manually. For example, on the object, there is a panel with added identifiers, but later you need to add these identifiers to the Link and a few more panels. So, you can import identifiers and they will automatically add to the Link and all available for you panels.



11.3.7.5 MQTT settings

Here you can check the MQTT broker status.

MQTT status


Type	Status	Actions
MQTT broker for devices	online	


Also, you can **configure client certificates use** and upload a self-signed certificate or private key file. If you use **the version with a web proxy** and upload the **Let'sencrypt certificate**, the data will be encrypted using it. But if **the**

version without a proxy is used and a certificate is not indicated at all, the data will be encrypted with a **self-signed certificate**.

MQTT Settings

Use client certificates

 Self-signed certificate ✕

 Private Key file ✕

CONFIRM

11.3.8 Mail Templates

In this tab, you can customize default mails for user registration invites, user password changes, and account password recovery. The system marks what obligatory data you must include, and all other info/language must be changed/added, e.g. the name of a residential area, its address, and so on.

11.3.8.1 How to create a mail template

1. Go to the General settings > **Mail Templates** tab.
2. Click **plus** icon in the low left corner.
3. Select the **Mail type** you want to edit.
4. Make necessary changes to the mail **subject** and **body**. HTML language is used for markup.

Obligatory for mentioning element turns red, if you skip it.

Add mail template

Mail type
Password recovery

Subject
Password recovery

Body

```
<p>Hi, :email,
<p>We noticed your problems with the password. Follow this <a href=':link'>link</a>
to reset your password.</p>
<p>Use the code to change your password in the Link app
```

:email
:link
:reset_token

Send test e-mail
test.b@gmail.com ➤

PREVIEW MAIL

CANCEL CONFIRM

5. Click **Preview** the mail if you need to check how it will look. Also, you can enter an **e-mail** to send a test version.
6. Confirm the template when all data are entered.



From the moment you create a template for any type of mail, it will be sent instead of a default email. To return default mail, delete the template for this type.



11.4 Licenses

In this section, you can check general information about purchased licenses for the project: validity period, available features (virtual number, mobile app, elevators, additional identifier types, SIP trunks, automatic creation of forward rules), and a number of available and used numbers.


Instance ID 8d26d1ce-0a04-11ec-9dbc-0242ac1e00

Virtual numbers Enabled	Total 5000	Used 449	Left 4551
SIP trunks Enabled	Web dialer Enabled		
Mobile app clients Enabled	Total 5000	Used 45	Left 4955
Edit group forward settings for mobil... Enabled			
Elevators Enabled			
Face recognition Enabled for guest identifiers			
License plates Enabled			

Also, you can check whether your license is active  . If it is expired  , you can upload a new license from the file or from the cloud.


 ADD FROM FILE
 ADD FROM CLOUD

Licenses

#5b2530bb-563b-4981-a26a-9a51226b7c13 

Name Enterprise pack #1	Valid from 2022-07-01	Valid until 2022-10-31	Issuer BAS-IP
Virtual numbers Enabled	Total 5000(Per user: 5)	Mobile app clients Enabled	Total 5000(Per user: 5)
Elevators Enabled	Face recognition Enabled for guest identifiers	License plates Enabled	

REMOVE

#ee79faed-5f60-48f4-954a-37c3806d7983 


Name Enterprise pack #1	Valid from 2022-06-01	Valid until 2022-07-01	Issuer BAS-IP
Virtual numbers Enabled	Total 5000(Per user: 8)	Mobile app clients Enabled	Total 5000(Per user: 5)
Elevators Enabled	Face recognition Enabled for guest identifiers	License plates Enabled	

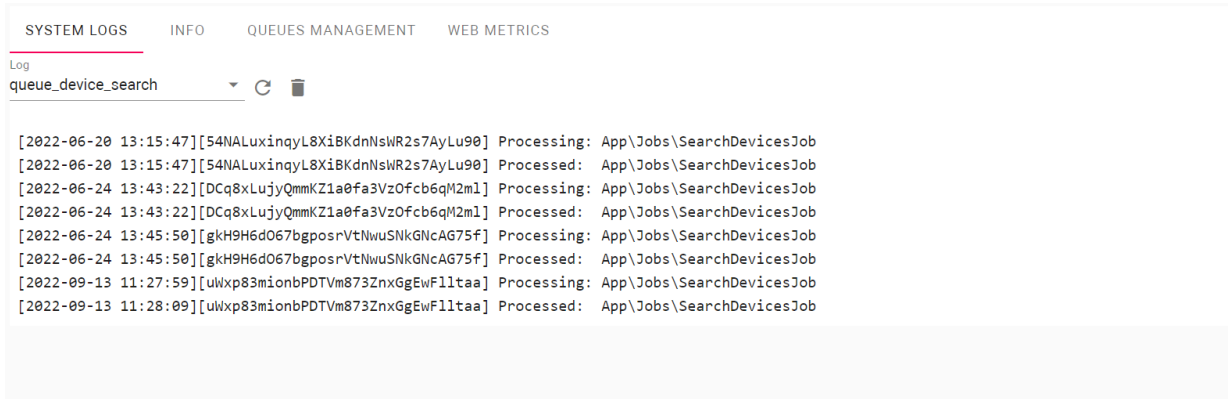
11.5 System info

This section contains information about events, processes, and system boot. Here you can monitor the system state and collect information.



- [System logs](#)(see page 133)
- [Info](#)(see page 133)
- [Queues management](#)(see page 134)
- [WEB metrics](#)(see page 134)

11.5.1 System logs

This tab contains logs of system managers responsible for executing processes in the Link. To display information, you need to select a log from the list and click  to display and update the information.



SYSTEM LOGS INFO QUEUES MANAGEMENT WEB METRICS

Log
queue_device_search  

```
[2022-06-20 13:15:47][54NALuxinqyL8XiBKdnNswR2s7AyLu90] Processing: App\Jobs\SearchDevicesJob
[2022-06-20 13:15:47][54NALuxinqyL8XiBKdnNswR2s7AyLu90] Processed: App\Jobs\SearchDevicesJob
[2022-06-24 13:43:22][DCq8xLujyQmmKZ1a0fa3Vz0fcb6qM2m1] Processing: App\Jobs\SearchDevicesJob
[2022-06-24 13:43:22][DCq8xLujyQmmKZ1a0fa3Vz0fcb6qM2m1] Processed: App\Jobs\SearchDevicesJob
[2022-06-24 13:45:50][gkH9H6d067bgposrVtNwuSNkGncAG75f] Processing: App\Jobs\SearchDevicesJob
[2022-06-24 13:45:50][gkH9H6d067bgposrVtNwuSNkGncAG75f] Processed: App\Jobs\SearchDevicesJob
[2022-09-13 11:27:59][uWxp83mionbPDTVm873ZnxGgEwF1ltaa] Processing: App\Jobs\SearchDevicesJob
[2022-09-13 11:28:09][uWxp83mionbPDTVm873ZnxGgEwF1ltaa] Processed: App\Jobs\SearchDevicesJob
```

List of logs:

- queue_alert - emergency alert queue manager logs;
- queue_access_matrix_processing - manager logs of queues for collecting information on the access matrix for generating key distribution packets for devices;
- queue_device_search - network search queue manager logs;
- queue_default - application base queue manager log;
- supervisor - service manager log in the system;
- queue_sip - SIP server queue manager logs;
- queue_announces - announcement queue manager logs;
- queue_device_task - task queue manager logs of sending IDs, schedules, and settings to devices;
- websocket - websocket logs for application;
- nginx_access - nginx server logs;
- nginx_error - nginx web server error logs;
- nginx_unit - application server logs;
- mysql_error - mysql database server logs;
- app - application logs.

To clear the data, delete  your search.

11.5.2 Info

This tab contains information about the system, application execution environment, running processes, used memory, CPU, and used disk space.

SYSTEM LOGS **INFO** QUEUES MANAGEMENT WEB METRICS

🔄 REFRESH DATA

```

top - 23:42:37 up 546 days, 12:02,  0 users,  load average: 0.28, 0.36, 0.36
Tasks: 36 total,  1 running, 35 sleeping,  0 stopped,  0 zombie
%Cpu(s):  7.6 us,  3.1 sy,  0.0 ni, 89.0 id,  0.1 wa,  0.0 hi,  0.2 s:
KiB Mem : 3940872 total,  378016 free, 1962732 used, 1600124 buff,
KiB Swap:  0 total,  0 free,  0 used. 1682004 avail.

Filesystem            1K-blocks      Used Available Use% Mounted on
overlay                39320220 24108676 13567512  64% /
tmpfs                  65536         0    65536     0% /dev
tmpfs                  1970436         0   1970436     0% /sys/fs/cgroup
/dev/sda1              39320220 24108676 13567512  64% /var/log
shm                    65536         0    65536     0% /dev/shm
tmpfs                  1970436         0   1970436     0% /proc/acpi
tmpfs                  1970436         0   1970436     0% /proc/scsi
tmpfs                  1970436         0   1970436     0% /sys/firmware


PID USER      PR  NI   VIRT   RES    SHR  S  %CPU  %MEM    TIME+  COMMAND
  1 root        20   0   18384   2380   2100  S   0.0   0.1   0:00.25  rsh
 65 root        20   0   64704  21792   7332  S   0.0   0.6  27:44.92  sshd
 68 root        20   0   709524  6700   2656  S   0.0   0.2   9:05.58  wpa_cli
 69 root        20   0   709772   7376   2756  S   0.0   0.2   9:33.50  lshd
 75 root        20   0   715784 10672   5508  S   0.0   0.3  44:25.66  lshd
 79 root        20   0   710260   8952   2708  S   0.0   0.2   9:19.46  lshd
 87 root        20   0   707888   3920   1960  S   0.0   0.1  17:22.07  lshd
 94 root        20   0   28360    2716   2444  S   0.0   0.1   0:31.81  csh
108 www-data    20   0   340448  41848  19916  S   0.0   1.1   9:35.28  plink
115 root        20   0   467824  26828  21368  S   0.0   0.7   2:10.39  plink
116 www-data    20   0   342500  44168  19832  S   0.0   1.1  53:26.35  plink
117 www-data    20   0   340448  41716  19784  S   0.0   1.1   9:39.67  plink
118 www-data    20   0   340448  42908  19860  S   0.0   1.1  26:20.38  plink
119 www-data    20   0   340448  41716  19784  S   0.0   1.1   9:42.11  plink
120 root        20   0   142280    9860   8432  S   0.0   0.3   0:00.02  nmap
121 www-data    20   0   346852  48408  20708  S   0.0   1.2   9:39.36  plink
                    
```

11.5.3 Queues management

This tab contains information about application queue managers and provides access to manage them. To display and update the list, click **Refresh data**.

11.5.4 WEB metrics

This tab contains information on the number of requests to the application.

SYSTEM LOGS	INFO	QUEUES MANAGEMENT	WEB METRICS
 REFRESH DATA	RESET		
POST_broadcasting/auth			6988
GET_api/v0/notifications/unread			1251
GET_api/v0/users/items			1890
GET_api/v0/devices/items			2268
GET_api/v0/identifiers/items			8794
GET_api/v0/devices/events			1705
POST_api/v0/mobile-client/invite/person			69
GET_api/v0/mobile-client/data			9155
GET_api/v0/profile			1364
GET_api/v0/frontend/resources/meta			1217
GET_api/v0/call-history/items			1548
GET_api/v0/sip-numbers/contacts			381
GET_api/v0/project/settings/general			140
GET_api/v0/project/settings/broker			21



12 FAQ

Here you can find quick recommendations for some features configuration.

- [What settings must be done on the device for the Link server correct operation?\(see page 136\)](#)
- [What server elements are required for a basic server functioning?\(see page 137\)](#)
- [How to register a new user?\(see page 137\)](#)
- [How limit users if they have not paid for some features?\(see page 139\)](#)
- [How to activate a user profile?\(see page 139\)](#)
- [How to add root group?\(see page 140\)](#)
- [How to generate root groups?\(see page 143\)](#)
- [How to create a guest identifier?\(see page 145\)](#)
- [Why access restriction is required?\(see page 147\)](#)
- [How to create access restriction?\(see page 147\)](#)
- [How to add an identifier?\(see page 148\)](#)
- [How to notify residents of important information or survey them?\(see page 149\)](#)
- [How to create a virtual number?\(see page 150\)](#)
- [How to add a device to the Link server?\(see page 152\)](#)
- [How to configure an elevator controller?\(see page 153\)](#)
- [How to create access restriction for an elevator?\(see page 156\)](#)
- [How to configure hosting of several independent projects on the one server?\(see page 156\)](#)

12.1 What settings must be done on the device for the Link server correct operation?

The management system must be enabled for the device:

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.

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 using the MQTT protocol as it is less complex, more effective, provides data security, and fast and efficient message delivery.

4. Enter all required data.

If you select MQTT, you must:

- enter management system broker **address** and **port**;
- create a **password** for interaction with the 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 default here without the ability to enable/disable it.

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.

5. Submit settings.


Management system BAS-IP Link SUBMIT

Mode
MQTT

URL Password
link.bas-ip.com:8883 *****

Send realtime logs to server Encrypted



Certificate Info

 File

12.2 What server elements are required for a basic server functioning?




The main server elements are groups, users, identifiers, access restrictions, and connections between them. These are the basic elements that must be configured at the beginning.

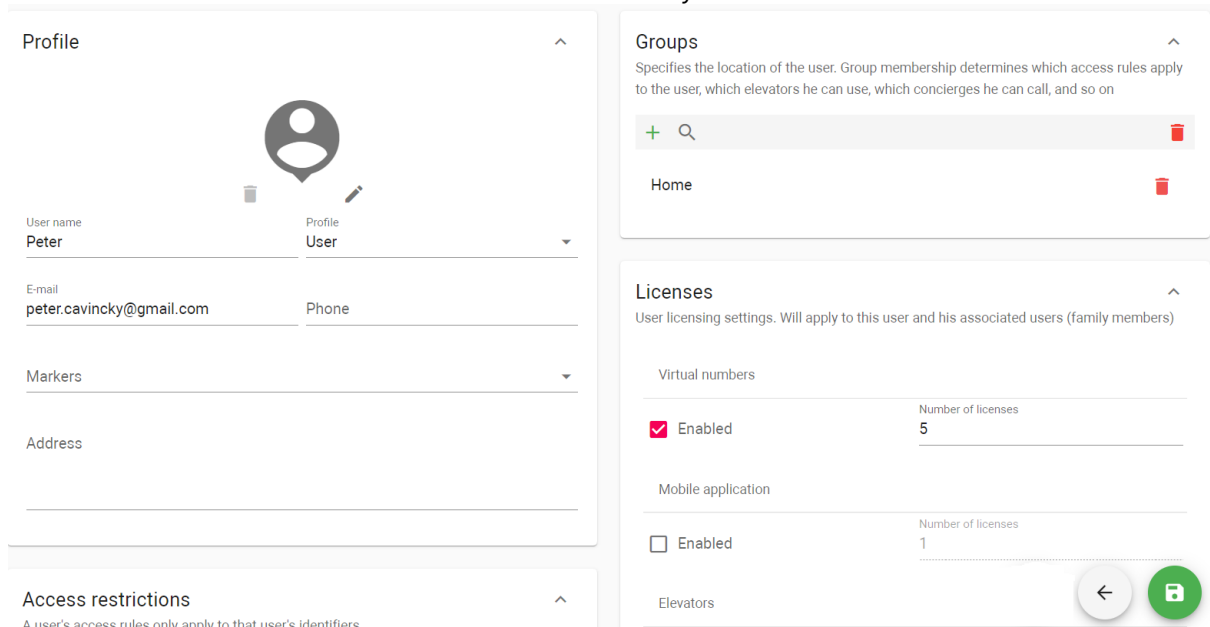
12.3 How to register a new user?

1. Open the **User** tab of the User management section.
2. Click **plus** icon in the left low corner.
3. Enter a user **name**.
4. Add user photo if necessary.
5. Select the **profile**⁸⁸ from created to give the user the required permissions.
6. Enter the user **email** to send the registration link.
7. Enter user **phone** number if necessary.
8. If required, select a **marker** for the user.
9. If necessary, enter user **address**.
10. Add  a user to a corresponding **group**⁸⁹ or create  a new one for this user.

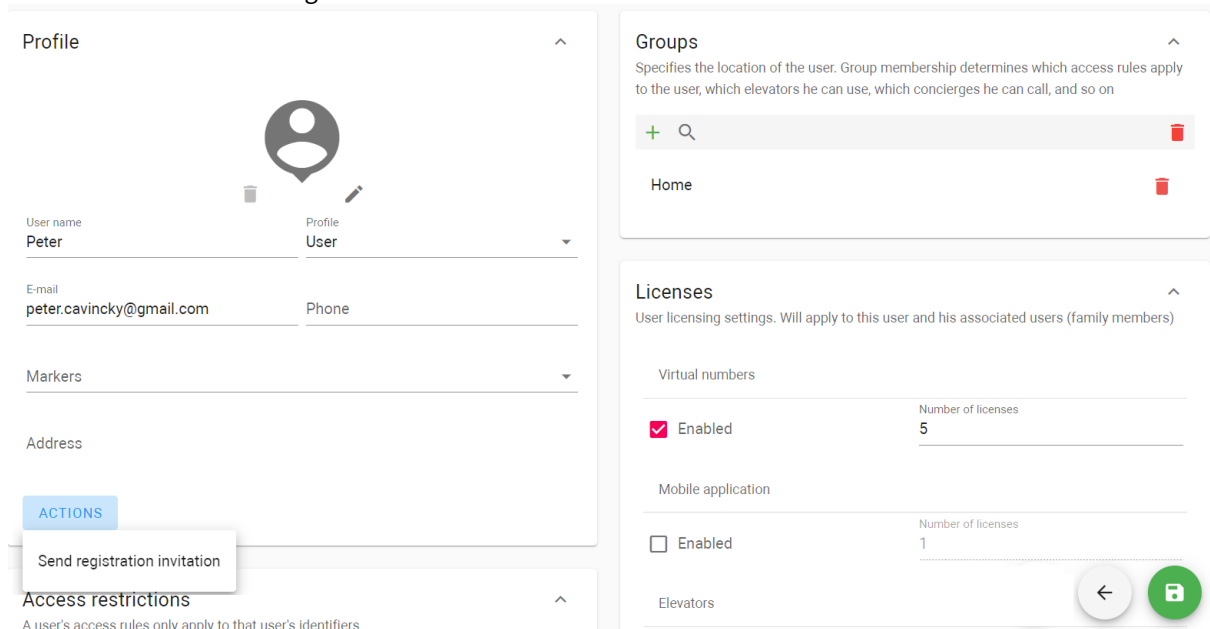
⁸⁸ <https://wiki.bas-ip.com/basiplinken/profiles-135955778.html>

⁸⁹ <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>

11. Select  from already added or create [access restrictions](#)⁹⁰. After clicking  you will be redirected to the [corresponding tab](#)⁹¹ where it is possible to create restrictions.
12. Select  [identifier/s](#)⁹² available for the user.
13. Set available for user **licenses** that they purchased.
14. Click the **Save** button in the left low corner when all necessary data is entered.



15. Open created user profile again.
16. Click **Actions** and send a registration invitation to the user.




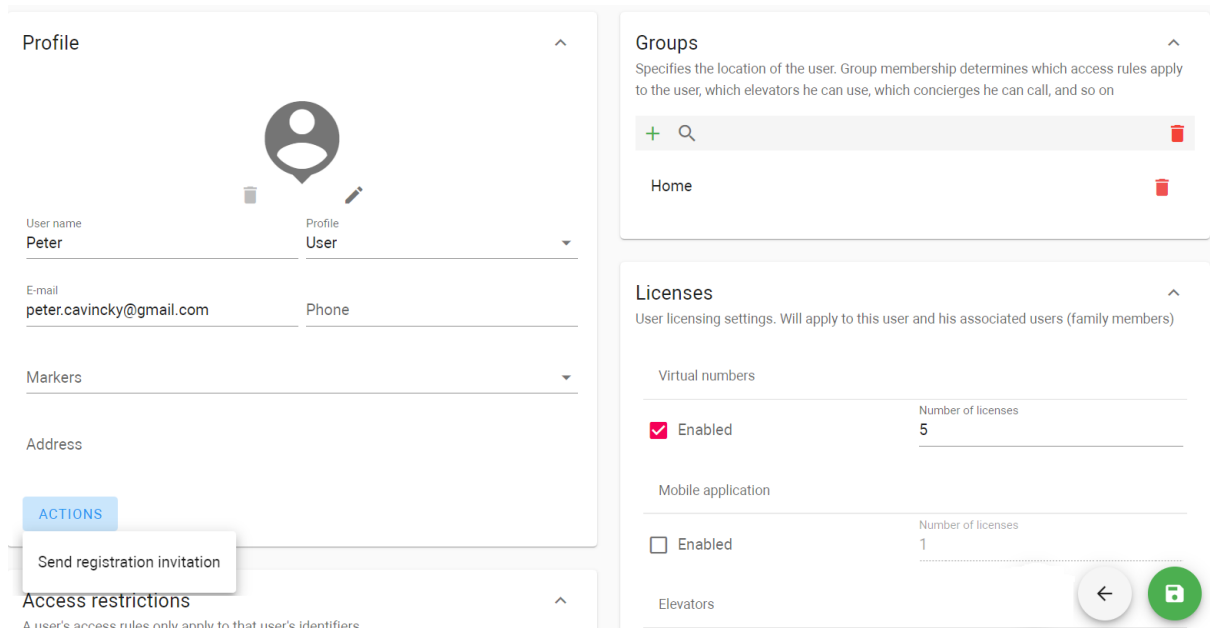
17. Close the profile.

90 <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>
 91 <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>
 92 <https://wiki.bas-ip.com/basiplinken/identifiers-135955834.html>

After receiving the invitation user must activate the profile.

12.4 How limit users if they have not paid for some features?

1. Open the **User** tab of the User management section.
2. Find the required user and click .
3. In the Licenses section, disable features that are not allowed for this user.
4. Click Save in the left low corner.



The screenshot displays the user management interface for a user named Peter. The interface is divided into several sections:

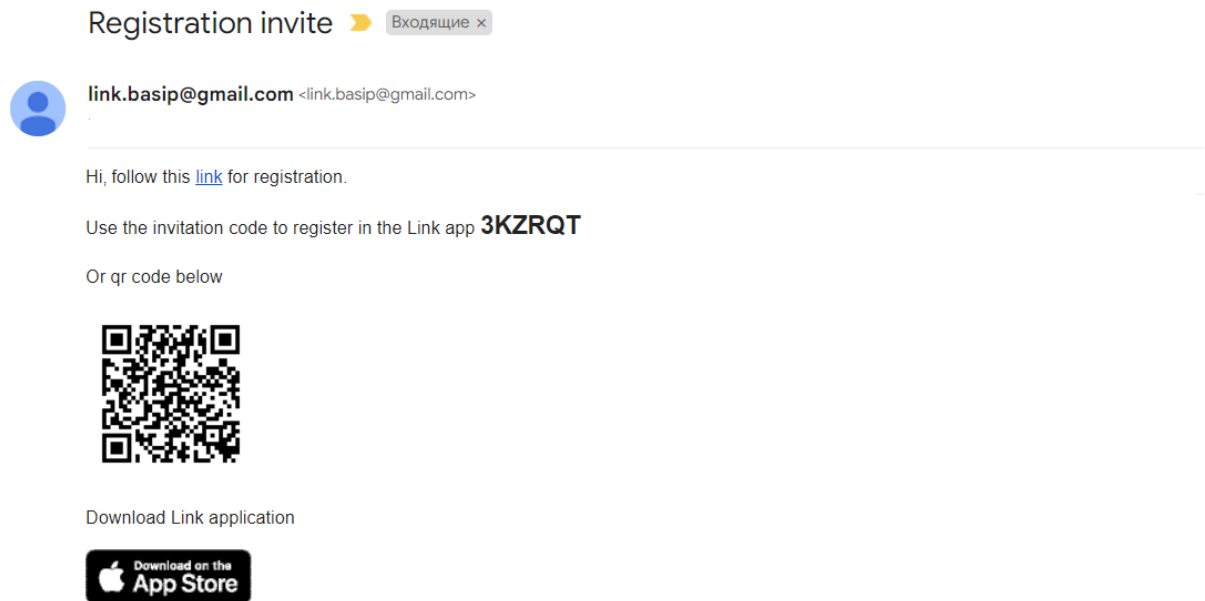
- Profile:** Shows the user's name (Peter), email (peter.cavincky@gmail.com), and a profile picture. There are icons for deleting and editing the profile.
- Groups:** Shows the user's group membership, currently 'Home'.
- Licenses:** Shows user licensing settings. It includes two sections:
 - Virtual numbers:** A checkbox labeled 'Enabled' is checked, and the 'Number of licenses' is set to 5.
 - Mobile application:** A checkbox labeled 'Enabled' is unchecked, and the 'Number of licenses' is set to 1.
- Actions:** A dropdown menu is open, showing the option 'Send registration invitation'.
- Access restrictions:** A section with a sub-note: 'A user's access rules only apply to that user's identifiers'.

When the user pays for the subscription, you can enable these options in the same way.

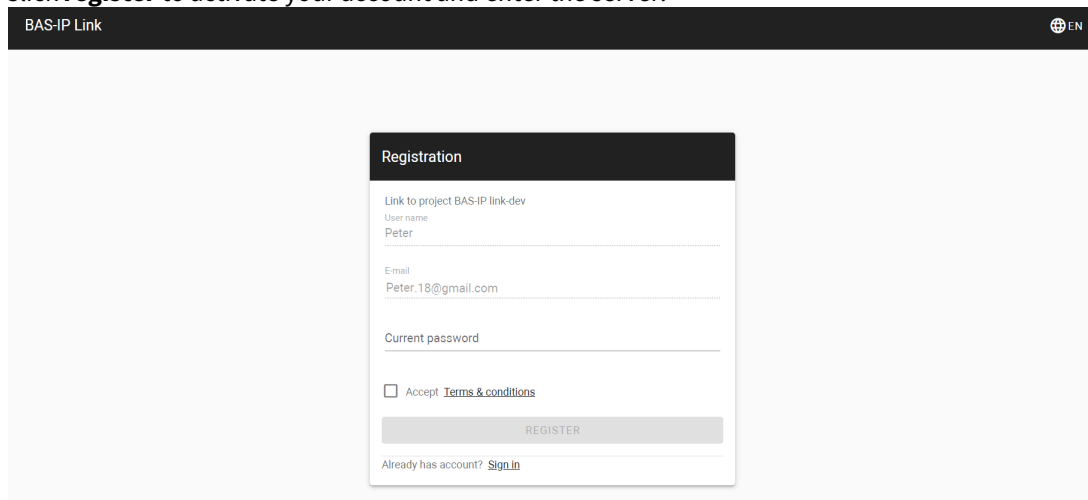
12.5 How to activate a user profile?

1. Open your email and find the invitation letter from the Link server.

2. Follow the **link** indicated in the letter.






3. Create a **password** for your account.
4. Accept **Terms & Conditions**.
5. Click **register** to activate your account and enter the server.



12.6 How to add root group?



1. Go to the **Groups** tab in the User management section.
2. Click **Add group** and select **Add root group**.
3. Enter a group **name**.
4. Select its **type**: if the group is for building, unit, floor, apartment, or custom (for parking or service rooms).
5. Enter a **logical address**: depending on the group type it can be Building No., Unit No., Floor No., or Apartment No.
6. Add a description, if necessary.

7. Select **users** (must be previously added in the [Users](#)⁹³ tab).
8. Select **devices** (must be previously added in the [Devices](#)⁹⁴ tab) installed in the place for what you are creating the group.
9. Create **access restrictions**  or select  from already created. After clicking  you will be redirected to the [corresponding tab](#)⁹⁵ where it is possible to create restrictions.

Applying access restriction is obligatory. This parameter helps to connect groups, devices, and users.

10. If necessary, enable and configure **forward settings** that will be applied to all group users.

It is also possible to create forward rules in the [corresponding tab](#)⁹⁶. The following options are available:

- to forward calls (from devices/users added to the group) **immediately** to all indicated in the call queue field/s numbers simultaneously;
- to forward calls to indicated in the call queue number/s **if there is no answer**;
- to set the **time** (5-30 sec) after which the call will be forwarded if there is no answer;
- **add** number/numbers (to which the call will be forwarded) to the **call queue** from the virtual number list;
- to set **call duration** by clicking  ;
- to set days and time when the forward is **valid** by clicking 
- forward calls to indicated in the call queue field/s numbers if the primary **number is busy or an error occurs**;

93 <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

94 <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

95 <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>

96 <https://wiki.bas-ip.com/basiplinken/forward-rules-135955902.html>

Immediately
 If no answer, then after 10 seconds forward to

☰ Call queue #1 ⚙️ 🗑️

Call duration: 🕒 60 seconds

Valid period: Mo Tu We Th Fr Sa Su 12:00 - 19:00

1009(1009) ✕ 1010(1010) ✕ +

+ ADD CALL QUEUE

If busy or error, forward to

☰ Call queue #1 ⚙️ 🗑️

1020(1020) ✕ +

+ ADD CALL QUEUE

You can get numbers for calls and forwardings in the [Virtual numbers⁹⁷](#) tab (if you have the corresponding license).

11. Click the **Save** button in the left low corner when all required data will be entered.

⁹⁷ <https://wiki.bas-ip.com/basiplink/en/virtual-numbers-47781248.html>

12.7 How to generate root groups?

1. Go to the **Groups** tab in the User management section.
2. Click **Add group** and select **Generate root groups**.
3. Click **Add group** in the opened window.
4. Select groups **type**: if the group is for building, unit, floor, apartment, or custom.
5. Enter groups **name**.
6. Indicate the **number of buildings** for which you need to create groups.
7. Set the number from which the numbering of buildings starts.
8. Click plus icon to add subgroups (e.g. Unit) and enter the same information for this section: type names, amount of units in one building, and the number from which the numbering starts.
9. Add and set the same settings for floors and apartment subgroups.

When entering the apartment amount, enter a general value of apartments on the one floor, not their No.

10. If there are any specific subgroups (parking or service rooms), you need to create and select a custom group type.

Generate groups

SETTINGS
RESULT

⋮ ▾ Add group Building with the name Building # in the amount of 2 , number from 1
🗑

⋮ ▾ Add group Unit with the name Unit # in the amount of 3 , number from 1
🗑

⋮ ▾ Add group Floor with the name Floor # in the amount of 5 , number from 1
🗑

⋮ ▾ Add group Apartment with the name Apartment # in the amount of 4 , number from 1
🗑

+

CLOSE
GENERATE

11. When all data is entered click **Generate** and all groups will be created according to the entered data.
12. Check the correctness. Open the **Settings** tab to edit entered data.

SETTINGS
RESULT

- ▾ Building #1(Type: Building, Logical address: 1)
 - ▾ Unit #1(Type: Unit, Logical address: 1)
 - ▾ Floor #1(Type: Floor, Floor number: 1)
 - Apartment #1(Type: Apartment, Logical address: 1)
 - Apartment #2(Type: Apartment, Logical address: 2)
 - Apartment #3(Type: Apartment, Logical address: 3)
 - Apartment #4(Type: Apartment, Logical address: 4)
 - Floor #2(Type: Floor, Floor number: 2)
 - Floor #3(Type: Floor, Floor number: 3)
 - Floor #4(Type: Floor, Floor number: 4)
 - Floor #5(Type: Floor, Floor number: 5)

13. Save generated groups and then add previously registered [users](#)⁹⁸, [devices](#)⁹⁹, or [access restrictions](#)¹⁰⁰.

12.8 How to create a guest identifier?

Only a user that has at least 1 access restriction and at least 1 device associated with this restriction can create a guest identifier.

1. Go to the **Guest access** tab in the Access management section.
2. Click **plus** icon in the left low corner.
3. Select ID **type**: **QR code** (available for panels with camera), **Access code** (available for panels with keypad), **URL** (available for all devices), or a **License plate** (available for panels and installed Axis camera with Axis License Plate Verifier software).
4. Select **guest type**: Courier or Guest.
5. Select the **access restrictions** you want to apply for the ID. Selected access restrictions must coincide with restrictions applied to the user is creates the ID.
6. Tick the **restriction period** field if it is necessary to limit the ID validity period.
7. Indicate the **beginning** and the **ending** of the ID active period. By default, the pass works for 1 day.
8. If necessary, tick the **limit the number of passes** field.
9. Enter the available **number of passes** for this ID. By default, 1 pass is available.

You may enable and set either a **restriction period** or a **number of passes** parameters.

10. Enter a **guest message** if required.

⁹⁸ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

⁹⁹ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

¹⁰⁰ <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>

11. Click confirm when all data is entered.

Guest access

Type
QR-code

Guest type
Guest

Access restrictions
Test(SD)

Restriction period

Valid from X Valid until X

Limit the number of passes

Maximum number of passes

Guest message

CANCEL **CONFIRM**

12. Copy the link/access code or download a QR code (or pkpass file for adding the QR code to Apple Wallet) and sent it to the guest for further use.

Name: Guest identifier



Valid time: 2022-09-06 00:01
2022-10-21 00:00

Number of passes: 3

DOWNLOAD QR-CODE

DOWNLOAD PKPASS-FILE

CLOSE

12.9 Why access restriction is required?

Access restrictions are an integral part of the Link server that links devices, users, and schedules.

12.10 How to create access restriction?

1. Go to the **Access restriction** tab of the Access management section.
2. Click **plus** icon in the left low corner.
3. Enter the restriction **name**.

4. If necessary, enable the possibility to **use** this restriction **for guest identifiers**.
5. Add description, if required.
6. Select **devices** from the list or add new ones to allow their use. Further access restrictions will be applied to [users](#)¹⁰¹ or [groups](#)¹⁰² to allow them to open indicated device/s.
7. If necessary, specify the access point the is allowed to use.
8. Select the number of locks (if 2 locks are connected) that are allowed to open by users: the first, the second or all
9. If necessary, select a **schedule** from the list or add a new one to indicate restriction functioning time.
10. Click the **Save** button in the low left corner after entering all required data.

The screenshot displays a configuration form for an access restriction. It is divided into three main sections:

- General:** Contains a 'Name' field with the value 'For cleaners', a checked checkbox for 'Use when issuing guest access', and a 'Description' field.
- Devices:** Features a search bar with a plus icon and a magnifying glass. Below it, a device named 'Unit 1 Entrance' is listed with an 'Access p...' field and a 'Lock' dropdown menu set to 'First'. A red trash icon is visible to the right of the device name.
- Schedules:** Includes a search bar and a 'No data' message, indicating no schedules are currently defined.

At the bottom right of the form, there are two circular buttons: a back arrow and a green 'Save' button.

12.11 How to add an identifier?



1. Go to the **Identifiers** tab in the Access management section.
2. Click **plus** icon in the left low corner.
3. Enter the identifier name.
4. Select the user of this ID.
5. Select the identifier type (pay attention to a device characteristics) and enter its value:
 - **card:** EM-Marin or Mifare card. In the **Identifier** 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](#)¹⁰³ to convert a value from one to another system;
 - **UKEY** allows using smartphones as identifiers ([BAS-IP UKEY](#)¹⁰⁴ app is required). You must enter the identifier number in the **Identifier** field;
 - **access code** that must be entered on the panel keypad to open lock/s. In the **Identifier** field, you must indicate a numeric code that will be used to open a lock;
 - **face ID** allows opening the lock by scanning visitors faces. When adding this identifier type, you must upload a user photo with a well-lit face and real face proportions in .jpeg format;

¹⁰¹ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

¹⁰² <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>

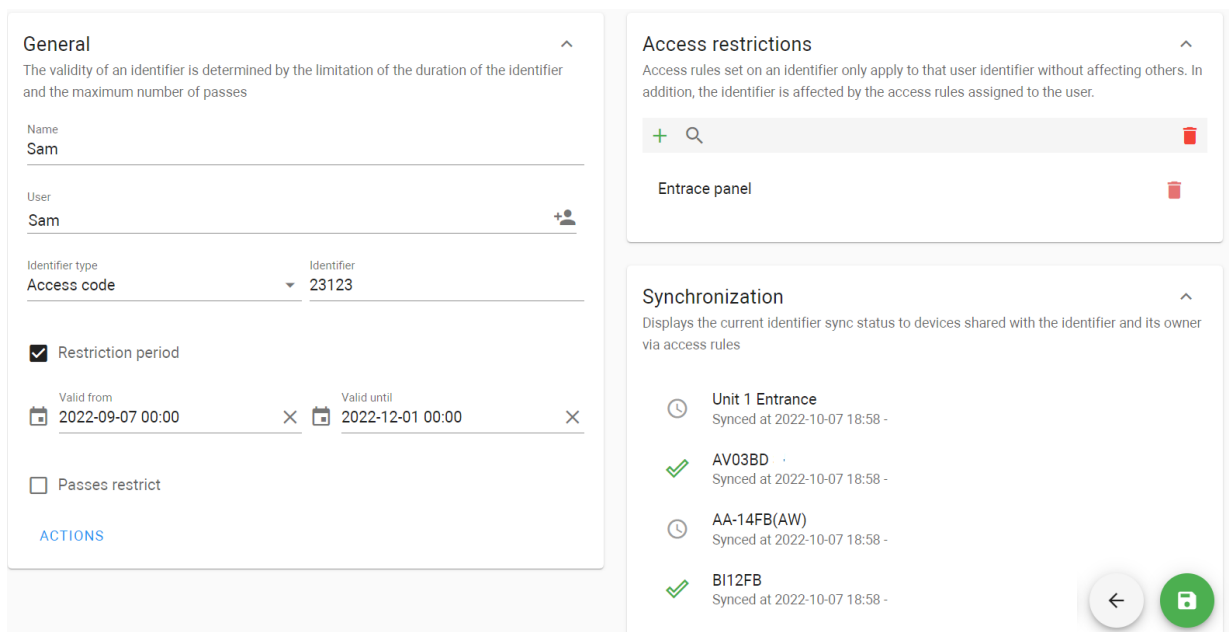
¹⁰³ <https://www.binaryhexconverter.com/hex-to-decimal-converter>

¹⁰⁴ <https://bas-ip.com/catalog/soft/bas-ip-ukey/>

- the automatically generated **QR code**. Enable the **Download QR code** option and after saving the identifier, it will be saved to the computer. Then it **must** be uploaded to a mobile device for further use;
 - **license plates** can be added and used to open lock/s. In the **Identifier** field, you enter the plate number. For this identifier to work, you need an Axis camera for plate scanning and installed AXIS License Plate Verifier software to send a number to the panel.
6. If necessary, enable and set restriction period restrictions for identifier validity.
 7. If necessary, enable and set the maximum number of passes in the passes **restrictions** field.
 8. Select  from already added or create **access restrictions**. After clicking  you will be redirected to the **corresponding tab**¹⁰⁵ where it is possible to create restrictions.

Applying access restriction is obligatory. This parameter helps to connect groups, devices, and users.

9. Click the **Save** button in the left low corner when all required data will be entered. The identifier will automatically be sent to the devices indicated in access restrictions. You can check where ID is added in the Synchronization section.



12.12 How to notify residents of important information or survey them?

A user with corresponding **permissions**¹⁰⁶ can create an announcement or poll.

1. Go to the **Announces** tab of the Communications section.
2. Click **plus** icon in the left low corner.
3. Enter the entry **name** that will be displayed in the Announces tab.
4. Add a **description** if necessary.

¹⁰⁵ <https://wiki.bas-ip.com/basiplink/en/creating-access-restrictions-15794714.html>

¹⁰⁶ <https://wiki.bas-ip.com/basiplinken/profiles-135955778.html>

5. Select the announce type: **info** (just message) or **poll** (message with a possibility to select variants or type answer).
6. Select in which way the announcement must be sent via **e-mail** or to **devices**.
7. Set the **date** of the announcement sending.
8. Add **recipients** in the corresponding section.
9. In the Content section enter data that will be displayed for recipients:
 - the **subject** of the announcement;
 - message **content**;
 - if you select a poll type, **add poll answers**;
 - for poll type, enable the options of selecting some variants of answer (**multi answers**) or typing free answer (**answer typed by user**).
10. Click the **Save** button in the left low corner when all required data will be entered.

The screenshot shows a configuration form for an announcement. It is divided into several sections:

- General:** Contains fields for 'Name' (filled with 'Cleaning'), 'Description', 'Announce type' (set to 'Poll'), 'Send via' (set to 'e-mail'), and 'Send on' (set to '2022-09-14 00:00').
- Recipients:** Shows a list of recipients, currently containing 'Administrator'.
- Content:** Contains a 'Subject' field (filled with 'Cleaning') and a rich text editor for the message content. The content entered is 'Do we need to clean the terrace more often?'. Below the editor are two checkboxes: 'Multi answers allowed' and 'Answer typed by user allowed', both of which are currently unchecked.
- Result:** A section at the bottom, currently empty.

12.13 How to create a virtual number?

1. Go to the **Virtual numbers** tab of the Telephony settings section.
2. Click **plus** icon in the left low corner.
3. The system will automatically generate a SIP number. Enter a name for the number.
4. Create the password for the number.
5. Tick the **Active** box to turn on the number operating.

To deactivate a number enable this box in the number settings.



6. Select the **user** (from previously added in the [User¹⁰⁷](#) tab) of the number.

7. Select the **device** on which the number must be used. If a user will use the number on a mobile device, leave the field blank.

The screenshot shows two configuration panels. The 'General' panel on the left includes a title 'General' with an expand/collapse arrow, a subtitle 'Belongs to the mobile client, editing is limited', and fields for 'Name' (set to 'For entrance panel') and 'Number' (set to '1031'). Below these is a 'Password' field with the value 'qwed12'. There is a checked checkbox for 'Active'. At the bottom, there are fields for 'User' (set to 'Administrator') and 'Device' (set to 'Unit 1 Entrance'). The 'Forward settings' panel on the right has a title 'Forward settings' with an expand/collapse arrow, a subtitle 'Allows you to more flexibly manage the call process, namely to set up forwarding queues for a given number', and a 'Forward mode' dropdown menu currently set to 'Disabled'. At the bottom right of the interface are two circular buttons: a back arrow and a lock icon.

8. If it is necessary, enable and **forward settings** for the number and set them manually or select a [forward rule](#)¹⁰⁸ from previously created.

The following options are available:

- to forward calls **immediately** to all indicated in the call queue field/s numbers;
- to forward calls to indicated in the call queue number/s **if there is no answer** from the main number;
- to set the **time** (5-30 sec) after which the call will be forwarded if there is no answer;
- **add** number/numbers (to which the call will be forwarded) to the **call queue** from the virtual number list;
- to set **call duration** by clicking  ;
- to set days and time when the forward is **valid** by clicking  ;
- forward calls to indicated in the call queue field/s numbers if the primary **number is busy or an error occurs**;

¹⁰⁸ <https://wiki.bas-ip.com/basiplinken/forward-rules-135955902.html>

The screenshot shows a configuration interface with two main sections:

- General:**
 - Belongs to the mobile client, editing is limited
 - Name: For entrance panel, Number: 1031
 - Password: qwed12
 - Active
 - User: Administrator, Device: Unit 1 Entrance
- Forward settings:**
 - Allows you to more flexibly manage the call process, namely to set up forwarding queues for a given number
 - Forward mode: Manual settings
 - Immediately
 - If no answer, then after 10 seconds forward to
 - + ADD CALL QUEUE
 - If busy or error, forward to
 - + ADD CALL QUEUE

Navigation buttons (back and save) are visible in the bottom right corner.

9. Click the **Save** button in the left low corner when all required data will be entered.

12.14 How to add a device to the Link server?

1. Go to the **Devices** tab of the Device management section.
2. Click **plus** icon in the left low corner.
3. Enter the device **name**.
4. Select its **type**: panel, monitor, access controller.
5. Select the device **model**.
6. Indicate the device **Serial number** (check the [Dashboard](#)¹⁰⁹ tab of the device web interface or device box).
7. Select a **group**/subgroup where the device is installed.
8. If necessary, set panels location **geodata**. This data is required for the Link app, when a visitor with a pass (added to Apple Wallet) approaches the available panel (with location), the pass will be automatically shown.
9. Add a **description**, if necessary.
10. Enable **using a camera to identify license plates**, if necessary.
11. Allow **remote lock opening** (from the device web interface, via API), if necessary.

Enter network settings for server and panel interaction:

- select the appropriate **communication protocol**: HTTP or MQTT (is recommended to use);
- enter the device **IP address** and **port**;
- enter **login** and **password** that are used to enter the device web interface;
- indicate server interaction password (is created in the Management system section ([Network](#)¹¹⁰ tab) of the device web interface).

Also, the same network settings as for the server must be entered in the device web interface. The management system must be enabled for the device:

¹⁰⁹ <https://wiki.bas-ip.com/aa07/dashboard-135955050.html>

¹¹⁰ <https://wiki.bas-ip.com/aa07/network-135955054.html>

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 required data.
5. Submit settings.

Detailed instructions are [here](#)¹¹¹.

Management system BAS-IP Link

SUBMIT

Mode
MQTT

URL
link.bas-ip.com:8883

Password

Send realtime logs to server

Encrypted

Certificate Info

File

13. Click the **Save** button in the left low corner when all required data will be entered.

12.15 How to configure an elevator controller?

Before controller configuration, it must be added in the [Device](#)¹¹² tab.

1. Open the **Elevators** tab of the Elevator management section.
2. Click **plus** icon in the left low corner.
3. Enter the elevator name.
4. Select a group where it is placed.
5. Tick **send elevator controller settings** on the device so that the settings data is transmitted to the controller.
6. Select available **mode**: Up (an elevator moves only in the upward direction), Down (movement is only in the downward direction), Up and down (both directions are available), Access by identifier (movement only to those floors that are available for the used identifier).
7. Select relay **type**: COM-NO/COM-NC.
8. Set the **time** during which the relay will be switched.
9. Set lift **release time** (during which relay will be closed/opened) for identifier and for API call.
10. If necessary, enable the **switching relay when turning on the device**.
11. You can see the number of available and used relays. For Up and down mode only 8 relays are available, for other modes 16 can be used.

¹¹¹ <https://wiki.bas-ip.com/aa07/network-135955054.html>

¹¹² <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

12. Create a list of floors and corresponding relays for a unit.

Edit controller relay

Mode

Mode Up and down ▼	Controller relays COM-NO ▼
Relay switch time (msec.) 100	
Lift release time for identifier (sec.) 2	Lift release time for API call (sec.) 3

Switch when turning on the device

Controller relays: (used 6 from 8)

+
🗑️

Floor name	Floor number	Relay numbers	
Floor 1	1	[1]	✏️ 🗑️
Этаж #2	2	[2]	✏️ 🗑️
Этаж #3	3	[3]	✏️ 🗑️

CANCEL CONFIRM

13. To add a floor click **plus** icon.
14. Enter **Floor No.** and **Relay No.** that connected to this floor at the controller.
15. Indicate whether the floor is public or not. Users will always have access to the public floor despite their identifier settings.
16. Select necessary apartments located on the floor (data is automatically taken from the Groups tab).

- Click **Confirm** to add the floor to the list.

Add controller relay

Floor name
Floor 1

Floor Relay numbers
Floor 1(Floor number: 1) **1**

Public floor

Apartments list

Add apartments on the floor
Apartment #1(1), Apartment #2(2), Apartment 3(3)

00-01
00-02
00-03

logical apartment address

CANCEL

CONFIRM

- Click **Confirm** to add the controller when you enter all necessary data.
- Click the **Save** button in the left low corner.

General ^

Name
lift

Group
Unit 1 ✎

Elevator access rules ^

No data

Controller settings ^

To operate the elevator, elevator controllers are used. Each controller corresponds to its range of floors, this is configured in the "Contacts of the controller" section

+ 🔍
✖

Elevator's controller	Controller mode	Controller direction	
lift controller 2	COM-NO	Up and down	✎ ✖

←
☑

- Open the **Device settings** tab of the Device management tab and find the controller.
- Check the correctness of settings (if they are the same as entered in the Elevators tab).
- Enable send on device feature to transmit entered settings to the controller.
- Save changes.

12.16 How to create access restriction for an elevator?

1. Go to the **Access restriction** tab of the Elevator management section.
2. Click **plus** icon in the left low corner.
3. Enter the restriction **name**.
4. Add **description**, if required.
5. Select **user/s**¹¹³ from the list to whom this restriction will be applied.
6. Select the **elevator**¹¹⁴ that the selected users can use.
7. Specify **floor/s** to which user/s will have access.
8. Click the **Save** button in the low left corner after entering all required data.

The screenshot shows the 'Access restriction' configuration page. It is organized into three panels:

- General:** Contains a 'Name' field with the value 'For cleaners' and a 'Description' field with the value '2 cleaners every week'. There is a green plus icon at the bottom right of this panel.
- Users:** Titled 'Users', it contains a search bar and a list of users: 'John' and 'Pete'. Each user name has a red trash icon to its right.
- Elevators:** Titled 'Elevators', it contains a search bar and a list of elevators: 'ANT'. Next to 'ANT' is a dropdown menu labeled 'Floors' with the value '2, 3' and a red trash icon.

At the bottom right of the interface, there are two circular buttons: a grey one with a left-pointing arrow and a green one with a white document icon (Save).

12.17 How to configure hosting of several independent projects on the one server?

It is possible to use a server for several small projects, e.g., for some separate areas with few devices. To configure this mechanism you must:

1. Create or generate the required number of **root groups** as explained earlier. Each root group stands for a single project.
2. Add the required number of **subgroups** (depending on the project structure) as described earlier.
3. Rename the default administrator role into **the master administrator** as this user has permissions to monitor and configure all projects available on the server.
4. Create a profile for **the root group administrator** as they must see only their root group, subgroups, device(s), user(s), role(s), access rule(s), logs, etc. You can use one profile for all projects or create profiles for each project. This profile must have the following permissions:

¹¹³ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

¹¹⁴ <https://wiki.bas-ip.com/basiplinken/elevators-135955962.html>

- **access restrictions:** can view/create/edit/delete access rules;
 - **announces:** can create/edit/delete/send announces, can view announces;
 - **conversations:** can create conversation/conversation message, can delete conversation, can accept messages from descendant users;
 - **devices:** can view device tasks, can create/edit/delete/view devices, can view device events;
 - **elevators:** can create/edit/delete elevator, can view elevators;
 - **emergency alerts:** can view emergency alerts, can create/edit/delete/playback emergency alerts;
 - **forward rules:** can view/create/edit/delete forward rules;
 - **groups:** can delete/edit group, can create group-descendant;
 - **identifiers:** can view identifiers; can create/edit/delete identifier; can create guest identifier, can import/export identifiers, can view ACS logs;
 - **markers:** can view/create/edit/delete/apply marker;
 - **profiles:** can view roles, can edit role (these rules are applied to the list of available profile types set in the corresponding section);
 - **schedule:** can view/create/edit/delete schedule;
 - **users:** create/edit/delete user;
 - **virtual numbers:** can create/edit/delete/activate virtual number, can mark system virtual numbers;
5. Edit the default profiles or create new ones for the user and concierge and set the permissions (they can differ depending on the project). It is very important to set permissions because this will determine their functionality and scope. The obligatory permissions for **concierge** are:
- **announces:** can create/edit/delete/send announces, can view announces;
 - **calls:** can receive call like concierge, can call to intercom;
 - **conversations:** can view all conversations, can send messages to all, can create conversation/conversation message, can accept messages from descendant users;
 - **emergency alerts:** can view particular emergency alerts, can playback emergency alerts;
 - **markers:** can view marker;
- User** must have such permissions as:
- **calls:** can call to intercom;
 - **conversations:** can create conversation message;
 - **identifiers:** can view identifiers; can create guest identifier;
6. Add [users¹¹⁵](#) to the server.
7. Apply corresponding profiles to users.
8. Add users to the created groups: root group administrator must be added to the root group (the main project group), and all other users must be added to the corresponding groups.

As a result, the administrator added to the root group can manage and monitor all linked with this group users, access restrictions, devices, schedules, etc. So, they can not influence and access other projects (root groups) they are not linked with.

¹¹⁵ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

13 Example of the server configuration for a basic project

Here you can find an example of a complete server (with SIP) configuration for 1 house project:

- 1. Configure basic server settings <https://wiki.bas-ip.com/basiplinken/first-authorization-and-the-server-initial-setup-135955740.html> for the correct functioning; (see page 158)
- 2. Add user profiles for various user and configure their permissions. (see page 158)
- 3. Add a group for the house/s. (see page 159)
- 4. Add users to the system. (see page 161)
- 5. Add devices to the system. (see page 163)
- 6. Add access restrictions for created groups/users. (see page 165)
- 7. Add identifiers for users. (see page 168)
- 8. Add and configure an elevator functioning. (see page 169)
- 9. Create virtual numbers for users. (see page 173)
- 10. Guest access providing. (see page 174)
- 11. Link app usage. (see page 186)

13.1 1. Configure **basic server settings**¹¹⁶ for the correct functioning:

- **main information**¹¹⁷;
- **mail server** (see page 117) for sending emails from the Link;
- **notifications** (see page 118) about the system that the administrator will get;
- **SIP settings**¹¹⁸ for calls functioning;
- **purchased license**¹¹⁹;
- **SIP trunks**¹²⁰ for call to mobile numbers functioning (if the corresponding license is used);
- the **appearance**¹²¹ of the guest pass for the **mobile app**¹²²;
- **information**¹²³ about the management company for display in the **mobile app**¹²⁴;
- invitation or other default **emails**¹²⁵.

13.2 2. Add user profiles for various user and configure their permissions.

In general, 3 profiles are enough for the basic project, and they are created by default:

- **administrator** controls the whole system and has all possible permissions to perform system installation, configuration, and support;
- **concierge** interacts with residents and visitors, manages access conditions, and sends announcements and messages: **announces** (can create/edit/delete/send announces, can view particular announces); **calls** (can receive call like concierge, can call to intercom); **conversations** (can create conversation/conversation message, can accept messages from descendant users); **devices** (can view devices, can view device events);

¹¹⁶ <https://wiki.bas-ip.com/basiplinken/first-authorization-and-the-server-initial-setup-135955740.html>

¹¹⁷ <https://wiki.bas-ip.com/basiplinken/general-135955998.html>

¹¹⁸ <https://wiki.bas-ip.com/basiplinken/sip-settings-135956014.html>

¹¹⁹ <https://wiki.bas-ip.com/basiplinken/licenses-135956024.html>

¹²⁰ <https://wiki.bas-ip.com/basiplinken/sip-trunks-135958438.html>

¹²¹ <https://wiki.bas-ip.com/basiplinken/additional-settings-135956004.html>

¹²² <https://wiki.bas-ip.com/basiplinkapp/guest-passes-110561627.html>

¹²³ <https://wiki.bas-ip.com/basiplinken/additional-settings-135956004.html>

¹²⁴ <https://wiki.bas-ip.com/basiplinkapp/bas-ip-link-110561562.html>

¹²⁵ <https://wiki.bas-ip.com/basiplinken/mail-templates-135958471.html>

- elevators** (can view elevators); **emergency alerts** (can view emergency alerts, can playback emergency alerts); **group types** (can view group type); **markers** (can view marker);
- user** is a profile for residents with the following permissions: **access restrictions** (can view/create/delete access rules); **announces** (can particular announces); **calls** (can call to intercom); **conversations** (can create conversation/conversation message); **devices** (can view devices/all devices); **group types** (can view group type); **identifiers** (can view particular identifiers; can create/delete identifiers; can create guest identifiers, can export identifiers); **profiles** (can view available roles only);

If necessary, you can edit these profiles in the [corresponding tab](#)¹²⁶ and add other permissions or create new profiles:

1. Go to the **Profiles** tab of the User management section.
2. Click plus icon (in the low left corner).
3. Enter a profile **name** and add a description (if required).
4. Select the required permissions.
5. Save data by clicking the corresponding button in the low left corner.

Also, it is possible to use one server for several small projects, e.g., for some separate areas with few devices. You can read about this configuration by following the [link](#)(see page 156).

13.3 3. Add a group for the house/s.

For example, there is 1 house with 2 units, 20 floors, and 4 apartments on each floor. So, [manual group creation](#)(see page 44) for example looks like this:

1. Go to the **Groups** tab in the User management section.
2. Click **Add group** and select **Add root group**.
3. Enter a group **name**, e.g. Heathfield House1.
4. Select custom for **type**.
5. Add a **description**, if necessary.
6. Click the **Save** button in the low left corner when all required data is entered.

The screenshot displays the configuration page for a new group. It is divided into several sections:

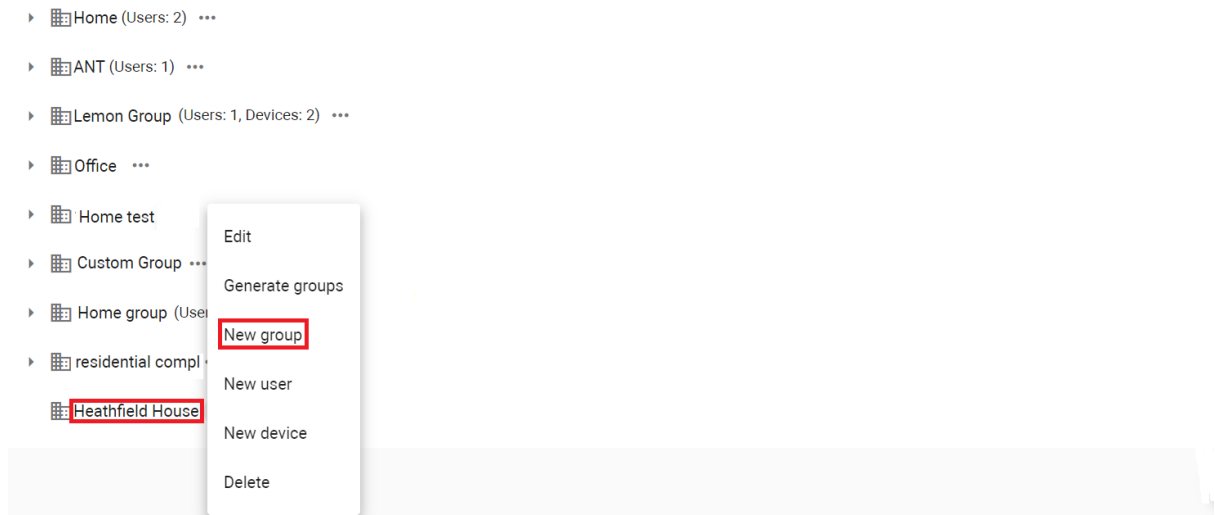
- General:** Contains fields for 'Name' (filled with 'Heathfield House'), 'Type' (set to 'Custom'), and 'Description'.
- Users:** A section titled 'Users who are in a group get access to passageways, elevators, concierge calls from this group and higher groups'. It features a search bar with a plus icon and a trash icon, and currently shows 'No data'.
- Access restrictions:** A section titled 'Access rules assigned to a group apply not only to this group, but also to its descendants'. It also has a search bar and currently shows 'No data'.
- Devices:** A section titled 'The belonging of a device to a group determines the physical location of the device in the project. And access to devices is determined by access rules'. It has a search bar.
- Forward settings:** A section titled 'General forwarding rules. Affect calls of users of this group and its descendants'. It includes a checkbox labeled 'Enabled' which is currently unchecked.

At the bottom right of the interface, there are three circular icons: a yellow one with a telephone handset, a grey one with a left-pointing arrow, and a green one with a document icon.

¹²⁶ <https://wiki.bas-ip.com/basiplinken/profiles-135955778.html>

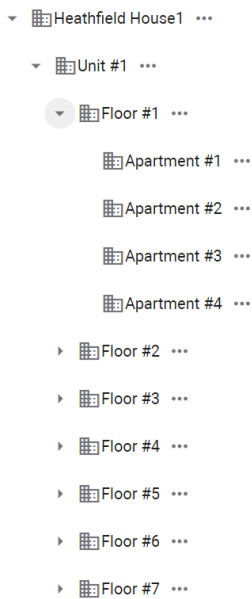
When the root (basic) group is created, you are required to add subgroups for each unit, floor, and apartment. To do this:

1. Find previously created root group in the list.
2. Click **3 dots** near the group name.
3. Select a **new group**. Menu for adding a group will open.



4. Enter all data that you've entered for the root group, but pay attention that this group stands for unit:
 - enter a group **name**, e.g. Unit 1;
 - Select unit for **type**;
 - Enter a **logical address**: Unit No., e.g. 1;
 - Add a **description**, if necessary.
5. Click the **Save** button in the low left corner when all required data is entered.
6. Repeat steps 1-5 to add a group for the 2nd unit. Pay attention, logical address must differ for the 2nd unit.
7. Repeat steps 1-5 to add subgroups for 20 floors in every unit and for 4 apartments on each floor. Select the corresponding group type for Pay attention, that subgroups for floors must be added to a unit group, and subgroups for apartments must be added to a floor group.

As a result, you will receive the following hierarchy:




Also, you can enter data about **groups** you are required to create and they **can be generated automatically**. Detailed steps you can read [here](#)¹²⁷ or watch the video.

Further, you must add [users](#)¹²⁸ and [devices](#)¹²⁹ to the required subgroup (unit/floor/apartment) and set [access restrictions](#)¹³⁰ for them.

13.4 4. Add users to the system.

All residents and service staff must be added to the Link:

1. Open the **User tab** of the User management section.
2. Click **plus** icon in the low left corner.
3. Enter a user name.
4. Add a user photo if necessary.
5. Select the user [profile](#)¹³¹ (from created in the previous steps).
6. Enter the user email to send the registration link.
7. Enter user phone number if necessary.
8. If necessary, enter user address.
9. Add  a user to a corresponding [group](#)¹³². For example, Mr. Clark lives on the 2nd floor of the 1st unit in Heathfield House1. So, you must add Mr. Clark exactly to this group.

¹²⁷ <https://wiki.bas-ip.com/basiplink/en/groups-15794622.html#id-Созданиегрупп-Howtogeneraterootgroups>

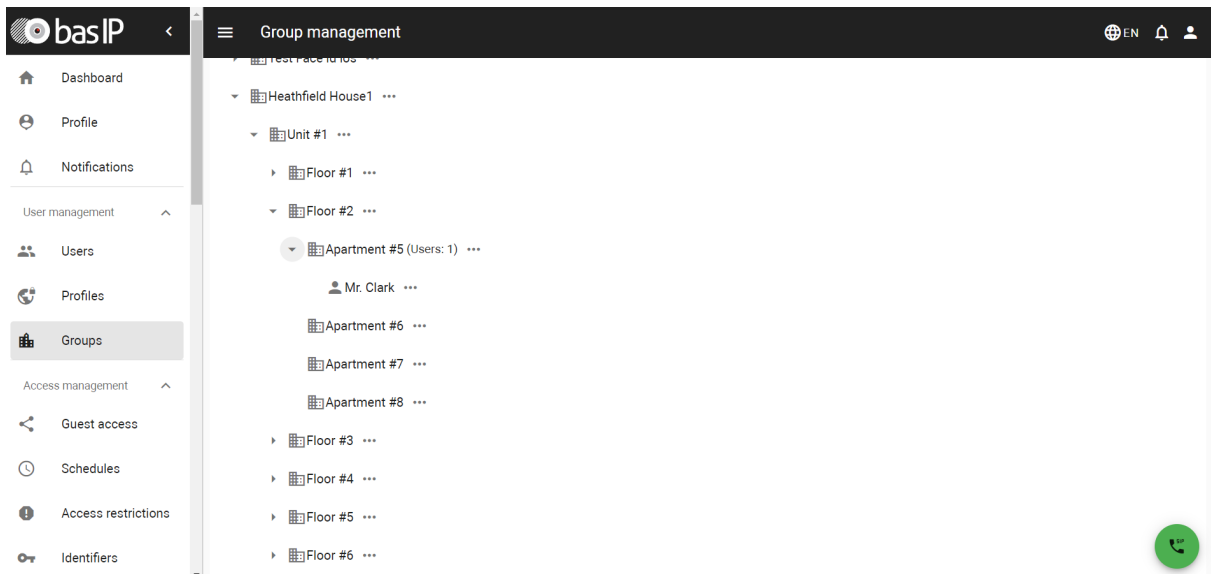
¹²⁸ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

¹²⁹ <https://wiki.bas-ip.com/basiplinken/devices-135955918.html>

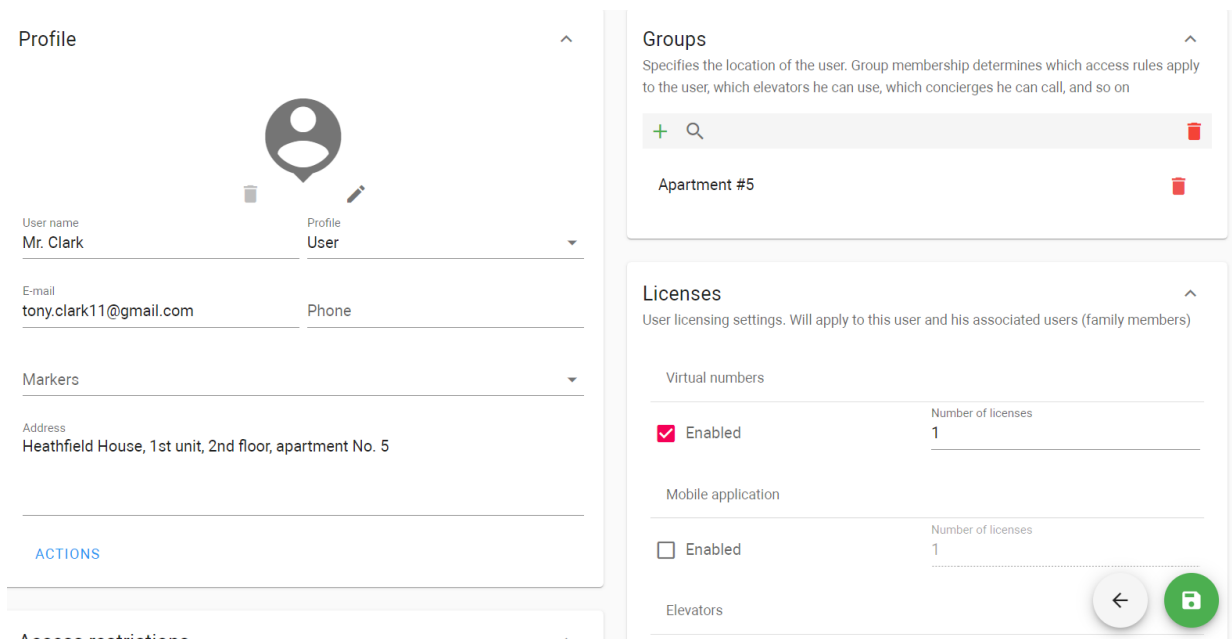
¹³⁰ <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>

¹³¹ <https://wiki.bas-ip.com/basiplinken/profiles-135955778.html>

¹³² <https://wiki.bas-ip.com/basiplinken/groups-135955783.html>



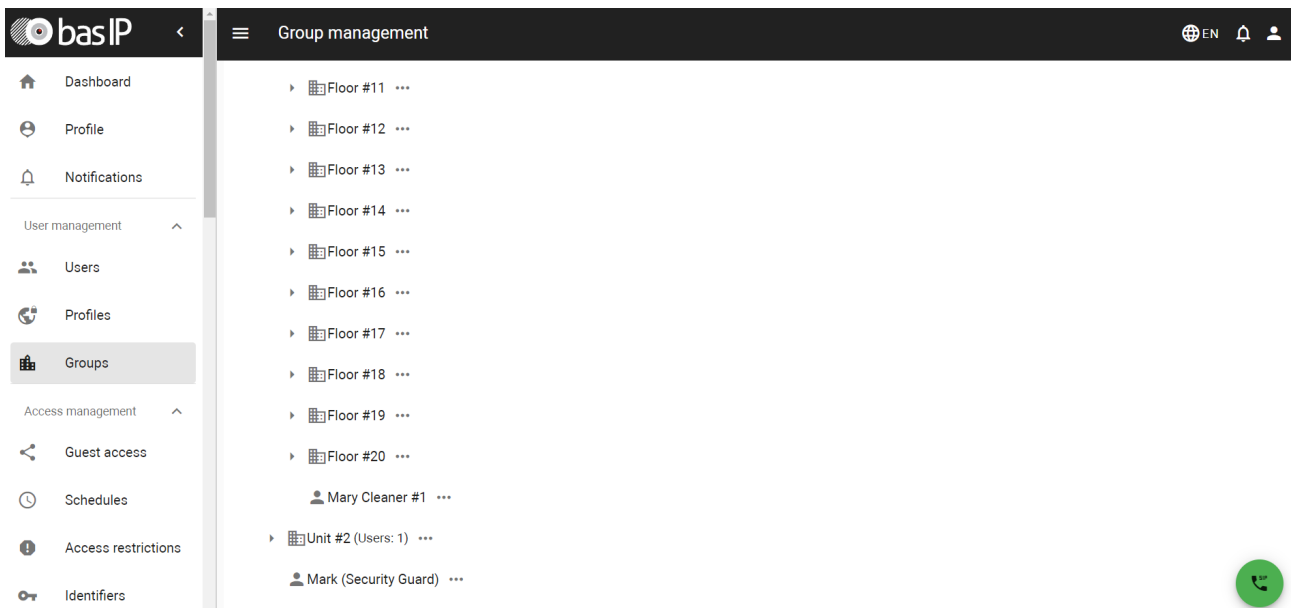
10. Set available for user licenses that they purchased.
11. Click the Save button in the low left corner when all necessary data is entered.



Further, you must add identifiers and set [access restrictions](#)¹³³ for users.

Also, you must add users for cleaners and security guards completing the previously described steps. Depending on what access they must have, you can add them to the root (house) group, e.g. Heathfield House1, or to the exact unit/floor group. If you add a user to the root group, they can pass only devices added to this root group, so they can only enter the house territory. This variant is appropriate for security guards. If you add user to unit group/s (e.g. a cleaner), they can use devices added to the root and unit group, so they can enter the house territory and unit/s.

¹³³ <https://wiki.bas-ip.com/basiplinken/access-restrictions-135955826.html>



13.5 5. Add devices to the system.

All devices (panels, controllers, monitors) must be added to the Link server to associate physical devices with data on the server. To do it:

1. Go to the **Devices** tab of the Device management section.
2. Click **plus** icon in the low left corner.
3. Enter the device **name**.
4. Select its **type**: panel, monitor, access controller.
5. Select the device **model**.
6. Indicate the device **Serial number** (check the [Dashboard](#)¹³⁴ tab of the device web interface or device box).
7. Select a **group**/subgroup where the device is installed.
8. Set panels location **geodata**. This data is required for the Link app, when a visitor with a pass (added to Apple Wallet) approaches the available panel (with location), the pass will be automatically shown.

General ^ Status - Name Unit 1 Entrance <hr/> Type Panel Model AA12 <hr/> Serial number qwerty2 Group Heathfield House1 ✎ <hr/> Geodata Latitude 51,55995469768316 Longitude -0,13581848354078832 ✎		Additional settings ^ Additional settings for devices <input type="checkbox"/> Used with a camera to identify license plate <input type="checkbox"/> Allow remote lock opening
		Network ^ Settings for connecting the device to the server. The IP address and port only need to be specified if the http protocol is used.

9. Add a **description**, if necessary.
10. Enable **using a camera to identify license plates**, if necessary.
11. Allow **remote lock opening** (from the device web interface, via API), if necessary.
12. Enter network settings for server and panel interaction:

¹³⁴ <https://wiki.bas-ip.com/aa07/dashboard-135955050.html>

- select the MQTT **communication protocol**;
- enter the device **IP address** and **port** (for HTTP only);
- enter **login** and **password** that are used to enter the device web interface;
- indicate server interaction password (is created in the Management system section ([Network](#)¹³⁵ tab) of the device web interface).

Also, the same network settings as for the server must be entered in the device web interface. The management system must be enabled for the device:

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 MQTT **protocol**.
4. Enter all required data.
5. Submit settings.

Detailed instructions are [here](#)¹³⁶.

Management system BAS-IP Link
SUBMIT

Mode
MQTT

URL
link.bas-ip.com:8883

Send realtime logs to server

Password

Encrypted

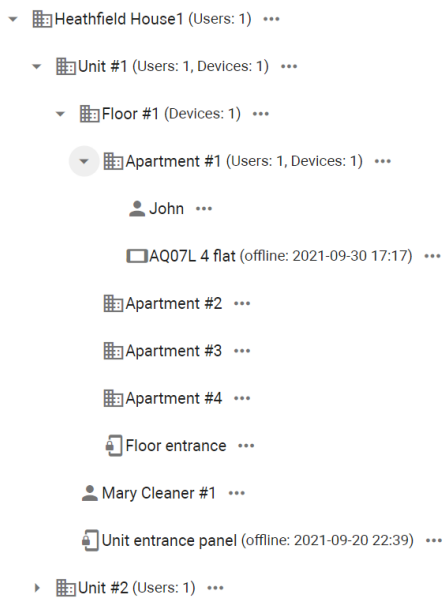
Certificate Info

File

As an example, there is 1 entrance panel in the Heathfield House1 to access its territory, 1 panel is near the entrance for each unit and each floor, and 1 monitor is in each apartment. So, repeat all previous steps to add each device for the corresponding group.

¹³⁵ <https://wiki.bas-ip.com/aa07/network-135955054.html>

¹³⁶ <https://wiki.bas-ip.com/aa07/network-135955054.html>



Also, you can remotely enter SIP, Network, and Address settings and **send** them **on the device** to prepare the device for functioning. More details you can read [here](#)¹³⁷.

13.6 6. Add access restrictions for created groups/users.

Access links devices, users, and [schedules](#)¹³⁸ (if required) and you can quickly configure giving access or not to these or those devices for concrete users. Access restrictions must be applied to groups with added devices and users.


To create access restrictions, e.g. for users who live in the 1st unit and 1st floor to have access to the Heathfield territory, their unit, and floor:

1. Go to the **Access restriction** tab of the Access management section.
2. Click **plus** icon in the low left corner.
3. Enter the restriction **name**.
4. Enable the possibility to **use** this restriction **for guest identifiers**.
5. Add description, if required.
6. Select **devices** from the list to allow their use. So, to access the Heathfield territory, 1st unit, and floor, you must select devices added to these areas.
7. Select the number of locks (if 2 locks are connected) that are allowed to open by users: the first, the second, or all.


¹³⁷ <https://wiki.bas-ip.com/pages/viewpage.action?pageId=15794626#id-Устройства-Remotedeviceconfiguration>

¹³⁸ <https://wiki.bas-ip.com/basiplinken/schedules-135955813.html>

8. Click the **Save** button in the low left corner after entering all required data.

9. Go to the **Groups** tab and find the corresponding group for which the rule is created. In our case, it is for users who live in the 1st unit and 1st floor, so 1st floor group must be selected.
10. Click **3 dots** near the group name and select edit.
11. Select  previously created access restriction.
12. Save changes.



If you want to apply access restriction to an exact user (e.g. cleaner or security guard), you must:

1. Go to the **Access restriction** tab of the Access management section.
2. Click **plus** icon in the low left corner.
3. Enter the restriction **name**.
4. Add description, if required.
5. Select **devices** from the list to allow their use, e.g workers must have access to all areas. So, you must select all devices located on the object.
6. Create  a schedule to limit active time for users and their identifiers, e.g., workers are required to have access to the areas at the exact time

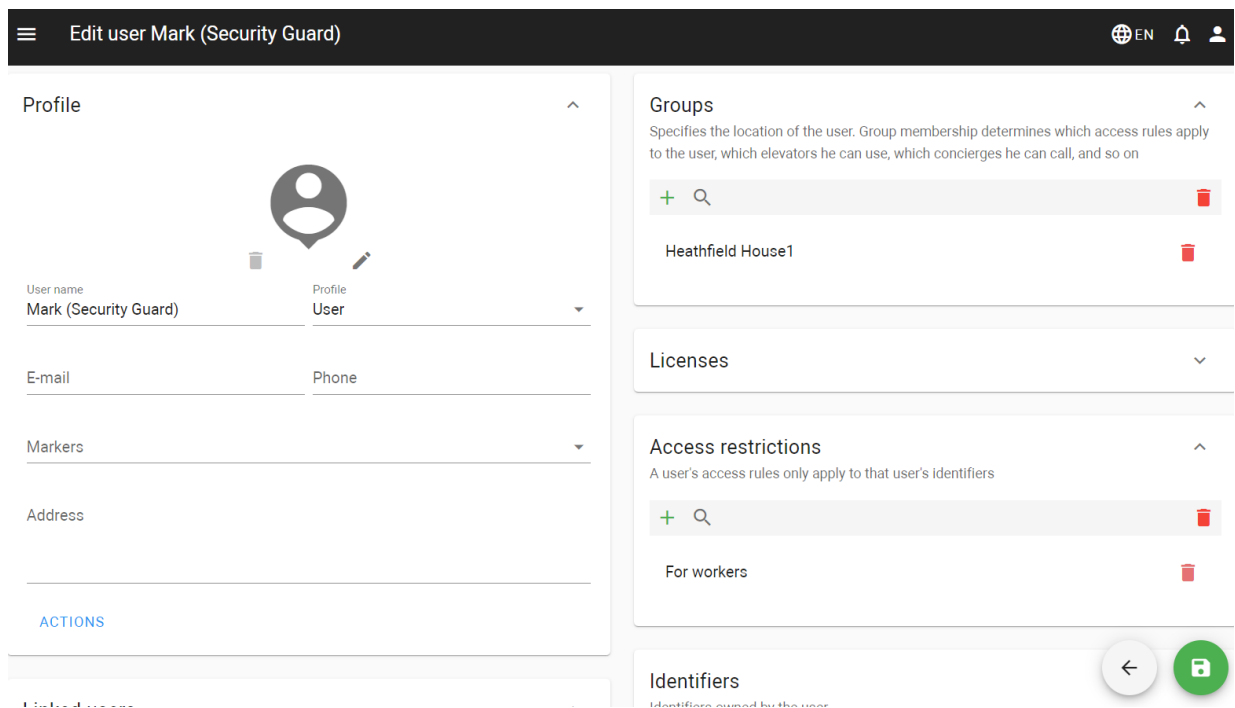
- enter the schedule **name**;
- add a **description**, if required;
- disable the **All day** option and specify the date (day/month/year) this schedule is active and set the **start** and **end** time of this schedule functioning, e.g. from 9 a.m. till 19 p.m.;
- select **daily** repetition of the schedule and workers will have access to the areas every day from 9 a.m. to 19 p.m.;
- save schedule;

<p>General ^</p> <p>Name Access for cleaners and security guards</p> <hr/> <p>Description</p> <hr/> <hr/> <p>Access restrictions ^</p>	<p>Settings ^</p> <p><input type="checkbox"/> All day</p> <p>Start at <input type="text" value="2022-11-01 09:00"/> × End at <input type="text" value="2022-11-01 19:00"/> ×</p> <p>Repeat Daily</p> <p>Repeat duration Always</p>
---	---

More details about schedules you can read [here](#)¹³⁹.

7. Save access restriction.
8. Go to the **User** tab and find the user you want to apply created access restriction.
9. Click edit  the user.
10. In the Access restriction section, select  created for the user restriction.
11. Save changes.

¹³⁹ <https://wiki.bas-ip.com/basiplinken/schedules-135955813.html>




13.7 7. Add identifiers for users.

To provide an identifier for a user, you must:

1. Go to the **Identifiers** tab in the Access management section.
2. Click **plus** icon in the low left corner.
3. Enter the identifier name.
4. Select the user of this ID.
5. Select the identifier type (pay attention to a device characteristics) and enter its value:
 - **card**: EM-Marin or Mifare card. In the **Identifier** 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](#)¹⁴⁰ to convert a value from one to another system;
 - **UKEY** allows using smartphones as identifiers (**BAS-IP UKEY**¹⁴¹ app is required). You must enter the identifier number in the **Identifier** field;
 - **access code** that must be entered on the panel keypad to open lock/s. In the **Identifier** field, you must indicate a numeric code that will be used to open a lock;
 - **face ID** allows opening the lock by scanning visitors faces. When adding this identifier type, you must upload a user photo with a well-lit face and real face proportions in .jpeg format;
 - the automatically generated **QR code**. Enable the **Download QR code** option and after saving the identifier, it will be saved to the computer. Then it must be uploaded to a mobile device for further use;
 - **license plates** can be added and used to open lock/s. In the **Identifier** field, you enter the plate number. For this identifier to work, you need an Axis camera for plate scanning and installed AXIS License Plate Verifier software to send a number to the panel.
6. If necessary, enable and set restriction period restrictions for identifier validity.
7. If necessary, enable and set the maximum number of passes in the passes **restrictions** field.

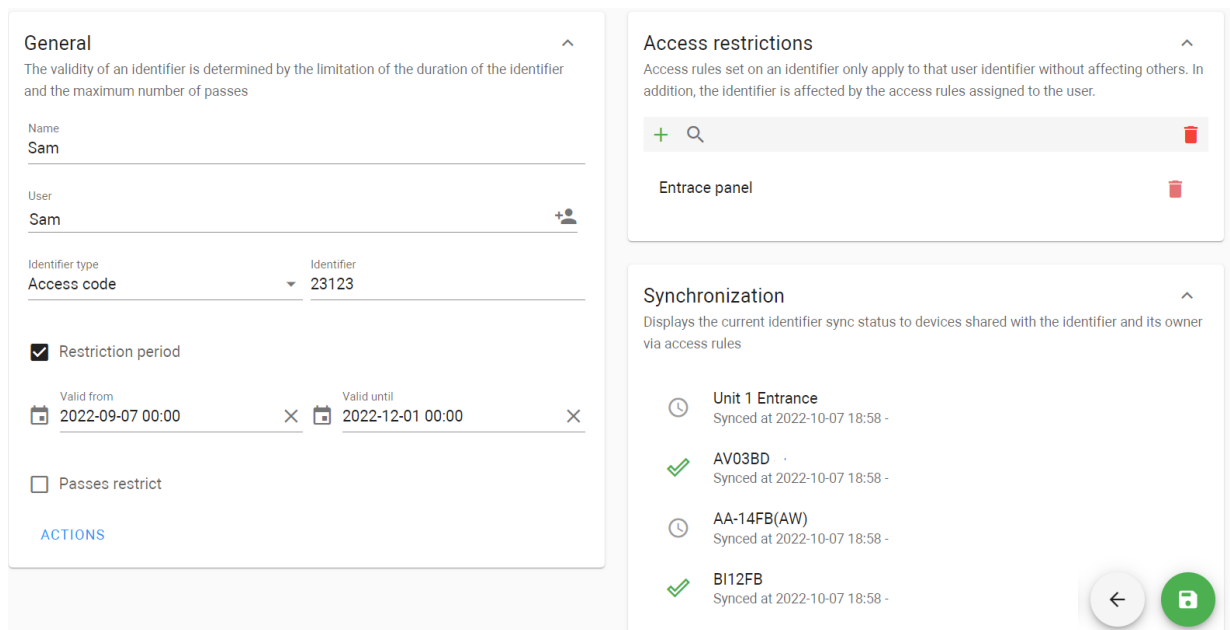
¹⁴⁰ <https://www.binaryhexconverter.com/hex-to-decimal-converter>

¹⁴¹ <https://bas-ip.com/catalog/soft/bas-ip-ukey/>

8. Select  **access restrictions** from already added, e.g. Entrance panel.

Applying access restriction is obligatory. This parameter helps to connect groups, devices, and users.

9. Click the **Save** button in the low left corner when all required data will be entered. The identifier will automatically be sent to all devices indicated in access restrictions. You can check where ID is added in the Synchronization section.



The screenshot displays the configuration interface for an identifier. It is divided into two main sections: 'General' and 'Access restrictions'.

General Section:

- Name:** Sam
- User:** Sam
- Identifier type:** Access code
- Identifier:** 23123
- Restriction period**
 - Valid from:** 2022-09-07 00:00
 - Valid until:** 2022-12-01 00:00
- Passes restrict**
- ACTIONS** (button)

Access restrictions Section:

- Access rules set on an identifier only apply to that user identifier without affecting others. In addition, the identifier is affected by the access rules assigned to the user.
- Search bar with a plus icon and a magnifying glass icon.
- Entrance panel** (selected rule)

Synchronization Section:

- Displays the current identifier sync status to devices shared with the identifier and its owner via access rules.
- Unit 1 Entrance** (clock icon) Synced at 2022-10-07 18:58 -
- AV03BD** (checkmark icon) Synced at 2022-10-07 18:58 -
- AA-14FB(AW)** (clock icon) Synced at 2022-10-07 18:58 -
- BI12FB** (checkmark icon) Synced at 2022-10-07 18:58 -

Navigation buttons (back and save) are visible at the bottom right of the synchronization section.

13.8 8. Add and configure an elevator functioning.

If you have a connected **EVRC-IP controller**¹⁴², first of all, you must add it in the Devices tab (see step 5 above or check the video with subtitles).

After adding a device, you must configure the controller work:

1. Open the **Elevators** tab of the Elevator management section.
2. Click **plus** icon in the left low corner.
3. Enter the elevator name.
4. Select a group where it is placed, e.g. Heathfield House1
5. Tick **send elevator controller settings** on the device so that the settings data is transmitted to the controller.
6. Select available **mode**¹⁴³: Up (an elevator moves only in the upward direction), Down (movement is only in the downward direction), Up and down (both directions are available), Access by identifier (movement only to those floors that are available for the used identifier).
7. Select relay **type**: COM-NO/COM-NC.

¹⁴² <https://wiki.bas-ip.com/evrcip/evrc-ip-135957507.html>

¹⁴³ <https://wiki.bas-ip.com/en/device-2752601.html#id-Настройкаадреса-Devicesettings>

8. Set the **time** during which the relay will be switched.
9. Set lift **release time** (during which relay will be closed/opened) for identifier and for API call.
10. If necessary, enable the **switching relay when turning on the device**.
11. You can see the number of available and used relays. For Up and down mode only 8 relays are available, for other modes 16 can be used.
12. Create a list of floors and corresponding relays for a unit.

Edit controller relay

Mode

Mode Up and down ▼	Controller relays COM-NO ▼
Relay switch time (msec.) 100	
Lift release time for identifier (sec.) 2	Lift release time for API call (sec.) 3

Switch when turning on the device

Controller relays: (used 6 from 8)

+
-

Floor name	Floor number	Relay numbers	✎	🗑
Floor 1	1	[1]	✎	🗑
Этаж #2	2	[2]	✎	🗑
Этаж #3	3	[3]	✎	🗑

CANCEL
CONFIRM

13. To add a floor click **plus** icon.
14. Enter **Floor No.** and **Relay No.** that connected to this floor at the controller.
15. Indicate whether the floor is public or not (e.g., ground floor). Users will always have access to the public floor despite their identifier settings.
16. Select necessary apartments located on the floor (data is automatically taken from the Groups tab).

- Click Confirm to add the floor to the list.

Add controller relay

Floor name
Floor 1

Floor Floor 1(Floor number: 1) Relay numbers 1

Public floor

Apartments list

Add apartments on the floor
Apartment #1(1), Apartment #2(2), Apartment 3(3)

00-01 00-02 00-03

logical apartment address

CANCEL

CONFIRM

- Click **Confirm** to add the controller when you enter all necessary data.
- Click the **Save** button in the left low corner.

General

Name
lift

Group
Unit 1

Elevator access rules

No data

Controller settings

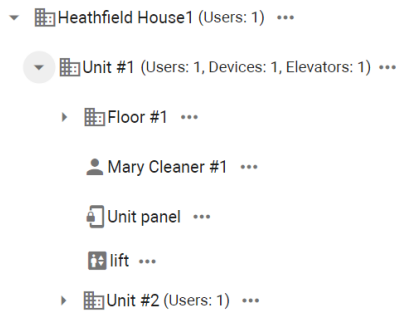
To operate the elevator, elevator controllers are used. Each controller corresponds to its range of floors, this is configured in the "Contacts of the controller" section

Elevator's controller	Controller mode	Controller direction	
lift controller 2	COM-NO	Up and down	✎ 🗑

← S

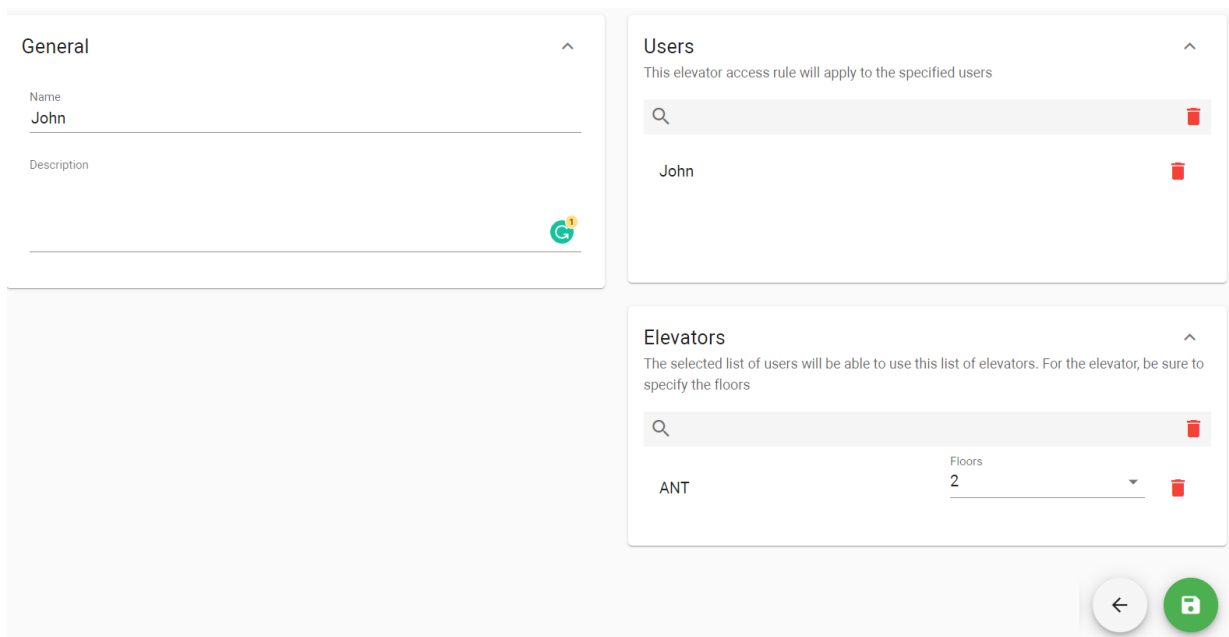
- Open the **Device settings** tab of the Device management tab and find the controller.
- Check the correctness of settings (if they are the same as entered in the Elevators tab).
- Enable send on device feature to transmit entered settings to the controller.
- Save changes.

As result, an elevator will be added to the group.



In addition, you can add **access restrictions** for users and elevators:

1. Go to the **Access restriction** tab of the Elevator management section.
2. Click **plus** icon in the low left corner.
3. Enter the restriction **name**.
4. Add **description**, if required.
5. Select **user/s**¹⁴⁴ from the list to whom this restriction will be applied.
6. Select the **elevator**¹⁴⁵ that the selected users can use.
7. Specify **floor/s** to which user/s will have access. Users will always have access to the floor marked as public.
8. Click the **Save** button in the low left corner after entering all required data.



144 <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

145 <https://wiki.bas-ip.com/basiplinken/elevators-135955962.html>

13.9 9. Create virtual numbers for users.

To make a call between devices, users and devices must have virtual numbers. For a user registered in the Link app, a virtual number is created and applied automatically. You can check the number in the user [profile](#)¹⁴⁶. For other devices, you must create a virtual number:

1. Go to the **Virtual numbers** tab of the Telephony settings section.
2. Click **plus** icon in the low left corner.
3. The system will automatically generate a SIP number. Enter a name for the number.
4. Create the password for the number.
5. Tick the **Active** box to turn on the number operating.


To deactivate a number enable this box in the number settings.

6. Select the **user** (from previously added in the [User](#)¹⁴⁷ tab) of the number.
7. Select the **device** on which the number must be used. If a user will use the number on a mobile device, leave the field blank.
8. Click the **Save** button in the low left corner when all required data will be entered.

The screenshot shows the configuration interface for a virtual number. It is divided into two main sections: 'General' and 'Forward settings'.

- General:**
 - Sub-header: "Belongs to the mobile client, editing is limited"
 - Name: "For entrance panel"
 - Number: "1031"
 - Password: "qwed12"
 - Active: Active
 - User: "Administrator"
 - Device: "Unit 1 Entrance"
- Forward settings:**
 - Sub-header: "Allows you to more flexibly manage the call process, namely to set up forwarding queues for a given number"
 - Forward mode: "Disabled"

At the bottom right, there are navigation buttons: a back arrow and a green save button.

When you apply a number for a device, the ability to call this device () will appear in the Link app.

¹⁴⁶ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

¹⁴⁷ <https://wiki.bas-ip.com/basiplinken/users-135955765.html>

13.10 10. Guest access providing.

Temporary identifiers for guests, couriers, taxi drivers, etc can be provided by a concierge in the Link or by a user in the Link app. It's possible to configure areas visitors will have access to, the time and date when the ID will work, and the number of available passes.

Only a user that has at least 1 access restriction and at least 1 device associated with this restriction can create a guest identifier.

To **create a guest pass in the Link** (by concierge, for example), the concierge must:

1. Go to the **Guest access** tab in the Access management section.
2. Click **plus** icon in the low left corner.
3. Select ID **type**: **QR code** (available for panels with camera), **Access code** (available for panels with keypad), **URL** (available for all devices), or a **License plate** (available for panels and installed Axis camera with Axis License Plate Verifier software).
4. Select **guest type**: Courier or Guest.
5. Select the **access restrictions** you want to apply for the ID. Selected access restrictions must coincide with restrictions applied to the user is creates the ID.
6. Tick the **restriction period** field if it is necessary to limit the ID validity period.
7. Indicate the **beginning** and the **ending** of the ID active period. By default, the pass works for 1 day.
8. If necessary, tick the **limit the number of passes** field.
9. Enter the available **number of passes** for this ID. By default, 1 pass is available.

You may enable and set either a **restriction period** or a **number of passes** parameters.

10. Enter a **guest message** if required.

- Click confirm when all data is entered.

Guest access

Type
QR-code ▼

Guest type
Guest ▼

Access restrictions
Test(SD) ▼

Restriction period

Valid from

📅
2022-09-06 00:01

×

Valid until

📅
2022-10-21 00:00

×

Limit the number of passes

Maximum number of passes
3

Guest message

CANCEL CONFIRM

- Copy the link/access code or download a QR code (or pkpass file for adding the QR code to Apple Wallet) and sent it to the guest for further use.

Name: Guest identifier



Valid time: 2022-09-06 00:01
2022-10-21 00:00

Number of passes: 3

DOWNLOAD QR-CODE

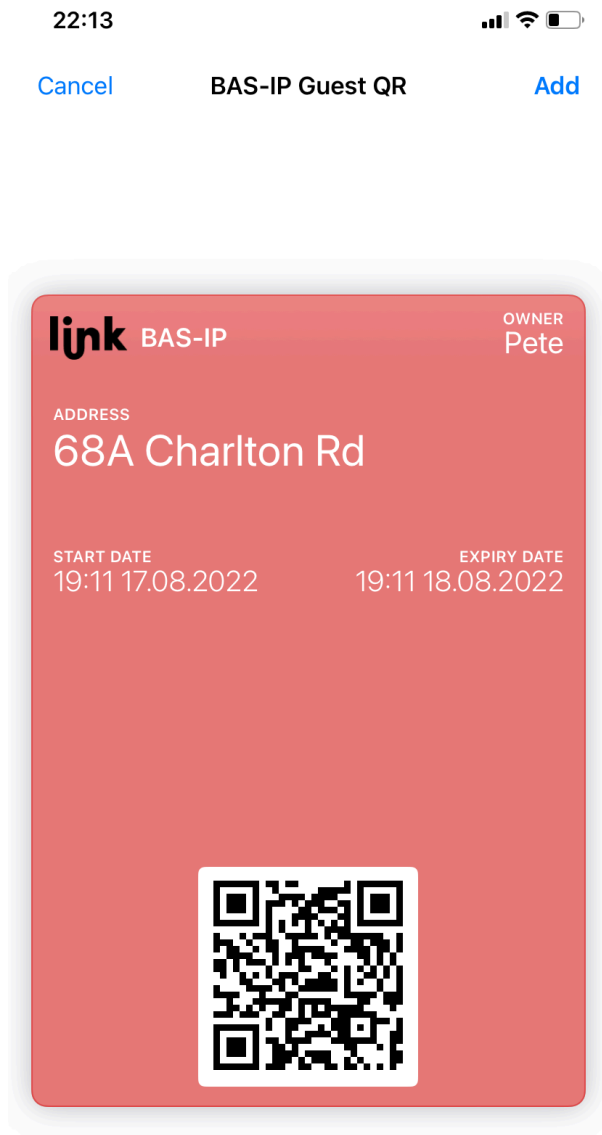
DOWNLOAD PKPASS-FILE

CLOSE

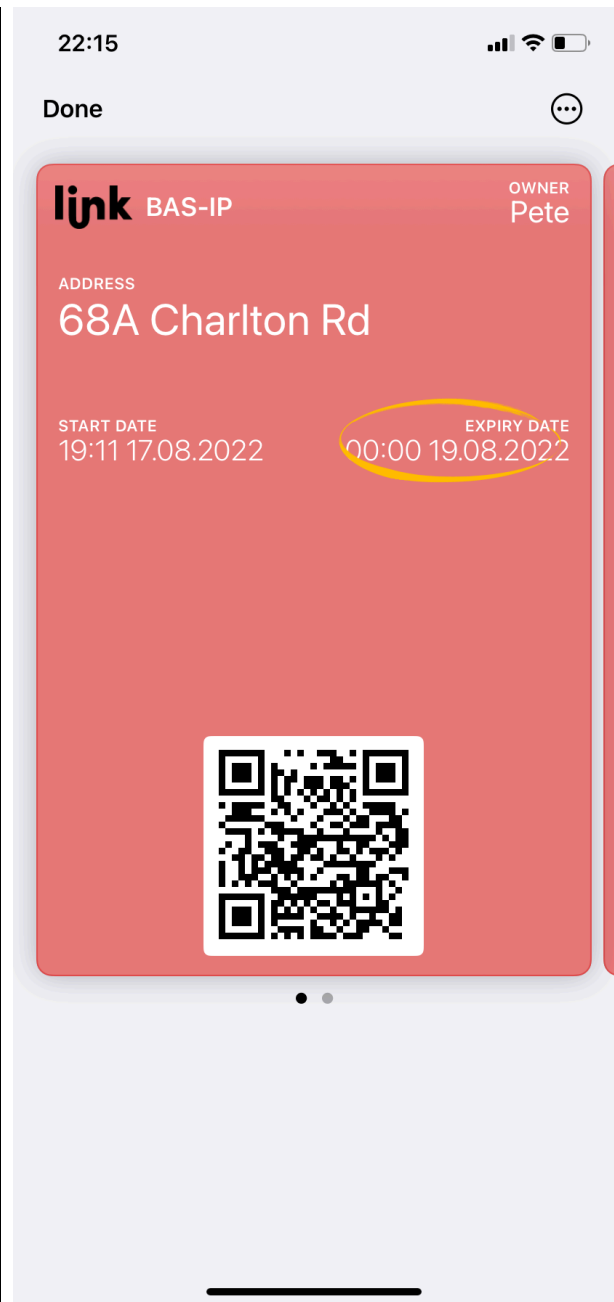
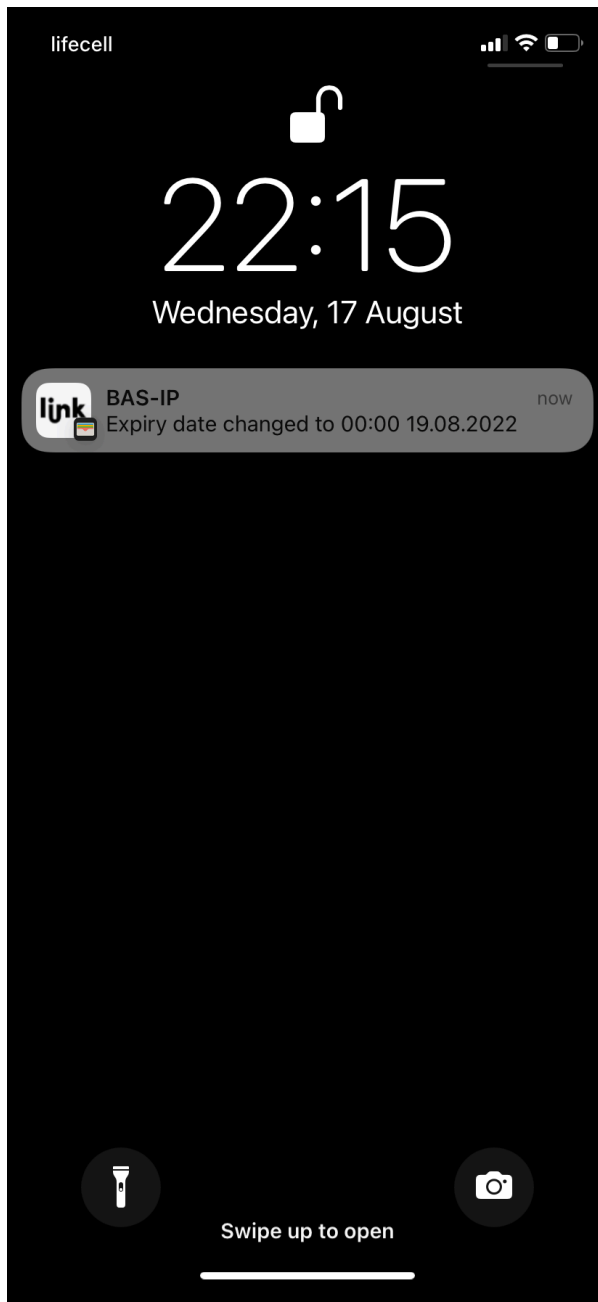
When you select a **QR-code** pass, you can share it as an image of the code and all the main information. Visitor can check all the necessary information (validity period, the number of available passes) and has to open it and show for entrance panel scanning.



In addition to the image, the QR code can be shared in a format for adding it to Apple Wallet if you/your visitor use **IOS**. When receiving a pass, a visitor must open it and press **Add** button. As a result, the visitor will get access to the pass by opening Apple Wallet.



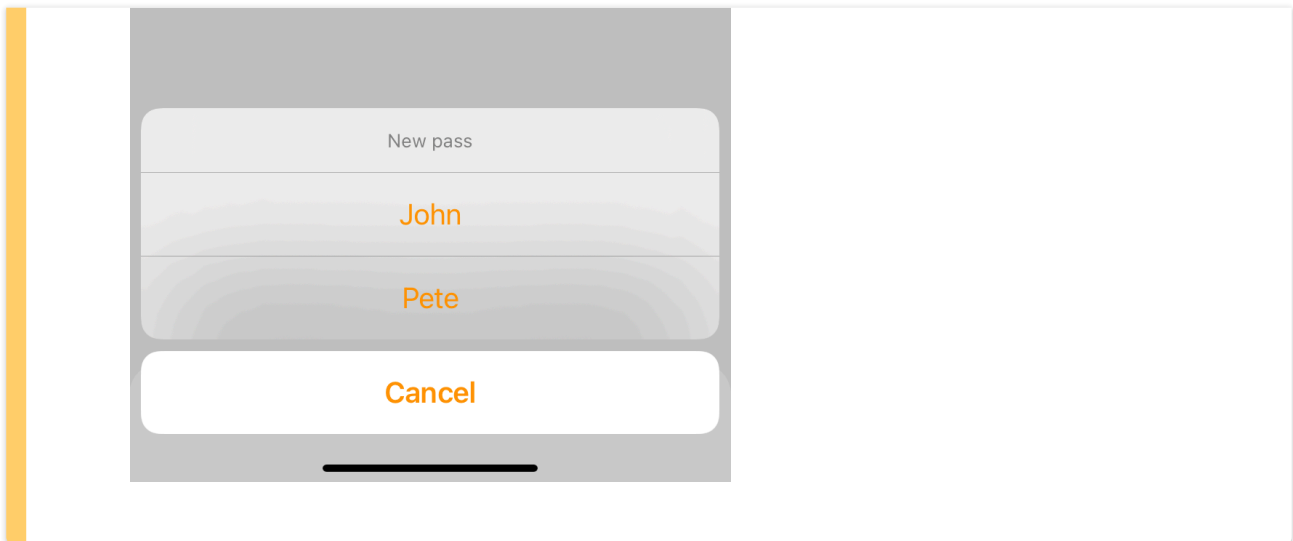
Also, if some changes about the pass are done on the Link server, the visitor will be notified about it and they will be automatically applied. So, there is no need to send another pass.



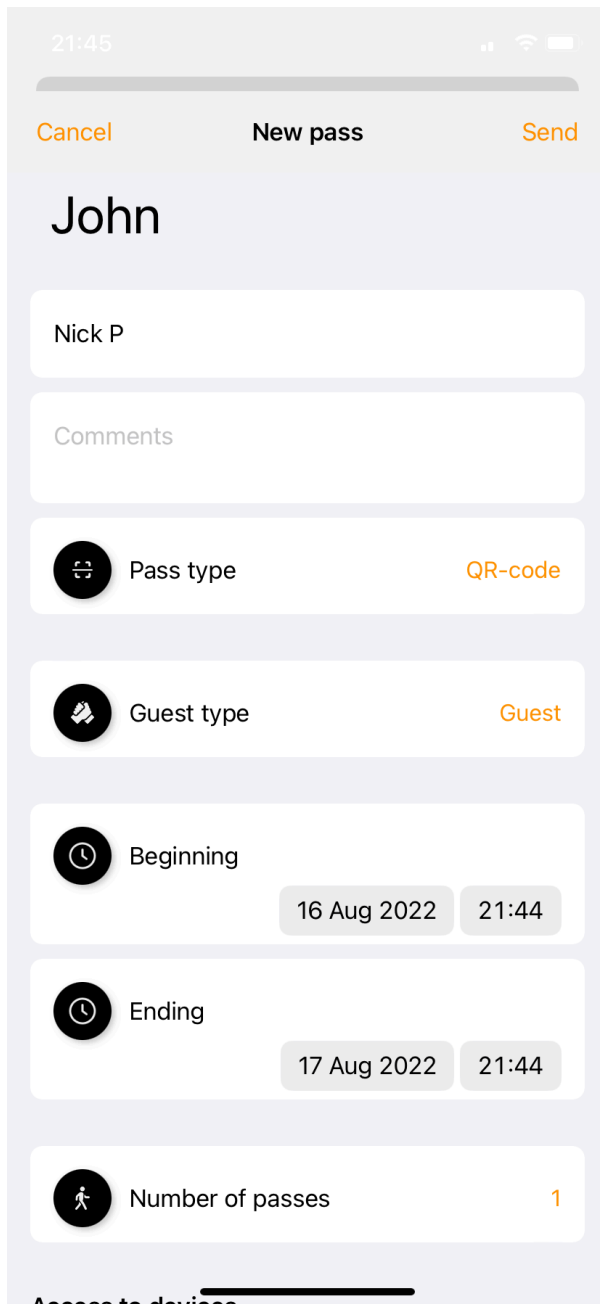
To **create a guest pass in the Link app**, a user must:

1. Press **Add pass** in the Passes tab.

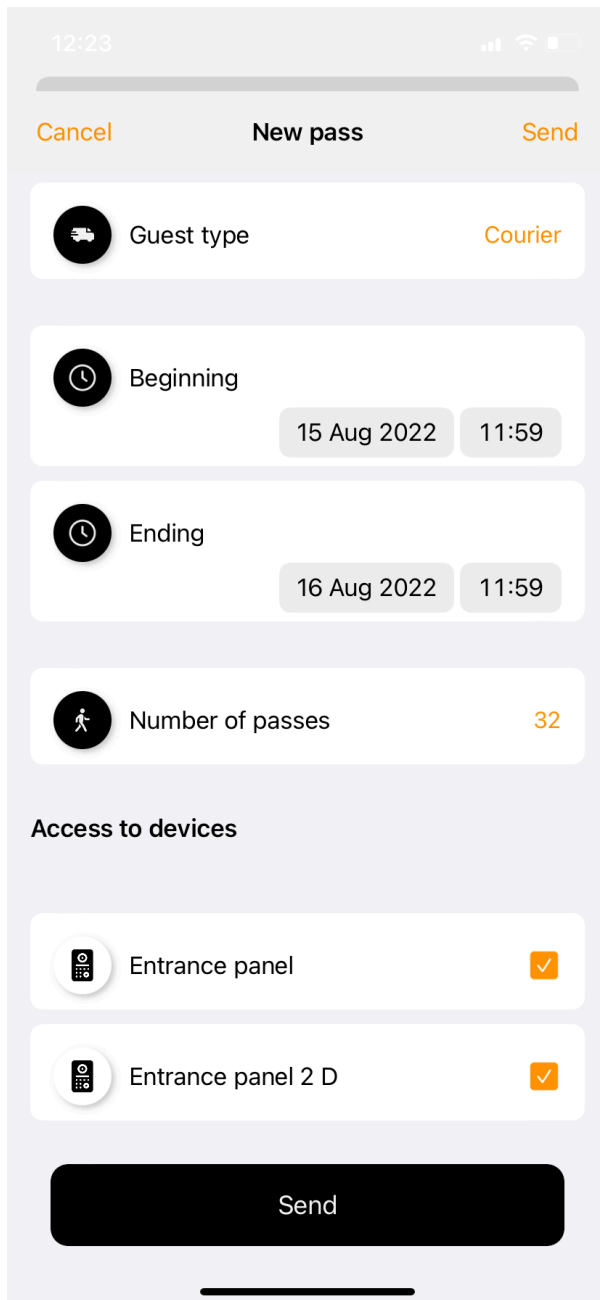
If several profiles are authorized with the app, select the profile want to use for pass creation.



2. Enter the owner **name** of this pass. If you skip a name, the app will generate it. You also may leave **comments** if necessary.
3. Select **pass type**: QR-code (available for panels with camera), Access code (available for panels with keypad), or URL (available for all devices).
4. Select **guest type**: Courier or Guest.
5. Indicate the **beginning** and the **ending** of the pass active period. By default, the pass works for 1 day.
6. If necessary, set the available **number of passes** for the identifier. By default, 1 pass is available.

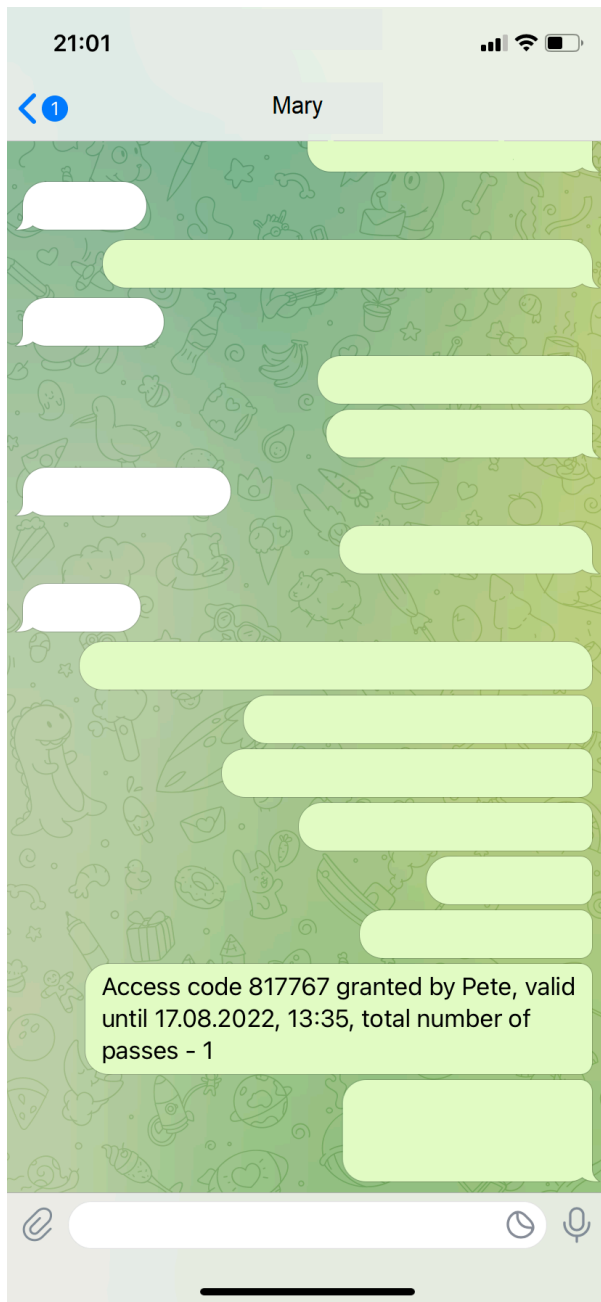


7. Select the devices to which you want to grant access. For example, the pass can open the door only to the unit only, or also to your apartment. By default, all devices are selected for pass opening.

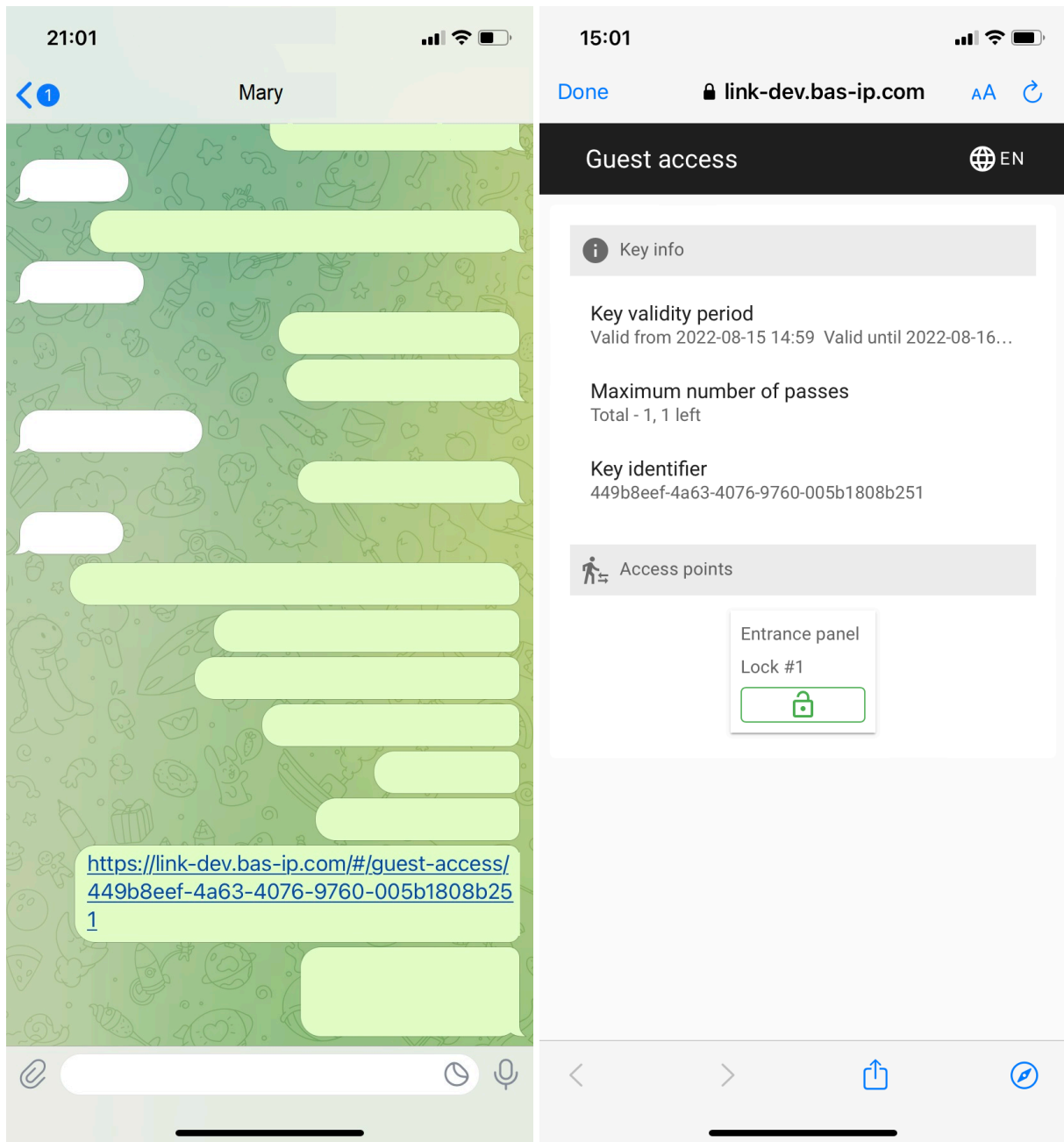


8. Press **Send** to share the pass via any messenger when all data will be entered.

You can send a pass via any messenger or e-mail after pressing **Send** button when creating a pass. When you select an **access code**, it will be generated in text with all the necessary information (validity period, the number of available passes) to open the lock.

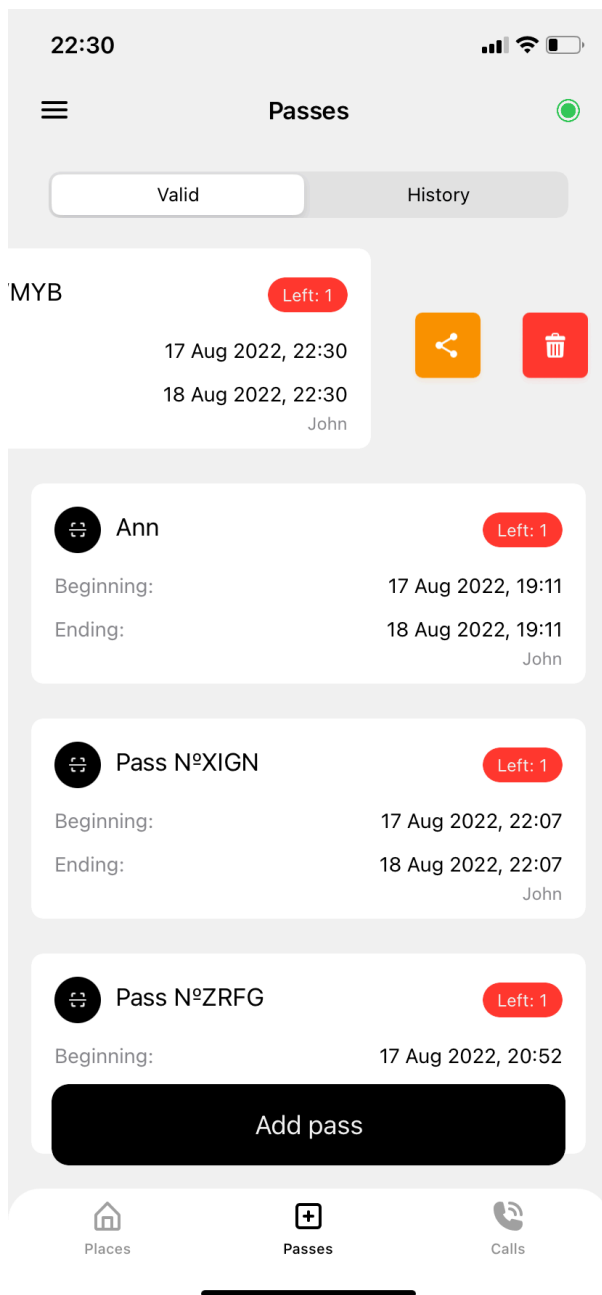



When you select a **link**, it will be generated in the URL. A visitor must open it to get information about the validity period, the number of available passes, and the ability to open the lock.

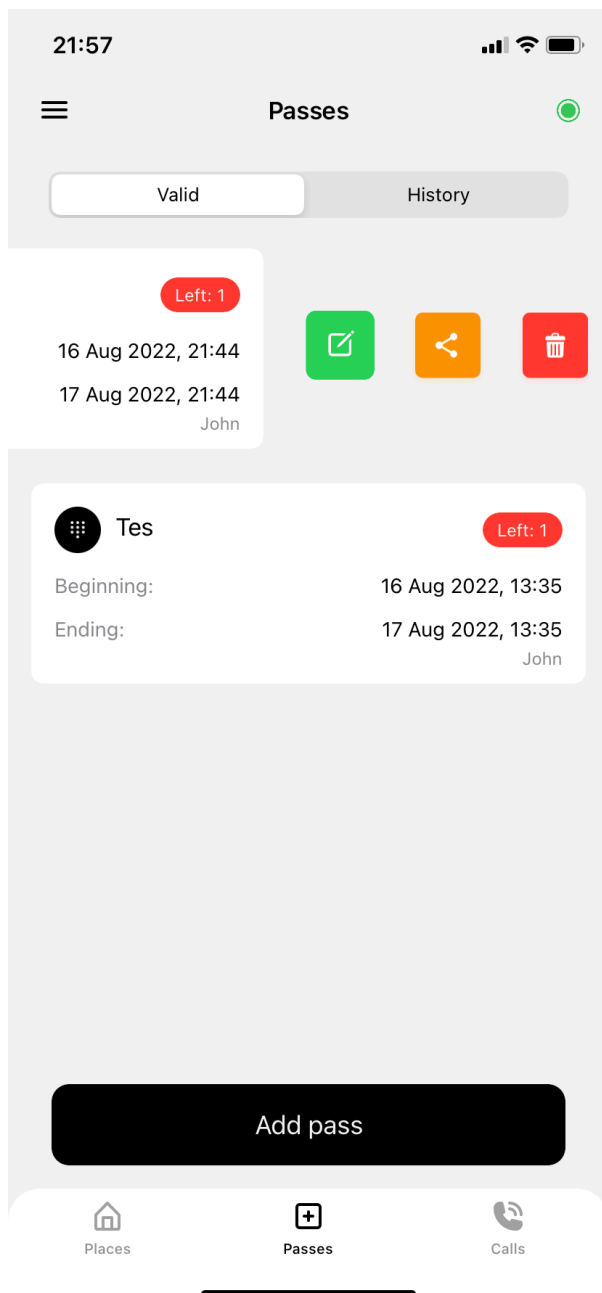


The process of sharing **QR codes** is described above (how to create a guest pass in the Link).

The other way to share the pass is to swipe it left and press share  button. Also you can delete  the pass.



For QR-code pass you can edit  guest type, pass active period, number of available passes and devices.



13.11 11. Link app usage.

BAS-IP Link app is a perfect addition to the Link software. Detailed information about all features you can read [here](https://wiki.bas-ip.com/basiplinkapp/bas-ip-link-110561562.html)¹⁴⁸. Here are the basic ones:

- a user has a list of available for them [places](https://wiki.bas-ip.com/basiplinkapp/places-110561623.html)¹⁴⁹ (property objects) with devices. They can watch a stream from entrance panels and/or monitors to check the situation at home or the office. Also, they can open the lock via Bluetooth, and call an elevator to the required floor.

¹⁴⁸ <https://wiki.bas-ip.com/basiplinkapp/bas-ip-link-110561562.html>

¹⁴⁹ <https://wiki.bas-ip.com/basiplinkapp/places-110561623.html>

Place/s displayed in the menu is a group/s to which the user is added on the Link server. All available **devices** are also added to the group together with the user. Also, access rules must be applied to the group for its display in the app;

- a user can [call a device](#)¹⁵⁰ from the list available or get a call from the other device;
- a user can provide [temporary identifiers](#)¹⁵¹ for visitors;
- a user can [open the lock](#)¹⁵² via Bluetooth;
- a user can [invite up to 5 family members](#)¹⁵³ to share the features of the app;
- a user can use the app for an [Apple watch](#)¹⁵⁴;

150 <https://wiki.bas-ip.com/basiplinkapp/accepting-making-calls-110561625.html>

151 <https://wiki.bas-ip.com/basiplinkapp/guest-passes-110561627.html>

152 <https://wiki.bas-ip.com/display/BASIPLinkapp/Profiles#Profiles-HowtoaddUKEYidentifier>

153 <https://wiki.bas-ip.com/display/BASIPLinkapp/Profiles#Profiles-Howtoaddafamilymember>

154 <https://wiki.bas-ip.com/basiplinkapp/app-for-apple-watch-110562156.html>

14 Link mobile app

BAS-IP Link app is a perfect addition to BAS-IP Link software. With this app, you can watch a stream from entrance panels and/or indoor video entry phones and monitor the situation at home or office. Also, the user can open the lock via Bluetooth, call an elevator to the required floor for you or your guests, and quickly create guest passes.

The use of BAS-IP Link software is obligatory for the app functioning.

The main functions:

- support of VoIP/push notifications for incoming calls;
- video stream from the panel/monitor camera before answering the call;
- possibility of registration/authorization on different Link servers;
- ability to add multiple devices;
- guest passes (QR-codes, access codes, and links) creation;
- calling the elevator (when the [EVRC-IP¹⁵⁵](#) module is used);
- opening the lock using UKEY (availability of UKEY identifier is required);
- availability of an archive with all calls;
- family members invitation.



For correct application functioning, especially for UKEY, you need to allow access to your location for permanent use, as well as activate Bluetooth on your smartphone. By giving permission to use the smartphone features, you agree to all the terms and conditions set forth in [the privacy policy¹⁵⁶](#).

The main menus and features are described here:

- [BAS-IP Link server preparation to the app¹⁵⁷](#)
- [Registration¹⁵⁸](#)
- [Authorization¹⁵⁹](#)
- [Places¹⁶⁰](#)

¹⁵⁵ <https://bas-ip.com/catalog/accessories/evrc-ip/>

¹⁵⁶ <https://www.bas-ip.com/privacy/>

¹⁵⁷ <https://wiki.bas-ip.com/display/BASIPLinkapp/BAS-IP+Link+server+preparation+to+the+app>

¹⁵⁸ <https://wiki.bas-ip.com/display/BASIPLinkapp/Registration>

¹⁵⁹ <https://wiki.bas-ip.com/display/BASIPLinkapp/Authorization>

¹⁶⁰ <https://wiki.bas-ip.com/display/BASIPLinkapp/Places>

- [Accepting/making calls](#)¹⁶¹
- [Guest passes](#)¹⁶²
- [Recent calls](#)¹⁶³
- [Settings](#)¹⁶⁴
- [Profiles](#)¹⁶⁵
- [App for Apple Watch](#)¹⁶⁶

161 <https://wiki.bas-ip.com/pages/viewpage.action?pageId=110561625>

162 <https://wiki.bas-ip.com/display/BASIPLinkapp/Guest+passes>

163 <https://wiki.bas-ip.com/display/BASIPLinkapp/Recent+calls>

164 <https://wiki.bas-ip.com/display/BASIPLinkapp/Settings>

165 <https://wiki.bas-ip.com/display/BASIPLinkapp/Profiles>

166 <https://wiki.bas-ip.com/display/BASIPLinkapp/App+for+Apple+Watch>